Hardening de Sistemas com CIS *Benchmark*

Mestrado em Cibersegurança e Informática Forense

Jéssica Pereira Ferreira

Leiria, dezembro de 2020

Hardening de Sistemas com CIS *Benchmark*

Mestrado em Cibersegurança e Informática Forense

Jéssica Pereira Ferreira

Estágio realizado por Jéssica Pereira Ferreira sob a orientação da Professora Doutora Beatriz Piedade e supervisão de Andreia Francisco.

Leiria, dezembro 2020

Originalidade e Direitos de Autor

O presente relatório de estágio é original, elaborado unicamente para este fim, tendo sido devidamente citados todos os autores cujos estudos e publicações contribuíram para o elaborar.

Agradecimentos

Desde o início da licenciatura até ao presente momento de conclusão do grau de mestre, contei com a confiança e apoio de inúmeras pessoas. A elaboração deste documento e o meu sucesso ao finalizar esta etapa da minha vida não seria possível sem o apoio direto ou indireto das pessoas que caminharam ao meu lado e que nunca me deixaram vacilar. A todos quero expressar o meu sincero agradecimento.

Em primeiro lugar à minha orientadora Beatriz Piedade pelo apoio na concretização deste projeto. Obrigada por todo o conhecimento transmitido e a total disponibilidade para esclarecer dúvidas e incertezas.

Um agradecimento especial à minha orientadora na empresa, Andreia Francisco, por me guiar no melhor caminho e me dar força todos os dias. Pela incansável disponibilidade e boa disposição, por acreditar em mim e me motivar a seguir em frente nos momentos difíceis. Obrigada pela enorme paciência, profissionalismo e interesse neste projeto e no meu trabalho. Uma amizade que espero guardar para a vida.

Eterna gratidão aos meus pais, por serem a minha rocha desde o início da minha vida, por nunca me deixarem desistir e estarem sempre presentes com uma palavra de conforto, carinho e motivação. Estou grata pelos valores, apoio e compreensão demonstrados constantemente que foram, e são, a minha força diariamente. Dedico todo o meu sucesso passado, presente e, certamente, futuro a vocês.

Às minhas irmãs um obrigado especial por me guiarem com a vossa sabedoria, pelo amor de irmão todos os dias, pelas palavras de incentivo e pelas palavras de repreensão, mesmo estando longe estão sempre presentes. Gostaria de deixar um agradecimento muito especial aos meus sobrinhos, o melhor que a vida me deu.

Nada do que possa dizer fará justiça à gratidão que sinto pelo que fizeste por mim ao longo destes anos. Mal posso esperar para ver tudo o que alcançaremos juntos, obrigada, João Marques.

Obrigada à família que esta academia me deu: João Galvão, Marisa Borges, Tiago Sousa. Incansáveis sempre, os irmãos que eu escolhi.

Não podia ter escolhido melhor instituição na qual prosseguir os meus estudos, obrigada Politécnico de Leiria. Eterna gratidão a todos os docentes que me ensinaram tudo o que sei hoje. Um agradecimento muito especial ao Professor Mário Antunes que tanta força e alento me deu, por despertar em mim força e determinação que não pensava ter e por acreditar, especialmente quando eu não acreditava, que eu podia ser mais e através das suas palavras hoje sou mais.

Resumo

No que toca à segurança de dados, é importante garantir que o perímetro de ataque a sistemas críticos é o menor possível adotando medidas, entre as quais, a implementação de um plano de conformidade com configurações de sistemas operativos consideradas seguras.

Um plano de conformidade deve conter todos os passos necessários para implementar configurações de acordo com *benchmarks* de segurança aceites e definidas mundialmente por profissionais. Uma *benchmark* de segurança é um conjunto de instruções e procedimentos para a configuração de um produto informático, de modo a verificar que esse mesmo produto foi configurado adequadamente. Estas configurações quando aplicadas a sistemas operativos devem ser analisadas e implementadas de modo a mitigar as vulnerabilidades associadas a configurações por defeito.

As *benchmarks* de segurança fazem parte de um processo de segurança mais abrangente denominado *hardening* cujo objetivo final é o de eliminar os meios de intrusão disponíveis num sistema através da correção de vulnerabilidades e da desativação de serviços não essenciais.

Este documento apresenta todo o trabalho desenvolvido em âmbito de estágio enquadrado no Mestrado em Cibersegurança e Informática Forense do Instituto Politécnico de Leiria. O projeto principal do estágio foi o de definição de um plano de conformidade com a *benchmark* disponibilizada pela CIS (*Center for Internet Security*), utilizando como ferramenta de análise de não conformidades o *Cyberwatch*. São apresentadas ao longo do documento, *benchmarks* e soluções de análise de não conformidade alternativas acompanhadas de respetivo estudo comparativo. Adicionalmente ao trabalho de conformidade descrito são descritas tarefas de resposta a incidentes de segurança e aplicação de mecanismos de segurança em ambiente *kubernetes* na *Google Cloud*.

Apresenta-se no final deste documento uma reflexão crítica onde se propõe uma ferramenta alternativa à *Cyberwatch* utilizada em âmbito de estágio, para análise de conformidades com a CIS *Benchmark*.

Palavras-chave: Segurança de Sistemas, Segurança na Cloud, *Hardening*, *Benchmark*, Vulnerabilidade, Conformidade.

Abstract

It is important when it comes to data security, to ensure that the perimeter of potential security attacks to critical systems is as small as possible through the implementation of security measures such a compliance plan with system configurations that are considered more secure than the ones presented by default.

A compliance plan should include all the necessary steps to implement system configurations according to security benchmarks accepted and defined by contributing security professionals around the world. A security benchmark is a series of instructions or procedures used to configure an IT product and help verify if said product was configured correctly. These configurations, when applied to operating systems, must be analysed, and implemented to correct vulnerabilities associated with default configurations.

Security benchmarks are a part of a broader security process called hardening, which final goal is to eliminate the means of unauthorized system access through the correction of vulnerability issues and the disabling of non-essential services.

This document shows the work developed during an internship within the scope of the Master's degree in Cybersecurity and Digital Forensics by the Polytechnic Institute of Leiria. The main project that took place during the internship was the development of a compliance plan with the benchmark provided by the Center for Internet Security, using Cyberwatch as the non-compliance analyses tool. Throughout the document, alternatives to the benchmark and Cyberwatch tool are presented along with concerning comparative studies. In addition to the developed compliance work, this document describes tasks regarding incident response analysis and security mechanisms in Google Kubernetes Environment.

A critical analysis is presented at the end of this document, where an alternative tool to the Cyberwatch used for the internship is suggested along with a comparative study between them.

Keywords: System Security, Cloud Security Hardening, CIS Benchmark, Vulnerability, Compliance.

Índice

Lista de Figuras

Lista de Tabelas

Lista de Siglas e Acrónimos

ARF	Abuse Reporting Format
AWS	Amazon Web Services
CCE	Common Configuration Enumeration
CCSS	Common Configuration Scoring System
CIS	Center for Internet Security
CIS-CAT	CIS-Configuration Assessment Tool
CNA	CVE Numbering Authorities
CPE	Common Platform Enumeration
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DDoS	Distributed Denial of Service
DEV	Development
DISA	Defence Information System Agency
EUA	Estados Unidos da América
GCP	Google Cloud Platform
GKE	Google Kubernetes Environment
IAM	Identity and Access Management
ISO	International Organization for Standardization

NCP	National Checklist Program
NIST	National Institute of Standards and Technology
NIST-NCP	NIST-National Checklist Program
OCIL	Open Checklist Interactive Language
OPA	Open Policy Agent
OPS	Operations
OVAL	Open Vulnerability and Assessment Language
OWASP	Open Web Application Security Project
PCI DSS	Payment Card Industry – Data Security Standard
RACI	Responsible Accountable Consulted Informed
RBAC	Role-Base Access Control
SaaS	Software as a Service
SCAP	Security Content Automation Protocol
SIEM	Security Information and Event Management
SOC	Security Operations Center
SQL	Structured Query Language
SRG	Security Requirement Guides
STIG	Security Technical Implementation Guides
SWID	SoftWare IDentification
TMSAD	Trust Model for Security Automation Data
XCCDF	Extensible Configuration Checklist Description Format
XML	Extensible Markup Language

1 Introdução

Em 1999, Peter Ducker no seu livro *Management challenges for the 21st century* [1], considerou que "a difusão de tecnologia e a comercialização de informação transforma o papel da informação num recurso igualmente valioso a recursos que tradicionalmente o eram, como terreno e património". Esta afirmação previu com exatidão aquilo que vivemos nos dias de hoje, onde os bens críticos de uma empresa são, principalmente, a sua informação e reputação.

As empresas procuram cada vez mais a digitalização dos seus processos de negócio inserindo-se desta forma no mercado global que vemos atualmente. De modo a proteger a informação crítica é necessária a implementação de mecanismos de segurança nos sistemas que a contêm e que mitiguem vulnerabilidades potencialmente exploradas no roubo de informação.

À medida que vão sendo descobertas, informações sobre vulnerabilidades em sistemas informáticos são adicionadas a um repositório público aumentado a sua visibilidade. Este repositório é uma mais valia não só para profissionais de segurança como também para atacantes pois, para o primeiro, permite a mitigação de vulnerabilidades para que estas não sejam exploradas, para o último, permite que estas sejam rapidamente exploradas num ataque quando não são mitigadas prontamente. Esta informação disponibilizada publicamente, incentiva as empresas a adotar processos de gestão de vulnerabilidades.

À medida que os sistemas informáticos se tornam mais robustos, as técnicas de intrusão e exploração indevida acompanham esta evolução reinventando-se e desenvolvendo novos vetores de ataque. Dito isto, os profissionais de segurança informática devem definir políticas, processos e mecanismos não só para análise e mitigação de vulnerabilidades, mas também para a resposta a incidentes de segurança. Estes são fundamentais para garantir a segurança da informação e, no caso de intrusão, reduzir significativamente a perda de dados e de reputação.

Um aspeto nos sistemas informáticos onde existem vulnerabilidades que podem ser ignoradas são nas configurações existentes por defeito. Grande parte dos sistemas e

aplicações informáticas apresentam configurações que permitem que estes sejam utilizados pelo público em geral, o que significa um aumento na simplicidade da sua utilização em detrimento da sua segurança. Num ambiente empresarial este cenário não é ideal devido à importância que a informação contida digitalmente significa para o negócio. Desta forma, é necessário definir para estes sistemas um conjunto de configurações consideradas seguras minimizando assim as vulnerabilidades apresentadas por configurações padrão.

A implementação de mecanismos de segurança é um processo árduo devido à complexidade e heterogeneidade dos sistemas informáticos utilizados em contexto empresarial. Dada a variedade de tecnologias, protocolos, sistemas operativos e aplicações que constituem um negócio, o estudo das inúmeras configurações necessárias para garantir a segurança destes, torna-se impraticável ou insuficiente sem um documento que o normalize.

Dada esta necessidade, institutos e especialistas de segurança desenvolveram documentos com listas extensas de configurações seguras aplicáveis a uma grande variedade de componentes informáticos desde sistemas operativos a aplicações, a ferramentas e processos *cloud*. A estes documentos dá-se o nome de *checklists* ou *benchmarks* de segurança. Estas *benchmarks* garantem que as empresas conseguem atingir um nível satisfatório de segurança pois as configurações ativas estão limitadas ao mínimo e essencial para o funcionamento devido do sistema. Para além das vantagens de segurança apresentadas no uso de *benchmarks*, estas também permitem uma melhor monitorização e administração do sistema na sua generalidade, dado que existe um maior controlo sobre o que este contém.

As *checklists* de segurança fazem parte de um processo denominado de *hardening*, processo este que deve fazer parte de uma política de segurança e pretende definir uma base de segurança para sistemas. *Hardening* aplica a regra de *least priviledge* (privilégio mínimo) a um sistema, ou seja:

- Os privilégios de acesso concedidos a sistemas são os menores possíveis, mas que ainda assim permitam executar as tarefas necessárias no sistema de modo transparente.
- Os serviços, ferramentas, aplicações e portos de rede presentes no sistema são reduzidos ao estritamente necessário caso contrário devem ser desativados ou removidos.

A aplicação da regra de *least priviledge* reduz significativamente os vetores de intrusão num sistema uma vez que tudo o que é utilizado é identificado, documentado e a sua necessidade é justificada.

As *benchmarks* reconhecidas por instituições e especialistas de segurança são a *Center for Internet Security Benchmarks* (CIS *Benchmark*) e as DISA-STIG (*Defence Information System Agency - Security Technical Implementation Guides*), ambas apresentam configurações seguras igualmente válidas que serão abordadas e comparadas neste trabalho.

O processo de análise de conformidade com *benchmarks*, tem uma dificuldade acrescida quando esta não é automatizada através de ferramentas e protocolos que garantam a interoperabilidade das operações. Dada esta necessidade, este trabalho sugere várias ferramentas e protocolos, reconhecidos por especialistas e considerados *standard*, que agilizam o processo de configuração segura de sistemas.

O foco principal do trabalho desenvolvido em âmbito de estágio enquadrado no Mestrado em Cibersegurança e Informática Forense, foi a implementação prática de todos estes conceitos. Este documento representa um caso de estudo no que toca a definição, manutenção e implementação de um plano de configurações seguras em sistemas operativos Unix utilizando como principal diretriz a CIS *Benchmark*, numa empresa de *e-commerce*.

1.1 Objetivos de Estágio

Os objetivos do estágio enquadrado no mestrado de cibersegurança e informática forense são:

- Obtenção de conhecimentos aprofundados sobre *benchmarks* de segurança com foco nas diretrizes da CIS *Benchmark*.
- Estudo de ferramentas e protocolos utilizados na análise de não conformidades com *benchmarks* de segurança, tais como a ferramenta *Cyberwatch*.
- Formação de administração e gestão da ferramenta *Cyberwatch*.
- Teste de implementação das diretrizes CIS *Benchmark* no sistema operativo Unix.
- Definição de um plano de conformidade com a CIS B*enchmark* para sistemas Unix da empresa onde decorreu o estágio.
- Definição de um plano corretivo de não conformidades com a CIS B*enchmark* para todas as máquinas Unix da empresa onde decorreu o estágio.

- Elaboração de documentação sobre os trabalhos de conformidade desenvolvidos.
- Execução de tarefas diárias e participação em projetos empresariais ao abrigo da equipa de segurança.
- Integração no mercado de trabalho.

1.2 Organização do Documento

Para além do presente capítulo este documento está organizado da seguinte forma:

No Capítulo 2, caracteriza-se a entidade de acolhimento e descreve-se as diferentes equipas que fazem parte da empresa com destaque na equipa de segurança, as suas responsabilidades e os seus maiores desafios.

No Capítulo 3, abordam-se conceitos fundamentais sobre vulnerabilidades, *hardening*, *benchmarks* de segurança e segurança por defeito.

No Capítulo 4, desenvolveu-se um estudo sobre normas de segurança e mecanismos utilizados na sua automatização.

No Capítulo 5, descreve-se todo o trabalho realizado em âmbito de estágio e apresentam-se os resultados obtidos nos projetos desenvolvidos nomeadamente o plano de conformidade com a CIS *Benchmark*, resolução de incidentes de segurança e a definição de mecanismos de segurança em *Google Kubernetes Environment*.

No Capítulo 6, apresenta-se uma análise crítica e proposta de melhoria.

No Capítulo 7, reflete-se sobre todo o trabalho desenvolvido no estágio curricular enquadrado no Mestrado de Cibersegurança e Informática Forense.

2 Caracterização da Entidade de Acolhimento

Este capítulo tem como principal objetivo caracterizar e apresentar a empresa no âmbito da qual o estágio decorreu.

