O Ecossistema de Cibersegurança em Portugal

Mestrado em Cibersegurança e Informática Forense

Vítor Manuel Sabino Morais

Dissertação realizada sob a orientação do Professor Doutor Mário João Gonçalves Antunes.

Leiria, Setembro de 2022

Originalidade e Direitos de Autor

A presente dissertação é original, elaborada unicamente para este fim, tendo sido devidamente citados todos os autores cujos estudos e publicações contribuíram para a elaborar.

Resumo

A cibersegurança ocupa um papel preponderante nos Estados modernos. A dependência dos sistemas de informação, agora transversais a toda a sociedade, torna a cibersegurança incontornável para qualquer país.

Atualmente, o ecossistema de cibersegurança nacional não se encontra tipificado e é difuso no que concerne às funções formais que cada entidade aí desempenha. Relativamente aos mecanismos de interoperabilidade existentes, são ainda bastante incipientes e, no seu estado atual, não permitem uma eficaz e eficiente troca de indicadores e conhecimento, como seria desejável. A tipologia de entidades que constituem o ecossistema de cibersegurança nacional, o normativo que as rege, a tipologia de informações e a dispersão de sistemas de informação com características ímpares, dificultam este processo.

Este tema, apesar de ainda não ter tido a atenção merecida por parte dos investigadores, granjeia, pelas suas características específicas e interesse nacional, toda a atenção e interesse no seu desenvolvimento.

A dissertação aqui apresentada versa sobre "O ecossistema de cibersegurança em Portugal". O ecossistema da cibersegurança é delimitado e caracterizado, sendo propostos mecanismos de interoperabilidade para a informação classificada e não classificada, o que inclui o tratamento, classificação e armazenamento da mesma. Finalmente, apresentam-se algumas sugestões de melhoria das soluções existentes.

A dissertação comporta uma análise densa e desafiadora do ecossistema de cibersegurança em Portugal, identificando-se um potencial interesse estratégico, tático e operacional para a comunidade de cibersegurança nacional.

Palavras-chave: Cibersegurança nacional, ecossistema de cibersegurança, MISP, normativo de cibersegurança, partilha de informação, classificação da informação.

Abstract

Cybersecurity occupies a leading role in modern states. Dependence on information systems, is now transversal to the whole of society, making cybersecurity unavoidable for any country.

Currently, the national cybersecurity ecosystem is not typified and is diffuse with regard to the formal functions that each entity performs in relation to the existing interoperability mechanisms, being quite incipient and, in their current state, not allowing an effective and efficient exchange of indicators of compromise and knowledge, as would be desirable. The typology of entities that make up the national cybersecurity ecosystem, the regulations that govern them, the typology of information and the dispersion of information systems with unique characteristics, make this process difficult.

This theme, despite not having yet received the attention it deserves from researchers, has, due to its specific characteristics and national interest, all the attention and interest in its development.

The dissertation presented here is about "The cybersecurity ecosystem in Portugal". The cybersecurity ecosystem is delimited and characterized, and interoperability mechanisms are proposed for classified and unclassified information, which includes its treatment, classification, and storage. Finally, some suggestions for improving existing solutions are presented.

The dissertation comprises a dense and challenging analysis of the cybersecurity ecosystem in Portugal, identifying a potential interest at strategic, tactical, and operational level for the national cybersecurity community.

Keywords: National cybersecurity, cybersecurity ecosystem, MISP, cybersecurity regulations, information sharing, information classification.

Índice

Lista de Figuras

Lista de tabelas

Lista de siglas e acrónimos

ADM	Armas de Destruição em Massa
AMT	Autoridade da Mobilidade e dos Transportes
ANAC	Autoridade Nacional da Aviação Civil
APT	*Advance Persistent Threat*
ASAE	Autoridade de Segurança Alimentar e Económica
AT	Autoridade Tributária
CCD	Centro de Ciberdefesa
CD	*Compact Disk*
CERT	*Computer Emergence Response Team*
CIRCL	*Computer Incident Response Center Luxembourg*
CISMIL	Centro de Informações e Segurança Militares
CMVM	Comissão do Mercado de Valores Imobiliários
CNCS	Centro Nacional de Cibersegurança
CNPD	Comissão Nacional de Proteção de Dados
CSIRT	*Computer Security Incident Response Team*
DDoS	*Distributed Denial of Service*
DIRCSI	Direção de Comunicações e Sistemas de Informação
DoS	*Denial of Service*
EMGFA	Estado-Maior General das Forças Armadas
ERSE	Entidade Reguladora dos Serviços Energéticos
ESTG	Escola Superior de Tecnologia e Gestão
EU	*European Union*
EUA	Estados Unidos da América
FA	Forças Armadas
GNR	Guarda Nacional Republicana
IoC	Indicadores de Comprometimento
IRS	Imposto sobre os Rendimentos Singulares
ISAC	*Information Sharing and Analysis Centers*
IXP	*Internet Exchange Point*

LOIC	Lei de Organização da Investigação Criminal
MISP	*Malware Information Sharing Platform*
MP	Ministério Público
NATO	*North Atlantic Treaty Organization*
OPC	Órgão(s) de Polícia Criminal
OTAN	Organização do Tratado do Atlântico Norte
PII	*Personal Identifiable Information*
PJ	Polícia Judiciária
PSP	Polícia de Segurança Pública
QNRCS	Quadro Nacional de Referência para a Cibersegurança
RGPD	Regime Geral de Proteção de Dados
RJSC	Regime Jurídico da Segurança do Ciberespaço
SEGNAC	Segurança Nacional das Matérias Classificadas
SIED	Serviço de Informações Estratégicas de Defesa
SIRP	Sistema de Informações da República Portuguesa
SIS	Serviço de Informações de Segurança
SOC	*Security Operation Center*
TI	Tecnologias de Informação
TLD	*Top-Level Domain*
TLP	*Traffic Light Protocol*
UE	União Europeia
UNC3T	Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica
USB	*Universal Serial Bus*

1. Introdução

O espaço cibernético, usualmente designado por ciberespaço, constitui-se como mais um espaço de soberania nacional. A crescente dependência dos Estados e das entidades que nele coexistem e aí desenvolvem atividade, torna a sua segurança crítica para o desenvolvimento económico e social [1]. A segurança do ciberespaço nacional depende de um conjunto de entidades, públicas e privadas, que, idealmente, devem constituir o que designaremos nesta dissertação como o "Ecossistema de Cibersegurança Nacional". Esta dissertação pretende definir e caracterizar este ecossistema, assim como sugerir metodologias de interoperabilidade a adotar, entre as entidades que o constituem, em segmentos considerados estratégicos para o bom funcionamento de um ecossistema com características próprias. Estas metodologias têm em vista permitir uma troca de informações entre as entidades da comunidade de cibersegurança, de acordo com os acessos a níveis de classificação de segurança da informação, permitindo que todas as entidades tenham acesso a informação de incidentes de cibersegurança (ciberincidentes) de acordo com a sua necessidade de conhecer.

1.1. Objetivos

O objetivo desta dissertação começa por, inicialmente, definir e caracterizar o ecossistema de segurança do ciberespaço nacional. Este ecossistema é constituído por um conjunto de entidades, públicas e privadas, como o Centro Nacional de Cibersegurança, o Centro de Ciberdefesa, o Serviço de Informações de Segurança, a Polícia Judiciária, as infraestruturas críticas e os prestadores de serviços essenciais e sensíveis, entidades empresariais e académicas e, até mesmo a população em geral, que desempenham missões específicas.

Neste momento, por não estarem plenamente conscientes da sua especificidade e das suas obrigações legais ou, inclusive, porque a legislação nacional e respetivas leis orgânicas não serem suficientemente claras, não interagem com a devida e necessária eficácia. Tal torna ineficiente a tão necessária partilha de indicadores de comprometimento (IoC) e de conhecimento, inviabilizando a constituição de um verdadeiro ecossistema de cibersegurança com características simbióticas.

Alguns estudos académicos e publicações tendem a concentrar a importância da partilha de informações em comunidades específicas [2], o que constitui, por si só, um bom ponto de

partida. Apesar de existirem características próprias em comunidades específicas, como por exemplo na comunidade das informações ou na comunidade bancária, a transversalidade da maioria dos ataques e o seu alcance, justificam que a partilha de indicadores seja acessível a todas as comunidades [3].

É este o desafio desta dissertação: disponibilizar um estudo transversal à comunidade alargada de cibersegurança e propor uma metodologia de partilha de informação e conhecimento, salvaguardando todas as especificidades dos respetivos agentes de cibersegurança, públicos e privados.

Definido e caracterizado o ecossistema, é necessário sugerir mecanismos de interoperabilidade entre entidades. A dispersão de sistemas e de metodologias de recolha, tratamento, análise e disseminação de informação é bastante complexo. Os mecanismos de interoperabilidade existentes, além de escassos, não demonstram a flexibilidade necessária para lidar com uma tipologia alargada de informação classificada e não classificada.

Atualmente, apenas um pequeno número de entidades troca informação de cibersegurança através de redes classificadas criadas para o efeito e pela via tradicional de documentação em suporte físico. Mesmo as entidades que legalmente devem reportar informação ao CNCS, como por exemplo, as instituições bancárias fazem-no através de *email* cifrado ou optam pela entrega de dados em suportes amovíveis (por exemplo, *pen* USB ou CD).

Acresce ainda que a classificação da informação manuseada e gerada nalgumas destas entidades não está apenas restrita à classificação de segurança nacional (SEGNAC), da União Europeia (EU) e da *North Atlantic Treaty Organization* (NATO), mas também a sistemas de classificação de informação específicos, como é o caso do *Traffic Light Protocol* (TLP) utilizado pela comunidade de grupos de resposta a incidentes de cibersegurança (*Computer Emergency Response Team* – CERT).

No âmbito dos informalmente designados quatro pilares da cibersegurança nacional, constituídos pelo Centro Nacional de Cibersegurança, pelo Centro de Ciberdefesa, pela Polícia Judiciária e pelo Serviço de Informações de Segurança, existem ainda classificações de segurança suplementares, nomeadamente o "segredo de justiça" e o "segredo de Estado". Uma parte desta especificidade foi estudada aquando do ataque terrorista às torres gémeas, nos Estados Unidos, por Joseph Pfeifer [4]. O autor verifica que, apesar de existir informação

que poderia prever o ataque de 11 de setembro de 2001, a inexistência de mecanismos eficientes de partilha de informação tornou os sistemas ineficazes.

Os desafios da partilha de informação têm sido estudados no âmbito da cibersegurança desde há pelo menos duas décadas. Em 2005, Olívia, L. M. [5] publicou um estudo onde apresentava estes desafios numa moldura não-técnica. No entanto, a vertente técnica é igualmente desafiante. Nesta perspetiva, Rantos *et al.* [6] apresentam os desafios das organizações quando decidem investir em sistemas eficazes e interoperáveis que permitam a partilha de informações de cibersegurança.

Face ao estado da arte dos mecanismos de interoperabilidade e de partilha de informação e conhecimento, que se encontram ainda num estado inicial, esta dissertação pretende sugerir a primeira metodologia de tratamento da informação classificada e sensível, que permita ser acedida de acordo com a legislação em vigor e com o princípio da necessidade de conhecer e, essencialmente, com vista a ancorar o paradigma da necessidade de partilhar, objetivo subjacente e enformador desta dissertação. Tanto quanto é do conhecimento do autor, com base na informação técnico-científica disponível sobre o tema, a metodologia aqui proposta, face à sua alta complexidade em termos das necessidades especificas de cada tipologia de entidade e de informação, é inovadora e não existia até à data da realização deste trabalho de investigação.

No âmbito desta dissertação sugere-se ainda uma plataforma de partilha de informação, baseada na *Malware Information Sharing Platform* (MISP), desenvolvida pela autoridade nacional de cibersegurança luxemburguesa (CIRCL). De acordo com a tipologia de utilizadores e respetivos acessos, propõe-se a constituição de uma galáxia de instâncias MISP que garantam uma troca de indicadores e conhecimento acionáveis por todos os integrantes do ecossistema nacional.

A utilização desta plataforma provou já ser de utilidade acrescida para os sistemas de partilha de indicadores de compromisso e de conhecimento. Wagner *et al.* estudaram a aplicação desta plataforma de partilha como mecanismo de prevenção em casos de fraude [7]. O sucesso desta experiência pode ser alavancado numa perspetiva multissectorial, o que se enquadra no âmbito proposto para esta dissertação. Note-se ainda que os mecanismos de anonimização de dados terão necessariamente de ser instituídos para níveis de acesso mais baixos ou para níveis de acesso onde a necessidade de conhecer não é imperativa, garantido

desta forma a proteção do emissor da informação face a outros utilizadores com os quais poderá ter, por exemplo, relações de concorrência no mercado.

Além dos desafios já enunciados, outro contributo desta dissertação é a potencial integração da informação contida em sistemas diversos e em várias entidades, em instâncias que permitam uma gestão adequada da informação. Os mecanismos automatizados de carregamento e extração de informação das instâncias MISP poderão ser desenvolvidos para este desiderato. O estudo efetuado por Barrete *et al.* [8] constitui um bom ponto de partida para escalar a problemática da partilha de informação interorganizações para uma escala nacional.

Finalmente, por forma a constituir uma base de conhecimento robusta, estruturada e relacionável com todos os outros sistemas, onde estejam armazenados dados de incidentes de segurança, indicadores de compromisso, investigações sobre ataques, caracterização de agentes de ameaça, entre outros elementos de informação, uma abordagem única à classificação de incidentes de segurança tem de ser obrigatoriamente adotada por todas as entidades constituintes.

Um bom ponto de partida é a taxonomia europeia dos CERT, já adotada por diversas entidades nacionais e europeias. Os modelos de pontuação inscritos na própria plataforma MISP são também uma mais-valia. O trabalho efetuado por Mokaddem *et al.* [9] lança a discussão sobre estes modelos e a vantagem da sua aplicação.

Como se verifica, apesar de existir a tecnologia necessária à implementação deste sistema, falta ainda uma conceptualização do ecossistema, metodologias de catalogação, tratamento e classificação de informação e, não menos importante, uma plataforma tecnológica que permita a troca e armazenamento de informação com segurança e resiliência a ataques informáticos.

Esta tema, embora seja a miúde comentado na comunidade de cibersegurança nacional, nunca mereceu uma análise nem uma proposta concreta, quer pela comunidade académica, quer pelas entidades que constituem a comunidade, quer pelo legislador.

1.2. Estudos existentes

Existem vários estudos que concorrem com uma visão específica para partes desta dissertação. De entre os diversos trabalhos académicos e publicações consultados, destacaram-se pela sua pertinência e acuidade os seguintes:

1. *Network Fusion Information and Intelligence Sharing for a Networked World* [4]

A ideia deste documento nasceu após o 11 de setembro de 2001, e centrou-se no facto de se ter chegado à conclusão que existia informação disponível, embora não partilhada, nos Serviços de Informações e socorristas nos EUA (*intelligence and first-responder communities*), que poderia ser utilizada para prevenir este famigerado ataque. Desta forma, o autor propôs um design inovador para partilha de informações e *intelligence* através da fusão de redes, o que incentiva a colaboração em várias disciplinas, aproveitando a tecnologia para ligar os não-ligados, nos níveis classificados e não classificados.

Segundo o autor, à medida que os terroristas passam para novos métodos de ataque, as autoridades responsáveis pela aplicação da lei e os *incident responders* devem usar informações abrangentes e oportunas para antecipar possíveis ameaças e garantir uma alta adaptabilidade nas respostas.

Este artigo define a fusão de rede, isto é, um sistema de partilha de informações que funde informações e *intelligence* de várias fontes para permitir que os decisores se adaptem melhor a um ambiente de ameaças em mudança. Este sistema assenta na criação de diversos *hubs* regionais, aos quais as entidades se podem ligar e inserir e consultar informação no sistema central. Apresenta, também, outras arquiteturas para conectividade no âmbito da segurança nacional nos EUA, de acordo com as tipologias de rede existentes (hierárquica, ligações co-localizadas, *hub-and-spoke* e *network fusion*) explora os desafios atuais da partilha de informações e *intelligence*, examina como a fusão de rede pode aprimorar os centros de fusão, com vista a ajudar os *incident responders* e forças e serviços de segurança e faz, ainda, várias recomendações para implementar a fusão de rede.

2. *Interoperability Challenges in the Cybersecurity Information Sharing Ecosystem* [6]

Este artigo aborda os desafios que as organizações enfrentam quando decidem investir na partilha de informações de segurança cibernética de forma eficaz e interoperável, categorizando-as, para tal, num modelo em camadas.

Aborda, ainda, os desafios de interoperabilidade que a comunidade enfrenta ao adotar soluções de partilha de informação específicas. Esses desafios decorrem principalmente da adoção de vários padrões, estratégias e políticas entre as partes interessadas, juntamente com restrições legais relacionadas à partilha de informações. O objetivo deste trabalho foi destacar pontos que impedem a ampla adoção da partilha de informações de segurança informática e a automação necessária do processo de partilha. De acordo com os autores, os analistas de segurança, se beneficiassem dessa automação, poderiam dedicar mais tempo à análise dos dados interoperáveis recolhidos, em vez de dedicar os seus esforços ao próprio processo de recolha. A interoperabilidade também é um meio de ampliar o espectro de partilha de informação e envolver mais partes interessadas no processo de intercâmbio, desenvolvendo assim um escudo global contra ameaças emergentes, com benefícios significativos para a comunidade.

A pesquisa realizada com base neste modelo provou que existe uma diversidade significativa na maneira como as informações de segurança informática são partilhadas pelas fontes envolvidas. Essa abordagem afeta diretamente a interoperabilidade, tanto na perspetiva da partilha como do consumo, como torna igualmente mais difícil para os analistas de segurança extrair efetivamente o conhecimento.

3. *Inter-Organization Information Sharing Systems* [8]

Este artigo aborda a utilização da plataforma MISP para partilha de conhecimento. De acordo com os autores, a comunidade de TI é confrontada com incidentes de todos os tipos e natureza e novas ameaças, que aparecem diariamente.

A partilha de informações sobre ameaças entre a comunidade tornou-se um elemento-chave na resposta a incidentes para conseguir manter patamares de segurança mínimos. Para tal, recursos de informações confiáveis que forneçam informações acionáveis, são, portanto, essenciais para a comunidade de TI, ou mesmo, em maior escala, para as comunidades judiciais, de *intelligence* ou grupos de deteção de fraudes, abordados como exemplo neste artigo.

Este documento apresenta o MISP e o projeto de partilha de ameaças, uma plataforma confiável, que permite a recolha e a partilha de indicadores de comprometimento (IoC) de ataques direcionados, mas também outras ameaças à segurança das informações, como

vulnerabilidades ou informações financeiras relacionadas e, ainda, indicadores utilizados em casos de fraude.

A implementação do MISP não é trivial e deve ser executada de acordo com as necessidades concretas dos destinatários e utilizadores. Este artigo fornece uma visão geral de sua implementação técnica tendo em conta as comunidades aqui selecionadas. O objetivo deste projeto foi fornecer uma plataforma na qual os atores de comunidades de TI públicas ou privadas pudessem partilhar informações e IoC sobre ameaças existentes de vários domínios, como a cibersegurança, finanças, etc., com vista a contribuir para uma melhor compreensão geral da segurança dos sistemas de informação.

Como tal, o objetivo do MISP é ajudar a estabelecer ações preventivas e contramedidas usadas contra esta tipologia de ataques direcionados. Uma destas ações preventivas é a deteção, por meio da partilha de conhecimento colaborativo, sobre *malware* existente e outras ameaças.

4. *Taxonomy driven indicator scoring in MISP threat intelligence platforms* [9]

De acordo com os autores, a comunidade de cibersegurança enfrenta uma mudança de tendência de grupos de trabalho fechados para abertos e de informações restritivas para a divulgação e partilha completa de informações.

Um recurso importante para essa mudança de tendência é o número de incidentes e vários IoC que aparecem diariamente, que só podem ser enfrentados e resolvidos de forma colaborativa. Partilhar informações é essencial para todos se manterem atualizados sobre as ameaças emergentes.

Para cobrir as necessidades de ter um meio de informação partilhado, diferentes iniciativas foram tomadas, e uma tem sido adotada por diversas entidades com bastante sucesso: a utilização da plataforma *Malware Information Sharing Platform* (MISP). No estado atual, esta plataforma de partilha e recolha tornou-se muito mais do que uma plataforma de partilha de informações sobre *malware*. Esta plataforma inclui todos os tipos de IoC, *malware* e vulnerabilidades, mas também informações sobre ameaças ou fraudes financeiras. Portanto, o volume de informações está a aumentar e a evoluir.

