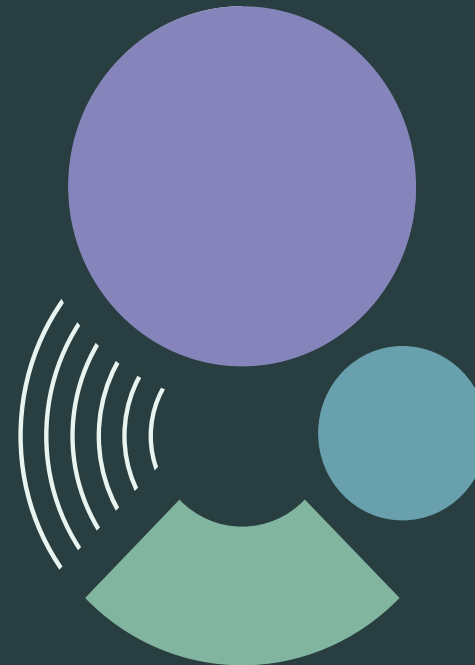
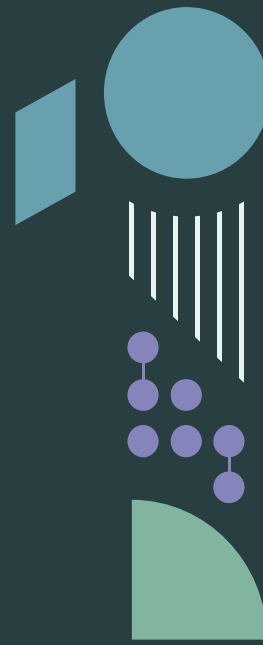


now summit



24 Oktober • Frankfurt

servicenow



servicenow™

ServiceNow Security Operations

New features and use cases

Bernhard Reich

Product Line Sales Manager
Security & Risk

Manoj Patel

Senior Advisory Solution Consultant
Security & Risk EMEA



Speaker introduction



Name: Manoj Patel

Title: Senior Advisor

Function: Security & Risk Practice Global Practice

Company: ServiceNow

servicenow[™]

Manoj Patel, serves as Senior Advisory Solution Consultant for ServiceNow's Global Security and Risk BU, focused on solving Enterprise Risk & Cyber Security challenges. He brings a total of 20+ years of experience in Enterprise Service & Legal Management, Governance, Risk & Compliance & Security space.

He is a regular guest speaker at ISACA EuroCACS, ISACA CSX and Gartner conferences for GRC, GDPR & CyberSecurity topics. His blog posts on GDPR & Cyber Security can be found on LinkedIn. He holds an MBA (Finance & Marketing) from UK, M.S (Computer Science) from Germany, and B.Sc. (Physics) from India. He is certified as GRCP (OCEG) and in CyberSecurity (CSX).

Speaker introduction



Name: Bernhard Reich

Title: Product Line Sales Manager, SecOps & GRC

Function: Security & Risk Practice Product Line Sales

Company: ServiceNow

servicenow™

- **EXPERIENCE:** 22 years in IT/Software Industry in Sales and Management, 13 years in Security
- **FOCUS AREAS:** Systems & Security Architectures, Security Operations, Governance Risk & Compliance
- **CURRENT PROJECTS:** ServiceNow Security Operations & GRC



Agenda

▶ Today's problems

▶ Where the industry is going

▶ What's new in London?

