



QUALYS SECURITY CONFERENCE 2018

Qualys Compliance Solutions

Automate the Assessment of Technical Controls & Mandate-based Security Requirements

Tim White

Director, Product Management, Qualys, Inc.

Compliance Challenges

Continuing Expansion of
Industry & Regulatory
Mandates

Ensuring Coverage of Technical
& Non-Technical Controls

Maintaining Visibility Across
Silos

Due Diligence Beyond
Regulated Environment



Necessities to Support Digital Transformation

Complete Visibility across Business Units, Technologies, and Environments

Simplified Processes, So they can focus on improving security rather than running products

Flexibility options for capturing required compliance data

Support for emerging technologies and capabilities

Necessities to Support Digital Transformation

Tight integration across security technologies to support complex mandates and audit requirements

Automation and process integration to support DevSecOps

Comprehensive reporting against regulations, mandates & audit objectives

Qualys Security Compliance Apps



Policy Compliance



File Integrity Monitoring



Security Assessment Questionnaire

Use Case: ISO Compliance via unified security program

Customer: EU Financial institution

Digital Transformation underway
Leveraging ISO for control objectives company wide
GDPR IT Security Goals as a function of ISO

Goals

Address **ISO certification readiness** as a bi-product of good cybersecurity practices
Consolidated cybersecurity dashboard based on the ISO objectives

Requires

Security Vendor Consolidation
Integrated Solutions
Strong Regulatory Content
End-End mandate reporting



Start with a Strong Foundation

Asset Management

AI

SYN

Technical Vulnerability
Management

VM

CM

TP

Restrictions on Changes
to software packages

AI

CM

PC

FIM

Access Control

PC

Operations and
Communications
Security

PC

FIM

Procedural Controls &
Supplier relationships

SAQ

Continuously Assess Controls with Qualys Policy Compliance



Define Policies and Controls



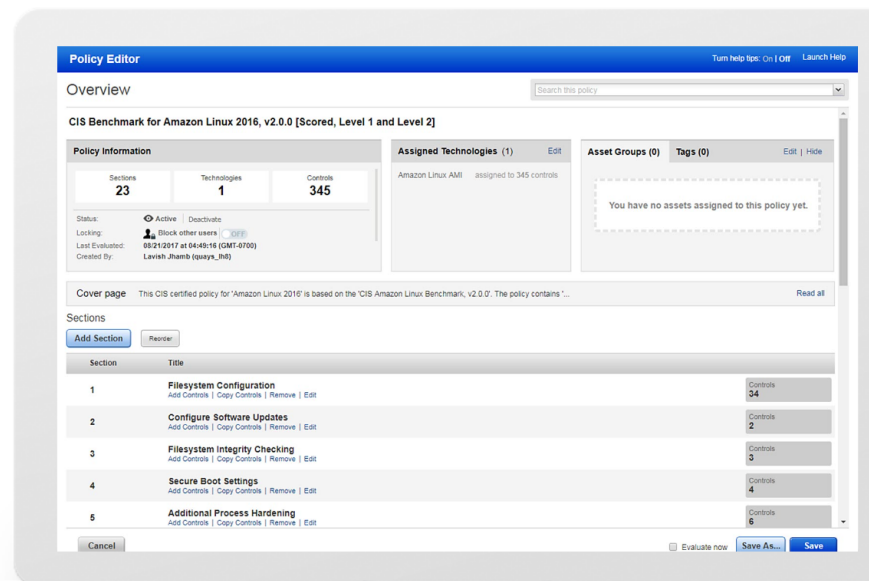
Continuously Assess



Report, Inform & Remediate



Manage Exceptions



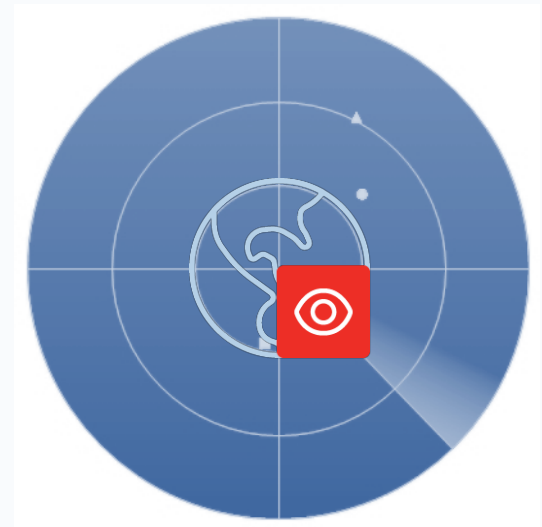
Complete Visibility

Assessment for Out-of-band Configurations

Expanded UDC Support

- Cloud Agent Support for OS UDC's
- Database UDC
- Windows File Content
- Command UDC

PC Dashboard



Broad Technology & Control Coverage to support Emerging Technologies & Digital Transformation

Network Devices
Applications
Operating Systems

Emerging Technologies

Containers
Cloud Security

Qualys Platform Security Report
Security Gap Assessment



Coming Soon: PC Dashboard & Control Search



Policy Compliance 2 ▾

DASHBOARD

CONTROLS

POLICIES

SCANS

REPORTS

EXCEPTIONS

ASSETS

USERS

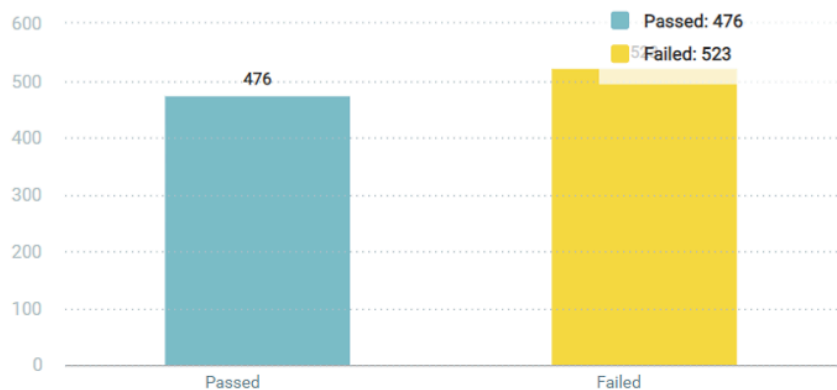
Kuldeep jadhav (quays_kj) ▾



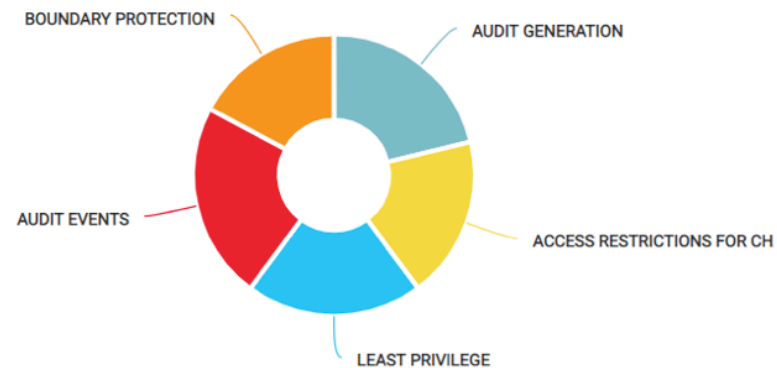
NIST Dashboard ▾



CONTROL STATUS FOR NIST RELATED CONTROLS



TOP FAILING NIST CATEGORIES



Database UDC

Initial Support: MSSQL,
Oracle, MongoDB

Define DB Query (read
only), Customizable by DB
Version

Set a query to return tabular
data to evaluate (which can
include evidence)

