.conf18 splunk>

Enabling Your Mission Through Automated Alignment With NIST's Risk Management Framework

or Your Framework!

Steve Vetter | Cisco Federal Strategist and Senior Strategic Solution Executive

Rutger Thomschutz | Qmulos Director of Technical Engagements

October 2018 | Orlando, Florida

Forward-Looking Statements

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 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.

Rutger Thomschutz

Qmulos Director of Technical Engagements

- 13 Years consulting
- Splunking for 5 years, last 3 as Splunk PS
- 4th .Conf

Steve Vetter

Cisco Federal Strategist and Senior Strategic Solution Executive

- 15+ Years of IT industry strategic leadership experience
- Retired Naval Intelligence Commander
- .Conf Virgin

Agenda

Proactive, Compliant Security

The FOUNDATION - Fundamental Transformative Drivers are Here!

- Explosion of Devices and Data
- Dynamic Evolving Threats

The MEANS – Mission Enablement with Data and Security Frameworks

- NIST Risk Management and Cybersecurity Management Frameworks
- Pragmatic Mission Accomplishment
  - Not just *“actionable insights”*, but *“automated security and compliance”* driven by insights
- Machine learning (AI) are Game Changers for Network and Security Automation

The OUTCOME – Automated Framework Alignment to Assure the Mission

- Framework Alignment and Automation
- Compliance Reporting and Tracking

The Foundation

Fundamental Transformative Drivers are Here!

Keys to Mission and Business Success

Technology is Changing

The unstoppable fundamentals!

- Connected devices and sensors are skyrocketing
  - Consumerization of IT – NextGen! (and OT/IIoT/FRCS)
- Data is exploding
- The “Cyber-Physical Systems” of the 4th Industrial Revolution are arriving

Of increasing importance…

- Cloud / Containers / Mobility / IoT / Big Data and Analytics / The Edge

Security Threat Landscape

Security is Transforming

Cybersecurity threat and potential adverse impact have never been greater

- Need (and expectation) to connect / communicate / collaborate is exploding and essential to enhance mission / business outcomes
- Increased availability and number of attack surfaces and attack vectors (cloud / IoT / edge)
- Availability of automated and compromised tools, vulnerabilities and knowledge
  - *Shadow Brokers:* Double Pulsar / Eternal Blue, Meltdown, Spectre, etc.
- Rapidly evolving, dynamic nature of the threat

Creates the need for:

- Real-time visibility across the entire network and support infrastructure
  - And the data and applications that ride across them
- Real-time enforcement of network policies for security and performance
- Ability to dynamically change the network – especially in response to anomalous behavior
- Zero Trust Security

The Means

Mission Enablement with Data and Security Frameworks

It Takes a Team!

splunk> + cisco + qmulos

Data Doesn't Lie

IN ADDITION TO ISO 9000, WE WILL STRIVE TO BE QS-9000 COMPLIANT.
scottadams@aol.com
www.dilbert.com
THAT MEANS FALSIFYING THE FOLLOWING DOC-UMENTS: QSR, APQP, FMEA, MSA, SPC, PPAP AND QSA.
© 1999 United Feature Syndicate, Inc.
11/29/99
REMEMBER, YOU CAN'T SPELL COMPLIANCE WITHOUT "LIANCE."

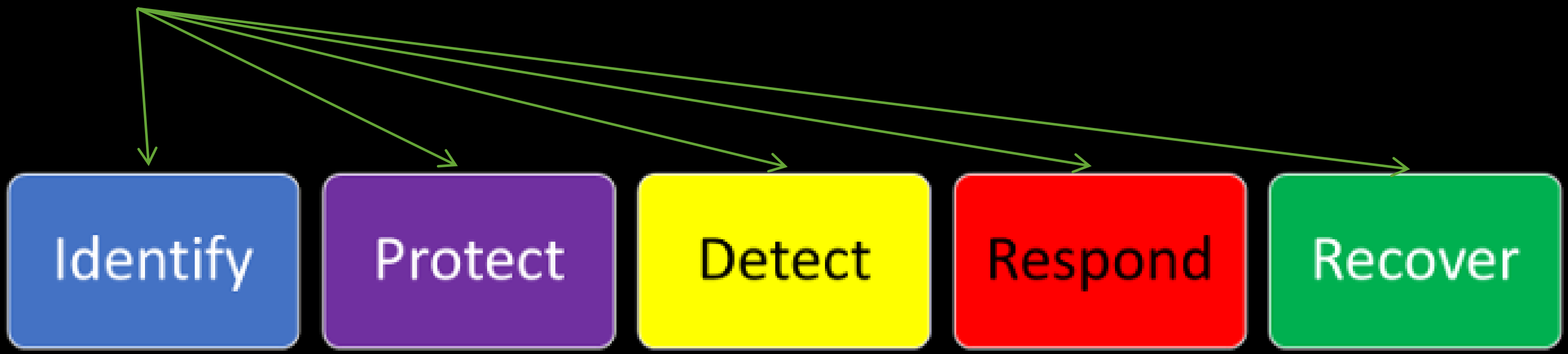
But how much does it really help?

The NIST CyberSecurity Framework

Enables More Effective Management of Risk

- **What:** Prioritized, flexible, repeatable, performance-based, cost-effective approach
- **Goal:** Identify, assess and manage cyber risks
- Business drivers guide cyber resources and activities to help manage risk
- **3 parts:** Framework Core / 4 Maturity Tiers / Your Profile
  - Core alignment with business requirements, risk tolerance and organizational resources
- Adaptable to IT / IoT / ICS / CPS

The Core:



Identify

Protect

Detect

Respond

Recover

It's FLEXIBLE……and it's NOT a Checklist!!!

Mission Enablement with Pragmatic RMF Compliance

The Means – from a Splunk “Leading Data Analytics Platform” Perspective

“Real-time” operational intelligence becomes “real-time” operational actions

- Splunk’s real-time data insights are operationalized by Cisco’s security and networking technologies and Qmulos’ RMF technical compliance controls real-time reporting and streamlining capabilities

Take Splunk’s capabilities to the next level

- Automation doesn’t just “alert,” it RESOLVES performance and security issues
- Real-time actions to ensure performance, availability AND SECURITY

Can operationalize network microsegmentation and real-time response to dynamic security threats

Actionable insights still require action!

