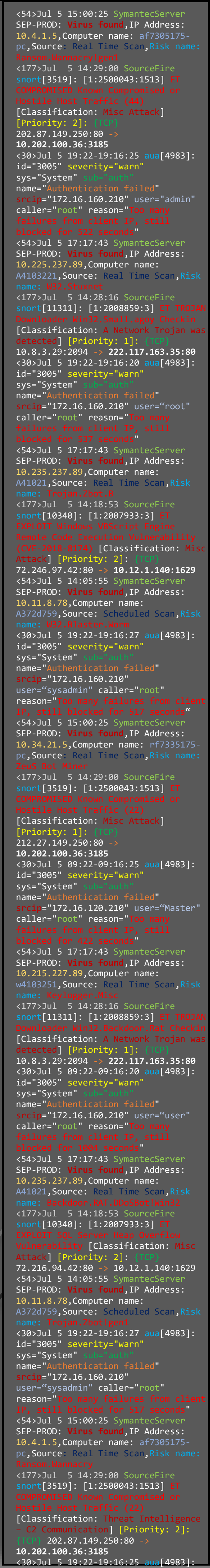
The “SPEED” SIEM Use Case Framework

SimPle and EffectivE Detection

Author: **Jurgen Visser**
Version: v**1.0**



```
<54>Jul 5 15:00:25 SymantecServer
SEP-PROD: Virus found,IP Address:
10.4.1.5,Computer name: af7305175-
pc,Source: Real Time Scan,Risk name:
Ransom.Wannacry!gen1
<177>Jul  5 14:29:00 SourceFire
snort[3519]: [1:2500043:1513] ET
COMPROMISED Known Compromised or
Hostile Host Traffic (44)
[Classification: Misc Attack]
[Priority: 2]: {TCP}
202.87.149.250:80 ->
10.202.100.36:3185
<30>Jul 5 19:22-19:16:25 aua[4983]:
id="3005" severity="warn"
sys="System" sub="auth"
name="Authentication failed"
srcip="172.16.160.210" user="admin"
caller="root" reason="Too many
failures from client IP, still
blocked for 522 seconds"
<54>Jul 5 17:17:43 SymantecServer
SEP-PROD: Virus found,IP Address:
10.225.237.89,Computer name:
A4103221,Source: Real Time Scan,Risk
name: W32.Stuxnet
<177>Jul  5 14:28:16 SourceFire
snort[11311]: [1:2008859:3] ET TROJAN
Downloader Win32.Small.agoy Checkin
[Classification: A Network Trojan was
detected] [Priority: 1]: {TCP}
10.8.3.29:2094 -> 222.117.163.35:80
<30>Jul 5 19:22-19:16:20 aua[4983]:
id="3005" severity="warn"
sys="System" sub="auth"
name="Authentication failed"
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: Trojan.Zbot.B
<177>Jul  5 14:18:53 SourceFire
snort[10340]: [1:2007933:3] ET
EXPLOIT Windows VBScript Engine
Remote Code Execution Vulnerability
(CVE-2018-8174) [Classification: Misc
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: W32.Blaster.Worm
<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“
<54>Jul 5 15:00:25 SymantecServer
SEP-PROD: Virus found,IP Address:
10.34.21.5,Computer name: rf7335175-
pc,Source: Real Time Scan,Risk name:
ZeuS Bot Miner
<177>Jul  5 14:29:00 SourceFire
snort[3519]: [1:2500043:1513] ET
COMPROMISED Known Compromised or
Hostile Host Traffic (22)
[Classification: Misc Attack]
[Priority: 1]: {TCP}
212.27.149.250:80 ->
10.202.100.36:3185
<30>Jul 5 09:22-09:16:25 aua[4983]:
id="3005" severity="warn"
sys="System" sub="auth"
name="Authentication failed"
srcip="172.16.120.210" user=“Master"
caller="root" reason="Too many
failures from client IP, still
blocked for 422 seconds"
<54>Jul 5 17:17:43 SymantecServer
SEP-PROD: Virus found,IP Address:
10.215.227.89,Computer name:
w4103251,Source: Real Time Scan,Risk
name: Keylogger.Misc
<177>Jul  5 14:28:16 SourceFire
snort[11311]: [1:2008859:3] ET TROJAN
Downloader Win32.Backdoor.Rat Checkin
[Classification: A Network Trojan was
detected] [Priority: 1]: {TCP}
10.8.3.29:2094 -> 222.117.163.35:80
<30>Jul 5 09:22-09:16:20 aua[4983]:
id="3005" severity="warn"
sys="System" sub="auth"
name="Authentication failed"
srcip="172.16.160.210" user=“user"
caller="root" reason="Too many
failures from client IP, still
blocked for 1004 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.RAT.DDoSBot!Win32
<177>Jul  5 14:18:53 SourceFire
snort[10340]: [1:2007933:3] ET
EXPLOIT SQL Server Heap Overflow
Vulnerability [Classification: Misc
Attack] [Priority: 2]: {TCP}
72.216.94.42:80 -> 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: Trojan.Zbot!gen1
<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"
<54>Jul 5 15:00:25 SymantecServer
SEP-PROD: Virus found,IP Address:
10.4.1.5,Computer name: af7305175-
pc,Source: Real Time Scan,Risk name:
Ransom.Wannacry
<177>Jul  5 14:29:00 SourceFire
snort[3519]: [1:2500043:1513] ET
COMPROMISED Known Compromised or
Hostile Host Traffic (22)
[Classification: Threat Intelligence
- C2 Communication] [Priority: 2]:
{TCP} 202.87.149.250:80 ->
10.202.100.36:3185
<30>Jul 5 19:22-19:16:25 aua[4983]:
```

Document Information

Document Audience

This a document written for the Cyber Security Threat Detection community.

Document Purpose

This document describes the “SPEED use case framework”, it describes Framework’s principles, use case categories and naming conventions.

Revision History

Version(s)	Date	Status	Revised by	Comments
0.1	*15-04-2020*	*Draft*	*Jurgen Visser*	*Initial Draft*
1.0	**23-04-2020**	**Final**	**Jurgen Visser**	**Final version**

Where significant changes are made to this document, the version number will be incremented by 1.0. Where changes are made for clarity and reading ease only and no change is made to the meaning or intention of this document, the version number will be increased by 0.1

Executive Summary

What is a Use Case Framework?

A Use Case Framework is an analytical tool that has a series of cyber security related distinctions which are translated into a directory structure (or categories) that facilitate the organization of cyber security detection rules. The objective of building a Use Case Framework is to better protect the organization's valuable assets by designing and developing detection use cases using a holistic approach that connects (with always newly emerging) regulatory, compliance and threat requirements. The framework provides more granular control over its detection coverage and ongoing development.

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 are the Key "SPEED Use Case Framework" differentiators?

A. Vendor neutral
B. Separate from the Use Case Lifecycle Management.
C. Agile and Flexible (can be changed later-on)
D. Simple and clear by design.
E. Addresses Qualitative and Quantitative Threat modelling requirements from the Cyber Threat Intelligence (CTI) team.
F. Specific Naming conventions allowing easier integration with SOAR Playbook categorizations.

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 modeling using the kill-chain
- Location for threat modeling threat actors like "North Korea" 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

What Can I do to implement the SPEED Use Case Framework?

1. Initial SIEM installation (or existing SIEM installation)
2. Disable All Rules (or disable those who you don't actively use)
3. Structure Rule Directories
4. Determine Implementation Criteria and a Use Case Framework
5. Start implementing and migrating out-of-the-box Use cases to a chosen Use Case Framework with corresponding implementation criteria.

