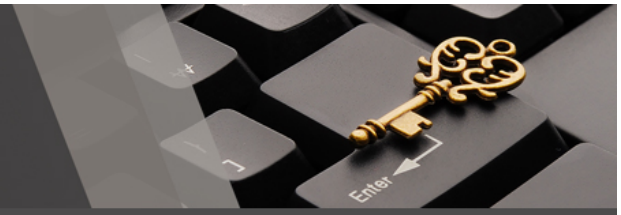
QSC 2019 Presentation

Using Qualys Policy Compliance to Achieve Vulnerability Management Program & Security Compliance Program Goals

By: John Njenga

QSC 2019



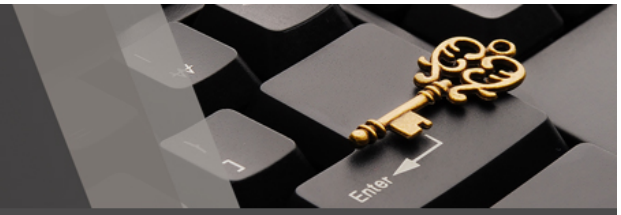
Using Qualys Policy Compliance to Achieve Vulnerability Management Program & Security Risk Compliance Goals

Introduction:

To most Cybersecurity Practitioners it is a well-known fact that the reduction of Security Risks can only be achieved and maintained by practicing;-

- ❑ A rigorous Vulnerability Management & Risk Assessment Program
- ❑ Good Asset Management and Configuration Hygiene
- ❑ Employing layered security defenses

In this session, you will learn a proven approach towards achieving specific VMP, Security Risk and Compliance goals by using the Qualys Policy Compliance for Asset Configuration benchmarking, as well validating controls for Regulatory Compliance requirements (SOX and PCI).

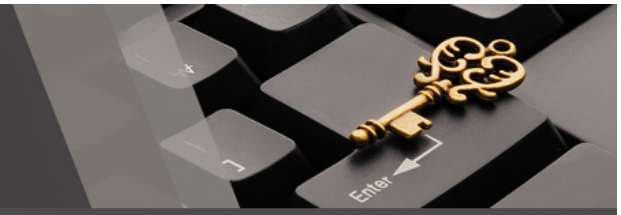


What is Vulnerability Management?

As described in multiple IT Frameworks, Vulnerability Management as an IT domain, focuses on those processes by which organizations **Identify**, **Analyze** and **Manage Vulnerability Risk** within a critical service operating environment.

- Vulnerability Management is one of the core components of a holistic Information Technology Security Program but unfortunately some organizations barely give it the attention it deserves, so unpatched vulnerabilities continue to proliferate within.
- Yet the news headlines are full reports of security and data breaches, which are most often attributed to unpatched or misconfigured IT assets.

Much of the problem involves the maturity of Vulnerability Management Programs and priority given to Vulnerability Management and Risk remediation practices.

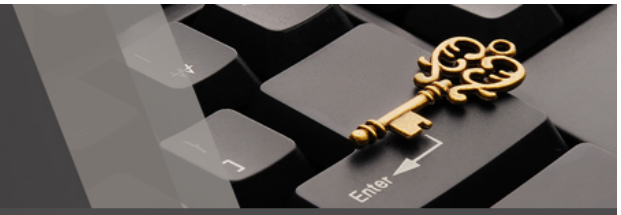


Why is Vulnerability Management Important?

While the Cyber security threat landscape continues to evolve everyday for the worse and with the sophistication of threats increasing daily, Vulnerability Management Strategy and Practices and must adapt quickly.