Neste artigo, os autores apresentam formas de implementar métodos de interação de dados distribuídos para MISP, seguidos por um modelo de pontuação genérico, para informações

históricas partilhadas nas comunidades MISP. Como os membros da comunidade MISP não têm os mesmos objetivos, são também discutidos casos de uso e implementações do modelo de pontuação.

1.3. Processo metodológico

O processo metodológico seguido nesta dissertação assenta em diversas fases que, de acordo com a especificidade da temática subjacente, irão variar desde um processo exploratório e de investigação até à conceptualização de metodologias, normativos, regras, arquiteturas tecnológicas e conceptualização de plataformas digitais que permitam atingir o objetivo desta dissertação.

Na primeira fase pretende-se dar a conhecer alguns fundamentos que concorrem para a definição de uma *framework* de partilha de indicadores de comprometimento e de criação de conhecimento, nomeadamente:

1. Definir e caracterizar os quatro pilares da cibersegurança nacional
    a. O Centro Nacional de Cibersegurança (CNCS)
    b. O Centro de Ciberdefesa (CCD)
    c. A Polícia Judiciária (PJ)
    d. O Serviço de Informações de Segurança (SIS)
2. Contextualizar e definir atores e respetivas funções para a prevenção em cibersegurança
    a. Consciencialização
    b. Formação para a literacia em cibersegurança
    c. Prevenção contra atos criminosos ou outros que ponham em causa o Estado de direito
3. Enquadrar a deteção de incidentes de Cibersegurança
    a. O papel do CNCS, do CCD, da PJ e do SIS
    b. As entidades do Estado
    c. As entidades privadas
    d. O funcionamento dos *Security Operation Centers* (SOC)
4. Enquadrar a reação a ciberincidentes
    a. O CERT.PT
    b. O sistema criminal
    c. O Serviço de Informações

d. Os CSIRT setoriais
e. A Associação Nacional de CSIRT
f. Proliferação de CSIRT

Na segunda fase, ir-se-á definir uma *framework* original de partilha de indicadores de comprometimento e de criação de conhecimento, desenvolvendo uma metodologia para implementar os mecanismos de interoperabilidade e respetiva plataforma de partilha. Pretende-se nomeadamente:

1. Determinar as condicionantes à circulação e partilha de informação e sugerir um método de partilha de informação, com base nos seguintes pontos:
    a. A classificação de segurança da informação
    b. O Segredo de Justiça
    c. O Segredo de Estado
    d. O *Traffic Light Protocol* (TLP)
    e. A taxonomia
    f. Sugerir a criação e dinamização de galáxias de partilha de informação (*Information Sharing and Analysis Centers* - ISAC)
2. Identificar e sugerir alterações à aplicação MISP para aplicação na *framework* proposta nesta dissertação.

Finalmente, esta dissertação descreve, através de exemplos concretos, a aplicação da *framework* e a sua aplicação à realidade nacional. São descritos exemplos dos fluxos de informação gerados entre entidades em três cenários distintos.

2. Fundamentos

Um Estado de direito democrático assenta o seu funcionamento com base em três pressupostos essenciais: justiça, segurança e defesa. Não me querendo alargar em torno dos conceitos inerentes, para os fins propostos nesta dissertação irei apenas debruçar-me sobre os agentes de ação principais, no âmbito do ciberespaço, nas vertentes da justiça criminal, da segurança interna e da defesa nacional.

A tipologia de agentes afetos a cada uma destas vertentes é variável de acordo com os sistemas e filosofias políticas adotadas por cada Estado. No entanto, existem grupos, mais ou menos estanques, com tipologias de função idênticas. Com vista a simplificar e a generalizar a aplicação destas propostas a qualquer realidade, foram constituídas doze categorias genéricas de entidades sendo elas:

1. Os serviços de informações (*intelligence services*);
2. As forças de segurança (*law enforcement*);
3. Os Centros Nacionais de Cibersegurança (*National Cybersecurity Centers*);
4. Os Centros Nacionais de Ciberdefesa (*National Cyberdefense Center*);
5. Os CERT nacionais (*National CERTs*);
6. Os CERT;
7. As infraestruturas críticas (*critical infrastructures*);
8. Os fornecedores de serviços essenciais (*essential service providers*);
9. A indústria de cibersegurança (*cybersecurity industry*);
10. Os centros de partilha de informação e análise de cibersegurança (*cybersecurity ISACs*);
11. A Academia (*academy*); e
12. Uma entidade genérica que engloba os restantes agentes de cibersegurança identificada com a designação “outros” (*others*).

No entanto, as cinco primeiras tipologias genéricas de entidades constituem, de facto, pilares essenciais da atuação do Estado no domínio da cibersegurança e da ciberdefesa. Em Portugal, decorrente das opções políticas efetuadas aquando da criação do Centro Nacional de Cibersegurança, optou-se pela integração do CERT nacional na estrutura do Centro

Nacional de Cibersegurança, reduzindo assim os cinco pilares essenciais a quatro estruturas destintas sobre as quais nos iremos focar na primeira parte deste trabalho.

O pilar dos serviços de informações, que atua no horizonte estratégico da segurança interna, numa perspetiva eminentemente preventiva e de apoio ao decisor político, é desempenhado pelo Serviço de informações de Segurança (SIS). O SIS é o único organismo com competência legal para atuar em Território Nacional no campo das informações.

O Sistema de Informações da República Portuguesa (SIRP) é constituído pelo Secretário-Geral do SIRP, pelo Serviço de Informações de Segurança e pelo Serviço de Informações Estratégicas e de Defesa (SIED). Existe ainda no campo dos serviços de informações o Centro de Informações Militares (CISMIL) que, tal como o SIED, não desempenham atividades no âmbito da Segurança Interna e, por tal, não serão focados numa perspetiva estrita do ecossistema de cibersegurança nacional, não obstante, numa perspetiva lata, concorrerem para a cibersegurança numa perspetiva externa (SIED) e de defesa (CISMIL).

No âmbito da justiça criminal o principal ator é de facto a Polícia Judiciária (PJ) tendo sob a sua alçada a maioria da criminalidade complexa e altamente organizada e a chancela de investigação de crimes de competência reservada a este órgão de polícia criminal.

Existem, porém, outros órgãos de polícia criminal (OPC) com competências de investigação nesta área, mas com maior pendor para a investigação de crimes de menor complexidade e, normalmente, sem implicações a nível da segurança nacional. Por este facto, entidades como a Polícia de Segurança Pública (PSP), a Guarda Nacional Republicana (GNR) e a Autoridade de Segurança Alimentar e Económica (ASAE), entre outras, desempenham igualmente um papel relevante no combate à criminalidade cibernética, mas orientada, maioritariamente, para a denominada pequena criminalidade.

Na esfera da defesa nacional, considerando duas situações de atuação destintas, de acordo com a determinação ou não de estados de exceção e, nomeadamente do estado de guerra, surge o Centro de Ciberdefesa (CCD).

Num estado de paz, o CCD atua como o *Computer Emergency Response Team* (CERT) das Forças Armadas (FA). Isto é, em situação de normalidade, o CCD acompanha, apoia e responde a incidentes de cibersegurança que incidam sobre os sistemas de informação dos ramos das Forças Armadas Portuguesas. Já quando o Estado de Guerra é declarado pelo Presidente da República, as suas funções passam a ser as de coordenador das atividades de

defesa a nível nacional e é a entidade responsável pelos esforços de resposta e atividade ofensiva cibernética do Estado Português.

Por último, não atuando diretamente em nenhuma das grandes áreas atrás focadas, mas contribuindo para todas elas em complemento às restantes entidades, erguer-se o Centro Nacional de Cibersegurança (CNCS).

De acordo com a estrutura atualmente vigente, o CNCS engloba as funções de Autoridade Nacional de Cibersegurança e, ainda, as funções de CERT nacional, o CERT.PT. Em tempo de normalidade, quando estados de exceção não estão em vigor, o CERT.PT coordena a atividade de defesa das entidades públicas e das infraestruturas críticas como entidade que recebe as comunicações de ciber incidentes previstos no Regime Jurídico do Ciberespaço Nacional e divulga alertas e indicadores de compromisso que concorrem para a cibersegurança do ciberespaço nacional. Já na sua qualidade de Autoridade, o CNCS é a entidade responsável por propor normativos nacionais de cibersegurança nas suas diversas vertentes e fiscalizar a sua adoção pelas entidades sob a sua alçada administrativa.

Com vista a uma visão mais precisa das dependências hierárquicas e respetivas interdependências, a Figura 1 esquematiza um organograma onde se apresentam alguns dos atores descritos anteriormente, assim como outros que, embora tenham um papel de coadjuvação, desempenham igualmente missões de extrema importância para a segurança e defesa do ciberespaço de interesse nacional.

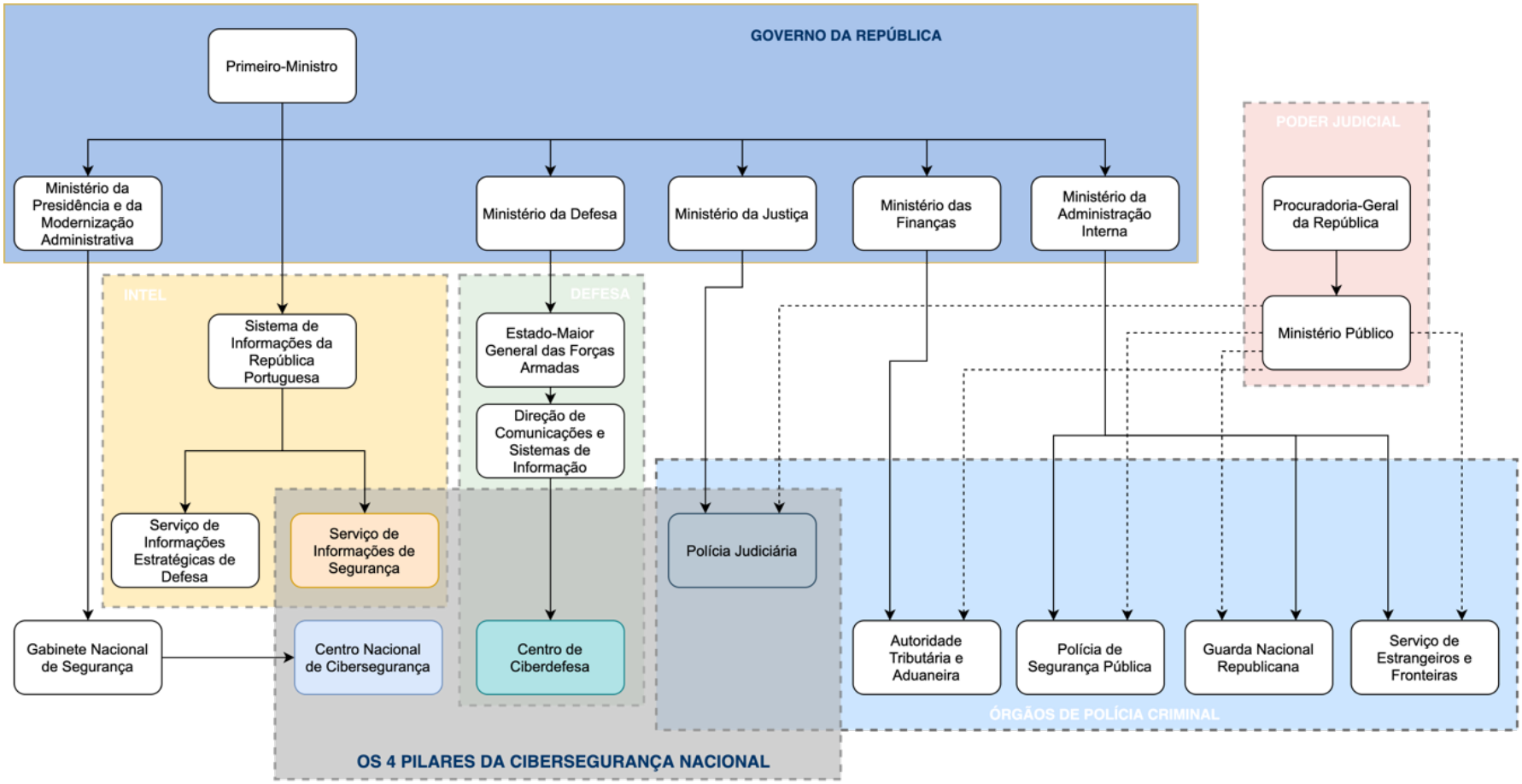

Figura 1 - Organograma de dependências hierárquicas

2.1. O Centro Nacional de Cibersegurança[1]

O Centro Nacional de Cibersegurança opera como coordenador operacional e autoridade nacional especialista em matéria de cibersegurança junto das entidades do Estado, operadores de Infraestruturas Críticas nacionais, operadores de serviços essenciais e prestadores de serviços digitais, garantindo que o ciberespaço é utilizado como espaço de liberdade, segurança e justiça, para proteção dos setores da sociedade que materializam a soberania nacional e o Estado de Direito Democrático. Nos termos do Decreto-Lei nº 136/2017, de 6 de novembro, o Centro Nacional de Cibersegurança funciona no âmbito do Gabinete Nacional de Segurança.

O Centro Nacional de Cibersegurança, tem por missão contribuir para que o país use o ciberespaço de uma forma livre, confiável e segura, através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional, em articulação com todas as autoridades competentes. Inclui ainda a implementação das medidas e instrumentos necessários à antecipação, à deteção, à reação e à recuperação de situações que, face à iminência ou ocorrência de incidentes ou ciberataques, ponham em causa o funcionamento das infraestruturas críticas e os interesses nacionais.

O CNCS possui as seguintes competências[10]:

a) Desenvolver as capacidades nacionais de prevenção, monitorização, deteção, reação, análise e correção destinadas a fazer face a incidentes de cibersegurança e ciberataques;

b) Promover a formação e a qualificação de recursos humanos na área da cibersegurança, com vista à formação de uma comunidade de conhecimento e de uma cultura nacional de cibersegurança;

c) Exercer os poderes de autoridade nacional competente em matéria de cibersegurança, relativamente ao Estado e aos operadores de infraestruturas críticas nacionais;

d) Contribuir para assegurar a segurança dos sistemas de informação e comunicação do Estado e das infraestruturas críticas nacionais;

[1] https://www.cncs.gov.pt

e) Promover e assegurar a articulação e a cooperação entre os vários intervenientes e responsáveis nacionais na área da cibersegurança;

f) Assegurar a produção de referenciais normativos em matéria de cibersegurança;

g) Apoiar o desenvolvimento das capacidades técnicas, científicas e industriais, promovendo projetos de inovação e desenvolvimento na área da cibersegurança;

h) Assegurar o planeamento da utilização não militar do ciberespaço em situação de crise ou de conflito armado, no âmbito do planeamento civil de emergência;

i) Coordenar a cooperação internacional em matérias da cibersegurança, em articulação com o Ministério dos Negócios Estrangeiros;

j) Exercer as demais competências que lhe sejam atribuídas por lei.

As competências acima descritas não prejudicam as atribuições e competências legalmente cometidas a outras entidades públicas em matéria de segurança do ciberespaço e é exercida em coordenação com estas, através de elementos de ligação, designados por Oficiais de Ligação, bem como em cooperação com entidades privadas que exerçam funções naquela matéria.

O CNCS atua ainda em articulação e estreita cooperação com as estruturas nacionais responsáveis pela ciberespionagem, ciberdefesa, cibercrime e ciberterrorismo, devendo comunicar à Polícia Judiciária, no mais curto prazo, os factos de que tenha conhecimento relativos à preparação e execução de crimes.

2.2. O Centro de Ciberdefesa[2]

O Centro de Ciberdefesa (CCD) é um órgão conjunto, inserido no Estado-Maior General das Forças Armadas, de agora em diante designado por EMGFA, é constituído por militares dos 3 ramos (Marinha, Exército e Força Aérea) e funciona como o braço das Forças Armadas no ciberespaço. Tem como missão garantir a integridade, confidencialidade e disponibilidade da informação e dos sistemas de informação da Defesa Nacional, essenciais ao exercício da

[2] https://www.defesa.gov.pt/pt/pdefesa/ciberdefesa/centro

nossa soberania, levando a cabo ações de defesa e, eventualmente, a criação de efeitos no, e através do, ciberespaço.

O CCD, é uma unidade integrada na Direção de Comunicações e Sistemas de Informação (DIRCSI), do EMGFA.

A DIRCSI tem por missão planear, estudar, dirigir, coordenar e executar as atividades inerentes aos sistemas de informação e tecnologias de informação e comunicação necessários ao exercício do comando e controlo nas Forças Armadas.

A DIRCSI, no âmbito da ciberdefesa, tem por missão coordenar a proteção dos valores da integridade, confidencialidade e disponibilidade da informação e dos sistemas de informação das Forças Armadas.

A DIRCSI tem ainda por missão, no âmbito da cibersegurança setorial da defesa nacional, coordenar a proteção dos valores da integridade, confidencialidade e disponibilidade da informação e dos sistemas de informação do restante universo da defesa nacional.

2.3. A Polícia Judiciária[3]

A Polícia Judiciária (PJ), tem por missão coadjuvar as autoridades judiciárias na investigação criminal que lhe esteja especificamente cometida pela Lei de Organização da Investigação Criminal (LOIC) ou que lhe seja delegada pelas autoridades judiciárias competentes.

A PJ tem as seguintes competências[11]:

a) Desenvolver e promover as ações de prevenção, deteção e investigação criminal da sua competência ou que lhe sejam cometidas pela Lei de Segurança Interna, pela Lei-Quadro da Política Criminal e pelas estratégias nacionais que definem os objetivos, as prioridades e as orientações de política criminal;

b) Realizar, enquanto entidade oficial, perícias e exames.

No plano da coadjuvação das autoridades judiciárias, a PJ assiste estas autoridades em processos relativos a crimes cuja deteção ou investigação seja da sua competência reservada

[3] https://www.policiajudiciaria.pt

ou que lhe seja cometida pelas autoridades judiciárias, bem como quando se afigure necessária, em qualquer fase processual, a prática de atos que requeiram conhecimentos ou meios técnicos especiais.

Neste sentido, a PJ atua no processo sob a direção das autoridades judiciárias e na sua dependência funcional, sem prejuízo da respetiva organização hierárquica e autonomia técnica e tática. Note-se que recentemente, foi criada na PJ a Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T) com especiais responsabilidades sobre a cibercriminalidade. De acordo com a legislação em vigor, a UNC3T é a unidade operacional especializada que dá resposta preventiva e repressiva ao fenómeno do cibercrime.

2.4. O Serviço de Informações de Segurança[4]

O Serviço de Informações de Segurança é um dos órgãos constituintes do Sistema de Informações da República Portuguesa (SIRP[5]).

O SIRP é o organismo público que tem a responsabilidade de prestar apoio ao decisor político, antecipando e avaliando as diferentes ameaças que visem Portugal e os seus interesses: a segurança interna e externa, a independência, os seus interesses nacionais, a integridade da unidade do Estado.

O SIRP, com as informações que produz, contribui para a salvaguarda, segurança e defesa desses mesmos interesses. Fá-lo numa vertente interna, pela ação do Serviço de Informações de Segurança e, numa vertente externa, onde conta com o Serviço de Informações Estratégicas de Defesa (SIED[6]). Nesta sua ação o SIRP respeita, observa e promove:

a) As prioridades que resultam das avaliações de ameaça;
b) As prioridades definidas na Diretiva de Informações, para a qual contribuem órgãos de soberania e instituições com responsabilidade nas áreas da defesa e da segurança;
c) As prioridades de política externa;
d) Os compromissos firmados em sede de Acordos e Protocolos internacionais;

[4] https://www.sis.pt
[5] https://www.sirp.pt
[6] https://www.sied.pt

e) As orientações que resultam das instituições internacionais de que Portugal é membro no respeito pelo princípio da soberania nacional e da subsidiariedade;
f) O seu papel como ativo estratégico tal como definido no Conceito Estratégico de Defesa Nacional;
g) O princípio da segurança cooperativa na luta contra o terrorismo, a criminalidade organizada internacional, o cibercrime, a sabotagem.

No âmbito do SIRP, o Serviço de Informações de Segurança (SIS), é o organismo incumbido da produção de informações que contribuam para a salvaguarda da segurança interna e a prevenção da sabotagem, do terrorismo, da espionagem e a prática de atos que, pela sua natureza, possam alterar ou destruir o Estado de direito constitucionalmente estabelecido. É neste conjunto de ameaças que se desenvolvem as suas competências em matérias de cibersegurança, ciberespionagem, ciberterrorismo e no combate ao cibercrime.

Ao SIS compete a produção de informações de segurança para apoio à tomada de decisão do Executivo, numa perspetiva preventiva, procurando antecipar fenómenos, conhecendo *a priori* as ameaças que se colocam à segurança coletiva e antecipando a tutela do Estado relativamente à investigação criminal.

