knowledge17

http://clabs.link/lab132019

WORK at LIGHTSPEED

Accelerating Security Incident Response, Including Threat Intelligence

Joseph Wheeler
Advisory Solution Consultant
ServiceNow

Erich Dobroth
Advisory Solution Consultant
ServiceNow

© 2017 ServiceNow All Rights Reserved

servicenow

Agenda

- Introductions
- Presentation
  - Why did ServiceNow create a Security Incident application?
  - What is in the application?
- Lab
  - 6 labs taking you through the end-to-end life of a Security Incident

© 2017 ServiceNow All Rights Reserved

Speaker Introduction



Name: Joseph Wheeler

Title: Advisory Solution Consultant

Function: Sales

Company: ServiceNow

Experience: 6 years with ServiceNow, 7 years with Tripwire

Expertise: JRPGs and bad jokes

Achievements: Most colorful use of language

Current Projects: Internal training and working with customers

© 2017 ServiceNow All Rights Reserved

Speaker Introduction



Name: Erich Dobroth

Title: Advisory Solution Consultant

Function: Sales

Company: ServiceNow

Experience: 5 years with ServiceNow, 10 years with Tripwire

Expertise: Super-long passwords and most areas of the ServiceNow platform

Achievements: Close to 40 years of playing D&D (his mom was his first DM)

Current Projects: Removed due to security restraints

© 2017 ServiceNow All Rights Reserved

Verizon Breach Report – 2015 – BREACHED!

