Welcome

Crypto.Banking.Simplified.

Date: June 26, 2024

Mastering the SOC Automation Journey:

'Holy Grail' or Essential for Success in Cybersecurity Operations?

In the ever-evolving landscape of cybersecurity, organizations grapple with mounting threats, overwhelming volume of alerts and incidents and resource constraints. The concept of “SOC Automation” can be considered as a critical solution.

This talk will energize security teams to assess their opportunities for automating their SOC operations and streamline incident response, mitigate alert fatigue, and maximize protection.

Join us as we explore whether SOC automation is the elusive "Holy Grail" or an indispensable path to cybersecurity success.

Agenda

1 Introduction

2 The Holy Grail of Incident Detection and Response

3 Current State of Threat Information use

4 The Need for Automation

5 Implementing Automation in a SOC

6 Conclusion

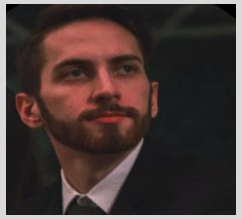
7 Questions

AMINA Bank AG

Located in Zug, Swiss (FINMA) regulated. Banking that breaks down the barriers between traditional financial services and support for digital assets.

Great success depends upon having a great team!

Shipra Verma
Senior IT Security Analyst, Identity and Security Awareness Specialist (IN)



Manuel Ricciardi
Senior IT Security Engineer, In-house pen tester and Threat Hunter (CH)

Jeff Schiemann
Chief Information Security Officer, Threat Information enthusiast (CH)

Coen Bongers
Head of IT Security, Manager of the SOC (CH)

What is our goal for today?

- Take you along our Threat Intelligence (TI) and Incident Response (IR) integration and automation journey
- Trigger your curiosity and help you start on a similar journey.
- NOT, to give you a manual on how to do this. It is your own journey!

What is Threat Information?

"Threat intelligence is evidence-based knowledge (e.g., context, mechanisms, indicators, implications and action-oriented advice) about existing or emerging menaces or hazards to assets."

– Gartner

Threat Information is a critical component of modern cybersecurity, providing valuable insights to stay ahead of cyber threats and protect digital assets.

❖ It should cover the following aspects about the threat:

- TTP's and IOC's -> How does the Adversary Operate?
- Attribution -> Who are they?
- Attacker profiles -> What are their capabilities and what is their intent?
- Attacker Information Position -> What do they know about a target, about us?

❖ It needs to be Contextual (Relevant), Timely and Actionable

❖ It should be Gathered, disseminated and applied throughout all the phases of the incident lifecycle

Protect →Detect →Respond (Triage, Contain, Investigate and Remediate) → Recover

- TTP's and IOC's → Protect and Detect
- Artefacts reputation → Respond, by Enriching for Triage and Contain
- Attribution → Investigate and Remediate
- Intent and Capabilities → Recover, Hunting and Improve Security Posture

❖ When done correctly it supports an approach of Threat Informed Defense

Threat Information Use Cases

Do what everybody else does?

Don’t be a CTI Security sheep!

Wolves thrive in crowds.

Threat Information is commonly utilized in medium-sized companies for enhancing cybersecurity measures.

Some of the more common uses are:

- **Threat Hunting:** identifying previously unknown or ongoing non-remediated threats within an organization.
- **Incident Prevention**: Identifying potential security threats and weaknesses to prevent breaches.
- **TTP Analysis**: Understanding attackers’ tactics, techniques, and procedures.
- **Security Enhancement**: Informing decision-making for better threat response.
- **Risk Management**: Analyzing current and potential attacks to safeguard digital assets.

These practices help companies proactively manage cyber risks and improve their overall security posture, but they have little to none impact on the Security Operations Center’s effectiveness in recognizing, containing and remediating dynamic threats, as break out times get lower and lower.

The Holy Grail of Incident Detection and Response

The average breakout time has decreased significantly.

In 2023, adversaries took only 62 minutes to move from an initially compromised host to another within an organization.

The fastest recorded breakout time was an astonishingly swift 2 minutes and 7 seconds.

(According to the 2024 CrowdStrike Global Threat Report)

A (close to) ideal state of Threat Information Integration and Automation for a modern SOC would involves several key components:

Automated Threat Information Ingestion:

- Gather data from various, relevant sources.
- Analyze TI Artifacts in real time.
- Prioritize threats.

Integrated with Security Operations:

- Centralize and operationalize threat Information.
- Map to Weaknesses in the environment.
- Create attack patterns and map to possible attack paths.

Automated Detection and Response:

- Detect (and respond to) threats in real time.
- Prioritize speed over accuracy
- Map to alerts & incidents in correlation to ‘MITRE ATTACK’
- Triage, Enrich, Contain and Recover automatically.