Deste modo, compete-lhe recolher, processar e difundir informações no quadro da Segurança Interna, nos domínios:

- da sabotagem,
- do terrorismo,
- da espionagem, incluindo a espionagem económica, tecnológica e científica, e
- de todos os demais atos que, pela sua natureza, possam alterar ou destruir o Estado de direito democrático[7] .

Para executar a sua missão, o SIS tem o dever legal de *"acionar todos os meios técnicos e humanos (...) para a recolha e tratamento de informações"*[12], trabalhando sempre no pleno respeito dos direitos, liberdades e garantias fundamentais, constitucionalmente consagrados, bem como do quadro legal em vigor.

[7] Incluindo os movimentos que promovem a violência (designadamente de inspiração xenófoba ou alegadamente religiosa, política ou desportiva) e fenómenos graves de criminalidade organizada, mormente de carácter transnacional, tais como a proliferação de armas de destruição em massa, o branqueamento de capitais, o tráfico de droga, o tráfico de pessoas e o estabelecimento de redes de imigração ilegal.

O legislador foi aliás muito claro na distinção dos campos de ação das informações de segurança, comummente designadas pelo termo anglo-saxónico de *intelligence*, das da investigação criminal, criando, para as duas áreas, instrumentos distintos: o Sistema de Informações e o Sistema de Investigação Criminal.

Desta forma, o SIS desenvolve a sua ação, com vista a fazer face às seguintes ameaças:

a. Terrorismo Transnacional;
b. Espionagem clássica;
c. Espionagem económica;
d. Crime Organizado;
e. Extremismos ideológicos, religiosos;
f. Branqueamento de Capitais;
g. Tráfico internacional de Armas de Destruição em Massa (ADM) - Proliferação;
h. Tráfico de Seres Humanos e Migrações ilegais;
i. Cibercriminalidade;
j. Novas Formas de Crime.

2.5.Sumário

Como se pode constatar, existem doze categorias genéricas de entidades num ecossistema de cibersegurança, mas as cinco primeiras desempenham um papel essencial no âmbito da justiça, segurança e defesa. Essas cinco entidades no caso português, resume-se às quatro entidades caracterizadas neste capítulo uma vez que o CNCS engloba o CERT.PT.

Estas entidades serão aquelas com níveis de acesso mais elevado e com um maior conhecimento do ecossistema de cibersegurança em Portugal. Por tal, o CNCS e o CERT.PT, o CCD, o SIS e a PJ, serão entidades base neste ecossistema.

As restantes entidades, muitas delas com um caráter mais dinâmico no seu ciclo de criação e extinção enquanto entidades comerciais, entrarão e sairão do ecossistema com uma frequência muito superior às quatro aqui focadas que tendem a ser os pilares que garantem a cibersegurança e ciberdefesa do país.

Desta forma, uma caracterização destas quatro entidades torna-se essencial para um melhor entendimento dos fluxos de informação necessários à criação das galáxias e sistemas adiante sugeridos.

3. Framework proposto

O objetivo principal desta dissertação é a criação de uma *framework* de partilha de informação entre todos os agentes de cibersegurança que contribua, a montante, para a prevenção de incidentes de cibersegurança e, a jusante, para a reação e mitigação dos incidentes que não foram possíveis prever e evitar com as medidas de cibersegurança implementadas por cada organização.

Para este objetivo foram criadas tipologias base de entidades, designadas por **galáxias,** que cobrem a totalidade dos agentes de cibersegurança descritos no Capítulo 2, e que os categoriza por afinidade de missão e níveis de necessidade de acesso à informação.

No entanto, antes de mergulharmos na definição das galáxias, na sua interação e no acesso à informação constante num repositório centralizado ou distribuído, há que esclarecer as razões que sustentam a necessidade de desenvolver e disponibilizar esta *framework*.

A figura da prevenção em cibersegurança assume diversas formas de acordo com as funções e missões especificas de cada entidade. Embora a generalidade das entidades que concorrem para a formação do ecossistema de cibersegurança nacional desempenhe algumas ou todas as funções aqui apresentadas, apenas algumas têm funções especificas e legalmente enquadradas nesta matéria.

Desta forma, ir-me-ei debruçar sobre algumas funções de prevenção em cibersegurança e descrever, de forma breve, as razões, formas e objetivos destas funções no quadro da atividade da prevenção em cibersegurança.

3.1. Consciencialização em cibersegurança

O termo consciencialização pode ser definido como o ato de tomada de consciência sobre algo. A consciencialização é, em cibersegurança, uma matéria imprescindível uma vez que uma parte substancial da segurança dos sistemas de informação depende diretamente das ações dos respetivos utilizadores.

A tomada de consciência dos perigos cibernéticos é essencial para manter um nível mínimo de segurança. Os resultados do estudo sobre o Impacto da Vulnerabilidade Humana na Cibersegurança, de M. Alsharif *et al.* [13], demostra a falta de conscientização da

generalidade das pessoas sobre engenharia social (37%), media social (35%), *phishing* (30%), passwords (30%), uso de e-mail (22%), antivírus (33%) e proteção de dados (29%).

A consciencialização em cibersegurança (também designada por ciberconsciencialização) é um esforço coletivo e permanente de todos os agentes de cibersegurança. No entanto, recai especialmente sobre o CNCS, decorrente das suas atribuições legais, o dever de efetuar ações de consciencialização permanentes e sistemáticas a todos os utilizadores do ciberespaço.

3.2. Formação para a literacia em cibersegurança

Em complemento às ações de consciencialização, a formação para a literacia em cibersegurança é outro elemento essencial ao desenvolvimento de um ciberespaço seguro. O conhecimento dos perigos, dos riscos e das ameaças, por um lado, e das práticas e medidas de segurança na utilização, criação, desenvolvimento e manutenção dos sistemas de informação e dos serviços assentes em plataformas digitais, por outro, são igualmente de grande importância para a manutenção de um ciberespaço seguro.

Neste campo, o CNCS e a Academia (Instituições de Ensino Superior, Centros de Investigação e outros agentes do sistema de ensino em Portugal) desempenham um papel determinante no desenvolvimento e atualização de conteúdos e programas de formação que contribuam para o aprofundamento da literacia em cibersegurança. Note-se que este desiderato não é exclusivo destas entidades. Empresas e outras organizações da mais variada índole, devem igualmente contribuir para a literacia em cibersegurança através de formações específicas com o intuito de aumentar a sua própria segurança cibernética e, em consequência, aumentar a cibersegurança nacional.

3.3. Prevenção contra atos criminosos ou outros que coloquem em causa o Estado de direito

A prevenção em cibersegurança contra atos criminosos divide-se, *lato sensu*, em dois tipos: a prevenção geral e a prevenção criminal. A prevenção geral é aquela que visa prevenir a realização de atos criminosos antes da sua execução e que pode tomar as mais variadas formas, desde ações de consciencialização para a população em geral, até ações de esclarecimento específicas a uma entidade em particular. A prevenção criminal também

assenta as suas premissas na prevenção geral, sendo normalmente efetuada por agentes de prevenção criminal, nomeadamente os serviços de informações e as forças de segurança.

3.4. Enquadramento da deteção de incidentes de Cibersegurança

A deteção de incidentes de cibersegurança é um processo essencial para a segurança dos sistemas de informação e para a manutenção da operacionalidade e dos objetivos para os quais foram criados. Embora a deteção de incidentes *per si* seja uma atividade das equipas de cibersegurança de cada organização, a partilha de indicadores de comprometimento de forma célere e universal não é só desejável, mas uma ferramenta incontornável para a prevenção de ataques maliciosos.

De acordo com o Quadro Nacional de Referência para a Cibersegurança (QNRCS), detetar é a *"definição e implementação de medidas destinadas a identificar, de forma atempada, os incidentes. Ou seja, a deteção de eventos com um efeito adverso real na segurança das redes e dos sistemas de informação."* [14].

A deteção e o registo dos incidentes de cibersegurança, numa primeira fase, é extremamente importante para a correta avaliação do mesmo e para a preparação das fases seguintes. Desta forma, o registo e monitorização dos eventos de rede, dos sistemas e das aplicações é o primeiro passo. A recolha da informação situacional permite assim detetar anomalias. A disponibilidade de capacidades para descobrir ciberincidentes e comunicá-los de forma estruturada e célere às estruturas apropriadas é, como tal, de importância capital. No entanto, as ações de catalogação e armazenamento seguro de todos os indícios devem, igualmente, ser asseguradas como mecanismo de suporte à resposta a ciberincidentes e para a criação de conhecimento que melhorará o processo de deteção e a segurança como um todo.

3.5. Enquadramento da reação a ciberincidentes

De acordo com QNRCS, responder é a *"definição e implementação de medidas de ação apropriadas, em caso de deteção de um incidente. As medidas propostas no âmbito deste objetivo pretendem mitigar o impacto do incidente, ou seja, reduzir os seus potenciais efeitos adversos."* [14].

A reação ou resposta a ciberincidentes comporta, normalmente, duas fases essenciais: a contenção do incidente e a sua mitigação. Após se detetar um ciberincidente a prioridade

máxima é conter o seu impacto na organização por forma a evitar a sua possível propagação a outros sistemas e redes e, desta forma, evitar um dano maior como, por exemplo, a exfiltração de dados para fora da organização.

Na fase da contenção realiza-se uma triagem, que consiste em avaliar toda a informação recolhida até ao momento e procede-se a uma classificação e priorização do incidente em função da criticidade da informação e dos sistemas afetados. Em complementaridade, devem ser identificados possíveis impactos ao negócio e identificar as estruturas internas potencialmente afetadas para estabelecimento de canais de comunicação rápida. Simultaneamente, de acordo com a criticidade do incidente e a legislação vigente, devem ser contactadas autoridades e forças e serviços de segurança por forma a conter com a máxima celeridade e eficácia determinada tipologia de incidentes e melhorar o processo de deteção.

As medidas de mitigação, por seu lado, dependerão do tipo de incidente e, em certos casos, o contacto com fornecedores de serviços é desejável e recomendável.

3.6. As condicionantes à circulação e partilha de informação

Um dos principais obstáculos a ultrapassar na criação desta *framework* são as condicionantes à partilha de informação.

Inês Sofia de Oliveira, no seu artigo "*Challenges to Information Sharing, Perceptions and Realities*" [15], define a partilha de informação como a *"arte do possível"*. Este artigo levanta uma série de questões que obstam a uma partilha completa da informação entre diversos agentes e propõe um conjunto de recomendações balanceando e pesando a segurança com a continua proteção dos dados e da privacidade e, simultaneamente, mantendo a consistência com os princípios da necessidade e proporcionalidade.

Desta forma, são propostas as seguintes recomendações:

- Os regulamentos atuais devem ser clarificados e complementados com orientações adicionais, em resposta às preocupações expressas pelo sector privado de que são confusas e difíceis de compreender, de modo que a partilha de informações seja maximizada nos quadros existentes.
- As autoridades estatais devem fornecer uma melhor orientação aos seus sectores regulamentados, de modo que as quantidades excessivas de dados apresentados por

esses sectores e retidos pela aplicação da lei possam ser reduzidas, em conformidade com os conceitos de "necessidade" e "proporcionalidade".

- A legislação deve permitir a partilha de informações entre privados e privados de acordo com os princípios da "necessidade" e da "proporcionalidade".
- Deve ser mente ponderada a expansão do papel e das "competências" do sector privado no combate à criminalidade financeira, nomeadamente tendo em conta as expectativas crescentes de que o seu envolvimento na disrupção da criminalidade financeira possa vir a expandir-se. Isto deve incluir a possibilidade de partilha voluntária de informações.
- O sector privado deve rever as políticas e salvaguardas de proteção de dados para garantir aos clientes que as informações recolhidas para combater a criminalidade financeira não são utilizadas para outros fins.

No entanto, as recomendações aqui reproduzidas carecem ainda de uma visão mais ampla e que inclui todos os agentes de cibersegurança num ecossistema nacional e supranacional de combate à cibercriminalidade, mas, também, de criação e disseminação de IoC e de criação de conhecimento na forma de boas práticas e mecanismos de resposta e mitigação de ciberincidentes.

Partindo desta visão, há que ter em conta ainda legislação especial no domínio da classificação de segurança e da proteção da privacidade dos dados e da informação.

Esta *framework* tem em conta não só a legislação geral de proteção de dados, mas igualmente o normativo de segurança da informação, o segredo de justiça, o segredo de Estado e a própria dinâmica da concorrência num mercado livre.

3.7. Partilha de dados

Face aos condicionalismos anteriormente descritos, houve necessidade, numa primeira fase, de equacionar e definir criteriosamente os itens a partilhar e com quem os partilhar. Numa segunda fase foi necessário definir quais os sistemas a implementar para garantir que a informação certa chega às entidades certas e, finalmente, como partilhar esta informação.

3.7.1. O que partilhar

Ao nível da base, todas as entidades deverão ter acesso aos indicadores de comprometimento que lhes permita configurar sistemas de deteção e prevenção de intrusões e outros sistemas de prevenção com base em IoC. Estes dados deverão ser anonimizados e estarem protegidos dos intervenientes no incidente. Idealmente, todos os agentes de cibersegurança deverão ter acesso a estes dados que constituem a base da informação constante neste sistema de partilha.

3.7.2. Com quem partilhar

Esta é uma das questões mais complexas desta *framework*. A partilha de dados pelas entidades poderá ser de duas formas: genérica ou específica. Na forma genérica, não são definidos destinatários ou categorias de destinatários – galáxias – e a informação é automaticamente propagada pelas diversas entidades de acordo com os acessos previamente estipulados para a tipologia de entidade. Na forma específica, um conjunto de filtros terá de ser aplicado, nomeadamente, quais as entidades que podem aceder e a que tipo de informação estas podem aceder. O filtro de entidade poderá ser aplicado para tipologia de entidade, para entidades específicas e ainda, para regiões específicas, caso seja aplicado por diversos países ou regiões com, por exemplo, enquadramentos legais destintos. O filtro de informação poderá ser aplicado de forma genérica a todas as entidades ou, de uma forma mais precisa se o emissor entenda como necessário, a cada campo de informação constante no MISP.

Desta forma garante-se que o emissor controla totalmente a informação que insere podendo escolher a granularidade das entidades com quem partilha e a o nível de dados que partilha garantindo a salvaguarda e proteção dos sistemas e entidades envolvidas bem como os seus legítimos interesses comerciais quando estes existam.

3.7.3. Garantia de anonimização e proteção de dados pessoais

A anonimização e proteção de dados são garantidos pelos mecanismos constantes da MISP e, também, pela entidade que inserir os dados na aplicação para efeitos de partilha da informação.

Entidades com autorização legal e missões de soberania nacional poderão ter acesso aos dados dos intervenientes nos incidentes, quando devidamente autorizados, bem como acesso aos dados pessoais para os efeitos definidos nas respetivas legislações quando disponibilizados em sistema pelos originadores da informação.

3.8. Criação de repositórios de informação

Finalmente, tendo em conta todos os condicionalismos acima referidos, há que estabelecer as já mencionadas galáxias – tipologias genéricas de entidades – e o modo como comunicam entre si de acordo com o nível de acesso à informação tipificado para cada uma destas galáxias.

A Tabela 1 indica as tipologias genéricas, aplicáveis a qualquer Estado, e que agregam todos os agentes de cibersegurança:

Entity Type	Code
Intelligence Service	A1
Law Enforcement	A2
National Cybersecurity Center	A3
National Cyber defense Center	A4
National CERT	A5
CERT	B1
Critical Infrastructure	B2
Essential Service Providers	B3
Cybersecurity Industry	C1
Cybersecurity ISAC	C2
Academia	C3
Other	D1

Tabela 1- Tipologia de Entidades

Definidas as galáxias por tipologia, definiu-se os respetivos níveis de acesso à informação de acordo com o nível de credenciação de segurança e acesso a informação classificada. Estes acessos estão representados na Tabela 2:

	Security Clearance Level		
Entity Type	**National**	**European Union**	**NATO**
Intelligence Services	Top Secret	Top Secret	Cosmic Top Secret
Law Enforcement	Top Secret	Top Secret	
National Cybersecurity Center	Top Secret	Top Secret	
National Cyberdefense Center	Top Secret	Top Secret	Cosmic Top Secret
National CERT	Top Secret	Top Secret	
CERT	Secret		
Critical Infrastructures	Secret		

Essential Service Providers	Secret		
Cybersecurity Industry	Secret		
Cybersecurity ISAC	Confidential		
Academia	Confidential		
Other	Unclassified		

Tabela 2 - Níveis de acesso de segurança

Integrando no quadro anterior a proteção de dados pessoais, necessária para verificar quais as entidades que podem aceder a estes nos casos legalmente previsto, foi efetuado o quadro descrito na Tabela 3, com os níveis de credenciação e acesso aos dados pessoais por parte de cada entidade.

		Security Certification Level			Personal Identifiable Information (PII)
Entity Type	**Code**	**National**	**European Union**	**NATO**	**Access**
Intelligence Service	A1	Top Secret	Top Secret	Cosmic Top Secret	yes
Law Enforcement	A2	Top Secret	Top Secret		yes
National Cibersecurity Center	A3	Top Secret	Top Secret		yes
National Ciberdefense Center	A4	Top Secret	Top Secret	Cosmic Top Secret	yes
National CERT	A5	Top Secret	Top Secret		yes
CERT	B1	Secret			self-produced
Critical Infrastructure	B2	Secret			self-produced
Essential Services Providers	B3	Secret			self-produced
Cibersecurity Industry	C1	Secret			self-produced
Cibersecurity ISAC	C2	Confidential			self-produced
Academia	C3	Confidential			self-produced
Other	D1	Unclassified			self-produced

Tabela 3 - Níveis de credenciação e acesso a dados pessoais

Para coadjuvar a interpretação da Tabela 3, foram desenvolvidas duas árvores de decisão que indicam em que situações é legalmente obrigatório o reporte do incidente e a quem reportar:

Na árvore de decisão ilustrada na Figura 2 descrevemos o processo que integra as predisposições descritas nas Tabelas 1, 2 e 3. Desta forma, no caso de ser detetado um incidente de cibersegurança, esta árvore de decisão permitirá uma automatização de registo de acordo com o tipo de entidade, classificação de segurança da informação a remeter e, ainda, se existem informações pessoais.

