



SECURIX



SIEM Data Check

Know Your Coverage — Identify Your Gaps

David Vogels, SECURIX Deutschland GmbH

Introduction

SECURIX

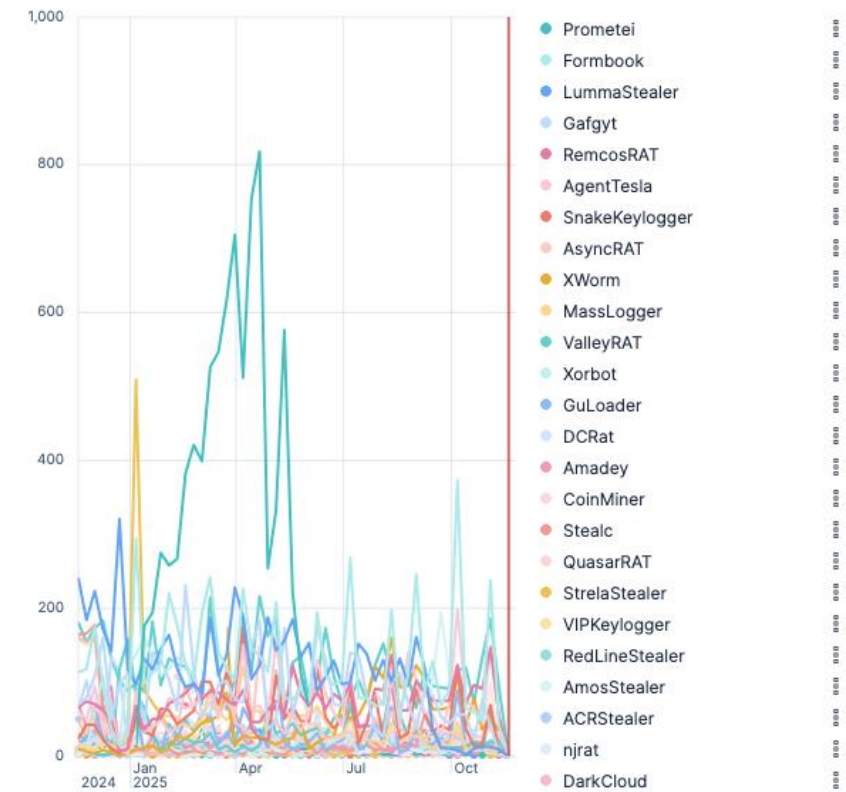


- **David Vogels**
- Senior IT Consultant (Observability)
- david.vogels@securix.swiss
- www.securix.swiss

Let's pick a malware

- Example: Prometei
- Steals credentials for self-propagation
- Host machine joins a botnet
- Purpose: To mine cryptocurrency (Monero)

Malware by #Entries (Malwarebazar)