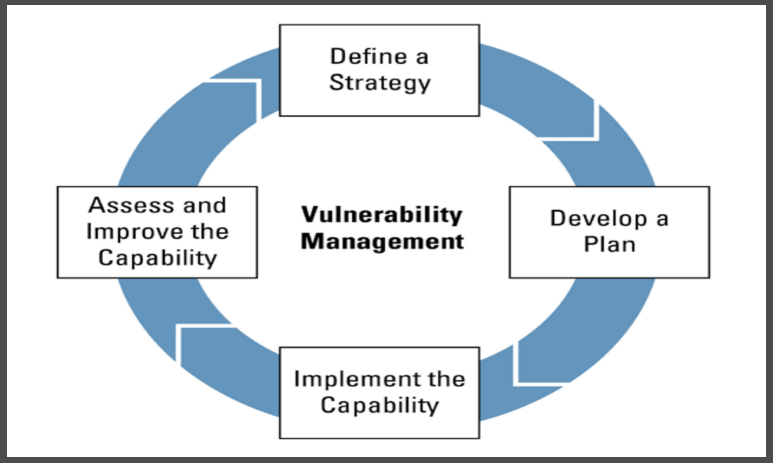
- While many organizations understand that Annual, Quarterly or Periodic scans aren't enough, most struggle with the prioritization of resources to address vulnerability risk.

To create an effective risk-based vulnerability management program and maintain it, every organization must prioritize building an effective vulnerability management strategy to improve capabilities for managing and remediating vulnerability risks.

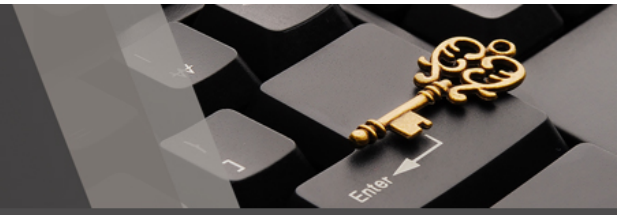


What is Vulnerability Management? (continued.)

An effective Vulnerability Management Program strategy includes these components

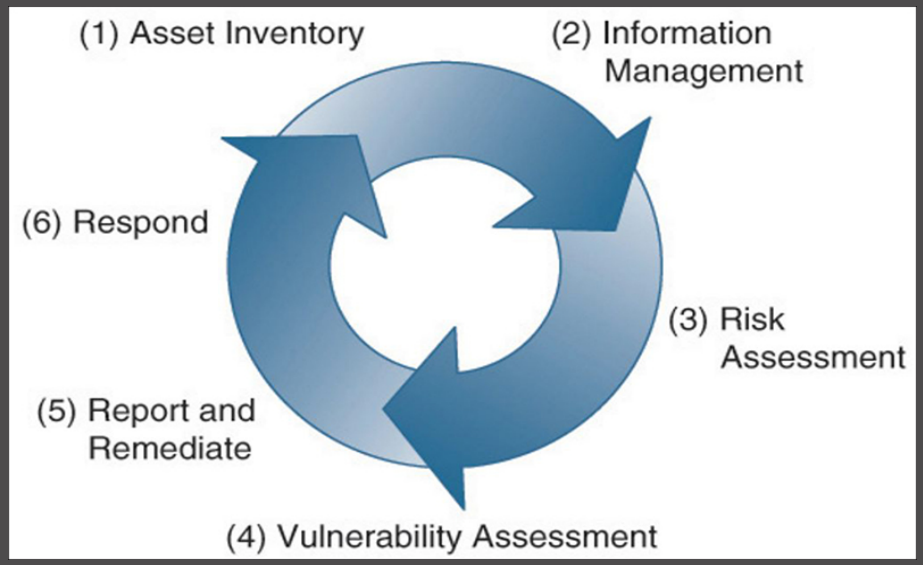


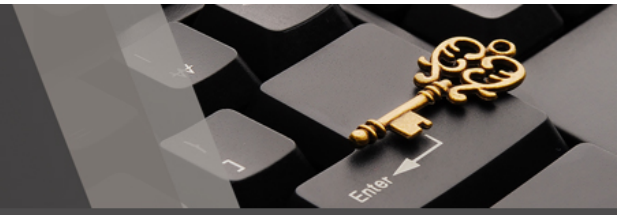
- Define a Vulnerability Analysis and Resolution Strategy
- Develop a Plan for Vulnerability Management
- Implement the Vulnerability Analysis and Resolution Capability
- Assess and Improve the Capability



Vulnerability Management Life Cycle Review

To develop an effective vulnerability management strategy, a continuous review of the vulnerability management life cycle is necessary to assess capabilities as shown in the SANS Vulnerability Management Model below.