Security Incidents

79,790

Confirmed Data Breaches

2,122

Countries represented

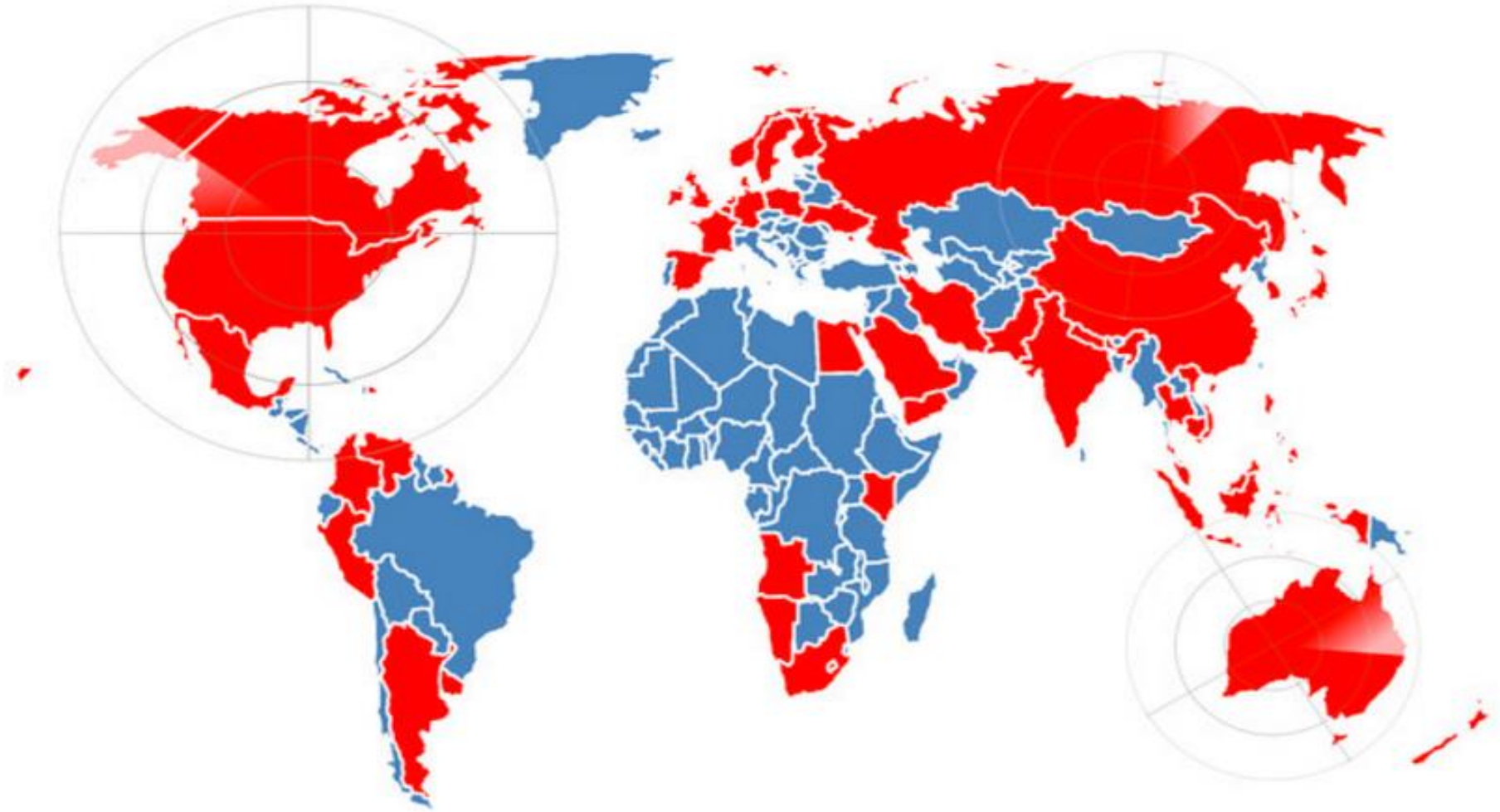
61

Comprised Records

700M

Cost*

$400B

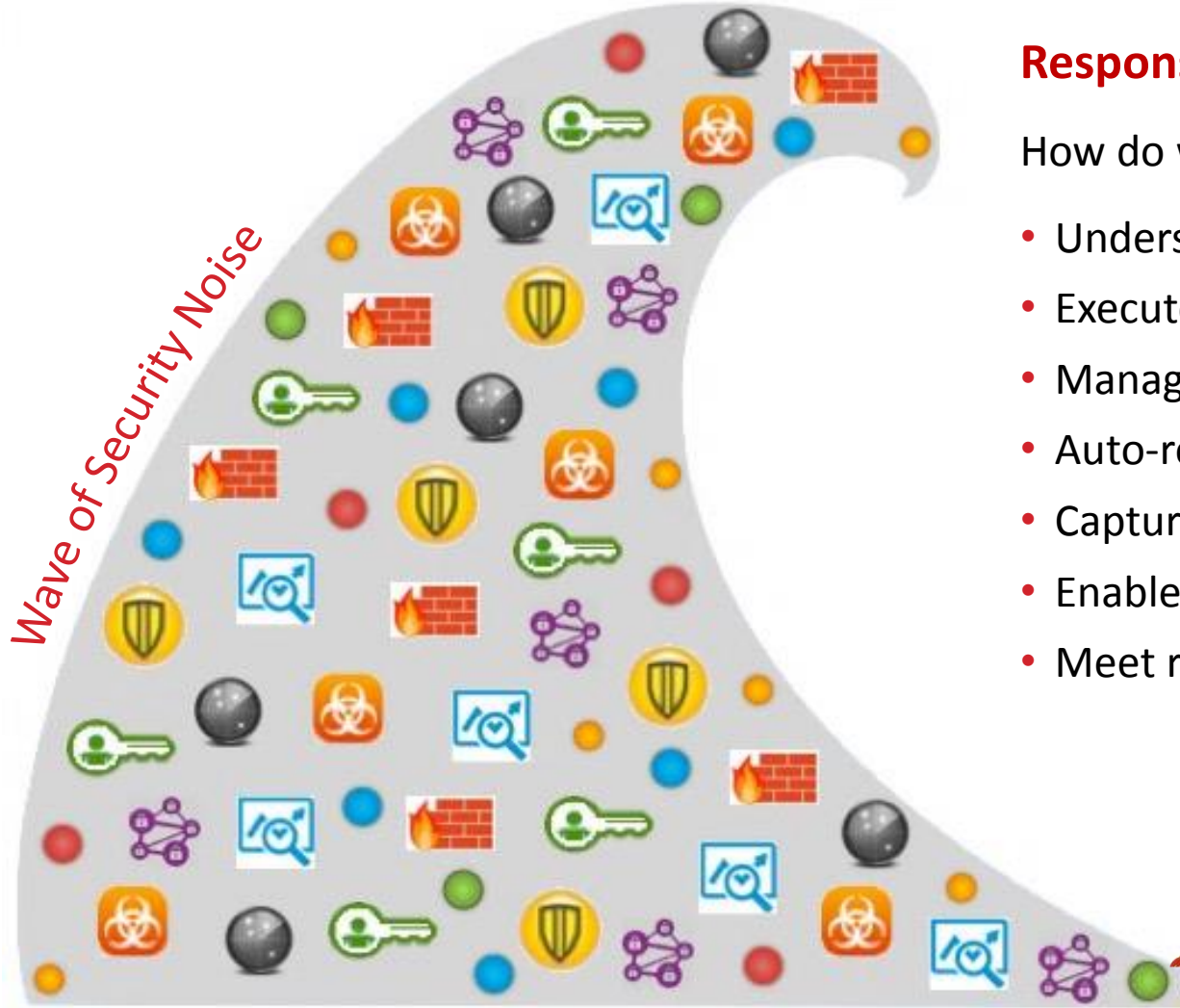


© 2017 ServiceNow All Rights Reserved

The Core Problem – Information Overload

Detection

- SIEM
- Firewall/IPS/IDS
- Security Endpoint
- Identity & Access
- Threat/Intel
- Network Security
- Vulnerability Detection



Response

How do we quickly organize and act?

- Understand business impact
- Execute consistent workflow
- Manage service levels
- Auto-remediate
- Capture metrics
- Enable IT, Security, & BU collaboration
- Meet regulatory requirements



Security
&
IT Teams

© 2017 ServiceNow All Rights Reserved

Why Are Security Solutions Failing? Disconnected Silos









© 2017 ServiceNow All Rights Reserved

Why Are Security Teams Overwhelmed? Wrong Tools for Response






These methods don’t scale

© 2017 ServiceNow All Rights Reserved

Why Are Security Teams Overwhelmed? Wrong Tools for Response

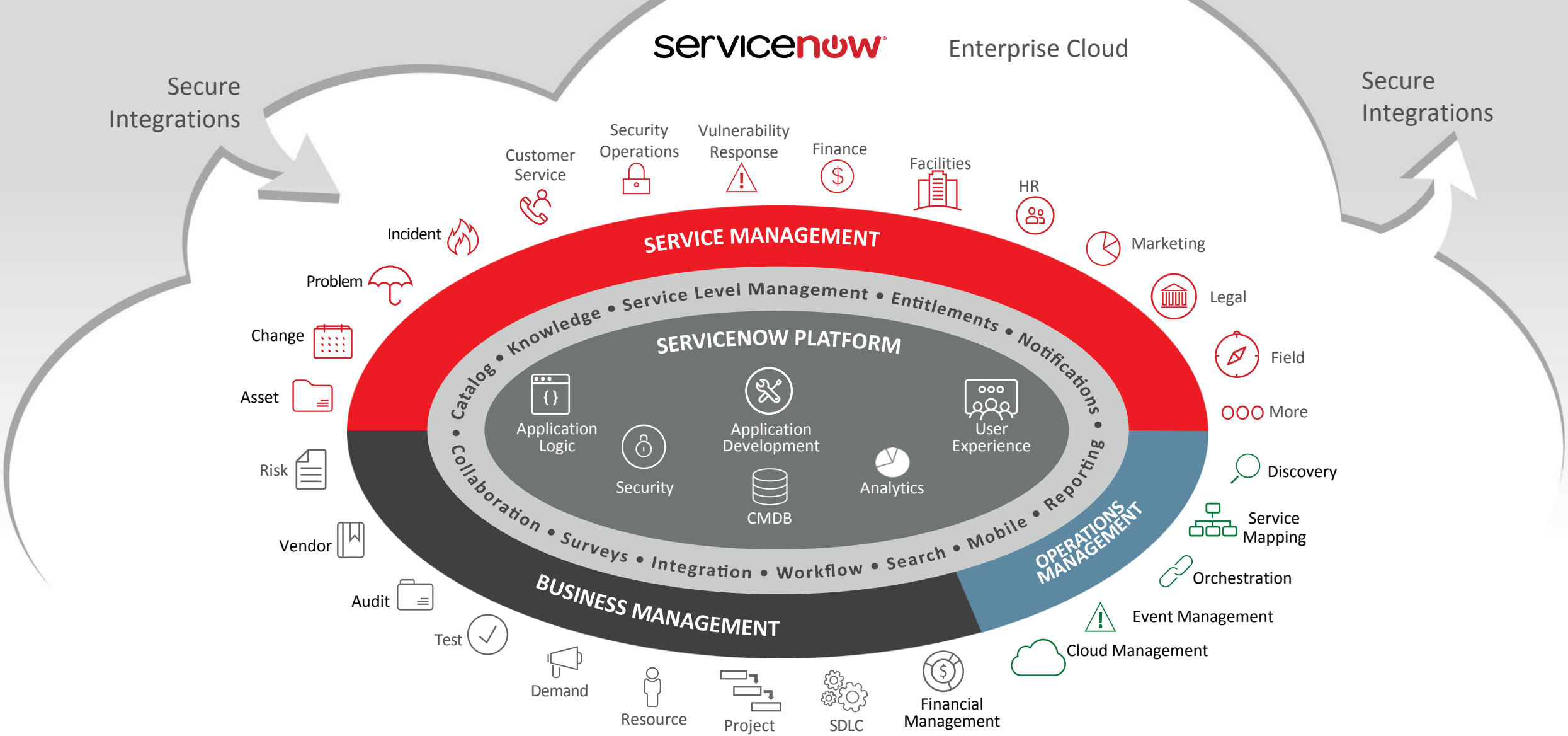
Lack of Metrics, Workflow, Task Management







