Keeping up with the Joneses: SIEM Rules Edition
Introduction

• **Nick Ascoli**
  - Consultant - Security Risk Advisors
  - GCDA

• **Kevin Foster**
  - Manager – Security Risk Advisors
  - GCFA | GREM
Detection Challenges
A relatable story

4:45 PM
New malware is on a workstation

5:15 PM
Bad actor is on a workstation

9:30 PM
Bad actor is exfiltrating data

Days Later
Endpoint product alerts of compromise
Rule Creation: Traditional SIEM

**RULE SOURCES**
- Analyst
- Vendor

**SIEM Correlation Engine**

**Log Storage**

**SIEM Console**

- Analysis
- Alerts
# Rule Creation: Difficulties

## Knowing where you stand
- No easy way to benchmark rules based on threat profile
- Challenging to identify rule improvements

## Staying current
- Hard to stay current with emerging TTPs
- Scattered literature on collecting newer data sources

## Vendor lock in
- Most queries stored in proprietary format
- Transfer of rules requires high level of effort and time

## Endpoint hardening dependent on vendor updates
- Can take days for signature updates to reach endpoint products
- The logs are there – but you don’t have the rules for alerting
Finding Solutions
## Rule Creation: Challenges

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format for Sharing</td>
<td>?</td>
</tr>
<tr>
<td>Method of Sharing</td>
<td>?</td>
</tr>
<tr>
<td>Automated Sharing/Ingestion</td>
<td>?</td>
</tr>
</tbody>
</table>
## Rule Creation: Challenges

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format for Sharing</td>
<td><img src="https://securityriskadvisors.com/logo.png" alt="SIGMA" /></td>
</tr>
<tr>
<td>Method of Sharing</td>
<td>?</td>
</tr>
<tr>
<td>Automated Sharing/Ingestion</td>
<td>?</td>
</tr>
</tbody>
</table>
Setting the stage with Sigma

- Developed by Florian Roth and Thomas Patzke
- Generic signature format for SIEM rules
- Represented in YAML
- Growing community adoption
### Rule Creation: Challenges

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format for Sharing</td>
<td>✓ SIGMA</td>
</tr>
<tr>
<td>Method of Sharing</td>
<td>?</td>
</tr>
<tr>
<td>Automated Sharing/Ingestion</td>
<td>?</td>
</tr>
</tbody>
</table>
## Rule Creation: Challenges

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format for Sharing</td>
<td><img src="image" alt="SIGMA" /> ✔️</td>
</tr>
<tr>
<td>Method of Sharing</td>
<td><img src="image" alt="STIX TAXII" /> ✔️</td>
</tr>
<tr>
<td>Automated Sharing/Ingestion</td>
<td>?</td>
</tr>
</tbody>
</table>
Sharing via STIX / TAXII

- Maintained by OASIS CTI TC
- **Format** **STIX**
  - STIX = Structured Threat Information Expression
  - Supports creation of custom objects
- **Exchange Method** **TAXII**
  - TAXII = Trusted Automated Exchange of Intelligence Information

<table>
<thead>
<tr>
<th>STIX Domain Objects:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Actor</td>
<td>Course of Action</td>
</tr>
<tr>
<td>Campaign</td>
<td>Identity</td>
</tr>
<tr>
<td>Indicator</td>
<td>Intrusion Set</td>
</tr>
<tr>
<td>Malware</td>
<td>Observed Data</td>
</tr>
<tr>
<td>Report</td>
<td>Attack Pattern</td>
</tr>
<tr>
<td>Tool</td>
<td>Vulnerability</td>
</tr>
</tbody>
</table>
## Rule Creation: Challenges

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format for Sharing</td>
<td>![Sigma]</td>
</tr>
<tr>
<td>Method of Sharing</td>
<td>![STIX]</td>
</tr>
<tr>
<td>Automated Sharing/Ingestion</td>
<td>![TAXII]</td>
</tr>
</tbody>
</table>
## Rule Creation: Challenges

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format for Sharing</td>
<td>![Sigma Logo] (SIGMA)</td>
</tr>
<tr>
<td>Method of Sharing</td>
<td>![STIX Logo] (STIX) ![ TAXII Logo] (TAXII)</td>
</tr>
<tr>
<td>Automated Sharing/Ingestion</td>
<td>![TALR Logo] (TALR)</td>
</tr>
</tbody>
</table>
Threat Alert Logic Repository (TALR)
TALR: Introduction

What

- **Public Repo** and **TAXII server in modified sigma**
- Rules developed **internally** / collected from repos
- Organized by **ATT&CK Tactics**

Why

- **Automate** sharing and ingestion of detection rules
- **Facilitate** community **sharing** of detection logic
- Encourage threat **mapping**

Where

- SRA Github: https://github.com/SecurityRiskAdvisors/
TALR: Rule Automation Concept

Internet

TAXII Servers
- Industry
- Research
- ISAC

On-Prem Infrastructure

SIEM Correlation Engine

NEW

TAXII Servers

Pull Rules Locally
Local TAXII Client

Send Bundles
stix2sigmac

Translate Rules
Rule Logic
SIEM Architecture: Current State

RULE SOURCES

Analyst

Vendor

SIEM Correlation Engine

Rule Logic

Analysis

Alerts

Log Storage

SIEM Console
SIEM Architecture: With TALR

RULE SOURCES
- TALR
- Analyst
- Vendor

New detection rules feeding in

SIEM Correlation Engine

Log Storage

Analysis

Alerts

SIEM Console
TALR: Analyst Benefit

SIEM Console

TALR SIEM Rule Alert

Make Informed Changes

Security Infrastructure

Incident Response Team

Analyst

Actor, Campaign, Malware, Indicator

Local TAXII Client

Pull Rules Locally

Anything Related?

