



## 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<sup>®</sup> GmbH & Co. KG Fahrenheitstraße 9 D-28359 Bremen https://www.decoit.de daneshgadeh@decoit.de

#### Open Source. Open Solutions. Open Strategies.



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

#### Open Source. Open Solutions. Open Strategies.



- 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<sup>®</sup> 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



© DECOIT GmbH & Co. KG

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)

Open Source. Open Solutions. Open Strategies.



Advanced Persistent Attack (APT)

- In 2022: at least <u>403 reported cyber attack</u> incidents against energy sectors, with <u>179</u> successful data breaches.
- In 2022: Cyber attacks cost the energy sector <u>4.72</u> 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 → spearphishing emails and watering hole attack against Energy sector from 2011.





- Detection of technical faults in power plants via KPItrending 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**

### Al-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??

Open Source. Open Solutions. Open Strategies.



### **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

#### Open Source. Open Solutions. Open Strategies.



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

#### Open Source. Open Solutions. Open Strategies.



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



Open Source. Open Solutions. Open Strategies.



**APT Attack Tree** 



Open Source. Open Solutions. Open Strategies.



### **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



#### Open Source. Open Solutions. Open Strategies.



**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

#### Open Source. Open Solutions. Open Strategies.



### 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

Open Source. Open Solutions. Open Strategies.



#8149 Rule Engine: SSH Ou	utbound Scan	т	icket-Actions
Ticket Data Incident Data Lo	ogs Playbooks Actor-Actions		
General			📽 Take ticket
Name:	Rule Engine: SSH Outbound Scan	🖥 Delete 🛛 🔀	
Criticality: Priority: Playbook Progress:	low Iowest 22.22	A	Affected data
Tags: Description: (show less)	MITRE: Resource Development	A	Affected assets
General     This rule detect internal machin     A corresponding machine could	ines which make ssh scan on internet. Id be a part of botnet.	A	#1947: Asset
Alert History 01.08.2023 07:55:51.442 (UTC)	Internal Interna	s	
Creator: Assigned:	siemroot (siemroot)		
Status: Created: Updated: Due: Closed: Estimated time:	2023/08/01 09:55:58 2023/08/01 09:55:58		
Worked time:			

#### Open Source. Open Solutions. Open Strategies.

### 

### Example of a Playbook

SSH-Scanning-Bot (T1584)	¥
Contact User/Manager	salva 🗸 🛇
Show details 1	2023/08/02 09:37:22
<ul> <li>Does user confirm the activity (does he have a reason for it)?</li> </ul>	
· Yes	
Add a comment to the Ticket (False Positive)	
No	
Close SSH connection to internet via firewall except known systems	
	Comment 📝
	✓ Finish playbook
llear Containmant	calva 🗸 🛇
Show details ^	2023/08/02 09:37:24
Disable user account	
<ul> <li>Preventing user to access any shared services and workspaces (e.g. Microsoft Teams and Slack)</li> </ul>	
Clear user sessions	
	Comment 🗗
	Comment 🕑
	Comment <b>I</b> ∕ ≫ Finish playbook
Isolate Endpoint	Comment <b>Z</b> ⇒ Finish playbook
Isolate Endpoint Show details ↑	Comment <b>2</b>
Isolate Endpoint Show details ↑ • Host-based/endpoint containment	Comment 2
Isolate Endpoint Show details ↑ • Host-based/endpoint containment ○ Network Isolation	Comment C Finish playbook C 2023/08/01 09:55:58
Isolate Endpoint Show details ↑ • Host-based/endpoint containment • Network Isolation • Make a system backup	Comment C Finish playbook V Q 2023/08/01 09:55:58
Isolate Endpoint Show details ↑ • Host-based/endpoint containment • Network Isolation • Make a system backup • Terminate susplicious network connections to/from the compromised endpoint • Torminate susplicious network connections to/from the compromised endpoint	Comment 2 Finish playbook V Q 2023/08/01 09:55:58
Isolate Endpoint Show details ↑ • Host-based/endpoint containment • Network Isolation • Make a system backup • Terminate suspicious network connections to/from the compromised endpoint • Terminate suspicious processes on the compromised endpoint	Comment 2 ✓ Finish playbook ✓ Q 2023/08/01 09:55:58
Isolate Endpoint Show details ↑  • Host-based/endpoint containment  • Network Isolation  • Make a system backup  • Terminate suspicious network connections to/from the compromised endpoint  • Terminate suspicious processes on the compromised endpoint	Comment 2 ✓ Finish playbook ✓ © 2023/08/01 09:55:58 Comment 2
Isolate Endpoint Show details ↑ • Host-based/endpoint containment • Network Isolation • Make a system backup • Terminate suspicious network connections to/from the compromised endpoint • Terminate suspicious processes on the compromised endpoint	Comment 2 Finish playbook Comment 2 Comment 2 Finish playbook
Isolate Endpoint Show details ↑  • Host-based/endpoint containment • Network Isolation • Make a system backup • Terminate suspicious network connections to/from the compromised endpoint • Terminate suspicious processes on the compromised endpoint	Comment C Finish playbook COMMENT Comment C Finish playbook
Isolate Endpoint Show details ↑  • Host-based/endpoint containment  • Network Isolation  • Make a system backup  • Terminate suspicious network connections to/from the compromised endpoint  • Terminate suspicious processes on the compromised endpoint  Investigate incident Show details ↓	Comment C Finish playbook 2023/08/01 09:55:58 Comment C Finish playbook 2023/08/01 09:55:58
Isolate Endpoint         Show details ↑         • Host-based/endpoint containment         • Network Isolation         • Make a system backup         • Terminate suspicious network connections to/from the compromised endpoint         • Terminate suspicious processes on the compromised endpoint	Comment 2 Finish playbook Comment 2 Finish playbook 2023/08/01 09:55:58 Comment 2 2023/08/01 09:55:58 Comment 2 Comment
Isolate Endpoint Show details ↑  • Host-based/endpoint containment • Network Isolation • Make a system backup • Terminate suspicious network connections to/from the compromised endpoint • Terminate suspicious processes on the compromised endpoint • Terminate suspicious processes on the compromised endpoint • Terminate suspicious processes on the compromised endpoint	Comment C Finish playbook COMMENT Comment C Finish playbook Comment C Comment C Finish playbook
Isolate Endpoint         Show details ↑         • Host-based/endpoint containment         • Network Isolation         • Make a system backup         • Terminate suspicious network connections to/from the compromised endpoint         • Terminate suspicious processes on the compromised endpoint         • Terminat	Comment C Finish playbook COMMENT C Comment C Finish playbook Comment C Comment C Comment C Comment C Comment C Comment C Comment C
Isolate Endpoint         Show details ↑         • Host-based/endpoint containment         • Network Isolation         • Make a system backup         • Terminate suspicious network connections to/from the compromised endpoint         • Terminate suspicious processes on the compromised endpoint         • Terminat	Comment C Finish playbook COMMENT C 2023/08/01 09:55:58 Comment C S Finish playbook Comment C S Finish playbook Comment C S Finish playbook

#### Open Source. Open Solutions. Open Strategies.



### 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 <u>annoyance</u> to the attacker but not a <u>hindrance</u>





Conclusion

- A solution based on ELK stack (free license)
- Is testable with the public abilities of the MITRE CALDERA framework.

Open Source. Open Solutions. Open Strategies.

![](_page_21_Picture_0.jpeg)

# Thank you for your attention!

![](_page_21_Picture_2.jpeg)

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

![](_page_21_Picture_4.jpeg)

#### Open Source. Open Solutions. Open Strategies.