



splunk®

Prioritize and Automate Response to Critical Threats Fast with Accurate Business Context

Steve Anderson | Sr. Mgr. Product Management, ServiceNow
Janene Casella | Director, Product Marketing, ServiceNow

October 2, 2018

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2018 Splunk Inc. All rights reserved.

Challenges Facing Security Response



Too many alerts, no prioritization



Manual tools



Security siloed from IT

Reality for Today's Operations Teams

More systems and data

Apps & infrastructure are moving to the cloud

Faster release cycles

It's becoming harder to correlate & prioritize needs



Before You Can Prioritize... You Need to Know What You Have

Basic CIS Controls

- | | | | |
|----------|--|----------|---|
| 1 | Inventory and Control of Hardware Assets | 2 | Inventory and Control of Software Assets |
| 3 | Continuous Vulnerability Management | 4 | Controlled Use of Administrative Privileges |
| 5 | Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers | 6 | Maintenance, Monitoring and Analysis of Audit Logs |

Center for Internet Security Critical Security Controls

Deliver Real-time Visibility into Enterprise Infrastructure and Services



Uncover your Estate with Discovery

- ▶ Discover agentless
- ▶ Guided set up
- ▶ Classify and correlate configuration items
- ▶ Bulk import
- ▶ Populate and enrich the CMDB

now

Discovery Dashboard

Active Discovery Status

Number ▾ Created Description S

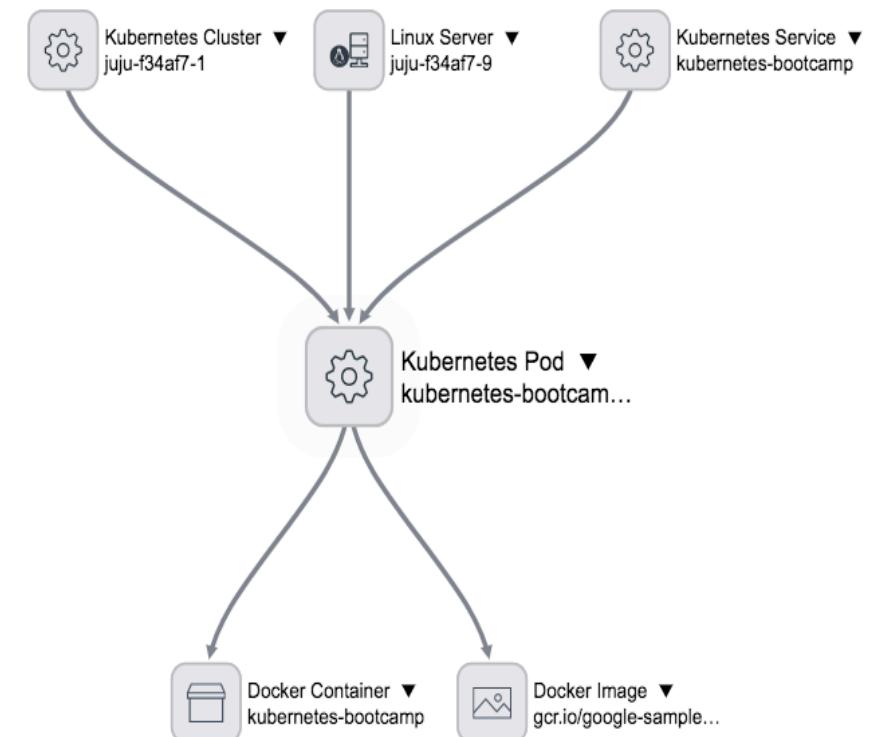
	ID	Created	Description
<input type="checkbox"/>	DIS0010307	2018-07-09 16:00:11	Scheduled
<input type="checkbox"/>	DIS0010306	2018-07-09 02:00:07	Scheduled
<input type="checkbox"/>	DIS0010304	2018-07-09 00:00:47	Scheduled
<input type="checkbox"/>	DIS0010303	2018-07-09 00:00:25	Scheduled
<input type="checkbox"/>	DIS0010246	2018-06-26 09:54:02	Discover Now