Num primeiro momento descreve-se a empresa e o seu modelo de negócio.

Seguidamente apresenta-se, de um modo geral, as equipas envolvidas no negócio.

Na secção 2.3 descreve-se a equipa de segurança na qual se integrou o estágio e os seus principais desafios.

Finalmente na secção 2.4 expõem-se uma síntese de todos os aspetos a reter sobre a entidade de acolhimento.

2.1 Negócio

A empresa na qual o estágio curricular se integrou caracteriza-se, quanto ao negócio, como comércio digital, ou seja, e-commerce. Segundo o glossário da Gartner [1] , " *digital commerce* permite a compra de bens e serviços através de uma experiência interativa e *self-service*. Inclui pessoas, processos e tecnologias necessárias para executar a oferta de desenvolvimento de conteúdo, análise, promoção, preçários, aquisição e retenção de clientes em todos os pontos no processo de compra".

No que diz respeito à localização, a empresa caracteriza-se como sendo uma multinacional, ou seja, incorpora várias filiais em países diferentes que trabalham em conjunto para manter a plataforma de vendas online disponível continuamente. A entrega de artigos está disponível mundialmente com foco na Europa e Rússia.

Com mais de 180 anos de existência, esta empresa modernizou-se ao longo dos anos para se manter relevante no mercado. No passado, os seus artigos eram consultados através de catálogos físicos e encomendados por via telefónica ou por carta. Já nos dias de hoje, todo o processo de venda ocorre exclusivamente através do *website* disponível para o efeito. Esta presença online agiliza todo o processo de venda de artigos e coloca uma maior carga na componente informática que serve de base ao negócio.

Tendo em conta que toda a base do negócio assenta numa plataforma online, a prioridade de todas as equipas é de a manter funcional e com o mínimo de inatividade possível, dado que o mal funcionamento desta, leva a uma direta diminuição de encomendas e, consequentemente, perdas de faturação.

2.2 Departamentos

A empresa divide-se em departamentos todos eles com papéis distintos e importantes para o negócio. Destes é possível destacar dois de maior relevância para o estágio: Desenvolvimento (DEV) e Operações (OPS).

2.2.1 Desenvolvimento

O departamento de desenvolvimento é responsável pelo desenvolvimento de aplicações para o sistema informático da empresa, estando diretamente relacionado com o departamento de operações e com as equipas que fazem a ponte entre as tecnologias de informação e o negócio.

2.2.2 Operações

O departamento de operações abrange a equipa de segurança e foca-se principalmente em serviços informáticos que mantêm toda a infraestrutura empresarial disponível vinte e quatro horas por dia.

As principais responsabilidades deste departamento são:

- Criação e manutenção de servidores;
- Gestão e comunicação direta com parceiros de negócio, *Datacenters* e *Cloud providers*;
- Implementação e manutenção de processos de monitorização da infraestrutura;
- Supervisão de serviços e resposta a incidentes vinte e quatro horas por dia;
- Teste de aplicações em ambientes controlados;
- Automatização de processos e investigação de novas tecnologias.

2.3 Equipa de Segurança

Esta equipa é transversal a todas as outras, ou seja, não só tem a seu encargo tarefas únicas de segurança como também participa ativamente na mitigação de problemas que ocorram noutras equipa e dá o seu parecer na maior parte das decisões de cariz informático.

De um modo geral, a equipa de segurança tem os seguintes encargos:

- Resolução e mitigação de incidentes de segurança;
- Gestão de atualizações em sistemas;
- Definição de regras e políticas de segurança;
- Aumento constante do nível de segurança através de processos tais como testes de penetração aos serviços e aplicações da empresa.

2.3.1 Desafios de Segurança

A empresa deve o seu sucesso atual à sua forte presença no online. No entanto, esta presença é também responsável por grande parte dos desafios de segurança que a empresa enfrenta.

É da responsabilidade da equipa de segurança manter o *website* seguro contra incidentes de segurança informática. Este processo envolve vários controlos nos quais se podem destacar:

- Garantir que os servidores estão atualizados e em conformidade com *standards* de segurança;
- Controlar e avaliar permissões de utilizadores;
- Gerir políticas de passwords;
- Definir processos de resposta a incidentes de segurança.

2.4 Síntese

A empresa na qual se inseriu o estágio curricular caracteriza-se quanto ao negócio como *e-commerce*, ou seja, é um negócio de venda de bens através da internet. Representa uma empresa multinacional de venda de produtos de artigos de vestuário e têxtil-lar com mais de 180 anos de existência.

Os departamentos com mais impacto para o estágio foram os de desenvolvimento e operações, cada um com tarefas bem definidas de suporte ao negócio.

A equipa de segurança é transversal a todas as outras trabalhando ativamente na mitigação de problemas e no aconselhamento de assuntos de segurança.

Os principais desafios de segurança que a empresa enfrenta são provenientes da sua forte presença online através de ataques DDoS, como por exemplo, *credencial scrapping* onde se pretende obter credenciais de utilizadores da plataforma de vendas através da inserção repetitiva de credenciais até à autenticação com sucesso.

3 Conceitos Fundamentais

Neste capítulo serão abordados os conceitos fundamentais à compreensão do trabalho desenvolvido em estágio.

Primeiramente aborda-se o conceito de vulnerabilidades em sistemas informáticos e os processos inerentes ao mesmo.

Seguidamente aborda-se o conceito de *hardening* e *benchmarks* assim como as vantagens da implementação de *hardening* e a importância da automatização destes processos.

Na secção 3.3 apresenta-se do conceito de segurança por defeito.

Finalmente na secção 3.4 disponibiliza-se uma síntese de todos estes conceitos fundamentais apresentando as ideias principais a reter deste capítulo.

3.1 Vulnerabilidades em Sistemas Informáticos

A NIST (*National Institute of Standards and Technology*), na sua diretriz de controlos de acessos [2], define vulnerabilidade como sendo "um ponto fraco nos procedimentos, hardware, desenho, implementação, controlos internos, controlos técnicos, controlos físicos ou outros controlos de sistemas de segurança que podem ser acionados acidentalmente ou explorados intencionalmente resultando numa violação das políticas de segurança de um sistema".

De modo a entender os desafios de segurança que as empresas enfrentam é necessário entender as vulnerabilidades que existem nos sistemas e que podem ser utilizadas por entidades maliciosas para os comprometer. Dada esta necessidade, surgiram listas disponibilizadas publicamente contendo informações detalhadas sobre vulnerabilidades, conhecidas como CVE (*Common Vulnerabilities and Exposures*).

O site oficial da entidade responsável pelas listas de CVE, MITRE, define-as como [3] uma lista de identificadores comuns para vulnerabilidades de segurança conhecidas publicamente. O uso de registos CVE, que são atribuídos por CNAs (CVE *Numbering*

Authorities) por todo o mundo, garantem confidencialidade entre entidades quando utilizados para discutir ou partilhar informação sobre uma vulnerabilidade única de um *software* ou *firmware*, oferece uma base para avaliação de ferramentas, e possibilita a troca de dados de forma automatizada. Os CVE são recomendados pela indústria via CNA, quadro CVE e outros produtos e serviços que utilizam CVE, e oferecem:

- Um identificador único para uma vulnerabilidade ou erro;
- Uma descrição com um formato pré-definido para cada vulnerabilidade ou erro;
- Um dicionário de vulnerabilidades e não uma base de dados;
- O modo como diferentes bases de dados e ferramentas com diferentes linguagens conseguem comunicar de forma transparente;
- O caminho para interoperabilidade e uma maior abrangência de segurança;
- Uma base para avaliação de serviços, ferramentas e bases de dados;
- Transferência livre e uso público.

As listas de vulnerabilidades dependem dos esforços voluntários dos CNAs dos quais fazem parte fabricantes de tecnologias, investigadores de vulnerabilidades, entidades certificadoras e programas de *bug bounty*. Quando é descoberta uma vulnerabilidade, estas entidades têm a autoridade para lhe atribuir um registo CVE e disponibilizá-lo publicamente sem aprovação ou comunicação direta com as equipas CVE.

A disponibilização ao público dos detalhes e informações destas vulnerabilidades permite que várias entidades, como é o caso da NIST [4], criem bases de dados com estas informações o que, consequentemente, facilita o processo de descoberta e mitigação de vulnerabilidades. Estas bases de dados CVE permitem a criação de mecanismos de gestão automatizada de vulnerabilidades e a avaliação do nível de segurança de um sistema.

Os CVE são também classificados de modo a determinar a gravidade de uma eventual exploração da vulnerabilidade que representam. Os passos para esta classificação são definidos no CVSS (*Common Vulnerability Scoring System*), uma *framework* pública que divulga as características e a gravidade associadas a vulnerabilidades em sistemas [5]. Na Tabela 1 pode-se constatar o sistema de pontuação utilizado pelo CVSS, sendo que quanto maior a pontuação maior o impacto que a vulnerabilidade pode ter nos sistemas informáticos.

Gravidade	*Pontuação Base*
Nenhuma	0.0
Baixa	0.1-3.9
Média	4.0-6.9
Alta	7.0-8.9
Crítica	9.0-10.0

Tabela 1 – Pontuação para determinação de gravidade de vulnerabilidades

O sistema de classificação baseia-se em três grupos de métricas: base, temporal e ambiental definidos como [6] :

- Base: representam as qualidades intrínsecas de uma vulnerabilidade que são constantes ao logo do tempo e transversais a todos os ambientes.
- Temporal: este grupo representa as características de uma vulnerabilidade que mudam ao longo do tempo.
- Ambiental: representa as características de uma vulnerabilidade que mudam tendo em conta o seu contexto (ambiente).

Com base nos fatores acima e como apresentado na Tabela 1, é possível determinar e atribuir o grau de gravidade de uma vulnerabilidade, podendo este ser um dos seguintes:

- Baixo: Vulnerabilidade que, quando explorada num ataque informático, tem um impacto baixo no negócio. Para tirar partido desta vulnerabilidade é necessário, tipicamente, acesso local ou físico aos sistemas.
- Médio: Vulnerabilidades que, para serem exploradas, exigem que um atacante manipule um indivíduo através de técnicas de engenharia social, realize ataques de negação de serviço de difícil configuração, execute *exploits* na mesma rede do sistema alvo ou obtenha uma conta de utilizador com privilégios de acesso ao sistema tipicamente limitados.
- Alto: A vulnerabilidade é difícil de explorar, mas, quando bem sucedida, resulta em privilégios de administração de sistema e perdas de dados significativas ao longo do tempo.

- Crítico: A exploração de uma vulnerabilidade com esta classificação resulta em acessos com privilégios *root*. Tipicamente não requer conhecimentos aprofundados sobre técnicas de intrusão. As atualizações de segurança são imperativas após a deteção de vulnerabilidades com esta gravidade.

Esta classificação, obtida através dos critérios disponibilizados pela CVSS, é utilizada pelas empresas de forma a priorizar a mitigação de vulnerabilidades. Tipicamente priorizam-se as vulnerabilidades críticas e altas pois representam danos significativos para o negócio.

Os fabricantes de tecnologias e sistemas disponibilizam periodicamente atualizações de segurança que mitigam vulnerabilidades com CVE público referentes aos seus ativos. Este facto ilustra a importância que um processo de gestão de atualizações tem numa gestão eficiente de vulnerabilidades.

Outros tipos de vulnerabilidades de segurança como as representadas aquando de definição de passwords fracas e de configurações inseguras, não têm um CVE associado que seja detetável em *scans* de vulnerabilidades, logo necessitam de políticas e processos de segurança adicionais para serem mitigadas. Este processo é abrangido pelo conceito de *hardening* de sistemas.

3.2 *Hardening*

Segundo a publicação especial da NIST sobre sistemas de gestão de chaves de cifra [7] , *Hardening* é definido como "um processo cujo objetivo final é o de eliminar os meios de intrusão disponíveis num sistema através da correção de vulnerabilidades e da desativação de serviços não essenciais".

A maneira mais eficaz de criação de processos de *hardening* por parte das empresas, é através da sua adaptação seguindo diretrizes e boas práticas de segurança comprovadas como eficazes pelas entidades especialistas. Esta abordagem torna os processos robustos e abrangentes, sem retirar a flexibilidade de adaptação às exigências de segurança e objetivos de negócios únicos a cada empresa.

Um dos passos na elaboração de processos de *hardening* é a escolha e implementação de um conjunto de configurações seguras para sistemas operativos e aplicações. Para este efeito, existem documentos denominados *benchmarks* ou *checklist* de segurança, que

oferecem um conjunto de configurações consideradas seguras por especialistas e que as empresas podem adaptar às suas necessidades de *hardening*.

3.2.1 *Benchmarks* de Segurança

Segundo a publicação especial da NIST 800-70 *National Checklist Program for IT Products – Guidelines for Checklist Users and Developers* [8] , uma *checklist* de configurações de segurança (também definida como *lockdown*, guias de *hardening*, guias de segurança, *security technical implementation guides* e *benchmarks*) são um conjunto de instruções e procedimentos para a configuração de um produto informático, de modo a verificar que este foi configurado adequadamente, e/ou para identificar mudanças não autorizadas ao produto."

Os documentos de *benchmarks* de segurança contêm um conjunto de diretrizes que representam um estado de segurança alvo, estas são utilizadas consequentemente como meio comparativo com o estado atual de outros sistemas. Esta comparação permite definir um plano com um conjunto de processos adicionais, de modo a implementar as configurações de segurança consideradas relevantes posteriormente.

As *checklists* estão disponibilizadas na internet para transferência gratuita e são estudadas e definidas por fabricantes de *software*/*hardware* e/ou por outras organizações tecnicamente competentes em assuntos de segurança de informação.

Fazem parte do conteúdo de uma *benchmark* ou *checklist* de segurança:

- Ficheiros de configuração que analisam ou implementam várias configurações relacionadas com segurança (e.g. executáveis, *templates* de segurança com capacidade de alteração de definições, ficheiros em formato XML (*Extensible Markup Language*) de SCAP (S*ecurity Content Automation Protocol*) e scripts).
- Documentação (e.g. ficheiros de texto) de guia à implementação da *benchmark* manualmente.
- Apresentação de métodos recomendados para instalar e configurar o sistema.

3.2.2 Vantagens do uso de *Benchmarks*

A aplicação de uma *benchmark* de segurança, é utilizada para reforçar a postura de segurança de uma organização. Adicionalmente, os benefícios do uso de configurações de segurança definidas pela indústria são, segundo a NIST [8]:

- Obtenção de um nível de segurança base para proteção contra ameaças locais e remotas comuns (e.g. *malware*, ataques *Denial of Service* e acesso não autorizado).
- Redução significativa do tempo e esforço necessário na pesquisa e desenvolvimento de configurações de segurança em sistemas e aplicações.
- Possibilidade de empresas pequenas utilizarem recursos eficientes para implementação de configurações de segurança.
- Redução de perda de reputação como resultado de sistemas comprometidos por uma intrusão aos sistemas informáticos.

3.2.3 Automatização

Quando se trabalha com documentos de *benchmark* é necessário compreender que estes são tipicamente ficheiros longos, por exemplo, as diretrizes da CIS *Benchmark* (*Center for Internet Security Benchmark*) sugerem cerca de 216 configurações para o sistema operativo CentOS7. Tendo em conta que existe uma *benchmark* específica para cada versão de um sistema operativo, a análise, teste e reconfiguração manual dos sistemas é um processo impraticável no contexto empresarial.

A automatização destes processos é fundamental pois reduz a carga de trabalhos e o erro humano resultante de implementações manuais. Dada esta necessidade, surgiram ferramentas capazes de apresentar cada diretriz num formato executável, automatizando o processo de teste de conformidade do sistema alvo com a *benchmark* escolhida. O estudo de ferramentas de automatização de *benchmarks* e outras diretrizes de segurança deve ser uma prioridade para as empresas.

