knowledge17

WORK at LIGHTSPEED™

# Bridging the Gap Between Security & IT to Build Better Security Response

MYKE LYONS
*DIRECTOR, SECURITY BUSINESS UNIT*
ServiceNow

© 2017 ServiceNow All Rights Reserved

servicenow

# Speaker Introduction



**NAME:** Myke Lyons

**TITLE:** Director, Security Business Unit

**FUNCTION:** Head of Security Strategy

**COMPANY:** ServiceNow

**EXPERIENCE:** 16+ years in IT / Security

**EXPERTISE:** Security, Ops, Cooking

**ACHIEVEMENTS:** Intra-preneur

**CURRENT PROJECTS:** Driving process efficiencies. Automating all security and compliance work streams



© 2017 ServiceNow All Rights Reserved

# Session Overview



## Objectives

- Automation, how and where to begin



## What You Will Learn

- Some of the definition(s) of Automation
- Learn about automating Enterprise Security Response
- Crawl, walk, run


© 2017 ServiceNow All Rights Reserved

# Key Security Question





© 2017 ServiceNow All Rights Reserved

# Organizations Have Invested in LOTS of Security Products




*Logos shown are trademarks or registered trademarks of their respective owners and not ServiceNow*

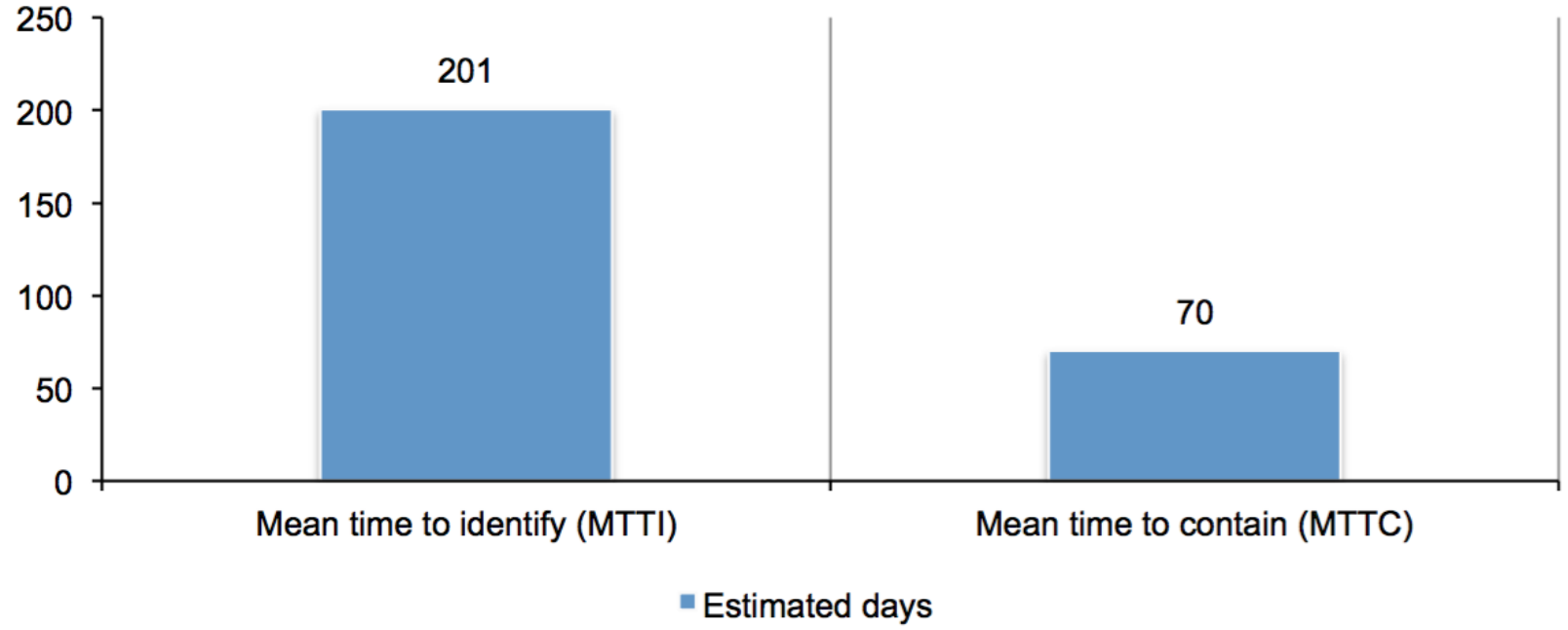
**But what happens when something goes wrong?**



© 2017 ServiceNow All Rights Reserved

# Most are Struggling to Find and Stop Breaches…

**Figure 20. Mean time to identify and contain data breach incidents (in days)**
Consolidated view (n = 383)




On average, it took respondents **201 days to spot a breach** caused by a malicious attacker, and **70 days to contain it.**