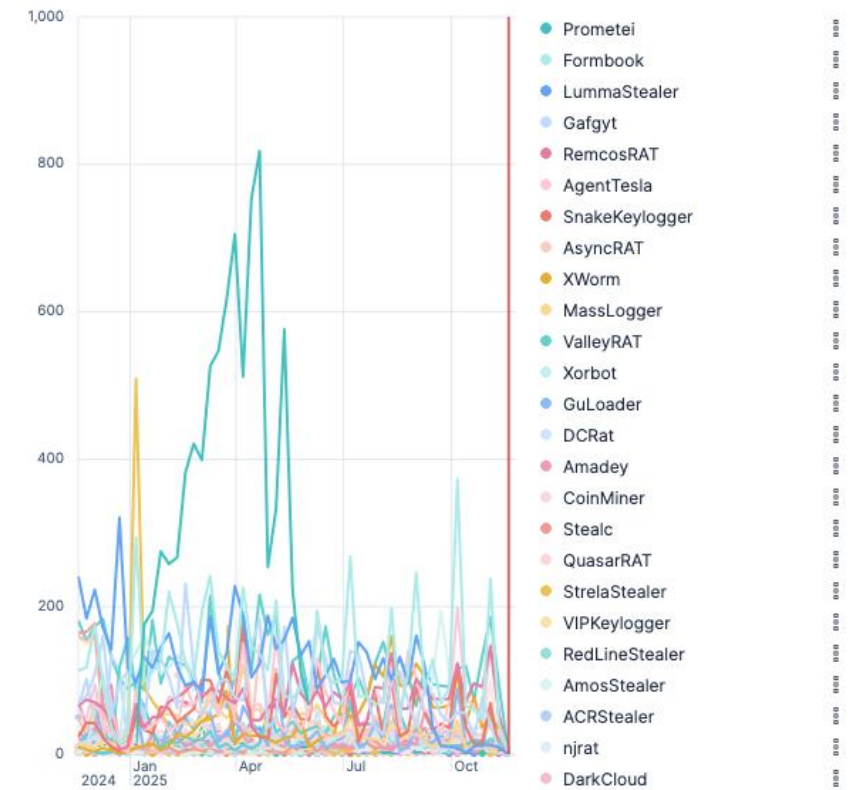


<https://blog.talosintelligence.com/prometei-botnet-and-its-quest-for-monero/>

Some facts about Prometei

- 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`

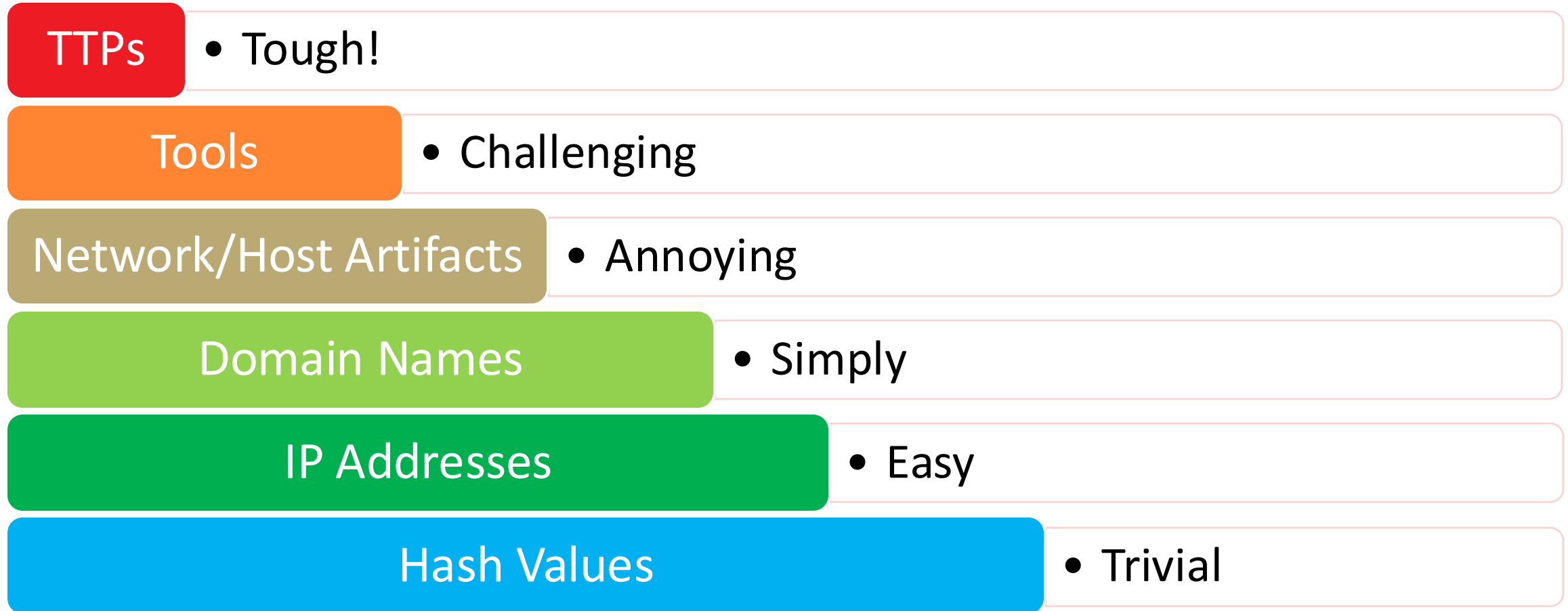
Malware by #Entries (Malwarebazar)



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

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

The Pyramid of Pain (David J. Bianco)



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

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

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?

