NET+ Splunk Community Call 2023

This call brought to you by the NET+ Splunk program supported by campuses signing up for the NET+ Splunk program.

We will start at 5 min after the hour to allow others time to join.

Agenda

- The call, announcements, reminder the call is being recorded, etc
- NET+ Splunk Community Call 2023 – Baylor’s transition to Splunk Cloud
- Open discussion and questions
- Feedback on this call or NET+ Splunk

Baylor University’s Transition to Splunk Cloud

- Jon Allen Associate Vice President CIO & CISO
- Ruben Castillo Director Cybersecurity Operations

Why The Journey

- Splunk on premise for nearly ten years
- Significant staff and technology resources were required to operate the platform
- Limited time for staff to innovate new processes
- Total ROI not just tech ROI
- Launching a 24/7 SOC operation
- Wanted a Security Operations force multiplier

Starting Line

- Licensing Model
  - Review pros-cons for license models (Workload vs Ingest-Based)
  - Baylor moved to an Splunk Virtual Compute (SVC) model
- Products
  - On premise: Splunk Core and SplunkES (Enterprise Security)
  - Splunk Cloud: Added Splunk SOAR (Security Orchestration, Automation, and Response)
- Professional Services Engagement
  - Shed historic setup
  - Move to current best practices

Decision Points

- Organization Splunk Cloud Operational Objectives
  - What do you want to accomplish – status quo or integrate new operations?
- Splunk Cloud Architecture Options
  - Distributed Clustered Deployment + SHC - Single Site
- Understand Splunk Roles and your Responsibilities WRT O&M
  - Less maintenance time spent (you)
  - More time for operations (you)
  - Splunk maintenance (Splunk Support)

