SIEM Data Check

Know Your Coverage — Identify Your Gaps

David Vogels, SECURIX Deutschland GmbH

Introduction

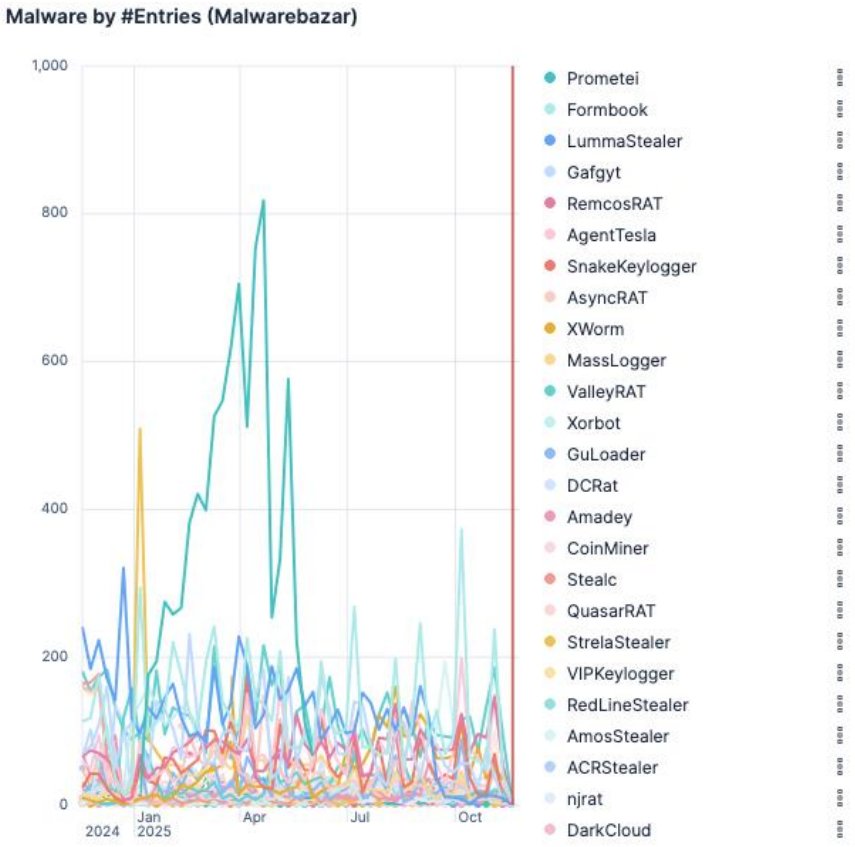
SECURIX

- **David Vogels**
- Senior IT Consultant (Observability)
- david.vogels@securix.swiss
- www.securix.swiss

Let's pick a malware

- Example: Prometei
- Steals credentials for self-propagation
- Host machine joins a botnet

- Purpose: To mine cryptocurrency (Monero)

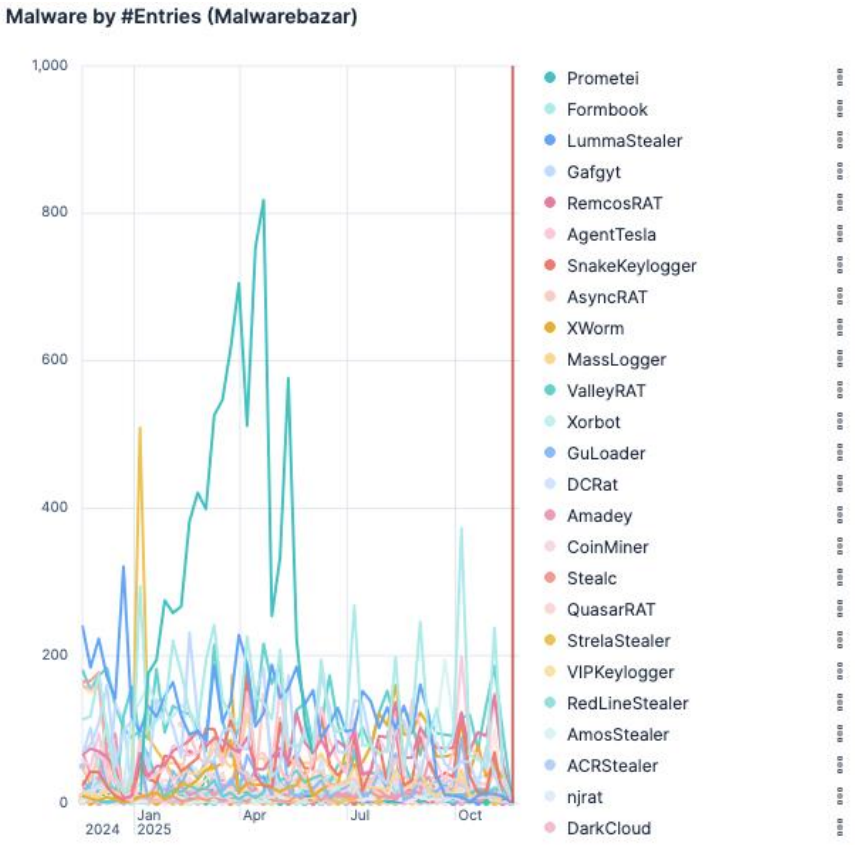


https://blog.talosintelligence.com/prometei-botnet-and-its-quest-for-monero/

Some facts about Prometei

SECURIX

- After infecting a system, a multi-stage download and unpacking begins
  - Using 7zip and Powershell
- About 8400 sample records on Malwarebazar
  - Almost all of them with unique file hashes
- Uses a Domain Generation Algorithm (DGA) for its C&C infrastructure
- Uses innocuous names to avoid detection
  - `uplugandplay.b64`
  - `winhlpx64.exe`



