Qualys CertView
Managing Digital Certificates

Asif Karel
Director, Product Management, Qualys, Inc.
Agenda

Introduction
Evolving browser markers
Introducing CertView
Key Use Cases and Capabilities
Demo
Q&A
Refresher: What does SSL give you?

- Confidentiality
- Authentication
- Message Integrity
- Non-repudiation
Certificates are Everywhere

Public-Facing Services

Internal Services

Machine-to-machine communication

API endpoints

Services in Public Clouds
Evolving security indicators

Users should expect that the web is safe by default, and they’ll be warned when there’s an issue\(^1\).

- Security Team

1 https://blog.chromium.org/2018/05/evolving-chromes-security-indicators.html
Timeline of Chrome’s Evolution

July 2018 (Chrome 68) – All HTTP sites marked Not Secure
Timeline of Chrome’s Evolution

Sept 2018 (Chrome 69) – Secure sites marked neutral instead of the green Secure
Timeline of Chrome’s Evolution

Oct 2018 (Chrome 70) – RED ‘Not Secure’ marker if user interacts with any input field
Timeline of Chrome’s Evolution

Eventual treatment of all HTTP pages in Chrome:

⚠️ Not secure example.com

Schedule to disable TLS 1.0 / 1.1

• Chrome: Jan 2020
• Firefox/Safari: March 2020
• IE: First half of 2020

TLS 1.3 is faster and removes support for insecure features and ciphers
SSL Pulse

The Good
• No SHA1 or 1024 bit keys

The Bad (~35% inadequate)
• Expired certificates: ~5,200
• Expiring in the next 2 weeks: ~4,500
• Weak/Insecure cipher suites: ~4,200
• SSLv2/SSLv3: ~15,000
• TLSv1.0: ~99,000 (72%)
• RC4 enabled: ~22,000 (16%)
Security Solution w/o a Certificate Management System
High-end Security Solution w/o a Certificate Management System
Tinkering with Security Solutions w/o a Certificate Management System
Dangers of Incomplete Security Solutions

- Hiding Malicious Actions
  - Malware
  - Ransomware
  - Virus
  - Trojan
  - Botnet

- Hiding the Initial Infection
  Before the call back to a C&C

- Hiding Data Exfiltration
  Bypass other controls such as DLP
Security Solutions w/o a Certificate Management system
### Current State of Most Organizations

<table>
<thead>
<tr>
<th>Limited Visibility</th>
<th>Expirations Missed</th>
<th>Compliance</th>
<th>Reliance on Manual Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>95% of organizations don't know where certs are in their networks</td>
<td>Unplanned outages</td>
<td>Certificates from unapproved CAs</td>
<td>Spreadsheets are error prone and out-of-date</td>
</tr>
<tr>
<td>Limited ownership information</td>
<td>Many more “near misses”</td>
<td>Responding to audits are manually intensive exercises</td>
<td>Expensive, not scalable as certificates increase</td>
</tr>
<tr>
<td>The unknown is difficult to manage</td>
<td></td>
<td></td>
<td>Troubleshooting issues is challenging</td>
</tr>
</tbody>
</table>
The average Global 5,000 company spends about $15 million to recover from the loss of business due to a certificate outage¹

Challenges of Existing Solutions

**Visibility**
Point tools, increasing effort and ownership costs

**Scalability**
Operational silos
Work in on-premises or cloud-only mode
Require multiple or complex deployments to cover large environments

**Maturity**
Most solutions are off-the-shelf vulnerability-only or certificate-only “tools”
Network is down, Certificate expired again!

We have no visibility into certificates outside the firewall

We can't inspect encrypted traffic

What's DevOps doing, I just found 5,000 self-signed certificates!