Newly discovered devices

Device Type	Count
IP Switch	3
Windows Server	2

Newly discovered applications

Application Type	Count
MySQL Instance	29
MS SQL Database	18
IIS Virtual Direct...	6
Tomcat WAR	4
MongoDB Instance	2
MySQL Web Site	2
Microsoft Web Site	2
Mongos Server	1
SharePoint	1
Tomcat	1
Oracle Instance	1
SQL Server Analysis	1



Reduce Noise with ServiceNow Event Management

- ▶ Collect, filter, and normalize events from Splunk
 - ▶ Rapidly understand impact to service

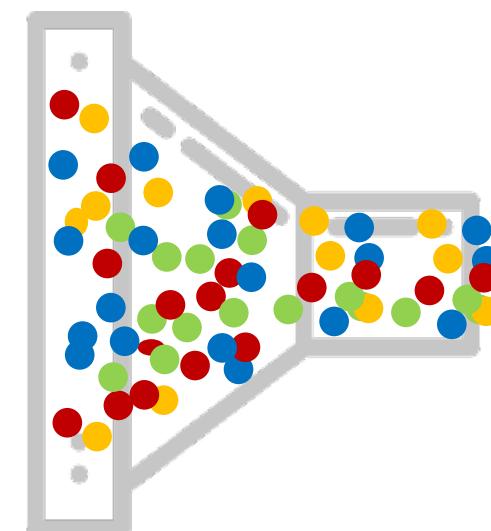


The dashboard displays a map of ServiceNow components and their status. Components include APAC Billing, Corp E-M, Credit Ch, Customer Man, EU - Customer Pu, Order fulfilment, Prod, QA Audit, UK, APAC Customer S, APAC Document, CRM, EU Billing, Production Audit, UK Customer, UK Loyalty Cl, US, APAC Loyalty Clu, Asia Portal, Customer, Demographics, mydemo123, North America E-, Production Report, UK Portal, US Loyalty Cl, UNIX_Server, and User Verificati. Alerts are shown at the bottom, with one minor alert (Alert0010016) for memory utilization above 95%.

Number	Group	Severity	Priority group	Priority	Source	Description	Node	Configuration item	Maintenance	Task	Acknowledged
Alert0010016		Minor	Urgent		35206 Group Alert	Physical Memory utilization is above 95%	RHEL-5-32-WMB.localhost.localdomain	RHEL-5-32-WMB.localhost.localdomain	false	INC0010010	true
Alert0010070		Minor	Urgent		35206 SolarWinds	Interface is down	RHEL-5-32-WMB.localhost.localdomain	RHEL-5-32-WMB.localhost.localdomain	false	INC0010012	false

Reduce MTTR with Real-time Correlated View of Health KPIs

DevOps	
Incident & Change Financial Management	
End User Experience Monitoring	
Application Performance	
Infrastructure, APIs, Cloud Services	



