Relatório Final

Entidade: Citeforma
Curso: Técnico Especialista em Cibersegurança

Autor: João Rodrigo Mota da Costa

Data de criação: 13 de outubro de 2023
Data de revisão: 17 de outubro de 2023

Índice

Resumo

No âmbito deste relatório, delineio a minha jornada ao longo do curso de Técnico Especialista em Cibersegurança no Citeforma, e do subsequente estágio, que decorreu na Wide Shift, uma MSP situada em São João da Talha, de maio a setembro de 2023. Irei proporcionar uma análise detalhada das minhas interações e experiências com os formadores, destacando as suas contribuições para o meu desenvolvimento profissional. Enfatizarei as tecnologias que integrei na minha formação e aplicação prática, elucidando a sua relevância no contexto da cibersegurança. Por último, examinarei a conexão essencial entre o curso e o estágio, destacando como a minha formação académica preparou-me para as demandas do mundo real e como a experiência de estágio enriqueceu o meu conhecimento e competências. Este relatório visa oferecer uma visão abrangente do meu percurso e demonstrar o meu crescimento como profissional na área da cibersegurança.

Abstract

Português de Portugal

Neste relatório, é apresentada uma análise detalhada do percurso académico e profissional do autor, abrangendo o curso de Técnico Especialista em Cibersegurança e um estágio de três meses e meio na Wide Shift, uma MSP, realizado entre maio e setembro de 2023. O relatório destaca a interação do autor com os formadores, enfatiza as tecnologias fundamentais para a cibersegurança exploradas ao longo do percurso e examina a sinergia entre a formação académica e a experiência de estágio. Este relatório oferece uma visão abrangente da evolução do autor como profissional de cibersegurança, evidenciando o papel fundamental do ensino e da aplicação prática na preparação para desafios do mundo real.

American English

This report provides a detailed analysis of the author's academic and professional journey, encompassing the Technical Specialist in Cybersecurity course and a three-and-a-half-month internship at Wide Shift, an MSP, conducted between May and September of 2023. The report highlights the author's interactions with instructors, underscores the fundamental technologies explored in the field of cybersecurity, and examines the synergy between academic training and internship experience. This report offers a comprehensive view of the author's evolution as a cybersecurity professional, emphasizing the pivotal role of education and practical application in preparation for real-world challenges.

Glossário

Este glossário destina-se a fornecer uma referência rápida e útil para os termos e conceitos essenciais utilizados ao longo deste relatório. A cibersegurança é um campo em constante evolução, repleto de terminologia técnica específica, e este recurso foi criado para auxilio na compreensão e interpretação do conteúdo apresentado.

Termo	Significado	Definição
AES	Advanced Encryption Standard	Padrão de criptografia amplamente utilizado para proteger dados sensíveis por meio de algoritmos de criptografia.
eTOM	Enhanced Telecom Operations Map	Modelo de processo que descreve as operações de telecomunicações de uma organização e fornece uma estrutura de gestão eficiente.
ITIL	Information Technology Infrastructure Library	Práticas recomendadas para a gestão de serviços de IT que visa melhorar a eficiência e a eficácia da entrega de serviços de IT numa organização.
MSP	Managed Services Provider	Empresa que oferece serviços geridos de TI, como monitorização, manutenção e suporte para organizações.
OWASP	Open Web Application Security Project	Comunidade de especialistas em segurança informática que fornece informações e recursos para ajudar a proteger aplicações web contra ameaças de segurança, como ataques informáticos.
PBX	Private Branch Exchange	Sistema de telecomunicações que permite às organizações encaminhar chamadas telefónicas internas e externas para os ramais dos funcionários numa rede telefónica privada.
QEMU/KVM	Quick Emulator/Kernel-based Virtual Machine	Combinação de virtualização que permite a execução de máquinas virtuais com desempenho próximo ao nativo em sistemas Linux.
RSA	Rivest-Shamir-Adleman	Um dos algoritmos de criptografia assimétrica mais utilizados, com base na cálculo fatorial de números inteiros grandes.
SIEM	Security Information and Event Management	Sistema que recolhe, correlaciona e analisa eventos de segurança numa rede, permitindo que as organizações detetem e respondam a possíveis ameaças de segurança.
SSH	Secure Shell	Protocolo de rede que fornece segurança na comunicação entre computadores, geralmente usado para acessar remotamente sistemas e servidores.
SQL	Structured Query Language	Linguagem de programação utilizada para gerir e consultar bancos de dados relacionais.

Tecnologias envolvidas

Ao longo do meu percurso no curso de Técnico Especialista em Cibersegurança e no estágio subsequente, deparei-me com um vasto leque de tecnologias essenciais para o campo da cibersegurança. Estas ferramentas desempenharam um papel fundamental na minha formação e experiência prática, permitindo-me desenvolver as competências necessárias para enfrentar os desafios do mundo da segurança cibernética. Nesta secção, destacarei as tecnologias que explorei e utilizei ao longo destas duas etapas da minha jornada académica e profissional.

