APT Detection: an Incremental Correlation Approach

S.D. Cakmakci, K.-O. Detken (DECOIT®)

G. Gkoktsis (Fraunhofer SIT — ATHENE)

R. Buchta, F. Heine, C. Kleiner · T. Laue (University of Applied Sciences Hanover)

Dr. Salva Daneshgadeh Cakmakcı
DECOIT® GmbH & Co. KG
Fahrenheitstraße 9
D-28359 Bremen
https://www.decoit.de
daneshgadeh@decoit.de

Agenda

- Introduction
- SecDER project
- Advanced Persistent Attack (APT)
- Research questions
- System architecture
- Attack phases
- Detection rules
- Discussion
- Conclusion

The project

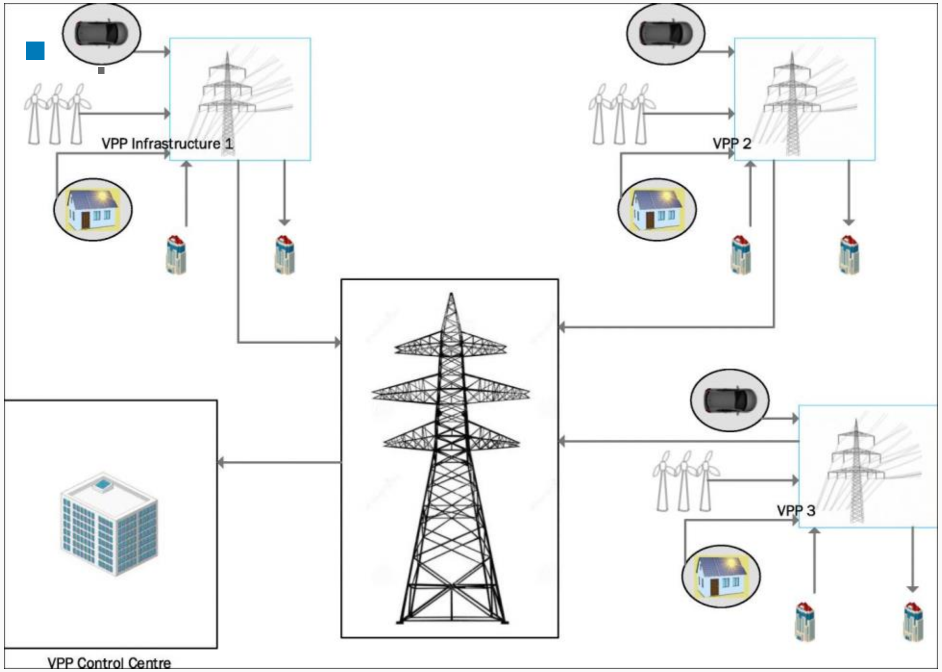
- SecDER = Incident Information System for Virtual Power Plants
  - https://secder-project.de
  - April 2021-March 2024
- Cooperation project within the German BMWi
- Partners:
  - Fraunhofer IEE: coordinator, research, and specialist for IT solutions of renewable energies
  - Fraunhofer SIT: research and IT security specialist, e.g. trusted computing and AI-assisted attack detection
  - DECOIT® GmbH & Co. KG: developer, and SIEM specialist
  - University of Applied Sciences of Hanover: research and IT security / trusted computing specialist
  - ENERTRAG: Energy supplier and provider of the PowerTrade virtual power plant

Federal Ministry
of Economics
and Technology

Introduction

- Prediction: 2035–2040
- IoT devices in electricity system will mostly communicate through VPPs
- More IT/OT dependent → more cyber attack prone

- Virtual Power Plant (VPP) : are not exist in the solid and-turbine sense



S.K. Venkatachary et al. (2021)

Advanced Persistent Attack (APT)

- In 2022: at least 403 reported cyber attack incidents against energy sectors, with 179 successful data breaches.
- In 2022: Cyber attacks cost the energy sector 4.72 million per incident on average.
- **Ukraine 2015 and 2016 Attacks**: against 3 regional power distribution companies. → power outage
- **U.S. Grid Intrusion 2014 →** infiltration
- **Dragonfly/Energetic Bear Campaign →** spear-phishing emails and watering hole attack against Energy sector from 2011.