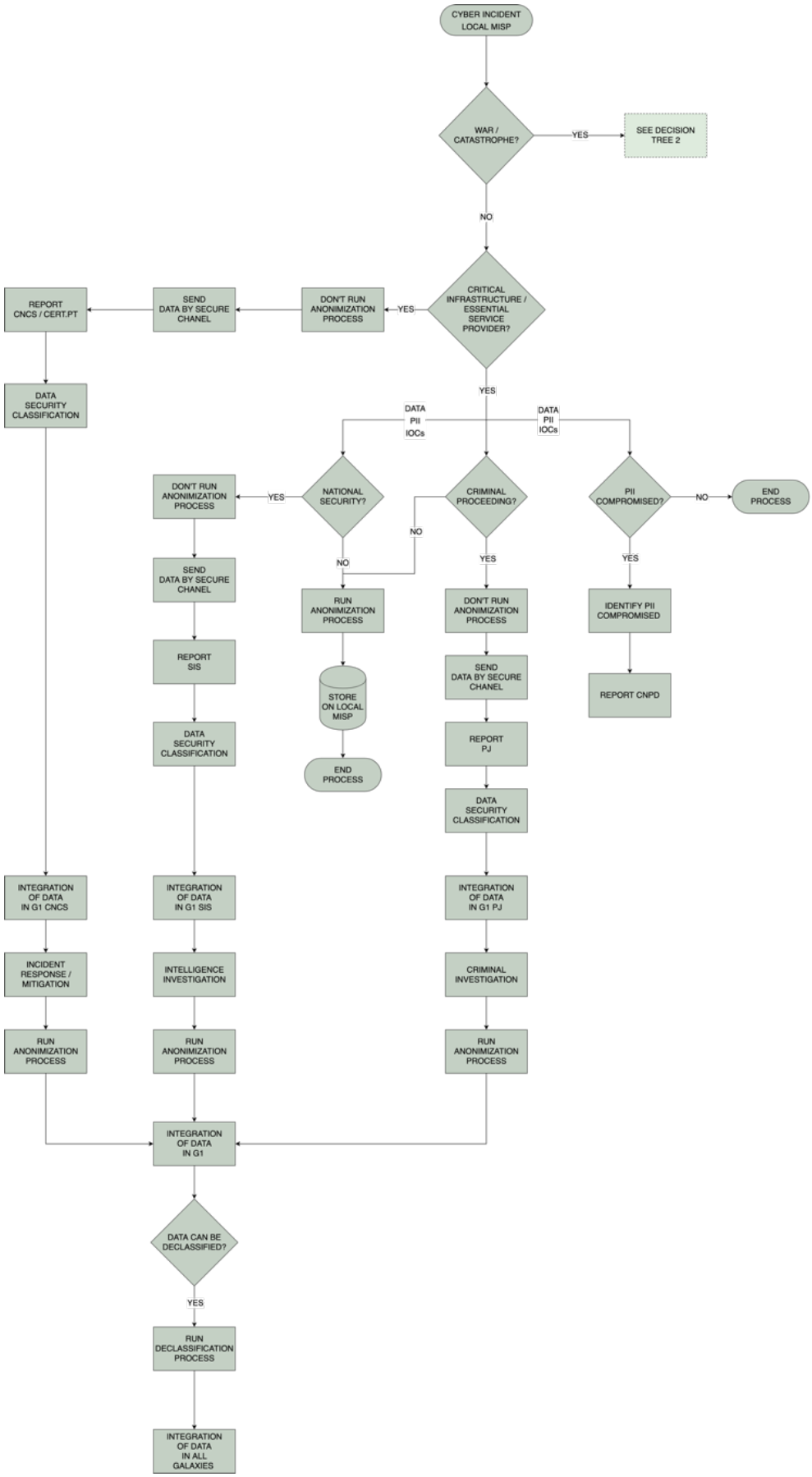

Figura 2 - Árvore de decisão 1 de nível de segurança e acesso a dados pessoais

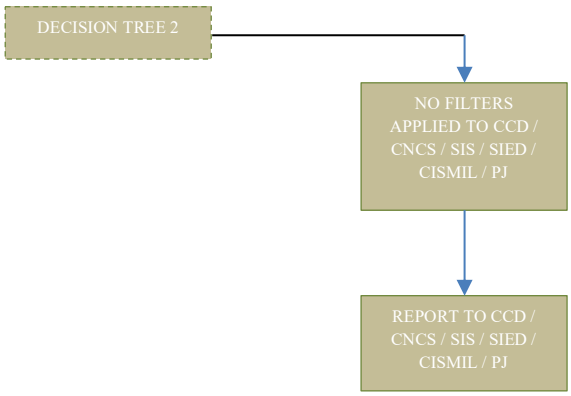

Figura 3 - Árvore de decisão 2 de nível de segurança e acesso a dados pessoais

Na Figura 3, descrevemos o processo simplificado a ser utilizado no caso de guerra. Neste estado de exceção, os quatro pilares da do ecossistema de cibersegurança em Portugal devem receber a informação integral, não filtrada, de todos os ciberincidentes a decorrer em Portugal. Desta forma, o acervo de informação angariada poderá ajudar a proteger contra as agressões externas e a responder de forma mais eficaz nos campos da defesa, segurança e justiça. Por último, esta informação será ainda usada como elemento crítico de apoio à decisão política e de defesa.

Neste momento temos disponíveis todos os dados necessários à criação de todas as galáxias para as entidades do ecossistema de cibersegurança em Portugal, incluindo as regras a aplicar para acesso a diferentes tipologias de dados. Este conjunto de definições e regras constituem a *framework* proposta para esta dissertação.

No entanto, foi ainda proposto inicialmente a criação de uma plataforma tecnológica que permita a aplicação desta *framework*. Como já foi referido anteriormente, a plataforma escolhida foi o MISP e para que a *framework* possa ser aplicada, foi efetuado um levantamento exaustivo dos campos constantes na aplicação e verificou-se quais os campos em falta para que esta *framework* possa ser implementada.

Note-se que no MISP, por se tratar de uma aplicação de código aberto livre, as alterações podem ser efetuadas com um nível de complexidade mínimo e com baixos custos de desenvolvimento.

O mapeamento de todos os campos e alterações necessárias podem ser consultados na íntegra, no Anexo A. Nessa Tabela é possível identificar o mapeamento de toda a informação

em falta no MISP atual, permitindo, desta forma, aplicar todas as regras de segurança da informação descrita nas Tabelas 2 e 3. O mapa apresenta ainda uma grelha de tipologias de entidades que permite a troca de indicadores de comprometimento e de conhecimento de acordo com o princípio da necessidade de conhecer, com a legislação em vigor, garantindo a segurança da informação e a sua otimização para a criação de conhecimento e aumento do nível de cibersegurança.

Note-se que, com a tabela do Anexo A, as equipas de desenvolvimento podem efetuar, com relativa facilidade, a implementação desta *framework* a uma versão *standard* do MISP, descarregada diretamente do repositório de acesso livre *online*. Uma vez que todos os campos foram mapeados e adaptados às condicionantes desta *framework*, a simples transposição desta tabela na reprogramação dos campos é relativamente simples e direta.

Com vista a um melhor entendimento do Anexo A, extraíram-se apenas dois campos ("ail-leak" e "ais-info") para exemplificar o mapeamento e alterações necessárias à totalidade dos campos existentes no MISP.

Na Tabela 4, verificamos que para os campos selecionados e para informação não classificada, todas as entidades têm acesso. Para a informação classificada como segredo de Estado, apenas as entidades constantes galáxia A1 têm acesso a esta informação. Para a informação classificada como segredo de justiça, apenas as entidades constantes na galáxia A2 podem aceder a esta informação. Para a informação classificada na marca[8] Nacional, verificamos que, de acordo com cada grau de classificação (*reserved, confidential, secret* e *top secret*), um número decrescente de galáxias têm acesso à informação (de acordo com o previamente estipulado na Tabela 2).

Security objects	**SHARING LEVEL**						
security-classification	Default Level			National			
	Unclassified	**State-Secret**	**Justice-Secret**	**Reserved**	**Confidential**	**Secret**	**Top-secret**
MISP objects							
ail-leak	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5
ais-info	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5

Tabela 4 - Acesso das galáxias a informação classificada na marca Nacional

[8] As designações "marca" e "grau de classificação" encontram-se definidas nas normas de segurança das matérias classificadas (SEGNAC). As marcas existentes são a Nacional, EU e NATO. Os graus de classificação variam de acordo com as marcas. Para a marca Nacional são: não classificado, reservado, confidencial, secreto e muito secreto. Para a marca EU são: *unclassified, reserved, confidential, secret* e *top secret*. Para a marca NATO são: *unclassified, reserved, confidential, secret, top secret* e *cosmic top secret*.

Na Tabela 5, estão representados os acessos das respetivas galáxias, mas agora para a marca União Europeia nos respetivos graus (*reserved, confidential, secret* e *top secret*) e para os campos selecionados.

Security objects	SHARING LEVEL						
security-classification	Default Level			Eurpean-Union			
	Unclassified	State-Secret	Justice-Secret	Reserved	Confidential	Secret	Top-secret
MISP objects							
ail-leak	ALL	A1	A2	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5
ais-info	ALL	A1	A2	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5

Tabela 5 - Acesso das galáxias a informação classificada na marca União Europeia

Na Tabela 6, verificamos quais as galáxias com acesso à informação classificada na marca NATO nos seus respetivos graus (*reserved, confidential, secret*, *top secret* e *cosmic top secret*).

Security objects	SHARING LEVEL							
security-classification	Default Level			NATO				
	Unclassified	State-Secret	Justice-Secret	Reserved	Confidential	Secret	Top-secret	Cosmic-top-secret
MISP objects								
ail-leak	ALL	A1	A2	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4
ais-info	ALL	A1	A2	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4

Tabela 6 - Acesso das galáxias a informação classificada na marca NATO

Na Tabela 7, aplicamos os níveis de acesso à informação constantes no *Traffic Light Protocol* (*white, green, amber* e *red*), maioritariamente utilizados pela comunidade CERT, e na última coluna se o campo contém informação pessoal para aplicação do preconizado na Tabela 3.

Security objects	SHARING LEVEL							
security-classification	Default Level			TLP				Contains PII
	Unclassified	State-Secret	Justice-Secret	white	green	amber	red	
MISP objects								
ail-leak	ALL	A1	A2	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
ais-info	ALL	A1	A2	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no

Tabela 7 - Acesso das galáxias a informação classificada pelo *Traffic Light Protocol* e identificação de PII

Após a criação da *framework* e a sua respetiva base tecnológica, com vista a um melhor entendimento da mesma, no sentido de exemplificar a sua aplicação a um Estado, efetuou-se um estudo de caso, tendo sido escolhido para este desiderato, Portugal. Assim, no próximo capítulo irei descrever a possível aplicação da *framework* à realidade portuguesa e às entidades que constituem o ecossistema de cibersegurança português.

4. Caso de Estudo – A aplicação do modelo a Portugal

Para este caso de estudo, foi selecionado o ecossistema português de cibersegurança como exemplo para a aplicação da *framework*. No entanto, o tipo de entidades e o apuramento de segurança necessários são semelhantes a nível global, em qualquer país. Assim, é razoável afirmar que esta *framework* poderia ser implementado em qualquer país com uma estrutura de cibersegurança semelhante (a maioria dos países europeus e norte-americanos), com as devidas alterações resultantes do enquadramento jurídico-legal em vigor. Esta *framework* poderia igualmente estender-se à partilha de IoC entre entidades em diversos países e jurisdições.

A aplicação da tipologia genérica de entidades ao caso nacional foi efetuada na Tabela 5. Estas entidades constituem o ecossistema nacional de cibersegurança e todas têm tarefas específicas no que diz respeito ao sistema nacional de cibersegurança.

GENERIC TYPE OF ENTITIES	CASE STUDY ENTITIES (PT)
INTELLIGENCE SERVICES	SIS
LAW ENFORCEMENT	PJ / PSP / GNR
NATIONAL CYBERSECURITY CENTER	CNCS
NATIONAL CYBERDEFENSE CENTER	CCD
NATIONAL CERT	CERT.PT
CERTs	CERTs
CRITICAL INFRASTRUCTURES	CRITICAL INFRASTRUCTURES
ESSENTIAL SERVICES PROVIDERS	ESSENTIAL SERVICES PROVIDERS
CYBERSECURITY INDUSTRY	CYBERSECURITY INDUSTRY
CYBERSECURITY ISAC	CYBERSECURITY ISAC
ACADEMIA	ACADEMIA
OTHERS	OTHERS

Tabela 8 - Aplicação das entidades genéricas à realidade nacional

Descrevem-se de seguida as entidades elencadas na Tabela 5. Os serviços de informações são responsáveis pela prevenção de ciberataques que podem colocar a segurança nacional em perigo. Concorrem igualmente para o processo de atribuição de ciberataques e para apoio aos decisores políticos. Os serviços de informações trabalham frequentemente de forma confidencial e a informação tratada por estes serviços não é apenas classificada a um nível de segurança elevado, mas também como a nível do Segredo de Estado.

As forças da segurança são responsáveis pelos procedimentos criminais que precedem um ataque. O principal objetivo é a prevenção criminal, parar o cibercrime e levar criminosos a tribunal. As forças de segurança também trabalham a um nível elevado de classificação de segurança e, num Estado de direito, sob a alçada do Segredo de Justiça.

As autoridades nacionais de cibersegurança trabalham num nível mais baixo de classificação de segurança. No entanto, em alguns casos, precisam de colaborar com os serviços de informações e com as forças de segurança e, por tal, precisam de ter acesso a dados classificados. Note-se que a maioria dos dados tratados pelas autoridades nacionais de cibersegurança não é classificada. No caso português, o CERT nacional faz parte da autoridade nacional de cibersegurança e, neste caso, o nível de autorização de segurança exigida deve ser o mesmo para ambos.

As autoridades nacionais de defesa cibernética, por definição, têm alta autorização de segurança. No caso português, atua como CERT das Forças Armadas, em tempos de paz, e como entidade de coordenação para a proteção do espaço cibernético nacional em tempos de guerra ou catástrofe.

As outras entidades, de acordo com a criticidade da segurança nacional, deverão ser catalogadas de acordo com a Tabela 3 de forma a ter acesso suficiente aos dados classificados, que possam ser utilizados para manter os canais adequados de partilha de informação entre todas as entidades do ecossistema, de acordo com o princípio da necessidade de saber.

O princípio da necessidade de saber, estabelece que cada entidade só deve ter acesso à informação que necessita de utilizar de acordo com as respetivas missões e competências legais. A Tabela 6 avalia a necessidade das principais entidades para aceder a cada um dos tipos de informação.

Desta forma, para cada coluna foi definido uma tipologia especial de atuação. Na primeira coluna verifica-se se dados pessoais foram comprometidos, na segunda coluna, se o incidente está abrangido pelo Regime Jurídico da Segurança do Ciberespaço (RJSC) [16], na quarta coluna, se a vítima apresenta queixa-crime, na quinta coluna, se o incidente tem implicações na segurança nacional e, finalmente, na sexta coluna, se estamos perante um estado de exceção.

Para cada caso especial, vemos na Tabela 6 quais as entidades que têm acesso à informação e competências legais para investigar os incidentes de cibersegurança específicos.

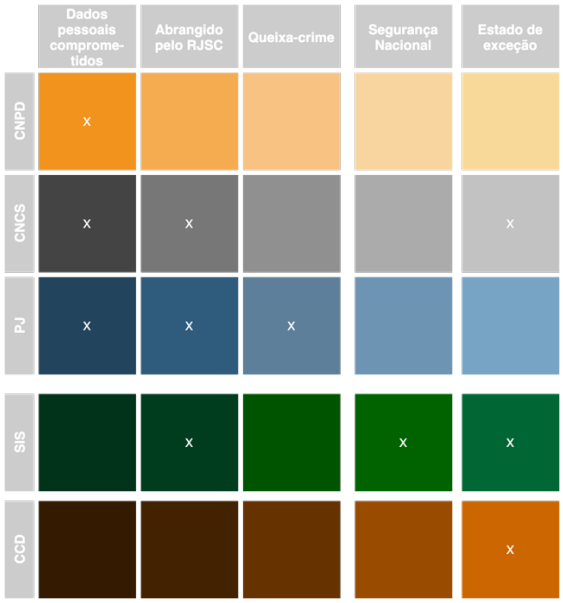

Tabela 9 - Acessos a informação classificada

4.1. Níveis de Autorização de Segurança

Cada tipo de entidade deve ter o nível recomendado de autorização de segurança para poder trocar e aceder aos dados que precisa de saber para melhor prevenir e se defender dos ataques aos seus próprios sistemas de informação.

Para o efeito, de acordo com a *framework* proposta, recomendamos que cada entidade seja integrada nos níveis de acesso elencados na Tabela 7.

	Security Clearance Level		
Entity Type	**National**	**European Union**	**NATO**
Intelligence Services	Top Secret	Top Secret	Cosmic Top Secret

Law Enforcement	Top Secret	Top Secret	
National Cybersecurity Center	Top Secret	Top Secret	
National Cyberdefense Center	Top Secret	Top Secret	Cosmic Top Secret
National CERT	Top Secret	Top Secret	
CERT	Secret		
Critical Infrastructures	Secret		
Essential Service Providers	Secret		
Cybersecurity Industry	Secret		
Cybersecurity ISAC	Confidential		
Academia	Confidential		
Other	Unclassified		

Tabela 10 - Níveis de autorização de segurança

Como se pode constatar na Tabela 7, existem diversas categorias de classificação de segurança de acordo com o originador da informação ou de acordo com o destinatário da informação. Simplificando, se a informação for originada em Portugal e se destinar apenas a entidades nacionais será classificada num determinado grau (*unclassified, confidential, secret, top secret*) na marca Nacional. O mesmo se passa com as restantes marcas (EU e NATO) no âmbito destas organizações. Note-se que se uma informação for originada em Portugal e tiver de ser difundida para uma destas instituições, passará a ter uma dupla ou tripla classificação de segurança.

4.2. Plataforma de partilha de informação de *malware*

O MISP, de acordo com os programadores, é *"uma plataforma de partilha de informações de ameaça, que armazena e correlaciona indicadores de comprometimento, de ataques direcionados, de agentes de ameaça, de informações sobre fraude financeira, de informações sobre vulnerabilidades ou, até mesmo, de informações contra o terrorismo"* [17].

O MISP (https://www.misp-project.org), como descrito, é uma plataforma de partilha, de código aberto livre, amplamente utilizada por vários CERT e organizações em todo o mundo. Embora tenha sido construído para partilhar informações não classificadas e para anonimizar

informações pessoais identificáveis, certos tipos de entidades, no entanto, precisam de aceder a este tipo de informação. É o caso dos serviços de informações e das forças de segurança.

Existem disponíveis outras plataformas no mercado, sendo que as com funcionalidades semelhantes são *software* comercial que requer licenças de utilização. O MISP, no momento da realização desta dissertação, é a plataforma que apresenta um rácio custo-benefício claramente superior e, acresce, que já é utilizado por um conjunto de organizações em todo o mundo (por exemplo, a comunidade CERT internacional, e comunidades com níveis de maturidade bastante elevadas com as instituições bancárias nacionais e internacionais). Por último, o MISP encontra-se num patamar de desenvolvimento muito avançado que responde quase na totalidade aos requisitos propostos para esta dissertação.

Para tal, o MISP deve ser manipulado apenas para aplicar estes mecanismos a determinadas entidades. Para as entidades que necessitem de aceder a esta informação, depois de autorizadas pelo titular dos dados e se estiver em conformidade com a legislação nacional, o MISP deverá permitir o acesso a este tipo de dados.

Tendo isto em conta, deve ser implementado o código para cada tipo de entidade no processo de decisão para a anonimização, descrito na Tabela 8. Deverão igualmente ser incluídas as arvores de decisão apresentadas nas Figuras 2 e 3 (Secção 3.8).

Entity Type	Code
Intelligence Service	A1
Law Enforcement	A2
National Cybersecurity Center	A3
National Cyber defense Center	A4
National CERT	A5
CERT	B1
Critical Infrastructure	B2
Essential Service Providers	B3
Cybersecurity Industry	C1
Cybersecurity ISAC	C2
Academia	C3
Other	D1

Tabela 11 - Tipo de entidades

Como se pode constatar na Tabela 8, as entidades estão classificadas com quatro códigos destintos (A, B, C e D). As entidades com o código A, são os designados pilares da cibersegurança e com os maiores níveis de acesso (serviços de informações, forças de

segurança, centros nacionais de cibersegurança, centros nacionais de ciberdefesa e CERT nacionais). As entidades com o código B, são as entidades consideradas críticas e sensíveis (CERT, infraestruturas críticas e provedores de serviços essenciais) e com acesso a informação classificada de nível intermédio. As entidades com o código C, são as entidades que têm acesso a informação num nível de classificação mais baixo, mas que ainda necessitam de ser credenciadas para o efeito. Finalmente, as entidades com o código D, que são a grande generalidade das entidades, apenas tem acesso a informação não classificada.

Outro requisito consiste na classificação de segurança da informação. Conforme apresentado na Tabela 7, cada entidade deve ter um nível de autorização de segurança predefinido. O conteúdo da Tabela 7 deve também integrar com o processo de decisão, antes da informação ser distribuída pela comunidade dentro ou fora da respetiva galáxia. Para implementar este processo no MISP, deverá ser aplicado o preconizado na tabela constante no Anexo A.

A tabela constante no Anexo A mapeia os objetos MISP com os níveis de acesso de cada entidade antes do processo de anonimização e classificação de segurança. Note-se que o proprietário dos dados deve primeiro dar permissão de acesso específico e *ad-hoc* a cada entidade antes do início do processo. Com esta autorização, o titular dos dados pode dar acesso a uma entidade específica, a um objeto específico ou a uma peça específica de *Personal Identifiable Information* (PII), de acordo com a lei e face à necessidade de conhecer.

4.3. Criação das galáxias

As galáxias são entidades que partilham objetivos ou missões comuns, e devem ter o mesmo nível de acesso. As galáxias foram criadas a partir das tipologias base de entidades que cobrem a totalidade dos agentes de cibersegurança descritos no Capítulo 2, e que os categoriza por afinidade de missão e necessidade de informação

De acordo com a Tabela 9 e a aplicação da restante *framework*, o modelo prevê doze galáxias principais, sendo que cada galáxia contém um ou mais tipos de entidades.

Algumas galáxias devem ter privilégios e acessos especiais devido à natureza da sua missão legal. É o caso da galáxia de informações, da galáxia das forças de segurança e das galáxias nacionais de cibersegurança e defesa cibernética. Note-se, no entanto, que apesar de algumas entidades poderem aceder a todos os dados dentro da sua galáxia, devido ao princípio da

necessidade de conhecer, apenas as entidades que são autorizadas pelo originador ou proprietário dos dados podem aceder a essa informação (Tabela 9).

