RSAConference2019
San Francisco | March 4–8 | Moscone Center

BETTER.

SESSION ID: HUM-R11

Automation vs Human Eyes: Optimizing Human Intuition for Success

Tonia Dudley
Security Solutions Advisor
Cofense
@_tdudley

Unwelcome Visitors

2016

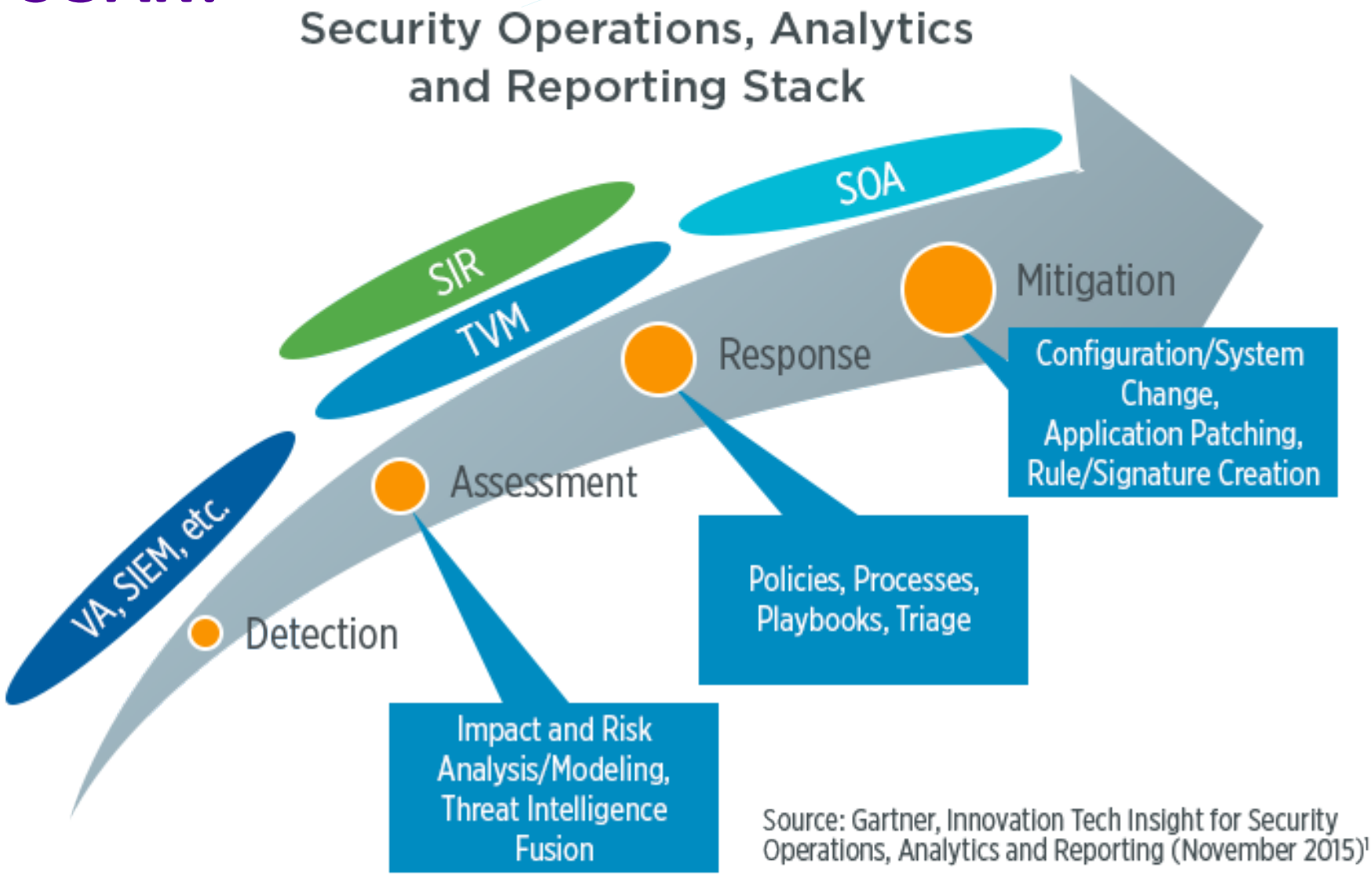
2017

Piles of Logs

WE'VE ASKED FOR VISIBILITY – NOW WHAT?

Now we have all these logs, how do we sift through the noise?

What is SOAR?



