Dau Trong Hoang

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

Experience

TeraBox Technology
Security Engineer
Dec 2023 - Present

- Deployed and configured Wazuh & Graylog SIEM solutions for small and medium-sized businesses, establishing real-time threat detection, centralized log management, and comprehensive security monitoring across diverse environments (networks, endpoints, cloud).
- Implemented over 20 Graylog processing rules within pipelines, significantly reducing log noise and enhancing data enrichment from Wazuh sources for improved analysis accuracy and faster incident identification.
- Managed a set of over 100 custom Wazuh detection rules and active responses, enabling proactive identification and automated mitigation of emerging malware threats and suspicious activities.
- Continuously enhanced a comprehensive security monitoring solution centered on Wazuh, integrating 10+ diverse open-source tools and APIs (including threat intelligence feeds, vulnerability scanners, and custom scripts) to meet specific organizational security requirements and improve defensive posture.
- Executed Security Configuration Assessments (SCA) based on CIS Benchmarks across Windows Server 2022 environments, consistently achieving up to 96% compliance scores and demonstrably reducing server and Remote Desktop Protocol (RDP) attack surfaces.
- Regularly monitored the cyber threat landscape by analyzing Open Source Intelligence (OSINT), threat feeds, and security advisories (tracking APTs, IoCs, vulnerabilities), translating threat intelligence into actionable insights to refine defensive strategies and security controls.
- Applied robust SSH hardening techniques across Linux server fleets to mitigate risks associated with brute-force and configuration-based attacks.
- Implemented configuration hardening on Palo Alto firewalls' VPN and network security to ensure secure remote connectivity and system availability.
- Partnered with the compliance department to develop and deliver targeted security awareness training programs, execute internal compliance audits against established frameworks, and conduct comprehensive risk assessments to identify, prioritize, and track remediation of security gaps.

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), Network Security (OPNsense/Palo Alto/Sophos), Vulnerability Scanner (Wazuh/Nessus), Endpoint Security Monitoring (Sysmon), Threat Intel (MISP/CrowdSec/Maltrail/EPSS/VirusTotal), Web App Security (ZAP)

Frameworks

MITRE ATT&CK, OWASP

Operating Systems

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

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