Projektthema / Thesis

Konzeption und prototypische Umsetzung einer Scoring-Engine für ein Open-Source-SIEM

Ziel:
Konzeption und prototypische Umsetzung einer Scoring-Engine, die sicherheitsrelevante Ereignisse in einem Open-Source-SIEM zu quantifizierbaren Risiko- oder Relevanzwerten darstellt. Die Engine soll Ereignisse aus bestehenden Erkennungsmechanismen (z. B. regelbasierte Alerts) bewerten und in eine einheitliche, für Analysten nutzbare Score-Struktur überführen. Im Fokus steht eine nachvollziehbare, erweiterbare Architektur, die sowohl einfache Einstiegsmechanismen als auch spätere Erweiterungen (z. B. zusätzliche Kontextfaktoren) ermöglicht. Die Ergebnisse sollen in einer geeigneten Datenstruktur abgelegt werden, um sie für Dashboards, Priorisierung und automatisierte Reaktionen nutzbar zu machen

Aufgaben:

- Analyse bestehender Ansätze zur Risiko- und Relevanzbewertung in SIEM- und Security-Analytics-Systemen
- Erarbeitung eines fachlichen Modells zur Bewertung sicherheitsrelevanter Ereignisse (z. B. Basis-Score, Gewichtungen, zeitliche Aspekte)
- Design einer skalierbaren Architektur für eine Scoring-Engine auf Basis eines bestehenden Open-Source-SIEM-Stacks
- Definition eines Datenmodells für die Speicherung und Abfrage von Scores (z. B. pro Entität wie Benutzer, Host, IP)
- Prototypische Implementierung einer ersten Ausbaustufe der Scoring-Engine inkl. Schnittstellen zum SIEM
- Dokumentation von Architektur, Implementierungsansatz, Grenzen und möglichen Erweiterungsstufen

Basis-Technologien (Environment): OpenSearch, OpenSearch Dashboards, SIGMA, Linux, Python/Go, REST-APIs, JSON, Git, Docker/Kubernetes

Ideen/Referenzen:

[1] Risk scoring in Splunk Enterprise Security: https://help.splunk.com/en/splunk-enterprise-security-8/administer/8.4/risk-based-alerting/risk-scoring-in-splunk-enterprise-security

[2] Elastic Entity Risk Scoring: https://www.elastic.co/docs/solutions/security/advanced-entity-analytics/entity-risk-scoring

[3] UEBA risk score customization and its significance in threat detection: https://www.manageengine.com/log-management/cyber-security/ueba-risk-score-customization-and-its-importance-in-threat-detection.html

[4] RISK-BASED ALERTING IN SIEM ENTERPRISE SECURITY: ENHANCING ATTACK SCENARIO MONITORING THROUGH ADAPTIVE RISK SCORING: https://doi.org/10.34218/IJCET_11_02_009

[5] Dynamic Risk Thresholds for SIEM Alerting Based on Machine Learning: https://ieeexplore.ieee.org/iel8/6287639/10820123/11078272.pdf

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

Design and Prototypical Implementation of a Scoring Engine for an Open-Source SIEM System

Objective:
The goal is to design and implement a prototype of a scoring engine that translates security-relevant events within an open-source SIEM system into quantifiable risk or relevance values. The engine should evaluate events generated by existing detection mechanisms (e.g., rule-based alerts) and convert them into a unified, analyst-friendly scoring structure. The focus is on a transparent, extensible architecture that supports both straightforward initial scoring mechanisms and future extensions (e.g., additional contextual factors). The results are to be stored in a suitable data model, enabling their use in dashboards, prioritization processes, and automated response mechanisms.

Tasks:

- Analyze existing approaches to risk and relevance scoring in SIEM and security analytics systems
- Develop a conceptual model for assessing security-relevant events (e.g., base score, weighting, temporal aspects)
- Design a scalable architecture for a scoring engine based on an existing open-source SIEM stack
- Define a data model for storing and querying scores (e.g., per entity such as user, host, or IP)
- Implement a prototype of the scoring engine, including interfaces to the SIEM platform
- Document the architecture, implementation approach, limitations, and possible extensions

Base Technologies (Environment): OpenSearch, OpenSearch Dashboards, SIGMA, Linux, Python/Go, REST APIs, JSON, Git, Docker/Kubernetes

References and Inspiration:

[1] Risk scoring in Splunk Enterprise Security: https://help.splunk.com/en/splunk-enterprise-security-8/administer/8.4/risk-based-alerting/risk-scoring-in-splunk-enterprise-security

[2] Elastic Entity Risk Scoring: https://www.elastic.co/docs/solutions/security/advanced-entity-analytics/entity-risk-scoring

[3] UEBA risk score customization and its significance in threat detection: https://www.manageengine.com/log-management/cyber-security/ueba-risk-score-customization-and-its-importance-in-threat-detection.html

[4] RISK-BASED ALERTING IN SIEM ENTERPRISE SECURITY: ENHANCING ATTACK SCENARIO MONITORING THROUGH ADAPTIVE RISK SCORING: https://doi.org/10.34218/IJCET_11_02_009

[5] Dynamic Risk Thresholds for SIEM Alerting Based on Machine Learning: https://ieeexplore.ieee.org/iel8/6287639/10820123/11078272.pdf

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) and include their PSSO transcript