Source: Gartner, Innovation Tech Insight for Security Operations, Analytics and Reporting (November 2015)[1]

What Does the Survey Say…

- **62%** cite lack of skilled staff, **53%** cite inadequate automation/orchestration as the most common self-identified shortcomings.

- **Lack of automation/orchestration, integrated toolsets and processes/playbooks were the next most commonly referenced barriers.** These three areas are critical to providing "force multipliers" to allow limited staff to identify issues, keep up with vulnerabilities and threats, and prioritize action and response.

What Does the Survey Say…

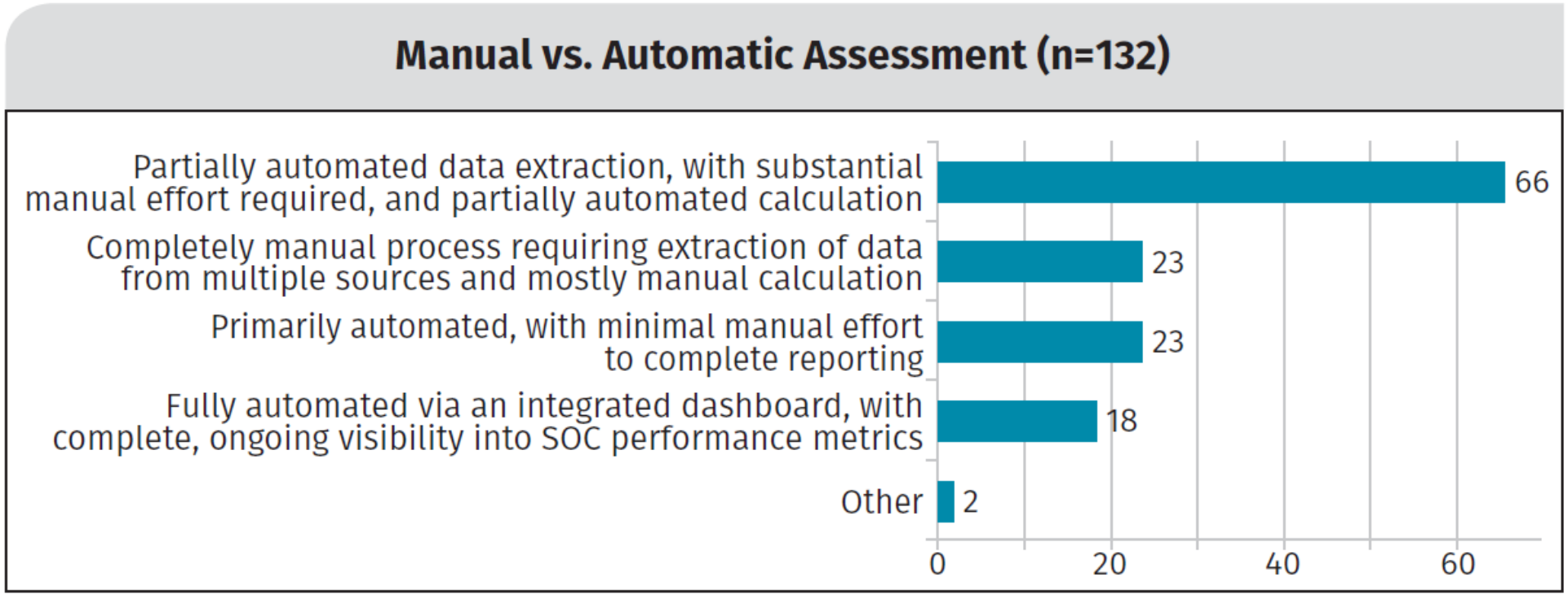


Figure 13. Manual vs. Automatic Assessment n=132

What Does the Survey Say…

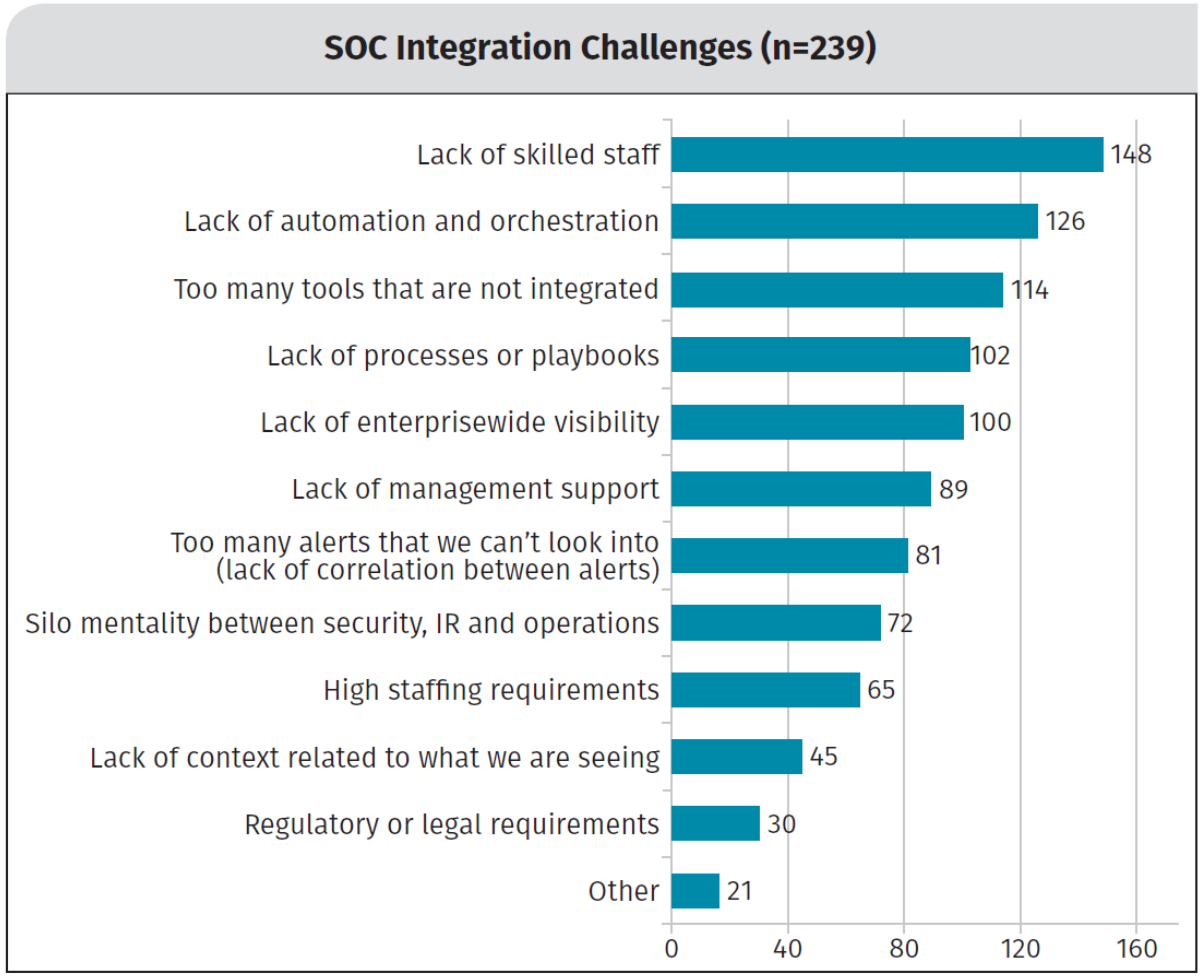


Figure 22. SOC Challenges

Where is the Framework?

TESTING AUTOMATION

Cloud Security Automation

What is your process?

JUST BECAUSE YOU HAVE A CHECKLIST

Does that mean it's something you can automate?

Malicious Email

PROCESS FLOW WHEN WE IDENTIFY A MALICIOUS EMAIL

Automate from the start OR once recognized?

What skillset do you need?