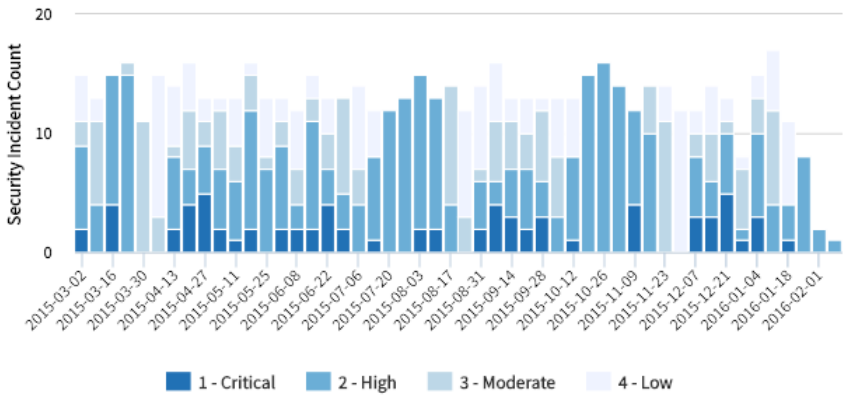
© 2017 ServiceNow All Rights Reserved



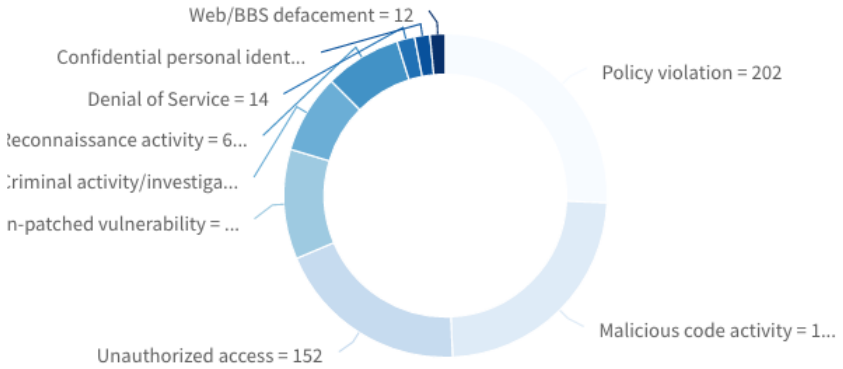
© 2017 ServiceNow All Rights Reserved

Measure Success, Identify Areas for Improvement

Security Incident Closures by Priority



Security Incidents by Attack Category



Security Incident Assignment Heatmap

	1 – Critical	2 – High	3 – Moderate	4 – Low
Application Security	5	26	14	11
Directory Infrast...	7	30	13	11
Endpoint Security	7	36	14	8
Forensics	12	28	11	14
Network Security	6	31	11	11
Red Team Operations	6	36	10	12
SecOps APAC	6	28	17	16
SecOps EMEA	11	28	10	15
SecOps NASA	5	29	11	10
Security Incident...	8	14	12	13
SOC Tier 2	1			
Unix Security	11	24	12	20
Vulnerability Res...	10	24	14	12
Windows Security	7	32	17	8

Matching Security Incidents

795

Security Incident - Category

All

Security Incident - Subcategory

All

Priority

All

Security Incident - Active

- (•) All
- ( ) True
- ( ) False

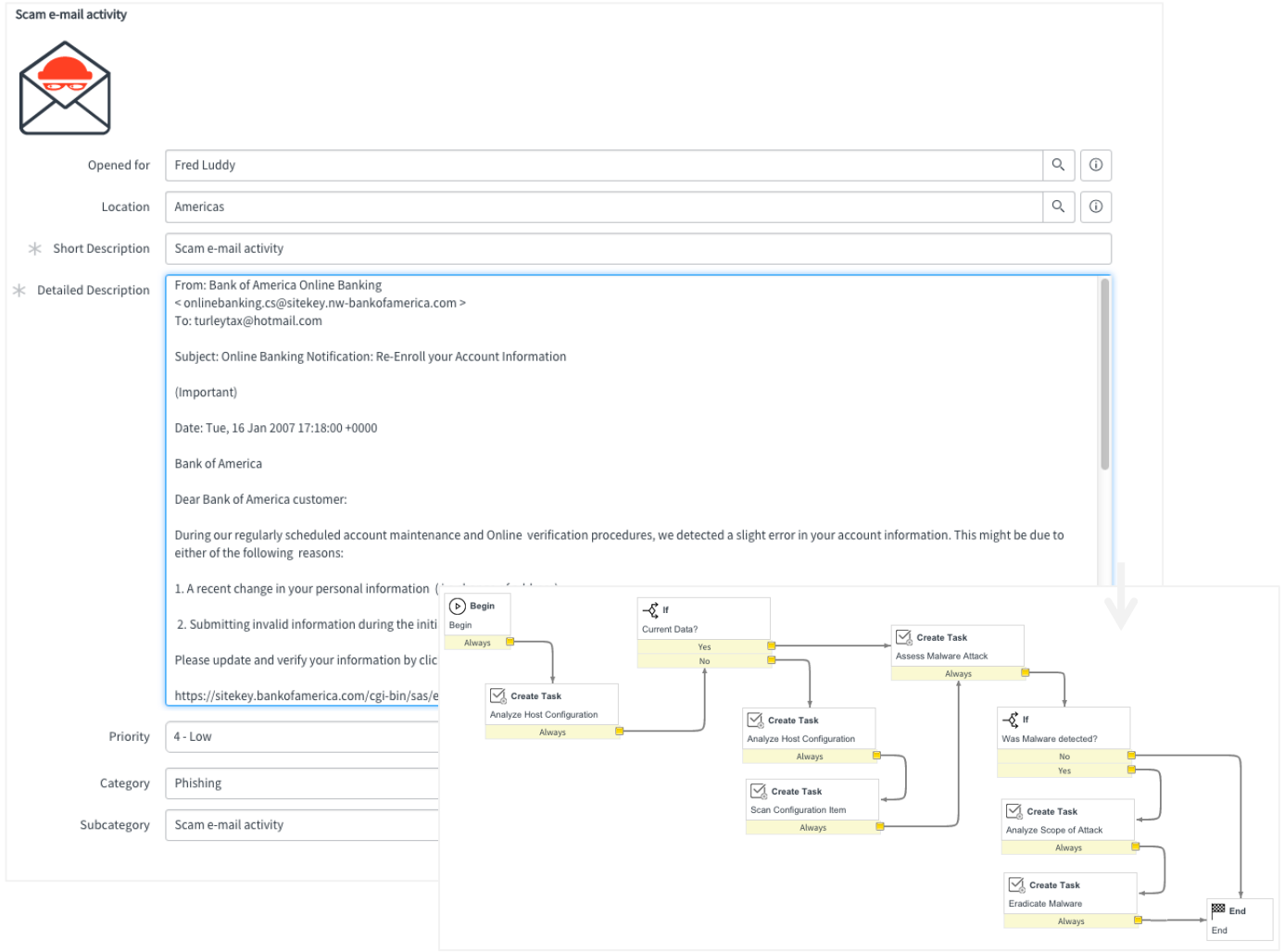
Security Incident - Business Criticality