The screenshot shows the 'Database UDC' configuration page in the Qualys Enterprise interface. The page has a blue header with the Qualys logo and 'Enterprise' text. Below the header is a navigation bar with a back arrow and 'Database UDC'. On the left, there is a sidebar with 'STEPS 1 / 3' and four steps: 1. General Information (selected), 2. Technologies, 3. Scan Options, and 4. References. The main content area is titled 'Technology' and includes the instruction 'Select the technology and add the default control properties.' Below this is a 'Technology Family' dropdown menu with 'Oracle' selected. Under 'Default Control Properties', there are three sections: 'Rationale' with the text 'Accounts not logged in in last 90 days should be expired', 'Remediation' with the text 'In User Management application, set Automated Account Expiration should be set to 90 days', and 'SQL Statement' with the text 'SELECT UserID, UserName, Role, LastLogin, AccountEnabled from UserTable'. At the bottom right, there are 'Cancel' and 'Save' buttons.

Control: Status of first module for 'password' stack, in file '/etc/pam.d/password-auth'

Control Values by Technologies (3)

Actions

Windows 10

The 'Windows Firewall' connection rules used to prevent users from creating Policies, which will be according to the needs of the business.

This Integer value indicates the status of the security rules using the registry key path HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PublicProfile\LogFile. A value of 0 indicates that the log file is not found.

- ☐ No (0)
- ☒ Yes (1)
- ☐ Key not found

Windows 10

The 'Windows Firewall' connection rules used to prevent users from creating Policies, which will be according to the needs of the business.

This List String value(s) X indicate the current status of the setting Windows Firewall: Public: Logging: Name using the registry key path HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\PublicProfile\LogFile.

Matches regular expression list `\\%SYSTEMROOT%\System32\logfiles\firewall\publicfw.log`

- ☐ Key not found

Define Pass/Fail Criteria

Technology

Microsoft SQL Server 2008

Enabled Boolean = True

Evaluation Criteria Matches Column Criteria

When Any Row Matches LastLogin DateTime >= 90 Days



Cancel

Save

Simplifying Processes

Expanded Library Content
Instance Discovery & Controls
Migration to New UI – Up First:

- PC Dashboard
- Policy & Control Library
- Reporting

Mandate-based Policy Configurator
Leverage Asset Inventory for Asset
Lifecycle Management



Mandate Policy Configurator

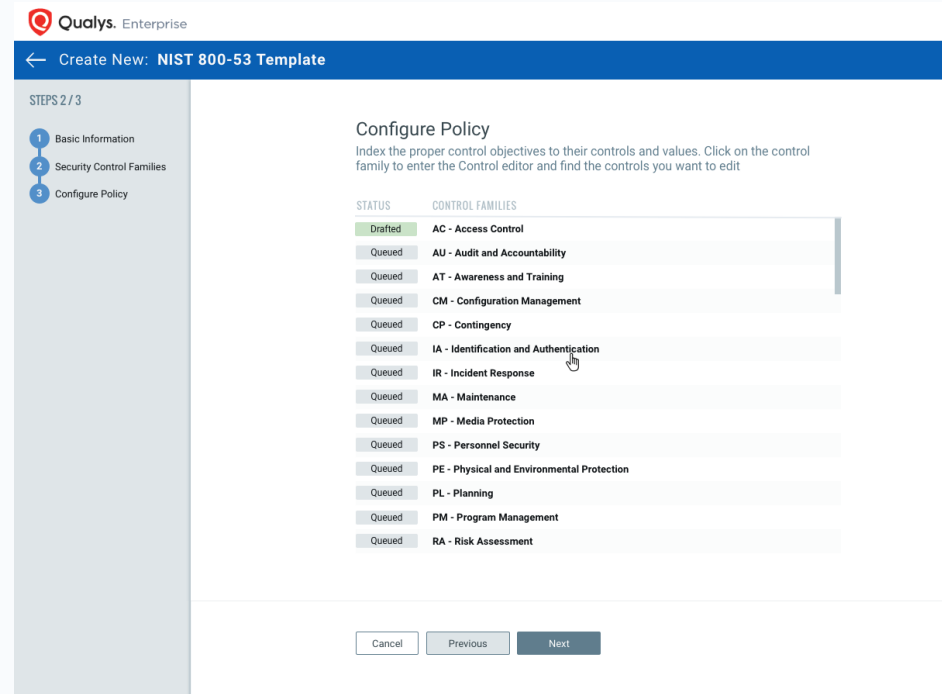
More Granular, Customizable
Control Objectives

Custom & Library Mandates

Generate Policies from
Mandate

Mandate-specific Reports

Gap Analysis Reports



STEPS 2 / 3

- 1 Basic Information
- 2 **Security Control Families**
- 3 Configure Policy

Security Control Families

Select all or just the security controls families you want to configure in this template.

CONTROL FAMILIES:

☒ **Select Families** ☐ Minimum Security Controls

BUILD LIST OF CONTROL FAMILIES:

10 CONTROL FAMILIES

[Remove all](#)

AC - Access Control	<input checked="" type="checkbox"/>
AU - Audit and Accountability	<input checked="" type="checkbox"/>
AT - Awareness and Training	<input checked="" type="checkbox"/>
CM - Configuration Management	<input checked="" type="checkbox"/>
CP - Contingency	<input checked="" type="checkbox"/>
IA - Identification and Authentication	<input checked="" type="checkbox"/>

Objective: IA - Identification and Authentication

Cancel

Done

Search Options ▾

Search...

