Security Operations Challenges in 2021

How adversarial insights and automation can keep us ahead of cyber criminals

Karl Klaessig
ServiceNow

ISACA VIRTUAL SUMMIT

Today's Speaker

Karl Klaessig

Director of Product Marketing, Security Operations
ServiceNow

Learning Objectives

- **The security challenges** our SOC and IT teams face
- **Learn how automation of workflows** can help scale your team's capacity to respond and accelerate response
- **Know the integrations** that offer your analysts insights into an attacker's profile and tactics they use
- **Gain the tracking and reporting** needed to plan effectively for team and technical resource usage and expansion

2020 in review and what we are seeing in 2021

IN 2020 WE ALL BECAME REMOTE EMPLOYEES

And opened more doors for cyber criminals

- Phishing is worse than ever
  – spam is 45%[1] of all emails sent
- Ransomware attacks grew dramatically
  – over one third more ransomware is paid out in 2020 vs 2019[1]
- What's old is new
  - as the majority of attacks utilized[1] vulnerabilities from 2017 and older!

It's estimated that digital transformation was advanced by up to seven years …*in just months*

IN 2021 REMOTE EMPLOYMENT IS STILL DOMINANT!

And the doors opened even wider for cyber criminals

- Phishing attacks comprise 80% of reported security incidents
  – ~$17,700 is lost every minute due to a phishing attack[1]

- Ransomware attacks show no sign of letting up in 2021
  – 43% increase in ransom payment in Q1 of 2021 vs Q4 2020[2]

- Global damages related to ransomware
  - could reach $6 trillion annually![3]

1 CISO Online
2 https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound
3 https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

https://t.me/learningnets

ISACA VIRTUAL SUMMIT

CHALLENGES FACING IT & SECURITY TEAMS

Inability to prioritize vulnerabilities quickly

No context

76%

of organizations have no common view of assets and applications across security and IT[1]

Few resources

#1

increased workload is the #1 reason for SOC burnout and turnover[2]

Manual and delayed incident response processes

Manual process

56%

of organizations say that things slip through the cracks because emails and spreadsheets are used to manage response processes[1]

Silos

67%

of analysts say internal battles over “who is in charge of what” are major obstacle to their SOC’s success.[2]

[1] **Source:** “COSTS AND CONSEQUENCES OF GAPS IN VULNERABILITY RESPONSE“, Ponemon Institute 2019

[2] Devo 2020 SOC Performance Report

TODAY'S SECURITY OPERATIONS TEAMS ARE IN A CONSTANT STATE OF IMPROMPTU PRIORITIZATION

And no view into adversary intent or ability to scale!

- Too many threats to address
- Not responding fast enough and often blind to attacks
- Lack of insight into attackers behavior and tactics
- **How to stop the crazy cycle?**

Let's explore how ***automated workflows and adversarial knowledge*** can transform your teams from reactionary to visionaries!

Why Automation?

WITH THESE CHALLENGES IN MIND…*How important is automation and orchestration between Security and IT teams?*

$2.5 Million Average cost of breach savings by companies with fully deployed automated security solutions[1]

Really Important! Driving Cyber Resilience and Operational Efficiencies

[1]*Source: "2019 COST of a Data Breach Report", Ponemon Institute*

Security Orchestration Automation and Response (SOAR)

- Effectively manage the evolving threats to your business
- Proactively manage exposure
- Ensure cyber resilience
- Drive efficiencies and accelerate reaction time