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

© 2017 ServiceNow All Rights Reserved

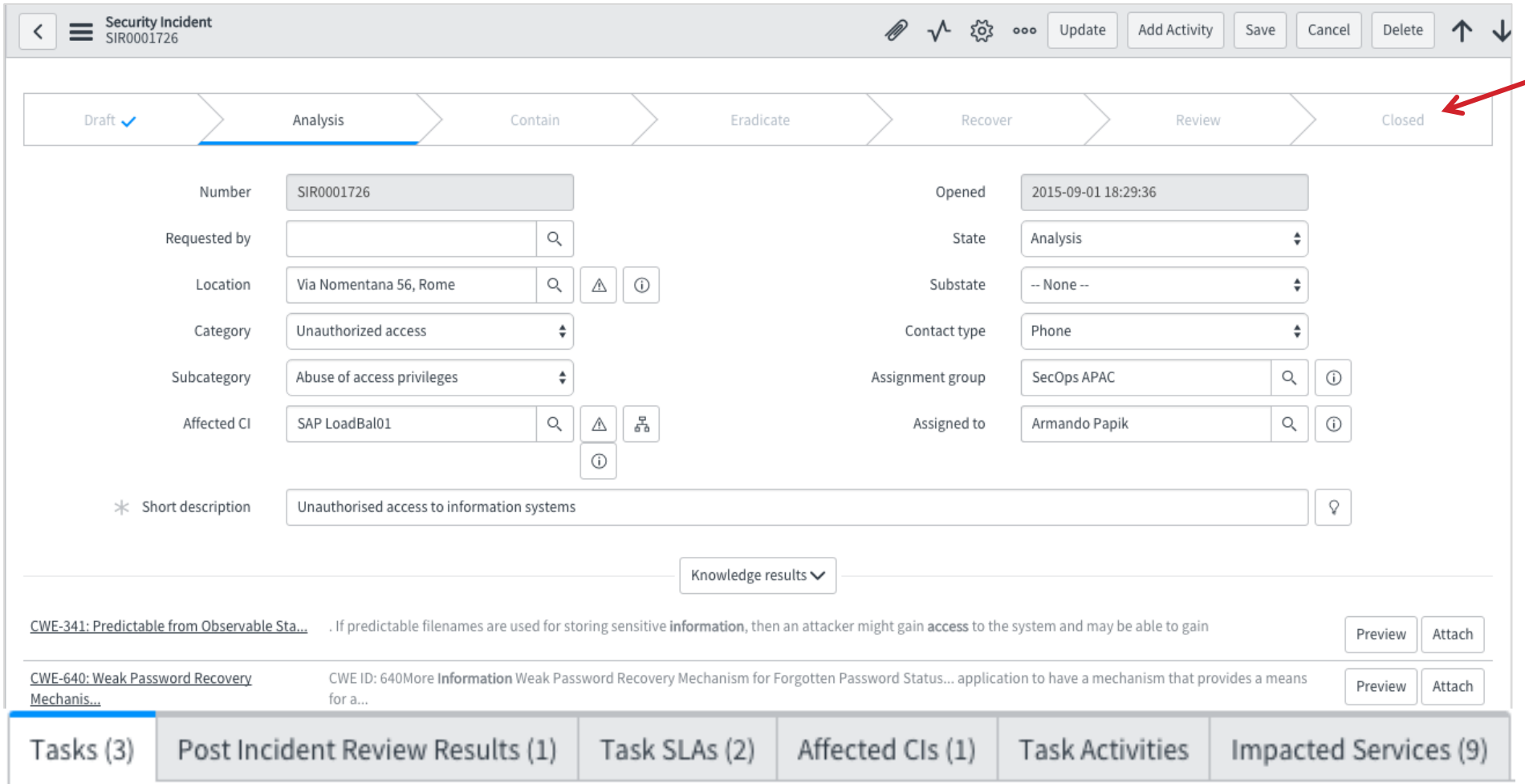
Security Service Catalog





© 2017 ServiceNow All Rights Reserved

Single System of Record



National Institute of Standards & Technology (NIST) – based process

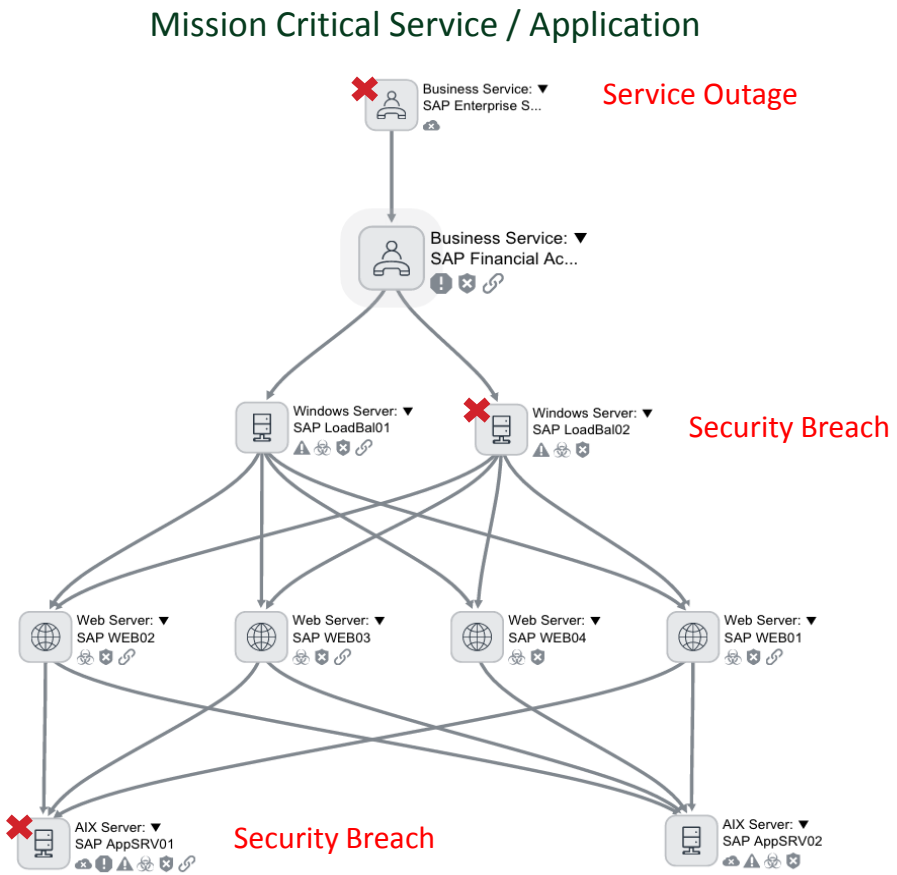
Securely Captures

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

* Role-based access ensures sensitive data is only shared on a need-to-know basis.

