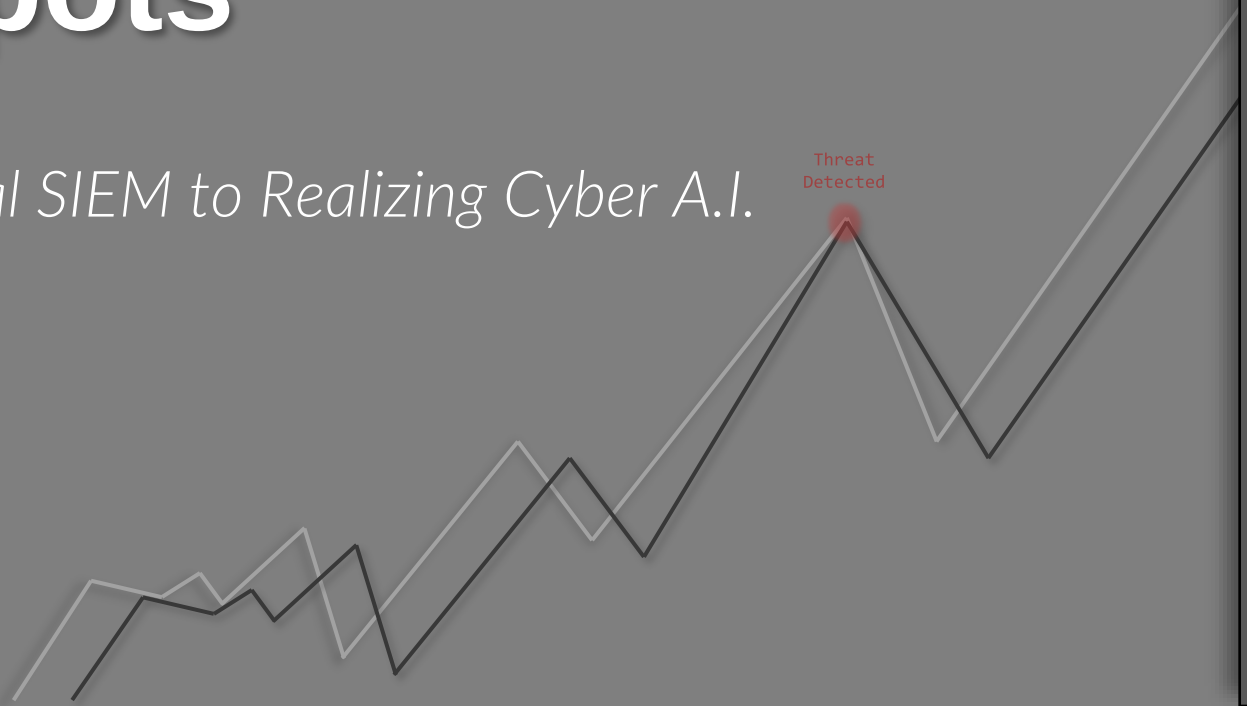
Designing The SIEM Monitoring Environment To Address Visibility and Blind Spots

From Foundational SIEM to Realizing Cyber A.I.

Jurgen Visser




```
srcip="172.16.160.210" user="root"
caller="root" reason="Too many failures
from client IP, still blocked for 537
seconds"
<54>Jul 5 17:17:43 SymantecServer SEP-
PROD: Virus found,IP Address:
10.235.237.89,Computer name:
A41021,Source: Real Time Scan,Risk name:
Backdoor.IRCBot!win32
<177>Jul  5 14:18:53 SourceFire
snort[10340]: [1:2007933:3] ET EXPLOIT
Microsoft Office Memory Corruption
Vulnerability (CVE-2017-11882)
[Classification: Microsoft Application
Attack] [Priority: 2]: {TCP}
72.246.97.42:80 -> 10.12.1.140:1629
<54>Jul 5 14:05:55 SymantecServer SEP-
PROD: Virus found,IP Address:
10.11.8.78,Computer name:
A372d759,Source: Scheduled Scan,Risk
name: W97M.Melissa.A
<30>Jul 5 19:22-19:16:27 aua[4983]:
id="3005" severity="warn" sys="System"
sub="auth" name="Authentication failed"
srcip="172.16.160.210" user="sysadmin"
caller="root" reason="Too many failures
from client IP, still blocked for 517
seconds"
```

Jurgen Visser

Security Operations Center (SOC) Architect

Professional Skills

Cyber Security Specialist passionate about analyzing cyber security risks and strategizing, architecting, building, maturing them into enterprise level cyber security initiatives.

- **11 years+** of working experience in **Cyber Security** and Information Technology (IT).
- University Bachelor degree in **Information Security Management**.
- 3x General Cyber Security Certified: **CISSP, CISSP-ISSAP, CEH**
- 3x Standards Certified: **ITIL, ISFS ISO27001, Agile SCRUM**
- 5x Cloud Certified: **1x CCSP, 2x Amazon AWS, 1x Microsoft Azure, 1x Google GCP**
- 3x Threat Intelligence Certified: **GCTI, CTIA, CRTIA**
- 10x SIEM Certified: **4x ArcSight, 4x IBM QRadar, 1x Splunk and 1x ELK**
- Native in **Dutch** and **English**, intermediate at **Mandarin Chinese** (HSK3).
- Strategic, Critical, Abstract, Design, Analytical, Holistic and Systems Thinker.
- Information Security Blogger at **www.correlatedsecurity.com**

Context

- A large sized business has hired a **new CISO**!
- The CISO has **a big budget** and wants to **rapidly expand security**!
- The CISO hires **YOU** to handle anything related to SOC
- Questions or needs from CISO come sudden and out of the blue and **you need to come up with solutions**


I need
use cases!
Threat
Detected
Let’s do a constructive
Use Case Strategy!

Data Strategy: Asset, Software and Attacker-Centric

External Threats

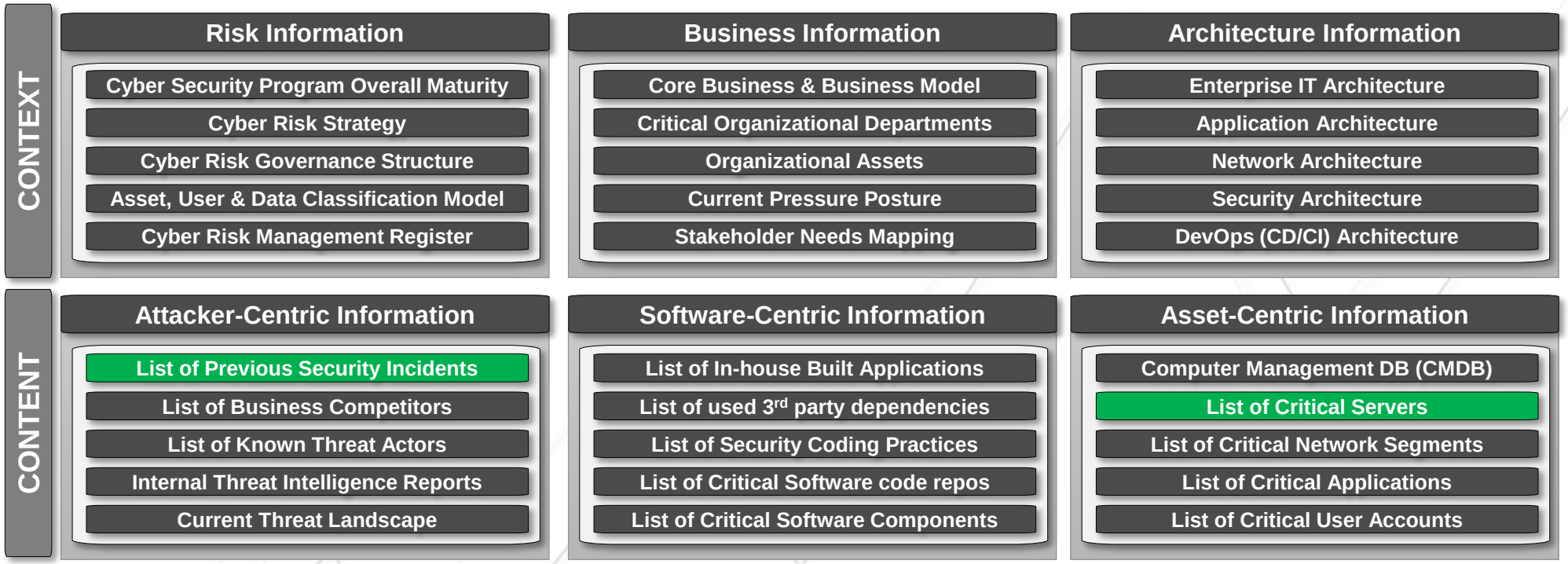
- Attacker-centric threat modelling

Internal Threats

- Asset-centric Threat modelling
- Software-centric threat modelling

Methodology for Building an Organizational Context and Content-Informed Cyber Threat modelling Strategy that aligns with an Use Case Management Program

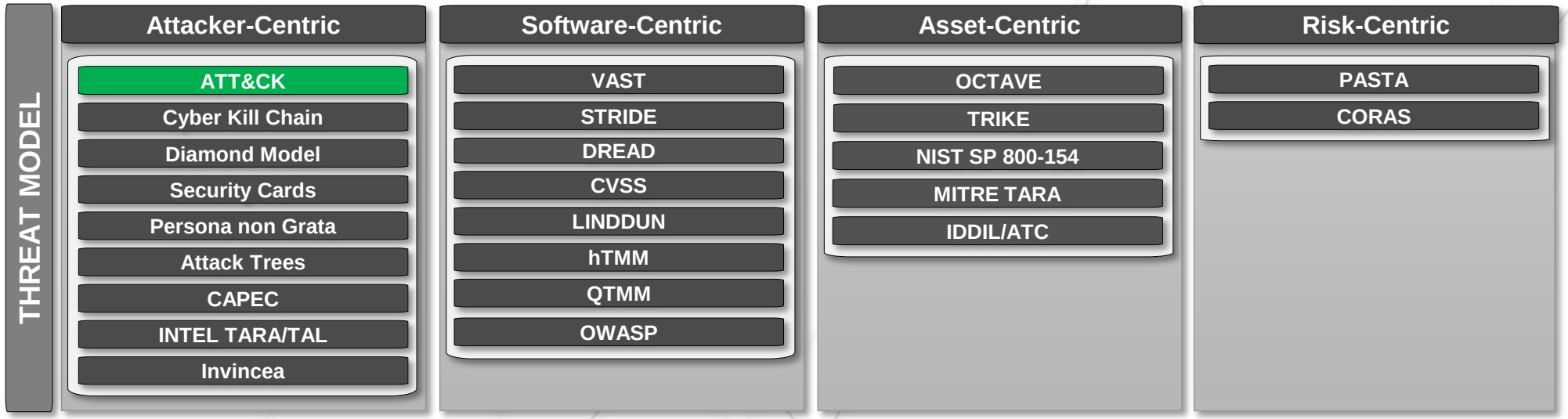
1. Collect, Identify and Prioritize Risks, Attackers, Software and Assets



2. Decide and Apply a "Threat Modeling Strategy" based on Attacker, Software, Asset or Risk-Centric Threat Models

Methodology for Building an Organizational Context and Content-Informed Cyber Threat modelling Strategy that aligns with an Use Case Management Program

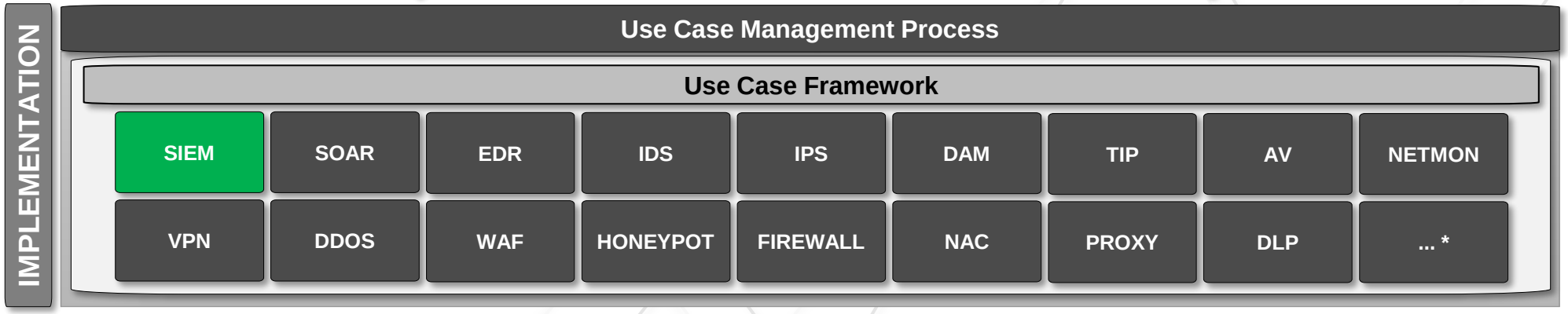
2. Decide and Apply a "Threat Modeling Strategy" based on Attacker, Software, Asset or Risk-Centric Threat Models