Common pain points demand integrated solutions

Respond faster with collaboration across teams

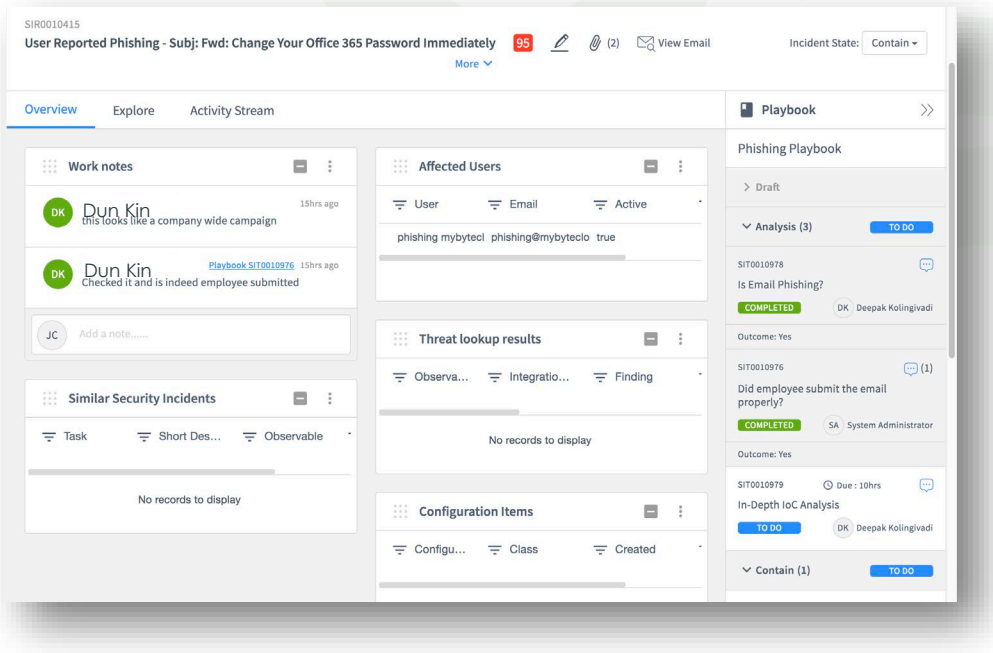
Route work seamlessly between security, and IT teams, so they can:

- **Accelerate** resolution with automated workflows
- **Automate** incident assignment
- **View** Real-time incident status and track remediation processes
- **Centralize** data and reporting

Drive accurate prioritization and Cyber Resilience

Enables repeatable and collaborative workflows that scale your teams.