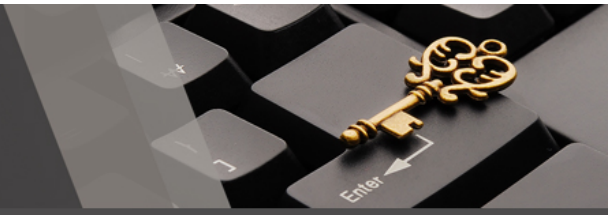




Vulnerability Management Strategy Development

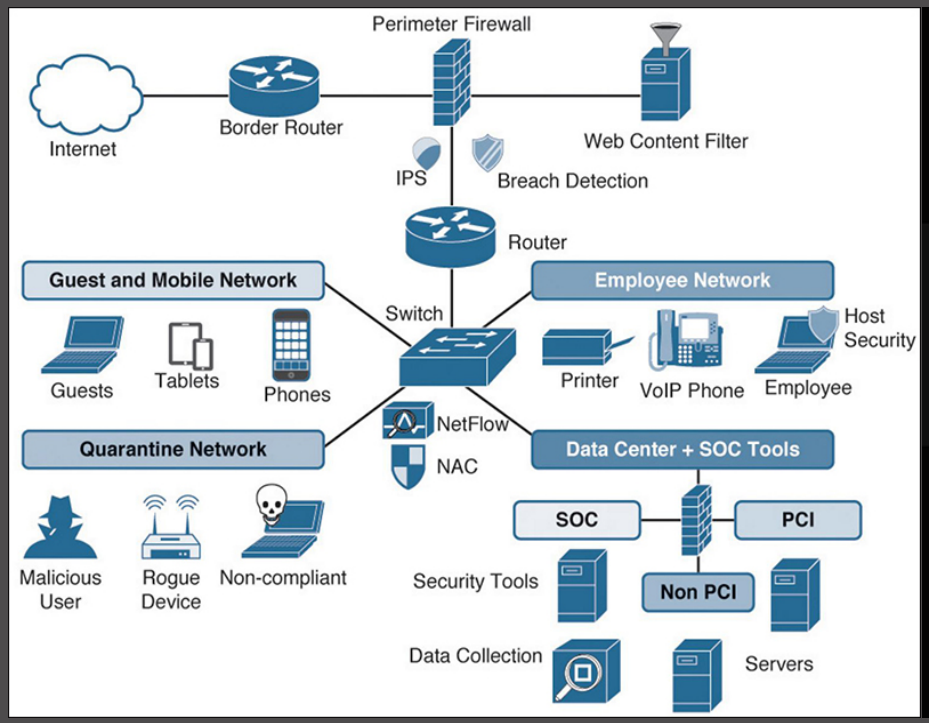
- A review of the vulnerability management lifecycle is required in order to develop an effective strategy and must include an assessment of security technology and tools used to identify and qualify vulnerability risks, as well as the different approaches to calculate how much risk is associated with a threat in order to determine how to mitigate, transfer, accept, or avoid the vulnerability.
- While there are many flavors of security technologies, a recommended best practice advocates making sure that both the security tools and chosen approach leverages layered capabilities, so that if a defense measure fails to detect an attack, another measure or control is available to help prevent the attack.

