knowledge17

WORK at LIGHTSPEED™

Moving from Vulnerability Assessment to Vulnerability Management

JEFF BATTAGLINO
DIRECTOR, IT SERVICE MANAGEMENT, COMPLIANCE & SECURITY
Seton Hall University

© 2017 ServiceNow All Rights Reserved

servicenow

Speaker Introduction



NAME: Jeff Battaglino

TITLE: Director, IT Service Management, Compliance & Security

FUNCTION: ITIL and ITSM Design, Implementation and Maintenance

COMPANY: Seton Hall University

EXPERIENCE: Over 25 years managing various departments in IT Service Management

EXPERTISE: ITSM, ITIL, Production Support, Technical Support, Analytics, Security

ACHIEVEMENTS: Designed and built ITSM infrastructures for 4 different organizations, ITIL v3 Foundations Certified

CURRENT PROJECTS: IT Security Operations Management, Contract Management, Configuration Management

© 2017 ServiceNow All Rights Reserved

About Seton Hall University

One of the country's leading Catholic universities, Seton Hall University has been developing students in mind, heart and spirit since 1856. Home to nearly 10,000 undergraduate and graduate students and offering more than 90 rigorous majors, Seton Hall's academic excellence has been singled out for distinction by The Princeton Review, U.S. News & World Report and Bloomberg Businessweek. Seton Hall's 58-acre main campus is located in the quaint town of South Orange, New Jersey, only 14 miles from Manhattan. The University's nationally-ranked School of Law is located in nearby Newark, New Jersey.

History

- Founded: 1856 by Bishop James Roosevelt Bayley
- Namesake: Elizabeth Ann Seton, first American-born saint
- Affiliation: Catholic, one of the oldest diocesan universities in the U.S., under the Archdiocese of Newark
- Location: South Orange, New Jersey, suburban setting 30 minutes from NYC

Undergraduate enrollment: 5,800

- 59% female/41% male
- 44% diversity rate
- 70 countries represented
- 80% of freshmen live on campus

Graduate enrollment: 4,300

Faculty and Academics

- Programs: 90+
- Average class size: 21 students
- Freshman English classes: 15 students
- Student-to-faculty ratio: 14:1
- Students in internships: 81%
- Employment Rate: 86%
  (About 20% higher than the national average)

© 2017 ServiceNow All Rights Reserved

IT Service Management Evolution Timeline – 2010

- Shared ServiceNow Instance with 70+ Higher Ed Institutions
- Needed unanimous buy-in for any changes (minor or major)
- Vetting process for changes to system took months
- Ticket categorization not in line with reporting needs

© 2017 ServiceNow All Rights Reserved

IT Service Management Evolution Timeline – 2011

- Purchased proprietary ServiceNow Instance for SHU
- Fully implemented Incident, Request, Change in 4 months (Aspen) ITIL standard categorization model and taxonomy
- Began gathering information for meaningful reports

© 2017 ServiceNow All Rights Reserved

IT Service Management Evolution Timeline – 2012

- Upgraded to Berlin version
- Implemented Problem and Knowledge Management
- Began sending Surveys for each Incident
- Created first workflows for approvals

© 2017 ServiceNow All Rights Reserved

IT Service Management Evolution Timeline – 2013

- Upgraded to Dublin version (Skipped Calgary)
- Implemented Project module
- Began investigating Asset Management module
- Attended first Knowledge Conference (Presented)

© 2017 ServiceNow All Rights Reserved

IT Service Management Evolution Timeline – 2014

- Began investigating Asset Management
- Created first application (Module) for Notifcations
- Activated first Integration (Knowledge Management)
- Began preparing for Eureka upgrade

© 2017 ServiceNow All Rights Reserved

IT Service Management Evolution Timeline – 2015

- Implemented Asset and Risk Management modules
- Upgraded to Fuji version (skipped Eureka)
- Learned about IT Security and Vulnerability Management module

© 2017 ServiceNow All Rights Reserved

IT Service Management Evolution Timeline – 2016

- Upgraded to Helsinki (patch 3) in September (skipped Geneva)
- CMDB fully operational with hardware and software assets
- Began to implement IT Security Operations Module

