knowledge17

WORK at LIGHTSPEED™

The Need for Enterprise Security Response

An Introduction to ServiceNow® Security Operations

JANENE CASELLA
SR. PRODUCT MARKETING MANAGER
ServiceNow

© 2017 ServiceNow All Rights Reserved

servicenow

Session Overview



Objectives

- Resolve security incidents and vulnerabilities faster



What You Will Learn

- Problems Security Operations is designed to solve
- Why we built this solution
- Where it fits in the security ecosystem
- How it works

© 2017 ServiceNow All Rights Reserved

Speaker Introduction



NAME: Janene Casella

TITLE: Sr. Product Marketing Manager

FUNCTION: Security

COMPANY: ServiceNow

EXPERIENCE: 5 years security product marketing, 6 years hardware product management

EXPERTISE: Bridging customers and engineering

CURRENT PROJECTS: ServiceNow Security Operations

© 2017 ServiceNow All Rights Reserved

Organizations have Invested in LOTS of Security Products



But what happens when something goes wrong?

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

© 2017 ServiceNow All Rights Reserved

Security Teams are Overwhelmed

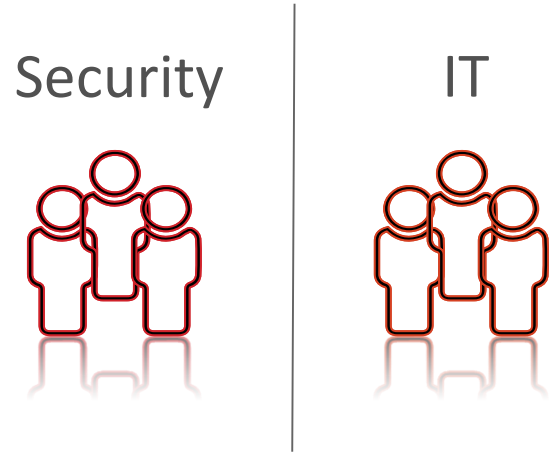
Too Many Alerts & No Context



Manual Tools



Siloed from IT



© 2017 ServiceNow All Rights Reserved

But ServiceNow Can Help

servicenow securityoperations



- Find and Prioritize Critical Threats
  - Business context and threat intelligence enrichment



- Reduce Manual Tasks
  - Automate investigations; orchestrate tools



- Connect Security and IT
  - Single platform for collaboration and accountability

© 2017 ServiceNow All Rights Reserved

Why Did ServiceNow Build a Security Product?

Let’s go back to the year 2012…



© 2017 ServiceNow All Rights Reserved

Introducing Enterprise Security Response



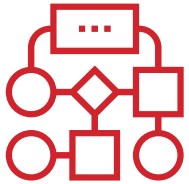
Security Incident Response



Vulnerability Response



Threat Intelligence



Workflow



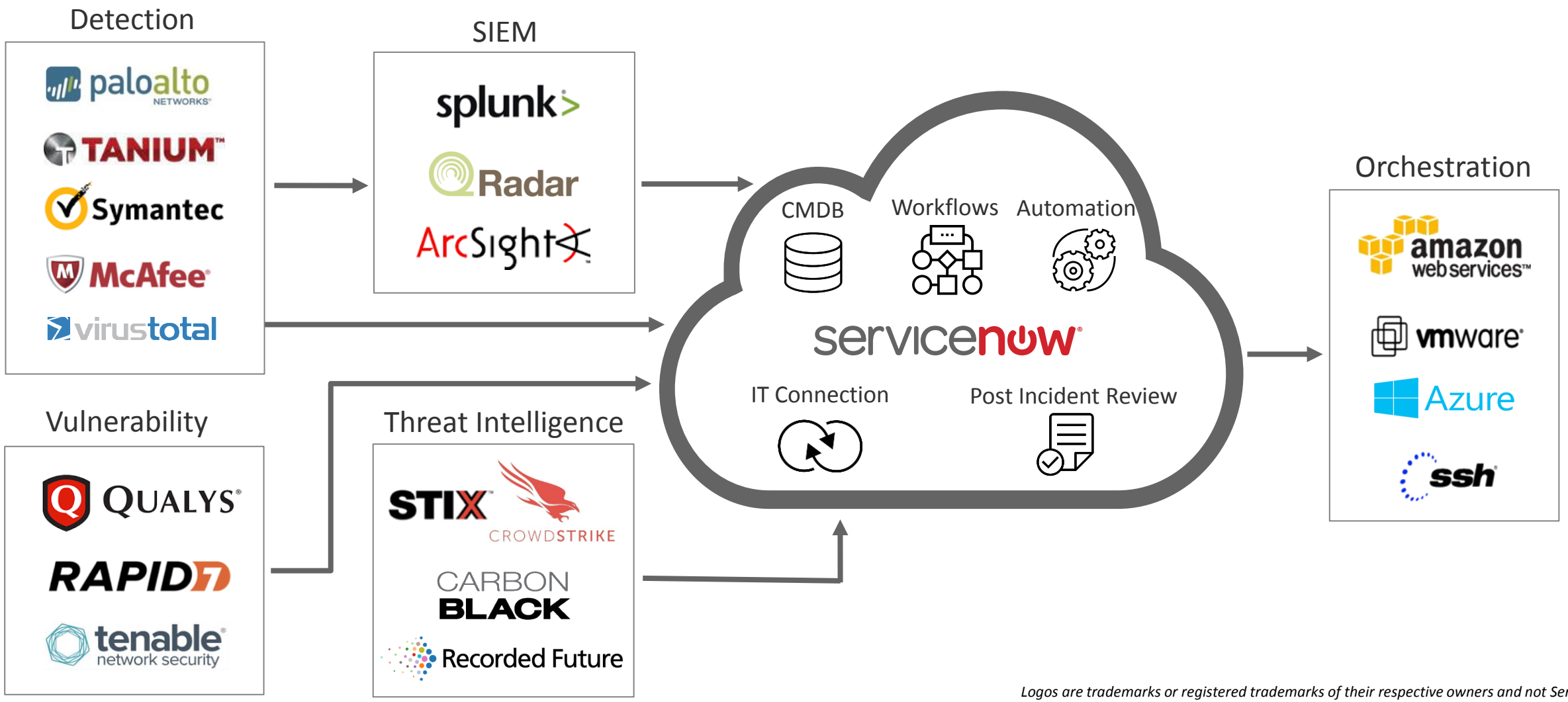
Automation & Orchestration



Deep IT Integration

© 2017 ServiceNow All Rights Reserved

Where Does Security Operations Fit?