3.3 Segurança por defeito

No desenvolvimento de aplicações, existe o conceito de *shift left* cujo objetivo é a introdução de um processo contínuo de resolução de problemas à medida que estes vão surgindo através da implementação de etapas de teste em todo o ciclo de vida de desenvolvimento de software.

Em segurança, este conceito também se aplica através do conceito de segurança por defeito onde se procura implementar processos, mecanismos e políticas de segurança cada vez mais cedo nas infraestruturas empresariais. Esta abordagem garante que a segurança não é uma ação pontual, mas sim um processo em contante mudança e adaptável ao seu contexto.

A segurança deve ser conveniente, disponível, transparente e eficiente. É necessário dar aos colaboradores ferramentas que estes possam compreender e executar sozinhos. Para se atingir segurança por defeito é necessário incluir as pessoas na política de segurança para que estas possam ser também uma linha de defesa contra o cibercrime. Ações de formação periódicas sobre a política de segurança e o papel do colaborador como agente de segurança na empresa, devem ser obrigatórias.

3.4 Síntese

Uma vulnerabilidade é uma falha de segurança num sistema informático que, quando não é mitigada atempadamente, pode ser explorada num ataque informático do qual podem resultar perdas substanciais para um negócio. Todas as vulnerabilidades descobertas são publicadas em repositórios públicos com um identificador único (CVE) e uma classificação de gravidade (CVSS). Todos estes indicadores que caracterizam uma vulnerabilidade são atribuídos por entidades voluntárias (CNA). A classificação de gravidade atribuída a um CVE ajuda as empresas a definir prioridades na mitigação de vulnerabilidades. São necessários processos de gestão de atualizações uma vez que é através destes que fabricantes disponibilizam mitigações para vulnerabilidades dos sistemas aos quais dão suporte.

As *Benchmarks* fazem parte de uma política de segurança sendo utilizadas no processo de comparação do estado de segurança de um sistema com um estado de segurança desejado. Este estado é representa um conjunto de configurações consideradas mais seguras do que as disponíveis num sistema por defeito. As *benchmarks* são documentos extensos com centenas de configurações de segurança que podem ser adaptadas às necessidades de segurança

especificas de um negócio. Existem ferramentas que permitem analisar as não conformidades com *benchmarks* de forma automatizada reduzindo assim a carga de trabalhos acrescida aquando de verificações manuais assim como o erro humano associado a estas.

Processos, tais como os de *hardening* de um sistema operativo, estão sujeitos a mudanças constantes. Á medida que o sistema evolui os processos de *hardening* devem evoluir com ele.

A segurança por defeito requer a implementação de mecanismos de segurança o mais cedo possível na infraestrutura e processos de negócio de uma organização, desta forma, a segurança pode evoluir e adaptar-se às exigências do negócio ao longo do tempo.

A segurança deve ser conveniente, disponível, transparente e eficiente quando aplicada ao trabalho de colaboradores. Desta forma garante-se que as ações inseguras são as mais difíceis de executar enquanto que as ações seguras são a maneira mais fácil e intuitiva de trabalhar.

Uma empresa pode ter uma política de segurança abrangente e processos de segurança devidamente implementados, mas todos estes podem ser comprometidos se as pessoas não souberem o seu papel como agentes ativos contra ataques informáticos.

4 Estado da Arte

Neste capítulo são abordados exemplos de *benchmaks* de segurança e mecanismos de apoio à adoção das diretrizes.

Num primeiro momento serão abordadas normas de segurança, especificamente a CIS *Benchmark* e a DISA-STIG, seguida de uma análise comparativa das mesmas.

Seguidamente serão apresentados mecanismos de apoio à automatização de *benchmarks* de segurança, especificamente CIS-CAT, SCAP, NIST NCP e processos de gestão centralizada de configurações.

Finalmente na secção 4.3 será feita uma síntese com ideias principais a reter deste capítulo.

4.1 Normas de Segurança

Dada a presença online, muitas vezes indispensável das empresas, são desenvolvidas normas de segurança para proteção contra ataques aos sistemas informáticos e para garantir a disponibilidade, integridade e confidencialidade de informação. Muitas vezes a conformidade com estas regras é obrigatória sendo precedida de uma certificação por parte de uma entidade reguladora.

A Figura 1 retirada de [9], representa *standards* utilizados mundialmente. A ISO 27001 (*International Organization for Standardization*) apresenta diretrizes e conselhos sobre como definir, implementar e manter um ambiente empresarial seguro. A conformidade com esta norma é obrigatória, mas é recomendada pois os seus conselhos são transversais para qualquer organização com sistemas informáticos que pretenda aumentar os seus níveis de segurança.

A PCI-DSS (*Payment Industry Data Security Standard*) por sua vez, é uma norma de conformidade obrigatória para qualquer entidade que lide com dados de cartões de crédito. Este negócio exige regras rígidas tendo em conta a sensibilidade dos dados armazenados, processados e transmitidos pelos sistemas. Para normas sujeitas a obrigatoriedade, as empresas são alvo de auditorias rigorosas onde devem mostrar evidências da aplicação da mesma.

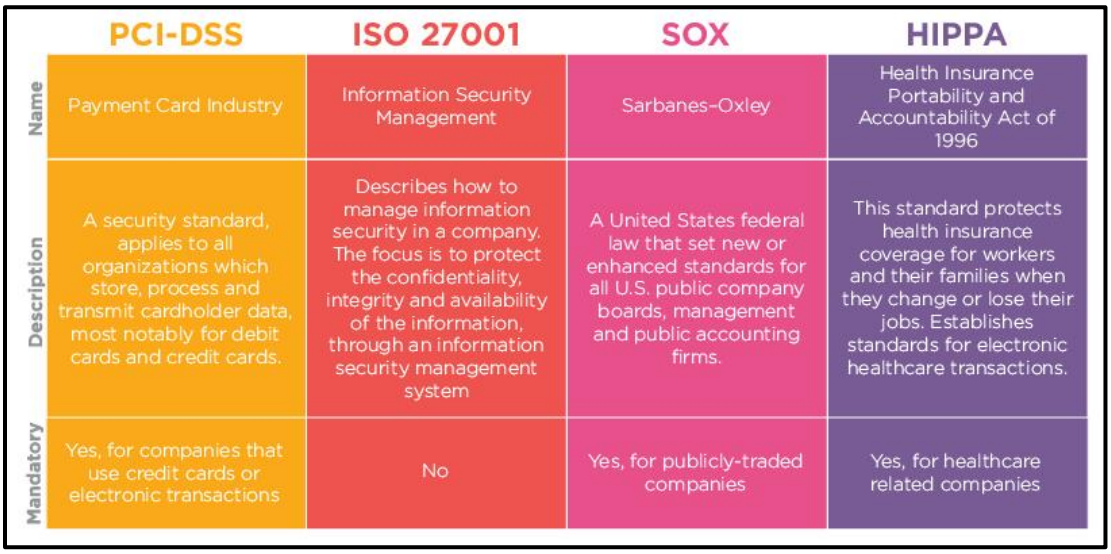

Figura 1 – *Standards* de segurança utilizados mundialmente

Para uma empresa que não tem obrigatoriedades normativas, existem *benchmarks*, ou *checklists*, que pretendem disponibilizar um conjunto de configurações seguras que podem ser adaptadas e incorporadas nas políticas de segurança empresariais. Muitas das vulnerabilidades ou falhas exploradas num ataque informático originam de configurações por defeito que são inseguras, o que torna o uso destas diretrizes uma ação recomendada por especialistas.

As *benchmarks* da CIS (*Center for Internet Security)* ou as DISA-STIG (*Department of Defense – Security Technical Implementation Guides*) são alguns exemplos destas diretrizes.

4.1.1 **CIS *Benchmark***

A CIS *Benchmark* é mantida pela CIS [10] e é uma norma reconhecida por profissionais que fornece diretrizes de configurações seguras, sob a forma de *checklists* abrangentes e consensuais, que ajudam a identificar e mitigar vulnerabilidades numa vasta gama de plataformas. Estas configurações são definidas e mantidas através de trabalho voluntário de especialistas em *standards*, fabricantes de tecnologia e da equipa de desenvolvimento oficial da CIS.

Trata-se de um documento extenso, em formato PDF, onde cada configuração inclui uma descrição detalhada do problema de segurança que pretende resolver assim como passos

para auditoria, processo corretivo e identificação de possíveis problemas resultantes da reconfiguração dos sistemas.

A publicação de novas diretrizes não tem uma data definida uma vez que depende dos trabalhos desenvolvidos pela comunidade e das datas de lançamento ou atualizações dos sistemas abordados.

As diretrizes estão distribuídas em dois grupos que constituem perfis de configuração:

- Nível 1: Conjunto de diretrizes que representam uma base de segurança abrangente caso sejam adotadas. A sua implementação é executada rapidamente e, tipicamente, sem impactos no desempenho dos sistemas. O objetivo deste nível de conformidade é o de diminuir a área de ataque mantendo os sistemas informáticos funcionais.
- Nível 2: As recomendações contempladas neste nível podem ter consequências adversas para a organização se forem implementadas de modo inadequado. Este conjunto de diretrizes estão direcionadas a ambientes que necessitam de uma postura de segurança restrita.

Tendo em conta as criticidades associadas aos diferentes níveis de perfis de configuração, todas as diretrizes devem ser analisadas tendo em conta os objetivos da empresa, políticas de segurança pré-existentes e o risco que esta está disposta a aceitar caso seja necessário.

No ANEXO A – Exemplos de diretrizes de configuração CIS *Benchmark*, encontram-se três exemplos de configurações de segurança recomendadas por esta norma. É possível, através das imagens, verificar a disposição do documento e as informações geralmente apresentadas numa diretriz de configuração CIS:

- Perfil de configuração;
- Descrição do controlo;
- Exposição do problema de segurança apresentado aquando da não conformidade com a diretriz de configuração;
- Processo de auditoria que verifica se a máquina apresenta a configuração;
- Sugestões de guias de implementação da configuração;
- Notas com informação adicional sobre a configuração e como a implementar devidamente.

4.1.2 **DISA-STIG**

Este conjunto de diretrizes são definidas pela agência de defesa de sistemas de informação, DISA (*Defense Information System Agency*), dos Estados Unidos da América e é obrigatória em todos os sistemas do departamento de defesa desse país. Estes sistemas devem estar em conformidade com *frameworks* de *hardening* conhecidas pelo acrónimo STIG (*Security Technical Implementation Guide*).

Apesar destas diretrizes serem especialmente desenvolvidas para conformidade com requisitos governamentais dos Estados Unidos e outras agências do país, não invalida que a STIG seja utilizada em setores privados e noutros países. Empresas em todo o mundo e outros governos utilizam as STIG pela confiança que existe nesta *benchmark* por serem alvo de estudos extensos e revisões rigorosas.

Estas configurações existem para consulta num formato baseado em XML (*Extensible Markup Language*), segundo o *website* oficial da DISA-STIG [11], as STIGs são disponibilizadas no formato XCCDF (*Extensible Configuration Checklist Description Format*) para poderem ser analisadas por ferramentas com protocolo SCAP (*Security Content Automation Protocol*) utilizado em ferramentas de automatização de análise de não conformidades com *benchmarks*. O *website* oferece a sua própria ferramenta para leitura de STIG denominada STIG *viewer*, mas também podem ser utilizadas outras ferramentas que consigam analisar ficheiros XCCDF.

No ANEXO B – Exemplo de diretriz de configuração DISA-STIG encontra-se um exemplo de configurações de segurança recomendadas por esta. É possível, através da imagem, verificar a disposição do documento e as informações geralmente apresentadas numa diretriz de configuração DISA-STIG:

- Informação sobre Ids, grupos, classificação e gravidade da diretriz;
- Título da diretriz;
- Campo *discussion* expõe o problema de segurança que a configuração pretende resolver;
- Campo *check text* apresenta a forma de verificar se o sistema já se encontra em conformidade com a configuração sugerida;
- Campo *fix text* contém sugestões para implementação da configuração em caso de não conformidade.

4.1.3 **Comparação**

A STIG e a CIS são as principais *benchmarks* adotadas em empresas tanto publicas como privadas. A utilização destas normas na seleção de um grupo de configurações seguras para aplicação em sistemas de informação, é um ponto de partida na definição de processos de segurança robustos. As características de ambas as diretrizes de segurança foram comparadas tal como ilustra a Tabela 2.

	CIS	*DISA-STIG*
Público Alvo	Organizações comerciais	Sistemas governamentais dos EUA.
Obrigação de Implementação	Voluntária	Obrigatória para sistemas governamentais dos EUA.
Formato e Ferramentas	PDF	XCCDF
Ativos Abrangidos	Conjuntos de regras específicos para ativos específicos	Conjuntos de regras generalizadas
Custo de Remediação Automatizada	Pago	Grátis
Custo de *scans* de diretrizes	Grátis	Grátis

Tabela 2 – Comparação entre CIS e DISA-STIG

De um modo geral, ambas as *benchmarks* contêm informação semelhante para resolução dos mesmos problemas. As maiores diferenças são no formato de disponibilização da *benchmark*, público alvo e meios de automatização imediata.

Quanto ao público alvo ambas as normas são utilizadas em setores privados e públicos pois as suas informações são válidas e fidedignas para todos os sistemas de informação. No entanto, as STIGs foram especificamente desenvolvidas para abranger os requisitos impostos nos sistemas de agências governamentais dos EUA. A CIS *Benchmark* é utilizada amplamente em organizações comerciais e também em algumas agências governamentais dos EUA. As *benchmarks* CIS, ao contrário das DISA-STIGs, não são

validadas num registo institucional, mas são revistas pela comunidade, o que as torna tanto ou mais válidas e seguras do que as STIGS.

Onde este conjunto de diretrizes difere consideravelmente é no formato em que são distribuídas para consulta. A CIS distribui todas as suas diretrizes em formato de documento PDF, enquanto que a STIG disponibiliza o seu conteúdo em formato XCCDF o que implica a instalação de um XML *parser* ou de uma ferramenta desenvolvida pela DISA para o efeito.

A consulta do conteúdo de uma STIG no seu formato XCCDF, não é tão acessível como o formato de documento PDF disponibilizado pela CIS. No entanto, a vantagem principal associada ao formato XCCDF é o facto de este ser *machine readable*, ou seja, permite a automatização dos processos de remediação de não conformidades enquanto que, a CIS *Benchmark* com o seu formato PDF, não permite a automatização de processos à partida.

Em ambas as ferramentas o *scan* de análise de não conformidades é grátis. Na STIG o seu formato garante integração com protocolos SCAP utilizados em ferramentas gratuitas. No caso da CIS *Benchmark*, a CIS disponibiliza uma ferramenta gratuita, CIS-CAT Lite, que permite realizar *scans* ilimitados de não conformidade com as *checklist*.

Nos Anexos A e B é possível verificar as principais diferenças na apresentação da mesma diretriz abordada por ambas as *benchmarks*. Enquanto que a DISA-STIG expõe o problema de uma maneira abrangente e indicando várias configurações para um problema abrangente, a CIS divide o mesmo problema em várias diretrizes cada uma com o seu racional e remediação. As duas *benchmarks* abordam o mesmo problema de maneiras diferentes, mas remediam-no de igual modo.

A STIG tem uma abordagem mais generalista o que a torna mais fácil de aplicar em sistemas e aplicações personalizadas ou desenvolvidas internamente por uma empresa enquanto que a CIS contém documentos específicos para sistemas e tecnologias já existentes no mercado. Por exemplo, enquanto que a CIS contém documentos com conjuntos de diretrizes específicos para a AWS (*Amazon Web Services*), GCP (*Google Cloud Platform*) e *Microsoft Azure*, a STIG tem um guia genérico de Computação Cloud com capacidade de abranger todas estas tecnologias.

