Detection Engineering

Mikko Koivunen, <mikko@koivusec.fi>
TurkuSec 14.06.2024

Hello, who’s this?

What do I do?

- I work as a self-employed security consultant.
- Clients include inhouse security teams and SOC service providers.
- Websites: koivusec.fi & secopslab.substack.com.

How I got started in security?

- BBS scene in the ‘90s introduced me to things like Phrack, 2600…
- After school went to work in IT: helpdesk -> infrastructure -> security.

Definitions

- A **detection** is a piece of logic inside a monitoring tool (often SIEM or EDR) to identify a specific activity based on logs, telemetry, behaviour or events.
- **Detection engineering** is the systematic approach to creating, deploying and refining these detections, to identify and respond to threats not already covered by existing security tooling.

Who’s it for?

- Detection engineering is a **human-centric** activity.
- Requires a team with deep understanding of data, threat landscape, users, business services, IT architecture and security controls.
- Maturity jump from just consuming tools and vendor content.
- At the heart of a **modern SOC:**
  “hands on keyboards” instead of “eyes on glass”.

Benefits

- Reduced mean time to detect (MTTD).
- Increased awareness of both external and internal threats.
- Forces our focus to threat-informed defense.
- Coverage and confidence.
- Increased trust both in the team and the toolkit.
- Measurement and reporting.

Requirements

- Inputs: threat modelling, threat intelligence, security testing.
- Evidence: know what malicious activities look like.
- Data: SIEM, EDR agents, OS and app logs and telemetry.

Indicators for high quality detections

1. Low false positives
    - Are the false alerts low / rare enough so the team is not overwhelmed?
2. True positives validated
    - Is the detection properly tested to ensure it works in real cases?
3. Robustness
    - Does the detection fire on all possible variations of an activity?
4. Documentation
    - Are relevant external resources referenced: threat intelligence, blogs, tweets?
    - Are potential false positives identified?
    - Do we have investigation notes & a response playbook?
    - Is the detection mapped to MITRE ATT&CK techniques?

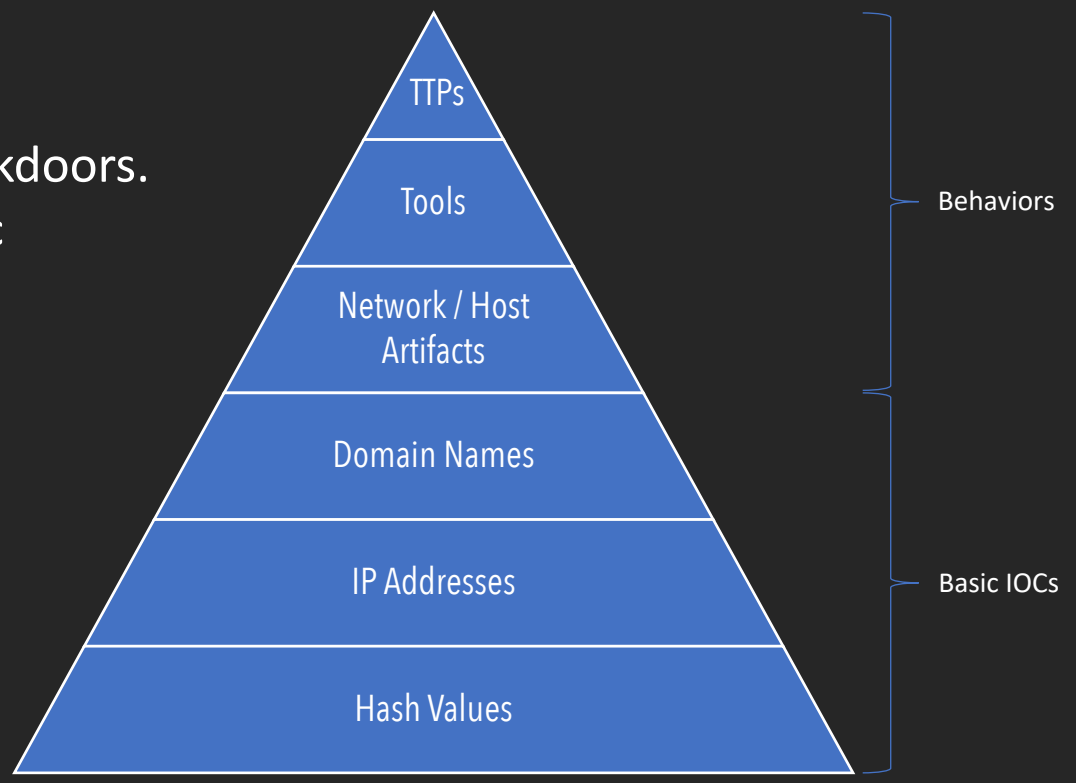
What to focus on?

Common detection focuses:

- Threats like malware, hack tools, attacker activity, backdoors.
- Anomalies related to time, location, uncommon traffic patterns, uncommon file, process, registry events.
- Internal policy violations.

