QUALYS SECURITY CONFERENCE 2018

Policy Compliance & Security Configuration Assessment

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

Compliance Challenges

Continuing Expansion of Industry & Regulatory Mandates

Ensuring Coverage of Technical & Non-Technical Controls

Maintaining Visibility Across Silos

Due Diligence Beyond Regulated Environment

FISMA
HIPAA
Health Insurance Portability & Accountability Act
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
NIST
National Institute of Standards and Technology
U.S. Department of Commerce
PCI
PARTICIPATING ORGANIZATION
Security Benchmarks
GDPR

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

Use Case:

FedRAMP/NIST Compliance via unified security program

Customer: Cloud-based Infrastructure solution Provider

- Digital Transformation underway
- FedRAMP certification driving compliance unification
- Leveraging NIST for control objectives company wide

Goals:

- Address **FedRAMP compliance** as a bi-product of good cybersecurity practices
- Consolidated cybersecurity dashboard based on the NIST objectives

Requires:

- Security Vendor Consolidation
- Integrated Solutions
- Strong Regulatory Content
- End-End mandate reporting
- Breadth & Depth of Coverage

FedRAMP

NIST National Institute of Standards and Technology
U.S. Department of Commerce

NIST Control	NIST Control Objective	Qualys Applications
CM	Information System Component Inventory	AI SYN
CM	Inventory of Authorized and Unauthorized Software	AI SYN VM PC
CM	Secure Configuration for Hardware and Software	TP
RA-5	Continuous Vulnerability Assessment & Remediation	VM PC TP CM
AC, IA	Controlled Used of Administrative Privileges	PC
AU	Maintenance, Monitoring and Analysis of Audit Logs	PC FIM
AC	Email and Web Browser Protection	VM PC SAQ
SI-4	Malware Defense	PC IOC WAS WAF FIM
CM, SA	Limitation and Control of Network Ports	VM PC CM WAF
CP	Data Recovery Capability	PC SAQ
CM, RA	Secure Configurations for Network Devices	VM PC

NIST Control	NIST Control Objective	Qualys Applications
AC, SI	Boundary Defense	VM PC CS WAS WAF
AU	Maintenance, Monitoring, and Analysis of Audit Logs	PC FIM
AC, IA	Controlled Access Based on the Need to Know	PC CS
AC-17, AC-18	Wireless Access Control	VM
AC, IA	Account Monitoring and Control	PC SAQ
AT	Security Skills Assessment and Appropriate Training to Fill Gaps	SAQ
RA, CM	Vendor Controls Assessment	IOC CS WAS WAF
IR	Incident Response and Management	PC IOC FIM
CA	Penetration Tests and Red Team Exercises	VM TP IOC

They started with critical requirements for Quick Wins…

1. Inventory Your Systems AI SYN

2. Inventory and Restrict Software AI SYN PC VM

3. Secure Configurations PC FIM SCA

4. Continuous Vulnerability Management VM CM TP SCA

5. Review Rights & Permissions PC

6. Definition, Automated Evaluation & Review of Processes SAQ

Complete Visibility

Assessment for Out-of-band Configurations

Expanded UDC Support

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

PC Dashboard

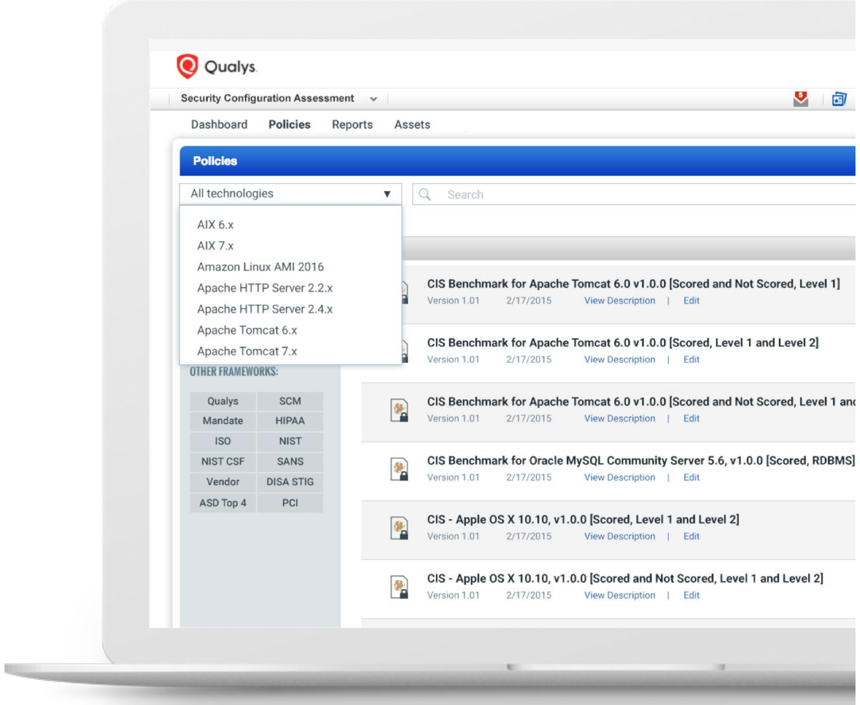
Assess ALL your assets against CIS

With Qualys Security Configuration Assessment

SCA 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!



CIS Benchmark for Apache Tomcat 6.0 v1.0.0 [Scored and Not Scored, Level 1]
Version 1.01 2/17/2015 View Description | Edit

CIS Benchmark for Apache Tomcat 6.0 v1.0.0 [Scored, Level 1 and Level 2]
Version 1.01 2/17/2015 View Description | Edit

CIS Benchmark for Apache Tomcat 6.0 v1.0.0 [Scored and Not Scored, Level 1 anc
Version 1.01 2/17/2015 View Description | Edit

CIS Benchmark for Oracle MySQL Community Server 5.6, v1.0.0 [Scored, RDBMS]
Version 1.01 2/17/2015 View Description | Edit

CIS - Apple OS X 10.10, v1.0.0 [Scored, Level 1 and Level 2]
Version 1.01 2/17/2015 View Description | Edit

CIS - Apple OS X 10.10, v1.0.0 [Scored and Not Scored, Level 1 and Level 2]
Version 1.01 2/17/2015 View Description | Edit

