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> .conf18

Challenges Facing Security Response

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…

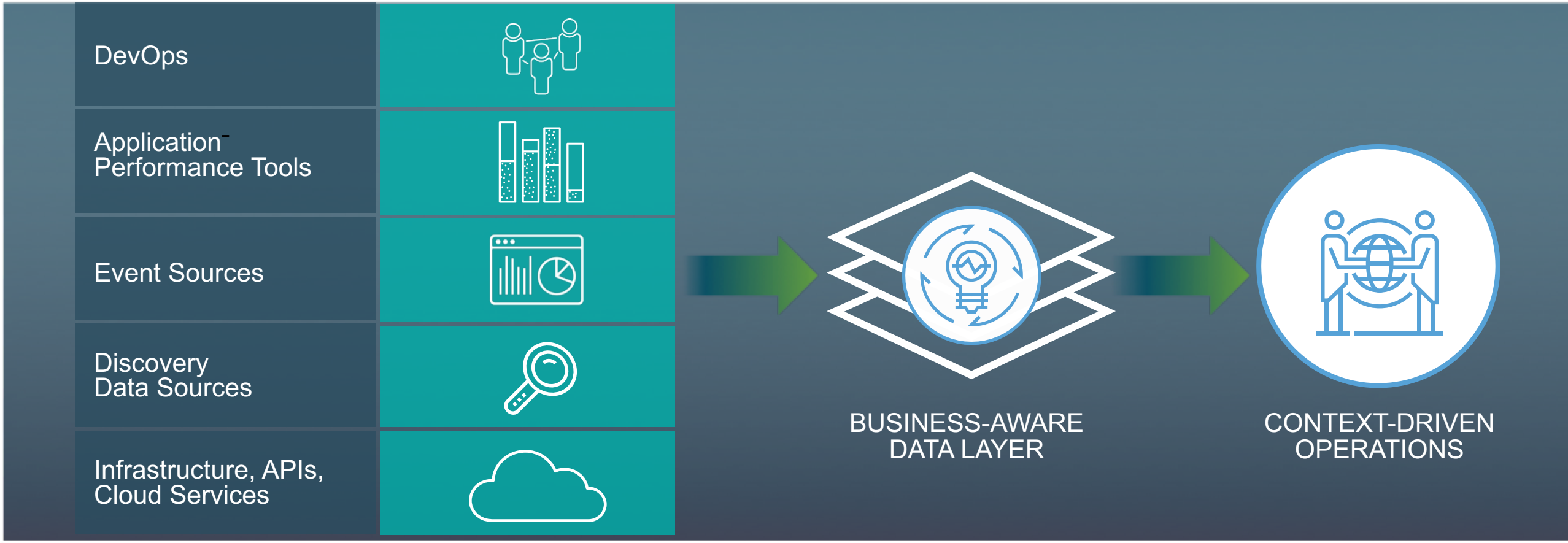
You Need to Know What You Have

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

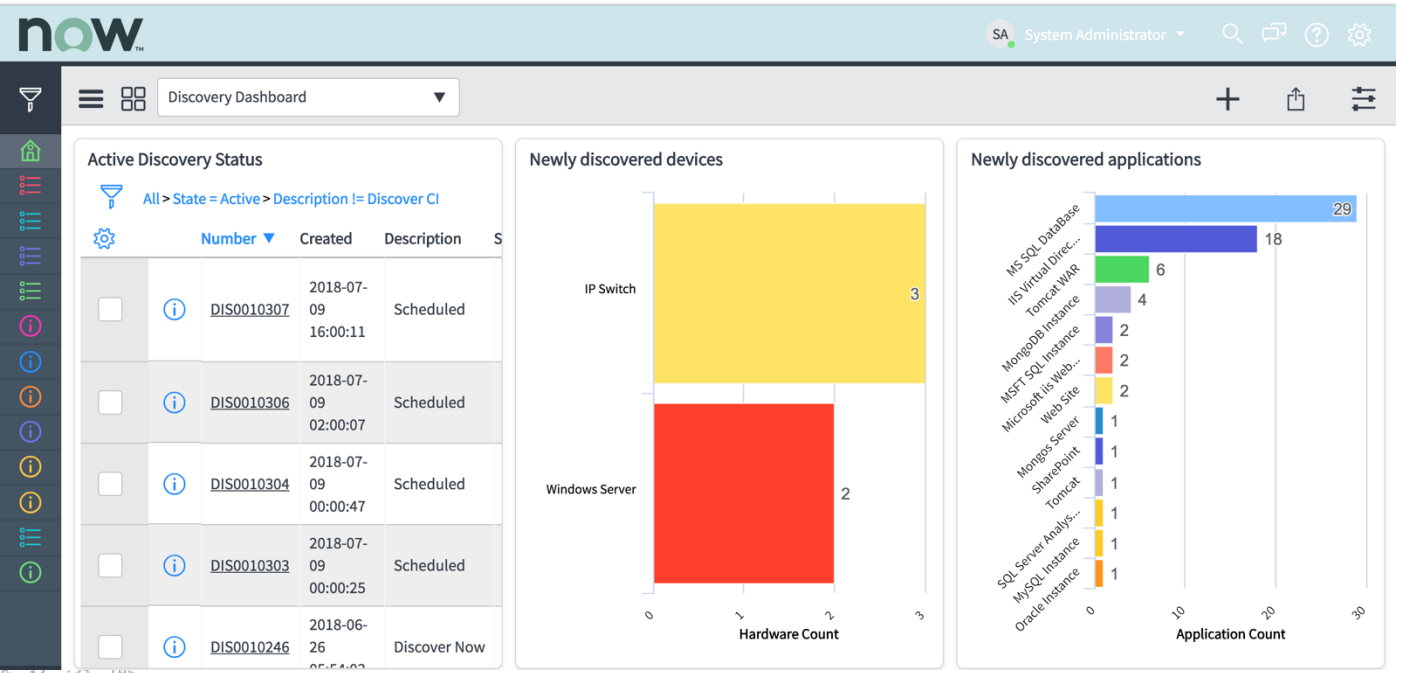
Center for Internet Security Critical Security Controls