- 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

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
11 techniques	8 techniques	11 techniques	17 techniques	23 techniques	14 techniques	47 techniques	17 techniques	34 techniques	9 techniques	17 techniques	18 techniques	9 techniques	15 techniques
Active Scanning (3) Gather Victim Host Information (4) Gather Victim Identity Information (3) Gather Victim Network Information (6) Gather Victim Org Information (4) Phishing for Information (4) Search Closed Sources (2) Search Open Technical Databases (5) Search Open Websites/ Domains (3) Search Threat Vendor Data Search Victim-Owned Websites	Acquire Access Acquire Infrastructure (8) Compromise Accounts (3) Compromise Infrastructure (8) Develop Capabilities (4) Establish Accounts (3) Obtain Capabilities (7) Stage Capabilities (6)	Content Injection Drive-by Compromise Exploit Public-Facing Application External Remote Services Hardware Additions Phishing (4) Replication Through Removable Media Supply Chain Compromise (3) Trusted Relationship Valid Accounts (4) Wi-Fi Networks	Cloud Administration Command Command and Scripting Interpreter (13) Container Administration Command Deploy Container ESXi Administration Command Exploitation for Client Execution Input Injection Inter-Process Communication (3) Native API Poisoned Pipeline Execution Scheduled Task/ Job (5) Serverless Execution Shared Modules Software Deployment Tools System Services (3) User Execution (5)	Account Manipulation (7) BITS Jobs Boot or Logon Autostart Execution (14) Boot or Logon Initialization Scripts (5) Cloud Application Integration Compromise Host Software Binary Create Account (3) Create or Modify System Process (5) Event Triggered Execution (18) Exclusive Control External Remote Services Hijack Execution Flow (12) Implant Internal Image Modify Authentication Process (9)	Abuse Elevation Control Mechanism (6) Access Token Manipulation (5) Account Manipulation (7) Boot or Logon Autostart Execution (14) Boot or Logon Initialization Scripts (5) Create or Modify System Process (5) Domain or Tenant Policy Modification (2) Escape to Host Event Triggered Execution (18) Exploitation for Privilege Escalation Hijack Execution Flow (12) Process Injection (12) Scheduled Task/ Job (5)	Abuse Elevation Control Mechanism (6) Access Token Manipulation (5) BITS Jobs Build Image on Host Debugger Evasion Delay Execution Deobfuscate/Decode Files or Information Deploy Container Direct Volume Access Domain or Tenant Policy Modification (2) Email Spoofing Execution Guardrails (2) Exploitation for Defense Evasion File and Directory Permissions Modification (2) Hide Artifacts (14) Hijack Execution Flow (12)	Adversary-in-the-Middle (4) Brute Force (4) Credentials from Password Stores (6) Exploitation for Credential Access Forced Authentication Forge Web Credentials (2) Input Capture (4) Modify Authentication Process (9) Multi-Factor Authentication Interception Multi-Factor Authentication Request Generation Network Sniffing OS Credential Dumping (8) Steal Application Access Token Steal or Forge Authentication	Account Discovery (4) Application Window Discovery Browser Information Discovery Cloud Infrastructure Discovery Cloud Service Dashboard Cloud Service Discovery Cloud Storage Object Discovery Container and Resource Discovery Debugger Evasion Device Driver Discovery Domain Trust Discovery File and Directory Discovery Group Policy Discovery Local Storage Discovery	Exploitation of Remote Services Internal Spearphishing Lateral Tool Transfer Remote Service Session Hijacking (2) Remote Services (8) Replication Through Removable Media Software Deployment Tools Taint Shared Content Use Alternate Authentication Material (4)	Adversary-in-the-Middle (4) Archive Collected Data (3) Audio Capture Automated Collection Browser Session Hijacking Clipboard Data Data from Cloud Storage Data from Configuration Repository (2) Data from Information Repositories (6) Data from Local System Data from Network Shared Drive Data from Removable Media Data Staged (2) Email Collection (3) Input Capture (4)	Application Layer Protocol (5) Communication Through Removable Media Content Injection Data Encoding (2) Data Obfuscation (3) Dynamic Resolution (3) Encrypted Channel (2) Fallback Channels Hide Infrastructure Ingress Tool Transfer Multi-Stage Channels Non-Application Layer Protocol Non-Standard Port Protocol Tunneling Proxy (4) Remote Access Tools (3) Traffic	Automated Exfiltration (1) Data Transfer Size Limits Exfiltration Over Alternative Protocol (3) Exfiltration Over C2 Channel Exfiltration Over Other Network Medium (1) Exfiltration Over Physical Medium (1) Exfiltration Over Web Service (4) Scheduled Transfer Transfer Data to Cloud Account	Account Access Removal Data Destruction (1) Data Encrypted for Impact Data Manipulation (3) Defacement (2) Disk Wipe (2) Email Bombing Endpoint Denial of Service (4) Financial Theft Firmware Corruption Inhibit System Recovery Network Denial of Service (2) Resource Hijacking (4) Service Stop System Shutdown/ Reboot