- Response process and actions
- Analysts work notes
- Post Incident Reviews



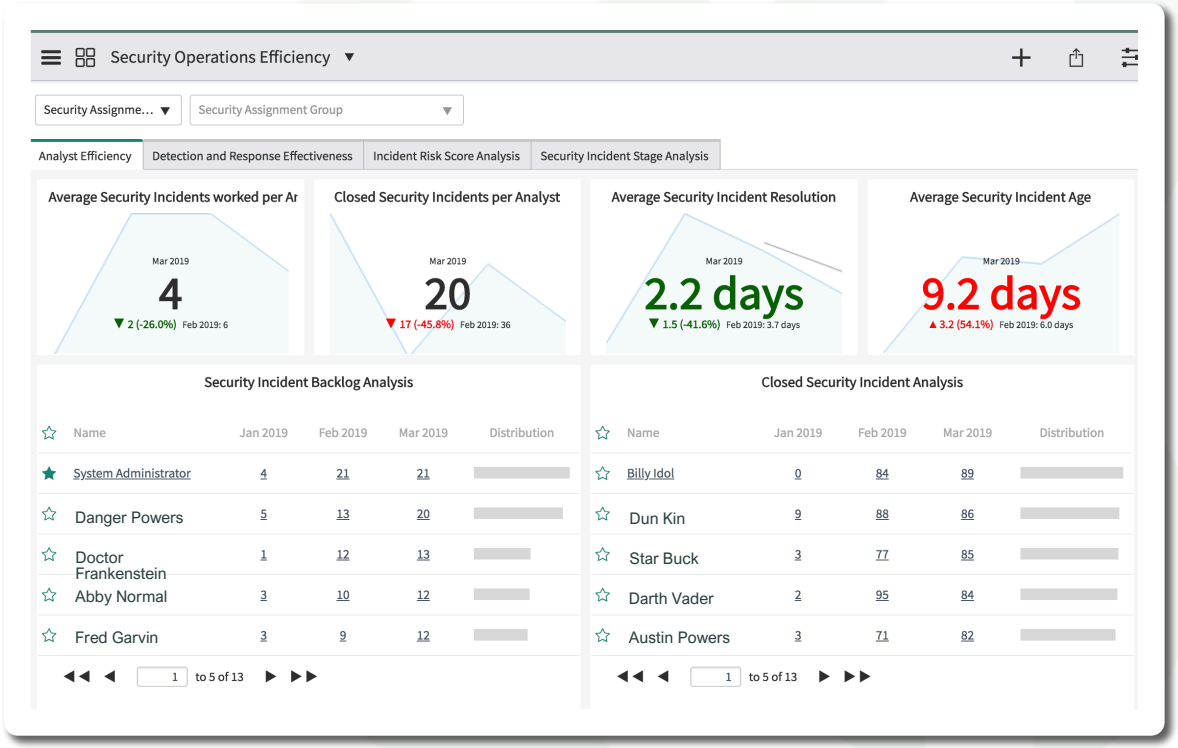
https://t.me/learningnets

ISACA VIRTUAL SUMMIT

Report, Review and Plan for Success

Know how your security team is performing.

