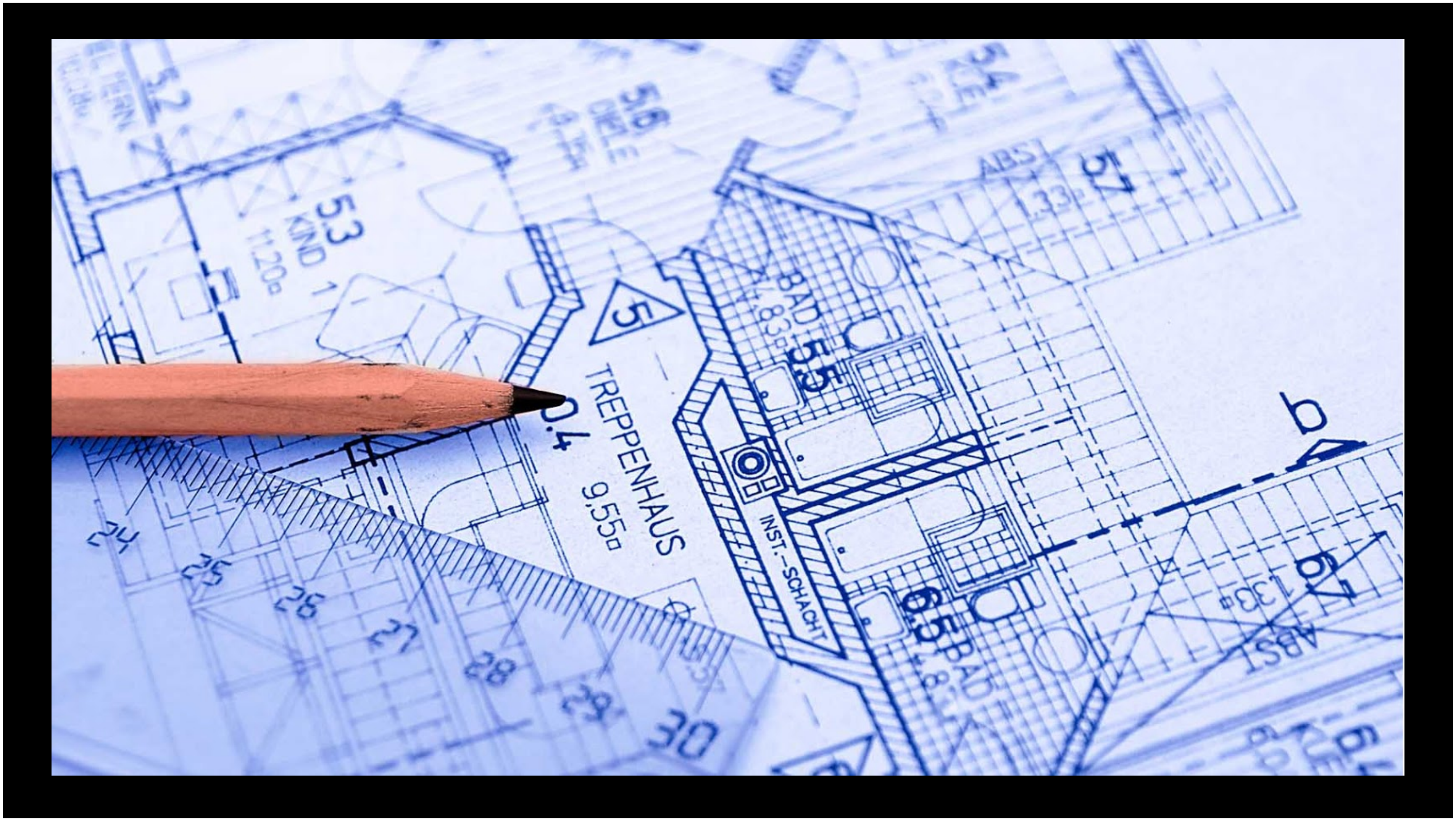
Practical Steps Taken to Reboot Vulnerability Management for Modern IT and Mature Business