11

Total Control Objectives



Actions ▾



NAME

PRIORITY

SECTIONS

CONTROLS



IA-5 Authenticator Management

P1

15

384

The organization manages information system authenticators by:
a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;



IA-5(1) Authenticator Management | Password-Based Authentication



6

242

IA-5(2) Authenticator Management | PKI-Based Authentication

4

48

IA-5(3) Authenticator Management | In-Person or Trusted Third=Party Registration

1

IA-5(4) Authenticator Management | Automated Support for Password Strength Determination

31

IA-5(5) Authenticator Management | Change Authenticators Prior to Delivery

1

IA-5(6) Authenticator Management | Protection of Authenticators

8

IA-5(7) Authenticator Management | No Embedded Unencrypted Static Authenticators

4

IA-5(8) Authenticator Management | Multiple Information System Accounts

0

MINIMUM SECURITY CONTROLS

High	3.01K
Moderate	982
Low	89

PRIORITY

P0 - Priority Level 0	3.01K
P1 - Priority Level 1	982
P2 - Priority Level 2	89
P3 - Priority Level 3	89

TECHNOLOGY

Windows 2012 Server	25
Windows Server 2012 R2	16
Debian GNU/Linux 9.x	5
Docker 1.x	23
F5 BIG-IP 11.x	15

10 more

Objective: IA - Identification and Authentication

Cancel

Done

Search Options ▾

Search...

11

Total Control Objectives

Actions ▾



NAME

PRIORITY

SECTIONS

CONTROLS

IA-5 Authenticator Management

P1

15

384

The organization manages information system authenticators by:
a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator, ...

IA-5(1) Authenticator Management | Password-Based Authentication

6

242

The information system, for password-based authentication:

IA-5 (1)(a)

Enforces minimum password complexity of [Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type];

36

IA-5 (1)(b)

Enforces at least the following number of changed characters when new passwords are created: [Assignment: organization-defined number]

11

IA-5 (1)(c)

Stores and transmits only cryptographically-protected passwords;

27

IA-5 (1)(d)

Enforces password minimum and maximum lifetime restrictions of [Assignment: organization-defined numbers for lifetime minimum

63

MINIMUM SECURITY CONTROLS

High	3.01K
Moderate	982
Low	89

PRIORITY

P0 - Priority Level 0	3.01K
P1 - Priority Level 1	982
P2 - Priority Level 2	89
P3 - Priority Level 3	89

TECHNOLOGY

Windows 2012 Server	25
Windows Server 2012 R2	16
Debian GNU/Linux 9.x	5
Docker 1.x	23
F5 BIG-IP 11.x	15

10 more

← Controls: NIST 800-53 for Windows

36

Controls

IMPACT BASELINE

HIGH	3.01K
MODERATE	982
LOW	89

TYPE

ANSSI	3.01K
Qualys	982
CIS	89
DISA	89

TECHNOLOGY

Windows 2012 Server	25
Windows Server 2012 R2	16
Debian GNU/Linux 9.x	5
Docker 1.x	23
F5 BIG-IP 11.x	15

≡ 10 more

Search Options ▾

🔍 Search...



Actions ▾



CID

STATEMENT / TECHNOLOGIES

TYPE

CATEGORY

BASELINE

3376

Status of the 'Maximum Password Age' setting (expiration)

Windows 2012 Server, Windows Server 2012 R2, Solaris 11.x



IA-5 (1)(a)

HIGH

10734

Status of the 'number of days before a [Prompt user] password expiration warning prompt is displayed at login' for 'users with a password' setting

Ubuntu 11.x, Windows 2000 Active Directory, Docker 1.x



IA-5 (1)(a)

MODERATE

10965

Status of first module for 'password' stack, in file '/etc/pam.d/password-auth'

Windows 2012 Server, Windows Server 2012 R2, Solaris 11.x



IA-5 (1)(a)

HIGH

11468

Status of the 'try_first_pass' setting for pam_cracklib.so module in PAM configuration file '/etc/pam.d/common-password'

Docker 1.x, Windows 2012 Server



IA-5 (1)(a)

HIGH

11524

Status of 'fail_interval' setting in the file '/etc/pam.d/password-auth'

Windows 2012 Server



IA-5 (1)(a)

HIGH

10911

Status of 'turn off certificate revocation list (CRL) checking at the Key Distribution

Windows 2012 Server, Windows Server 2012 R2



IA-5 (1)(a)

HIGH

Control Values by Technologies (3)

☐ Actions ▾ Technology: All ▾

Windows 10

The 'Windows Firewall: Apply local connection security rules (Domain)' setting enables domain-based connection rules that govern IPSec connections. As this setting enables or restricts local administrative users from creating such local connection rules, in addition to the connection security rules in Group Policies, which will increase the exposure of the system to remote attacks, this should be configured according to the needs of the business.

This Integer value **X** indicates the current status of the setting **Windows Firewall: Domain: Apply local connection security rules** using the registry key path **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsFirewall\DomainProfile\AllowLocalIPsecPolicyMerge**. A value of **0** indicates the setting is set to **No**, A value of **1** indicates the setting is set to **Yes**.

- ☐ No (0)
☒ Yes (1)
☐ Key not found

Windows 10

The "Windows Firewall: Public: Logging: Name" setting is used to specify the path and name of the file in which Windows Firewall will write its log information. If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users. It should be used according to the needs of the business.

ABOUT CONTROL



Status of first module for 'password' stack, in file '/etc/pam.d/password-auth'
 Last modified: Apr 12, 2017

Identification




Statement: Status of first module for 'password' stack, in file '/etc/pam.d/password-auth'

CID: 10965

Baseline: **HIGH**

Reference: 17.15.2.1

Status: **Active**

Technologies:
 Windows 2012 Server
 Windows 10
 Solaris 11.x

Activity

Last User Login: .\KCTech

Created on: March 1, 2017 10:33 AM

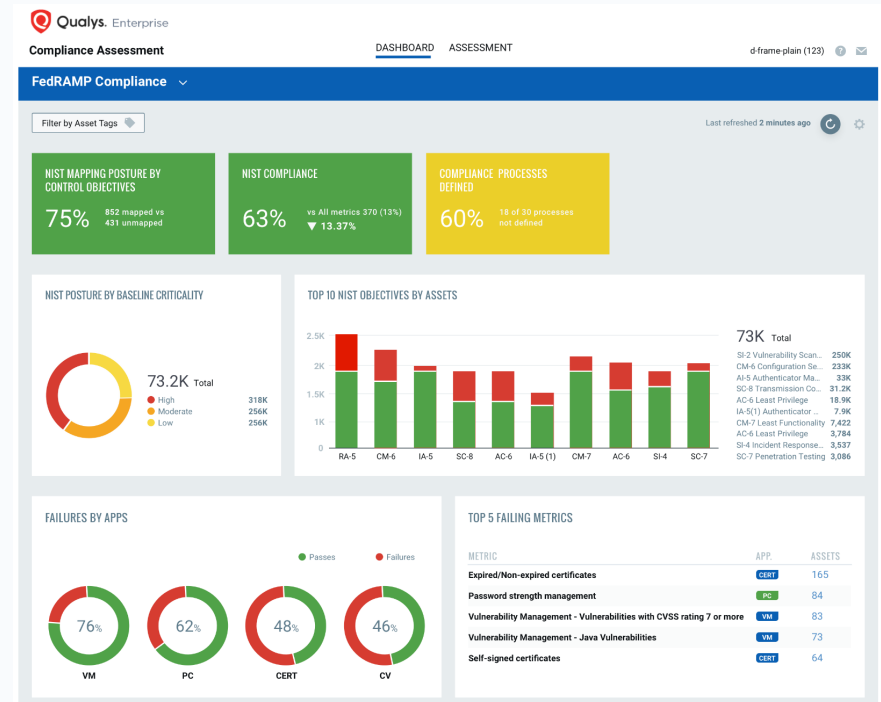
Last Modified on: 8 Mins ago 8:32 AM

Integration Across the Platform: Unified Compliance Assessment

Out of the box Library of Metrics
SAQ Self-Assessments
Vendor Risk Violations
VM & PC Remediation SLA Failures