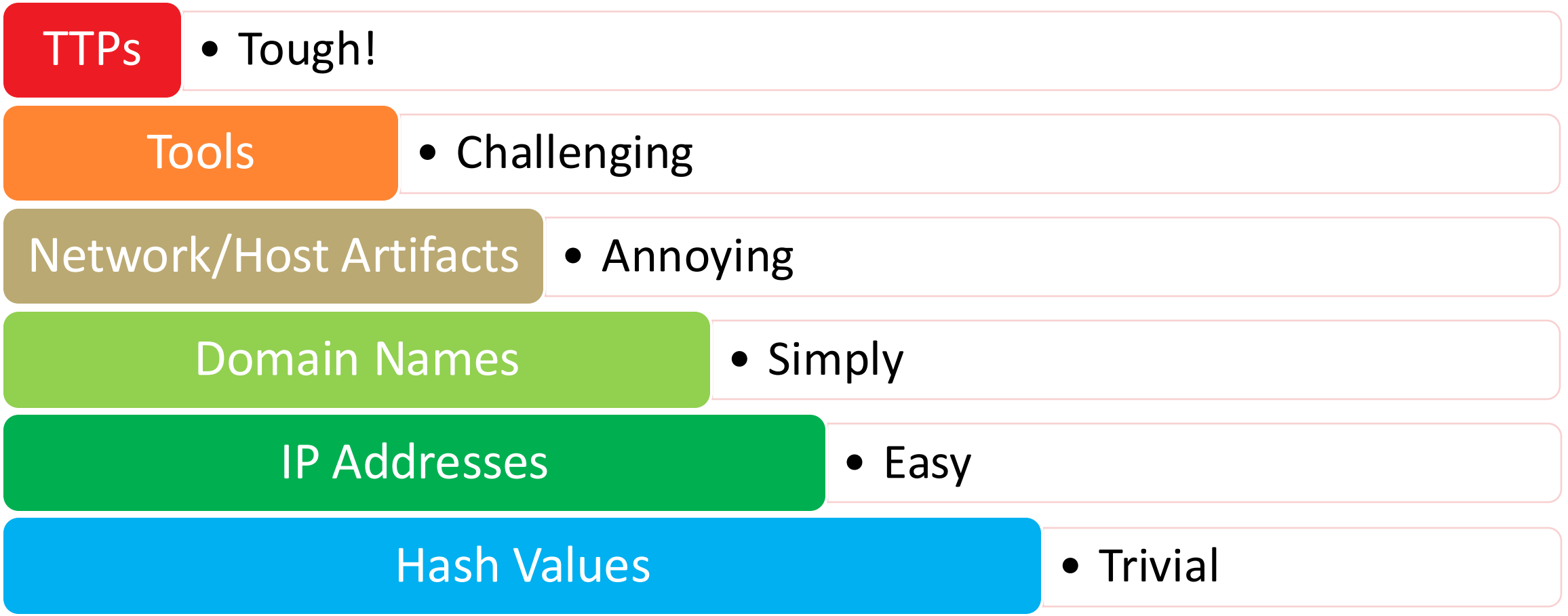
https://www.trendmicro.com/en_us/research/24/j/unmasking-prometei-a-deep-dive-into-our-mxdr-findings.html

The Problem

How can we detect attacks, when they change and adapt that quickly?

The Pyramid of Pain (David J. Bianco)

SECURIX



https://www.attackiq.com/glossary/pyramid-of-pain-2/

Prometei

SECURIX

TTPs	• ???
Tools	• PowerShell for deployment/lateral movement
Network/Host Artifacts	• Sets some specific registry keys
Domain Names	• Domain Generation Algorithm (DGA)
IP Addresses	• Cheap hosting; Botnet infra
Hash Values	• 8400 unique hashes

What are TTPs

SECURIX

Tactic

What is the purpose of the attacker's action?

Technique

What action does the attacker perform?

Procedure

How does the implementation of the action look like?

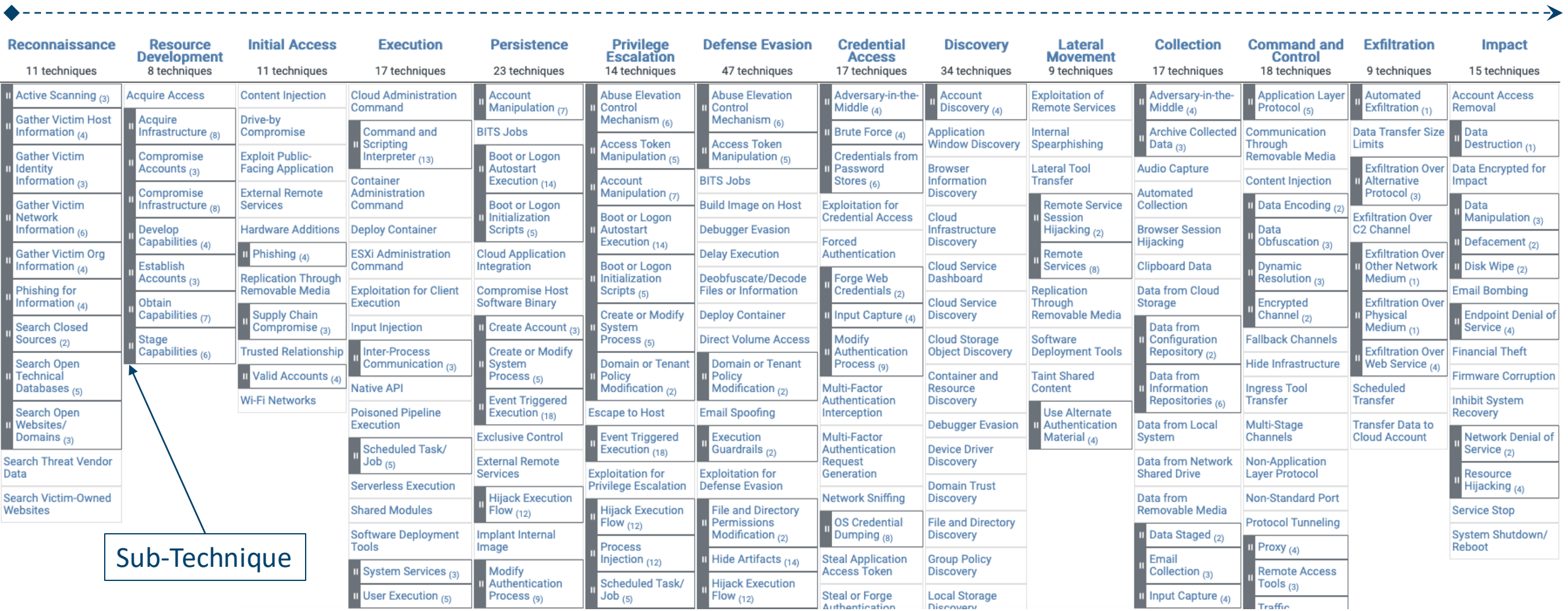
The Mitre Att&ck® Framework

SECURIX

- A model that systematically categorizes attacker behavior
- Lists Tactics in order of execution
  - For example: Reconnaissance first, later Initial Access, C&C even later.
- For each Tactic there are several Techniques
  - Sometimes there are Sub-Techniques for a specific Technique
- Example:
  - Tactic: Initial Access (TA0001)
  - Technique: Phishing (T1566)
  - Sub-Technique: Spearphishing Voice (T1566.004)
  - Example Procedure: Someone calling a victim and claiming they are legitimate IT personnel

The Mitre Att&ck® Framework

SECURIX



https://attack.mitre.org/versions/v18/

Using the Model in practice

SECURIX

- Forwards-Approach
  - What attacks are there?
  - How are they executed?
  - How can they be detected?
  - Which Assets to I need to monitor?

