knowledge17

WORK at LIGHTSPEED

True Vulnerability Management: Take Control and Improve Your Security Posture

Jonathan Walker
Security Solutions Architect
ServiceNow Security & Risk Practice

David Bell
Security Solutions Architect
ServiceNow Security & Risk Practice

© 2017 ServiceNow All Rights Reserved

servicenow

Agenda

- Speaker Introductions
- Understanding the problem – The current state of vulnerability management
- How ServiceNow can help
- Labs
  - Lab 1 - Define Success
  - Lab 2 - Automate the response
  - Lab 3 - Manage vulnerabilities in bulk
  - Lab 4 - Create the right reports
  - Lab 5 - Create dashboards for visibility
  - Demo – Live demo & follow along of everything we just accomplished
- Q&A (time permitting)

© 2017 ServiceNow All Rights Reserved

Speaker Introductions

© 2017 ServiceNow All Rights Reserved

Speaker Introduction



Name: Jonathan Walker

Title: Security Solutions Architect

Function: Pre-Sales

Company: ServiceNow, Security & Risk Practice

Experience: Almost 1yr at ServiceNow, previous experience includes running the vulnerability management program at FEMA, technical team lead conducting vulnerability and threat assessments for the U.S. Gov. Intelligence Community, Federal Consultant for cyber security compliance

Expertise: Vulnerability Management and Security Incident Response

Achievements: Within 6 weeks, reducing customer's vulnerability response time by 60%; processing, prioritizing, and assigning a majority of vulnerabilities within 24hrs of implementation; elevated CMDB maturity by automatically mapping IP's to configuration items via scan data from vulnerability scans

Current Projects: Driving process efficiencies. Automating enterprise vulnerability and security incident response to decrease average time to identify, remediate, contain, and eradicate vulnerabilities and threats

© 2017 ServiceNow All Rights Reserved

Speaker Introduction

Note: Please read the notes section for guidance on using this slide.



Name: David Bell

Title: Security Solutions Architect

Function: Pre-Sales

Company: ServiceNow, Security & Risk Practice

Experience: 7 months with ServiceNow based in Melbourne Australia covering the ANZ region.12 years with 3 major security software vendors as a Solutions Achitect selling Idendity Access Management, SIEM, Vulnerability Management and FIM Solutions. SIR Architect at Australian Dept of Defence SOC (Restricted and Secret Networks).

Expertise: Vulnerability Management and Security Incident Response

Achievements: Within 6 weeks, reducing customer's vulnerability response time by 60%; processing, prioritizing, and assigning a majority of vulnerabilities within 24hrs of implementation; elevated CMDB maturity by automatically mapping IP's to configuration items via scan data from vulnerability scans

Current Projects: Driving process efficiencies. Automating enterprise vulnerability and security incident response to decrease average time to identify, remediate, contain, and eradicate vulnerabilities and threats