Focus of SEC DER

- Detection of technical faults in power plants via KPI-trending and AI-based models (LSTM)
- Detection of cyber attack via rules (aggregation of various security events)
- Detection of cyber attack via AI-based methods (provenance graph)
- Cyber resilient defense strategy: to increase availability, integrity and confidentiality of power plants against cyber attacks and technical disruptions

Focus of paper: Advanced Persistent Attack (APT)

- Advanced: it has the resources and technical capability to stealthily and effectively compromise the target
- Persistent: it insists in its efforts until it accomplishes its objective
- Threat: it has the malicious intent, capability and opportunity to attack

APT Detection

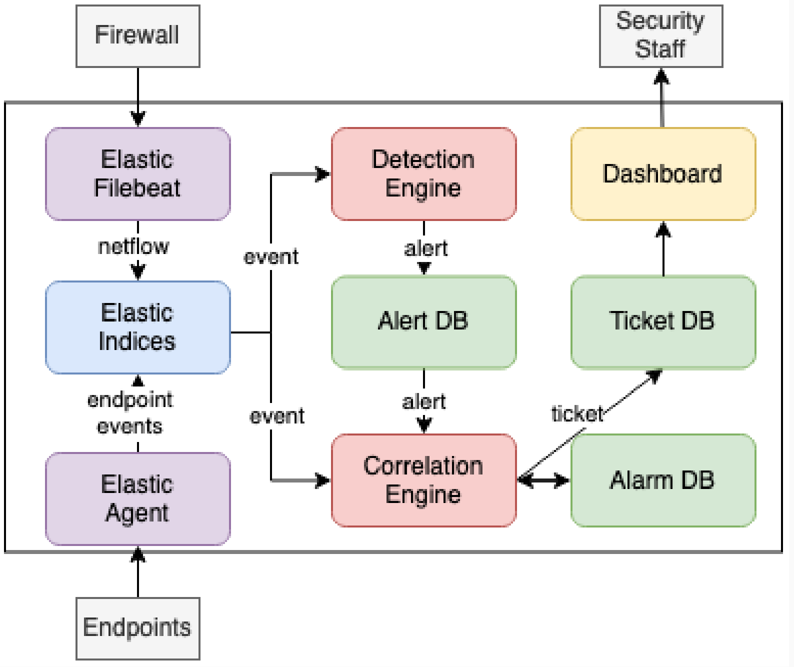
- AI-based methods
  - Initial methods: Machine Learning, Deep Learning → usually concentration on a single step of APT
- Current trend in the <u>LITERATURE</u>:
  - Provenance graph + semantic techniques for reasoning about causality
- Real-world??

Research questions

- Market analysis:
  - All SIEMs provide rule-based attack detection.
- Motivation of research:
  - How can existing rule-based systems be adapted to the requirements of APT attacks by correlating events?
  - What is the trade-off of using rule-based systems in terms of APT detection?
  - Concentration: SMEs

Proposed Framework

- Backbone : Elasticsearch and Elastic Security
- ScanBox (SIEM)
  - Core features:
    - data collection
    - data parsing and normalizing
    - detection engine (running simple rules)
  - Integrated features:
    - Correlation engine
    - Comprehensive tickets
    - Playbooks



Proposed Framework (Detection engine)

- Simple rule
  - if (host.os.type = "windows" and event.id =4625)
- Threshold rule:
  - if (host.os.type = "windows" and *count* ((event.id =4625))>3 in 5 minutes)
- Sequential rule:
  - if (host.os.type = "windows" and *count* ((event.id =4625))>3 in 5 minutes) and then event.id =4624)
- Threat inteligent rule:
  - if (source.ip matchs CTI.IP)
- Alert: event(s) that causes a match

