Avoid Fines & Save Money! Automating Regulatory Compliance

Matt Coose

Founder and CEO, Qmulos

Scott Armstrong

Chief Strategy Officer, Qmulos

Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not, be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Agenda

Agenda

- What Is IT Security Compliance?
- Technical Elements
- Lessons Learned
- Benefits
- Use Cases
- Live Demo Of Compliance And Audit Capabilities

IT Security Compliance – Key Requirements

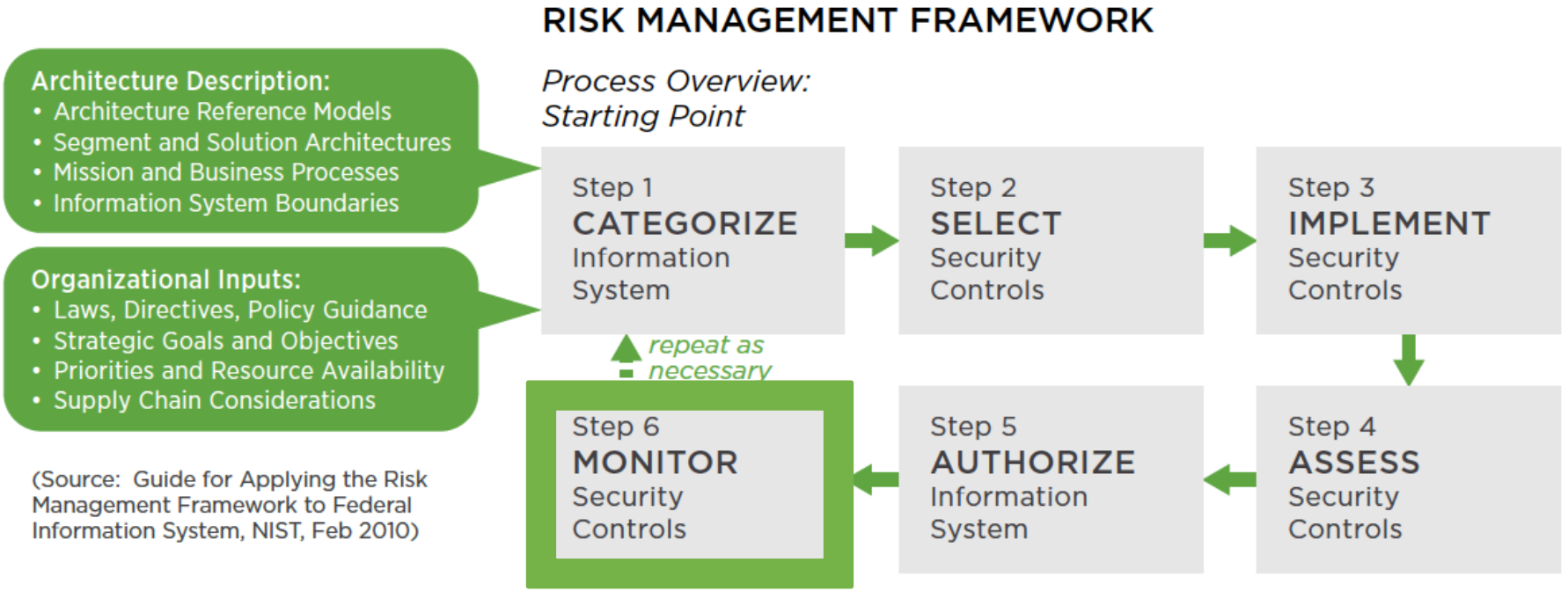
What Is IT Security Compliance?

In this context, it means providing ***EVIDENCE*** that you are doing ***risk management processes*** according to the appropriate IT Security **framework(s)**

Automated solutions must address:

- **Processes**
- **Monitoring** of frameworks/security controls
- **Evidence** collection

Process



(Source: Guide for Applying the Risk Management Framework to Federal Information System, NIST, Feb 2010)

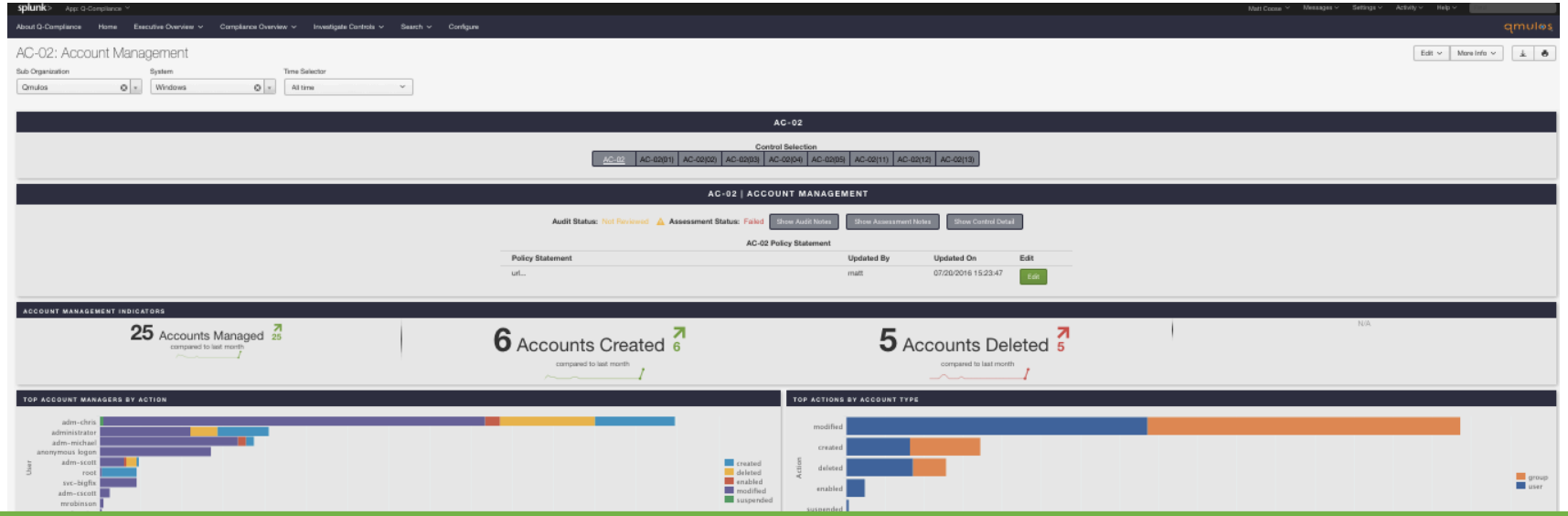
Monitoring

- Potentially thousands of controls, sub-controls, and enhancements
- Different types of controls include management, operational, and technical
- Technical controls and continuous monitoring
- Enable actionable compliance

Evidence

- Different sources and frequencies
- Policies, procedures, documents
- Technical
- Human activity!
- Dynamic evidence – auditor questions!

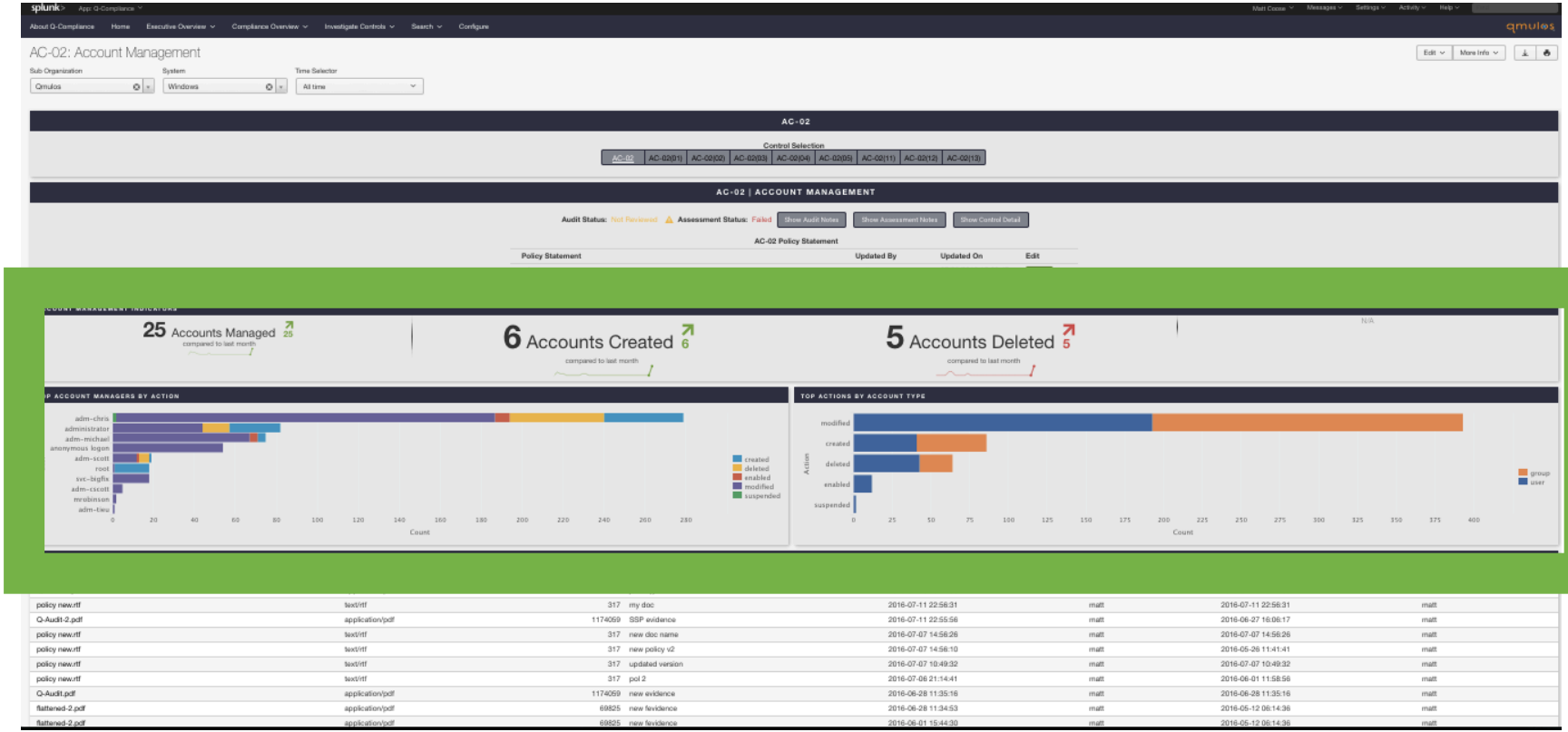
Policy Evidence



ASSIGNED EVIDENCE

File Name	Content Type	Content Size	Description	Assigned	Assigned By	Uploaded	Uploaded By
Q-Audit-2.pdf	application/pdf	1174059	jewkrqlj	2016-07-20 15:24:33	matt	2016-07-20 15:24:33	matt
policy new.rtf	text/rtf	317	my doc	2016-07-11 22:56:31	matt	2016-07-11 22:56:31	matt
Q-Audit-2.pdf	application/pdf	1174059	SSP evidence	2016-07-11 22:55:56	matt	2016-06-27 16:06:17	matt
policy new.rtf	text/rtf	317	new doc name	2016-07-07 14:56:26	matt	2016-07-07 14:56:26	matt
policy new.rtf	text/rtf	317	new policy v2	2016-07-07 14:56:10	matt	2016-05-26 11:41:41	matt
policy new.rtf	text/rtf	317	updated version	2016-07-07 10:49:32	matt	2016-07-07 10:49:32	matt
policy new.rtf	text/rtf	317	pol 2	2016-07-06 21:14:41	matt	2016-06-01 11:58:56	matt
Q-Audit.pdf	application/pdf	1174059	new evidence	2016-06-28 11:35:16	matt	2016-06-28 11:35:16	matt