© 2017 ServiceNow All Rights Reserved

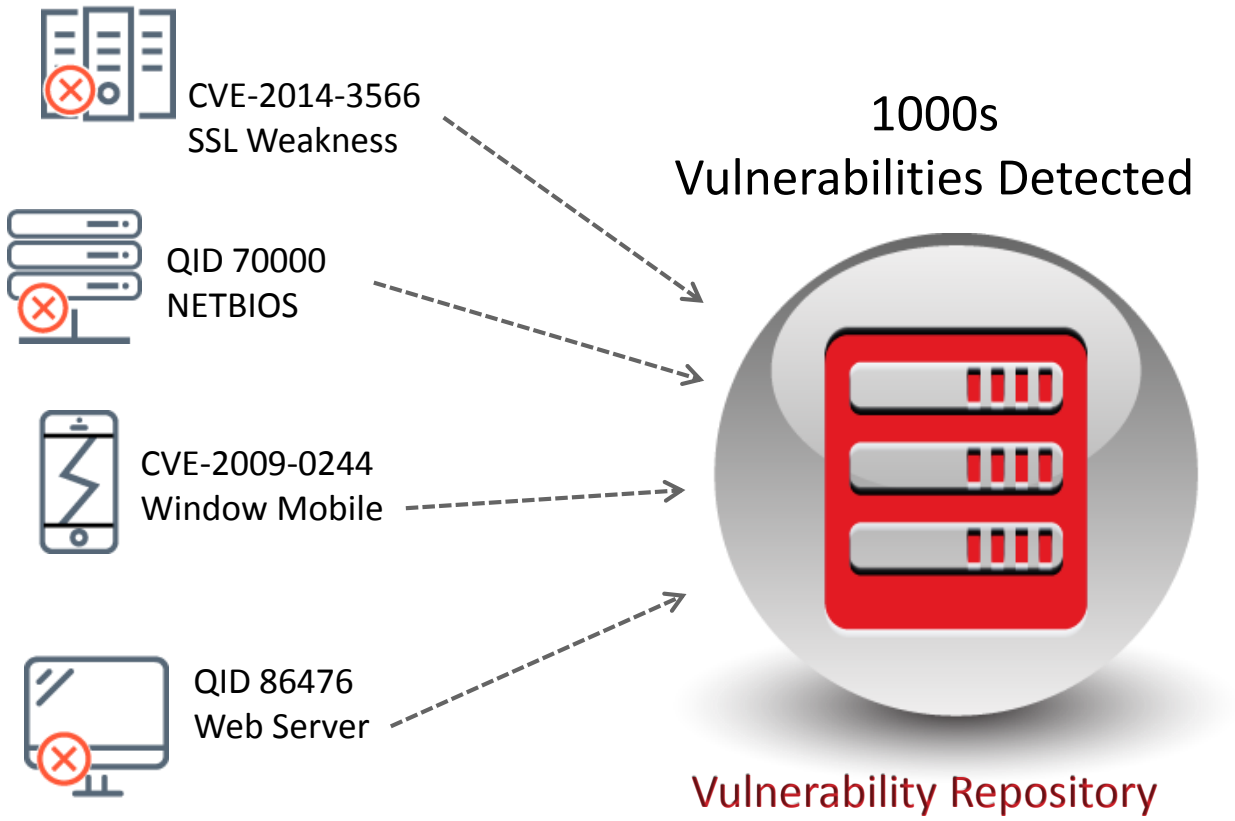
Understanding the problem

© 2017 ServiceNow All Rights Reserved



© 2017 ServiceNow All Rights Reserved

The Majority of Breaches are Due to Existing Vulnerabilities

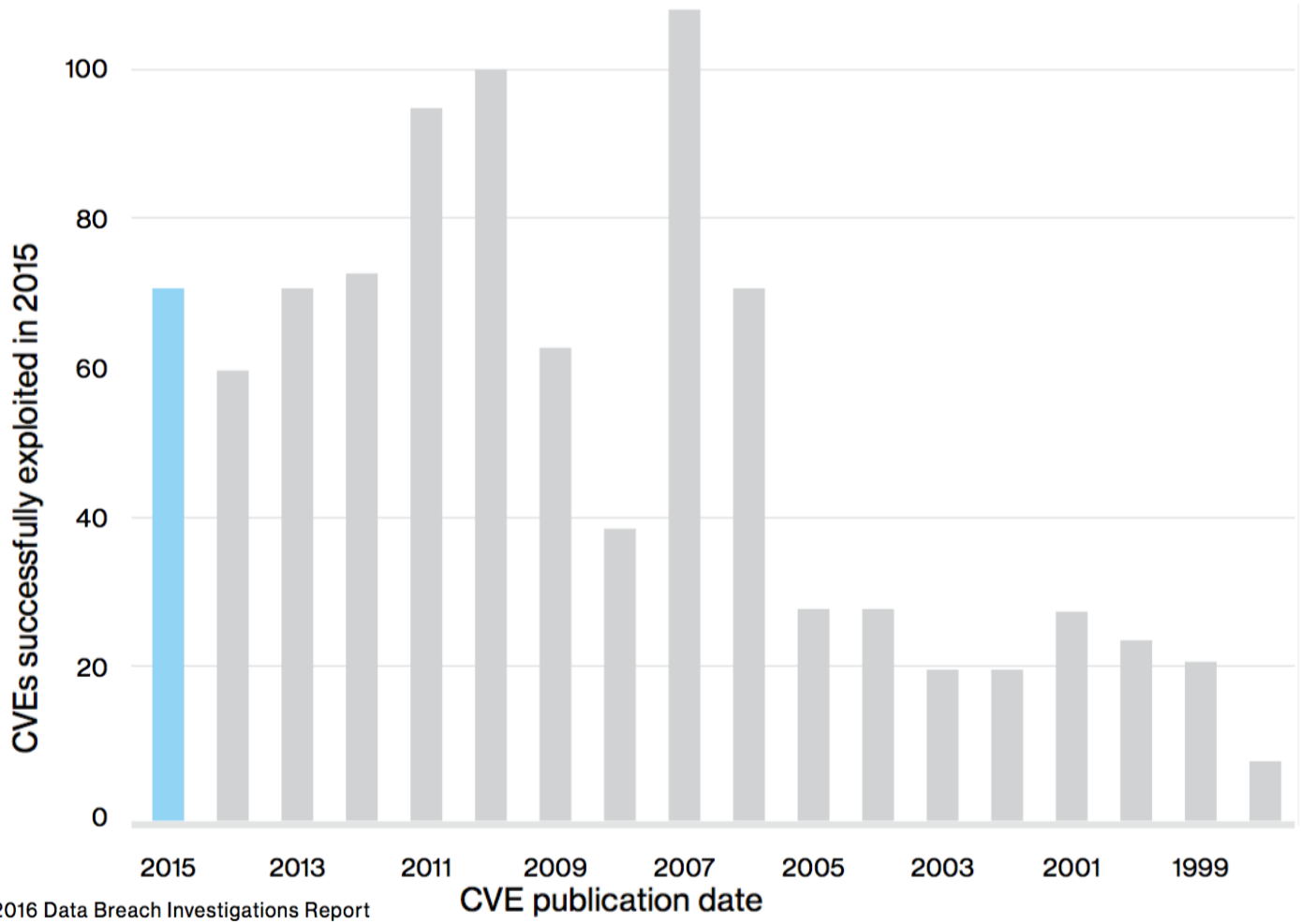


NOW WHAT? You need to:

- Determine if there is a patch or if it's a configuration change (CVE or CCE?)
- What vulnerabilities do we focus on 1st?
- Prioritize remediation schedule
- Follow the change process
- Coordinate with Service Owners
- Patch in Developoment first to ensure patches don't cause OUTAGES!

© 2017 ServiceNow All Rights Reserved

Count of CVEs Exploited in 2016 by CVE Publication Date



Verizon 2016 Data Breach Investigations Report

- "Oldies are still goodies," hackers continue to exploit old vulnerabilities.
- Do we know specifically why older vulnerabilities are the riskiest?
- With the majority of breaches caused by existing vulnerabilities, 99.9% of those exploited vulnerabilities were compromised more than a year after the CVE was published.
- Why are vulnerabilities over a year old inherently riskier?
- A CVE being added to Metasploit is probably the single most reliable predictor of exploitation in the wild.

© 2017 ServiceNow All Rights Reserved

Where this leaves most organizations

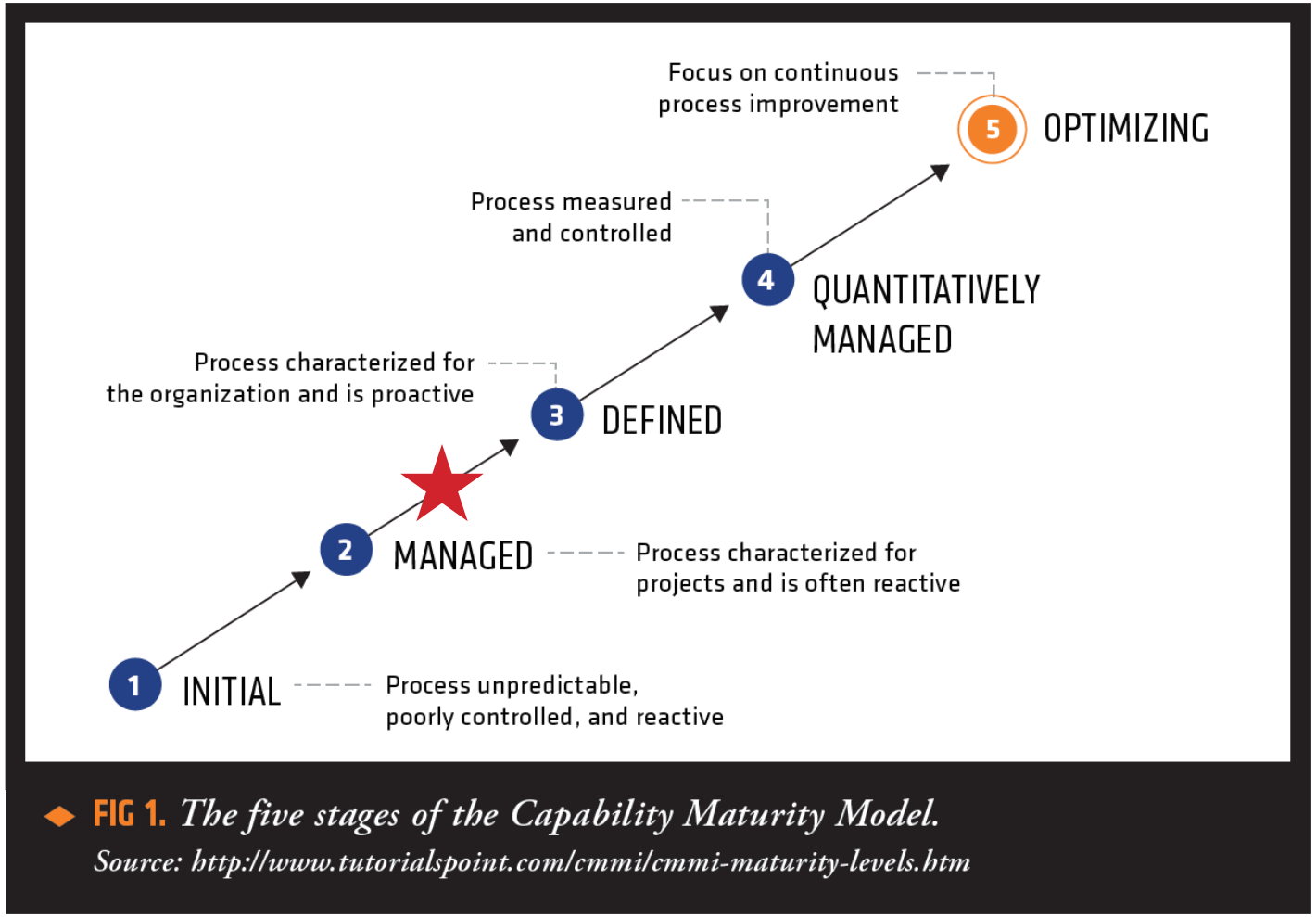


FIG 1. *The five stages of the Capability Maturity Model.*
Source: http://www.tutorialspoint.com/cmmi/cmmi-maturity-levels.htm

- Most organizations float between managed and defined, with some processes outlined but still struggling to keep up
- Manual processes and lack of visibility into the data that is most important stifles maturity
- Inability to prioritize the sheer number of vulnerabilities leaves organizations overwhelmed and overly exposed to risk

© 2017 ServiceNow All Rights Reserved

Why The Vulnerability Management Team is Overwhelmed?






Disconnected Tools for Response & Remediation

© 2017 ServiceNow All Rights Reserved

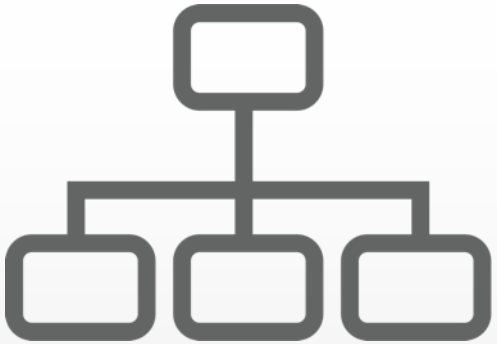
How can ServiceNow help secure your enterprise?

© 2017 ServiceNow All Rights Reserved

ServiceNow Vulnerability Response Key Focus Areas:



Deliver Automated Vulnerability Response



Coordinate and Streamline Remediation

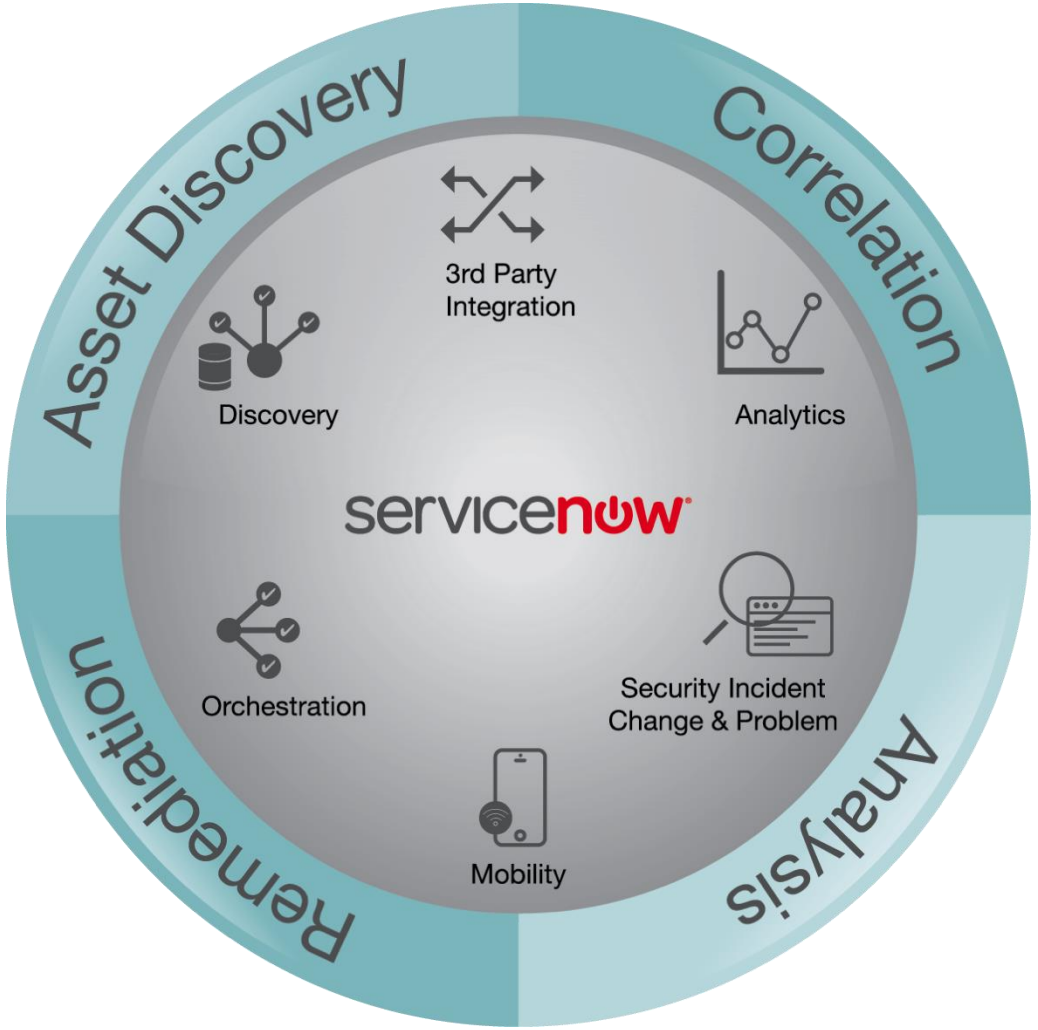


Visualize Your Security Posture

© 2017 ServiceNow All Rights Reserved

Vulnerability Response

- A platform for managing not just vulnerabilities, but vulnerability response
- Coordinate and automate remediation activities
- Manage vulnerabilities in bulk with vulnerability grouping
- 3rd party integrations major vulnerability scan engines
- Seamless integration with other platform features:
  - Security Incident Response plans
  - Incident/Problem/Change Management
  - Risk Management



© 2017 ServiceNow All Rights Reserved

Key ServiceNow Vulnerability Response out of the box Integrations



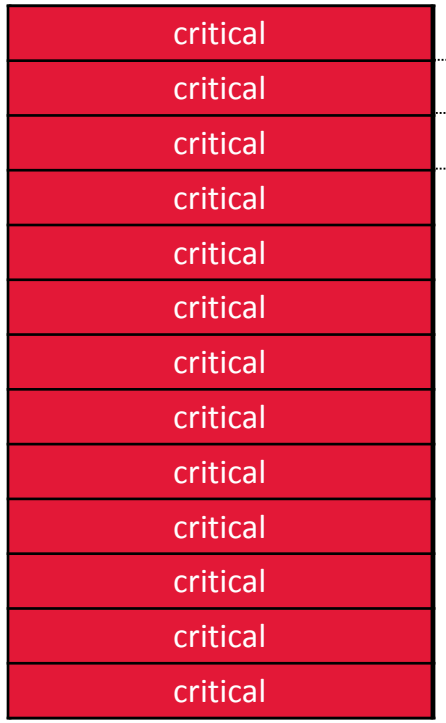




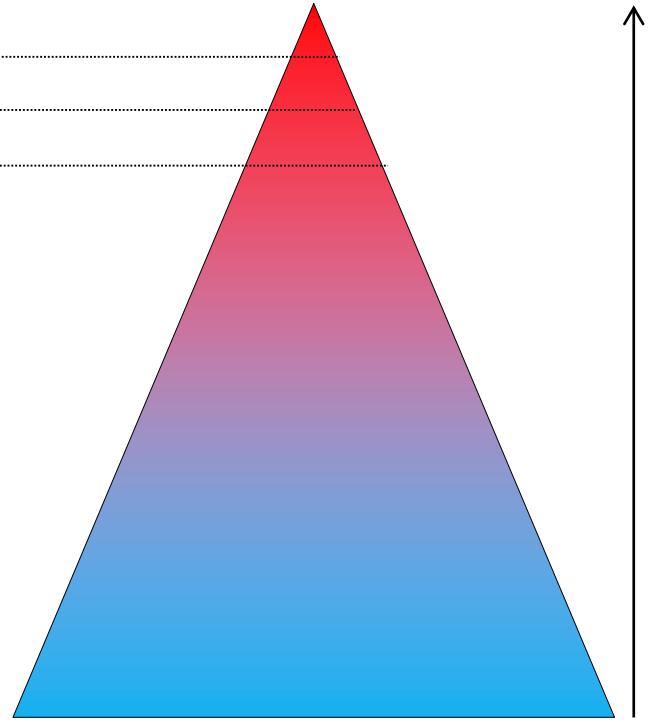
© 2017 ServiceNow All Rights Reserved

How can you prioritize and remediate the overwhelming wave of critical vulnerabilities?

Too Many “Critical” Vulnerabilities



Critical Risks



How can we prioritize to reduce the sheer number of “Critical” Vulnerabilities?

Who can think of a few risk multipliers?

Criteria:

- Ease of Exploit
- Vulnerability Score
- Vulnerability Age
- Your Business Context

Traditional Vulnerability Scoring

Advanced Vulnerability Prioritization with ServiceNow

© 2017 ServiceNow All Rights Reserved

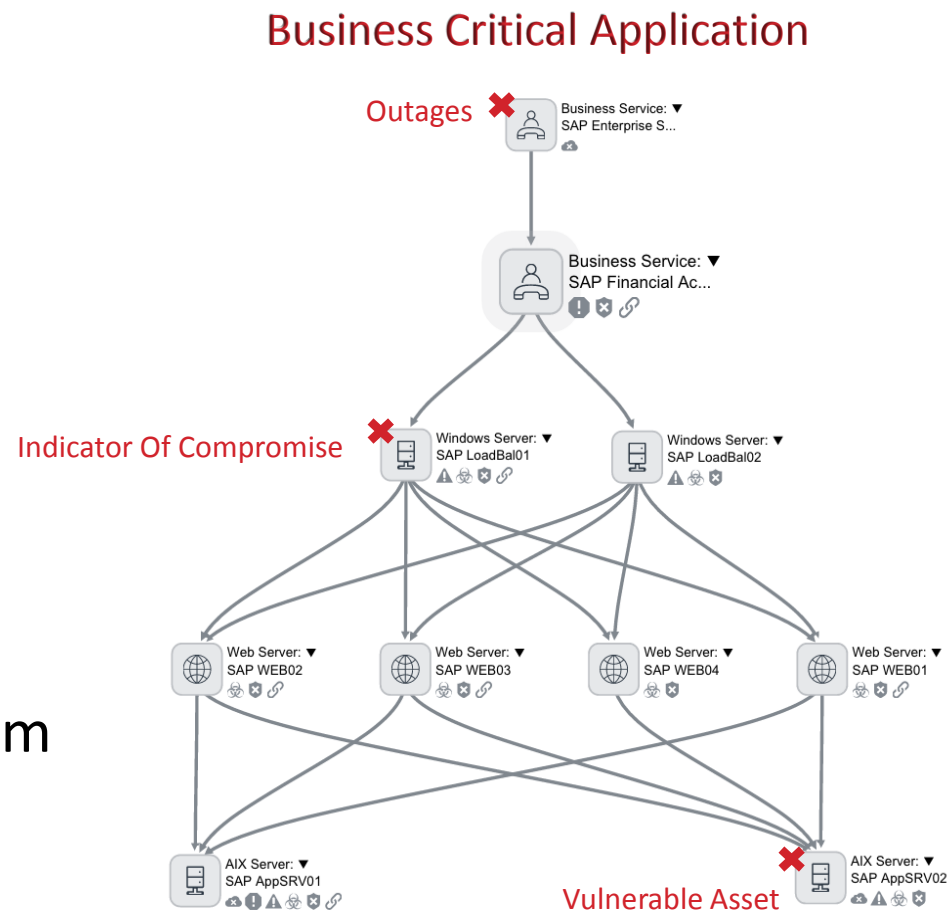
Reduce Risk through Automated Vulnerability Remediation

Situational Awareness:

- Who supports/owns the asset?
- What business risks are related to these assets?
- Are there any associated external threats?
- What changes have recently happened?