- Develop a picture of how the SOC is performing
- Review Analyst Efficiency Metrics
- Evaluate and shape Detection and Response processes and workflows



https://t.me/learningnets

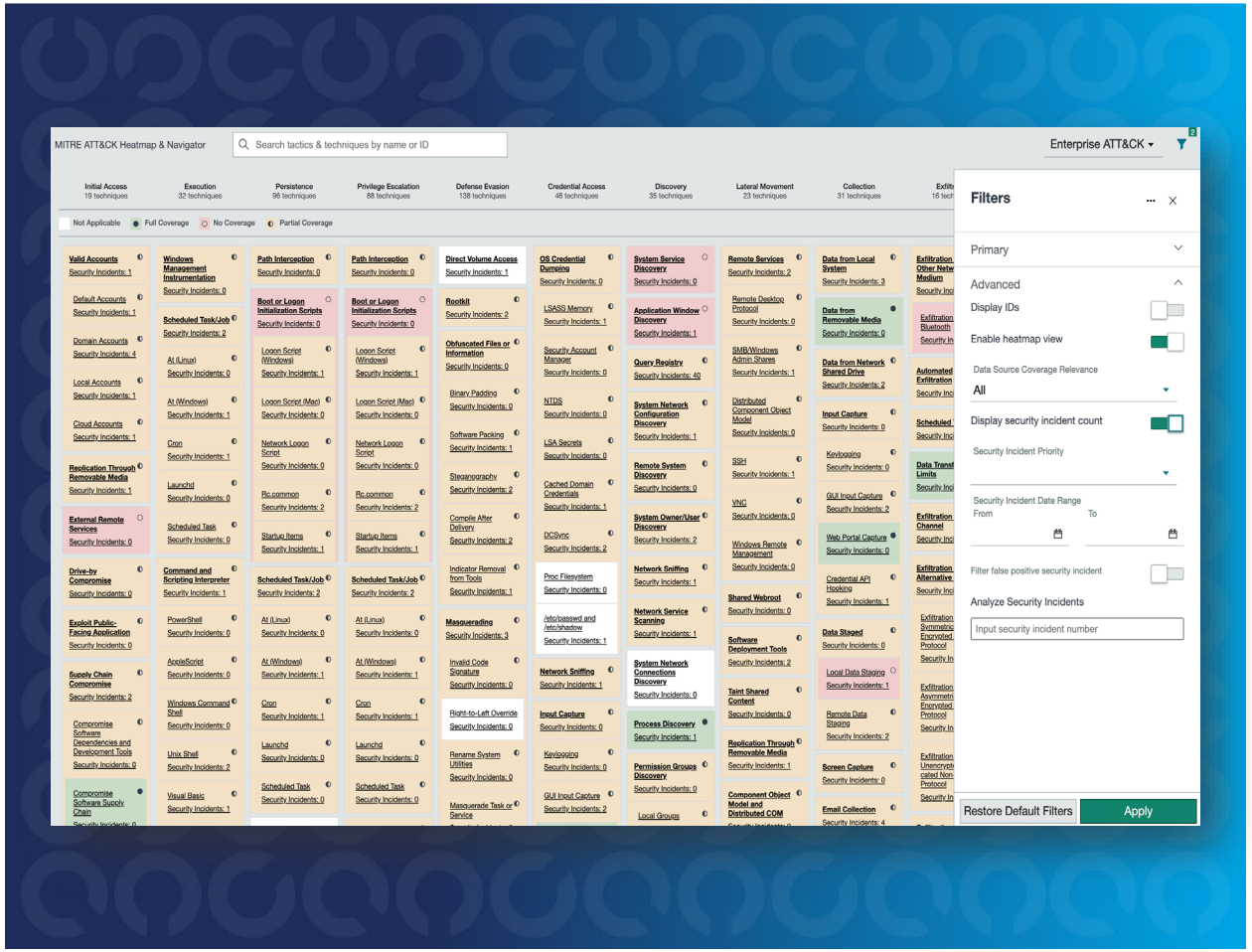
Know your adversaries?

