

.conf19

splunk®>

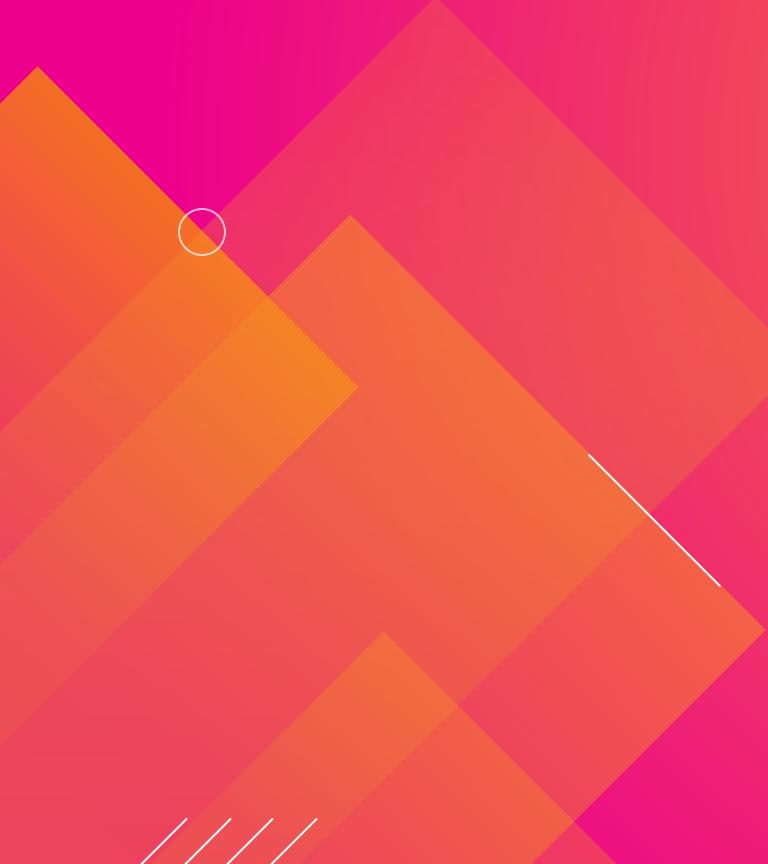
Breaking Free From Legacy GRC

Achieving real-time integrated risk
visibility

Matt Coose
CEO | Qmulos

Anthony Perez
Director of Public Sector Field Technology | Splunk

Forward-Looking Statements



//////

During the course of this presentation, we may make forward-looking statements regarding future events or plans 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 may differ materially. The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

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 functionalities described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Turn Data Into Doing, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. ©2019 Splunk Inc. All rights reserved.



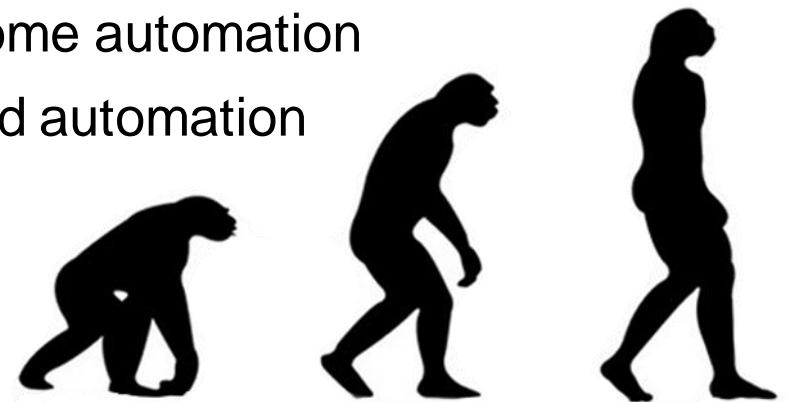
One Size Does Not Fit All

Every organization is at a different state of maturity

One Size Does Not Fit All

Different organizations are in different places

- Compliance and risk **frameworks may be consistent** across organizations
- Even when consistent, every organization has different needs based on their maturity
- Organizational maturity states may include:
 - **Crawl:** Basic processes, manual evidence, but limited visibility
 - **Walk:** Limited real-time insights and reporting visibility – some automation
 - **Run:** Comprehensive near real-time insights, reporting, and automation



One Size Does Not Fit All

Different organizations are in different places

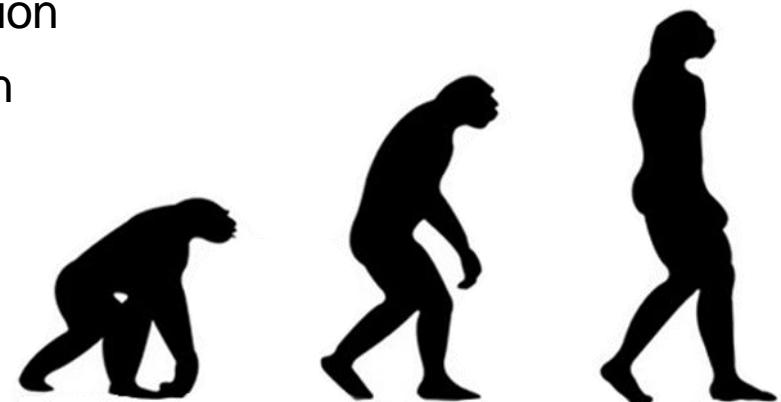
Compliance and risk **frameworks may be consistent** across organizations

Even when consistent, every organization has different needs based on their maturity

Organizational maturity states may include:

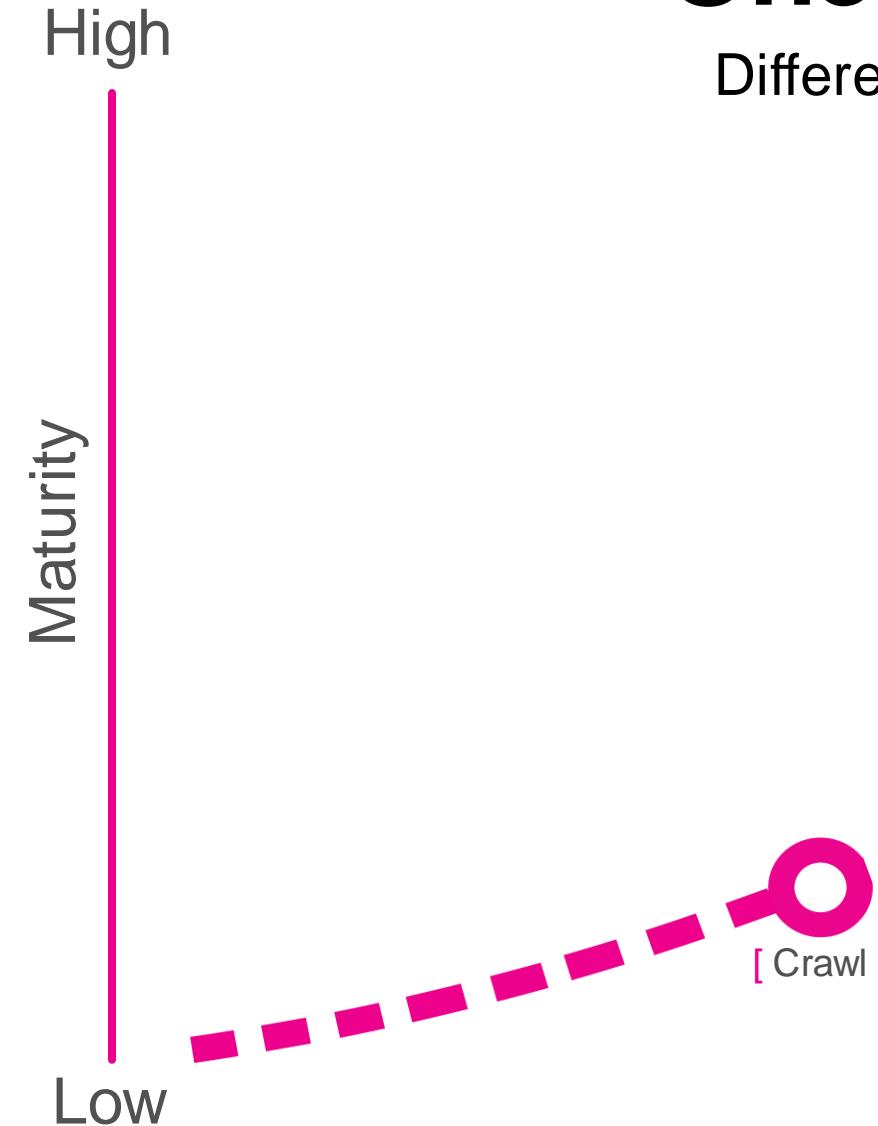
- **Crawl:** Basic processes, manual evidence, but limited visibility
- **Walk:** Limited real-time insights and reporting visibility – some automation
- **Run:** Comprehensive near real-time insights, reporting, and automation