- Backwards-Approach
  - Which Assets do I have?
  - What attack vectors do I open myself up to?

The Mitre Att&ck® Framework

SECURIX

Detection Strategies

How can the used Technique be detected?

Data Components

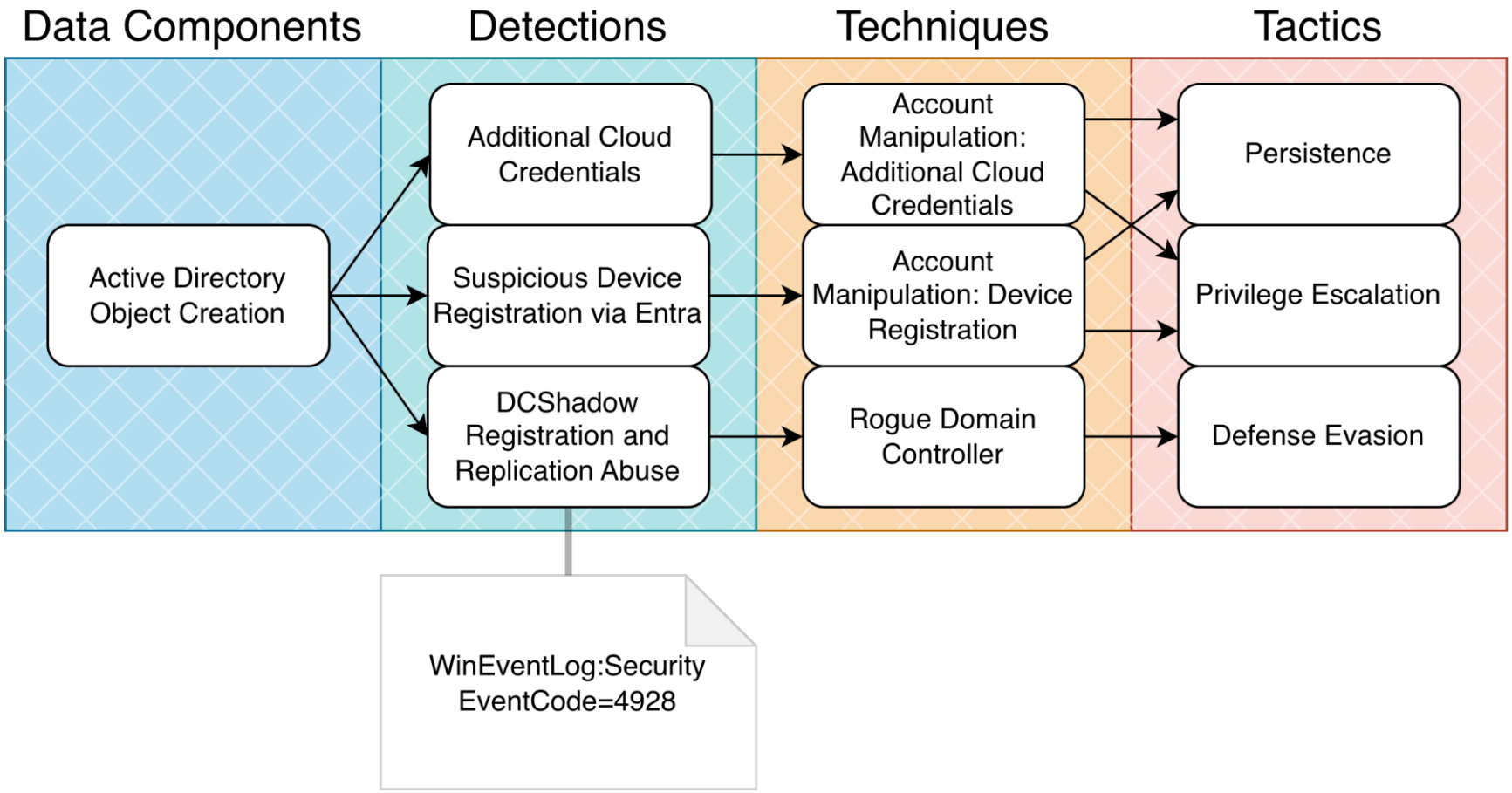
Are linked to one or more Detection Strategies

Mitigations

Containing the impact and/or probability of an attack

The Mitre Att&ck® Framework

SECURIX



SECURIX SIEM Data Check

SECURIX

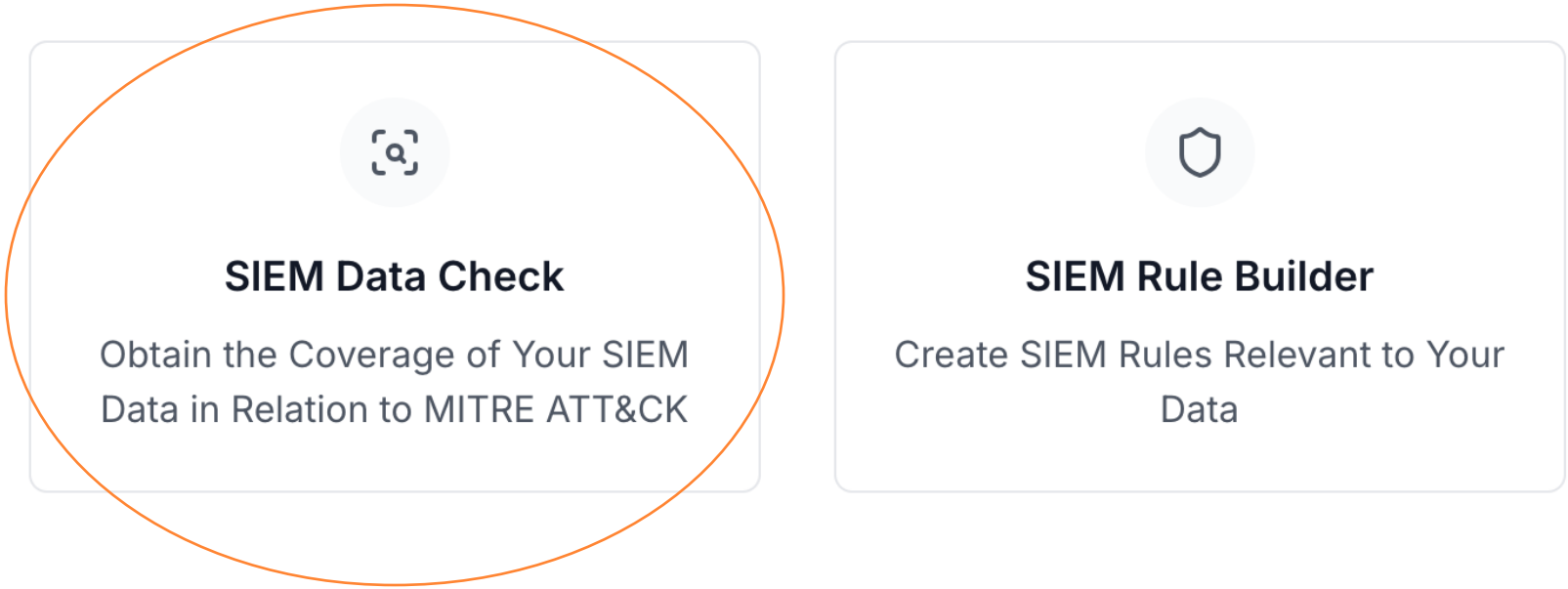
- Allows you to go from a list of assets to a list of tasks