Criptografia

- AES
- OpenPGP
- RSA
- Xiao Steganography

Investigação forense

- Autopsy
- FTK Imager

Linguagens de programação

- Bash
- Batch
- C++
- G-BASIC
- Markdown (HTML + CSS)
- Powershell
- Python
- SQL

Redes e segurança de redes

- Cisco Packet Tracer
- Nmap
- Wireshark
- OpenCanary
- Snort
- Wazuh

Scanners de vulnerabilidades

- OpenVAS
- Tenable Nessus

Servidores e serviços web

- Apache
- Asterisk
- Bind9
- NGINX
- Openfire
- OpenSSH
- Postfix
- Squid Proxy

Sistemas operativos

- Arch Linux
- Debian
- Fedora
- Kali Linux
- Linux Mint
- OPNsense
- Parrot OS
- pfSense
- Red Hat Enterprise Linux 7/9
- Rocky Linux
- Ubuntu Desktop 22.10
- Ubuntu Server 22.04
- Windows 10/11
- Windows Server 2022

Testes de segurança e *pentesting*

- Aircrack-ng
- Burp Suite
- Ettercap
- GoPhish
- Maltego
- Shodan
- Wifite

Virtualização

- Hyper-V
- QEMU / KVM
- VirtualBox
- VMware ESXi
- VMware Workstation

Desenvolvimento do curso

Análise de evidências e vulnerabilidades

Formador: Rogélio Rodrigues

UFCDs lecionadas:

- UFCD 9189 | Tecnologias de analise de evidências
- UFCD 9191 | Introdução às Técnicas de Análise de Evidências
- UFCD 9192 | Análise de vulnerabilidades - iniciação
- UFCD 9193 | Análise de vulnerabilidades - desenvolvimento

Temas abordados:

- Aplicação de scans de vulnerabilidades
- Configuração e gestão de router e firewalls pfSense
- Configuração e gestão de servidores Windows e Linux
- Configuração e utilização de sistemas PBX
- Configuração e utilização de sistemas SIEM
- Exploração de vulnerabilidades inventariadas pelo OWASP

Cibersegurança e ciberdefesa

Formadores: João Almeida, Luís Roque, Paulo Vaz, Ricardo Lobo

UFCDs lecionadas:

- UFCD 9188 | Fundamentos de cibersegurança
- UFCD 9194 | Introdução à cibersegurança e à ciberdefesa
- UFCD 9195 | Enquadramento operacional de cibersegurança
- UFCD 9196 | Cibersegurança Ativa
- UFCD 9197 | Wargaming

Temas abordados:

- Desenvolvimento das capacidades de análise forense
- Desenvolvimento de atividades de *hacking* ético
- Desenvolvimento de documentação relacionada com a cibersegurança
- Identificação dos diferentes tipos de ataques informáticos
- Identificação das fases da "*Kill Chain*"
- Identificação do perfil e motivação de ataques informáticos

Desenvolvimento profissional

Formador: João Delgado

UFCDs lecionadas:

- UFCD 0683 | Ética e deontologia profissionais
- UFCD 5065 | Empresa - estrutura e funções
- UFCD 9187 | Legislação, segurança e privacidade

Temas abordados:

- Conscientização sobre a lei da cibersegurança
- Desenvolvimento das capacidades de apresentação em ambiente profissional
- Identificação dos valores morais, éticos e deontológicos associados à atividade profissional

Formação geral

Formadores: José Luís Louro, Manuela Laranjeira

UFCDs lecionadas:

- UFCD 3769 | Probabilidades e estatística
- UFCD 5064 | Matemática
- UFCD 5745 | Inglês Técnico

Temas abordados:

- Cálculo de probabilidades condicionais
- Métodos de arredondamento de números
- Métodos de cálculos de matrizes
- Métodos de conversão entre bases

Programação

Formadores: Luís Roque, Maria João Duarte

UFCDs lecionadas:

- UFCD 5089 | Programação - Algoritmos
- UFCD 5117 | Primeiros conceitos de programação e algoritmia
- UFCD 5410 | Bases de dados - conceitos
- UFCD 9190 | Introdução à programação aplicada à cibersegurança

Temas abordados:

- Desenvolvimento de algoritmos em pseudo-código
- Desenvolvimento de fluxogramas
- Elaboração de *scripts* em C++ e Python
- Identificação de sistemas de informação

Redes e telecomunicações

Formadores: João Pina, Manuel Ramos

UFCDs lecionadas:

- UFCD 5101 | Hardware e redes de computadores
- UFCD 5102 | Redes de computadores (avançado)
- UFCD 5104 | Instalação de redes locais
- UFCD 5106 | Serviços de rede
- UFCD 5892 | Modelos de gestão de redes e de suporte a clientes

Temas abordados:

- Configuração de equipamentos Cisco
- Introdução aos modelos eTOM e ITIL
- Introdução a redes de computadores
- Planeamento de redes e sub-redes