Across Incident Lifecycle:

- Prevent (Noise reduction)
- Detect (Security Operational Awareness)
- Respond (Contain over Recover)
- Learn (Adapt and Overcome)

The Need for Automation

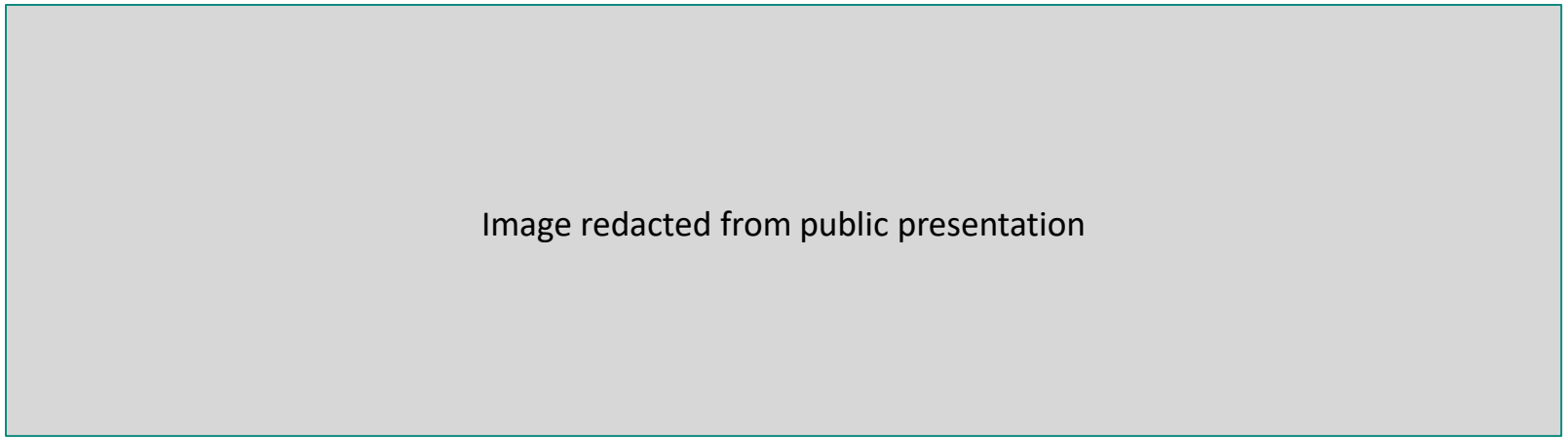
Some concepts we apply:

- *One alert is no alert.*
- *No response to Informational alerts*
- *Auto close non-actionable incidents, based on TI enrichment.*

Breakout time in cybersecurity refers to the time it takes for an intruder to move laterally from their initial point of compromise (often referred to as the “beachhead”) to other systems within a network.

It’s a critical metric because it dictates how much time an organization has to detect and contain/eject the intruder before an incident turns into a full-blown breach.
(John Boyd’s OODA loop. You need to get inside the adversary’s loop)

We believe we are inside most adversaries ‘OODA Loop’:



Implementing Automation in a (our) SOC

Everything is ‘as code’ today.

The Security Operations Center is no exception.

- **Detection as Code**
- **Response as Code**

Threat Information:

- Real time TI based enrichment is embedded in every incident triage operation. The reputation of the artifacts reported in a given incident directs the strength and the impact of the countermeasures deployed through an end-to-end integration with the underlying XDR technology. Threat Intel feeds are stored and collected continuously from paid and free sources; they are consequently matched with endpoints and user generated logs to trigger ad-hoc detections.
- Developing new detection as code, based on Threat Intelligence, as part of ‘Purple teaming’

XDR Integration:

- Automation rules and playbooks are critical components of the incident response (IR) workflow. Device and user-based IR actions are automatically deployed from a central location (SOAR) based on multiple prompt signals gathered during the triage phase, including: artifacts reputation, behavioral.
- analysis, device risk score, anomalies.

Remediation:

- Whenever applicable, user and device based self-remediating actions trigger upon incident closure. Self-remediating actions can include: device de-isolation, unblock users.

Attack Simulation:

- Execution of semi-automated attack simulation campaigns against production-like endpoints. The results of the campaigns are used to strengthen the detection capabilities, cover TTPs gaps, and improve IR automated actions and the overall workflow.

Health Checks and reporting:

- Daily health checks are sent through the main alerting mechanisms (eg: Slack, Teams) to provide the security team useful updates on threat intel news, incidents, critical IR actions, daily overview of the highlights of the previous 24 hours (incidents, IR actions, vulnerabilities, recently impacted users / devices).

Conclusion

Threat-Informed Defense requires applying a deep understanding of adversary tradecraft and technology to protect against, detect and mitigate cyber attacks.

It's a community-based approach to a worldwide challenge.

Threat Information is a critical component of modern cybersecurity, providing valuable insights to stay ahead of cyber threats and protect digital assets.

Defending at the "Speed of Threat" is very different from Defending at the "Speed of Vulnerability"

Effective application of Threat Information throughout the SOC organization is key

Use Threat Information to move faster and more effective.

Speed of Response & Respond-to-contain vs Analysis Paralysis