MITRE ATT&CK

Knowledge base of adversary tactics and techniques

"Think like the enemy…"

- Tactics represent the "why" of an ATT&CK technique
- Techniques represent "how" an adversary achieves a tactical objective
- Know the vectors adversaries use to gain a foothold within a network



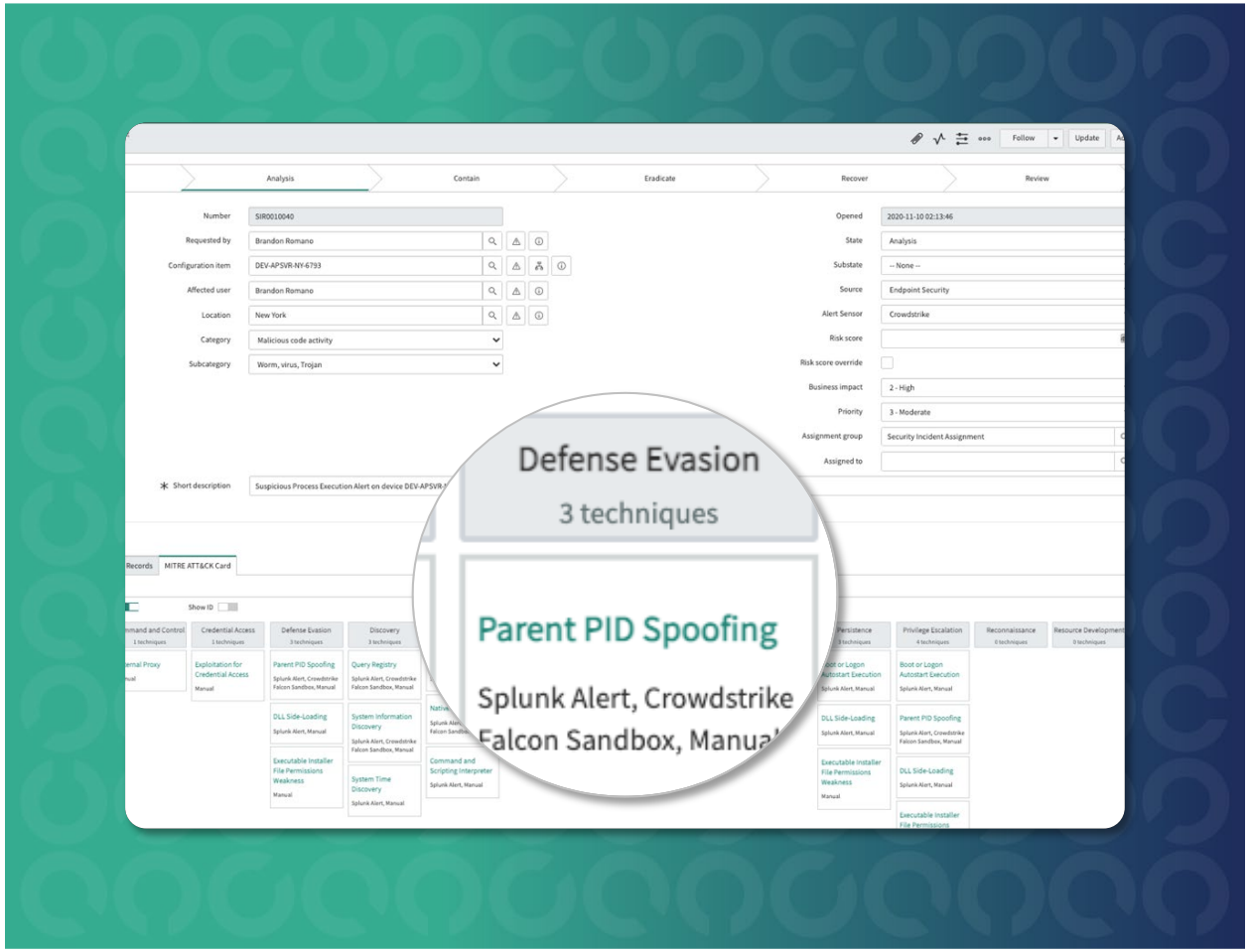
https://t.me/learningnets

ISACA VIRTUAL SUMMIT

Know a bad actors next move!

Leverage the kill-chain info card

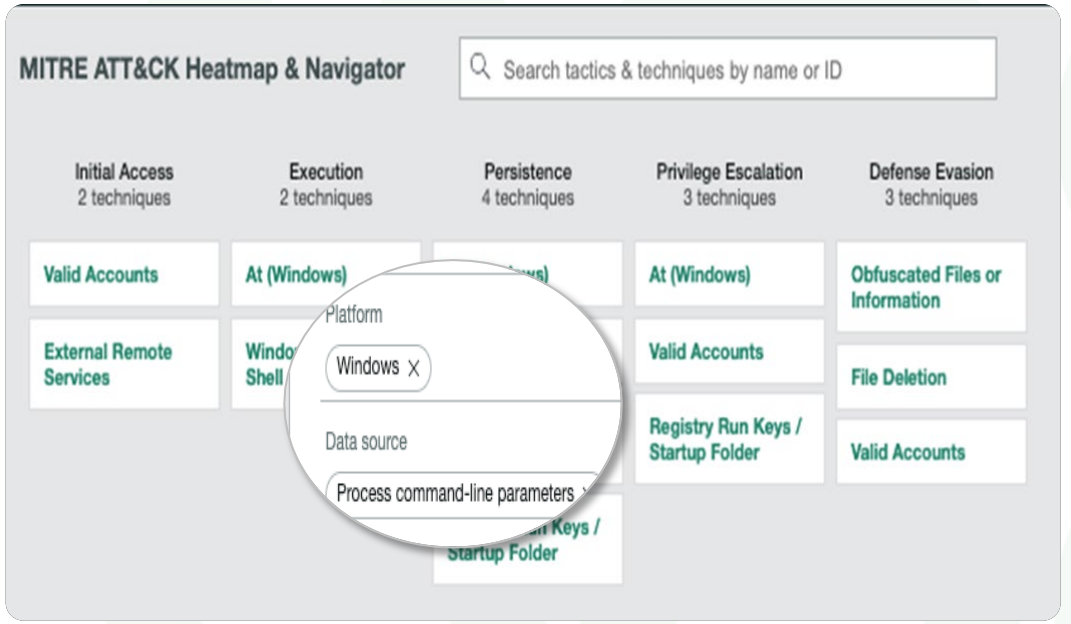
- Gain context on threat tactics
- Tactics and techniques are mapped to the adversary profile and MITRE ATT&CK card
- See where individual security events fit into an overall attack



Threat actor modeling

Threat hunting with the kill-chain TTP Map!