3. Identify, Prioritize and Operationalize: Use Cases and Integrations

Methodology for Building an Organizational Context and Content-Informed Cyber Threat modelling Strategy that aligns with an Use Case Management Program

3. Identify, Prioritize and Operationalize: Use Cases and Integrations

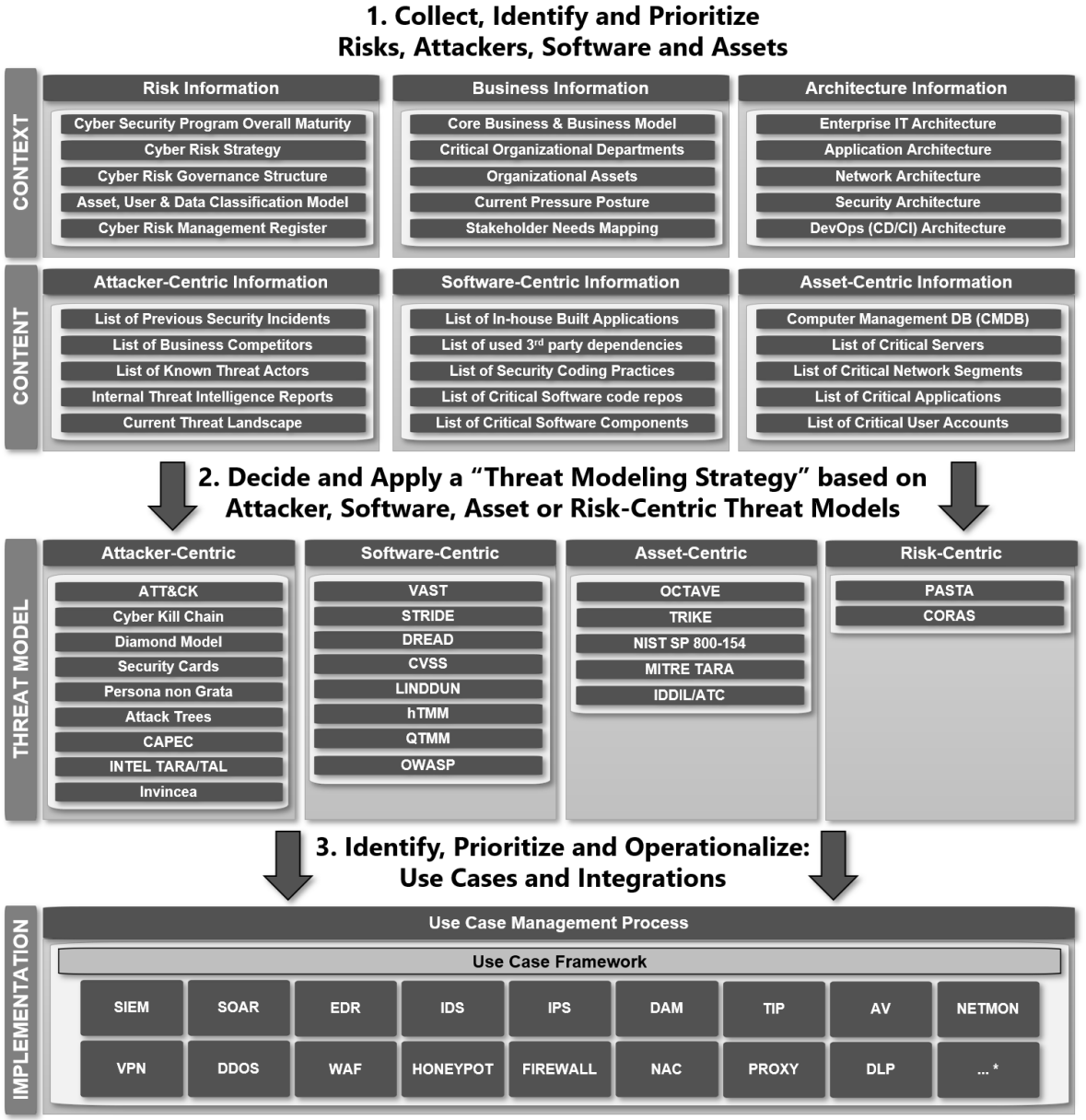


In Summary

- 1st. Elaborate Organizational Content and Contextual Analysis

- 2nd. Determination on Threat modeling strategy: 1st: Asset-centric 2nd: Attacker-centric Threat modeling methodology

- 3rd. Use a Use Case Framework that can house different threat modeling methodologies and allows for flexible prioritization.

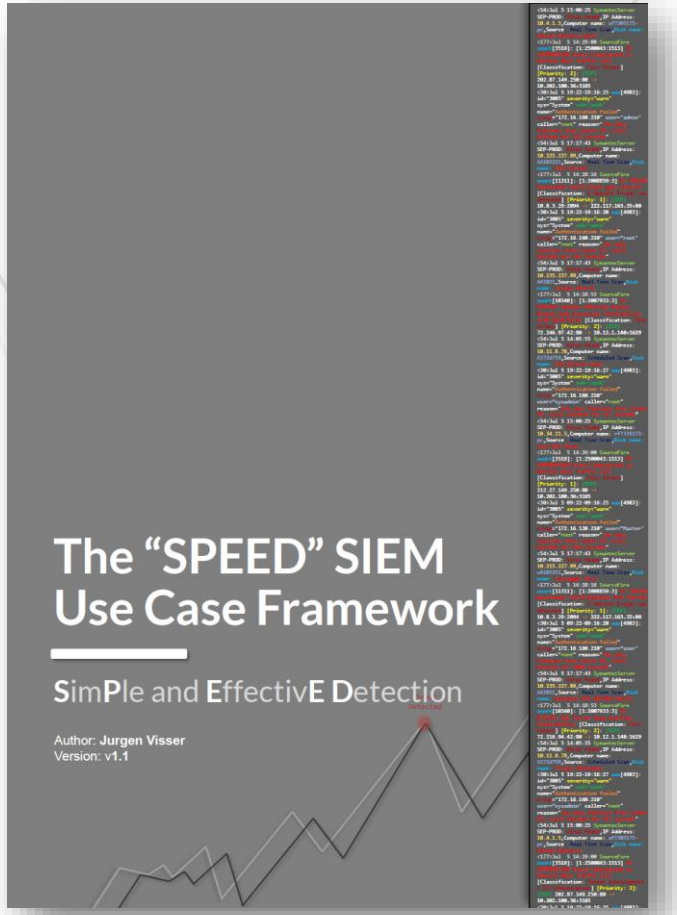



I Need Use Case Coverage Reporting!
Threat Detected
Let’s use the a Use Case Framework to organize SIEM use cases building

SPEED Use Case Framework

Why a Use Case Framework?

- To have a holistic **“frame of reference”** where detection use cases can be categorized into.
- To quickly see where your use cases are **lacking and need more attention (blind spots)**.
- To facilitate a **phased approach** of expanding new use cases based on a large variety of inputs and priorities (Use Case Roadmap).

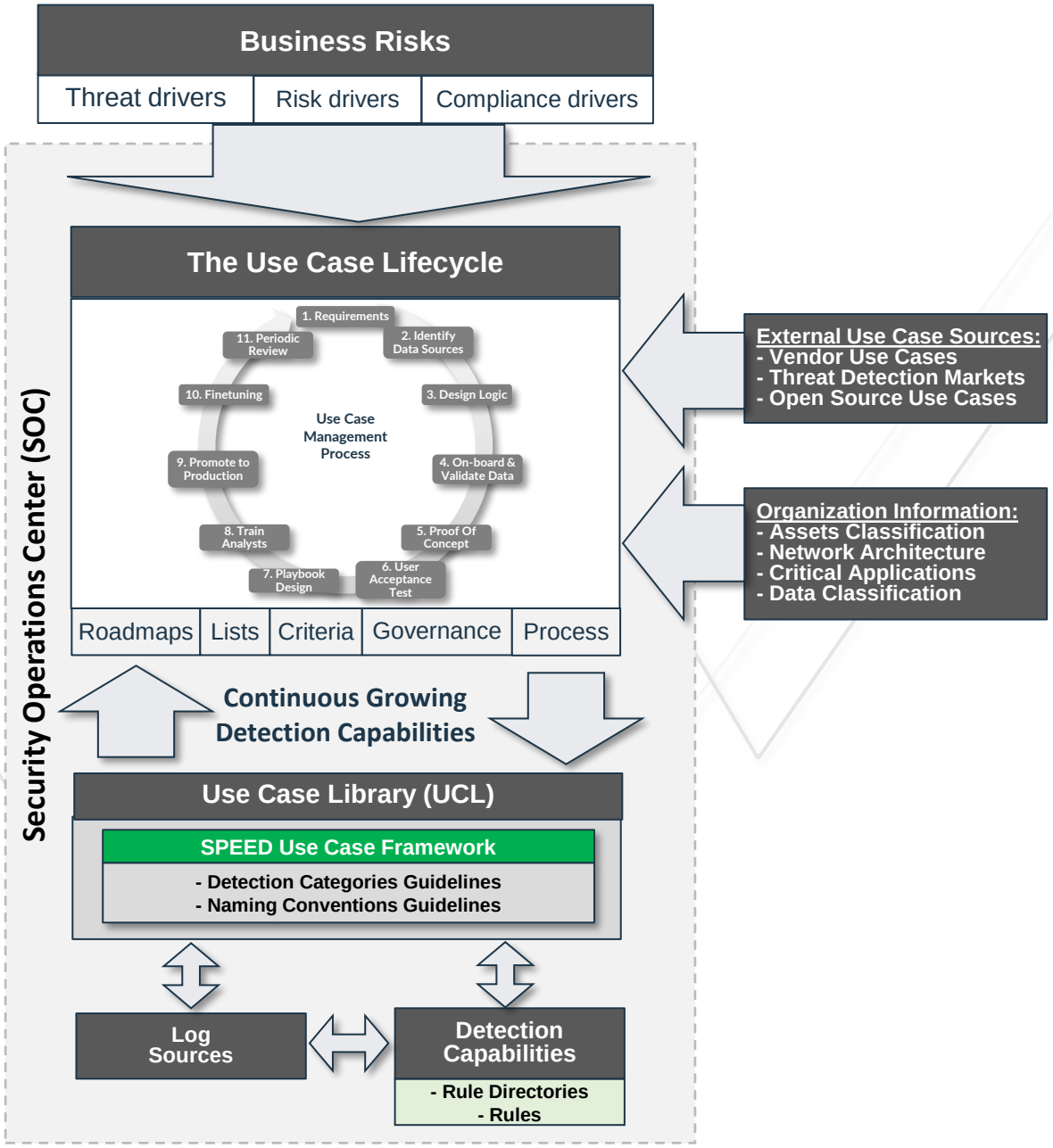


What is the Added value by the SPEED Use Case Framework?

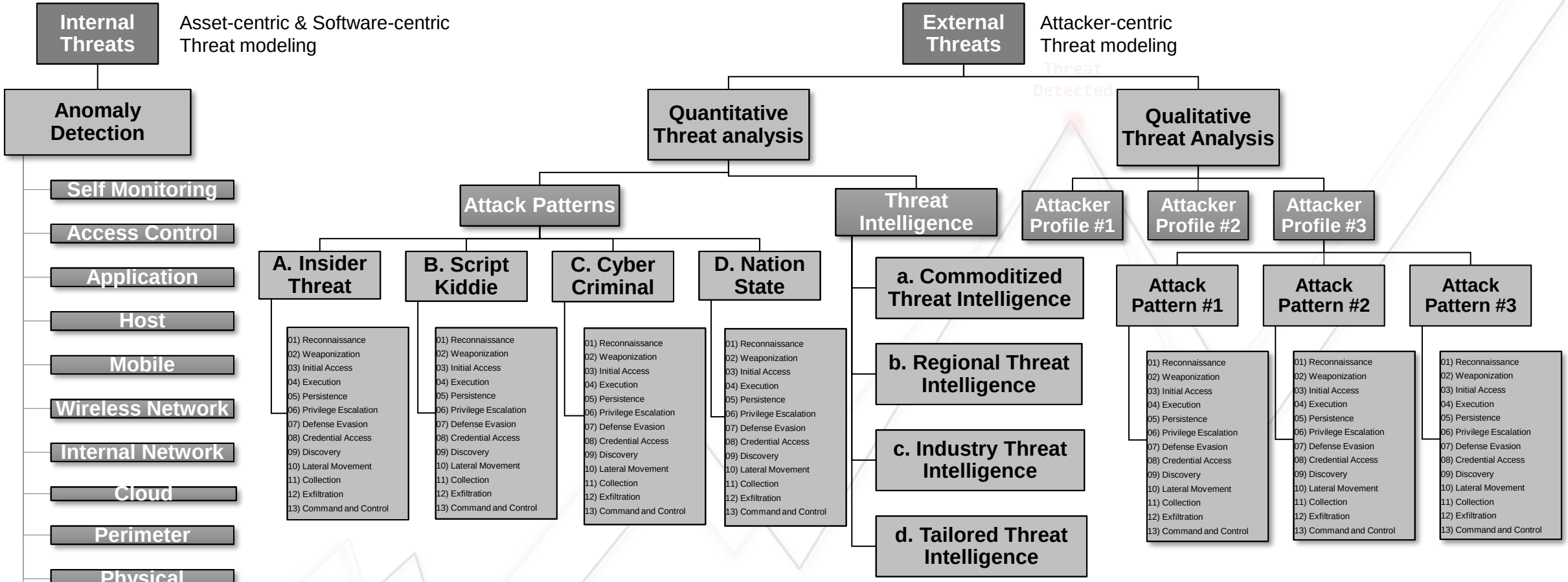
- Clear Location for log source monitoring use cases
- Location for generic Threat actor Threat modelling using the kill-chain
- Location for threat modelling threat actors like “APT1” using the kill-chain
- Key Distinctions between Threat intelligence types
- Key Distinction between Attacker-centric and Defense in depth model
- Very clearly defined naming conventions that are consistent all over the framework