Finally, a quick and **completely unscientific** poll



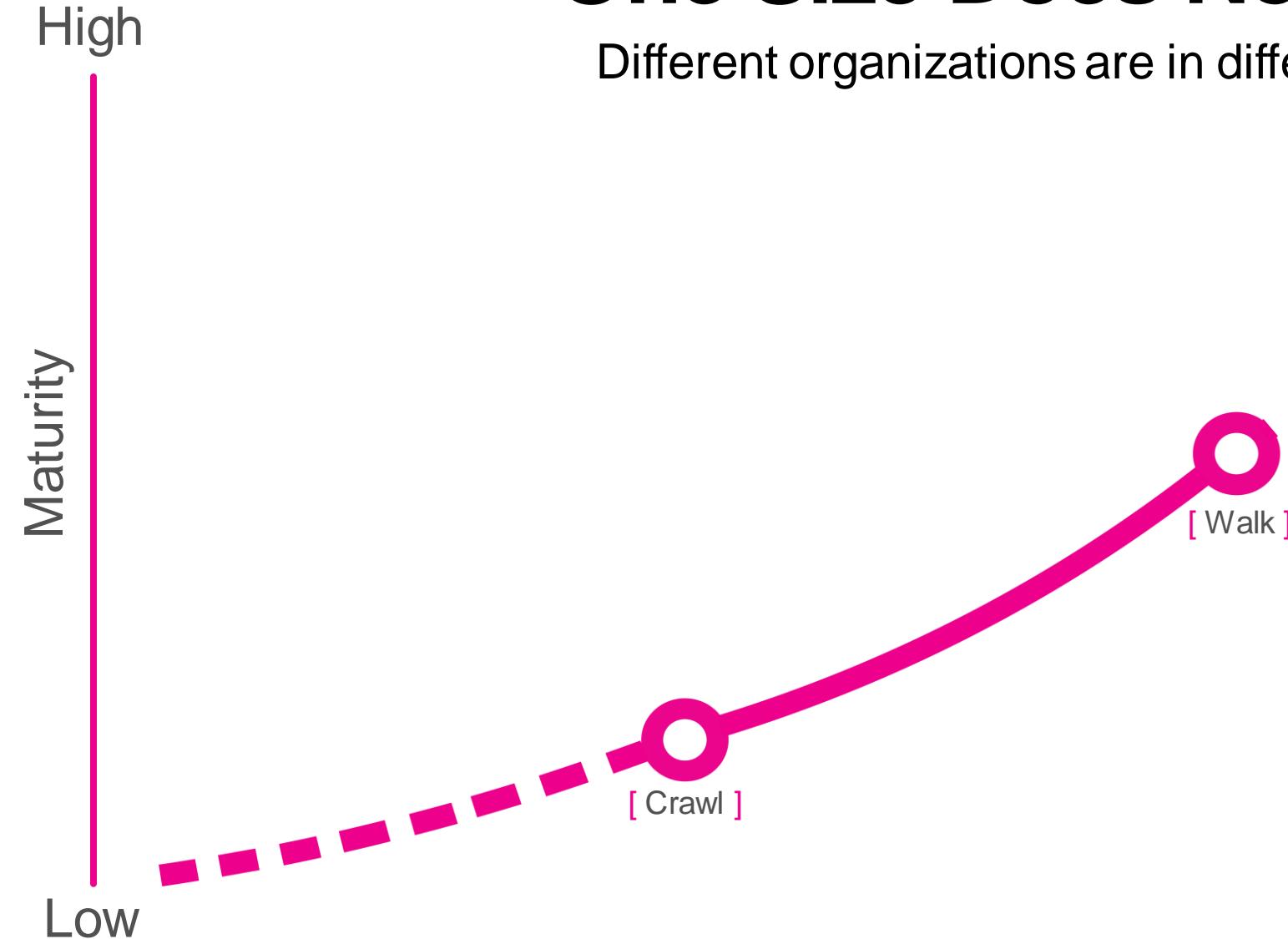
One Size Does Not Fit All

Different organizations are in different places



One Size Does Not Fit All

Different organizations are in different places



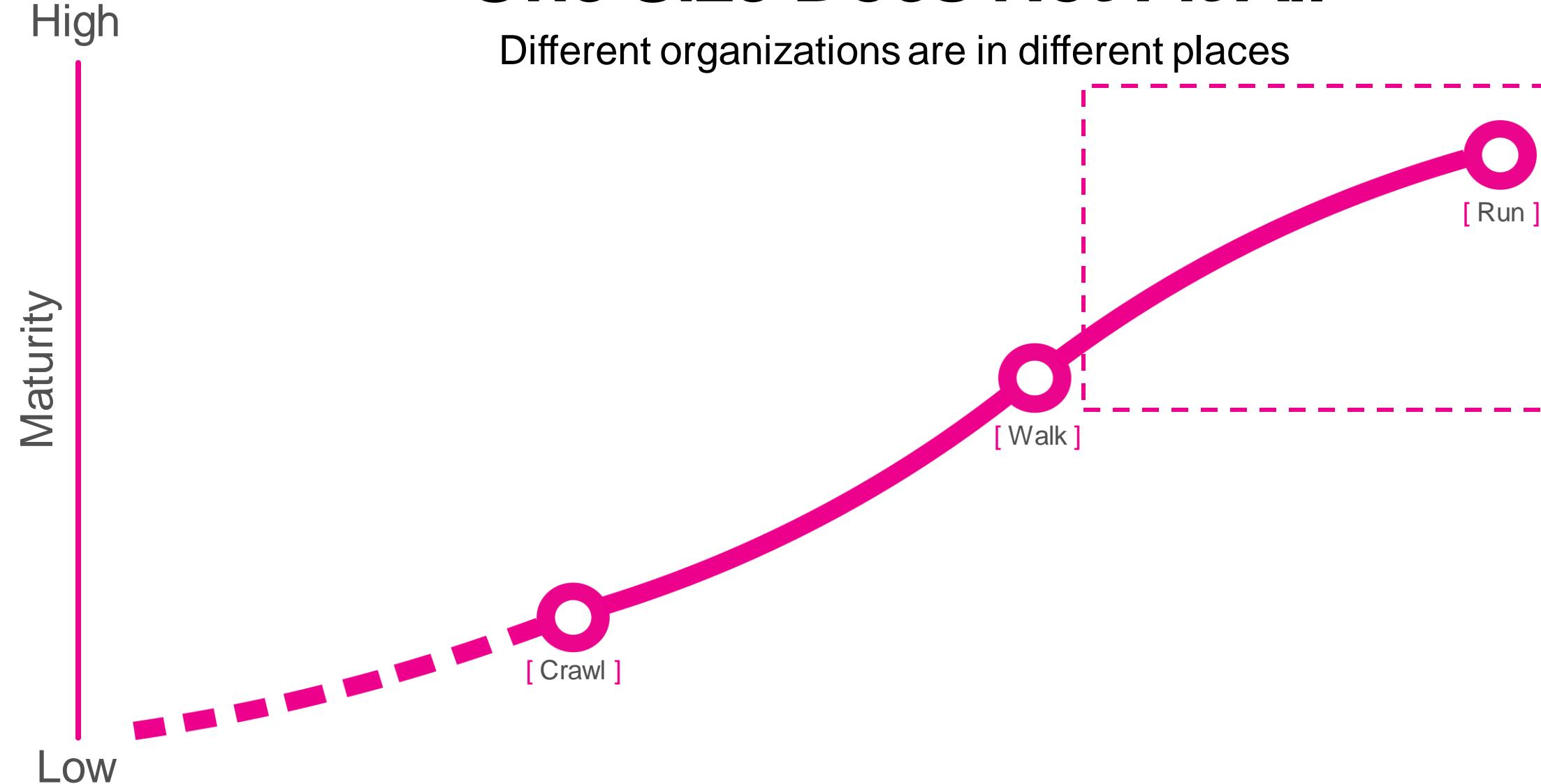
One Size Does Not Fit All

Different organizations are in different places



One Size Does Not Fit All

Different organizations are in different places





Consistently Inconsistent

Common obstacles to success with legacy GRC tools

Consistently Inconsistent

Common obstacles to success with legacy GRC tools



Scope and Scale

- ▶ Multiple systems, organizations, sub-organizations, and locations of various structures and sizes
- ▶ High frequency of events and high volume of data
- ▶ Real-world performance of legacy GRC solutions struggles to keep up

Consistently Inconsistent

Common obstacles to success with legacy GRC tools

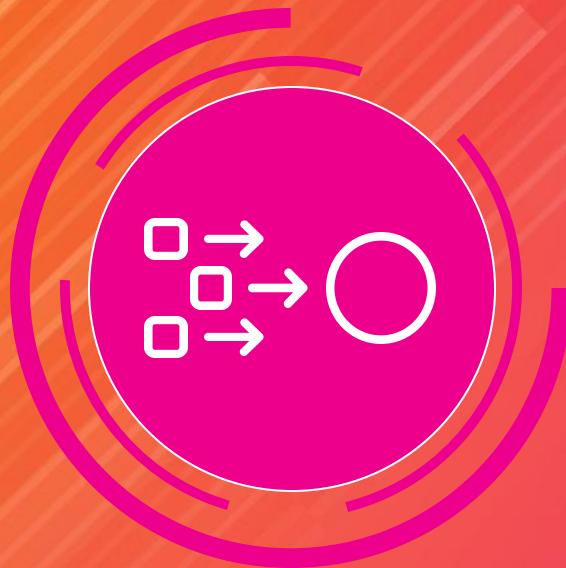


Visibility

- ▶ Visualization capabilities of legacy GRC solutions often fail at larger scales
- ▶ Representation of organizations, systems, and security posture is commonly outdated or slow
- ▶ Actual security and compliance posture can be unclear

Consistently Inconsistent

Common obstacles to success with legacy GRC tools



Diversity

- ▶ Multiple systems, vendors, geographic locations, organizations, and data formats create **significant complexity**
- ▶ This complexity is **nearly impossible** to normalize effectively using legacy GRC solutions
- ▶ This **normalization challenge** is an additional contributor to the “**Visibility**” challenge

Consistently Inconsistent

Common obstacles to success with legacy GRC tools



Retroactive

- ▶ Data latency and system **slowness injects analytic lag**
- ▶ Analytic lag means that analysts and information system security officers (ISSOs) are **constantly looking at stale data**
- ▶ This **prevents genuine data-driven decision making** and real-world continuous monitoring (COMMON)

Consistently Inconsistent

Common obstacles to success with legacy GRC tools



Rigidity

- ▶ Constantly evolving technology ecosystems drive a need for **frequent up-keep and modifications** to legacy GRC solutions
- ▶ This need for up-keep and modifications commonly drive **high maintenance and extension costs**
- ▶ While these extensions and modifications are underway, **organizations face blind-spots** in their COMMON



Saying Goodbye to Rigidity

Breaking free from the constraints of legacy
GRC tools

Saying Goodbye to Rigidity

Breaking free from the constraints of legacy GRC tools

High

Maturity

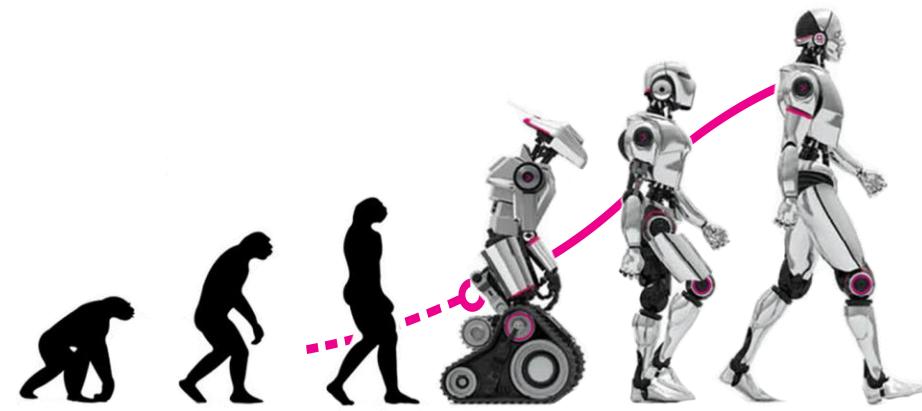
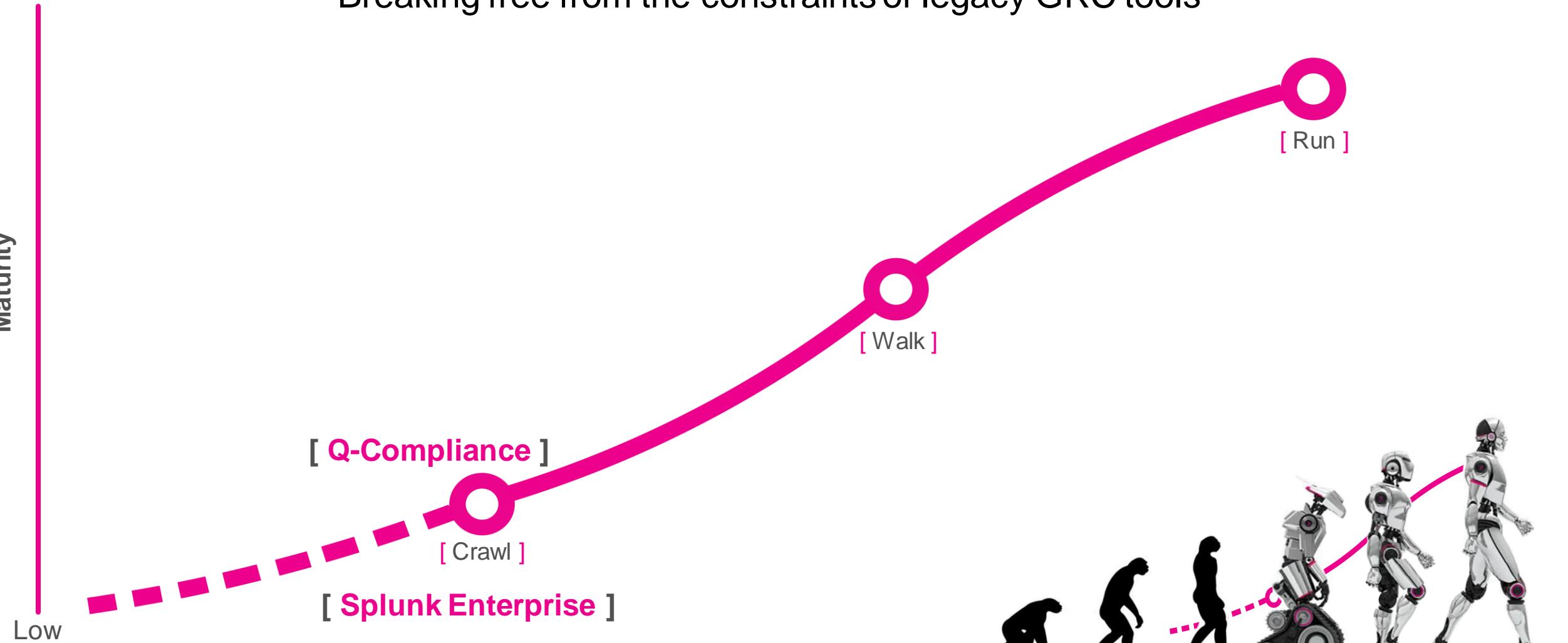