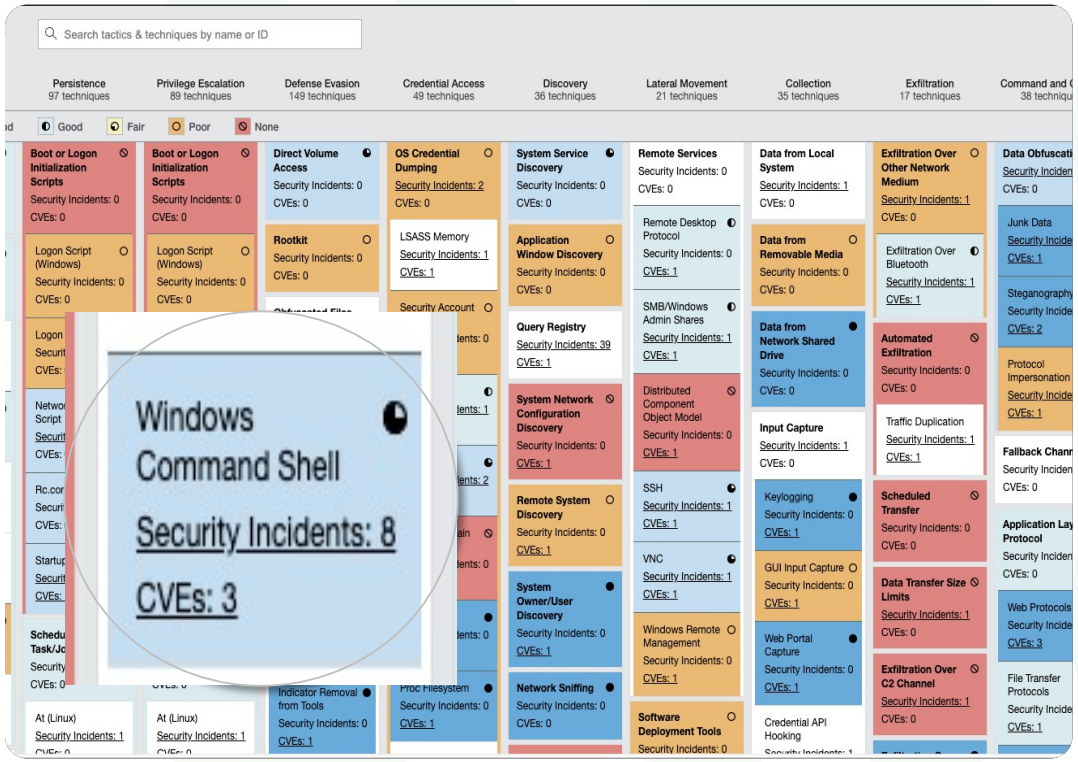
- Targeted views of adversary behavior
- Assess scope and relationships of individual attacks
- Know what actions are most effective for response and containment