- Take inventory of your infrastructure
- Your blind spots are directly mapped out to Techniques

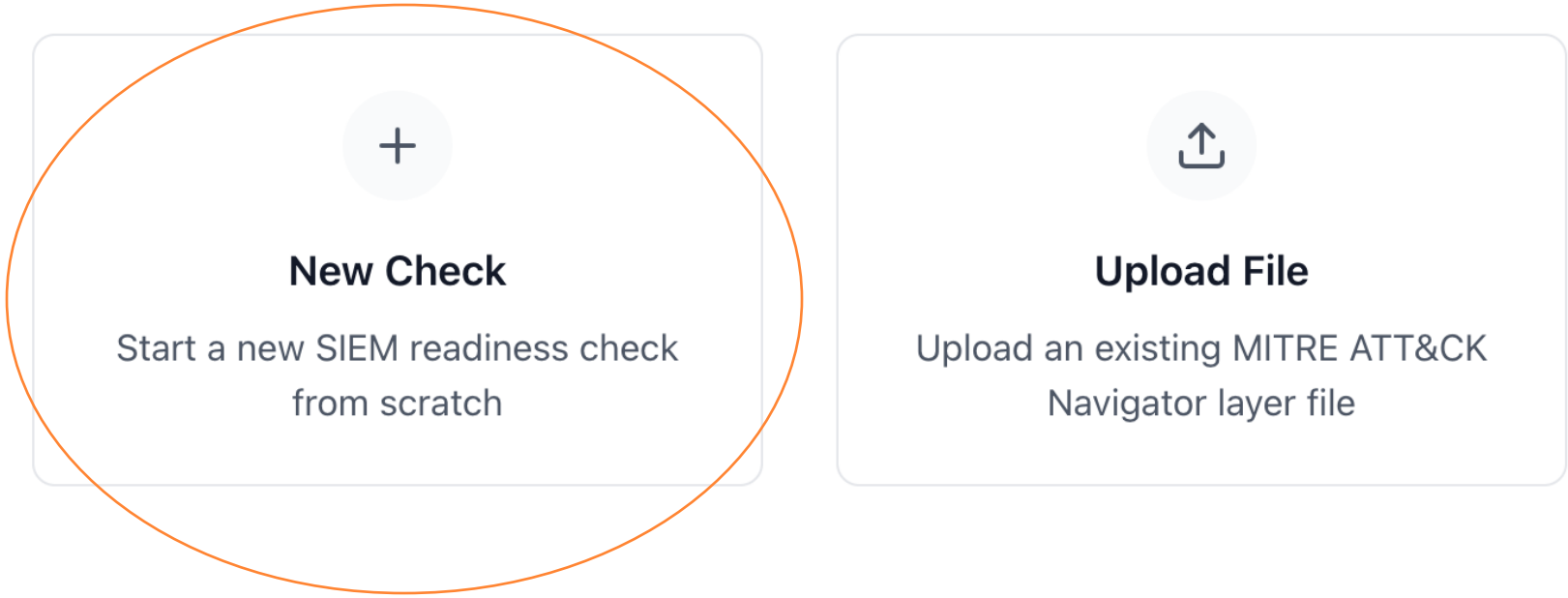
- Shows where to put your engineering efforts for the most effective targets