Broad Technology & Control Coverage

to support Emerging Technologies & Digital Transformation

Network Devices
Applications
Operating Systems

Emerging Technologies

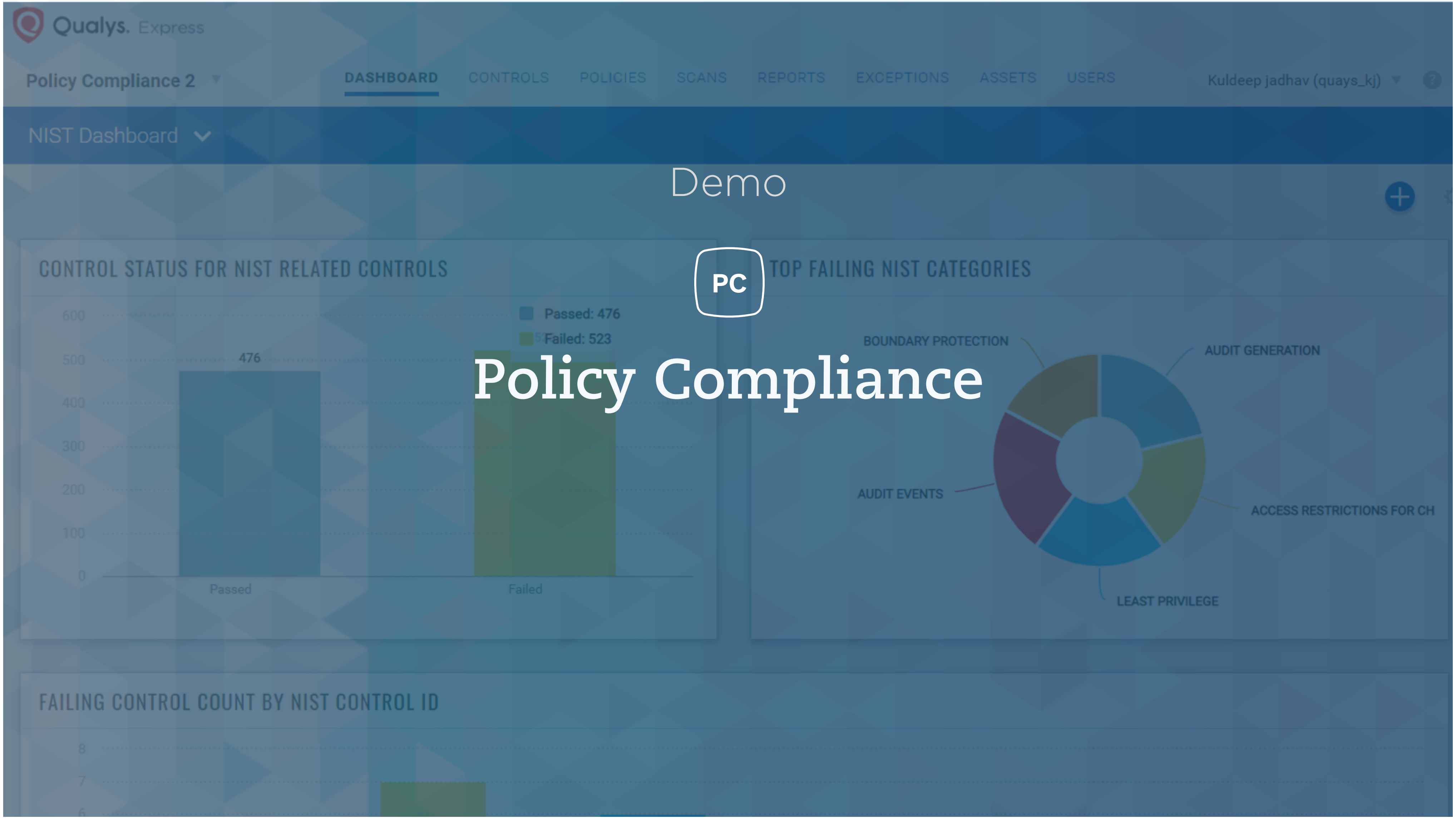
Containers
Cloud Security

Qualys Platform Security Report
Security Gap Assessment

Demo

PC

Policy Compliance

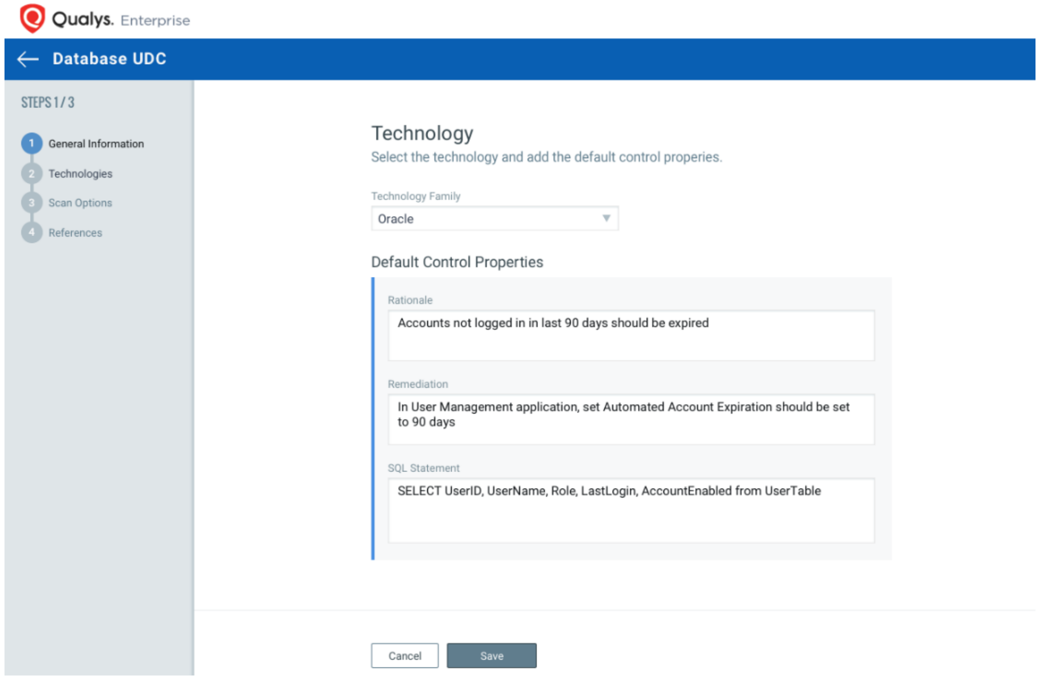


Database UDC

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)



Technology

Select the technology and add the default control properies.

Technology Family: Oracle

Default Control Properties

Rationale: Accounts not logged in in last 90 days should be expired

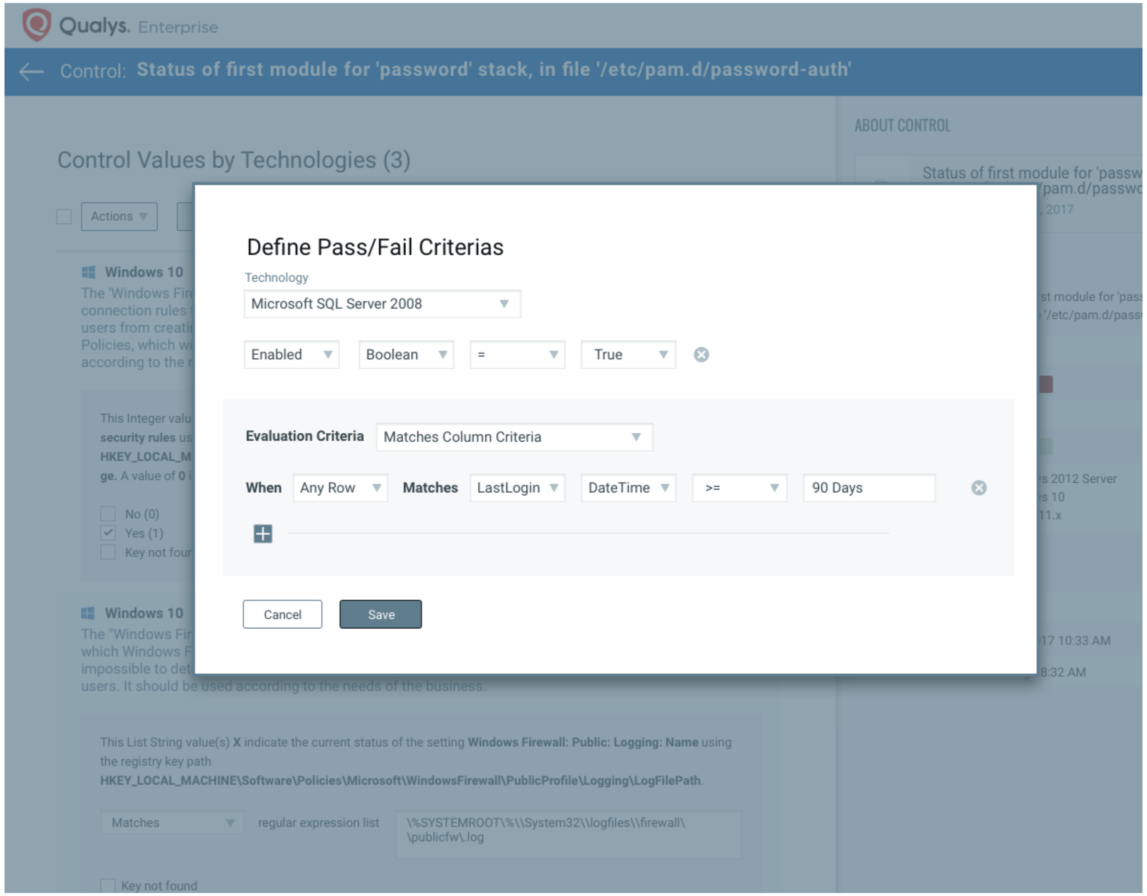
Remediation: In User Management application, set Automated Account Expiration should be set to 90 days

SQL Statement: SELECT UserID, UserName, Role, LastLogin, AccountEnabled from UserTable

Then, Configure Pass/Fail Criteria

Define a Post-Filter, Then Evaulate based on:

- Empty Result Set
- Row Count Threshold
- Always Pass/Fail (for data gathering)
- Match Column Criteria



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

Control Values by Technologies (3)

Define Pass/Fail Criterias

Technology: Microsoft SQL Server 2008

Enabled | Boolean | = | True

Evaluation Criteria Matches Column Criteria

When Any Row **Matches** LastLogin | DateTime | >= | 90 Days

Windows 10

The "Windows Fir… which Windows F… impossible to det… users. It should be used 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\Logging\LogFilePath**.

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

□ Key not found

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

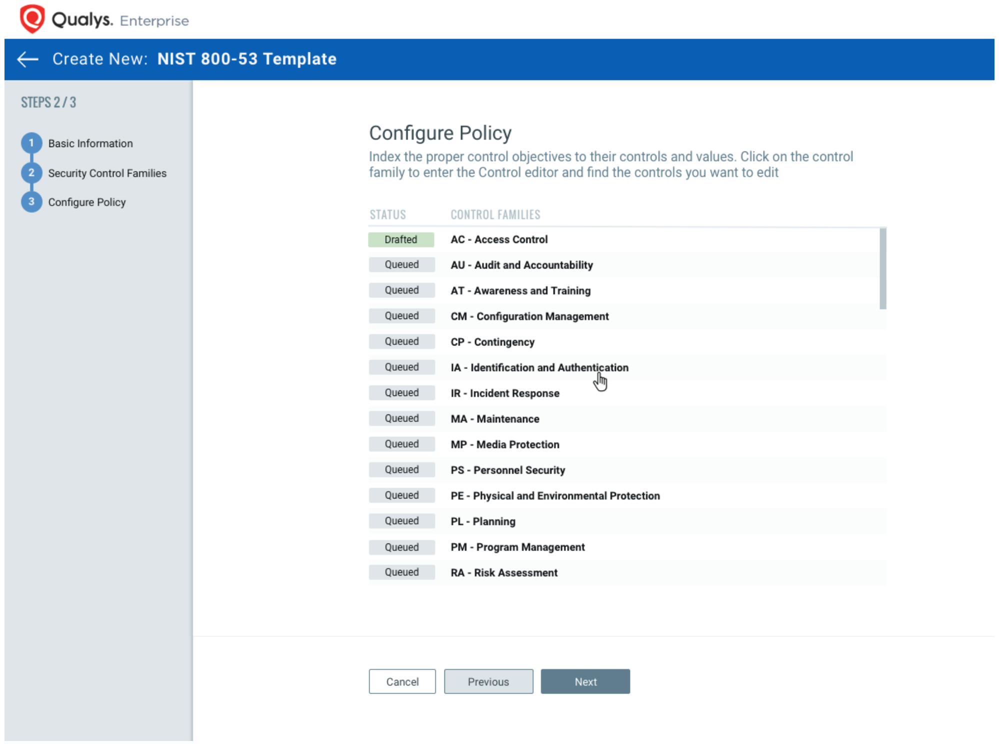
More Granular, Customizable Control Objectives