Tooling

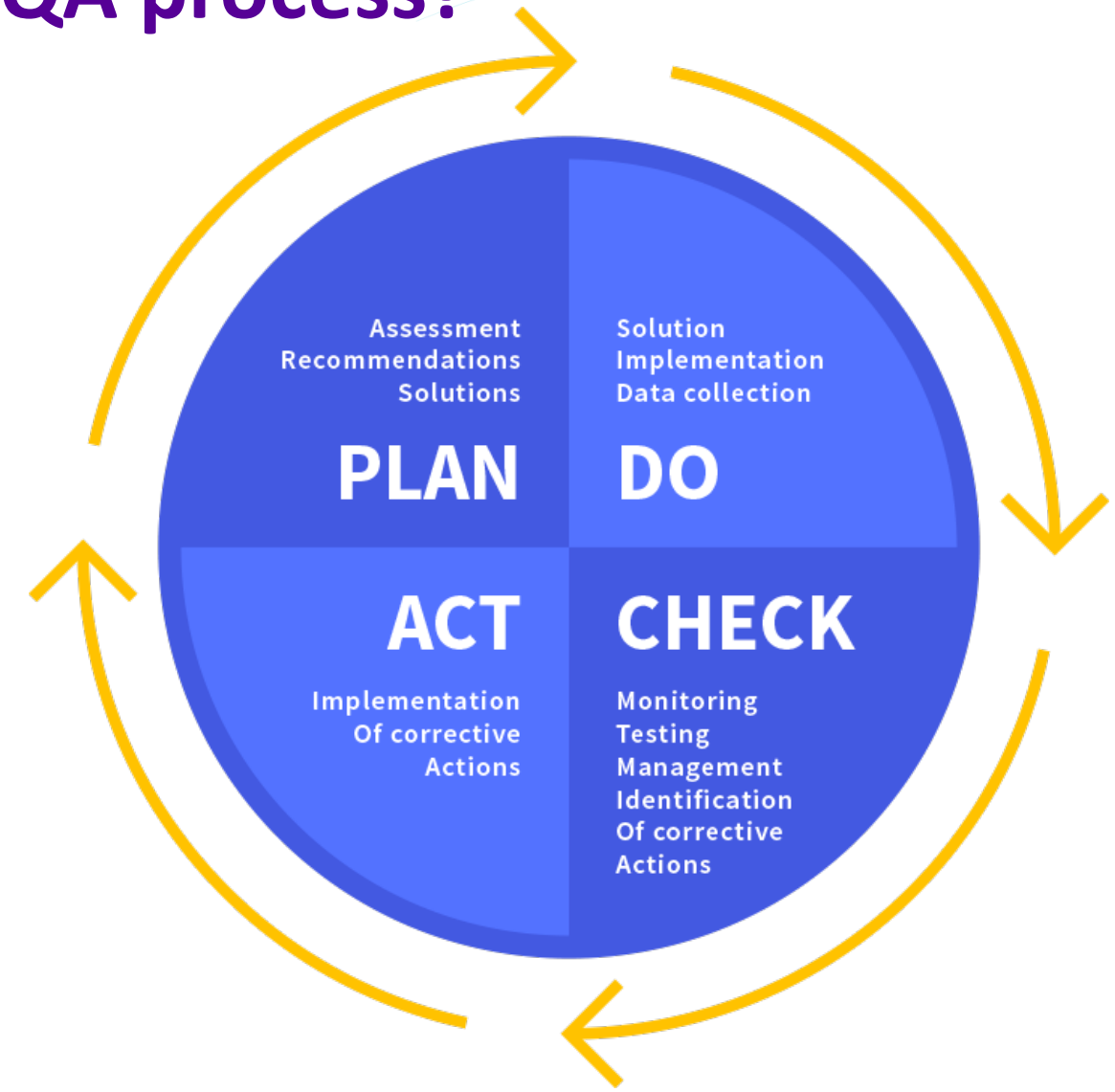
WHAT TOOLS DO YOU ALREADY HAVE IN YOUR TOOLBOX?

What are the gaps that you need to fill? Is Open Source an option?

Where to start….

IN ORDER TO FIND A STARTING PLACE – LOOK AT THE PAST

What is your QA process?



Who needs Change Control?

WHAT IS THE CRITERIA FOR MAKING CHANGES TO YOUR AUTOMATION?

Maintenance Review

Example: Email Reported by User

```
strings:
    $a1 = "diet" nocase
    $a2 = "spam" nocase
condition:
     any of ($a*)
```

PROCESS STEPS

User Reports | Yara Rule tag | Close Ticket | Respond to user

Example

DIET SPAM – NOISY USER REPORT

BUT. What if the email wasn't really spam and was indeed a malicious email?

Example: Internal Email Reported by User

```
strings:
    $a1 = "company A" nocase
    $a2 = "company B" nocase
condition:
     any of ($a*)
```

YOU TRUST AN INTERNAL EMAIL REPORTED BY USERS

User Reports | Yara Rule tag | Close Ticket | Respond to user

Example: Validated Third Party Provider

HR WANTS YOU TO VOTE FOR BEST COMPANY

When you have enough indicators to be right 100% of the time, automate.