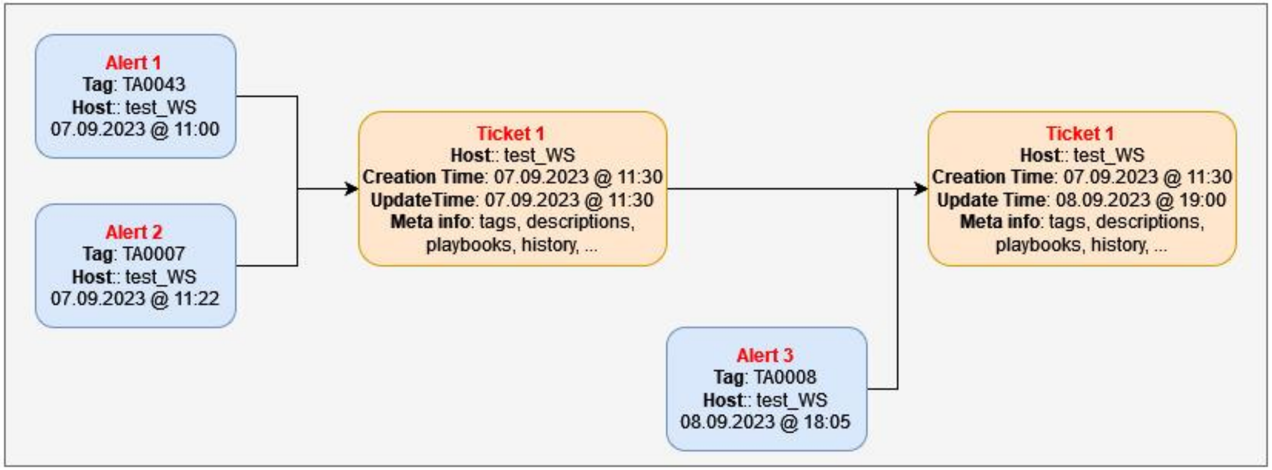
  Alert = Event info + Tags +Timestamp
- Tags : Mitre Tactic and Technique id, Asset identifier, Affected asset

Proposed Framework (Correlation engine 1)

- Incremental correlation approach:
  - Spatial Dimension: (e.g., Host, IP address, user)
  - Methodical Dimension: (e.g, TA0043, TA0007)
  - Temporal Dimension: (e.g., one hour, 1 day, one week)
- Correlates low level alerts:
  - Example 1: user accesses with unfamiliar GoIP and scans the selective ports.
  - Example 2: two alerts with different ATT&CK Tactics (e.g, TA0043, TA0007) on a single host
- Correlates alarm and alert
  - Example 3 : a new alert with MITRE tactic id of TA0008 is created on the same host that caused ticket in Example 2

Proposed Framework (Correlation engine 2)