Use Case Overview

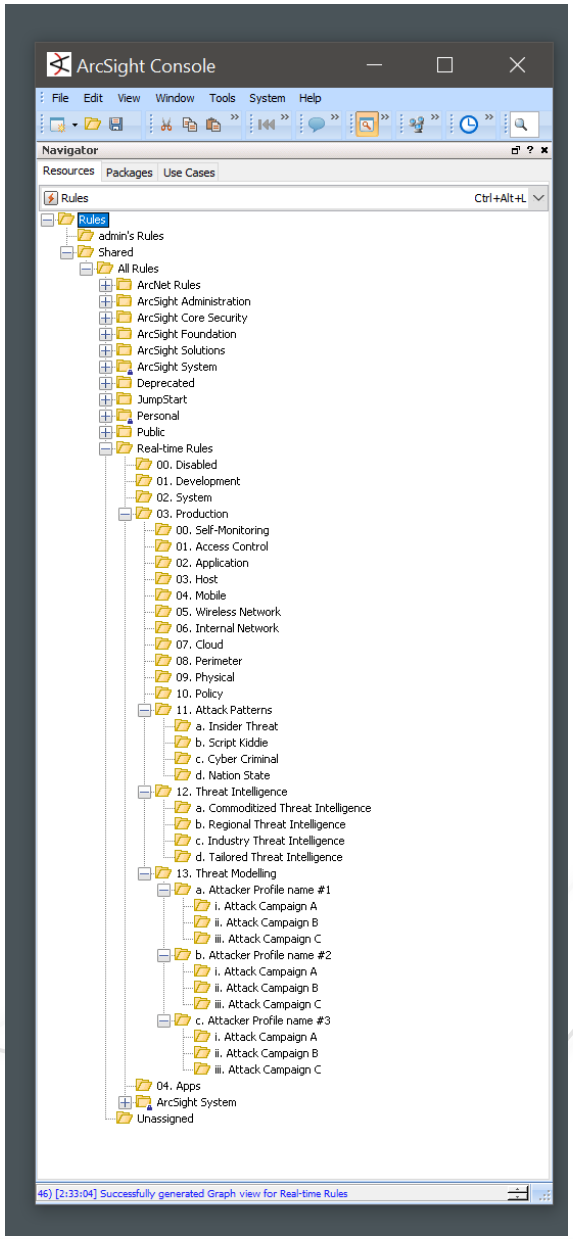
- Combining the Process and Use Case Framework in one.

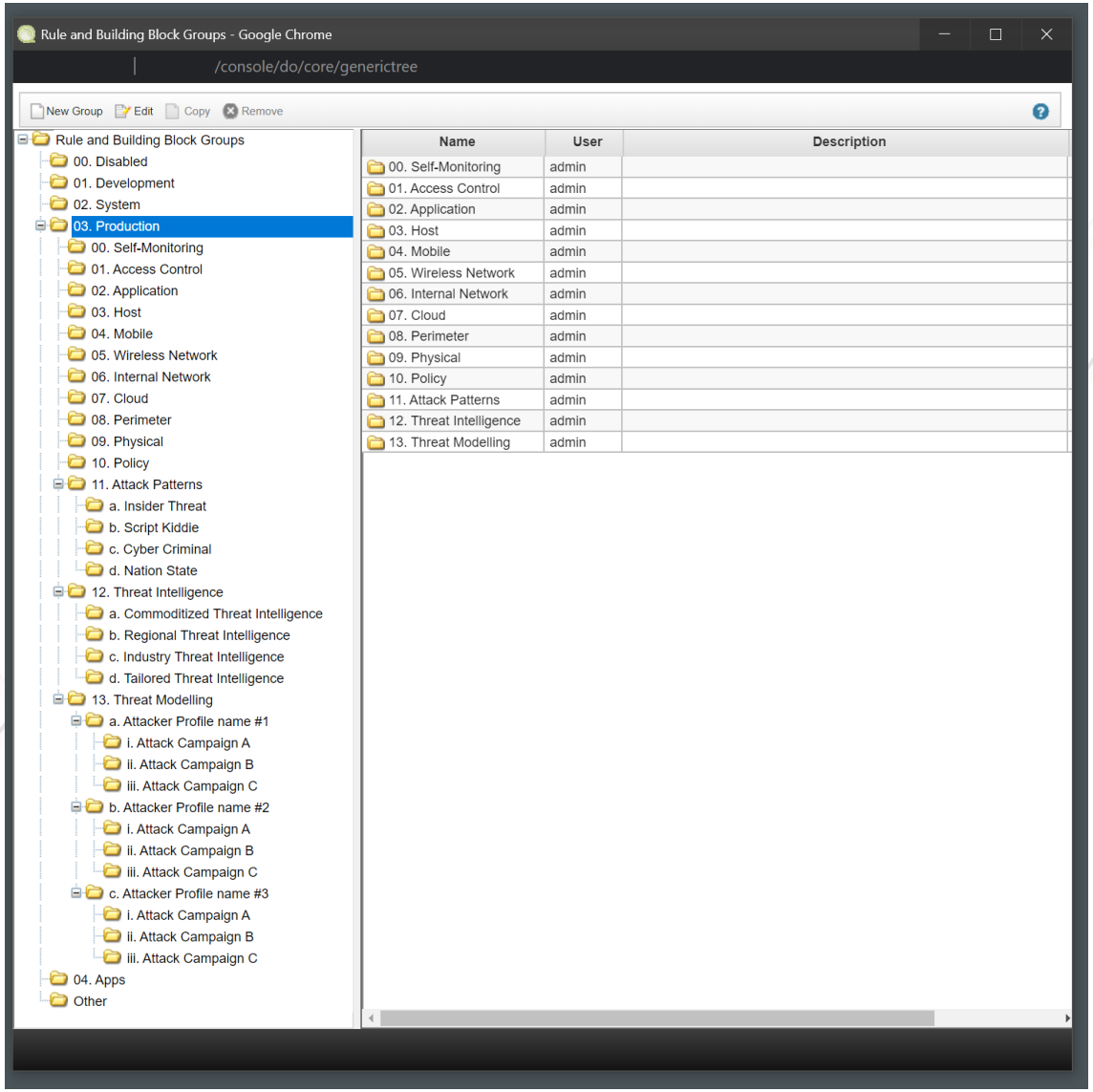


SPEED Use Case Framework



ArcSight & QRadar SIEM examples

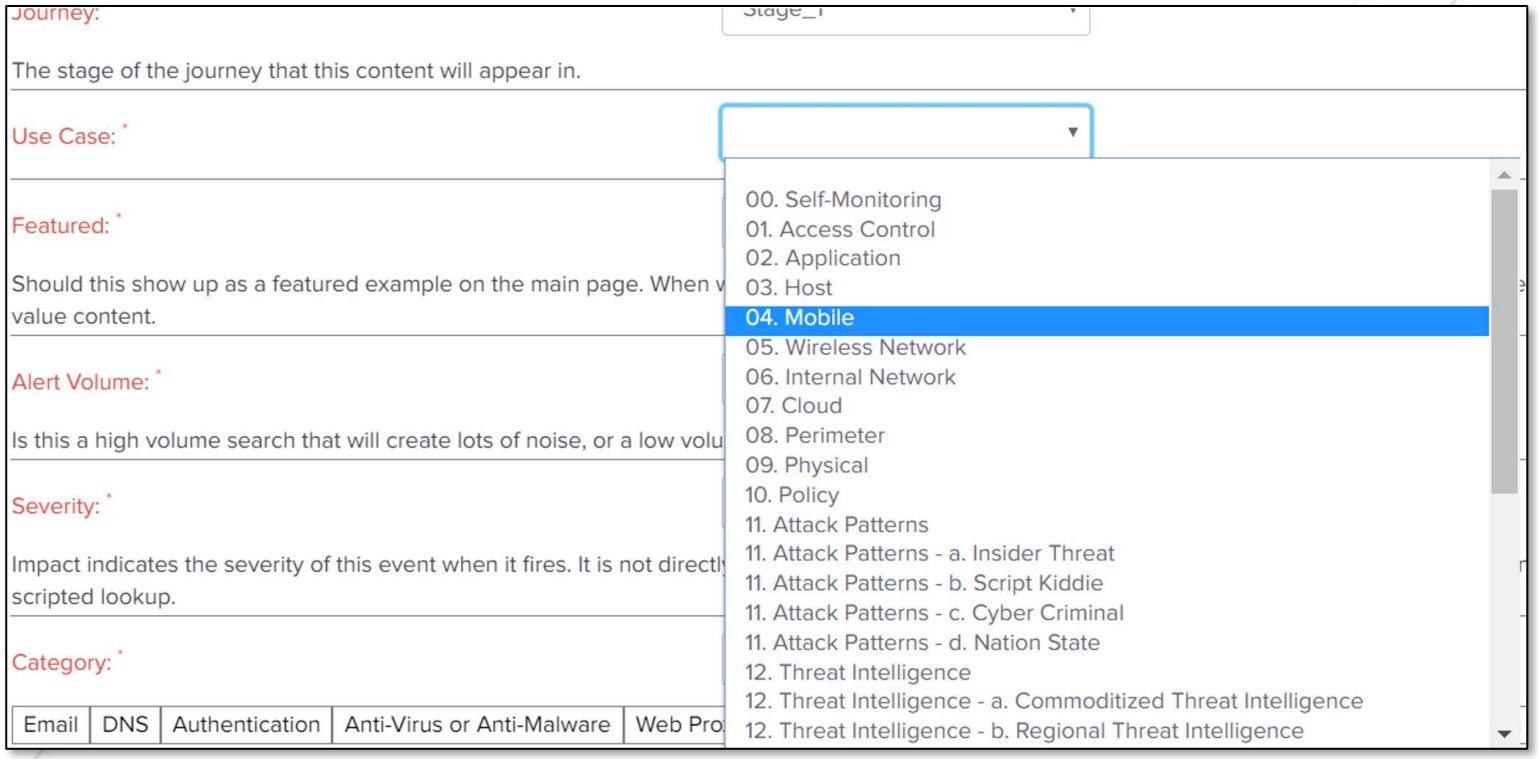




ELK & Splunk Examples

```
[root@elasticsearch  rules]# pwd
/opt/elastalert/rules
[root@elasticsearch  rules]# tree
.
├── 00. Disabled
├── 01. Development
├── 02. System
├── 03. Production
│   ├── 00. Self-Monitoring
│   ├── 01. Access Control
│   ├── 02. Application
│   ├── 03. Host
│   ├── 04. Mobile
│   ├── 05. Wireless Network
│   ├── 06. Internal Network
│   ├── 07. Cloud
│   ├── 08. Perimeter
│   ├── 09. Physical
│   ├── 10. Policy
│   ├── 11. Attack Patterns
│   │   ├── a. Insider Threat
│   │   ├── b. Script Kiddie
│   │   ├── c. Cyber Criminal
│   │   └── d. Nation State
│   ├── 12. Threat Intelligence
│   │   ├── a. Commoditized Threat Intelligence
│   │   ├── b. Regional Threat Intelligence
│   │   ├── c. Industry Threat Intelligence
│   │   └── d. Tailored Threat Intelligence
│   └── 13. Threat Modelling
│       ├── a. Attacker Profile name #1
│       │   ├── i. Attack Campaign A
│       │   ├── ii. Attack Campaign B
│       │   └── iii. Attack Campaign C
│       ├── b. Attacker Profile name #2
│       │   ├── i. Attack Campaign A
│       │   ├── ii. Attack Campaign B
│       │   └── iii. Attack Campaign C
│       └── c. Attacker Profile name #3
│           ├── i. Attack Campaign A
│           ├── ii. Attack Campaign B
│           └── iii. Attack Campaign C
└── 04. Apps

39 directories, 0 files
[root@elasticsearch  rules]#
```