Indicators of compromise used in detection:

- The “Pyramid of Pain”.
- Top = most value, difficult to detect.
- Bottom = least value, trivial to detect.



Detection as Code

- To do Detection Engineering at scale, modern software engineering practices are needed.
- Detections are managed as code in repositories and deployed with automated pipelines.
- Examples how certain products support Detection as Code:

Microsoft Sentinel	Google Chronicle	Panther
Native API. Built-in deployment feature from Azure DevOps and GitHub.	Native API. No built-in deployment feature.	Native API. Built-in deployment and testing feature using CircleCI.
Detections written as ARM templates and KQL queries.	Detections written as YARA-L rules.	Detections written as Python code.

Using detections from external sources

“Built-in”

Microsoft Sentinel | Content hub

Selected workspace: 'law-secopslab-sec-001'

Refresh | Install/Update | Delete | SIEM Migration | Guides & Feedback

356	275	24	17
Solutions	Standalone contents	Installed	Updates

Content title
A client made a web request to a potentially harmful file (ASIM Web Session schema)
A host is potentially running a crypto miner (ASIM Web Session schema)
A host is potentially running a hacking tool (ASIM Web Session schema)
A host is potentially running PowerShell to send HTTP(S) requests (ASIM Web Session schema)
Account added and removed from privileged groups
Account created from non-approved sources
AD account with Don't Expire Password

“Curated”

INTELLIGENCE 11,339 | THREATS 2,852 | DETECTIONS 2,260 | COLLECTIONS 7,755

SNAPATTACK COMMUNITY EDITION

Showing 1-1,000 of 2,260 matching detections

Name	Validation	Severity	Confidence	Logsource
Hook Created by Git.exe	Untested	MEDIUM	HIGHEST	FILE_EVENT WIND
Network Connection Initiated From Users\Public Folder	Unvalidated	LOWEST	MEDIUM	NETWORK_CONNI
RMM Tool Installation		HIGH	HIGH	FILE_EVENT WIND
RMM Tool Service Installation		HIGH	HIGH	WINDOWS SECURI
Bash Reverse Shell		MEDIUM	HIGHEST	PROCESS_CREATI
Suspicious Mirth Connect Child Process		MEDIUM	HIGH	PROCESS_CREATI
Active Directory Computers Enumeration With Get-AdComputer	Validated	MEDIUM	HIGHEST	PS_SCRIPT WINDO
Dynamic .NET Compilation Via Csc.EXE - Hunting	Validated	HIGH	UNKNOWN	PROCESS_CREATI
WinAPI Library Calls Via PowerShell Scripts	Detection Gap	LOW	UNKNOWN	PS_SCRIPT WINDO
Abusable DLL Potential Sideloading From Suspicious Location	Untested	MEDIUM	UNKNOWN	IMAGE_LOAD WIN

Sigma

Sigma
Detection Format

Open Source | Introducing new SigmaHQ Rule Packs →

SIEM Detection Format

The shareable detection format for security professionals.

Get the most out of the Sigma ecosystem in your SIEM, and start using thousands of great security detections from the community and beyond.

Get Started | Download Sigma Rule Packages

```
title: AWS Root Credentials
description: Detects AWS root account usage
logsource:
    product: aws
    service: cloudtrail
detection:
    selection:
        userIdentity.type: Root
    filter:
        eventType: AwsServiceEvent
    condition: selection and not filter
falsepositives:
    - AWS Tasks That Require Root User Credentials
level: medium
```

SigmaHQ / sigma Public

Spon

Code | Issues 15 | Pull requests 7 | Discussions | Actions | Wiki | Security | Insights