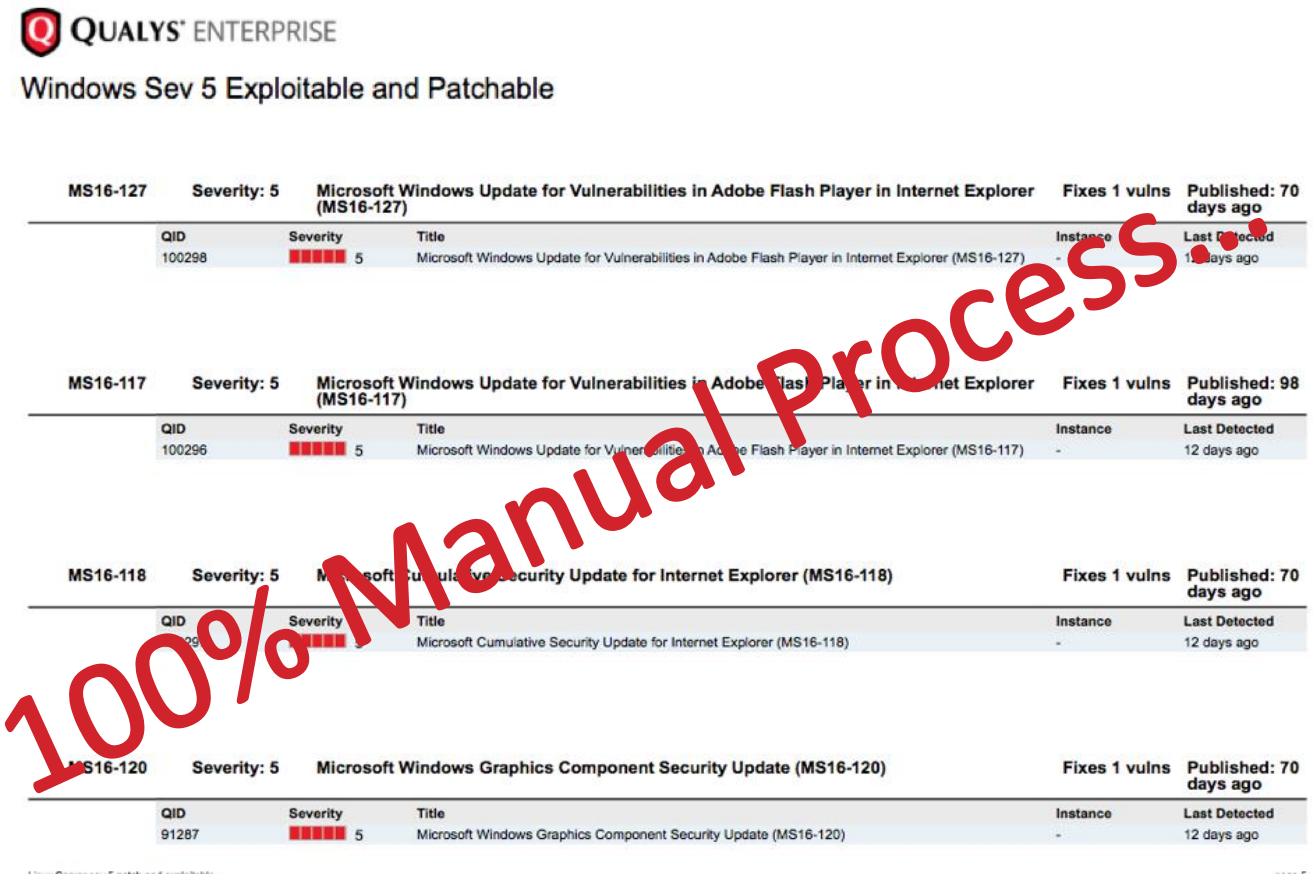
© 2017 ServiceNow All Rights Reserved

IT Service Management Evolution Timeline – 2017 YTD

- 140 active ITIL licenses (40 are STAs)
- Expecting to have Contract and Configuration Management active before year-end
- Complete and finalize IT Security Operations module for both Security and Vulnerability

© 2017 ServiceNow All Rights Reserved

Vulnerability Management: Where We Were…



QUALYS ENTERPRISE

Windows Sev 5 Exploitable and Patchable

MS16-127	Severity: 5	Microsoft Windows Update for Vulnerabilities in Adobe Flash Player in Internet Explorer (MS16-127)		Fixes 1 vulns	Published: 70 days ago
	QID	Severity	Title	Instance	Last Detected
	100298	5	Microsoft Windows Update for Vulnerabilities in Adobe Flash Player in Internet Explorer (MS16-127)	-	12 days ago
MS16-117	Severity: 5	Microsoft Windows Update for Vulnerabilities in Adobe Flash Player in Internet Explorer (MS16-117)		Fixes 1 vulns	Published: 98 days ago
	QID	Severity	Title	Instance	Last Detected
	100296	5	Microsoft Windows Update for Vulnerabilities in Adobe Flash Player in Internet Explorer (MS16-117)	-	12 days ago
MS16-118	Severity: 5	Microsoft Cumulative Security Update for Internet Explorer (MS16-118)		Fixes 1 vulns	Published: 70 days ago
	QID	Severity	Title	Instance	Last Detected
	[illegible]	[illegible]	Microsoft Cumulative Security Update for Internet Explorer (MS16-118)	-	12 days ago
MS16-120	Severity: 5	Microsoft Windows Graphics Component Security Update (MS16-120)		Fixes 1 vulns	Published: 70 days ago
	QID	Severity	Title	Instance	Last Detected
	91287	5	Microsoft Windows Graphics Component Security Update (MS16-120)	-	12 days ago