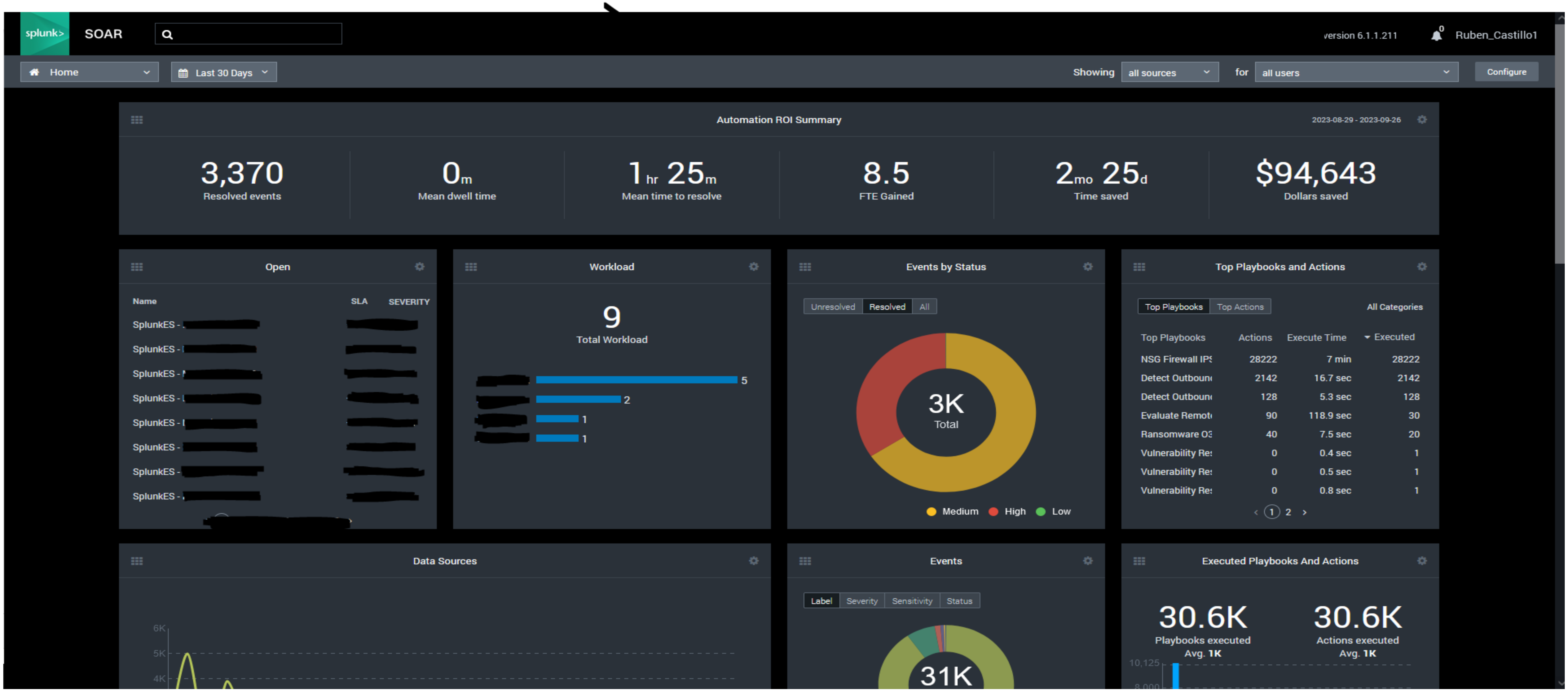
Homework

- Splunk Migration Assessment App (Environment Health Check)
  - Wants vs Needs
  - Connect with Splunk Account Manager
- Data Collection
  - The origin of your data: On-Prem, Cloud Apps, etc
- Optimize your environment
  - Unnecessary apps (Legacy), indexes, reports, etc.
- Searchable data/Archive data
  - CISO/CIO

Outcomes

- Live in Summer 2023
- Continuing to build out Baylor content
- Want to see great community cooperation
  - All using the same product should enable practice sharing
- Always room for improvement
  - Dynamic Microsoft data integration

Success snapshot – 9/27/2023



Automation ROI Summary 2023-08-29 - 2023-09-26

3,370	0m	1 hr 25m	8.5	2mo 25d	$94,643
Resolved events	Mean dwell time	Mean time to resolve	FTE Gained	Time saved	Dollars saved

Open

Name	SLA	SEVERITY
SplunkES - [redacted]	[redacted]	
SplunkES - [redacted]	[redacted]	
SplunkES - [redacted]	[redacted]	
SplunkES - [redacted]	[redacted]	
SplunkES - [redacted]	[redacted]	
SplunkES - [redacted]	[redacted]	
SplunkES - [redacted]	[redacted]	
SplunkES - [redacted]	[redacted]	

[redacted]

Workload

9
Total Workload

[redacted]	5
[redacted]	2
[redacted]	1
[redacted]	1

Events by Status

Top Playbooks and Actions

Top Playbooks	Actions	Execute Time	Executed
NSG Firewall IPS	28222	7 min	28222
Detect Outbound	2142	16.7 sec	2142
Detect Outbound	128	5.3 sec	128
Evaluate Remote	90	118.9 sec	30
Ransomware O3	40	7.5 sec	20
Vulnerability Res	0	0.4 sec	1
Vulnerability Res	0	0.5 sec	1
Vulnerability Res	0	0.8 sec	1

Data Sources

Events

Executed Playbooks And Actions

30.6K
Playbooks executed
Avg. 1K

30.6K
Actions executed
Avg. 1K

Questions

- Questions on the Baylor’s transition
- Other campuses looking to make this transition?

Net+ Splunk Updates

- Cisco acquisition of Splunk
  - https://www.splunk.com/en_us/newsroom/press-releases/2023/cisco-to-acquire-splunk-to-help-make-organizations-more-secure-and-resilient-in-an-ai-powered-world.html\
  - Splunk at EDUCAUSE
  - Splunk Workshops
  - https://discover.splunk.com/public-sector-virtual-workshop-series.html
  - Splunk Academic Alliances Program
  - Academic License Application Pledge for Good | Splunk

Closing and Thank you!

- Next call – topics and schedule?
- Registration for future calls for the calendar invite and call-in details will be sent out when we schedule the next call
- Recordings posted to:
  - https://spaces.at.internet2.edu/pages/viewpage.action?pageId=154764174
- If you have any questions, please the advisory board at splunk-advisory@internet2.edu or Nick Lewis (nlewis@internet2.edu)