Key Networking and Security Factors

Performance

Scale

Security

Scale
Performance
Security

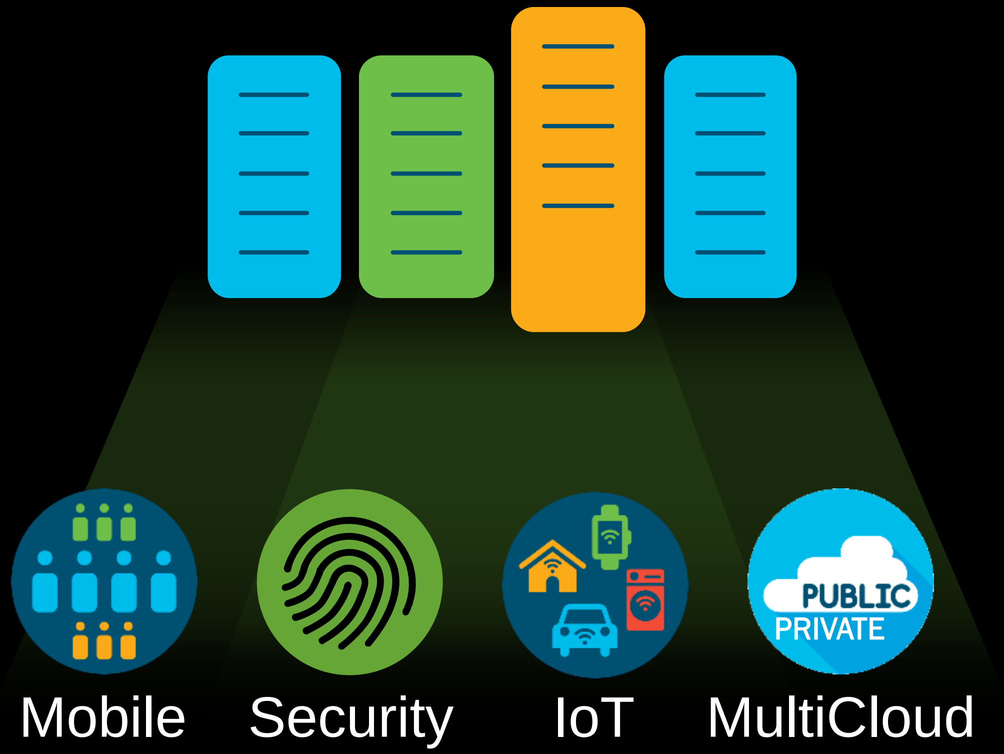
Performance at Scale with Security

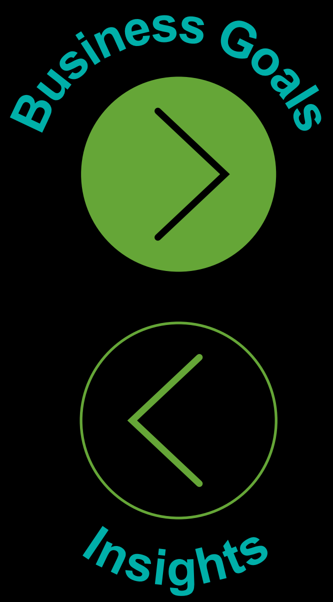
- **The Means:** Automation / Machine Learning (AI) / Intent-Based Networking
- **The Benefits:** Network Consolidation / Enhanced Security / Savings

These are game changers for mission and security!

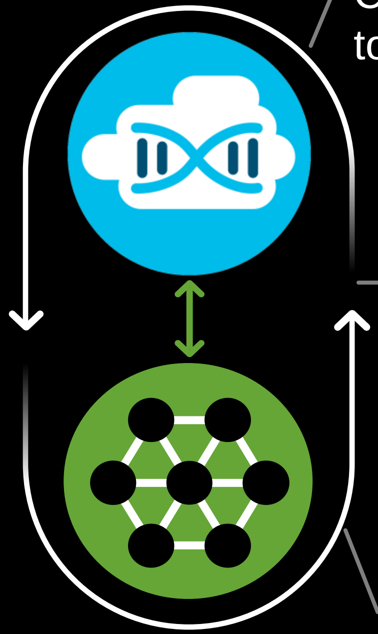
Intent-Based Networking

Digital Mission & Business





Network



Translation & Validation

Captures business intent, translates to policies, and check integrity

The “what” to the “how”

Activation & Awareness

Orchestrate policies & configures systems automatically

Performs the “how” / Context
Real time network status

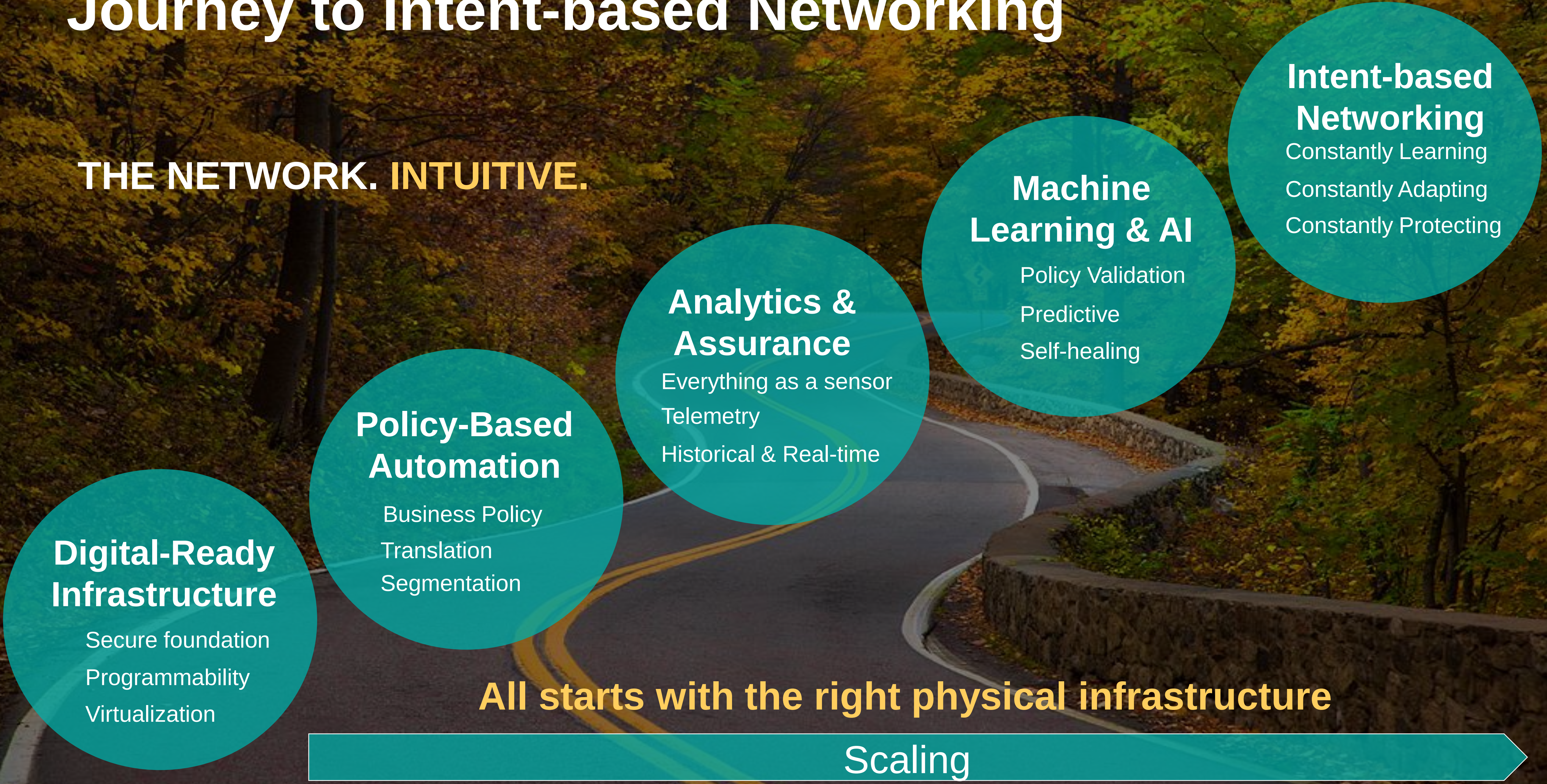
Dynamic Assurance

Continuous verification, visibility - corrective / proactive actions

The “how” is doing the “what”

Journey to Intent-based Networking

THE NETWORK. INTUITIVE.



