NCR ATLEOS

Qualys Cloud Agent and Software Composition Analysis

October 10, 2024

About Our Presenter

Theo Bowman

Vulnerability Management Engineer.

- Lives in Dallas, TX.
- Joined NCR Atleos in 2019.
- Five years of experience with Qualys and Vulnerability Management.
- Hobbies are reef aquariums and competitive barbecuing.

About NCR Atleos

$4.19 billion
Gross annual revenue

Global organization with a presence in more than
60 countries

20,000+
employees

NCR ATLEOS

Leader in self-service banking solutions, including:

- ATMaaS
- Telecom & Technology
- Multi-vendor software
- ATM networks

Allpoint

World's largest independent ATM network

NCR Atleos Environment Overview

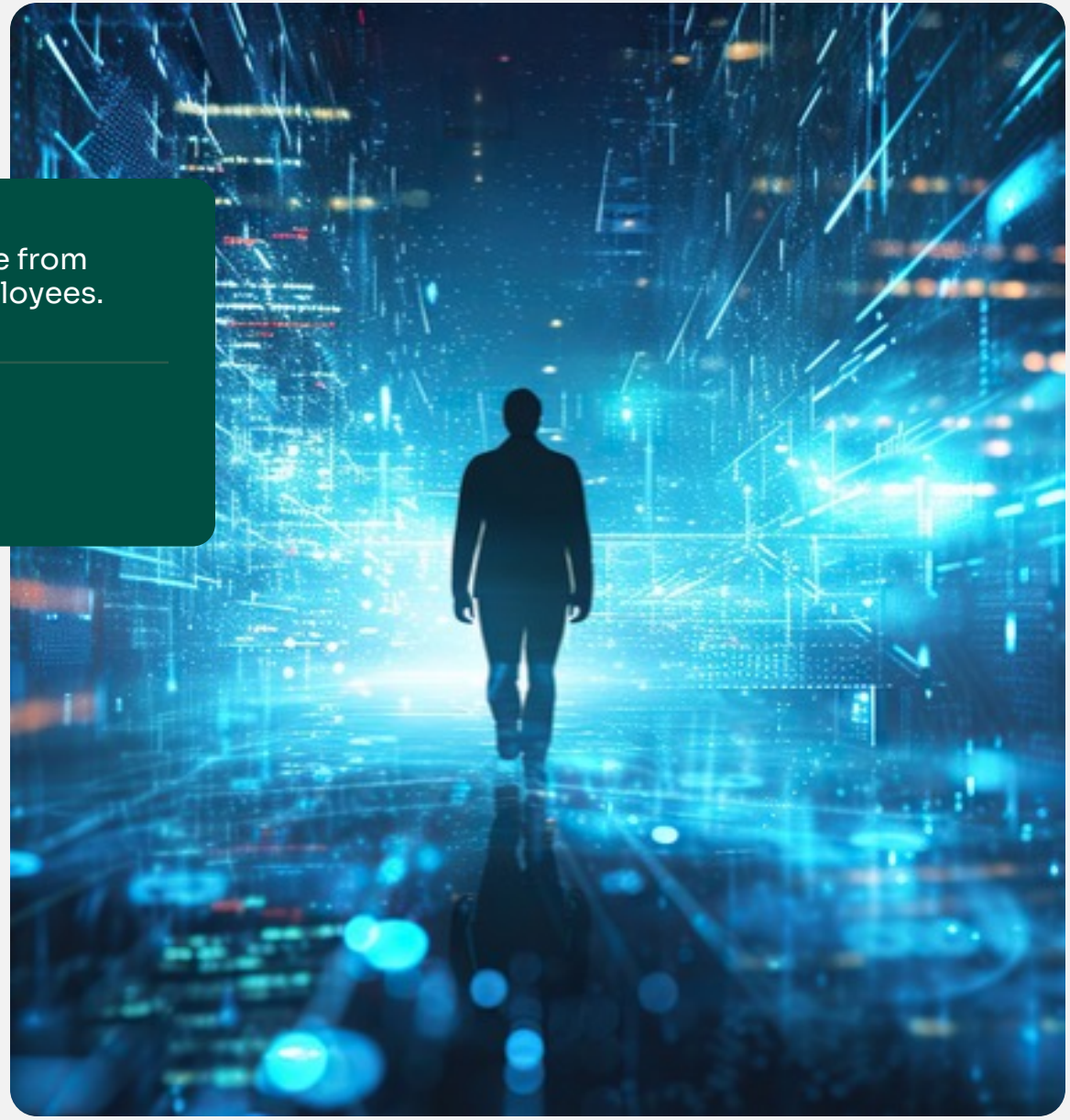
Acquired by a large company using Rapid7.	Acquisition increased workforce from 2,500 to more than 25,000 employees.
Migrated from Rapid7 to Qualys.	Originally used Qualys for 2,500 employees – now 25,000.

Post-split, we have new interna/external IPs, larger list of Web apps to scan, different firewall and firewall rules.

More employees means a much larger footprint in Cloud, Azure, GCP.

Complex and segmented environment.

More servers due to the split.



