Real-Time Vulnerability Management
Operationalizing the VM process from detection to remediation

Jimmy Graham
Director, Product Management, Qualys, Inc.
Agenda

Expanding Vulnerability Management

Introducing Qualys Patch Management

Unified Dashboard
Vulnerability Management Lifecycle

- Asset Inventory
- Patch Management
- Vulnerability Management
- Threat Risk and Prioritization
- Discover at Scale
- Report & Research
- Remediate / Patch
- Prioritize Threats
Expanding Vulnerability Management

- Containers
- IoT Devices
- Mobile Devices
- Public Cloud
- Private Cloud
- ICS / SCADA
- Workstations
- On Premise
Vulnerability Management
Platform Evolution
Elastic VM Dashboard

Merges AssetView technology into Qualys VM

Build widgets with vulnerability counts

Search filters for quickly building queries

Replace long-running reports with live widgets

November 16, 2018
QSC Conference, 2018
Opening Up the VM Detections Platform

Custom Remote Detections

Qualys Remote Detection Interface (QRDI)

Create your own or share on Qualys Community

Supports HTTP(S) and raw TCP

Regex grouping and capturing

LUA scripting for advanced logic
### Elastic VM Dashboard

#### Patch Catalog

<table>
<thead>
<tr>
<th>Operating Systems</th>
<th>Missing</th>
<th>Installed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>3.01K</td>
<td>982</td>
</tr>
<tr>
<td>Linux</td>
<td>960</td>
<td>99</td>
</tr>
<tr>
<td>Mac</td>
<td>480</td>
<td>26</td>
</tr>
</tbody>
</table>

#### Patch Status

<table>
<thead>
<tr>
<th>Patch Status</th>
<th>Missing</th>
<th>Installed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Missing</td>
<td>10</td>
<td>23</td>
</tr>
</tbody>
</table>

#### Update Type

<table>
<thead>
<tr>
<th>Update Type</th>
<th>Security</th>
<th>Non-Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>435</td>
<td>27</td>
</tr>
<tr>
<td>Non-Security</td>
<td>97</td>
<td>205</td>
</tr>
</tbody>
</table>

#### Type

<table>
<thead>
<tr>
<th>Type</th>
<th>OS 97</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS 97</td>
<td>97</td>
<td>205</td>
</tr>
</tbody>
</table>

#### Vendor Severity

<table>
<thead>
<tr>
<th>Vendor Severity</th>
<th>Critical</th>
<th>Important</th>
<th>Critical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>3</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Important</td>
<td>1</td>
<td>3</td>
<td>0</td>
</tr>
</tbody>
</table>

#### Patch Details

<table>
<thead>
<tr>
<th>PATCH TITLE</th>
<th>BULLETIN</th>
<th>TYPE</th>
<th>VENDOR SEVERITY</th>
<th>QID</th>
<th>CVE</th>
<th>REBOOT</th>
<th>PATCH STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe Reader and Acrobat Security Update April 2017</td>
<td>MS17-041</td>
<td>APP</td>
<td>CRITICAL</td>
<td>4015221</td>
<td>CVE-2016-3427, CVE-2016-2077</td>
<td>No</td>
<td>2</td>
</tr>
<tr>
<td>Microsoft .NET Framework Security Update April 2017</td>
<td>APSB11-03</td>
<td>OS</td>
<td>CRITICAL</td>
<td>4015264</td>
<td>CVE-2018-1000</td>
<td>Yes</td>
<td>2</td>
</tr>
<tr>
<td>Microsoft SQL Server 2008 R2 Service Pack 3 (KB2979597)</td>
<td></td>
<td>APP</td>
<td>NONE</td>
<td>2979597</td>
<td>CVE-2017-6871</td>
<td>Yes</td>
<td>1</td>
</tr>
<tr>
<td>Microsoft Windows Security Update May 2017</td>
<td>MS17-04</td>
<td>OS</td>
<td>CRITICAL</td>
<td>4019263, 4019264,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oracle Java SE Critical Patch Update - April 2017</td>
<td>MS17-04</td>
<td>APP</td>
<td>CRITICAL</td>
<td>170682</td>
<td>CVE-2018-6791</td>
<td>No</td>
<td>3</td>
</tr>
<tr>
<td>Security Update for Windows Server 2008 x64 Edition...</td>
<td>MS16-02</td>
<td>APP</td>
<td>CRITICAL</td>
<td>170682</td>
<td>CVE-2018-6791</td>
<td>No</td>
<td>3</td>
</tr>
</tbody>
</table>
Qualys Patch Management
Overview
Current Patch Management Tools

Challenges and Impact

- Manual correlation of vulnerability to patch leads to delayed mean-time-to-remediation
- Waiting for vulnerability reports to confirm the patch has fixed the vulnerability
- Remote systems only patched when connected to corporate network
- Limited or no coverage of third-party apps
- Multiple patching solutions for each OS type
Introducing Qualys’ Integrated Patch Management

Automated correlation of vulnerability and patch data – Which patch fixes the CVE?