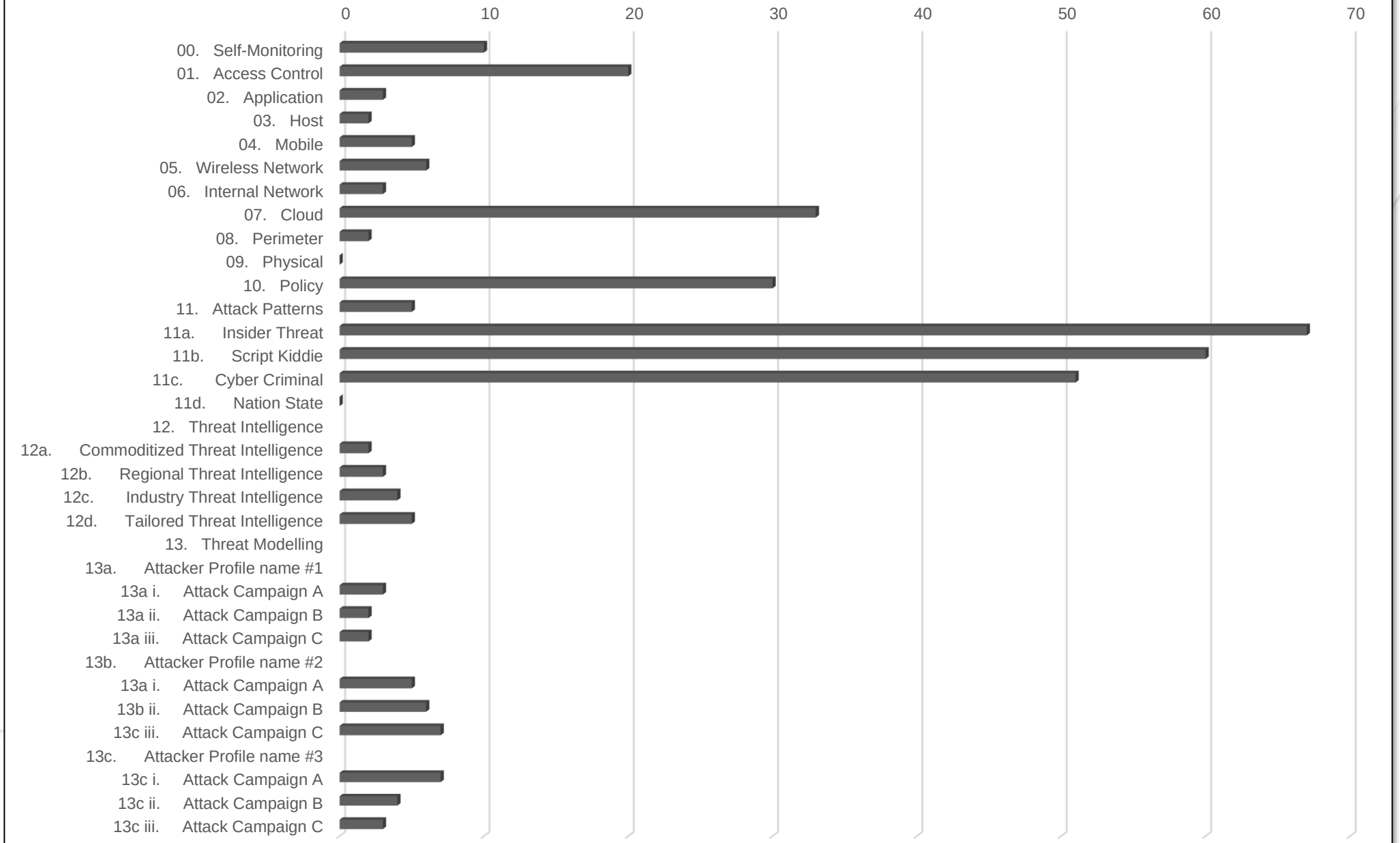


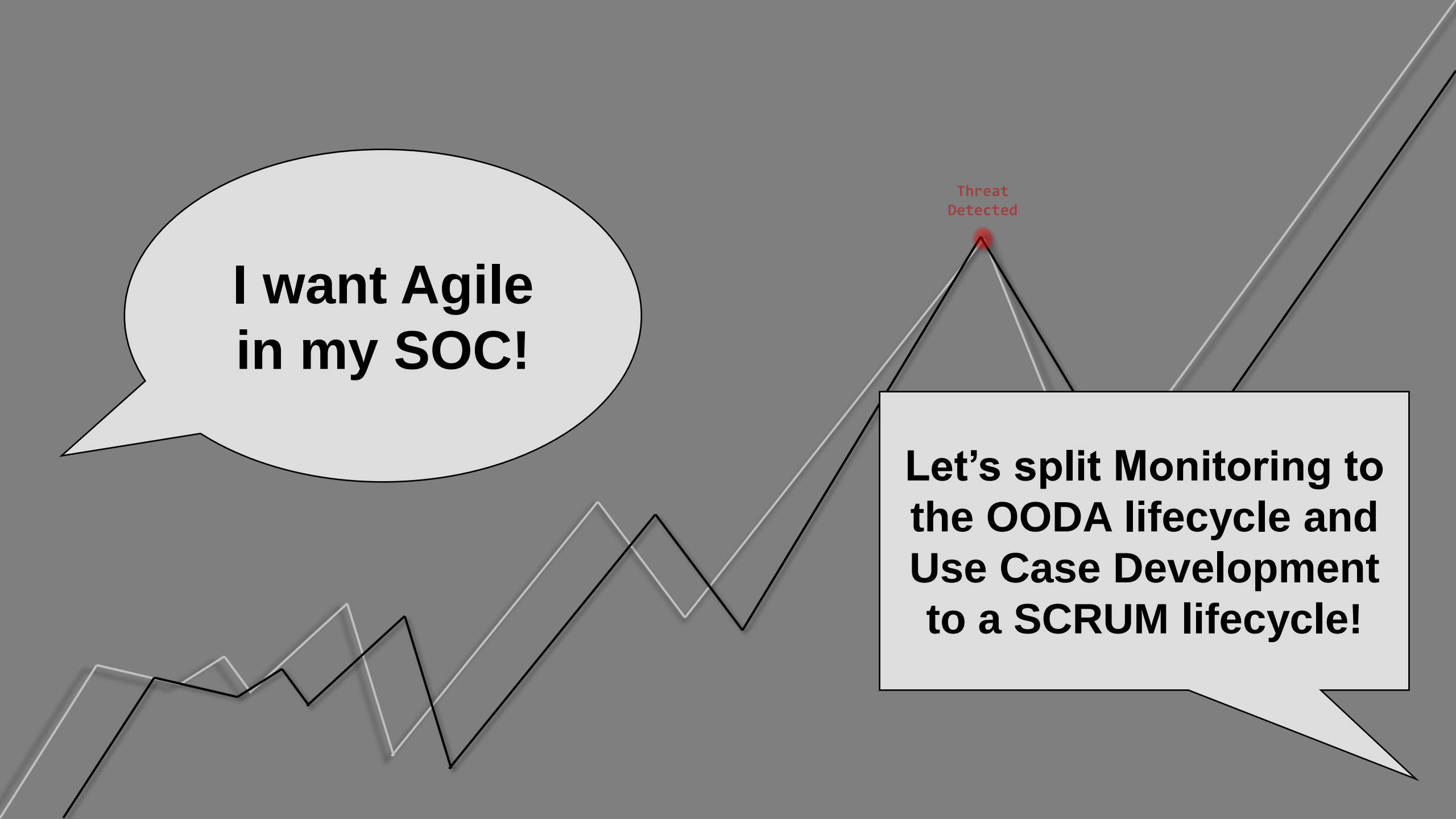
Naming conventions for Rules

Category	Naming Convention Standard
00. Self-Monitoring	
No events have been received	SELFMONIT-NOEVENTS-001 – No events received for 720 minutes on SIEM SELFMONIT-NOEVENTS-002 – No events received for 1 week on SIEM SELFMONIT-NOEVENTS-003 – Abnormally low event rate detected on SIEM
01. Access Control	
Massive Failed Token Auths Detected	ACCESSCONT-FAILEDTOKEN-001 – Failed token auth detected on 2FA system ACCESSCONT-FAILEDTOKEN-002 – Failed token auth detected on 2FA system ACCESSCONT-FAILEDTOKEN-003 – Failed token auth detected on 2FA system
02. Application	
Application Brute Force Detected	APPLICATION-APPBRUTE-001 - Brute force detected on Web application APPLICATION-APPBRUTE-002 - Brute force detected on HR application APPLICATION-APPBRUTE-003 - Brute force detected on Symantec application
03. Host	
Mass deletion of Virtual Host Detected	HOST-MASSDEL-001 – Mass VMWare machine deletion on VMWare HOST-MASSDEL-002 – Mass VMWare machine deletion on VMWare HOST-MASSDEL-003 – Mass VMWare machine deletion on VMWare
04. Mobile	
Mobile device locked out detected	MOBILE-LOCKEDOUT-001 – Device Locked out detected on MDM MOBILE-LOCKEDOUT-002 – Device Locked out detected on MDM MOBILE-LOCKEDOUT-003 – Device Locked out detected on MDM
05. Wireless Network	
Wireless Reconnaissance detected	WIRELESS-RECON-001 – Netstumbler Detected on WLC WIRELESS-RECON-002 – General scan tool Detected WLC WIRELESS-RECON-003 – Wireless scanner Detected WLC
06. Internal Network	
High amount of proxy denies detected	INTERNALNET-PROXDENIES-001 – Massive HTTPS denies detected on proxy INTERNALNET-PROXDENIES-002 – Massive HTTP denies detected on proxy INTERNALNET-PROXDENIES-003 – Massive 8080 denies detected on proxy
07. Cloud	
High amount of VPC deletions detected	CLOUD-VPCDEL-001 – Unauthorized deletion of a Critical VPC detected on AWS CLOUD-VPCDEL-002 – Unauthorized deletion of a DMZ VPC detected on AWS CLOUD-VPCDEL-003 – Unauthorized deletion of a Internal VPC detected on AWS
08. Perimeter	
Mass Drops on Perimeter Detected	PERIMETER-MASSDROP-001 – Massive Drops Detected on Firewall PERIMETER-MASSDROP-002 – Massive Drops from China Detected on Firewall PERIMETER-MASSDROP-003 – Massive Drops In to Outbound Detected on Firewall
09. Physical	
High amount of denies on Card Reader	PHYSICAL-CARDSPIKE-001 – High amount of denies on RFC Card reader PHYSICAL-CARDSPIKE-002 – High amount of denies on RFID reader PHYSICAL-CARDSPIKE-003 – High amount of denies on Swipe Card reader
10. Policy	
Authorization rights policy violation detected	POLICY-AUTHVIOL-001 – Authorization rights policy violation on Windows POLICY-AUTHVIOL-001 – Authorization rights policy violation on Windows POLICY-AUTHVIOL-001 – Authorization rights policy violation on Windows