Custom & Library Mandates

Generate Policies from Mandate

Mandate-specific Reports

Gap Analysis Reports



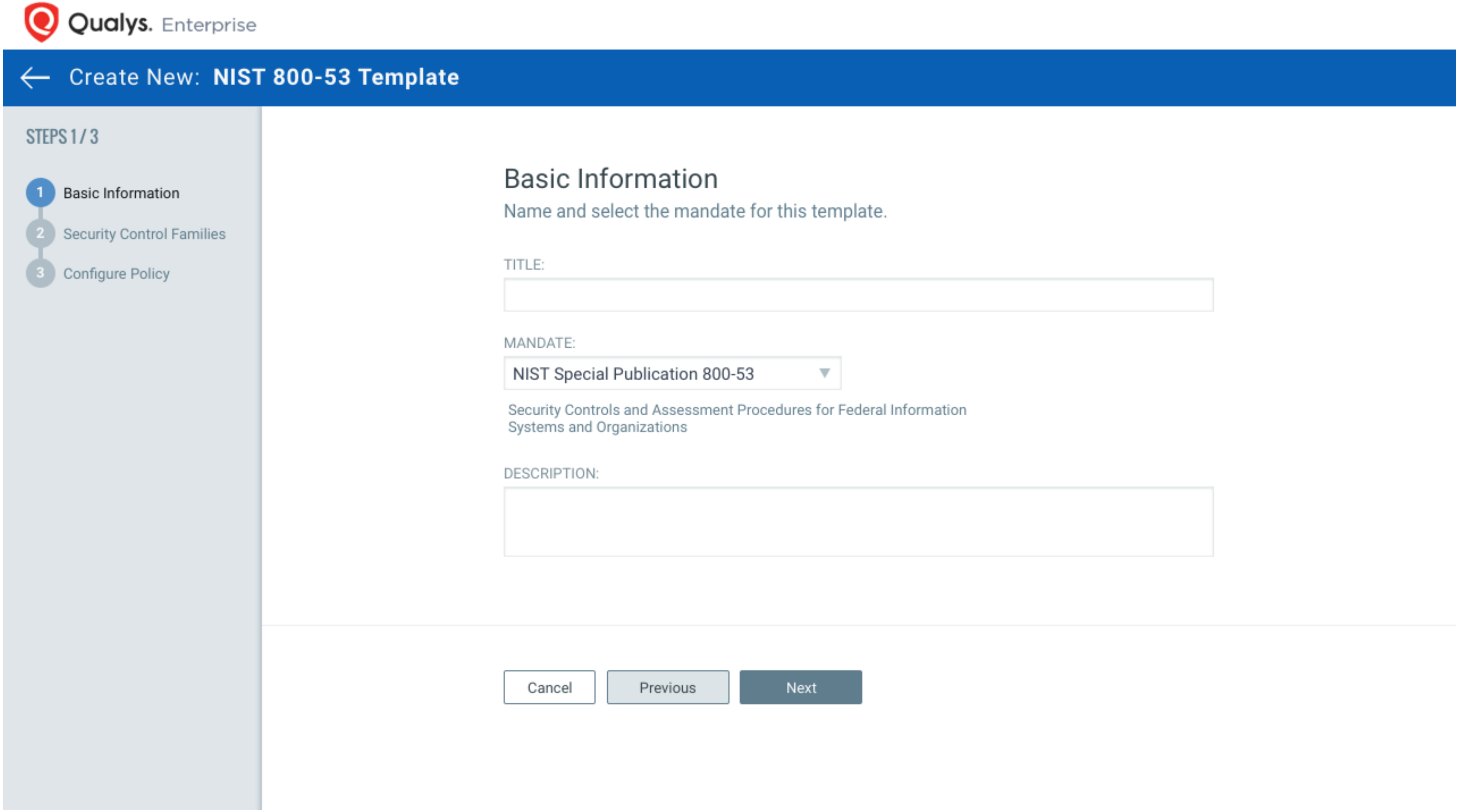
Qualys. Enterprise

← Create New: **NIST 800-53 Template**

Configure Policy

Index the proper control objectives to their controls and values. Click on the control family to enter the Control editor and find the controls you want to edit

STATUS	CONTROL FAMILIES
Drafted	AC - Access Control
Queued	AU - Audit and Accountability
Queued	AT - Awareness and Training
Queued	CM - Configuration Management
Queued	CP - Contingency
Queued	IA - Identification and Authentication
Queued	IR - Incident Response
Queued	MA - Maintenance
Queued	MP - Media Protection
Queued	PS - Personnel Security
Queued	PE - Physical and Environmental Protection
Queued	PL - Planning
Queued	PM - Program Management
Queued	RA - Risk Assessment



Qualys. Enterprise

Create New: **NIST 800-53 Template**

STEPS 1 / 3

1 Basic Information

2 Security Control Families

3 Configure Policy

Basic Information

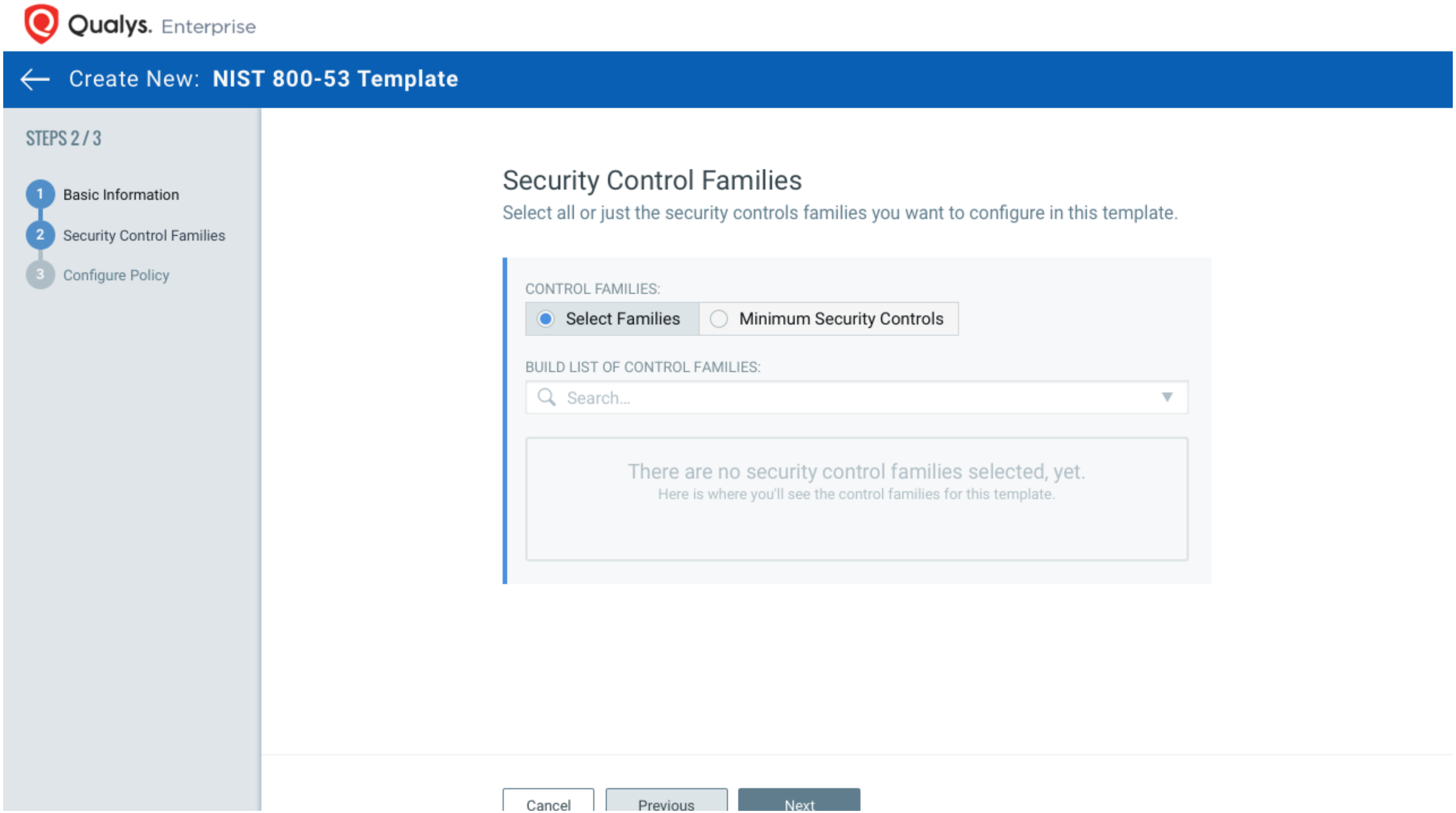
Name and select the mandate for this template.

TITLE:

MANDATE: NIST Special Publication 800-53

Security Controls and Assessment Procedures for Federal Information Systems and Organizations

DESCRIPTION:



Security Control Families

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

CONTROL FAMILIES:

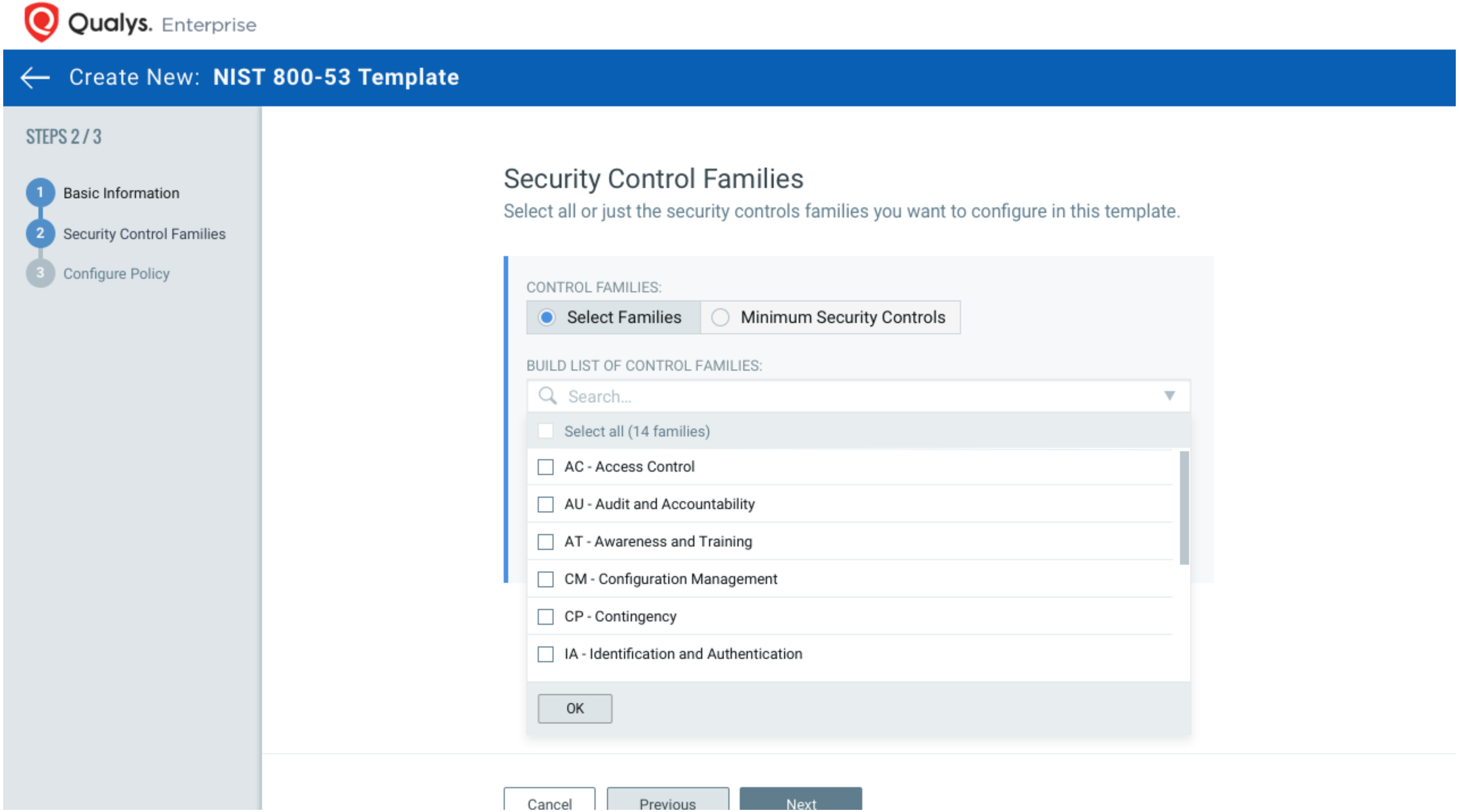
● Select Families ○ Minimum Security Controls

BUILD LIST OF CONTROL FAMILIES:

Search...

There are no security control families selected, yet.

Here is where you'll see the control families for this template.



Qualys. Enterprise

← Create New: **NIST 800-53 Template**

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:

Search...

□ Select all (14 families)

□ AC - Access Control

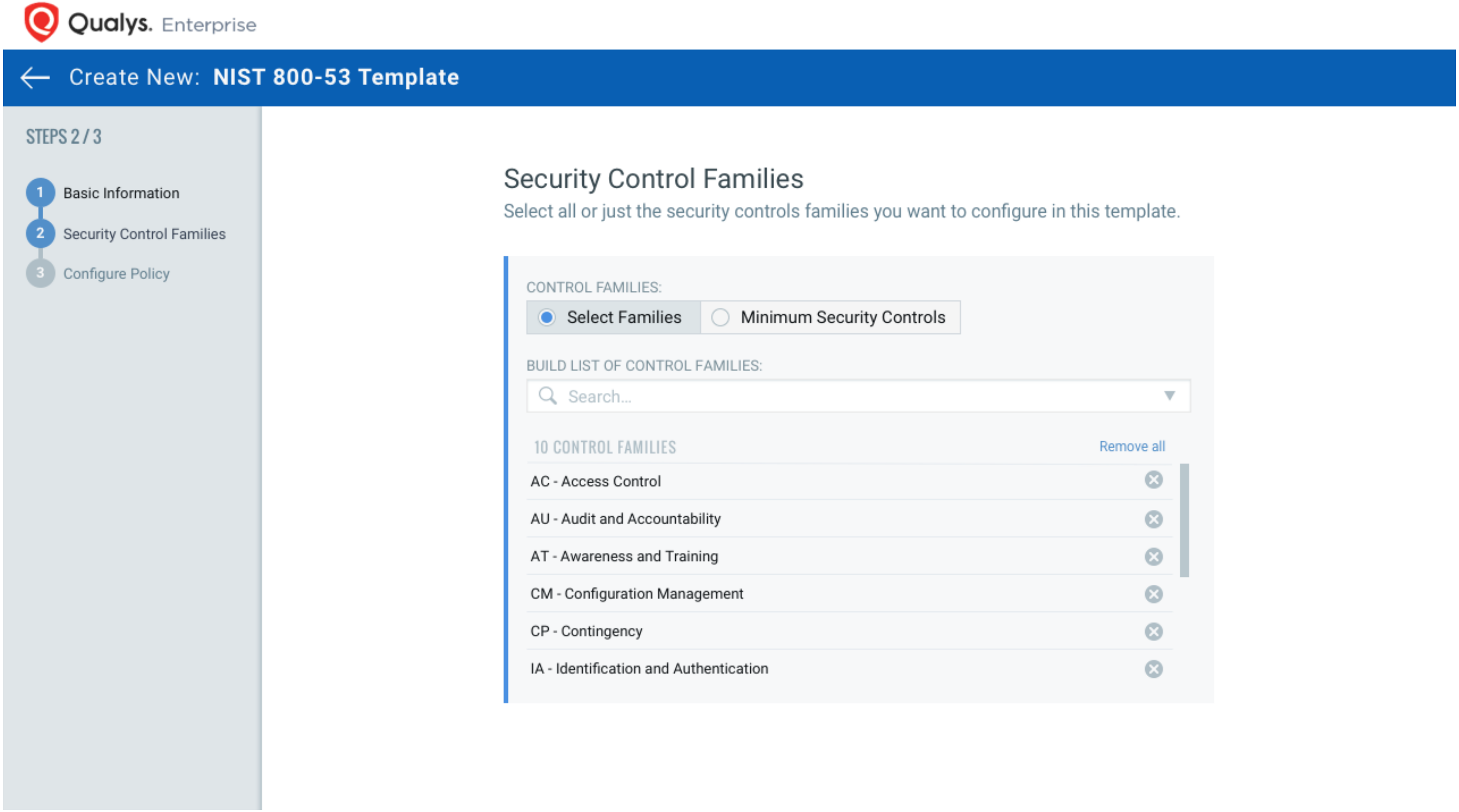
□ AU - Audit and Accountability

□ AT - Awareness and Training

□ CM - Configuration Management

□ CP - Contingency

□ IA - Identification and Authentication



Qualys. Enterprise

← Create New: **NIST 800-53 Template**

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:

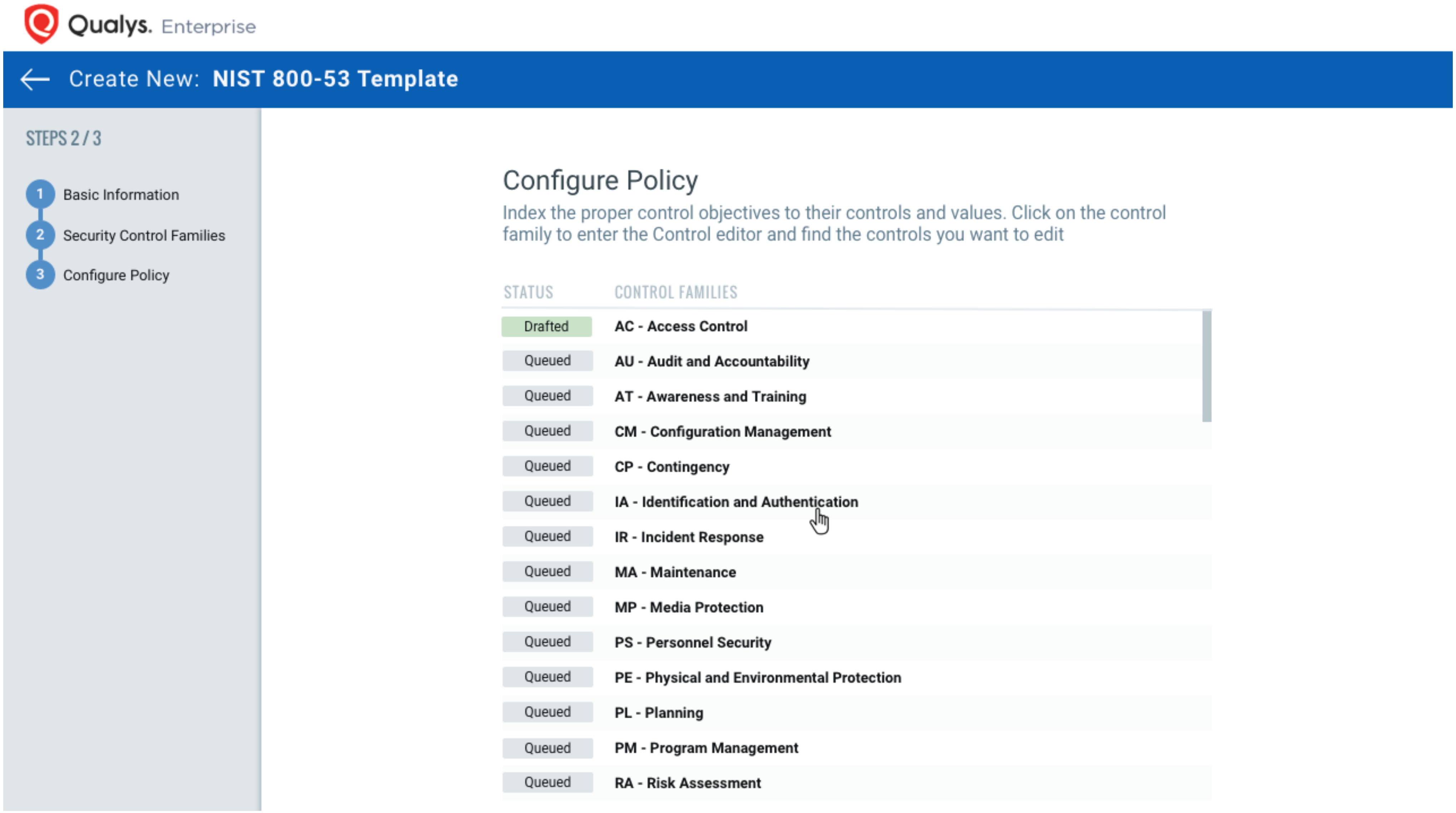
● Select Families ○ Minimum Security Controls

BUILD LIST OF CONTROL FAMILIES:

Search...