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

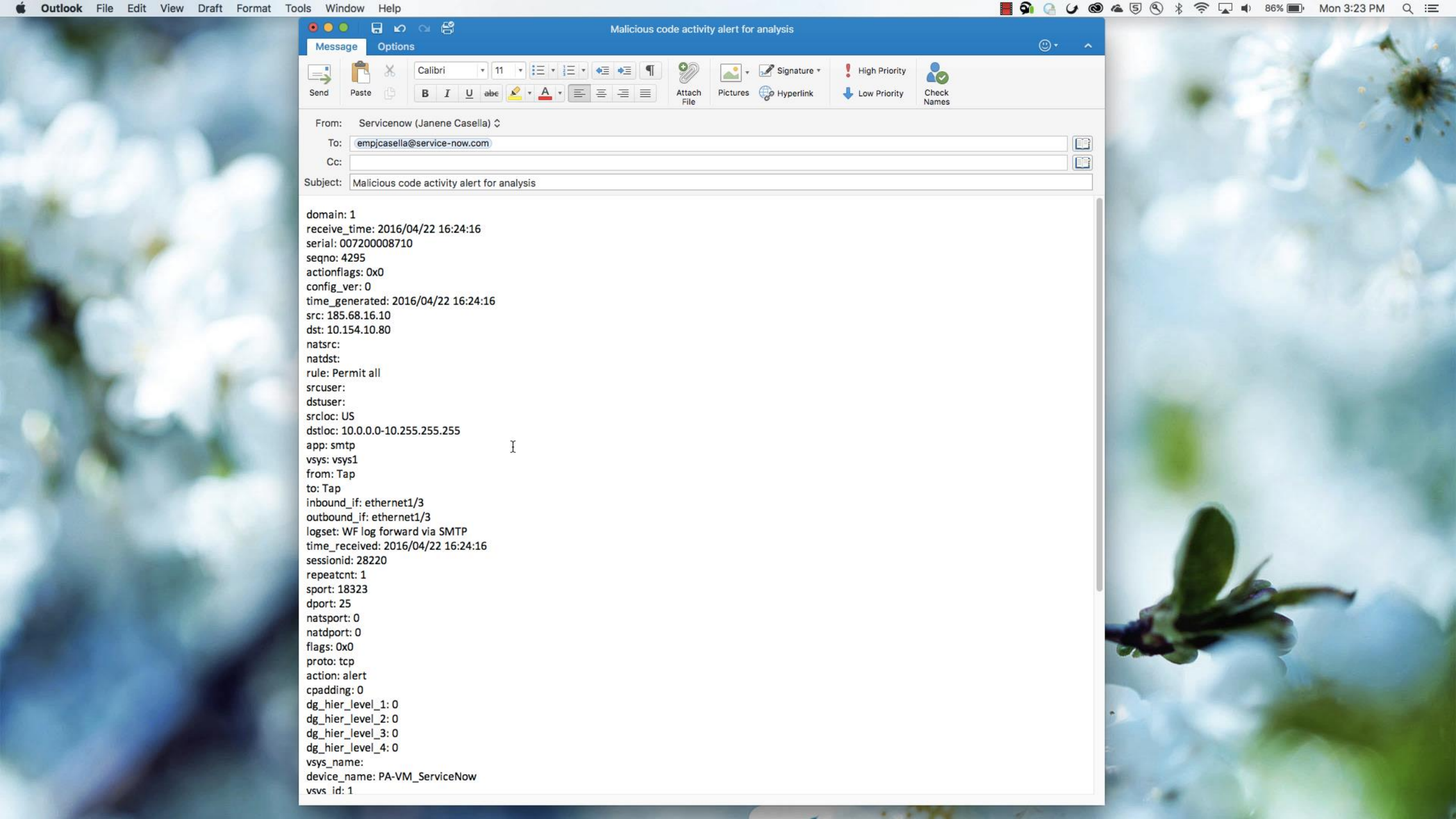
© 2017 ServiceNow All Rights Reserved

With Security Operations, You Can Automatically…

- Prioritize based on the business criticality of the asset
- Correlate threat intelligence data
- Request enrichment from additional security tools
- Assign tasks to the right people
- Apply emergency patches
- Create post-incident reviews



© 2017 ServiceNow All Rights Reserved


Outlook File Edit View Draft Format Tools Window Help
86% Mon 3:23 PM
Malicious code activity alert for analysis
Message Options
Send Paste Calibri 11 Attach File Pictures Signature Hyperlink High Priority Low Priority Check Names
From: Servicenow (Janene Casella)
To: empjcasella@service-now.com
Cc:
Subject: Malicious code activity alert for analysis
domain: 1
receive_time: 2016/04/22 16:24:16
serial: 007200008710
seqno: 4295
actionflags: 0x0
config_ver: 0
time_generated: 2016/04/22 16:24:16
src: 185.68.16.10
dst: 10.154.10.80
natsrc:
natdst:
rule: Permit all
srcuser:
dstuser:
srcloc: US
dstloc: 10.0.0.0-10.255.255.255
app: smtp
vsys: vsys1
from: Tap
to: Tap
inbound_if: ethernet1/3
outbound_if: ethernet1/3
logset: WF log forward via SMTP
time_received: 2016/04/22 16:24:16
sessionid: 28220
repeatcnt: 1
sport: 18323
dport: 25
natsport: 0
natdport: 0
flags: 0x0
proto: tcp
action: alert
cpadding: 0
dg_hier_level_1: 0
dg_hier_level_2: 0
dg_hier_level_3: 0
dg_hier_level_4: 0
vsys_name:
device_name: PA-VM_ServiceNow
vsys_id: 1

Outlook File Edit View Draft Format Tools Window Help

Malicious code activity alert for analysis

Message Options

Send Paste Calibri 11 Attach File Pictures Signature Hyperlink High Priority Low Priority Check Names

From: Servicenow (Janene Casella)

To: empjcasella@service-now.com

Cc:

Subject: Malicious code activity alert for analysis

domain: 1
receive_time: 2016/04/22 16:24:16
serial: 007200008710
seqno: 4295
actionflags: 0x0
config_ver: 0
time_generated: 2016/04/22 16:24:16
src: 185.68.16.10
dst: 10.154.10.80
natsrc:
natdst:
rule: Permit all
srcuser:
dstuser:
srcloc: US
dstloc: 10.0.0.0-10.255.255.255
app: smtp
vsys: vsys1
from: Tap
to: Tap
inbound_if: ethernet1/3
outbound_if: ethernet1/3
logset: WF log forward via SMTP
time_received: 2016/04/22 16:24:16
sessionid: 28220
repeatcnt: 1
sport: 18323
dport: 25
natsport: 0
natdport: 0
flags: 0x0
proto: tcp
action: alert
cpadding: 0
dg_hier_level_1: 0
dg_hier_level_2: 0
dg_hier_level_3: 0
dg_hier_level_4: 0
vsys_name:
device_name: PA-VM_ServiceNow
vsys_id: 1

Security Email Events
Malicious code activity alert for analysis

From	janene.casella@servicenow.com
To	empjcasella@service-now.com
Subject	Malicious code activity alert for analysis
Body	domain: 1 receive_time: 2016/04/22 16:24:16 serial: 007200008710 seqno: 4295 actionflags: 0x0 config_ver: 0 time_generated: 2016/04/22 16:24:16 src: 185.68.16.10 dst: 10.154.10.80 natsrc: natdst: rule: Permit all srcuser: dstuser: srcloc: US dstloc: 10.0.0.0-10.255.255.255 app: smtp vsys: vsys1 from: Tap to: Tap inbound_if: ethernet1/3 outbound_if: ethernet1/3 logset: WF log forward via SMTP
Matched	☑

Related Links

Force to Update Set

Security Incident
SIR0012006

Follow | Update | Add Response Task | Lookup attachments | Cancel | Delete

Manage Attachments (3): 9ac69101daee24a43f98f5895415abb1b4b5905020ad93c51254e51e2169e0fe.pdf [rename] [view] 9ac69101daee24a43f98f5895415abb1b4b5905020ad93c51254e51e2169e0fe.xml [rename] [view]

Draft ✓ | Analysis | Contain | Eradicate | Recover | Review | Closed

Number	SIR0012006	Opened	2017-04-03 15:26:43
Requested by		State	Analysis
Configuration item	SAP AppSRV01	Substate	-- None --
Affected user		Source	-- None --
Location	4193 University Avenue, San Diego,CA	Business criticality	1 - Critical
Category	-- None --	Priority	1 - Critical
Subcategory	-- None --	Assignment group	Security Incident Assignment
		Assigned to	Waldo Sisk

* Short description: Malicious code activity alert for analysis

Knowledge results

CWE-506: Embedded Malicious Code	CWE ID: 506More Information Embedded Malicious Code Status: IncompleteType: Weakness Description The application contains code that appears...	Preview Attach
CWE-508: Non-Replicating Malicious Code	CWE ID: 508More Information Non-Replicating Malicious Code Status: IncompleteType: Weakness Description Non-replicating malicious code	Preview Attach
CWE-509: Replicating Malicious Code (Vir...	CWE ID: 509More Information Replicating Malicious Code (Virus or Worm) Status: IncompleteType: Weakness Description Replicating malicious <...	Preview Attach
Malicious Code	Software (e.g., Trojan horse) that appears to perform a useful or desirable function, but actually gains unauthorized access to system resources or tricks a use...	Preview Attach

Malicious Code	Software (e.g., Trojan horse) that appears to perform a useful or desirable function, but actually gains unauthorized access to system resources or tricks a use...	Preview Attach
CWE-545: Use of Dynamic Class Loading	Description Dynamically loaded code has the potential to be malicious. Time of Introduction Architecture and Design Implementation Common Consequ...	Preview Attach

Incident Details | Related Records | Security Incident Observables | Enrichment Data | Threat Intelligence | Vulnerability Details | Post Incident Review

Source IP	185.68.16.10	Malware hash	9ac69101daee24a43f98f5895415abb1b4b590502 0ad93c51254e51e2169e0fe
Destination IP	10.154.10.80	Other IoC	
Malware URL			
Referrer URL			

Update | Add Response Task | Lookup attachments | Cancel | Delete

Related Links

View Manual Runbook
Response Workflow
Scan for Vulnerabilities
Force to Update Set

Response Tasks | Task SLAs (1) | Configuration Items (1) | Affected Users | Groups Associated to CIs | Child Security Incidents | Similar Security Incidents (30) | Similar Security Incidents (30) | Exchange Search | Affected Services (9)
Security Scan Requests (1) | Risks

Response Tasks New Go to Number Search

		Preview	Attach
Malicious Code	Software (e.g., Trojan horse) that appears to perform a useful or desirable function, but actually gains unauthorized access to system resources or tricks a use...	Preview	Attach
CWE-545: Use of Dynamic Class Loading	Description Dynamically loaded code has the potential to be malicious. Time of Introduction Architecture and Design Implementation Common Consequ...	Preview	Attach

Incident Details | Related Records | Security Incident Observables | Enrichment Data | Threat Intelligence | Vulnerability Details | Post Incident Review

Security Enrichment Data

1 to 2 of 2

Name	Configuration item	Reference value	Enrichment mapping	Created
Retrieve Malware Results		9ac69101daee24a43f98f5895415abb1b4b59050...	Palo Alto WildFire	2017-04-03 15:26:59
Retrieve Malware Results		{"operator":"all","children":[{"field":"...	Palo Alto AutoFocus	2017-04-03 15:27:22

Malware Results

1 to 2 of 2

Malware Type	Value	Possible malware	Source	First found
Hash	9ac69101daee24a43f98f5895415abb1b4b59050...	yes	Retrieve Malware Results	2017-04-03 15:27:02
IP	185.68.16.10	UNKNOWN	Retrieve Malware Results	2017-04-03 15:27:22

Running Processes

Name ▲	Configuration item	Owner	Owner SID	Owner domain	PID	Path	Hash	Source	Created

Configuration Item	Applied	Applied date	Manual proposed change	XML
SAP AppSRV01	false	(empty)	false	

Users with Similar IoC

User

Update | Add Response Task | Lookup attachments | Cancel | Delete

Related Links

View Manual Runbook
Response Workflow
Scan for Vulnerabilities
Force to Update Set