Sub-Technique

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

- Forwards-Approach
 - What attacks are there?
 - How are they executed?
 - How can they be detected?
 - Which Assets do I need to monitor?
- Backwards-Approach
 - Which Assets do I have?
 - What attack vectors do I open myself up to?

Detection Strategies

How can the used Technique be detected?

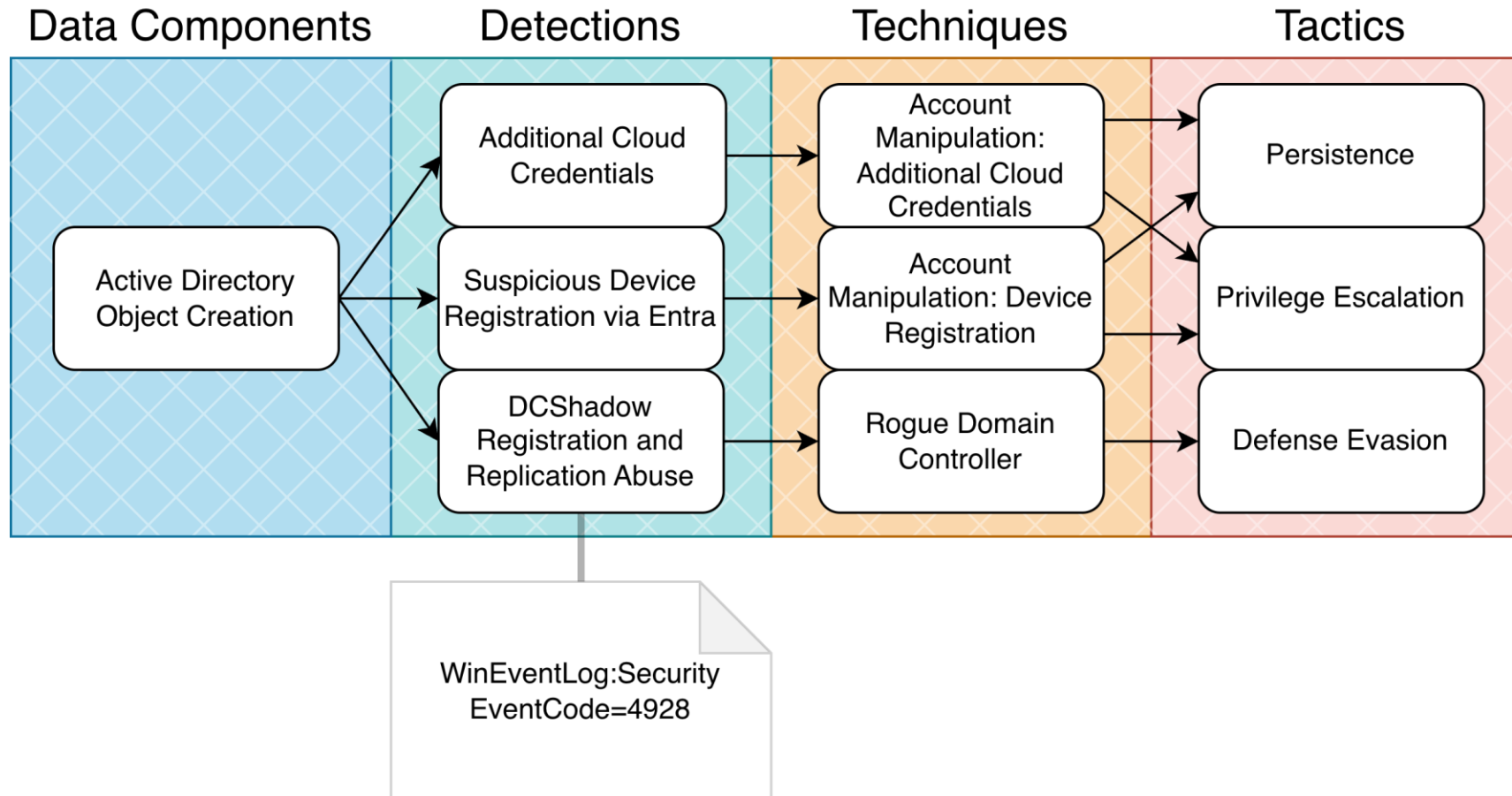
Data Components

Are linked to one or more Detection Strategies

Mitigations