10 CONTROL FAMILIES Remove all

- AC - Access Control ⊗
- AU - Audit and Accountability ⊗
- AT - Awareness and Training ⊗
- CM - Configuration Management ⊗
- CP - Contingency ⊗
- IA - Identification and Authentication ⊗



Qualys. Enterprise

Create New: **NIST 800-53 Template**

STEPS 2 / 3

1 Basic Information

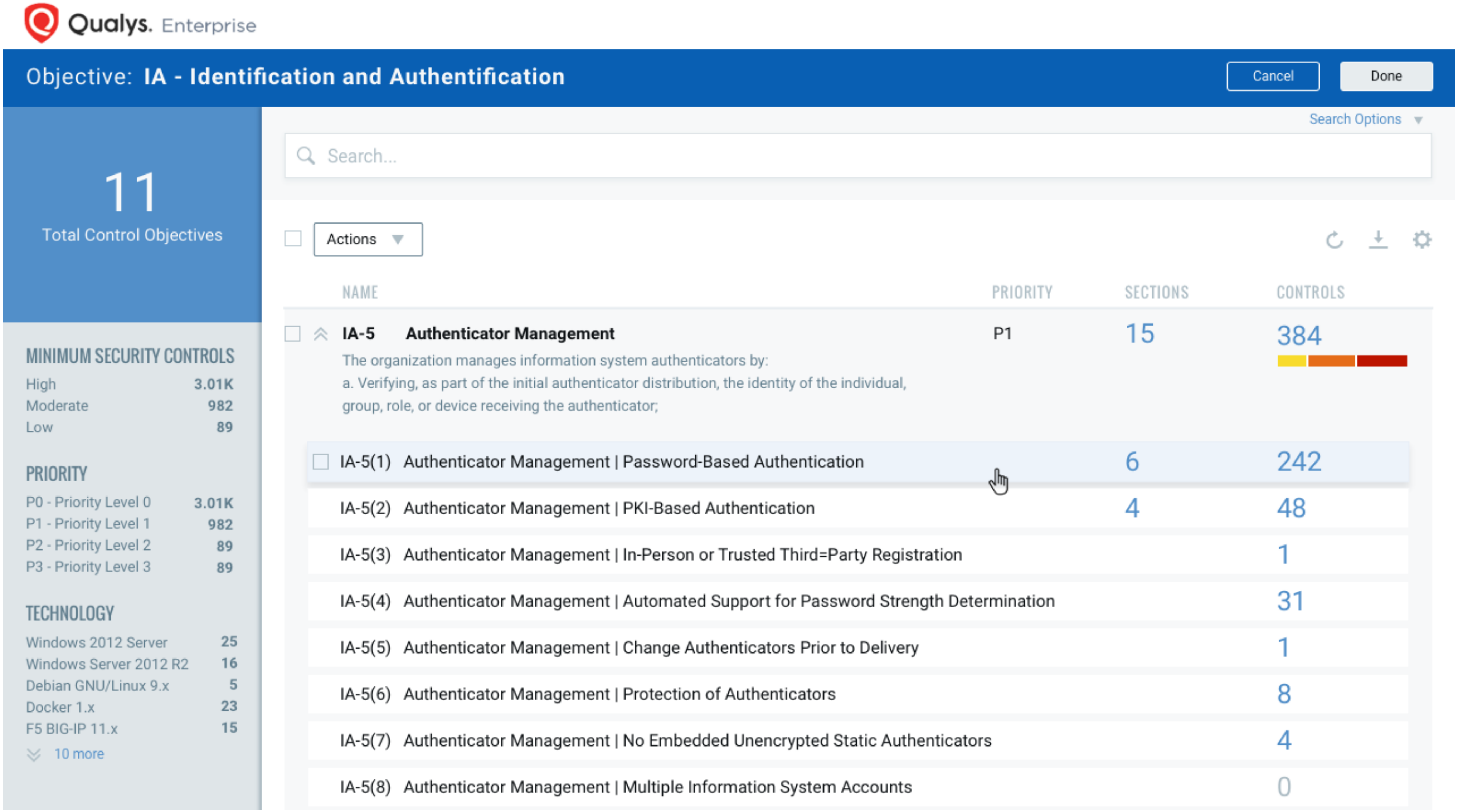
2 Security Control Families

3 Configure Policy

Configure Policy

Index the proper control objectives to their controls and values. Click on the control family to enter the Control editor and find the controls you want to edit

STATUS	CONTROL FAMILIES
Drafted	**AC - Access Control**
Queued	**AU - Audit and Accountability**
Queued	**AT - Awareness and Training**
Queued	**CM - Configuration Management**
Queued	**CP - Contingency**
Queued	**IA - Identification and Authentication**
Queued	**IR - Incident Response**
Queued	**MA - Maintenance**
Queued	**MP - Media Protection**
Queued	**PS - Personnel Security**
Queued	**PE - Physical and Environmental Protection**
Queued	**PL - Planning**
Queued	**PM - Program Management**
Queued	**RA - Risk Assessment**



Objective: **IA - Identification and Authentification**

11
Total Control Objectives

MINIMUM SECURITY CONTROLS

High	3.01K
Moderate	982
Low	89

PRIORITY

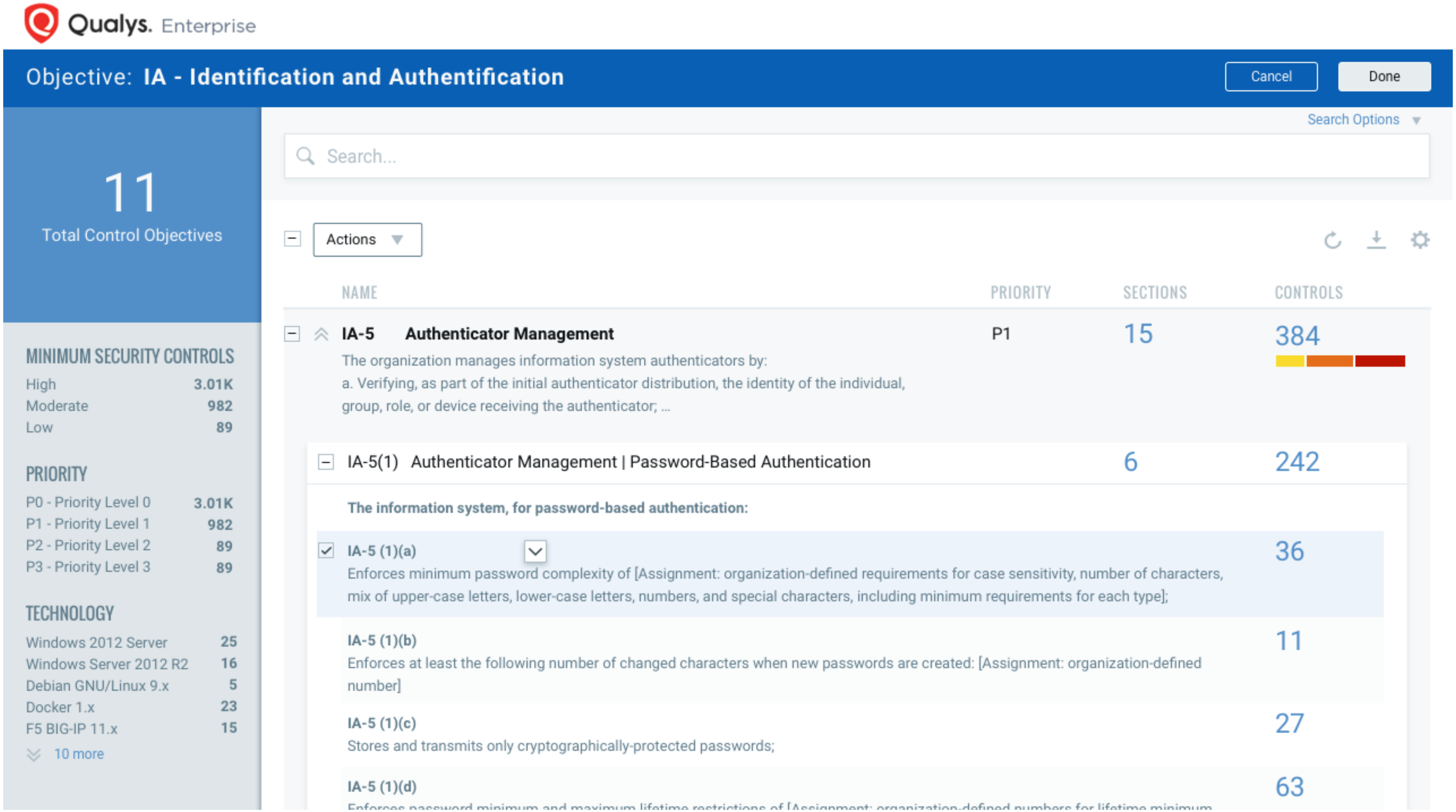
P0 - Priority Level 0	3.01K
P1 - Priority Level 1	982
P2 - Priority Level 2	89
P3 - Priority Level 3	89

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

NAME	PRIORITY	SECTIONS	CONTROLS
□ **IA-5 Authenticator Management** 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;	P1	15	384
□ 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



Qualys. Enterprise

Objective: **IA - Identification and Authentification**

Cancel Done

Search Options ▼

Search...