Automate Remediation:

- Leverage Orchestration to remediate
- Distribute Workloads automatically to the right team
- Assign SLAs for critical fixes
- Align with Risk Mitigation/Deferment process



© 2017 ServiceNow All Rights Reserved

Conclusion: Vulnerability Management is like…

Sloth from Goonies



© 2017 ServiceNow All Rights Reserved



- Definitely not as sexy as our cyber security brothers Incident Response and Threat Intelligence

© 2017 ServiceNow All Rights Reserved



- Normally left out of the process in the “security” basement
- Very scary and seems like maybe a lot of work at first!!

© 2017 ServiceNow All Rights Reserved



- There’s probably one guy in the organization that appreciates VM.

© 2017 ServiceNow All Rights Reserved



- The only reward we get is enjoying some Rocky Road ice cream after a long day

© 2017 ServiceNow All Rights Reserved



- Or maybe somebody gives us some free Halloween candy in the breakroom once a year

© 2017 ServiceNow All Rights Reserved



- But VM is integral to cyber security…& in the end VM saves the day!!

© 2017 ServiceNow All Rights Reserved



- And when we have the right processes and prioritize our efforts, VM shows immediate value

© 2017 ServiceNow All Rights Reserved



- Finally….when understood, VM is loved by all!!

© 2017 ServiceNow All Rights Reserved

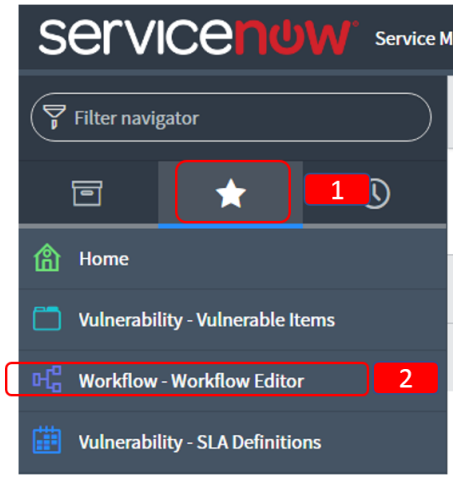
Labs

#Know17 | http://clabs.link/lab132024

© 2017 ServiceNow All Rights Reserved

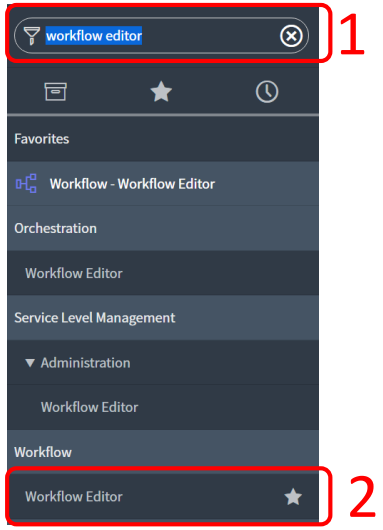
Overall Lab Typos and / or tips

- **There are no favorites, so type what you are looking for in the filter navigator…IE: When creating a workflow, instead of going to favorites & finding workflow editor …**



Instead, type workflow editor into

Your filter navigator & click

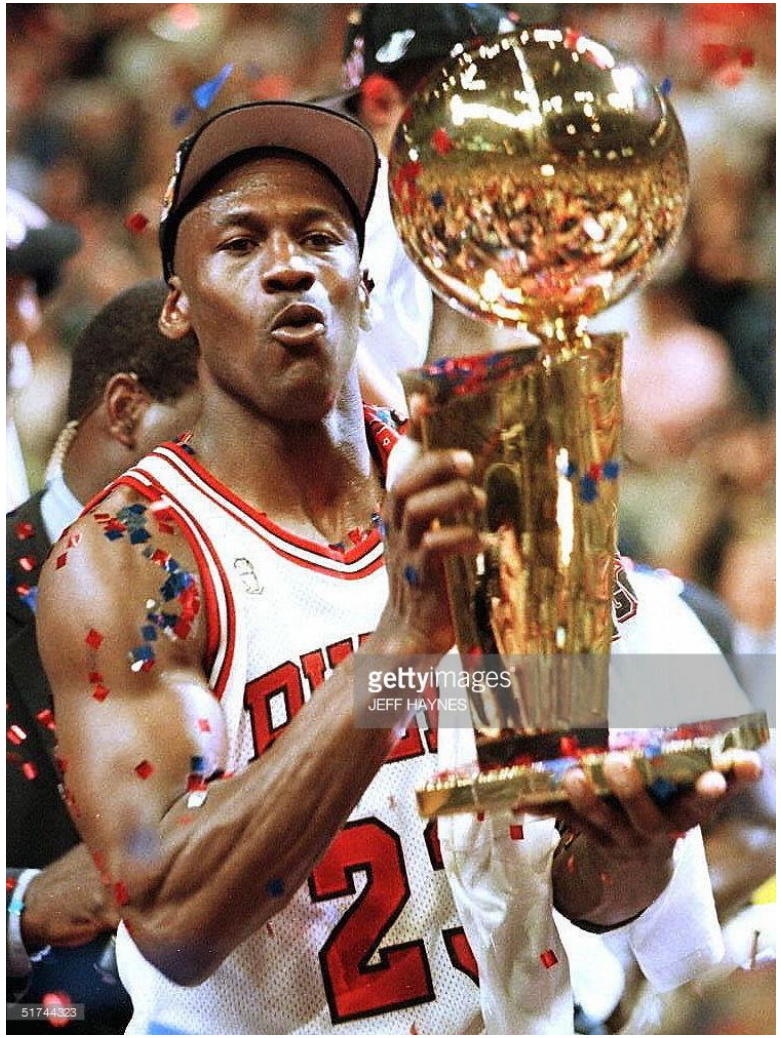


- **Also, just remember once you choose "show related fields" for one condition…you don't have to do it again…so ignore this instruction for the 2nd and 3rd conditions.**

© 2017 ServiceNow All Rights Reserved

Lab 1

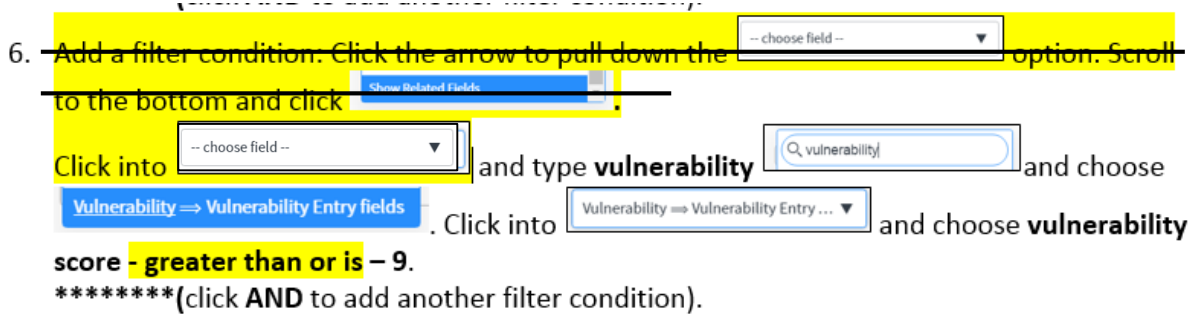
- Define Success



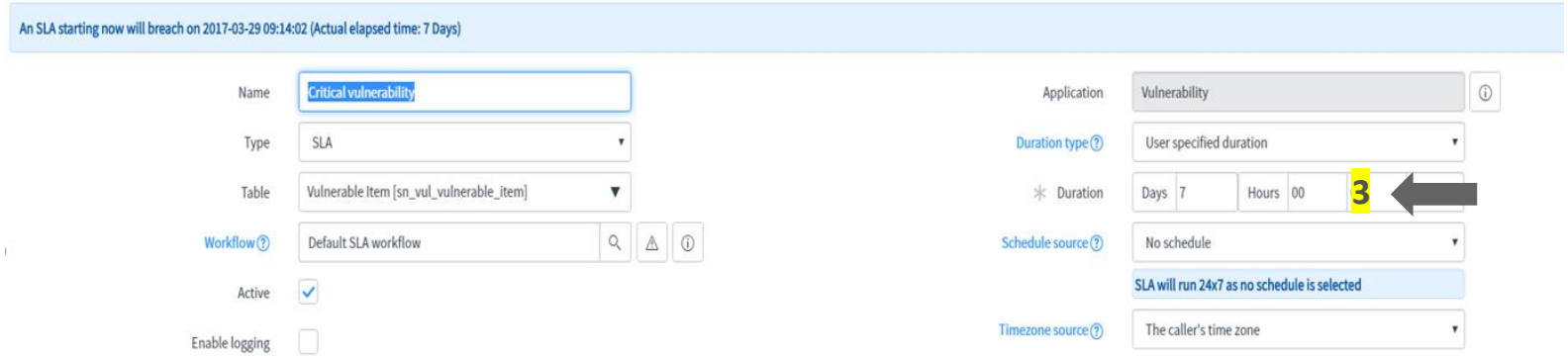
© 2017 ServiceNow All Rights Reserved

Lab 1 Typos and / or tips

- **Pg 2 ----- #6 ------**once you choose “show related fields” for one condition…you don’t have to do it again…so ignore this instruction for the 2nd and 3rd conditions. **Also on Pg 2 ----#6-----** vulnerability score should be “greater than or is” – 9….AS SEEN BELOW