Containing the impact and/or probability of an attack

The Mitre Att&ck® Framework



- 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

Welcome, david.vogels to SX-Tools



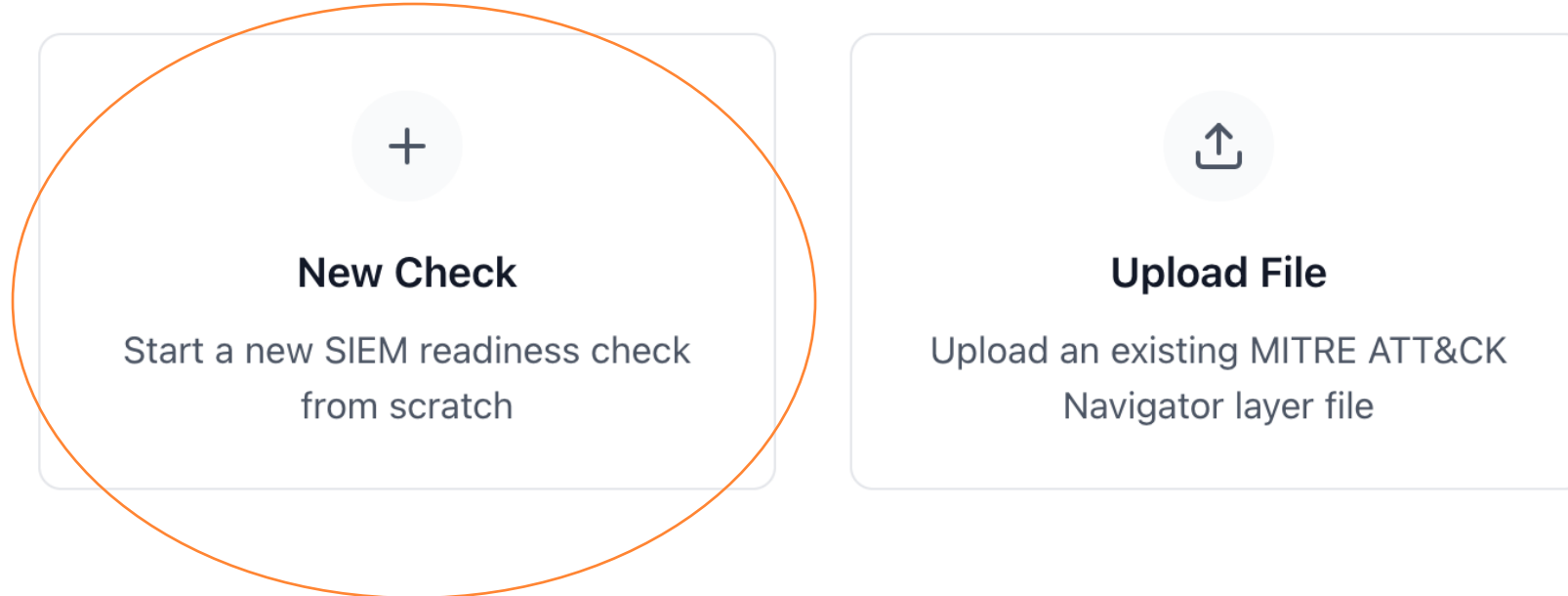
SIEM Data Check

Obtain the Coverage of Your SIEM
Data in Relation to MITRE ATT&CK



SIEM Rule Builder

Create SIEM Rules Relevant to Your
Data



- Guides you through all Data Components
- For each that Component that applies, select your **Coverage Level**