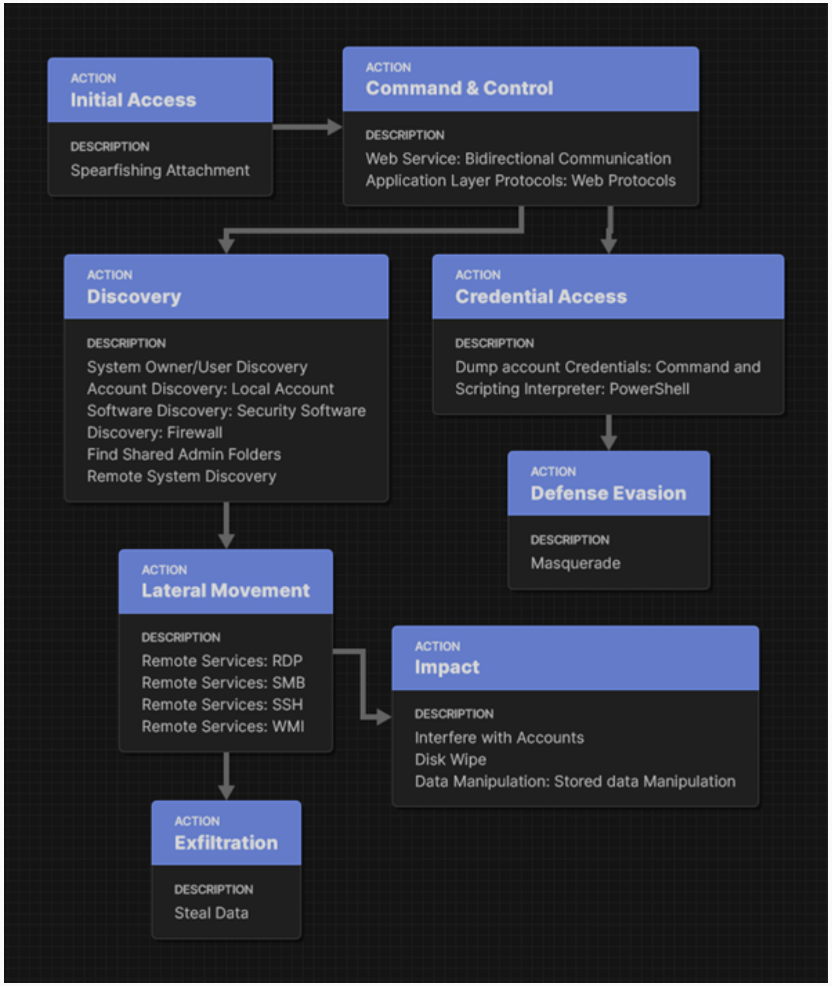
- Correlates low level alerts:
  - Example 1: user access with unfamiliar GoIP and scan the selective ports.
  - Example 2: two alerts with different ATT&CK Tactics (e.g, TA0043, TA0007) on a single host
- Correlates alarm and alert
  - Example 3: a new alert with MITRE tactic id of TA0008 is created on the same host that caused ticket in Example 2



APT Attack Tree

Attack Scenario

1. Send phishing e-mail
2. Establish a channel for C2 communication (via SSH)
3. Perform various discoveries
   - AV, FW identification
   - Find new victim (privileged user) and/or DC
4. Disable AV and/or FW
5. Install Mimikataz
   - Obtain the password hash of a privileged user
6. Connect to DC via RDP
   - Disable all users
   - Create new user



