Practical Steps Taken to Reboot Vulnerability Management for Modern IT and Mature Business

Brian Canaday
IT Security Analyst/Engineer
CSAA, Insurance Group a AAA Insurer
Key Talking Points

• A Three-Phase Approach to Meeting our Vulnerability Management Goals with Qualys

• Scan Configurations & Schedule Tuning

• Cloud Agent Configuration & Testing with Application Teams
Foundational Requirements

• The Requirements May Vary for Your Organization
• Scanning coverage – All routable IP addresses
• Scanning frequency – Full scans of the Environment Every 7 days
• Scans Cannot Cause Operational Instability or Availability Issues
• Cloud Agents – All Windows Servers, Red Hat Servers and User Endpoints
1. What is Our Scope?
   ALL Available IP Addresses in Our Environment

2. Build Asset Groups by CIDR and Define Local Scan Appliances

3. Configure Option Profile to Boost Performance and Accuracy
1. Plan and Configure Agent Configuration Profile
2. Identify Targets for Agent Usage – Any System Capable of Running the Agent
3. Identify Test Groups for Stability and Performance Testing. We chose to work with all our groups who had experienced issues in the past with the Agent.
4. Test, Tune, and Analyze Results
5. Deploy in Phases to all Non-Production Systems (over 1 week)
6. Deploy in Phases to all Production Systems (over 1 week)
1. Create an Option Profile to Scan for Remote-Only Vulnerabilities (# QIDs in List: 6,667 vs. 39,641)
2. Update Existing Scans to Filter Out Scan Assets With the Cloud Agent Tag
3. Create Scan Schedule for all Assets With the Cloud Agent Tag Using the New Remote Detection Only Dynamic Option Profile
4. Tuning Scan Schedules After the Option Profile Changes and Splitting up the Cloud Agent Scans from the Non Agent Full Scans.
• Utilizing Qualys’ API Interface we Download Our Scan and Agent Results Every Four Hours and Pivot That off of Our CMDB and HR Structure Data.

With These Elements we can do the Following:

1. Apply our Internal Patch Management Policy & Standards to Display Only Items Our Staff Need to Remediate Based on Policy.
2. Show Trends and Results by Rollup to the Various VPs and Offer the Ability to Drill Down to the System Owner Responsible for the System.
3. Track Compliance to our Patch Management Policy & Standards Leveraging the Same Rollup/Drill Down Capabilities.
Outcomes

• With cleaner more relevant data we can detect changes in our environment sooner

• With faster results and less impact on the systems the Qualys Cloud Agent has quickly become the one security agent our Operations Teams depend on and expect immediate remediation of any agent not reporting in

• By leveraging the API from Qualys and our CMDB we use a custom reporting solution where we rollup under the VP for each area and the leaders under them
Questions