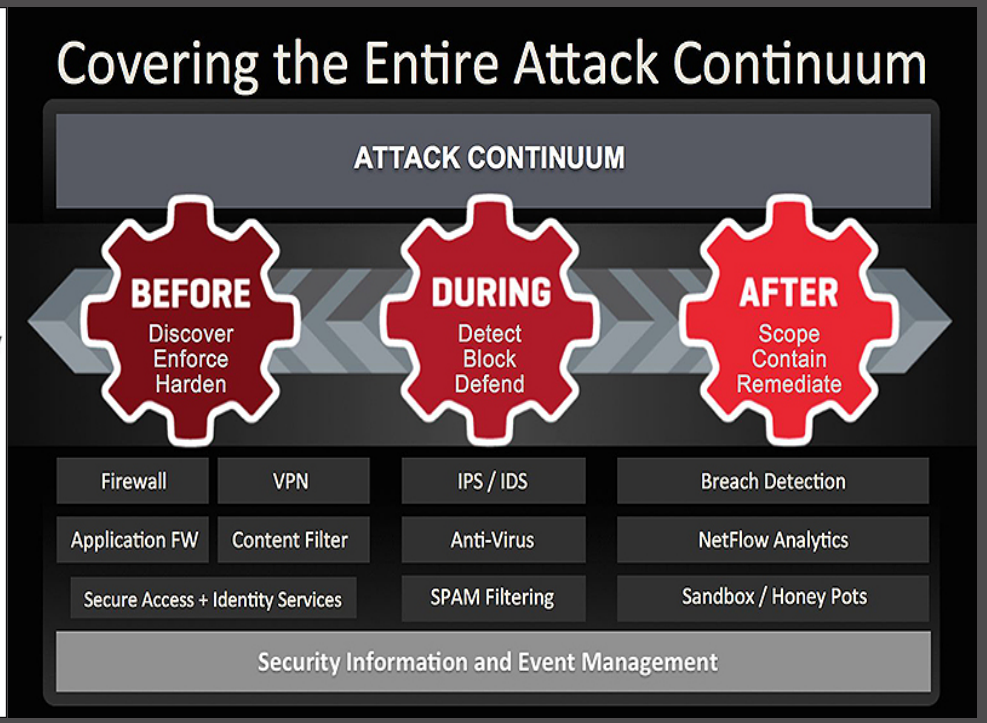
✓ Vulnerability Scanning tools (for assessing the network infrastructure, cloud and container infrastructure)
✓ Static Application Testing (SAST)
✓ Dynamic or Web application Testing (DAST)
✓ Software Composition Analysis (SCA) (for identifying software vulnerabilities)
✓ Other dedicated, specialized monitoring and assessment tools for Business Applications, Mobile, IoT and OT environments.