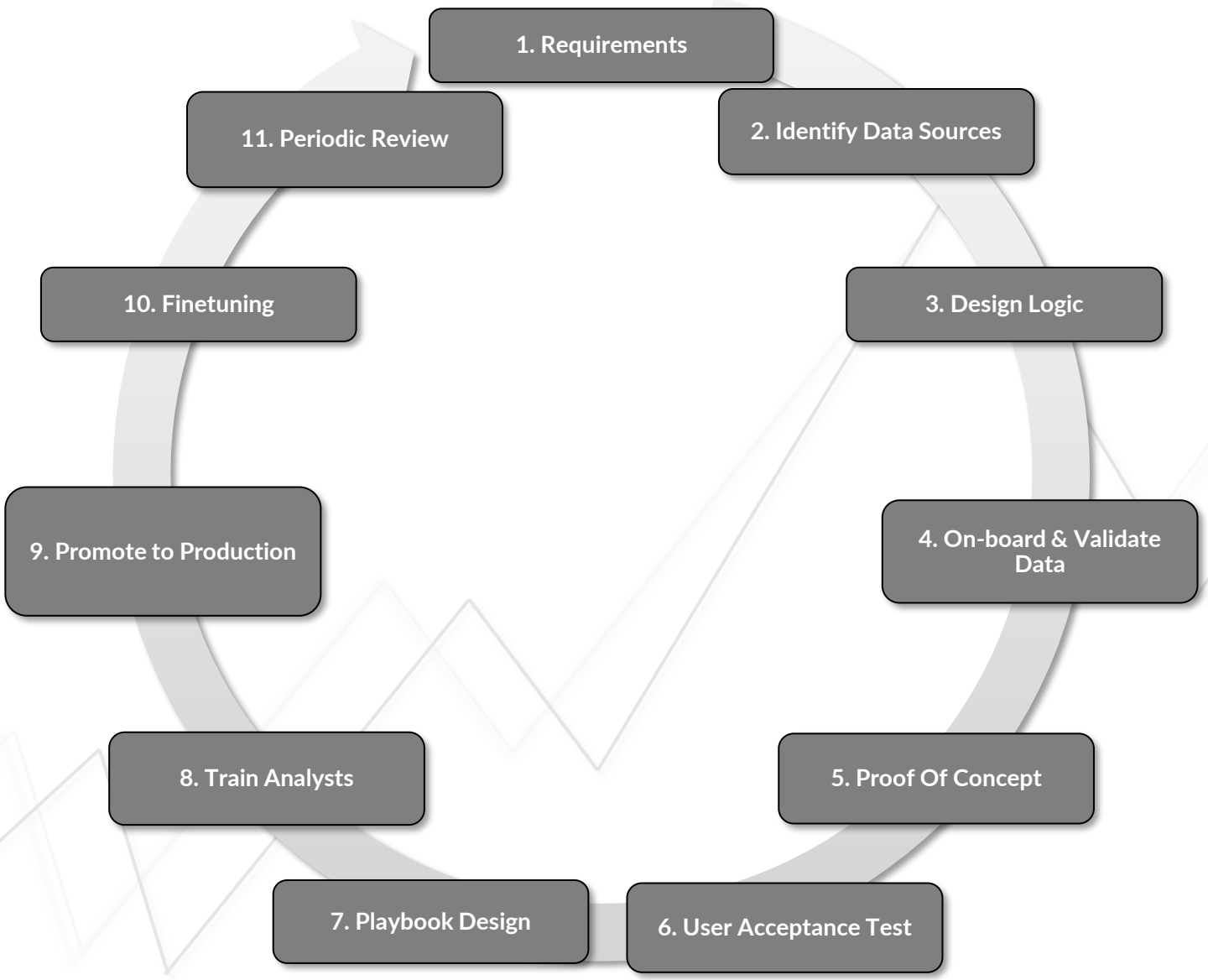
11. Attack Patterns	
A. Insider Threat	ATTACKP-INSIDERTH-RECON-001 – Insider threat reconnaissance on Firewall
B. Script Kiddie	ATTACKP-SCRIPTKID-RECON-001 – Script kiddie reconnaissance on Firewall detected ATTACKP-SCRIPTKID-WEAPON-001 – Script kiddie weaponization on Linux detected ATTACKP-SCRIPTKID-INITIALACC-001 – Script kiddie Initial Access on Endpoint detected ATTACKP-SCRIPTKID-EXECUTION-001 – Script kiddie Execution on Endpoint detected ATTACKP-SCRIPTKID-PERSISTENCE-001 – Script kiddie Persistence on Endpoint detected ATTACKP-SCRIPTKID-PRIVESC-001 – Script kiddie Privilege Escalation on Endpoint detected ATTACKP-SCRIPTKID-DEFEVASION-001– Script kiddie Defense evasion on Endpoint detected ATTACKP-SCRIPTKID-CREDACCESS-001– Script kiddie Credential Access on Endpoint detected ATTACKP-SCRIPTKID-DISCOVERY-001– Script kiddie Discovery on Network detected ATTACKP-SCRIPTKID-LATERAL-001– Script kiddie Lateral Movement on Network detected ATTACKP-SCRIPTKID-COLLECTION-001 – Script kiddie Data Collection on Endpoint detected ATTACKP-SCRIPTKID-C2-001 – Script kiddie C2 on Network detected ATTACKP-SCRIPTKID-EXFIL-001 – Script kiddie Actions on Objectives on Endpoint detected
C. Cyber Criminal	ATTACKP-CYBERCRIME-RECON-001 – Cyber Criminal reconnaissance on Firewall
D. Nation State	ATTACKP-NATIONSTATE-RECON-001 – Nation State reconnaissance on Firewall
12. Threat Intelligence	
A. Commoditized Threat Intelligence XFORCE ISIGHT	THREATINTEL-COMMOD-XFORCE-FIREWALL-001 - Outbound C2 Communication Detected THREATINTEL-COMMOD-XFORCE-VPN-001 - Outbound Malware Request Detected THREATINTEL-COMMOD-XFORCE-DNS-001 - Outbound DNS Request Detected
B. Regional Threat Intelligence	THREATINTEL-REGIONAL-NATCERT-001 – Outbound C2 Communication Detected
C. Industry Threat Intelligence	THREATINTEL-INDUSTRY-FSAC-001 – Outbound C2 Communication Detected
D. Tailored Threat Intelligence	THREATINTEL-TAILORED-HONEYP-001 – Outbound C2 Communication Detected
13. Threat Modelling	
a. BLACKPANDA	
i. Black October Campaign	THREATMODEL-BLACKPANDA-CAMP1-RECON-001 – Black Panda Campaign 1 reconnaissance on Firewall detected THREATMODEL-BLACKPANDA-CAMP1-WEAPON-001 – Black Panda Campaign 1 weaponization on Linux detected THREATMODEL-BLACKPANDA-CAMP1-INITIALACC-001 – Black Panda Campaign 1 Initial Access on Endpoint detected THREATMODEL-BLACKPANDA-CAMP1-EXECUTION-001 – Black Panda Campaign 1 Execution on Endpoint detected THREATMODEL-BLACKPANDA-CAMP1-PERSISTENCE-001 – Black Panda Campaign 1 Persistence on Endpoint detected THREATMODEL-BLACKPANDA-CAMP1-PRIVESC-001 – Black Panda Campaign 1 Privilege Escalation on Endpoint detected THREATMODEL-BLACKPANDA-CAMP1-DEFEVASION-001– Black Panda Campaign 1 Defense evasion on Endpoint detected THREATMODEL-BLACKPANDA-CAMP1-CREDACCESS-001– Black Panda Campaign 1 Credential Access on Endpoint detected THREATMODEL-BLACKPANDA-CAMP1-DISCOVERY-001– Black Panda Campaign 1 Discovery on Network detected THREATMODEL-BLACKPANDA-CAMP1-LATERAL-001– Black Panda Campaign 1 Lateral Movement on Network detected THREATMODEL-BLACKPANDA-CAMP1-COLLECTION-001 – Black Panda Campaign 1 Data Collection on Endpoint detected THREATMODEL-BLACKPANDA-CAMP1-C2-001 – Black Panda Campaign 1 C2 on Network detected THREATMODEL-BLACKPANDA-CAMP1-EXFIL-001 – Black Panda Campaign 1 Actions on Objectives on Endpoint detected

Use Case Coverage Report

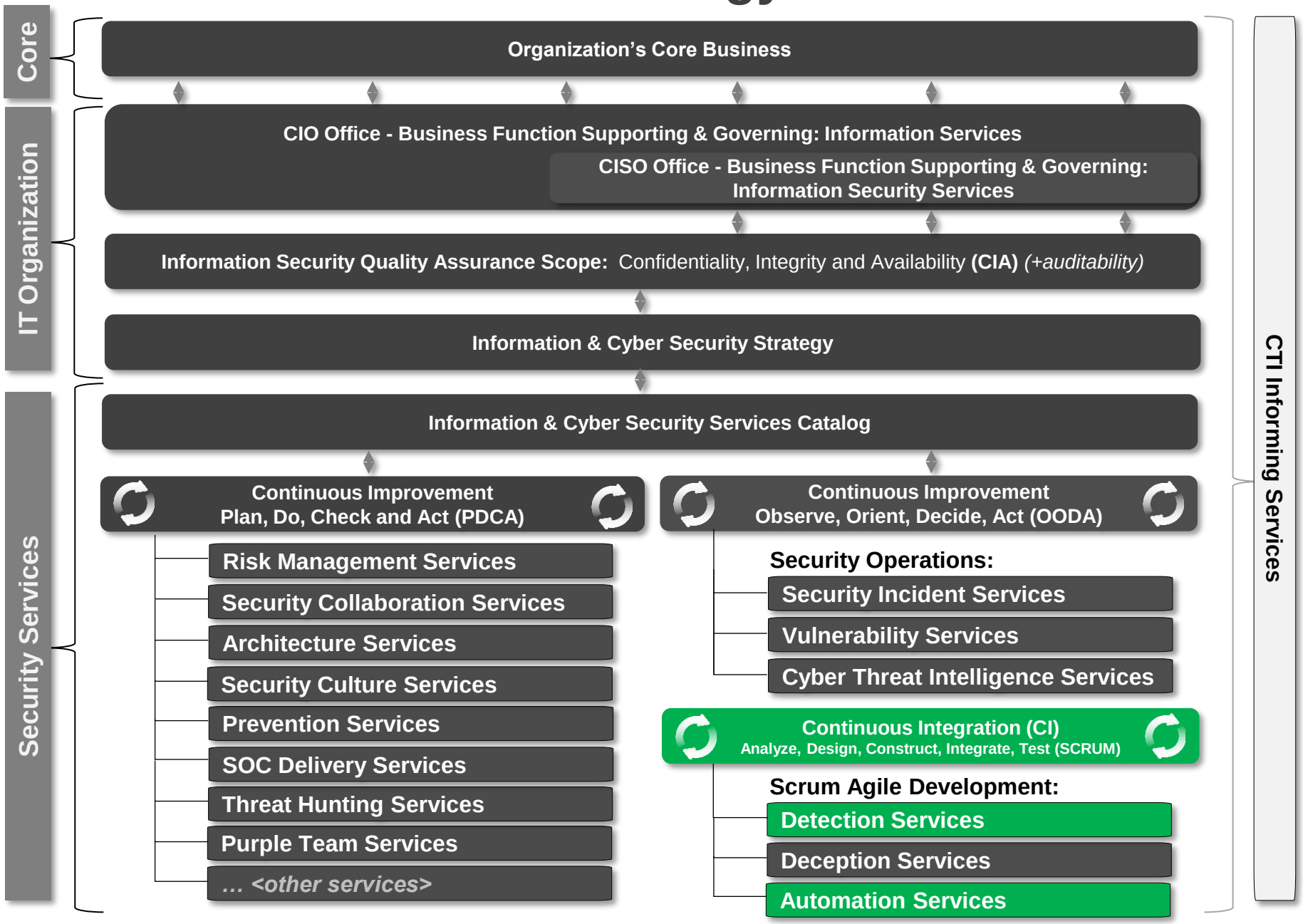



I want Agile in my SOC!
Threat Detected
Let’s split Monitoring to the OODA lifecycle and Use Case Development to a SCRUM lifecycle!