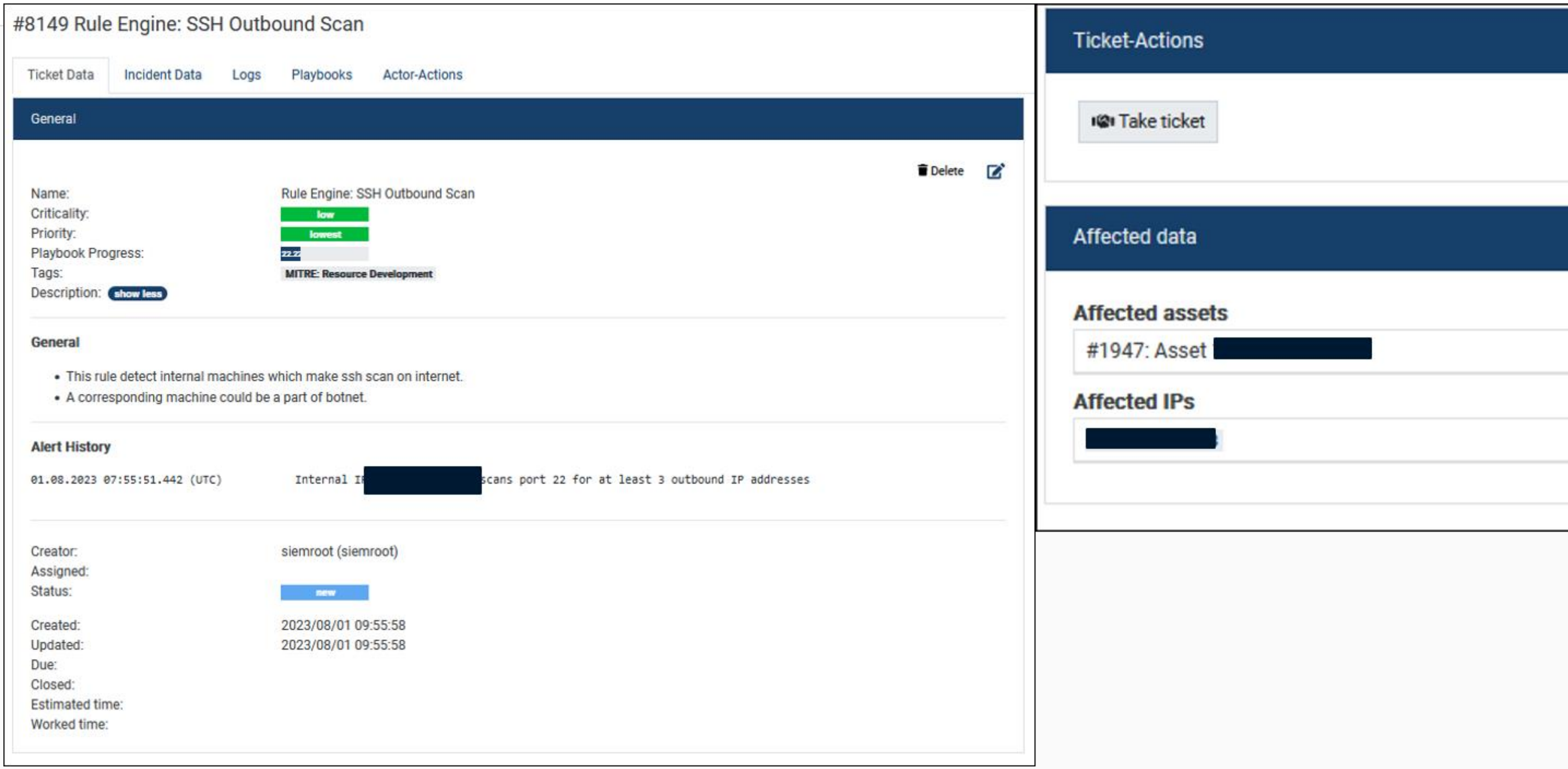
Detection Rules

- Elastic prebuilt rules for network and OS application data sources:
  - Example 1: detection of C2 communications via the registered domains which used by specific threat groups
  - Example 2: detection of discovery attempts via the execution of the \`whoami\`,\`net\` and \`wmic\` utilities or Get-SmbShare module
  - Example 3: PowerShell scripts that load Mimikataz in memory, like Invoke-Mimikataz
- Customized rules:
  - Example 1: unusual user activity time
  - Example 2: unusual user location
  - Example 3: unusual user activity
- Correlation rules (Python scripting)
  - Username, MITRE tags, Time
  - Host, MITRE Tags, Time