Digital-Ready Infrastructure

Secure foundation

Programmability

Virtualization

Policy-Based Automation

Business Policy

Translation

Segmentation

Analytics & Assurance

Everything as a sensor

Telemetry

Historical & Real-time

Machine Learning & AI

Policy Validation

Predictive

Self-healing

Intent-based Networking

Constantly Learning

Constantly Adapting

Constantly Protecting

All starts with the right physical infrastructure

Scaling

Comprehensive Network Traffic and Data Visibility

Full NetFlow is Key to Comprehensive Internal Network Visibility

Sampled = Partial

- Subset of traffic, usually less than 5%
- Gives a snapshot view into network activity
- Similar to reading every 20th page of a book

Full Netflow = All packets

- All traffic is collected
- Provides a comprehensive view into all activity on the network
- Equivalent to reading every word on every page of a book

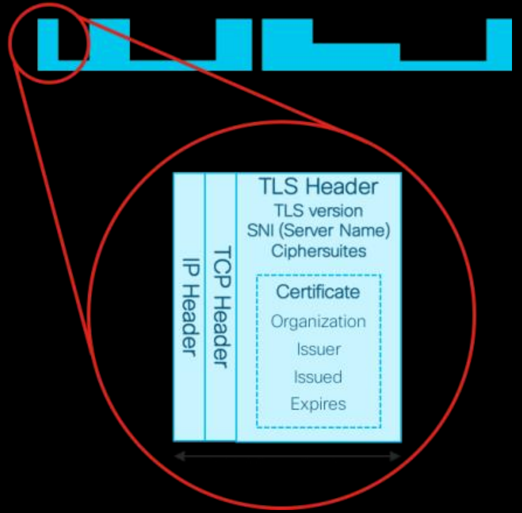
Sampling is sufficient for network performance, but not for security

Encrypted Traffic Analytics

The Future is Already Here

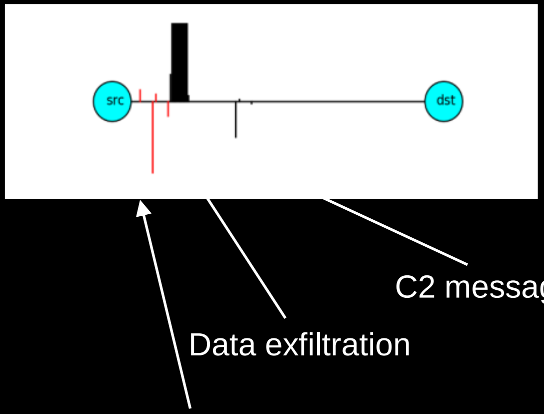
Initial Data Packet

Make the most of the unencrypted fields



Sequence of Packet Lengths and Times

Identify the content type through the size and timing of packets



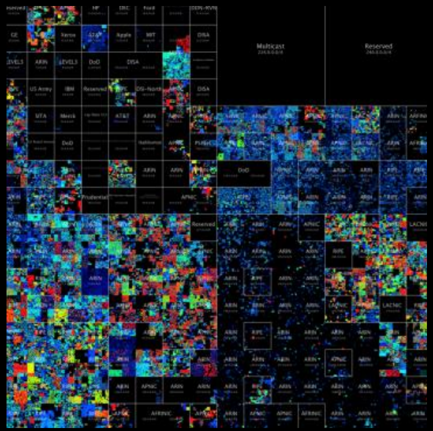
C2 message

Data exfiltration

Self-Signed certificate

Threat Intelligence Map

Who’s who of the Internet’s dark side



Key Takeaways

Our world is undergoing fundamental (and unstoppable) transformations

- Consumerization of IT – NextGen
- IoT / IIoT / OT
- Threat
- Technology advances
- Data

But how to harness these drivers for business and mission success?

- What data is optimal for Splunk to enhance organizational outcomes?
- What role does automation play and where?

The Potential: We can take the high ground back from adversaries

The Outcome

Automated Framework Alignment to Assure the Mission

The Outcome

It Takes a Team!