Table of Contents

1. Overview

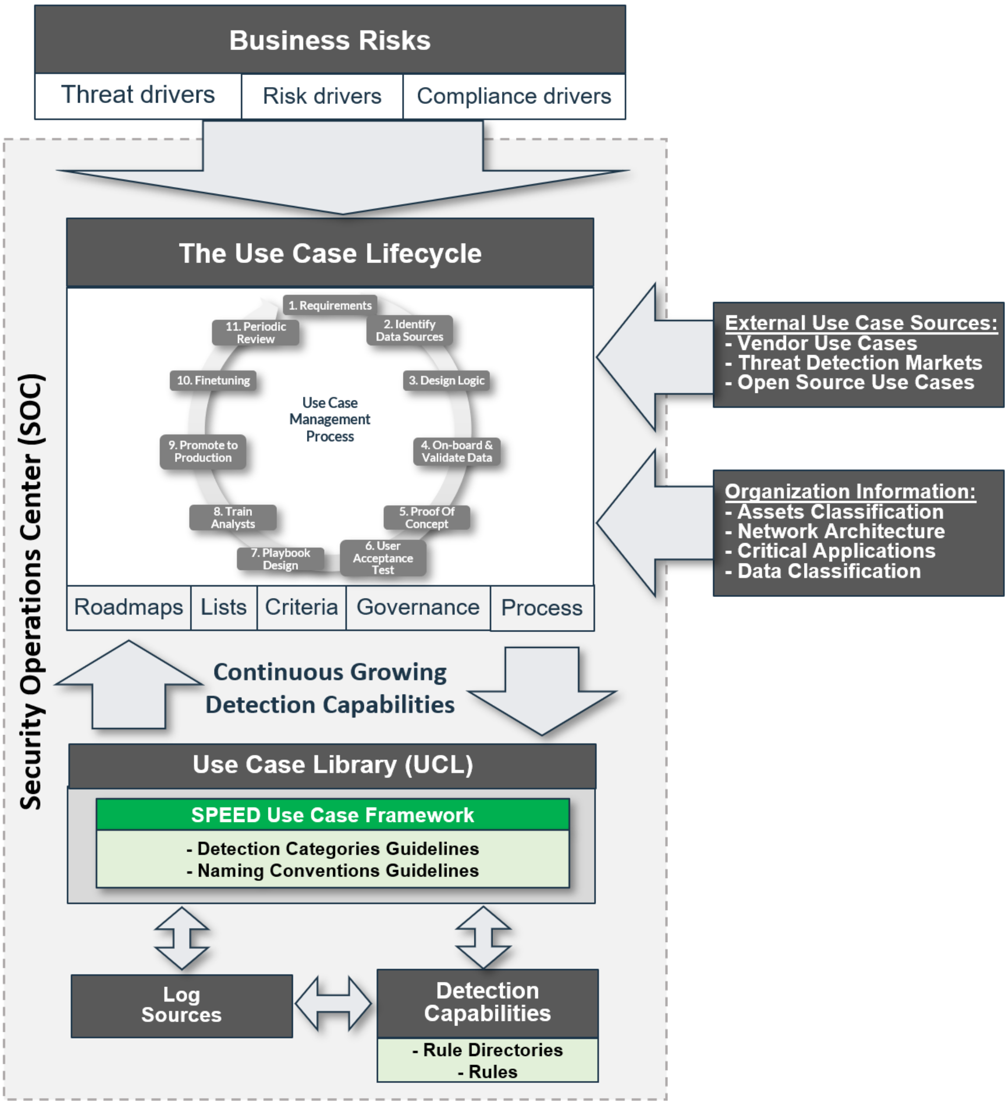
This chapter will describe a high-level overview of the context where the SPEED Use Case Framework sits in.

1.1 What is a Use Case Framework?

A Use Case Framework is an analytical tool that has a series of cyber security related distinctions which are translated into a directory structure (or categories) that facilitate the organization of cyber security detection rules. The objective of building a Use Case Framework is to better protect the organization's valuable assets by designing and developing detection use cases using a holistic approach that connects (with always newly emerging) regulatory, compliance and threat requirements. The framework provides more granular control over its detection coverage and ongoing development.

1.2 In which context does a Use Case Framework sit?

The following model shows where the Framework sits in the SOC organization in **GREEN**.



1.3 What is it NOT?

There are other SIEM Use Case Framework's that go beyond the rule structure and into Use Case Lifecycle Management and beyond. This Lifecycle includes for example:

- Use Case Management Process
- Use Case Roadmap
- Use Case Governance Structure
- Metrics for measuring Use Case Performance
- Rule priority List
- Acceptation Criteria for Use Cases to be promoted to Production

The SPEED Use Case Framework document **will NOT** cover these items (keep it simple!).

1.4 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).

1.5 What are the Key differentiators?

What are the key differentiators compared to other Use Case Frameworks? The SPEED Use Case Framework is primarily designed to be:

A. Vendor neutral
B. Separate from the Use Case Lifecycle Management.
C. Agile and Flexible (can be changed later-on)
D. Simple and clear by design.
E. Addresses Qualitative and Quantitative Threat modelling requirements from the Cyber Threat Intelligence (CTI) team.
F. Specific Naming conventions allowing easier integration with SOAR Playbook categorizations.

1.6 What does the SPEED Use Case Framework Consist of?

1. **The Risk and Threat Fundamentals** – Where the Use Case Approach will be based on.
2. **The Framework Approach** – Decisions on the framework structure.
3. **Use Case Framework** – The structure how the use cases will be categorized.
4. **Directory Structure and naming** conventions – for organizing use cases.
5. **Use Case Description Templates** – for documenting the use cases and procedures.

1.7 Added value by the SPEED Use Case Framework

- Clear Location for log source monitoring use cases
- Location for generic Threat actor Threat modeling using the kill-chain
- Location for threat modeling threat actors like "North Korea" 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

2. The SIEM “Detection” Problem Statement

This chapter outlines some problems with most SIEM’s.

2.1 Problem Statement

1. **No room for threat modeling**

Some Use Case Frameworks do not leave room for threat modelling on specific threat actors and external threat intelligence sources.

2. **No distinction between external and internal threats**

Some Use Case Frameworks does not make a distinction between internal threats vs. external threats.

3. **Out-of-the-box SIEM use cases are split-up while covering same scope.**

Most SIEM out-of-the-box **use cases are split up** from each other based on their rule content package which can be put (after some analysis of the detection logic) under the same "use case" as they have the same detection scope.

4. **No naming conventions or pre-determined directory structure**

Most SIEM out-of-the-box (and later custom added rules) **do not have an overarching naming convention over all rules**.

5. **Most use case approaches have an Attack-centric or quantitative detection bias**

Most SIEM Vendors have attempted to organize use cases in a Use Case Framework that primarily focuses on a single limited threat model (kill chain or ATT&CK Framework) this misses critical categories like Self-monitoring, localized anomaly detection (that is not attack-centric) and distinctions between quantitative threat modeling and qualitative threat modeling. This as a result will create a attack-centric and quantitative threat detection bias.

6. **Use Cases are hard to align with a SOAR playbooks platform without a framework**

Most SIEM vendors fail to accommodate the emergence of SOAR technologies that are trying to connect automated or semi-automated playbooks to SIEM use cases. Without a proper organized rule set according some form of framework mapping use cases to playbooks becomes increasingly challenging.

7. **SIEM Vendor Taxonomy overly complex or not generalizable**

Many SIEM vendors have attempted to standardize detection through taxonomy of detection categories but these categories are generally limited only to the SIEM vendor itself and hard to generalize to other detection technologies of other vendors like IDS, IPS, UBA and others.

3. Starting with a “clean Detection field”

This chapter proposes a simple approach to try to tackle the basic problems with messy out of the box rules and content made later on the usage of a SIEM solution.

3.1 How to start with a “Clean a Detection field”

The approach for delivering Use Cases to the organization in the best and effective way is to **start from zero**. This means **all out of-the-box rules will be disabled**. Followed by implementing bit by bit new use cases and documenting them.

If the SIEM has been in use for a while already, the rules can remain active, but temporarily moved to a “unorganized” folder within the SIEM. After this these rules can be migrated over to the new implementation rules and use case framework.

1. **Initial SIEM installation (or existing SIEM installation)**
   a. Initially there will be tons of out of the box rules in the system that will trigger continuously.
2. **Disable All Rules (or disable those who you don’t actively use)**
   a. All these rules will be initially disabled.
3. **Structure Rule Directories**
   a. On a high level implement the following directory structure:

Rule Directory Structure	Description
0. Disabled	Disabled out of the box content (rules and reports)
1. Development	Use Cases that are enabled for testing.
2. System	Host definitions, Key Building Blocks, Active lists, Session Lists, Lookup Tables etc.
3. Production	Rules and Use cases in production, this directory structure is filled in with the **Use Case Framework**
4. Apps	Rule packs put in by Apps or other external continuously updated imported content.

4. **Determine Implementation Criteria and a Use Case Framework**
   a. A list of requirements need to be determined before a rule can move from “2. Development” into “3. production”
   b. A Use case framework with a directory structure within “3. Production” and it’s naming conventions should be decided on.
5. **Start implementing and migrating out-of-the-box Use cases to a chosen Use Case Framework.**
   a. The Use Case Developer will start implementing and migrating existing rules into the newly determined Implementation criteria and Use Case Framework.

4. Risk and Threat Fundamentals

This chapter outlines the principles and distinctions the framework is built upon.

4.1 Overview

This Use Case Framework comprises of a framework approach, a framework model, directory structure and naming conventions and a list of use cases organized in a structured way. A Use Case Framework tackles the problem of "deciding where to focus on and on what time in a complex cyber security environment". Most organizations tend to deal on an ad-hoc basis of building use cases without any reference framework or train of thought. This introduces risks to the organization since their SOC is not properly being guided in an effective way. This Use Case framework allows for strategic and effective decision making when dealing in developing and implementing new use cases for the Security Operations Center (SOC).