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

Key Talking Points

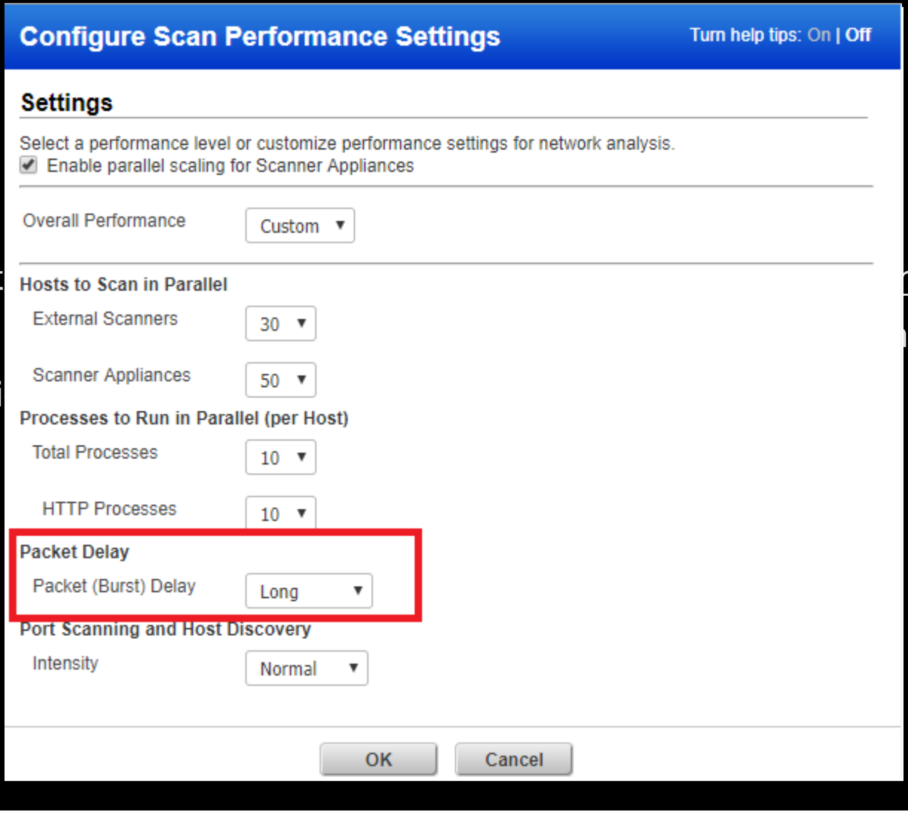
- A Three-Phase Approach to Meeting our Vulnerability Management Goals with Qualys
- Scan Configurations & Schedule Tuning
- Cloud Agent Configuration & Testing with Application Teams



5.2
5.6
DIELE
5.4
5.3
KIND
11,20
ABST
5.7
1,33
5
BAD
4,83
5.5
0.4
TREPPENHAUS
9,55
INST.-SCHACHT
b
6.7
1,33
ABST
6.5
BAD
24
25
26
27
28
29
30

PHASE 1

1. What nment
2. Build nces
3. Confi



Configure Scan Performance Settings

Turn help tips: On | Off

Settings

Select a performance level or customize performance settings for network analysis.

☑ Enable parallel scaling for Scanner Appliances

Overall Performance: Custom ▼

Hosts to Scan in Parallel

External Scanners: 30 ▼

Scanner Appliances: 50 ▼

Processes to Run in Parallel (per Host)