Simple dashboarding for tracking patch deployments

Patch using the Qualys Cloud Agent, anywhere

Patch OS and third-party applications

Single solution for Windows, macOS, and Linux
Shift From Reaction Mode to Operational Security

Always up-to-date on missing patches

Security and IT teams can “speak the same language”

Collaboration – key to successful digital transformation

Unify discovery, prioritization, and remediation into one platform

Rapid remediation of high-profile vulnerabilities in days vs. weeks

Regularly scheduled deployments are repeatable and reported on

November 16, 2018

QSC Conference, 2018
<table>
<thead>
<tr>
<th>Patch Title</th>
<th>Bulletin</th>
<th>Type</th>
<th>Vendor Severity</th>
<th>QID</th>
<th>CVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe Reader and Acrobat Security Update (SSMP-102)</td>
<td>MS17-04</td>
<td>APP</td>
<td>CRITICAL</td>
<td>277113</td>
<td>CVE-2016-3427, CVE-2016-2077</td>
</tr>
<tr>
<td>Microsoft .NET Framework Security Update April 2017</td>
<td>APSB11-03</td>
<td>OS</td>
<td>CRITICAL</td>
<td>197040</td>
<td>CVE-2018-1000...</td>
</tr>
<tr>
<td>Microsoft SQL Server 2008 R2 Service Pack 3 (KB2979597)</td>
<td></td>
<td>APP</td>
<td>NONE</td>
<td>351175</td>
<td>CVE-2017-6871</td>
</tr>
<tr>
<td>Microsoft Windows Security Update May 2017</td>
<td>MS17-04</td>
<td>OS</td>
<td>CRITICAL</td>
<td>197054</td>
<td>None</td>
</tr>
<tr>
<td>Oracle Java SE Critical Patch Update - April 2017</td>
<td>MS17-04</td>
<td>APP</td>
<td>CRITICAL</td>
<td>170682</td>
<td>CVE-2018-6791</td>
</tr>
<tr>
<td>Security Update for Windows Server 2008 x64 Edition...</td>
<td>MS16-02</td>
<td>APP</td>
<td>CRITICAL</td>
<td>170682</td>
<td>CVE-2018-6791</td>
</tr>
</tbody>
</table>

**Patch Management Beta**
Platform Support

XP SP3+
Vista
Windows 7
Windows 8/8.1
Windows 10
Server 2003 SP2+
Server 2008/R2
Server 2012/R2
Server 2016

OS X 10.10
Yosemite
OS X 10.11
El Capitan
macOS 10.12
Sierra
macOS 10.13
High Sierra
macOS 10.14
Mojave

RHEL 6,7
CentOS 5.4+,6,7
SUSE Linux
Enterprise Server/
Desktop 11,12,15
Oracle Ent Linux
6,7(Server)
Ubuntu 14.x,15.x,16.x,
18.x

* Beta will focus on Windows- other operating systems will follow later
* Roadmap items are future-looking; timing and specifications may change
Roadmap

Beta: Q4 2018 - Windows patch deployment
General Availability: Q1 2019

**Beta 1**
- Windows patching (desktops and servers)
- Qualys serves patches
- Third party Windows applications

**Beta 2**
- On-prem Caching of patches (QGS)
- Direct download from vendors for off-prem
- Additional tokens for dashboarding

**Upcoming**
- Mac patching
- Linux patching
- Repository integration
- Automation Rules & Approval workflows
Unified Dashboards
Overview
Unified Dashboard

Build dashboards with widgets from multiple Qualys Cloud Apps

Target servers, containers, instances, web apps, etc. using Asset Tags
# Unified Dashboard Preview

## Patch Catalog

<table>
<thead>
<tr>
<th>Patch Catalog</th>
</tr>
</thead>
<tbody>
<tr>
<td>301 Patches</td>
</tr>
</tbody>
</table>

### OPERATING SYSTEMS
- Windows: 3.01K
- Linux: 982
- Mac: 99

### PATCH STATUS
- Missing: 10
- Installed: 23

### UPDATE TYPE
- Security: 435
- Non-Security: 27

### TYPE
- OS: 97
- Application: 205

### VENDOR SEVERITY
- Critical: 164

## Patch Details

<table>
<thead>
<tr>
<th>Patch Title</th>
<th>Bulletin</th>
<th>Type</th>
<th>Vendor Severity</th>
<th>QID</th>
<th>CVE</th>
<th>Reboot</th>
<th>Patch Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe Reader and Acrobat Security Update (APPS-09-02)</td>
<td>MS17-04</td>
<td>APP</td>
<td>Critical</td>
<td>277113</td>
<td>CVE-2016-3427, CVE-2016-2077</td>
<td>No</td>
<td>2</td>
</tr>
<tr>
<td>Microsoft .NET Framework Security Update April 2017</td>
<td>APSB17-06</td>
<td>OS</td>
<td>Critical</td>
<td>197040</td>
<td>CVE-2018-1000·</td>
<td>Yes</td>
<td>2</td>
</tr>
<tr>
<td>Microsoft SQL Server 2008 R2 Service Pack 3 (KB2979597)</td>
<td></td>
<td>APP</td>
<td>None</td>
<td>351175</td>
<td>CVE-2017-6871</td>
<td>Yes</td>
<td>1</td>
</tr>
<tr>
<td>Microsoft Windows Security Update May 2017</td>
<td>MS17-04</td>
<td>OS</td>
<td>Critical</td>
<td>197064</td>
<td>None</td>
<td>Yes</td>
<td>3</td>
</tr>
<tr>
<td>Security Update for Windows Server 2008 x64 Edition...</td>
<td>MS16-02</td>
<td>APP</td>
<td>Critical</td>
<td>170682</td>
<td>CVE-2018-6791</td>
<td>No</td>
<td>3</td>
</tr>
</tbody>
</table>
Unified Dashboard Rollout

Phase 1
Unified Dashboard App
Global dashboard filters

Support for:
- VM
- PC
- FIM
- IOC
- AI
- PM
- CRI
- TP

Phase 2
Unified widget builder
Upgrade existing Cloud App Dashboards

Support for:
- WAS
- WAF
- SAQ
- CS
- CV
- VM
- PC
- FIM
- IOC
- AI
- PM
- CRI
- TP
Thank You

Jimmy Graham
jgraham@qualys.com