splunk>® + cisco + qmulos

Real-World Solution

Solving the Medical Device Security Challenge

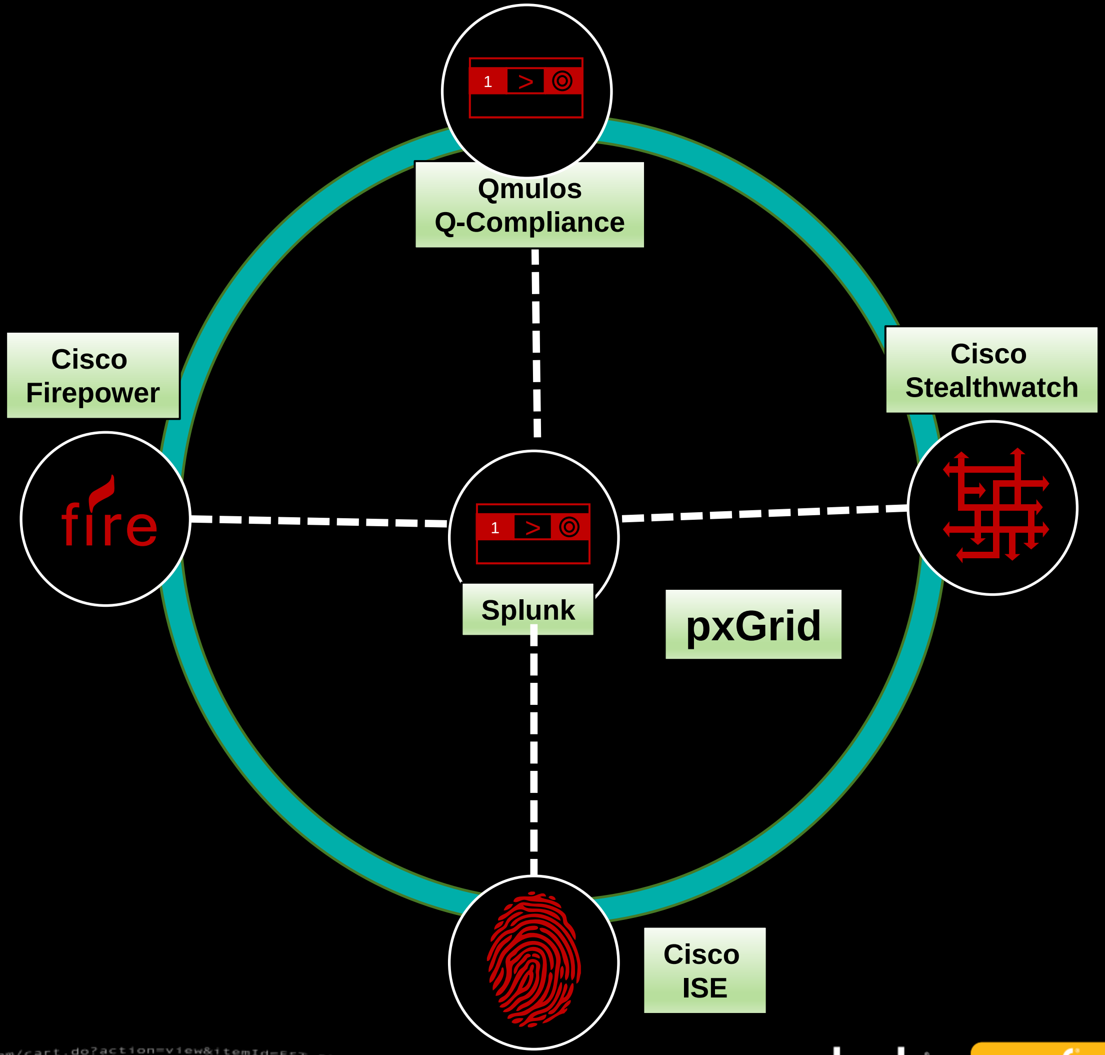
Medical provider

Adopted the trifecta

Automatically identify, classify and secure assets connected to the network

Dynamically change security controls based on vulnerabilities and threats

Stop complex threats faster



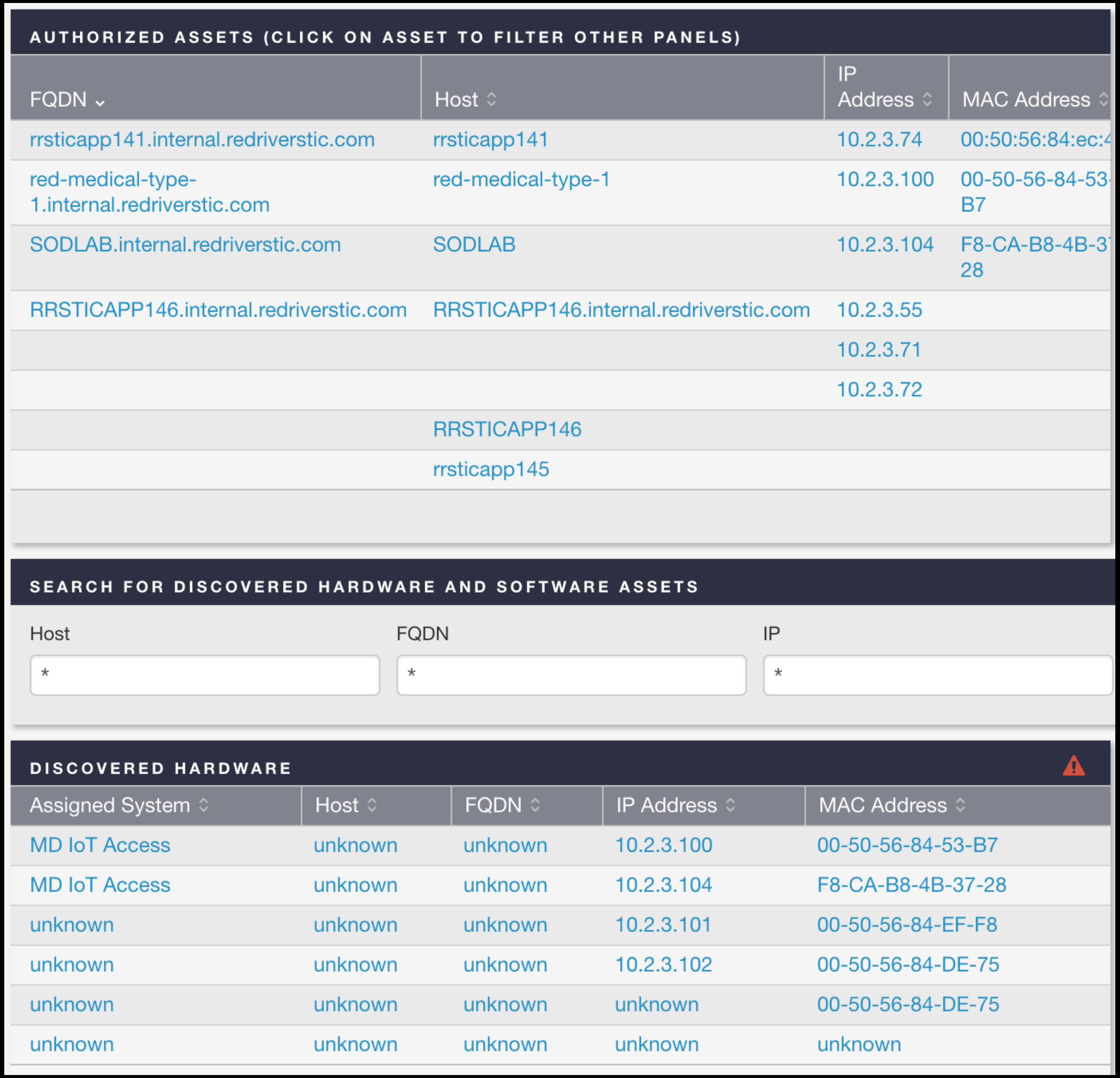
Asset Discovery

CM-08 Information System Component Inventory

Must discover all assets on the network

- Cisco’s Identity Services Engine (ISE) does this

Q-Compliance displays authorized and discovered assets



AUTHORIZED ASSETS (CLICK ON ASSET TO FILTER OTHER PANELS)

FQDN ⌄	Host ⇕	IP Address ⇕	MAC Address ⇕
rrsticapp141.internal.redriverstic.com	rrsticapp141	10.2.3.74	00:50:56:84:ec:4
red-medical-type-1.internal.redriverstic.com	red-medical-type-1	10.2.3.100	00-50-56-84-53-B7
SODLAB.internal.redriverstic.com	SODLAB	10.2.3.104	F8-CA-B8-4B-37-28
RRSTICAPP146.internal.redriverstic.com	RRSTICAPP146.internal.redriverstic.com	10.2.3.55	
		10.2.3.71	
		10.2.3.72	
	RRSTICAPP146		
	rrsticapp145		

SEARCH FOR DISCOVERED HARDWARE AND SOFTWARE ASSETS

Host: *

FQDN: *

IP: *

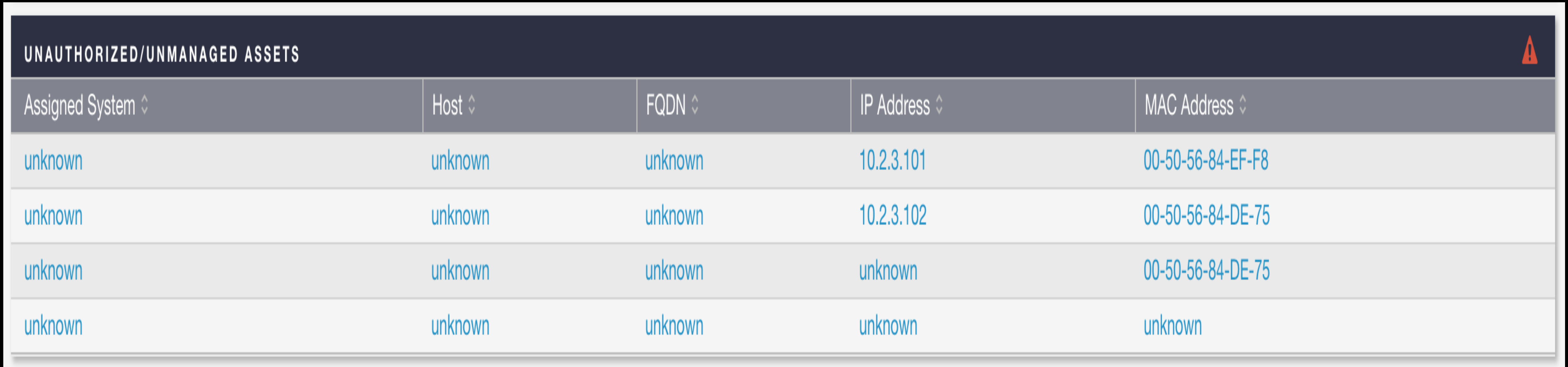
DISCOVERED HARDWARE

Assigned System ⇕	Host ⇕	FQDN ⇕	IP Address ⇕	MAC Address ⇕
MD IoT Access	unknown	unknown	10.2.3.100	00-50-56-84-53-B7
MD IoT Access	unknown	unknown	10.2.3.104	F8-CA-B8-4B-37-28
unknown	unknown	unknown	10.2.3.101	00-50-56-84-EF-F8
unknown	unknown	unknown	10.2.3.102	00-50-56-84-DE-75
unknown	unknown	unknown	unknown	00-50-56-84-DE-75
unknown	unknown	unknown	unknown	unknown

Asset Discovery (Cont.)