Total Processes: 10 ▼

HTTP Processes: 10 ▼

Packet Delay

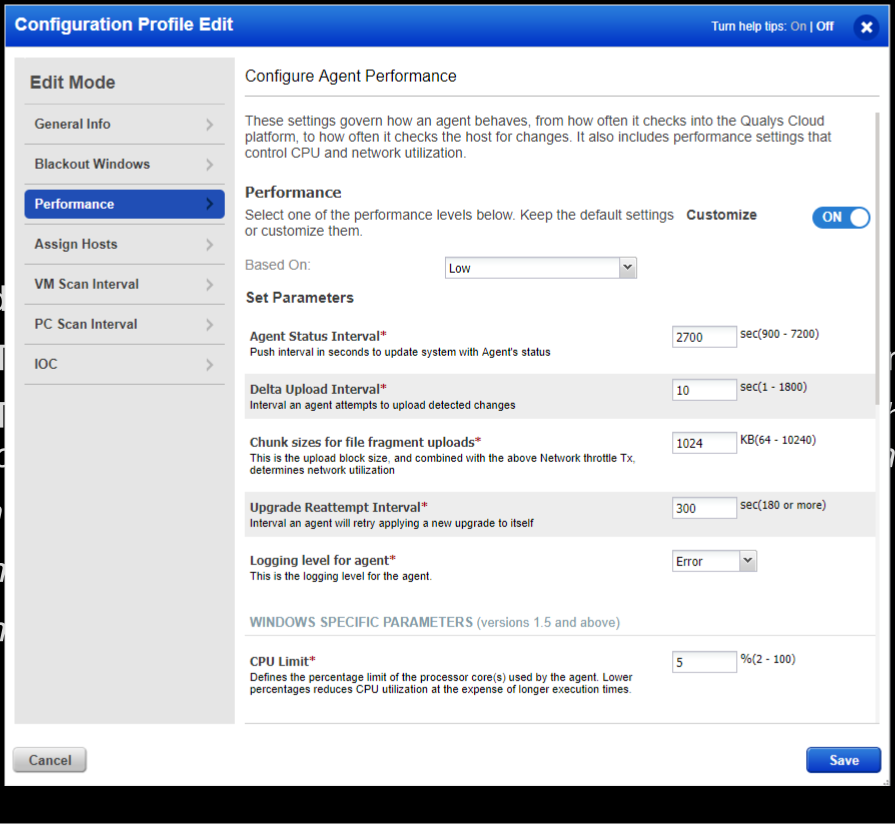
Packet (Burst) Delay: Long ▼

Port Scanning and Host Discovery

Intensity: Normal ▼

PHASE 2

1. Plan and
2. Identify T ng the Agent
3. Identify T hose to Work
   With all c n the Agent.
4. *Test, Tun*
5. *Deploy in*
6. *Deploy in*



Configure Agent Performance

These settings govern how an agent behaves, from how often it checks into the Qualys Cloud platform, to how often it checks the host for changes. It also includes performance settings that control CPU and network utilization.

Performance

Select one of the performance levels below. Keep the default settings or customize them. **Customize** ON