- Full
- Partial
- None

Progress 16%

[Previous](#) [Skip Group](#) [Next](#) [Finish](#)

Container
description ▾
[MITRE ID: DS0032](#)

Group Coverage Level
Set coverage for all ▾

Data Components 3 components

Container Enumeration
description ▾ None ▾

Container Creation
description ▾ None ▾

Container Start
description ▾ None ▾

What you get: Coverage Report

Coverage Summary (Filtered by 1 tactic)

No/Bad Coverage

814

98% of techniques

Partial Coverage

9

1% of techniques

Full Coverage

0

0% of techniques

Containers

defense-evasion

execution

Deploy Container (T1610) ⓘ

Overall Coverage: 50%

Data Components:

Container Start: Partial

Application Log Content: Full

Pod Creation: Full

Container Creation: Partial

Pod Modification: Full

What you get: Navigator Layer

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

SIEM Data Check

Edit Coverage

Download Navigator Layer

```
1 [{"name": "SIEM Readiness Check",
2  "description": "Coverage assessment based on data source availability",
3  "domain": "enterprise-attack",
4  "version": "4.5",
5  "techniques": [
6    {
7      "techniqueID": "T1053.007",
8      "score": 1,
9      "actualScore": 1.3333333333333333,
10     "color": "#ffcc66",
11     "comment": "Coverage: Partial\nData Sources: File Creation: Full, Container Creation: N
12 one, Scheduled Job Creation: Full"
13   },
14   {
15     "techniqueID": "T1053",
16     "score": 1,
17     "actualScore": 1.6666666666666667,
18     "color": "#ffcc66",
19     "comment": "Coverage: Partial\nData Sources: Scheduled Job Creation: Full, File Creatio
20 n: Full, Process Creation: Full, Container Creation: None, Command Execution: Full, File Modi
    }
  ]
}]
```

What you get: Navigator Layer

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

Execution 17 techniques	Persistence 23 techniques	Privilege Escalation 14 techniques	Defense Evasion 47 techniques	Credential Access 17 techniques	Discovery 34 techniques
Cloud Administration Command	Account Manipulation (0/7)	Abuse Elevation Control Mechanism (0/6)	Abuse Elevation Control Mechanism (0/6)	Adversary-in-the-Middle (0/4)	Account Discovery (0/4)
Command and Scripting Interpreter (0/13)	BITS Jobs (0/13)	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery (0/4)
Container Administration Command	Boot or Logon Autostart Execution (0/14)	Account Manipulation (0/7)	BITS Jobs (0/5)	Credentials from Password Stores (0/6)	Browser Information Discovery (0/6)
Deploy Container	Boot or Logon Initialization Scripts (0/5)	Account Manipulation (0/7)	Build Image on Host (0/7)	Exploitation for Credential Access (0/6)	Cloud Infrastructure Discovery (0/6)
ESXi Administration Command	Cloud Application Integration (0/14)	Boot or Logon Autostart Execution (0/14)	Debugger Evasion (0/14)	Forced Authentication (0/2)	Cloud Service Dashboard (0/2)
Exploitation for Client Execution	Compromise Host Software Binary (0/3)	Boot or Logon Initialization Scripts (0/5)	Delay Execution (0/2)	Forge Web Credentials (0/2)	Cloud Service Discovery (0/2)
Input Injection	Create Account (0/3)	Boot or Logon Initialization Scripts (0/5)	Deobfuscate/Decode Files or Information (0/4)	Input Capture (0/4)	Cloud Storage Object Discovery (0/4)
Inter-Process Communication (0/3)	Create or Modify System Process (1/5)	Create or Modify System Process (1/5)	Deploy Container (0/9)	Modify Authentication Process (0/9)	Container and Resource Discovery (0/9)
Native API	Event Triggered Execution (0/18)	Domain or Tenant Policy Modification (0/2)	Direct Volume Access (0/2)	Multi-Factor Authentication Interception (0/2)	Debugger Evasion (0/2)
Poisoned Pipeline Execution	Exclusive Control (0/18)	Escape to Host (0/18)	Domain or Tenant Policy Modification (0/2)	Multi-Factor Authentication Request Generation (0/2)	Device Driver Discovery (0/2)
Scheduled Task/Job (1/5)	External Remote Services (0/12)	Event Triggered Execution (0/18)	Email Spoofing (0/2)	Network Sniffing (0/2)	Domain Trust Discovery (0/2)
Serverless Execution	Hijack Execution Flow (0/12)	Exploitation for Privilege Escalation (0/12)	Execution Guardrails (0/2)	OS Credential Dumping (0/8)	File and Directory Discovery (0/8)
Shared Modules	Implant Internal Image (0/9)	Hijack Execution Flow (0/12)	Exploitation for Defense Evasion (0/2)	Steal Application Access Token (0/2)	Group Policy Discovery (0/2)
Software Deployment Tools	Modify Authentication Process (0/9)	Process Injection (0/12)	File and Directory Permissions Modification (0/2)	Steal or Forge Authentication Certificates (0/5)	Local Storage Discovery (0/5)
System Services (0/3)	Office Application Startup (0/12)	Scheduled Task/Job (1/5)	Hide Artifacts (0/14)	Steal or Forge Kerberos Tickets (0/5)	Log Enumeration (0/5)
User Execution (1/5)			Hijack Execution Flow (0/12)	Network Service Discovery (0/12)	Network Share Discovery (0/12)
Windows Management Instrumentation			Impair (0/12)		