CM-08(03) Information System Component Inventory
Automated Unauthorized Component Detection

Q-Compliance displays unmanaged/unauthorized assets discovered by ISE



UNAUTHORIZED/UNMANAGED ASSETS

Assigned System	Host	FQDN	IP Address	MAC Address
unknown	unknown	unknown	10.2.3.101	00-50-56-84-EF-F8
unknown	unknown	unknown	10.2.3.102	00-50-56-84-DE-75
unknown	unknown	unknown	unknown	00-50-56-84-DE-75
unknown	unknown	unknown	unknown	unknown

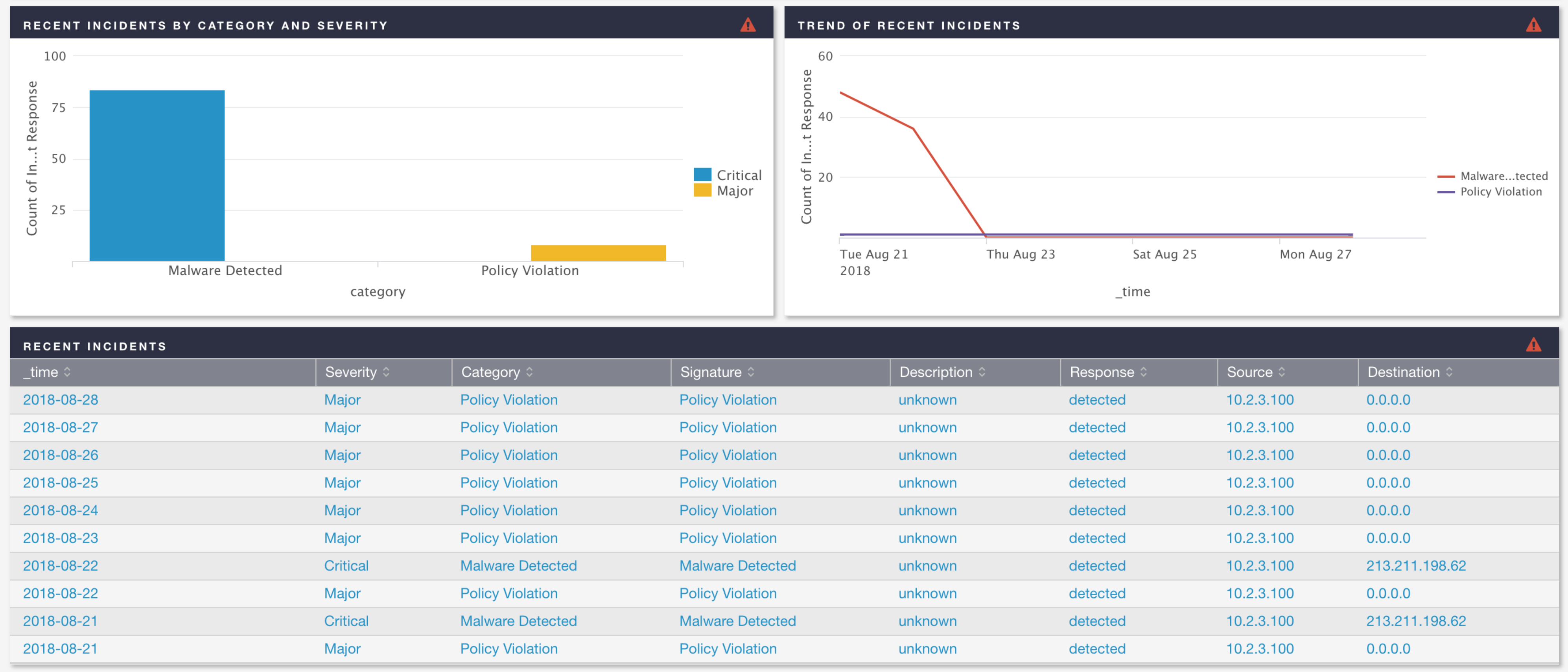
Monitoring Assets

IR-06 Incident Reporting

StealthWatch monitors assets/network for threats, malicious activity, incidents, etc.

- Direct integration into ISE for real-time response to anomalous / malicious activity