Response Tasks | Task SLAs (1) | Configuration Items (1) | Affected Users | Groups Associated to CIs | Child Security Incidents | Similar Security Incidents (1) | Similar Security Incidents (1) | Exchange Search | Affected Services (9)
Security Scan Requests (1) | Risks

Task SLAs | New | Go to | SLA definition | Search | 1 to 1 of 1

Task = SIR0012006

SLA definition	Stage	Start time	Breach time	Actual elapsed time	Actual elapsed percentage	Actual time left	Business elapsed time	Business elapsed percentage	E
15 minute	In progress	2017-04-03 15:26:47	2017-04-03 15:41:47	0 Seconds	0	15 Minutes	0 Seconds	0	15 M

Actions on selected rows... | 1 to 1 of 1

Update | Add Response Task | Lookup attachments | Cancel | Delete

Related Links

View Manual Runbook
Response Workflow
Scan for Vulnerabilities
Force to Update Set

Response Tasks | Task SLAs (1) | Configuration Items (1) | Affected Users | Groups Associated to CIs | Child Security Incidents | Similar Security Incidents (30) | Similar Security Incidents (30) | Exchange Search | Affected Services (9)
Security Scan Requests (1) | Risks

Affected Services | New | Edit... | Go to Business Service | Search | 1 to 9 of 9

Task = SIR0012006

Business Service	Manually added
SAP Labor Distribution	false
SAP Enterprise Services	false
SAP Controlling	false
SAP Financial Accounting	false
SAP Human Resources	false
SAP Plant Maintenance	false
SAP Materials Management	false
SAP Sales and Distribution	false
SAP Payroll	false

1 to 9 of 9

Security Technology Partners































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

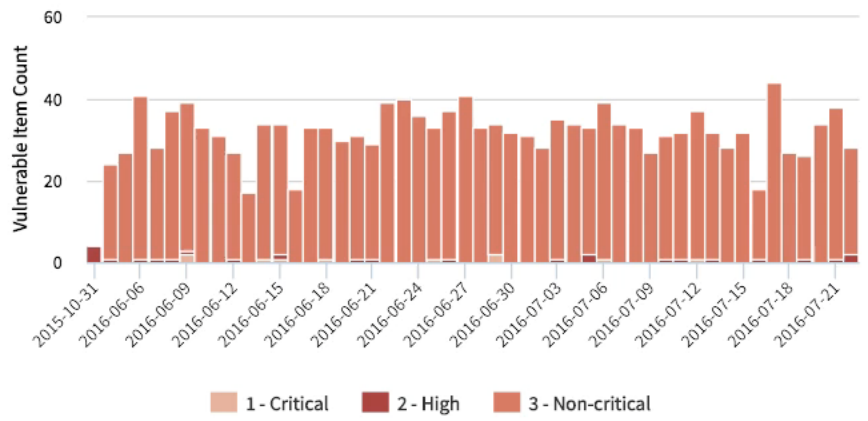
© 2017 ServiceNow All Rights Reserved

Add content

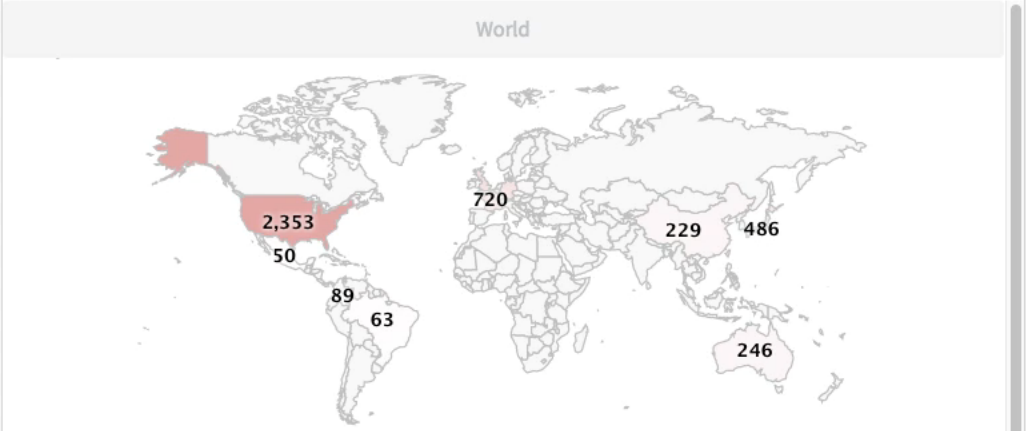
My Vulnerability Explorer (Advanced)

