Out-of-band Configuration Assessment (OCA)

Make your Inaccessible, Sensitive Assets visible to your Vulnerability and Compliance Program

Shailesh Athalye
Director, Compliance Solutions
Qualys, Inc.
Agenda

Use-cases on why some of the big customers eagerly waiting
Workflow and the Demo
Content support
Roadmap
Use case:

**Two of the biggest Banks**
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
Use case:
**Visibility Matters to the...**
search engine tech company and Healthcare network

**Impacts to security program include:**

- Incomplete Asset Inventory
- Exposure to Unknown Vulnerabilities & Misconfigurations
- Ineffective Risk Evaluation
- Compliance in silos
Current Options

Ad-hoc scripts

Procedural controls (manual assessment)
Outside audits

Limited software-based solutions
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
Configuration Upload Workflow

Push the Asset data

Upload Configuration Data

Qualys creates agent-based data snapshot

Report Generation
Out-of-Band Configuration Assessment
Qualys OCA Benefits

**Cover Your Blind Spots Quickly**
For urgently required technologies, as an interim method till scanner or agent support is available

**Flexible Data Collection**
Fully automate data collection out-of-band via API or upload manually via the UI.

**Complete Vulnerability & Compliance Visibility**
Assess isolated, and locked-down systems for misconfiguration and vulnerabilities

**Expanded Platform Coverage**
Extends Qualys coverage to legacy and uncommon platforms, including network devices, applications, appliances, mainframes, and more.
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

November 2018
v.0.9 release for limited customers
API-based Asset and Config Data Upload for PC

December 2018
UI-based Data Upload for PC
Bulk asset data upload (CSV)
Integration with AssetView

January 2019
Extend Support to VM
Support OCA for AS400 compliance

1H 2019
Possible SDK route
Expand Platform Coverage
CMDB Integration
FIM Integration
Thank You

Shailesh Athalye
sathalye@qualys.com
Security Assessment Questionnaire
Automate the Assessment of Procedural Controls & Vendor Risk

Shailesh Athalye
Director, Compliance Solutions, Qualys, Inc.
Agenda

How SAQ compliments Qualys technical security Apps -
  Internal Procedural controls Assessment
  Vendor Control & Risk Assessment
Content support
Demo
Roadmap
Preview of Future use case: Customer risk management as a vendor
One of the biggest Financial Institute

Assesses their Internal Procedural and Process controls

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

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

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

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

Dashboard the process deficiencies and risk posed by internal controls failure.

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
One of the biggest pharma company

Assessing their vendor risk through SAQ

- Vendors Profiling — Defines Criticality based on Service areas/Cybersecurity domains
- Uses out-of-the-box content, including regional mandates
- Easy online workflow for the vendors, receives reminders, alerts and status
- Assesses vendors per their risk profile, in a standardized (SIG) manner
- Dashboards the risk posed by the highly critical vendors and ranks them per risk
- 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
Security Assessment Questionnaire
SAQ Roadmap

**Q3 2018**
- User/Role/Privilege Management
- Question Bank
- Create template from library templates
- New campaign UI
- Risk scoring

**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

**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

*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
Thank You

Shailesh Athalye
sathalye@qualys.com