Customizable! Map back to Control
Objectives & Custom Mandates

Result: Single Pane of Glass for Reporting
Metrics & Compliance Violation Tracking
across the platform!



Defining Metrics & Mappings

Leverages new Alerting feature as exposed in apps

Define ANY QQL Query

Action is Log a Compliance Metric

Metrics are then mapped to Control Objectives, which are cross-mapped to regulations

Qualys.

← Create New: Rule

Rule Details
Something about what the user will need to know about the fields below.

Rule Information
Something about what the user will need to know about the fields below.

Action Name

Description OPTIONAL

Alert Query
Something about what the user will need to know about the fields below.

Sample Queries Test Query

Trigger Criteria

```
vulnerabilities.vulnerability.severity:"5" and vulnerabilities.vulnerability.patchAvailable:"true" and vulnerabilities.firstFound > now-90d
```

Security Metric Examples

High Severity Vulnerabilities/
Patching

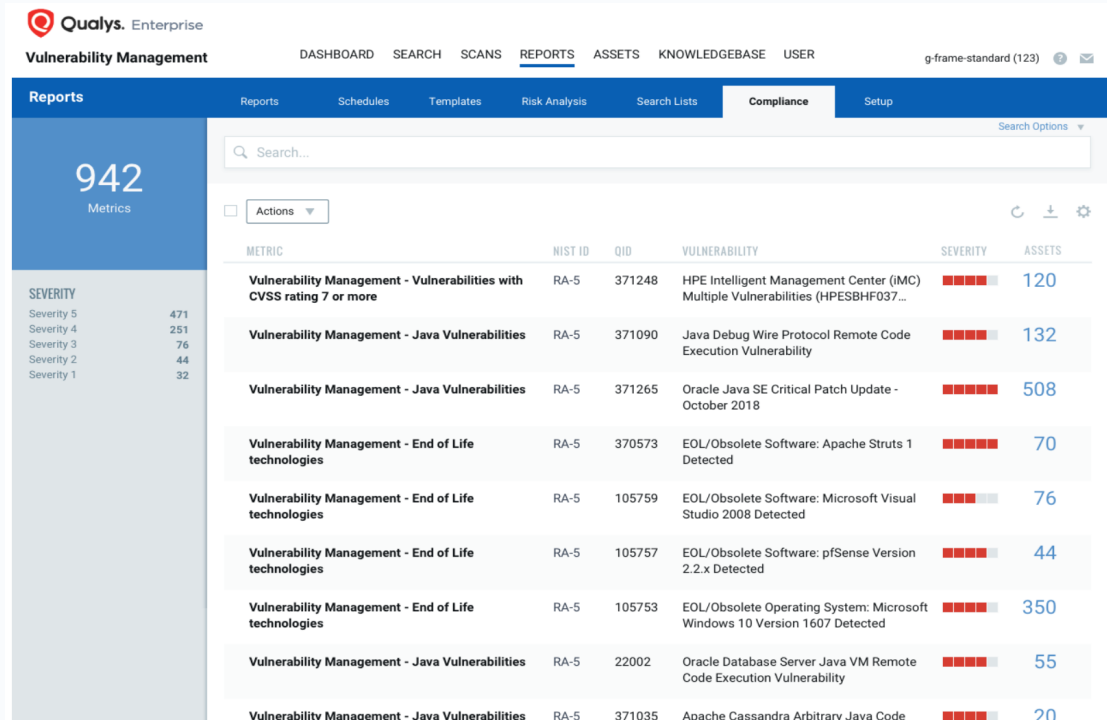
FIM Incident Review Expired

Cloud Security Configuration
Issues

Expired or Self-Signed
Certificates

Vendor Risk – Failure to
Respond

Procedural Control Gap
Identified



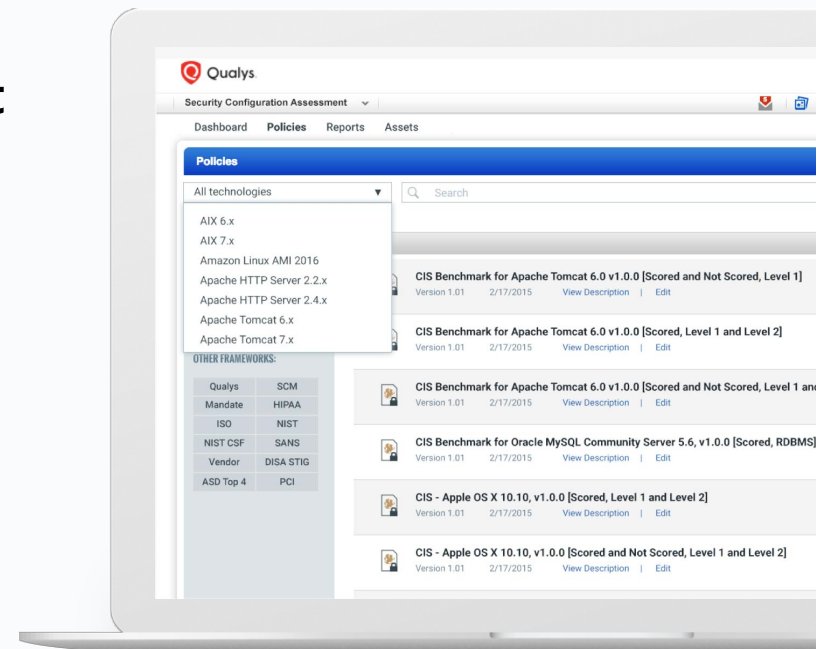
Assess ALL your assets against CIS

With Qualys Security Configuration Assessment

Security Configuration Assessment

Lightweight add-on to VM
Broad platform coverage
Accurate controls & content
Simple assessment workflow
Scan remotely or via agent
Powered by the Qualys Cloud Platform

Support for NIST Reporting coming soon!