This Use Case Framework consists of:

1. **The Risk and Threat Fundamentals -** where the Use Case Approach will be based on
2. **The Framework Approach** – how the framework will be decided on
3. **The SPEED use case framework** – the structure how the use cases will be categorized
4. **The SPEED use case framework categories and naming conventions** – the practical aspects
5. **The SPEED use case framework templates** – for documenting the use cases and procedures

These use case framework components are described in the various chapters followed. To decide on the right framework approach, we first need to state a set of distinctions and principles where this framework will be built on.

4.2 The Pareto Principle

The Pareto principle (also known as the 80/20 rule, the law of the vital few, or the principle of factor sparsity) states that, for many events, roughly 80% of the effects come from 20% of the causes. For Use Case selections, we recommend on focusing on the 20% of the use cases that cover 80% of the risks in the threat landscape. This should be the main guideline for deciding on this use cases to implement.

4.3 The KISS Principle

KISS is an acronym for "keep it simple and straightforward" as a design principle noted by the U.S. Navy in 1960. The KISS principle states that most systems work best if they are kept simple rather than made complicated; therefore, simplicity should be a key goal in design and unnecessary complexity should be avoided. The phrase has been associated with aircraft engineer Kelly Johnson (1910–1990).

4.4 Generalizable quality across other detection devices

The goal is to have a framework that primary focus is to maintain and manage detective counter measures in the form of use cases, across devices like IDS, IPS, EDR , SIEM etc.

4.5 Including room for "Threat Modelling"

Internal Threat Modelling is based on the notion that any enterprise has assets of value worth protecting. These assets have certain vulnerabilities, and internal or external threats exploit these vulnerabilities in order to cause damage to the assets, and appropriate security controls exist that mitigate the threats.

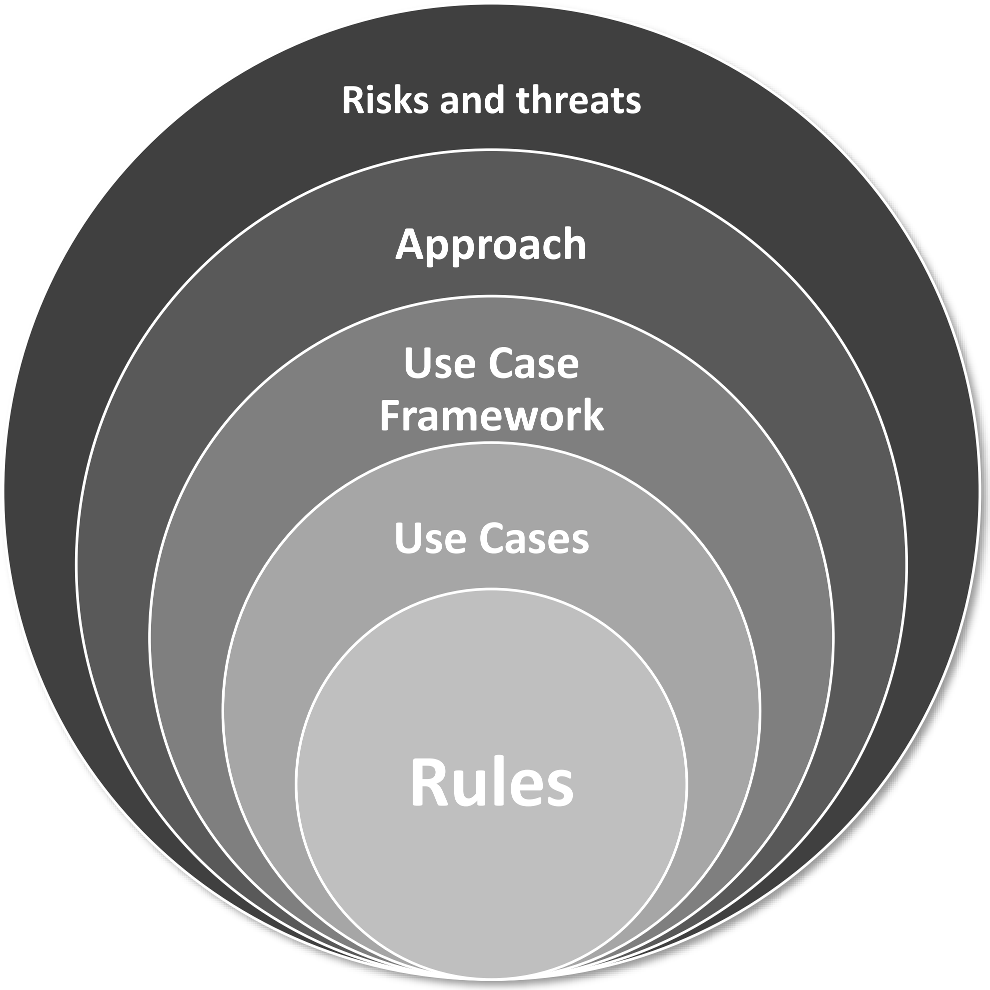
External Threat Modelling studies the global cyber threat landscape and emerging trends, and the Threat Intelligence feeds for any emerging threats and zero-day vulnerabilities; in addition, it analyses the threats specific to any organization's industry and its network environment, the vulnerabilities exist on the any organization's network devices and systems, and security controls in place. Based on the outcomes of the threat modelling, use cases will be developed.

4.6 Room for "Self-Monitoring"

Every SIEM system should have some controls in place to detect when a log source is not sending any logs and should be taken action on. This on its self will present itself as a use case category in the Use case framework.

4.7 Key Distinctions: Risks and threats, Approach, Use Case Framework, Use Cases, Rules

The model below shows the important distinctions made following the highest abstract from of a risk or a threat. Where this is made a decision on a approach and followed-up with a use case framework that is filled with use cases per category inside the framework. Within every use case there will be room for multiple rules which eventually is the detective control on the threat landscape.



5.The Framework Approach

The Use Case Framework can be approach through many different approaches. Here we summaries different approaches and choose one with the complementing arguments.

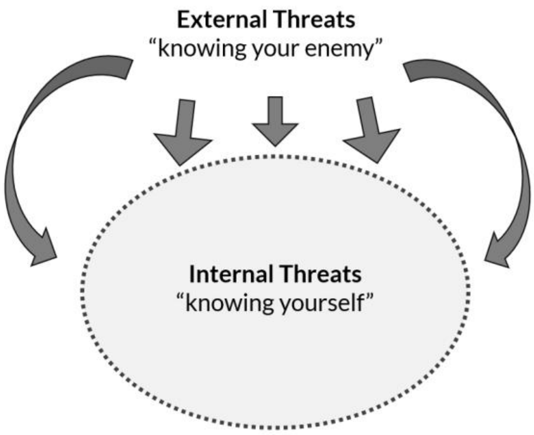
1. **The Risk Analysis approach** is essentially a top-down approach which studies how a threat or an attack enters an enterprise environment and bases on the flow of a threat or an attack to design use cases to detect these threats or attacks.
2. **The Data Source Analysis approach** is a bottom-up approach which studies the security events or activity logs on the data sources and designs use cases to look for the potential threats which might exist in the environment.
3. **The Compliance approach** studies the regulatory or compliance requirements of the enterprise and bases on the requirements to design use cases to achieve the goal of regulatory compliance. It is a middle-out approach which works up to the top for risk analysis and down to the bottom for data source analysis as per the regulatory or compliance requirements.
4. **The Customized approach** uses an existing known threats modeling models as a base and template, then customize it into a preferred form or shape to the requirements of the Use Case framework designer.

5.1 Key Approach Decision

This document is intended to create a KISS and 80/20 principle-based framework for use cases. Therefor it’s chosen to take the **Customized approach** which allows the use case framework to be stripped to the essence and use other inputs from existing risk analysis, requirements or other stakeholders be fed into this framework in order to have an 80/20 principle-based use case implementation process take place.