100% Manual Process…

- Obtained vulnerabilities in Qualys
- Analyzed for accuracy and validity
- Report sent to IT department heads
- Groups remediated vulnerabilities
- Groups notified IT Security of completion
- Follow-up Qualys scans were run for verification

© 2017 ServiceNow All Rights Reserved

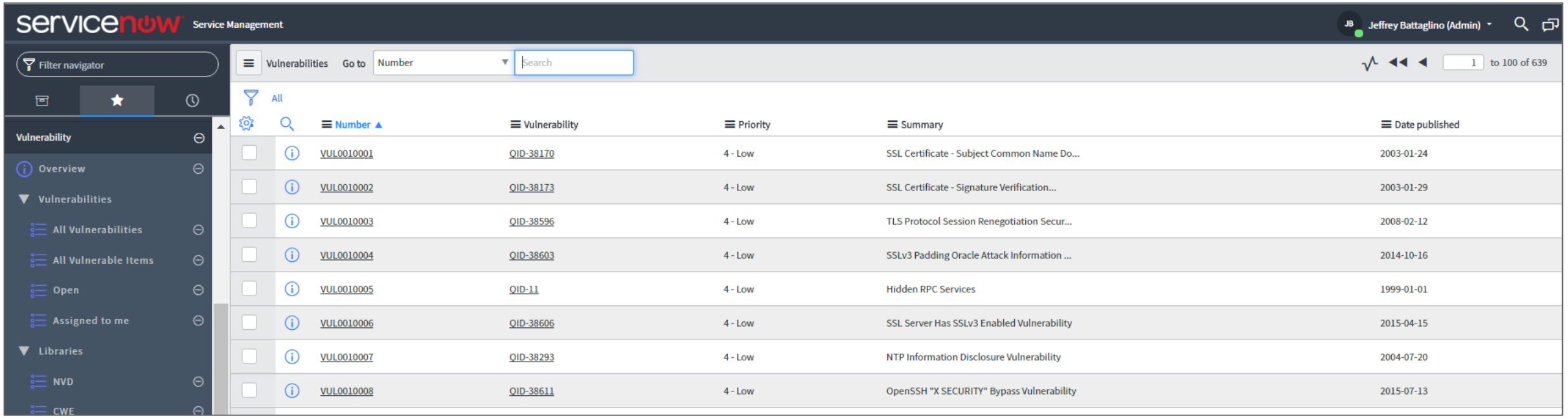
Vulnerability Management: Where We Were…

Challenges

- Keeping Vulnerability information in spreadsheets was difficult to update by different groups
- Spreadsheet version updates were extremely difficult to maintain
- Each update produced a new spreadsheet, which made historical tracking difficult and clumsy
- Tracking progress on Vulnerability remediation by group was impossible
- Tracking time spent on Vulnerability remediation was impossible