TALR SIEM Rule Alert

Analyst

Make Informed Changes

Actor, Campaign, Malware, Indicator

Local TAXII Client
Re-writing the story

9:00 AM
Daily bundle of new rules

4:45 PM
New malware is on a workstation

4:55 PM
SIEM rule fires on the behavior

5:30 PM
Incident Response begins
Under the Hood
Stix2sigmac Overview

1. Script Calling

```
$ ./stix2sigmac.sh import all /home/bundles/dailyBundle.json /home/siemRules/splunk none
```

Import filter  Specify locations (bundle & export)  Query syntax  Backend options

2. Script Starting

```
No output
```

Found 227 objects.

```
Checking rule 1: Hccktool_Use
This rule matches search parameters. Importing.
((EventID="4776" OR EventID="4624" OR EventID="4625") WorkstationName="RULER")
Moving to /imported/discovery/ Rule 1 complete
```

3. Script Finishing

```
Checking rule 227: Malicious_PowerShell_Keyword
This rule matches search parameters. Importing.
Moving to /imported/execuion/ Rule 227 complete
```

None! Imported 227 rules matching all out of 227 total objects.
Stix2sigmac Review

How do we use this internally?
• Improve relationship mapping between technique and detection
• Normalize and share detections agnostic of platform

Where can I find it?
• SRA Github - https://github.com/SecurityRiskAdvisors/
Extending the TALR Concept

VECTR

- Purple Teaming Tool
- Map detection logic back to red team activities

Where can I find it?

- VECTR - https://vectr.io/
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Progress</th>
<th>Outcome</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint Execution</td>
<td>Campaign</td>
<td>63%</td>
<td>38%</td>
<td>13%</td>
</tr>
<tr>
<td>External Port Scans</td>
<td>Campaign</td>
<td>33%</td>
<td>67%</td>
<td></td>
</tr>
<tr>
<td>External Web App Profiling</td>
<td>Campaign</td>
<td>33%</td>
<td>33%</td>
<td>33%</td>
</tr>
<tr>
<td>External Password Attacks</td>
<td>Campaign</td>
<td>50%</td>
<td>50%</td>
<td></td>
</tr>
<tr>
<td>External Automated Attacks</td>
<td>Campaign</td>
<td>100%</td>
<td>100%</td>
<td></td>
</tr>
<tr>
<td>Register Phishing Scans</td>
<td>Campaign</td>
<td>100%</td>
<td>100%</td>
<td></td>
</tr>
<tr>
<td>Email with Malicious Links</td>
<td>Campaign</td>
<td>100%</td>
<td>41%</td>
<td>40%</td>
</tr>
<tr>
<td>Email With Malicious Attachments</td>
<td>Campaign</td>
<td>100%</td>
<td>60%</td>
<td>40%</td>
</tr>
<tr>
<td>Client-side Attacks - Malicious Documents</td>
<td>Campaign</td>
<td>100%</td>
<td>67%</td>
<td>33%</td>
</tr>
<tr>
<td>C2 Channels</td>
<td>Campaign</td>
<td>100%</td>
<td>50%</td>
<td>50%</td>
</tr>
<tr>
<td>Persistence Methods</td>
<td>Campaign</td>
<td>100%</td>
<td>50%</td>
<td>25%</td>
</tr>
<tr>
<td>Physical Access</td>
<td>Campaign</td>
<td>100%</td>
<td>25%</td>
<td>75%</td>
</tr>
</tbody>
</table>
VECTR Overview

Test Cases

Timeline of campaign
VECTR Overview

Test Cases

Phase | Method | Test Case | Status | Outcome | Action
--- | --- | --- | --- | --- | ---
Exploitation | Trusted Windows Binary | Process Creation Using MSBuild | Completed | Not Detected | 
Exploitation | Trusted Windows Binary | PowerShell Downgrade | Completed | Not Detected | 
Exploitation | Trusted Windows Binary | Obfuscated Commands - PowerShell | Completed | Detected | 
Exploitation | Trusted Windows Binary | Process Creation Using WMI | Completed | Not Detected | 
Exploitation | Trusted Windows Binary | Process Creation Using VBS | NotPerformed | TBD | 
Exploitation | Trusted Windows Binary | Obfuscated Commands - CMD | NotPerformed | TBD | 
Exploitation | Trusted Windows Binary | Process Creation Using WMI Format Table | NotPerformed | TBD | 

Detection Status

- Not Detected: 50%
- Be Determined: 30%
- Detected: 13%
VECTR Overview
VECTR Overview

Detection Logic
VECTR Overview

Detection Logic
**Take-Aways**

- Detection rule sharing and automation is possible at scale with projects like TALR
- Sharing within the community is improving thanks to open source initiatives

**Where can I contribute?**
- Sigma - [https://github.com/Neo23x0/sigma/](https://github.com/Neo23x0/sigma/)
- STIX & TAXII - [https://oasis-open.github.io/](https://oasis-open.github.io/)
Standing on the shoulders of Giants

TALR IS MADE POSSIBLE THANKS TO:

**Sigma:** Florian Roth and Thomas Patzke

**STIX & TAXII:** MITRE and OASIS CTI TC

**SEC555:** Justin Henderson
Questions?
Thank You!