- **Pg3----- #9------** “Duration” should be 3 min. not 7 days



- **Pg3 -----** the last action says click “update”…it should be “submit”

© 2017 ServiceNow All Rights Reserved

Lab 2

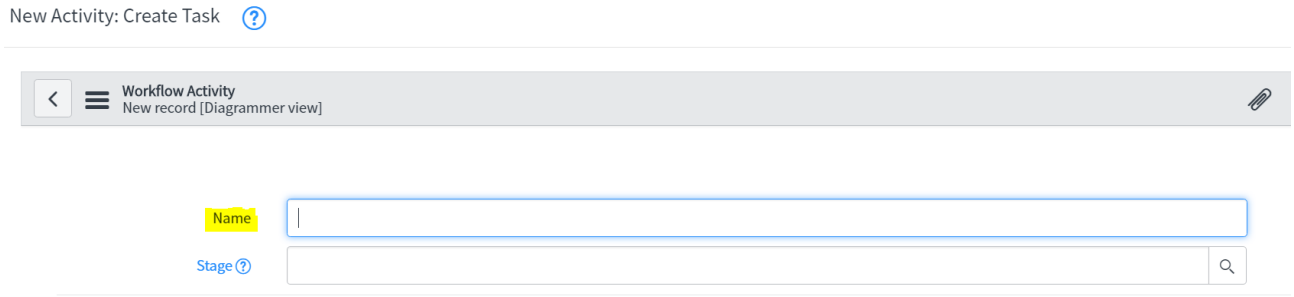
- Automate the response process



© 2017 ServiceNow All Rights Reserved

Lab 2 Typos and / or tips

- ***OVERALL NOTE: IF YOUR CONNECTOR LINES IN A WORKFLOW AREN'T CONNECTING FROM DRAGGING YOUR TASKS ON TOP OF THEM…JUST DROP THE TASK ON THE CANVAS, DELETE THE LINE & RE-CONNECT**
- Pg 11 ---- First entry before #1 should be to – Name your Task "**Patch installed / remediation action taken"**



- **PG 15 & 16 *****DON'T RIGHT CLICK THE HAMBURGER…JUST CLICK IT…
- **PG 16 --- within #18 ----** Once you click the hamburger, click "checkout"…click back into the hamburger & then you can click into properties
- **Pg 17 ----** click update at the end

© 2017 ServiceNow All Rights Reserved

Lab 3

- You say you're managing vulnerabilities in bulk?





© 2017 ServiceNow All Rights Reserved

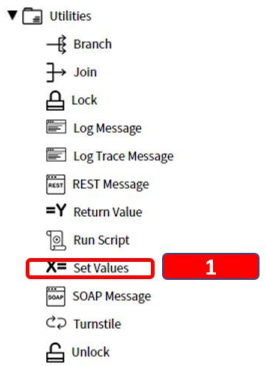
Lab 3 Typos and / or tips

- **Just remember once you choose “show related fields” for one condition…you don’t have to do it again…so ignore this instruction for the 2nd and 3rd conditions.**

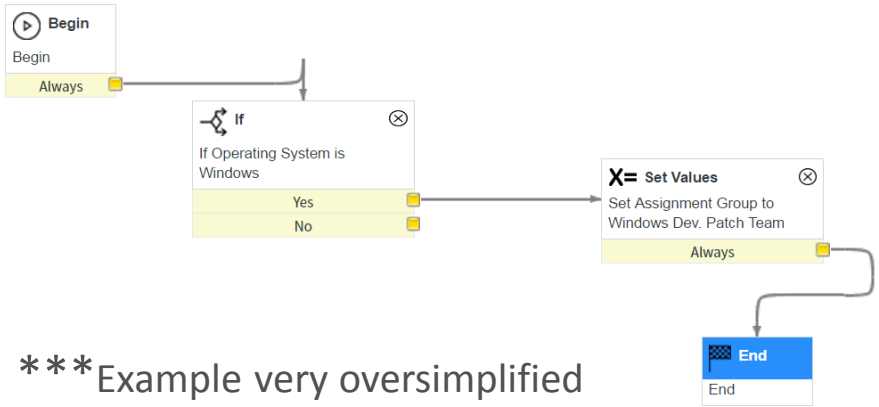
© 2017 ServiceNow All Rights Reserved

In Production…

- *******NOTE: We can assign ownership for patching / remediation with vulnerability groups, or even embed it in a workflow. We can harvest operating system or system owner information from the CMDB and / or scan data to create filter conditions for patching / remediation ownership as seen below.
- Because no two customers are the same in the way they assign ownership, this lab very simply assigned ownership to a generic “Dev. Patching Group.” BECAUSE WE ALWAYS TEST PATCHES BEFORE IMPLEMENTING IN PRODUCTION!!!







***Example very oversimplified

We can use a set value utility

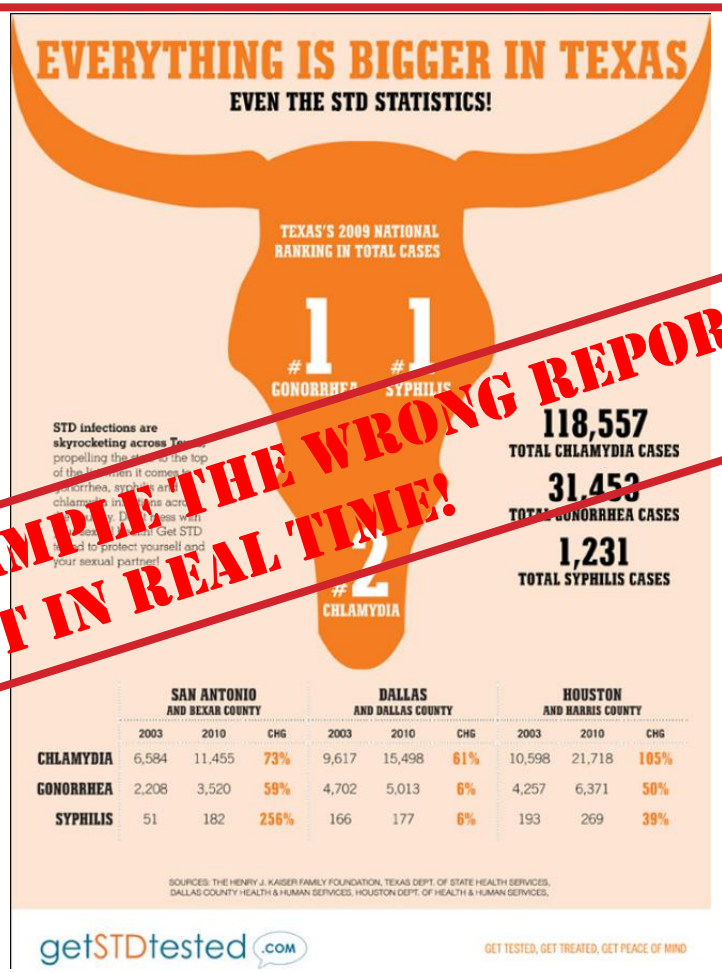
To assign ownership in a workflow

© 2017 ServiceNow All Rights Reserved

Lab 4

- Create the right reports. Get your data in real time.

EXAMPLE OF THE WRONG REPORT!



EXAMPLE THE WRONG REPORT NOT IN REAL TIME!