▶ Use case demos

▶ Customer value

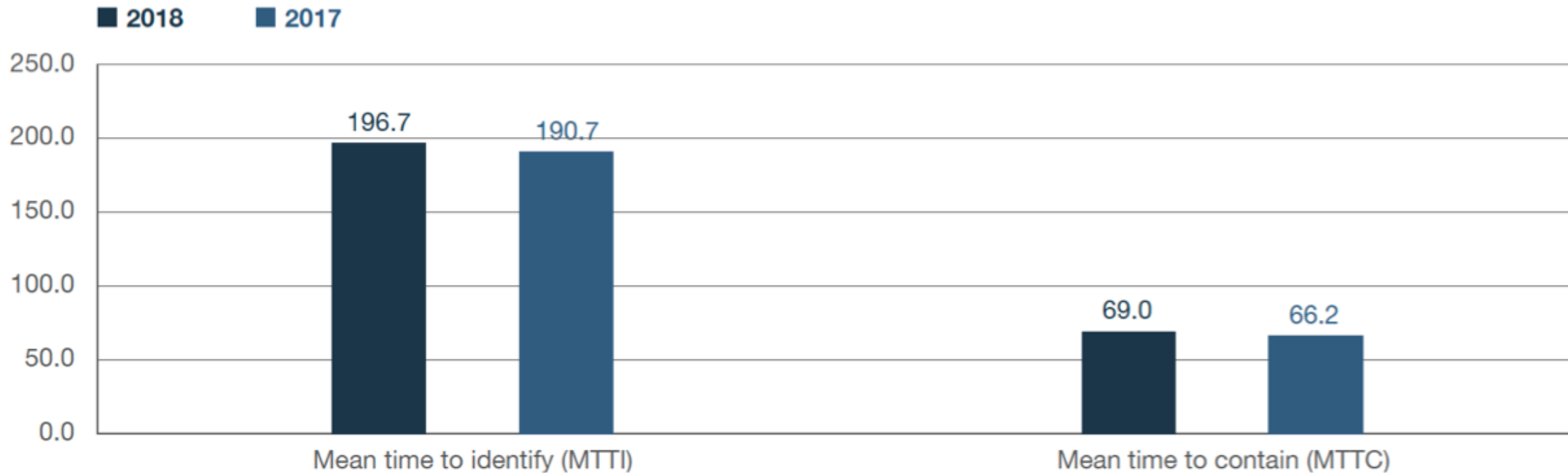
Organizations have invested in a LOT of security products

The image displays a collage of security product logos, organized into three categories represented by teal boxes and circles:

- Protect:** Includes logos for Lieberman Software, Damballa, McAfee, Symantec, Securonix, Dell SonicWall, FireEye, and Sophos. A large green circle with a white checkmark is overlaid on this category.
- Detect:** Includes logos for Cisco, Okta, Splunk, IBM, Tanium, and Malwarebytes. A large green circle with a white checkmark is overlaid on this category.
- Respond:** Includes logos for Cyphort, Guidance Software, Centrify, and Microsoft. A large dark grey circle with a white checkmark and the text "[NOT SO MUCH]" is overlaid on this category.

But they're struggling to find and stop breaches

Figure 24. Days to identify and contain the data breach over the past year



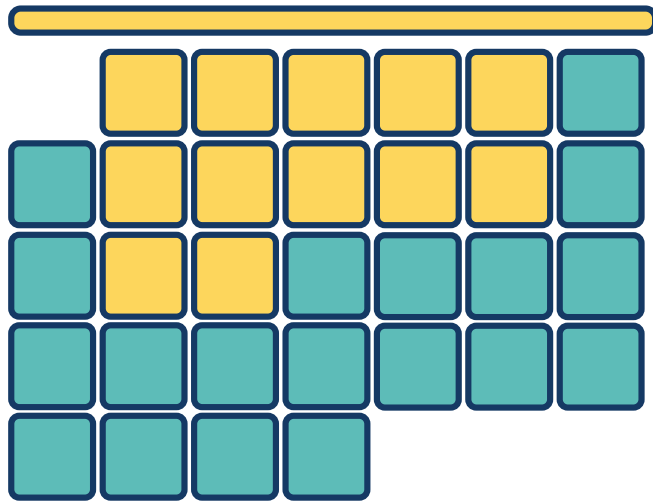
On average, it took respondents **197 days to spot a breach** caused by a malicious attacker, and **69 days to contain it.**



Source: Ponemon Institute 2018

© 2018 ServiceNow, Inc. All Rights Reserved. Confidential.