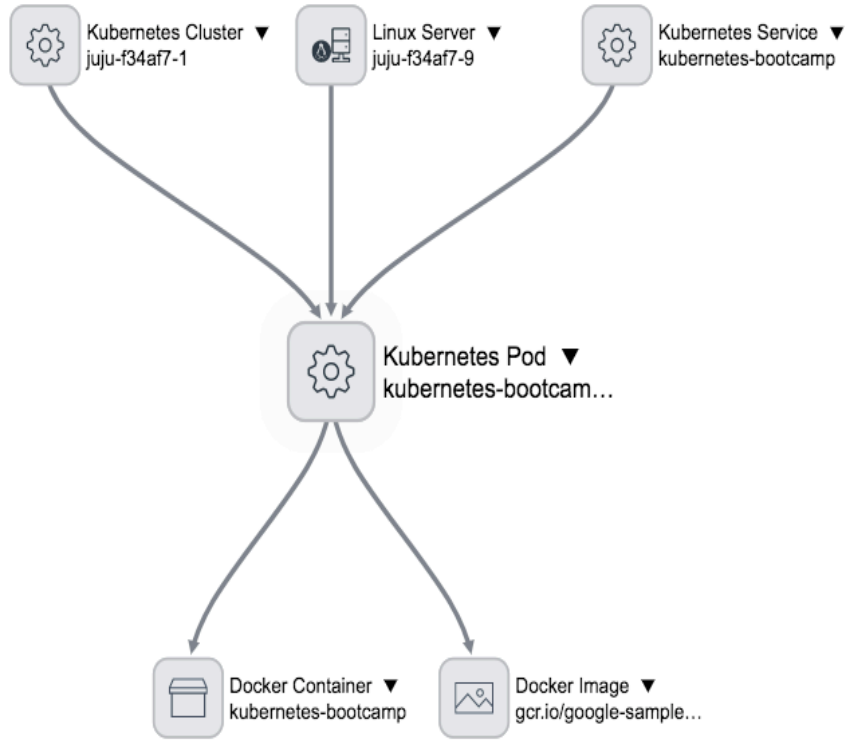
Deliver Real-time Visibility into Enterprise Infrastructure and Services