SECURIX SIEM Data Check

SECURIX

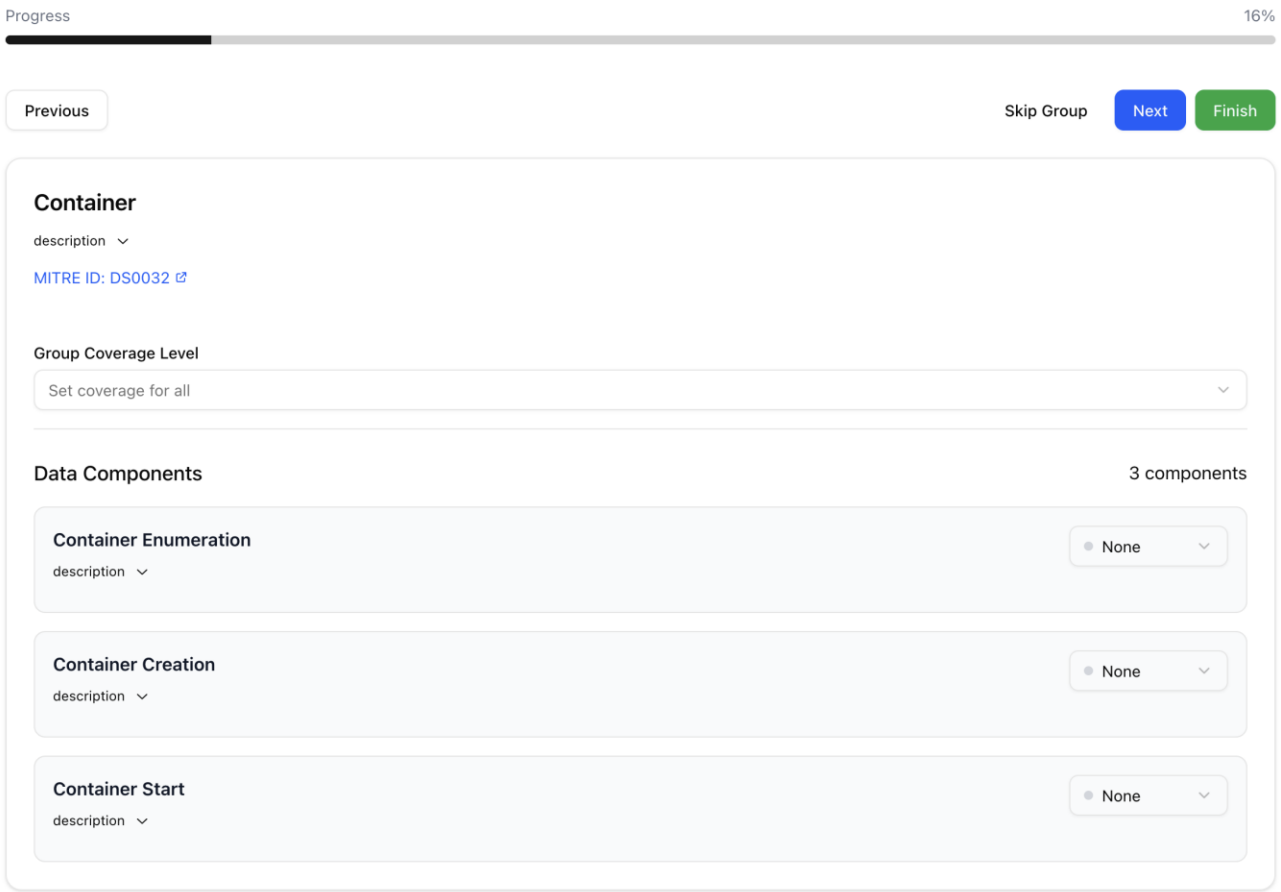


SECURIX SIEM Data Check



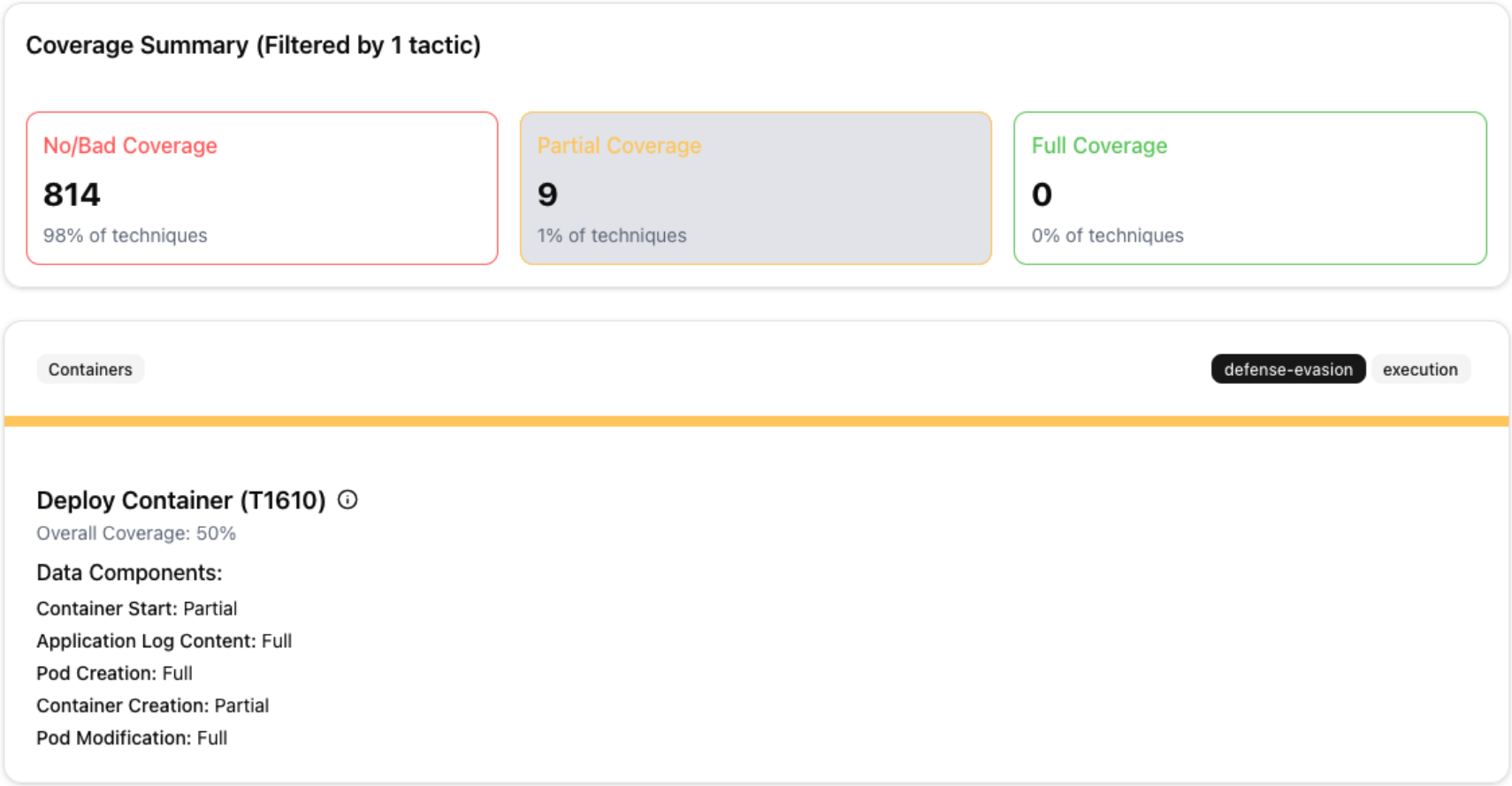
SECURIX SIEM Data Check

- Guides you through all Data Components
- For each that Component that applies, select your Coverage Level
  - Full
  - Partial
  - None