Saying Goodbye to Rigidity

Breaking free from the constraints of legacy GRC tools

High

Maturity

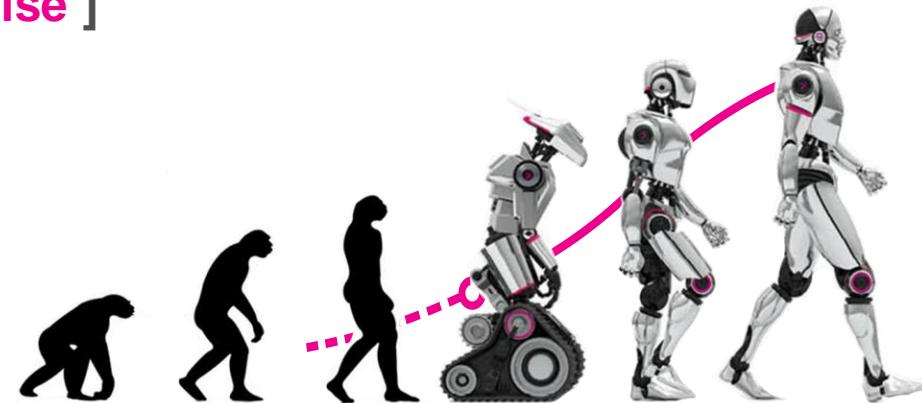
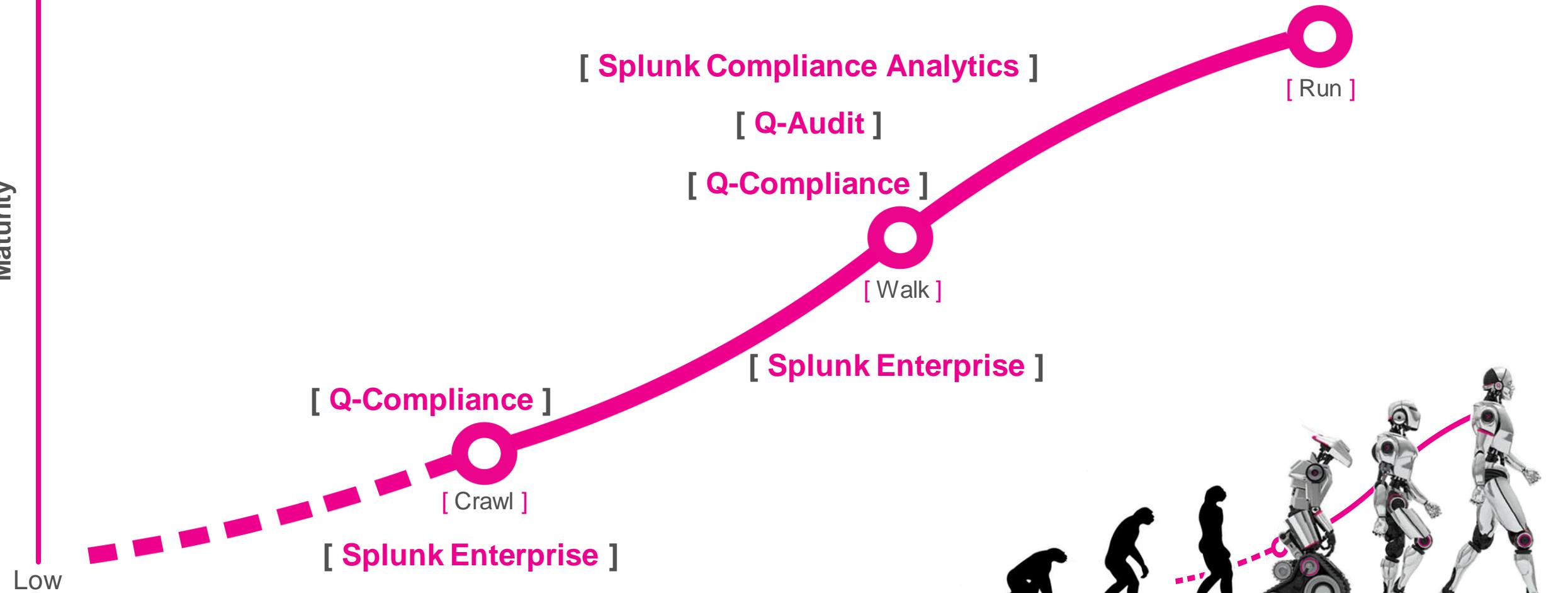


Saying Goodbye to Rigidity

Breaking free from the constraints of legacy GRC tools

High

Maturity

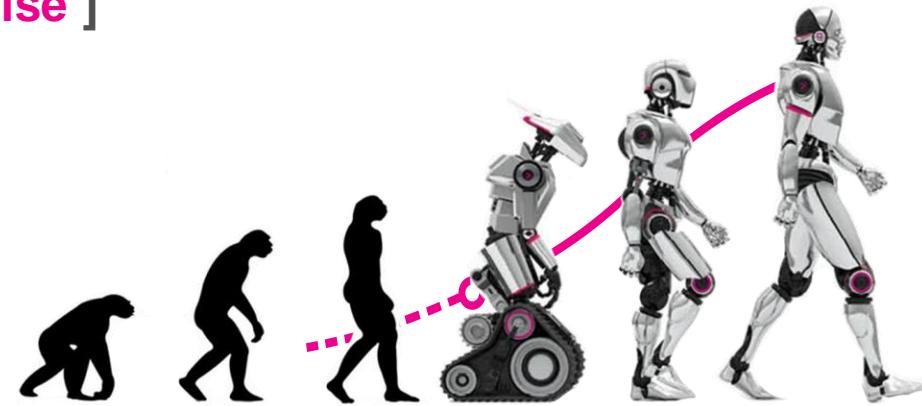
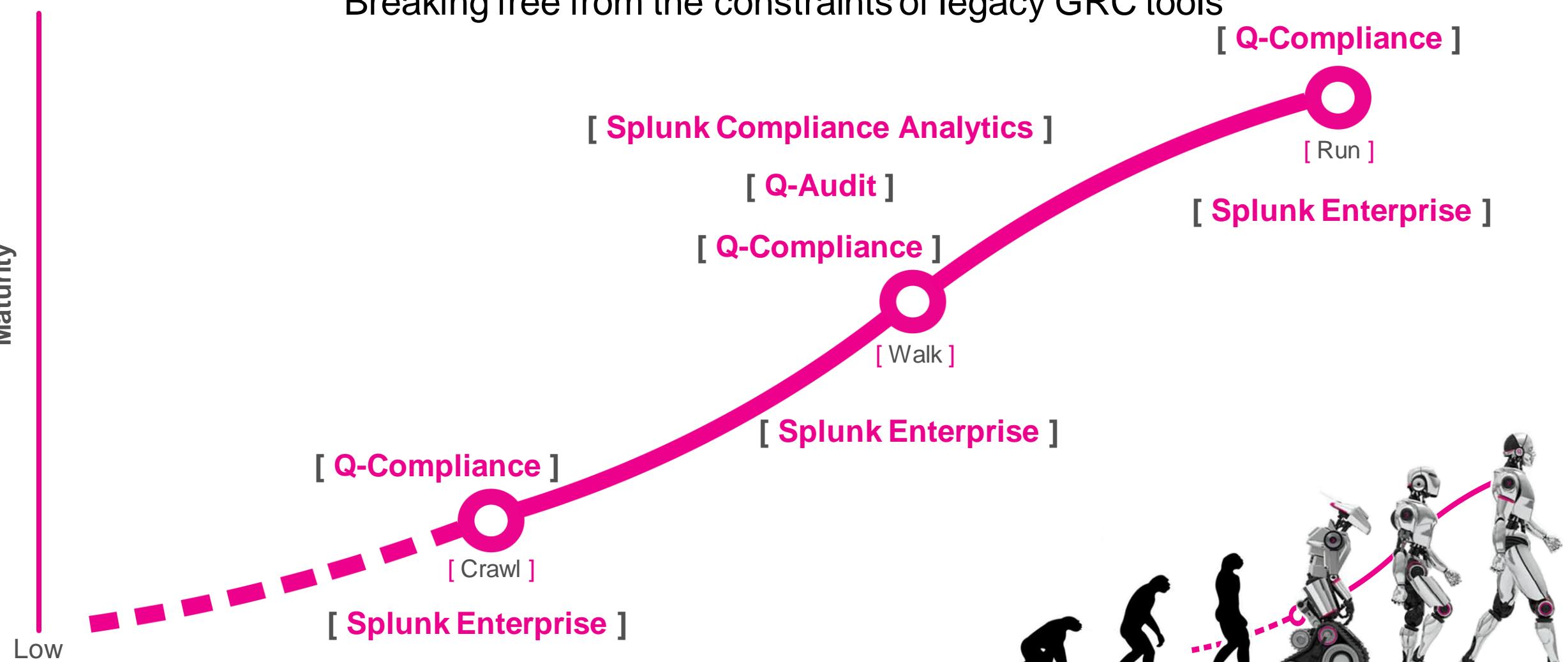


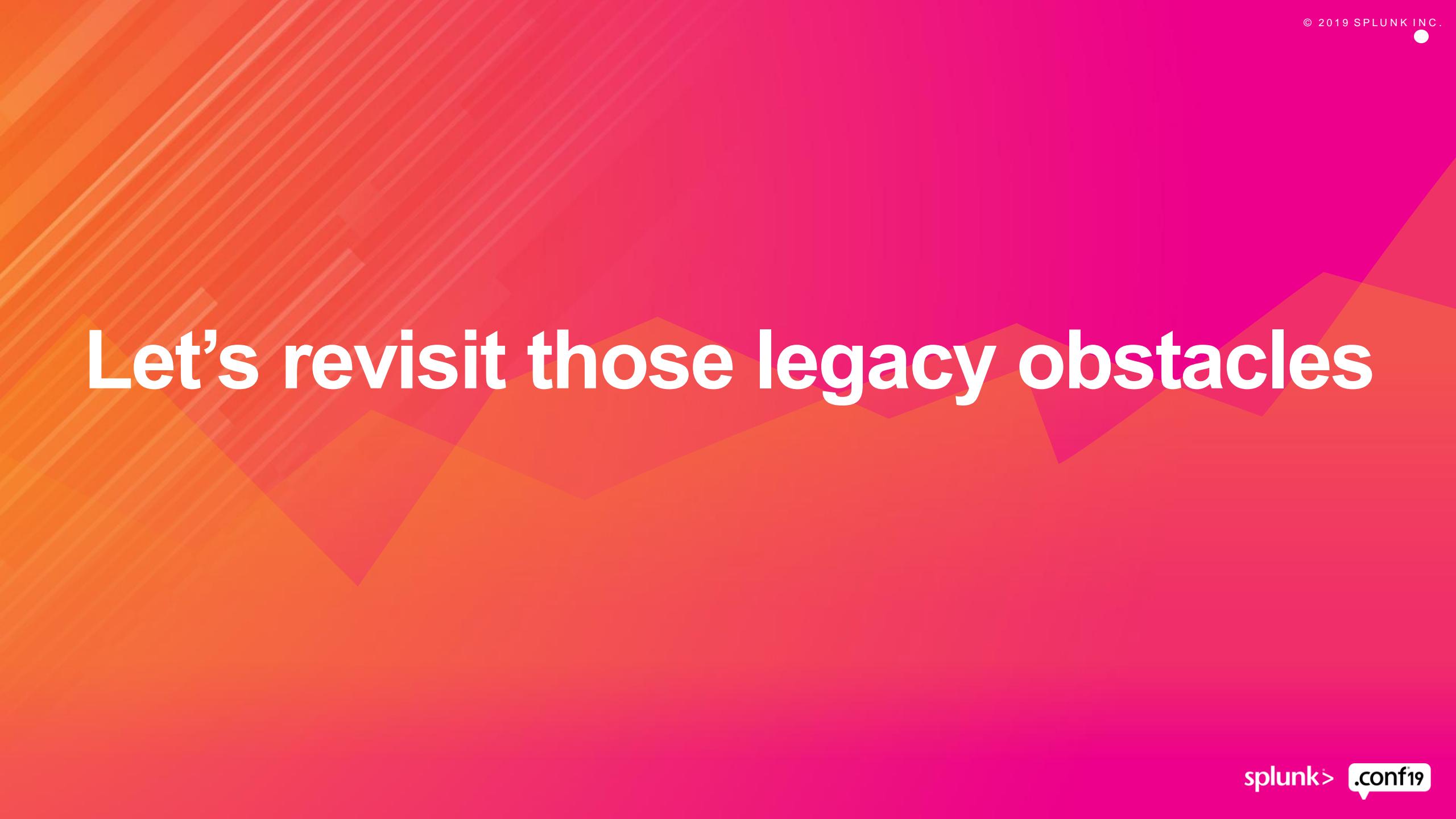
Saying Goodbye to Rigidity

Breaking free from the constraints of legacy GRC tools

High

Maturity





Let's revisit those legacy obstacles

Saying Goodbye to Rigidity

Revisiting common obstacles to success with legacy GRC



Scope and Scale

Historical Challenge	Breaking free with Splunk/Qmulos
X Multiple systems, organizations, sub-organizations, and locations of various structures and sizes	▪ Native tagging and lookup functionality enables org-specific data identification
X High frequency of events and high volume of data are often processing challenge	▪ Distributed architecture – on-prem, cloud, or hybrid ensure that performance can scale with real-world needs
X Real-world performance of legacy GRC solutions struggles to keep up	▪ Big-data architecture highly-performant at multi-Petabyte scale

Saying Goodbye to Rigidity

Revisiting common obstacles to success with legacy GRC

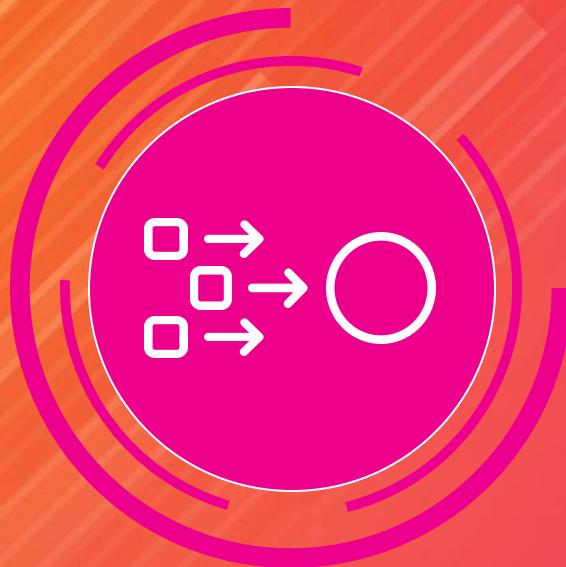


Visibility

Historical Challenge	Breaking free with Splunk/Qmulus
<p>✗ Visualization capabilities of legacy GRC solutions often fail at larger scales</p>	<ul style="list-style-type: none">▪ Holistic visibility of even very-large data sets is enabled by the platform and a breadth of visualization layouts
<p>✗ Representation of organizations, systems, and security posture is commonly outdated or slow</p>	<ul style="list-style-type: none">▪ Near real-time architecture ensures that security posture visibility is current and representative of the operating environment
<p>✗ Actual security and compliance posture can be unclear</p>	<ul style="list-style-type: none">▪ Wide variety of highly flexible visualizations combined with near real-time data flows drive visibility and insight