Introducing

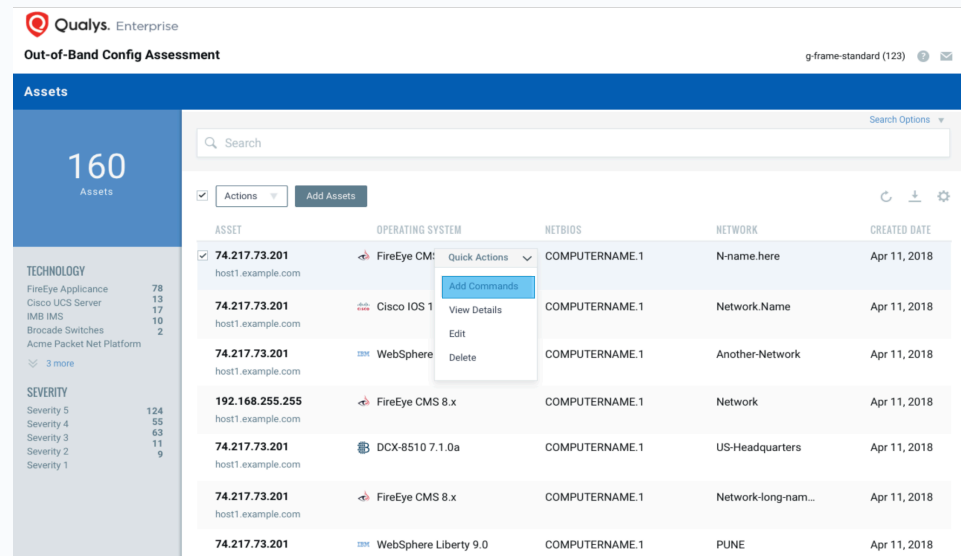
Out-of-Band Configuration Assessment

OCA, add-on to VM/PC

Flexible Data Collection via
API/UI

Support for Inventory,
Policy Compliance and
Vulnerability Assessment

Bulk data, Automated and
Customizable



Qualys. Enterprise
Out-of-Band Config Assessment

g-frame-standard (123)

Assets

160 Assets

TECHNOLOGY

FireEye Appliance	78
Cisco UCS Server	13
IMB IMS	17
Brocade Switches	10
Acme Packet Net Platform	2

3 more

SEVERITY

Severity 5	124
Severity 4	55
Severity 3	63
Severity 2	11
Severity 1	9

ASSET

OPERATING SYSTEM

NETBIOS

NETWORK

CREATED DATE

74.217.73.201 host1.example.com	FireEye CM	COMPUTERNAME.1	N-name.here	Apr 11, 2018
74.217.73.201 host1.example.com	Cisco IOS 1	COMPUTERNAME.1	Network.Name	Apr 11, 2018
74.217.73.201 host1.example.com	WebSphere	COMPUTERNAME.1	Another-Network	Apr 11, 2018
192.168.255.255 host1.example.com	FireEye CMS 8.x	COMPUTERNAME.1	Network	Apr 11, 2018
74.217.73.201 host1.example.com	DCX-8510 7.1.0a	COMPUTERNAME.1	US-Headquarters	Apr 11, 2018
74.217.73.201 host1.example.com	FireEye CMS 8.x	COMPUTERNAME.1	Network-long-nam...	Apr 11, 2018
74.217.73.201 host1.example.com	WebSphere Liberty 9.0	COMPUTERNAME.1	PUNE	Apr 11, 2018

Out of Band Configuration Assessment

Large Global Bank

Disconnected/Inaccessible systems to be a part of overall Vulnerability, Risk and Compliance program

Sensitive Systems/Regulated Devices

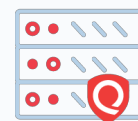
Legacy Systems

Highly locked down systems

Network Appliances

Air-gapped Networks

» Adtran AOS
» BlueCoat ProxySG
» Brocade FabricOS
» Check Point GAiA
» Cisco IOS
» Dell Force10 FTOS
» Extreme ExtremeXOS
» FireEye
» Fortigate FortiOS
» HP ProCurve
» Huawei VRP
» Juniper Junos
» NetApp Data ONTAP
» SonicWALL SonicOS



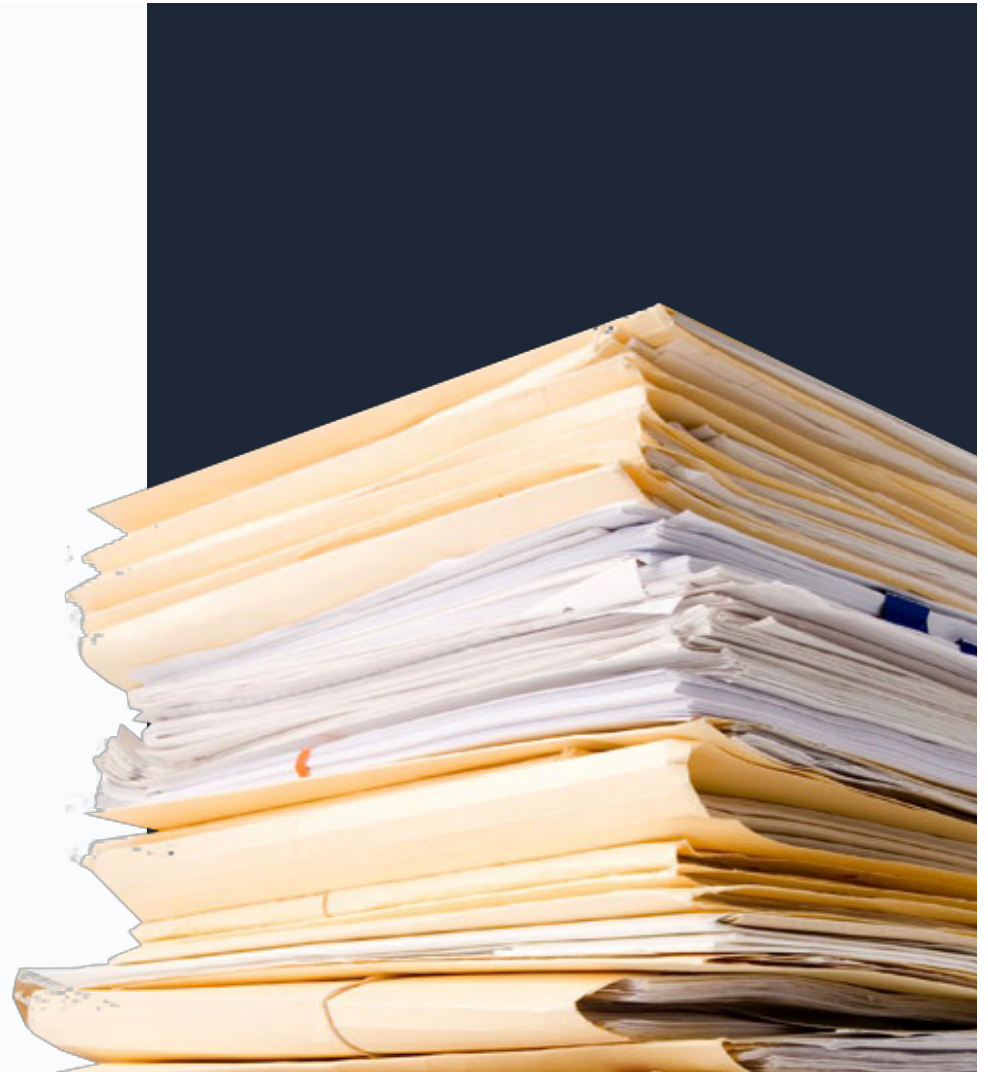
Current Options

Ad-hoc scripts

Procedural controls
(manual assessment)