Network is down, Certificate expired again!
Introducing Qualys CertView

Discover, inventory, monitor certificates

Discover, inventory, monitor host configurations & vulnerabilities

Coverage across both on-premises and cloud environments

Renew certificates from the same platform
## Use Cases

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outage Remediation</td>
<td>Stop expired certificates from interrupting business</td>
</tr>
<tr>
<td>Certificate Grades</td>
<td>Find out if your TLS configurations are following best practices</td>
</tr>
<tr>
<td>Baseline Normal Usage/ Full Visibility</td>
<td>Establish a baseline to be able to detect anomalies</td>
</tr>
<tr>
<td>Audits and Compliance</td>
<td>Achieve audit success and fast remediation</td>
</tr>
<tr>
<td>Certificate Renewal</td>
<td>Renew expiring certificates</td>
</tr>
</tbody>
</table>
Key Advantages of Qualys CertView

Uses the same Qualys scanners already deployed for Vulnerability Management or Policy Compliance

Qualys CertView meets much of the common use cases in version 1.0 – and we’re working on closing gaps quickly

Certificate Enrollment/Renewal
Releasing next month

Simplified delivery through Qualys Cloud Platform – easy for existing VM/PC customers to trial and deploy

Attractive Pricing
CertView Releases and Roadmap

Q4 2018*
CA Imports
Enroll/Renew (Digicert)
Approval workflow
Scan Consolidation

Q1 2019*
APIs
Alerts
Assign ownership
Enroll/Renew (Comodo/
Let’sEncrypt)
Certificate Validation

Q2 2019*
Enroll/Renew (Microsoft CA/ GoDaddy)
ServiceNow CMDB integration
Deploy on Apache

Q3 2019*
Cloud Agent support
Enroll/Renew (Entrust/EJBCA)
Deploy on IIS

* Roadmap items are future looking; timing and specifications may change
CertView is free, it’s how you use it (or not) that will cost you!

-Anonymous
## Certificate View

### Certificates

<table>
<thead>
<tr>
<th>HOME/ORGANIZATION</th>
<th>ISSUER</th>
<th>EXPIRATION</th>
<th>ALGORITHM</th>
<th>KEY SIZE</th>
<th>LAST FOUND</th>
<th>INSTANCES</th>
<th>ASSETS</th>
</tr>
</thead>
<tbody>
<tr>
<td>lyanna.qualys-demo...</td>
<td>Qualys Demo CA</td>
<td>Sep 22, 2017</td>
<td>SHA256withRSA</td>
<td>2048</td>
<td>Mar 27, 2018</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Qualys, Inc.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>stark.qualys-demo.c...</td>
<td>Qualys OA CA</td>
<td>Sep 15, 2018</td>
<td>SHA256withRSA</td>
<td>2048</td>
<td>Mar 27, 2018</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Qualys, Inc.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>baratheon.qualys-de...</td>
<td>Qualys</td>
<td>Jul 15, 2019</td>
<td>SHA1withRSA</td>
<td>1024</td>
<td>Mar 27, 2018</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>House Baratheon</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>khal.qualys-demo.c...</td>
<td>COMODO RSA Extender</td>
<td>Oct 14, 2018</td>
<td>SHA256withRSA</td>
<td>2048</td>
<td>Mar 27, 2018</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>COMODO CA Limited</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.113.196.189</td>
<td>sslabs</td>
<td>May 02, 2027</td>
<td>SHA256withRSA</td>
<td>2048</td>
<td>Mar 6, 2018</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Qualys Security Tec...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.113.196.191</td>
<td>sslabs</td>
<td>May 02, 2027</td>
<td>SHA256withRSA</td>
<td>2048</td>
<td>Mar 6, 2018</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Qualys Security Tec...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.113.196.190</td>
<td>sslabs</td>
<td>May 02, 2027</td>
<td>SHA1withRSA</td>
<td>2048</td>
<td>Mar 6, 2018</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Qualys Security Tec...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.113.196.192</td>
<td>sslabs</td>
<td>May 07, 2027</td>
<td>SHA256withRSA</td>
<td>2048</td>
<td>Mar 6, 2018</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Qualys Security Tec...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Thank You

Asif Karel
akarel@qualys.com