11
Total Control Objectives

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

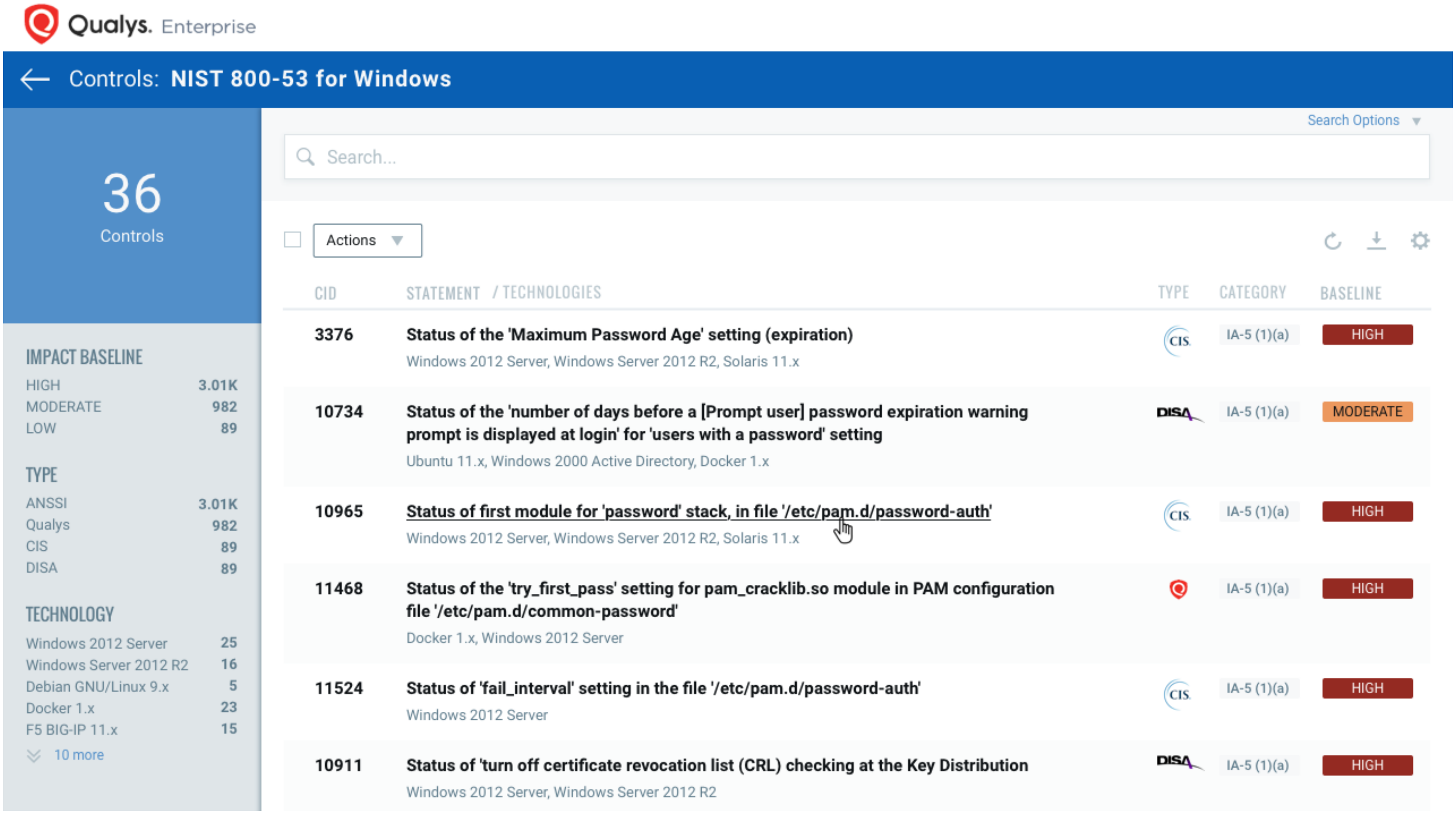
10 more

Actions ▼

NAME	PRIORITY	SECTIONS	CONTROLS
IA-5 Authenticator Management 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; ...	P1	15	384
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



Qualys. Enterprise

Controls: **NIST 800-53 for Windows**

Search Options ▾

Search...

36
Controls

IMPACT BASELINE

HIGH	3.01K
MODERATE	982
LOW	89

TYPE

ANSSI	3.01K
Qualys	982
CIS	89
DISA	89

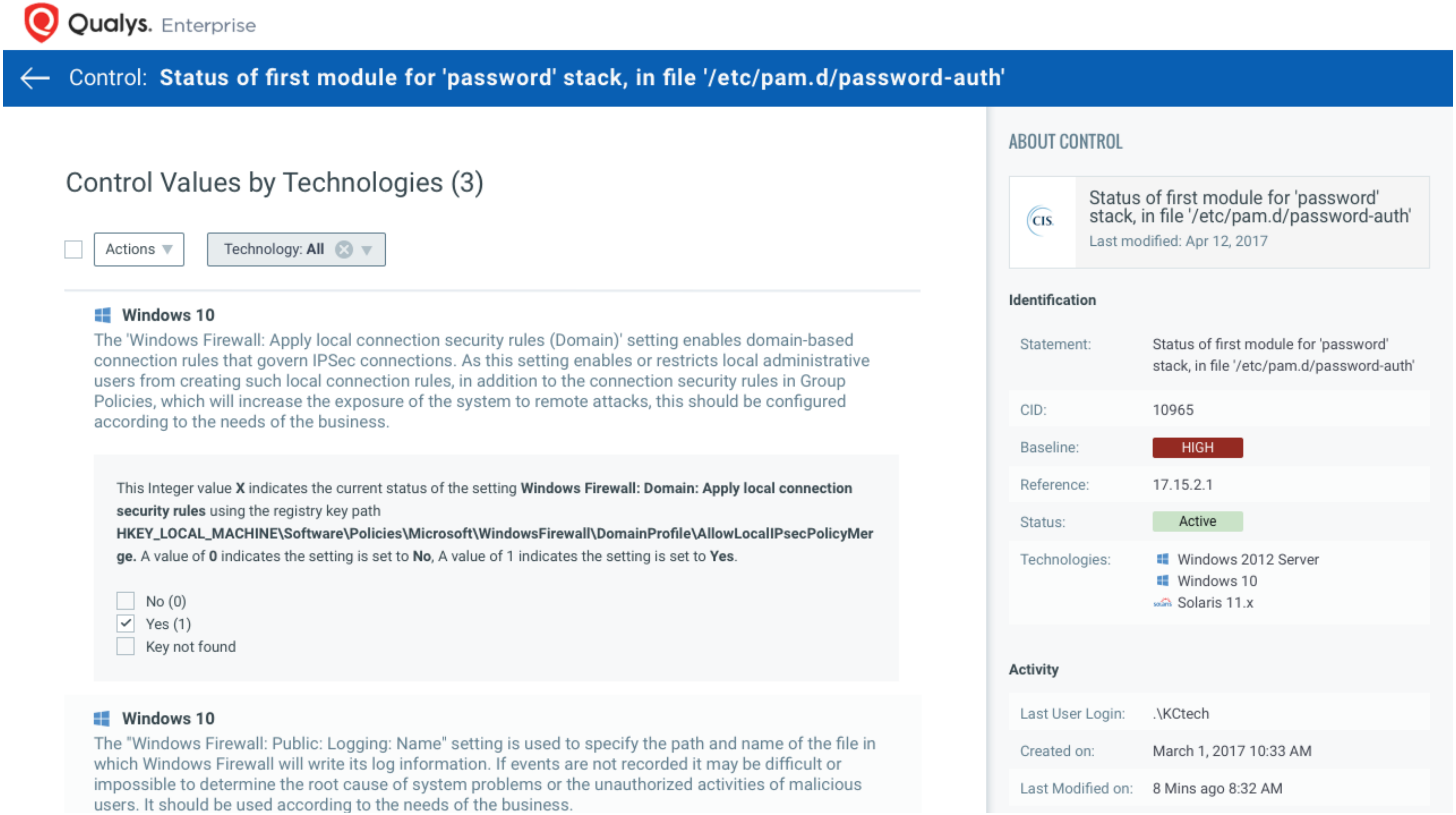
TECHNOLOGY

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

□ 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	CIS	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	DISA	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	CIS	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	CIS	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	DISA	IA-5 (1)(a)	HIGH



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

Control Values by Technologies (3)

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

CIS — 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

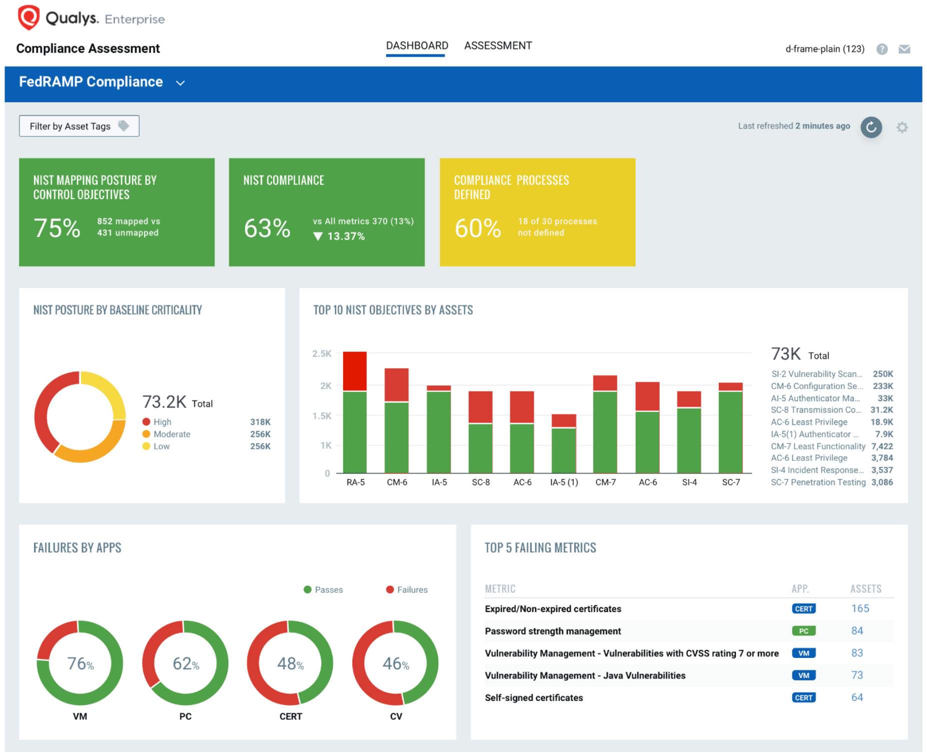
Integration Across the Platform: Unified Compliance Assessment

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!