Technical Evidence

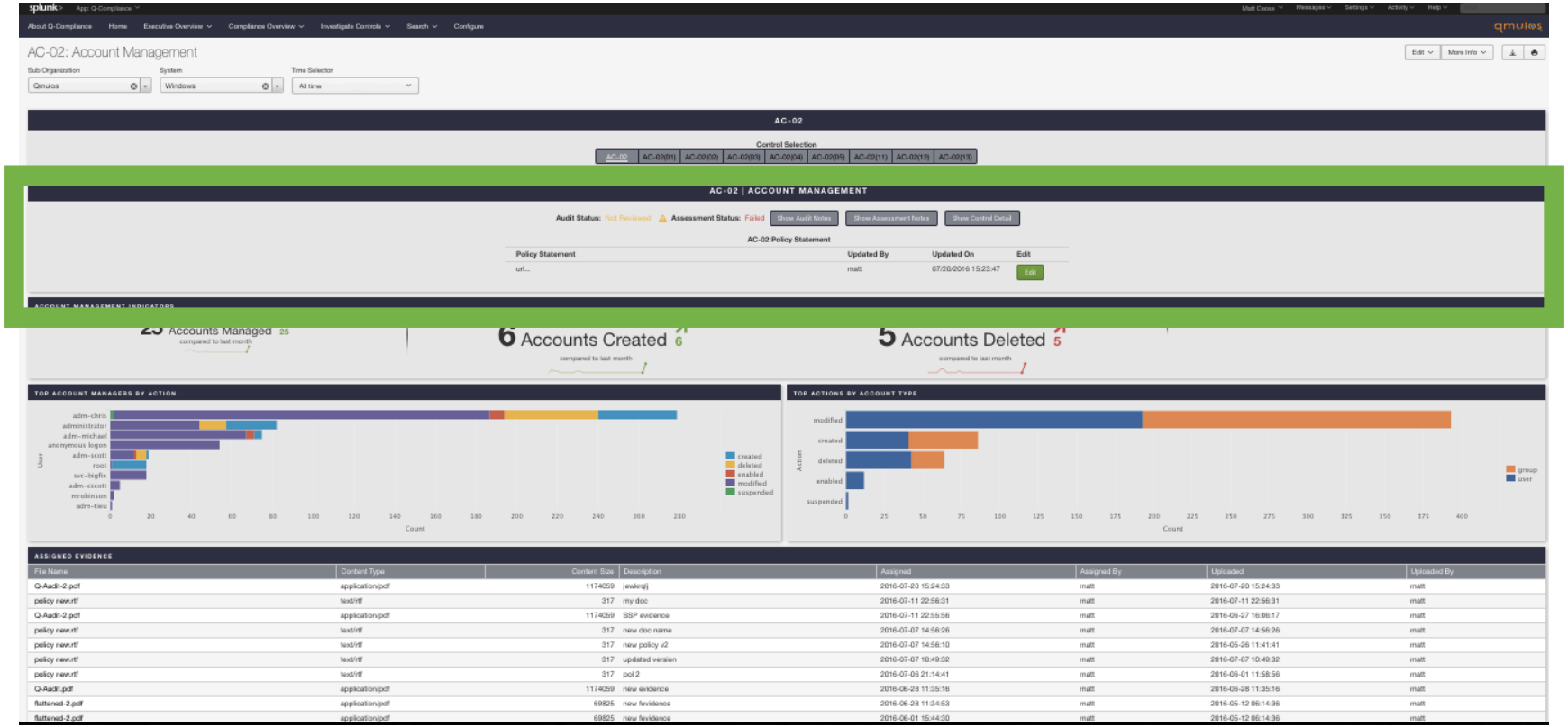


policy new.rtf	text/rtf	317	my doc	2016-07-11 22:56:31	matt	2016-07-11 22:56:31	matt
Q-Audit-2.pdf	application/pdf	1174059	SSP evidence	2016-07-11 22:55:56	matt	2016-06-27 16:06:17	matt
policy new.rtf	text/rtf	317	new doc name	2016-07-07 14:56:26	matt	2016-07-07 14:56:26	matt
policy new.rtf	text/rtf	317	new policy v2	2016-07-07 14:56:10	matt	2016-05-26 11:41:41	matt
policy new.rtf	text/rtf	317	updated version	2016-07-07 10:49:32	matt	2016-07-07 10:49:32	matt
policy new.rtf	text/rtf	317	pol 2	2016-07-06 21:14:41	matt	2016-06-01 11:58:56	matt
Q-Audit.pdf	application/pdf	1174059	new evidence	2016-06-28 11:35:16	matt	2016-06-28 11:35:16	matt
flattened-2.pdf	application/pdf	69825	new fevidence	2016-06-28 11:34:53	matt	2016-05-12 06:14:36	matt
flattened-2.pdf	application/pdf	69825	new fevidence	2016-06-01 15:44:30	matt	2016-05-12 06:14:36	matt

Technical Control Evidence In Machine Data

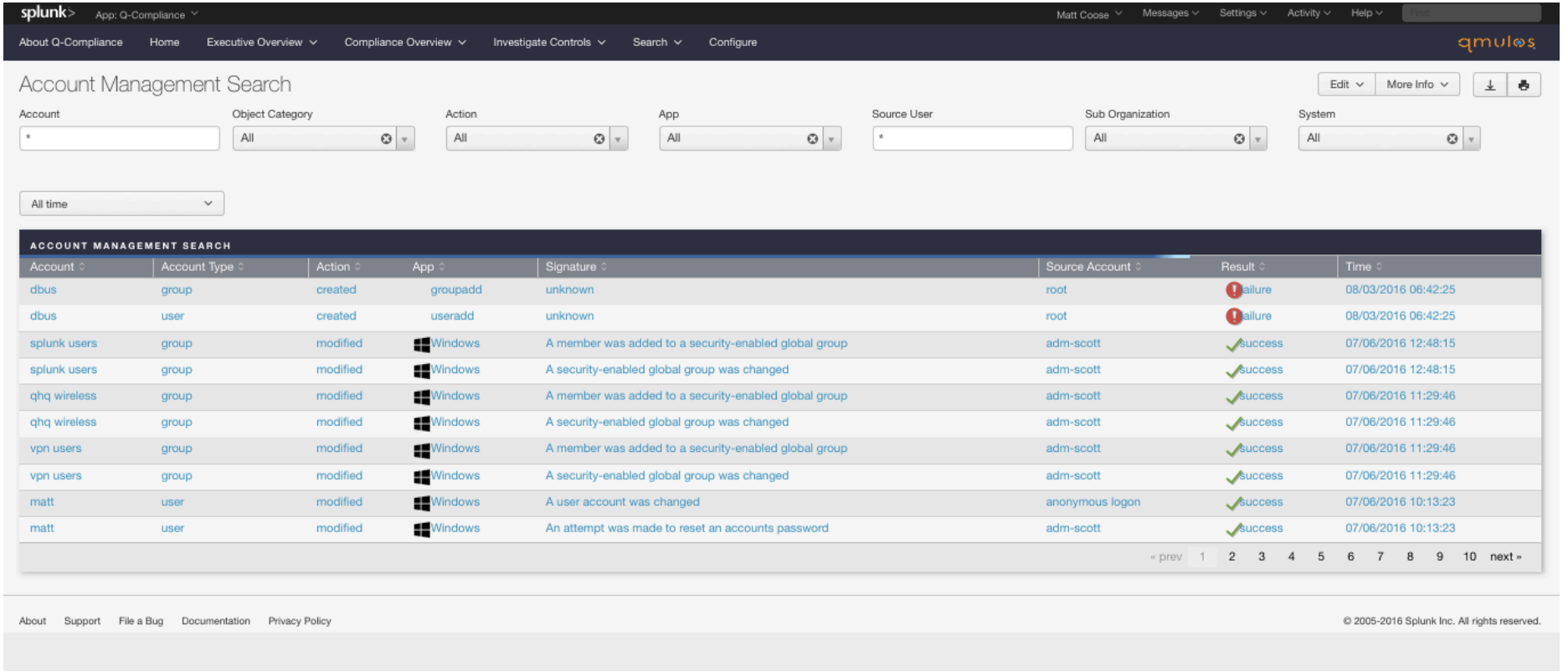
Evidence	Control Family	Data Source(s)
Monitoring use of information system accounts (creates, enables, modification, disables, and removes)	Access Control	AD, LDAP, Enterprise Authentication Sources
Monitoring information system audit events (type, timestamp, where, who, what, outcome, and the identity of any individuals or subjects)	Audit & Accountability	Operating Systems, Printer logs, AD
Monitoring changes to the configuration settings from baselines	Configuration Management	Configuration, Patch, and Authenticated Scanners
Proof that information system implements multifactor authentication for network access to privileged accounts	Identification & Authentication	IAM Systems
Proof that the organization employs automated mechanisms for tracking security incidents and the collection and analysis of incident information	Incident Response	Incident tracking system, SIEMs
Proof that the organization [prohibits] the use of [USB drives] on [all systems]	Media Protection	DLP Solutions
Monitoring for extreme temperatures and humidity	Physical & Environmental Protection	IOT: Environmental Data Center Sensors

Human Activity Evidence



splunk> .conf2016

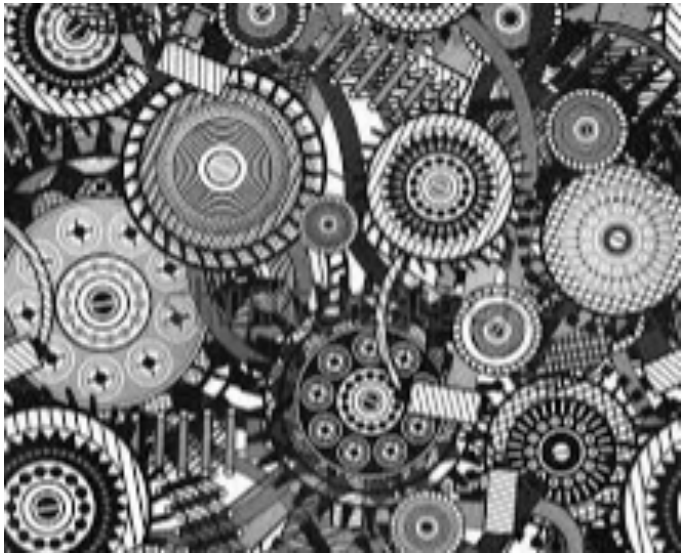
Dynamic Evidence (Search)



Technical Elements Of A Solution

Technical Elements

- Data Sources
- TAs/Tags/Event Types
- Data Models/Pivots/KV Stores



Lessons Learned And Benefits

Lessons Learned

- Define your approach based on real pain points
- Set simple compliance automation goals to start
- Be smart about which control catalog(s) you select – build once, report many
- Don’t assume you know compliance
- Align to data models but extend
- Leverage TAs but adapt

Benefits

$3.5 million is the average cost to achieve ”compliance” for a large enterprise; however, the average cost for organizations that experience non-compliance-related problems is far higher -- **$9.4 million**.[1]

SEC Charges Investment Adviser With Failing to Adopt Proper Cybersecurity Policies Prior To Breach
September 22, 2015

SEC Steps Up Cybersecurity Enforcement
Tuesday, October 6, 2015

SEC Enforcement Lays out Approach to Cybersecurity Cases
Monday, February 22, 2016

SEC Preparing Cases against firms for lack of cybersecurity preparedness
April 8, 2016

Expensive to do manually and more expensive not to do it!

1. “The True Cost of Compliance”, a 2011 Ponemon Institute research study

Other Benefits

- Reducing manual effort
- Reducing paperwork
- Increasing frequency of monitoring (ConMon)
- Technical insight
- Increasing flexibility
- Asking different questions of the same data sources multiplies ROI
- Enabling security!!

Use Case – Cloud Provider

Case Study – Cloud Provider

A provider of managed hosting services and data centers for information technology services and cloud computing with data centers in United States, the United Kingdom, and China.