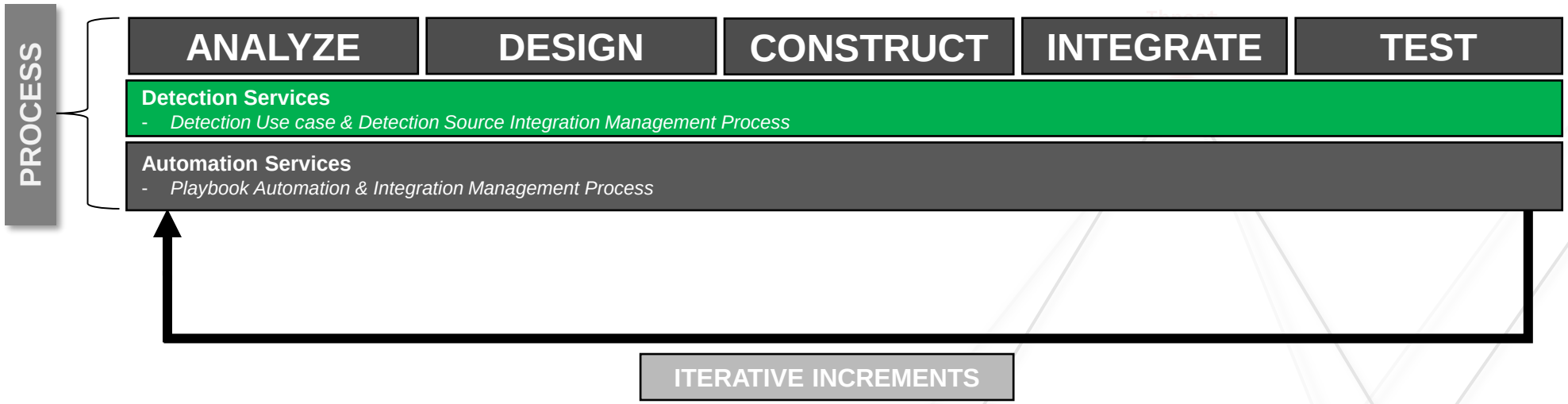
The Use Case Lifecycle

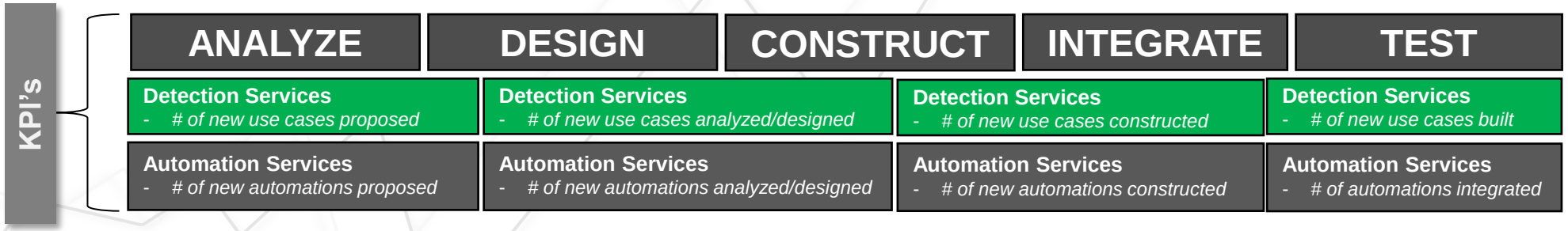


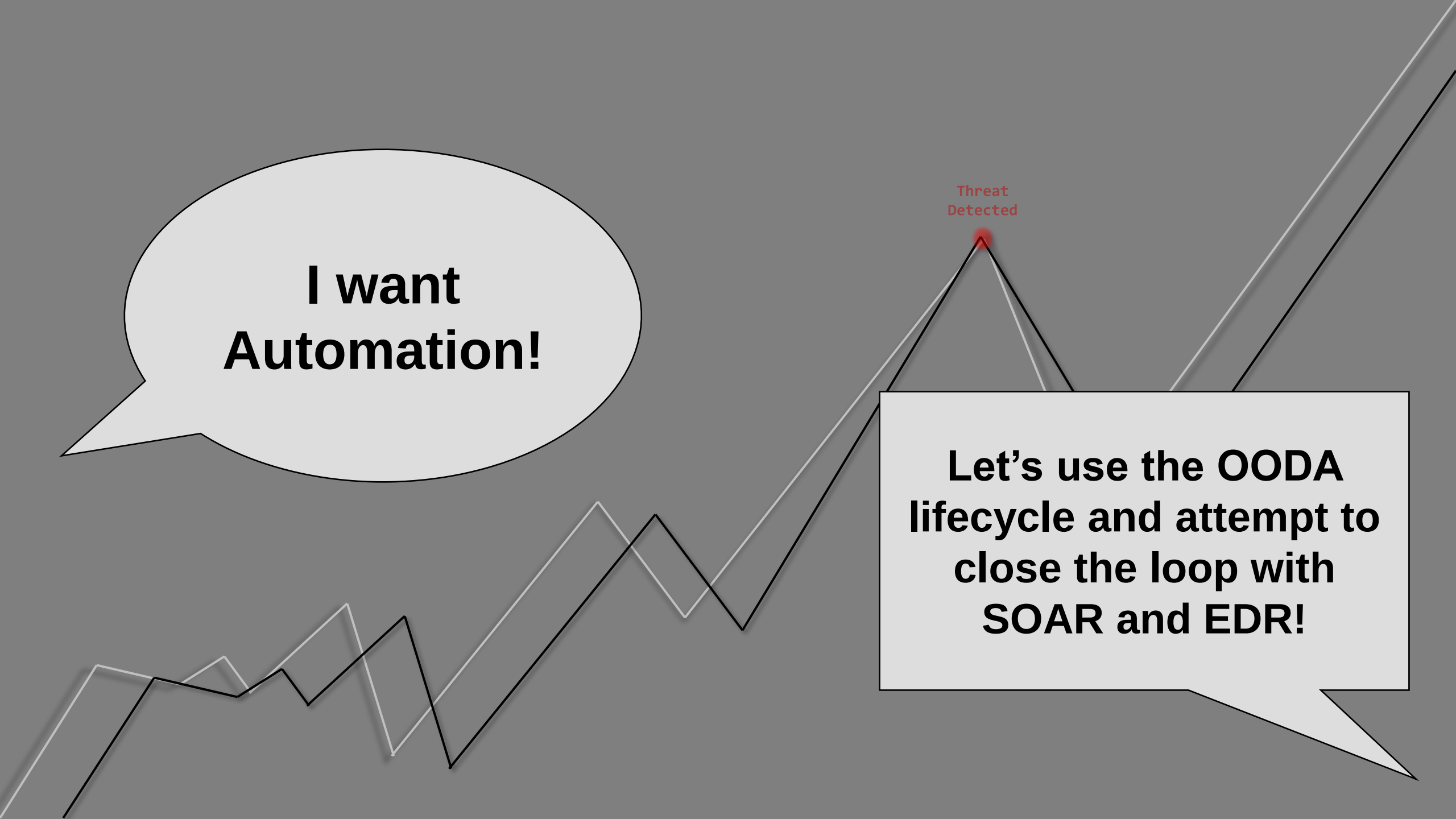
Process Strategy



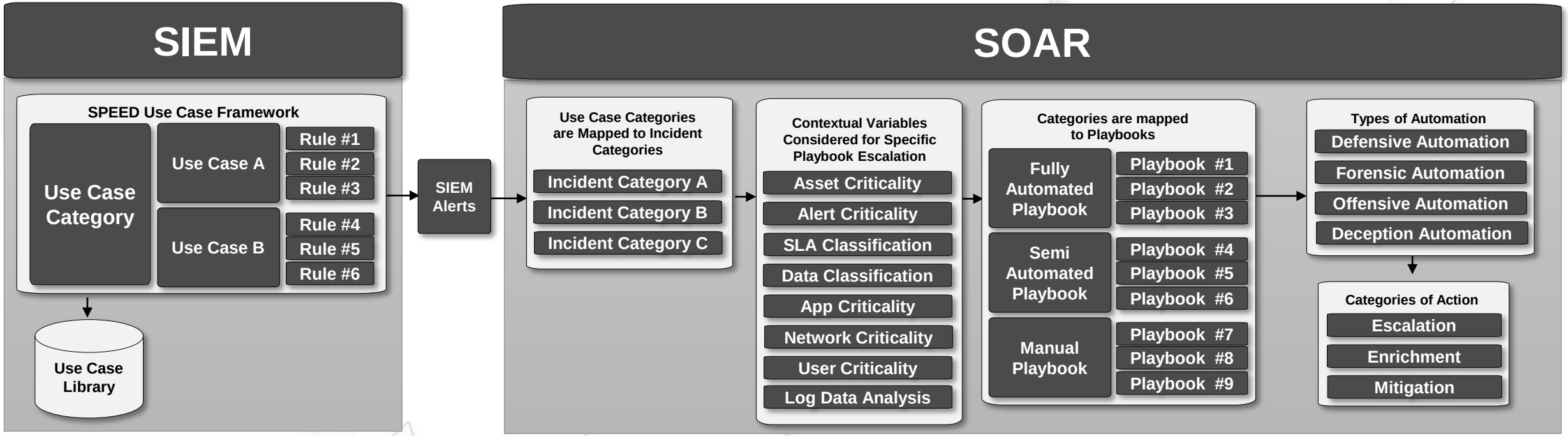
Process and KPI's related to SCRUM



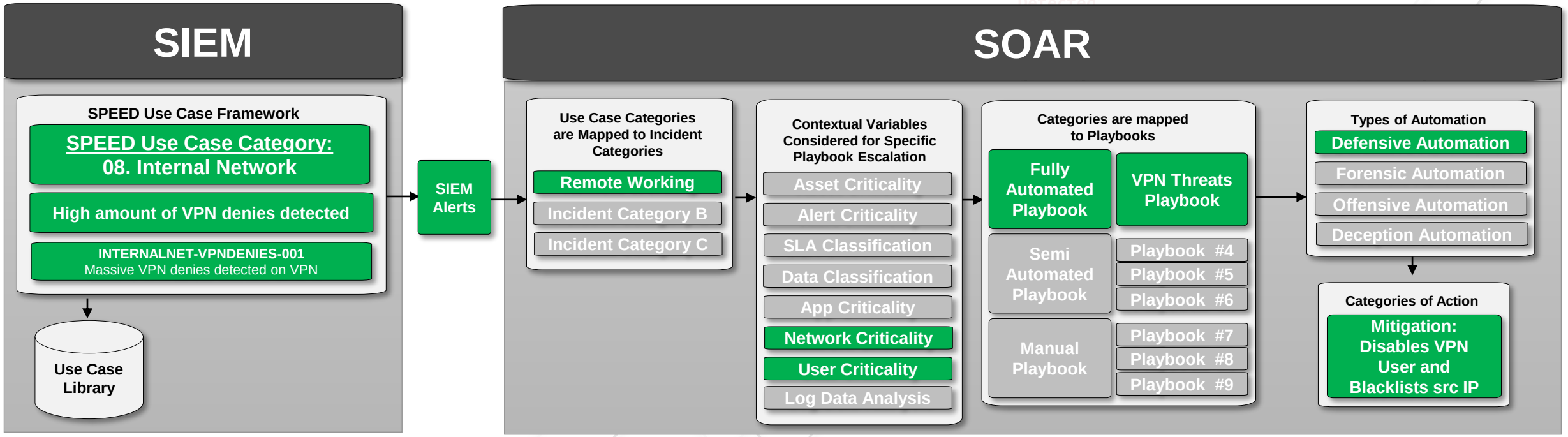


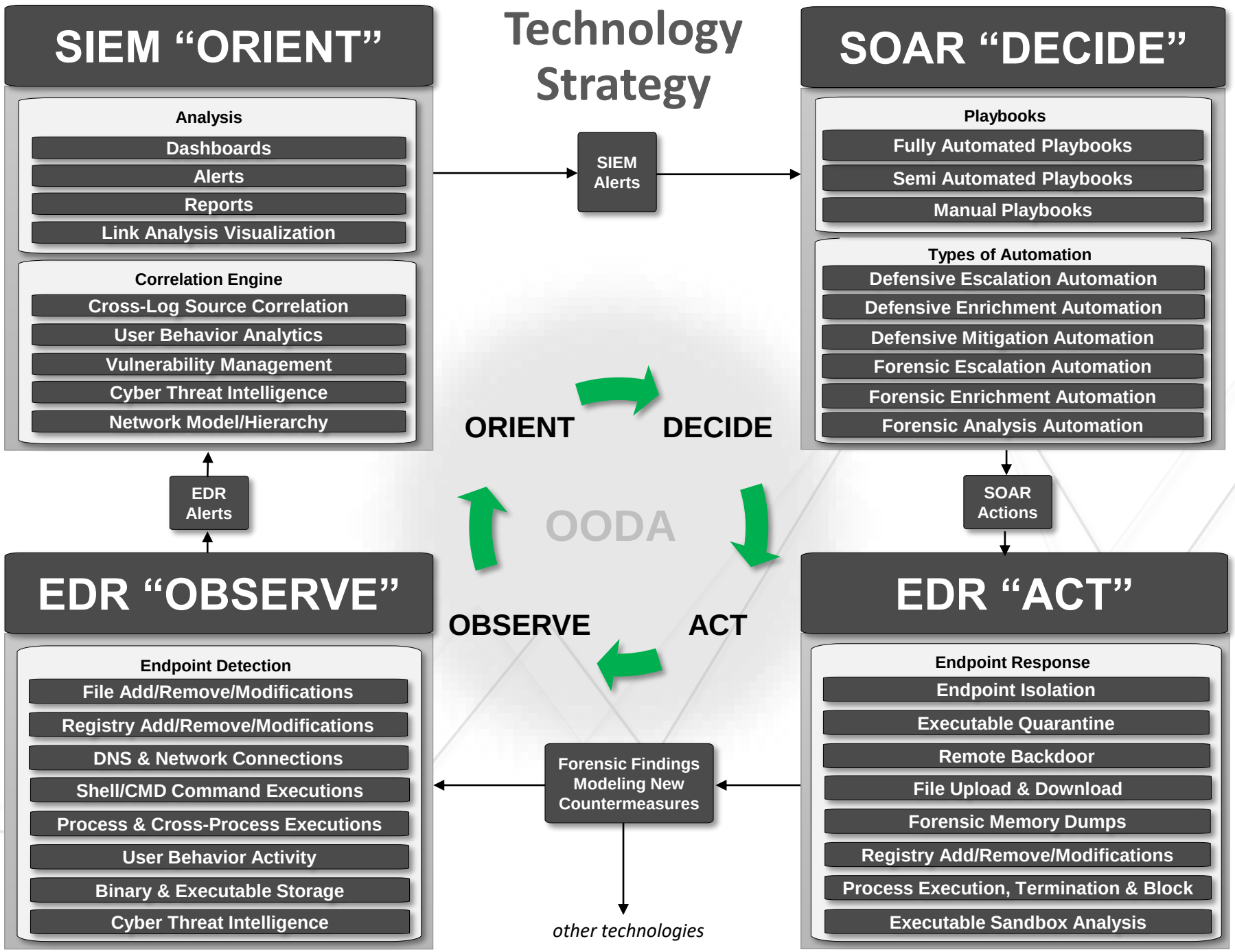

I want Automation!
Threat Detected
Let’s use the OODA lifecycle and attempt to close the loop with SOAR and EDR!