Uncover your Estate with Discovery

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

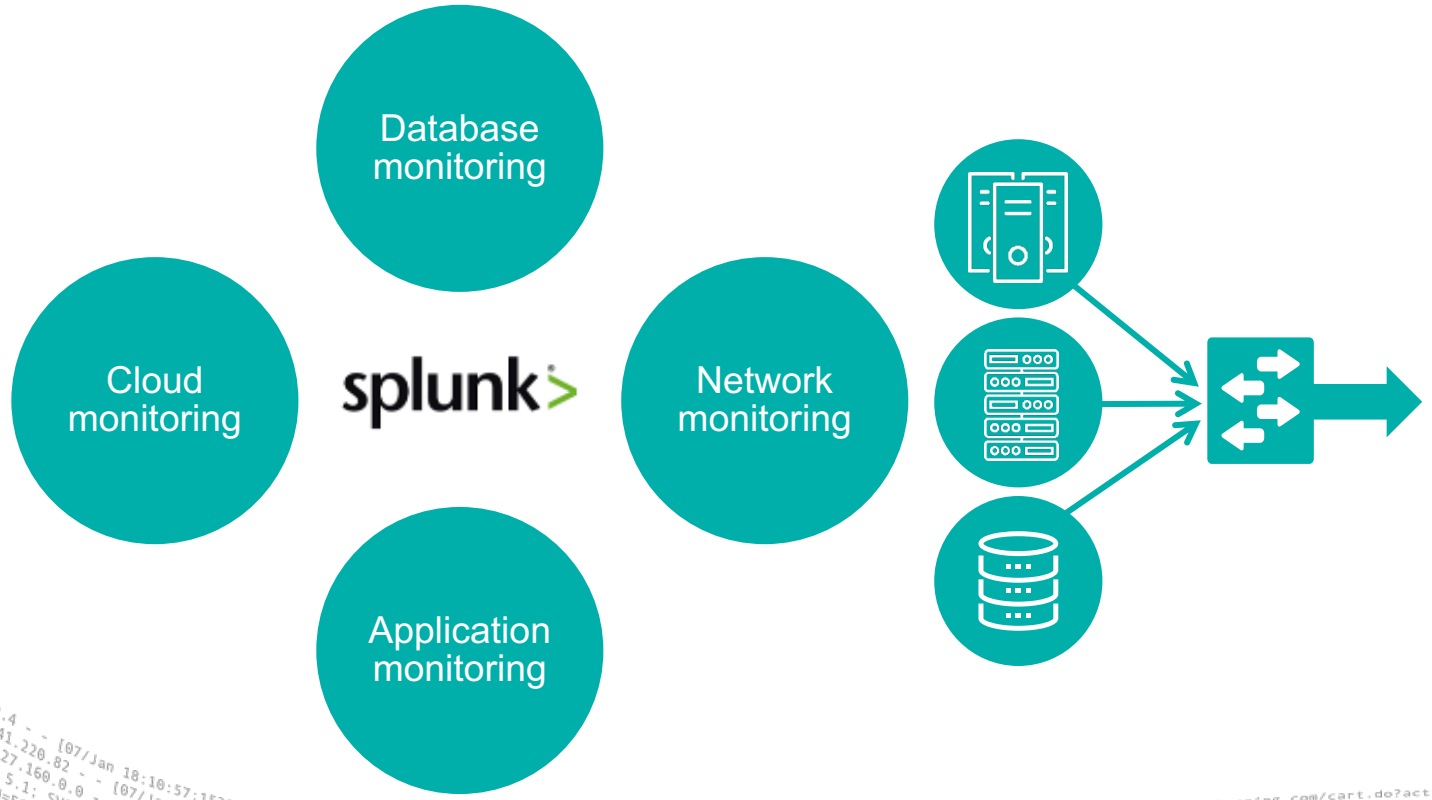


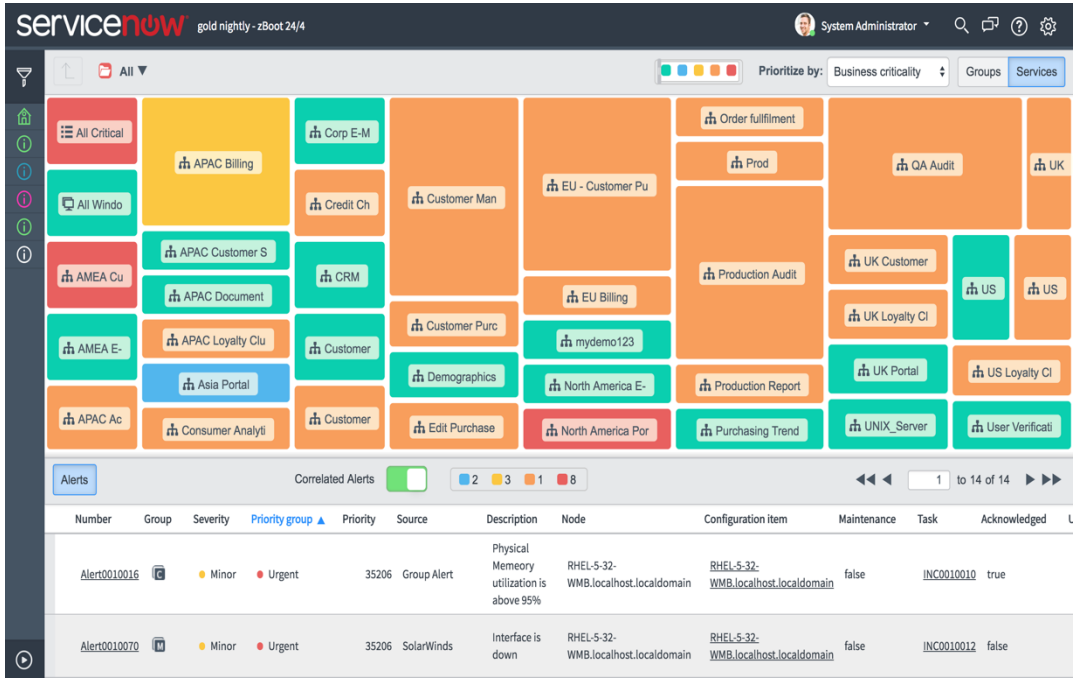


splunk> .conf18

Reduce Noise with ServiceNow Event Management

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

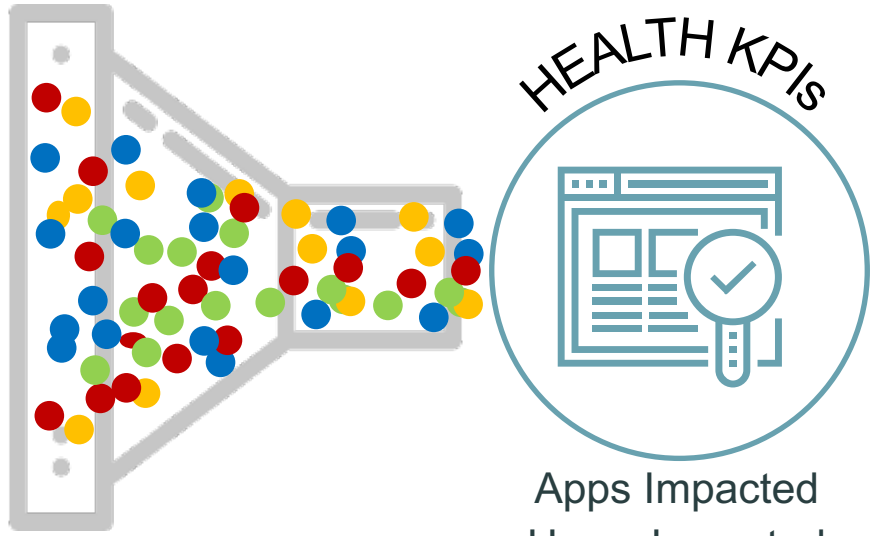




splunk> .conf18