4.2 Automatização de *Benchmarks*

Dada a complexidade e a quantidade de diretrizes de segurança que precisam de ser revistas e analisadas, é necessária a utilização de ferramentas que validem, de forma automatizada, a conformidade com *standards* e boas práticas de indústria no que diz respeito a configurações seguras de sistemas informáticos. As ferramentas recomendadas no livro *Hands-On Security in DevOps* [12] são a CIS-CAT Lite, gerida pela própria CIS, e a ferramenta OpenScap.

A Figura 2 retirada de [12], representa as três fases existentes no ciclo de vida de um processo de *hardening* em sistemas operativos:

- Fase 1 – Definir uma base de segurança tendo em conta práticas aprovadas por especialistas de segurança, tal como as *benchmarks* de segurança CIS ou a DISA-STIG.
- Fase 2 – Utilizar ferramentas de análise e *scan* de não conformidades com a *benchmark* de segurança, tais como o CIS-CAT.
- Fase 3 – A fase final consiste na monitorização de todas estas ferramentas e *benchmarks* de modo a garantir que todos os sistemas contêm configurações atualizadas e seguras.

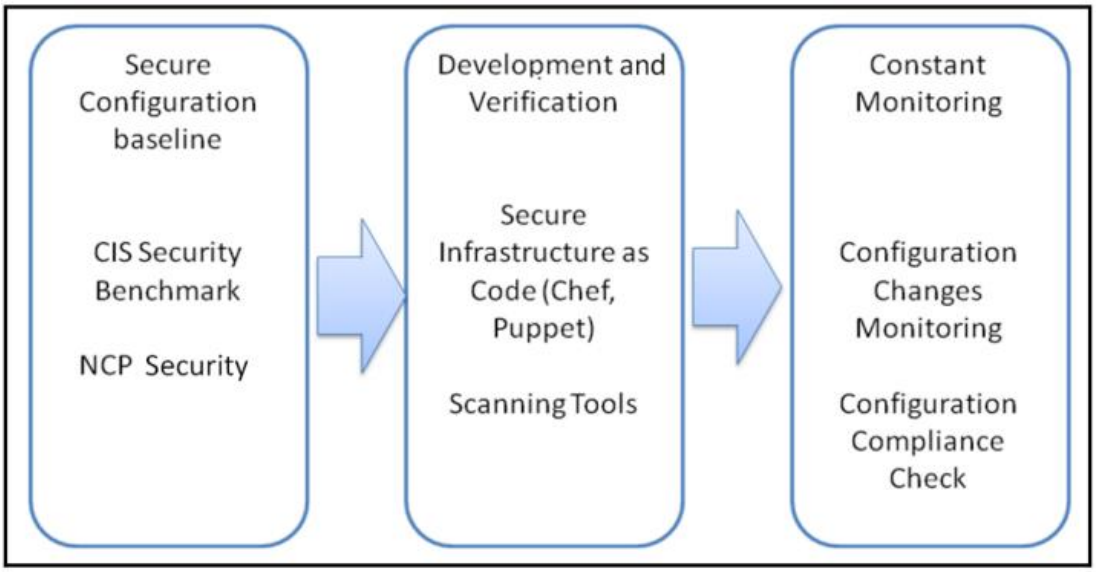

Figura 2 – Ciclo de vida de processos de *hardening* em sistemas informáticos.

4.2.1 **CIS-CAT**

Segundo o site oficial da CIS, a CIS-CAT (CIS-*Configuration Assessment Tool*) [13], "é a ferramenta de análise que compara um sistema a configurações seguras recomendadas em formato *machine-readable*, tendo em conta que o conteúdo está em conformidade com protocolos SCAP. A ferramenta foi desenvolvida para análise de conformidade com as recomendações de configuração da CIS *Benchmark* e disponibiliza um relatório de conformidade com pontuação de 0 a 100 com passos de remediação para cenários de não conformidade"

O CIS-CAT existe em duas versões, a *Lite* gratuita e a *Pro* paga. A Tabela 3 retirada de [14], representa detalhadamente as funcionalidades disponibilizadas por ambas as versões.

	Lite v3	Lite v4	Pro v3	Pro v4
CIS Benchmarks supported	Select*	Select*	90+	65+
SCAP 1.2 validated	✓	✓	✓	✓
Graphical User and Command Line Interface (GUI and CLI) Options	GUI only	CLI only	GUI and CLI	CLI only
CIS Controls Assessment Module		✓		✓
Measure assessment results on conformity scale of 0-100	✓	✓	✓	✓
Evidence-based reports in HTML format	✓	✓	✓	✓
Perform unlimited scans	✓	✓	✓	✓
Assess vulnerabilities	✓	✓	✓	✓
Assess against other SCAP content (i.e. DISA STIGS)			✓	✓
Remotely assess endpoints		✓		✓
Customize CIS Benchmark content via CIS WorkBench			✓	✓
Access to CIS Benchmarks in XML/XCCDF/OVAL			✓	✓
Assess multiple machines at one time via centralized workflows		✓	✓	✓
Analyze assessment results in CIS-CAT Pro Dashboard			✓	✓
Evidence-based reports in Text, Excel, and XML(ARF) formats			✓	✓

*Windows 10, Ubuntu, Mac OS (Lite v3 only) and Google Chrome

Tabela 3 – Funcionalidades CIS-CAT Lite e Pro

Em termos de funcionalidades, a versão *Lite* disponibiliza a análise de não conformidades com um conjunto limitado de *benchmarks*. A versão Pro, por sua vez, apresenta a mesma análise, mas num conjunto de mais de 90 CIS *benchmarks* e a possibilidade de remediação automatizada de não conformidades.

Como se pode verificar na Tabela 3 a versão paga desta ferramenta permite também fazer análises de não conformidades a outras *benchmarks* como a DISA-STIG através do uso do protocolo SCAP.

4.2.2 **SCAP**

Ao longo deste documento foi identificada a necessidade, por parte das empresas, da definição de uma abordagem automatizada ao tema de conformidade com *benchmarks* de segurança. De modo a ultrapassar estas necessidades e reduzir custos de gestão de segurança, a NIST desenvolveu um protocolo de automatização de conteúdos de segurança utilizando fontes públicas.

SCAP (*Security Content Automation Protocol*) é, segundo as especificações técnicas do protocolo na publicação especial da NIST 800-126 [15], "um conjunto de especificações que normalizam o formato e nomenclatura pelos quais as informações sobre falhas de software e configurações de segurança são transmitidas, tanto para máquinas como para pessoas." É uma *framework* que automatiza atividades e processos de suporte a análise de configurações, vulnerabilidades e atualizações, atividades técnicas de controlo de conformidade e classificação de segurança. O protocolo SCAP foi desenvolvido com o objetivo de normalizar a gestão de sistemas de segurança, promover a interoperabilidade entre produtos de segurança e incentivar o uso de mecanismos *standard* de segurança.

As *checklists* analisadas via SCAP são documentadas em formato XML o que torna a sua personalização fácil, permitindo que as empresas adicionem, alterem e eliminem configurações de *benchmarks* consoante necessidade.

Este protocolo é constituído por vários componentes disponíveis para consulta na Tabela 4. Verifica-se a adoção de formatos e mecanismos de segurança *standard* a nível de indústria tais como o CVE para identificação de vulnerabilidades conhecidas publicamente, CVSS utilizado na classificação da gravidade de vulnerabilidades, XCCDF utilizado pela

DISA-STIG como formato preferencial para disponibilização de informações sobre a sua *benchmark*.

Componente	*Formatos*	*Descrição*
Linguagem	XCCDF, OVAL, OCIL	Linguagem *standard* para expressar políticas de segurança.
Relatórios	ARF	Disponibiliza os mecanismos necessários para apresentar a informação recolhida num formato *standard*.
Sistemas de Identificação	CPE, SWID, CCE, CVE	Identificam conceitos chave como vulnerabilidades, através de um identificador *standard*.
Sistema de *Scoring*	CVSS, CCSS	Avaliação e classificação de características de uma vulnerabilidade de segurança.
Integridade	TMSAD	Ajuda a preservar a integridade de conteúdos e resultados.

Tabela 4 – Componentes do Protocolo SCAP

O SCAP utiliza dados como referência para determinar falhas de segurança de sistemas e de configurações *standard*. Estes dados são fornecidos pela *National Vulnerability Database* (NVD), gerida pela NIST.

4.2.3 NIST National Checklist Program

Segundo o *website* oficial da NIST *National Vulnerability Database* [16], o *National Checklist Program* (NCP), definido pela NIST SP 800-70 [8], é o repositório público de *checklists* de segurança (ou *benchmarks*) definido pelo governo dos EUA, que disponibiliza diretrizes de baixo nível para implementação de configurações de segurança em sistemas operativos e aplicações.

De forma a facilitar o desenvolvimento, consulta e atualização de *benchmarks* de segurança para sistemas informáticos, tornando-as mais estruturadas e úteis, a NIST criou o NCP. Os objetivos do NCP segundo a publicação especial 800-70 da NIST [8] são:

- Facilitar o desenvolvimento e partilha de *checklists* através da disponibilização de uma *framework* formal onde fabricantes e outras entidades relevantes podem submeter as suas diretrizes de segurança;
- Disponibilizar diretrizes que servem de base na criação de *checklists* para que estas tenham qualidade e sejam adaptáveis a ambientes operativos comuns;
- Disponibilizar orientações a nível de documentação das *checklists*;
- Encorajar fabricantes de aplicações e outras entidades a desenvolver *benchmarks* de segurança;
- Oferecer um processo controlado para revisão, atualização e manutenção de informações de *checklists*;
- Definir um repositório simples para consulta de informações sobre *checklists*;
- Disponibilizar *checklists* num formato *standard*;
- Encorajar o uso de tecnologias de automatização na aplicação de *checklists*.

O NCP permite fazer uma pesquisa sobre qualquer informação de segurança, sendo o resultado apresentando sempre com base em recursos válidos e *standard* de eficácia comprovada por entidades especialistas na matéria. Os recursos disponibilizados consistem em *metadados* e links para informações fidedignas tais como *checklists* de segurança com vários formatos e em conformidade com o protocolo SCAP.

Este repositório agrupa todas as configurações de segurança presentes em documentos e normas, não só as da NIST como também de outras como a CIS e a DISA-STIG. Disponibilizam também o código fonte para *scans* de diretrizes em vários formatos que podem ser executados utilizando o protocolo SCAP ou implementado em ferramentas de gestão de configurações que, tipicamente, já existem numa empresa, como o *Ansible* e o *Puppet*.

4.2.4 **Análise Centralizada de Configurações**

Para além das ferramentas já apresentadas para automatização de análise de diretrizes e remediação de não conformidades com *benchmarks* de segurança, este processo pode também ser integrado soluções de gestão de configurações tipicamente utilizadas em empresas.

Segundo o livro *Implementing DevOps with Ansible 2* [17], a gestão de configurações ajuda as organizações a gerir as suas infraestruturas através de automatização e gestão de alterações. As soluções disponíveis no mercado de gestão de configurações, permitem automatizar todos os processos automatizáveis, diminuindo assim o *overhead* associado à implementação manual de configurações em todos os sistemas informáticos empresariais. As configurações são disponibilizadas centralizadamente para que os sistemas as possam consultar, atualizando-se em conformidade.

Para o tema de conformidade com *benchmarks* de segurança, as vantagens da utilização de uma abordagem centralizada de gestão de configurações são:

- Automatização de tudo o que seja automatizável– Este é o princípio fundamental destas soluções, ou seja, se um sistema consegue fazer algo de forma automatizada então este deve estar programado para tal. Os esforços investidos na implementação de mecanismos de gestão centralizada de configurações são uma mais valia pois elimina a necessidade de execução de tarefas repetitivas.
- Infraestrutura reproduzível – Após a definição centralizada de configurações de uma máquina ou ambiente, estes podem ser reproduzidos ao longo da infraestrutura sem intervenção humana.
- Sincronização de configurações – Esta funcionalidade permite que um sistema verifique periodicamente se as suas configurações estão atualizadas tendo em conta o repositório central. O sistema, quando identifica não conformidade com as configurações centralizadas, reconfigura-se de forma automatizada.

Estas soluções permitem que a alteração de uma configuração no repositório central tenha efeito em todos os sistemas aplicáveis e que caso seja alterada uma configuração diretamente no sistema, este tenha capacidades automatizadas de reconfiguração tendo em conta os parâmetros definidos centralizadamente.

As soluções mais populares de gestão de configurações são *Ansible*, *Chef*, *Puppet* e *CFEngine*. Soluções como estas são maioritariamente de código aberto e utilizam uma linguagem de programação declarativas que diminui a curva de aprendizagem para sua gestão.

A gestão centralizada de configurações recorrendo a soluções como o *Ansible* ou o *Puppet*, permitem declarar quais são as configurações existentes nos sistemas. Após a seleção de configurações seguras das *benchmarks* de segurança, é possível implementá-las centralizadamente e os sistemas, por sua vez, irão reconfigurar-se de forma automatizada.

4.3 Síntese

As normas de segurança são desenvolvidas para que as empresas possam definir políticas, processos e mecanismos que pretendem garantir a confidencialidade, disponibilidade e integridade de dados. Em alguns negócios, a conformidade com *standards* é obrigatória estando precedida de auditorias periódicas por entidades reguladoras. São exemplos destas normas a PCI-DSS para entidades que lidam com dados sensíveis de cartões de crédito.

Para empresas cujo objetivo é definir mecanismos para obter una base de segurança nos seus sistemas, existem listas contendo diretrizes de configurações consideradas seguras. Este conjunto de diretrizes chama-se de *benchmark* ou *checklist*.

As duas *benchmarks* mais utilizadas são a CIS *Benchmark* e a DISA-STIG, ambas são similares no que diz respeito ao aconselhamento de configurações de segurança, mas apresentam com algumas diferenças:

- A DISA-STIG foi desenvolvida especificamente para atender às necessidades e requisitos impostos pelos sistemas de agências governamentais dos EUA, enquanto que a CIS *Benchmark* foi desenvolvida através do contributo voluntário de especialistas de segurança por todo o mundo.
- A CIS disponibiliza as diretrizes em formato PDF enquanto que a DISA fornece-as no formato XCCDF que requer uma ferramenta especial para sua leitura, mas permite integração com protocolos que automatizam o processo de análise de configurações de segurança.

A STIG tem uma abordagem mais generalista o que a torna mais fácil de aplicar em sistemas e aplicações personalizadas ou desenvolvidas internamente por uma empresa, enquanto que a CIS contém documentos específicos para sistemas e tecnologias especificas.

Apesar da CIS não disponibilizar a sua *benchmark* em formato automatizável, esta disponibiliza uma ferramenta gratuita, CIS-CAT, que permite analisar diretrizes de segurança nos sistemas. Na versão paga da ferramenta é possível remediar não conformidades de forma automatizada.

O protocolo utilizado para *scans* de configurações seguras quer da CIS *Benchmark* quer da DISA-STIG é o SCAP. Este protocolo contém um conjunto de especificações que normalizam o formato e nomenclatura pelos quais informação sobre falhas de software e configurações de segurança são transmitidas. Este protocolo tem vários componentes como o desenvolvimento de relatórios, classificação de vulnerabilidades, verificação de integridade de conteúdos, entre outros. O SCAP possibilita que produtos de segurança executem e verifiquem configurações automaticamente utilizando informações disponibilizados no repositório *National Checklist Program.*

Dada a necessidade de um local centralizado onde reunir conceitos e documentação de segurança, a NIST criou o NCP que é o repositório de *checklists* de segurança (ou *benchmarks*) publicamente disponibilizado pelo governo dos EUA. Este repositório disponibiliza diretrizes de baixo nível para implementação de configurações de segurança em sistemas operativos e aplicações. Este oferece um motor de busca para procura de conteúdos relacionados com segurança como por exemplo, *benchmarks*.