Compliance requirements span commercial and federal markets, with regulatory frameworks such as FedRamp, HIPAA, SOX, PCI

Initial focus: **FedRamp Compliance**

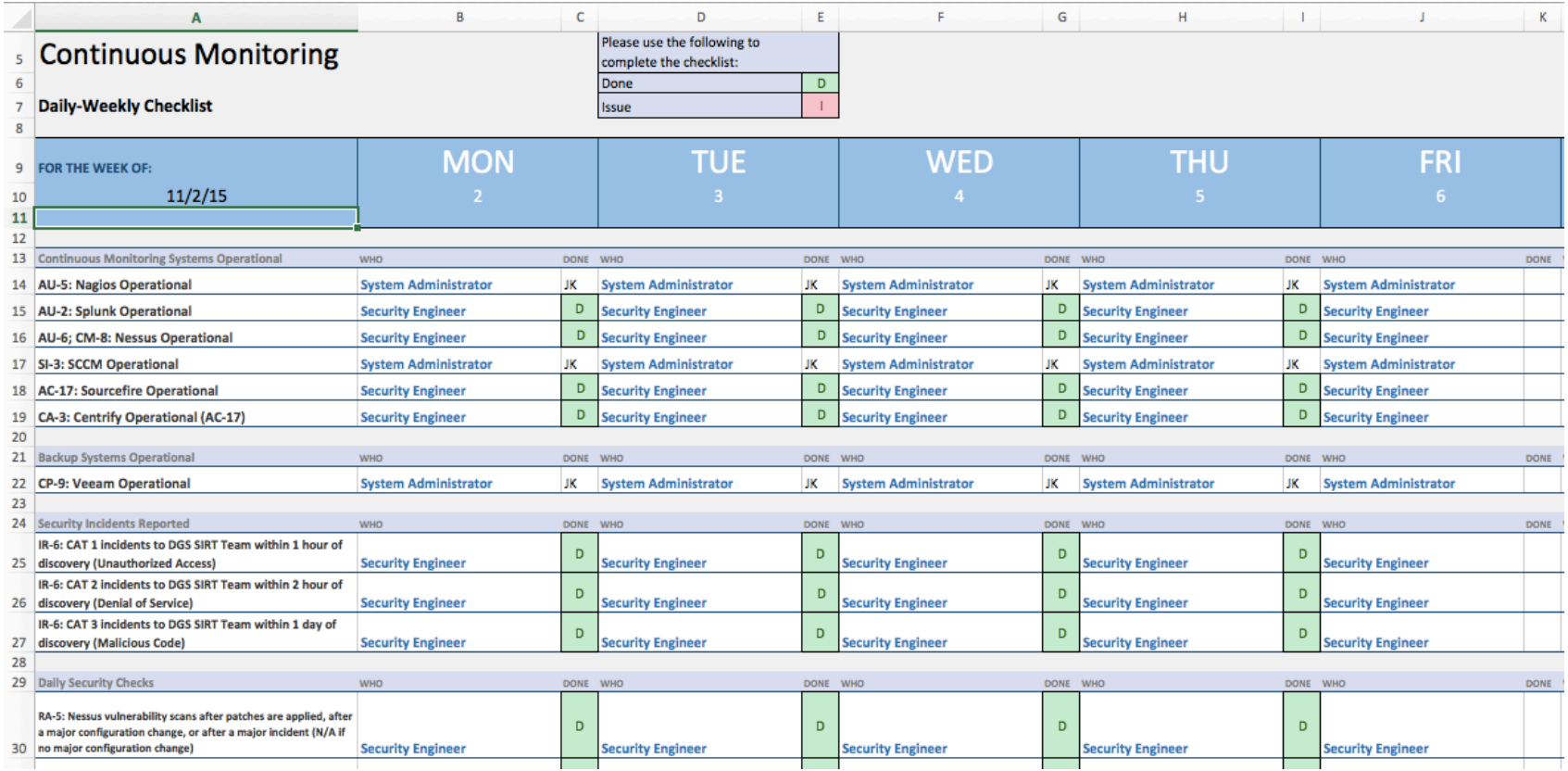
Timeline & Before State

- 2015 - last year for FedRamp audits based on NIST SP 800-53r3
- 5 PM EST Monday, December 15th, 2015 – Inbound call to Qmulos:
  "can you help us with FedRamp compliance?"

  – Answer: "Sure. Tell me about your infrastructure."

  – Response: "We use Splunk, ingest logs from what we think are all the relevant sources, but it takes about 2 months with the auditors reviewing consoles from each system and reviewing our manual checklists we use to demonstrate our monitoring audit trail. **Want to see our spreadsheet?"**

Spreadsheet Checklist For ConMon: Efficient?



Continuous Monitoring

Daily-Weekly Checklist

Please use the following to complete the checklist:	
Done	D
Issue	I

FOR THE WEEK OF:	MON	TUE	WED	THU	FRI
11/2/15	2	3	4	5	6

Continuous Monitoring Systems Operational	WHO	DONE	WHO	DONE	WHO	DONE	WHO	DONE	WHO	DONE
AU-5: Nagios Operational	System Administrator	JK	System Administrator	JK	System Administrator	JK	System Administrator	JK	System Administrator	
AU-2: Splunk Operational	Security Engineer	D	Security Engineer	D	Security Engineer	D	Security Engineer	D	Security Engineer	
AU-6; CM-8: Nessus Operational	Security Engineer	D	Security Engineer	D	Security Engineer	D	Security Engineer	D	Security Engineer	
SI-3: SCCM Operational	System Administrator	JK	System Administrator	JK	System Administrator	JK	System Administrator	JK	System Administrator	
AC-17: Sourcefire Operational	Security Engineer	D	Security Engineer	D	Security Engineer	D	Security Engineer	D	Security Engineer	
CA-3: Centrify Operational (AC-17)	Security Engineer	D	Security Engineer	D	Security Engineer	D	Security Engineer	D	Security Engineer	
Backup Systems Operational	**WHO**	**DONE**	**WHO**	**DONE**	**WHO**	**DONE**	**WHO**	**DONE**	**WHO**	**DONE**
CP-9: Veeam Operational	System Administrator	JK	System Administrator	JK	System Administrator	JK	System Administrator	JK	System Administrator	
Security Incidents Reported	**WHO**	**DONE**	**WHO**	**DONE**	**WHO**	**DONE**	**WHO**	**DONE**	**WHO**	**DONE**
IR-6: CAT 1 incidents to DGS SIRT Team within 1 hour of discovery (Unauthorized Access)	Security Engineer	D	Security Engineer	D	Security Engineer	D	Security Engineer	D	Security Engineer	
IR-6: CAT 2 incidents to DGS SIRT Team within 2 hour of discovery (Denial of Service)	Security Engineer	D	Security Engineer	D	Security Engineer	D	Security Engineer	D	Security Engineer	
IR-6: CAT 3 incidents to DGS SIRT Team within 1 day of discovery (Malicious Code)	Security Engineer	D	Security Engineer	D	Security Engineer	D	Security Engineer	D	Security Engineer	
Daily Security Checks	**WHO**	**DONE**	**WHO**	**DONE**	**WHO**	**DONE**	**WHO**	**DONE**	**WHO**	**DONE**
RA-5: Nessus vulnerability scans after patches are applied, after a major configuration change, or after a major incident (N/A if no major configuration change)	Security Engineer	D	Security Engineer	D	Security Engineer	D	Security Engineer	D	Security Engineer	

How Did We Get Started?

- Audited existing manual spreadsheet of controls, evidence required, ConMon requirements, and data sources against NIST SP 800-53r4
  - A few new controls/enhancements – ***same data sources***

- Prioritized technical controls that required staff to monitor on a daily, weekly, monthly basis and needed evidence that this was being performed
  - **mapped staff responsible & role to each control**

- Installed required apps (in this case, Q-Compliance & Q-Audit), configured apps to map data sources to systems and controls

Timelines

• Kickoff, prioritization, basic setup	1 week
• System & 10 data source mappings	4 days over week 2 & 3
• User training	2 days over week 2 & 3
• Control page customization	2 weeks over week 3 & 4

Results

- Passed the audit
  - Tip for the audience – start before the audit so that you can do an internal assessment and remediate in advance!

- Transitioned ConMon activities from multiple consoles for a range of users to a single console – and eliminated the spreadsheet

- Is there more to do? Yes – focus is continued automation and centralizing in one tool (Splunk) for additional controls (not just technical)

Use Case – Federal Agency

Case Study – Federal Agency

Small component of a large federal agency that manages a few systems critical to the whole agency

Proponent – agency Splunk Ninja – using free Splunkbase & internally created apps

Compliance requirements focused on FISMA based on NIST (800-53r4)

Limited staffing to support compliance & audit activities

Timeline & Before State

- Using Splunk to monitor IT Ops of Mission focused systems
- Decided to ***prototype control monitoring*** from some of the same data sources to provide a monitoring view for system
- Support audits as a very manual process, leveraging multiple system consoles, documents & workflows in Sharepoint, Splunk

How Did We Get Started?

- Defined **Project Goals**
  - streamline audit support process
  - provide added value to system owners
  - support current Agency processes
  - provide a showcase for broader Splunk use cases in the Agency

- Gained support of HQ

- Collaborated with SOC (evaluating Splunk ES for replacing legacy SIEM)

How Did We Get Started?

- Defined systems based on who could mitigate or accept the associated risks we would identify
  - Physical controls – data center team
  - Authentication – AD team
  - Configurations – Configuration management team
  - Agency Mission Systems – System Owner

- Installed required apps, configured apps to map data sources to systems and controls

- Identified key workflows (Sharepoint) for support

Results

- Implemented and did compliance configuration over a period of weeks based on current data sources for technical controls

- Dashboards now being viewed by system owners and others – for some, this is their first access to this level of real time compliance posture ala ConMon – new proponents for Splunk that had not be exposed to it before

- Performed and scored our first ***internal assessment -*** identified key weaknesses to be remediated

Questions?

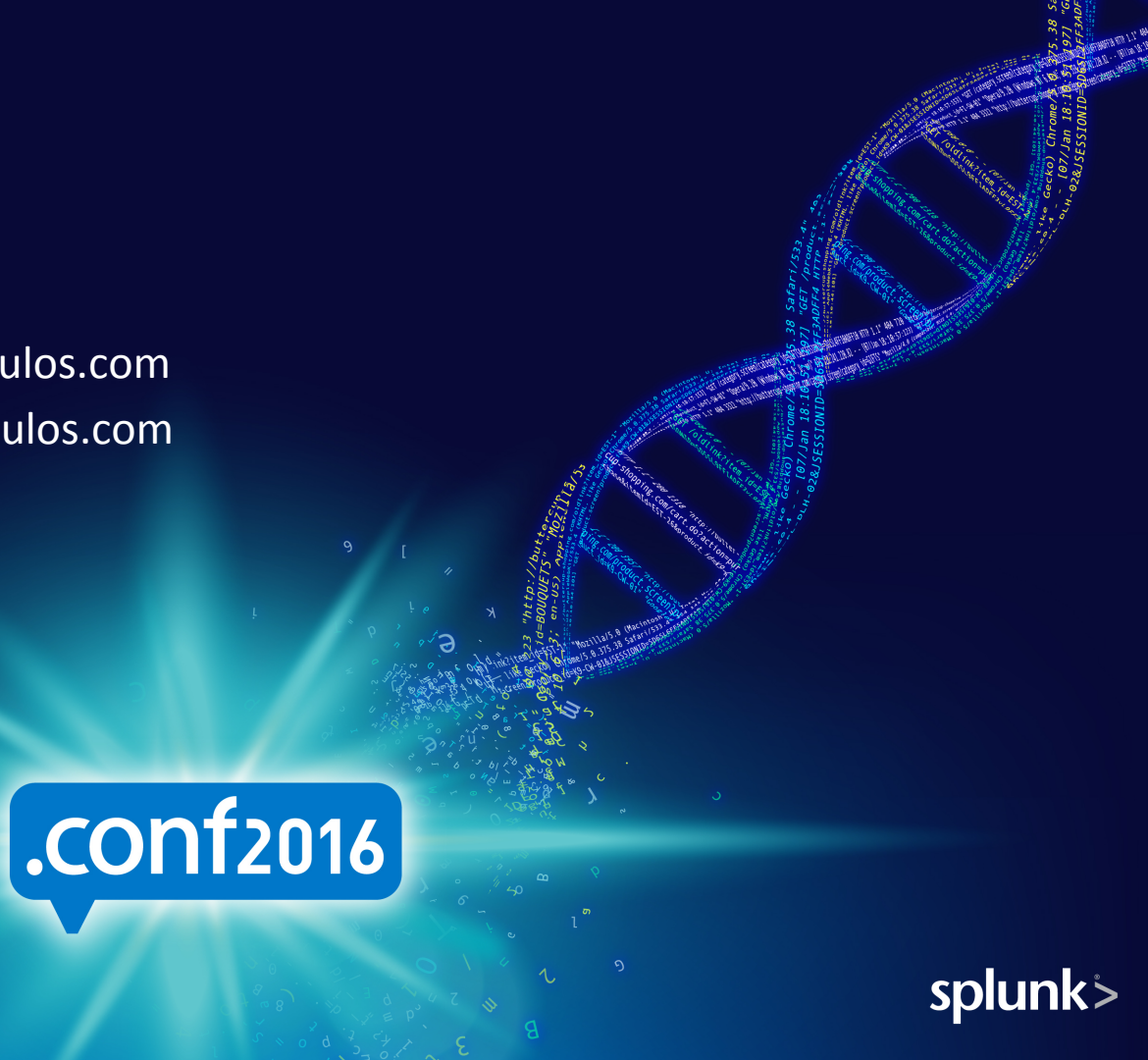
Demo Time!!