5.2 External Threat vs. Internal Threats

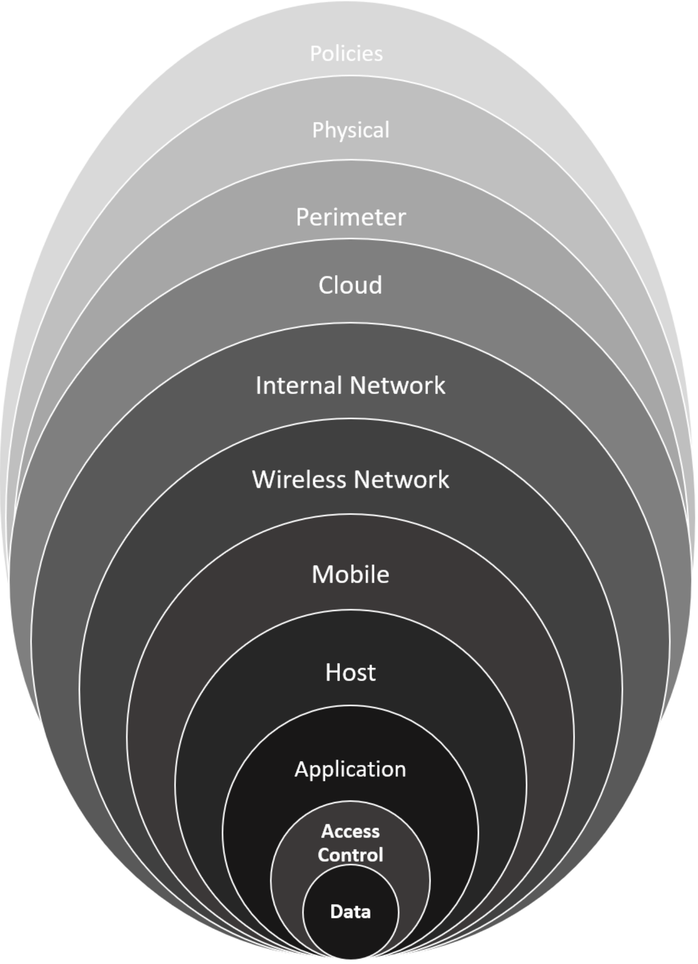
All a Use Case or rule does is model a threat or a certain risk inside the organization this can be either an external threat or an internal threat. Based on this principle model the rest of the use case framework will be derived more in depth later. External threats can be seen as attackers and internal threats as insider threats or user misconduct. These two categories can span very wide in terms of risks and threats. In order to derive a form of categorization later on from this model we need two models to further specificy internal and external threats more specifically.



5.3 **Internal Threats:** The Security Onion Model

The security onion model allows for a more detailed defense in depth view of the internal infrastructure. The many distinctions will act as categories later on in the framework in order to connect use cases on these categories.

Policies
GDPR, PCI DSS, ISO27001, Law and Industry regulation etc.
Physical
Badge scanners, Security Camera's, fingerprint scanners etc.
Perimeter
Firewalls, Anti-DDoS, VPN solutions etc,
Cloud
AWS, GCP, Azure, IBM Cloud etc.
Internal Network
Proxy, DNS, NTP, IPS, Load Balancers etc.
Wireless Network
Wireless Controllers, AccessPoint's etc.
Mobile
MDM, Apps, Android, IOS, etc.
Host
Windows, Linux, Mac OS X etc.
Application
Databases, Applications, Micro Services etc.
Access Control
Identity and Access Management, Soft/Hard Token, 2FA, etc
Data
The data you are trying to protect.



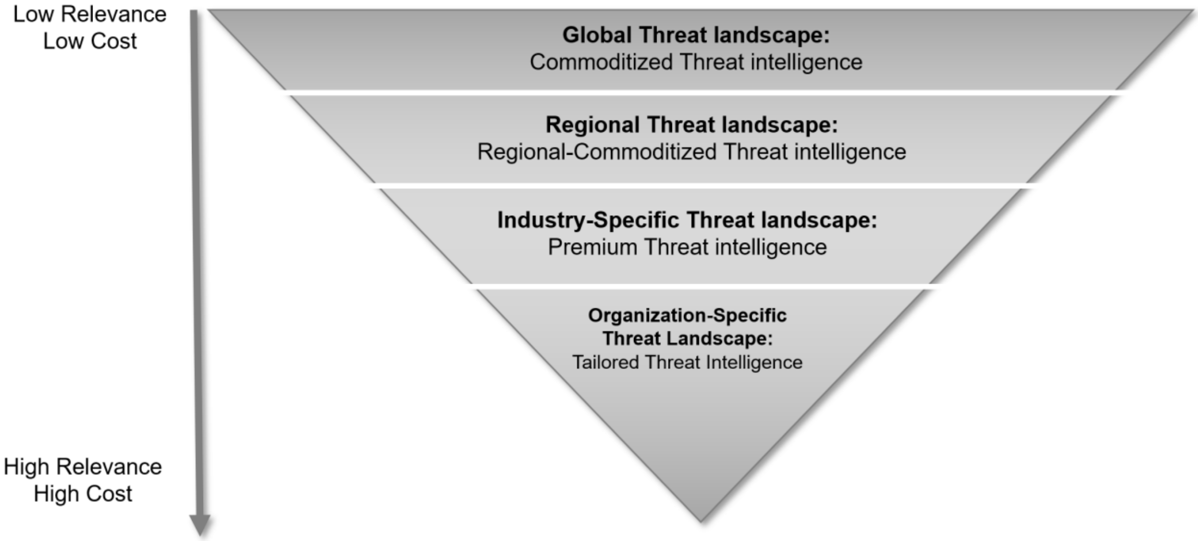
5.4 **External Threats:** Quantitative vs. Qualitative Threat Modeling

In order to deal with external threats there needs to be made a distinction in terms of **qualitative approach** (based on specific threat profile of an attacker) vs. a **quantitative threat profile** (a list of bad ip's associated with attackers, also known as quantitative threat intelligence).

5.5 **External Threats:** Quantitative threat model – Threat intelligence

A Quantitative threat model generally comes in with basic IOC's automatically that detection rules to automatically detects threats within a detection system. These can be put in four major categories:

1. **Commoditized Threat Intelligence**
   a. Global Threat intelligence OSINT feeds or paid feeds that cover the global threat landscape.
2. **Regional Threat Intelligence**
   a. Geographical or country specific threat intelligence provided by CIRTS or specific regional threat intelligence organizations.
3. **Industry-specific Threat Intelligence**
   a. Mostly provided by industry specific threat intelligence players providing threats to that specific industry.
4. **Tailored Threat intelligence**
   a. Your own honeypots or specific premium provider subscriptions.


Low Relevance
Low Cost
Global Threat landscape:
Commoditized Threat intelligence
Regional Threat landscape:
Regional-Commoditized Threat intelligence
Industry-Specific Threat landscape:
Premium Threat intelligence
Organization-Specific
Threat Landscape:
Tailored Threat Intelligence
High Relevance
High Cost

5.6 **External Threats:** Quantitative threat model – Attacker Patterns

Attack Patterns is a category based on general known attack patterns that do not relate to any specific attacker profile (threat model). These patterns rely heavily on the categorization of events inside a SIEM. For example, a "failed login" may relate to a Windows System, Network Device or Database. If the SIEM is capable of using proper categorization on all of these events across all types of devices then a use case like "brute force detected" can be created as a general attack pattern use case. Therefor this use case category is created to have general attack patterns to a generally known attacker profile based off generic event categorizations.

These generally known attacker profiles are mapped to four main archetypes that function as symbol of a general attacker style ranging from low sophistication to high sophistication and a symbolic attack style that shows a distinctive attack style.

Insider Threat	Script Kiddie	Cyber Criminal	Nation State
Motivation: Revenge, Disgruntled, Monetary Gain, Fault, Unintentional Mistake **Sophistication:** Low to high	**Motivation:** Activism, Notoriety, Nuisance, Curiosity, Advertising **Sophistication:** Low – Portscan	**Motivation:** Monetary Gain, Organized Crime, Spamming **Sophistication:** Medium – Ransomware	**Motivation:** Economic Espionage, Cyber Warfare, Geopolitical Motives **Sophistication:** High – APT

5.7 **External Threats:** Qualitative threat model – MITRE ATT&CK

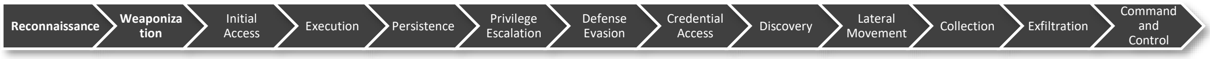
The MITRE ATT&CK™ framework is a comprehensive matrix of tactics and techniques used by threat hunters, red teamers, and defenders to better classify attacks and assess an organization's risk.

The aim of the framework is to improve post-compromise detection of adversaries in enterprises by illustrating the actions an attacker may have taken. How did the attacker get in? How are they moving around? The knowledge base is designed to help answer those questions that while contributing to the awareness of an organization's security posture at the perimeter and beyond. Organizations can use the framework to identify holes in defences, and prioritize them based on risk.

There are two parts of the framework:

1. PRE-ATT&CK
2. Enterprise ATT&CK

The PRE-ATT&CK model is kept at a high level (recon and weaponize) due to the fact that we are not monitoring the attacker's network in detail. Therefore, it's decided to keep it simple and only use the two main categories. Resulting in the following:



This model will be used for Quantitative and Qualitative threat models within the SPEED Use Case Framework.