As configurações disponíveis em *benchmarks* podem ser aplicadas em sistemas de modo automatizado, através de uma solução centralizada de gestão de configurações. Estas soluções, como o *Ansible* e o *Puppet*, permitem definir centralizadamente as configurações seguras de *benchmarks* permitindo que os próprios sistemas verifiquem, periodicamente, se as suas configurações estão em conformidade com as declaradas centralizadamente, caso não haja conformidade os sistemas reconfiguram-se.

5 Programa de Estágio

Este capítulo tem o principal objetivo de apresentar o trabalho que foi realizado, no âmbito do estágio, na empresa de acolhimento.

Num primeiro momento apresenta-se o plano de trabalhos e respetivas atividades de estágio.

Seguidamente abordar-se a ferramenta utilizada no projeto de conformidade com a CIS *Benchmark, Cyberwatch*.

Na secção 5.4 especifica-se as atividades desenvolvidas a nível de resolução de incidentes de segurança informática.

Na secção 5.5 será apresenta-se o projeto GKE (*Google Kubernetes Environment*) e o papel da equipa de segurança neste.

Na secção 5.6 apresenta-se os resultados de todas as atividades realizadas em contexto de estágio.

Finalmente na secção 5.7 expõe-se uma síntese de todos os trabalhos e principais resultados decorrentes destes.

5.1 Plano de Trabalhos

Durante a integração na empresa em âmbito de estágio houve a oportunidade de lidar com diversas ferramentas, tecnologias e conceitos relacionados com segurança de sistemas. O trabalho que mereceu o foco principal durante os 9 meses de permanência na empresa foi, a elaboração de um plano de conformidade com configurações seguras definidas pela CIS *Benchmark* utilizando a ferramenta *Cyberwatch*. No entanto, surgiram oportunidades para explorar outros conceitos como a resolução de incidentes e a implementação de mecanismos de segurança em ambientes disponibilizados por plataformas *Cloud* como é o caso do GKE (*Google Kubernetes Environment*).

Para além dos trabalhos já mencionados destaca-se também a participação em programas de sensibilização de segurança, otimização de processos, parametrização e investigação de ferramentas de segurança, escrita de procedimentos de segurança para a

equipa de operação, escrita de artigos no âmbito de segurança no *website* da empresa e a resolução de problemas impostos pelas ferramentas de segurança instaladas nos postos de trabalho.

Foram também desenvolvidas *soft skills* devido à área de ação transversal da equipa de segurança a toda a empresa, desta forma, houve a oportunidade de comunicar com equipas de segurança países diferentes na resolução de problemas comuns.

A Tabela 5 representa o plano de trabalhos consoante as atividades realizados em âmbito de estágio. É possível verificar que no mês de abril não foram realizadas atividades devido à suspensão temporária de estágio devido à pandemia COVID-19, após este mês as atividades retomaram com normalidade.

ATIVIDADES	**Setembro**	**Outubro**	**Novembro**	**Dezembro**	**Janeiro**	**Fevereiro**	**Março**	**Abril**	**Maio**	**Junho**	**Julho**
A	x	x	x								
B			x	x							
C				x							
D					x						
E					x	x	x				
F									x	x	
G			x	x	x	x	x		x	x	x
H	x	x	x	x	x	x	x				
I			x	x	x	x	x				

Tabela 5 – Plano de Atividade de Estágio

A. Levantamento e análise de configurações seguras segundo a CIS *Benchmark*;
B. Teste de configurações CIS *Benchmark* em máquinas virtuais num ambiente controlado;
C. Análise de risco do projeto de conformidade CIS *Benchmark*;
D. Elaboração do Plano de Conformidade com a CIS *Benchmark*;
E. Análise de não conformidades em todos os sistemas operativos Unix da empresa;
F. Aplicação do plano de conformidade com a CIS *Benchmark*;
G. Documentação de projeto de conformidade com a CIS *Benchmark*;
H. Resolução de incidentes de segurança;
I. Projeto de migração de processos de negócio para *Google Kubernetes Environment*.

5.2 Ferramenta *Cyberwatch*

O *Cyberwatch* é uma ferramenta de análise de vulnerabilidades proprietária de uma empresa que oferece vários serviços relacionados com segurança empresarial. A empresa descreve o propósito da ferramenta na sua documentação como o de "facilitar a gestão de vulnerabilidades disponibilizadas por especialistas, desde a sua deteção à sua resolução. O *Cyberwatch* gera *dashboards* úteis no processo de avaliação do risco tendo em conta o seu contexto de modo a auxiliar decisões empresariais".

As análises de diretrizes seguras executadas pela *interface web* da ferramenta *Cyberwatch* requerem a instalação de um agente em todas as máquinas que, por sua vez, cria um utilizador (*cyberwatch-agent)* para que este possa executar as suas tarefas. Este agente estabelece a comunicação com o servidor *web* de onde são despoletados comandos *bash* para máquinas selecionadas.

A Figura 3 apresenta a página principal do módulo de conformidade da ferramenta, é aqui que todos os *scans* de configurações CIS *Benchmark* são iniciados. É possível verificar nas opções de filtragem que a informação da imagem se refere ao sistema operativo CentOS7 e pode-se também observar a lista de máquinas perfazendo um total de 332. As máquinas são adicionadas a esta lista aquando da sua primeira comunicação com o servidor *web* imediatamente após a instalação com sucesso do agente, não sendo possível adicionar máquinas a esta ferramenta manualmente.

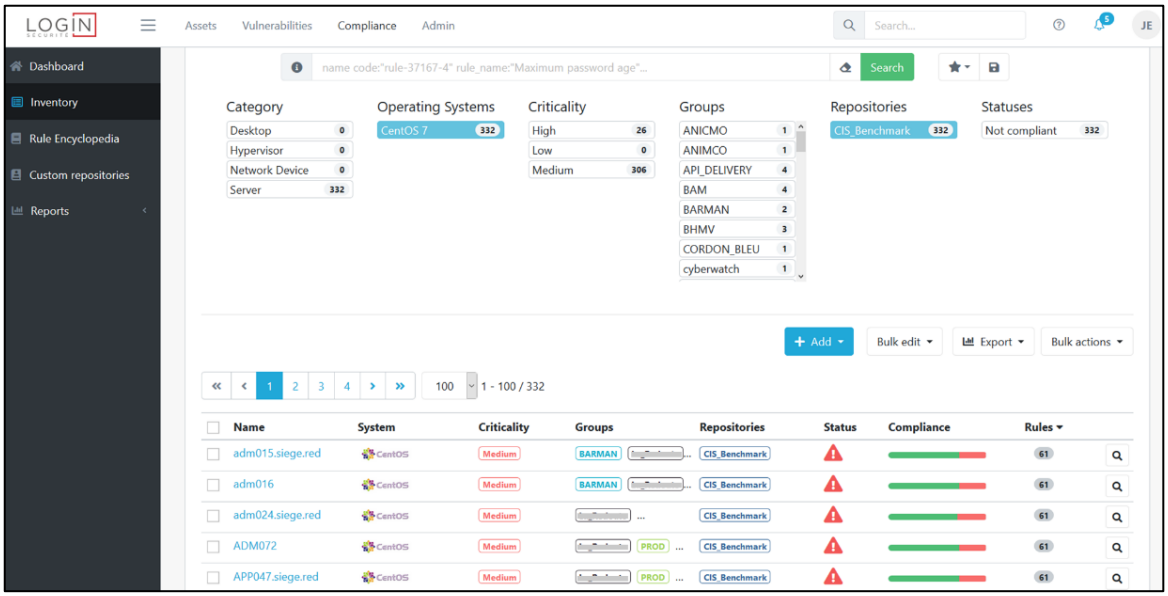

Figura 3 – Página inicial de *compliance* da ferramenta *Cyberwatch*.

A Figura 4 a um detalhe das listas de máquinas disponíveis para o sistema operativo CentOS. É possível verificar que a coluna *compliance* não apresenta qualquer valor, isto verifica-se porque a imagem ilustra a disposição da informação antes de serem feitas quaisquer análises de configurações às máquinas, enquanto que na Figura 5 é visível na mesma coluna uma barra representativa do nível de conformidade das máquinas com a *benchmark*.

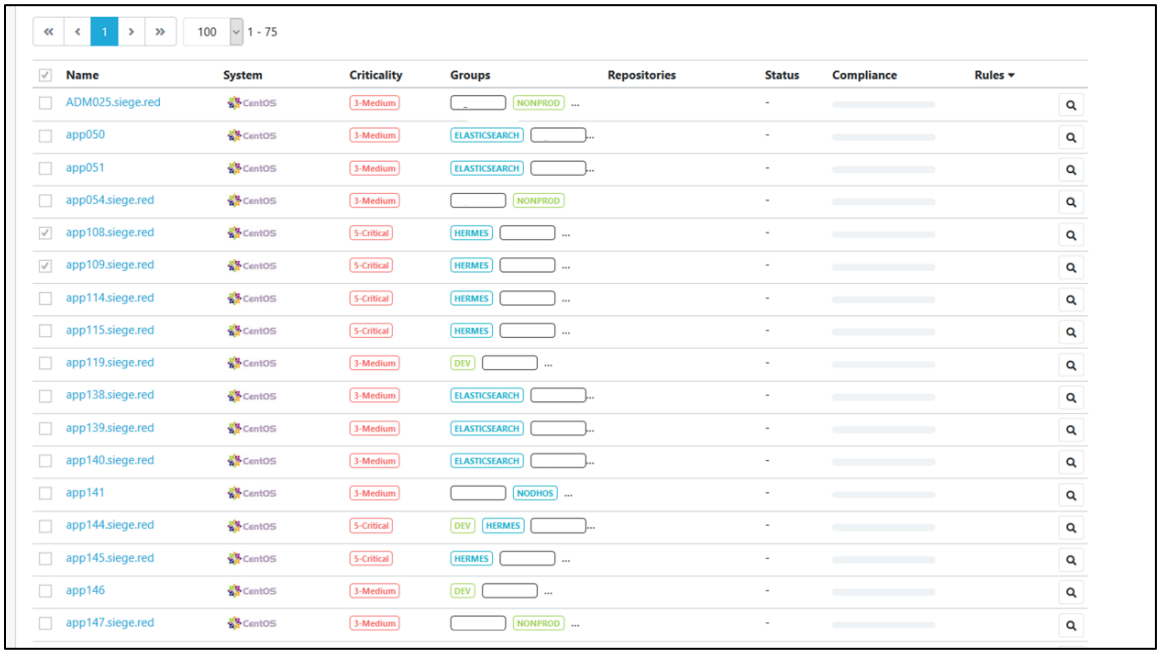

Figura 4 – Máquinas CentOS sem estado de *compliance*.

Na Figura 5 pode também observar-se as máquinas que contêm não conformidades através do seu estado na coluna *status*. Este campo pode ter três estados distintos: *Non-compliant*, apresentado a vermelho; *Compliant*, representado pela cor verde; *Analysing*, de cor amarela quando está a decorrer uma análise à máquina. A coluna *rules* representa o número de diretrizes de configuração da *benchmark* que foram analisadas em cada máquina.

Após selecionar uma das máquinas apresentadas nas listas quer da Figura 4 como na Figura 5, é apresentada uma outra lista com detalhes sobre as diretrizes que foram analisadas na máquina, assim como o seu estado (*non-compliant*, *compliant*, *analysing*), como é possível observar na Figura 6.

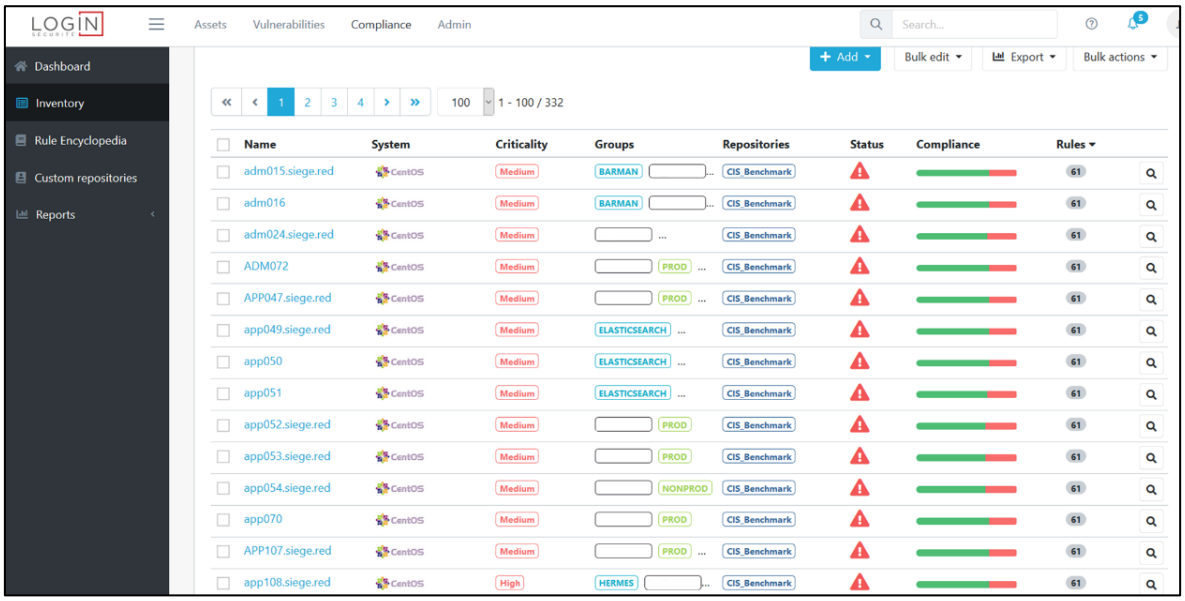

Figura 5 – Máquinas CentOS com estado de *compliance*.

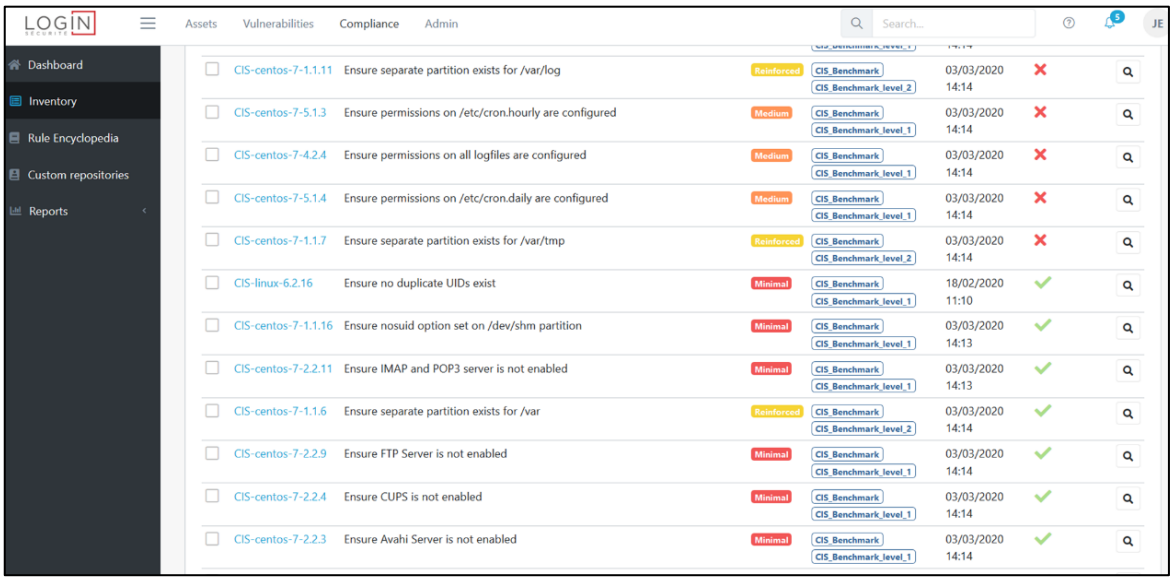

Figura 6 – Estado de conformidade com *benchmark* de uma máquina.