- Qmulos Premium Apps
  - Enterprise Compliance
  - Enterprise Audit
  - Find us on SplunkBase at:

    https://splunkbase.splunk.com/apps/#/page/1/search/qmulos/order/relevance

THANK YOU

Matt Coose matt@qmulos.com
Scott Armstrong scott@qmulos.com



.conf2016

splunk>

Demo Slides

splunk> App: Q-Compliance | Matt Coose | Messages | Settings | Activity | Help

About Q-Compliance | Home | Executive Overview | Compliance Overview | Investigate Controls | Search | Configure | qmulos

QMULOS ENTERPRISE COMPLIANCE (Q-COMPLIANCE)

Compliance to Enable Security

Automated compliance through continuous assessment

EXECUTIVE

About Q-Compliance
Organization Overview
Enterprise Opportunities
POAM Overview

COMPLIANCE OVERVIEW

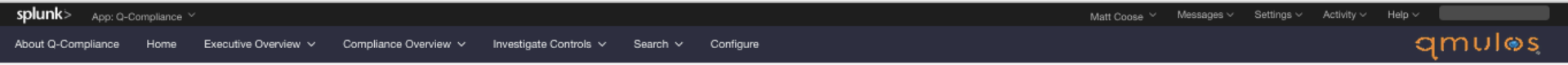
Family Overview
Control Overview

INVESTIGATE CONTROLS

Access Control
Awareness and Training
Audit and Accountability
Security Assessment and Authorization
Configuration Management
Contingency Planning
Identification and Authentication
Incident Response
Maintenance
Media Protection
Physical and Eviornmental Protection
Planning
Personnel Security
Risk Assessment
System and Services Acquisition
System and Communications Protection
System and Information Integrity

CONFIGURATION

Configuration Page



ABOUT QMULOS

Holistic Security Solutions

Qmulos is based in the Washington DC technology corridor. Our team has decades of proven compliance, cyber defense, and security research experience. We are focused on providing cost-effective automated compliance solutions, providing the foundation for securing the Enterprise. Qmulos is a proud Elite Splunk Partner.

ABOUT Q-COMPLIANCE

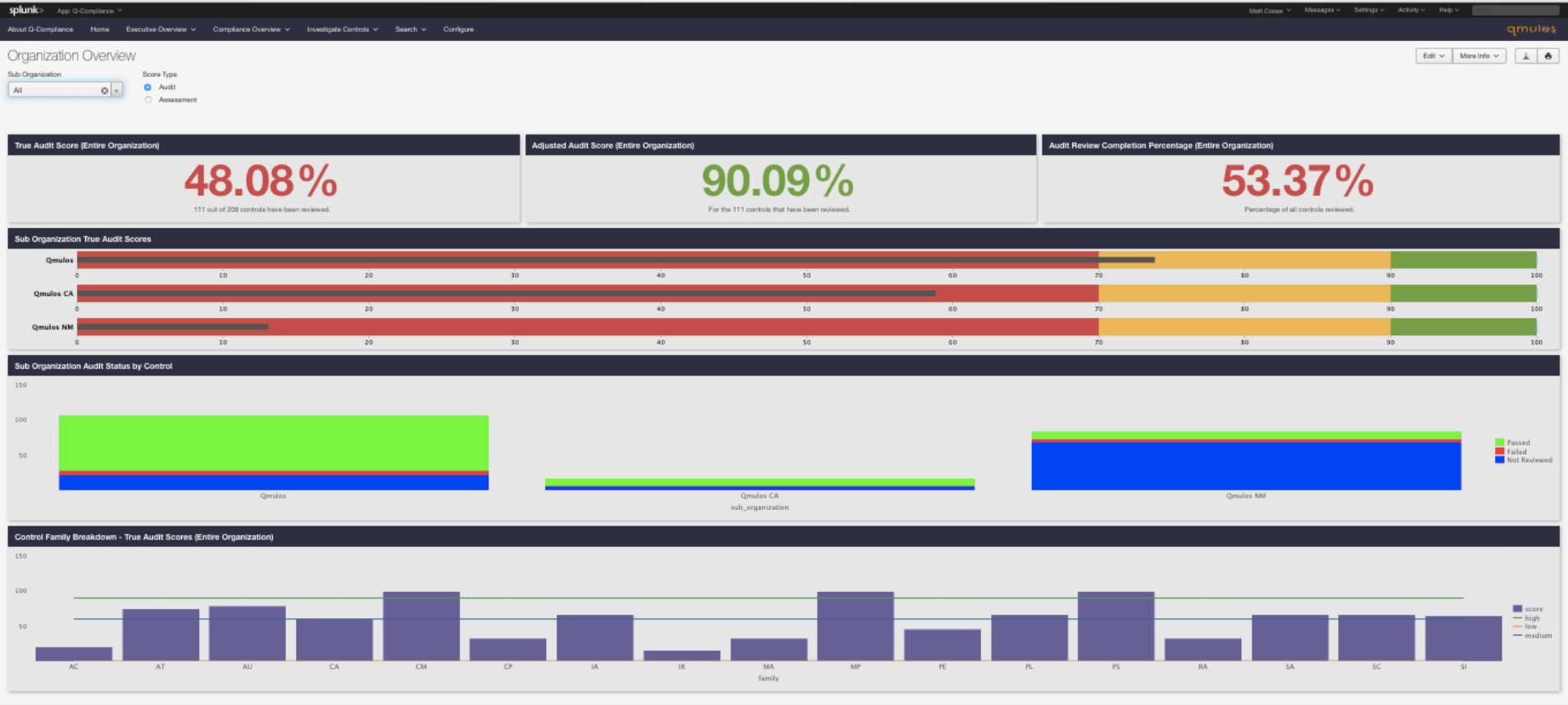
Compliance to Enable Security

Compliance is not the end game for security conscious organizations – but we think it's a great way to start securing your organization. Our Q-Compliance App provides a clear roadmap for making your organization compliant with cybersecurity standards and enables you to pass even the most rigorous audits.

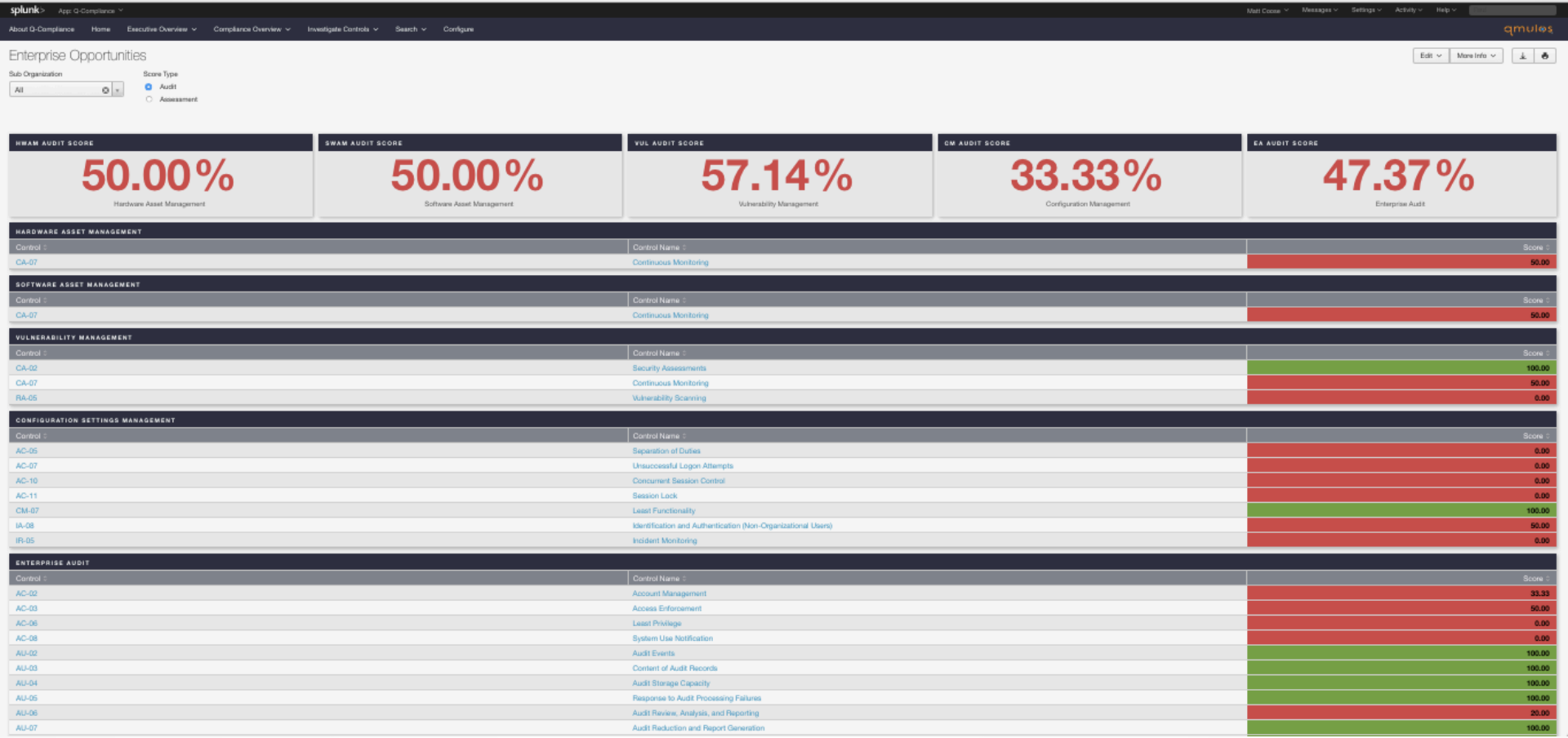
From the ground up, the App helps you identify how to properly instrument your networks and aggregate critical security data. Once you have visibility across these critical compliance domains, you can start working on getting those scores up, system by system, Division by Division, and even Enterprise-wide. This is the best way to truly understand and manage your cybersecurity risk.

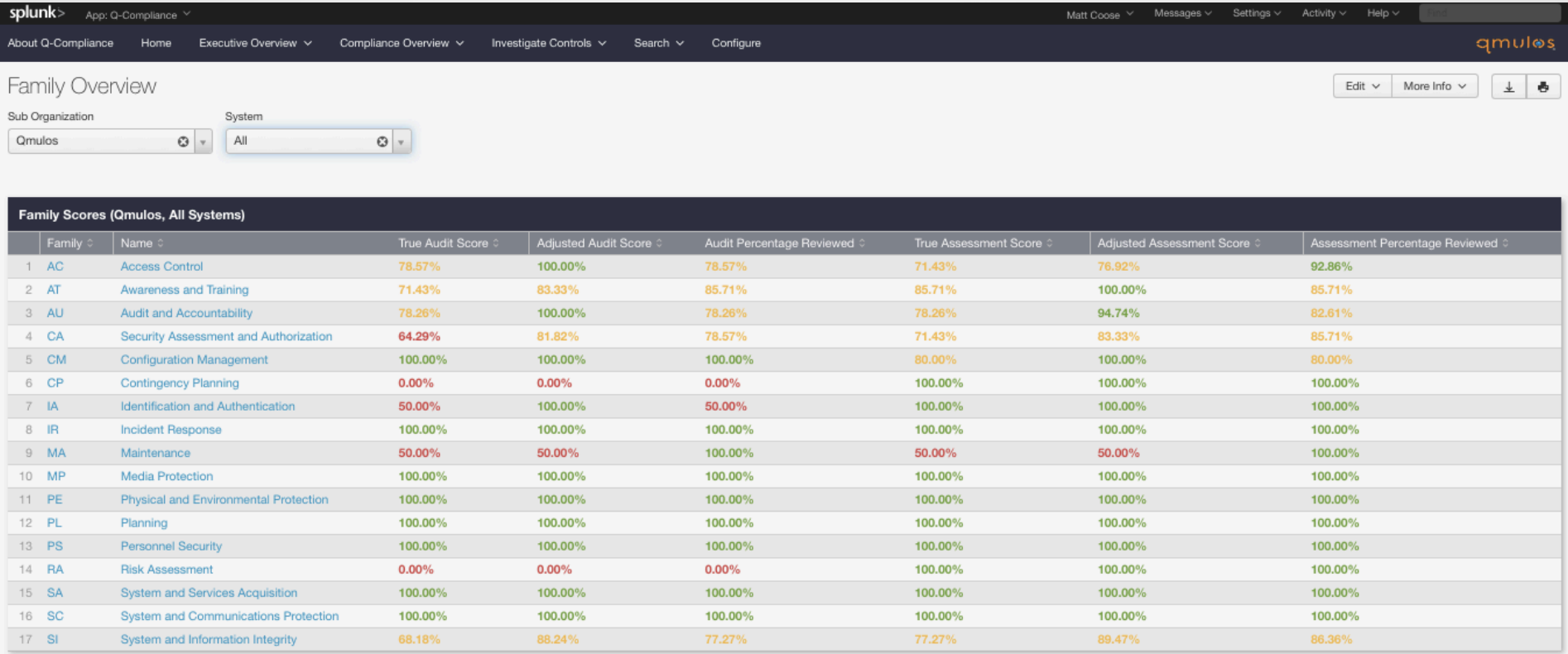
As the one-stop-shop for your security data, Q-Compliance also sets the stage for security beyond compliance – which IS the end game for security conscious organizations.

