Dau Trong Hoang

HCMC @ work@mizu.reisen https://mizu.reisen
dau-trong-hoang sakkarose mizu

Experience

TeraBox Technology
Security Engineer
Dec 2023 - Present

- Deployed and configured SIEM systems (Wazuh & Graylog) for small and medium-sized businesses, enabling real-time threat detection, log management, orchestration, and comprehensive security monitoring across networks, endpoints, and cloud environments.
- Developed and implemented 20+ Graylog rules, organized into pipelines, to effectively filter noise and enrich logs collected from Wazuh.
- Created and maintained 100+ Wazuh detection rules and active responses to proactively identify and mitigate emerging malware threats.
- Architected and enhanced a robust security solution, leveraging Wazuh as a core component and integrating with over 10 diverse open-source APIs and tools to meet specific organizational security requirements.
- Implemented Security Configuration Assessment (SCA) using CIS Benchmarks on Windows Server 2022 and Ubuntu Server 22.04, achieving compliance scores of 90-96% and significantly reducing server and remote desktop attack surfaces.
- Currently developing an automated solution to rapidly provision and update a Wazuh container stack, including pre-configured rules and active responses, enhancing deployment efficiency.
- Outside regular business hours, proactively monitored the threat landscape for APTs, IoCs, vulnerabilities, and emerging threats, utilizing this intelligence to inform and refine security strategies.
- Implemented SSH hardening on Linux servers to mitigate risks associated with SSH-based attacks.
- Collaborated with the compliance department to deliver impactful security awareness training, conduct thorough compliance audits, and perform comprehensive risk assessments.

https://terabox.vn

Education

University of Information Technology
7.2
BE, Computer Systems Networking and Telecommunications
2019 - 2024

Skills

Operations

Security Monitoring, Threat Detection, Incident Response, Vulnerability Management, Security Hardening, Threat Intelligence, Endpoint Security, Compliance Management

Technologies & Tools

SIEM (Wazuh/Graylog), SCA (CIS benchmark), SOAR (Shuffle), Visualization (Grafana), Endpoint Security Monitoring (Sysmon/Tetragon), Incident Response (Wazuh/Velociraptor), Web App Security (Nuclei/OWASP ZAP), Container Security (Grype), Network Security (OPNsense/Palo Alto/Sophos), Threat Intelligence (MISP/CrowdSec/Maltrail/EPSS/GrayNoise/VirusTotal), Vulnerability Scanner (Wazuh/Nessus)

Frameworks

MITRE ATT&CK, OWASP

Operating Systems

Windows, Windows Server, Void Linux, Tails, Kali Linux, Raspberry Pi OS, Alpine Linux

Programming Languages

Python (Intermediate), Shell (Intermediate), PowerShell (Basic)

Certifications

Google IT Automation with Python Specialization
Feb 2025

Google Cybersecurity Certificate
Oct 2024

Certified in Cybersecurity (CC)
Sep 2024

Projects

Homelab
Aug 2024 - Present

A self-hosting infrastructure built with Podman on Fedora CoreOS for learning security architecture and testing malware detection rules.

Personal Blog
Nov 2024 - Present

My personal corner of the internet, where I delve into cybersecurity. Built with Hugo and hosted on Cloudflare Pages.

https://mizu.reisen

WPA2 Pentest Research
Providing insights into common password pitfalls in Vietnam to help users avoid weak Wi-Fi security.
Dec 2021 - Present

https://github.com/sakkarose/vie_wpa2_pw