Sistemas operativos

Formador: António Matias

UFCDs lecionadas:

- UFCD 5113 | Sistema operativo cliente (plataforma proprietária)
- UFCD 5114 | Sistema operativo servidor (plataforma proprietária)

Temas abordados:

- Desenvolvimento de scripts em batch
- Introdução à configuração de sistemas Windows

Relação entre o curso e a formação em contexto de trabalho

O curso de Cibersegurança que frequentei desempenhou um papel fundamental na preparação e desenvolvimento das minhas competências, permitindo-me atuar de forma eficaz e segura no ambiente de trabalho da Wide Shift, uma MSP com uma carteira de cerca de 20 clientes. Ao longo do meu estágio, pude perceber a aplicabilidade direta dos conhecimentos adquiridos no âmbito do curso, o que contribuiu para uma maior eficiência e qualidade das minhas tarefas.

Uma das principais áreas em que o curso desempenhou um papel preponderante foi na criação de apresentações de cibersegurança para clientes. Através das competências desenvolvidas no curso, fui capaz de compreender de forma mais aprofundada os conceitos-chave da cibersegurança, traduzindo-os de forma clara e acessível para os clientes, enfatizando a importância de medidas preventivas e soluções específicas.

Além disso, a formação em Cibersegurança proporcionou-me a base necessária para elaborar documentação detalhada sobre auditorias de conformidade, alinhadas com os requisitos do Quadro Nacional de Referência da Cibersegurança (QNRCS) do Centro Nacional de Cibersegurança (CNCS). Isso permitiu-me contribuir ativamente para a garantia da segurança informática dos clientes da Wide Shift, fornecendo-lhes orientações claras e práticas para o cumprimento das normativas em vigor.

No desenvolvimento do plano de formações para o maior cliente da empresa, os conhecimentos adquiridos durante o curso permitiram-me identificar as necessidades específicas do cliente, adequando o conteúdo das formações de forma a abordar os tópicos mais relevantes e atuais em cibersegurança.

O curso também desempenhou um papel crucial na execução de testes de software, na análise forense de computadores de antigos colaboradores e na documentação de vários tópicos relacionados com a cibersegurança, tais como a encriptação de discos ou a gestão de credenciais. As competências técnicas e as metodologias aprendidas foram essenciais para conduzir investigações detalhadas e garantir a segurança dos sistemas.

A análise de websites para detetar possíveis intrusões também se beneficiou do conhecimento sólido em cibersegurança adquirido no curso, permitindo-me identificar vulnerabilidades e recomendar ações corretivas eficazes.

A criação de uma máquina virtual para campanhas de phishing com o GoPhish (e subsequente documentação) e o suporte pro-ativo aos clientes basearam-se em sólidos fundamentos de segurança informática, possibilitando a execução segura de atividades que requerem um alto nível de conscientização em relação a possíveis ameaças.

Além disso, o curso proporcionou uma compreensão profunda das melhores práticas de diagnóstico e manutenção de equipamentos, incluindo hardware e software, bem como a configuração de dispositivos para colaboradores. Essas habilidades foram essenciais na prestação de suporte eficaz aos clientes da Wide Shift.

Em conclusão, o curso de Cibersegurança desempenhou um papel vital na minha capacidade para realizar com sucesso as diversas tarefas desafiadoras no contexto da Wide Shift. Os conhecimentos adquiridos e as competências desenvolvidas foram uma base sólida para a minha atuação profissional, permitindo-me contribuir significativamente para a segurança informática dos clientes da empresa.

Conclusão

Cheguei ao fim deste relatório com a sensação de dever cumprido. Foi uma jornada intensa e desafiadora, mas extremamente gratificante. Ao longo do curso de Técnico Especialista em Cibersegurança, tive a oportunidade de aprender sobre as mais diversas tecnologias envolvidas na área, desde criptografia até testes de segurança e *pentesting*. Além disso, pude desenvolver minhas habilidades em programação, redes e sistemas operativos, entre outras áreas.

O estágio na Wide Shift foi uma experiência enriquecedora, que me permitiu aplicar na prática todo o conhecimento adquirido durante o curso. Foi uma oportunidade única de trabalhar num ambiente real, lidando com situações reais e aprendendo com profissionais experientes, sejam elas positivas ou negativas.

A relação entre o curso e a formação em contexto de trabalho foi fundamental para o meu desenvolvimento profissional. O curso preparou-me para as demandas do mundo real, e a experiência de estágio permitiu-me aprimorar as minhas habilidades e competências. Estou confiante de que estou preparado para enfrentar os desafios da área de cibersegurança e contribuir para a segurança digital das empresas e organizações.

Por fim, gostaria de agradecer ao Citeforma e à Wide Shift pela oportunidade de participar neste curso. Foi uma experiência única e inesquecível, que certamente contribuirá para o meu crescimento profissional e pessoal.