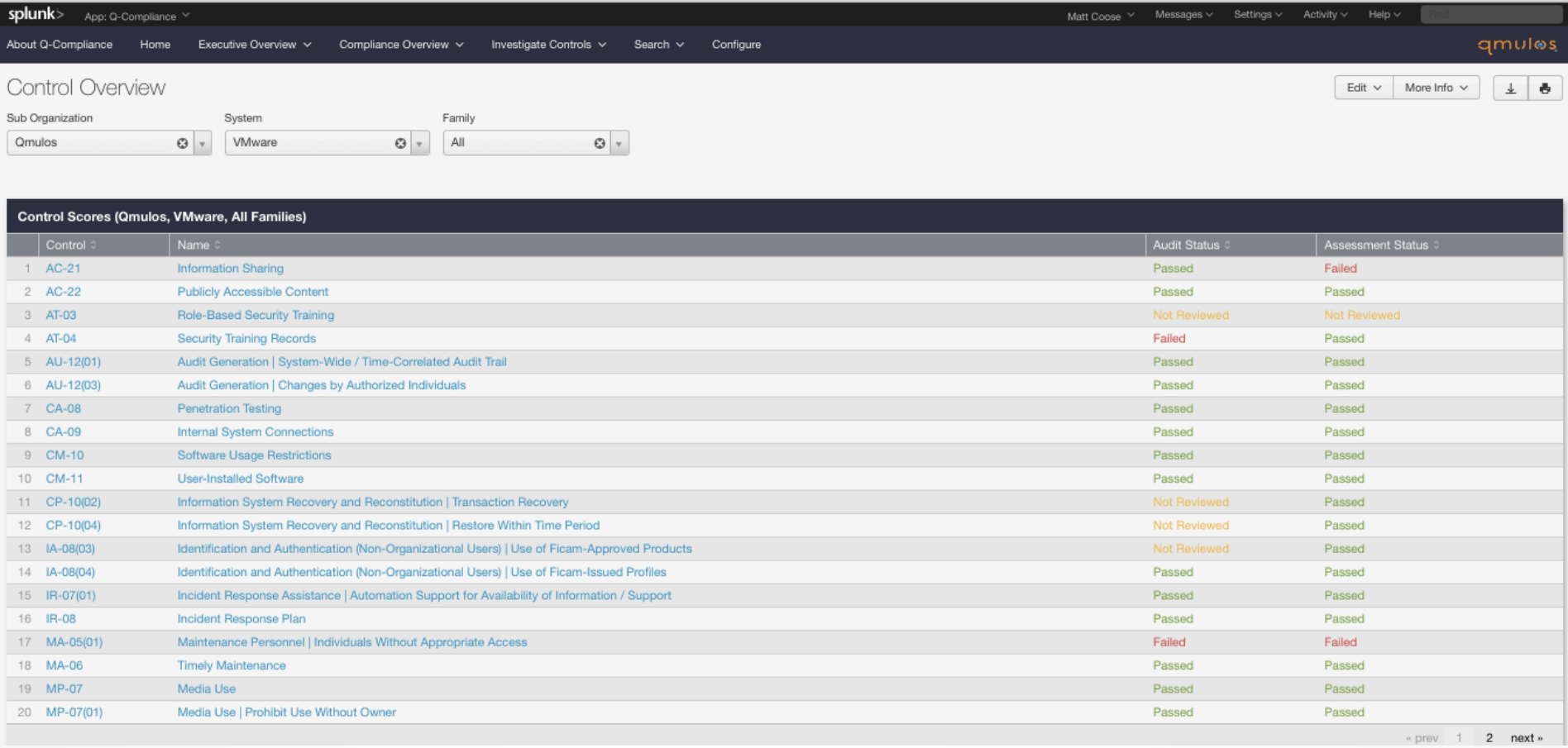
- ACCESS CONTROL
- AWARENESS AND TRAINING
- AUDIT AND ACCOUNTABILITY
- SECURITY ASSESSMENT AND AUTHORIZATION
- CONFIGURATION MANAGEMENT
- CONTINGENCY PLANNING
- IDENTIFICATION AND AUTHENTICATION
- INCIDENT RESPONSE
- MAINTENANCE
- MEDIA PROTECTION
- PHYSICAL ENVIRONMENTAL PROTECTION
- PLANNING
- PERSONNEL SECURITY
- RISK ASSESSMENT
- SYSTEM AND SERVICES ACQUISITION
- SYSTEM AND COMMUNICATIONS PROTECTION
- SYSTEM AND INFORMATION INTEGRITY

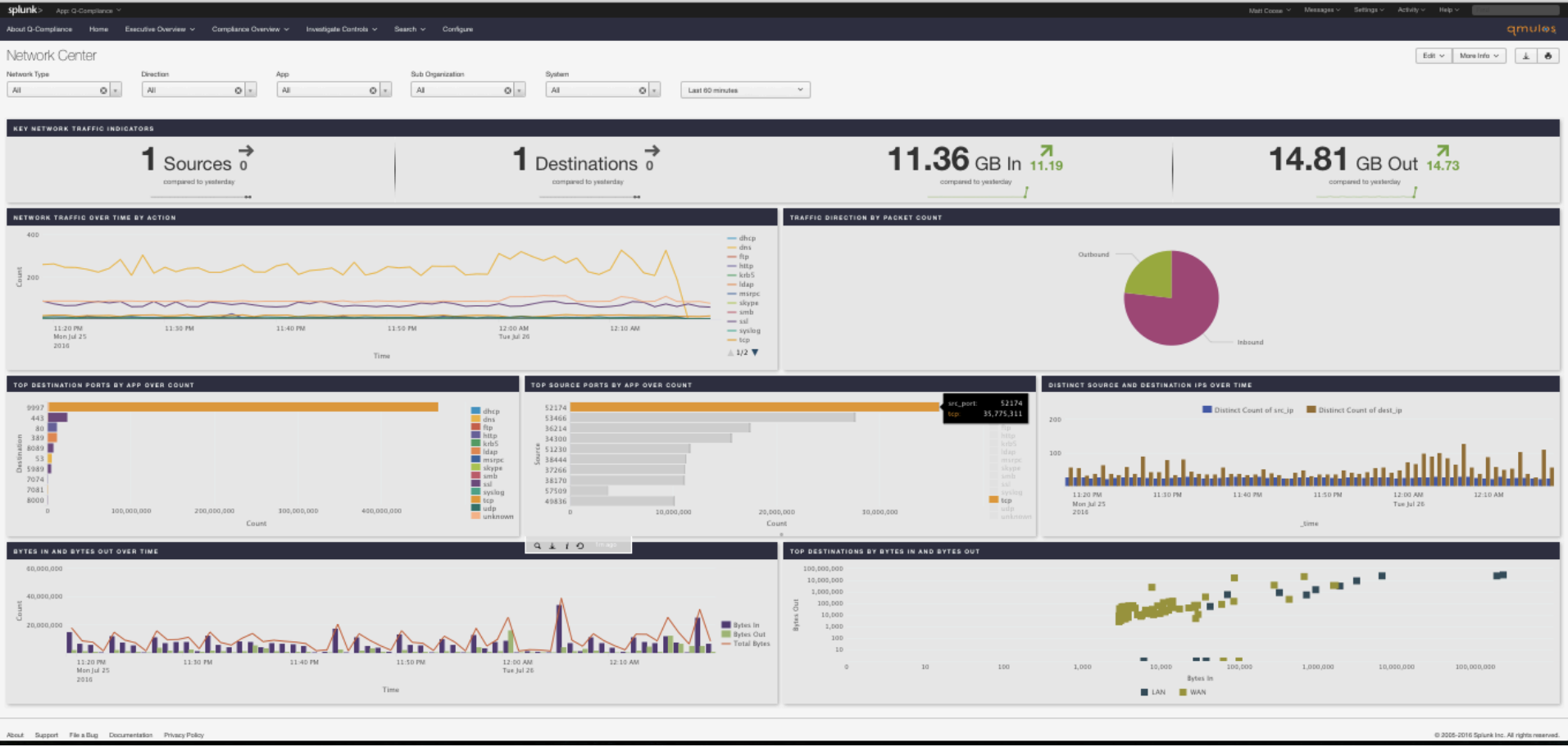

splunk>
App: Q-Compliance
About Q-Compliance
Home
Executive Overview
Compliance Overview
Investigate Controls
Search
Configure
qmulos
Organization Overview
Edit
More Info
Sub Organization
All
Score Type
Audit
Assessment
True Audit Score (Entire Organization)
48.08%
111 out of 208 controls have been reviewed.
Adjusted Audit Score (Entire Organization)
90.09%
For the 111 controls that have been reviewed.
Audit Review Completion Percentage (Entire Organization)
53.37%
Percentage of all controls reviewed.
Sub Organization True Audit Scores
Qmulos
Qmulos CA
Qmulos NM
0
10
20
30
40
50
60
70
80
90
100
Sub Organization Audit Status by Control
150
100
50
Qmulos
Qmulos CA
Qmulos NM
sub_organization
Passed
Failed
Not Reviewed
Control Family Breakdown - True Audit Scores (Entire Organization)
150
100
50
AC
AT
AU
CA
CM
CP
IA
IR
MA
MP
PE
PL
PS
RA
SA
SC
SI
family
score
high
low
medium
About
Support
File a Bug
Documentation
Privacy Policy
© 2005-2016 Splunk Inc. All rights reserved.