What you get: Coverage Report

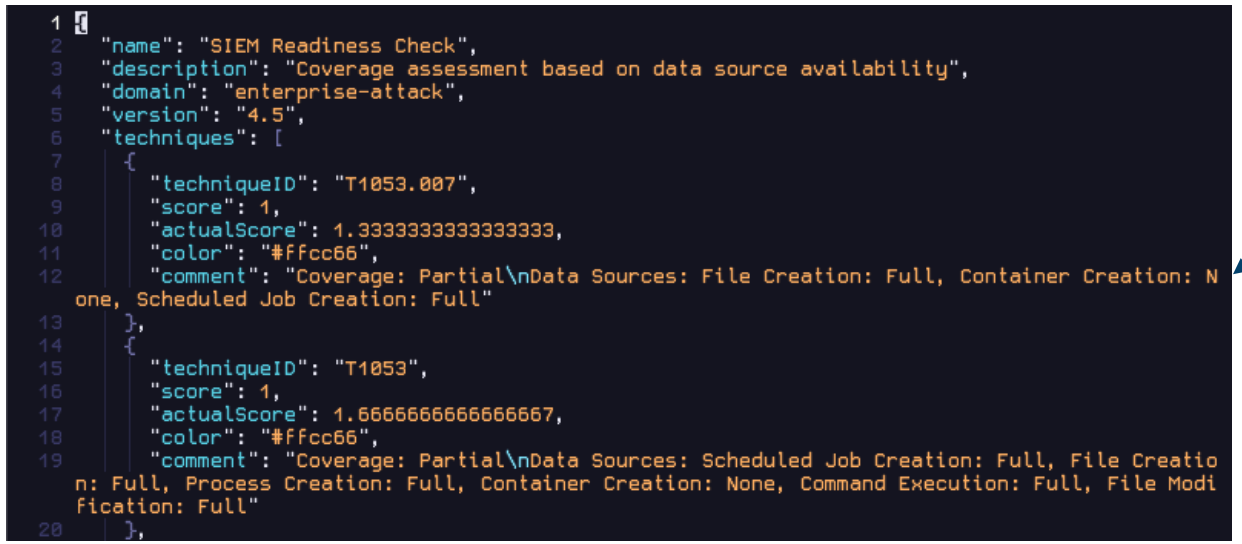
SECURIX



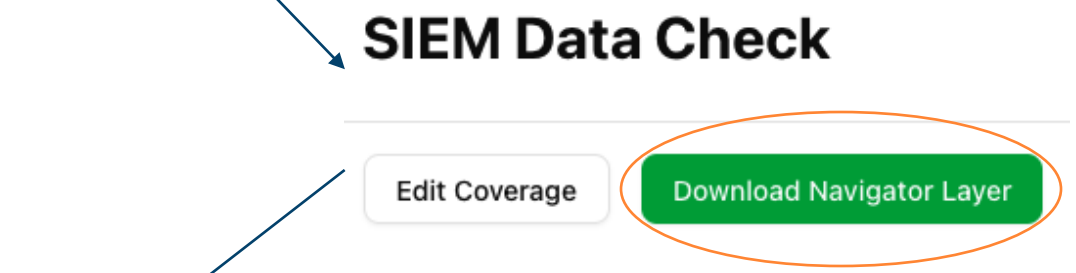
What you get: Navigator Layer

SECURIX

Get a JSON-file with a well-known-format that can be used in other tools.



```
{
  "name": "SIEM Readiness Check",
  "description": "Coverage assessment based on data source availability",
  "domain": "enterprise-attack",
  "version": "4.5",
  "techniques": [
    {
      "techniqueID": "T1053.007",
      "score": 1,
      "actualScore": 1.3333333333333333,
      "color": "#ffcc66",
      "comment": "Coverage: Partial\nData Sources: File Creation: Full, Container Creation: None, Scheduled Job Creation: Full"
    },
    {
      "techniqueID": "T1053",
      "score": 1,
      "actualScore": 1.6666666666666667,
      "color": "#ffcc66",
      "comment": "Coverage: Partial\nData Sources: Scheduled Job Creation: Full, File Creation: Full, Process Creation: Full, Container Creation: None, Command Execution: Full, File Modification: Full"
    },
```



What you get: Navigator Layer

SECURIX

- Upload your Navigator Layer to the Attack Navigator
  - https://mitre-attack.github.io/attack-navigator/
- Instantly view your coverage in the TTP overview

SECURIX SIEM Rule Builder

Expand your detection arsenal

Writing detections

SECURIX

- After you know your exposure, you want to reduce it
- Actually doing this can be a challenge
- MITRE can provide guidance, but can we do even better?

AN0770

Detection of rogue Domain Controller registration and Active Directory replication abuse by correlating: (1) creation/modification of nTDSDSA and server objects in the Configuration partition, (2) unexpected usage of Directory Replication Service SPNs (GC/ or E3514235-4B06-11D1-AB04-00C04FC2DCD2), (3) replication RPC calls (DrsAddEntry, DrsReplicaAdd, GetNCChanges) originating from non-DC hosts, and (4) Kerberos authentication by non-DC machines using DRS-related SPNs. These events in combination, especially from hosts outside the Domain Controllers OU, may indicate DCShadow or rogue DC activity.

Log Sources

Data Component	Name	Channel
Active Directory Object Creation (DC0087)	WinEventLog:Security	EventCode=4928
Active Directory Credential Request (DC0084)	WinEventLog:Security	EventCode=4929
Active Directory Object Access (DC0071)	WinEventLog:Security	EventCode=4662
Active Directory Object Modification (DC0066)	m365:dirsync	Replication cookie changes involving Configuration partition with new server/ nTDSDSA objects.
Network Traffic Content (DC0085)	NSM:Flow	DrsAddEntry, DrsReplicaAdd, GetNCChanges calls between non-DC and DCs.

Mutable Elements

Field	Description
TimeWindow	Window (seconds) between nTDSDSA object creation and subsequent replication traffic from same host (default 300s).
AllowedReplicationPartners	List of legitimate DCs authorized for replication to reduce false positives.
SuspiciousSPNs	SPNs indicating replication service usage (GC/, GUID E3514235-4B06-11D1-AB04-00C04FC2DCD2).
NonDCObjectCreationAlert	Trigger alerts only when AD object creation is by accounts not in Domain Admins or Enterprise Admins groups.