Q-Compliance displays any discovered incidents, attacks



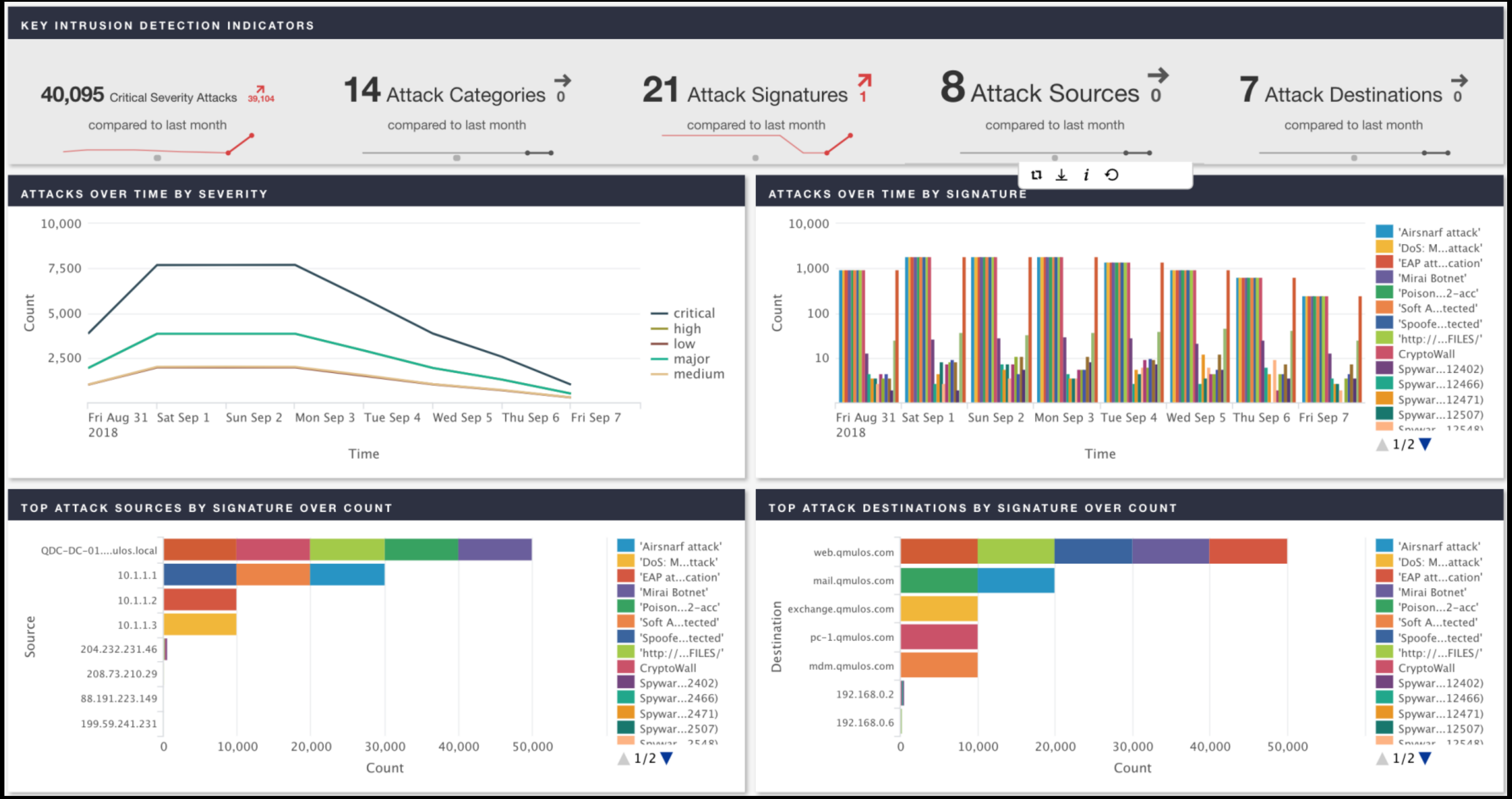
RECENT INCIDENTS

_time	Severity	Category	Signature	Description	Response	Source	Destination
2018-08-28	Major	Policy Violation	Policy Violation	unknown	detected	10.2.3.100	0.0.0.0
2018-08-27	Major	Policy Violation	Policy Violation	unknown	detected	10.2.3.100	0.0.0.0
2018-08-26	Major	Policy Violation	Policy Violation	unknown	detected	10.2.3.100	0.0.0.0
2018-08-25	Major	Policy Violation	Policy Violation	unknown	detected	10.2.3.100	0.0.0.0
2018-08-24	Major	Policy Violation	Policy Violation	unknown	detected	10.2.3.100	0.0.0.0
2018-08-23	Major	Policy Violation	Policy Violation	unknown	detected	10.2.3.100	0.0.0.0
2018-08-22	Critical	Malware Detected	Malware Detected	unknown	detected	10.2.3.100	213.211.198.62
2018-08-22	Major	Policy Violation	Policy Violation	unknown	detected	10.2.3.100	0.0.0.0
2018-08-21	Critical	Malware Detected	Malware Detected	unknown	detected	10.2.3.100	213.211.198.62
2018-08-21	Major	Policy Violation	Policy Violation	unknown	detected	10.2.3.100	0.0.0.0

Monitoring Assets (Cont.)

SI-04 Information System Monitoring

Discover incidents and attacks



KEY INTRUSION DETECTION INDICATORS

40,095 Critical Severity Attacks ↗ 39,104 compared to last month

14 Attack Categories → 0 compared to last month

21 Attack Signatures ↗ 1 compared to last month

8 Attack Sources → 0 compared to last month

7 Attack Destinations → 0 compared to last month

ATTACKS OVER TIME BY SEVERITY

ATTACKS OVER TIME BY SIGNATURE

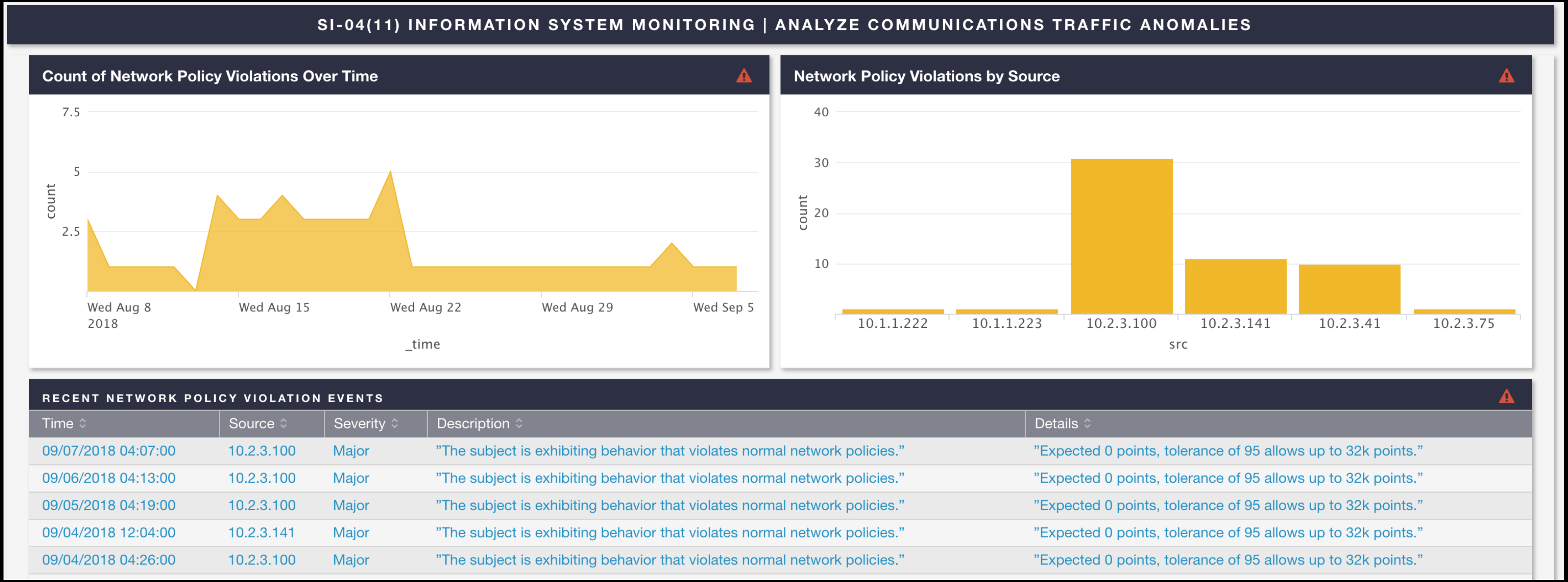
TOP ATTACK SOURCES BY SIGNATURE OVER COUNT

TOP ATTACK DESTINATIONS BY SIGNATURE OVER COUNT

Monitoring Assets (Cont.)

SI-04(11) Information System Monitoring | Analyze Communications Traffic Anomalies

Additionally, Q-Compliance shows any anomalies detected by StealthWatch

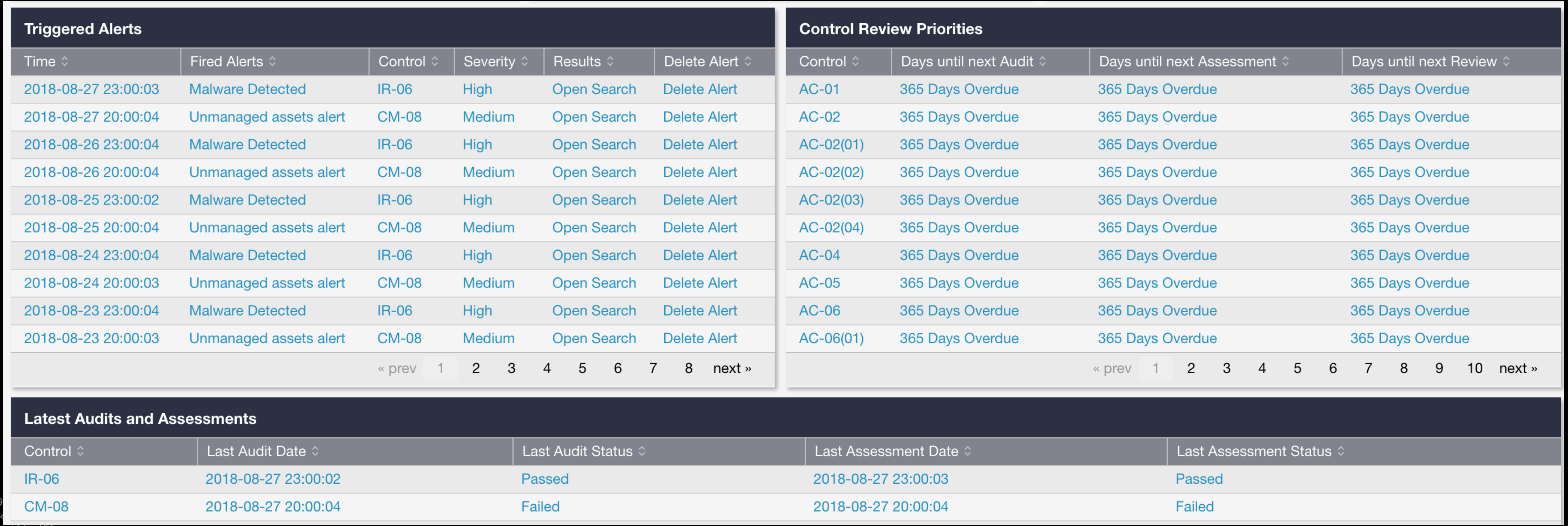

SI-04(11) INFORMATION SYSTEM MONITORING | ANALYZE COMMUNICATIONS TRAFFIC ANOMALIES
Count of Network Policy Violations Over Time
7.5
5
2.5
count
Wed Aug 8 2018
Wed Aug 15
Wed Aug 22
Wed Aug 29
Wed Sep 5
_time
Network Policy Violations by Source
40
30
20
10
count
10.1.1.222
10.1.1.223
10.2.3.100
10.2.3.141
10.2.3.41
10.2.3.75
src
RECENT NETWORK POLICY VIOLATION EVENTS