© 2017 ServiceNow All Rights Reserved

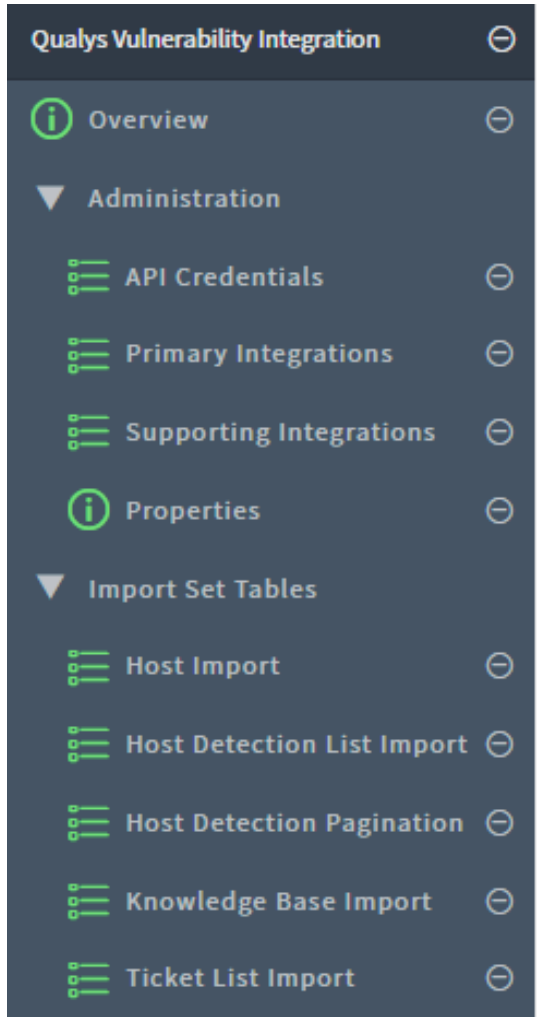
Vulnerability Management: Where We Are…



ServiceNow Security Operations module loaded with Qualys Integration

© 2017 ServiceNow All Rights Reserved

Vulnerability Management: Where We Are…



- Integration connects Qualys database to Vulnerability database in ServiceNow
- Selectable fields in Vulnerability tickets in ServiceNow
- Filter data by criteria selected in the integration
- Use Business Rules to Assign Vulnerabilities to specific groups

© 2017 ServiceNow All Rights Reserved

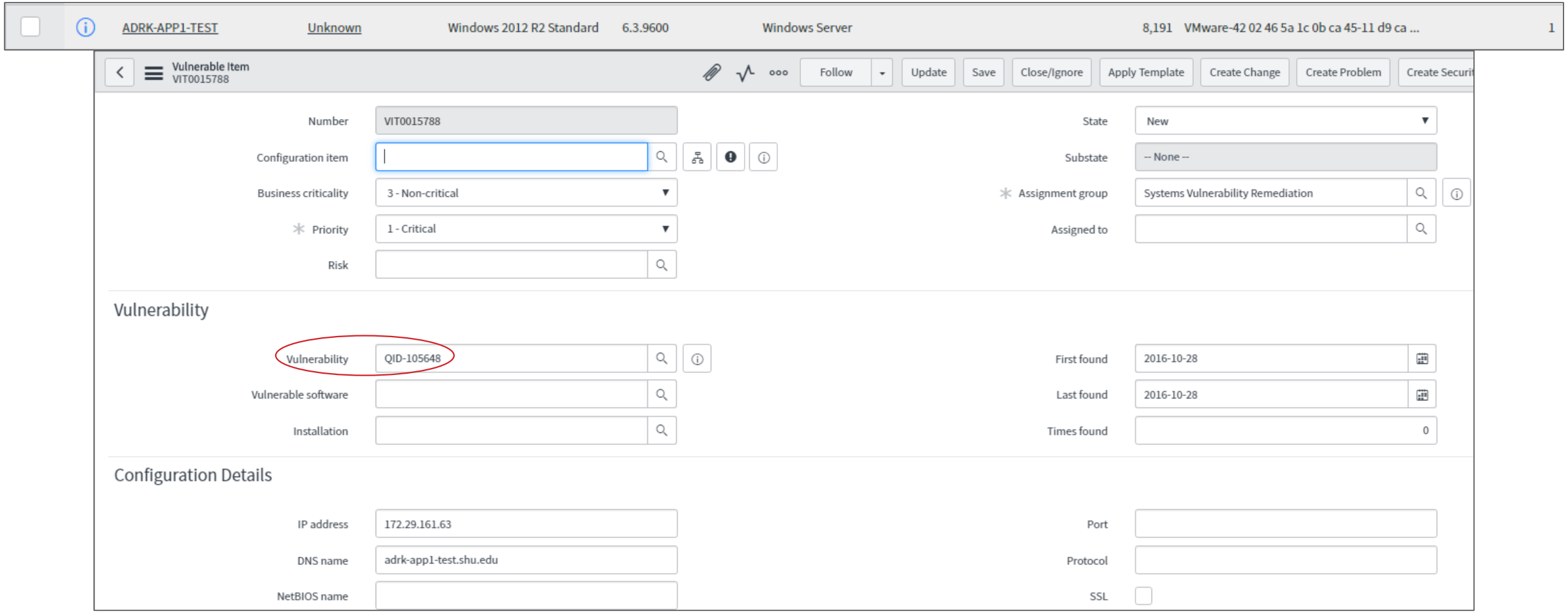
Vulnerability Management: Where We Are…

Challenges Met and Mastered…

- Vulnerabilities in ServiceNow allow for departments to update with full audit trails
- Detailed Vulnerability reporting allows for visible progress tracking
- Historical tracking made easy through worknotes
- Tracking progress on Vulnerability remediation by group now available
- Custom built time tracker easily added to Vulnerability module