Change Layout

Vulnerability Trend by Business Criticality



Vulnerability Map



Matching Vulnerabilities

6,122

CVE Identifier

All

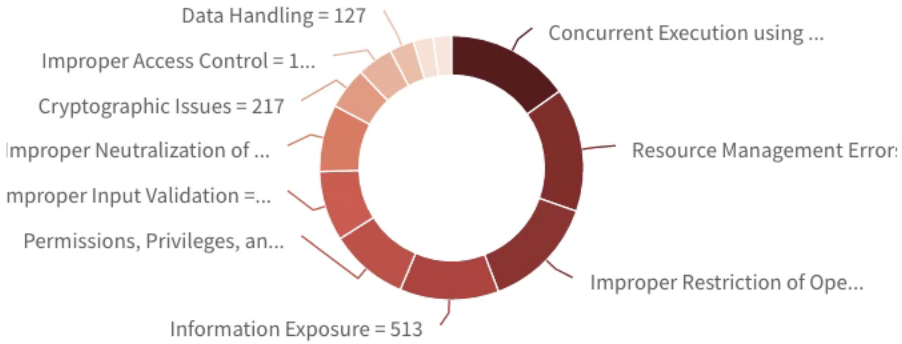
Vulnerability Business Criticality

- [x] All
- [x] 1 - Critical
- [x] 2 - High
- [x] 3 - Non-critical

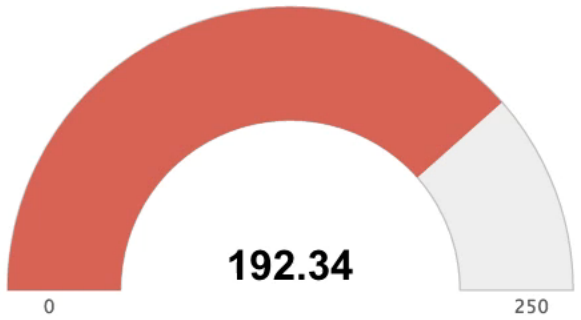
Vulnerability Active

- (•) All
- ( ) True
- ( ) False

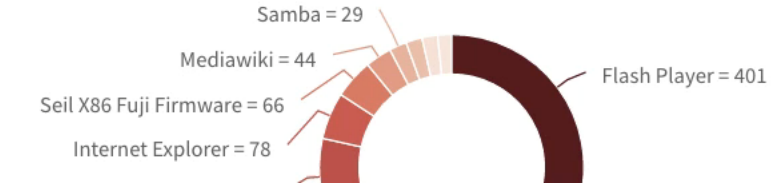
Most Prolific CWEs



Average Vulnerability Age



Most Vulnerable Models



Vulnerabilities by Assignment Group and Business Criticality

Change Management	6	12
Database	5	13



	1 - Critical	2 - High
Service Desk	11	11
Vulnerability Res...	4	72

Vulnerability Significance

Category: Vulnerability Significance: ...

Indicator: Vulnerability Significance: Critical

Services with Critically Significant Vulnerabilities





	1 - Critical	2 - High
Service Desk	11	11
Vulnerability Res...	4	72

Vulnerable Item
VIT0010140

Follow | Update | Close/Ignore | Create Change | Create Problem | Create Security Incident | Delete

Number	VIT0010140	State	Analysis
Configuration item	Product KIOSK	Substate	Awaiting Change
Business criticality	1 - Critical	Change Request	
Priority	1 - Critical	Assignment group	Vulnerability Response
		Assigned to	

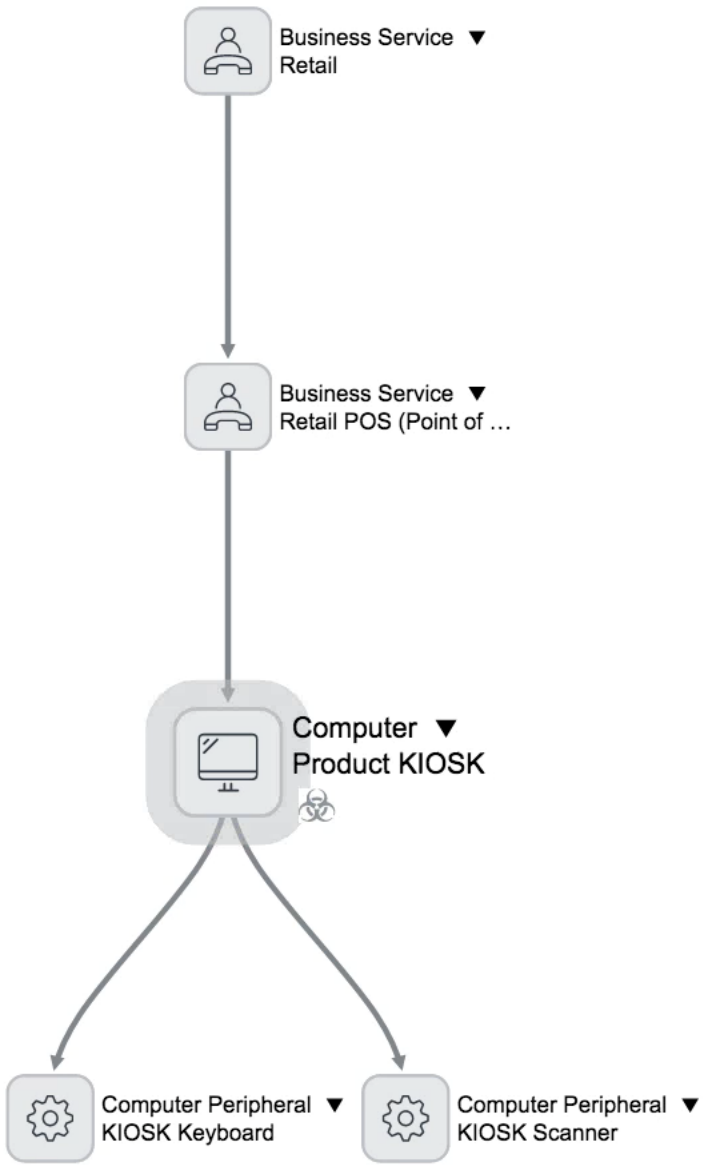
Vulnerability | Configuration Details | Notes | Qualys

Vulnerability	CVE-2015-0314	First found	2017-01-18
Vulnerable software	Adobe Flash Player 11.0.1.152	Last found	2017-03-22
Installation	Linux Linux Kernel 2.0.3	Times found	3

Update | Close/Ignore | Create Change | Create Problem | Create Security Incident | Delete

Related Links

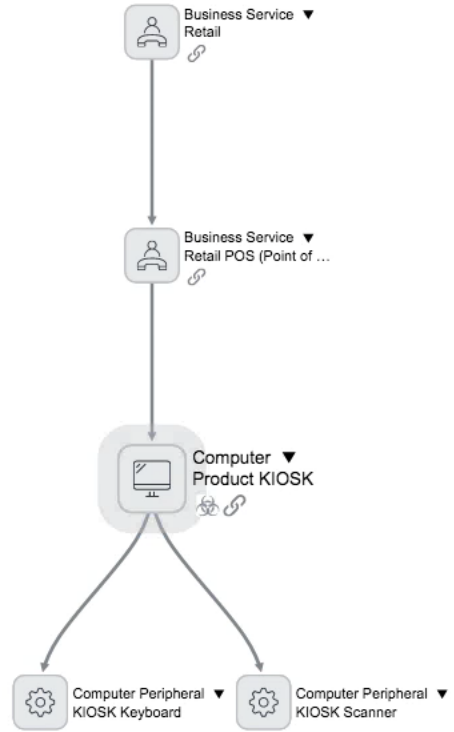
Calculate Criticality
Force to Update Set
Scan for Vulnerabilities
Show Workflow


Business Service
Retail
Business Service
Retail POS (Point of …
Computer
Product KIOSK
Computer Peripheral
KIOSK Keyboard
Computer Peripheral
KIOSK Scanner

Product KIOSK

Search for CI

Vertical | Horizontal | Radial | Force | Group | Details



Alerts | Changes - current | Financial Risk | Incident | PCI Risk | PII Risk | Problem | Security Incident | Vulnerable Item | Related Business Services