		Security Certification Level			Personal Identifiable Information (PII)
Entity Type	**Code**	**National**	**European Union**	**NATO**	**Access**
Intelligence Service	A1	Top Secret	Top Secret	Cosmic Top Secret	yes
Law Enforcement	A2	Top Secret	Top Secret		yes
National Cibersecurity Center	A3	Top Secret	Top Secret		yes
National Ciberdefense Center	A4	Top Secret	Top Secret	Cosmic Top Secret	yes
National CERT	A5	Top Secret	Top Secret		yes
CERT	B1	Secret			self-produced
Critical Infrastructure	B2	Secret			self-produced
Essential Services Providers	B3	Secret			self-produced
Cibersecurity Industry	C1	Secret			self-produced
Cibersecurity ISAC	C2	Confidential			self-produced
Academia	C3	Confidential			self-produced
Other	D1	Unclassified			self-produced

Tabela 12 - Níveis de acesso a informação classificada e dados pessoais

A aplicação desta *framework* pode ser adotada em duas modalidades: o modelo compreensivo e o modelo simplificado. No modelo compreensivo, a integralidade da *framework* é aplicada de forma específica a cada entidade e, no modelo simplificado, a *framework* é aplicado a uma tipologia genérica de entidade para facilitar a sua interpretação e compreensão neste caso de estudo.

Desta forma, no modelo compreensivo, a aplicação da *framework* ao caso de Portugal produziria as seguintes galáxias:

Modelo compreensivo

1. Galáxia 1 – Serviços de Informações (G1)

   Esta galáxia, no caso português, integra os três serviços de informações previstos na legislação nacional: o SIS, o SIED e o CISMIL (Figura 8). Como já foi anteriormente explicado, apenas o SIS desempenha funções de segurança interna, mas, no entanto, o acesso à informação contida nesta galáxia pode e deve ser utilizado para a nossa segurança externa, pelo SIED, e para efeitos de defesa no caso do CISMIL.

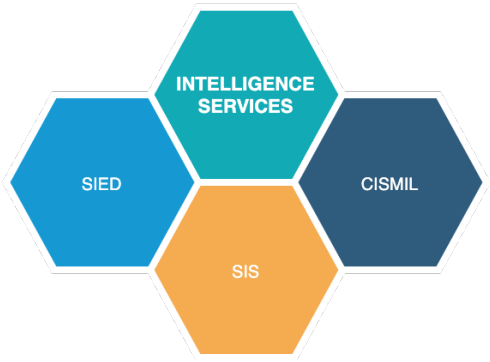

Figura 4 - Galáxia dos Serviços de Informações

2. Galáxia 2 – Forças de Segurança (G2)

A galáxia das Forças de Segurança está ilustrada na Figura 9 e integra a Polícia Judiciária, a Polícia de Segurança Pública e a Guarda Nacional Republicana. No âmbito de um processo crime, cabe ao juiz decidir qual das polícias efetua as diligências de investigação ou recolha de prova. Assim, no mesmo processo, podem ser ativadas várias polícias para este efeito.

Figura 5 - Galáxia das Forças de Segurança

Neste caso, duas abordagens podem ser utilizadas:

- Todas as Forças de Segurança têm acesso integral a esta galáxia;
- Apenas as Forças de Segurança que efetuam diligências num respetivo processo-crime acedem à informação pertinente de acordo com o princípio da necessidade de conhecer e de acordo com os trâmites legais constantes do processo penal e o segredo de justiça.

A primeira abordagem, apesar de dar mais garantias de informação aos investigadores e um melhor contexto com acesso a casos semelhantes ou

relacionados, terá de obrigar a um maior controlo por parte do Ministério Público às diligências efetuadas.

A segunda abordagem, já tem à partida um maior controlo automático, mas não permite aos investigadores uma visão mais ampla da situação o que poderá levar a limitações importantes no decurso da investigação e nos resultados obtidos.

3. Galáxia 3 – Autoridade Nacional de Cibersegurança (G3)

A galáxia da Autoridade Nacional de Cibersegurança em Portugal está descrita na Figura 10. Trata-se de uma galáxia simples e encontra-se facilitada, uma vez que o CERT.PT está integrado no Centro Nacional de Cibersegurança – a Autoridade Nacional de Cibersegurança.

Figura 6 - Galáxia da AN Cibersegurança

Neste caso, o fluxo de informação e acesso à mesma é indiferente devido a esta integração, não sendo necessária a criação de acessos diferenciados entre estas duas entidades. A informação remetida via MISP nas diferentes galáxias de classificação de segurança compatível, deverá ser centralizada na galáxia da Autoridade Nacional de Cibersegurança. Esta centralização é imprescindível para efeitos de tratamento, prevenção, fiscalização, resposta e mitigação de incidentes de cibersegurança de dimensão assinalável ou que afetem as entidades sob a alçada legal da missão do CNCS.

4. Galáxia 4 – Autoridade Nacional de Ciberdefesa (G4)

No caso da Autoridade Nacional de Ciberdefesa, o cenário é semelhante ao anterior e está ilustrado na Figura 11. O Centro de Ciberdefesa, em estado de normalidade, atua como CERT das Forças Armadas portuguesas. Note-se, no entanto que, neste caso, esta entidade pode integrar múltiplas galáxias de acordo com as funções que desempenha.

Figura 7 - Galáxia da AN Ciberdefesa

Em estado de normalidade, enquanto desempenha apenas funções de CERT das Forças Armadas, A autoridade nacional de ciberdefesa deverá ter uma galáxia própria, com informação especifica e com níveis de segurança apropriados às infraestruturas que protege. No entanto, em estado de guerra, o acesso à informação deve ser integral e incondicional. Como tal, deverá ser previsto um mecanismo que permita, em estado de guerra, este tipo de acesso a esta entidade.

5. Galáxia 5 – Indústria de Cibersegurança (G5)

A galáxia da indústria de cibersegurança está descrita na Figura 12. Esta galáxia integra três tipologias destintas, de acordo com as suas necessidades de acesso a informação: os provedores de serviços de cibersegurança, as empresas que desenvolvem *software* e os investigadores de cibersegurança.

Figura 8 - Galáxia da Indústria de Cibersegurança

Os provedores de serviços de cibersegurança deverão ter um acesso integral a indicadores de comprometimento não classificados e devidamente anonimizados. Estes indicadores poderão ser utilizados para aumentar significativamente a segurança dos seus produtos e o nível de cibersegurança dos seus clientes. No entanto, estas mesmas entidades, devem ser contribuintes ativas na inserção de IoC de base, contribuindo assim para uma base de conhecimento muitíssimo mais alargada e de utilidade muito superior.

As empresas que desenvolvem *software* poderão utilizar esta plataforma para verificar vulnerabilidades nos seus produtos ou produtos semelhantes e robustecer o software que desenvolvem. Podem ainda, se o entenderem, publicitar atualizações de segurança e atualizações críticas em tempo real à comunidade de cibersegurança nacional. Finalmente, os investigadores poderão ter acesso a um vasto conjunto de informação, muito difícil de aceder de outra forma e que poderá constituir por si só uma base de conhecimento de utilidade inquestionável.

6. Galáxia 6 – Academia (G6)

A galáxia da academia está ilustrada na Figura 13. Esta galáxia integra três entidades genéricas destintas: as universidades, os politécnicos e os institutos; os investigadores académicos; e os centros de competências.

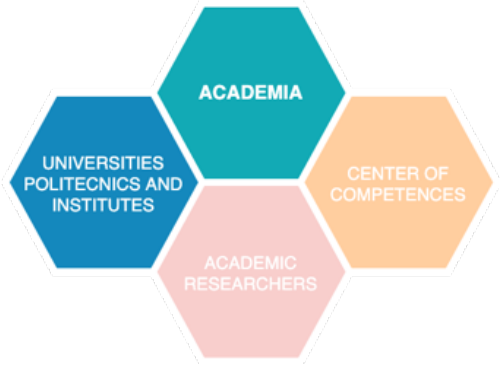

Figura 9 - Galáxia da Academia

O acervo de informação nesta galáxia será maioritariamente direcionado para o ensino, para a sensibilização e, no caso da investigação académica, como uma base de dados que permita o acesso a uma panóplia de dados extremamente úteis para projetos de investigação, não só na área da cibersegurança, mas também em áreas conexas.

7. Galáxia 7 – Energia (G7)

A galáxia da energia encontra-se dividida em quatro grandes áreas funcionais (Figura 14): petróleo, eletricidade, gás e uma sub-galáxia especifica para a entidade reguladora deste sector, a ERSE.

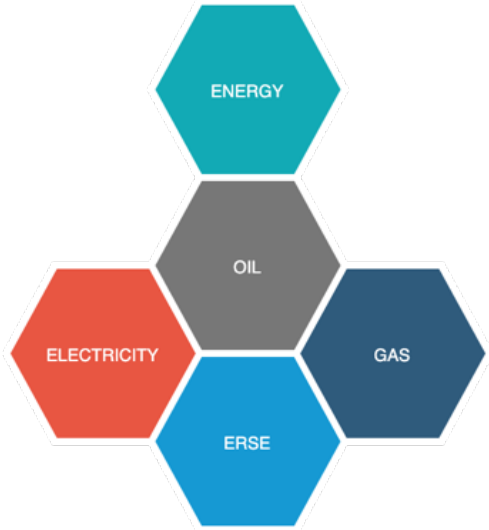

Figura 10 - Galáxia da Energia

No caso das três primeiras tipologias de entidades, face a sua especificidade em vários domínios, incluindo toda a infraestrutura informática, foram criadas sub-galáxias que irão beneficiar das vantagens da partilha de informação para cada sector

específico. No caso da ERSE, enquanto regulador, as vantagens serão óbvias para efeitos de criação de normativos que promovam o aumento de resiliência das entidades a operar nos setores que tutela.

8. Galáxia 8 – Transportes (G8)

A galáxia dos transportes (Figura 15) engloba as diversas entidades a operar neste setor de criticidade reconhecida. No caso dos transportes aéreos proposta é uma sub-galáxia para o transporte aéreo em geral e outra para o respetivo regulador, a ANAC.

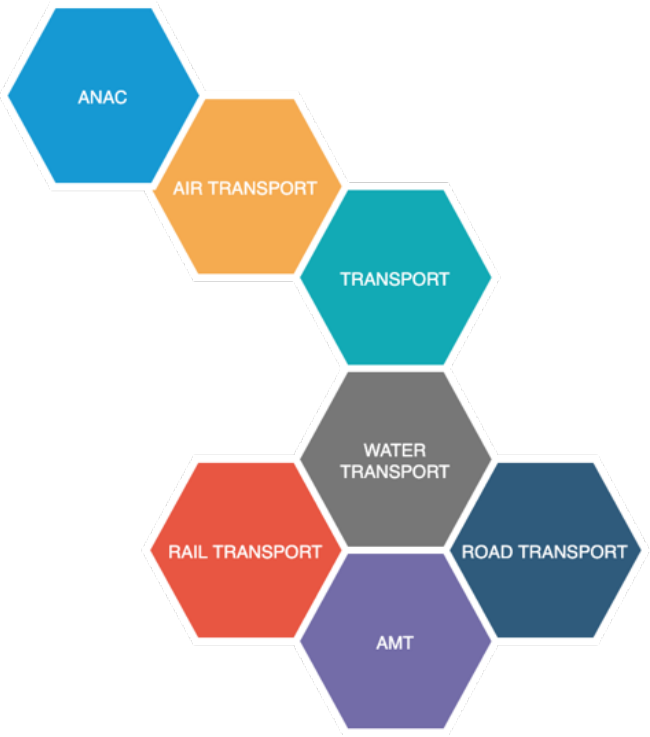

Figura 11 - Galáxia dos Transportes

O mesmo acontece para os restantes domínios de atuação no mar e em terra. No mar temos uma sub-galáxia para o transporte marítimo e, em terra, uma sub-galáxia para os transportes ferroviários e outra para os rodoviários. Nestes últimos domínios foi ainda criada uma sub-galáxia para o regulador de todas estas atividades, a AMT.

9. Galáxia 9 – Banca (G9)

A galáxia da banca integra três tipos de entidade (Figura 16): os bancos, as instituições de crédito e o respetivo regulador, o Banco de Portugal. Estas instituições já integram uma galáxia especifica para troca de IoC, mas infelizmente apenas funciona neste setor específico não partilhando informação de base com as restantes entidades da comunidade de cibersegurança.

Figura 12 - Galáxia da Banca

10. Galáxia 10 – Infraestruturas do Mercado Financeiro (G10)

Esta galáxia está ilustrada na Figura 17 e compreende três entidades destintas: os operadores de mercado, a central de compensação e o respetivo regulador, a CMVM. Note-se que estas entidades funcionam maioritariamente com transações em tempo real, pelo que a criticidade e bom funcionamento dos seus sistemas de transação dependem de um nível de segurança cibernética extremamente elevado.

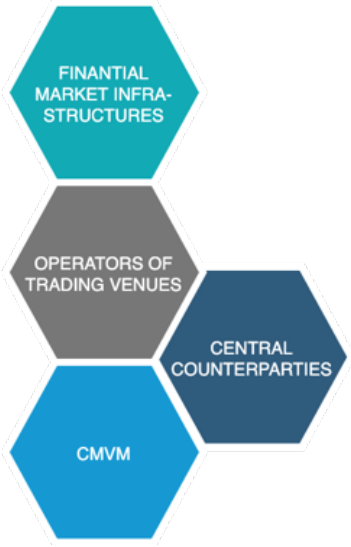

Figura 13 - Galáxia do Mercado Financeiro

11. Galáxia 11 – Saúde (G11)

A galáxia da saúde, ilustrada na Figura 18, apesar de ser simples na sua estrutura, constituída apenas pelos prestadores de cuidados de saúde e pelo respetivo regulador, os Serviços Partilhados do Ministério da Saúde (SPMS), é talvez uma das mais extensas e com maior cobertura a nível nacional.

Figura 14 - Galáxia da Saúde

Desta forma, a constituição de uma galáxia especifica para estes serviços é indispensável face à superfície de ataque que apresenta e face à criticidade do serviço prestado à população.

12. Galáxia 12 – Fornecedores e Distribuidores de Água (G12)

Esta galáxia, descrita na Figura 19, é igualmente simples na sua composição, mas de criticidade extremamente elevada. Os sistemas de aprovisionamento e distribuição de água são críticos para qualquer sociedade e a dependência deste bem e incontornável. Da mesma forma, os sistemas de monitorização de qualidade e de anomalias na rede são indispensáveis ao bom funcionamento do sistema pelo que o acesso a vulnerabilidades e a ataques perpetrados contra estas entidades constitui uma mais valia importante.

Figura 15 - Galáxia dos Fornecedores e Distribuidores de Água

13. Galáxia 13 – Infraestruturas Digitais (G13)

A galáxia das infraestruturas digitais é de importância indiscutível para o mundo moderno e está ilustrada na Figura 20. É constituída pelos provedores de serviços de DNS, pelos provedores de registos de nomes TLD e pelos IXP. Estes serviços são a

base da Internet e ataques e vulnerabilidades nestas plataformas podem ter efeitos disruptivos consideráveis.

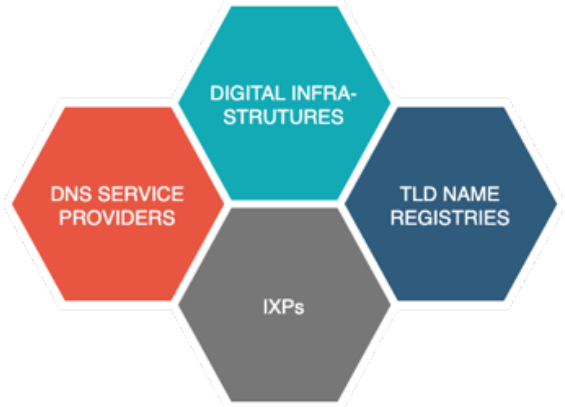

Figura 16 - Galáxia das Infraestruturas Digitais

14. Galáxia 14 – Outras (G14)

Esta galáxia abarca todas as restantes entidades que pela sua dimensão, criticidade ou importância relativa, não necessitem de galáxias especificas e apenas necessitem de informação de base não classificada. Não obstante, o modelo simplificado da Figura 21 pode ser estendido sempre que se entenda e novas galáxias podem ser adicionadas desde que os pressupostos da *framework* sejam respeitados.

Figura 17 - Galáxia Outras Entidades

4.4. Modelo simplificado

O modelo simplificado, visa facilitar a interpretação e compreensão da *framework* neste caso de estudo. Este modelo é aplicado a uma tipologia genérica de entidades em vez de uma forma mais exaustiva, a cada entidade de forma individual como no modelo compreensivo. Desta forma, cada galáxia está representada por um conjunto de características (níveis de

acesso a informação classificada e acesso a informação pessoal), visando uma aplicação mais simples da *framework*, inclusive como uma primeira etapa da adoção da *framework* a nível nacional ou internacional.

Assim, no modelo simplificado, a *framework* resultaria nas seguintes galáxias:

Modelo simplificado

1. Galáxia A – Serviço de Informações de Segurança (SIS) e Polícia Judiciária (PJ)
    - Nível de acesso à informação de sistema: Total
    - Acesso a informação classificada: Muito Secreto (*Top Secret*)
    - Acesso a informação pessoal: Sim
2. Galáxia B – Centro Nacional de Cibersegurança (CNCS), CERT.PT e Centro de Ciberdefesa (CCD)
    - Nível de acesso à informação de sistema: Parcial
    - Acesso a informação classificada: Secreto (*Secret*)
    - Acesso a informação pessoal: Sim
3. Galáxia C – CERT nacionais, infraestruturas críticas, fornecedores de serviços essenciais e indústria de cibersegurança
    - Nível de acesso à informação de sistema: Parcial
    - Acesso a informação classificada: Confidencial (*Confidential*)
    - Acesso a informação pessoal: CERT.PT: Sim / Restantes entidades: Não
    a. Galáxia C1 – ISAC
        - Nível de acesso à informação de sistema: Parcial
        - Acesso a informação classificada: infraestruturas críticas e fornecedores de serviços essências: Secreto (*Secret*) / restantes entidades: Não classificada (*Unclassified*)
        - Acesso a informação pessoal: Não
    b. Galáxia C2 – Outros
        - Nível de acesso à informação de sistema: Parcial
        - Acesso a informação classificada: Não Classificada (*Unclassified*)
        - Acesso a informação pessoal: Não

Note-se, que neste modelo, existem apenas três galáxias principais e duas sub-galáxias. Apesar deste modelo se afastar da opção ótima, revela ainda características importantes ao

nível da partilha de indicadores e na criação de conhecimento, que devem ser tidos em conta face à simplificação da sua implementação a nível nacional. Poderá ser ainda, numa perspetiva faseada de evolução da implementação, um primeiro passo para a aplicação da *framework* na sua totalidade após comprovação das suas qualidades e utilidade.

4.5. Comunicações, Sistema de Entrega e Redes

Face à natureza da classificação de segurança dos indicadores, por si só, ou de alguns dos dados agregados, os sistemas de comunicação, os sistemas de entrega e as redes deverão ser construídos e dimensionados tendo em conta os normativos nacionais e internacionais que regem as matérias classificadas. Embora este tema extravase o âmbito desta dissertação, deixa-se um contributo para a construção e dimensionamento destes sistemas.

Como se pode ver na Figura 22, existem clusters definidos por classificação de segurança das matérias que repousam e circulam nestes sistemas. Para as entidades com níveis de acesso mais elevados (G1 a G4), deverá existir um cluster de segurança máxima, isolado do exterior e com sistemas de entrega baseados em *air-gap* ou outro com níveis de segurança similares ou superiores.