Qualys. Enterprise

Compliance Assessment

Last refreshed **2 minutes ago**

NIST MAPPING POSTURE BY CONTROL OBJECTIVES
75% 852 mapped vs 431 unmapped

NIST COMPLIANCE
63% vs All metrics 370 (13%) ▼ 13.37%

COMPLIANCE PROCESSES DEFINED
60% 18 of 30 processes not defined

NIST POSTURE BY BASELINE CRITICALITY

73.2K Total

● High	318K
● Moderate	256K
● Low	256K

TOP 10 NIST OBJECTIVES BY ASSETS

73K Total

SI-2 Vulnerability Scan...	250K
CM-6 Configuration Se...	233K
AI-5 Authenticator Ma...	33K
SC-8 Transmission Co...	31.2K
AC-6 Least Privilege	18.9K
IA-5(1) Authenticator ...	7.9K
CM-7 Least Functionality	7,422
AC-6 Least Privilege	3,784
SI-4 Incident Response...	3,537
SC-7 Penetration Testing	3,086

FAILURES BY APPS

TOP 5 FAILING METRICS

METRIC	APP.	ASSETS
Expired/Non-expired certificates	CERT	165
Password strength management	PC	84
Vulnerability Management - Vulnerabilities with CVSS rating 7 or more	VM	83
Vulnerability Management - Java Vulnerabilities	VM	73
Self-signed certificates	CERT	64

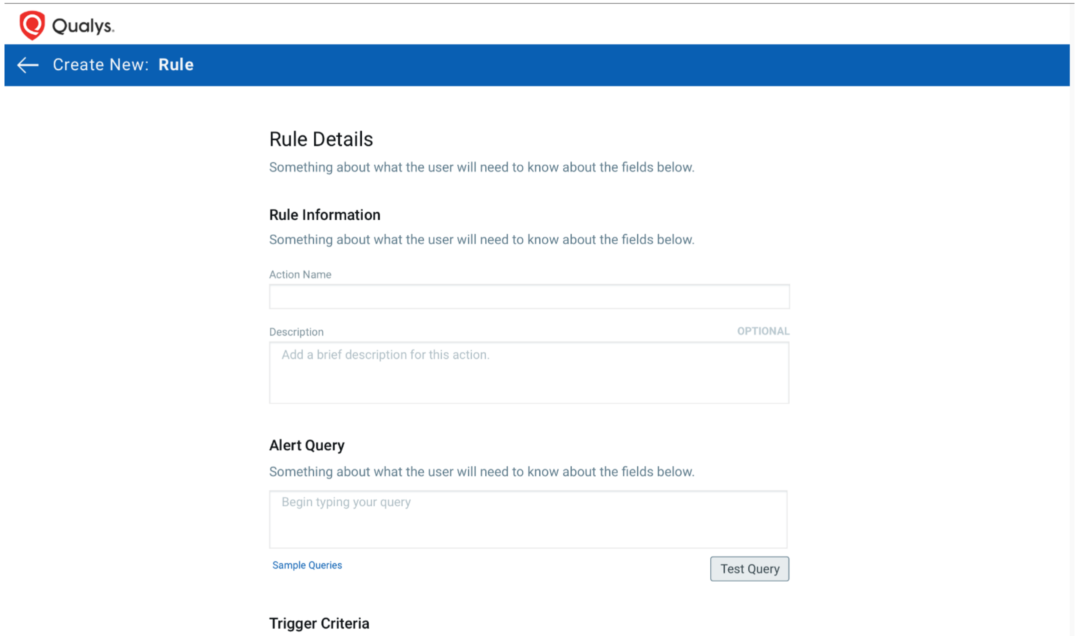
Defining Metrics & Mappings

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



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

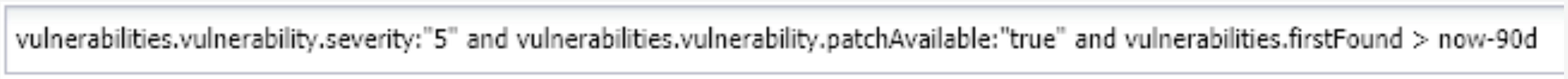
Add a brief description for this action.

Alert Query

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

Begin typing your query

Trigger Criteria



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

Security Metric Examples

High Severity Vulnerabilities/ Patching

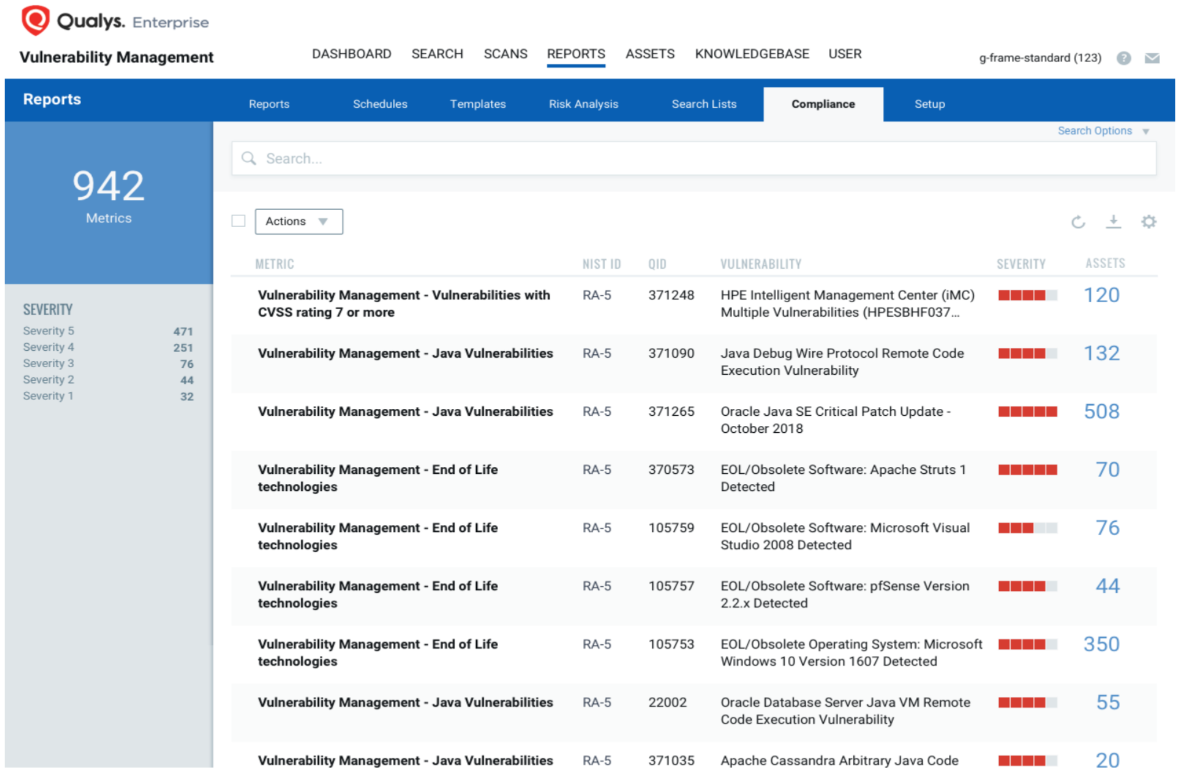
FIM Incident Review Expired

Cloud Security Configuration Issues

Expired or Self-Signed Certificates

Vendor Risk – Failure to Respond

Procedural Control Gap Identified



942
Metrics

SEVERITY

Severity 5	471
Severity 4	251
Severity 3	76
Severity 2	44
Severity 1	32

METRIC	NIST ID	QID	VULNERABILITY	SEVERITY	ASSETS
Vulnerability Management - Vulnerabilities with CVSS rating 7 or more	RA-5	371248	HPE Intelligent Management Center (iMC) Multiple Vulnerabilities (HPESBHF037…	🟥🟥🟥🟥⬜	120
Vulnerability Management - Java Vulnerabilities	RA-5	371090	Java Debug Wire Protocol Remote Code Execution Vulnerability	🟥🟥🟥🟥⬜	132
Vulnerability Management - Java Vulnerabilities	RA-5	371265	Oracle Java SE Critical Patch Update - October 2018	🟥🟥🟥🟥🟥	508
Vulnerability Management - End of Life technologies	RA-5	370573	EOL/Obsolete Software: Apache Struts 1 Detected	🟥🟥🟥🟥🟥	70
Vulnerability Management - End of Life technologies	RA-5	105759	EOL/Obsolete Software: Microsoft Visual Studio 2008 Detected	🟥🟥🟥⬜⬜	76
Vulnerability Management - End of Life technologies	RA-5	105757	EOL/Obsolete Software: pfSense Version 2.2.x Detected	🟥🟥🟥🟥⬜	44
Vulnerability Management - End of Life technologies	RA-5	105753	EOL/Obsolete Operating System: Microsoft Windows 10 Version 1607 Detected	🟥🟥🟥🟥⬜	350
Vulnerability Management - Java Vulnerabilities	RA-5	22002	Oracle Database Server Java VM Remote Code Execution Vulnerability	🟥🟥🟥🟥⬜	55
Vulnerability Management - Java Vulnerabilities	RA-5	371035	Apache Cassandra Arbitrary Java Code	🟥🟥🟥🟥⬜	20