Saying Goodbye to Rigidity

Revisiting common obstacles to success with legacy GRC



Diversity

Historical Challenge	Breaking free with Splunk/Qmulus
X Multiple systems, vendors, geographic locations, organizations, and data formats create significant complexity	▪ Vendor, data, location and format agnostic
X This complexity is nearly impossible to normalize effectively using legacy GRC solutions	▪ If the data exists in a human-readable form and you have access to it, you can analyze it
X This normalization challenge is an additional contributor to the “Visibility” challenge	▪ Native data normalization through common information models

Saying Goodbye to Rigidity

Revisiting common obstacles to success with legacy GRC



Retroactive

Historical Challenge	Breaking free with Splunk/Qmulus
X Data latency and system slowness injects analytic lag	▪ Analytic insights on timelines typically measured in milliseconds or seconds
X Analytic lag means that analysts and ISSOs are constantly looking at stale data	▪ Near real-time visibility prevents a false sense of security that may be created by stale data
X This prevents data-driven decision making and real-world COMMON	▪ Executives and security leaders are genuinely empowered to make data-driven decisions for their orgs

Saying Goodbye to Rigidity

Revisiting common obstacles to success with legacy GRC



Rigidity

Historical Challenge	Breaking free with Splunk/Qmulos
X Constantly evolving technology ecosystems drive a need for frequent up-keep and modifications to legacy GRC solutions	▪ Data source abstraction through common information models provide a highly flexible foundation
X This need for up-keep and modifications commonly drive high maintenance and extension costs	▪ Platform agility and vendor agnostic analytic / visualization framework is inherently flexible
X While these extensions and modifications are underway, organizations face blind-spots in their CONMON	▪ Platform flexibility and architecture are inherently resilient and naturally well-suited for CONMON and real-world computer network defense



Giant Leaps Toward Maturity

Achieving real-time integrated risk visibility

Giant Leaps Toward Maturity

Achieving real-time integrated risk visibility – **Splunk Compliance Analytics**

Splunk Enterprise + Splunk Compliance Analytics provide a **quick-start solution**

SCA provides a path to **rapidly jump up the maturity curve** and offers extensibility

- This is a great starting point for technical control monitoring, but it is not the top-tier of the maturity curve
- Your organization may require more out-of-the-box

Key Features:

- Provides a quick-start way to rapidly jump up the maturity curve
- Baseline technical controls for near real-time visibility
- tstats-based searches for performance
- Easily scalable / customizable for org-specific needs



DEMO

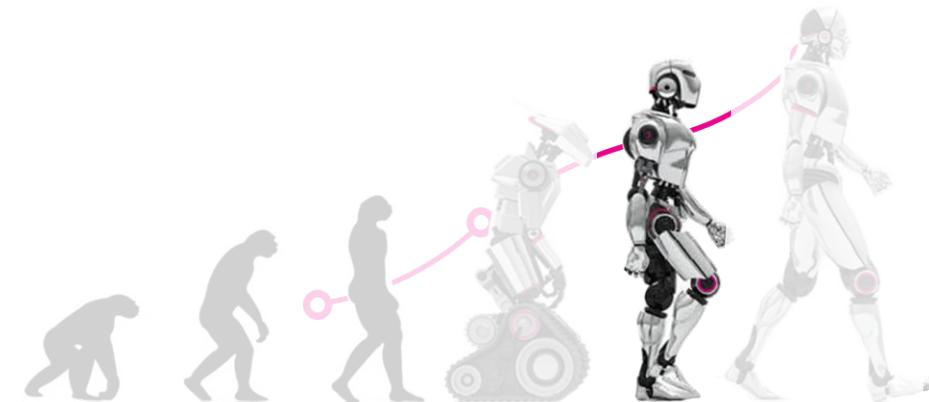
Giant Leaps Toward Maturity

Achieving real-time integrated risk visibility – *Qmulos Q-Audit*

- ▶ Contextualization of logs is highly valuable
- ▶ Q-Audit enables a deep-dive into audit controls
 - Provides prescriptive audit policy (ICS 500-27) and analytics to monitor them – out of the box
- ▶ Tough part is mapping the vendor-specific event codes to the audit policy and auditable event categories

Key Insights:

- A lot of organizations use Splunk to just store audit logs
- Q-Audit takes things to a whole different level
 - Shows what you should log
 - How to monitor those logs and alert in real time
 - Enables actual monitoring of users and device activity
- This ensures that your org is fulfilling the actual purpose of audit controls



Giant Leaps Toward Maturity

Achieving real-time integrated risk visibility – *Qmulos Q-Audit*

- ▶ Contextualization of logs is highly valuable
- ▶ Q-Audit enables a deep-dive into audit controls
 - Provides prescriptive audit policy (ICS 500-27) and analytics to monitor them – out of the box
- ▶ Tough part is mapping the vendor-specific event codes to the audit policy and auditable event categories

Key Insights:

- A lot of organizations use Splunk to just store audit logs
- Q-Audit takes things to a whole different level
 - Shows what you should log
 - How to monitor those logs and alert in real time
 - Enables actual monitoring of users and device activity
- This ensures that your org is fulfilling the actual purpose of audit controls

“Here’s what you should be logging”

“Here’s how to monitor those logs and alert on them in real-time”

***“You’re not just checking the logs, you’re actually monitoring the user and device activities on your network
– This is actually the purpose of the audit and control activities in the first place”***

DEMO

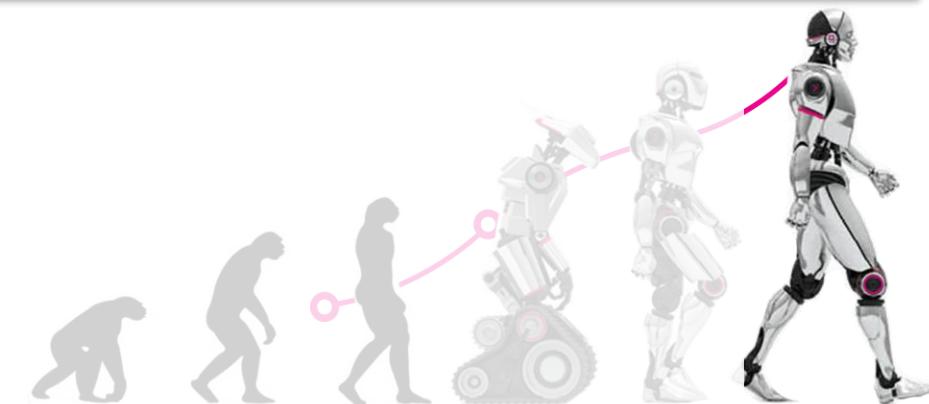
Giant Leaps Toward Maturity

Achieving real-time integrated risk visibility – *Qmulos Q-Compliance*

- ▶ Q-compliance is a **wholly new paradigm** for integrated risk visibility
- ▶ Key functionality expected from GRC, but built on a big-data platform
- ▶ User interface to set up the environment across the **full risk management process**
- ▶ Dashboards, workflows, alerts, and POAMs to manage operational compliance activities
- ▶ Assess, audit, and monitor all controls – including **technical and custom controls**

Key Features:

- *Complete control sets and numerous frameworks*
- *Multi-level organizational hierarchies*
- *Multi-tenant organization based access control*
- *System boundaries and control inheritance*
- *Built-in control baselines and various overlays*
- *Custom controls and control overlays*
- *Hundreds of pre-built control analytics*
- *Supports all three types of evidence*
- *Automated control assessments*



DEMO

What Do You Want Out Of a Capability?

Choosing the best fit for your organization

Maturity	Capability Highlights	Splunk Compliance Analytics*	Q-Audit*	Q-Compliance*
Run (Complete)	<ul style="list-style-type: none">Enables ongoing assessment and continuous monitoring of virtually all technical controls and custom controlsEnables automated assessment of technical controlsCreate automated actions to detect, report and respond to compliance findingsAutomate multiple compliance standards and frameworks			
Walk (Partial)	<ul style="list-style-type: none">Enables monitoring of basic cyber hygiene technical controls such as HWAM/SWAM/VUL/CSM (Q-Compliance)Enables monitoring of Audit (AU) related controls (Q-Audit)Enables monitoring of various technical controls (SCA)			
Crawl (Manual)	<ul style="list-style-type: none">Cost effective legacy GRC capabilitiesManually perform and capture audit/assessment resultsScore compliance posture of systemsDefine assessment boundaries and control baselinesManual evidence collection and uploadCapture compliance work history and POAMsGenerate compliance artifacts (e.g. SSPs)Establishes foundational architecture for centralized and/or federated technical data collection			

*All solutions require Splunk Enterprise

So now what?

Next steps
recommendations

1. Figure out where you are on the curve.
Take the free Qmulos Readiness Assessment: www.qmulos.com/getready
2. Build it from scratch or talk to Splunk / Qmulos (Booth 109) for the solution that fits your organization (crawl, walk, or run).
3. Start doing compliance in a way that delivers **real operational security value!**



Q&A

Matt Coose | CEO, Qmulus

Anthony Perez | Director of Public Sector
Field Technology, Splunk

.conf19

splunk>

Thank
You!

Go to the .conf19 mobile app to

RATE THIS SESSION



Backup

splunk[®] turn data into doing™

Splunk Compliance
Analytics



splunk>enterprise App: Splunk Compliance Analytics

Administrator 2 Messages Settings Activity Help Find

Control Families Access Overview Other Menus

CA Splunk Compliance Analytics

Export ...

Select your Compliance Framework:

Please select one of three selectors to load the application in your selected context. After selection you can come back to this page at any time to change the context of the application. Descriptions of each context are listed below.

FISMA

This context provides an overview of NIST SP 800-53 rev5 Controls that must be monitored according to FISMA. The Controls in this Splunk app are intentionally focused on the technical controls specified in SP 800-53 rev5.



RMF

This context provides an overview of NIST SP 800-53 rev5 Controls that must be monitored according to DoD Instruction 8510.1, which establishes the Risk Management Framework (RMF) for DoD IT. The Controls in this Splunk app are intentionally focused on the technical controls specified in SP 800-53 rev5 in support of NIST Risk Management Framework (SP 800-37), both referenced in DoD 8510.1.



DFARS

This context provides an overview of NIST 800-171 rev1 Controls that must be monitored per Defense Federal Acquisition Regulation Supplement (DFARS). The available Controls are limited to those that include data-driven monitoring requirements and have relevant data ingested in Splunk.



Splunk Compliance
Analytics



splunk>enterprise App: Splunk Compliance Analytics ▾

Anthony Perez ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

FISMA Control Families ▾ Access Overview Other Menus ▾

CA Splunk Compliance Analytics

Control Families Overview

Page Accessed: a few seconds ago by aperez

Export ▾ ...

Introduction

Page Description:

This page provides an overview of NIST SP 800-53 rev5 Control Families that must be monitored according to FISMA. The Control Families in this Splunk app are intentionally focused on the technical controls specified in SP 800-53 rev5. From this page, you may select control families to drill-down to individual technical controls and their corresponding dynamic audit reports.

AC - Access Control Monitoring account administration, and login attempts and failures for accounts 35 Audit Reports	AU - Audit and Accountability Audit and data management activities include audit generation, retention, and analysis 5 Audit Reports	CA - Assessment, Authorization, and Monitoring Analysis of continuous monitoring posture 1 Audit Report
CM - Configuration Management Monitoring configuration and change management within the information technology enclave 8 Audit Reports	IA - Identification and Authentication Monitoring user and service identification and authentication mechanisms, using zero-trust security principals 3 Audit Reports	IR - Incident Response Data associated with incident reporting workflows 7 Audit Reports
RA - Risk Assessment Assessment of information technology risk posture 6 Audit Reports	SI - System and Information Integrity Monitoring cybersecurity data and services provided by point solutions 14 Audit Reports	

Splunk Compliance
Analytics



splunk>enterprise App: Splunk Compliance Analytics ▾

Anthony Perez ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

FISMA Control Families ▾ Access Overview Other Menus ▾ Splunk Compliance Analytics

Export ▾ ...

Control Families Overview

Page Accessed: a few seconds ago by aperez

Introduction

Page Description:

This page provides an overview of NIST SP 800-53 rev5 Control Families that must be monitored according to FISMA. The Control Families in this Splunk app are intentionally focused on the technical controls specified in SP 800-53 rev5. From this page, you may select control families to drill-down to individual technical controls and their corresponding dynamic audit reports.