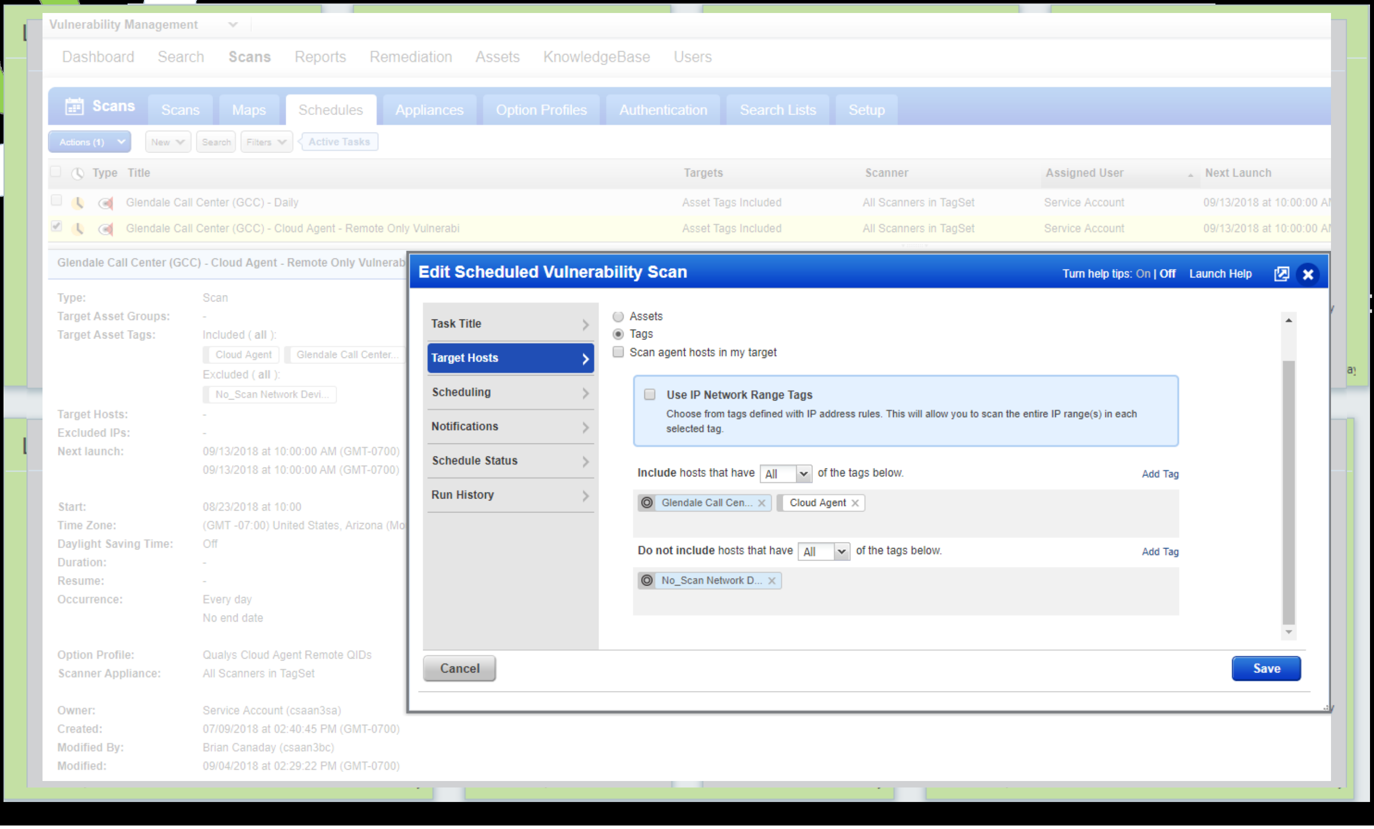
Based On: Low

Set Parameters

Agent Status Interval* Push interval in seconds to update system with Agent's status	2700	sec(900 - 7200)
Delta Upload Interval* Interval an agent attempts to upload detected changes	10	sec(1 - 1800)
Chunk sizes for file fragment uploads* This is the upload block size, and combined with the above Network throttle Tx, determines network utilization	1024	KB(64 - 10240)
Upgrade Reattempt Interval* Interval an agent will retry applying a new upgrade to itself	300	sec(180 or more)
Logging level for agent* This is the logging level for the agent.	Error	

WINDOWS SPECIFIC PARAMETERS (versions 1.5 and above)

CPU Limit* Defines the percentage limit of the processor core(s) used by the agent. Lower percentages reduces CPU utilization at the expense of longer execution times.	5	%(2 - 100)



	Type	Title	Targets	Scanner	Assigned User	Next Launch
□		Glendale Call Center (GCC) - Daily	Asset Tags Included	All Scanners in TagSet	Service Account	09/13/2018 at 10:00:00 AI
☑		Glendale Call Center (GCC) - Cloud Agent - Remote Only Vulnerabi	Asset Tags Included	All Scanners in TagSet	Service Account	09/13/2018 at 10:00:00 AI

Glendale Call Center (GCC) - Cloud Agent - Remote Only Vulnerab

Type: Scan
Target Asset Groups: -
Target Asset Tags: Included (all):
Cloud Agent
Glendale Call Center...
Excluded (all):
No_Scan Network Devi...
Target Hosts: -
Excluded IPs: -
Next launch: 09/13/2018 at 10:00:00 AM (GMT-0700)
09/13/2018 at 10:00:00 AM (GMT-0700)

Start: 08/23/2018 at 10:00
Time Zone: (GMT -07:00) United States, Arizona (Mo
Daylight Saving Time: Off
Duration: -
Resume: -
Occurrence: Every day
No end date

Option Profile: Qualys Cloud Agent Remote QIDs
Scanner Appliance: All Scanners in TagSet

Owner: Service Account (csaan3sa)
Created: 07/09/2018 at 02:40:45 PM (GMT-0700)
Modified By: Brian Canaday (csaan3bc)
Modified: 09/04/2018 at 02:29:22 PM (GMT-0700)

Edit Scheduled Vulnerability Scan

○ Assets
● Tags
□ Scan agent hosts in my target

□ **Use IP Network Range Tags**
Choose from tags defined with IP address rules. This will allow you to scan the entire IP range(s) in each selected tag.