Visualize your security effectiveness

Align adversary behavior and attack campaigns to overall detection coverage

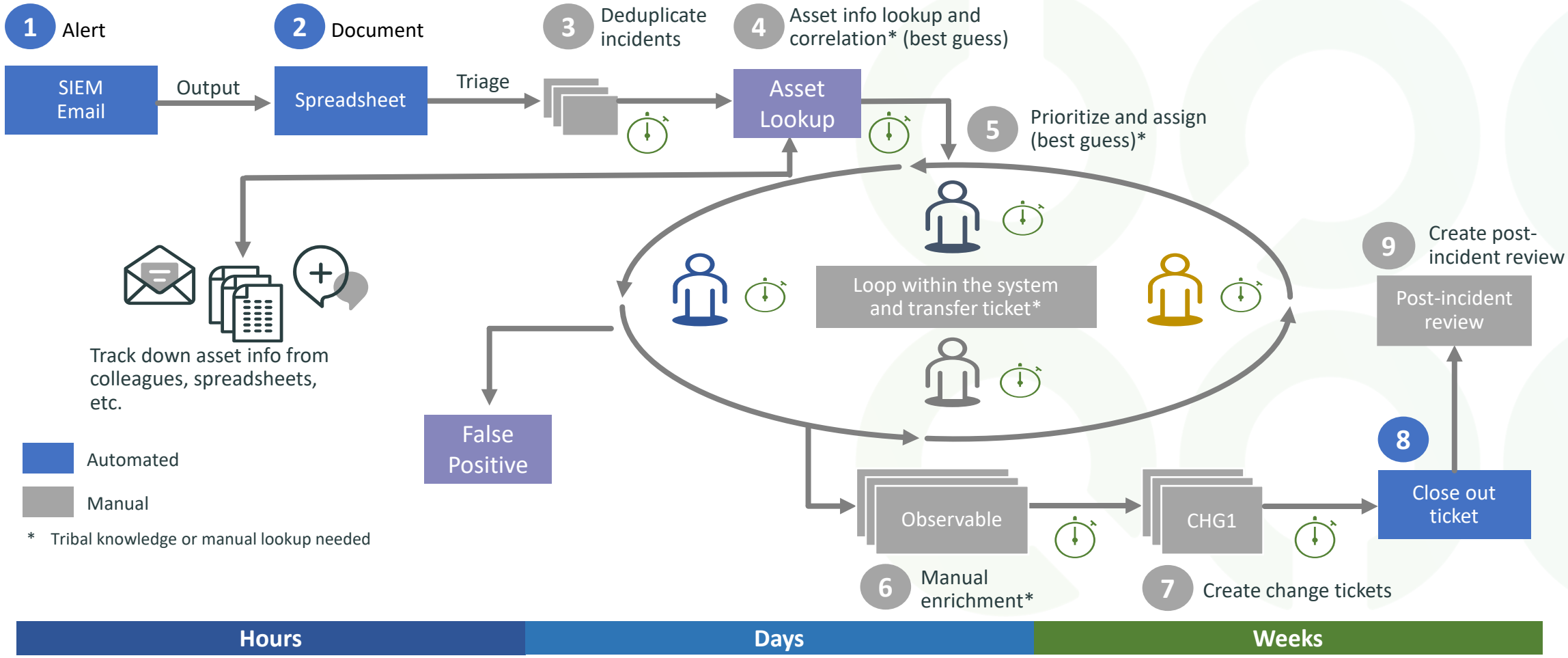
- Gain security posture visibility via technique detection capabilities and gaps
- Search ongoing and past incidents to uncover hidden threats
- Optimize processes and skills against evolving attack techniques
- Use these visualizations to conduct post-mortems after attacks



In summary?