Example: DS Rogue Domain Controller Registration

https://attack.mitre.org/detectionstrategies/DET0276/

Introducing Sigma

SECURIX

- Open SIEM Detection Rule Format

Sigma

SIEM Detection Format

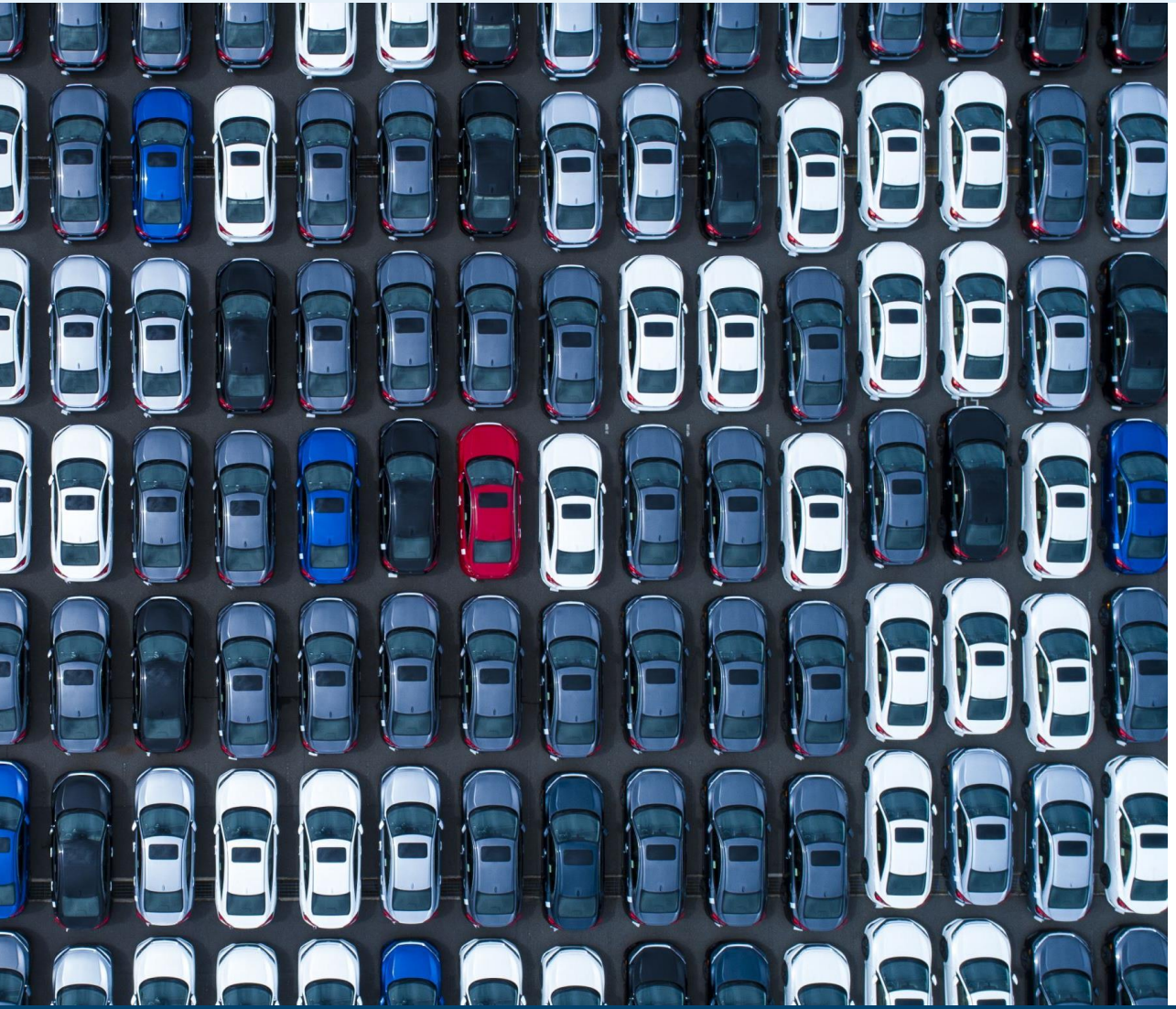
- Collection of 3000+ detection rules
- Rules can be auto-converted for different SIEM solutions

- Idea: Since everyone is doing the same work, why not reuse the results?

https://sigmahq.io/

"So I just pick all of them, right?"