AC - Access Control
Monitoring account administration, and login attempts and failures for accounts
35 Audit Reports

AU - Audit and Accountability
Audit and data management activities include audit generation, retention, and analysis
5 Audit Reports

CA - Assessment, Authorization, and Monitoring
Analysis of continuous monitoring posture
1 Audit Report

CM - Configuration Management
Monitoring configuration and change management within the information technology enclave
8 Audit Reports

IA - Identification and Authentication
Monitoring user and service identification and authentication mechanisms, using zero-trust security principals
3 Audit Reports

IR - Incident Response
Data associated with incident reporting workflows
7 Audit Reports

RA - Risk Assessment
Assessment of information technology risk posture
6 Audit Reports

SI - System and Information Integrity
Monitoring cybersecurity data and services provided by point solutions
14 Audit Reports

Splunk Compliance
Analytics

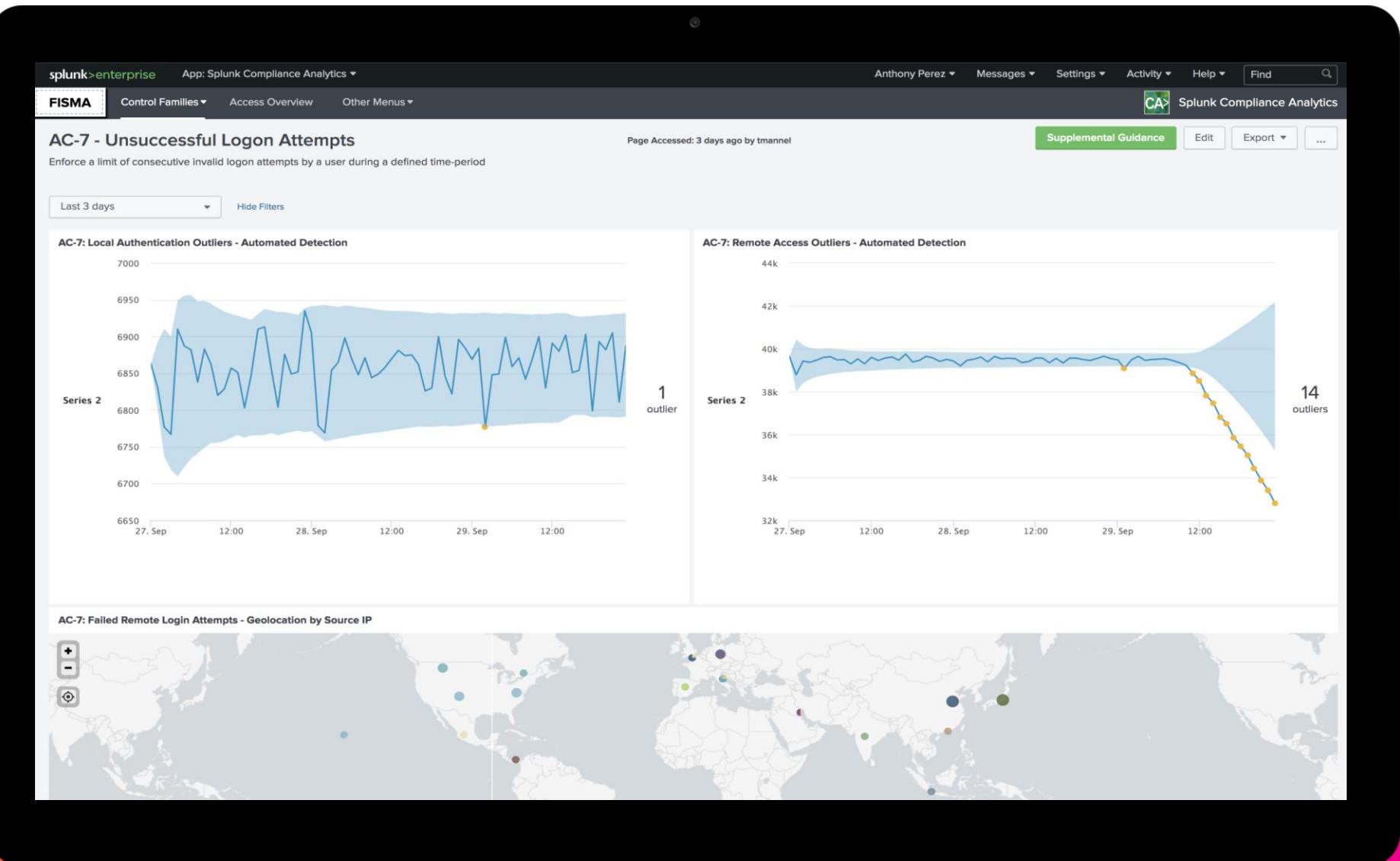


The screenshot shows the Splunk Compliance Analytics interface. At the top, there's a navigation bar with links for 'splunk>enterprise' (highlighted in green), 'App: Splunk Compliance Analytics ▾', 'Control Families ▾', 'Access Overview', and 'Other Menus ▾'. On the right side of the top bar are user profile, message, settings, activity, help, and search icons. Below the top bar, the title 'FISMA' is displayed in a yellow box. The main content area is titled 'Controls Overview' and includes a 'Page Description' section stating: 'From this page, you may select an individual control to navigate to its respective dashboard(s) and dynamic audit reports.' A green button labeled '6 selected ▾' is present. The central part of the page is titled 'Access Control' and contains six cards, each representing a different control:

- AC-2 - Account Management**: Monitor the use of system accounts.
- AC-3 - Access Enforcement**: Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.
- AC-7 - Unsuccessful Logon Attempts**: Enforce a limit of consecutive invalid logon attempts by a user during a defined time-period.
- AC-12 - Session Termination**: Automatically terminate a user session after by time or event triggers.
- AC-17 - Remote Access**: Authorize remote access to the system prior to allowing such connections.
- AC-18 - Wireless Access**: Authorize wireless access to the system prior to allowing such connections.

Splunk Compliance
Analytics





splunk>enterprise App: Splunk Compliance Analytics ▾

FISMA Control Families ▾ Access Overview Other Menus ▾

Administrator ▾ 3 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

CA Splunk Compliance Analytics

Control Families Overview

Page Accessed: a few seconds ago by admin

Export ▾ ...

Introduction

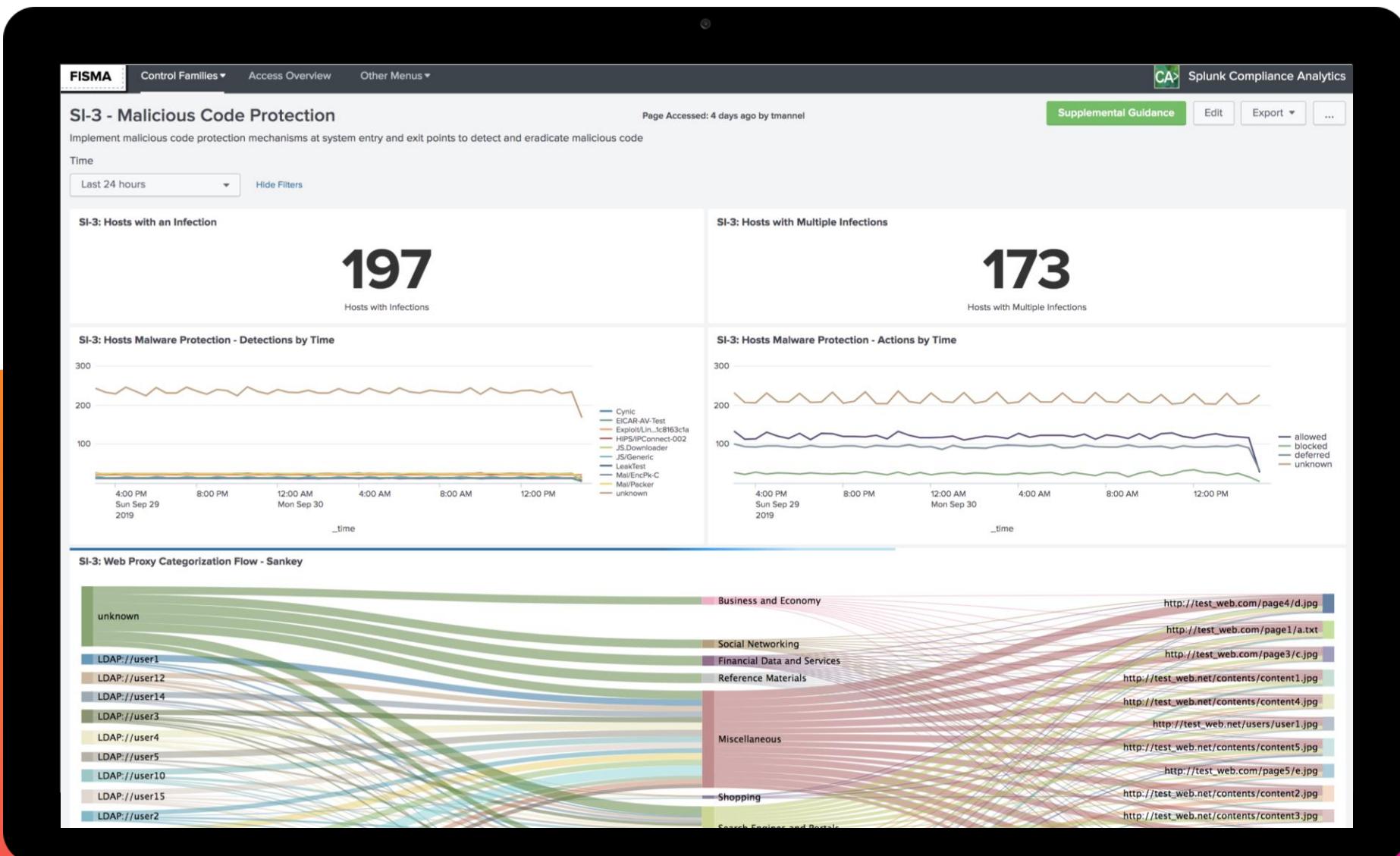
Page Description:

This page provides an overview of NIST SP 800-53 rev5 Control Families that must be monitored according to FISMA. The Control Families in this Splunk app are intentionally focused on the technical controls specified in SP 800-53 rev5. From this page, you may select control families to drill-down to individual technical controls and their corresponding dynamic audit reports.

 AC - Access Control Monitoring account administration, and login attempts and failures for accounts 35 Audit Reports	 AU - Audit and Accountability Audit and data management activities include audit generation, retention, and analysis 5 Audit Reports	 CA - Assessment, Authorization, and Monitoring Analysis of continuous monitoring posture 1 Audit Report
 CM - Configuration Management Monitoring configuration and change management within the information technology enclave 8 Audit Reports	 IA - Identification and Authentication Monitoring user and service identification and authentication mechanisms, using zero-trust security principals 3 Audit Reports	 IR - Incident Response Data associated with incident reporting workflows 7 Audit Reports
 RA - Risk Assessment Assessment of information technology risk posture 6 Audit Reports	 SI - System and Information Integrity Monitoring cybersecurity data and services provided by point solutions 14 Audit Reports	

Splunk Compliance Analytics





Splunk Compliance
Analytics



The screenshot shows the 'Control Families Overview' page within the Splunk Compliance Analytics app. The top navigation bar includes tabs for 'FISMA', 'Control Families', 'Access Overview' (which is highlighted with a red box and has a red arrow pointing to it), and 'Other Menus'. The main content area displays nine control families, each represented by a card with an icon, a title, a description, and the number of audit reports:

Control Family	Description	Audit Reports
AC - Access Control	Monitoring account administration, and login attempts and failures for accounts	35 Audit Reports
AU - Audit and Accountability	Audit and data management activities include audit generation, retention, and analysis	5 Audit Reports
CA - Assessment, Authorization, and Monitoring	Analysis of continuous monitoring posture	1 Audit Report
CM - Configuration Management	Monitoring configuration and change management within the information technology enclave	8 Audit Reports
IA - Identification and Authentication	Monitoring user and service identification and authentication mechanisms, using zero-trust security principals	3 Audit Reports
IR - Incident Response	Data associated with incident reporting workflows	7 Audit Reports
RA - Risk Assessment	Assessment of information technology risk posture	6 Audit Reports
SI - System and Information Integrity	Monitoring cybersecurity data and services provided by point solutions	14 Audit Reports

Splunk Compliance
Analytics



splunk>enterprise App: Splunk Compliance Analytics ▾

FISMA Control Families ▾ Access Overview Other Menus ▾

Anthony Perez ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

CA Splunk Compliance Analytics

Page Accessed: 4 days ago by tschiottog

Access Overview

This page provides an reporting and analysis of page views within the Compliance Posture Analytics App. Use this page to assess compliance op-tempo, focus areas, and areas for improvement in-terms of continuous monitoring practices.