Reduce MTTR with Real-time Correlated View of Health KPIs

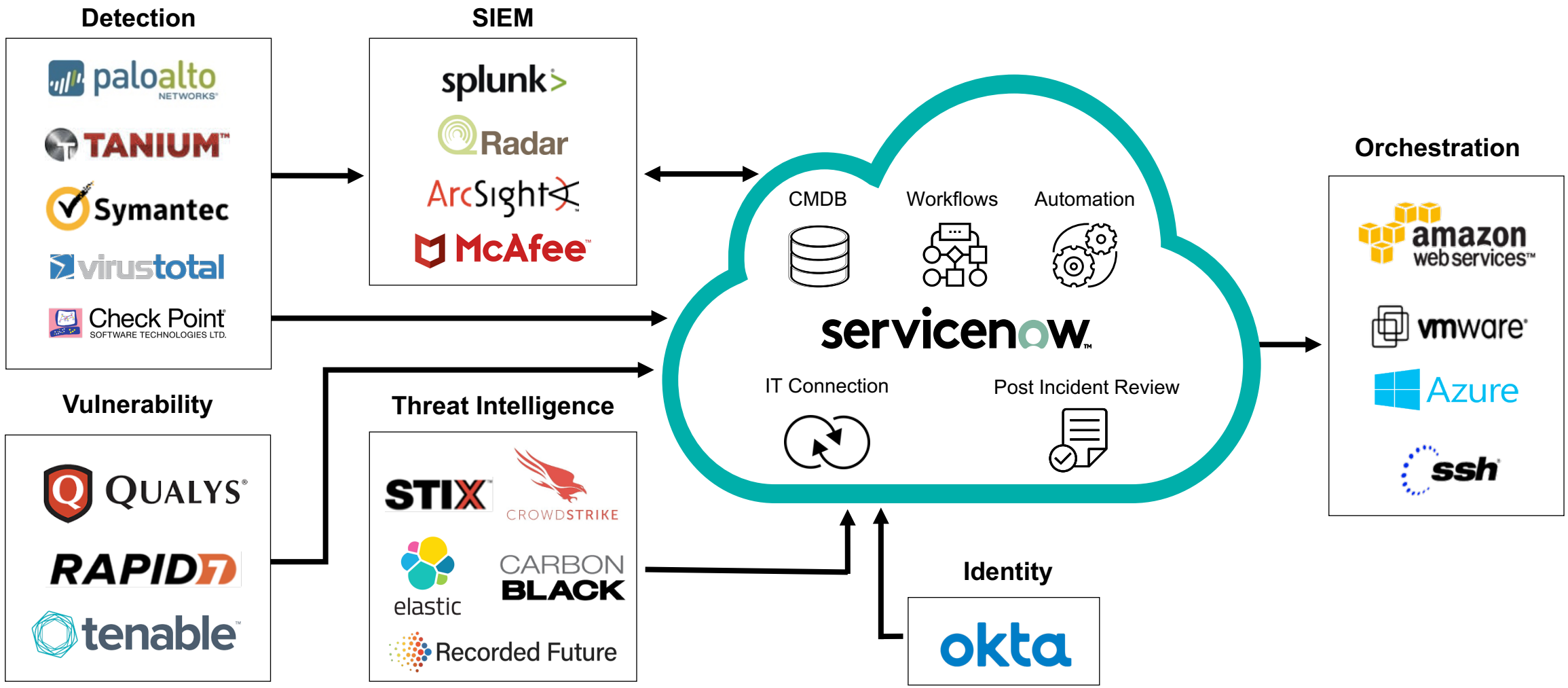
DevOps	
Incident & Change Financial Management	
End User Experience Monitoring	
Application Performance	
Infrastructure, APIs, Cloud Services	



splunk> .conf18

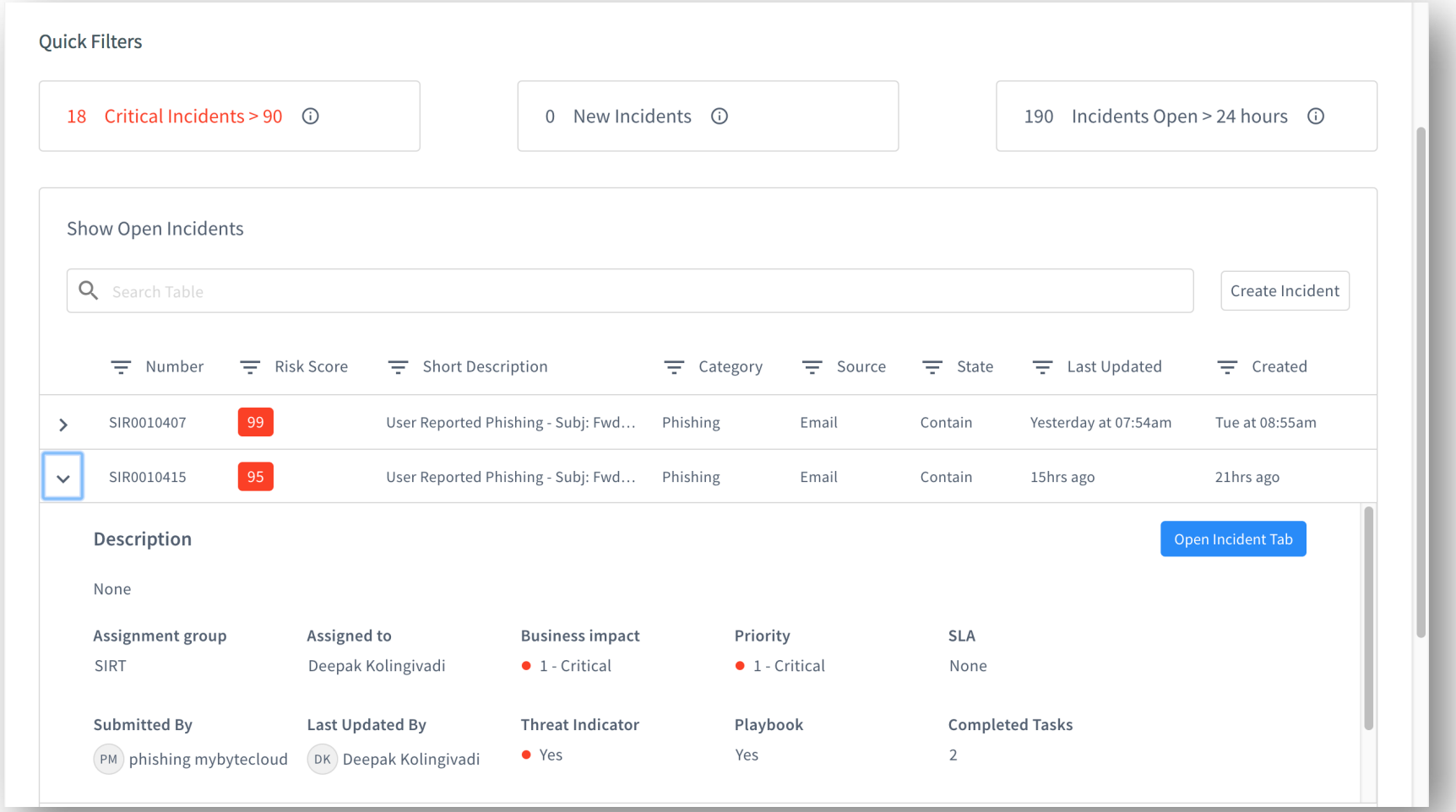
Connect Your Security Tools for Faster Response