© 2017 ServiceNow All Rights Reserved

Business Service Map



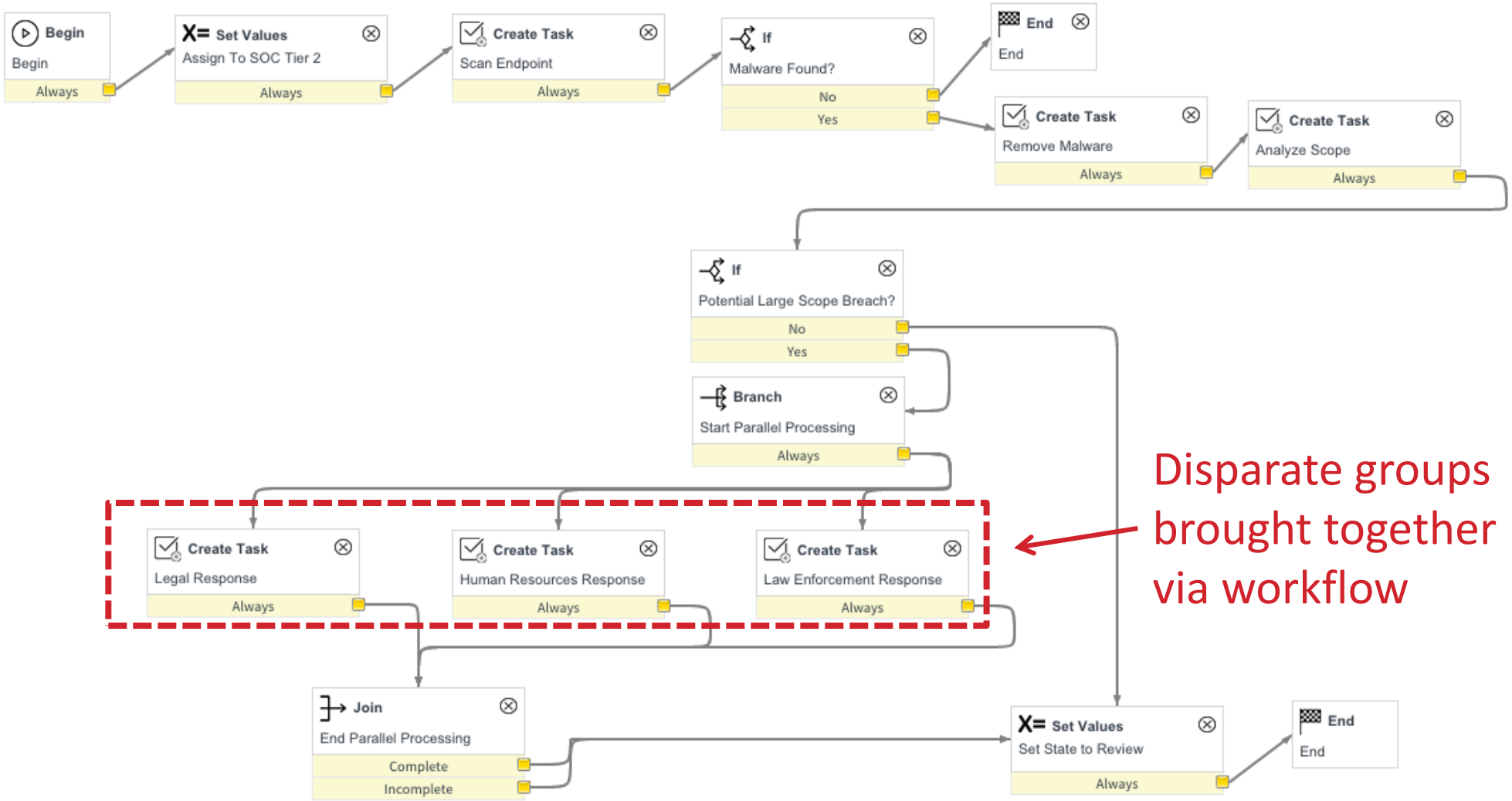
You can't secure what you don't know about

- Security Teams lack insight into mission critical Business Service and Application alignment to underlying infrastructure
- Patching or taking breached systems offline can cause huge business disruption at high costs if they support critical Services
- Lack of a Relational CMDB leads to misunderstanding broader breaches
- Lack of Asset ownership information, slows investigation
- SLAs are missed due to misunderstood impact and priority

ServiceWatch automatically maps applications and infrastructure components to business services