A ferramenta é intuitiva e as suas funcionalidades são de fácil compreensão. A navegação na interface *web* é agradável com uma representação gráfica esclarecedora quanto ao estado de conformidade com a *benchmark* de toda a infraestrutura.

5.3 Plano de Conformidade com a CIS *Benchmark*

Para a implementação com sucesso de novas configurações em sistemas empresarias, é essencial a elaboração de um plano com ações bem definidas dado que, a alteração de configurações pode causar distúrbios ao funcionamento normal dos sistemas. O plano de conformidade com as diretrizes CIS *Benchmark* em sistemas operativos Unix, dividiu-se em três fases distintas que serão abordadas neste capítulo.

A Fase 1 e 2 referem-se à análise do estado geral de conformidade da infraestrutura com a *benchmark*, ou seja, cada uma das configurações seguras sugeridas pela CIS *Benchmark* serão comparadas com as configurações existentes em todas as máquinas para determinar quantas diretrizes falham.

A Fase 3 refere-se à definição e implementação de um plano corretivo com base nas configurações que falharam nas fases anteriores.

5.3.1 Fase 1: Análise em Ambiente de Não Produção

- **Compreender os impactos da análise de diretrizes seguras nas máquinas da infraestrutura.** Como foi referido anteriormente, a ferramenta *Cyberwatch* requer a instalação de um agente em todas as máquinas onde, através deste, são executadas instruções diretamente na máquina. De modo a compreender estes potenciais problemas, foi enviado um email à entidade responsável pelo suporte da aplicação *Cyberwatch* cuja resposta foi a seguinte: A execução desta ação pode resultar no aumento de atividade no servidor alvo e, por conseguinte, torná-lo lento durante um curto espaço de tempo. Conclui-se então que os servidores deverão ser monitorizados com de modo a identificar um consumo anormal de recursos por parte do agente.
- **Lista de passos necessários para análise de diretrizes.** De modo a permitir que a avaliação de configurações possa ser feita no futuro aquando da manutenção do plano, deverá ser criada uma lista de passos necessários para a conclusão desta tarefa. Esta lista não consta no presente relatório pois são abordadas ferramentas internas da empresa.
- **Identificação de todas as máquinas de ambiente de não produção.** De modo a dar início à análise, as máquinas alvo desta devem ser identificadas. Nesta fase inicial o foco principal é o ambiente de não produção para que haja o menor impacto possível

para a empresa caso algo não corra como o esperado. Nesta tarefa foi desenvolvida uma lista contendo identificações de todas as máquinas e os seus endereços para referência futura.

- **Análise de diretrizes seguras em máquinas de não produção.** Tendo em conta a informação já apresentada, foram identificados dois passos chave para a concretização desta tarefa: Analisar os conjuntos de configurações nas máquinas de um modo faseado e monitorizar os recursos continuamente. Caso se identifique um consumo de recursos elevado que impeça o normal funcionamento do servidor, a análise será imediatamente parada. O objetivo principal desta tarefa é a elaboração de um conjunto de fatores a ter em conta na próxima fase pois esta implica ambientes de maior risco.

Esta primeira análise das configurações de segurança em ambientes de teste foi um sucesso, não se identificou um consumo de recursos inesperado por parte das máquinas, e foi possível ter uma visão geral do estado de conformidade com a *benchmark* de toda a infraestrutura.

5.3.2 Fase 2: Análise em Ambiente de Produção

- **Identificação de todas as máquinas de ambiente de produção e equipas responsáveis por elas.** Tal como definido anteriormente é necessário identificar as máquinas alvo de análise. Tendo em conta que a análise terá lugar em ambiente de produção, são necessários cuidados acrescidos devido à criticidade do mesmo. Toda a empresa deverá ser avisada sobre as ações que a equipa de segurança executará na infraestrutura, para isso devem ser identificados os responsáveis por cada máquina de produção para que estes sejam devidamente notificados. O objetivo desta tarefa é a elaboração de um documento com informações sobre todas as máquinas de produção agrupadas por equipa responsável.
- **Agendamento da intervenção.** A intervenção será agendada para que toda a empresa tenha conhecimento dela, deverá ser também enviado um email informativo a todas as equipas que irá expor o âmbito da intervenção, os passos a tomar, as máquinas afetadas, objetivos e possíveis impactos**.** Todas as equipas serão incentivadas a reportar quaisquer problemas que identifiquem.

- **Intervenção.** Execução da análise de configurações das máquinas de produção tendo em conta os prazos agendados. Na intervenção serão utilizadas todas as informações recolhidas nas fases anteriores.
- **Avaliação do estado de conformidade com a *benchmark* da infraestrutura.** Após as ações executadas na intervenção é possível identificar, através da aplicação *Cyberwatch*, um conjunto de configurações que não se encontram em conformidade com as diretrizes CIS *Benchmark*. Estes dados devem ser estudados de forma a identificar as configurações menos seguras e que ocorrem mais vezes em toda a infraestrutura.

Os resultados desta fase foram apresentados a equipas pertinentes para definir os próximos passos quanto à implementação de um plano corretivo nas máquinas.

5.3.3 Fase 3: Execução de Plano Corretivo

- **Criação de um *Custom Rule Set*.** Esta é uma funcionalidade disponibilizada pela ferramenta *Cyberwatch* que permite selecionar um conjunto de configurações da *benchmark* de maneira que, em análises futuras não seja necessário a análise de toda a *benchmark*. Foi agendada uma reunião com todas as equipas relevantes onde se debateu quais seriam as configurações que seriam alvo de correção e acrescentadas a este *custom rule set*. Com as configurações a implementar selecionadas é necessário definir o modo de implementação do plano corretivo em toda a infraestrutura.
- **Implementação do plano corretivo.** A implementação do plano será discutida em mais detalhe no subcapítulo 5.6.4, Solução Final.

5.4 Resolução de Incidentes

Na empresa na qual se inseriu o estágio muitas das ações no âmbito de SOC (*Security Operations Center*) e de resposta a incidentes de segurança são executadas por uma equipa subcontratada para o efeito. Este facto deve-se principalmente há falta de uma equipa dedicada a eventos de segurança 24/7, existindo sim uma equipa de operação generalista com procedimentos bem definidos que lhes permitem mitigar rapidamente todos os eventos e alertas que são despoletados pelos sistemas. No entanto, a equipa de segurança é responsável por resolver incidentes de segurança com a equipa de operações em horário

laboral e é responsável pela sua análise consequente, identificação de possíveis danos e sugestão de melhorias nos processos de resposta a incidentes de segurança.

De um modo geral, as ferramentas utilizadas foram:

- **IBM QRadar**. Esta ferramenta é uma SIEM (*Security Information ad Event Management*) que, segundo o glossário da Gartner [18] , pode ser definido como uma tecnologia de apoio à deteção de ameaças e gestão de incidentes de segurança através da recolha e análise não só de eventos de segurança, mas também de outros eventos e fontes de dados. As suas principais características são a capacidade de recolha e gestão de uma vasta gama de *logs*, a capacidade de análise de *logs* e outros dados de fontes heterogéneas, e capacidades operacionais (tais como gestão de incidentes, *dashboards* e relatórios). A grande maioria das máquinas e aplicações cujas operações são essenciais ao negócio, direcionavam os seus *logs* para o SIEM. Aquando de um evento considerado suspeito, eram enviados alertas em forma de email para as equipas responsáveis pela possível resolução de incidentes. Após alerta o evento era investigado para definição de passos a seguir;
- ***DataDome*.** Tendo em conta o facto de a empresa ter toda a sua presença e negócio online, a proteção contra ataques automatizados realizados por *bots* é uma prioridade. O *website* oficial da ferramenta [19] descreve-a como sendo "A única solução de proteção contra *bots* SaaS (*Software as a Service*) para e-commerce e negócios classificados. Oferece proteção utilizando inteligência artificial em tempo real contra todas as ameaças automatizadas OWASP (*Open Web Application Security Project*), incluindo *credential stuffing*, ataques DDoS na *layer* 7, SQL *injection & intense scraping*". Num ataque de negação de serviço típico são utilizados centenas ou milhares de *bots* para executarem ações repetitivas num *website* levando-o à exaustão de recursos, quebra na disponibilidade do serviço e potencial roubo de credenciais. É necessária uma ferramenta que consiga criar uma barreira entre o *bot* e a ação que este pretende executar. O trabalho da ferramenta *DataDome* é a ativação de um *captcha* na página onde está a decorrer o ataque. Este mecanismo permite adicionar um desafio no processo de acesso ao site e, dado que os *bots* agem de uma maneira programada, ficam bloqueados na página *captcha*. O *Datadome* permite definir os endereços aos quais são aplicados os *captchas* e categorizar *bots* como sendo bons, maus ou comerciais. A cada categoria são implementados mecanismos diferentes já

que existem *bots* que são uma mais valia para o site como é o caso de *bots* de publicidade da Google.

- ***ElasticSearch*.** Os *logs* das máquinas que não são enviados para o SIEM são analisados na ferramenta *Elasticsearch*. Este permite executar consultas complexas representadas graficamente pela ferramenta *Kibana*;

Aquando de uma análise de um evento de segurança, estas ferramentas raramente são utilizadas sozinhas trabalhando sempre em conjunto para mitigar os problemas.

No fim de cada incidente é elaborado um comunicado a toda a empresa onde são apresentados possíveis impactos à plataforma tais como o tempo de *downtime* e o número de contas comprometidas. Sempre que se identificam contas comprometidas resultantes de um ataque informático, são enviados emails a todos os prejudicados que tentam explicar de forma clara o sucedido fornecendo links para mudança de password apelando à elaboração de uma palavra passe forte.

5.5 *Google Kubernetes Environment*

O estágio decorreu numa altura crítica para a empresa onde esta se encontrava no processo de mudança no que diz respeito ao local onde dados e aplicações de negócio estavam alojados. Neste sentido, houve uma transição de alojamento em *Data Centers* para alojamento *as a service* na *Google Cloud*. Todas as aplicações e processos de negócios foram migrados para o serviço GKE (*Google Kubernetes Environment*).

A equipa de segurança teve um papel chave neste projeto de definição do ambiente *kubernetes*, destacam-se as seguintes tarefas:

- Definição de regras de controlo de acesso ao ambiente *kubernetes* através do RBAC (*Role Based Access Control*);
- Definição de ferramentas e mecanismos de aplicação de regras definidas em contexto RBAC: OPA (*Open Policy Agent*) e *Gatekeeper*.
- Definição e implementação de políticas de controlo de acesso à *cloud* com o Google IAM (*Identity Access Management*).
- Elaboração de matrizes de responsabilidade RACI (*Responsible, Accountable, Consulted, Informed*) para o RBAC, IAM e outros mecanismos de segurança.

- Definição e implementação de ferramentas de análise estática de código para as equipas de desenvolvimento (*SonarQube*).
- Escrita de documentos com boas práticas e recomendações de segurança sobre componentes do ambiente *kubernetes*.
- Aconselhamento em matérias de segurança como regras de rede, segurança nos *pods*, estratégias de backups e recuperação de desastres.
- Implementação de passos de segurança na *pipeline* de desenvolvimento, com efeitos bloqueantes caso algo não se encontre em conformidade com parâmetros definidos.

Todos os mecanismos automáticos de segurança definidos neste projeto têm o propósito de mudar o paradigma empresarial para *DevSecOps* onde são previstos que os processos de segurança sejam automatizados e transparentes em todo o ciclo de vida de desenvolvimento de aplicações.

5.6 Resultados do Projeto de Conformidade com CIS *Benchmark*

No que diz respeito ao projeto em que se incidiu o estágio, elaboração de um plano de conformidade com as diretrizes CIS *Benchmark* em sistemas operativos Unix, foram elaborados os seguintes documentos e estudos de suporte ao processo:

- Lista de passos necessários para análise de conformidade com configurações seguras;
- Lista de todas as máquinas da empresa divididas por ambiente;
- Lista de todas as máquinas da empresa divididas por equipa responsável;
- Documento com todos os problemas comuns a todas as máquinas, justificação do possível risco de segurança e apresentação de soluções;
- Elaboração de documento para implementação do plano de conformidade com a *benchmark* por parte da equipa competente.
- Elaboração de documentação que aborde todos os passos de desenvolvimento do projeto, dificuldades encontradas e como as mitigar, justificação por detrás de todas as decisões tomadas.

5.6.1 **Conclusões de Testes Iniciais**

Antes da implementação do plano de conformidade com a CIS *Benchmark*, ocorreram, uma fase inicial, testes num ambiente controlado para obter uma visão geral de possíveis desafios.

As não conformidades com as configurações de segurança disponibilizadas pela CIS *Benchmark* foram remediadas manualmente em duas máquinas virtuais com duas versões distintas do sistema operativo CentOs. Este teste teve o objetivo de obter um melhor entendimento sobre a ferramenta *Cyberwatch*, as configurações da *benchmark* e o impacto que este processo pode ter nas máquinas da empresa.

A ferramenta *Cyberwatch*, aquando desta análise, não inclui todas as configurações do documento oficial CIS, sendo apenas testadas 80 das 216. Após a análise inicial, foram aplicadas todas as configurações de segurança sugeridas pela norma, utilizando *scripts* e comandos *bash*. As máquinas utilizadas para este teste continham as configurações definidas por defeito aquando da criação de uma nova máquina virtual. Tendo em conta os testes executados concluiu-se que:

- **A ferramenta *Cyberwatch* precisa de privilégios administrativos**. Alguns dos comandos *shell* executados para garantir conformidade com as normas não estavam a ser executados com sucesso devido à falta de privilégios de administração. O utilizador "*cyberwatch-agent"* criado para gerir o agente dentro das máquinas, precisa de acessos *sudo* e *login* sem password de forma a que os comandos de *scan* iniciados pelo agente, possam ser executados de forma automatizada.
- **Alguns serviços precisam de ficar ativos.** Consta das recomendações da norma CIS que alguns serviços sejam desativados por não terem suporte por parte do fabricante ou por conterem problemas de segurança. No entanto, os objetivos de negócio são sempre uma prioridade e alguns destes serviços podem ser utilizados na empresa e serem inclusive, um ponto fulcral no funcionamento de alguns processo de negócio. Estes objetivos devem ser levados em conta para analisar se as configurações, apesar de serem seguras, podem realisticamente ser implementadas.
- **Algumas configurações podem ter impactos em máquinas existentes.** Algumas diretrizes da CIS sugerem alterações de configurações consideradas intrusivas, especialmente quando se consideram sistemas já existentes e parte do modelo de negócio. Um exemplo de configurações desta natureza são as que sugerem mudanças

nas partições do sistema operativo, alterações desta dimensão podem não impactar uma máquina virtual nova, mas pode ser catastrófico para máquinas mais antigas.

- **A maioria das falhas de configurações seguras referem-se a permissões de acesso a ficheiros.** A resolução de problemas desta natureza são uma sólida base de segurança nos sistemas uma vez que ficheiros críticos não devem ser acedidos pela maioria dos utilizadores. É necessário garantir que ficheiros críticos só são acedidos por contas com permissões de acesso de administração, mantendo o sistema seguro contra roubo de informação se, durante a intrusão ao sistema operativo, o atacante não consiga obter um nível de acesso administrativo.