ServiceNow Security Operations



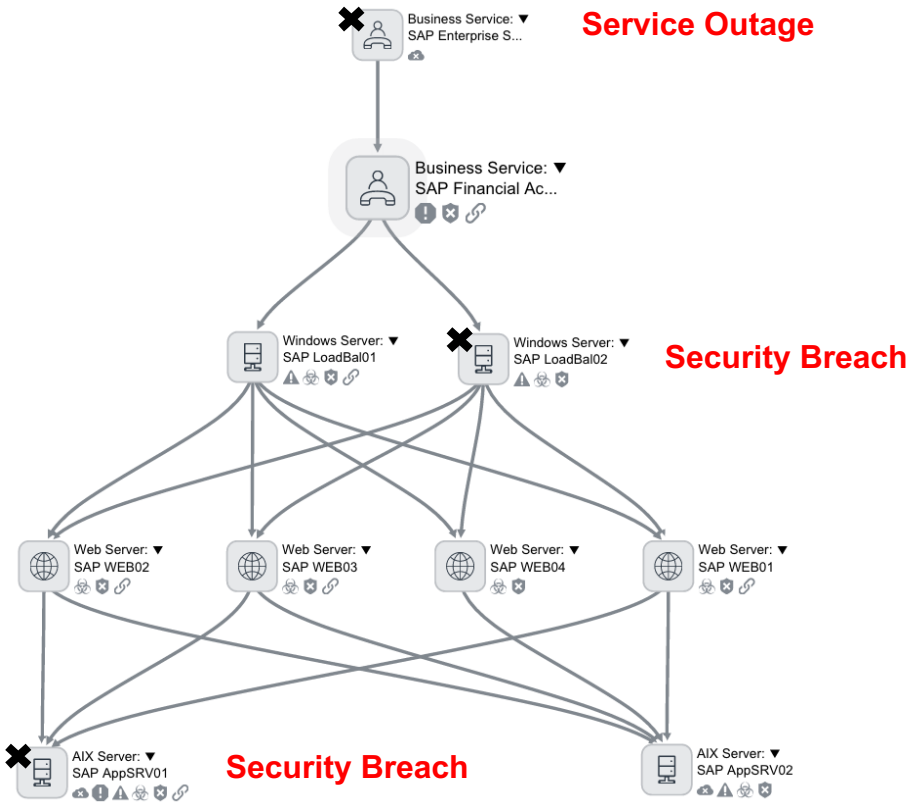
Prioritize Incidents that Impact your Business