All Page Accesses: **5,313**

Page Access Last 30 Days: **366** ↑
160

Page Access Last 7 Days: **7** ↓
-15

Page Access Over Time

Page Name: All User: All Time Period: Last 7 days

Legend:

- AC-2 - Account Management
- AC-7 - Unsuccessful Logon Attempts
- AU-4 - Audit Storage Capacity
- AU-6 - Audit Review, Analysis, and Reporting
- Access Overview
- CA-7 - Continuous Monitoring
- CM-11 - User-Installed Software
- Control Families Overview
- Controls Overview
- IR-4 - Incident Handling
- OTHER

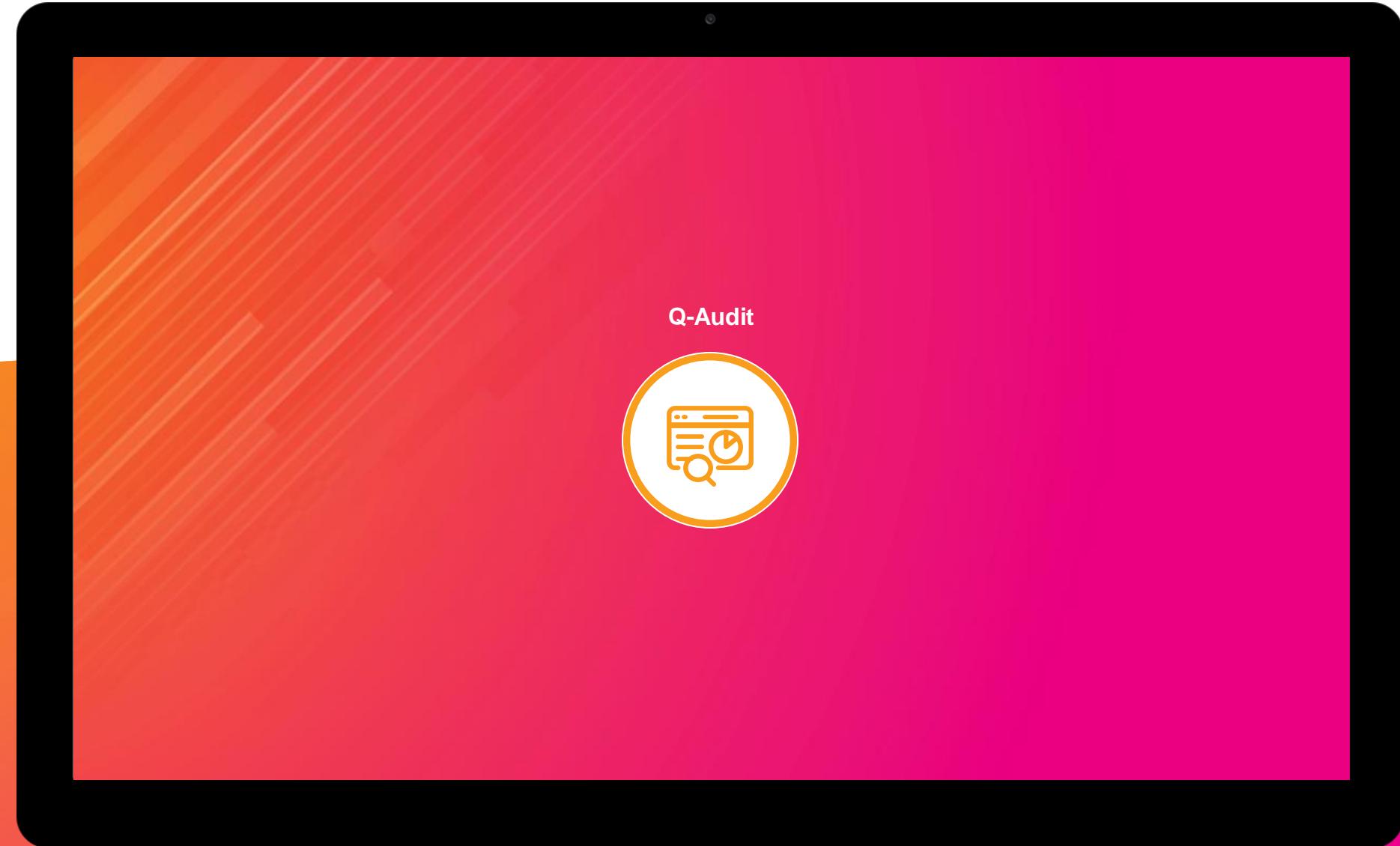
Most Recent Page Access Times by User

User: All

User	Page Accessed	Page Link	Last Access Time	Time Spent on the Page
abrill	IA-2 - Identification and Authentication AC-3 - Access Enforcement Access Overview Control Families Overview	ia_2 ac_3 access_overview home	11-29-2018 1:32 PM 11-29-2018 1:27 PM 11-29-2018 1:27 PM 11-29-2018 1:27 PM	Unknown 5 Minute(s) and 33 Second(s) 0 Minute(s) and 11 Second(s) 0 Minute(s) and 9 Second(s)
adayton	Controls Overview Control Families Overview IR-4 - Incident Handling	contents home ir_4	04-29-2019 10:12 PM 04-29-2019 10:12 PM 04-19-2019 8:00 PM	Unknown 0 Minute(s) and 26 Second(s) Unknown
adee	Controls Overview Control Families Overview CM-11 - User-Installed Software AC-7 - Unsuccessful Logon Attempts Access Overview SI-3 - Malicious Code Protection	contents home cm_11 ac_7 access_overview si_3	07-01-2019 11:11 AM 07-01-2019 11:10 AM 11-13-2018 10:36 AM 11-13-2018 10:31 AM 11-13-2018 9:46 AM 11-13-2018 9:24 AM	32 Minute(s) and 31 Second(s) 1 Minute(s) and 58 Second(s) Unknown 2 Minute(s) and 58 Second(s) 4 Minute(s) and 9 Second(s) 22 Minute(s) and 15 Second(s)

Splunk Compliance
Analytics





splunk>enterprise App: Q-Audit

Administrator 2 Messages Settings Activity Help Find

About Enterprise Audit Home Data Summary Real Time Monitoring Event Families User/Host Investigation Search Configure

QMULOS ENTERPRISE AUDIT (Q-AUDIT)

Auditing to Enable Security

Automated audits through continuous assessment

COLLECTION

About Q-Audit

EVENT FAMILIES

Admin Access and Escalation
Applications
Authentication
Data Movement
File and Objects
Privileged Access
System
User and Group Management
Attributable Events

CONFIGURATION

Baseline Users and Hosts
Baseline/Watchlist Apps
Configure Alerts

Q-Audit



splunk>enterprise App: Q-Audit ▾

Administrator ▾ 2 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

About Enterprise Audit Home Data Summary Real Time Monitoring Event Families ▾ User/Host Investigation Search ▾ Configure ▾ ...

Data Summary

KEY DATA STATISTICS (YESTERDAY)

50 Hosts

Compared to the prior day

54 Sourcetypes

Compared to the prior day

379 Users

Compared to the prior day

UNIQUE HOSTS PER Q-AUDIT FAMILY OVER TIME

Date	Admin A...cation	Application	Authenticatio...	File and Object...	Privileged Access...	System	User an...gement
Tue Oct 8 2019	10	12	11	10	10	10	10
Wed Oct 9	11	13	12	11	11	11	11
Thu Oct 10	10	12	11	10	10	10	10
Fri Oct 11	11	13	12	11	11	11	11
Sat Oct 12	10	12	11	10	10	10	10
Sun Oct 13	11	13	12	11	11	11	11
Mon Oct 14	12	14	13	12	12	12	12

Time

TOP SOURCETYPES OVER TIME BY COUNT

Date	audittrail	aws:configure:log	aws:inspector:log	eventgen	eventgen_metrics	kvstore	splunk:r_e_usage	splunkd_access	splunkd_searches	OTHER
Tue Oct 8 2019	10,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000
Wed Oct 9	10,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000
Thu Oct 10	10,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000
Fri Oct 11	10,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000
Sat Oct 12	10,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000
Sun Oct 13	10,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000
Mon Oct 14	10,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000

Time

DATA COLLECTED TODAY

Sourcetype	Unique Hosts	Number of Events	Most Recent Event Time
wids_eventgen	1	73	10/15/2019 11:57:38
watchguard:traffic	1	17	10/15/2019 11:08:43
ssl_traffic_eventgen	1	32	10/15/2019 10:08:18
shutdown_eventgen	2	4	10/15/2019 11:48:33
security_policy_eventgen	2	4	10/15/2019 11:08:30
secrets_mgmt_eventgen	1	40	10/15/2019 10:08:18

Q-Audit

splunk>enterprise App: Q-Audit ▾

Administrator ▾ 2 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

About Enterprise Audit Home Data Summary Real Time Monitoring Event Families ▾ User/Host Investigation Search ▾ Configure ▾

Real Time Monitoring

User Host Time Selector

All All Last 7 days Hide Filters

Fired Alerts for Attributable Events

Time	Fired Alerts	Severity	Results	Delete
2019-10-15 13:35:02 EDT	Unauthorized Local Device Access	High	Open Search	Delete
2019-10-15 13:20:02 EDT	System Reset/Reboot	High	Open Search	Delete
2019-10-15 13:10:02 EDT	Unauthorized Privileged Access	High	Open Search	Delete
2019-10-15 13:10:02 EDT	System Reset/Reboot	High	Open Search	Delete
2019-10-15 13:10:02 EDT	Unauthorized Local Device Access	High	Open Search	Delete
2019-10-15 12:35:02 EDT	System Reset/Reboot	High	Open Search	Delete
2019-10-15 12:10:03 EDT	Unauthorized Local Device Access	High	Open Search	Delete
2019-10-15 12:05:02 EDT	Unauthorized Local Device Access	High	Open Search	Delete
2019-10-15 11:50:02 EDT	System Reset/Reboot	High	Open Search	Delete
2019-10-15 10:40:03 EDT	Unauthorized Local Device Access	High	Open Search	Delete

« Prev 1 2 Next »

RECENT ACCOUNT MANAGEMENT EVENTS

Time	Category	Host	Account Manager	User	Domain	Group
10/15/2019 13:08:28	group	QDC-01	alfred_ian	cn=ingrid jex,ou=q_domain admins,dc=q_domain,dc=local	Q_DOMAIN	Splunk Users
10/15/2019 13:08:28	group	QDC-01	greg_lee	greg_lee	Q_DOMAIN	Splunk Users

RECENT AUTHENTICATION EVENTS

Time	Host	User	Description	Status
10/15/2019 14:56:56	qdc-demo-spsh-01.qmulos.local	admin	Splunk Logon	success
10/15/2019 14:25:12	linux_heavy_tester	freddy	Local Logoff	success
10/15/2019 14:25:12	linux_heavy_tester	freddy	Local Logon	success

Q-Audit

Admin Access and Escalation

User Host

All All

TOP USERS BY PRIVILEGED EXECUTIONS

User	Count of Privileged Execution
annie_vincent	~48
elizabeth_sealy	~45
jennifer_stine	~45
nakayama_tim	~45
latoria_mcclasky	~45
mike_bell	~45
mindy_purvis	~45
don_ben	~45
jane_jones	~45
mathew_hewlett	~45

PROCESSES WITH PRIVILEGED EXECUTIONS

Process	Count of Privileged Execution
Special Logon	~7,500
iexplore.exe	~1,500
App1	~1,000
svchost.exe	~1,000
App3	~1,000
App2	~1,000
Srv32.exe	~1,000
rundll32.exe	~1,000
sachostc.exe	~1,000
syscfg32.exe	~1,000

Successful Admin Logins

Failed Admin Logins

Successful Privileged Executions

Failed Privileged Executions

Event Families

- Admin Access and Escalation
- Application
- Authentication
- Data Movement
- File and Object
- Privileged Access
- System
- User and Group Management
- Attributable Events

Search

Configure

qmulos

<https://products.qmulus.com:9443/en-US/app/Q-Audit/authentication>

Q-Audit



The screenshot shows a Splunk Enterprise dashboard titled "User/Host Investigation". The top navigation bar includes links for "About Enterprise Audit", "Home", "Data Summary", "Real Time Monitoring", "Event Families", "User/Host Investigation", "Search", and "Configure". The top right corner shows the user is "Administrator" with 2 messages, and there are "Find", "Edit", "Export", and "..." buttons.