Time ⇕	Source ⇕	Severity ⇕	Description ⇕	Details ⇕
09/07/2018 04:07:00	10.2.3.100	Major	"The subject is exhibiting behavior that violates normal network policies."	"Expected 0 points, tolerance of 95 allows up to 32k points."
09/06/2018 04:13:00	10.2.3.100	Major	"The subject is exhibiting behavior that violates normal network policies."	"Expected 0 points, tolerance of 95 allows up to 32k points."
09/05/2018 04:19:00	10.2.3.100	Major	"The subject is exhibiting behavior that violates normal network policies."	"Expected 0 points, tolerance of 95 allows up to 32k points."
09/04/2018 12:04:00	10.2.3.141	Major	"The subject is exhibiting behavior that violates normal network policies."	"Expected 0 points, tolerance of 95 allows up to 32k points."
09/04/2018 04:26:00	10.2.3.100	Major	"The subject is exhibiting behavior that violates normal network policies."	"Expected 0 points, tolerance of 95 allows up to 32k points."

splunk> .conf18

Alerting

In Q-Compliance, set up an alert (e.g. AC-03) to notify the system owners on the System Actions dashboard



Triggered Alerts

Time	Fired Alerts	Control	Severity	Results	Delete Alert
2018-08-27 23:00:03	Malware Detected	IR-06	High	Open Search	Delete Alert
2018-08-27 20:00:04	Unmanaged assets alert	CM-08	Medium	Open Search	Delete Alert
2018-08-26 23:00:04	Malware Detected	IR-06	High	Open Search	Delete Alert
2018-08-26 20:00:04	Unmanaged assets alert	CM-08	Medium	Open Search	Delete Alert
2018-08-25 23:00:02	Malware Detected	IR-06	High	Open Search	Delete Alert
2018-08-25 20:00:04	Unmanaged assets alert	CM-08	Medium	Open Search	Delete Alert
2018-08-24 23:00:04	Malware Detected	IR-06	High	Open Search	Delete Alert
2018-08-24 20:00:03	Unmanaged assets alert	CM-08	Medium	Open Search	Delete Alert
2018-08-23 23:00:04	Malware Detected	IR-06	High	Open Search	Delete Alert
2018-08-23 20:00:03	Unmanaged assets alert	CM-08	Medium	Open Search	Delete Alert

« prev 1 2 3 4 5 6 7 8 next »

Control Review Priorities

Control	Days until next Audit	Days until next Assessment	Days until next Review
AC-01	365 Days Overdue	365 Days Overdue	365 Days Overdue
AC-02	365 Days Overdue	365 Days Overdue	365 Days Overdue
AC-02(01)	365 Days Overdue	365 Days Overdue	365 Days Overdue
AC-02(02)	365 Days Overdue	365 Days Overdue	365 Days Overdue
AC-02(03)	365 Days Overdue	365 Days Overdue	365 Days Overdue
AC-02(04)	365 Days Overdue	365 Days Overdue	365 Days Overdue
AC-04	365 Days Overdue	365 Days Overdue	365 Days Overdue
AC-05	365 Days Overdue	365 Days Overdue	365 Days Overdue
AC-06	365 Days Overdue	365 Days Overdue	365 Days Overdue
AC-06(01)	365 Days Overdue	365 Days Overdue	365 Days Overdue

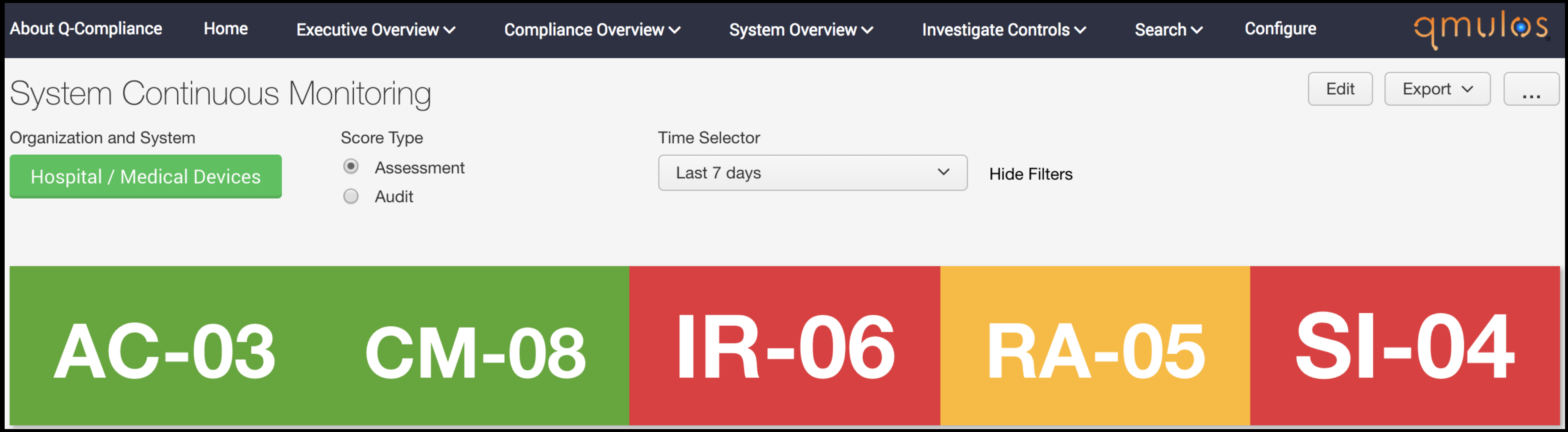
« prev 1 2 3 4 5 6 7 8 9 10 next »

Latest Audits and Assessments

Control	Last Audit Date	Last Audit Status	Last Assessment Date	Last Assessment Status
IR-06	2018-08-27 23:00:02	Passed	2018-08-27 23:00:03	Passed
CM-08	2018-08-27 20:00:04	Failed	2018-08-27 20:00:04	Failed

Automation

Use Splunk's adaptive response capabilities to quarantine a device in ISE that has a discovered incident on it



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

qmulos

System Continuous Monitoring

Edit | Export | ...