SIEM to SOAR relationship



SIEM to SOAR relationship: example

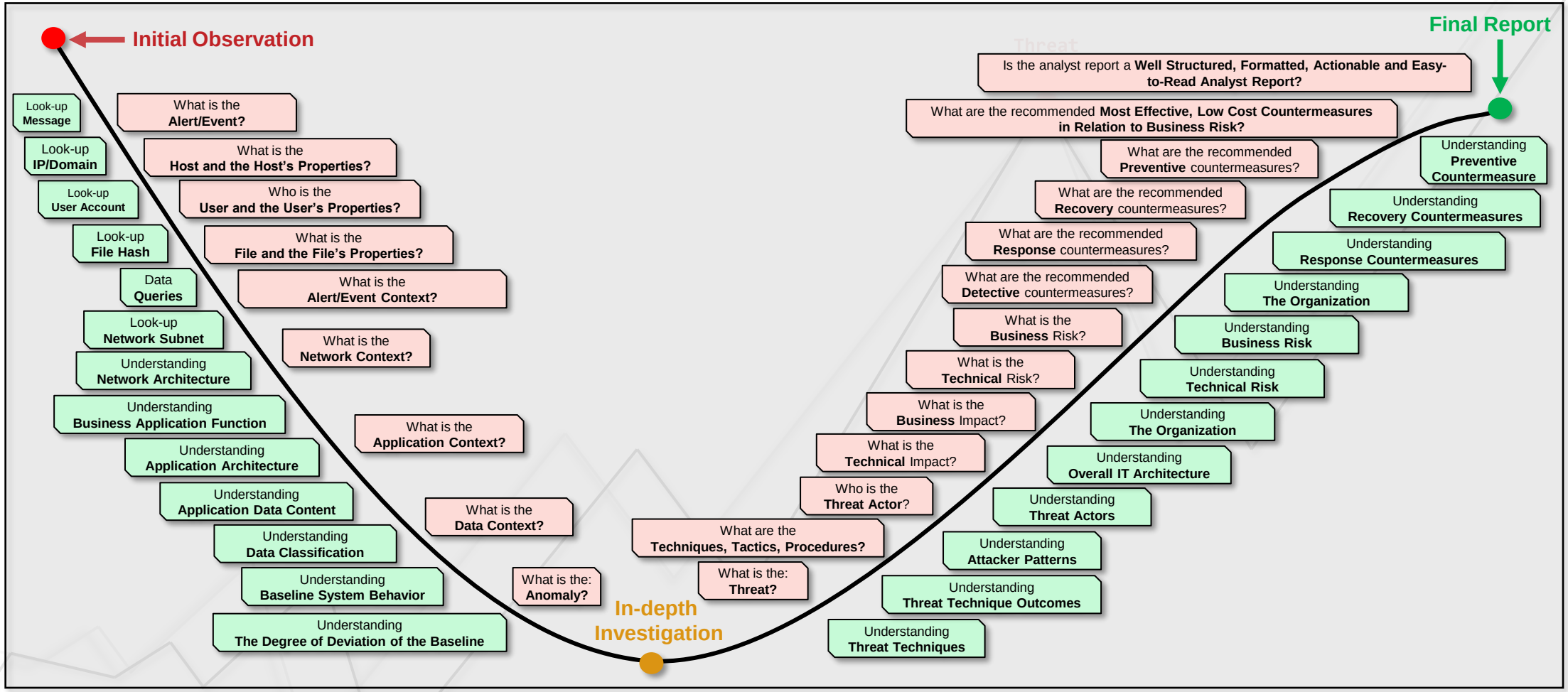


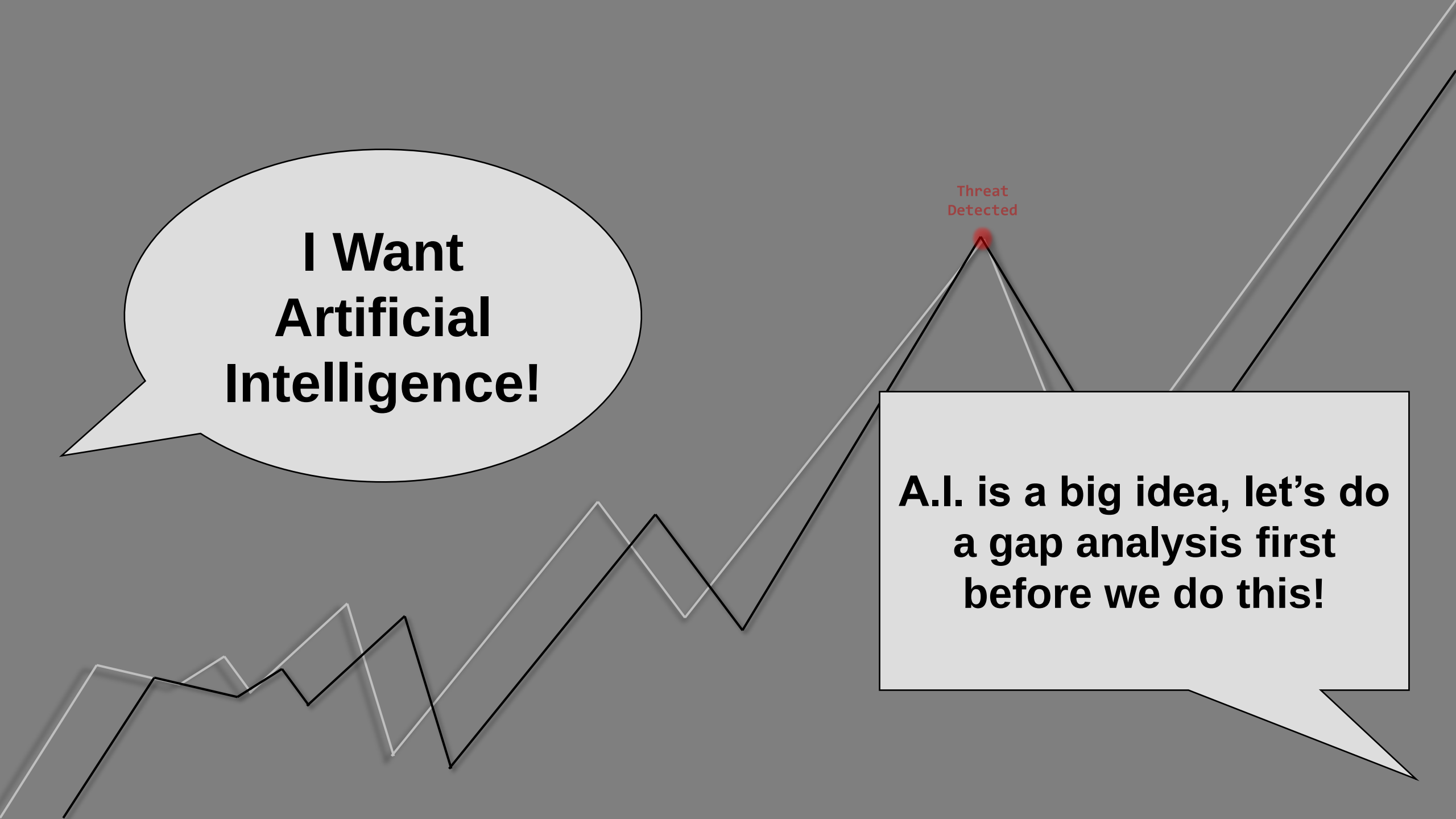

SIEM "ORIENT"
Analysis
Dashboards
Alerts
Reports
Link Analysis Visualization
Correlation Engine
Cross-Log Source Correlation
User Behavior Analytics
Vulnerability Management
Cyber Threat Intelligence
Network Model/Hierarchy
Technology Strategy
SIEM Alerts
SOAR "DECIDE"
Playbooks
Fully Automated Playbooks
Semi Automated Playbooks
Manual Playbooks
Types of Automation
Defensive Escalation Automation
Defensive Enrichment Automation
Defensive Mitigation Automation
Forensic Escalation Automation
Forensic Enrichment Automation
Forensic Analysis Automation
ORIENT
DECIDE
OODA
OBSERVE
ACT
EDR Alerts
SOAR Actions
EDR "OBSERVE"
Endpoint Detection
File Add/Remove/Modifications
Registry Add/Remove/Modifications
DNS & Network Connections
Shell/CMD Command Executions
Process & Cross-Process Executions
User Behavior Activity
Binary & Executable Storage
Cyber Threat Intelligence
EDR "ACT"
Endpoint Response
Endpoint Isolation
Executable Quarantine
Remote Backdoor
File Upload & Download
Forensic Memory Dumps
Registry Add/Remove/Modifications
Process Execution, Termination & Block
Executable Sandbox Analysis
Forensic Findings Modeling New Countermeasures
other technologies


I want world class analysts!
Threat Detected
Let’s hire a mix of junior, medior and senior security analysts!

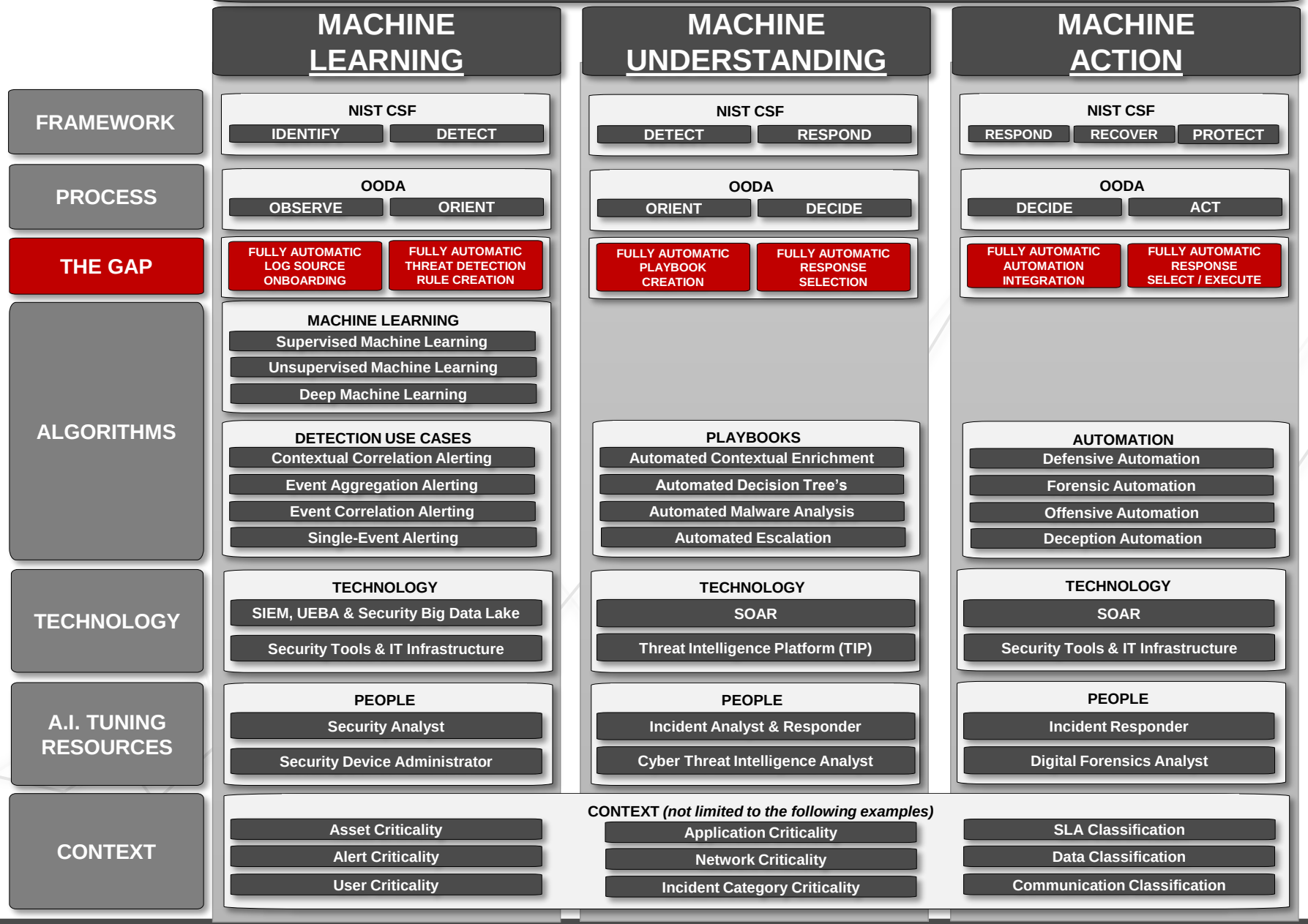
Cyber Security Analyst Maturity Curve

*"A senior cyber security analyst should be able to reach the **simplicity at the far side of complexity** and to be able to communicate the cyber security risks, threats and related countermeasures **simply, effectively and actionable.**"*




I Want Artificial Intelligence!
Threat Detected
A.I. is a big idea, let's do a gap analysis first before we do this!

CYBER SECURITY ARTIFICIAL INTELLIGENCE



1. FULLY AUTOMATIC LOG SOURCE ONBOARDING

CURRENT STATE

Automated:
No Automation

Semi-Automated:
No Semi-Automation

Manual work:
A. Configuring a log source to send logs
B. Building or relying on a vendor for a data parser.

THE GAP

Automated:
A. Application log monitoring integration as part of the **DevSecOps Continuous Monitoring (CM)** Pipeline (for Containers using FluentD).
B. Use **Terraform** to create log sources
C. Standardized **Instance Images or Start-up Scripts** with log forwarding agent embedded.

Semi-Automated:
A. Assigning existing parsers to a log source (heavily depends on collection protocol and SIEM vendor of choice).

Manual work:
A. Any Custom Application logs, non-supported API or non-cloud log source will require intensive manual work on collection and parsing. – Many vendors or developers are still not making a log API a high priority.