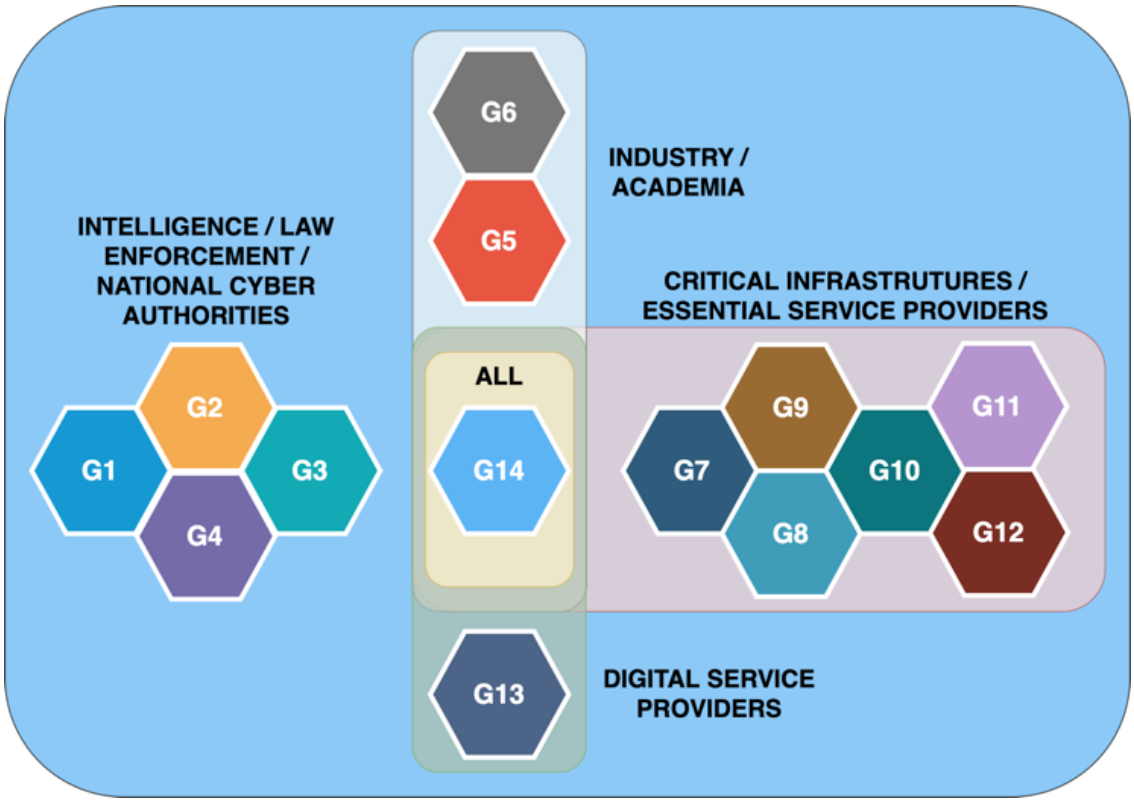

Figura 18 – Exemplo de Distribuição das Galáxias no caso nacional

As galáxias restantes (G5 a G13), com a exceção da galáxia outros (G14), deverão ter mecanismos de segurança adequados à classificação das matérias a que têm acesso (vide a Tabela 8 da aplicação da f*ramework*). Por fim, a galáxia 14 deverá ter igualmente sistemas de segurança adequados, mas para um nível de sistemas não classificados.

A utilização de tecnologias que garantam a fiabilidade da informação e a segurança do seu histórico, como o *blockchain*, deve ser especialmente considerada pois introduz níveis de segurança e resiliência superiores.

A automatização do sistema de entrega é igualmente desejável e, do ponto de vista da aplicação da *framework*, indispensável. Com vista a facilitar a programação dos sistemas de entrega, foram elaboradas árvores de decisão já apresentadas na Figura 2 e Figura 3, que permitem verificar que entidades devem ser informadas quando um determinado incidente de segurança é detetado e que tipo de informação deve ser transmitida de acordo com a sua sensibilidade e classificação de segurança.

4.6. Competências e atribuições

Finalmente, com vista a uma melhor perceção das competências e atribuições dos quatro pilares da cibersegurança a nível nacional já explicadas anteriormente, desenvolveu-se um organograma (Figura 23) que permite uma visão abrangente destas competências de acordo com cada entidade nacional.

Desta forma, partindo da deteção de um incidente de segurança, há que verificar se a vítima se encontra abrangida pelo RJCS. Conforme se pode ver na Figura 23, a obrigatoriedade de reporte do incidente a algumas entidades depende deste fator. No caso de constar, o reporte do incidente é obrigatório ao CNCS, no caso de não constar, o reporte é desejável, mas facultativo.

Outro elemento importante a ter em conta é se o incidente está abrangido no RGPD. Sempre que dados pessoais sejam acedidos, alterados, ou exfiltrados, a CNPD deve ser obrigatoriamente informada independentemente se a entidade consta ou não do RJCS.

Face a esta primeira triagem, verificamos o potencial fluxo de informação pelas restantes entidades e, não menos importante, em que campo de atuação cada uma participa na reação ao incidente. No caso da CNPD, esta atua no campo da proteção dos dados pessoais. O CNCS, atua no campo da mitigação e apoio à resposta a ciberincidentes. A PJ, atua no campo

da prevenção e punição de atos criminosos. E finalmente, o SIS, atua no campo da atribuição dos ataques e no apoio à decisão política.

As funções específicas simplificadas de cada entidade estão igualmente descritas na Figura 23 – CNPD: procedimento administrativo, CNCS: procedimento administrativo; PJ: processo-crime e, SIS: produção de informações.

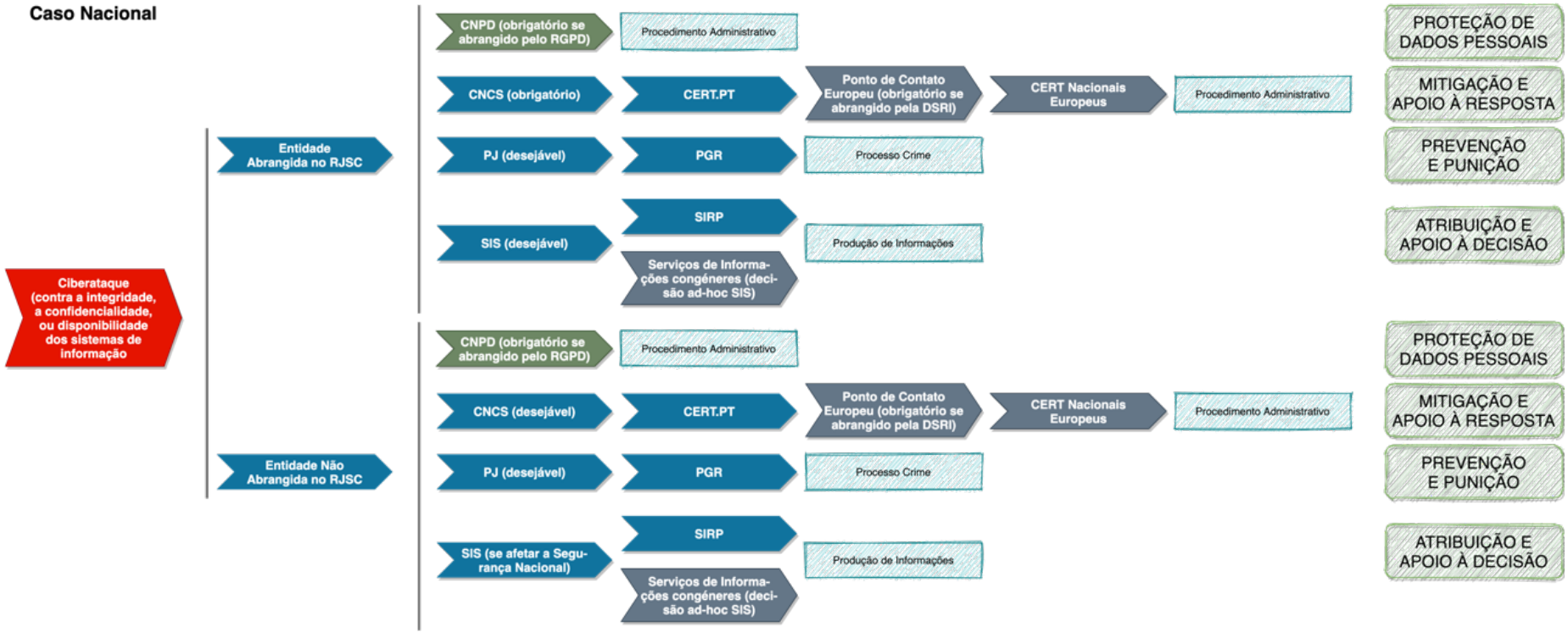

Figura 19 - Competências e Atribuições

5. Cenários

Com vista a demonstrar as entidades a ativar e os respetivos fluxos de informação previstos na f*ramework*, em diferentes tipos de incidentes de segurança, foram criados três cenários que demonstram quais as entidades envolvidas e como deve a informação fluir. Uma vez mais, todos os cenários são aplicados à realidade nacional de acordo com a sugestão de implementação efetuada no capítulo 4.

5.1. Cenário com entidade do Estado

Incidente: Um DDoS atinge o portal das finanças durante o período de entrega do IRS, afetando com impacto significativo a disponibilidade do serviço. Não houve comprometimento de quaisquer dados.

Pressupostos:

- O ataque foi aparentemente perpetrado com o apoio do Estado russo pelo grupo APT29.
- O ataque é considerado como uma operação de destabilização de um agente de ameaça patrocinado por um Estado.

Como se pode verificar na Figura 24, a entidade originadora e a vítima direta do ataque é a Autoridade Tributaria (AT). Uma vez detetado o ataque e tendo em conta os pressupostos do cenário, a AT informa automaticamente a sua tutela, o Ministério das Finanças e, simultaneamente, o CNCS, o SIS e a PJ. Esta comunicação deve conter todos os IoC e informação pertinente - definida pela aplicação da *framework* - para iniciar todos os processos subsequentes.
A partir deste momento, diversos tipos de informação são canalizados de acordo com o princípio de conhecer, nomeadamente:

1. A tutela da AT, o Ministério das Finanças (MF) e informado sobre a generalidade do incidente, mas informação técnica não devera ser enviada não havendo necessidade de conhecer por parte do MF. O MF, por sua vez, comunica o sucedido ao primeiro-ministro que, se o entender, comunica ao Presidente da República.

2. Da parte do CNCS, é ativado imediatamente o CERT.PT que, se assim entendido por parte da AT, poderá ajudar no esforço de resposta e mitigação do incidente. Durante este processo, o CNCS e o CERT.PT poderão ativar os parceiros internacionais para obtenção de informação complementar e/ou para comunicar IoC de base a estas entidades para prevenção imediata. O CNCS poderá ainda comunicar o incidente ao Centro de Ciberdefesa (CCD), uma vez que o grupo APT29 está associado a uma estrutura militar russa. O CCD deve informar o serviço de informações militares – CISMIL – com vista a informar sobre possível operação cibernética militar hostil por parte de Estado estrangeiro.
3. O SIS inicia a sua investigação na vertente da *intelligence* e fornece, logo que possível, as informações de contextualização sobre técnicas, táticas e procedimentos (TTP) do agente da ameaça, assim como a sua caracterização e contextualização. Em simultâneo, comunica informação genérica de contexto à sua tutela, o SIRP, e ativa, caso julgue necessário, os serviços de informações congéneres para obtenção de informação complementar. Relatórios destintos são enviados para a AT e para os decisores políticos para informação e suporte à decisão.
4. A PJ inicia a sua investigação na vertente criminal após comunicação com a PGR e ativa as suas congéneres estrangeiras, caso seja necessário, de acordo com os pressupostos do normativo penal.
5. Após este fluxo de informação inicial, a troca de informações entre as entidades envolvidas intensifica-se e cada uma suporta as restantes de acordo com as suas missões e limitações legais. A troca de informação técnica ocorre principalmente entre as entidades a azul. As restantes entidades, dependendo dos seus níveis de acesso e tipologia, recebem pontos de situação – especialmente a nível político – ou informação técnica de base e anonimizada.
6. Caso os decisores políticos entendam que este incidente reveste um caráter de ameaça ao Estado, o Ministério dos Negócios Estrangeiros poderá ser chamado a intervir junto dos representantes diplomáticos em Portugal do país agressor ou diretamente com os decisores políticos desse país pela via diplomática.

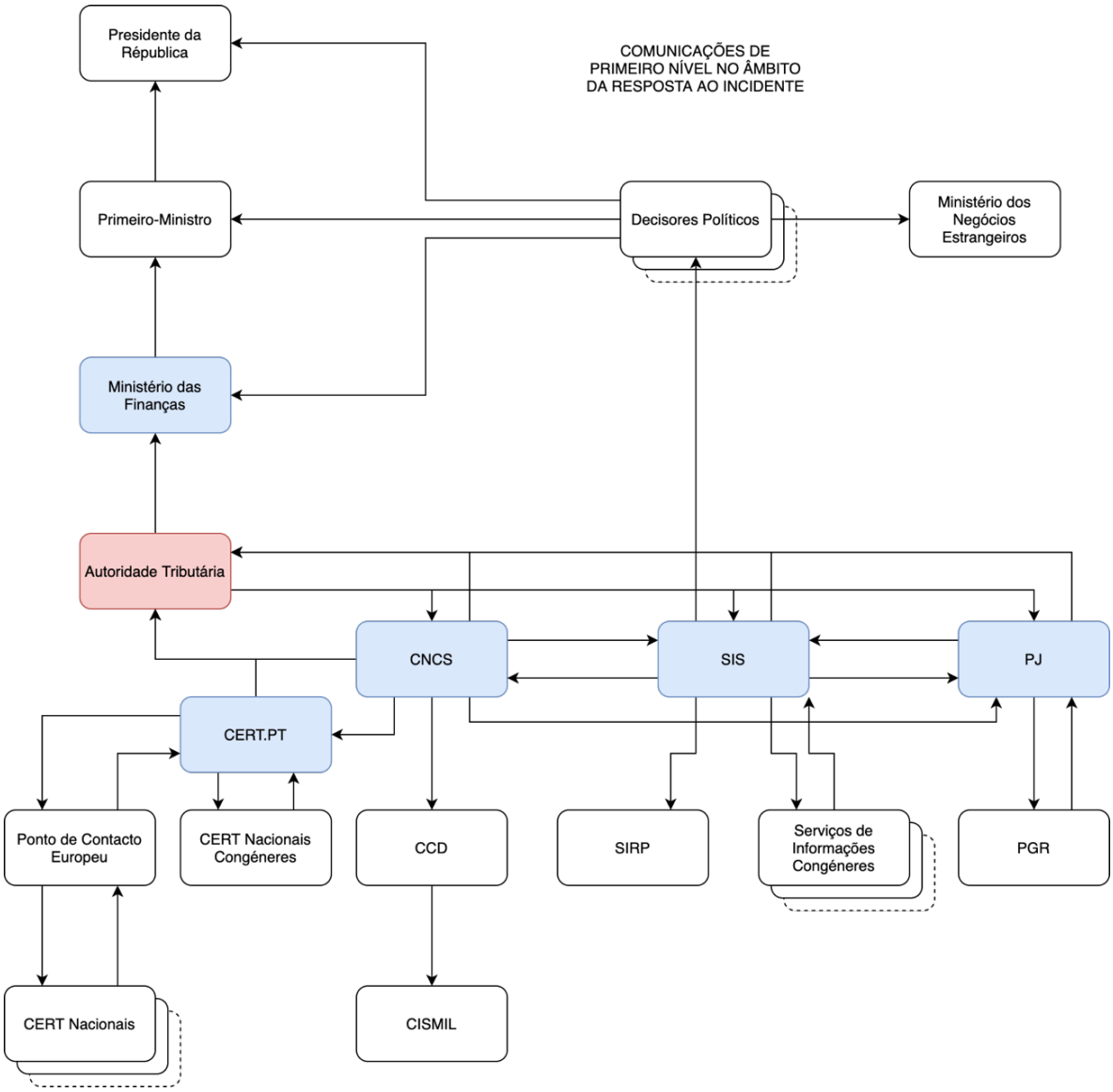

Figura 20 - Organograma Cenário 1

5.2. Cenário com infraestrutura crítica

Incidente: Um ataque via cadeia de abastecimento (*supply-chain*) resultou no comprometimento da rede informática da EDP. Uma *backdoor* foi identificada e esta permitiu a injeção de um *malware* que resultou na exfiltração de dados (incluindo dados pessoais).

Pressupostos:

- O ataque parece ter sido efetuado com o apoio do Estado chinês, nomeadamente pelo grupo APT10.
- O ataque é considerado uma operação de ciberespionagem de um agente de ameaça patrocinado por um Estado estrangeiro.

Neste cenário, representado na Figura 25, a vítima é uma empresa privada, mas considerada uma infraestrutura crítica: a EDP. O fluxo de informação inicial é em tudo idêntico ao cenário anterior, salvaguardadas as seguintes exceções:

1. A EDP não tem tutela. No entanto poderá comunicar o incidente, se o entender ou o normativo interno o prever, aos seus acionistas qualificados.
2. Neste caso, foi identificada a exfiltração de dados pessoais. De acordo com a *framework*, que incorpora o estipulado na legislação nacional, uma comunicação tem de ser efetuada no mais curto espaço de tempo a Comissão Nacional de Proteção de Dados (CNPD) nos termos estipulados pelo normativo legal.

Todo o restante processo decorre de forma semelhante ao descrito no primeiro cenário.

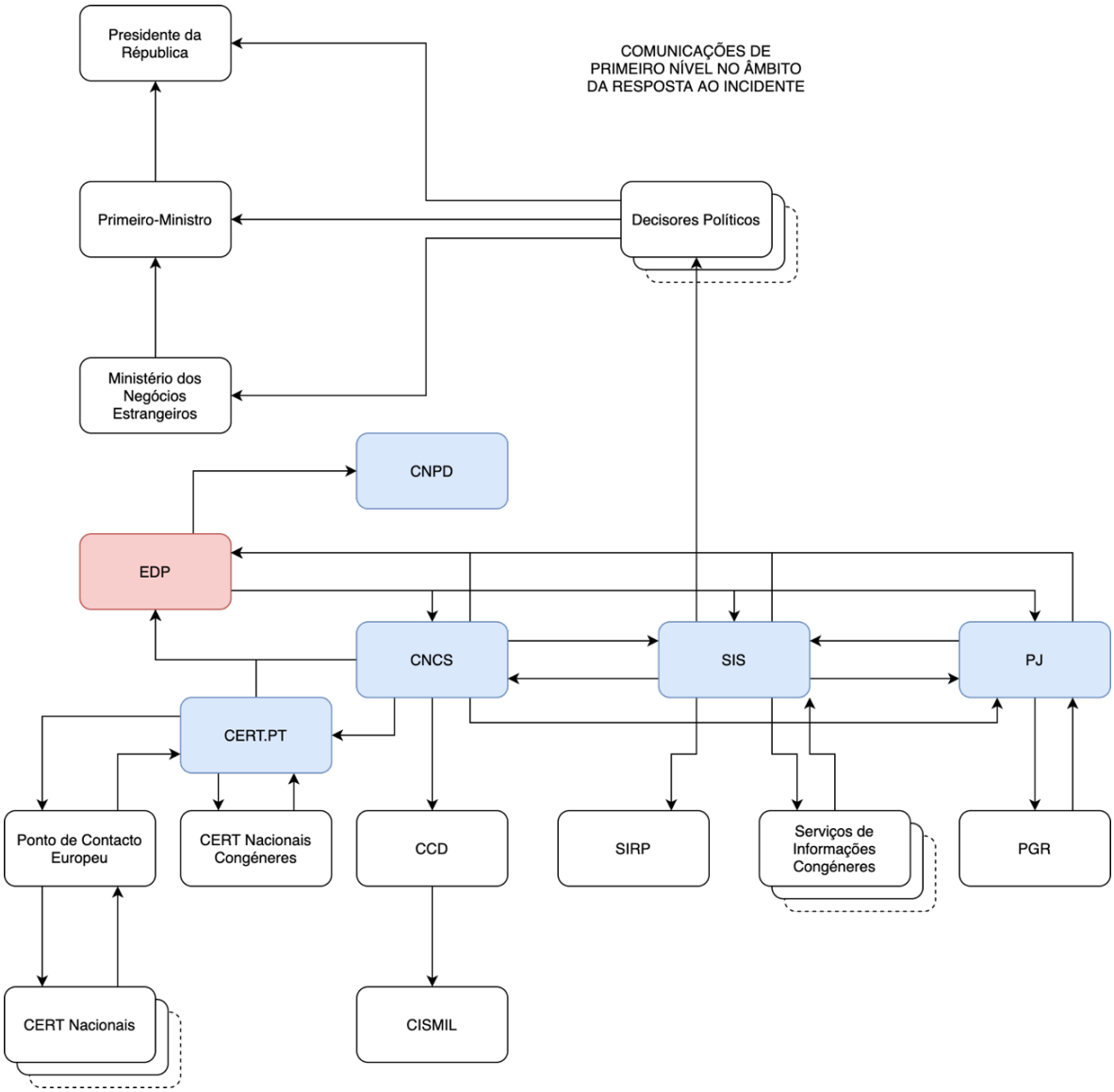

Figura 21 - Organograma Cenário 2

5.3. Cenário com entidade privada não considerada crítica ou sensível

Incidente: Um ataque de *ransomware* comprometeu a disponibilidade dos sistemas de informação e o sistema de produção automatizado da Plastimoldes, uma empresa de dimensão média, dedicada à injeção de plásticos. Não foram exfiltrados dados nem houve acesso aos mesmos.

Pressupostos:

- O ataque parece ter sido efetuado por um *hacker* através de uma plataforma de *ransomware-as-a-service* (RaaS).
- O ataque parece ter todas as características de uma operação isolada efetuada por cibercriminosos com motivações meramente financeiras.

Este cenário visa representar a maioria dos incidentes de cibersegurança mais comuns. Trata-se de um ataque a uma entidade que não é considerada uma infraestrutura crítica ou sensível e por um agente de ameaça que não é patrocinado por um Estado. Neste caso, como se pode verificar na Figura 26, o fluxo de informação e as entidades ativadas são muito menos e a comunicação do acidente pela vítima é facultativa.