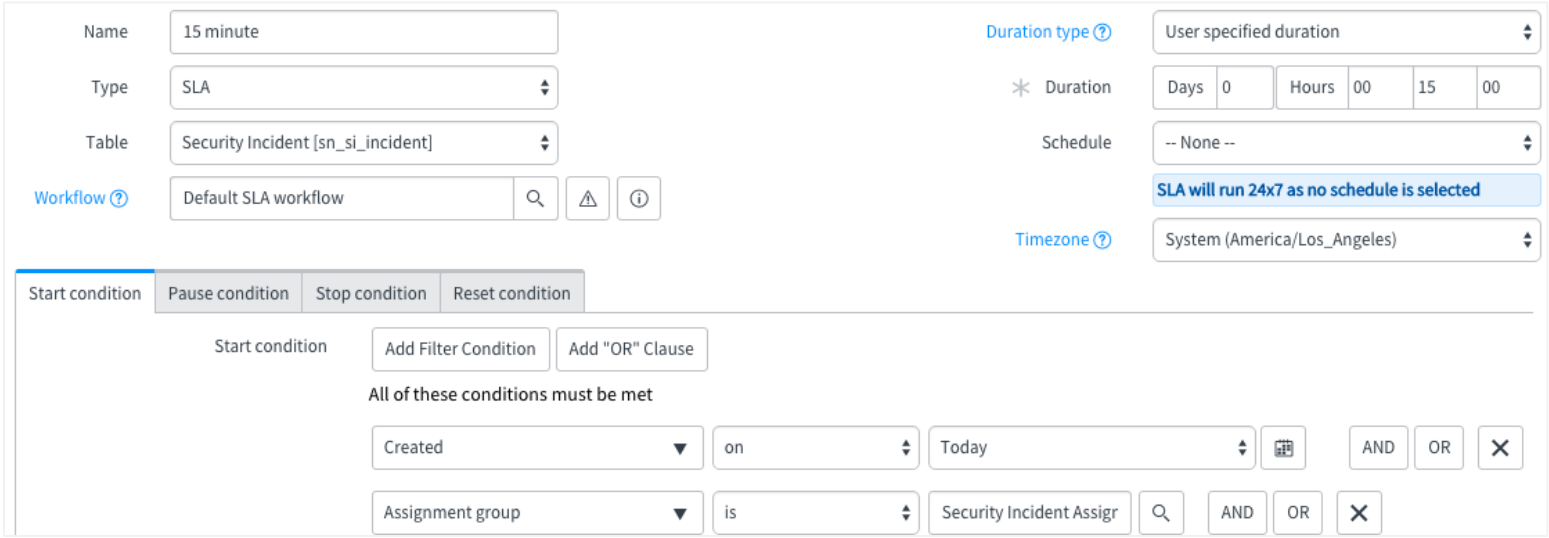
© 2017 ServiceNow All Rights Reserved

Workflow



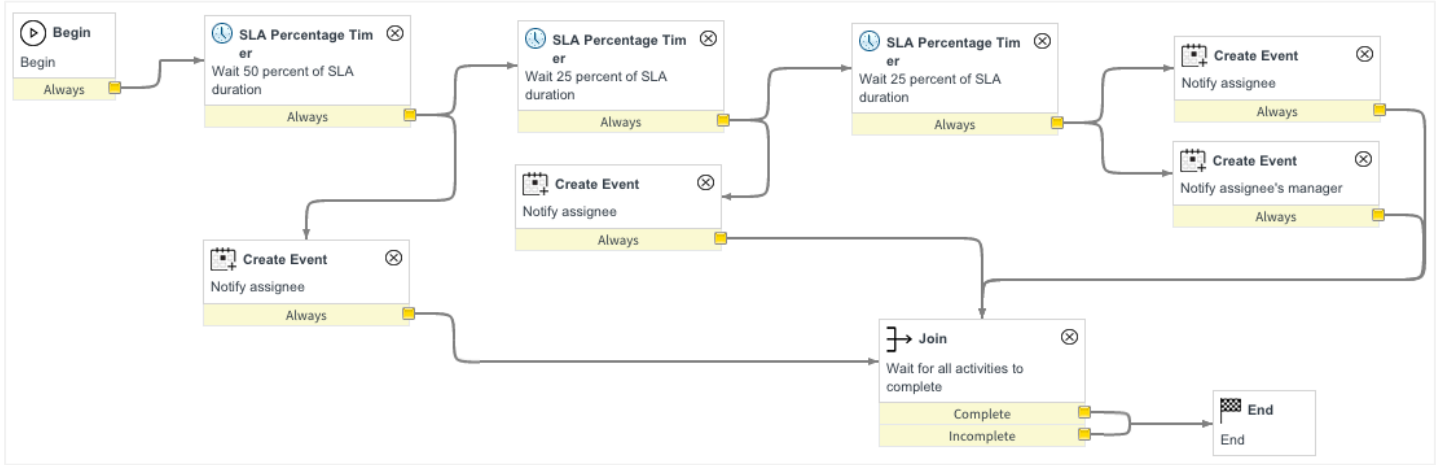
© 2017 ServiceNow All Rights Reserved

Service Level Management



Every Security Incident Type can have a distinct Service Level Agreement

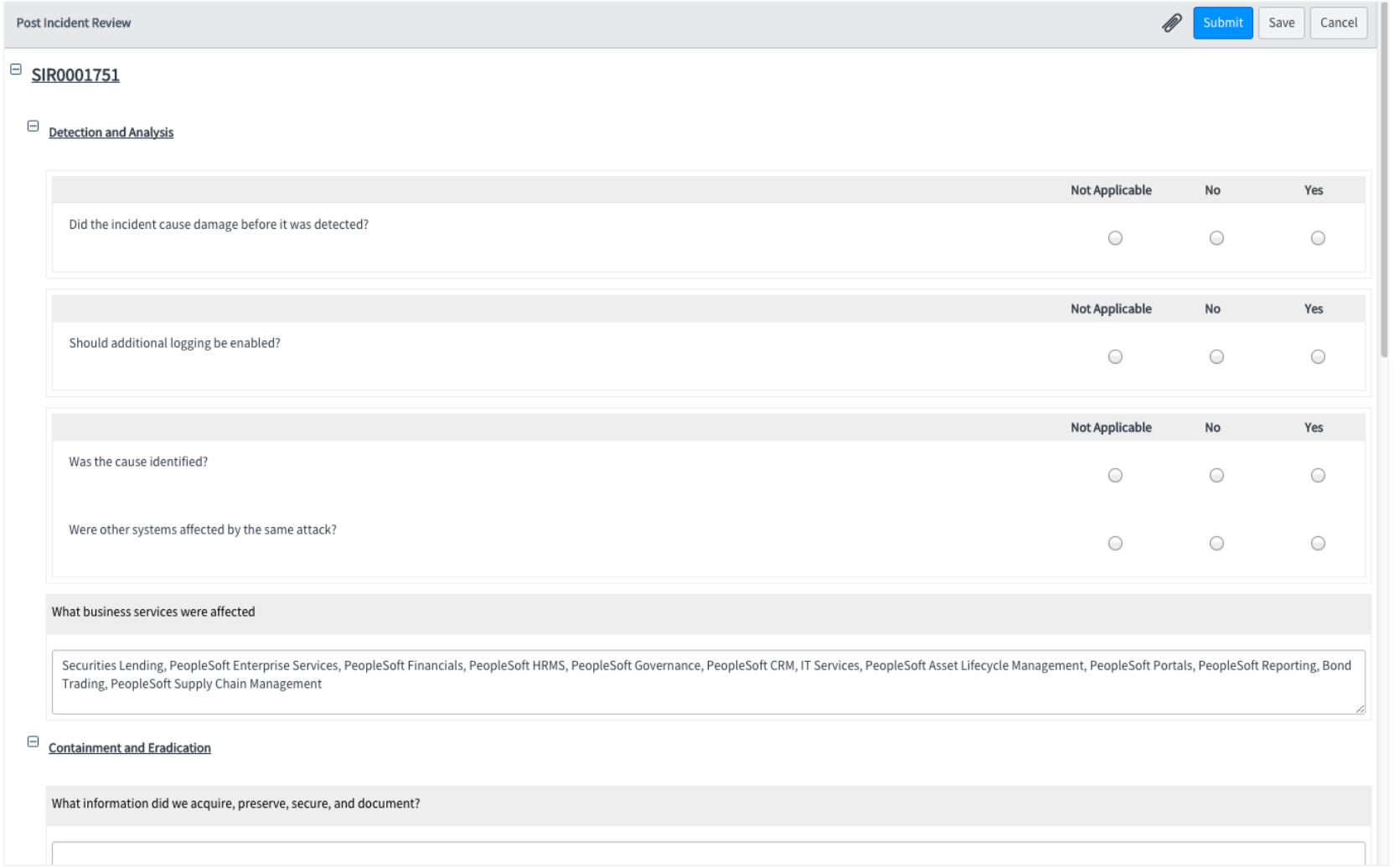
When a Security Incident comes in with “matching” conditions … the SLA process starts.



© 2017 ServiceNow All Rights Reserved

Security Incident Assessments

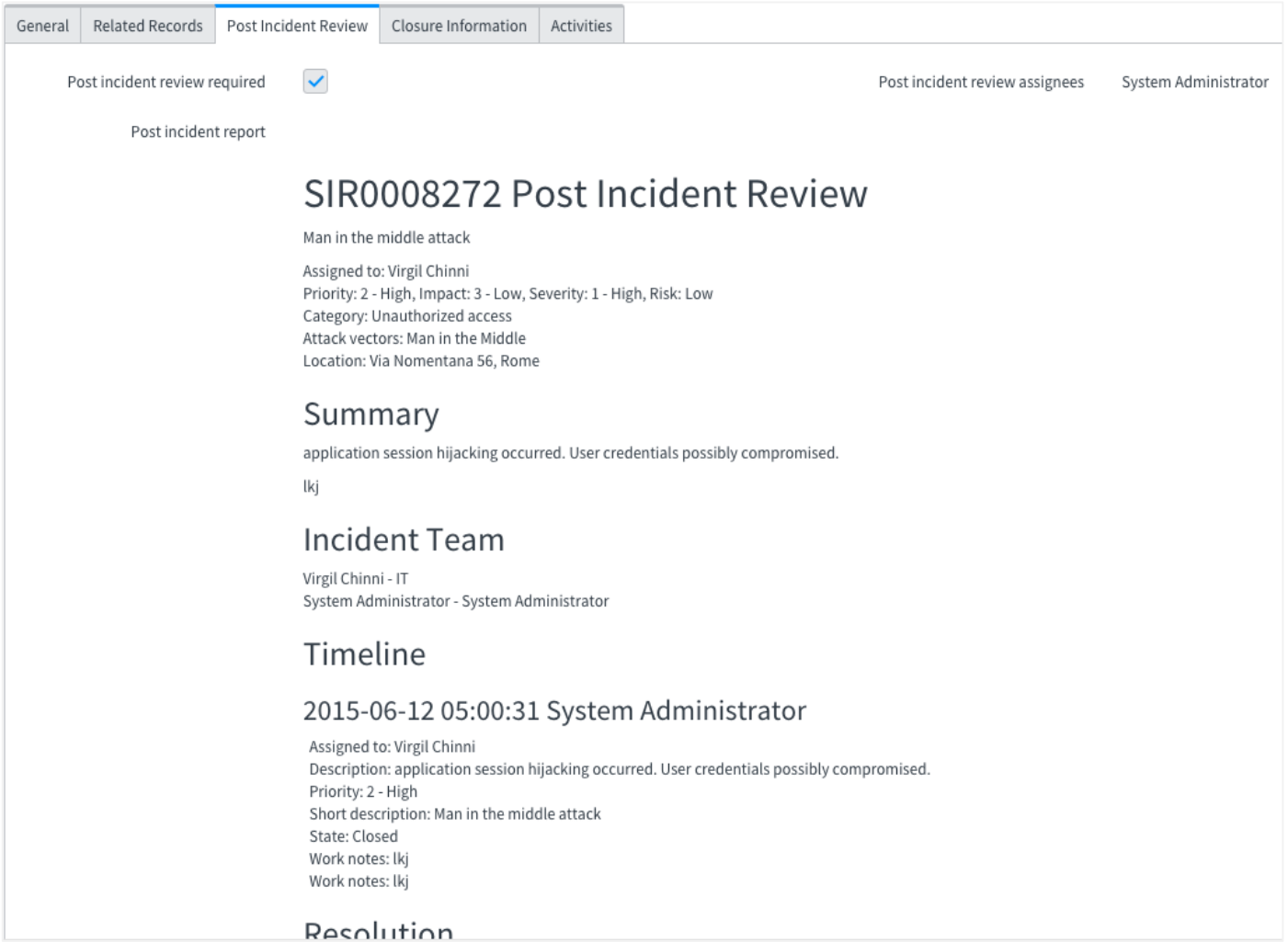
- Assessments collect critical response information from various teams
- Assessment results automatically added to Post Incident Review
- Provides valuable lessons learned and helps improve the security process