HEALTH KPIs

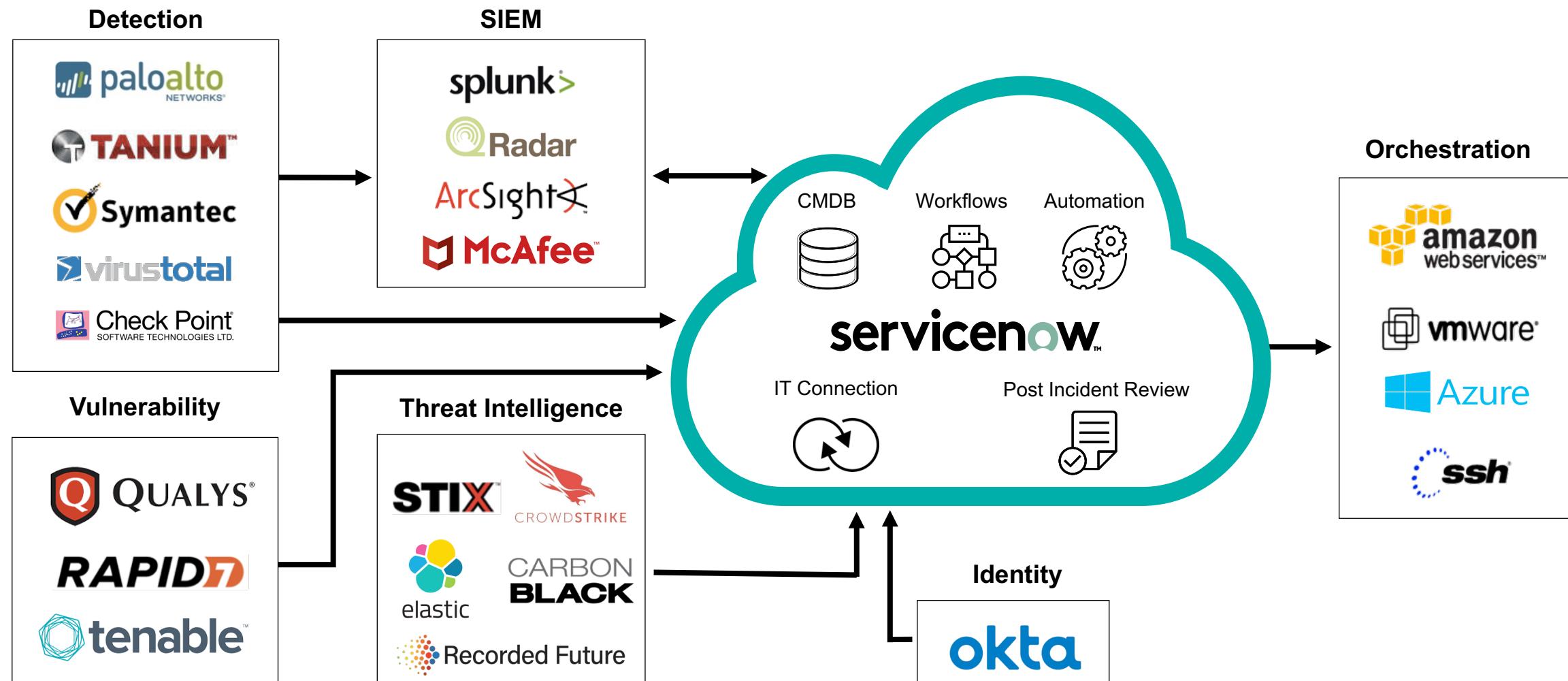


Apps Impacted
Users Impacted
Regions Impacted



Connect Your Security Tools for Faster Response

ServiceNow Security Operations



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

Prioritize Incidents that Impact your Business

- ▶ Correlate with CMDB
- ▶ Business criticality
- ▶ Risk score

Quick Filters

18 Critical Incidents > 90
0 New Incidents
190 Incidents Open > 24 hours

Show Open Incidents

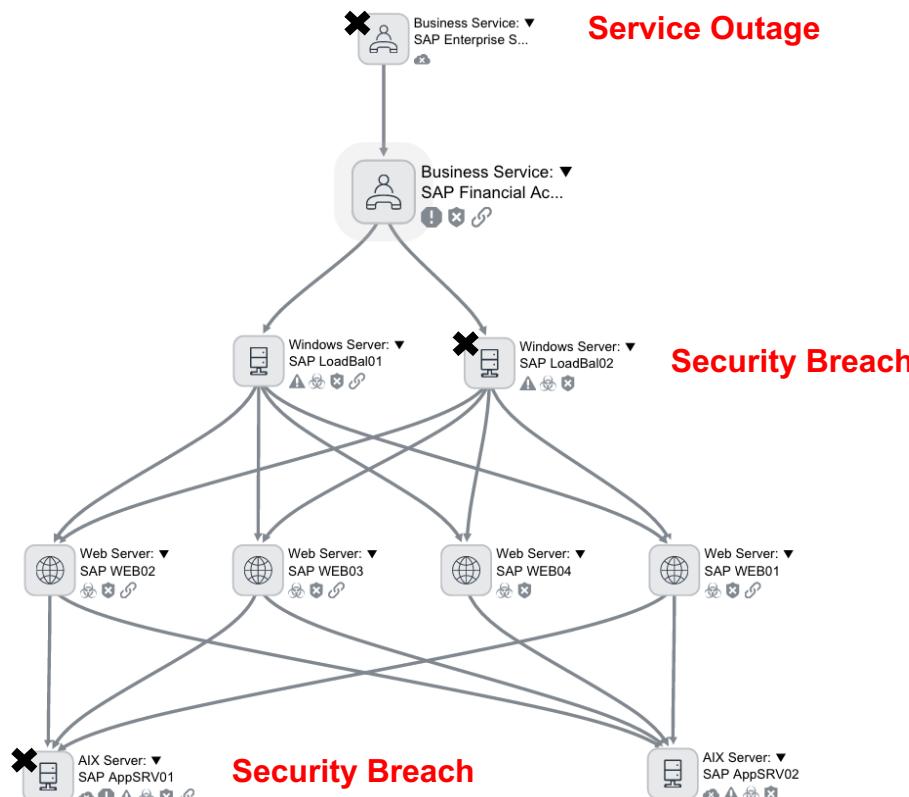
Number	Risk Score	Short Description	Category	Source	State	Last Updated	Created
SIR0010407	99	User Reported Phishing - Subj: Fwd...	Phishing	Email	Contain	Yesterday at 07:54am	Tue at 08:55am
SIR0010415	95	User Reported Phishing - Subj: Fwd...	Phishing	Email	Contain	15hrs ago	21hrs ago

Description

[Open Incident Tab](#)

None				
Assignment group	Assigned to	Business impact	Priority	SLA
SIRT	Deepak Kolingivadi	● 1 - Critical	● 1 - Critical	None
Submitted By	Last Updated By	Threat Indicator	Playbook	Completed Tasks
PM phishing mybytecloud	DK Deepak Kolingivadi	● Yes	Yes	2

Understand Impact Before Taking Action



- ▶ Avoid business disruption when patching or taking systems offline
 - ▶ See the broad impact of an incident affecting multiple systems
 - ▶ Immediately know who owns an asset

Service Mapping automatically maps applications and infrastructure components to business services

See All Relevant Info in One Screen

SIR0010415
User Reported Phishing - Subj: Fwd: Change Your Office 365 Password Immediately 95 (2) Incident State: Contain

Overview Explore Activity Stream

Work notes

- DK Deepak Kolingivadi 15hrs ago
this looks like a company wide campaign
- DK Deepak Kolingivadi 15hrs ago
Checked it and is indeed employee submitted
- JC Add a note.....

Similar Security Incidents

Task	Short Des...	Observable
No records to display		

Affected Users

User	Email	Active
phishing mybytecl	phishing@mybyteclo	true

Threat lookup results

Observa...	Integratio...	Finding
No records to display		

Configuration Items

Configu...	Class	Created

Playbook

Phishing Playbook

> Draft

Analysis (3)

SIT0010978
Is Email Phishing?
COMPLETED DK Deepak Kolingivadi
Outcome: Yes

SIT0010976
Did employee submit the email properly?
COMPLETED SA System Administrator
Outcome: Yes