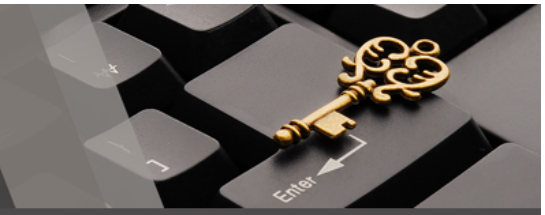


Vulnerability Strategy & Tools Assessment – Layered Approach

Source: J. Muniz http://www.ciscopress.com/articles/printerfriendly/2460771



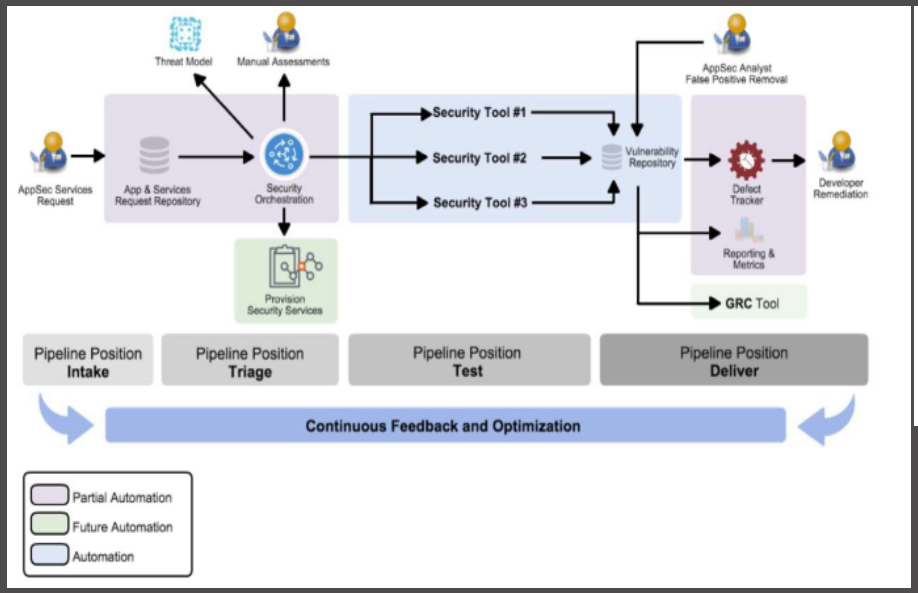


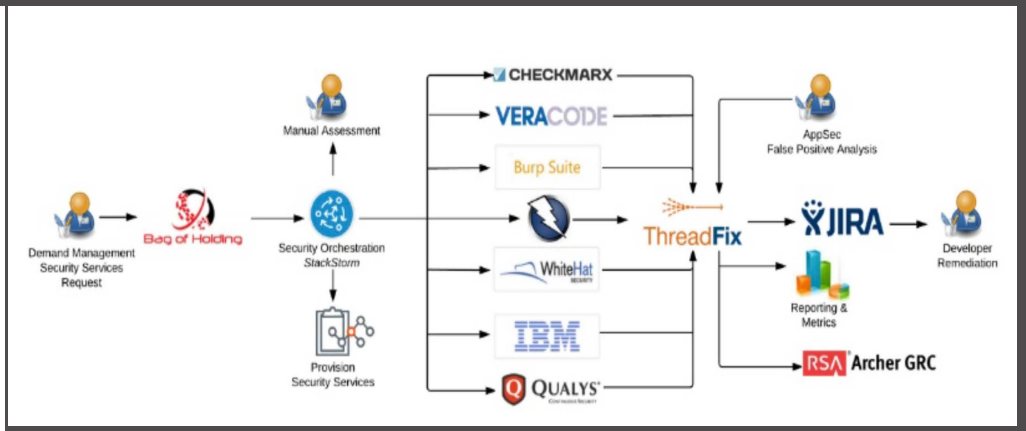


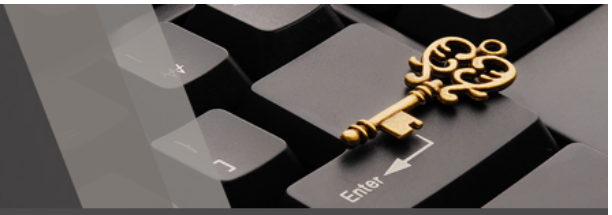
Vulnerability Management Life Cycle Review – Tools in DevOps

Vulnerability Management Lifecycle in a DevOps Environment

Source: https://www.slideshare.net/secfigo/practical-devsecops-course-part-1-82334619



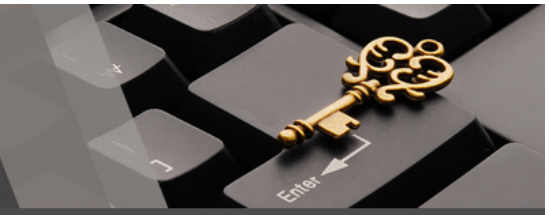




Vulnerability Management Strategy – Tools Capability

The capabilities of the selected tools can also be supplemented with penetration testing or bug bounty programs; however, the effectiveness of a vulnerability management program depends on how well the organization orchestrates them toward the common goal of reducing threats and vulnerability risks posed to the organization.

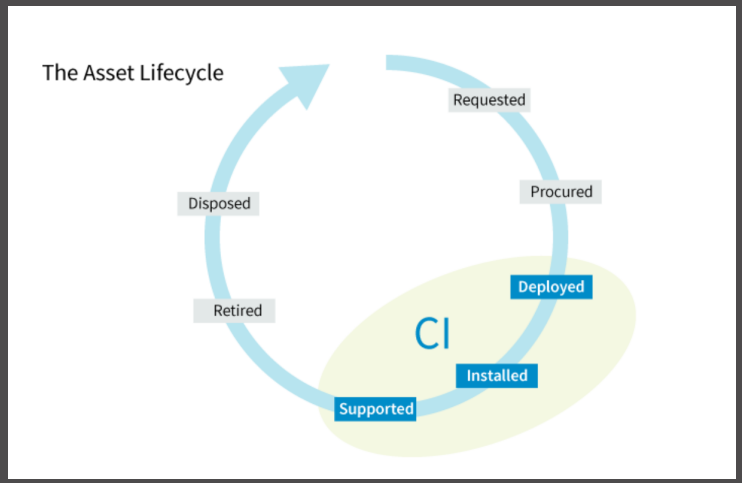
QSC 2019



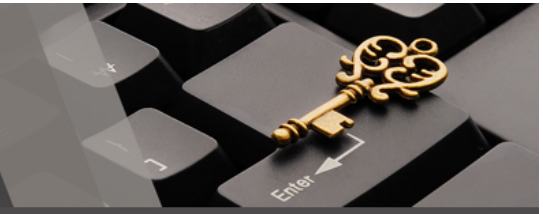
IT Asset Management & Configuration Management Hygiene

What is IT Asset Management?

