Continuous Compliance in Hybrid Environment

Shailesh Athalye
VP, Compliance Solutions, Qualys, Inc
2014: Good Old Days of Compliance

Avoid Treating Audits As A Discovery Exercise, Audits Should be Confirmation Exercise!
2020: Matured Cybersecurity Risk Management

Performing vulnerability management with a context to reduce the “attack surface”

Quick continuous assessment and fix cycles before images are in production
Teams Speak Different Languages

Elastic, Kafka, custom web servers

Identify risk and compliance

Secure hosts, config/integrity/vulnerability management

Security & Compliance assessment should be baked into DevOps
Start Compliant, Stay Compliant

QUALYS POLICY COMPLIANCE RESULTS

<table>
<thead>
<tr>
<th>CID</th>
<th>Title</th>
<th>Technology</th>
<th>Criticality</th>
</tr>
</thead>
<tbody>
<tr>
<td>14602</td>
<td>Status of the 'nosuid' option for '/tmp' partition using 'mount' command</td>
<td>CentOS 7</td>
<td>4</td>
</tr>
<tr>
<td>10804</td>
<td>Status of the SELinux current mode (running configuration)</td>
<td>CentOS 7</td>
<td>4</td>
</tr>
<tr>
<td>10643</td>
<td>Status of iptables package</td>
<td>CentOS 7</td>
<td>4</td>
</tr>
<tr>
<td>12815</td>
<td>List of runtime audit rules for '/etc/passwd' file, using auditd</td>
<td>CentOS 7</td>
<td>4</td>
</tr>
<tr>
<td>10664</td>
<td>Status of the 'OPTIONS' setting within '/etc/sysconfig/chrony' file</td>
<td>CentOS 7</td>
<td>4</td>
</tr>
<tr>
<td>9473</td>
<td>Existence of the 'extraneous' files and directories (Sensitive files/Directories)</td>
<td>Tomcat 8</td>
<td>3</td>
</tr>
<tr>
<td>9477</td>
<td>Status of 'X-Powered-By' setting within 'server.xml' file</td>
<td>Tomcat 8</td>
<td>4</td>
</tr>
<tr>
<td>9551</td>
<td>Status of the 'secure' attribute for each 'Connector' elements whose 'SSL Enabled' are set to 'true'</td>
<td>Tomcat 8</td>
<td>4</td>
</tr>
<tr>
<td>9605</td>
<td>Status of the command-line flag 'STRICT_SERVLET_COMMPLIANCE' set for the 'Tomcat process'</td>
<td>CentOS 7</td>
<td>4</td>
</tr>
<tr>
<td>9565</td>
<td>Status of the 'web server processes' which are not started with 'Security Manager'</td>
<td>CentOS 7</td>
<td>4</td>
</tr>
</tbody>
</table>
Monitor Critical Files From CD Phase

<table>
<thead>
<tr>
<th>Embed Qualys Cloud Agent</th>
<th>VM</th>
<th>PC</th>
<th>FIM: Apply OS Base Profile</th>
<th>FIM: Create and apply application specific profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>59ms</td>
<td>60ms</td>
<td>60ms</td>
<td>60ms</td>
<td>60ms</td>
</tr>
<tr>
<td>failed</td>
<td>failed</td>
<td>failed</td>
<td>10min</td>
<td>10min</td>
</tr>
<tr>
<td>59ms</td>
<td>63ms</td>
<td>63ms</td>
<td>63ms</td>
<td>63ms</td>
</tr>
<tr>
<td>failed</td>
<td>failed</td>
<td>failed</td>
<td>10min</td>
<td>10min</td>
</tr>
</tbody>
</table>
Discover and Assess Middleware Automatically

Discover unauthorized technologies based on host scans.
Security Control Validation (SCV)

**Top five** responsibilities of CISOs

- Pre-requisites and configurations
- Native security features

| Anti-virus | FIM Agents | Splunk | Kafka | Native Malware Protection | Jenkins |
Schedule
Schedule the remediation job to run on demand or in the future.

Remediation Window
You can configure a remediation window to run to

- None
- Set Duration

Note: Not setting the patch window will allow the cloud agent to take as much time as it needs to complete the job.
New Policy
Compliance UI
Security for Inaccessible & Exotic Hosts

Use APIs/UI and push data to Qualys

- Create custom assets
- Push command output, vulnerability, config data

Validate settings and data

Report vulnerabilities, security and misconfigurations

Qualys Out-of-Band Config Assessment (OCA)
New-Age File Integrity Monitoring

Built on the same Qualys Cloud Agent you use for VM, PC, Inventory

Real-time detection for high volume, high scale

Automated incident management and alerting

Out of the box PCI monitoring profiles for OS and applications

No infrastructure or data load for you to manage
Authorized vs Unauthorized Changes
Open APIs for Integration
Context of Changes in Cloud
Assess Vendor Security

Manage vendor risk per vendor criticality

Unify Vendor security and process compliance with technical security
SaaS Applications Challenges

Public cloud spending rockets as SaaS shines

IDC: Cloud spending to grow 21% by 2021

Microsoft, Google Make Cloud Offerings More Enticing

HR gets the cloud treatment

Workday Rises on Demand for Business Cloud-Based Software

Spending On CRM Apps Predicted To Soar In 2018

Microsoft, Google Make Cloud Offerings More Enticing
SaaS Security and Compliance

Inventory

Access

Exposure

Security Configurations

Office365, Google Suite, Salesforce
GitHub, Okta, Slack
Sensitive Data Discovery and Security

Discovery
Access Visibility
Activity Monitoring
Context for security
On Premises Unstructured Data

Cloud Applications

Qualys Agent (MFT)

Unstructured Data Discovery

Visibility in ITAM – know assets hold sensitive data

Secure through PC - Create permission/share/access controls to check their access

Compliance
GDPR / CCA / HIPAA/ etc

Monitor through FIM
Thank You

Compliance Team and Shailesh Athalye
sathalye@qualys.com