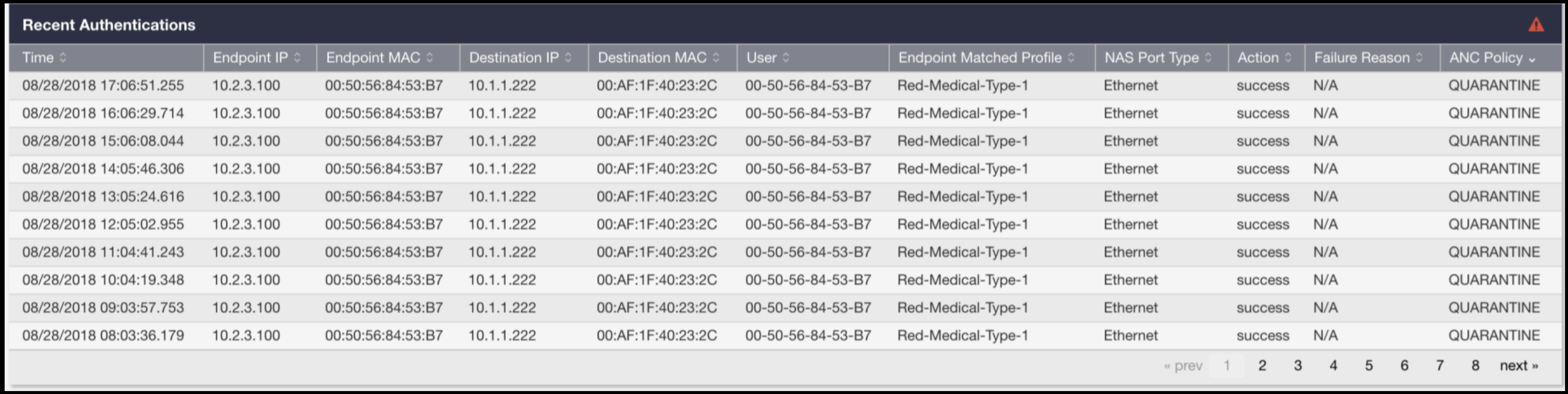
Organization and System: Hospital / Medical Devices

Score Type: ● Assessment ○ Audit

Time Selector: Last 7 days

Hide Filters

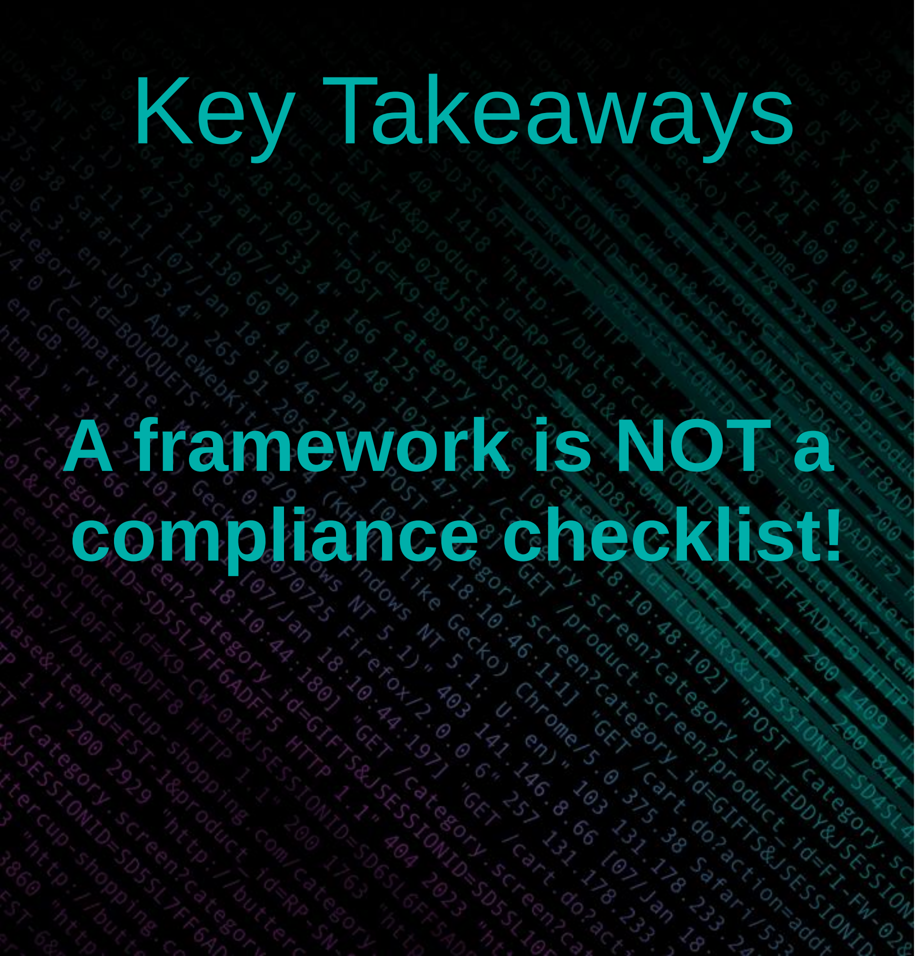
AC-03	CM-08	IR-06	RA-05	SI-04



Recent Authentications

Time	Endpoint IP	Endpoint MAC	Destination IP	Destination MAC	User	Endpoint Matched Profile	NAS Port Type	Action	Failure Reason	ANC Policy
08/28/2018 17:06:51.255	10.2.3.100	00:50:56:84:53:B7	10.1.1.222	00:AF:1F:40:23:2C	00-50-56-84-53-B7	Red-Medical-Type-1	Ethernet	success	N/A	QUARANTINE
08/28/2018 16:06:29.714	10.2.3.100	00:50:56:84:53:B7	10.1.1.222	00:AF:1F:40:23:2C	00-50-56-84-53-B7	Red-Medical-Type-1	Ethernet	success	N/A	QUARANTINE
08/28/2018 15:06:08.044	10.2.3.100	00:50:56:84:53:B7	10.1.1.222	00:AF:1F:40:23:2C	00-50-56-84-53-B7	Red-Medical-Type-1	Ethernet	success	N/A	QUARANTINE
08/28/2018 14:05:46.306	10.2.3.100	00:50:56:84:53:B7	10.1.1.222	00:AF:1F:40:23:2C	00-50-56-84-53-B7	Red-Medical-Type-1	Ethernet	success	N/A	QUARANTINE
08/28/2018 13:05:24.616	10.2.3.100	00:50:56:84:53:B7	10.1.1.222	00:AF:1F:40:23:2C	00-50-56-84-53-B7	Red-Medical-Type-1	Ethernet	success	N/A	QUARANTINE
08/28/2018 12:05:02.955	10.2.3.100	00:50:56:84:53:B7	10.1.1.222	00:AF:1F:40:23:2C	00-50-56-84-53-B7	Red-Medical-Type-1	Ethernet	success	N/A	QUARANTINE
08/28/2018 11:04:41.243	10.2.3.100	00:50:56:84:53:B7	10.1.1.222	00:AF:1F:40:23:2C	00-50-56-84-53-B7	Red-Medical-Type-1	Ethernet	success	N/A	QUARANTINE
08/28/2018 10:04:19.348	10.2.3.100	00:50:56:84:53:B7	10.1.1.222	00:AF:1F:40:23:2C	00-50-56-84-53-B7	Red-Medical-Type-1	Ethernet	success	N/A	QUARANTINE
08/28/2018 09:03:57.753	10.2.3.100	00:50:56:84:53:B7	10.1.1.222	00:AF:1F:40:23:2C	00-50-56-84-53-B7	Red-Medical-Type-1	Ethernet	success	N/A	QUARANTINE
08/28/2018 08:03:36.179	10.2.3.100	00:50:56:84:53:B7	10.1.1.222	00:AF:1F:40:23:2C	00-50-56-84-53-B7	Red-Medical-Type-1	Ethernet	success	N/A	QUARANTINE

« prev 1 2 3 4 5 6 7 8 next »



Key Takeaways

A framework is NOT a compliance checklist!

1. Legacy security and compliance is dead
2. Today’s security threats are dynamic and rapidly evolving
3. Security and compliance must be “real-time”
4. Automation is paramount
5. Proof of compliance is key to a successful security journey
6. Splunk + Cisco + Qmulos have proven this approach helps ensure mission success!

OUTATIME
THE FUTURE IS NOW!

Thank You

Don't forget to rate this session in the .conf18 mobile app

.conf18

splunk>