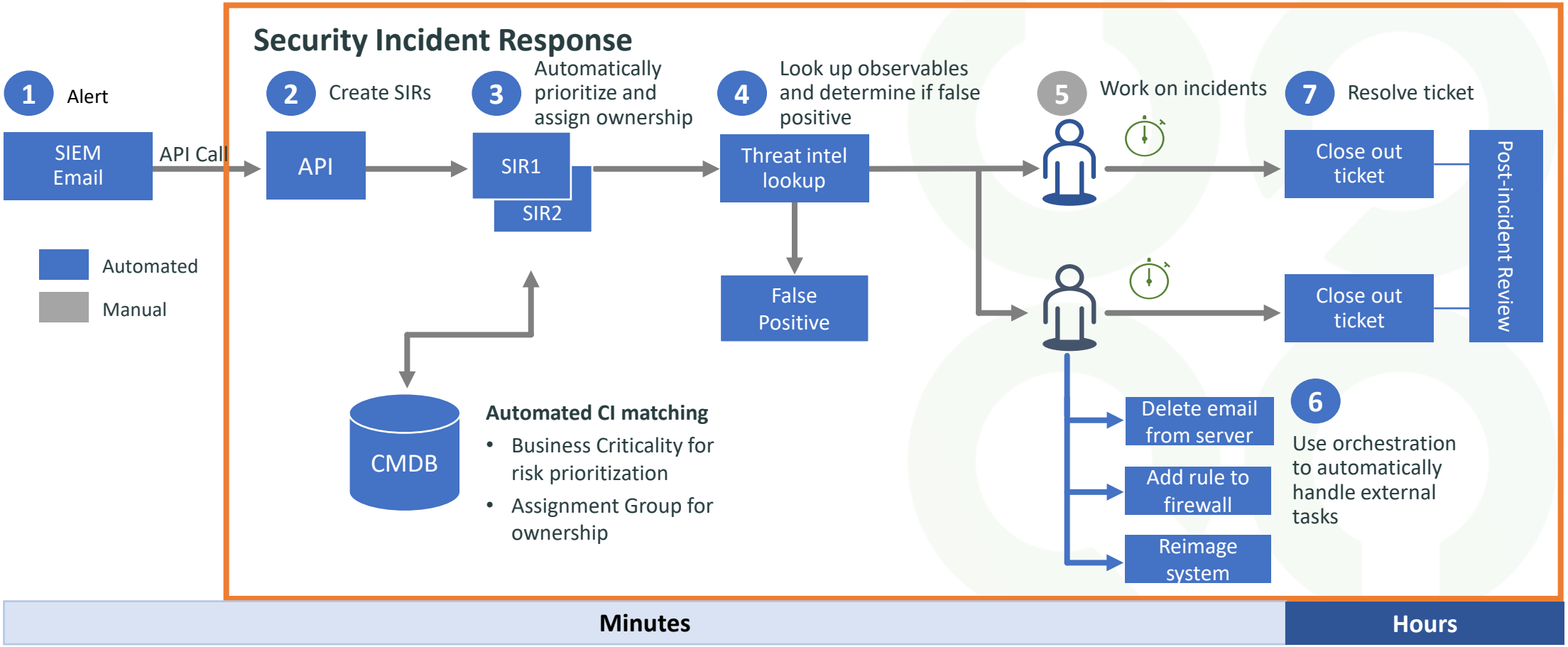
Automating Incident Response

Manual Security Incident Response Process



Automating Incident Response

Automated Security Incident Response Process

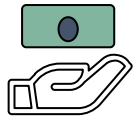


Automating Incident Response

- Effectively manage the evolving threats to your business
- Proactively manage exposure with visibility into high-impact threats and MITRE ATT&CK insights
- Ensure cyber resilience with real-time view into your security posture to quickly prioritize security incidents
- Drive efficiencies and accelerate reaction time with insights across teams to effectively Orchestrate and Automate actions

Real Results

Automated incident workflows scale capacity and increase cyber-resilience.



Reduce Costs

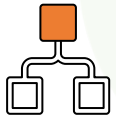
3x

Security Analyst efficiency

Improve Security Posture

85%

“Mean time to contain” improvement



Break Down Silos

80%

Reduction in open vulnerabilities

Improve Business Results

8,700

Hours saved annually via automation

Transform Security Operations

Connect security to the rest of the enterprise.

Gain visibility & insight in real-time

Prioritize based on risk and business context

Collaborate via automated, AI-powered workflows

Track performance across the org

Q & A

THANK YOU FOR ATTENDING THIS ISACA VIRTUAL SUMMIT SESSION

ISACA VIRTUAL SUMMIT

This training content ("content") is provided to you without warranty, "as is" and "with all faults". ISACA makes no representations or warranties express or implied, including those of merchantability, fitness for a particular purpose or performance, and non-infringement, all of which are hereby expressly disclaimed.

You assume the entire risk for the use of the content and acknowledge that: ISACA has designed the content primarily as an educational resource for IT professionals and therefore the content should not be deemed either to set forth all appropriate procedures, tests, or controls or to suggest that other procedures, tests, or controls that are not included may not be appropriate; ISACA does not claim that use of the content will assure a successful outcome and you are responsible for applying professional judgement to the specific circumstances presented to determining the appropriate procedures, tests, or controls.