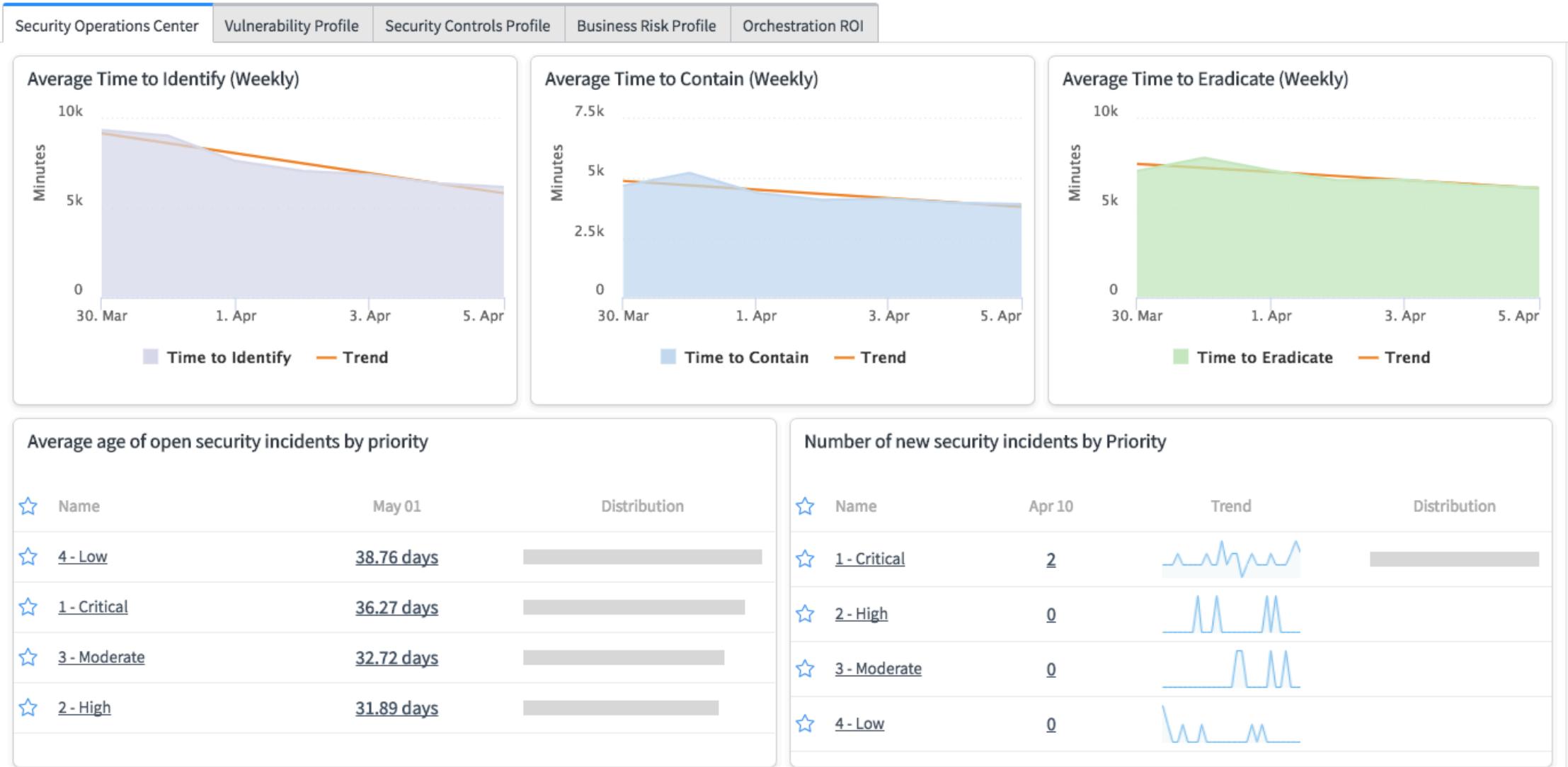
SIT0010979
In-Depth IoC Analysis
TO DO DK Deepak Kolingivadi
Contain (1)

Single system of record captures everything related to the incident:

- Tasks
- Attachments
- Post Incident Reviews
- Work Notes
- Etc.