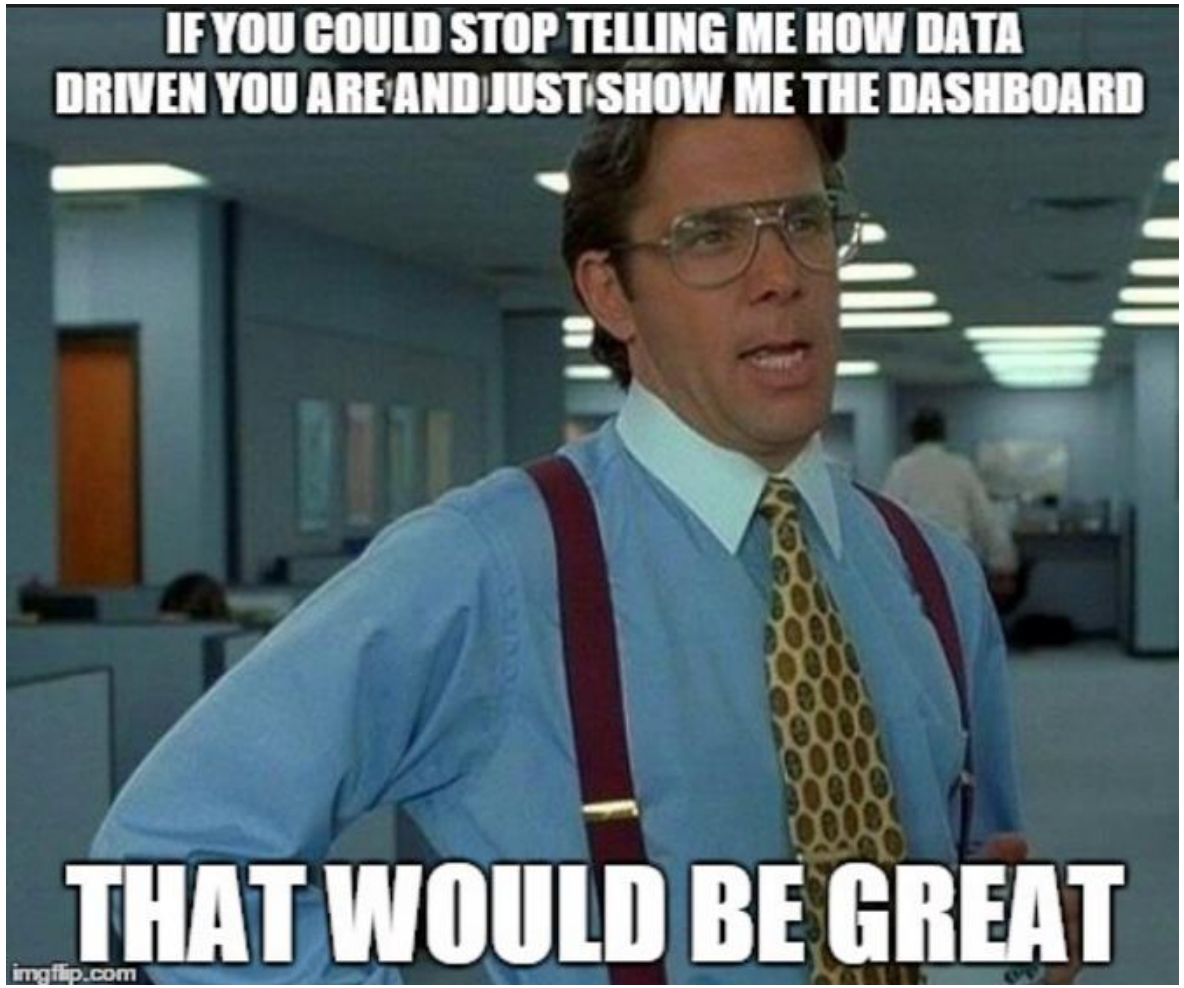
I relocated to Austin, TX in July 2016 without access to this report!!



© 2017 ServiceNow All Rights Reserved

Lab 5

- Create your dashboards. Get complete visibility into the entire enterprise



© 2017 ServiceNow All Rights Reserved

Lab 5 Typos and / or tips

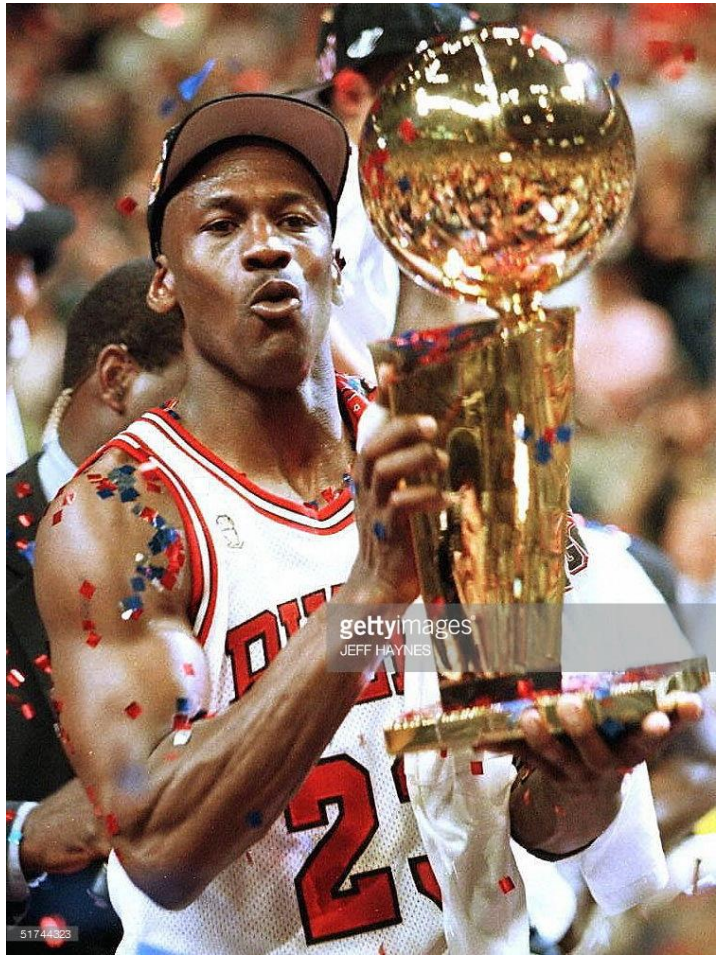
- **Pg 28 --- #1 ---** indicates just click on servicenow icon in top left…then the + sign will appear for #2

- **Pg 32 ---- #10 --- sub item at bottom of page,#3 -----** the chosen report should be “vulnerabilities” not “Vulnerable items by state”

© 2017 ServiceNow All Rights Reserved

Demo & Follow Along

- Live demo & follow along of everything we just accomplished

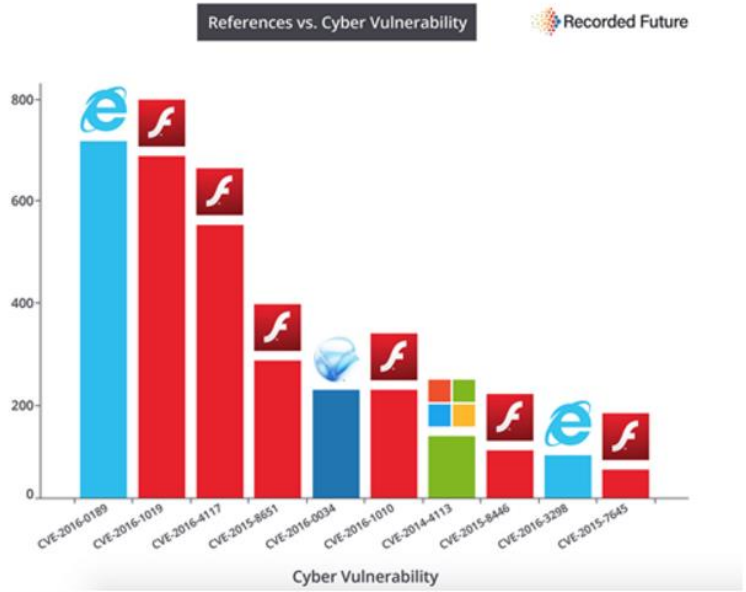


We Won!!!!!!!!

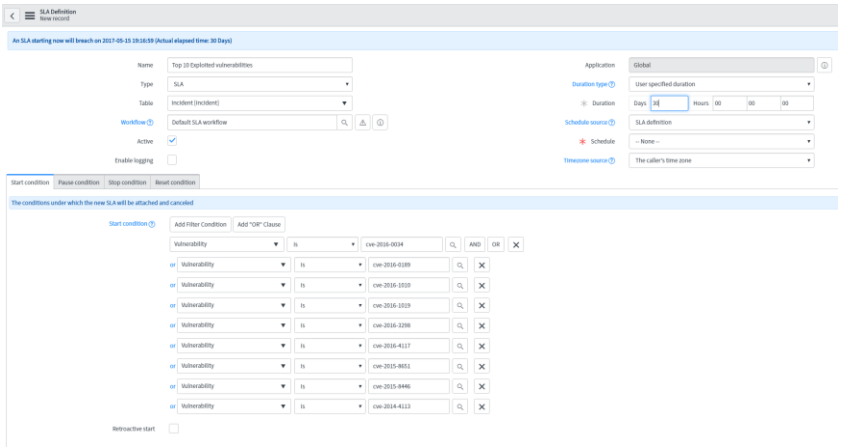
© 2017 ServiceNow All Rights Reserved

Food for thought – Take it to the next level!