© 2017 ServiceNow All Rights Reserved

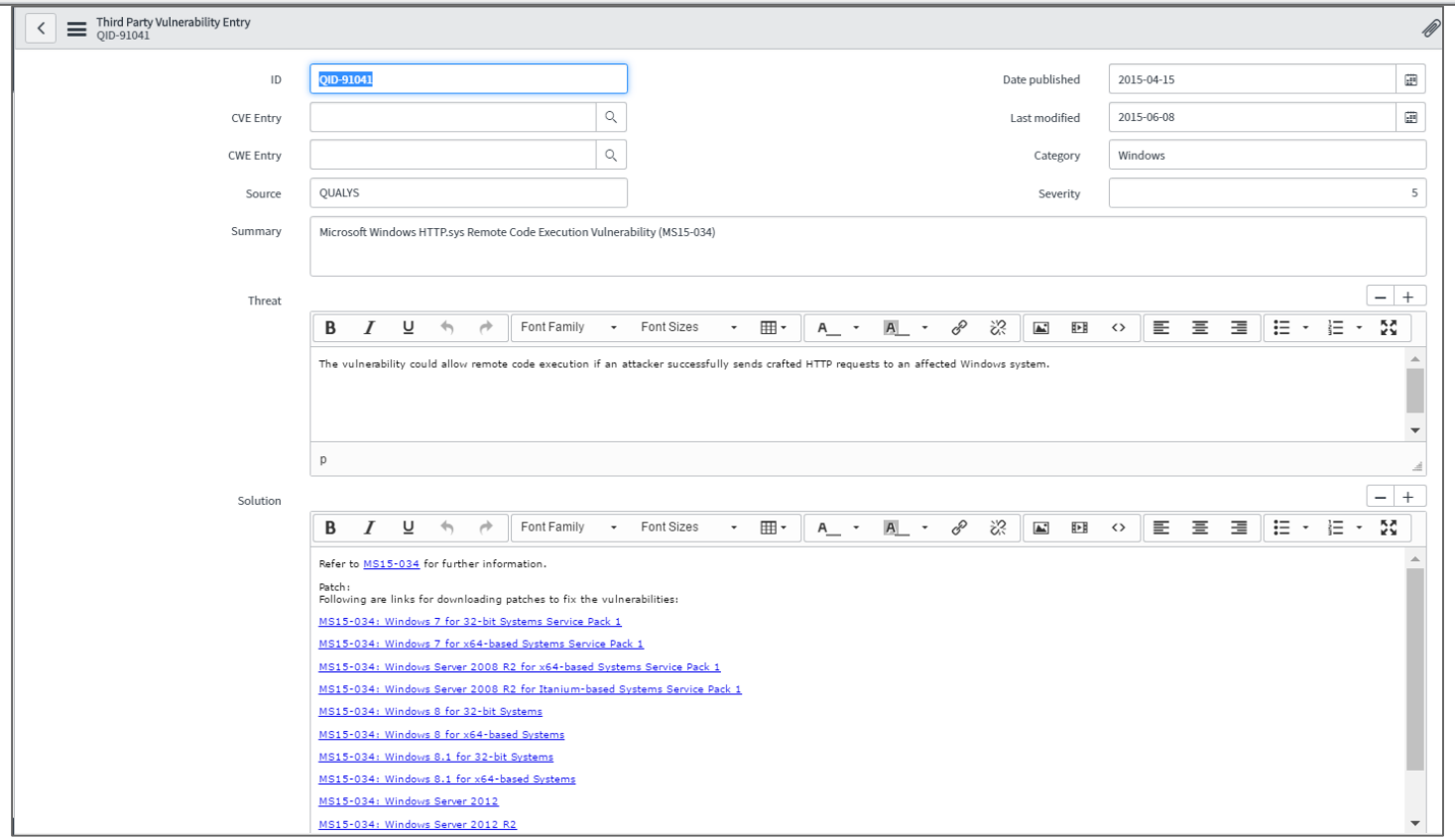
Vulnerable Items



© 2017 ServiceNow All Rights Reserved

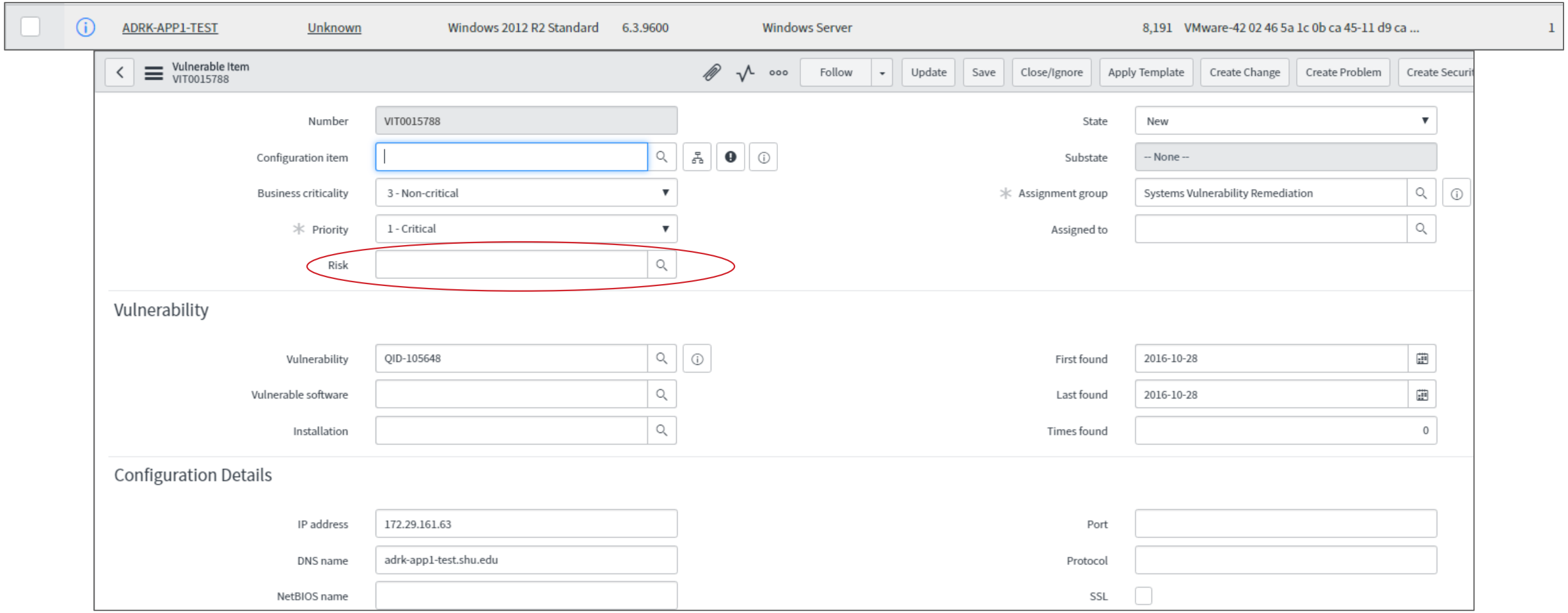
Vulnerable Items

☐	ⓘ	ADRK-APP1-TEST	Unknown	Windows 2012 R2 Standard	6.3.9600	Windows Server	8,191	VMware-42 02 46 5a 1c 0b ca 45-11 d9 ca ...	1