Building a Vulnerability Management Program

Challenges

Coverages	Vulnerability Remediation	Managing Third-Party Risk
Ensure all assets get scanned.	Identifying superseded vulnerabilities (built out in Splunk).	Identifying risks and application owners.
Vulnerability scanning performed globally.	Reporting issues required ad hoc reporting in Splunk.	Issues related to third-party vulnerabilities.
Traditional scanning with scanner appliance, agent scanning, Cloud connector.	Manually managed ticketing and remediation.	Manual deployment required.
Firewall rules.	Identifying ownership of remediation.	Limited testing and vendor information functionality.
Determining if agent was installed.	Manual follow-up was labor intensive.	No on-demand scans required re-scans from the appliance.

Software Composition Analysis (SwCA)

Leadership emphasis on true risk.	Scheduled to run daily.
Support from management to identify risk.	Currently on 28,000 assets.
New assets because the split increased our load.	Currently no false positives.
Proposed implementing SwCA to management.	Ramped up the implementation.
Learned about SwCA while creating cloud agent activation key for MACs.	Liked open-source software scanning and ability to properly assess risk outside of BAU patching.
Researched the module and determined a use case for SwCA.	No changes required to integrate automated ticketing.
Increased view of vulnerabilities in our environment. • More detail are given about the finding • These findings are not easily remediated.	All SwCA vulnerabilities are confirmed.

Remediating log4j

Deployed SwCA and discovered log4j vulnerabilities within our environment

Assigned those vulnerabilities to the appropriate teams

Ran a re-scan using SwCA to validate the remediation

Able to re-scan individual assets

Triaged the log4j vulnerabilities to determine the urgency

JNDI

Old versions

Qualys has 166 log4j vulnerabilities

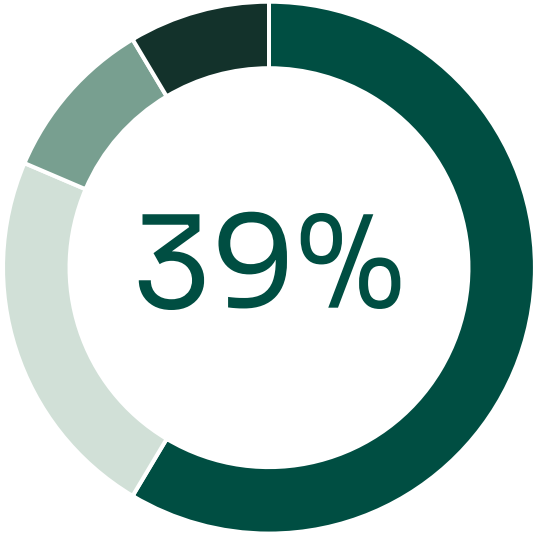
15 new QID checks with SwCA

NCR Atleos Qualys Cloud Agent

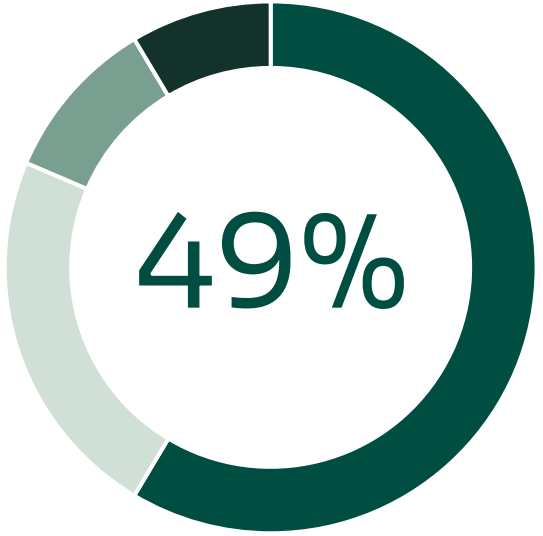
Qualys activation key	Deployment	Elevated Executive Confidence	Increased situational awareness	Implementation
Cybersecurity Asset Management (CSAM)	28,000k+ Cloud agents were deployed (laptops, VMs, Cloud assets and servers)	Report weekly and monthly metrics	Cloud Connector in our environment. • AWS • Azure • Google Cloud Platform	Made Splunk reporting and dashboards to address superseded vulnerability issue
Vulnerability Management (VM)	Agents get deployed for baseline image	Identify changes in vulnerabilities totals		Integrated Qualys with ServiceNow (SNOW) to automate ticketing process.
Secure Config Assessment (SCA)	PCI reporting			Created tags in the Qualys platform to allow SNOW to auto-assign tickets.
Software Composition Analysis (SwCA)	CIS benchmarking			Integrated SLAs in the Qualys module.
				Began using Qualys module for metrics and timelines in SNOW.
				Used Qualys Detection Score (QDS) to identify team priorities based on Top 10 counts.

Determining Success

SwCA Implementation Improved Visibility of Vulnerability



August 2024



September 2024

Next Steps

1

Implement TruRisk, which identifies asset exposure by true risk, using QDS and QVS

- This will help us identify those assets with the highest risk factors
- Mission = 0 or minimal TruRisk assets in environment

2

Ensure patching is not routine and targeted to high-risk assets and vulnerabilities

3

Provides IT team a more focused approach to patching

4

Begin using the Cloud Connector for OCI

5

After our authentication improves, we will use QIDs for agent discovery

6

Use Cloud Agent Passes Sensor (CAP) to monitor network traffic and provide an enhanced view of our environment

Why use SwCA?

Summary

- Ability to assess our environment at a high level
- Data keeps us risk aware
- Centrally managed – don’t need additional tooling to assess third-party risk
- Customize our scope and leverage our dashboards for remediation based on risk assessment

Thank You