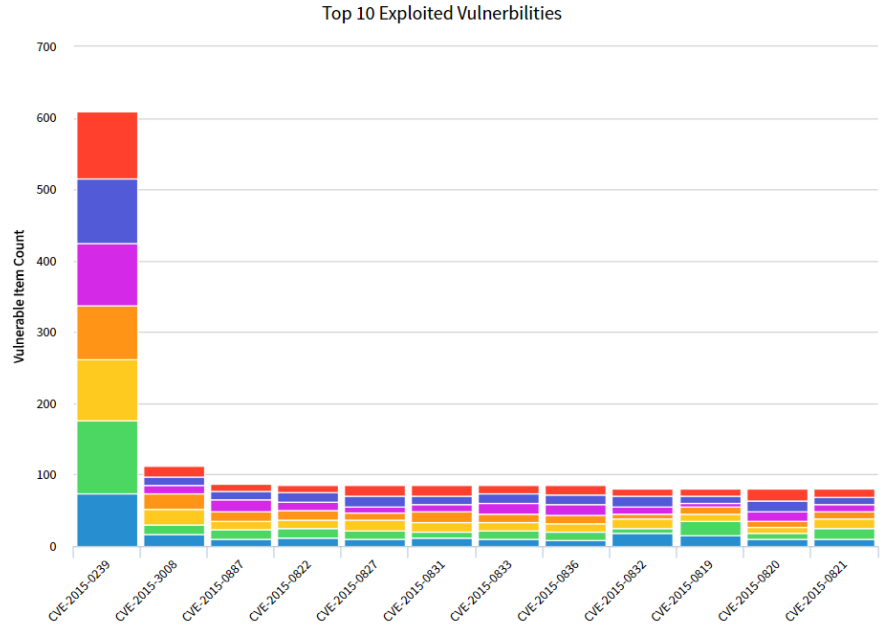
Of the breaches that occurred from exploiting vulnerabilities, 99.9% were over 1 yr old…85% of those are from only __ # of vulnerabilities? Answer: 10



Top 10 vulnerabilities exploited by threat actors



SLA's , Vuln. Groups, & Workflows created fc
top 10 exploited vulnerabilities



Dashboard for top 10 exploited vulnerabilities

Identify Define Visualize

© 2017 ServiceNow All Rights Reserved

Value Outcomes we're seeing with customers

60%

Reduction in vulnerability response times



Processing, prioritizing, and assigning a majority of vulnerabilities within 24hrs of implementation

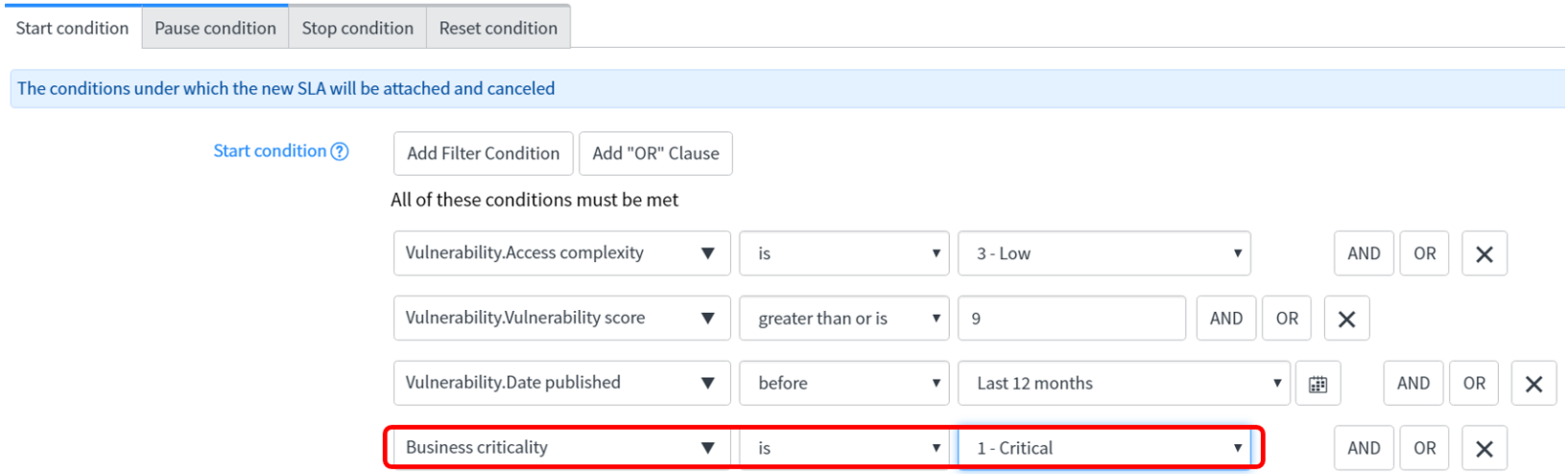
50%

Improved accuracy of asset information in the CMDB with authoritative IP info. coming from vulnerability scans

© 2017 ServiceNow All Rights Reserved

***NOTE

- The lab today was done completely without using business criticality as a risk multiplier; allowing customers to realize immediate value & ROI even without a mature CMDB, and accelerating value with one.
- Adding business criticality to any SLA, Vuln. Group, or Workflow is a simple add of a condition



© 2017 ServiceNow All Rights Reserved

Top Takeaways

1

You are not alone! A majority of organizations are struggling to keep up with the overwhelming amount of vulnerabilities

2

Prioritizing the response process according to true vulnerability risk and business criticality with tie in to the CMDB allows organizations to focus on what matters

3

Defining success, automating the response process, and providing real time visibility allows organizations to continually improve their processes

© 2017 ServiceNow All Rights Reserved

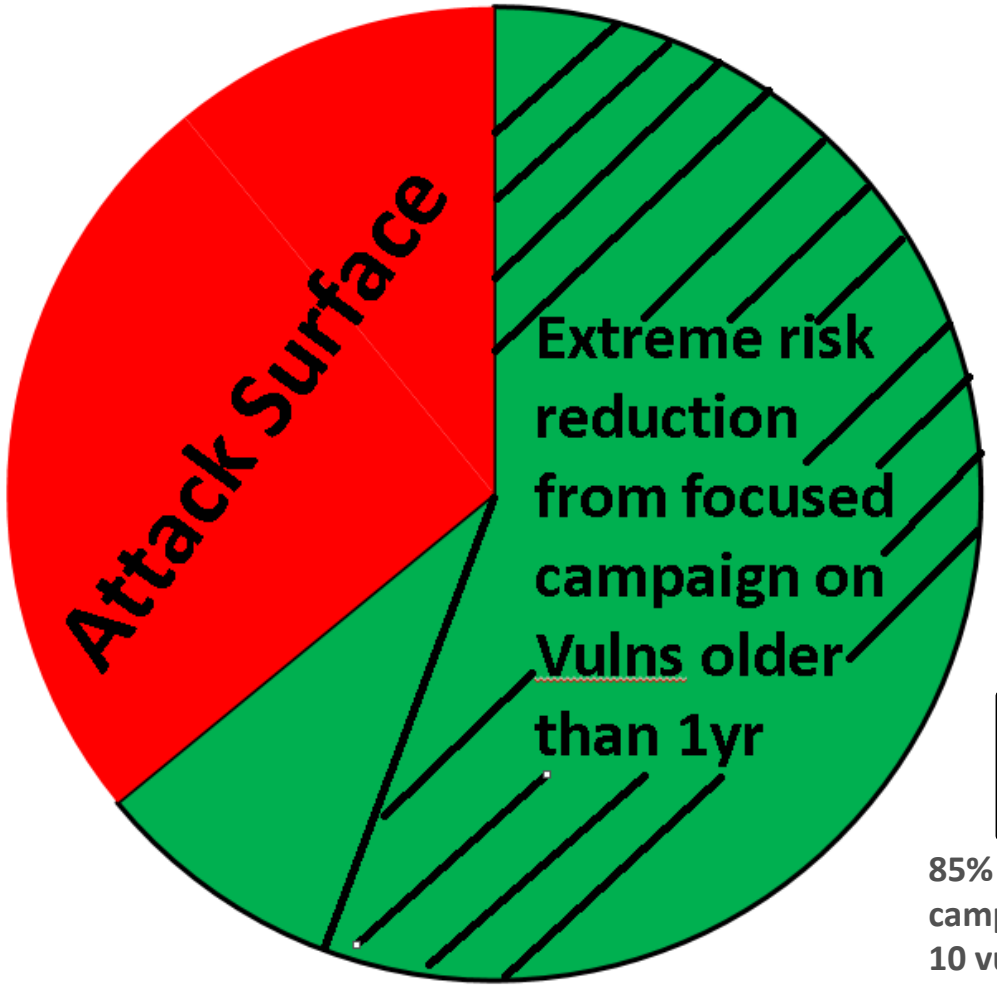
How can we not get better?

- We know a majority of breaches occur because of existing vulnerabilities.
- Of those breaches, we know 99.9% of them occur because of vulnerabilities over a year old.
- Of those year old vulnerabilities we know bad actors exploit only 10 vulnerabilities 85% of the time.
- If we focus on the top 10 first…and vulnerabilities over a year old after those…how can we lose?
- In theory we could turn off our vulnerability scanner for a year…

© 2017 ServiceNow All Rights Reserved

Have the conversation, champion the cause!!