1 to 6 of 12

Number	State	Configuration item	Vulnerability	Last found
VIT0010140	Analysis	Product KIOSK	CVE-2015-0314	2017-03-22
VIT0005523	New	Product KIOSK	CVE-2015-0240	2016-11-29
VIT0005329	New	Product KIOSK	CVE-2015-0669	2016-10-14
VIT0004613	New	Product KIOSK	CVE-2015-0239	2016-10-29
VIT0004587	New	Product KIOSK	CVE-2015-0124	2016-10-08
VIT0003829	New	Product KIOSK	CVE-2015-0637	2016-10-07

ID	CVE-2015-0314	Date published	2015-02-05
CWE Entry		Last modified	2015-02-20

Summary: Adobe Flash Player before 13.0.0.269 and 14.x through 16.x before 16.0.0.305 on Windows and OS X and before 11.2.202.442 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-0316, CVE-2015-0318, CVE-2015-0321, CVE-2015-0329, and CVE-2015-0330.

Common Vulnerability Scoring System

Vulnerability score	10	Score generated	2015-02-06
Access vector	Network	Source	http://nvd.nist.gov
Access complexity	3 - Low		
Confidentiality impact	Complete		
Integrity impact	Complete		
Availability impact	Complete		
Authentication	-- None --		

Related Links

Force to Update Set

Vulnerable Items (8) | Vulnerable Software (16) | Vulnerability References (11)

Vulnerable Items | New | Search | for text | Search | 1 to 8 of 8

Vulnerability = CVE-2015-0314

Configuration item	Vulnerable software	Last found
Product KIOSK	Adobe Flash Player 11.0.1.152	2017-03-22

Adobe Security Bulletin

Security updates available for Adobe Flash Player

Release date: February 5, 2015

Last updated: February 19, 2015

Vulnerability identifier: APSB15-04

Priority: See table below

CVE number: CVE-2015-0313, CVE-2015-0314, CVE-2015-0315, CVE-2015-0316, CVE-2015-0317, CVE-2015-0318, CVE-2015-0319, CVE-2015-0320, CVE-2015-0321, CVE-2015-0322, CVE-2015-0323, CVE-2015-0324, CVE-2015-0325, CVE-2015-0326, CVE-2015-0327, CVE-2015-0328, CVE-2015-0329, CVE-2015-0330, CVE-2015-0331

Platform: All Platforms

Summary

Adobe has released security updates for Adobe Flash Player for Windows, Macintosh and Linux. These updates address vulnerabilities that could potentially allow an attacker to take control of the affected system.

Adobe is aware of reports that CVE-2015-0313 is actively being exploited in the wild via drive-by-download attacks against systems running Internet Explorer and Firefox on Windows 8.1 and below. Adobe recommends users update their product installations to the latest versions:

- Users of the Adobe Flash Player desktop runtime for Windows and Macintosh should update to Adobe Flash Player 16.0.0.305.
- Users of the Adobe Flash Player Extended Support Release should update to Adobe Flash Player 13.0.0.269.
- Users of Adobe Flash Player for Linux should update to Adobe Flash Player 11.2.202.442.
- Adobe Flash Player installed with Google Chrome, as well as Internet Explorer on Windows 8.x, will automatically update to version 16.0.0.305.

Affected software versions

- Adobe Flash Player 16.0.0.296 and earlier versions
- Adobe Flash Player 13.0.0.264 and earlier 13.x versions
- Adobe Flash Player 11.2.202.440 and earlier 11.x versions

To verify the version of Adobe Flash Player installed on your system, access the About Flash Player page, or right-click on content running in Flash Player and select "About Adobe (or Macromedia) Flash Player" from the menu. If you use multiple browsers, perform the check for each browser you have installed on your system.

