Qualys.

ROCon 25

The Risk Operations Conference

APAC

Eliminate the Risk of Audit Failure

Qualys.

ROCon 25

The Risk Operations Conference

APAC

Shailesh Athalye

Senior Vice President, Product Management, Qualys

Shekhar Rana

Principal Subject Matter Expert, Compliance Solutions, Qualys

Cyber Incidents hurt;
Audit Failures take
business license...

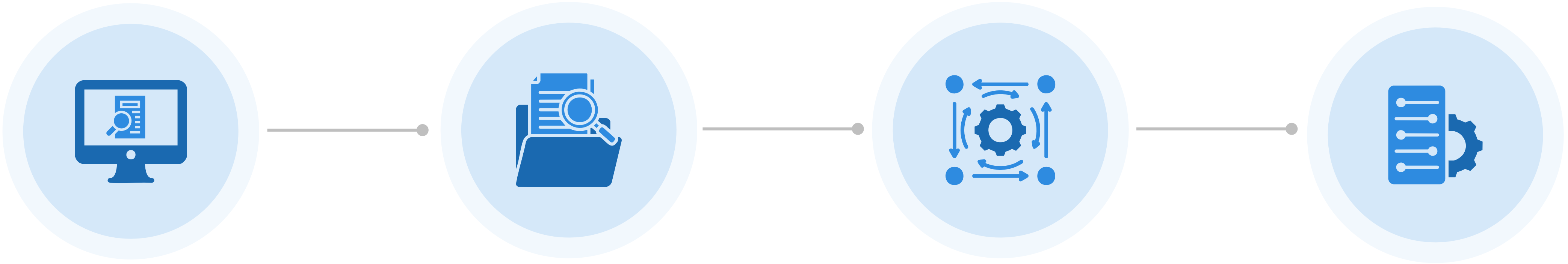
Why Audit Failure is a Growing Risk?

1 Evolving mandates & Increasing Regulatory Pressure – DPDP, RBI, SOC

2 Need Technical and procedural evidence

3 Growing cost, time and efforts in maintaining

Continuous Audit Readiness



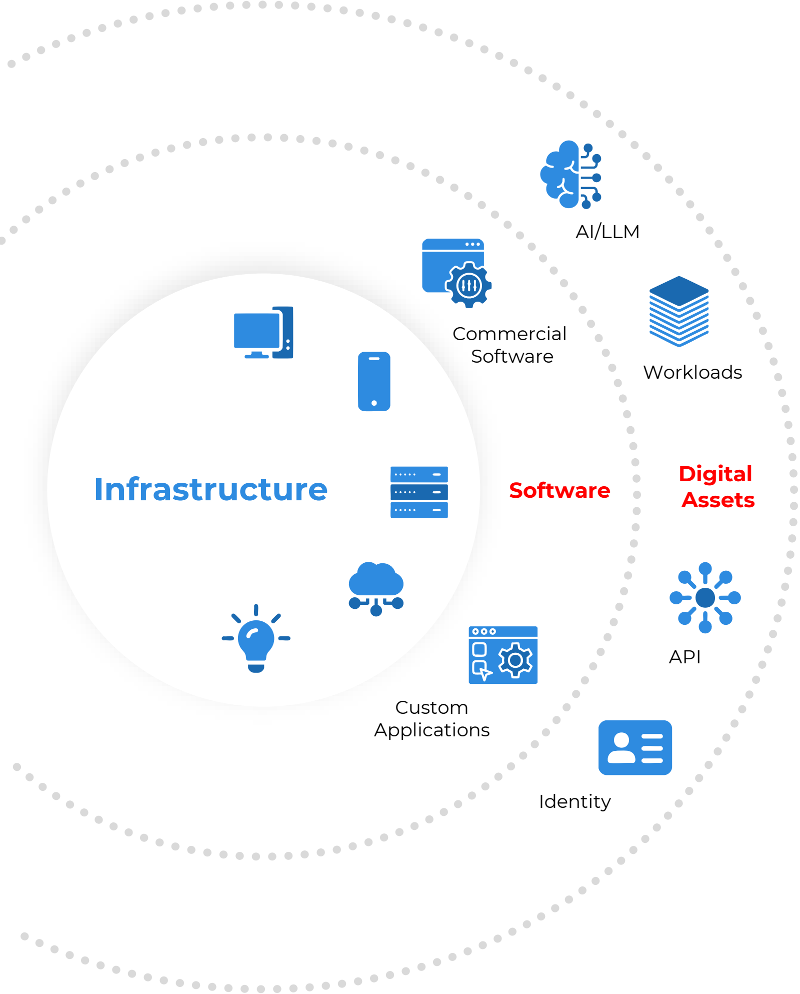
Collect technical evidence

Collect procedural evidence

Real-time map evidence to common controls

Continuously monitor your audit readiness against policies, frameworks and mandates