© 2017 ServiceNow All Rights Reserved

Post Incident Review

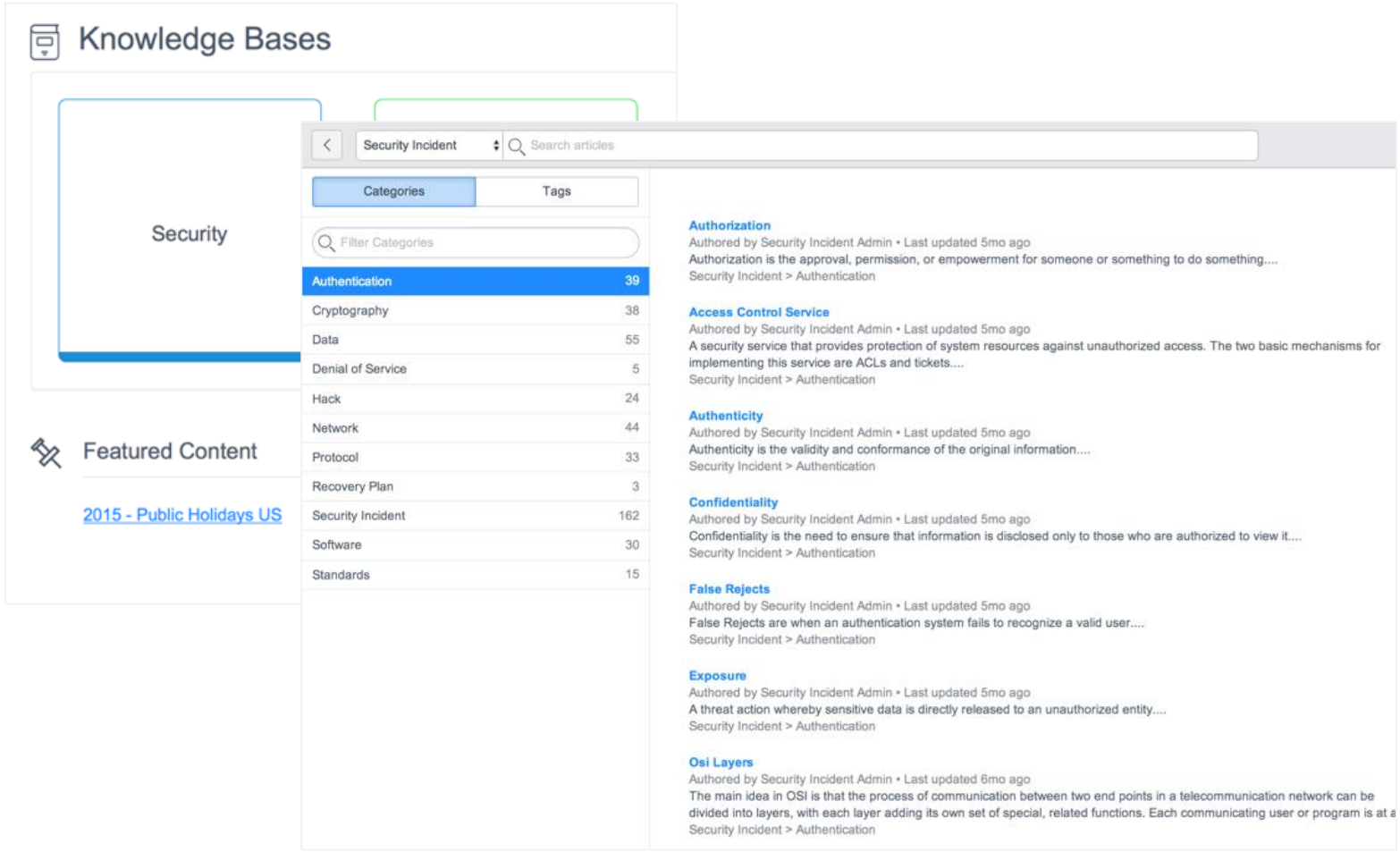
- Accurately represents the timeline of events for a security breach
- Includes work notes from extended teams (Change, HR, GRC, SDLC, etc.)
- Saves time from gathering evidence manually from multiple sources
- Can be shared with extended teams to improve the security process