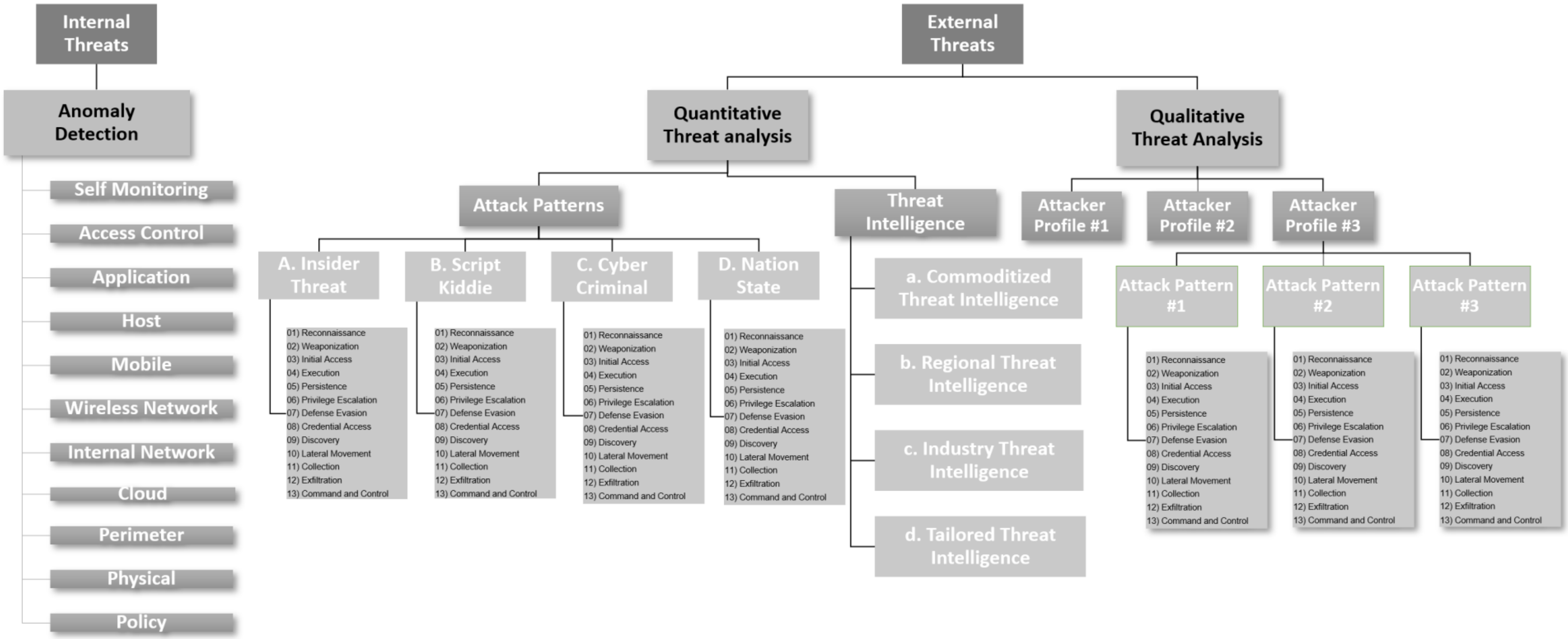
6. The SPEED use case framework

The Use Case Framework is derived from the previously proposed models and principles. This chapter will unify all these inputs into one single framework.

6.1 SPEED use case framework

The following model shows the unified version based on the previous distinctions and models.

Please see next page for full image.


Internal Threats
Anomaly Detection
Self Monitoring
Access Control
Application
Host
Mobile
Wireless Network
Internal Network
Cloud
Perimeter
Physical
Policy
External Threats
Quantitative Threat analysis
Attack Patterns
A. Insider Threat
01) Reconnaissance
02) Weaponization
03) Initial Access
04) Execution
05) Persistence
06) Privilege Escalation
07) Defense Evasion
08) Credential Access
09) Discovery
10) Lateral Movement
11) Collection
12) Exfiltration
13) Command and Control
B. Script Kiddie
01) Reconnaissance
02) Weaponization
03) Initial Access
04) Execution
05) Persistence
06) Privilege Escalation
07) Defense Evasion
08) Credential Access
09) Discovery
10) Lateral Movement
11) Collection
12) Exfiltration
13) Command and Control
C. Cyber Criminal
01) Reconnaissance
02) Weaponization
03) Initial Access
04) Execution
05) Persistence
06) Privilege Escalation
07) Defense Evasion
08) Credential Access
09) Discovery
10) Lateral Movement
11) Collection
12) Exfiltration
13) Command and Control
D. Nation State
01) Reconnaissance
02) Weaponization
03) Initial Access
04) Execution
05) Persistence
06) Privilege Escalation
07) Defense Evasion
08) Credential Access
09) Discovery
10) Lateral Movement
11) Collection
12) Exfiltration
13) Command and Control
Threat Intelligence
a. Commoditized Threat Intelligence
b. Regional Threat Intelligence
c. Industry Threat Intelligence
d. Tailored Threat Intelligence
Qualitative Threat Analysis
Attacker Profile #1
Attacker Profile #2
Attacker Profile #3
Attack Pattern #1
01) Reconnaissance
02) Weaponization
03) Initial Access
04) Execution
05) Persistence
06) Privilege Escalation
07) Defense Evasion
08) Credential Access
09) Discovery
10) Lateral Movement
11) Collection
12) Exfiltration
13) Command and Control
Attack Pattern #2
01) Reconnaissance
02) Weaponization
03) Initial Access
04) Execution
05) Persistence
06) Privilege Escalation
07) Defense Evasion
08) Credential Access
09) Discovery
10) Lateral Movement
11) Collection
12) Exfiltration
13) Command and Control
Attack Pattern #3
01) Reconnaissance
02) Weaponization
03) Initial Access
04) Execution
05) Persistence
06) Privilege Escalation
07) Defense Evasion
08) Credential Access
09) Discovery
10) Lateral Movement
11) Collection
12) Exfiltration
13) Command and Control

7. Categories and Naming Conventions

In order to make the use case Framework practical it needs to be converted into a directory structure which will be implemented in the knowledge base and in the rule structure of the SIEM solution.

7.1 SPEED use case framework Categories

This is the following directory structure proposed based on the use case framework.

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
        i. 01) Reconnaissance
        ii. 02) Weaponization
        iii. 03) Initial Access
        iv. 04) Execution
        v. 05) Persistence
        vi. 06) Privilege Escalation
        vii. 07) Defense Evasion
        viii. 08) Credential Access
        ix. 09) Discovery
        x. 10) Lateral Movement
        xi. 11) Collection
        xii. 12) Exfiltration
        xiii. 13) Command and Control
    b. Script Kiddie
        i. 01) Reconnaissance
        ii. 02) Weaponization
        iii. 03) Initial Access
        iv. 04) Execution
        v. 05) Persistence
        vi. 06) Privilege Escalation
        vii. 07) Defense Evasion
        viii. 08) Credential Access
        ix. 09) Discovery
        x. 10) Lateral Movement
        xi. 11) Collection
        xii. 12) Exfiltration
        xiii. 13) Command and Control
    c. Cyber Criminal
        i. 01) Reconnaissance
        ii. 02) Weaponization
        iii. 03) Initial Access
        iv. 04) Execution
        v. 05) Persistence
        vi. 06) Privilege Escalation
        vii. 07) Defense Evasion
        viii. 08) Credential Access
        ix. 09) Discovery
        x. 10) Lateral Movement
        xi. 11) Collection
        xii. 12) Exfiltration
        xiii. 13) Command and Control
    d. Nation State
        i. 01) Reconnaissance
        ii. 02) Weaponization
        iii. 03) Initial Access
        iv. 04) Execution
        v. 05) Persistence
        vi. 06) Privilege Escalation
        vii. 07) Defense Evasion
        viii. 08) Credential Access
        ix. 09) Discovery
        x. 10) Lateral Movement
        xi. 11) Collection
        xii. 12) Exfiltration
        xiii. 13) Command and Control
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