Outside audits

Limited software-based
solutions



Configuration Upload Workflow

Push the Asset data

Upload Configuration Data

Qualys creates agent-based data snapshot

Report Generation

The screenshot displays the Qualys API interface for asset provisioning. It shows a POST request to `http://{{base_url}}/oca/v1.0/asset` and a GET request to `http://swarm01.p17.eng.sjc01.qualys.com:53670/oca/v1.0/asset/03df1879-458c-495d-873d-7ab2daa34045/commands/PolicyCompliance`. The GET response is a JSON object with a 200 status code and a data field containing a list of items: version, tscklockserver, configshow -all, and syslogdipshow. Below the JSON response, there is a section for uploading command outputs, showing a POST request to `http://{{base_url}}/oca/v1.0/asset/03df1879-458c-495d-873d-7ab2daa34045/command/output/{{type}}`. The interface includes tabs for Params, Authorization, Headers (3), Body, Pre-request Script, and Tests. The Body tab is selected, showing a table with columns for KEY, VALUE, and DESCRIPTION. The table contains four rows: configshow -all, syslogdipshow, tscklockserver..., and version. Each row has a checkbox in the KEY column and a corresponding value in the VALUE column.

KEY	VALUE	DESCRIPTION
<input checked="" type="checkbox"/> configshow -all	Choose Files No file chosen	
<input checked="" type="checkbox"/> syslogdipshow	syslog.1 10.170.65.31	
<input checked="" type="checkbox"/> tscklockserver...	Active NTP Server 10.170.158.12...	
<input checked="" type="checkbox"/> version	Kernel: 2.6.14.2 ...	
Key	Value	Description

Technology Support

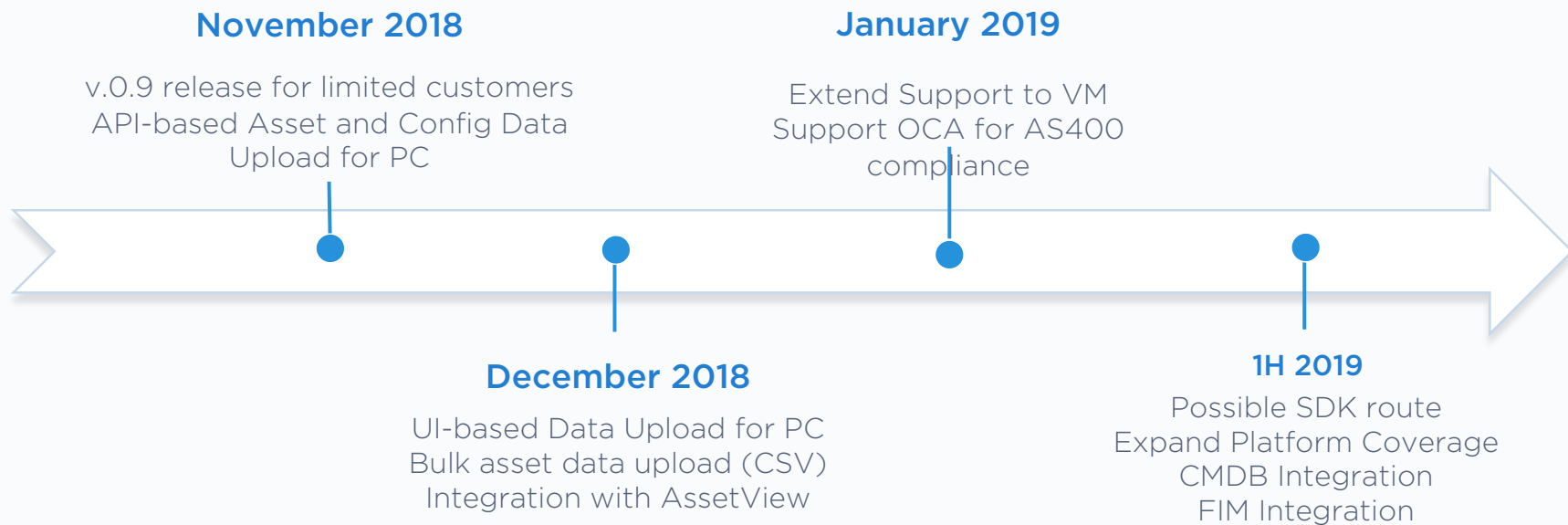
V0.9 and v1.0 release November - 2018

FireEye Appliances
BigIP F5
Brocade DCX Switch
Acme Packet Net
Imperva Firewall
Cisco Wireless Lan Controller 7
Cisco UCS Server
NetApp OnTap
Juniper IVE

Future Priorities

AS/400
Cisco Meraki
Sonic Firewall
Fortinet Firewalls
Aruba WLC
Dell EMC Data Domain
Oracle Tape Library

Availability & Roadmap





QUALYS SECURITY CONFERENCE 2018

File Integrity Monitoring

Log and track file changes across global IT systems.

Validating Integrity

Why do organizations need File Integrity Monitoring solutions?

