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
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
<table>
<thead>
<tr>
<th>NIST Control</th>
<th>NIST Control Objective</th>
<th>Qualys Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>CM</td>
<td>Information System Component Inventory</td>
<td>AI, SYN</td>
</tr>
<tr>
<td>CM</td>
<td>Inventory of Authorized and Unauthorized Software</td>
<td>AI, SYN, VM, PC</td>
</tr>
<tr>
<td>CM</td>
<td>Secure Configuration for Hardware and Software</td>
<td>TP</td>
</tr>
<tr>
<td>RA-5</td>
<td>Continuous Vulnerability Assessment &amp; Remediation</td>
<td>VM, PC, TP, CM</td>
</tr>
<tr>
<td>AC, IA</td>
<td>Controlled Used of Administrative Privileges</td>
<td>PC</td>
</tr>
<tr>
<td>AU</td>
<td>Maintenance, Monitoring and Analysis of Audit Logs</td>
<td>PC, FIM</td>
</tr>
<tr>
<td>AC</td>
<td>Email and Web Browser Protection</td>
<td>VM, PC, SAQ</td>
</tr>
<tr>
<td>SI-4</td>
<td>Malware Defense</td>
<td>PC, IOC, WAS, WAF, FIM</td>
</tr>
<tr>
<td>CM, SA</td>
<td>Limitation and Control of Network Ports</td>
<td>VM, PC, CM, WAF</td>
</tr>
<tr>
<td>CP</td>
<td>Data Recovery Capability</td>
<td>PC, SAQ</td>
</tr>
<tr>
<td>CM, RA</td>
<td>Secure Configurations for Network Devices</td>
<td>VM, PC</td>
</tr>
<tr>
<td>NIST Control</td>
<td>NIST Control Objective</td>
<td>Qualys Applications</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------------------------------------------------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>AC, SI</td>
<td>Boundary Defense</td>
<td>VM, PC, CS, WAS, WAF</td>
</tr>
<tr>
<td>AU</td>
<td>Maintenance, Monitoring, and Analysis of Audit Logs</td>
<td>PC, FIM</td>
</tr>
<tr>
<td>AC, IA</td>
<td>Controlled Access Based on the Need to Know</td>
<td>PC, CS</td>
</tr>
<tr>
<td>AC-17, AC-18</td>
<td>Wireless Access Control</td>
<td>VM</td>
</tr>
<tr>
<td>AC, IA</td>
<td>Account Monitoring and Control</td>
<td>PC, SAQ</td>
</tr>
<tr>
<td>AT</td>
<td>Security Skills Assessment and Appropriate Training to Fill Gaps</td>
<td>SAQ</td>
</tr>
<tr>
<td>RA, CM</td>
<td>Vendor Controls Assessment</td>
<td>IOC, CS, WAS, WAF</td>
</tr>
<tr>
<td>IR</td>
<td>Incident Response and Management</td>
<td>PC, IOC, FIM</td>
</tr>
<tr>
<td>CA</td>
<td>Penetration Tests and Red Team Exercises</td>
<td>VM, TP, IOC</td>
</tr>
</tbody>
</table>
They started with critical requirements for Quick Wins…

1. Inventory Your Systems
2. Inventory and Restrict Software
3. Secure Configurations
4. Continuous Vulnerability Management
5. Review Rights & Permissions
6. Definition, Automated Evaluation & Review of Processes
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

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!
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
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)
Then, Configure Pass/Fail Criteria

Define a Post-Filter, Then Evaluate based on:
- Empty Result Set
- Row Count Threshold
- Always Pass/Fail (for data gathering)
- Match Column Criteria
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
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.
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:
- Select all (14 families)
- AC - Access Control
- AU - Audit and Accountability
- AT - Awareness and Training
- CM - Configuration Management
- CP - Contingency
- IA - Identification and Authentication

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

<table>
<thead>
<tr>
<th>CONTROL FAMILIES</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>[ ] Select Families</td>
<td></td>
</tr>
<tr>
<td>[ ] Minimum Security Controls</td>
<td></td>
</tr>
</tbody>
</table>

BUILD LIST OF CONTROL FAMILIES:

**10 CONTROL FAMILIES**

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

Remove all
## 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.