01) Reconnaissance
02) Weaponization
03) Initial Access
04) Execution
05) Persistence
06) Privilege Escalation
07) Defense Evasion
08) Credential Access
09) Discovery
10) Lateral Movement
11) Collection
12) Exfiltration
13) Command and Control

ii. Attack Campaign B

01) Reconnaissance
02) Weaponization
03) Initial Access
04) Execution
05) Persistence
06) Privilege Escalation
07) Defense Evasion
08) Credential Access
09) Discovery
10) Lateral Movement
11) Collection
12) Exfiltration
13) Command and Control

iii. Attack Campaign C

01) Reconnaissance
02) Weaponization
03) Initial Access
04) Execution
05) Persistence
06) Privilege Escalation
07) Defense Evasion
08) Credential Access
09) Discovery
10) Lateral Movement
11) Collection
12) Exfiltration
13) Command and Control

b. Attacker Profile name #2

i. Attack Campaign A

01) Reconnaissance
02) Weaponization
03) Initial Access
04) Execution
05) Persistence
06) Privilege Escalation
07) Defense Evasion
08) Credential Access
09) Discovery
10) Lateral Movement
11) Collection
12) Exfiltration
13) Command and Control

ii. Attack Campaign B

01) Reconnaissance
02) Weaponization
03) Initial Access
04) Execution
05) Persistence
06) Privilege Escalation
07) Defense Evasion
08) Credential Access
09) Discovery
10) Lateral Movement
11) Collection
12) Exfiltration
13) Command and Control

iii. Attack Campaign C

01) Reconnaissance
02) Weaponization
03) Initial Access
04) Execution
05) Persistence
06) Privilege Escalation
07) Defense Evasion
08) Credential Access
09) Discovery
10) Lateral Movement
11) Collection
12) Exfiltration
13) Command and Control

c. Attacker Profile name #3

i. Attack Campaign A

01) Reconnaissance
02) Weaponization
03) Initial Access

        - 04) Execution
        - 05) Persistence
        - 06) Privilege Escalation
        - 07) Defense Evasion
        - 08) Credential Access
        - 09) Discovery
        - 10) Lateral Movement
        - 11) Collection
        - 12) Exfiltration
        - 13) Command and Control
    - ii. *Attack Campaign B*
        - 01) Reconnaissance
        - 02) Weaponization
        - 03) Initial Access
        - 04) Execution
        - 05) Persistence
        - 06) Privilege Escalation
        - 07) Defense Evasion
        - 08) Credential Access
        - 09) Discovery
        - 10) Lateral Movement
        - 11) Collection
        - 12) Exfiltration
        - 13) Command and Control
    - iii. *Attack Campaign C*
        - 01) Reconnaissance
        - 02) Weaponization
        - 03) Initial Access
        - 04) Execution
        - 05) Persistence
        - 06) Privilege Escalation
        - 07) Defense Evasion
        - 08) Credential Access
        - 09) Discovery
        - 10) Lateral Movement
        - 11) Collection
        - 12) Exfiltration
        - 13) Command and Control

7.2 SPEED Use Case Framework Naming Conventions

The use case name conventions should follow the following format

- Use Case Name: (Note: the reference of the Use case category)
    - “<USE CASE NAME> Detected”

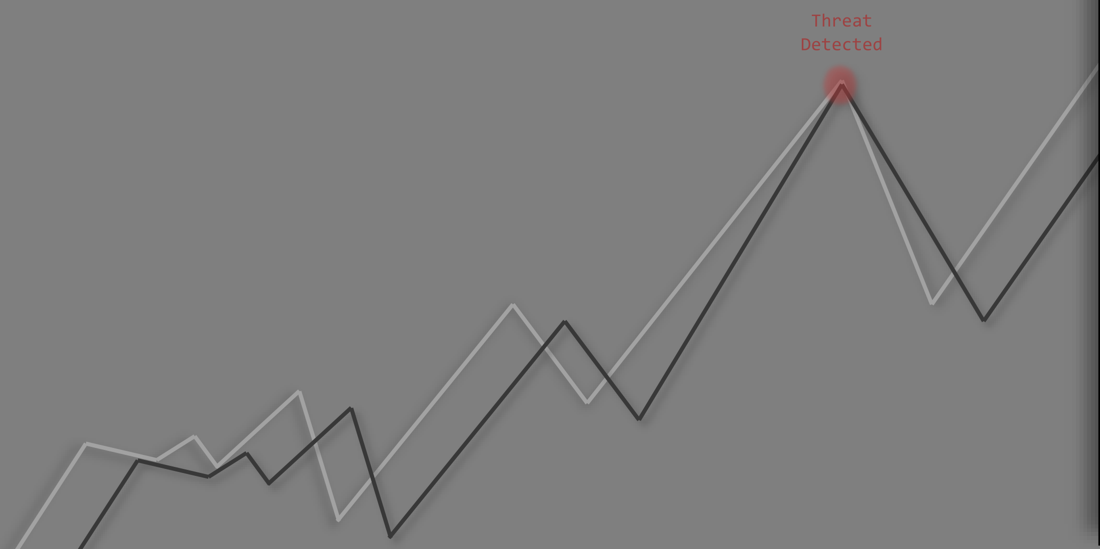
- SIEM Rule Name:
    - <USE CASE CATEGORY>**-<USE CASE>-<#> -** <SIEM RULE NAME> On <INFRASTRUCTURE VECTOR>

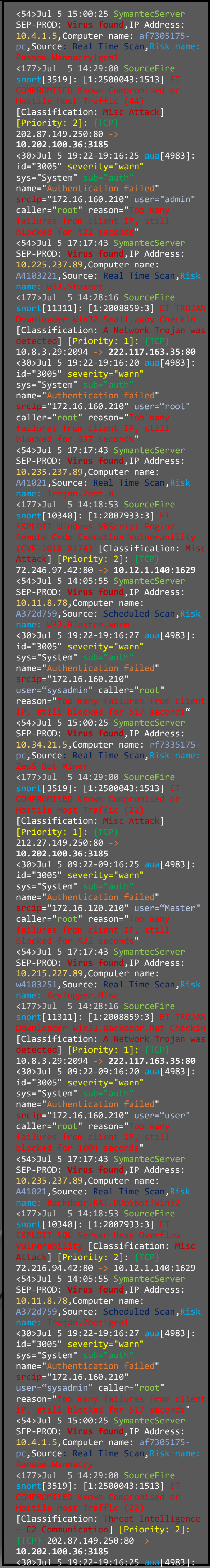
7.3 SPEED Use Case Framework Naming Conventions Example

