

Exercício 1: Avaliação de Conhecimento

Autor

Simão Andrade - 118345

Necessidade

Reconhecimento das necessidades atuais no setor da segurança da informação, com foco em identificar lacunas específicas, propor soluções alinhadas às exigências técnicas e organizacionais e tornar-me um excelente **profissional em efetuar Auditorias de Segurança**.

Metodologia

Para atingir esse objetivo, a abordagem foi estruturada em **três pilares** principais:

1. **Análise de necessidades no tecido empresarial e interações com especialistas.**
2. **Estudo das ferramentas mais atualmente utilizadas.**
3. **Aprendizagem mediante formações.**

Execução

A **primeira etapa** centrou-se no levantamento de necessidades tecnológicas, humanas e organizacionais. Para isso, foram feitas interações com membros de equipas de cibersegurança, privacidade e segurança da informação de diferentes empresas. Este processo incluiu a participação em seminários e conversas para identificar desafios reais enfrentados por estas equipas, como a falta de ferramentas integradas, dificuldades na análise de tráfego de rede e a ausência de processos robustos de resposta a incidentes. Paralelamente, foi realizado um trabalho de reconhecimento junto a profissionais de áreas não técnicas, para compreender a carência de conhecimentos básicos de ciber higiene e os comportamentos que contribuem para o aumento de vulnerabilidades. Isto permitiu além de expandir o meu conhecimento das necessidades atuais, melhorou as minhas *soft skills*, como empatia, gestão de tempo e comunicação. Este trabalho revelou, por exemplo, que muitas organizações ainda sofrem com a falta de políticas claras para a gestão de dispositivos pessoais (*Bring Your Own Device*) e práticas inadequadas de autenticação e autorização.

A **segunda etapa** foi dedicada ao estudo do estado da arte das ferramentas de proteção de infraestruturas, incluindo tanto *software* quanto *hardware*. Este estudo envolveu a análise detalhada de soluções utilizadas para segurança de redes, gestão de vulnerabilidades e proteção de endpoints. O foco compreendeu em como essas ferramentas abordam os

principais desafios, como a implementação de *firewalls*, sistemas de prevenção de intrusões (IPS), EDR (*Endpoint Detection and Response*), e mecanismos de segmentação de redes.

A aprendizagem nesta etapa incluiu a obtenção de conhecimento técnico dos princípios que regem estas soluções, como o Triângulo CIA (confidencialidade, integridade e disponibilidade), e a aplicação prática de metodologias de defesa, como a gestão de *patches* e segmentação de acesso.

A **terceira etapa** teve como foco a aprendizagem tanto a nível prático como teórico via formações específicas. Estas ofereceram uma base sólida para compreender as necessidades do mercado e as tecnologias disponíveis.

Durante este processo, foram adquiridos conhecimentos sobre:

- **Segurança de redes e defesa de infraestrutura:** Como configurar e gerir dispositivos de rede, incluindo *firewalls* e *switches*, e como implementar estratégias de segmentação para mitigar ataques.
- **Gestão de vulnerabilidades:** Métodos de identificação e priorização de vulnerabilidades, considerando o risco e a facilidade de exploração, bem como técnicas de reporte eficiente.
- **Análise de rede:** Uso de ferramentas como Wireshark para compreender tráfego de rede, identificar anomalias e correlacionar eventos para detetar atividades maliciosas.
- **Resposta a incidentes:** Aplicação de metodologias práticas para gerir incidentes de segurança, desde a deteção inicial até à contenção e mitigação.

Adicionalmente, o estudo incluiu temas emergentes, como a utilização do OSINT (*Open Source Intelligence*) para recolha de dados públicos de forma ética e legal, e o entendimento das operações na *Dark Web*, com foco na monitorização de ameaças e geração de relatórios.

Este processo permitiu-me criar uma visão ampla e prática da cibersegurança, com ênfase nas necessidades reais do mercado e nas soluções inovadoras para os desafios identificados.

Provas

Search by name, course 🔍

Badge



COURSE

Introduction to Cybersecurity

Issued On: Sep 05, 2024

Badge



COURSE

Cyber Threat Management


Issued On: Sep 05, 2024

Courses Progress

Check your learning path progress!

Training Courses

	Introduction to Network Analysis	100%	
	Introduction to OSINT	100%	
	Introduction to Threat Hunting	72%	
	Introduction to Vulnerability Management	82%	
	Cybersecurity Interview Preparation	20%	
	Introduction to Bash	100%	
	Introduction to PowerShell	41%	

 Search course, training

Academy


All


 |

Type All

BEGINNER



 Cisco Academy


Course | Self-paced


Networking Devices and Initial Configuration

Continue learning networking essentials and build your foundational skills.

Part of career path
Junior Cybersecurity Analyst

BEGINNER



 Cisco Academy


Course | Self-paced


Networking Basics

Start learning the basics of computer networking and discover how networks operate.

Part of career path
Junior Cybersecurity Analyst

BEGINNER



 Cisco Academy

Course | Self-paced

Network Defense

Learn how to monitor and protect your network and evaluate security alerts.

Part of career path
Junior Cybersecurity Analyst

BEGINNER