<table>
<thead>
<tr>
<th>STATUS</th>
<th>CONTROL FAMILIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drafted</td>
<td>AC - Access Control</td>
</tr>
<tr>
<td>Queued</td>
<td>AU - Audit and Accountability</td>
</tr>
<tr>
<td>Queued</td>
<td>AT - Awareness and Training</td>
</tr>
<tr>
<td>Queued</td>
<td>CM - Configuration Management</td>
</tr>
<tr>
<td>Queued</td>
<td>CP - Contingency</td>
</tr>
<tr>
<td>Queued</td>
<td>IA - Identification and Authentication</td>
</tr>
<tr>
<td>Queued</td>
<td>IR - Incident Response</td>
</tr>
<tr>
<td>Queued</td>
<td>MA - Maintenance</td>
</tr>
<tr>
<td>Queued</td>
<td>MP - Media Protection</td>
</tr>
<tr>
<td>Queued</td>
<td>PS - Personnel Security</td>
</tr>
<tr>
<td>Queued</td>
<td>PE - Physical and Environmental Protection</td>
</tr>
<tr>
<td>Queued</td>
<td>PL - Planning</td>
</tr>
<tr>
<td>Queued</td>
<td>PM - Program Management</td>
</tr>
<tr>
<td>Queued</td>
<td>RA - Risk Assessment</td>
</tr>
</tbody>
</table>
### Objective: IA - Identification and Authentication

Total Control Objectives: 11

<table>
<thead>
<tr>
<th>Name</th>
<th>Priority</th>
<th>Sections</th>
<th>Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IA-5</strong> Authenticator Management</td>
<td>P1</td>
<td>15</td>
<td>384</td>
</tr>
<tr>
<td><strong>IA-5(1)</strong> Authenticator Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>IA-5(2)</strong> Authenticator Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>IA-5(3)</strong> Authenticator Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>IA-5(4)</strong> Authenticator Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>IA-5(5)</strong> Authenticator Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>IA-5(6)</strong> Authenticator Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>IA-5(7)</strong> Authenticator Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>IA-5(8)</strong> Authenticator Management</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### 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**

**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


**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;

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

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];

- **IA-5 (1)(b)** Enforces at least the following number of changed characters when new passwords are created: [Assignment: organization-defined number]

- **IA-5 (1)(c)** Stores and transmits only cryptographically protected passwords;

- **IA-5 (1)(d)** Enforces password minimum and maximum lifetime restrictions of [Assignment: organization-defined numbers for lifetime minimum]
### Controls: NIST 800-53 for Windows

#### Impact Baseline
- **High**: 3,018
- **Moderate**: 982
- **Low**: 89

#### Type
- ANSI: 3,018
- 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
- FS Big-IP 11.x: 15
- 10 more

<table>
<thead>
<tr>
<th>CID</th>
<th>Statement / Technologies</th>
<th>Type</th>
<th>Category</th>
<th>Baseline</th>
</tr>
</thead>
<tbody>
<tr>
<td>3376</td>
<td>Status of the 'Maximum Password Age' setting (expiration)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows 2012 Server, Windows Server 2012 R2, Solaris 11.x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10734</td>
<td>Status of the number of days before a [Prompt user] password expiration warning prompt is displayed at login for 'users with a password' setting</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ubuntu 11.x, Windows 2000 Active Directory, Docker 1.x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10965</td>
<td>Status of first module for 'password' stack, in file '/etc/pam.d/password-auth'</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows 2012 Server, Windows Server 2012 R2, Solaris 11.x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11468</td>
<td>Status of the 'try_first_pass' setting for pam_cracklib.so module in PAM configuration file '/etc/pam.d/common-password'</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Docker 1.x, Windows 2012 Server</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11524</td>
<td>Status of 'fail_interval' setting in the file '/etc/pam.d/password-auth'</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows 2012 Server</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10911</td>
<td>Status of 'turn off certificate revocation list (CRL) checking at the Key Distribution'</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows 2012 Server, Windows Server 2012 R2</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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:

\[ HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsFirewall\DomainProfile\AllowLocalIPsecPolicy\Merge. \]

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.
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

```sql
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
Policy Compliance
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
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 Reporting
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

**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