- Change control enforcement
- Compliance & audit requirements
- Explicit mandates like PCI
- Security best practices
- Compromise detection



Qualys File Integrity Monitoring

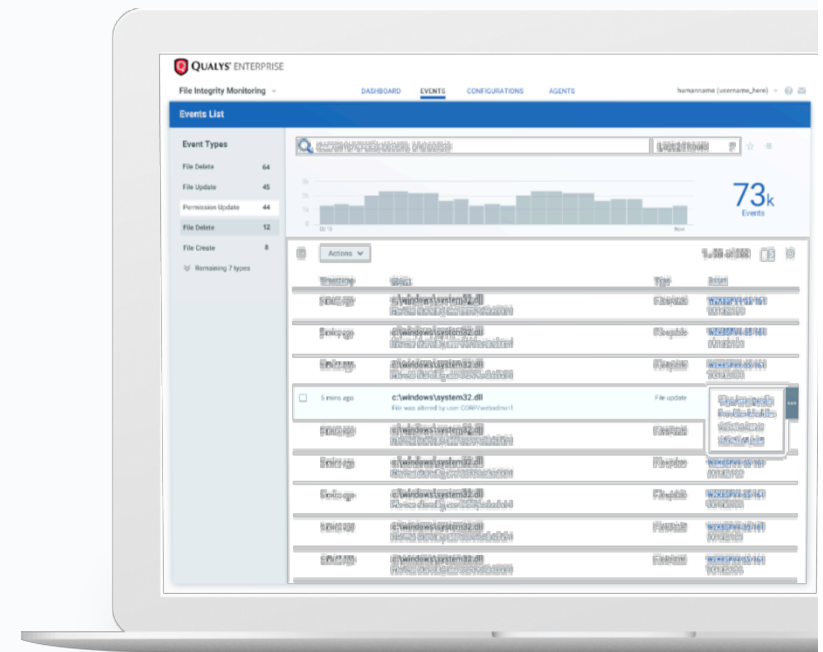


Real-time detection

Built on the Qualys Cloud Agent

Easy to install, configure and manage

No expensive infrastructure to deploy



Use Case:

File Integrity Monitoring for PCI

Customer: Retail

Distributed network environment that benefits from cloud-based model
20k+ Windows systems
Large Linux back end infrastructure on-prem and in the cloud

Goals

Monitor for change control enforcement
PCI auditor requirements

Requires

Scalable, cloud-based solution
Hands-off management of distributed agents
VM+PC+FIM at the Point of Sale
Broad Linux platform support

FIM Challenges

Deciding what depth to monitor

Tuning out noise, but not missing important events

Scalability of legacy solutions

Meeting auditor event review requirements

What Are Customers Monitoring?

Critical Operating System Binaries

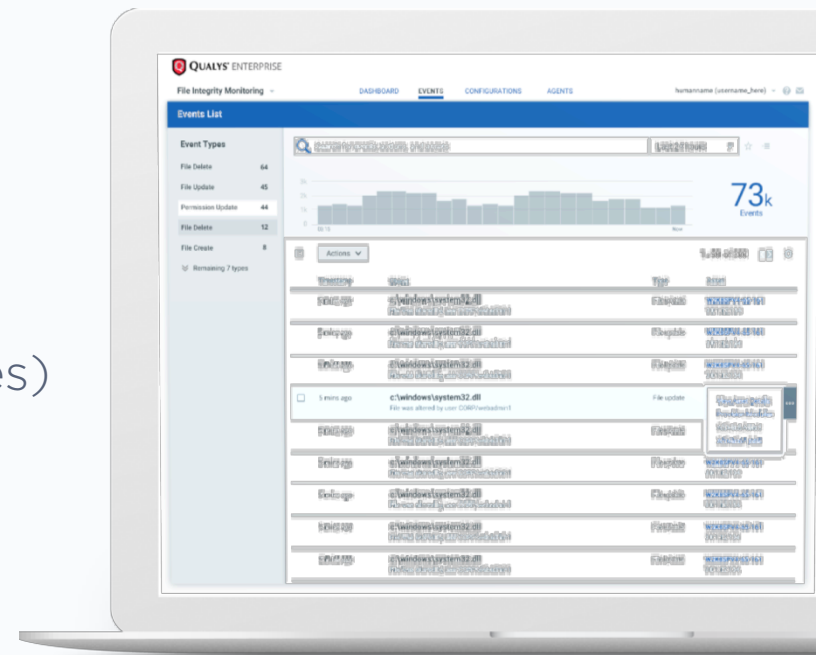
OS and Application Configuration Files

Content, such as Web source

Permissions (such as on Database Stores)

Security Data (Logs, Folder Audit Settings)

User & Authentication Configurations



Focus for 2019

Simplest tuning in the industry!