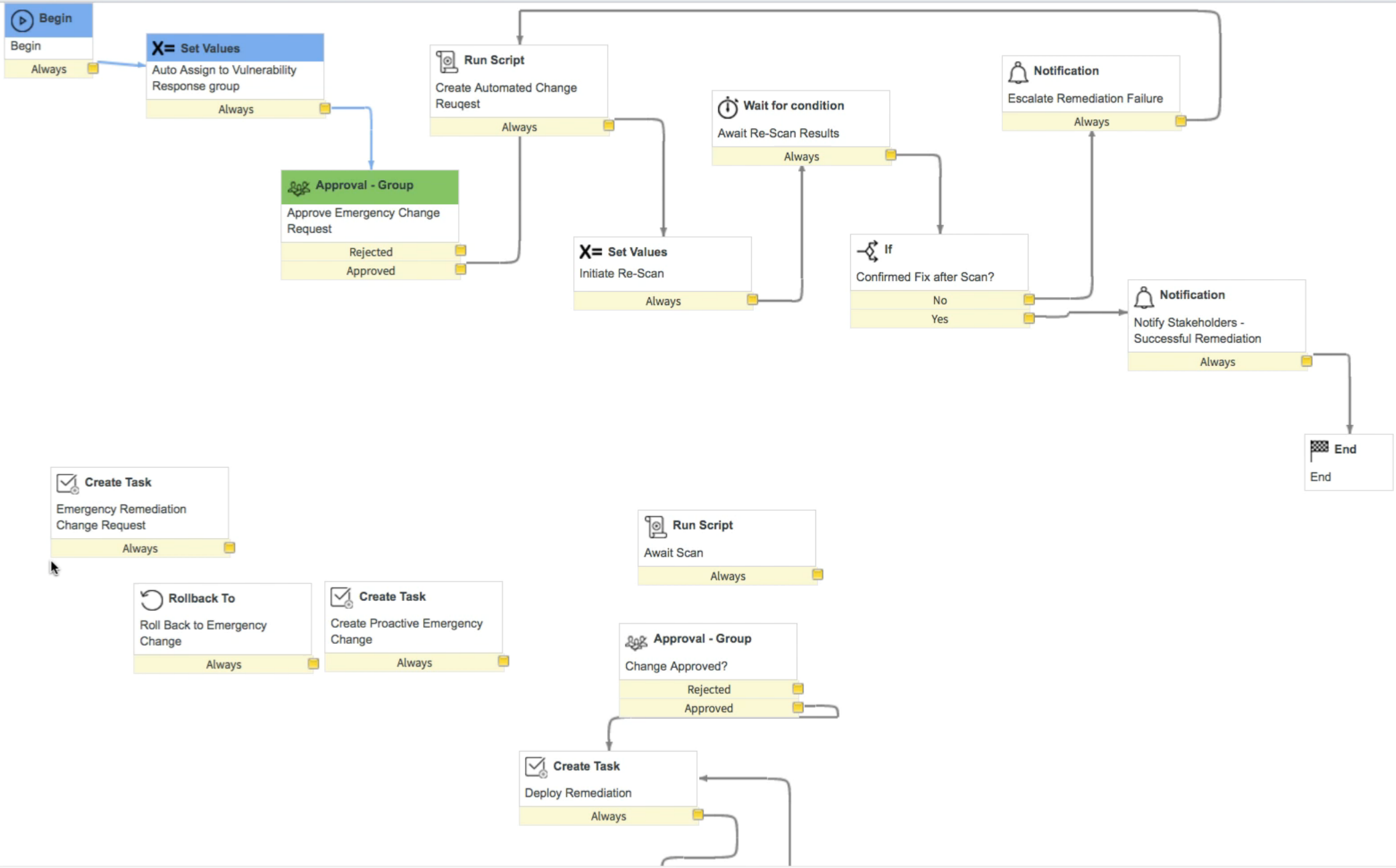
Solution

Adobe recommends users update their software installations by following the instructions below:

- Adobe recommends users of the Adobe Flash Player desktop runtime for Windows and Macintosh update to Adobe Flash Player 16.0.0.305 by visiting the Adobe Flash Player Download Center, or via the update mechanism within the product when prompted.
- Adobe recommends users of the Adobe Flash Player Extended Support Release should update

Vulnerability Response - Critical

State: Executing 2017-03-22 14:50:25 -



Approver: Janene Casella

State: Requested

Approving: Vulnerable Item: VIT0010140

Comments

Post

Activity

JC Janene Casella 2017-03-22 14:50:26

Approver: Janene Casella
State: Requested

Update Approve Reject Delete

Related Links

Force to Update Set

Summary of Item being approved

Vulnerable Item

Hold SHIFT and move the cursor to keep this window open

Number	VIT0010140	State	Analysis
Configuration item	Product KIOSK	Substate	Awaiting Change
Business criticality	1 - Critical	Change Request	
Priority	1 - Critical	Assignment group	Vulnerability Response
		Assigned to	

Number	VIT0010140	State	Pending Confirmation
Configuration item	Product KIOSK	Substate	Fixed
Business criticality	1 - Critical	Assignment group	Vulnerability Response
Priority	1 - Critical	Assigned to	

Vulnerability | Configuration Details | Notes | Qualys

Vulnerability	CVE-2015-0314	First found	2017-01-18
Vulnerable software	Adobe Flash Player 11.0.1.152	Last found	2017-03-22
Installation	Linux Linux Kernel 2.0.3	Times found	3

Update | Create Change | Create Problem | Create Security Incident | Delete

Related Links

Calculate Criticality
Force to Update Set
Scan for Vulnerabilities
Show Workflow
Repair SLAs

Approvers (6) | Tasks (1) | Impacted Services (2) | Task SLAs (1) | Affecting Tasks | Associated Vulnerable Group (1) | Scan (1)

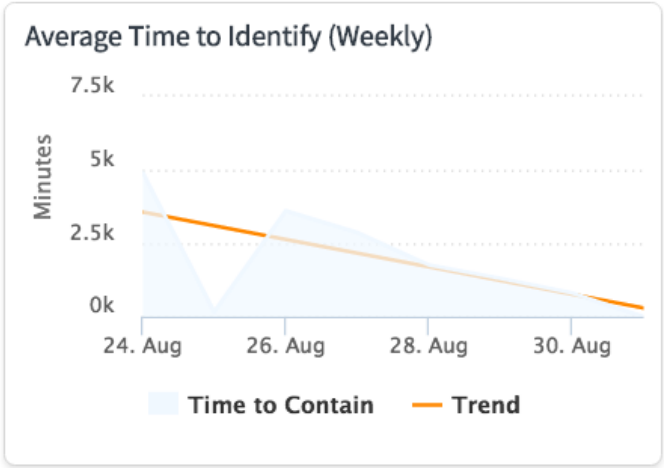
Approvers | New | Edit... | Go to | State | Search | 1 to 6 of 6

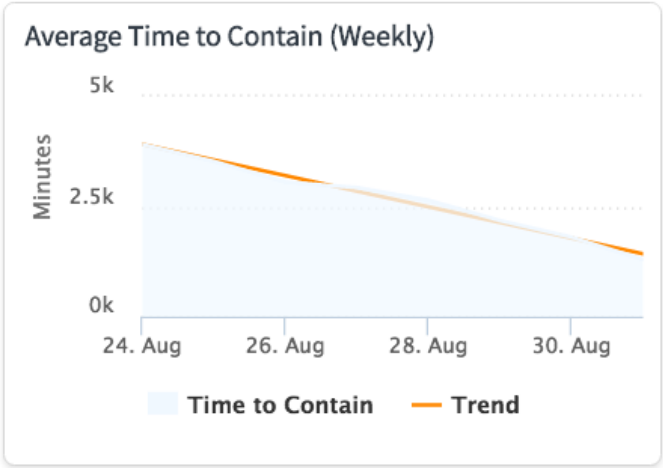
Approval for = VIT0010140

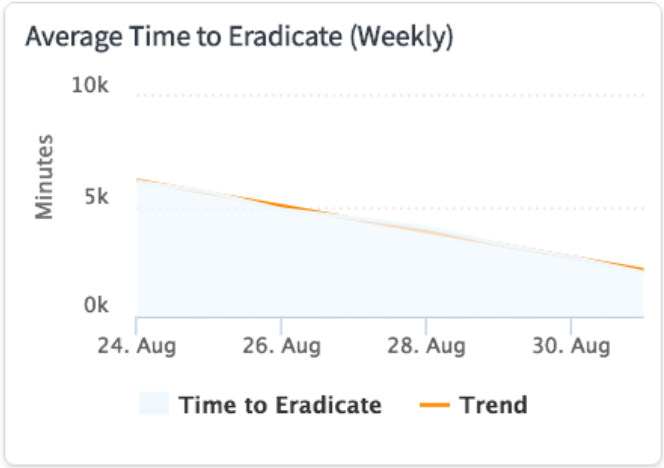
State	Approver	Comments	Created
No Longer Required	Virgil Chinni		2017-03-22 14:50:26
No Longer Required	Vanessa Lewallen		2017-03-22 14:50:26
Approved	Janene Casella		2017-03-22 14:50:26