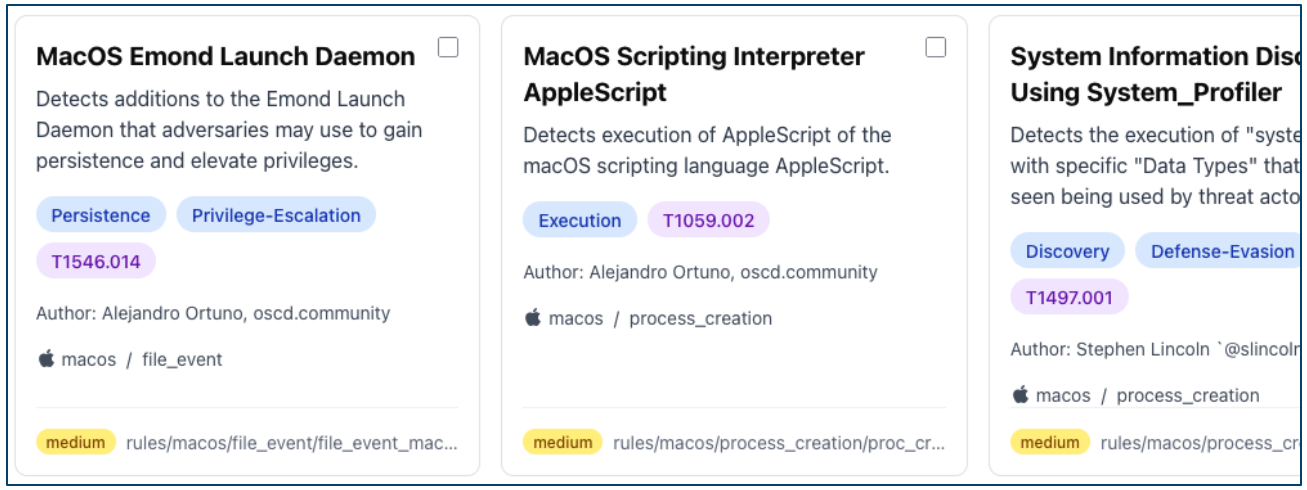
SECURIX



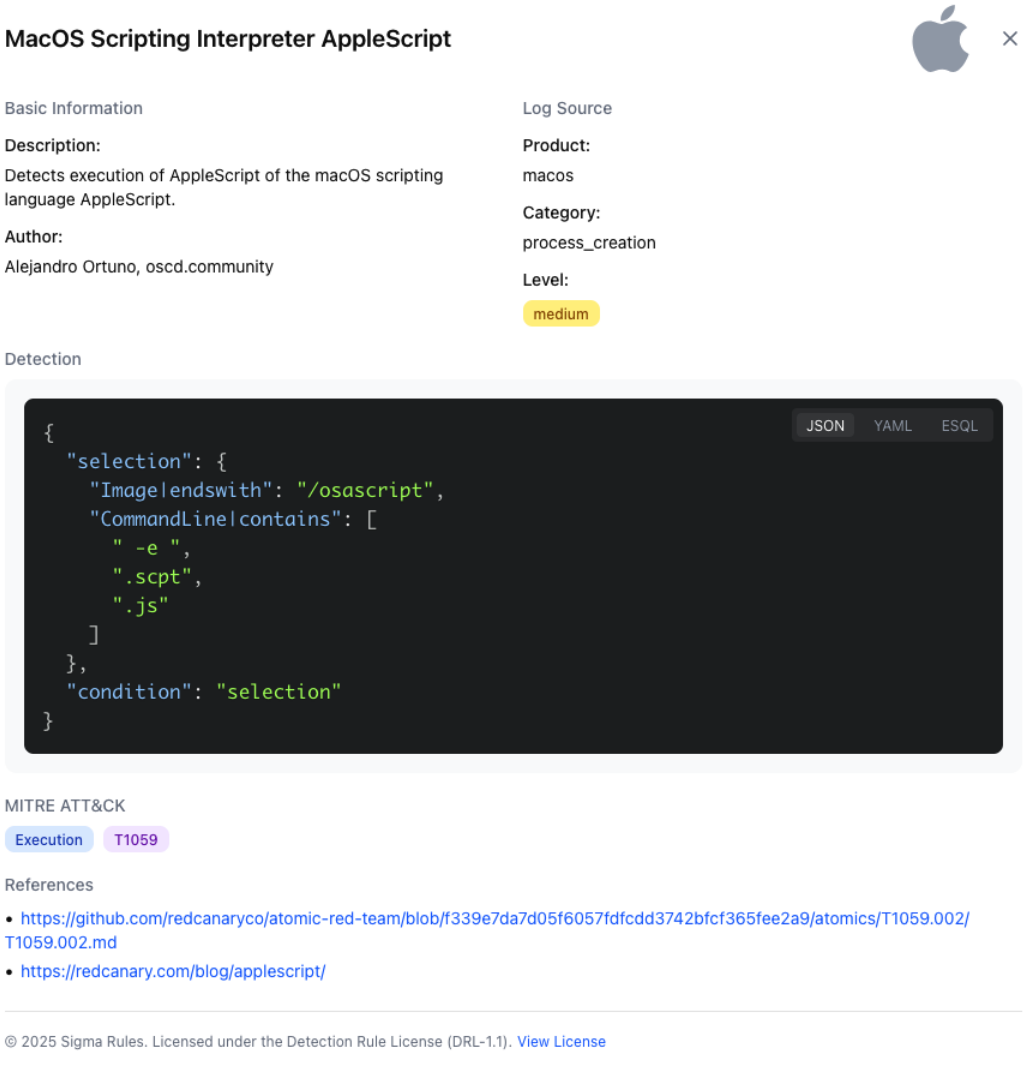
- SIEM rules need to be curated carefully
- Alerts need to be meaningful

- Alert Fatigue is not just a nuisance
  - It's a threat

SECURIX SIEM Rule Builder



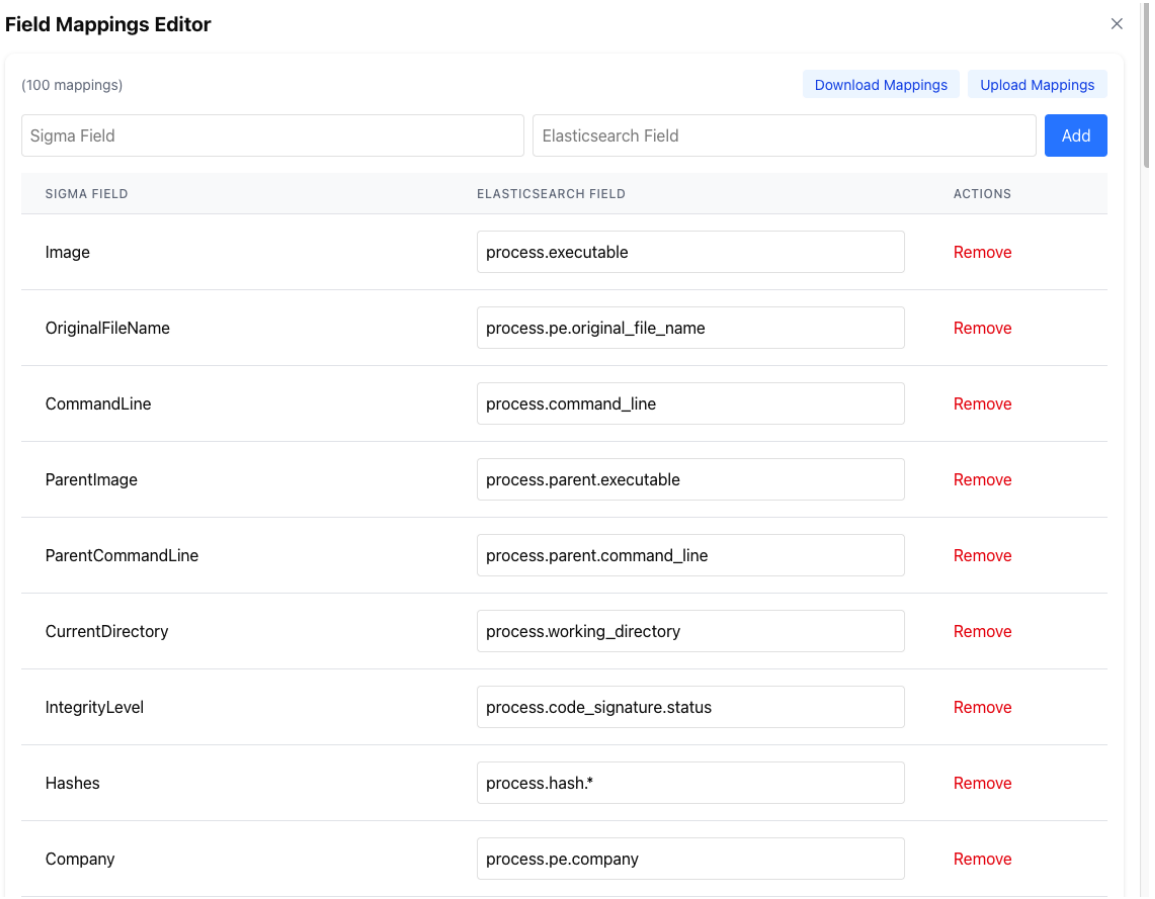
- Default: View all rules
  - Apply different filters
  - See rule definitions and MITRE Att&ck® associations



MITRE Att&ack® integration

SECURIX

- Download Rules
  - Sigma Format
  - Kibana Format
- Not ECS compliant? No problem.
  - Adjust your mappings directly
- Downloaded rules can be imported directly into Kibana



SIEM Readiness Check Workflow

SECURIX

- Use the Navigator Layer from the SECURIX SIEM Readiness Check
- Shows only rules, that apply to you

Go from asset definition directly to a curated set of SIEM Rules

Try it out

SECURIX

tools.securix.swiss