SECURIX SIEM Rule Builder

Expand your detection arsenal

Writing detections

- 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:dirdsync	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.

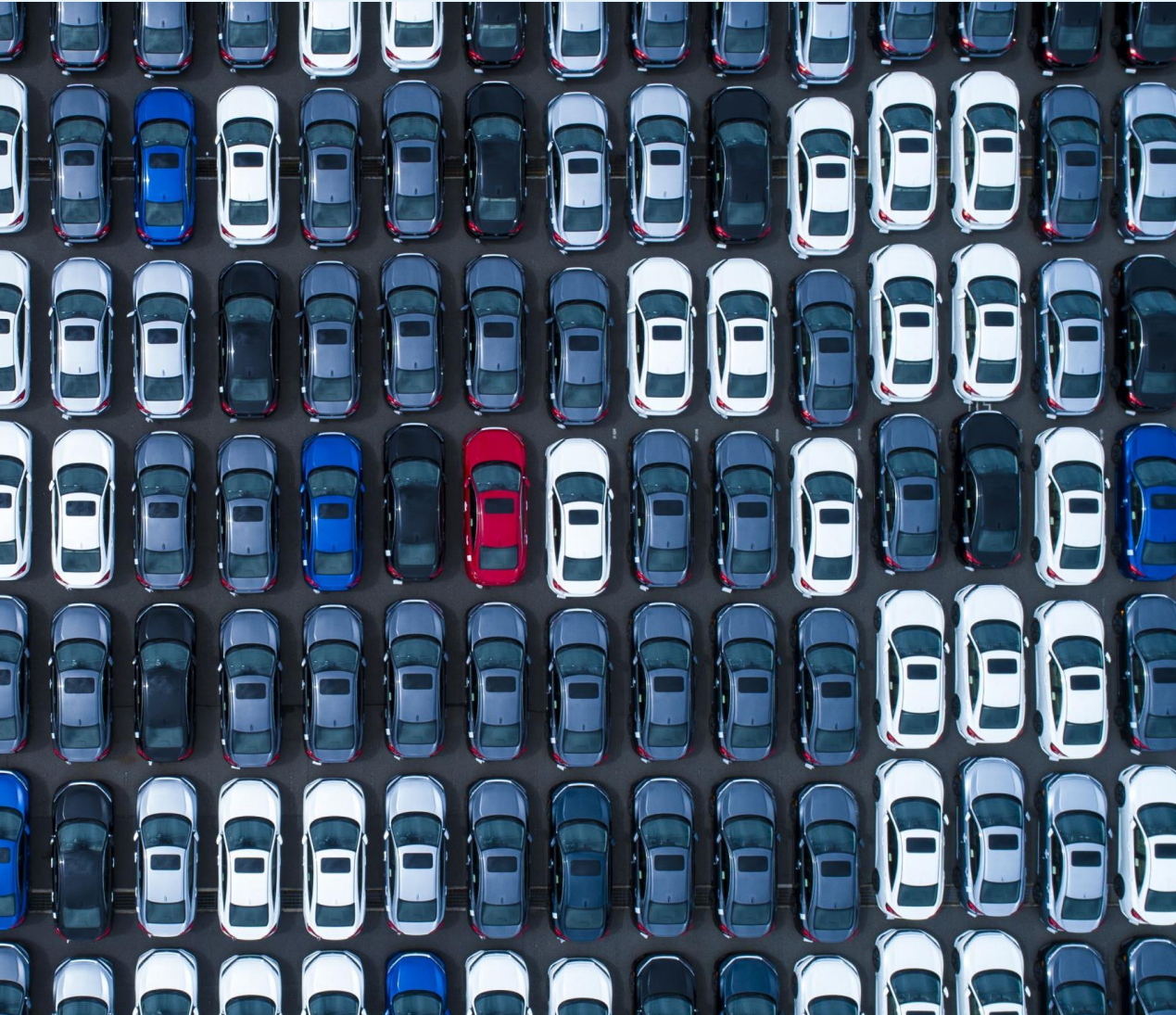
Example: DS Rogue Domain Controller Registration