5.6.2 Problemas Comuns

A ferramenta *Cyberwatch* oferece 80 diretrizes para análise, destas, 18 falharam em todas as máquinas da infraestrutura e 27 falharam em algumas máquinas. A Tabela 6 lista todas as diretrizes que falharam em todas as máquinas da infraestrutura da empresa.

De um modo geral, os problemas de conformidade com a CIS *Benchmark* da empresa são:

- **Desativação de sistemas de ficheiros não utilizados.** Este grupo de configurações visa a divisão do sistema operativo em partições, cada uma delas com diferentes opções de *mount* para proteger o sistema contra ataques provenientes da exploração de vulnerabilidades em sistemas de ficheiros.
- **Desativação de serviços especiais**. Deste grupo de configurações constam serviços que podem estar ativos no sistema operativo e são considerados não seguros. Estes serviços podem apresentar vulnerabilidades conhecidas e mostrar-se uma porta de entrada a intrusões. Caso algum destes serviços seja essencial ao negócio, é necessária uma avaliação de segurança ao mesmo de modo a implementar medidas de segurança de perímetro ou a mudança do mesmo por completo.
- **Alteração de permissões de acesso a ficheiros críticos no sistema**. Este grupo inclui ficheiros com informações consideradas sensíveis. As permissões que a *benchmark* aconselha são, de um modo geral: *Root* deve ser o *user* e *group owner* (root:root), ou seja, só o dono do ficheiro passará a poder aceder ao ficheiro, sendo o dono o utilizador *root*; Remoção de permissões *other* e remoção de *write/read* para *group* (rwx—x---), ou seja, acesso a grupos só a nível de execução mantendo todas

as permissões para o dono do ficheiro. Estas restrições são mais uma barreira defensiva a intrusões pois evita que o atacante sem acessos privilegiados possa extrair informação crítica que comprometa a empresa.

Control	*Description*
1.1.1	**Disable unused filesystems**
1.1.11	Ensure separate partition exists for /var/log (Scored)
1.1.12	Ensure separate partition exists for /var/log/audit (Scored)
1.1.14	Ensure nodev option set on /home partition (Scored)
1.1.17	Ensure noexec option set on /dev/shm partition (Scored)
1.1.3	Ensure nodev option set on /tmp partition (Scored)
1.1.4	Ensure nosuid option set on /tmp partition (Scored)
1.1.5	Ensure noexec option set on /tmp partition (Scored)
1.1.7	Ensure separate partition exists for /var/tmp (Scored)
2.2	**Special Porpuse Services**
2.2.14	Ensure SNMP Server is not enabled (Scored)
4.1.1	**Configure Data Retention**
4.1.1.3	Ensure audit logs are not automatically deleted (Scored)
4.2.2	**Configure syslog-ng**
4.2.4	Ensure permissions on all logfiles are configured (Scored)
5.1	**Configure cron**
5.1.2	Ensure permissions on /etc/crontab are configured (Scored)
5.1.3	Ensure permissions on /etc/cron.hourly are configured (Scored)
5.1.4	Ensure permissions on /etc/cron.daily are configured (Scored)
5.1.5	Ensure permissions on /etc/cron.weekly are configured (Scored)
5.1.6	Ensure permissions on /etc/cron.monthly are configured (Scored)
5.1.7	Ensure permissions on /etc/cron.d are configured (Scored)
5.3	**Configure PAM**
5.3.2	Ensure lockout for failed password attempts is configured (Scored)
Total	**18**

Tabela 6 – Diretrizes que falharam em todas as máquinas.

5.6.3 Análise de Risco

Foram identificados possíveis riscos no que diz respeito ao projeto de conformidade com a CIS *Benchmark*.

A. **Agente não se encontra instalado corretamente ou instalação falha** – Este problema pode causar análises irregulares levando a resultados inconclusivos.
B. **Comprometer a conta de utilizador criada pela ferramenta**– O *user cyberwatch-agent* utilizado pela ferramenta, foi configurado de forma a que fosse possível executar tarefas em ficheiros críticos, com necessidade de privilégios *root*, sem necessidade de introdução de password. Esta conta pode constituir um risco de elevação de privilégios caso um atacante consiga entrar no sistema.
C. **Problemas de desempenho nas máquinas** – Dado o grande número de diretrizes que precisam de ser analisadas, este processo pode levar a perda de desempenho por parte da máquina alvo de *scans* às suas configurações. No pior dos casos o processo de *scan* pode exigir muito poder de processamento bloqueando a máquina, o que pode trazer resultados catastróficos dependendo da criticidade do sistema para o negócio.
D. **Configuração indevida nos sistemas** – As correções de problemas de conformidade com *benchmarks* envolvem a reconfiguração de sistemas com parâmetros considerados seguro. Uma falha na implementação destas novas configurações pode resultar em danos ao sistema operativo e ao negócio.

Após a identificação dos potenciais problemas deste projeto é necessária uma avaliação do risco. Esta avaliação pretende classificar o risco para que se possa entender quais são os mais críticos e que devem ser monitorizados atentamente.

O grau de risco apresentado por um evento é determinado pela probabilidade (chance de o evento ocorrer) e pela gravidade (impacto de um evento). A Tabela 7 ilustra todos os riscos identificados acima e a sua classificação tendo em conta gravidade e probabilidade.

Probabilidade refere-se à possibilidade de um certo risco ocorrer e é representado qualitativamente (alta, média baixa). Gravidade por sua vez refere-se à dimensão do impacto do risco na empresa e pode ser representado utilizando adjetivos que descrevem a magnitude da gravidade (insignificante, mínima, moderada, significante e grave).

Gravidade Probabilidade	Insignificante (1)	Mínima (2)	Moderada (3)	Significante (4)	Grave (5)
Baixa (1)			**A**	**C**	**B**
Média (2)				**D**	
Alta (3)					

Tabela 7- Classificação do risco tendo em conta gravidade e probabilidade

Após esta primeira classificação, a classificação do risco foi calculada tendo em conta a Tabela 8 abaixo. Este processo de cálculo combina a probabilidade da ocorrência do risco com a gravidade que este pode apresentar. Considerando os dados numéricos da tabela anterior, a classificação do risco é feita através da multiplicação da probabilidade com a gravidade.

Tendo em conta a Tabela 8, o risco mais alto é aquele cujo resultado da multiplicação é maior, desta forma, pode classificar-se o risco por ordem decrescente como:

1. Configuração indevida nos sistemas;
2. Obtenção de controlo sobre o agente;
3. Problemas de desempenho nas máquinas;
4. Agente não se encontra instalado corretamente ou instalação falha.

Risco	Probabilidade	Gravidade	Resultado
A	1	3	3
B	1	5	5
C	1	4	4
D	2	4	8

Tabela 8 – Cálculo de classificação do risco

De seguida apresenta-se uma proposta de tratamento dos risco identificados anteriormente:

1. **Configuração indevida nos sistemas -** Alterar as configurações aplicadas para as pré-existentes. Caso o problema persista, fazer *rollback* da máquina para o último estado estável e proceder a uma investigação abrangente à causa deste problema.
2. **Obtenção de controlo sobre o agente** - Remover o utilizador *cyberwatch-agent* e investigar o problema. Devem ser seguidos procedimentos de resposta a incidentes de segurança.
3. **Problemas de desempenho nas máquinas** - Se o desempenho das máquinas é impactado devido ao *scans* de diretrizes levado a cabo pelo agente *Cyberwatch*, os *scans* necessitam de ser terminados utilizando a ferramenta *Cyberwatch* imediatamente. Caso o problema persista, o processo *cyberwatch-agent* deve ser terminado diretamente no sistema através de comando *bash* para o efeito.
4. **Agente não se encontra instalado corretamente ou instalação falha** - De modo a determinar se o agente está instalado ou não na máquina, um alerta precisa de ser criado na ferramenta de monitorização da empresa que verifique se, para cada máquina, o processo *cyberwatch-agent* se encontra em execução. Se o processo se verificar na máquina significa que o agente foi devidamente instalado, caso contrário deve prosseguir-se à instalação seguindo o procedimento definido para o efeito. Se a instalação falhar, deve verificar-se que a máquina consegue comunicar com o servidor do serviço *Cyberwatch* pois, caso não se verifique, devem ser definidas regras de firewall para que o agente consiga comunicar com normalidade. A falha na instalação deste agente deve ser devidamente documentada para análise posterior.

Todo risco indicado neste estudo deve ser mitigado ou aceite. Caso a empresa decida aceitar o risco, este deve ser precedido de uma autorização formal por parte da gerência da empresa ou de outro cargo de igual responsabilidade.

5.6.4 **Solução Final**

Tendo em conta todos os trabalhos de análise realizado e o risco introduzido pela ferramenta *Cyberwatch*, decidiu-se, em reunião com representantes de todas as equipas conhecedoras da infraestrutura, que a melhor abordagem seria a de implementar as configurações consideradas seguras nas máquinas novas e, em trabalho futuro, e tendo como

base o trabalho já feito, analisar e estudar formas de as introduzir em máquinas já existentes na infraestrutura.

Todas as máquinas novas, quando são configuradas seguem um documento estabelecido com as configurações base. Apresentou-se à equipa encarregue de criar estas máquinas, uma lista de configurações adicionais provenientes da CIS *Benchmark*, que foram aprovadas pela gestão da empresa. Estas configurações serão acrescentadas aos procedimentos de criação de novos servidores e às imagens ISO utilizadas também como um *template* de criação de máquinas.

O conjunto de novas configurações seguras estão presentes na Tabela 9 . Fazem parte destas diretrizes 10 das 18 configurações não conformes transversalmente, nos sistemas Unix, tendo em conta a *benchmark.*

Control	*Description*
1.1.1	**Disable unused filesystems**
1.1.11	Ensure separate partition exists for /var/log (Scored)
1.1.14	Ensure nodev option set on /home partition (Scored)
1.1.17	Ensure noexec option set on /dev/shm partition (Scored)
1.1.7	Ensure separate partition exists for /var/tmp (Scored)
5.1	**Configure cron**
5.1.2	Ensure permissions on /etc/crontab are configured (Scored)
5.1.3	Ensure permissions on /etc/cron.hourly are configured (Scored)
5.1.4	Ensure permissions on /etc/cron.daily are configured (Scored)
5.1.5	Ensure permissions on /etc/cron.weekly are configured (Scored)
5.1.6	Ensure permissions on /etc/cron.monthly are configured (Scored)
5.1.7	Ensure permissions on /etc/cron.d are configured (Scored)

Tabela 9 – Diretrizes adicionadas ao ISO de novas máquinas

Foi desenvolvido um documento final com os resultados obtidos, que será acrescentado à documentação oficial da empresa para uso interno, assim como uma apresentação para toda a empresa com o objetivo de divulgar o trabalho feito pela equipa de segurança.

5.7 Síntese

O foco do estágio foi a elaboração de um plano de conformidade com as diretrizes de configurações seguras da CIS *Benchmark* para aplicação em todas as máquinas Unix da empresa. Nesse sentido foram testadas manualmente todas as configurações num ambiente controlado de modo a entender os possíveis impactos que estas configurações podem ter no negócio e a eficácia da ferramenta escolhida pela empresa para gerir não conformidades, *Cyberwatch*.

A ferramenta *Cyberwatch* apresenta uma interface *web* de onde é possível executar *scripts* nas máquinas da empresa desde que estas tenham o seu agente instalado, *cyberwatch-agent*. Estes *scripts* contêm comandos que permitem comparar as configurações presentes no sistema com a configuração segura associada. passam por comparar as configurações das máquinas alvo às configurações da *benchmark*,

O plano de conformidade com a CIS *Benchmark* desenvolvido prevê três fases diferentes para o sucesso do projeto:

- Análise em ambiente de não produção. Nesta fase é feito um *scan* às máquinas, ou seja, são comparadas as suas configurações com as da *benchmark*. Esta análise é faseada e os recursos das máquinas são monitorizados para identificação de problemas que se possam repetir aquando da mesma análise em ambientes de produção.
- Análise em ambiente de produção. São feitas as mesmas análises anteriores, mas com mais constrangimentos e regras dada a natureza do ambiente em questão. São aplicadas as lições aprendidas no primeiro *scan*.
- Execução de plano corretivo. Elaboração de um plano corretivo com configurações de segurança relevantes tendo em conta o estudo de não conformidades identificadas nos *scans* anteriores.

No decorrer da definição das diferentes fases do plano foram identificados e classificados os riscos inerentes ao uso da ferramenta *Cyberwatch* e da implementação de *checklists* nas máquinas sendo estes, por ordem de gravidade:

1. Configuração indevida nos sistemas;
2. Obtenção de controlo sobre o agente;
3. Problemas de desempenho nas máquinas;

4. Agente não se encontra instalado corretamente ou instalação falha.

Na documentação do projeto estão identificados passos de mitigação do risco identificado.

A solução final desenvolvida para este projeto foi a definição de um conjunto de configurações de segurança, aprovadas pela equipa de segurança e restantes equipas envolvidas no projeto, que serão adicionadas somente ao conjunto de configurações de máquinas novas e ao ficheiro ISO de criação de máquinas virtuais.

Para além dos trabalhos de conformidade com a CIS *Benchmark*, o estágio também incluiu as seguintes tarefas:

- Resolução de incidentes de segurança. Utilizando a ferramenta IBM Qradar, *DataDome* e *Elasticsearch* assim como aplicação de processos remediativos, escrita de documentação e elaboração de comunicados à empresa e clientes após um incidente de segurança.
- *Google Kubernetes Environment*. Dado que a empresa na qual se integrou o estágio se encontrava a definir um ambiente *Kubernetes* na *cloud*, houve uma participação em várias tarefas por parte da equipa de segurança no sentido de definir mecanismos e políticas de segurança no ambiente.

6 Análise Crítica e Proposta de Melhoria

Tal como é mencionado ao longo deste documento, um projeto de definição, implementação e manutenção de um plano de conformidade com *checklists* de segurança é extenso, dado que para o seu sucesso é necessária uma análise profunda de todos os sistemas de modo a garantir que as alterações nas suas configurações não afetam processos críticos de negócio.

O projeto de conformidade com a CIS *Benchmark*, requer o apoio de várias equipas , tipicamente as empresas têm uma equipa inteira encarregue de tarefas de manutenção de um plano de conformidade com *benchmarks*. Desta forma, a conclusão de um projeto desta dimensão com o número reduzido de participantes envolvidos é um cenário impraticável.

Dado que não foi possível definir um plano para gestão de não conformidades com a CIS *Benchmark*, desenvolveu-se uma alternativa a este. Foi a apresentada uma lista de configurações seguras para que estas sejam implementadas aquando da criação de novas máquinas virtuais. Esta lista é apresentada no capítulo 5.6.4 Solução Final e pretende ser um primeiro passo na definição de um processo de gestão de conformidade com a *benchmark*.

São mencionados nos subcapítulos 5.6.2 e 5.6.3 os riscos e limitações do uso da ferramenta proprietária *Cyberwatch*. Tendo por base esta análise conclui-se ainda que a ferramenta não está pronta para ser colocada em produção dado que é alvo de atualizações sem aviso prévio que resultam em perturbações a trabalhos já desenvolvidos e que podem resultar em distúrbios nos sistemas.

Como foi mencionado neste documento, a ferramenta *Cyberwatch* não disponibiliza as diretrizes CIS na sua totalidade estando presentes somente 80 das cerca de 200 diretrizes definidas, o que torna os *scans* realizados pelo *Cyberwatch* incompletos.

A solução final apresentada, como já referido, foi a de selecionar um conjunto de configurações seguras disponibilizadas pela CIS *Benchmarks* para que estas sejam implementadas nos procedimentos de criação de novas máquinas virtuais assim como nas imagens ISO utilizadas para as criar. Tendo em conta a lista incompleta de diretrizes de configuração disponibilizada pela ferramenta, podem existir vulnerabilidades não

abrangidas pelas configurações testadas pelo *Cyberwatch*, este facto torna a eficácia da implementação da solução final, reduzida.