1. A Plastimoldes deve, mas não é legalmente obrigada, a comunicar o incidente e respetivos IoC ao CNCS. Caso esta comunicação aconteça, o CERT.PT pode ser ativado e se solicitado a participar na resposta ao incidente, deverá estabelecer um fluxo de informação com a vítima. No caso de o CNCS ser informado, deve informar o SIS e a PJ do sucedido e remeter os IoC angariados.
2. A Plastimoldes, se o entender, poderá comunicar diretamente ao SIS e à PJ (especialmente a esta última se pretender apresentar queixa-crime).
3. O SIS e a PJ, caso o entendam, de acordo com a avaliação que fazem do incidente, poderão encetar contactos com os respetivos congéneres no âmbito das suas respetivas missões.

Note-se, no entanto, que as comunicações apesar de facultativas são de todo desejáveis para o robustecimento da plataforma com dados substantivos e para a criação de conhecimento. Estas comunicações contribuem ainda para um melhor conhecimento do contexto nacional e permitirão análises de granularidade muito mais fina.

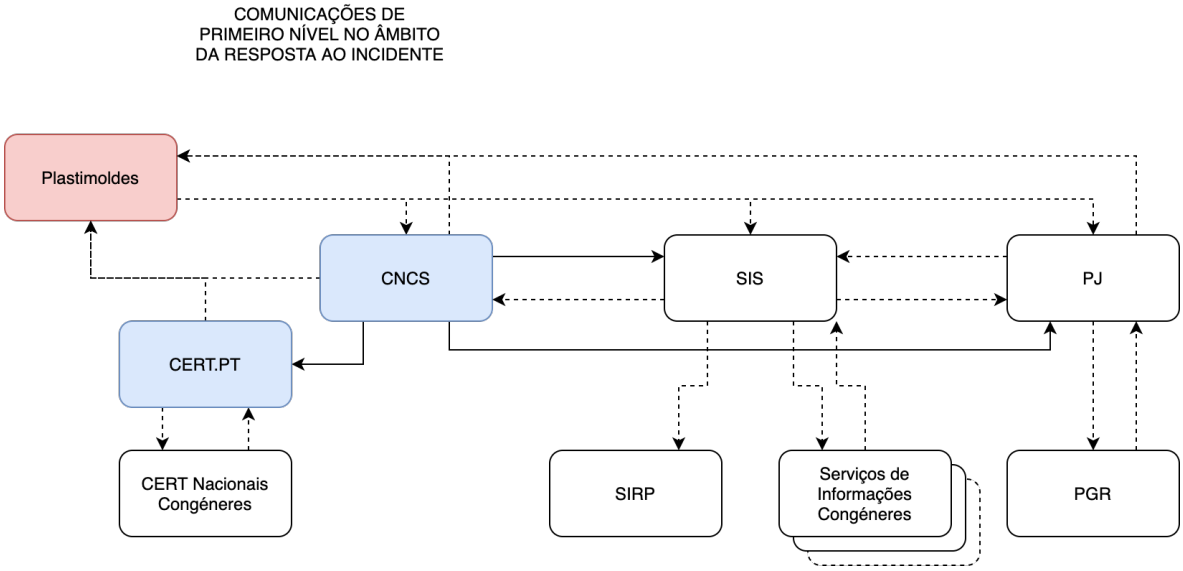

Figura 22 - Organograma Cenário 3

6. Conclusões

O objetivo desta dissertação foi, inicialmente, definir e caracterizar um ecossistema de segurança do ciberespaço e exemplificar este ecossistema com a realidade nacional. Concluiu-se que as entidades integrantes não interagem com a devida e necessária eficácia, tornando ineficiente a tão necessária partilha de indicadores de comprometimento e de conhecimento, e inviabilizando assim a constituição de um verdadeiro ecossistema de cibersegurança com características simbióticas.

O estudo efetuado nesta dissertação foi transversal à comunidade alargada de cibersegurança e resultou na proposta de uma *framework* que visa a partilha de informação e conhecimento, salvaguardadas todas as especificidades e missões dos respetivos agentes de cibersegurança, públicos e privados.

Esta *framework* sugere igualmente os tão necessários mecanismos de interoperabilidade entre entidades. A dispersão de sistemas e de metodologias de recolha, tratamento, análise e disseminação de informação é atualmente bastante complexo. Os mecanismos de interoperabilidade existentes, além de escassos, não demonstram a flexibilidade necessária para lidar com uma tipologia alargada de informação classificada e não classificada.

Desta forma, esta dissertação sugere a primeira metodologia de tratamento da informação que permite acesso a IoC e a conhecimento armazenado numa plataforma de recolha e tratamento de informação, de acordo com a legislação em vigor, de acordo com o princípio da necessidade de conhecer e que visa, essencialmente, ancorar o paradigma da necessidade de partilhar.

A *framework* aqui proposta, face à sua alta complexidade em termos das necessidades especificas de cada tipologia de entidade e de informação, não existia até à data.

A utilização da *Malware Information Sharing Platform* (MISP), após as modificações propostas na *framework*, de acordo com a tipologia de utilizadores e respetivos acessos, constituirá uma galáxia de instâncias MISP que garantem uma troca de indicadores e conhecimento acionáveis por todos os integrantes do ecossistema nacional.

A utilização do MISP permitirá também a integração da informação contida em sistemas diversos e em diversas entidades, em instâncias que permitam uma gestão adequada da

informação. Estão igualmente previstos na *framework* os mecanismos automatizados de carregamento e extração de informação das instâncias MISP.

Apesar de existir a tecnologia necessária à implementação deste sistema, faltava uma conceptualização do ecossistema, metodologias de catalogação, tratamento e classificação de informação e, não menos importante, uma plataforma tecnológica que permitia a troca e armazenamento de informação com segurança e resiliência a ataques informáticos.

Assim, esta dissertação entrega uma *framework*, sustentada por um estudo de caso e três cenários de aplicação, que representa o primeiro passo para a sua implementação a nível nacional e/ou internacional, permitindo um aumento significativo da partilha de informação e, em consequência desta partilha, um potencial de aumento dos níveis de cibersegurança individuais e coletivos de enorme monta.

Em termos futuros, com vista à implementação desta *framework*, é ainda necessário:

- Definir quais as entidades administradoras de toda a informação ou de partes da informação que constituem os repositórios de dados.
- Definir e implementar que tipo de infraestrutura e tecnologia suportarão os repositórios de informação (a utilização de tecnologias que garantam a fiabilidade da informação e a segurança do seu histórico, como o *blockchain*, deve ser especialmente considerada pois introduz níveis de segurança e resiliência superiores);
- Aplicar as alterações ao código fonte, aqui desenvolvidas, no MISP (criação e alteração dos campos);
- Implementar a automatização dos sistemas de entrega da informação de acordo com a *framework*; e
- Definir e implementar mecanismos seguros de transferência de informação (preferencialmente com recurso a sistemas *air-gap*) entre redes e repositórios de informação com graus de classificação diferenciados e sistemas de classificação destintos (TLP, Nacional, União Europeia e NATO).

Estas decisões extravasam o âmbito desta dissertação uma vez que dependem de decisões legais, políticas e tecnológicas onde a *framework* pretende ser agnóstica.

Bibliografia ou Referências Bibliográficas

[1] J. P. Aguiar and M. Defesa, "Resolução do Conselho de Ministros n.º 36/2015 de 12 de junho," pp. 3738–3742, 2015.

[2] W. Zhao and G. White, "A collaborative information sharing framework for community cyber security," *2012 IEEE Int. Conf. Technol. Homel. Secur. HST 2012*, pp. 457–462, 2012.

[3] ENISA, *Information Sharing and Analysis Centres (ISACs) Cooperative models*. 2017.

[4] J. Pfeifer, "Network Fusion: Information and Intelligence Sharing for a Networked World," *Homel. Secur. Aff.*, vol. 8, no. 1, 2012.

[5] L. M. Oliva and L. M. Oliva, "21st Century Challenges to Sharing Information," *Inf. Resour. Manag. J.*, vol. 18, 2005.

[6] K. Rantos, A. Spyros, A. Papanikolaou, A. Kritsas, C. Ilioudis, and V. Katos, "Interoperability challenges in the cybersecurity information sharing ecosystem," *Computers*, vol. 9, no. 1, pp. 1–17, 2020.

[7] C. Wagner, A. Dulaunoy, G. Wagener, and A. Iklody, "MISP - The design and implementation of a collaborative threat intelligence sharing platform," in *WISCS 2016 - Proceedings of the 2016 ACM Workshop on Information Sharing and Collaborative Security, co-located with CCS 2016*, 2016, pp. 49–56.

[8] S. Barrett and B. Konsynski, "Inter-Organization Information Sharing Systems," *MIS Q.*, vol. 6, p. 93, Dec. 1982.

[9] S. Mokaddem, G. Wagener, A. Dulaunoy, and A. Iklody, "Taxonomy driven indicator scoring in MISP threat intelligence platforms," 2019.

[10] E. Portugu, S. Galileo, G. Nacional, C. Nacional, and A. Nacional, "Decreto-Lei n.º 136/2017, de 6 de novembro," *Presidência e da Mod. Adm.*, 2017.

[11] L. E. I. Org and C. I. A. Judici, "Decreto-Lei n.º 275-A/2000." 2010.

[12] de 13 de agosto Lei n.º 50/2014, "Orgânica do Secretário-Geral do Sistema de

Informações da República Portuguesa, do Serviço de Informações Estratégicas de Defesa (SIED) e do Serviço de Informações de Segurança (SIS),” pp. 4206–4221, 2014.

[13] M. Alsharif, S. Mishra, and M. AlShehri, “Impact of Human Vulnerabilities on Cybersecurity,” *Comput. Syst. Sci. Eng.*, vol. 40, no. 3, pp. 1153–1166, 2021.

[14] CNCS, “Quadro Nacional de Referência para a Cibersegurança.”, https://www.cncs.gov.pt/pt/quadro-nacional/.

[15] S. De Oliveira, “Challenges to Information Sharing Perceptions and Realities,” 2016.

[16] Decreto-Lei nº 65, “Presidência do Conselho de Ministros. Resolução do Conselho de Ministros 59/2001,” *Diário da República - I Série-B*, vol. 25, no. 2, pp. 3179–3182, 2021.

[17] “MISP.” Malware Information Sharing Platform, CIRCL, https://www.misp-project.org.

Anexos

Anexo A – Tabela de campos do MISP com níveis de acesso de segurança e acessos a informação pessoal.

Anexo A - Tabela de campos do MISP com níveis de acesso de segurança e acessos a informação pessoal.

Nota: Códigos das entidades constam na Tabela 8 (ex.: A1, A2, B1, C2, etc).

Security objects	**SHARING LEVEL**																				**Contain PII**
security-classification	Default Level			**National**				**Eurpean-Union**				**NATO**					**TLP**				
	Unclassified	**State-Secret**	**Justice-Secret**	**Reserved**	**Confidential**	**Secret**	**Top-secret**	**Reserved**	**Confidential**	**Secret**	**Top-secret**	**Reserved**	**Confidential**	**Secret**	**Top-secret**	**Cosmic-top-secret**	**white**	**green**	**amber**	**red**	
MISP objects																					
ail-leak	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
ais-info	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
credential	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
ddos	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
device	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
dns-record	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
domain-ip	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
email	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
employee	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
file	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
forensic-case	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
forensic-evidence	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
intel471-vulnerability-intelligence	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
intelmq_event	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no

intelmq_report	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A5	A1 A2 A4	A1 A2 A5	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A4	A1 A2 A5	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
interpol-notice	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A5	A1 A2 A4	A1 A2 A5	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A4	A1 A2 A5	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
iot-device	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A5	A1 A2 A4	A1 A2 A5	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A4	A1 A2 A5	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
iot-firmware	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A5	A1 A2 A4	A1 A2 A5	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A4	A1 A2 A5	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
ip-port	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A5	A1 A2 A4	A1 A2 A5	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A4	A1 A2 A5	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
leaked-document	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A5	A1 A2 A4	A1 A2 A5	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A4	A1 A2 A5	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
legal-entity	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A5	A1 A2 A4	A1 A2 A5	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A4	A1 A2 A5	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
person	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A5	A1 A2 A4	A1 A2 A5	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A4	A1 A2 A5	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
phishing	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A5	A1 A2 A4	A1 A2 A5	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A4	A1 A2 A5	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
process	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A5	A1 A2 A4	A1 A2 A5	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A4	A1 A2 A5	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
publication	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A5	A1 A2 A4	A1 A2 A5	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A4	A1 A2 A5	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
target-system	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A5	A1 A2 A4	A1 A2 A5	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A4	A1 A2 A5	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
victim	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A5	A1 A2 A4	A1 A2 A5	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A4	A1 A2 A5	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
vulnerability	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A5	A1 A2 A4	A1 A2 A5	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A4	A1 A2 A5	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
credit-card	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A5	A1 A2 A4	A1 A2 A5	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A4	A1 A2 A5	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
facebook-account	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A5	A1 A2 A4	A1 A2 A5	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A4	A1 A2 A5	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
facebook-group	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A5	A1 A2 A4	A1 A2 A5	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A4	A1 A2 A5	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
facebook-page	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A5	A1 A2 A4	A1 A2 A5	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A4	A1 A2 A5	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
facebook-post	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A5	A1 A2 A4	A1 A2 A5	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A4	A1 A2 A5	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
tor-hiddenservice	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A5	A1 A2 A4	A1 A2 A5	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A4	A1 A2 A5	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
tor-node	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A5	A1 A2 A4	A1 A2 A5	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A4	A1 A2 A5	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no

twitter-account	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
twitter-list	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
twitter-post	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
url	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
user-account	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
vehicle	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
android-app	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
android-permission	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
annotation	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
anonymisation	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
asn	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
attack-pattern	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
authentication-failure-report	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
authenticode-signerinfo	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
av-signature	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
bank-account	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
bgp-hijack	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
bgp-ranking	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
blog	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
boleto	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
btc-transaction	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no

btc-wallet	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
cap-alert	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
cap-info	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
cap-resource	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
coin-address	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
command	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
command-line	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
cookie	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
cortex	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
cortex-taxonomy	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
course-of-action	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
covid19-csse-daily-report	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
covid19-dxy-live-city	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
covid19-dxy-live-province	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
cowrie	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
cpe-asset	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
crypto-material	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
cytomic-orion-file	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
cytomic-orion-machine	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
dark-pattern-item	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
diameter-attack	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes

domain-crawled	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
elf	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
elf-section	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
exploit-poc	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
facial-composite	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
fail2ban	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
forged-document	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no/yes
ftm-Airplane	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-Assessment	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-Asset	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-Associate	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-Audio	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-BankAccount	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-Call	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-Company	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-Contract	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-ContractAward	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-CourtCase	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-CourtCaseParty	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-Debt	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-Directorship	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used

ftm-Document	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-Documentation	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-EconomicActivity	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-Email	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-Event	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-Family	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-Folder	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-HyperText	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-Image	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-Land	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-LegalEntity	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-License	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-Membership	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-Message	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-Organization	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-Ownership	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-Package	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-Page	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-Pages	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-Passport	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-Payment	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used

ftm-Person	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-PlainText	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-PublicBody	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-RealEstate	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-Representation	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-Row	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-Sanction	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-Succession	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-Table	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-TaxRoll	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-UnknownLink	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-UserAccount	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-Vehicle	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-Vessel	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-Video	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ftm-Workbook	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
geolocation	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
git-vuln-finder	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
github-user	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
gitlab-user	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
gtp-attack	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no

http-request	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
ilr-impact	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
ilr-notification-incident	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	not used
image	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no/yes
impersonation	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
imsi-catcher	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
instant-message	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
instant-message-group	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
internal-reference	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
ip-api-address	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
irc	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
ja3	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
keybase-account	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
lnk	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
macho	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
macho-section	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
mactime-timeline-analysis	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
malware-config	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
meme-image	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
microblog	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
mutex	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no

narrative	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
netflow	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
network-connection	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
network-socket	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
news-agency	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A5 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
news-media	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
organization	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
original-imported-file	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
parler-account	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
parler-comment	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
parler-post	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
passive-dns	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
paste	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no/yes
pcap-metadata	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
pe	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
pe-section	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
pgp-meta	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
phishing-kit	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
phone	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
python-etvx-event-log	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
r2graphity	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4 A5	A1 A2 A3 A4 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no

reddit-account	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
reddit-comment	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
reddit-post	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
reddit-subreddit	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	yes
regexp	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
registry-key	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
regripper-NTUser	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
regripper-sam-hive-single-user	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
regripper-sam-hive-user-group	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
regripper-software-hive-BHO	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
regripper-software-hive-appInit-DLLS	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
regripper-software-hive-application-paths	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
regripper-software-hive-applications-installed	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
regripper-software-hive-command-shell	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
regripper-software-hive-software-run	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
regripper-software-hive-userprofile-winlogon	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
regripper-software-hive-windows-general-info	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
regripper-system-hive-firewall-configuration	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
regripper-system-hive-general-configuration	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
regripper-system-hive-network-information	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
regripper-system-hive-services-drivers	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no