User/Host Investigation

User Host Time Selector
All All Last 7 days Hide Filters

ADMIN OR ROOT-LEVEL ACCESS - SUMMARY STATISTICS

7,493 Successful Admin logins	0 Failed Admin logins	8,722 Privileged Executions	1,761 Failed Privileged Executions
---	---------------------------------	---------------------------------------	--

RECENT ADMIN EVENTS (CLICK TO EXPAND)

Process	Description	Status
*	*	*

APPLICATION INITIALIZATION - SUMMARY STATISTICS

1,310 Application Initializations	82 Off-Profile Apps Observed	1 Watchlisted Apps Seen	15 Watchlisted Initializations
---	--	-----------------------------------	--

RECENT APPLICATION INITIALIZATIONS (CLICK TO EXPAND)

AUTHENTICATION - SUMMARY STATISTICS

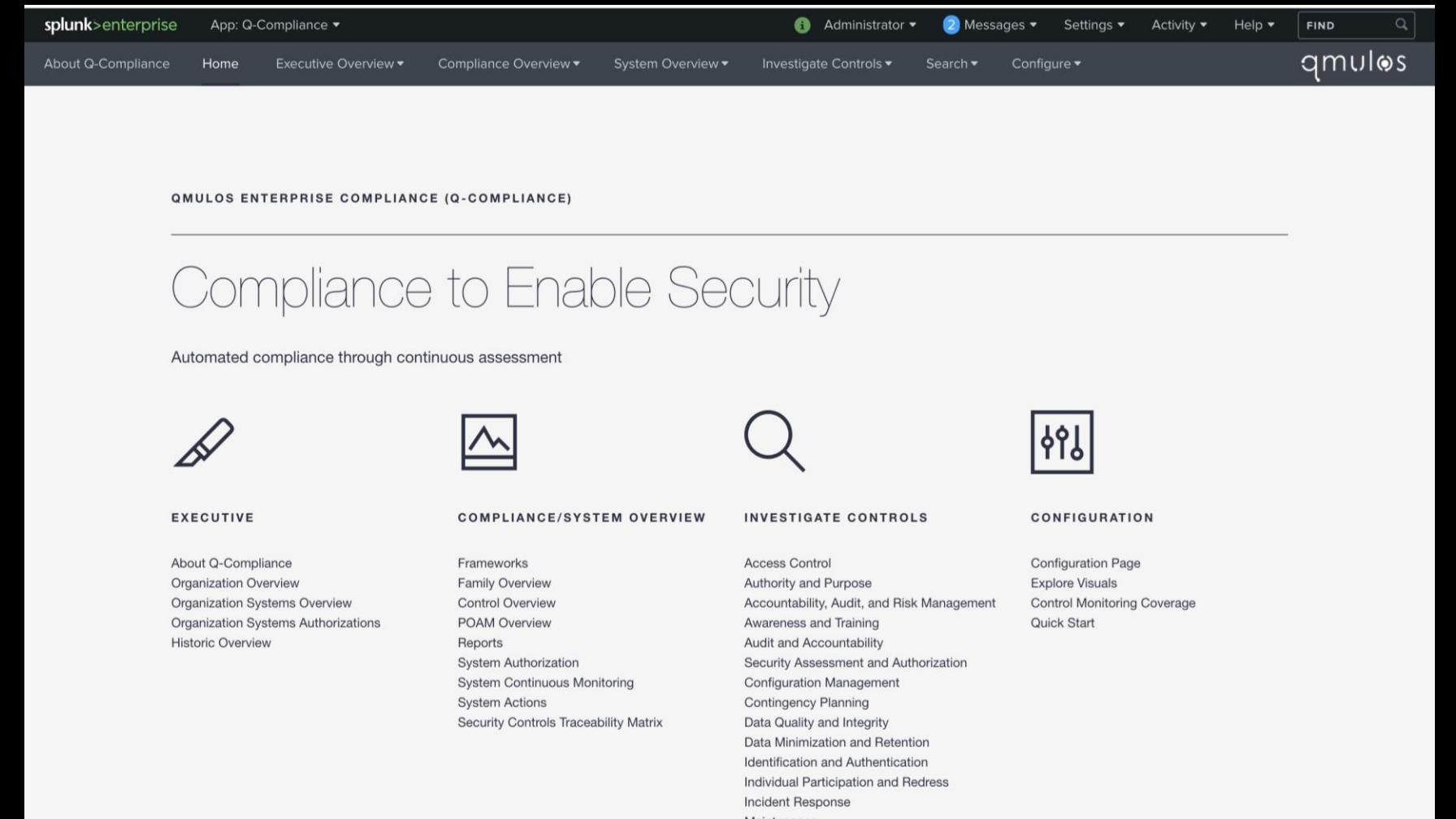
9,085	2,301	7,170
--------------	--------------	--------------

Q-Audit



Q-Compliance





The image shows a screenshot of the Splunk Enterprise Q-Compliance app interface. At the top, there's a navigation bar with links for "About Q-Compliance", "Home", "Executive Overview", "Compliance Overview", "System Overview", "Investigate Controls", "Search", and "Configure". On the right side of the top bar, there are icons for "Administrator", "Messages", "Settings", "Activity", "Help", and search functions. The main title "QMULOS ENTERPRISE COMPLIANCE (Q-COMPLIANCE)" is centered above a large heading "Compliance to Enable Security". Below this, a subtext reads "Automated compliance through continuous assessment". The interface is divided into four main sections: "EXECUTIVE" (with a pen icon), "COMPLIANCE/SYSTEM OVERVIEW" (with a mountain icon), "INVESTIGATE CONTROLS" (with a magnifying glass icon), and "CONFIGURATION" (with a wrench and screwdriver icon). Each section contains a list of related topics or links.

QMULOS

QMULOS ENTERPRISE COMPLIANCE (Q-COMPLIANCE)

Compliance to Enable Security

Automated compliance through continuous assessment

EXECUTIVE

- About Q-Compliance
- Organization Overview
- Organization Systems Overview
- Organization Systems Authorizations
- Historic Overview

COMPLIANCE/SYSTEM OVERVIEW

- Frameworks
- Family Overview
- Control Overview
- POAM Overview
- Reports
- System Authorization
- System Continuous Monitoring
- System Actions
- Security Controls Traceability Matrix

INVESTIGATE CONTROLS

- Access Control
- Authority and Purpose
- Accountability, Audit, and Risk Management
- Awareness and Training
- Audit and Accountability
- Security Assessment and Authorization
- Configuration Management
- Contingency Planning
- Data Quality and Integrity
- Data Minimization and Retention
- Identification and Authentication
- Individual Participation and Redress
- Incident Response
- Maintenance

CONFIGURATION

- Configuration Page
- Explore Visuals
- Control Monitoring Coverage
- Quick Start

Q-Compliance



splunk>enterprise App: Q-Compliance

Administrator 2 Messages Settings Activity Help Find

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

Organization Overview

Organization: Qmulos Score Type: Assessment Hide Filters

Assessment Audit

True Assessment Score (Qmulos)

78.99%

Passing out of the 2704 total applicable controls.

Adjusted Assessment Score (Qmulos)

98.61%

Passing out of the 2166 controls that have been reviewed.

Assessment Review Completion Percentage (Qmulos)

80.10%

2166 out of 2704 controls have been reviewed.

HISTORIC TRUE ASSESSMENT SCORE

A stacked area chart showing the percentage of Passed (green), Failed (red), and Not Audited (grey) controls from Sun Sep 15, 2019, to Wed Oct 9, 2019. The y-axis represents Percentage (%) from 0 to 150. The chart shows a relatively stable distribution with a slight increase in Failed controls towards the end of the period.

HISTORIC ADJUSTED ASSESSMENT SCORE

A stacked area chart showing the percentage of Passed (green) and Failed (red) controls from Sun Sep 15, 2019, to Wed Oct 9, 2019. The y-axis represents Percentage (%) from 0 to 150. The chart shows a high percentage of Passed controls with a small number of Failed controls.

HISTORIC ASSESSMENT REVIEW COMPLETION

A stacked area chart showing the percentage of Reviewed (teal) and Not Reviewed (grey) controls from Sun Sep 15, 2019, to Wed Oct 9, 2019. The y-axis represents Percentage (%) from 0 to 150. The chart shows a high percentage of Reviewed controls with a small number of Not Reviewed controls.

Sub Organization True Assessment Scores

Directly Owned Systems

Q-Compliance





Q-Compliance



splunk>enterprise App: Q-Compliance ▾

Administrator ▾ 2 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

About Q-Compliance Home Executive Overview ▾ Compliance Overview ▾ System Overview ▾ Investigate Controls ▾ Search ▾ Configure ▾

Family Overview

Organization and System Score Type Control Library

Qmulos / Windows Assessment All Hide Filters Audit

Family Scores (Qmulos, Windows)				
Control Library	Name	True Assessment Score	Adjusted Assessment Score	Assessment Percentage Reviewed
NIST 800-53 (Rev. 4)	AC: Access Control	97.22%	97.22%	100.00%
NIST 800-53 (Rev. 4)	AR: Accountability, Audit, and Risk Management	0.00%	0.00%	0.00%
NIST 800-53 (Rev. 4)	AT: Awareness and Training	100.00%	100.00%	100.00%
NIST 800-53 (Rev. 4)	AU: Audit and Accountability	94.74%	100.00%	94.74%
NIST 800-53 (Rev. 4)	CA: Security Assessment and Authorization	90.00%	90.00%	100.00%
NIST 800-53 (Rev. 4)	CM: Configuration Management	90.48%	95.00%	95.24%
NIST 800-53 (Rev. 4)	CP: Contingency Planning	100.00%	100.00%	100.00%
NIST 800-53 (Rev. 4)	IA: Identification and Authentication	87.50%	95.45%	91.67%
NIST 800-53 (Rev. 4)	IR: Incident Response	100.00%	100.00%	100.00%
NIST 800-53 (Rev. 4)	MA: Maintenance	100.00%	100.00%	100.00%
NIST 800-53 (Rev. 4)	MP: Media Protection	100.00%	100.00%	100.00%
NIST 800-53 (Rev. 4)	PE: Physical and Environmental Protection	100.00%	100.00%	100.00%
NIST 800-53 (Rev. 4)	PL: Planning	100.00%	100.00%	100.00%
NIST 800-53 (Rev. 4)	PS: Personnel Security	100.00%	100.00%	100.00%
NIST 800-53 (Rev. 4)	RA: Risk Assessment	100.00%	100.00%	100.00%

Q-Compliance

splunk>enterprise App: Q-Compliance ▾

Administrator ▾ 2 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

About Q-Compliance Home Executive Overview ▾ Compliance Overview ▾ System Overview ▾ Investigate Controls ▾ Search ▾ Configure ▾

Control Overview

Organization and System Control Library Control Category

Qmulus / Windows NIST 800-53 (Rev. 4) ▾ X AC: Access Control ▾ X Hide Filters

Control Name	Audit Status	Assessment Status
AC-01 : Access Control Policy and Procedures	Passed	Passed
AC-02 : Account Management	Failed	Failed
AC-02(01) : Account Management Automated System Account Management	Passed	Passed
AC-02(02) : Account Management Removal of Temporary / Emergency Accounts	Passed	Passed
AC-02(03) : Account Management Disable Inactive Accounts	Passed	Passed
AC-02(04) : Account Management Automated Audit Actions	Failed	Passed
AC-03 : Access Enforcement	Passed	Passed
AC-04 : Information Flow Enforcement	Passed	Passed
AC-05 : Separation of Duties	Passed	Passed
AC-06 : Least Privilege	Passed	Passed
AC-06(01) : Least Privilege Authorize Access to Security Functions	Passed	Passed
AC-06(02) : Least Privilege Non-Privileged Access for Nonsecurity Functions	Passed	Passed
AC-06(05) : Least Privilege Privileged Accounts	Passed	Passed
AC-06(09) : Least Privilege Auditing Use of Privileged Functions	Passed	Passed
AC-06(10) : Least Privilege Prohibit Non-Privileged Users from Executing Privileged Functions	Passed	Passed
AC-07 : Unsuccessful Logon Attempts	Passed	Passed

Q-Compliance



AC-02 | ACCOUNT MANAGEMENT

AUDIT STATUS

FAILED

ASSESSMENT STATUS

FAILED

CONTROL RECORDS | POAMS | TEST PROCEDURES | IMPLEMENTATION STATEMENTS ... (CLICK TO SELECT)

Control Record	Updated By	Updated On
I did that manual thing.	admin	05/03/2019 15:01:13.9
Monitored technical indicators for control AC-02	admin	03/21/2019 09:35:27.75
Monitored technical indicators for control AC-02	adm-swhipkey	03/20/2019 13:13:22.69
I reviewed.	admin	03/11/2019 14:56:45.89
I reviewed the acct mgr list.	admin	02/22/2019 10:28:47.04

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

[Add Record](#)

ACCOUNT MANAGEMENT INDICATORS

135 Accounts Managed ▲ 135

compared to last month

30 Accounts Created ▲ 30

compared to last month

31 Accounts Deleted ▲ 31

compared to last month

13 Accounts Disabled ▲ 13

compared to last month

ACCOUNT MANAGEMENT OVER TIME BY APP

TOP ACCOUNT MANAGERS BY ACTION

User	created	deleted	enabled	modified	sus...ded
fred_lim	10	5	2	15	10
sergei_lahv	5	2	1	10	5
chodray_gosh	15	5	2	10	5
greg_lee	10	5	2	15	5
vincent_seef	5	2	1	10	5
sam_bhatnagar	10	5	2	15	5
johnny_liu	5	2	1	10	5
alfred_ian	10	5	2	15	5
mimi_nguyen	5	2	1	10	5