Include hosts that have All of the tags below.
Glendale Call Cen... ×
Cloud Agent ×

Do not include hosts that have All of the tags below.
No_Scan Network D... ×

Reporting - Better Data, Better Results

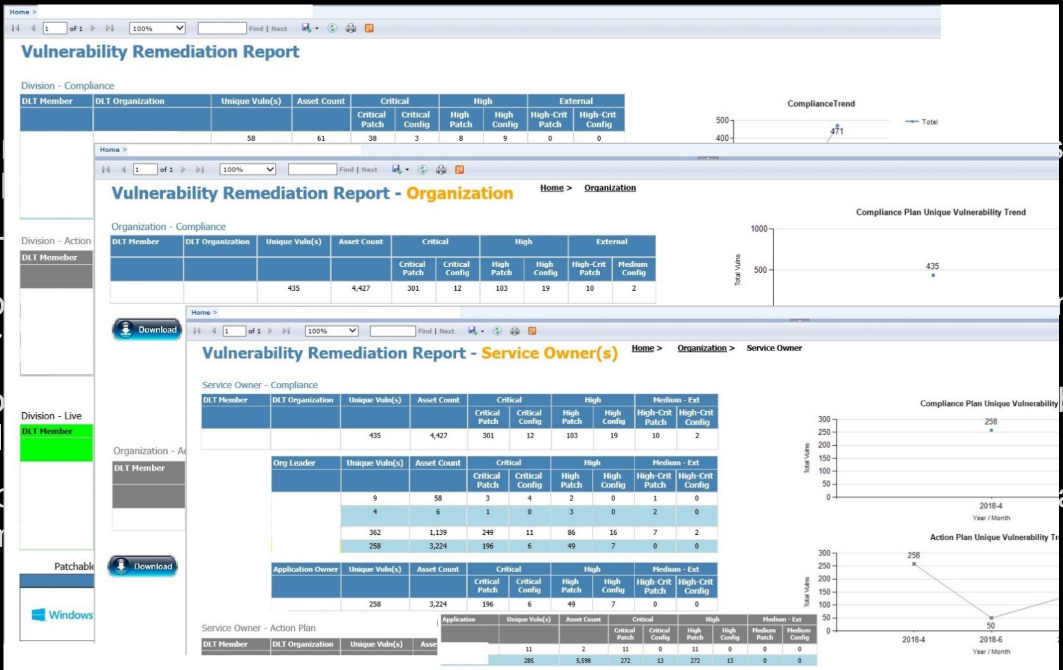
- Utilizi s Every
  Four I

With Th

1. App nly Items
   Our

2. Sho bility to
   Drill

3. Trac aging the
   Sam



Vulnerability Remediation Report

Division - Compliance

DLT Member	DLT Organization	Unique Vuln(s)	Asset Count	Critical		High		External	
				Critical Patch	Critical Config	High Patch	High Config	High-Crit Patch	High-Crit Config
		58	61	38	3	8	9	0	0

Vulnerability Remediation Report - Organization

Organization - Compliance

DLT Member	DLT Organization	Unique Vuln(s)	Asset Count	Critical		High		External	
				Critical Patch	Critical Config	High Patch	High Config	High-Crit Patch	Medium Config
		435	4,427	301	12	103	19	10	2

Vulnerability Remediation Report - Service Owner(s)

Service Owner - Compliance

DLT Member	DLT Organization	Unique Vuln(s)	Asset Count	Critical		High		Medium - Ext	
				Critical Patch	Critical Config	High Patch	High Config	High-Crit Patch	High-Crit Config
		435	4,427	301	12	103	19	10	2

Org Leader	Unique Vuln(s)	Asset Count	Critical		High		Medium - Ext	
			Critical Patch	Critical Config	High Patch	High Config	High-Crit Patch	High-Crit Config
	9	58	3	4	2	0	1	0
	4	6	1	0	3	0	2	0
	362	1,139	249	11	86	16	7	2
	258	3,224	196	6	49	7	0	0

Application Owner	Unique Vuln(s)	Asset Count	Critical		High		Medium - Ext	
			Critical Patch	Critical Config	High Patch	High Config	High-Crit Patch	High-Crit Config
	258	3,224	196	6	49	7	0	0

Service Owner - Action Plan

DLT Member	DLT Organization	Unique Vuln(s)	Asse

Application	Unique Vuln(s)	Asset Count	Critical		High		Medium - Ext	
			Critical Patch	Critical Config	High Patch	High Config	Medium Patch	Medium Config
	11	2	11	0	11	0	0	0
	285	5,598	272	13	272	13	0	0

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