The use case name conventions

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

Appendix

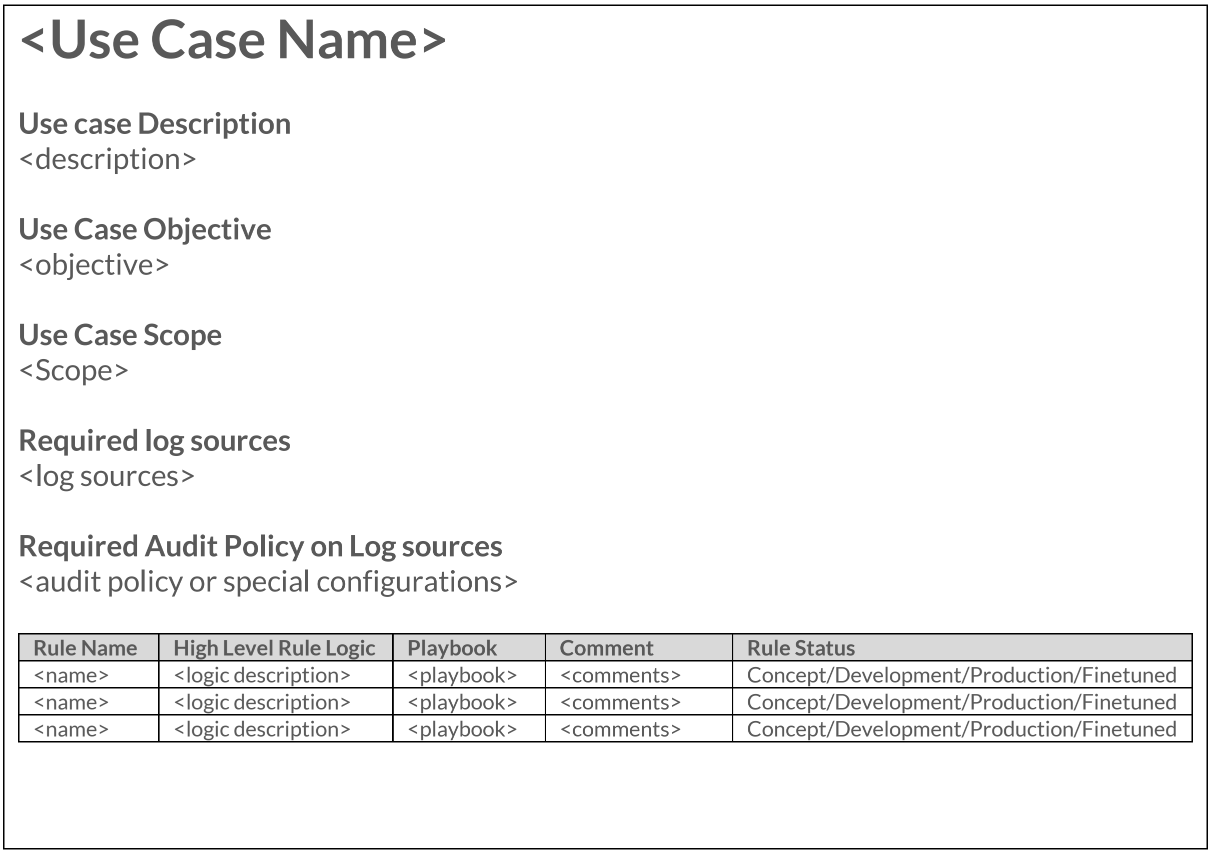




```
<54>Jul 5 15:00:25 SymantecServer
SEP-PROD: Virus found,IP Address:
10.4.1.5,Computer name: af7305175-
pc,Source: Real Time Scan,Risk name:
Ransom.Wannacry!gen1
<177>Jul  5 14:29:00 SourceFire
snort[3519]: [1:2500043:1513] ET
COMPROMISED Known Compromised or
Hostile Host Traffic (44)
[Classification: Misc Attack]
[Priority: 2]: {TCP}
202.87.149.250:80 ->
10.202.100.36:3185
<30>Jul 5 19:22-19:16:25 aua[4983]:
id="3005" severity="warn"
sys="System" sub="auth"
name="Authentication failed"
srcip="172.16.160.210" user="admin"
caller="root" reason="Too many
failures from client IP, still
blocked for 522 seconds"
<54>Jul 5 17:17:43 SymantecServer
SEP-PROD: Virus found,IP Address:
10.225.237.89,Computer name:
A4103221,Source: Real Time Scan,Risk
name: W32.Stuxnet
<177>Jul  5 14:28:16 SourceFire
snort[11311]: [1:2008859:3] ET TROJAN
Downloader Win32.Small.agoy Checkin
[Classification: A Network Trojan was
detected] [Priority: 1]: {TCP}
10.8.3.29:2094 -> 222.117.163.35:80
<30>Jul 5 19:22-19:16:20 aua[4983]:
id="3005" severity="warn"
sys="System" sub="auth"
name="Authentication failed"
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: Trojan.Zbot.B
<177>Jul  5 14:18:53 SourceFire
snort[10340]: [1:2007933:3] ET
EXPLOIT Windows VBScript Engine
Remote Code Execution Vulnerability
(CVE-2018-8174) [Classification: Misc
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: W32.Blaster.Worm
<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"
<54>Jul 5 15:00:25 SymantecServer
SEP-PROD: Virus found,IP Address:
10.34.21.5,Computer name: rf7335175-
pc,Source: Real Time Scan,Risk name:
ZeuS Bot Miner
<177>Jul  5 14:29:00 SourceFire
snort[3519]: [1:2500043:1513] ET
COMPROMISED Known Compromised or
Hostile Host Traffic (22)
[Classification: Misc Attack]
[Priority: 1]: {TCP}
212.27.149.250:80 ->
10.202.100.36:3185
<30>Jul 5 09:22-09:16:25 aua[4983]:
id="3005" severity="warn"
sys="System" sub="auth"
name="Authentication failed"
srcip="172.16.120.210" user="Master"
caller="root" reason="Too many
failures from client IP, still
blocked for 422 seconds"
<54>Jul 5 17:17:43 SymantecServer
SEP-PROD: Virus found,IP Address:
10.215.227.89,Computer name:
w4103251,Source: Real Time Scan,Risk
name: Keylogger.Misc
<177>Jul  5 14:28:16 SourceFire
snort[11311]: [1:2008859:3] ET TROJAN
Downloader Win32.Backdoor.Rat Checkin
[Classification: A Network Trojan was
detected] [Priority: 1]: {TCP}
10.8.3.29:2094 -> 222.117.163.35:80
<30>Jul 5 09:22-09:16:20 aua[4983]:
id="3005" severity="warn"
sys="System" sub="auth"
name="Authentication failed"
srcip="172.16.160.210" user="user"
caller="root" reason="Too many
failures from client IP, still
blocked for 1004 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.RAT.DDoSBot!Win32
<177>Jul  5 14:18:53 SourceFire
snort[10340]: [1:2007933:3] ET
EXPLOIT SQL Server Heap Overflow
Vulnerability [Classification: Misc
Attack] [Priority: 2]: {TCP}
72.216.94.42:80 -> 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: Trojan.Zbot!gen1
<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"
<54>Jul 5 15:00:25 SymantecServer
SEP-PROD: Virus found,IP Address:
10.4.1.5,Computer name: af7305175-
pc,Source: Real Time Scan,Risk name:
Ransom.Wannacry
<177>Jul  5 14:29:00 SourceFire
snort[3519]: [1:2500043:1513] ET
COMPROMISED Known Compromised or
Hostile Host Traffic (22)
[Classification: Threat Intelligence
- C2 Communication] [Priority: 2]:
{TCP} 202.87.149.250:80 ->
10.202.100.36:3185
<30>Jul 5 19:22-19:16:25 aua[4983]:
```

Appendix A: Use Case Documentation Template Example

For documenting use cases here is a example template provided.



<Use Case Name>

Use case Description
<description>

Use Case Objective
<objective>

Use Case Scope
<Scope>

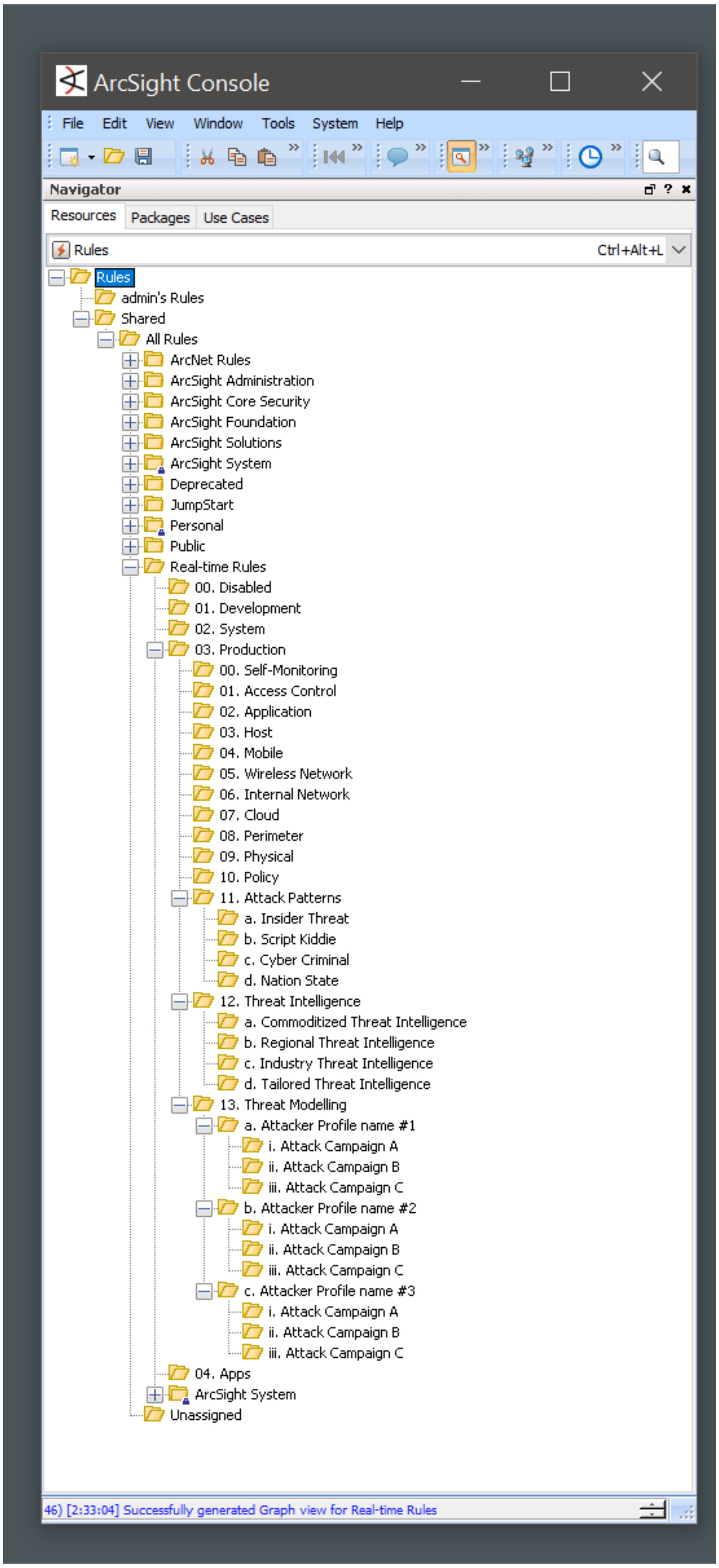
Required log sources
<log sources>

Required Audit Policy on Log sources
<audit policy or special configurations>

Rule Name	High Level Rule Logic	Playbook	Comment	Rule Status
<name>	<logic description>	<playbook>	<comments>	Concept/Development/Production/Finetuned
<name>	<logic description>	<playbook>	<comments>	Concept/Development/Production/Finetuned
<name>	<logic description>	<playbook>	<comments>	Concept/Development/Production/Finetuned

Appendix B: ArcSight SIEM Example

This is an ArcSight implementation example.