- Can you go to your Director, CISO or CIO with a solid plan to reduce risk?
- If our attack surface can be drastically reduced by 51% + in a short period of time…can we focus resources to accomplish this?
- If we could get 85% of the way there by taking two weeks to remediate only 10 vulnerabilities…why would we not?



85% reduction with a short campaign focused on the top 10 vulnerabilities

© 2017 ServiceNow All Rights Reserved

We can do this!!!

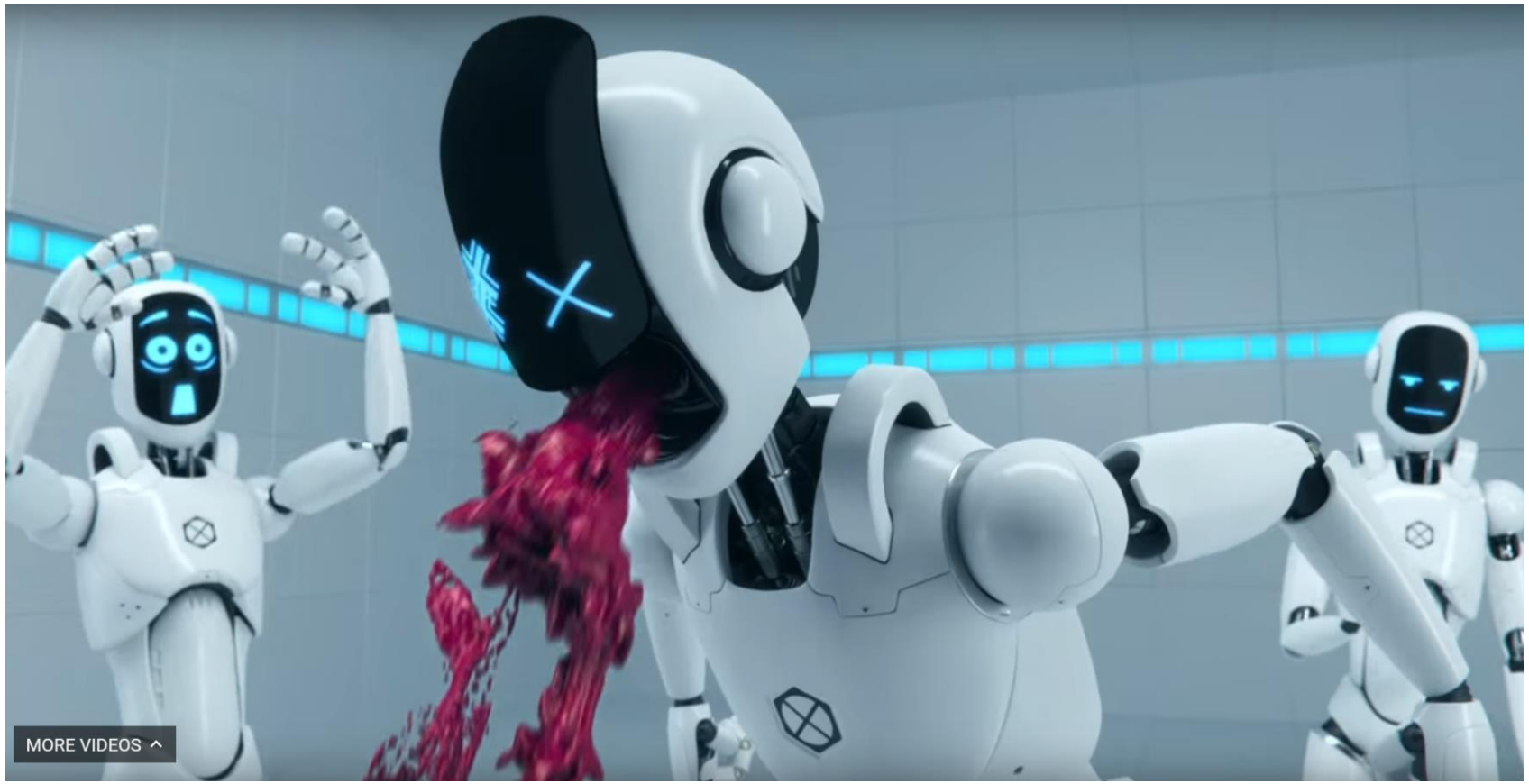
- **We can be cyber superheroes!!!!!!!!!**



© 2017 ServiceNow All Rights Reserved

And if we don’t?

This is what a breach feels like to our systems!!



© 2017 ServiceNow All Rights Reserved

Thank You

Jonathan Walker
Security Solutions Architect
ServiceNow, Security & Risk Practice

David Bell
Security Solutions Architect
ServiceNow, Security & Risk Practice

#Know17 | http://clabs.link/lab132024

© 2017 ServiceNow All Rights Reserved

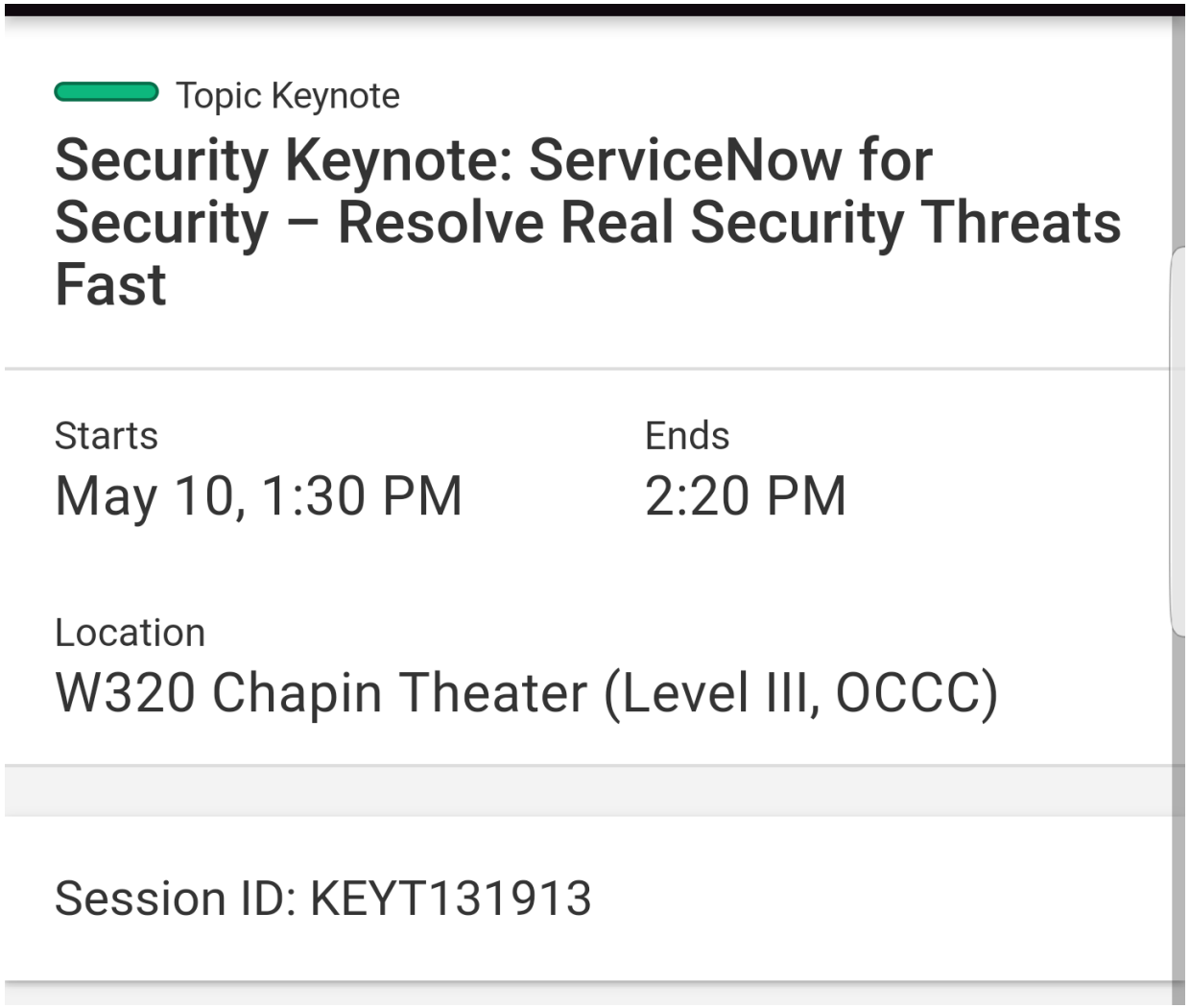
Q & A

Jonathan Walker
Security Solutions Architect
ServiceNow, Security & Risk Practice

David Bell
Security Solutions Architect
ServiceNow, Security & Risk Practice

© 2017 ServiceNow All Rights Reserved

Also, don’t forget to attend our Security Keynote tomorrow at 1:30pm



© 2017 ServiceNow All Rights Reserved