Dito isto, a ferramenta CIS-CAT analisada neste documento (subcapítulo 4.2.1), apresenta uma solução com as mesmas funcionalidades, mas com o suporte e experiência da entidade que define a própria *benchmark*. A Tabela 10 apresenta as diferenças principais entre as ferramentas.

	CIS-CAT Lite	*Cyberwatch*	*CIS-CAT Pro*
Custo	**Grátis**	**Pago**	**Pago**
Benchmarks de sistemas operativos	✓	✓	✓
Benchmarks de Google Chrome	✓		✓
Outras *Benchmarks*			✓
Resolução automatizada de não conformidades			✓
Funcionalidades de *scan* de diretrizes	✓	✓	✓
Levantamento de vulnerabilidades	✓	✓	✓
Repositórios de configurações completos e íntegros	✓		✓

Tabela 10 – Comparação entre *Cyberwatch* e CIS-CAT

A versão grátis da ferramenta CIS-CAT tem as mesmas funcionalidades do *Cyberwatch*, ou seja, consegue fazer *scans* a configurações de um sistema e compará-las com a *benchmark* para atribuir um estado de conformidade, no entanto, a CIS-CAT é gratuita e disponibiliza a diretrizes na integra possibilitando uma análise abrangente ao estado de segurança dos sistemas. A reconfiguração do sistema tendo em conta a *benchmark* é possível com a versão paga CIS-CAT, funcionalidade esta que a ferramenta *Cyberwatch*, igualmente paga, não disponibiliza.

Em suma, as funcionalidades gratuitas da ferramenta CIS-CAT abrangem todas as disponibilizadas pela ferramenta paga *Cyberwatch*. Através da subscrição ao serviço pago

CIS-CAT obtêm-se todas as funcionalidades da versão gratuita com a possibilidade acrescida de implementação automatizada de não conformidades, análise de conformidade com mais de 90 *benchmarks* e o suporte oferecido à ferramenta pela entidade que define as *benchmarks* em análise.

7 Conclusão

Sem políticas de segurança as empresas estão expostas a incidentes, comprometendo todas as suas operações e colocando o negócio em risco não só de perdas monetárias, mas também de perda de credibilidade e confiança por parte dos seus clientes. De modo a minimizar a superfície de ataque no que diz respeito a configurações por defeito, mecanismos de *hardening* no sentido de aplicar configurações seguras devem ser impostos.

Não existe nenhuma *checklist* que consiga tornar um sistema ou produto completamente seguro e o seu uso não elimina a necessidade de processos de manutenção como a gestão de atualizações. No entanto, o uso de *checklists* que reforcem não só o processo de *hardening* de sistemas face a vulnerabilidades de software, mas também a configurações seguras de sistemas, resultará na redução de meios de ataque ao sistema.

As falhas em configurações base são um dos pontos a ser explorados numa possível intrusão, no entanto, uma configuração mesmo que considerada segura, pode afetar processos críticos de negócio quando aplicada. Isto pode ser observado principalmente quando os sistemas alvo de *benchmark* foram configurados na fase inicial do negócio onde a segurança não era uma prioridade. Estas máquinas tendem a não sofrer nenhum tipo de atualização ou alteração ao longo dos anos, tornando-as muito vulneráveis e cada vez mais difíceis de tornar seguras dada a sua criticidade.

Apesar das *checklists* serem baseadas em conhecimentos coerentes e verdadeiros de especialistas sobre ameaças de segurança, estas não consideram requisitos operacionais, controlos de segurança, e outros fatores específicos a cada empresa e que possam necessitar de alterações. As diretrizes devem ser avaliadas cuidadosamente e adaptadas aos objetivos e processos existentes. Antes da implementação de alterações a configurações estas devem ser testadas em ambientes controlados para verificar se existe algum impacto na segurança e funcionamento dos sistemas. O teste deve ser seguido da documentação dos resultados e dos passos a seguir para mitigar possíveis incidentes.

Apesar de haver mudanças de configurações que não podem ser implementadas, o risco de segurança que estas apresentam não pode ser ignorado, este deve ser identificado, categorizado e monitorizado para que não possa ser utilizado em intrusões.

As *Benchmarks* e outros processos de segurança devem ser incorporados o mais cedo possível no ciclo de vida de aplicações e sistemas, de modo a que seja progressivamente mais fácil adaptar as políticas de segurança existentes às necessidades evolutivas do negócio e da segurança de informação.

A sensibilização para assuntos de segurança deve ser uma prioridade para as empresas e parte integrante nos seus planos de formação. Sessões sobre este assunto encorajam os colaboradores a serem mais conscientes e a reportar comportamentos anómalos no dia-a-dia. Isto só é possível quando as pessoas detêm o conhecimento necessário para identificar os problemas de segurança.

Os objetivos de negócio são o fator com mais peso em decisões que envolvem a empresa, mas vai sempre custar menos prevenir problemas do que os corrigir.

Este estágio permitiu solidificar e aplicar os conhecimentos obtidos ao longo da parte curricular do mestrado, face aos problemas reais de segurança que as empresas enfrentam. Dada a longa duração da integração na empresa, houve a oportunidade de interagir com pessoas de diferentes nacionalidades, deter um papel de responsabilidade elevada na equipa, aprender conceitos práticos e fundamentais de segurança, explorar novas ferramentas e entender os desafios reais que uma empresa enfrenta, o que demonstrou ser um paradigma diferente do académico até agora experienciado. Houve um desenvolvimento significativo de *soft skills* dada a autonomia conferida nos projetos, a participação em campanhas de sensibilização de segurança e a interação transversal com as equipas da empresa quer em Portugal quer no estrangeiro.

A experiência de estágio demonstrou ser uma mais valia para enfrentar o mercado de trabalho com conhecimentos reforçados e facilidade na expressão, discussão e aplicação de conceitos de segurança. Desta forma, os objetivos de estágio definidos inicialmente foram totalmente cumpridos.

Bibliografia

[1] Gartner, "Digital Commerce," [Online]. Available: https://www.gartner.com/en/information-technology/glossary/digital-commerce. [Acedido em Outubro 2020].

[2] V. C. Hu, D. F. Ferraiolo e R. Kuhn, "Assessment of Access Control Systems," National Institute of Standards and Technology, [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7316.pdf. [Acedido em Outubro 2020].

[3] MITRE, "About CVE," [Online]. Available: https://cve.mitre.org/about/index.html. [Acedido em Outubro 2020].

[4] National Institute of Standards and Technology, "National Vulnerability Database," [Online]. Available: https://nvd.nist.gov. [Acedido em Outubro 2020].

[5] National Institute of Standards and Technology, "Vulnerability Metrics," [Online]. Available: https://nvd.nist.gov/vuln-metrics/cvss. [Acedido em Outubro 2020].

[6] FIRST, "Common Vulnerability Scoring System version 3.1: User Guide," [Online]. Available: https://www.first.org/cvss/user-guide. [Acedido em Outubro 2020].

[7] E. Baker, M. Smid e D. Branstad, "A Profile for U.S. Federal Cryptographic Key Management Systems," National Institute of Standards and Technology, [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-152.pdf. [Acedido em Outubro 2020].

[8] S. D. Quinn, M. Souppaya, M. Cook e K. Scarfone, "National Checklist Program for IT Products – Guidelines for Checklist Users and Developers," National Institute of Standards and Technology, 02 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-70r4.pdf. [Acedido em Outubro 2020].

[9] Belatrix, "Information security for Agile companies," Novembro 2017. [Online]. Available: https://www.belatrixsf.com/whitepapers/security-agile-companies. [Acedido em Outubro 2020].

[10] Center for Internet Security, "CIS Benchmark Hardening/Vulnerability Checklist," [Online]. Available: https://www.newnettechnologies.com/cis-benchmark.html. [Acedido em Outubro 2020].

[11] Defense Information System Agency, "SRG/ STIG Tools," [Online]. Available: https://public.cyber.mil/stigs/srg-stig-tools/. [Acedido em Outubro 2020].

[12] T. Hsu, Hands-On Security in DevOps, Birmingham: Packt Publishing Ltd., 2018.

[13] Center for Internet Security, "CIS-CAT® FAQ," [Online]. Available: https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/cis-cat-faq/. [Acedido em Outubro 2020].

[14] Center for Internet Security, "Compare Key Features," [Online]. Available: https://learn.cisecurity.org/cis-cat-lite. [Acedido em Novembro 2020].

[15] D. Waltermire, S. Quinn, H. Booth, K. Scarfone e D. Prisaca, "The Technical Specification for the Security Content Automation Protocol (SCAP)," National Institute of Standards and Technology, 02 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-126r3.pdf. [Acedido em Outubro 2020].

[16] National Institute of Standards and Technology - National Vulnerability Database, "National Checklist Program Repository," [Online]. Available: https://nvd.nist.gov/ncp/repository. [Acedido em Outubro 2020].

[17] J. McAllister, Implementing DevOps with Ansible 2, Birmingham: Packt Publishng Ltd., 2017.

[18] Gartner, "Gartner Glossary/ Security Information And Event Management (SIEM)," [Online]. Available: https://www.gartner.com/en/information-

technology/glossary/security-information-and-event-management-siem. [Acedido em Setembro 2020].

[19] DataDome, "The new standard in anti-bot protection and mitigation," [Online]. Available: https://datadome.co/bot-protection/. [Acedido em Setembro 2020].

[20] F. D. Peter, Management Challenges for the 21st Century, Inglaterra: Elsevier Ltd., 1999.

[21] Gartner, "Gartner Glossary/ Benchmarking," [Online]. Available: https://www.gartner.com/en/information-technology/glossary/benchmarking. [Acedido em Outubro 2020].

[22] Center for Internet Secuirty, "CIS Benchmark FAQ," [Online]. Available: https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq/. [Acedido em Outubro 2020].

[23] Center for Internet Security, "5 Tips for Securing Systems On-Prem or in the Cloud," [Online]. Available: www.cisecurity.org/blog/5-tips-for-securing-systems-on-prem-or-in-the-cloud. [Acedido em Outubro 2020].

[24] Center for Internet Security, "Download Our Free Benchmark PDFs," [Online]. Available: https://learn.cisecurity.org/benchmarks. [Acedido em Outubro 2020].

[25] V. Ferreira, "Transformação digital: em Portugal ainda reina a imaturidade," Público, 24 Outubro 2018. [Online]. Available: https://www.publico.pt/2018/10/24/economia/noticia/transformacao-digital-portugal-reina-imaturidade-1848685. [Acedido em Outubro 2020].

ANEXO A – Exemplos de diretrizes de configuração CIS *Benchmark*

1.1.15 Ensure nodev option set on /dev/shm partition (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `nodev` mount option specifies that the filesystem cannot contain special devices.

Rationale:

Since the `/dev/shm` filesystem is not intended to support devices, set this option to ensure that users cannot attempt to create special devices in `/dev/shm` partitions.

Audit:

Run the following command and verify that the `nodev` option is set on `/dev/shm`.

```
# mount | grep /dev/shm
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev,noexec,relatime)
```

Remediation:

Edit the `/etc/fstab` file and add `nodev` to the fourth field (mounting options) for the `/dev/shm` partition. See the `fstab(5)` manual page for more information.
Run the following command to remount `/dev/shm`:

```
# mount -o remount,nodev /dev/shm
```

Notes:

`/dev/shm` is not specified in `/etc/fstab` despite being mounted by default. The following line will implement the recommended `/dev/shm` mount options in `/etc/fstab`:

```
tmpfs   /dev/shm   tmpfs   defaults,nodev,nosuid,noexec   0 0
```

1.1.16 Ensure nosuid option set on /dev/shm partition (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `nosuid` mount option specifies that the filesystem cannot contain `setuid` files.

Rationale:

Setting this option on a file system prevents users from introducing privileged programs onto the system and allowing non-root users to execute them.

Audit:

Run the following command and verify that the no `suid` option is set on `/dev/shm`.

```
# mount | grep /dev/shm
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev,noexec,relatime)
```

Remediation:

Edit the `/etc/fstab` file and add `nosuid` to the fourth field (mounting options) for the `/dev/shm` partition. See the `fstab(5)` manual page for more information.
Run the following command to remount `/dev/shm`:

```
# mount -o remount,nosuid /dev/shm
```

Notes:

`/dev/shm` is not specified in `/etc/fstab` despite being mounted by default. The following line will implement the recommended `/dev/shm` mount options in `/etc/fstab`:

```
tmpfs   /dev/shm   tmpfs   defaults,nodev,nosuid,noexec   0 0
```

1.1.17 Ensure noexec option set on /dev/shm partition (Scored)

Profile Applicability:

- Level 1 - Server
- Level 1 - Workstation

Description:

The `noexec` mount option specifies that the filesystem cannot contain executable binaries.

Rationale:

Setting this option on a file system prevents users from executing programs from shared memory. This deters users from introducing potentially malicious software on the system.

Audit:

Run the following command and verify that the `noexec` option is set on `/dev/shm`.

```
# mount | grep /dev/shm
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev,noexec,relatime)
```

Remediation:

Edit the `/etc/fstab` file and add `noexec` to the fourth field (mounting options) for the `/dev/shm` partition. See the `fstab(5)` manual page for more information.
Run the following command to remount `/dev/shm`:

```
# mount -o remount,noexec /dev/shm
```

Notes:

`/dev/shm` is not specified in `/etc/fstab` despite being mounted by default. The following line will implement the recommended `/dev/shm` mount options in `/etc/fstab`:

```
tmpfs   /dev/shm   tmpfs   defaults,nodev,nosuid,noexec   0 0
```

ANEXO B – Exemplo de diretriz de configuração DISA-STIG

Red Hat Enterprise Linux 7 Security Technical Implementation Guide :: Version 3, Release: 1 Benchmark Date: 23 Oct 2020

Vul ID: V-204486 **Rule ID**: SV-204486r505924_rule **STIG ID**: RHEL-07-021024

Severity: CAT III **Classification**: Unclass **Legacy IDs**: V-81013; SV-95725

Group Title: SRG-OS-000368-GPOS-00154

Rule Title: The Red Hat Enterprise Linux operating system must mount /dev/shm with secure options.

Discussion: The "noexec" mount option causes the system to not execute binary files. This option must be used for mounting any file system not containing approved binary files as they may be incompatible. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nodev" mount option causes the system to not interpret character or block special devices. Executing character or block special devices from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

The "nosuid" mount option causes the system to not execute "setuid" and "setgid" files with owner privileges. This option must be used for mounting any file system not containing approved "setuid" and "setguid" files. Executing files from untrusted file systems increases the opportunity for unprivileged users to attain unauthorized administrative access.

Check Text: Verify that the "nodev","nosuid", and "noexec" options are configured for /dev/shm:

cat /etc/fstab | grep /dev/shm

tmpfs /dev/shm tmpfs defaults,nodev,nosuid,noexec 0 0

If results are returned and the "nodev", "nosuid", or "noexec" options are missing, this is a finding.

Verify "/dev/shm" is mounted with the "nodev", "nosuid", and "noexec" options:

mount | grep /dev/shm

tmpfs on /dev/shm type tmpfs (rw,nodev,nosuid,noexec,seclabel)

If /dev/shm is mounted without secure options "nodev", "nosuid", and "noexec", this is a finding.

Fix Text: Configure the system so that /dev/shm is mounted with the "nodev", "nosuid", and "noexec" options b adding /modifying the /etc/fstab with the following line:

tmpfs /dev/shm tmpfs defaults,nodev,nosuid,noexec 0 0