A process used to Identify, control, record, report, audit and verify a service asset and configuration items, including versions, baselines, constituent components, their attributes, and relationships.

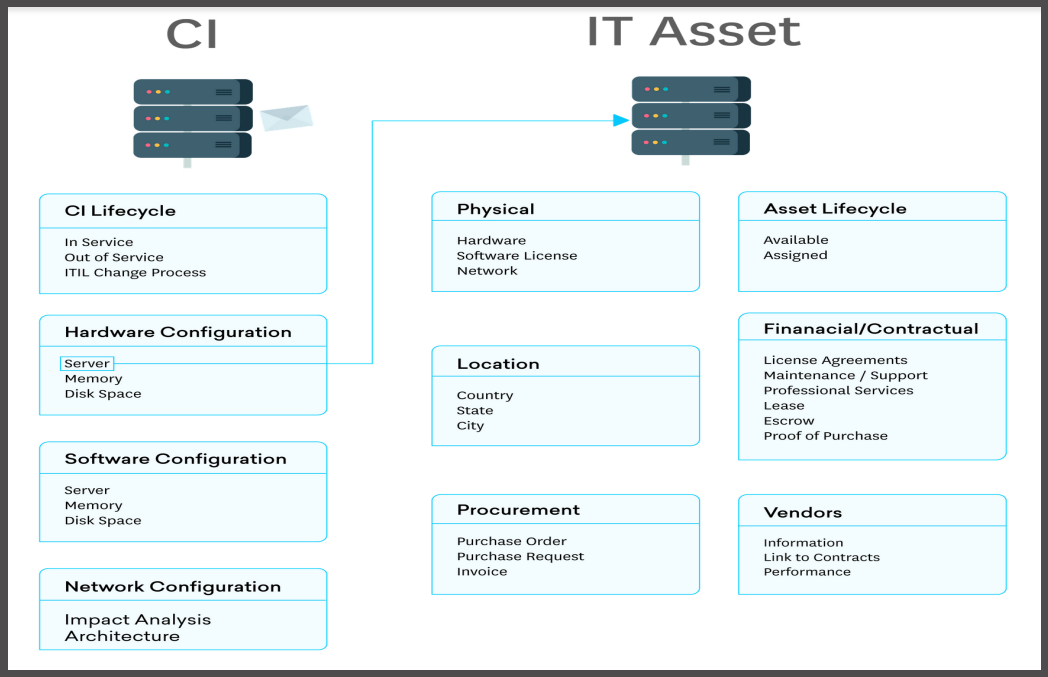


QSC 2019

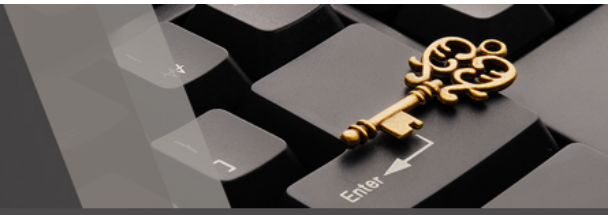


IT Asset Management & Configuration Management Hygiene

What is IT Asset Management & Configuration Item?



QSC 2019

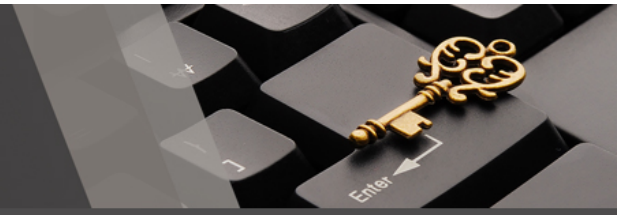


IT Asset Management & Configuration Hygiene

Why is IT Asset Management and Configuration Hygiene Important?

- ✓ Without a clear picture of the IT Assets which exist within an organization, there is no telling, how much exposure an organization has to a potential security attack.
- ✓ IT Asset Management supports a big part of the Vulnerability Management Life Cycle including IT Risk assessment, Vulnerability Patching, Incident Response and Change Configuration.
- ✓ All of these processes make use of the asset management data to ensure completeness and sound decision making.
- ✓ With asset data which is out of date, incomplete or not properly managed within the likelihood of an impact of security events impacting business operations are significantly elevated.