TARGET STATE

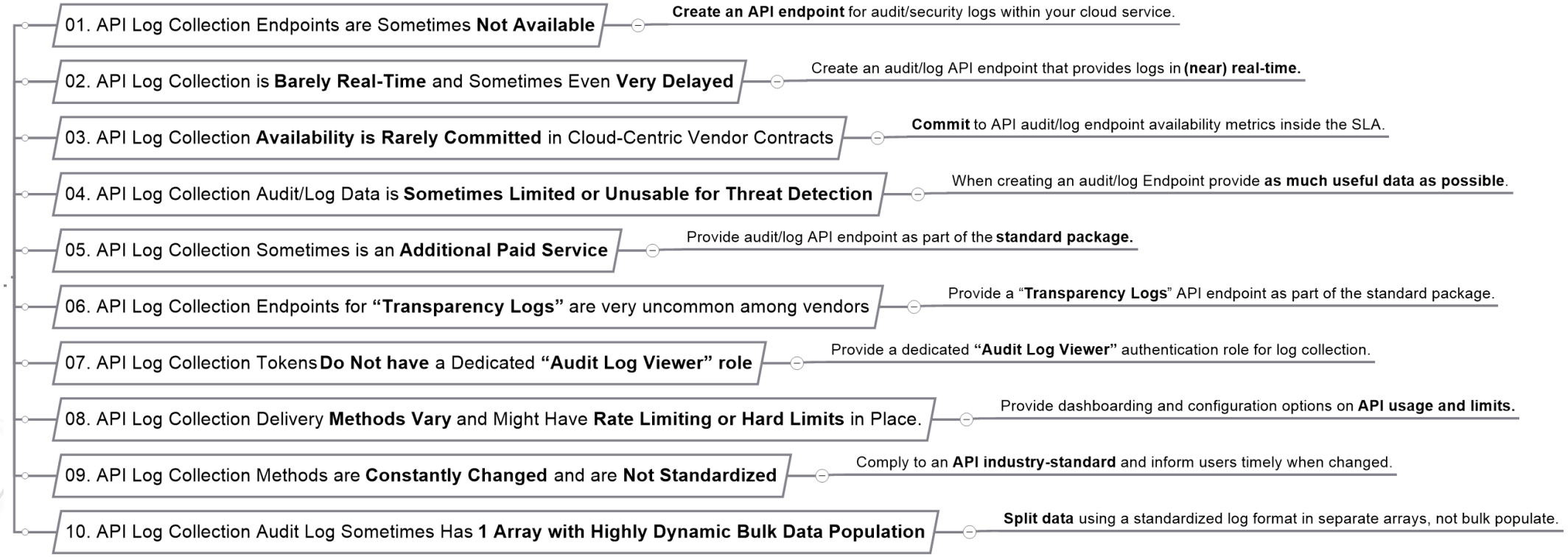
Automated:
A. Automated Log source onboarding
B. Automated Parser Building

Semi-Automated:
No Semi-Automation

Manual work:
No Manual Work

There is still a major challenge with API Standardization for log collection

10 Major API Log Collection Challenges for Threat Detection in a Cloud-Native World



2. FULLY AUTOMATIC THREAT DETECTION RULE CREATION

CURRENT STATE

Automated:
No Automation

Semi-Automated:
No Semi-Automation

Manual work:
A. Creating or importing rule sets.
B. Finetuning the rule is still required before promoting to production

THE GAP

Automated:
A. Pull in newly created rules by open source community. **SIGMA** is a open standard for formatting search rules in SIEM.
Pulling these automatically in.

Semi-Automated:
A. Creating log agnostic detection rules that automatically catch any data in new onboarded log sources.

Manual work:
A. Finetuning of the rules, every environment is unique so there might be false positives.

TARGET STATE

Automated:
A. Automated Rule Creation or Importing
B. Automated Rule Tuning

Semi-Automated:
No Semi-Automation

Manual work:
No Manual Work

3. FULLY AUTOMATIC PLAYBOOK CREATION
4. FULLY AUTOMATIC RESPONSE SELECTION

CURRENT STATE

Automated:
No Automation

Semi-Automated:
No Semi-Automation

Manual work:
A. Creating a playbook
B. Connecting the right response integrations to the playbook

THE GAP

Automated:
A. Pull in newly created rules by open source community. **CACAO** is a open standard for formatting for vendor neutral SOAR. Pulling these automatically in. **currently v1.0 JSON standard is still in draft.*

Semi-Automated:
N/A

Manual work:
A. Finetuning of the playbooks, every environment is unique so there might be things that do not work.
B. Integrations with the environment are highly dependent on the environment the system is residing in, therefore additional intensive work is required.

TARGET STATE

Automated:
A. Automated Playbook creation
B. Automated Response Integration Selection

Semi-Automated:
No Semi-Automation

Manual work:
No Manual Work

5. FULLY AUTOMATIC AUTOMATION INTEGRATION
6. FULLY AUTOMATIC RESPONSE SELECT / EXECUTE

CURRENT STATE

Automated:
No Automation

Semi-Automated:
No Semi-Automation

Manual work:
A. Creating or importing integrations
B. Configuration of Integrations with the correct parameters

THE GAP

Automated:
N/A

Semi-Automated:
A. Supported API's that are known and standardized like Cloud Services can be used as a templated and modified.

Manual work:
A. Integrations with the environment are highly dependent on the environment the system is residing in, therefore additional intensive work is required.

TARGET STATE

Automated:
A. Automated Automation integration
B. Automated Response configuration

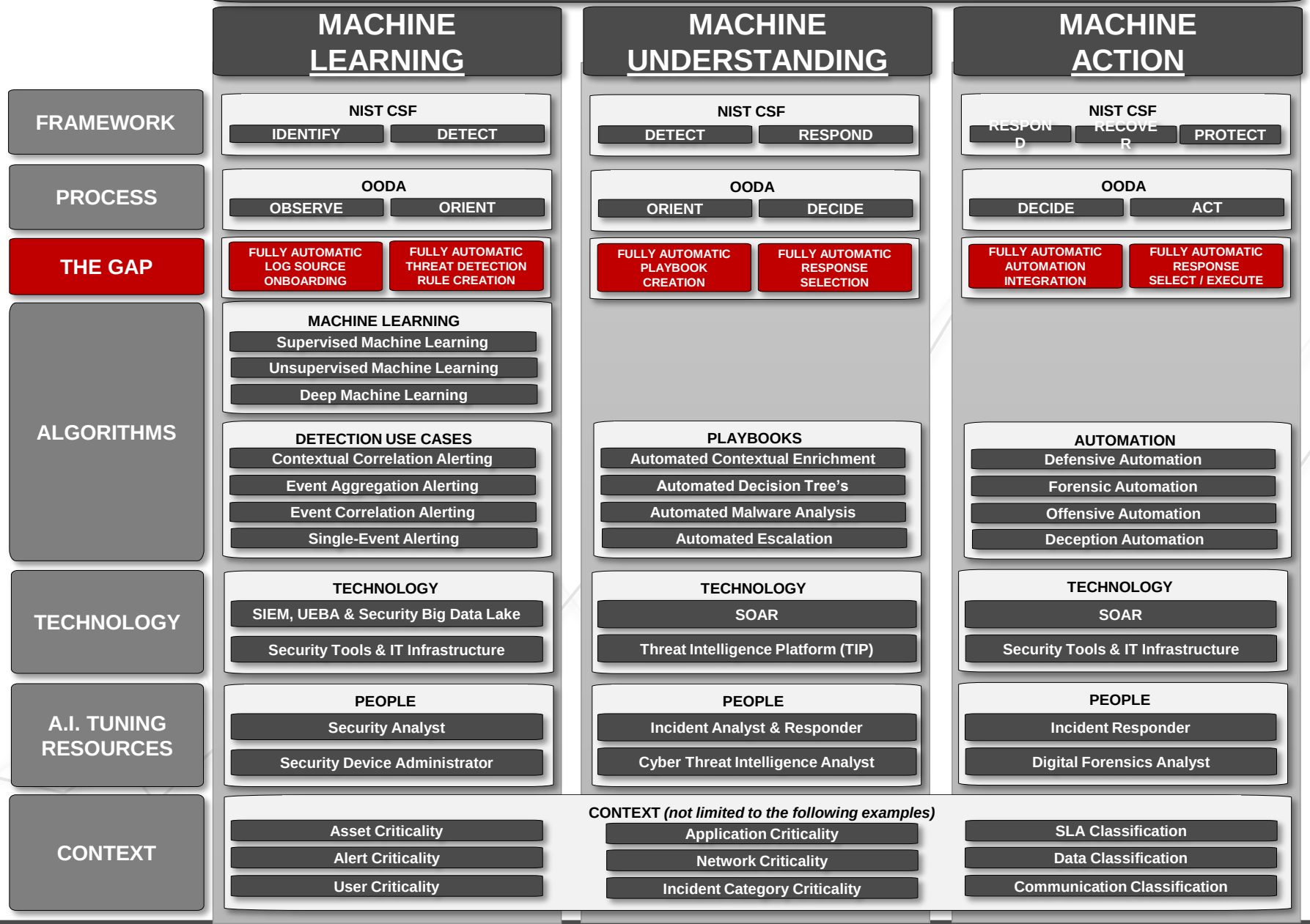
Semi-Automated:
No Semi-Automation

Manual work:
No Manual Work

CONCLUSION

- The A.I. GAP **cannot be entirely bridged** but we can start working towards it.
- Most cyber “A.I.” are very **narrow point solution** that only can do a limited use case.
- A.I. that does everything out of the box with a scope on the entire infrastructure **does not exist**.
- The cloud gives us a **great boost** towards realizing A.I. in Cyber Security
- If a organization is **100% in 1 cloud deployed** without any other dependency on any other vendor for applications in the infrastructure the organization can potentially get to the **closest of realizing A.I.** in it’s infrastructure

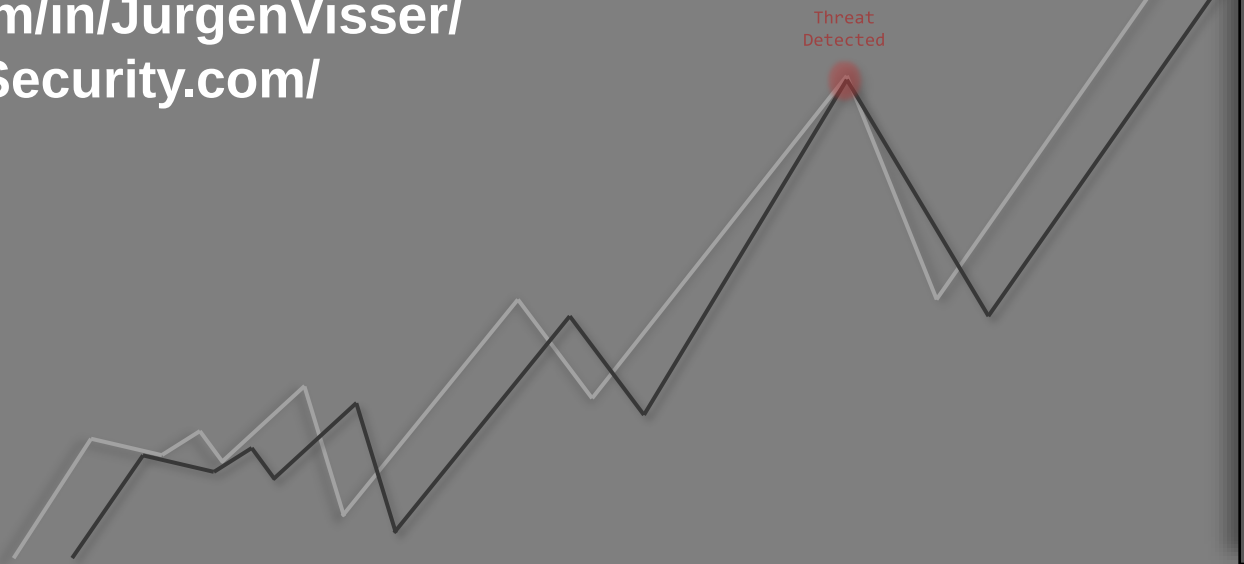
CYBER SECURITY ARTIFICIAL INTELLIGENCE



THANK YOU

- Jurgen Visser
- @jurgenvi
- www.linkedin.com/in/JurgenVisser/
- www.CorrelatedSecurity.com/

LinkedIn QR CODE



srcip="172.16.160.210" user="root" caller="root" reason="Too many failures from client IP, still blocked for 537 seconds"
<54>Jul 5 17:17:43 SymantecServer SEP-PROD: Virus found,IP Address: 10.235.237.89,Computer name: A41021,Source: Real Time Scan,Risk name: Backdoor.IRCBot!win32
<177>Jul 5 14:18:53 SourceFire snort[10340]: [1:2007933:3] ET EXPLOIT Microsoft Office Memory Corruption Vulnerability (CVE-2017-11882) [Classification: Microsoft Application Attack] [Priority: 2]: {TCP} 72.246.97.42:80 -> **10.12.1.140:1629**
<54>Jul 5 14:05:55 SymantecServer SEP-PROD: Virus found,IP Address: 10.11.8.78,Computer name: A372d759,Source: Scheduled Scan,Risk name: W97M.Melissa.A
<30>Jul 5 19:22-19:16:27 aua[4983]: id="3005" severity="warn" sys="System" sub="auth" name="Authentication failed" srcip="172.16.160.210" user="sysadmin" caller="root" reason="Too many failures from client IP, still blocked for 517 seconds"