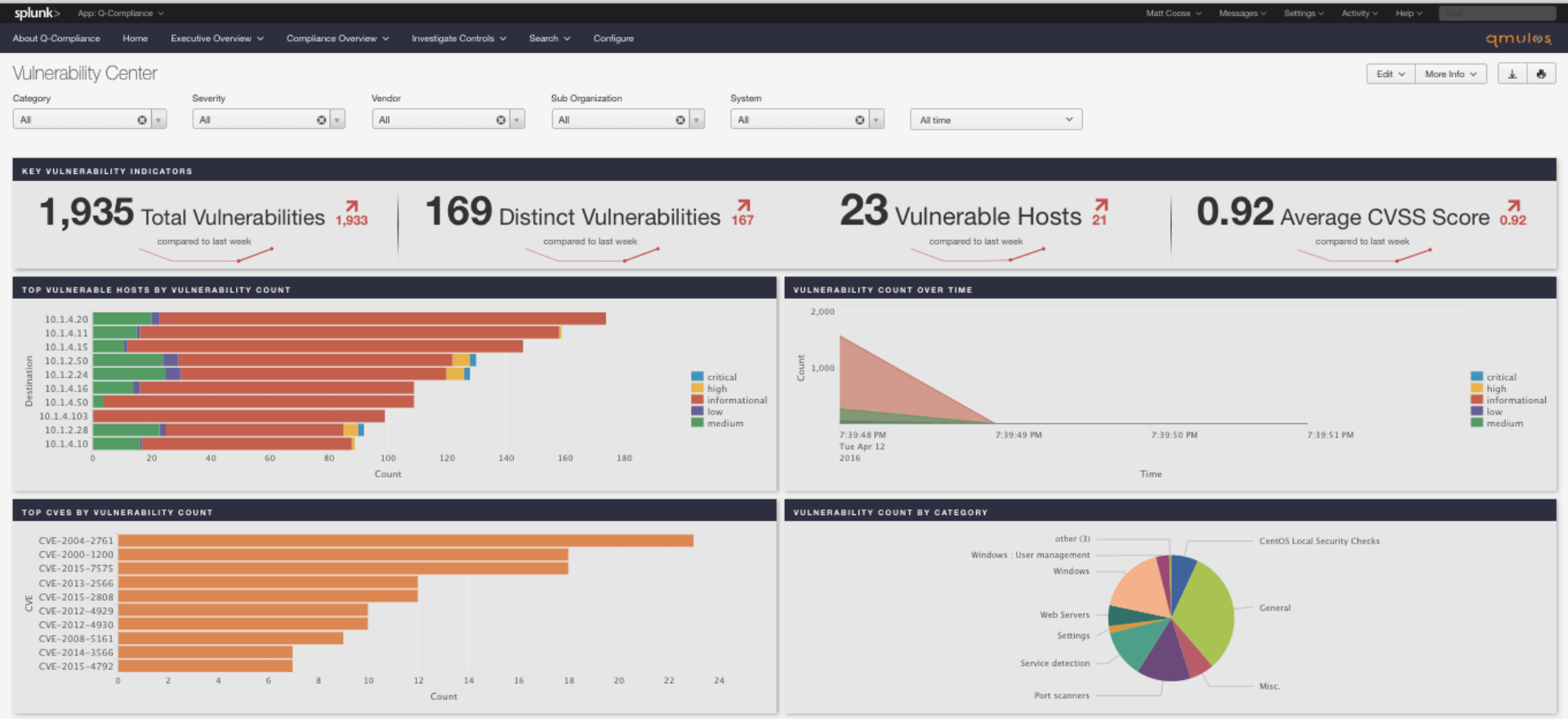
splunk>


splunk>
App: Q-Compliance
Matt Coose
Messages
Settings
Activity
Help
About Q-Compliance
Home
Executive Overview
Compliance Overview
Investigate Controls
Search
Configure
qmulos
Enterprise Opportunities
Edit
More Info
Sub Organization
All
Score Type
Audit
Assessment
HWAM AUDIT SCORE
50.00%
Hardware Asset Management
SWAM AUDIT SCORE
50.00%
Software Asset Management
VUL AUDIT SCORE
57.14%
Vulnerability Management
CM AUDIT SCORE
33.33%
Configuration Management
EA AUDIT SCORE
47.37%
Enterprise Audit
HARDWARE ASSET MANAGEMENT
Control
Control Name
Score
CA-07
Continuous Monitoring
50.00
SOFTWARE ASSET MANAGEMENT
Control
Control Name
Score
CA-07
Continuous Monitoring
50.00
VULNERABILITY MANAGEMENT
Control
Control Name
Score
CA-02
Security Assessments
100.00
CA-07
Continuous Monitoring
50.00
RA-05
Vulnerability Scanning
0.00
CONFIGURATION SETTINGS MANAGEMENT
Control
Control Name
Score
AC-05
Separation of Duties
0.00
AC-07
Unsuccessful Logon Attempts
0.00
AC-10
Concurrent Session Control
0.00
AC-11
Session Lock
0.00
CM-07
Least Functionality
100.00
IA-08
Identification and Authentication (Non-Organizational Users)
50.00
IR-05
Incident Monitoring
0.00
ENTERPRISE AUDIT
Control
Control Name
Score
AC-02
Account Management
33.33
AC-03
Access Enforcement
50.00
AC-06
Least Privilege
0.00
AC-08
System Use Notification
0.00
AU-02
Audit Events
100.00
AU-03
Content of Audit Records
100.00
AU-04
Audit Storage Capacity
100.00
AU-05
Response to Audit Processing Failures
100.00
AU-06
Audit Review, Analysis, and Reporting
20.00
AU-07
Audit Reduction and Report Generation
100.00

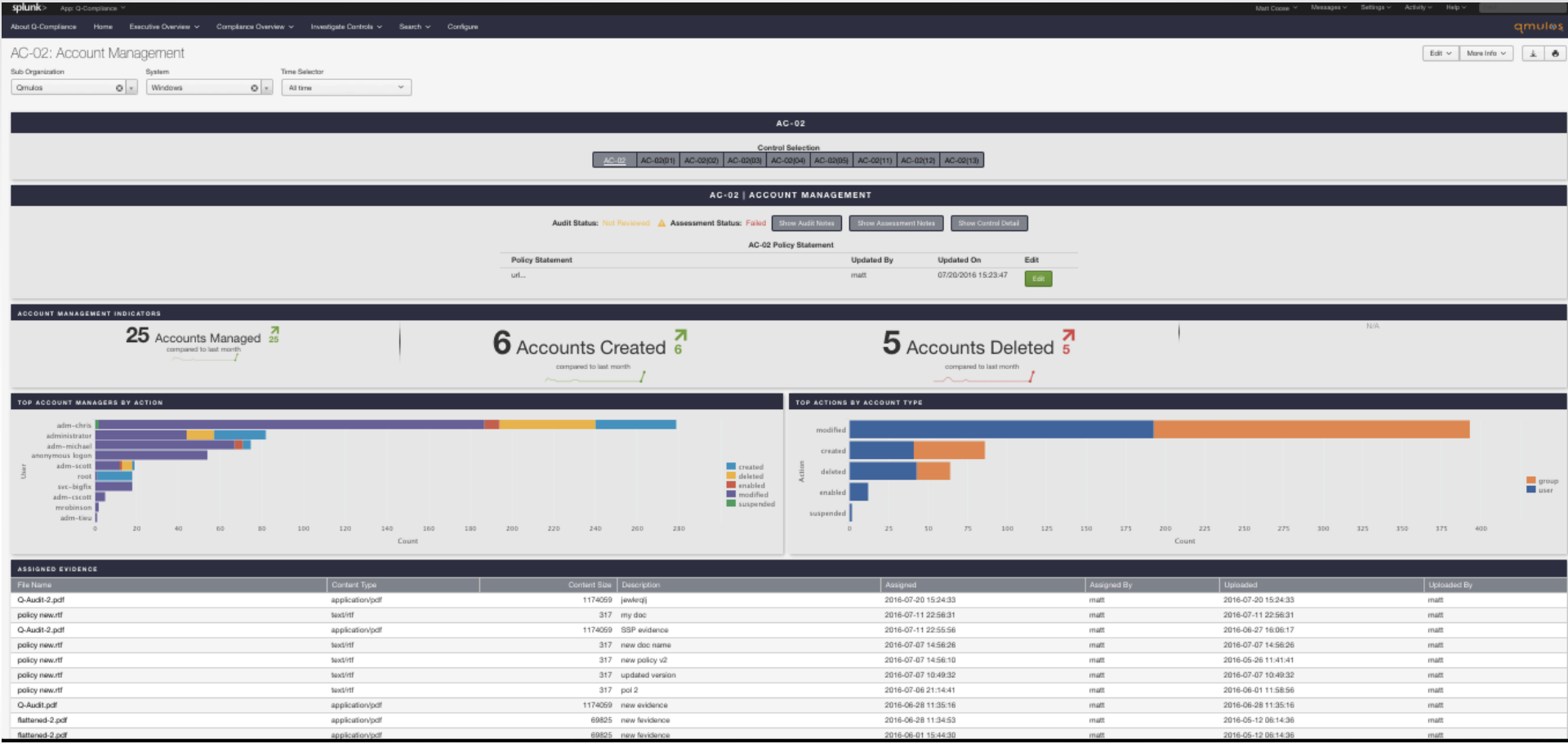

splunk> App: Q-Compliance
Matt Coose Messages Settings Activity Help
About Q-Compliance Home Executive Overview Compliance Overview Investigate Controls Search Configure
qmulos
Family Overview
Edit More Info
Sub Organization
Qmulos
System
All
Family Scores (Qmulos, All Systems)
Family Name True Audit Score Adjusted Audit Score Audit Percentage Reviewed True Assessment Score Adjusted Assessment Score Assessment Percentage Reviewed
1 AC Access Control 78.57% 100.00% 78.57% 71.43% 76.92% 92.86%
2 AT Awareness and Training 71.43% 83.33% 85.71% 85.71% 100.00% 85.71%
3 AU Audit and Accountability 78.26% 100.00% 78.26% 78.26% 94.74% 82.61%
4 CA Security Assessment and Authorization 64.29% 81.82% 78.57% 71.43% 83.33% 85.71%
5 CM Configuration Management 100.00% 100.00% 100.00% 80.00% 100.00% 80.00%
6 CP Contingency Planning 0.00% 0.00% 0.00% 100.00% 100.00% 100.00%
7 IA Identification and Authentication 50.00% 100.00% 50.00% 100.00% 100.00% 100.00%
8 IR Incident Response 100.00% 100.00% 100.00% 100.00% 100.00% 100.00%
9 MA Maintenance 50.00% 50.00% 100.00% 50.00% 50.00% 100.00%
10 MP Media Protection 100.00% 100.00% 100.00% 100.00% 100.00% 100.00%
11 PE Physical and Environmental Protection 100.00% 100.00% 100.00% 100.00% 100.00% 100.00%
12 PL Planning 100.00% 100.00% 100.00% 100.00% 100.00% 100.00%
13 PS Personnel Security 100.00% 100.00% 100.00% 100.00% 100.00% 100.00%
14 RA Risk Assessment 0.00% 0.00% 0.00% 100.00% 100.00% 100.00%
15 SA System and Services Acquisition 100.00% 100.00% 100.00% 100.00% 100.00% 100.00%
16 SC System and Communications Protection 100.00% 100.00% 100.00% 100.00% 100.00% 100.00%
17 SI System and Information Integrity 68.18% 88.24% 77.27% 77.27% 89.47% 86.36%
About Support File a Bug Documentation Privacy Policy
© 2005-2016 Splunk Inc. All rights reserved.


splunk> App: Q-Compliance
Matt Coose Messages Settings Activity Help
About Q-Compliance Home Executive Overview Compliance Overview Investigate Controls Search Configure
qmulos
Control Overview
Edit More Info
Sub Organization
Qmulos
System
VMware
Family
All
Control Scores (Qmulos, VMware, All Families)
Control Name Audit Status Assessment Status
1 AC-21 Information Sharing Passed Failed
2 AC-22 Publicly Accessible Content Passed Passed
3 AT-03 Role-Based Security Training Not Reviewed Not Reviewed
4 AT-04 Security Training Records Failed Passed
5 AU-12(01) Audit Generation | System-Wide / Time-Correlated Audit Trail Passed Passed
6 AU-12(03) Audit Generation | Changes by Authorized Individuals Passed Passed
7 CA-08 Penetration Testing Passed Passed
8 CA-09 Internal System Connections Passed Passed
9 CM-10 Software Usage Restrictions Passed Passed
10 CM-11 User-Installed Software Passed Passed
11 CP-10(02) Information System Recovery and Reconstitution | Transaction Recovery Not Reviewed Passed
12 CP-10(04) Information System Recovery and Reconstitution | Restore Within Time Period Not Reviewed Passed
13 IA-08(03) Identification and Authentication (Non-Organizational Users) | Use of Ficam-Approved Products Not Reviewed Passed
14 IA-08(04) Identification and Authentication (Non-Organizational Users) | Use of Ficam-Issued Profiles Passed Passed
15 IR-07(01) Incident Response Assistance | Automation Support for Availability of Information / Support Passed Passed
16 IR-08 Incident Response Plan Passed Passed
17 MA-05(01) Maintenance Personnel | Individuals Without Appropriate Access Failed Failed
18 MA-06 Timely Maintenance Passed Passed
19 MP-07 Media Use Passed Passed
20 MP-07(01) Media Use | Prohibit Use Without Owner Passed Passed
« prev 1 2 next »