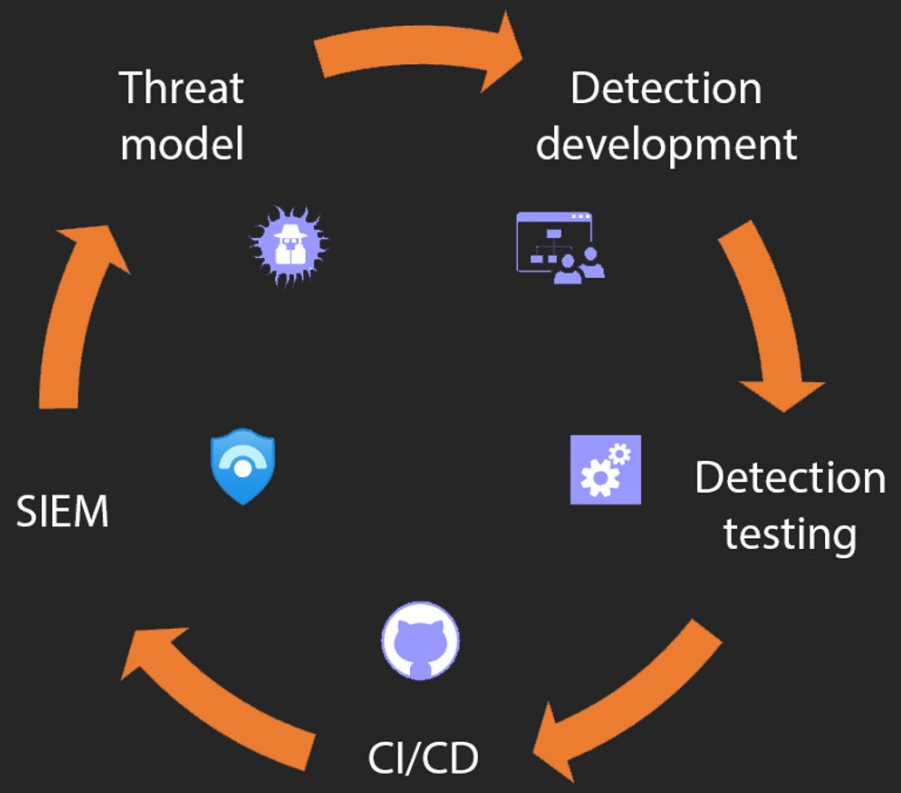
Release r2024-05-13 Latest

New Rules

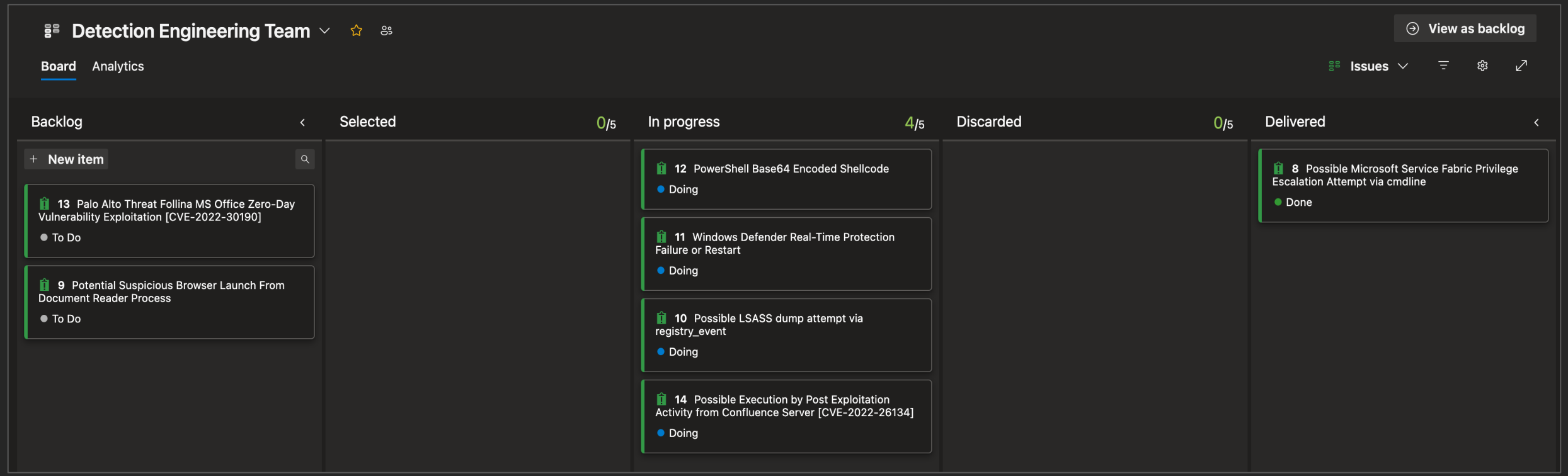
- new: Access To Windows Outlook Mail Files By Uncommon Application
- new: All Backups Deleted Via Wbadmin.EXE
- new: File Recovery From Backup Via Wbadmin.EXE
- new: Launch Agent/Daemon Execution Via Launchctl
- new: New Firewall Rule Added In Windows Firewall Exception List Via WmiPrvSE.EXE
- new: New RDP Connection Initiated From Domain Controller
- new: New Windows Firewall Rule Added Via New-NetFirewallRule Cmdlet
- new: New Windows Firewall Rule Added Via New-NetFirewallRule Cmdlet - ScriptBlock
- new: Potential Packet Capture Activity Via Start-NetEventSession - ScriptBlock
- new: Potentially Suspicious Child Process Of KeyScrambler.exe
- new: Potentially Suspicious Malware Callback Communication - Linux
- new: Sensitive File Dump Via Wbadmin.EXE
- new: Sensitive File Recovery From Backup Via Wbadmin.EXE
- new: Suspicious External WebDAV Execution
- new: UAC Notification Disabled
- new: UAC Secure Desktop Prompt Disabled

Process & Workflow

- Build a repeatable process for identifying, developing, testing and deploying detections.
- Technical side is fun, but this is how you succeed.



Development board example



More detections != better SOC

(alert fatique)

Better detections == better SOC

(high fidelity, actionable alerts)