- Correlate with CMDB
- Business criticality
- Risk score



splunk> .conf18

Understand Impact Before Taking Action

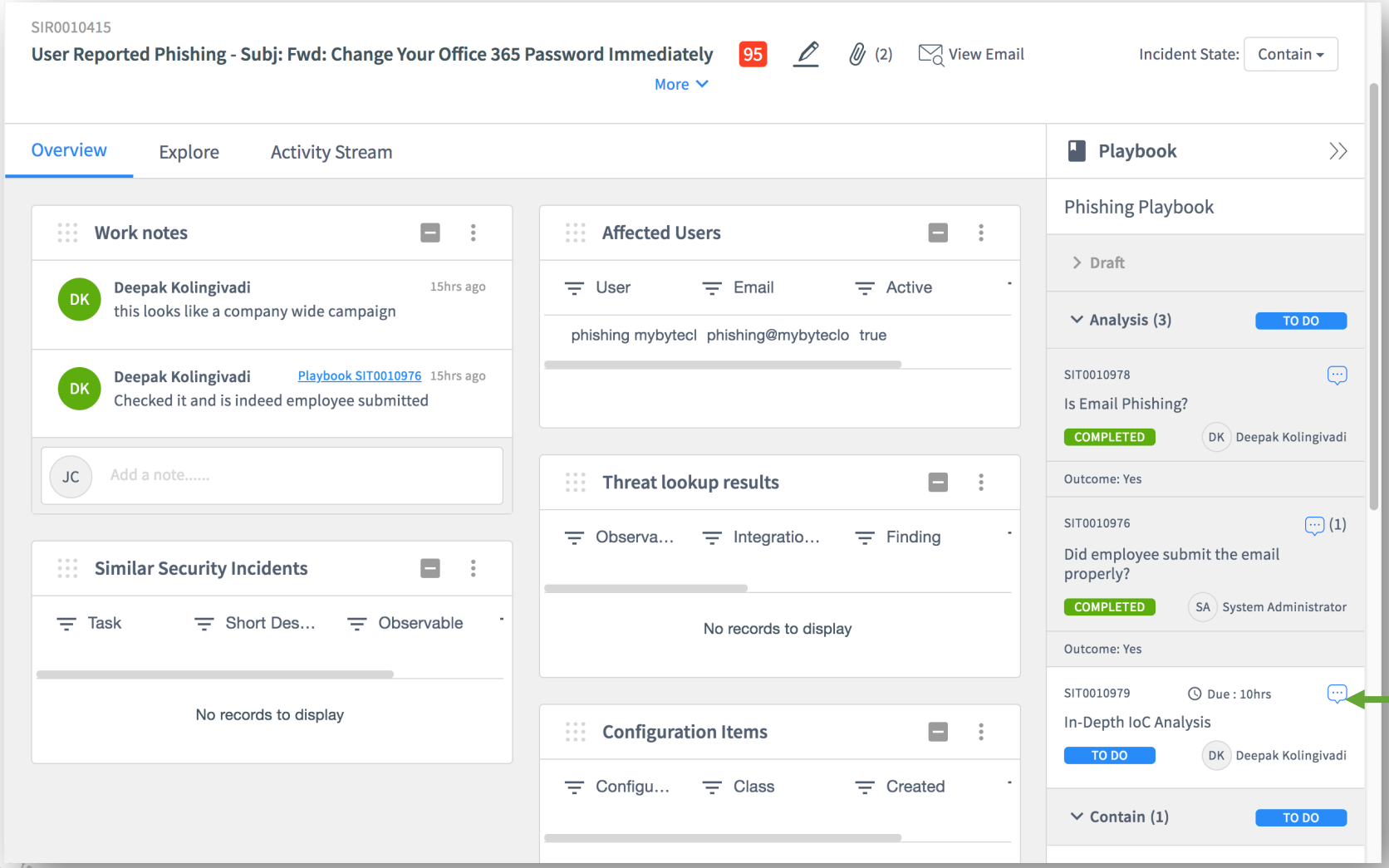


- Avoid business disruption when patching or taking systems offline
- See the broad impact of an incident affecting multiple systems
- Immediately know who owns an asset

Service Mapping automatically maps applications and infrastructure components to business services

splunk> .conf18

See All Relevant Info in One Screen



Single system of record captures everything related to the incident:

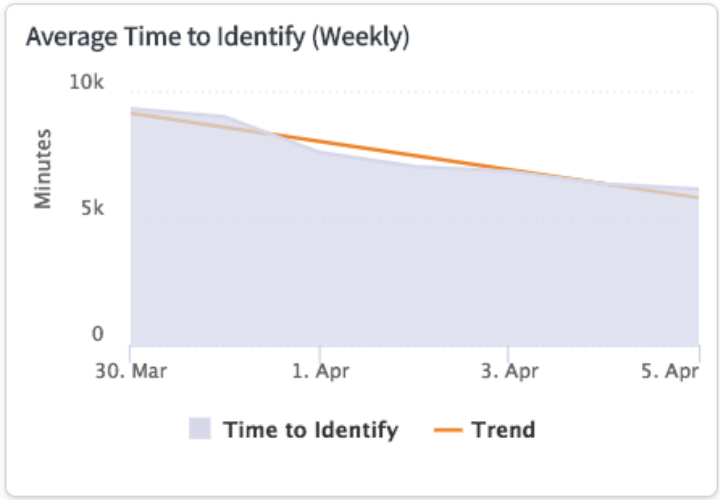
- Tasks
- Attachments
- Post Incident Reviews
- Work Notes
- Etc.

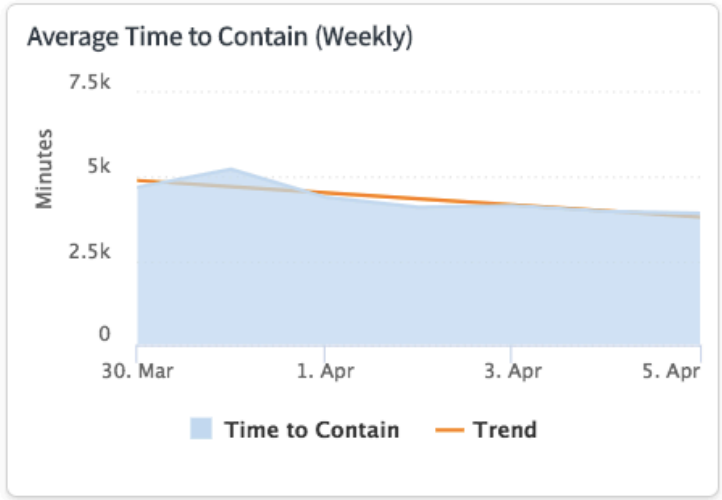
Easy to follow playbooks

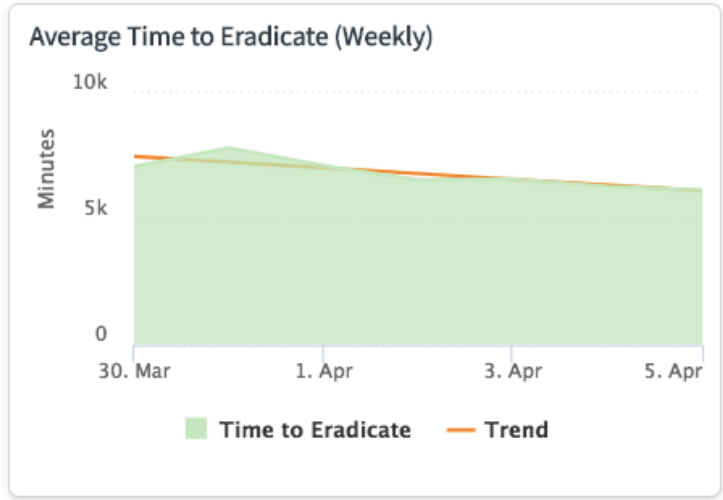
splunk> .conf18

Monitor Security Posture and Performance

Security Operations Center | Vulnerability Profile | Security Controls Profile | Business Risk Profile | Orchestration ROI