QSC 2019

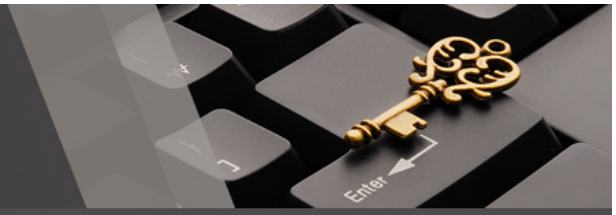


Using Qualys Policy Compliance as a layer for Vulnerability Management

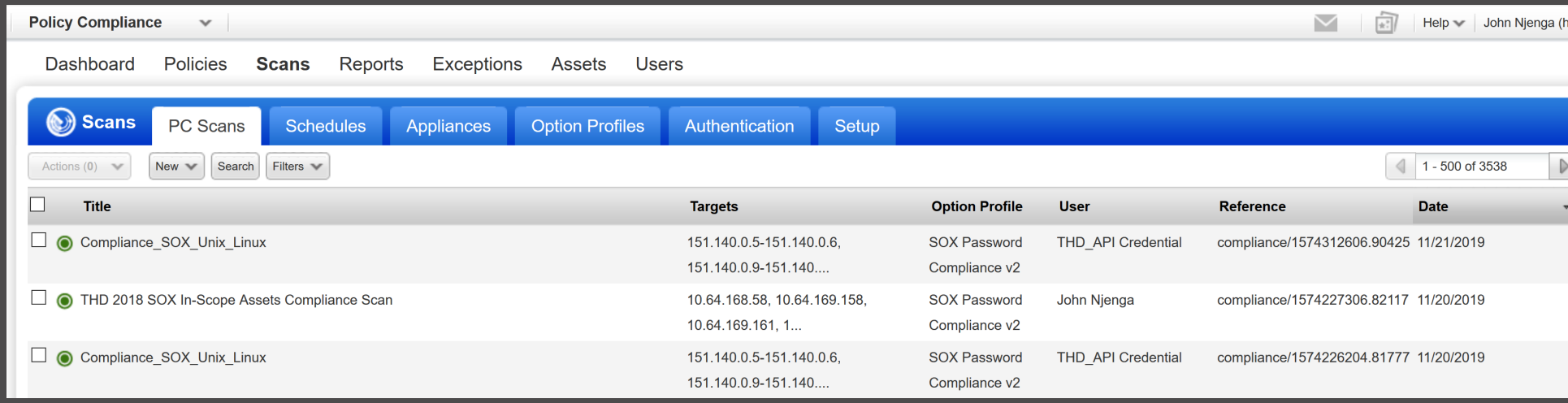
Within our organization we have implemented the Qualys Policy Compliance checks for Baseline Configuration Assessments of our;-

- **On Premise Server Platform Image Build** – We have implemented Baseline configuration checks using CIS Baseline Benchmarks to create Baseline Configuration Policies for use to validate server image builds for adherence to IT Security Policy and Regulatory Requirements.
- **Have implemented SOX Regulatory Policy Controls verification** using Custom Policies to verify our assets in scope are assessed on a weekly basis for adherence.
- **We have also implemented Custom Policies** to verify PCI DSS required controls configuration for all our PCI in scope assets.
- **Assess Network Devices** (Switches/Routers/Firewalls and Printers) against industry Configuration Baseline Benchmarks (CIS/NIST).

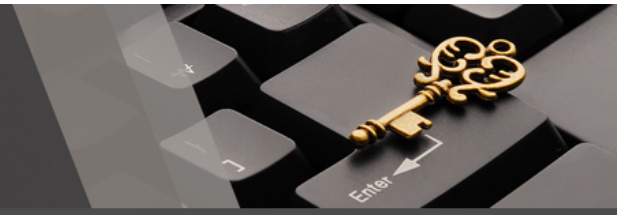
QSC 2019



Using Qualys Policy Compliance as a layer for Vulnerability Management



QSC 2019



Using Qualys Policy Compliance as a layer for Vulnerability Management

Qualys. Enterprise

Policy Compliance Report November 21, 2019

Sox Password Policy Report Scorecard

About Report — **Compliance Scorecard Report**

Report Title: **Compliance Scorecard Report**
Created: **11/21/2019 at 08:01:05 AM (GMT-0500)**
User Name: [redacted]
User Role:

Company:
Address: [redacted]
United States of America

Report Settings — **(10/22/2019-11/21/2019) 30 Day Report**

Template: **Compliance Scorecard Report**
# of Policies: **1**
Asset Groups: **SOX_UNIX_LINUX_2014_Q4**
Asset Tags:

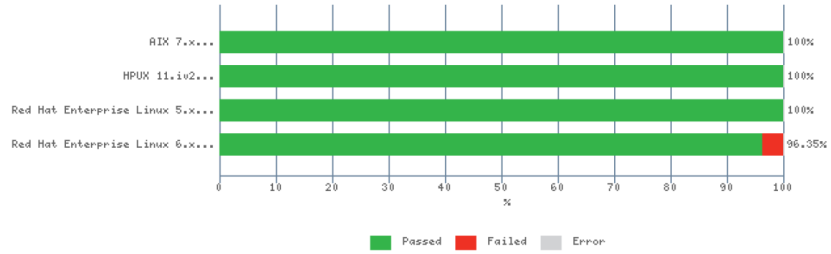
Report Timeframe: **10/22/2019-11/21/2019**
Criticality: **UNDEFINED, MINIMAL, MEDIUM, SERIOUS, CRITICAL, URGENT**

Report Discoveries — **(1) Total Policies**

Overall Compliance
97
Across **1** Unique Policies

Total Controls Detected
516
4 changed

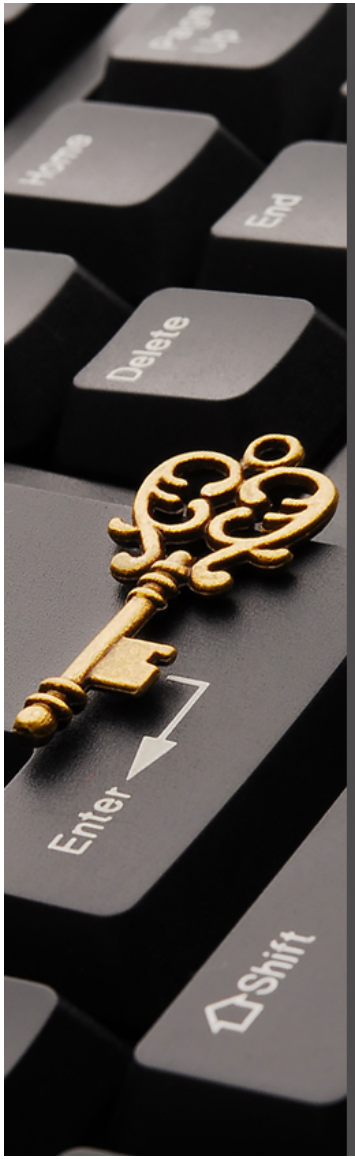
Compliance by Technology (10/22/2019-11/21/2019)



DETAILS(10/22/2019-11/21/2019)

By Technology

Technology	Control Instances	Passed		Failed		Error		Compliance
		Total	Changed	Total	Changed	Total	Changed	%
AIX 7.x	28	28	0	0	0	0	0	100%
HPUX 11.iv2	84	84	0	0	0	0	0	100%
Red Hat Enterprise Linux 5.x	20	20	0	0	0	0	0	100%
Red Hat Enterprise Linux 6.x	384	370	4	14	0	0	0	96.35%



QSC 2019 Presentation

References

1. SANS Paper - Why Your Vulnerability Management Strategy Is Not Working—and What to Do About It. By: Jake Williams April 2019.
2. CERT-CRM Model: https://www.us-cert.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-VM.pdf
3. "The Technology," in Security Operations Center: Building, Operating, and Maintaining Your SOC. J. J. Muniz: http://www.ciscopress.com/articles/printerfriendly/2460771
4. https://blog.opengroup.org/2016/02/05/the-new-generation-it-operating-model/ By: Yan Zhao, Ph.D, President, Chief Architect, ArchiTech Group LLC
5. Qualys Enterprise Platform