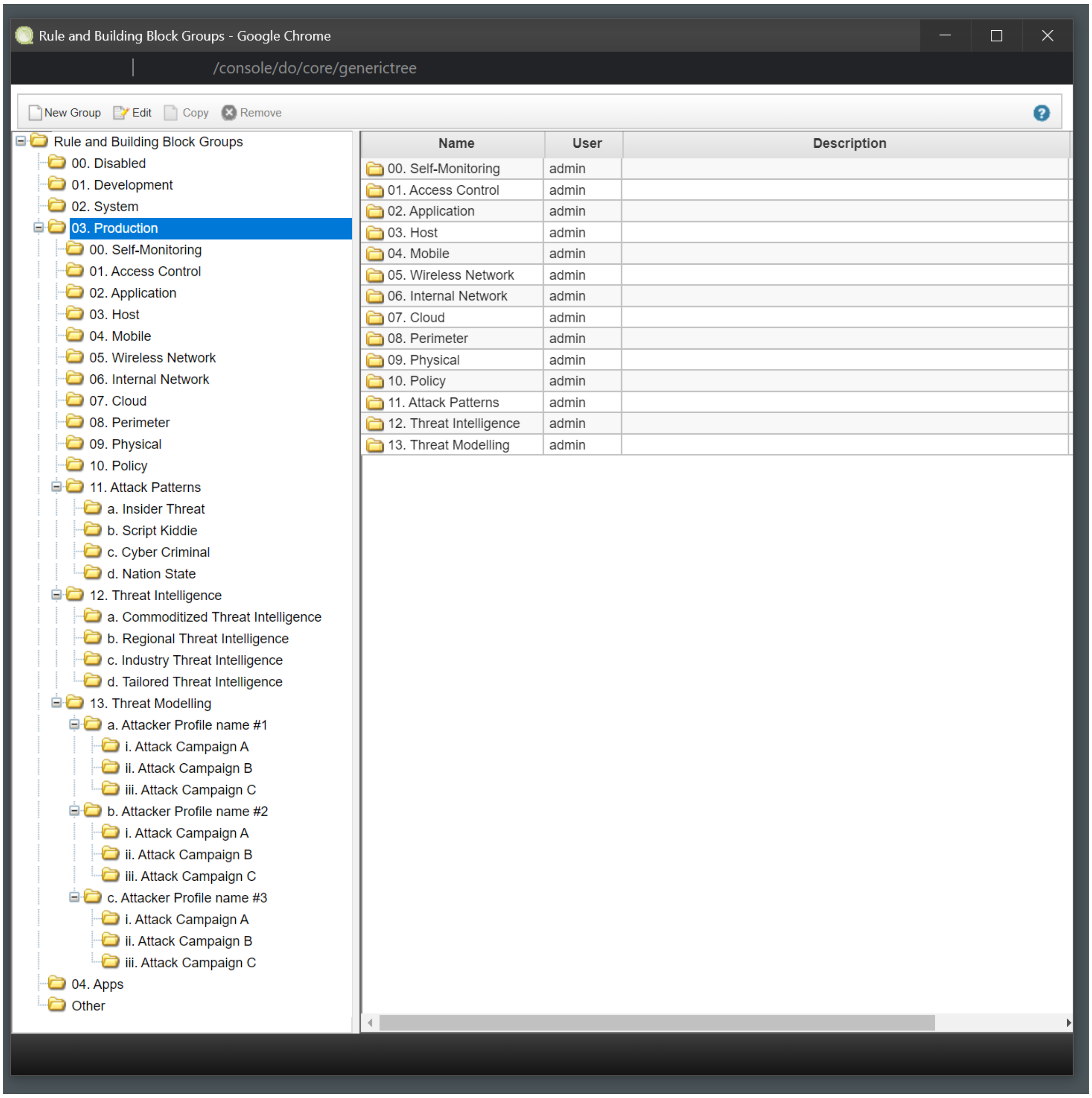


```
Rules
    admin's Rules
    Shared
        All Rules
            ArcNet Rules
            ArcSight Administration
            ArcSight Core Security
            ArcSight Foundation
            ArcSight Solutions
            ArcSight System
            Deprecated
            JumpStart
            Personal
            Public
            Real-time Rules
                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
                ArcSight System
            Unassigned
```

46) [2:33:04] Successfully generated Graph view for Real-time Rules

Appendix C: QRadar SIEM Example

This is a QRadar implementation example.

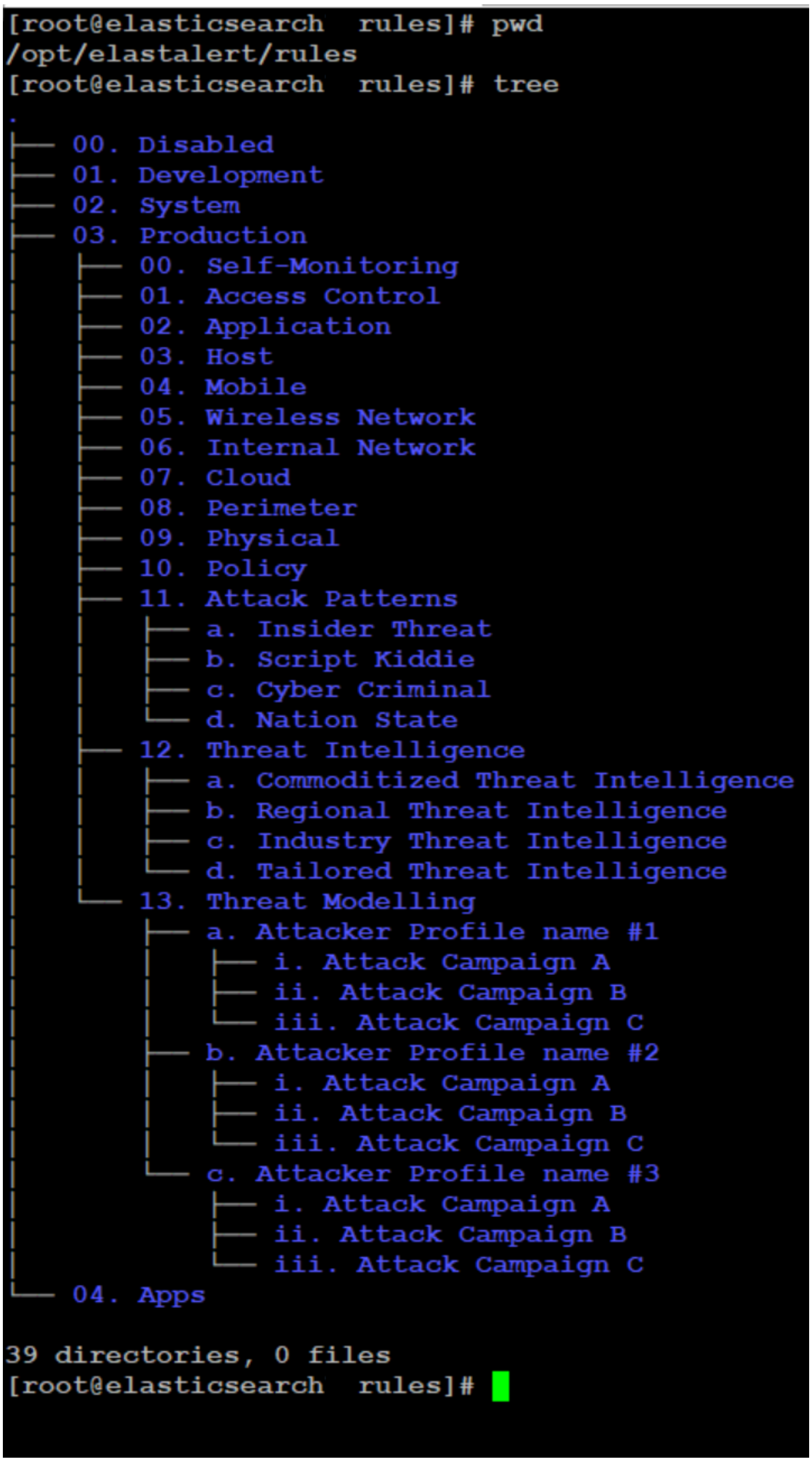


Rule and Building Block Groups - Google Chrome
/console/do/core/generictree
New Group
Edit
Copy
Remove

- Rule and Building Block Groups
  - 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
  - Other

Name	User	Description
00. Self-Monitoring	admin	
01. Access Control	admin	
02. Application	admin	
03. Host	admin	
04. Mobile	admin	
05. Wireless Network	admin	
06. Internal Network	admin	
07. Cloud	admin	
08. Perimeter	admin	
09. Physical	admin	
10. Policy	admin	
11. Attack Patterns	admin	
12. Threat Intelligence	admin	
13. Threat Modelling	admin	

Appendix D: ELK Elastalert Example



```
[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]#
```