Average age of open security incidents by priority

Name	May 01	Distribution
4 - Low	38.76 days	
1 - Critical	36.27 days	
3 - Moderate	32.72 days	
2 - High	31.89 days	

Number of new security incidents by Priority

Name	Apr 10	Trend	Distribution
1 - Critical	2		
2 - High	0		
3 - Moderate	0		
4 - Low	0		

splunk> .conf18

Monitor Outage Trends and Impact

VP of IT Operations

BusinessService.S…

BusinessService.Service

Overview | Cost Analysis | Incident Management | Problem Management | Change Management | Outages Analysis | Vendor Performance | Cloud Overview

Critical Service Outages this Month

Aug 2018

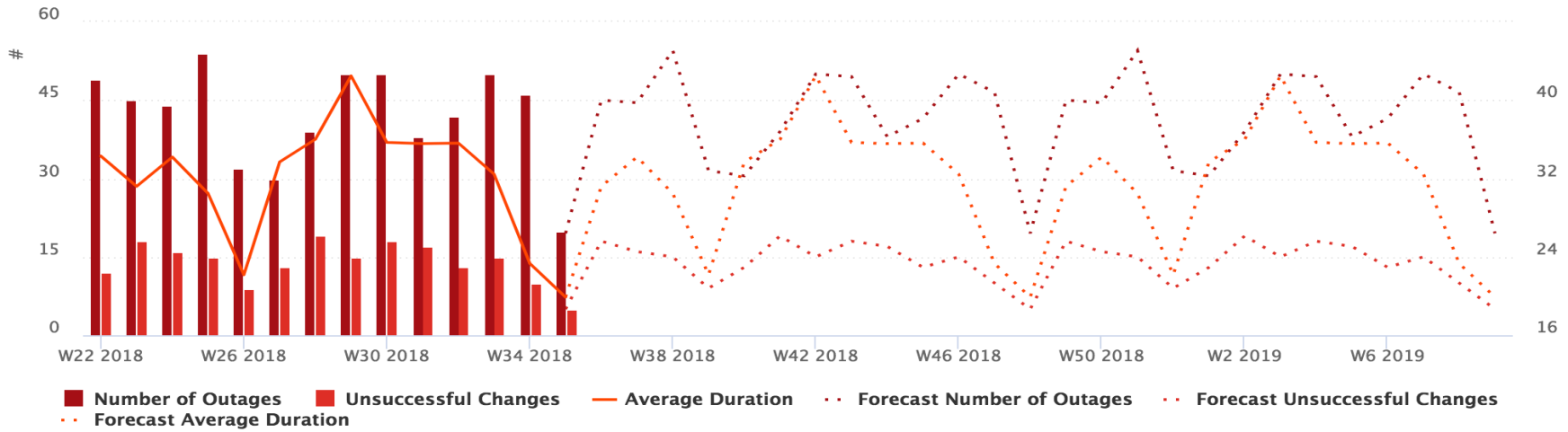
9 Change: ▼ 18 (-66.7%)

Cost Impact of Outages

Aug 2018

$1M Change: ▼ 284k (-20.7%)

Weekly Outage Trends



Number of Outages MtD

Name	Aug 2018	Change %	Trend
QA Audit	27	1,700.0%	
CRM	22	330.0%	
Order Fulfillment Service	14	-3.6%	