Demo

PC

Policy Compliance

Qualys. Enterprise

Vulnerability Management

942
Metrics

SEVERITY	
Severity 5	471
Severity 4	251
Severity 3	76
Severity 2	44
Severity 1	32

METRIC	NIST ID	QID	VULNERABILITY	SEVERITY	ASSETS
Vulnerability Management - Vulnerabilities with CVSS rating 7 or more	RA-5	[illegible]	HPE Intelligent Management Center (iMC) Multiple Vulnerabilities (HPESBHF037...	■■■■	120
Vulnerability Management - Java Vulnerabilities	RA-5	371090	Java Debug Wire Protocol Remote Code Execution Vulnerability	■■■■	132
Vulnerability Management - Java Vulnerabilities	RA-5	371265	Oracle Java SE Critical Patch Update - October 2018	■■■■■	508
Vulnerability Management - End of Life technologies	RA-5	370573	EOL/Obsolete Software: Apache Struts 1 Detected	■■■■■	70
Vulnerability Management - End of Life technologies	RA-5	105759	EOL/Obsolete Software: Microsoft Visual Studio 2008 Detected	■■■	76
Vulnerability Management - End of Life technologies	RA-5	105757	EOL/Obsolete Software: pfSense Version 2.2.x Detected	■■■■	44
Vulnerability Management - End of Life technologies	RA-5	105753	EOL/Obsolete Operating System: Microsoft Windows 10 Version 1607 Detected	■■■■	350

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

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

What Are Customers Monitoring?

Critical Operating System Binaries

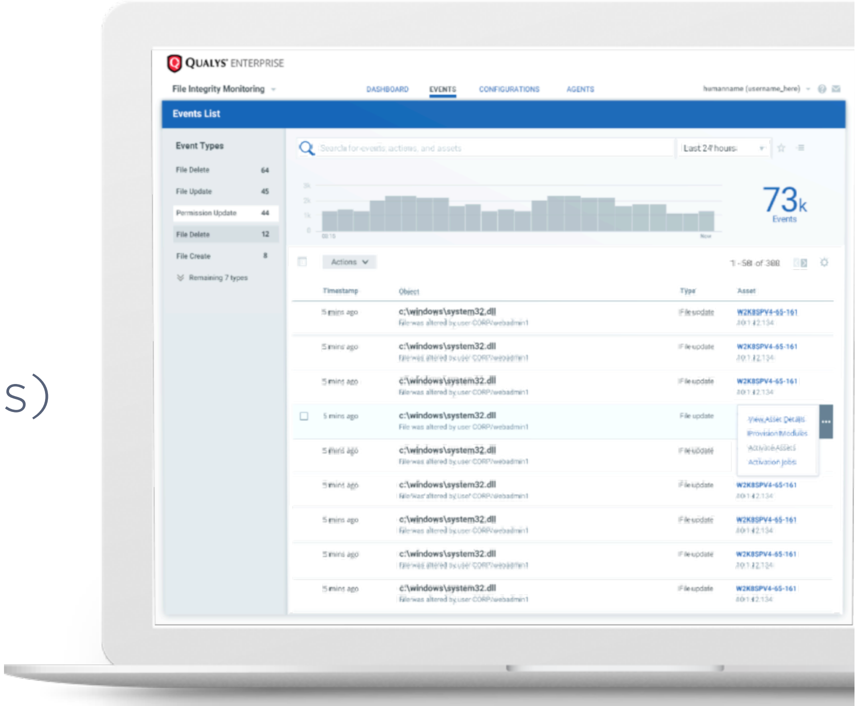
OS and Application Configuration Files

Content, such as Web source

Permissions (such as on Database Stores)

Security Data (Logs, Folder Audit Settings)

User & Authentication Configurations



Events List

Event Types	
File Delete	64
File Update	45
Permission Update	44
File Delete	12
File Create	8
Remaining 7 types	

Timestamp	Object	Type	Asset
5 mins ago	c:\windows\system32.dll File was altered by user CORP/webadmin1	File update	W2K8SPV4-65-161 10.1.12.134
5 mins ago	c:\windows\system32.dll File was altered by user CORP/webadmin1	File update	W2K8SPV4-65-161 10.1.12.134
5 mins ago	c:\windows\system32.dll File was altered by user CORP/webadmin1	File update	W2K8SPV4-65-161 10.1.12.134
5 mins ago	c:\windows\system32.dll File was altered by user CORP/webadmin1	File update	
5 mins ago	c:\windows\system32.dll File was altered by user CORP/webadmin1	File update	
5 mins ago	c:\windows\system32.dll File was altered by user CORP/webadmin1	File update	W2K8SPV4-65-161 10.1.12.134
5 mins ago	c:\windows\system32.dll File was altered by user CORP/webadmin1	File update	W2K8SPV4-65-161 10.1.12.134
5 mins ago	c:\windows\system32.dll File was altered by user CORP/webadmin1	File update	W2K8SPV4-65-161 10.1.12.134
5 mins ago	c:\windows\system32.dll File was altered by user CORP/webadmin1	File update	W2K8SPV4-65-161 10.1.12.134

FIM Challenges

Deciding what depth to monitor

Tuning out noise, but not missing important events

Scalability of legacy solutions

Meeting auditor event review requirements

Improvements since GA

Event Review & Incident Management Workflow

Library Content Improvements

AuditD Compatible Windows Agent (2.1.x)

Windows Feature Expansion & Updated Driver (2.1.x)

Several back-end releases for operational improvements & feature support

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

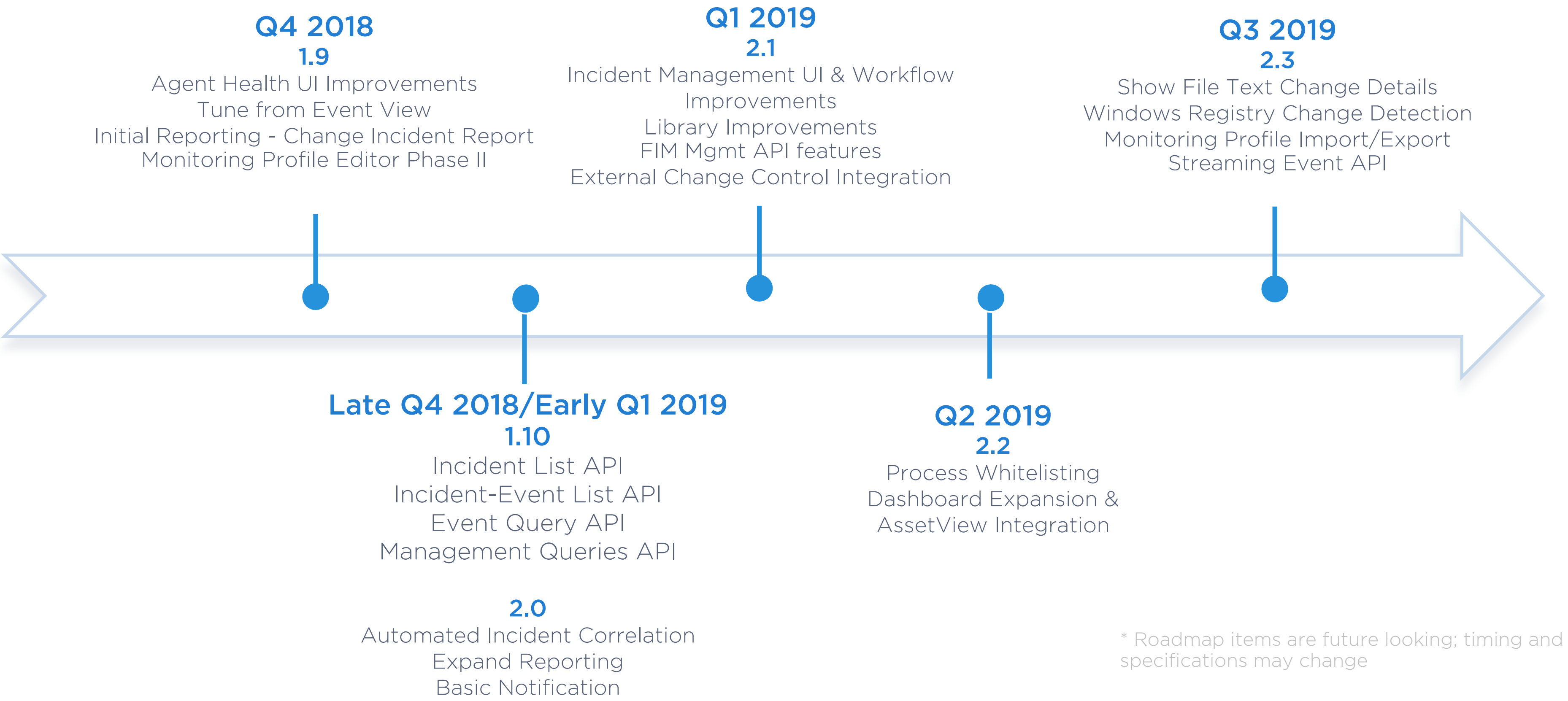
Expanded Platform Support

Demo

FIM

Policy Compliance

FIM Feature Roadmap



Q4 2018
1.9
Agent Health UI Improvements
Tune from Event View
Initial Reporting - Change Incident Report
Monitoring Profile Editor Phase II

Late Q4 2018/Early Q1 2019
1.10
Incident List API
Incident-Event List API
Event Query API
Management Queries API

2.0
Automated Incident Correlation
Expand Reporting
Basic Notification

Q1 2019
2.1
Incident Management UI & Workflow Improvements
Library Improvements
FIM Mgmt API features
External Change Control Integration

Q2 2019
2.2
Process Whitelisting
Dashboard Expansion & AssetView Integration

Q3 2019
2.3
Show File Text Change Details
Windows Registry Change Detection
Monitoring Profile Import/Export
Streaming Event API

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

Thank You

Tim White
twhite@qualys.com