Secondary Event Filtering and Automated Correlation

API access to data

Rule-based Alerting

Reporting

Expanded data collection & whitelisting features

Expanded Platform Support

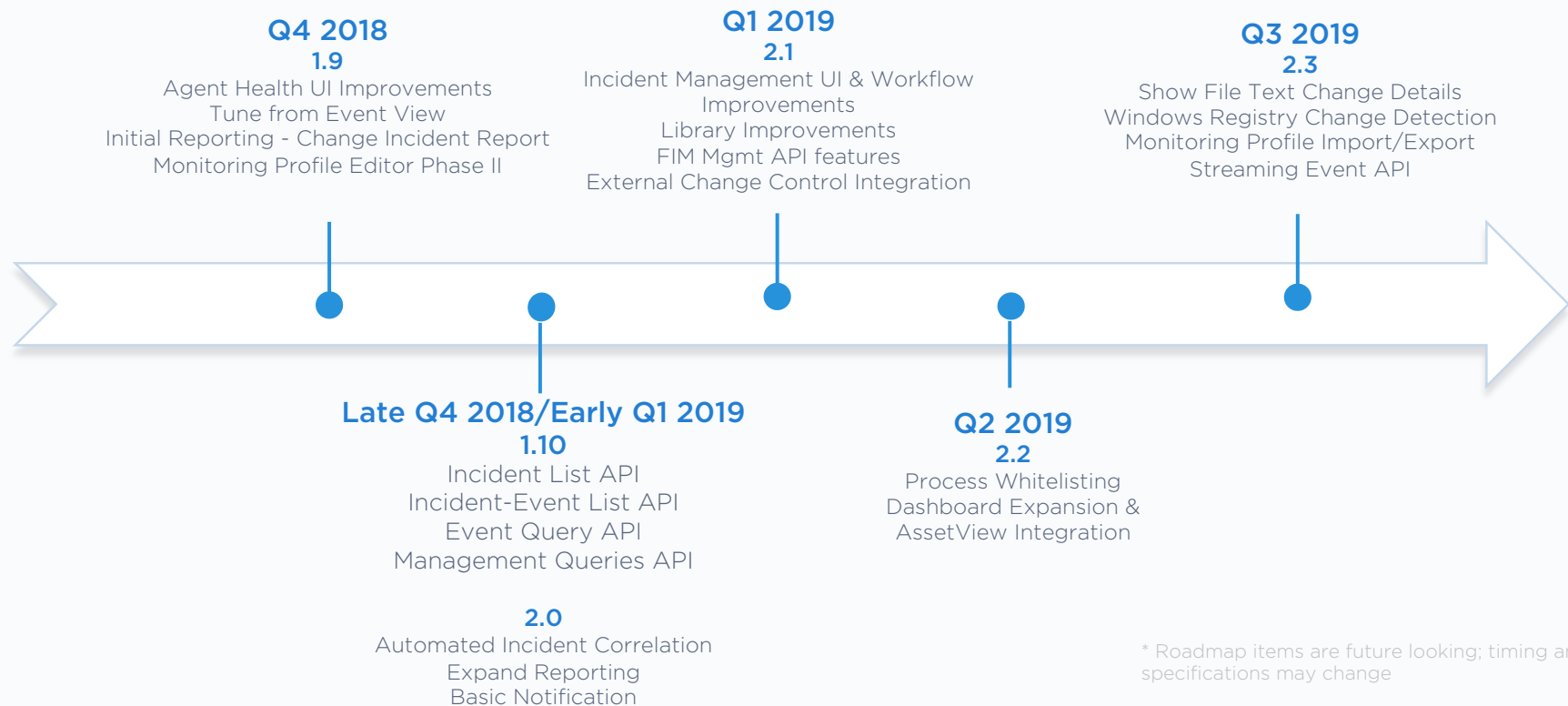


Demo



File Integrity Monitoring

FIM Feature Roadmap





QUALYS SECURITY CONFERENCE 2018

Security Assessment Questionnaire

Automate the Assessment of Procedural
Controls & Vendor Risk

Tim White

Director, Product Management, Qualys, Inc.

Assess Procedural Controls with Security Assessment Questionnaire



Cloud-Based Questionnaires

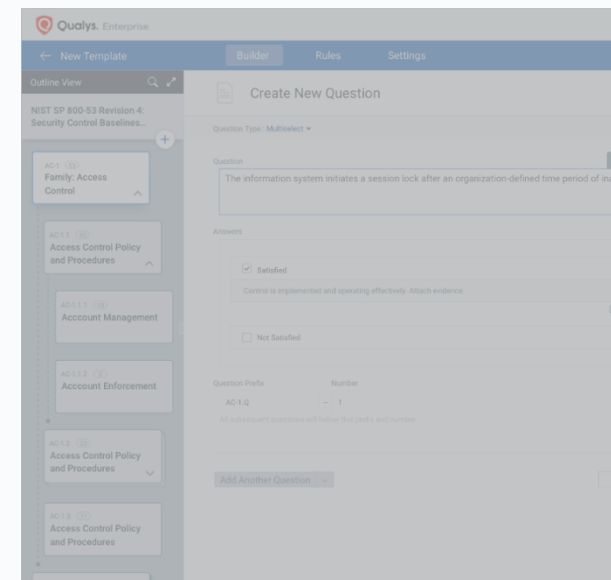
Visually design questionnaires

Assign assessment leveraging embedded workflow

Intuitive response

Track using an operational dashboard

Review answers and evidences



One of the biggest Financial Institutions

Assesses their Internal Procedural and Process controls

Need to comply with number of International and regional mandates/ standards.



Took 2 hours to rebuild Excel based 76 question assessment using web-based UI and Out-of-box Rich content

They understand >50% compliance requirements are related to assessing processes and procedures



Dashboards the process deficiencies and risk posed by Internal controls failure

Important that Respondents find it easy and make the collected data actionable



Consolidates the Internal procedural control posture with Technical compliance controls







New-age Vendor Assessment Challenges

Extend the Perimeter to include vendors
- security & vulnerability data collection

Vendor Profiling based on the services,
Vendor Assessment based on criticality

Vendor control data aggregation with
Internal security and compliance data

Automated workflow, operational
dashboards

	SOURCE OF ATTACK	FINANCIAL IMPACT	REPUTATIONAL IMPACT	BREACH ORIGIN
	Attackers stole credentials from 3 rd Party vendor to breach network	\$200 million in costs (to date)	✓	<div>Direct Breach 30% Third Parties 70%</div>
	Attackers breached network via 3 rd Party vendor	Estimated \$2-3 billion in fraud charges	✓	
	Breach due to 3 rd Party vendor	Estimated \$3 billion in fraud charges	✓	
	Google's Australia office hacked via 3 rd Party HVAC vendor	Impact TBD	✓	
	Yahoo Mail accounts hacked due to 3 rd Party database breach	Impact TBD	✓	
	T-Mobile customer PII data stolen from Experian (3 rd Party) server	15 million customers' PII stolen	✓	

One of the biggest pharmaceutical companies

Assessing their vendor risk through SAQ



Vendors Profiling — Defines Criticality based on Service areas/Cybersecurity domains



Assesses vendors per their risk profile, in a standardized (SIG) manner



Uses out-of-the-box content, including regional mandates



Dashboards the risk posed by the highly critical vendors and ranks them per risk



Easy online workflow for the vendors, receives reminders, alerts and status



Consolidates the vendor control posture with Internal procedural & technical compliance controls

Rich Template Library

Industry

PCI DSS SAQ A, B, C, D
IT for SOX
GLBA
BASEL 3 (IT)
HIPAA
HITRUST
NERC CIP v5
SWIFT
NERC CIP

Popular Standards

ISO 27001-2013 ISMS
NIST CSF
COBIT 5
FedRAMP
COSO
ITIL
CIS TOP 20 Controls
Shared Assessment (SIG)
*- vendor assessment

Regional

GDPR
Abu Dhabi Info Sec
Standards
ANSSI (France)
MAS IBTRM (Singapore)
BSP (Philippines)
BSI Germany
ISM (Australia)
UK Data Protection
RBI Guidelines (India)
California Privacy**
Canada Data Protection
2018**

Technical Services

CSA CAIQ v3.0.1
CSA CCM v3.0.1
Vendor Security for
Hosting Service Provider
AWS **
Procedural controls for
cloud, containers**

- ❖ Includes premium content – Shared Assessments (SIG)
- ❖ Use as-is or customize to your needs

SAQ Roadmap

Q3 2018

User/Role/Privilege Management
Question Bank
Create template from library templates
New campaign UI
Risk scoring

Q1 2019

Vendor-driven workflows to cater to customers

- Create answer bank,
- Upload customer required templates
- Match on Keywords
- Metrics, Dashboards on risk posed to my customers

Q4 2018

SAQ Lite – for PCI users
Vendor Risk Management workflows

- Vendor Onboarding, Profiling
- Automated assessment based on Vendor profiles/onboarding
- Compare vendors based on risk scores
- Dashboards on total Vendor risk/Trending/Top 5 risky vendors

* Roadmap items are future looking; timing and specifications may change

In the world where everyone is a vendor of someone

SAQ Feature coming up in Q1: Answer bank

Technology company wants to understand Risk posed to the customers



Receives 100s of questionnaires from their customers and answers them offline, through spread-sheets



Want to understand What risk they pose to their critical customers



Costly & resource-intensive to respond and gains no visibility into risk intelligence



Want to understand the top failing, passing cybersecurity areas/ answers to improve their own internal controls



Wants to drive the vendor-management project to showcase their good security practices and use the data for contract negotiation

Security Assessment Questionnaire

SAQ



QUALYS SECURITY CONFERENCE 2018

Thank You

Tim White
twhite@qualys.com