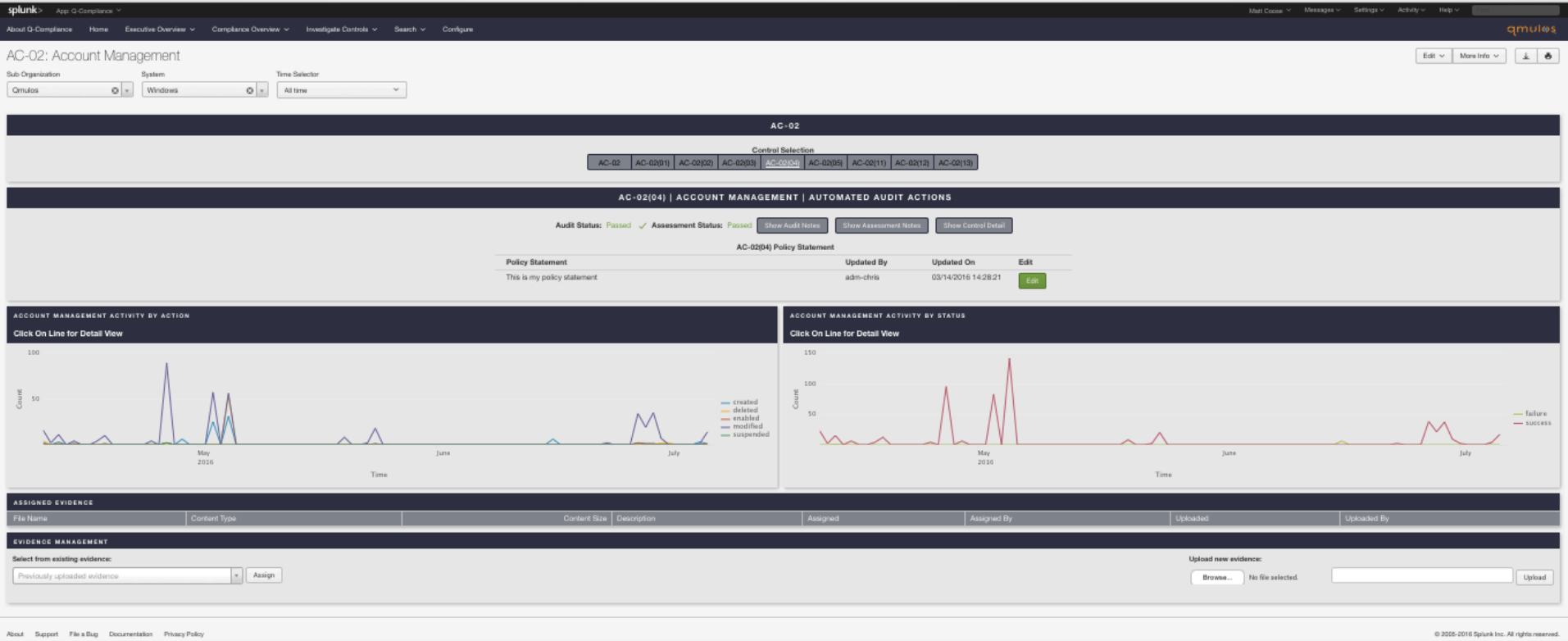

splunk>
App: Q-Compliance
About Q-Compliance
Home
Executive Overview
Compliance Overview
Investigate Controls
Search
Configure
qmulos
Network Center
Network Type
Direction
App
Sub Organization
System
Last 60 minutes
KEY NETWORK TRAFFIC INDICATORS
1 Sources 0
compared to yesterday
1 Destinations 0
compared to yesterday
11.36 GB In 11.19
compared to yesterday
14.81 GB Out 14.73
compared to yesterday
NETWORK TRAFFIC OVER TIME BY ACTION
Count
Time
dhcp
dns
ftp
http
krb5
ldap
msrpc
skype
smb
ssl
syslog
tcp
TRAFFIC DIRECTION BY PACKET COUNT
Outbound
Inbound
TOP DESTINATION PORTS BY APP OVER COUNT
Destination
Count
TOP SOURCE PORTS BY APP OVER COUNT
Source
src_port: 52174
tcp: 35,775,311
DISTINCT SOURCE AND DESTINATION IPS OVER TIME
Distinct Count of src_ip
Distinct Count of dest_ip
_time
BYTES IN AND BYTES OUT OVER TIME
Bytes In
Bytes Out
Total Bytes
TOP DESTINATIONS BY BYTES IN AND BYTES OUT
Bytes Out
Bytes In
LAN
WAN
About
Support
File a Bug
Documentation
Privacy Policy

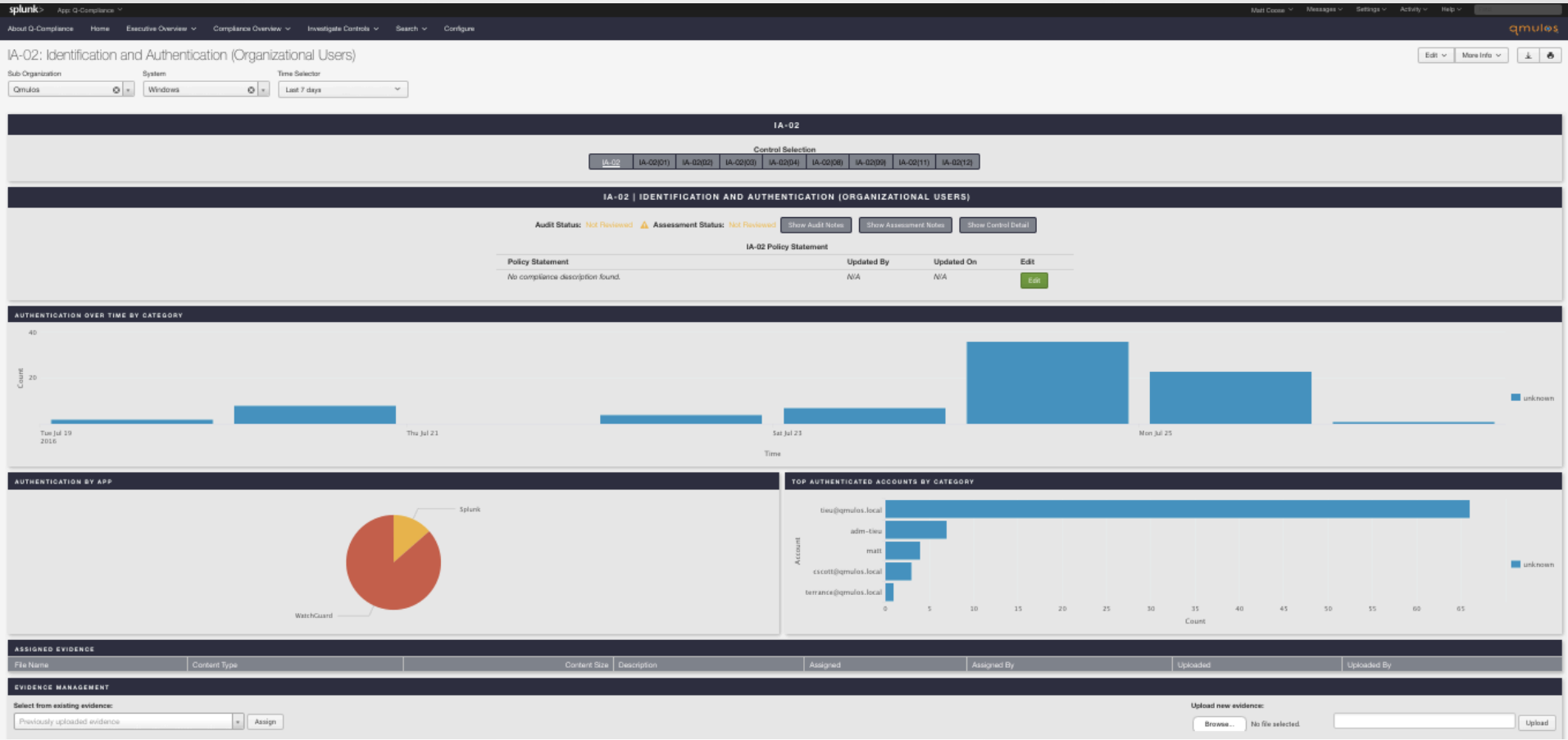

splunk> App: Q-Compliance
Matt Coose Messages Settings Activity Help
About Q-Compliance Home Executive Overview Compliance Overview Investigate Controls Search Configure
qmulos
Vulnerability Center
Edit More Info
Category All
Severity All
Vendor All
Sub Organization All
System All
All time
KEY VULNERABILITY INDICATORS
1,935 Total Vulnerabilities 1,933
compared to last week
169 Distinct Vulnerabilities 167
compared to last week
23 Vulnerable Hosts 21
compared to last week
0.92 Average CVSS Score 0.92
compared to last week
TOP VULNERABLE HOSTS BY VULNERABILITY COUNT
Destination
10.1.4.20
10.1.4.11
10.1.4.15
10.1.2.50
10.1.2.24
10.1.4.16
10.1.4.50
10.1.4.103
10.1.2.28
10.1.4.10
0 20 40 60 80 100 120 140 160 180
Count
critical
high
informational
low
medium
VULNERABILITY COUNT OVER TIME
Count
2,000
1,000
7:39:48 PM Tue Apr 12 2016
7:39:49 PM
7:39:50 PM
7:39:51 PM
Time
critical
high
informational
low
medium
TOP CVES BY VULNERABILITY COUNT
CVE
CVE-2004-2761
CVE-2000-1200
CVE-2015-7575
CVE-2013-2566
CVE-2015-2808
CVE-2012-4929
CVE-2012-4930
CVE-2008-5161
CVE-2014-3566
CVE-2015-4792
0 2 4 6 8 10 12 14 16 18 20 22 24
Count
VULNERABILITY COUNT BY CATEGORY
other (3)
Windows : User management
Windows
Web Servers
Settings
Service detection
Port scanners
CentOS Local Security Checks
General
Misc.

splunk>


splunk> App: Q-Compliance
Matt Cosse Messages Settings Activity Help
About Q-Compliance Home Executive Overview Compliance Overview Investigate Controls Search Configure
qmulos
AC-02: Account Management
Edit More Info
Sub-Organization
Qmulos
System
Windows
Time Selector
All time
AC-02
Control Selection
AC-02 AC-02(01) AC-02(02) AC-02(03) AC-02(04) AC-02(05) AC-02(11) AC-02(12) AC-02(13)
AC-02 | ACCOUNT MANAGEMENT
Audit Status: Not Reviewed Assessment Status: Failed
Show Audit Notes
Show Assessment Notes
Show Control Detail
AC-02 Policy Statement
Policy Statement
Updated By
Updated On
Edit
url...
matt
07/20/2016 15:23:47
Edit
ACCOUNT MANAGEMENT INDICATORS
25 Accounts Managed
25
compared to last month
6 Accounts Created
6
compared to last month
5 Accounts Deleted
5
compared to last month
N/A
TOP ACCOUNT MANAGERS BY ACTION
adm-chris
administrator
adm-michael
anonymous logon
adm-scott
root
svc-bigfix
adm-cscott
mrobinson
adm-tieu
User
0 20 40 60 80 100 120 140 160 180 200 220 240 260 280
Count
created
deleted
enabled
modified
suspended
TOP ACTIONS BY ACCOUNT TYPE
modified
created
deleted
enabled
suspended
Action
0 25 50 75 100 125 150 175 200 225 250 275 300 325 350 375 400
Count
group
user
ASSIGNED EVIDENCE
File Name
Content Type
Content Size
Description
Assigned
Assigned By
Uploaded
Uploaded By
Q-Audit-2.pdf application/pdf 1174059 jewlerqij 2016-07-20 15:24:33 matt 2016-07-20 15:24:33 matt
policy new.rtf text/rtf 317 my doc 2016-07-11 22:56:31 matt 2016-07-11 22:56:31 matt
Q-Audit-2.pdf application/pdf 1174059 SSP evidence 2016-07-11 22:55:56 matt 2016-06-27 16:06:17 matt
policy new.rtf text/rtf 317 new doc name 2016-07-07 14:56:26 matt 2016-07-07 14:56:26 matt
policy new.rtf text/rtf 317 new policy v2 2016-07-07 14:56:10 matt 2016-05-26 11:41:41 matt
policy new.rtf text/rtf 317 updated version 2016-07-07 10:49:32 matt 2016-07-07 10:49:32 matt
policy new.rtf text/rtf 317 pol 2 2016-07-06 21:14:41 matt 2016-06-01 11:58:56 matt
Q-Audit.pdf application/pdf 1174059 new evidence 2016-06-28 11:35:16 matt 2016-06-28 11:35:16 matt
flattened-2.pdf application/pdf 69825 new fevidence 2016-06-28 11:34:53 matt 2016-05-12 06:14:36 matt
flattened-2.pdf application/pdf 69825 new fevidence 2016-06-01 15:44:30 matt 2016-05-12 06:14:36 matt

splunk>


splunk>
App: Q-Compliance
About Q-Compliance
Home
Executive Overview
Compliance Overview
Investigate Controls
Search
Configure
qmulos
AC-02: Account Management
Edit
More Info
Sub Organization
Qmulos
System
Windows
Time Selector
All time
AC-02
Control Selection
AC-02
AC-02(01)
AC-02(02)
AC-02(03)
AC-02(04)
AC-02(05)
AC-02(11)
AC-02(12)
AC-02(13)
AC-02(04) | ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS
Audit Status: Passed
Assessment Status: Passed
Show Audit Notes
Show Assessment Notes
Show Control Detail
AC-02(04) Policy Statement
Policy Statement
Updated By
Updated On
Edit
This is my policy statement
adm-chris
03/14/2016 14:28:21
Edit
ACCOUNT MANAGEMENT ACTIVITY BY ACTION
Click On Line for Detail View
100
50
Count
May
2016
June
July
Time
created
deleted
enabled
modified
suspended
ACCOUNT MANAGEMENT ACTIVITY BY STATUS
Click On Line for Detail View
150
100
50
Count
May
2016
June
July
Time
failure
success
ASSIGNED EVIDENCE
File Name
Content Type
Content Size
Description
Assigned
Assigned By
Uploaded
Uploaded By
EVIDENCE MANAGEMENT
Select from existing evidence:
Previously uploaded evidence
Assign
Upload new evidence:
Browse...
No file selected.
Upload
About
Support
File a Bug
Documentation
Privacy Policy


splunk>
About Q-Compliance
Home
Executive Overview
Compliance Overview
Investigate Controls
Search
Configure
qmulos
IA-02: Identification and Authentication (Organizational Users)
Edit
More Info
Sub-Organization
Qmulos
System
Windows
Time Selector
Last 7 days
IA-02
Control Selection
IA-02
IA-02(01)
IA-02(02)
IA-02(03)
IA-02(04)
IA-02(08)
IA-02(09)
IA-02(11)
IA-02(12)
IA-02 | IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)
Audit Status: Not Reviewed
Assessment Status: Not Reviewed
Show Audit Notes
Show Assessment Notes
Show Control Detail
IA-02 Policy Statement
Policy Statement
Updated By
Updated On
Edit
No compliance description found.
N/A
N/A
Edit
AUTHENTICATION OVER TIME BY CATEGORY
40
20
Count
Tue Jul 19 2016
Thu Jul 21
Sat Jul 23
Mon Jul 25
Time
unknown
AUTHENTICATION BY APP
Splunk
WatchGuard
TOP AUTHENTICATED ACCOUNTS BY CATEGORY
tieu@qmulos.local
adm-tieu
matt
cscott@qmulos.local
terrance@qmulos.local
Account
0
5
10
15
20
25
30
35
40
45
50
55
60
65
Count
unknown
ASSIGNED EVIDENCE
File Name
Content Type
Content Size
Description
Assigned
Assigned By
Uploaded
Uploaded By
EVIDENCE MANAGEMENT
Select from existing evidence:
Previously uploaded evidence
Assign
Upload new evidence:
Browse...
No file selected.
Upload