Source: Ponemon Institute 2016

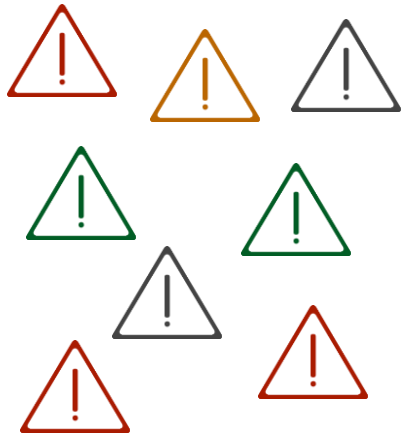
*Logos shown are trademarks or registered trademarks of their respective owners and not ServiceNow*



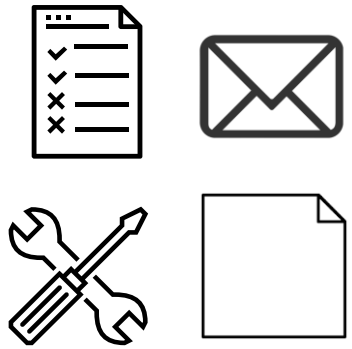
© 2017 ServiceNow All Rights Reserved

# Why? Security Teams are Overwhelmed

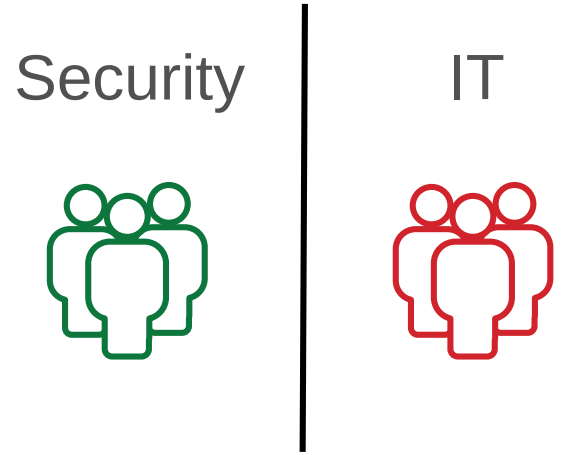
Too Many Alerts & No Context



Manual Tools



Siloed from IT





© 2017 ServiceNow All Rights Reserved

# Example of Today's Incident Response Workflow



Security Pro

"We believe we've detected malware on xyz host we need to contact the owner and scan the machine"

"Please have IT collect the asset and save a copy of the image"

"What are our policies regarding loss of sensitive financial data?"

"We believe sensitive financial data has been stolen, what do you need from us?"

"I'm getting lost in the communication string, I better copy some of these emails into my repository!"



"I have located the owner in our CMDB and will begin the scan now"

"The scan was unsuccessful"

"Our CFO is the host owner, he says there may be sensitive financial data on the machine"



IT Tools

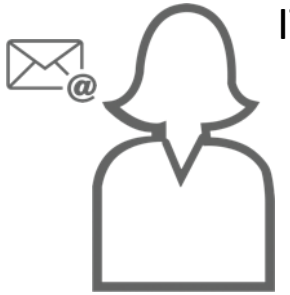
"Please collect this asset and save a copy of the image."



IT Support

"The legal department needs to know the exact nature of the stolen data"

"You need to contact the FBI immediately"



Finance

"We need a copy of the malware image if one exists and need detailed explanation of stolen data"



Law Enforcement



© 2017 ServiceNow All Rights Reserved

# Why is Security Failing? Wrong Tools for Response

Emails, Spreadsheets, Phone Calls, Meetings, and Text Messages are difficult to measure and don't provide an easy way to understand how your processes are performing, where the bottlenecks are, and how to improve them.