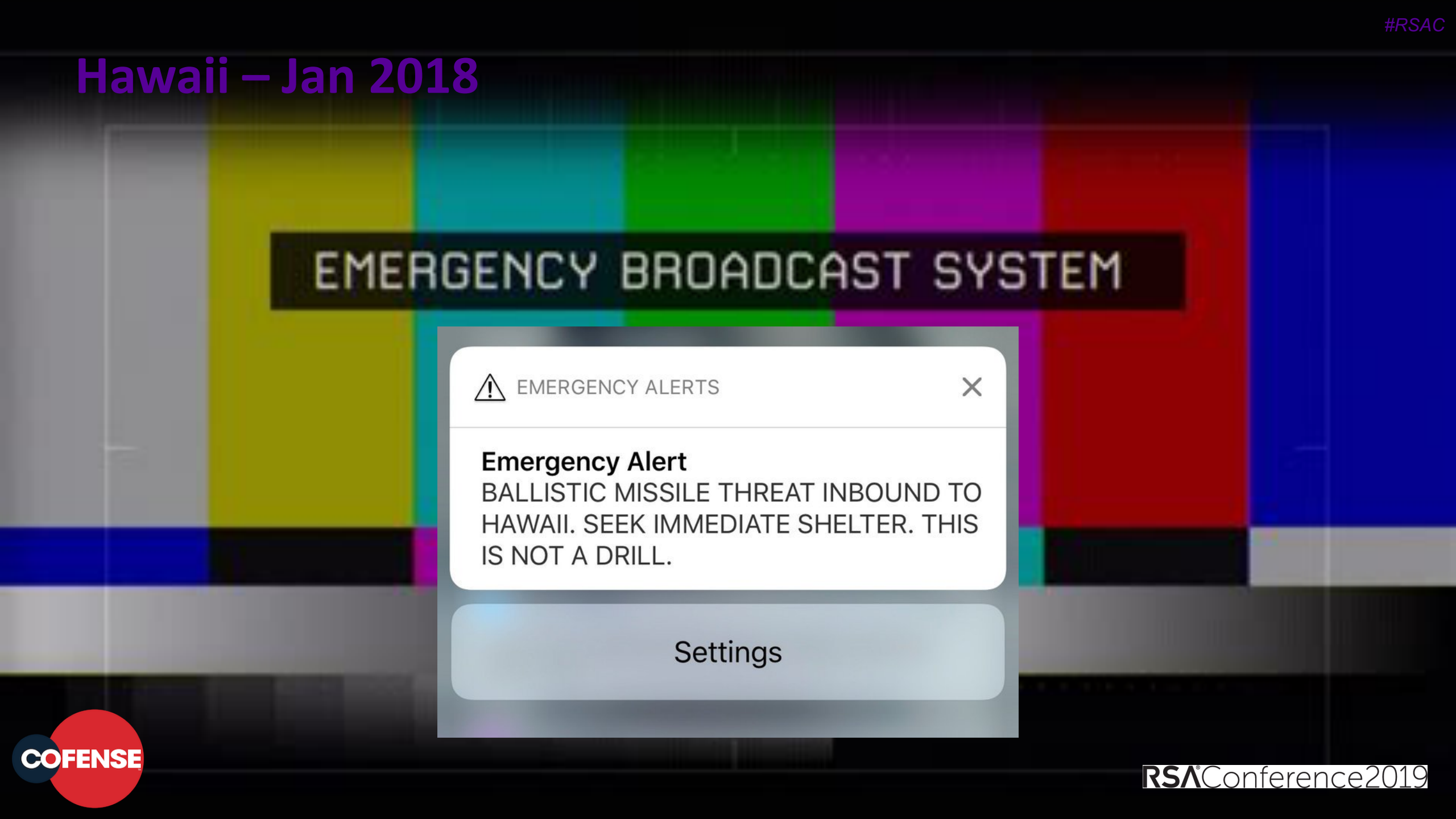
What's the ROI?

WHAT IS THE COST OF AUTOMATION?

Assurance

HOW DO YOU CONVINCE YOUR CISO MALICIOUS ALERTS WON'T GET MISSED?

Hawaii – Jan 2018



Apply: Where to Start

- Define your automation objectives
  - What are you trying to achieve
- Short term
  - Take an inventory of your playbooks
  - Identify high volume repeat processes
  - Find a resource able to provide support
- long term
  - Show value in first wave for support
  - Create synthetic transaction for validation

Questions

RESOURCES & REFERNCES

References

- FireEye M Trends:
  - https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf
- Gartner SOAR
  - https://blog.skyboxsecurity.com/gartner-defines-new-technology-class-for-security-operations-analytics-and-reporting/
- SANS Security Operations Survey
  - https://www.sans.org/reading-room/

RSAConference2019

Thank You!

Tonia Dudley
tonia.dudley@cofense.com
@_tdudley