Dau Trong Hoang

HCMC work@mizu.reisen https://mizu.reisen
LinkedIn GitHub TryHackMe

Experience

TeraBox Technology
Security Engineer
Dec 2023 - Present

- **Deployed a comprehensive security monitoring platform** using Wazuh and Graylog, establishing real-time threat detection and log management across firewalls, endpoints, and SaaS environments.
- Implemented over **20 Graylog processing rules** within pipelines, **reducing log noise by 20%** and enhancing data enrichment from Wazuh sources for improved analysis accuracy and faster incident identification.
- **Orchestrated the development and maintenance of over 100 custom Wazuh detection rules and active responses,** enabling proactive identification and automated mitigation of emerging malware threats.
- **Integrated a comprehensive security solution** by combining Wazuh with over 10 diverse open-source tools and APIs, including threat intelligence feeds and vulnerability scanners. This enhanced our defensive posture by providing actionable insights for strategic decision-making.
- **Executed Security Configuration Assessments (SCA)** based on CIS Benchmarks across Windows Server 2022 and Ubuntu 22.04 environments, consistently achieving **up to 96% compliance scores**. This demonstrably reduced the attack surface for servers and Remote Desktop Protocol (RDP) vulnerabilities.
- **Monitored the cyber threat landscape** with threat feeds, and security advisories (tracking APTs, IoCs, vulnerabilities), translating threat intelligence into actionable insights to refine defensive strategies and security controls.
- **Fortified our perimeters** by implementing robust SSH hardening on remote Linux servers to mitigate brute-force attacks and by applying advanced configuration hardening on Palo Alto firewalls for secure remote connectivity and system availability.
- **Developed a forensic playbook for logless Windows environments**, standardizing procedures for evidence preservation, data collection, and artifact analysis.
- **Collaborated with the compliance team to bridge security and GRC.** This included developing and delivering targeted security awareness trainings and conducting comprehensive risk assessments to identify, prioritize, and track the remediation of security gaps.

Compliance Engineer
Nov 2023 - Present

- **Collaborated with teams to design and implement a GRC program** that achieved and has maintained both ISO 9001:2015 and ISO 27001:2013 certifications since 2023. This included developing the ISMS, a comprehensive set of policies, and a Statement of Applicability (SoA).
- **Planned and suggested new technical controls to mitigate specific compliance risks.** For example, implementing a CIS-hardened VM template to reduce the "insecure VM configuration" risk and deploying a PAM solution like JumpServer to address "weak privileged OS passwords."
- **Led the creation and maintenance of compliant IT management systems and workflows.** This included designing Incident and Change Management processes on Jira to reduce change-related incidents to zero after 4 months.
- **Developed and executed a bi-annual security awareness training program for technical staff,** resulting in a measurable reduction of risk from new cyber threats, such as URL phishing and AiTM phishing.
- **Conducted regular security assessments and vulnerability testing,** driving the remediation of all critical vulnerabilities within a 30-day window and proactively reducing the organization's attack surface.

Education

University of Information Technology
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), Incident Response (Wazuh/Velociraptor), Vulnerability Scanner (Wazuh/Nessus), Endpoint Security Monitoring (Sysmon), Threat Intel (MISP/CrowdSec/Maltrail/VirusTotal)

Frameworks

MITRE ATT&CK, OWASP

Operating Systems

Windows (Server), Alpine, Kali, Void, Raspberry Pi, CoreOS

Programming Languages

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

Wazuh provisioning
Mar 2025 - Present

A fork of the official Wazuh Docker deployment, aiming enhancing and simplifying threat detection on docker single-node & all-in-one (AIO) server deployment.

https://github.com/sakkarose/wazuh-provision

Homelab
Aug 2024 - Present

This homelab aims to create an environment for: Running a Wazuh stack in rootless Docker, Learning new operating systems, Testing security technologies, tools and approaches, Self-hosting personal applications.

https://github.com/sakkarose/homelab

Personal Blog
Nov 2024 - Present

A static blog with Hugo as framework. This is where I share my insights on small projects and implementations related to my favorite fields: self-hosting, security, and operating systems.

https://mizu.reisen

WPA2 Pentest Research
Dec 2021 - Present

Providing insights into common password pitfalls in Vietnam to help users avoid weak Wi-Fi security.

https://github.com/sakkarose/vie_wpa2_pw