Sigma
SIEM Detection Format

- Open SIEM Detection Rule 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?

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



- 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



MacOS Emond Launch Daemon

Detects additions to the Emond Launch Daemon that adversaries may use to gain persistence and elevate privileges.

Persistence Privilege-Escalation

T1546.014

Author: Alejandro Ortuno, oscd.community

🍏 macos / file_event

medium rules/macos/file_event/file_event_mac...

MacOS Scripting Interpreter AppleScript

Detects execution of AppleScript of the macOS scripting language AppleScript.

Execution T1059.002

Author: Alejandro Ortuno, oscd.community

🍏 macos / process_creation

medium rules/macos/process_creation/proc_cr...

System Information Disc Using System_Profiler

Detects the execution of "system" with specific "Data Types" that are seen being used by threat actors.

Discovery Defense-Evasion

T1497.001

Author: Stephen Lincoln `@slincoln

🍏 macos / process_creation

medium rules/macos/process_cr...

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

MacOS Scripting Interpreter AppleScript



Basic Information

Description:

Detects execution of AppleScript of the macOS scripting language AppleScript.

Author:

Alejandro Ortuno, oscd.community

Log Source

Product:

macos

Category:

process_creation

Level:

medium

Detection

```
{
  "selection": {
    "ImageEndsWith": "/osascript",
    "CommandLineContains": [
      "-e ",
      ".scpt",
      ".js"
    ]
  },
  "condition": "selection"
}
```

MITRE ATT&CK

Execution T1059

References

- <https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057dfcdd3742bfcf365fee2a9/atomics/T1059.002.md>
- <https://redcanary.com/blog/applescript/>

MITRE Att&ack® integration



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

Field Mappings Editor ×

(100 mappings) Download Mappings Upload Mappings

Add

SIGMA FIELD	ELASTICSEARCH FIELD	ACTIONS
Image	<input type="text" value="process.executable"/>	Remove
OriginalFileName	<input type="text" value="process.pe.original_file_name"/>	Remove
CommandLine	<input type="text" value="process.command_line"/>	Remove
ParentImage	<input type="text" value="process.parent.executable"/>	Remove
ParentCommandLine	<input type="text" value="process.parent.command_line"/>	Remove
CurrentDirectory	<input type="text" value="process.working_directory"/>	Remove
IntegrityLevel	<input type="text" value="process.code_signature.status"/>	Remove
Hashes	<input type="text" value="process.hash.*"/>	Remove
Company	<input type="text" value="process.pe.company"/>	Remove

- 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

tools.securix.swiss

