HENRIQUE CARVALHO

Porto • henrique1781@gmail.com • linkedin.com/in/henrique-carvalho-849450156 •
https://github.com/henryu1781

Cybersecurity

Profissional emergente em Cibersegurança com foco especializado em Operações de Segurança (SOC) e Arquitetura Defensiva. Combino uma mentalidade analítica rigorosa com uma abordagem estruturada para a triagem de incidentes e mitigação de riscos. Proficiente na operação de ecossistemas Linux, executo inspeção profunda de tráfego de rede, monitorização de eventos de segurança e análise forense de logs para detetar e neutralizar ameaças. Impulsionado pela aprendizagem contínua e talhado para ambientes de alta pressão, estou preparado para auditar, proteger e fortalecer (hardening) infraestruturas críticas.

WORK EXPERIENCE

Setor da Hospitalidade
Gestão de Operações de Alta Pressão (Turno Noturno) **Porto**

- Executou o controlo operacional em ambientes de elevado stress e urgência temporal, mantendo precisão absoluta e foco sob pressão.
- Forjou competências avançadas de consciência situacional, tomada de decisão rápida e gestão de múltiplas tarefas em simultâneo.
- Manteve disciplina operacional rigorosa e colaboração de equipa perfeita durante os períodos críticos de pico. (Nota: Estas soft skills espelham diretamente os requisitos psicológicos exigidos num ambiente de Resposta a Incidentes / SOC).

EDUCATION

Curso Técnico Superior Profissional (CTeSP) em Cibersegurança
ISTEC Porto Porto

Foco Central: Segurança de Sistemas e Redes, Criptografia, Threat Modeling, Hardening, Redes e Protocolos, Resposta a Incidentes.

PROJECTS

Arquitetura de Aplicações Seguras & Refactoring

- Arquitetou a reestruturação de uma aplicação legacy de reporte de incidentes em PHP para um ambiente seguro e moderno em Flutter/Dart.
- Implementou padrões rigorosos de secure coding, aplicando conceitos de hashing de passwords Argon2id, princípios de encriptação AES-256 e gestão de sessões seguras baseadas em JWT.
- Elaborou documentação técnica exaustiva orientada para a gestão de incidentes, rastreabilidade e compliance rigoroso de segurança.
- Alinhou todo o ciclo de vida do projeto com os princípios de segurança defensiva.

Operações de SOC & Laboratórios de Forense de Rede

- Executou análise profunda de tráfego de rede utilizando o Wireshark para isolar padrões anormais e identificar assinaturas comportamentais maliciosas.
- Conduziu análise forense de logs em sistemas Linux para detetar vetores de falha de autenticação e potenciais intrusões por força bruta (brute-force).
- Mapeou os comportamentos de ameaça identificados diretamente para o framework MITRE ATT&CK, produzindo relatórios de inteligência estruturados e acionáveis.

- Implementou protocolos fundamentais de hardening de sistemas, focados em configurações estritas de SSH e políticas de controlo de acesso.

Desenho de Redes Empresariais & Routing

- Desenhou e provisionou topologias de rede altamente segmentadas utilizando VLANs e protocolos de routing dinâmico (OSPF, EIGRP, RIP) em ambientes simulados.
- Integrou DHCP centralizado, medidas precisas de autenticação e mecanismos de controlo de acesso.
- Otimizou o desenho da infraestrutura para maximizar a visibilidade da rede e a monitorização contínua de segurança, com foco específico na prontidão para operações de SOC.

Wargaming Operacional & Threat Modeling

- Aplicou as metodologias Cyber Kill Chain, Unified Kill Chain e MITRE ATT&CK para dissecar e analisar cenários complexos de ataque.
- Co-desenvolveu o TechVoyer, um framework personalizado de threat-modeling focado em reconhecimento agressivo e contramedidas defensivas.
- Formulou diagramas arquiteturais estruturados e relatórios de inteligência mapeando os TTPs (Tactics, Techniques, and Procedures) dos atacantes para controlos defensivos específicos.

SKILLS

Operações Defensivas (SOC): Análise e Resposta Básica a Incidentes, Monitorização de Eventos de Segurança, Triagem de Alertas

Infraestrutura & Hardening: Ambientes Linux (Arch Linux, Ubuntu Server), Docker, Gestão de Utilizadores & Permissões, Hardening de Sistemas

Inteligência de Rede: Análise de Tráfego (Wireshark), Deep Packet Inspection, DHCP, DNS, Segmentação de Redes, TCP/IP

Ferramentas de Segurança: Caido (Análise de Tráfego & Pedidos HTTP), Git/GitHub, Nmap (Reconhecimento)

Mindset Operacional: Colaboração em Equipa, Pensamento Altamente Analítico, Precisão sob Pressão, Resolução Rápida de Problemas