Average Duration of Outages

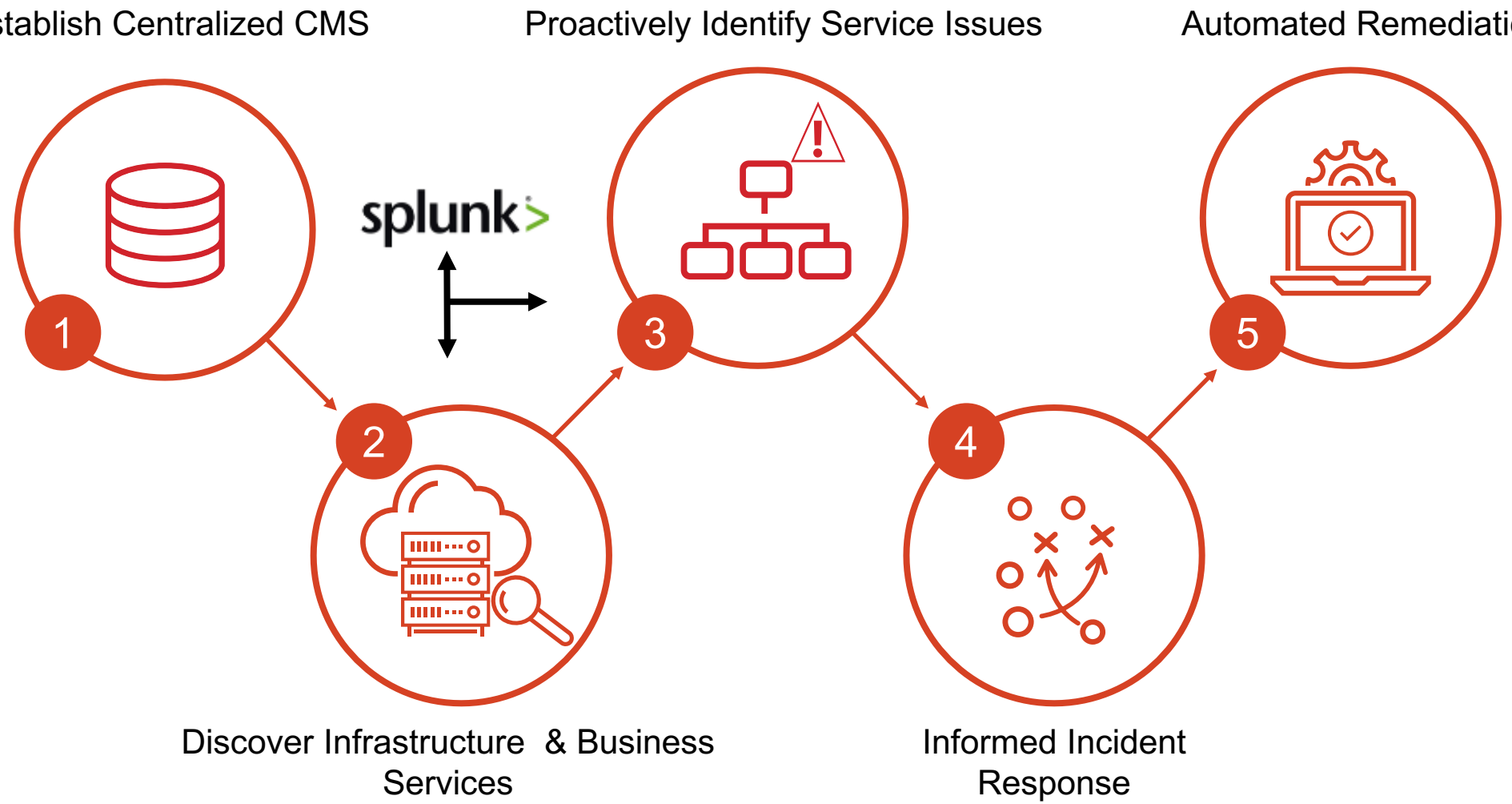
Name	Aug 2018	Change %	Trend
User Verification	43.85 Hrs	7.9%	
Customer Email	43.40 Hrs	1.7%	
APAC Billing	42.29 Hrs	-10.4%	

Cost Impact of Outages

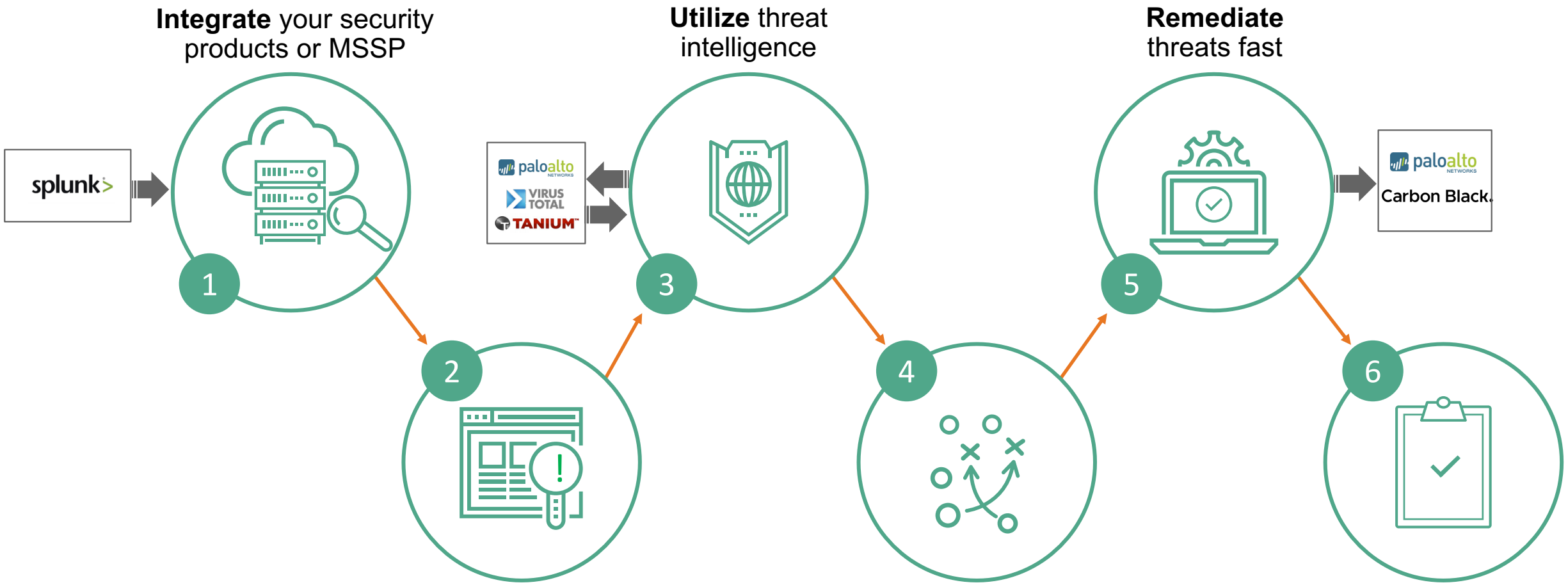
Name	Aug 2018	Change %	Trend
QA Audit	$180k	1,532.5%	
User Verification	$83k	-50.0%	
Order Fulfillment Service	$81k	-19.0%	

splunk> .conf18

Use Case: Eliminate Service Outages



Use Case: Prioritize & Automate Response



splunk> .conf18

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

splunk> .conf18

Thank You

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