© 2017 ServiceNow All Rights Reserved

Security Knowledge Base

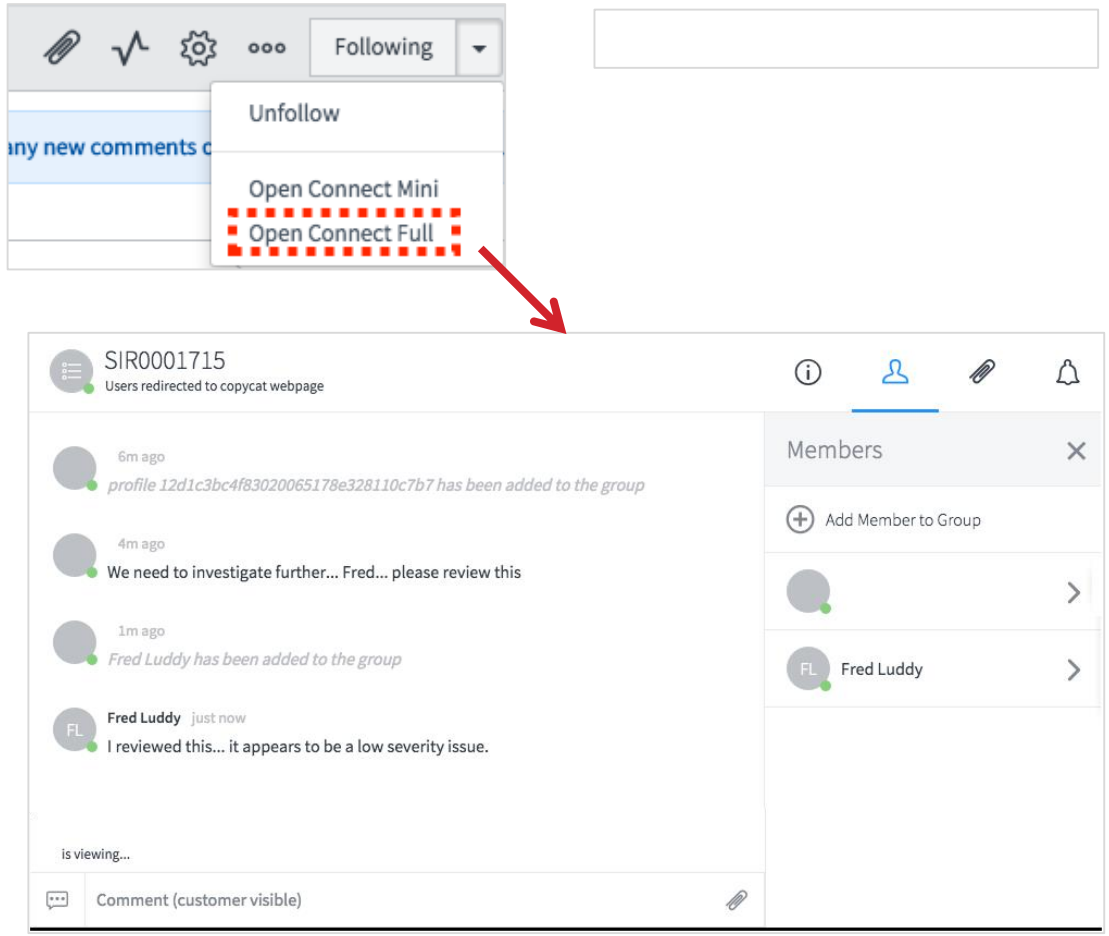
- Secure articles
- Imported CWE articles
- SOPs documentation
- Key contacts lists
- Vulnerability documentation
- Etc.



© 2017 ServiceNow All Rights Reserved

Connect

- Connect enables chat groups to be quickly assembled so critical resources can easily collaborate and audit response actions.



© 2017 ServiceNow All Rights Reserved

Lab Overview – Security Incident Simulation

This lab will walk you through the full lifecycle of a Security Incident

- You will leverage ServiceNow capabilities to help you close the incident including:
  - Security Dashboards
  - Automated Workflow
  - Business Service Maps
  - ServiceNow Connect
  - Security Event Management
  - The Amazing ServiceNow Platform
- Let us know if you have questions! We are here to help.

© 2017 ServiceNow All Rights Reserved

Lab Section 1.0 ALERT!! A New Security Incident Has Arisen!

You have received a notification from ServiceNow!
It is time to jump into action and start taking care of business!

In this section you will be the Security Incident Commander.

Let's go over the dashboard and then drill into our new incident.

Lab 1.0 New Security Incident Received

- Let's review the incident.
- Verify who the incident came from, and that it is assigned to your group.
- Check the short description to see what happened.
- Look at the related lists to make sure that a response task has opened and been assigned to one of your colleagues.

© 2017 ServiceNow All Rights Reserved

Lab Section 1.1 IT Department! You Have a Task Assigned to You that Requires Immediate Attention!

Lab 1.1
Work a
Security Task

You have received a notification from ServiceNow!
Let's fix the wrongdoing!

In this section we are involving IT in helping with a security incident.
Your Persona for this section is the IT Technician.

- Logged in as the IT Tech, you're looking at the Security Dashboard. Notice that it's only showing you items you are working on.
- Drill into the task you've been assigned and accept it to begin work!
- Work the task by looking for potential impact and other tasks that may interfere with you completing your work.
- After your work is complete, let your manager know with Collaborate!

© 2017 ServiceNow All Rights Reserved

Lab Section 1.2 Security Manager! You Have Received an Alert That a New Collaboration Chat Has Appeared In Your Queue!

You have received a notification of a new chat message in ServiceNow! Login as the manager and see who's messaged you!

You see your received message notification in the upper right. Open it up and respond.

It appears we need to get HR involved.

Lab 1.2 Verify Work and Get a New Task Assigned

- Click into the Security Incident in the chat to see how ServiceNow allows you to include other business units and applications in a single platform to help you with your Security Incidents.
- Update the new task and set it to ready so it can be assigned over to HR, you will see ServiceNow can automatically route this to a person as well.

© 2017 ServiceNow All Rights Reserved

Lab Section 1.2 Welcome to ServiceNow Human Resources! Log in and See What We Have for Today!

Lab 1.3 Verify Work and Get a New Task Assigned

You've just come into the office; time to login to ServiceNow and see what's on your plate for today!

Welcome to your HR Dashboard. Here, we can see all the work you may have for today.

You can see one of these reports is Critical HR Tasks! Click on the red number to drill into your important task!

- Start working on the task; note that you can see that it's related to a Security Incident, but your roles restrict your access to this incident.
- Work the task and reach out to the employee who's caused the problem and let them know to not do it again.
- Close out the task; it's back in Security's hands now!

© 2017 ServiceNow All Rights Reserved

Lab Section 1.5 All is Well, Time to Review and Assess!

Lab 1.5 Complete Your Assessments

Alright, Incident Commander, you have received a notification that HR has completed their work and you have a new assessment to fill out!

Login as the commander.

Use the left navigation to find all of your pending assessments.

- Click into your new assessment and fill out your responses.
- Thank you for your hard work, Commander! Your job is done!

© 2017 ServiceNow All Rights Reserved

Lab Section 1.6 All Work Is Complete and Ready for Your Review

All work, review, and assessments have been completed. Time for the manager to review and close out the incident.

Log back in as the manager. This time you will use the dashboard to find the incident.

Format the Post Incident Review.

Lab 1.6 Review and Close Out

- Close the incident out, don't forget your mandatory close notes.
- After closure, find the recently closed incident and now look over the auto-generated post incident review that ServiceNow has created for you!
- Excellent work! This Security Incident is complete!

© 2017 ServiceNow All Rights Reserved

Top Takeaways

1. Security Incident Response empowers security teams to rapidly respond to issues.
2. Automated workflow can help coordinate multiple teams to work together.
3. Post Incident reviews help improve security process.

© 2017 ServiceNow All Rights Reserved

Thank You

Lab Sponsored by Amazon Web Services



Joseph Wheeler
Advisory Solution Consultant
ServiceNow

Erich Dobroth
Advisory Solution Consultant
ServiceNow

© 2017 ServiceNow All Rights Reserved

Q & A

Joseph Wheeler
Advisory Solution Consultant
ServiceNow

Erich Dobroth
Advisory Solution Consultant
ServiceNow

© 2017 ServiceNow All Rights Reserved