AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

AMINER – ERKENNUNG SMARTER CYBER ANGRIFFE IN KOMPLEXEN INFRASTRUKTUREN

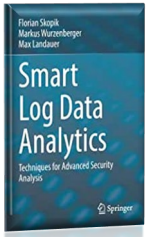
Ideenwettbewerb Innovationstagung Cyber und Informationstechnologie, 12.7.2023, München

Markus Wurzenberger, Florian Skopik, Max Landauer, Wolfgang Hotwagner

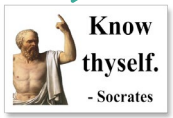
HERAUSFORDERUNGEN

Neuartige Bedrohungen	• Intelligente Angreifer mit zielgerichtetem Vorgehen (Im Schnitt 21 Tage bis zur Erkennung) • Ausnutzung gestohlener/kompromittierter Zugangsdaten • Fehlende und veraltete Signaturen (Mehr als 500.000 neue Malware Samples täglich) • Erwarteter Anstieg des finanziellen Schadens um 70% in den nächsten 5 Jahren
Massive Datenmengen	• Infrastrukturen, Datenstrukturen, und Angriffsfläche wachsen und ändern sich rapide • Manuelle Adaption der Angriffserkennung nicht zeitgerecht möglich • Mix unterschiedlicher Systeme: IT, OT, IoT, CPS, Legacy Systems, etc. • Manche Infrastrukturen generieren Milliarden an Logzeilen pro Tag (50GB Logdaten pro Stunde)
Echtzeit Analyse	• Online Verarbeitung von Daten (Single Pass) • Textuelle Analyse vs. Analyse numerischer Daten • Eingeschränkte Verfügbarkeit von Ressourcen und Konnektivität • 5.000 Logzeilen pro Sekunde und mehr müssen zu Spitzenzeiten verarbeitet werden
Alert Flooding	• 80% aller Alarme sind False Positives (Fehlalarme) • Triage von Alarmen derzeit nur manuell möglich und zeitaufwändig • Interpretation von kontextlosen Alarmen schwierig • Reduktion der manuell zu bearbeiten Security Events ist nötig um Personal zu entlasten

Quellen: AV-Test Institute, Mandiant, IBM, Lupovis, Statista

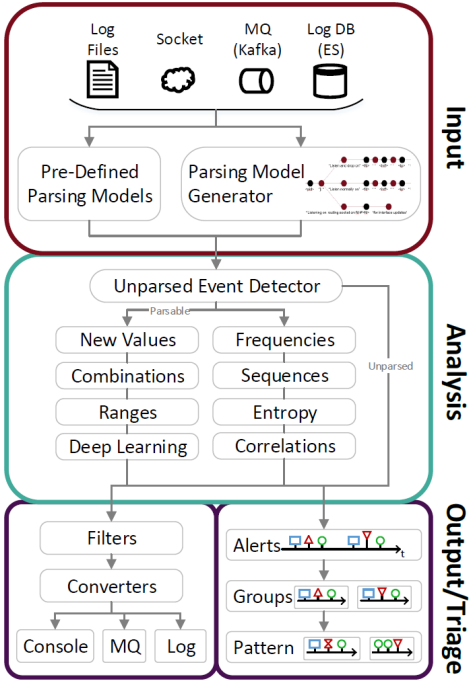


*„**AMiner observes** a system's log data to **learn** a model that represents the system's specific normal behavior and helps to **discover** deviations that represent emerging threats using its smart & patented anomaly detection."*



AMINER – A WAY OUT

- **Lücken schließen:** Ergänzung zu bestehenden Sicherheitslösungen
- **Privacy Preserving und Ressourcen schonend:** Dezentrale Analyse
- **Feingranulare Analyse:** Verarbeitung verboser Logdaten
- **Effizienter Parser:** Parser Generator und Baumstruktur
- **Online Analyse:** Effiziente Detektoren mit Single-Pass Verfahren
- **Automatische Anpassung:** Erkennung von Zero-Day Exploits
- **Triage durch Alert Aggregation:** Angriffsmuster erkennen und FP filtern



https://github.com/ait-aecid/logdata-anomaly-miner

FLEXIBLE ANWENDBARKEIT

AUSTRIAN INSTITUTE OF TECHNOLOGY

synERGY

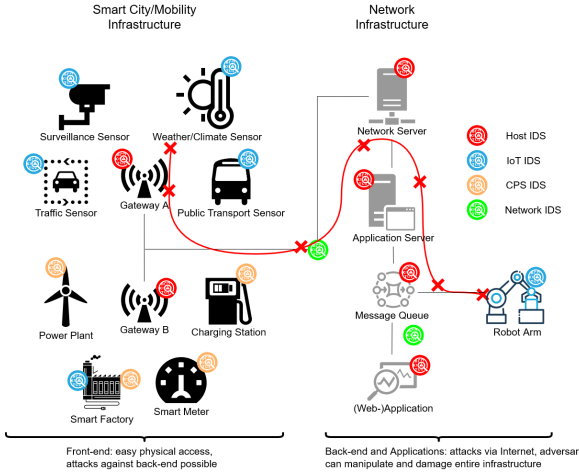
- Anomalieerkennung in gemischten IT und OT Netzen
- Beispiel Stromnetz

Bundesministerium
Klimaschutz, Umwelt,
Energie, Mobilität,
Innovation und Technologie

FFG Promoting Innovation.

DECEPT.

- Erkennung Cyber-physischer Angriffe
- Enterprise IT und BMS
- SIEM, Schließ- und Kamerasysteme



European Commission | Horizon 2020 European Union funding for Research & Innovation

GUARD

- Smart City und Smart Mobility
- Fernsteuerung dezentraler AMiner-Agents
- Generierung von actionable CTI

European Commission
EUROPEAN DEFENCE INDUSTRIAL DEVELOPMENT PROGRAMME

PANDORA

AInception
AI FRAMEWORK FOR IMPROVING CYBER DEFENCE OPERATIONS

- Threat Hunting für Cyber Defence
- Anwendung von Federated Learning
- Deep Learning für Logdatenanalyse
- AI gestützte Angriffsmustererkennung

EUROPEAN UNION
EUROPEAN DEFENCE FUND

NEWSROOM

- Anomalieerkennung als Beitrag zur CSA
- Missions-orientierte Bereitstellung von Lagebildern

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

DON‘T GET HACKED, GET AMINER!

Markus Wurzenberger, 12.7.2023