TOP ACTIONS BY ACCOUNT TYPE

Action	group	user
modified	100	80
deleted	20	20
created	20	20
enabled	10	10

Q-Compliance



Add Record

ACCOUNT MANAGEMENT ACTIVITY BY ACTION

Click On Line for Detail View



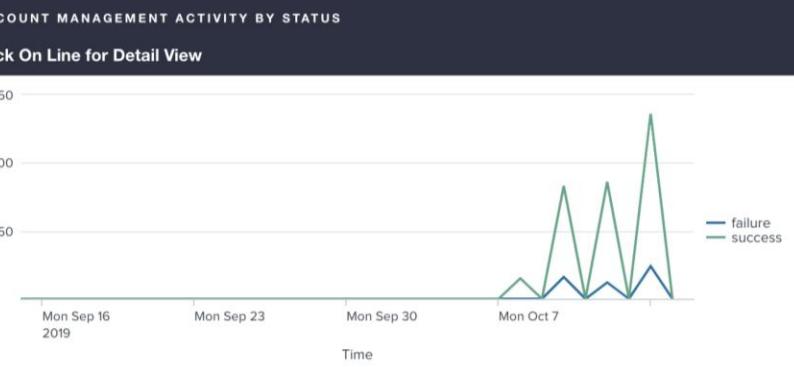
Count

Time

- created
- deleted
- enabled
- modified
- suspended

ACCOUNT MANAGEMENT ACTIVITY BY STATUS

Click On Line for Detail View



Count

Time

- failure
- success

SECURITY SCAN STATISTICS (CLICK ON STATS FOR ADDITIONAL DETAILS)
100.00%
Passing Results
0.00%
Failing Results
0.00%
Other Results

ASSIGNED EVIDENCE

File Name	Content Type	Content Size	Description	Assigned	Assigned By	Uploaded	Uploaded By
new screenshot	link	0	www.dos.gov	2018-07-12 10:25:46	admin	2018-07-12 10:25:46	admin

EVIDENCE MANAGEMENT

Select from existing evidence:

Previously uploaded evidence

Upload new evidence:

Q-Compliance



splunk>enterprise App: Q-Compliance Administrator 2 Messages Settings Activity Help Find

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

Historic Overview

Organization and System Score Type Assessment Audit Last 30 days Hide Filters

HISTORIC TREND INDICATORS

260 Controls Reviewed 1 **255** Controls Passed 0 **5** Controls Failed 1 **19** Controls Remaining 1

Historic True Assessment Score

Percentage (%) Date

Historic Adjusted Assessment Score

Percentage (%) Date

Historic Assessment Review Completion

Percentage (%) Date

True Assessment Score Breakdown

300 Date

Adjusted Assessment Score Breakdown

300 Date

Assessment Review Completion Breakdown

300 Date

Q-Compliance

splunk>enterprise App: Q-Compliance

About Q-Compliance Home Executive Overview Compliance Overview System Overview Investigate Controls Search Configure

Administrator 2 Messages Settings Activity Help FIND

qmulos

Framework Scorecards

ENTERPRISE OPPORTUNITIES ▾ FEDRAMP ▾ CUI SECURITY REQUIREMENTS ▾ CIS CRITICAL SECURITY CONTROLS ▾

NIST CYBER SECURITY FRAMEWORK ▾ CJIS SECURITY POLICIES ▾ HIPAA ▾ PCI DSS ▾

QMULOS TOP 5 ▾ BASIC CYBER HYGIENE ▾

Q-Compliance



The image shows a tablet displaying the Splunk Enterprise Q-Compliance app. The top navigation bar includes 'splunk>enterprise' and 'App: Q-Compliance'. On the right, there are links for 'Administrator', 'Messages' (with 2 notifications), 'Settings', 'Activity', 'Help', and search/filter options. The main content area is titled 'System Authorization' under 'Organization and System'. It shows a green button for 'Qmulos / Windows' and a 'Hide Filters' link. A large green circle with a checkmark indicates 'Status: Authorized'. Below it, details are listed: Issued by: adm-tieu, Issued on: 2019-10-15, Expires: 2020-10-14, and a note '(Click Icon/Text for Details)'. A section for 'PAST AUTHORIZATIONS' is shown with a table header and a message: 'No past system authorizations for the current system found.' The bottom section, 'SECURITY ASSESSMENT INFORMATION', displays three large boxes: 'True Assessment Score' at 91.40%, 'Adjusted Assessment Score' at 98.08%, and 'Assessment Review Completion Percentage' at 93.19%. Below these are dropdown menus for 'All Libraries' and 'All Categories'. At the bottom, a grid of compliance items is shown in colored boxes: AC-01 (green), AC-02 (red), AC-02(01) (green), AC-02(02) (green), AC-02(03) (green), AC-02(04) (green), AC-03 (green), AC-04 (green), AC-05 (green), AC-06 (green), AC-06(01) (green), AC-06(02) (green), AC-06(05) (green), AC-06(09) (green), AC-06(10) (green), AC-07 (green), AC-08 (green), AC-10 (green), AC-11 (green), AC-11(01) (green), AC-12 (green), AC-14 (green), AC-17 (green), AC-17(01) (green), AC-17(02) (green), AC-17(03) (green), AC-17(04) (green), AC-18 (green), AC-18(01) (green), AC-19 (green), AC-19(05) (green), AC-20 (green), AC-20(01) (green), AC-20(02) (green), AC-21 (green), AC-22 (green), AC-24 (yellow), AT-01 (green), AT-02 (green), AT-03 (green), AT-04 (green), AT-05 (green), AT-06 (green), AT-07 (green), and AT-08 (green).

Q-Compliance



splunk>enterprise App: Q-Compliance

Administrator 2 Messages Settings Activity Help Find

About Q-Compliance Home Executive Overview Compliance Overview System Overview Investigate Controls Search Configure

System Continuous Monitoring

Organization and System Score Type Time Selector

Qmulos / Windows Assessment Audit Last 7 days Hide Filters

AU-02 CM-06 CM-08 CSM HWAM

IA-02 IR-06 RA-05 SWAM VUL

AU-02 | AUDIT EVENTS

KEY AUDIT STATISTICS

56Hosts ↑ Compared to yesterday **61Sourcetypes ↗** Compared to yesterday **123Eventtypes ↗** Compared to yesterday

DEMOGRAPHICS OF SOURCES BEING COLLECTED

Sourcetype	Host Count	Event Count	Last Seen
audittrail	9	374713	10/15/2019 15:36:32
splunkd_access	2	417110	10/15/2019 15:36:32

TOP SOURCETYPES OVER TIME BY COUNT

MSAD:GPO
WinEventLog
app_eventgen
asset_inventory
audit_ch_ventgen
audittrail

Q-Compliance

System Actions Page

Organization and System

Qmulos / Windows Hide Filters

ITEMS REQUIRING ACTION

35	8	5	2	273	271
Alerts Triggered This Week	Controls Failing Audit	Controls Failing Assessment	POAMs Overdue	Audits Overdue	Assessments Overdue

Control Monitoring Overdue 270

COMPLIANCE INDICATORS

0	90%	91%	96%	98%	279
Tickets Created This Week	True Audit Score	True Assessment Score	Adjusted Audit Score	Adjusted Assessment Score	Total Applied Controls

1	1	0	0
POAMs Created This Week	Controls Reviewed This Week	Evidence Added This Week	SSPs Generated This Week

Q-Compliance



splunk>enterprise App: Q-Compliance ▾

Administrator ▾ 2 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

About Q-Compliance Home Executive Overview ▾ Compliance Overview ▾ System Overview ▾ Investigate Controls ▾ Search ▾ Configure ▾ **qmulos**

Security Controls Traceability Matrix

Organization and System	Control Library	Control Category	Applicability Type	Implementation Statement	Audit Status
Qmulos / Windows	All	All	All	All	All
Assessment Status	Test Results				
All	All	Hide Filters			

Show/hide additional fields: Justification Implementation Summary Audit Findings Assessment Findings

SECURITY CONTROLS TRACEABILITY MATRIX

Security Controls Traceability Matrix

Control Name	Control Title	Subcontrol	CCI	Applicability Type	Control Provider	Implementation Status	Audit Status	Assessment Status	Test Case	Test Results
AC-01	Access Control Policy and Procedures			Hybrid	Policy	As Planned	Passed	Passed	Testing this hybrid control Review procedures only.	Passed
AC-01	Access Control Policy and Procedures	AC-01 a 1	CCI-000001	Hybrid	Policy		Passed			
AC-02	Account Management			Tailored	N/A		Failed	Failed		
AC-02	Account Management	AC-02 a	CCI-002110	Tailored	N/A		Passed	1234		Passed
AC-02	Account Management	AC-02 a	CCI-002111	Tailored	N/A		Failed			
AC-02	Account Management	AC-02 b	CCI-002112	Tailored	N/A		Passed			
AC-02	Account Management	AC-02 c	CCI-002113	Tailored	N/A		Failed			

Q-Compliance

CONFIGURATION PAGE

SYSTEM MANAGEMENT

Manage system baselines and asset inventory.

CONTROL CONFIGURATION

View Control notes and applicability.

ORGANIZATION-DEFINED PARAMETERS

Configure organization-defined parameters.

OVERLAY MANAGEMENT

Create and customize overlays.

CONTROL LIBRARY MANAGEMENT

Manage control definitions and visualizations.

ALERTING

Edit existing alerts.

ORGANIZATION AND SYSTEM SETUP

Create or remove organizations and systems.

USER ORGANIZATION MANAGEMENT

Select what organizations users can see.

VULNERABILITY MANAGEMENT

Manage Vulnerabilities

EXPLORE VISUALS

Explore technical evidence panels

DEVICE RECORD MANAGEMENT

Manage Device Records

USER RECORD MANAGEMENT

Manage User Records

<https://products.qmulos.com:9443/en-US/app/Q-Compliance/Configuration#>

Q-Compliance



splunk>enterprise App: Q-Compliance

Administrator Messages Settings Activity Help Find

About Q-Compliance Home Executive Overview Compliance Overview System Overview Investigate Controls Search Configure

qmulos

Control Monitoring Coverage Dashboard

Control Library Control Category

Select a Control Library All Hide Filters

Control	Monitoring Status	Enhancement Monitoring Statuses
AC-01: Access Control Policy and Procedures	●	
AC-02: Account Management	●	AC-02(01) AC-02(02) AC-02(03) AC-02(04) AC-02(05) AC-02(06) AC-02(07) AC-02(08) AC-02(09) AC-02(10) AC-02(11) AC-02(12) AC-02(13)
AC-02(02) Configured Visualizations		Data Status
Recently Created Temporary Accounts		● no data
Temporary Accounts Expiring Over Time		● no data
Temporary Account Disablement		● has data
SECURITY SCAN STATISTICS (CLICK ON STATS FOR ADDITIONAL DETAILS)		
AC-03: Access Enforcement	●	AC-03(02) AC-03(03) AC-03(04) AC-03(05) AC-03(07) AC-03(08) AC-03(09) AC-03(10)
AC-04: Information Flow Enforcement	●	AC-04(01) AC-04(02) AC-04(03) AC-04(04) AC-04(05) AC-04(06) AC-04(07) AC-04(08) AC-04(09) AC-04(10) AC-04(11) AC-04(12) AC-04(13) AC-04(14) AC-04(15) AC-04(17) AC-04(18) AC-04(19) AC-04(20) AC-04(21) AC-04(22)
AC-05: Separation of Duties	●	
AC-06: Least Privilege	●	AC-06(01) AC-06(02) AC-06(03) AC-06(04) AC-06(05) AC-06(06) AC-06(07) AC-06(08) AC-06(09) AC-06(10)

Q-Compliance



splunk>enterprise App: Q-Compliance ▾

Administrator ▾ 2 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find qmulos

About Q-Compliance Home Executive Overview ▾ Compliance Overview ▾ System Overview ▾ Investigate Controls ▾ Search ▾ Configure ▾

POAM Overview

Organization and System Time Selector

Qmulos / All Systems Last 90 days Hide Filters

POAM STATUS INDICATORS

Status	Count	Description
Overdue	14	Out of Total
Open	8	Out of Total
In-Progress	8	Out of Total
Closed	5	Out of Total

Overdue Breakdown by Risk Level

Risk Level	Count
High	4
Moderate	5
Low	5

Open Status Breakdown by Risk Level

Risk Level	Count
High	4
Moderate	3
Low	1

In-Progress Status Breakdown by Risk Level

Risk Level	Count
High	4
Moderate	3
Low	1

Closed Status Breakdown by Risk Level

Risk Level	Count
High	3
Low	2

MILESTONE INDICATORS

Milestone Type	Count	Description
Milestones	4	Total
Overdue	2	Out of Total
Completed	0	Out of Total
In-Progress	4	Out of Total

Q-Compliance

