SOC_DatenVolumen

Souveränes Security Operations Center mit innovativem eBPF

Programm / Ausschreibung	KIRAS, F&E-Dienstleistungen, KIRAS-K-Pass-KMU Innovation AKUT KIA F&E Dienstleistungen (FED KIA_2024)	**Status**	laufend
Projektstart	01.02.2026	**Projektende**	31.01.2027
Zeitraum	2026 - 2027	**Projektlaufzeit**	12 Monate
Projektförderung	€ 99.997		
Keywords	Souveränität, CyberAbwehr, Anomalieerkennung, Alert-Fatigue		

Projektbeschreibung

Security Operations Centers müssen Protokolldaten und Logs über lange Zeiträume und aus diversen Quellen speichern um zu einem späteren Zeitpunkt Rückschlüsse über die Forensik eines Angriffes zu haben. Dieser „Sammle-alles“-Ansatz in verursacht hohe Kosten, erschwert die Identifikation relevanter Signale und führt zu Alert-Fatigue. In diesem Projekt schlagen wir einen neuartigen und digital souveränen Ansatz basierend auf Anomalieerkennung auf Kernel-Ebene vor, der durch eBPF und signierten Verhaltensprofile(„Software Bill of Behavior“, SBoB) realisiert wird. Unser Design überwacht Systemaufrufe, Netzwerkverkehr und Dateizugriffe in Echtzeit, erkennt signifikante Abweichungen und aktiviert ereignisgesteuerte, forensisch relevante Datenerfassung. Die zu prüfende Forschungsfrage ist, inwiefern das Datenvolumen reduziert, während die Detektionsqualität erhalten bleibt Hierzu evaluieren wir diverse False-Positives Tuning Ansätze. Ergänzend entwickeln wir eine Kubernetes-basierte Testumgebung, die eine skalierbare Evaluierung gegen bekannte Angriffsmuster (gemappt auf MITRE ATT&CK) ermöglicht. Das Projekt leistet einen Beitrag zur Effizienzsteigerung in der Cyberabwehr und zur Stärkung der digitalen Souveränität. Es ermöglicht den Ausweg aus der passiven, flächendeckenden Datensammlung hin zu einer aktiven, kontextsensitiven Analyse.
Perspektivisch bildet diese Technologie die Grundlage einer skalierbaren Abwehr auf allen Linux Systemen in kritischer Infrastruktur unseres Landes.

Abstract

Security Operations Center have the requirement to persist data over long timescales and across system layers in order to allow the future forensic triage of an attack. This prevailing “collect-everything” paradigm leads to excessive costs, low signal-to-noise ratios, and analyst alert fatigue. We propose a novel and digitally souvereign kernel-level anomaly based approach realised by eBPF and signed behavioral profiles (“Software Bill of Behavior”, SBoB). Our prototype continuously monitors system calls, network traffic, and file operations, detects significant deviations in real time, and triggers event-driven, forensic-grade data capture. A key research question is to measure the reduction of resulting data volumes while preserving detection quality. We thus compare various false-positives-tuning approaches. Additionally, we provide a

Kubernetes-based testbed for scalable evaluation against known attack patterns (mapped to MITRE ATT&CK). The project contributes to more efficient cyber defense and strengthens digital sovereignty by shifting from passive, large-scale data collection to active, context-aware analysis.
Our long term vision is to use this technology as basis for a nationwide scalable defense of all linux systems that make up the critical infrastructure of our country.

Projektkoordinator

- SBA Research gemeinnützige GmbH

Projektpartner

- Bundesministerium für Landesverteidigung
- WhizUs GmbH