Manual processes and siloed tools delay patching



12 DAYS

Time lost coordinating
patching across teams
per vulnerability

Automating security response is the future

#3

Technology prediction for 2018 by Forrester

Forrester: The Top Technology Trends To Watch: 2018–2020

15x

Adoption of SOAR tools expected by 2020

Gartner: Innovation Insight on Security Orchestration, Automation, and Response



Automation of threat-detection tasks will increase in 2018

CSO: Our top 7 cyber security predictions for 2018



Now Platform



IT



Security Risk



Intelligent Apps



HR



Customer Service

User Experience



Service Portal



Service Catalog



Mobile Native



Community



Agent Workspace

Service Intelligence



Supervised Machine Learning



Virtual Agent Designer



Virtual Agent



Actionable Analytics



Time-series Database

Service Experience



IntegrationHub



Flow Designer



Visual Taskboards



Mobile Designer



Service Aware CMDB

Introducing ServiceNow® Security Operations



Security Incident Response



Vulnerability Response



Threat Intelligence



Trusted Security Circles



Configuration Compliance



Workflow



Automation & Orchestration



Deep IT Integration

User Experience



Service Portal



Service Catalog



Mobile Native



Community



Agent Workspace

Service Intelligence



Supervised Machine Learning



Virtual Agent Designer



Virtual Agent



Actionable Analytics



Time-series Database

Service Experience



IntegrationHub



Flow Designer



Visual Taskboards



Mobile Designer



Service Aware CMDB

NOW ON NOW

How ServiceNow Uses Security Operations

“ ServiceNow Security Operations integrates all our security tools into one platform, enabling us to analyze and respond to threats faster. ”

Chris Bedi
CIO, ServiceNow

6X

FASTER ALERT PROCESSING VIA
AUTOMATION AND DATA INTEGRATION

\$420,000

SAVINGS IN SECURITY OPERATIONS
STAFFING COSTS

8700

HOURS SAVED ANNUALLY VIA SOC
AUTOMATION

50%

MORE CASES HANDLED PER STAFF THROUGH
OPERATIONAL EFFICIENCIES

What's New in London?

New User Interface for Security Incident Response

The screenshot displays a modern, tile-based user interface for Security Incident Response. The main content area is divided into three horizontal tiles:

- Affected Users:** A table with columns for User, Email, Active, and Time Zone. It shows one record for Sean Convery with email Sean@servicenow.com, active status true, and time zone US/Pacific.
- Configuration Items:** A table with columns for Configuration Item, Class, Created, and Created By. It displays "No records to display".
- Threat Lookup Results:** A table with columns for Observable, Integration Vendor, and Finding. It shows two records for the domain www.bbqdzx.com, both identified as Malicious by VirusTotal.

On the right side, there is a **Playbook** sidebar:

- Phishing Playbook:** A dropdown menu showing a "Draft" and a list of tasks.
- Analysis (3):** A section with a "TO DO" button containing three tasks:
 - SIT0010150:** "Is Email Phishing?" (COMPLETED) by Piero Depaoli. Outcome: Yes.
 - SIT0010132:** "Did employee submit the email properly?" (COMPLETED) by Piero Depaoli. Outcome: Yes.
 - SIT0010151:** "In-Depth IoC Analysis" (TO DO) by Piero Depaoli.
- Contain (1):** A section with a "TO DO" button containing one task:
 - SIT0010152:** "Did Others Receive Phishing Email?"

- Tile-based interface
- Configure personal view
- Easy-to-follow playbooks
- Quickly switch from investigation to containment
- Classic UI still available

Setup Assistant for Security Incident Response and Vulnerability Response

now SECURITY OPERATIONS

JC Janene Casella

Setup Assistant

16% Complete

The following steps help you set up Vulnerability Response for your environment. As you complete each step, click Mark as Complete to keep track of your progress.

System Administration (1/2 Tasks) System Administrator

This module covers essential user administration and installation of integration plugins.