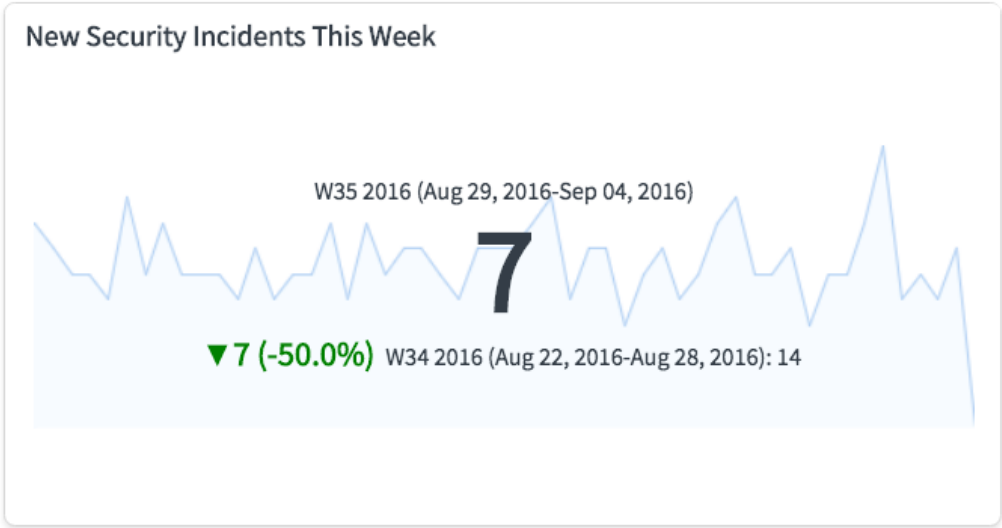
Know When Things are Going Well…or Not

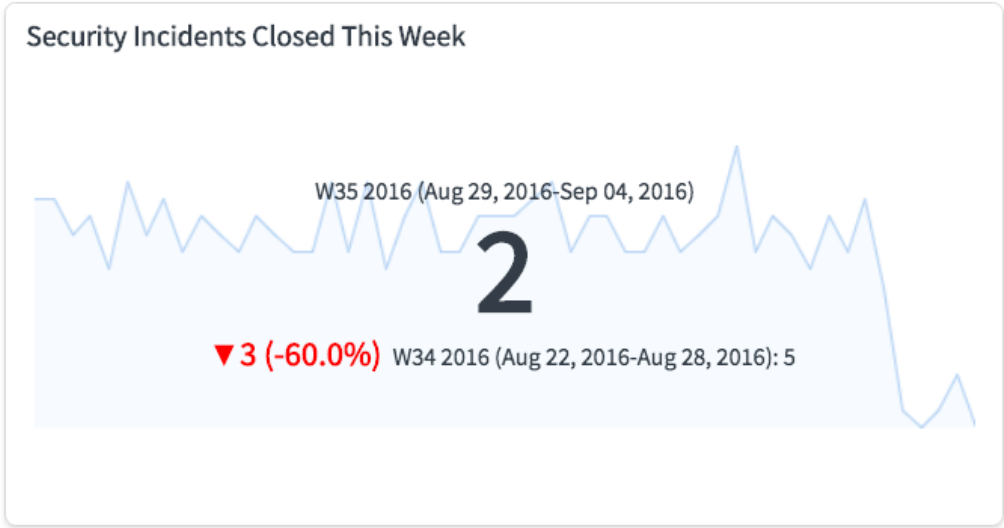
Security Operations Center | Vulnerability Profile | Security Controls Profile | Business Risk Profile











© 2017 ServiceNow All Rights Reserved

Top Takeaways

1

Prioritize and resolve incidents faster



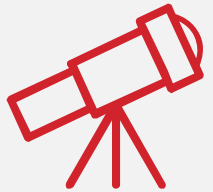
2

Collaborate efficiently with IT



3

Get a definitive view of your security posture



© 2017 ServiceNow All Rights Reserved

Don’t Just Take My Word for It

“Security Operations has given our organization a seamless path to linking Risks, CIs, and Asset Vulnerabilities.”

-Jeff Battaglino, IT Director of Service Management, Compliance and Security, Seton Hall University

Six Weeks to Security Operations on ServiceNow®	AMP & KPMG	Today at 1:30pm
Integrated Security Operations: The Difference Between Knowing and Guessing	DXC.technology	Today at 2:40pm
Moving from Vulnerability Assessment to Vulnerability Management	Seton Hall University	Today at 3:50pm
Vulnerability Management in One Day	Church of Latter Day Saints	Wednesday at 11:40am

© 2017 ServiceNow All Rights Reserved

Learn More About Security at ServiceNow

Security Automation That Won't Get You Fired	UP NEXT at 11:40am
Tales from the Trenches: Converting Your Security Runbook into Security Operations Workflows	Today at 5pm
Security Topic Keynote	Wednesday at 1:30pm
Threat Intelligence Sharing: How Participation Will Dramatically Improve Your Security Posture	Wednesday at 2:40pm
What's New in Security Operations in Jakarta and What's Coming Next	Wednesday at 3:50pm

© 2017 ServiceNow All Rights Reserved

ServiceNow Pavilion



© 2017 ServiceNow All Rights Reserved

Thank You

JANENE CASELLA
Sr. Product Marketing Manager
ServiceNow

BRYCE SCHROEDER
Sr. Director, Security & Risk Practice
ServiceNow

© 2017 ServiceNow All Rights Reserved

Q&A

JANENE CASELLA
Sr. Product Marketing Manager
ServiceNow

BRYCE SCHROEDER
Sr. Director, Security & Risk Practice
ServiceNow

© 2017 ServiceNow All Rights Reserved

Take the Survey

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

Thank You

Janene Casella

Sr. Product Marketing Manager

ServiceNow

Bryce Schcroeder

Sr. Director, Security & Risk Practice

ServiceNow

© 2017 ServiceNow All Rights Reserved