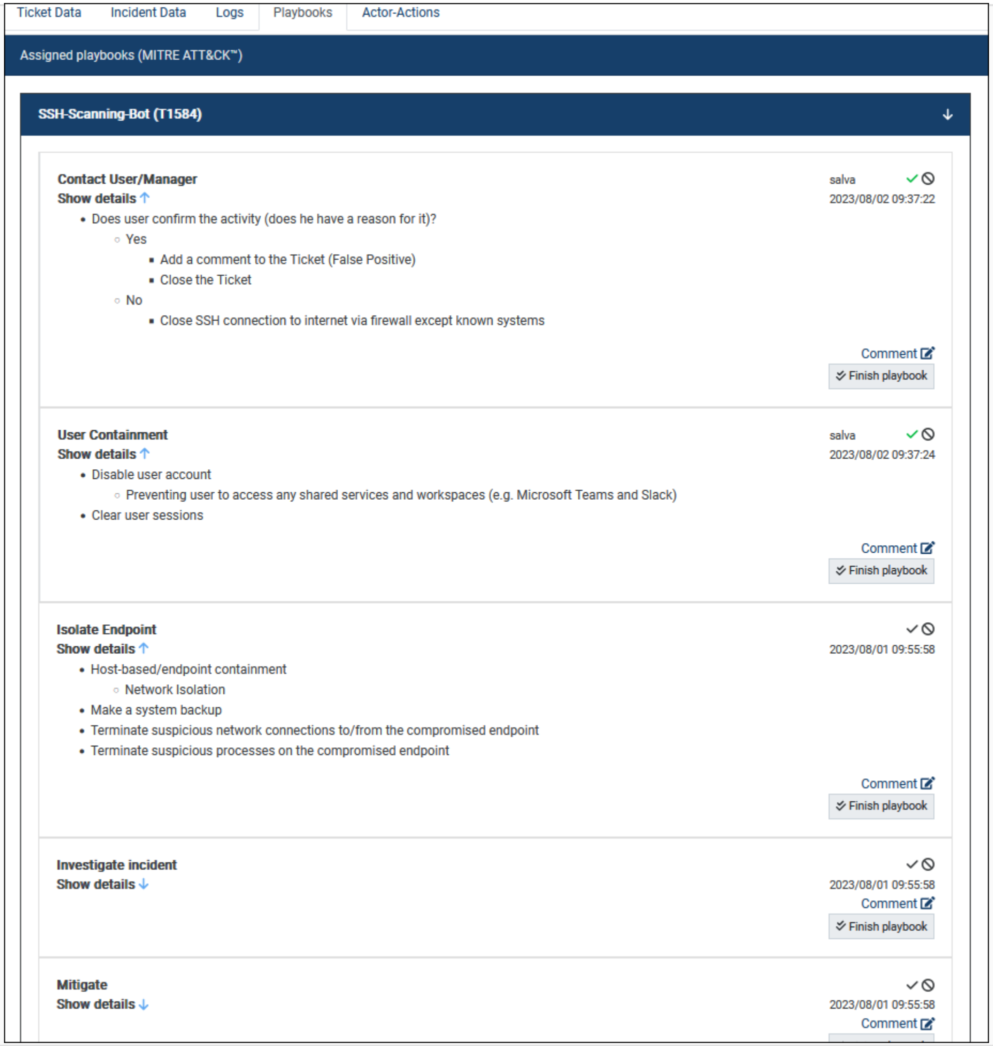
Implementation and test

- Ongoing project
- The whole system has not been tested yet!
- Difference with Elastic security:
  - Correlate only between alerts based on Host
  - No Incremental correlate of alerts

Example of a Ticket



Example of a Playbook



Discussion

- Advantages:
  - Re-use: community-driven or commercial rule sets
  - Easily extendable by adding new rules
  - Low chance of false positive alarms
  - Less resource problem (time and memory cost)
- Disadvantages:
  - Only detect known patterns
  - Known patterns should be hard-coded (maybe tens of correlation rules!!)
  - rule-based systems are more of an annoyance to the attacker but not a hindrance

Conclusion

- A rule-based APT attack detection scheme: correlates atomic intrusion detection alerts to form a high-level APT intrusion alarm
- A solution based on ELK stack (free license)
- Is testable with the public abilities of the MITRE CALDERA framework.

Thank you for your attention!

DECOIT GmbH & Co. KG
Fahrenheitstraße 9
D-28359 Bremen
https://www.decoit.de
info@decoit.de