- Vulnerability Response Users and Groups**
Select your Vulnerability Response administrator(s) and users. This can be individual users or user groups
- Integration Plugin Installation**
Install one or more third-party integration plugins to work with Vulnerability Response.

Integration Configuration (0/1 Tasks) Vulnerability Administrator

In this module, configure Vulnerability Response to work with the data from the third-party applications.

- Integrations**

- Guided implementation and continuing support
- User/group management
- Integration configuration
- Calculator setup
- Workflow triggers

Vulnerability Response enhancements

Multiple scanner and instance support

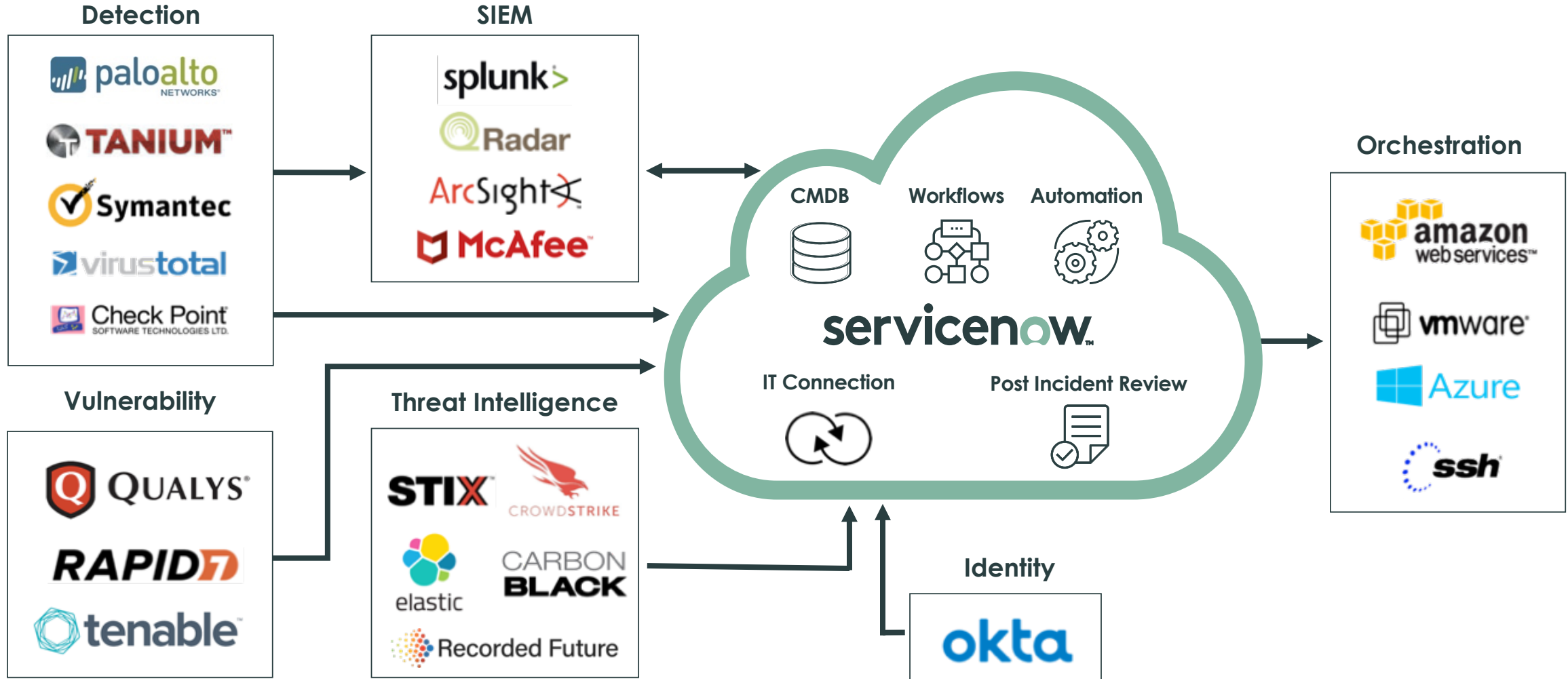
Configuration item management

Vulnerability Group Rules

Remediation Target Rules

Use Cases

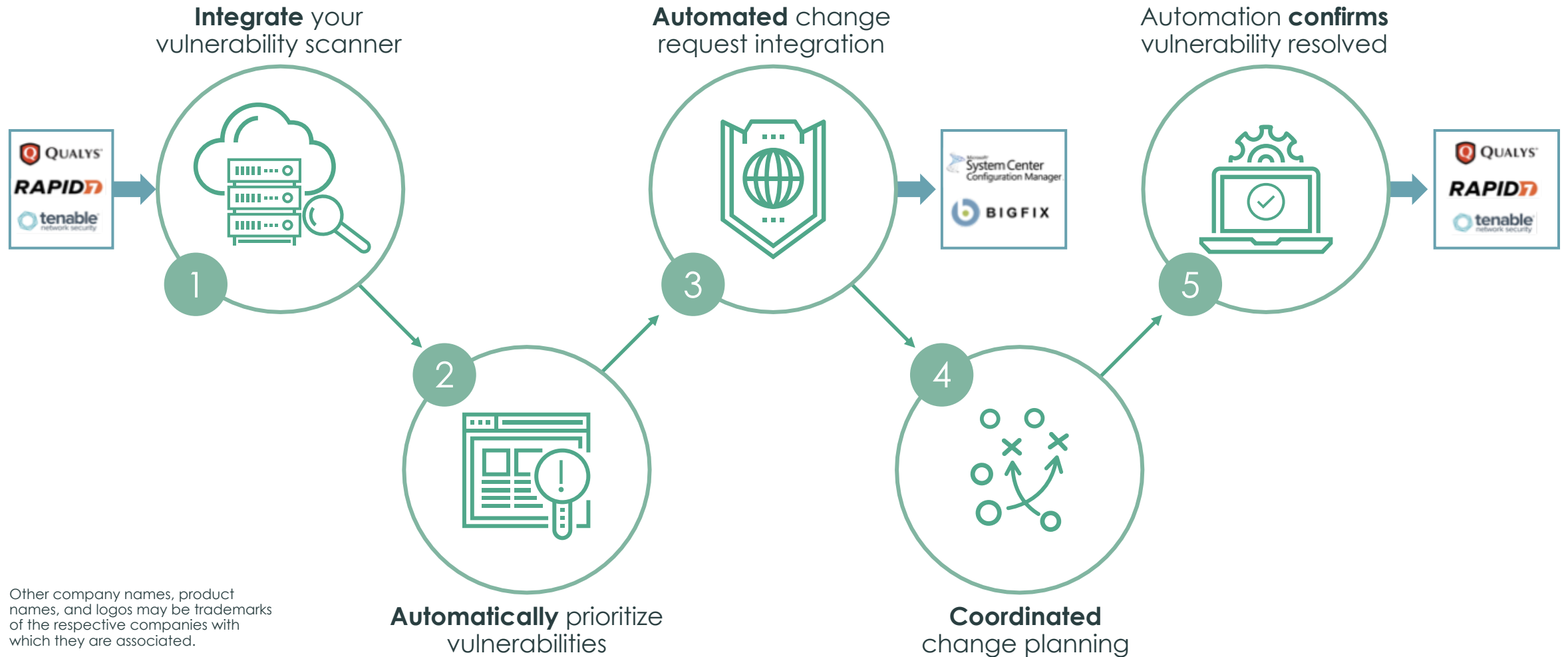
Where does Security Operations fit?