						A1 A2 A3 A4	A1 A2			A1 A2	A1 A2			A1 A2	A1 A2			A1 A2						
				A1 A2 A3 A4 A4	A1 A2 A3 A4 A4	A4 B1 B2 B3	A3 A4	A1 A2 A3 A4	A1 A2 A3 A4	A3 A4	A3 A4	A1 A2 A3	A1 A2 A3 A4	A3 A4	A3 A4			A3 A4	A1 A2 A3	A1 A2 A3		
report	ALL	A1	A2	B1 B2 B3 C1 C2 C3	B1 B2 B3 C1 C2 C3	C1	A5	A5 B1 B2 B3	A5 B1 B2 B3	A4	A5	A4 A2	A3	A4	A5	A1 A4	ALL	A5 B1	A4 A5 B1	A4 A5 B1	no				
						A1 A2 A3 A4	A1 A2			A1 A2	A1 A2			A1 A2	A1 A2			A1 A2						
				A1 A2 A3 A4 A4	A1 A2 A3 A4 A4	A4 B1 B2 B3	A3 A4	A1 A2 A3 A4	A1 A2 A3 A4	A3 A4	A3 A4	A1 A2 A3	A1 A2 A3 A4	A3 A4	A3 A4			A3 A4	A1 A2 A3	A1 A2 A3		
research-scanner	ALL	A1	A2	B1 B2 B3 C1 C2 C3	B1 B2 B3 C1 C2 C3	C1	A5	A5 B1 B2 B3	A5 B1 B2 B3	A4	A5	A4 A2	A3	A4	A5	A1 A4	ALL	A5 B1	A4 A5 B1	A4 A5 B1	no				
						A1 A2 A3 A4	A1 A2			A1 A2	A1 A2			A1 A2	A1 A2			A1 A2						
				A1 A2 A3 A4 A4	A1 A2 A3 A4 A4	A4 B1 B2 B3	A3 A4	A1 A2 A3 A4	A1 A2 A3 A4	A3 A4	A3 A4	A1 A2 A3	A1 A2 A3 A4	A3 A4	A3 A4			A3 A4	A1 A2 A3	A1 A2 A3		
rogue-dns	ALL	A1	A2	B1 B2 B3 C1 C2 C3	B1 B2 B3 C1 C2 C3	C1	A5	A5 B1 B2 B3	A5 B1 B2 B3	A4	A5	A4 A2	A3	A4	A5	A1 A4	ALL	A5 B1	A4 A5 B1	A4 A5 B1	no				
						A1 A2 A3 A4	A1 A2			A1 A2	A1 A2			A1 A2	A1 A2			A1 A2						
				A1 A2 A3 A4 A4	A1 A2 A3 A4 A4	A4 B1 B2 B3	A3 A4	A1 A2 A3 A4	A1 A2 A3 A4	A3 A4	A3 A4	A1 A2 A3	A1 A2 A3 A4	A3 A4	A3 A4			A3 A4	A1 A2 A3	A1 A2 A3		
rtir	ALL	A1	A2	B1 B2 B3 C1 C2 C3	B1 B2 B3 C1 C2 C3	C1	A5	A5 B1 B2 B3	A5 B1 B2 B3	A4	A5	A4 A2	A3	A4	A5	A1 A4	ALL	A5 B1	A4 A5 B1	A4 A5 B1	no				
						A1 A2 A3 A4	A1 A2			A1 A2	A1 A2			A1 A2	A1 A2			A1 A2						
				A1 A2 A3 A4 A4	A1 A2 A3 A4 A4	A4 B1 B2 B3	A3 A4	A1 A2 A3 A4	A1 A2 A3 A4	A3 A4	A3 A4	A1 A2 A3	A1 A2 A3 A4	A3 A4	A3 A4			A3 A4	A1 A2 A3	A1 A2 A3		
sandbox-report	ALL	A1	A2	B1 B2 B3 C1 C2 C3	B1 B2 B3 C1 C2 C3	C1	A5	A5 B1 B2 B3	A5 B1 B2 B3	A4	A5	A4 A2	A3	A4	A5	A1 A4	ALL	A5 B1	A4 A5 B1	A4 A5 B1	no				
						A1 A2 A3 A4	A1 A2			A1 A2	A1 A2			A1 A2	A1 A2			A1 A2						
				A1 A2 A3 A4 A4	A1 A2 A3 A4 A4	A4 B1 B2 B3	A3 A4	A1 A2 A3 A4	A1 A2 A3 A4	A3 A4	A3 A4	A1 A2 A3	A1 A2 A3 A4	A3 A4	A3 A4			A3 A4	A1 A2 A3	A1 A2 A3		
sb-signature	ALL	A1	A2	B1 B2 B3 C1 C2 C3	B1 B2 B3 C1 C2 C3	C1	A5	A5 B1 B2 B3	A5 B1 B2 B3	A4	A5	A4 A2	A3	A4	A5	A1 A4	ALL	A5 B1	A4 A5 B1	A4 A5 B1	no				
						A1 A2 A3 A4	A1 A2			A1 A2	A1 A2			A1 A2	A1 A2			A1 A2						
				A1 A2 A3 A4 A4	A1 A2 A3 A4 A4	A4 B1 B2 B3	A3 A4	A1 A2 A3 A4	A1 A2 A3 A4	A3 A4	A3 A4	A1 A2 A3	A1 A2 A3 A4	A3 A4	A3 A4			A3 A4	A1 A2 A3	A1 A2 A3		
scheduled-event	ALL	A1	A2	B1 B2 B3 C1 C2 C3	B1 B2 B3 C1 C2 C3	C1	A5	A5 B1 B2 B3	A5 B1 B2 B3	A4	A5	A4 A2	A3	A4	A5	A1 A4	ALL	A5 B1	A4 A5 B1	A4 A5 B1	yes				
						A1 A2 A3 A4	A1 A2			A1 A2	A1 A2			A1 A2	A1 A2			A1 A2						
				A1 A2 A3 A4 A4	A1 A2 A3 A4 A4	A4 B1 B2 B3	A3 A4	A1 A2 A3 A4	A1 A2 A3 A4	A3 A4	A3 A4	A1 A2 A3	A1 A2 A3 A4	A3 A4	A3 A4			A3 A4	A1 A2 A3	A1 A2 A3	not				
scrippsco2-c13-daily	ALL	A1	A2	B1 B2 B3 C1 C2 C3	B1 B2 B3 C1 C2 C3	C1	A5	A5 B1 B2 B3	A5 B1 B2 B3	A4	A5	A4 A2	A3	A4	A5	A1 A4	ALL	A5 B1	A4 A5 B1	A4 A5 B1	used				
						A1 A2 A3 A4	A1 A2			A1 A2	A1 A2			A1 A2	A1 A2			A1 A2						
				A1 A2 A3 A4 A4	A1 A2 A3 A4 A4	A4 B1 B2 B3	A3 A4	A1 A2 A3 A4	A1 A2 A3 A4	A3 A4	A3 A4	A1 A2 A3	A1 A2 A3 A4	A3 A4	A3 A4			A3 A4	A1 A2 A3	A1 A2 A3	not				
scrippsco2-c13-monthly	ALL	A1	A2	B1 B2 B3 C1 C2 C3	B1 B2 B3 C1 C2 C3	C1	A5	A5 B1 B2 B3	A5 B1 B2 B3	A4	A5	A4 A2	A3	A4	A5	A1 A4	ALL	A5 B1	A4 A5 B1	A4 A5 B1	used				
						A1 A2 A3 A4	A1 A2			A1 A2	A1 A2			A1 A2	A1 A2			A1 A2						
				A1 A2 A3 A4 A4	A1 A2 A3 A4 A4	A4 B1 B2 B3	A3 A4	A1 A2 A3 A4	A1 A2 A3 A4	A3 A4	A3 A4	A1 A2 A3	A1 A2 A3 A4	A3 A4	A3 A4			A3 A4	A1 A2 A3	A1 A2 A3	not				
scrippsco2-co2-daily	ALL	A1	A2	B1 B2 B3 C1 C2 C3	B1 B2 B3 C1 C2 C3	C1	A5	A5 B1 B2 B3	A5 B1 B2 B3	A4	A5	A4 A2	A3	A4	A5	A1 A4	ALL	A5 B1	A4 A5 B1	A4 A5 B1	used				
						A1 A2 A3 A4	A1 A2			A1 A2	A1 A2			A1 A2	A1 A2			A1 A2						
				A1 A2 A3 A4 A4	A1 A2 A3 A4 A4	A4 B1 B2 B3	A3 A4	A1 A2 A3 A4	A1 A2 A3 A4	A3 A4	A3 A4	A1 A2 A3	A1 A2 A3 A4	A3 A4	A3 A4			A3 A4	A1 A2 A3	A1 A2 A3	not				
scrippsco2-co2-monthly	ALL	A1	A2	B1 B2 B3 C1 C2 C3	B1 B2 B3 C1 C2 C3	C1	A5	A5 B1 B2 B3	A5 B1 B2 B3	A4	A5	A4 A2	A3	A4	A5	A1 A4	ALL	A5 B1	A4 A5 B1	A4 A5 B1	used				
						A1 A2 A3 A4	A1 A2			A1 A2	A1 A2			A1 A2	A1 A2			A1 A2						
				A1 A2 A3 A4 A4	A1 A2 A3 A4 A4	A4 B1 B2 B3	A3 A4	A1 A2 A3 A4	A1 A2 A3 A4	A3 A4	A3 A4	A1 A2 A3	A1 A2 A3 A4	A3 A4	A3 A4			A3 A4	A1 A2 A3	A1 A2 A3	not				
scrippsco2-o18-daily	ALL	A1	A2	B1 B2 B3 C1 C2 C3	B1 B2 B3 C1 C2 C3	C1	A5	A5 B1 B2 B3	A5 B1 B2 B3	A4	A5	A4 A2	A3	A4	A5	A1 A4	ALL	A5 B1	A4 A5 B1	A4 A5 B1	used				
						A1 A2 A3 A4	A1 A2			A1 A2	A1 A2			A1 A2	A1 A2			A1 A2						
				A1 A2 A3 A4 A4	A1 A2 A3 A4 A4	A4 B1 B2 B3	A3 A4	A1 A2 A3 A4	A1 A2 A3 A4	A3 A4	A3 A4	A1 A2 A3	A1 A2 A3 A4	A3 A4	A3 A4			A3 A4	A1 A2 A3	A1 A2 A3	not				
scrippsco2-o18-monthly	ALL	A1	A2	B1 B2 B3 C1 C2 C3	B1 B2 B3 C1 C2 C3	C1	A5	A5 B1 B2 B3	A5 B1 B2 B3	A4	A5	A4 A2	A3	A4	A5	A1 A4	ALL	A5 B1	A4 A5 B1	A4 A5 B1	used				
						A1 A2 A3 A4	A1 A2			A1 A2	A1 A2			A1 A2	A1 A2			A1 A2						
				A1 A2 A3 A4 A4	A1 A2 A3 A4 A4	A4 B1 B2 B3	A3 A4	A1 A2 A3 A4	A1 A2 A3 A4	A3 A4	A3 A4	A1 A2 A3	A1 A2 A3 A4	A3 A4	A3 A4			A3 A4	A1 A2 A3	A1 A2 A3					
script	ALL	A1	A2	B1 B2 B3 C1 C2 C3	B1 B2 B3 C1 C2 C3	C1	A5	A5 B1 B2 B3	A5 B1 B2 B3	A4	A5	A4 A2	A3	A4	A5	A1 A4	ALL	A5 B1	A4 A5 B1	A4 A5 B1	no				
						A1 A2 A3 A4	A1 A2			A1 A2	A1 A2			A1 A2	A1 A2			A1 A2						
				A1 A2 A3 A4 A4	A1 A2 A3 A4 A4	A4 B1 B2 B3	A3 A4	A1 A2 A3 A4	A1 A2 A3 A4	A3 A4	A3 A4	A1 A2 A3	A1 A2 A3 A4	A3 A4	A3 A4			A3 A4	A1 A2 A3	A1 A2 A3					
shell-commands	ALL	A1	A2	B1 B2 B3 C1 C2 C3	B1 B2 B3 C1 C2 C3	C1	A5	A5 B1 B2 B3	A5 B1 B2 B3	A4	A5	A4 A2	A3	A4	A5	A1 A4	ALL	A5 B1	A4 A5 B1	A4 A5 B1	no				
						A1 A2 A3 A4	A1 A2			A1 A2	A1 A2			A1 A2	A1 A2			A1 A2						
				A1 A2 A3 A4 A4	A1 A2 A3 A4 A4	A4 B1 B2 B3	A3 A4	A1 A2 A3 A4	A1 A2 A3 A4	A3 A4	A3 A4	A1 A2 A3	A1 A2 A3 A4	A3 A4	A3 A4			A3 A4	A1 A2 A3	A1 A2 A3					
shodan-report	ALL	A1	A2	B1 B2 B3 C1 C2 C3	B1 B2 B3 C1 C2 C3	C1	A5	A5 B1 B2 B3	A5 B1 B2 B3	A4	A5	A4 A2	A3	A4	A5	A1 A4	ALL	A5 B1	A4 A5 B1	A4 A5 B1	no				
						A1 A2 A3 A4	A1 A2			A1 A2	A1 A2			A1 A2	A1 A2			A1 A2						
				A1 A2 A3 A4 A4	A1 A2 A3 A4 A4	A4 B1 B2 B3	A3 A4	A1 A2 A3 A4	A1 A2 A3 A4	A3 A4	A3 A4	A1 A2 A3	A1 A2 A3 A4	A3 A4	A3 A4			A3 A4	A1 A2 A3	A1 A2 A3					
short-message-service	ALL	A1	A2	B1 B2 B3 C1 C2 C3	B1 B2 B3 C1 C2 C3	C1	A5	A5 B1 B2 B3	A5 B1 B2 B3	A4	A5	A4 A2	A3	A4	A5	A1 A4	ALL	A5 B1	A4 A5 B1	A4 A5 B1	yes				
						A1 A2 A3 A4	A1 A2			A1 A2	A1 A2			A1 A2	A1 A2			A1 A2						
				A1 A2 A3 A4 A4	A1 A2 A3 A4 A4	A4 B1 B2 B3	A3 A4	A1 A2 A3 A4	A1 A2 A3 A4	A3 A4	A3 A4	A1 A2 A3	A1 A2 A3 A4	A3 A4	A3 A4			A3 A4	A1 A2 A3	A1 A2 A3					
shortened-link	ALL	A1	A2	B1 B2 B3 C1 C2 C3	B1 B2 B3 C1 C2 C3	C1	A5	A5 B1 B2 B3	A5 B1 B2 B3	A4	A5	A4 A2	A3	A4	A5	A1 A4	ALL	A5 B1	A4 A5 B1	A4 A5 B1	no				
						A1 A2 A3 A4	A1 A2			A1 A2	A1 A2			A1 A2	A1 A2			A1 A2						
				A1 A2 A3 A4 A4	A1 A2 A3 A4 A4	A4 B1 B2 B3	A3 A4	A1 A2 A3 A4	A1 A2 A3 A4	A3 A4	A3 A4	A1 A2 A3	A1 A2 A3 A4	A3 A4	A3 A4			A3 A4	A1 A2 A3	A1 A2 A3					
social-media-group	ALL	A1	A2	B1 B2 B3 C1 C2 C3	B1 B2 B3 C1 C2 C3	C1	A5	A5 B1 B2 B3	A5 B1 B2 B3	A4	A5	A4 A2	A3	A4	A5	A1 A4	ALL	A5 B1	A4 A5 B1	A4 A5 B1	yes				
						A1 A2 A3 A4	A1 A2			A1 A2	A1 A2			A1 A2	A1 A2			A1 A2						
				A1 A2 A3 A4 A4	A1 A2 A3 A4 A4	A4 B1 B2 B3	A3 A4	A1 A2 A3 A4	A1 A2 A3 A4	A3 A4	A3 A4	A1 A2 A3	A1 A2 A3 A4	A3 A4	A3 A4			A3 A4	A1 A2 A3	A1 A2 A3					
splunk	ALL	A1	A2	B1 B2 B3 C1 C2 C3	B1 B2 B3 C1 C2 C3	C1	A5	A5 B1 B2 B3	A5 B1 B2 B3	A4	A5	A4 A2	A3	A4	A5	A1 A4	ALL	A5 B1	A4 A5 B1	A4 A5 B1	no				
						A1 A2 A3 A4	A1 A2			A1 A2	A1 A2			A1 A2	A1 A2			A1 A2						
				A1 A2 A3 A4 A4	A1 A2 A3 A4 A4	A4 B1 B2 B3	A3 A4	A1 A2 A3 A4	A1 A2 A3 A4	A3 A4	A3 A4	A1 A2 A3	A1 A2 A3 A4	A3 A4	A3 A4			A3 A4	A1 A2 A3	A1 A2 A3					
ss7-attack	ALL	A1	A2	B1 B2 B3 C1 C2 C3	B1 B2 B3 C1 C2 C3	C1	A5	A5 B1 B2 B3	A5 B1 B2 B3	A4	A5	A4 A2	A3	A4	A5	A1 A4	ALL	A5 B1	A4 A5 B1	A4 A5 B1	no				

ssh-authorized-keys	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
stix2-pattern	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
suricata	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
threatgrid-report	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
timecode	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
timesketch-timeline	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
timesketch_message	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
timestamp	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
tracking-id	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
transaction	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
translation	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
trustar_report	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
tsk-chats	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
tsk-web-bookmark	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
tsk-web-cookie	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
tsk-web-downloads	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
tsk-web-history	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
tsk-web-search-query	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
virustotal-graph	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
virustotal-report	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no
weakness	ALL	A1	A2	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1 C2 C3	A1 A2 A3 A4 A4 B1 B2 B3 C1	A1 A2 A3 A4 A5	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A5 B1 B2 B3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A2 A3 A4 A2	A1 A2 A3 A4 A3	A1 A2 A3 A4 A4	A1 A2 A3 A4 A5	A1 A4	ALL	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	A1 A2 A3 A4 A5 B1	no

						A1 A2 A3 A4	A1 A2				A1 A2	A1 A2				A1 A2	A1 A2			A1 A2				
				A1 A2 A3 A4 A4	A1 A2 A3 A4 A4	A4 B1 B2 B3	A3 A4	A1 A2 A3 A4	A1 A2 A3 A4	A3 A4	A3 A4	A1 A2 A3	A1 A2 A3 A4	A3 A4	A3 A4			A3 A4	A1 A2 A3	A1 A2 A3		
whois	ALL	A1	A2	B1 B2 B3 C1 C2 C3	B1 B2 B3 C1 C2 C3	C1	A5	A5 B1 B2 B3	A5 B1 B2 B3	A4	A5	A4 A2	A3	A4	A5	A1 A4	ALL	A5 B1	A4 A5 B1	A4 A5 B1	no			
						A1 A2 A3 A4	A1 A2			A1 A2	A1 A2			A1 A2	A1 A2			A1 A2						
				A1 A2 A3 A4 A4	A1 A2 A3 A4 A4	A4 B1 B2 B3	A3 A4	A1 A2 A3 A4	A1 A2 A3 A4	A3 A4	A3 A4	A1 A2 A3	A1 A2 A3 A4	A3 A4	A3 A4			A3 A4	A1 A2 A3	A1 A2 A3		
x509	ALL	A1	A2	B1 B2 B3 C1 C2 C3	B1 B2 B3 C1 C2 C3	C1	A5	A5 B1 B2 B3	A5 B1 B2 B3	A4	A5	A4 A2	A3	A4	A5	A1 A4	ALL	A5 B1	A4 A5 B1	A4 A5 B1	no			
						A1 A2 A3 A4	A1 A2			A1 A2	A1 A2			A1 A2	A1 A2			A1 A2						
				A1 A2 A3 A4 A4	A1 A2 A3 A4 A4	A4 B1 B2 B3	A3 A4	A1 A2 A3 A4	A1 A2 A3 A4	A3 A4	A3 A4	A1 A2 A3	A1 A2 A3 A4	A3 A4	A3 A4			A3 A4	A1 A2 A3	A1 A2 A3		
yabin	ALL	A1	A2	B1 B2 B3 C1 C2 C3	B1 B2 B3 C1 C2 C3	C1	A5	A5 B1 B2 B3	A5 B1 B2 B3	A4	A5	A4 A2	A3	A4	A5	A1 A4	ALL	A5 B1	A4 A5 B1	A4 A5 B1	no			
						A1 A2 A3 A4	A1 A2			A1 A2	A1 A2			A1 A2	A1 A2			A1 A2						
				A1 A2 A3 A4 A4	A1 A2 A3 A4 A4	A4 B1 B2 B3	A3 A4	A1 A2 A3 A4	A1 A2 A3 A4	A3 A4	A3 A4	A1 A2 A3	A1 A2 A3 A4	A3 A4	A3 A4			A3 A4	A1 A2 A3	A1 A2 A3		
yara	ALL	A1	A2	B1 B2 B3 C1 C2 C3	B1 B2 B3 C1 C2 C3	C1	A5	A5 B1 B2 B3	A5 B1 B2 B3	A4	A5	A4 A2	A3	A4	A5	A1 A4	ALL	A5 B1	A4 A5 B1	A4 A5 B1	no			
						A1 A2 A3 A4	A1 A2			A1 A2	A1 A2			A1 A2	A1 A2			A1 A2						
				A1 A2 A3 A4 A4	A1 A2 A3 A4 A4	A4 B1 B2 B3	A3 A4	A1 A2 A3 A4	A1 A2 A3 A4	A3 A4	A3 A4	A1 A2 A3	A1 A2 A3 A4	A3 A4	A3 A4			A3 A4	A1 A2 A3	A1 A2 A3		
youtube-channel	ALL	A1	A2	B1 B2 B3 C1 C2 C3	B1 B2 B3 C1 C2 C3	C1	A5	A5 B1 B2 B3	A5 B1 B2 B3	A4	A5	A4 A2	A3	A4	A5	A1 A4	ALL	A5 B1	A4 A5 B1	A4 A5 B1	no			
						A1 A2 A3 A4	A1 A2			A1 A2	A1 A2			A1 A2	A1 A2			A1 A2						
				A1 A2 A3 A4 A4	A1 A2 A3 A4 A4	A4 B1 B2 B3	A3 A4	A1 A2 A3 A4	A1 A2 A3 A4	A3 A4	A3 A4	A1 A2 A3	A1 A2 A3 A4	A3 A4	A3 A4			A3 A4	A1 A2 A3	A1 A2 A3		
youtube-comment	ALL	A1	A2	B1 B2 B3 C1 C2 C3	B1 B2 B3 C1 C2 C3	C1	A5	A5 B1 B2 B3	A5 B1 B2 B3	A4	A5	A4 A2	A3	A4	A5	A1 A4	ALL	A5 B1	A4 A5 B1	A4 A5 B1	yes			
						A1 A2 A3 A4	A1 A2			A1 A2	A1 A2			A1 A2	A1 A2			A1 A2						
				A1 A2 A3 A4 A4	A1 A2 A3 A4 A4	A4 B1 B2 B3	A3 A4	A1 A2 A3 A4	A1 A2 A3 A4	A3 A4	A3 A4	A1 A2 A3	A1 A2 A3 A4	A3 A4	A3 A4			A3 A4	A1 A2 A3	A1 A2 A3		
youtube-playlist	ALL	A1	A2	B1 B2 B3 C1 C2 C3	B1 B2 B3 C1 C2 C3	C1	A5	A5 B1 B2 B3	A5 B1 B2 B3	A4	A5	A4 A2	A3	A4	A5	A1 A4	ALL	A5 B1	A4 A5 B1	A4 A5 B1	no			
						A1 A2 A3 A4	A1 A2			A1 A2	A1 A2			A1 A2	A1 A2			A1 A2						
				A1 A2 A3 A4 A4	A1 A2 A3 A4 A4	A4 B1 B2 B3	A3 A4	A1 A2 A3 A4	A1 A2 A3 A4	A3 A4	A3 A4	A1 A2 A3	A1 A2 A3 A4	A3 A4	A3 A4			A3 A4	A1 A2 A3	A1 A2 A3		
youtube-video	ALL	A1	A2	B1 B2 B3 C1 C2 C3	B1 B2 B3 C1 C2 C3	C1	A5	A5 B1 B2 B3	A5 B1 B2 B3	A4	A5	A4 A2	A3	A4	A5	A1 A4	ALL	A5 B1	A4 A5 B1	A4 A5 B1	yes			