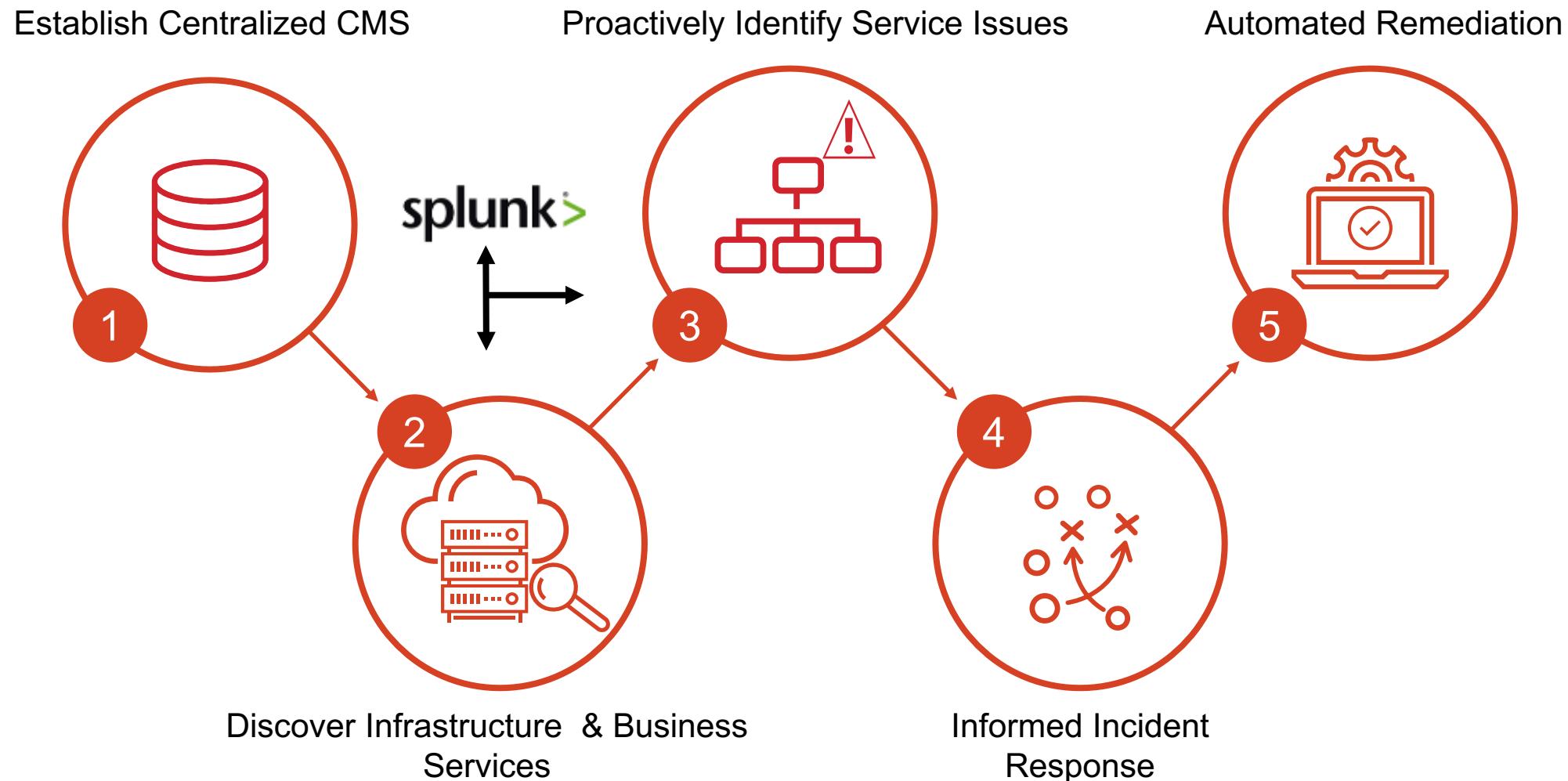
Easy to follow playbooks

Monitor Security Posture and Performance

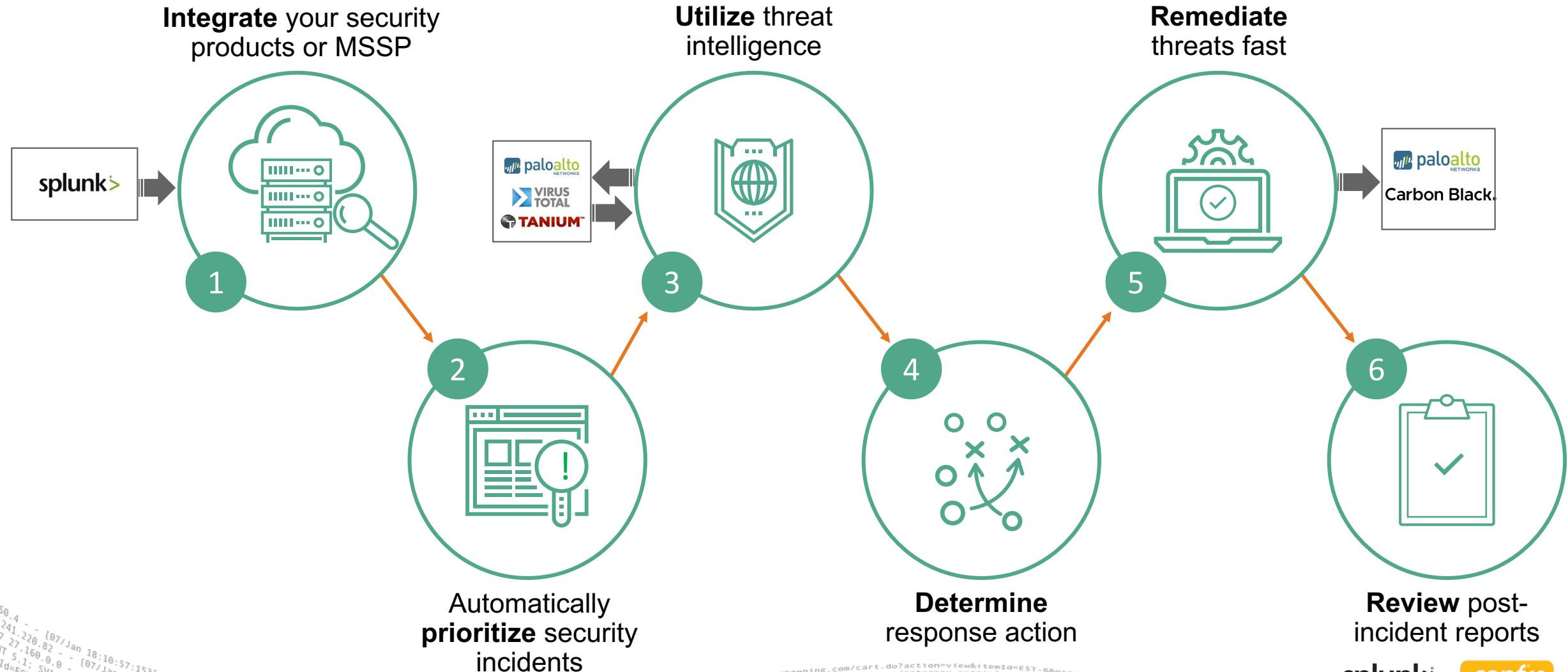


Monitor Outage Trends and Impact

Use Case: Eliminate Service Outages



Use Case: Prioritize & Automate Response



Demo

Responding to a security event with ServiceNow



Measured Value

Forrester Consulting Total Economic Impact™ Study

45%

faster security incident response

25%

faster vulnerability response

60%

faster vulnerability prioritization

Source: Forrester Consulting, The Total Economic Impact™ of ServiceNow Security Operations, January 2018

Q&A

Steve Anderson | Sr. Mgr. PM, ServiceNow
Janene Casella | Director PMM, ServiceNow

Thank You

Don't forget to rate this session
in the .conf18 mobile app

