Projektthema / Thesis

Aufbau eines virtuellen Referenznetzwerks für SIEM-Testszenarien auf Basis von Proxmox

Ziel:

Ziel ist die Konzeption und der Aufbau eines realitätsnahen, virtuellen Unternehmensnetzwerks, das als Referenzumgebung für die Weiterentwicklung und das Testen eines Open-Source-SIEM-Systems dient. Das Netzwerk soll typische Unternehmenskomponenten wie Windows-Server, Linux-Clients und Security-Appliances abbilden und eine heterogene, nachvollziehbare Infrastrukturstruktur aufweisen. Besonderes Augenmerk liegt auf der Automatisierbarkeit und Wiederholbarkeit des Aufbaus. Durch gezielte Automatisierung soll die Umgebung effizient bereitzustellen und zu rekonfigurieren sein, um künftige SIEM-Regel und -komponentenentwicklungen zu unterstützen.

Aufgaben:

- Analyse und Konzeptentwicklung für ein virtuelles Unternehmens-Referenznetz auf Basis von Proxmox
- Definition typischer Systemtypen und Netzwerkstrukturen (Clients, Server, Appliances, Netzsegmente)
- Evaluierung geeigneter Open-Source-Komponenten für Endpunkte und Sicherheitslösungen
- Aufbau einer reproduzierbaren Proxmox-Infrastruktur mit Fokus auf Automatisierung
- Entwicklung eines Ansatzes zur automatisierten Bereitstellung und auch Aktualisierung von Endpunkten
- Dokumentation der Architektur, Konfiguration und Automatisierungsschritte
- Bewertung der Umgebung hinsichtlich Realitätsnähe, Performance und Wartbarkeit
- Empfehlung für Erweiterungen (z. B. zusätzliche Log-Quellen, Security Appliances oder Monitoring-Dienste)

Ideen für Basis-Technologien (Environment):

- Proxmox, Terraform, Ansible, Linux (Debian/Ubuntu), Windows Server ggf. mit Active Directory, Windows Clients (10/11), NetBox IPAM, OPNsense/pfSense, Git, GitOps

Ideen/Referenzen:

[1] GOAD – Game of Active Directory: https://github.com/Orange-Cyberdefense/GOAD

[2] SOCBED: https://github.com/fkie-cad/socbed

[3] Building a Realistic Enterprise Level SOC LAB for Blue & Red Teamers: https://www.hackpie.com/posts/Building_SOC_LAB_PART1/

[4] Reproducible and Adaptable Log Data Generation for Sound Cybersecurity Experiments: https://arxiv.org/pdf/2111.07847

Level: geeignet für Bachelor oder Master (Anpassung des Niveaus)

Sprache: Deutsch oder Englisch

Beginn: sofort

Studierendenprojekt in Kooperation von DN.lab (TH Köln) und Procyde

Interessenten wenden sich an Thomas Karl (karriere@procyde.com) oder Prof. Grebe (andreas.grebe@th-koeln.de) und senden ihren PSSO-Auszug mit.

Projektthema / Thesis

Development of a Virtual Reference Network for SIEM Test Scenarios Based on Proxmox

Objective:

The goal is to design and implement a realistic, virtual enterprise network that serves as a reference environment for the further development and testing of an open-source SIEM system. The network should represent typical enterprise components such as Windows servers, Linux clients, and security appliances, providing a heterogeneous and transparent infrastructure structure. Particular emphasis is placed on automation and reproducibility.Through targeted automation, the environment should be deployable and reconfigurable efficiently to support future SIEM rule and component development.

Tasks:

- Analysis and conceptual design of a virtual enterprise reference network based on Proxmox
- Definition of typical system types and network structures (clients, servers, appliances, network segments)
- Evaluation of suitable open-source components for endpoints and security solutions
- Implementation of a reproducible Proxmox-based infrastructure with a focus on automation
- Development of an approach for automated deployment and updating of endpoints
- Documentation of the architecture, configuration, and automation steps
- Evaluation of the environment regarding realism, performance, and maintainability
- Recommendations for extensions (e.g., additional log sources, security appliances, or monitoring services)

Suggested Base Technologies (Environment):

Proxmox, Terraform, Ansible, Linux (Debian/Ubuntu), Windows Server (optionally with Active Directory), Windows Clients (10/11), NetBox IPAM, OPNsense/pfSense, Git, GitOps

References and Inspiration:

[1] GOAD – Game of Active Directory: https://github.com/Orange-Cyberdefense/GOAD

[2] SOCBED: https://github.com/fkie-cad/socbed

[3] Building a Realistic Enterprise Level SOC LAB for Blue & Red Teamers: https://www.hackpie.com/posts/Building_SOC_LAB_PART1/

[4] Reproducible and Adaptable Log Data Generation for Sound Cybersecurity Experiments: https://arxiv.org/pdf/2111.07847

Level: Suitable for Bachelor's or Master's thesis (depending on scope)

Language: German or English

Start: Immediately

Type: Student project in cooperation with DN.lab (TH Köln) and Procyde

Contact: Interested students should contact Thomas Karl (karriere@procyde.com) or Prof. Grebe (andreas.grebe@th-koeln.de)