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

Use case #1

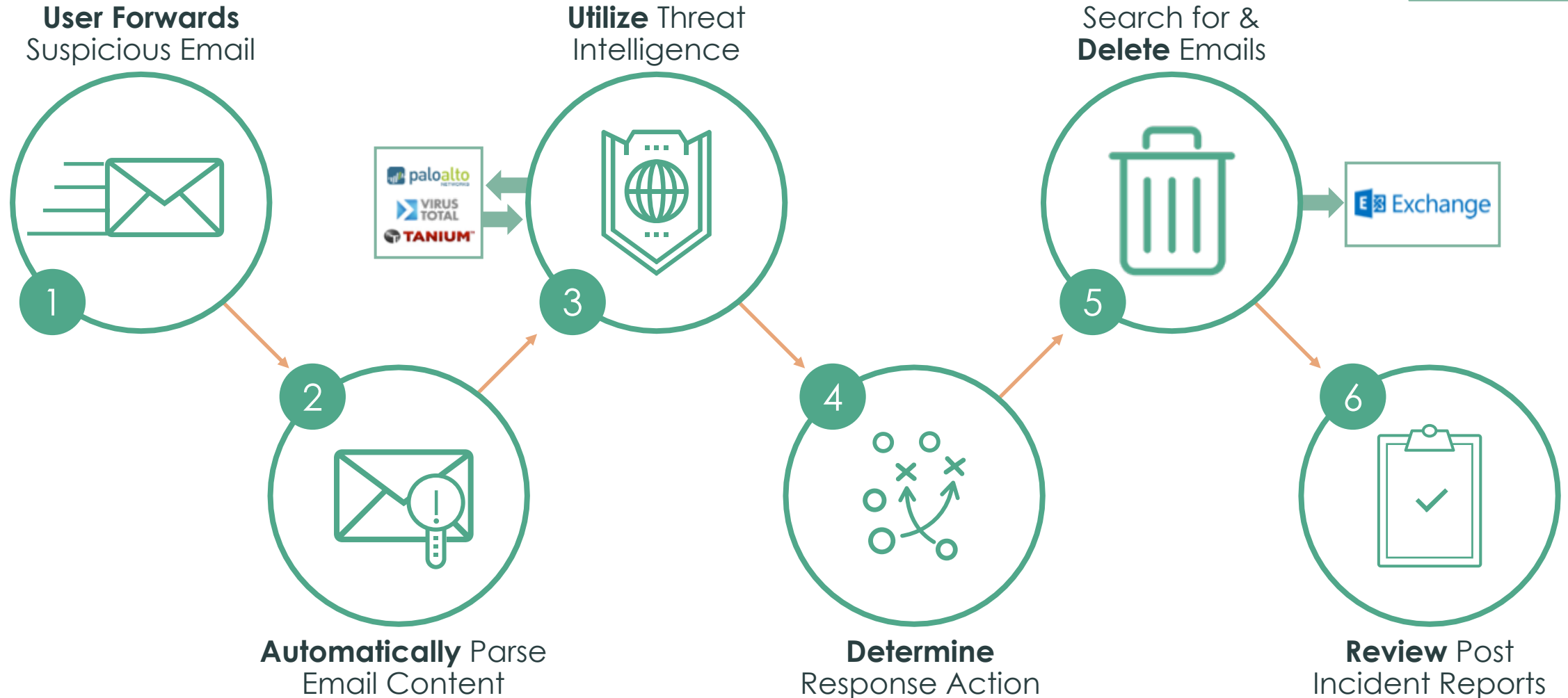
Respond to critical vulnerabilities



Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.

Use Case #2

Remediate user-reported phishing



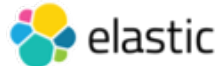
Integrate with your existing security products



Carbon Black.



digital shadows



Measured value

Forrester Total Economic Impact™ Study

45%

faster security
incident response

25%

faster vulnerability
response

60%

faster vulnerability
prioritization

Source: Forrester TEI Study 2018



Customer outcomes

60%

Reduction in vulnerability response time



50%

Increase in vulnerabilities resolved per month



50%

Reduction in security incident triage time



DXC.technology

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

Key takeaways

1

Prioritize and resolve security incidents and vulnerabilities faster.

2

Collaborate efficiently with IT.

3

Get a definitive view of your security posture.



servicenow™

Thank you