Multiple SPM tools and Scattered exposures



VM	CSPM
ISPM	DSPM
JIRA	WORKDAY

Asset Critically

Location of the Asset

Infra Vulnerabilities

Infra, DB misconfigurations/control failures

Certificates

Open-source software vulns

EOL Software

Web Application vulnerabilities

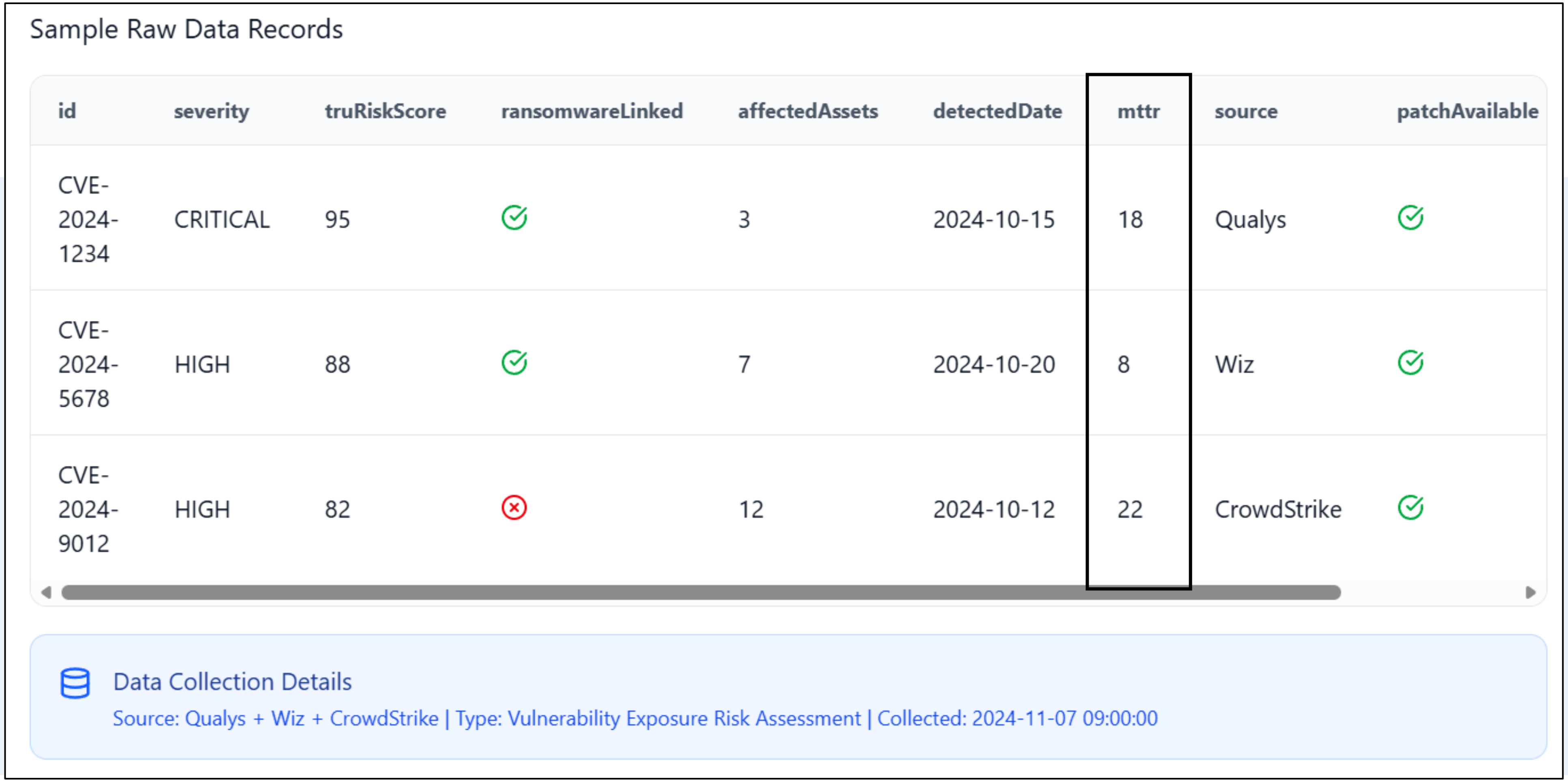
Security Awareness Training

Incident Response Policy & Procedures

Human Resource Security Policy

*Enterprises have **70+ security tools on average**

Control audit readiness: Collect Raw Data



Sample Raw Data Records

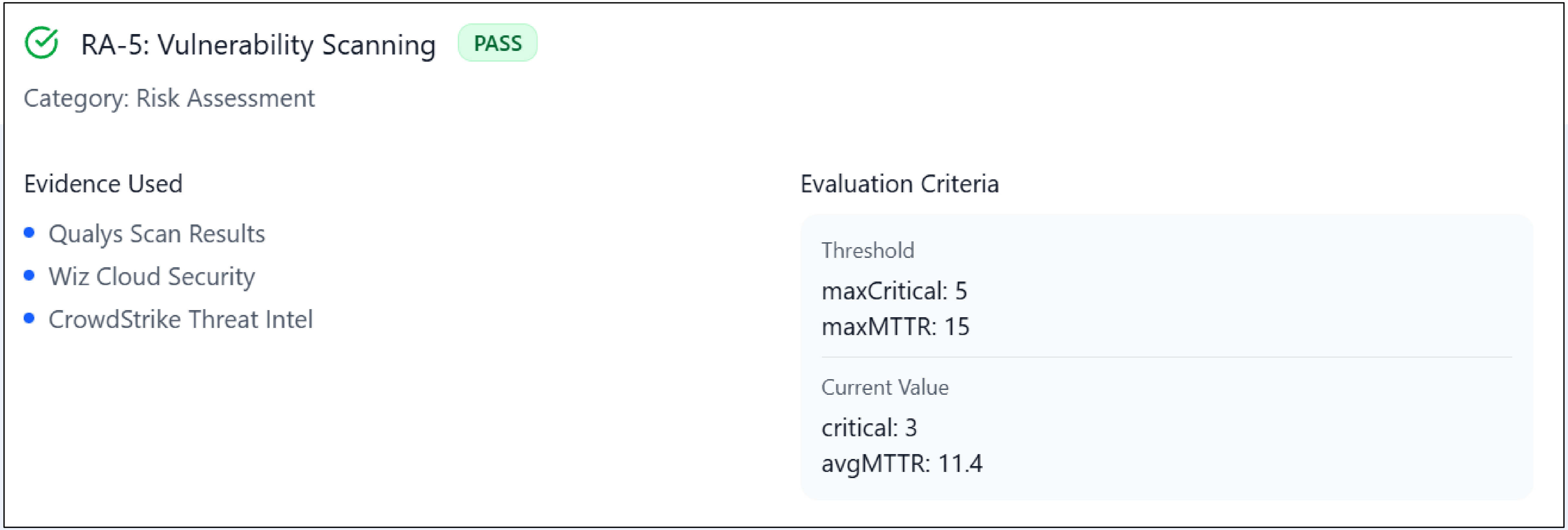
id	severity	truRiskScore	ransomwareLinked	affectedAssets	detectedDate	mttr	source	patchAvailable
CVE-2024-1234	CRITICAL	95	✓	3	2024-10-15	18	Qualys	✓
CVE-2024-5678	HIGH	88	✓	7	2024-10-20	8	Wiz	✓
CVE-2024-9012	HIGH	82	✗	12	2024-10-12	22	CrowdStrike	✓

Data Collection Details

Source: Qualys + Wiz + CrowdStrike | Type: Vulnerability Exposure Risk Assessment | Collected: 2024-11-07 09:00:00

Control audit readiness

Control Mapping: Evidence is automatically evaluated against predefined control thresholds. Multiple evidence sources are aggregated to provide comprehensive control assessment.