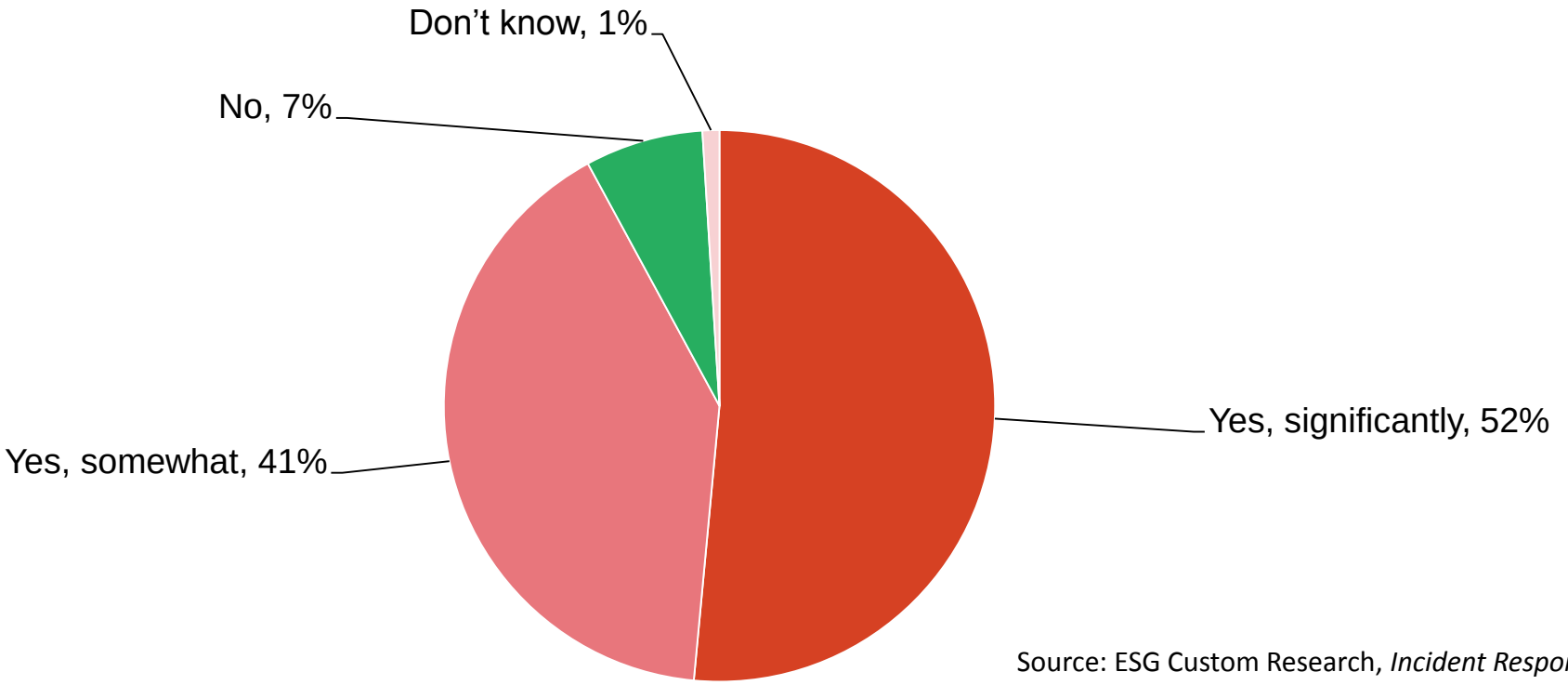



© 2017 ServiceNow All Rights Reserved

# These Issues are Widespread

Incident response effectiveness and efficiency is limited by the burden of manual processes

**Do you believe that your organization's incident response efficiency and effectiveness are limited by the time and effort required for manual processes? (Percent of respondents, N=184)**




Source: ESG Custom Research, *Incident Response Survey,* February 2016

*Logos shown are trademarks or registered trademarks of their respective owners and not ServiceNow*



© 2017 ServiceNow All Rights Reserved

# The Progression of Security



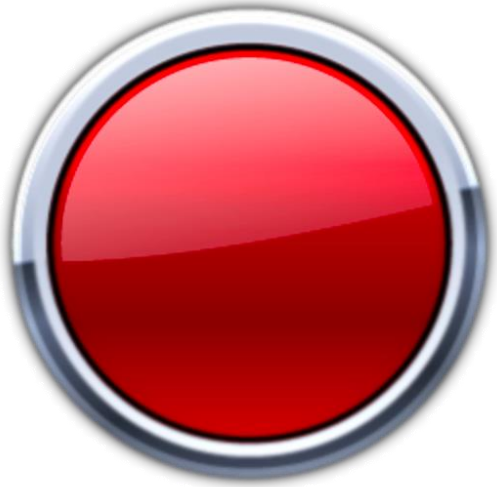
Protection



Detection



Visibility



Response!

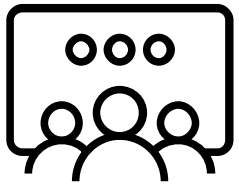

© 2017 ServiceNow All Rights Reserved

# Five Best Practices to Integrate Security & IT for Security Response

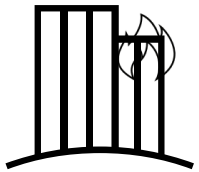


© 2017 ServiceNow All Rights Reserved

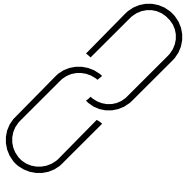
# Five Best Practices



Use a Single System for IT & Security



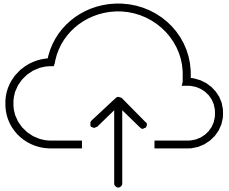
Correlate the Problem with the Business



Digitize Your Security Runbook



Track Progress, Find Gaps & Optimize



Integrate a Knowledge Base


© 2017 ServiceNow All Rights Reserved

# Build an Enterprise Security Response Program





© 2017 ServiceNow All Rights Reserved

# Thank You

MYKE LYONS
*DIRECTOR, SECURITY BUSINESS UNIT*
ServiceNow

@mykesec | #Know17

© 2017 ServiceNow All Rights Reserved

# Q & A

MYKE LYONS
*DIRECTOR, SECURITY BUSINESS UNIT*
ServiceNow



© 2017 ServiceNow All Rights Reserved




www.servicenow.com/sec-ops

# Take the Survey

Please take a moment to complete a session survey in the Knowledge17 app.

# Thank You

**Myke Lyons**

*Director, Security Business Unit*

ServiceNow



© 2017 ServiceNow All Rights Reserved