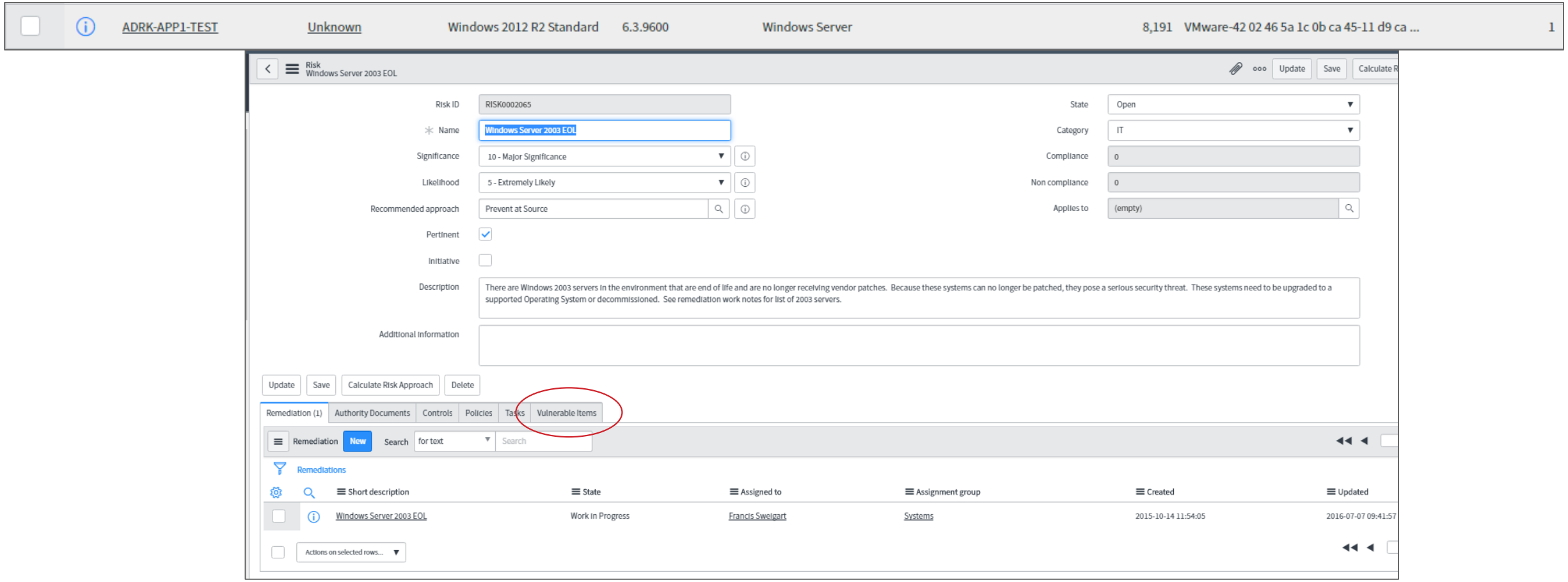
© 2017 ServiceNow All Rights Reserved

Vulnerable Items



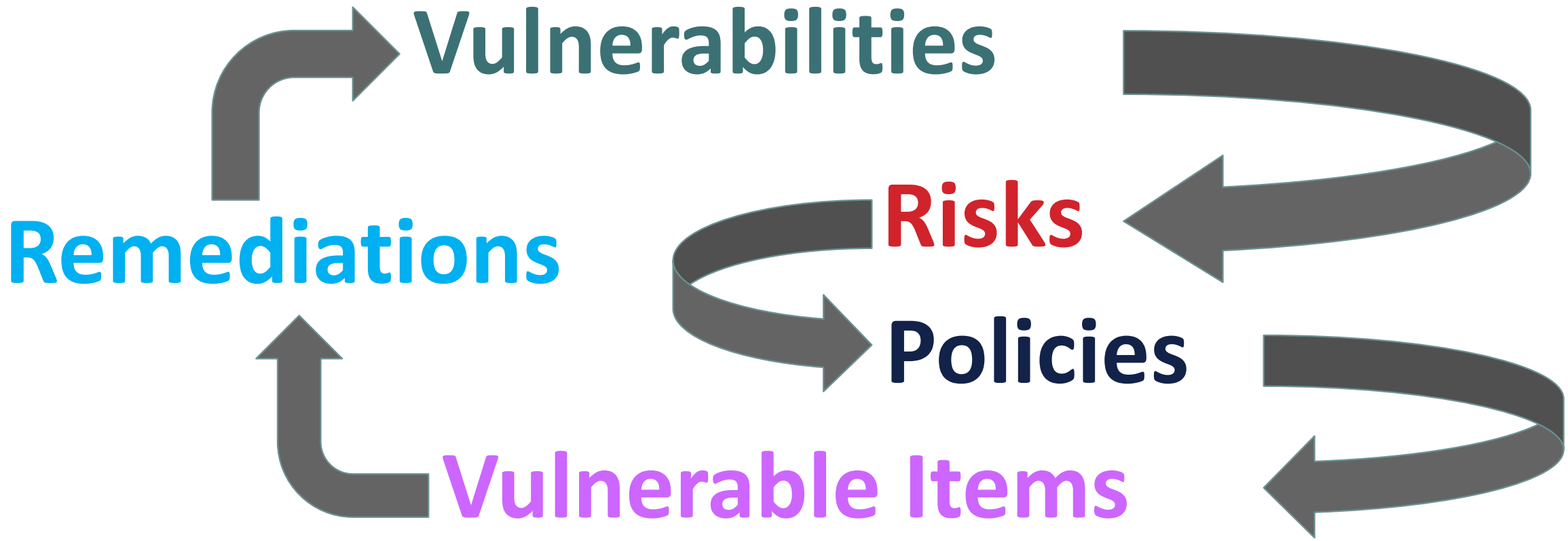
© 2017 ServiceNow All Rights Reserved

Vulnerable Items



© 2017 ServiceNow All Rights Reserved

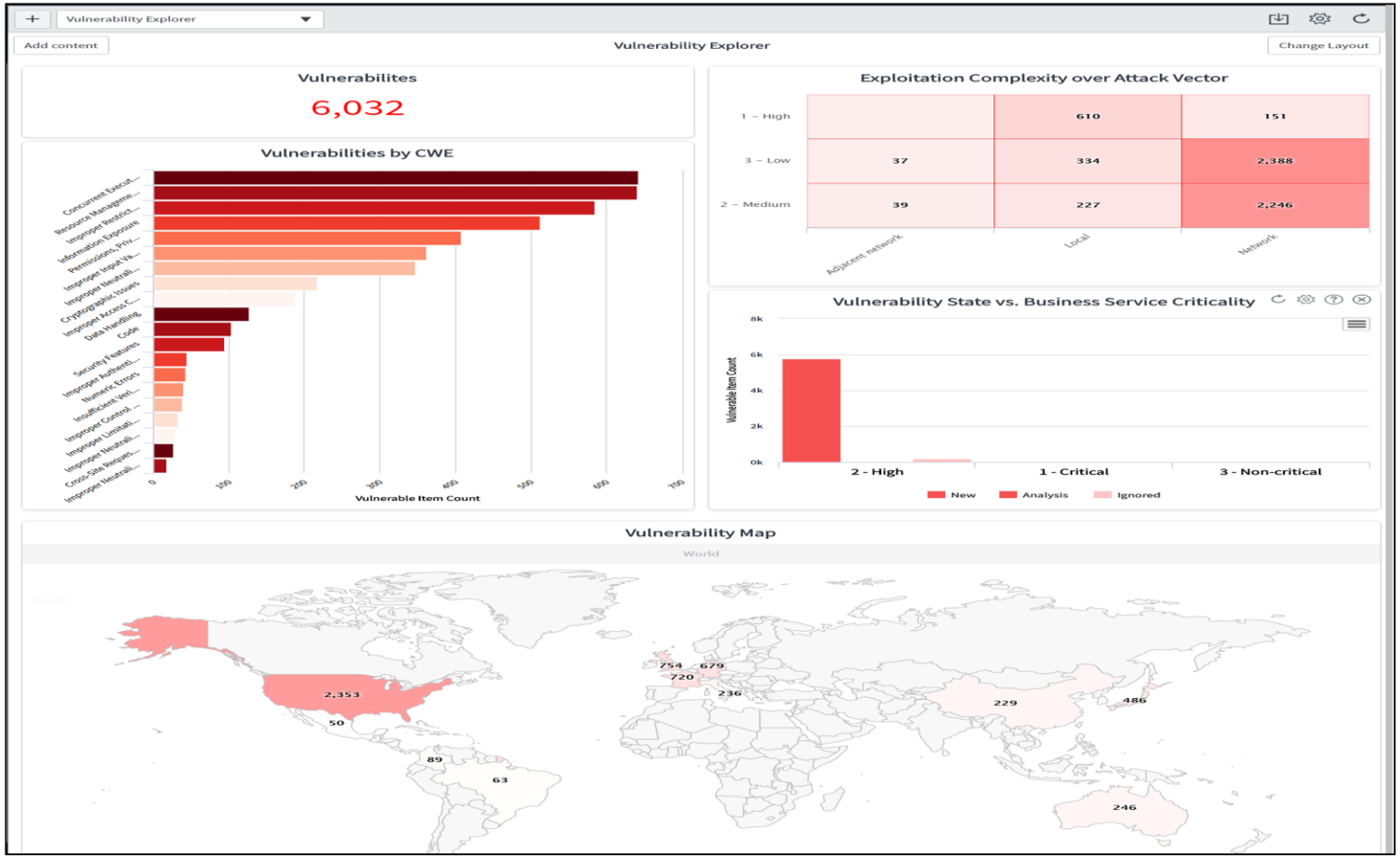
Seamless Integration



© 2017 ServiceNow All Rights Reserved

Performance Analytics Dashboards

(Some Included Without Subscription)



© 2017 ServiceNow All Rights Reserved

Lessons Learned

1. Do not try to duplicate current processes when moving to Security Operations and Vulnerability. Familiarize / Use the capabilities in the ServiceNow platform to streamline your processes and discover industry-standard solutions.

2. Utilize as much information as possible from external sources (Qualys, NVD, etc.)

3. Include all departments and contacts in your organization that have insights into vulnerabilities. This will be a great benefit in capturing your organization's vulnerability scope as a whole.

© 2017 ServiceNow All Rights Reserved

Our Next Steps



Continue to mitigate and reduce our vulnerabilities utilizing the ServiceNow platform



Expand our utilization of the other modules of the IT Security Operations Module in ServiceNow

© 2017 ServiceNow All Rights Reserved

Q&A

JEFF BATTAGLINO
DIRECTOR, IT SERVICE MANAGEMENT, COMPLIANCE & SECURITY
Seton Hall University

© 2017 ServiceNow All Rights Reserved

Thank You

JEFF BATTAGLINO
DIRECTOR, IT SERVICE MANAGEMENT, COMPLIANCE & SECURITY
Seton Hall University

© 2017 ServiceNow All Rights Reserved

Take the Survey

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

Thank You

Jeff Battaglino

Director, IT Service Management, Compliance & Security

Seton Hall University

© 2017 ServiceNow All Rights Reserved