Best Practices

- 1 To many relationship of data to controls-streamline where possible and get creative in defining systems to handle risks
- Risk based approach – can't mitigate everything but can show that you have a good grasp on what the risks actually are so you can mitigate, transfer, or accept that risk
- Assign risk to those who can mitigate or accept – this can be done via system definitions and data source mapping
- Group controls by data source or function-like data center or physical or policy – gets to inherited controls
- Tailor controls – don't just accept baselines (H, M, L – tailor as appropriate to fit the system and organization

Example Sources

- Windows Event Logs
- Linux Audit Logs
- Active Directory
- IBM Big Fix
- Tenable/Nessus
- Ticketing Systems

- Network Traffic
  - DNS/DHCP/FTP/HTTP
- IDS/IPS
- eGRC Tools
- Physical Access Readers…

TAs And Modifications

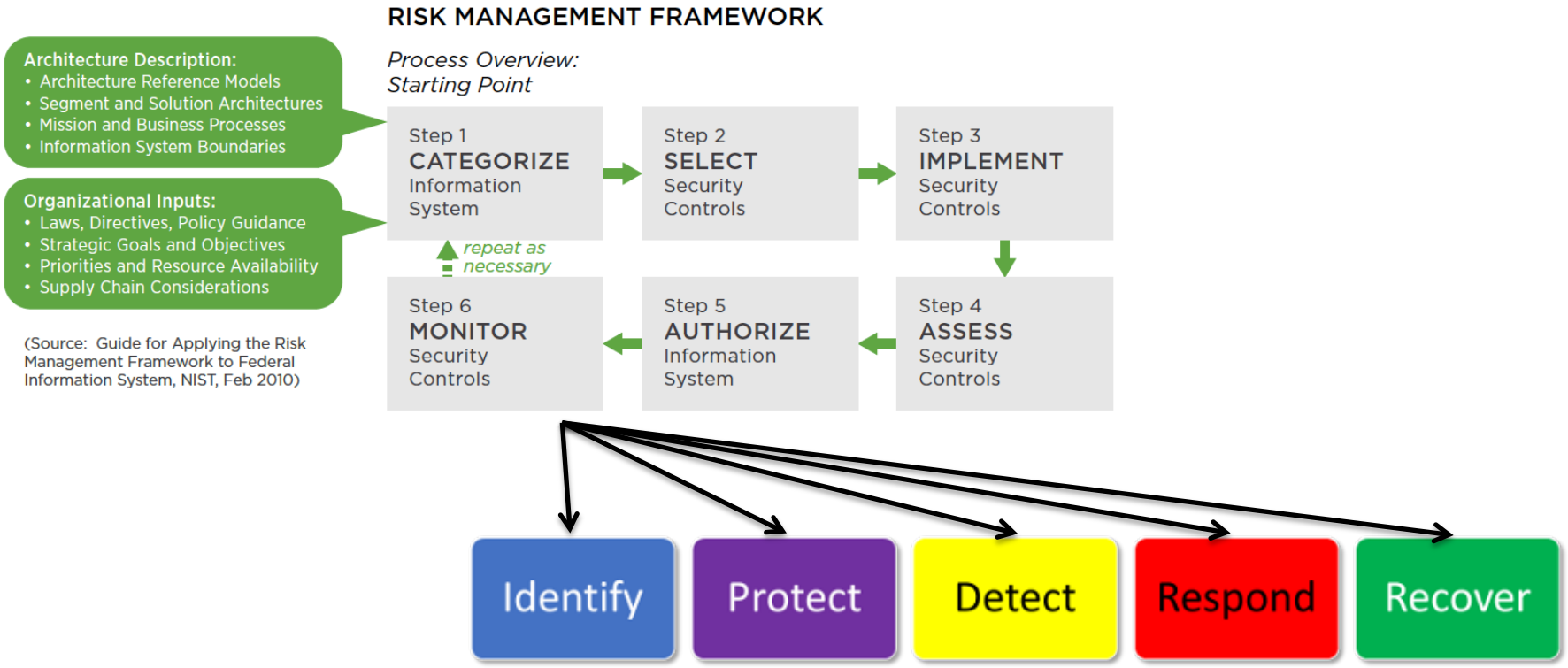
- Windows Add-on
- Splunk Add-on for *nix
- Splunk Add-on for Stream

- Qmulos Add-on for Linux
- " " Nessus
- " " Splunk
- " " Windows
- " " BitDefender
- " " Cisco
- " " R1Soft
- " " Stream
- " " WatchGuard…

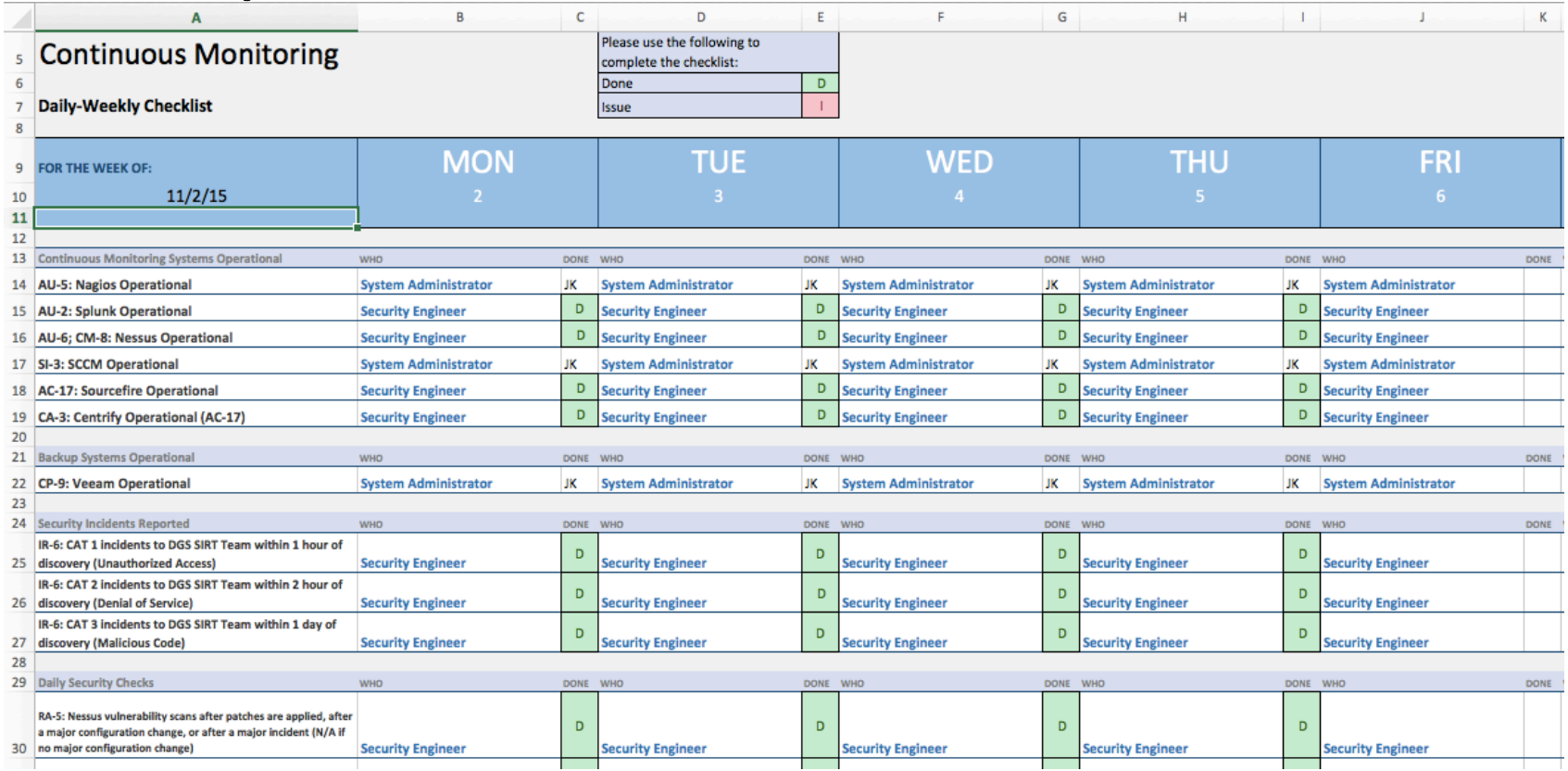
Data Models And KV Stores

- Flexibility is key
- Data models provide a common abstraction – enabling understanding across different data source events
- KVs provide for organizational variable input (e.g. system names)

Compliance (RMF) And Security



Example Of “Manual” ConMon Evidence



Continuous Monitoring

Daily-Weekly Checklist

Please use the following to complete the checklist:	
Done	D
Issue	I

FOR THE WEEK OF:	MON	TUE	WED	THU	FRI
11/2/15	2	3	4	5	6

Continuous Monitoring Systems Operational	WHO	DONE	WHO	DONE	WHO	DONE	WHO	DONE	WHO	DONE
AU-5: Nagios Operational	System Administrator	JK	System Administrator	JK	System Administrator	JK	System Administrator	JK	System Administrator	
AU-2: Splunk Operational	Security Engineer	D	Security Engineer	D	Security Engineer	D	Security Engineer	D	Security Engineer	
AU-6; CM-8: Nessus Operational	Security Engineer	D	Security Engineer	D	Security Engineer	D	Security Engineer	D	Security Engineer	
SI-3: SCCM Operational	System Administrator	JK	System Administrator	JK	System Administrator	JK	System Administrator	JK	System Administrator	
AC-17: Sourcefire Operational	Security Engineer	D	Security Engineer	D	Security Engineer	D	Security Engineer	D	Security Engineer	
CA-3: Centrify Operational (AC-17)	Security Engineer	D	Security Engineer	D	Security Engineer	D	Security Engineer	D	Security Engineer	
Backup Systems Operational	**WHO**	**DONE**	**WHO**	**DONE**	**WHO**	**DONE**	**WHO**	**DONE**	**WHO**	**DONE**
CP-9: Veeam Operational	System Administrator	JK	System Administrator	JK	System Administrator	JK	System Administrator	JK	System Administrator	
Security Incidents Reported	**WHO**	**DONE**	**WHO**	**DONE**	**WHO**	**DONE**	**WHO**	**DONE**	**WHO**	**DONE**
IR-6: CAT 1 incidents to DGS SIRT Team within 1 hour of discovery (Unauthorized Access)	Security Engineer	D	Security Engineer	D	Security Engineer	D	Security Engineer	D	Security Engineer	
IR-6: CAT 2 incidents to DGS SIRT Team within 2 hour of discovery (Denial of Service)	Security Engineer	D	Security Engineer	D	Security Engineer	D	Security Engineer	D	Security Engineer	
IR-6: CAT 3 incidents to DGS SIRT Team within 1 day of discovery (Malicious Code)	Security Engineer	D	Security Engineer	D	Security Engineer	D	Security Engineer	D	Security Engineer	
Daily Security Checks	**WHO**	**DONE**	**WHO**	**DONE**	**WHO**	**DONE**	**WHO**	**DONE**	**WHO**	**DONE**
RA-5: Nessus vulnerability scans after patches are applied, after a major configuration change, or after a major incident (N/A if no major configuration change)	Security Engineer	D	Security Engineer	D	Security Engineer	D	Security Engineer	D	Security Engineer	

THANK YOU

splunk>