✓ RA-5: Vulnerability Scanning PASS

Category: Risk Assessment

Evidence Used

- Qualys Scan Results
- Wiz Cloud Security
- CrowdStrike Threat Intel

Evaluation Criteria

Threshold

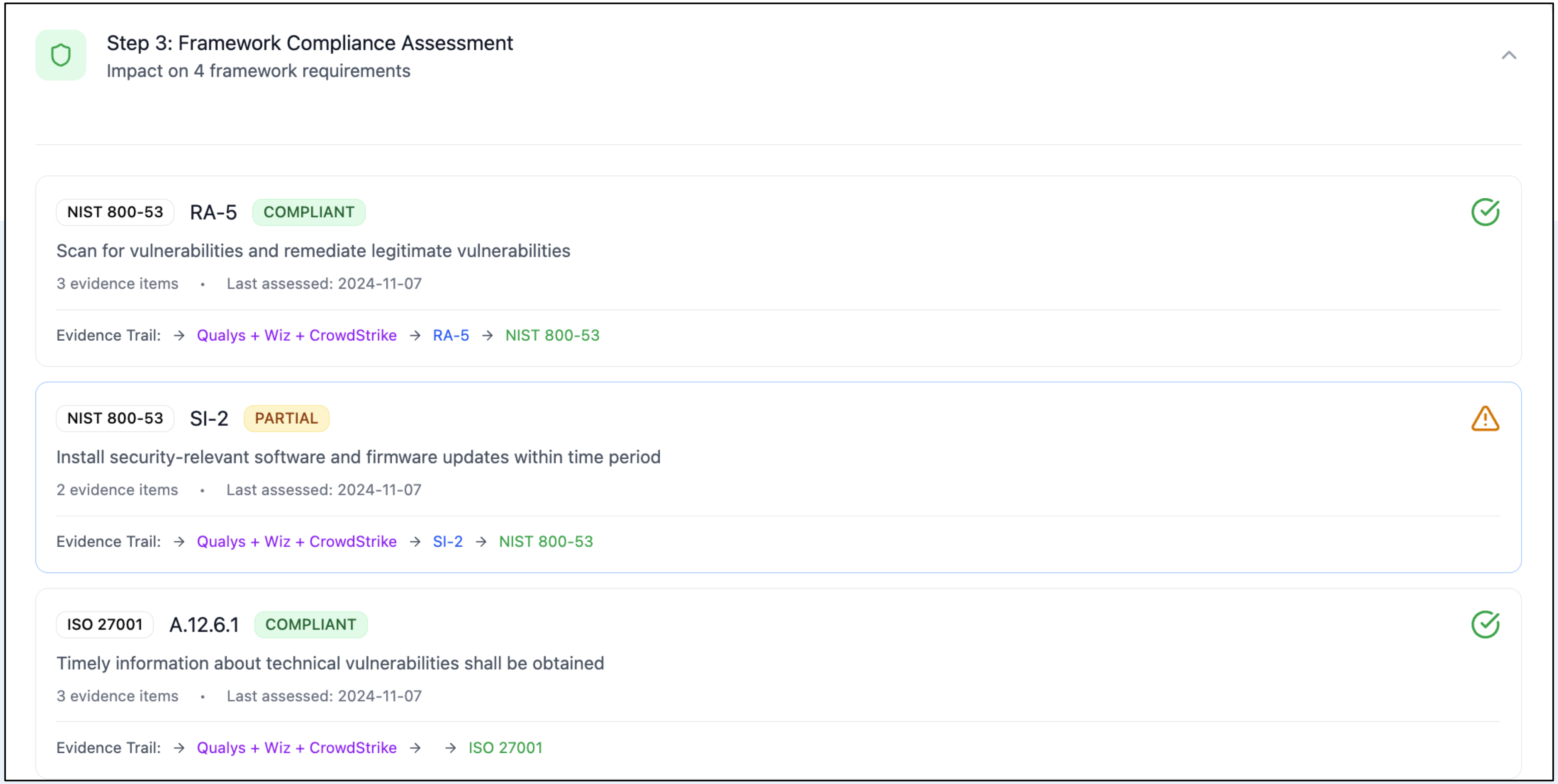
maxCritical: 5
maxMTTR: 15

Current Value

critical: 3
avgMTTR: 11.4

Control audit readiness: Framework assessment

Qualys. ROCon25 The Risk Operations Conference APAC



Step 3: Framework Compliance Assessment

Impact on 4 framework requirements

NIST 800-53 RA-5 COMPLIANT ✓

Scan for vulnerabilities and remediate legitimate vulnerabilities

3 evidence items • Last assessed: 2024-11-07

Evidence Trail: → Qualys + Wiz + CrowdStrike → RA-5 → NIST 800-53

NIST 800-53 SI-2 PARTIAL ⚠

Install security-relevant software and firmware updates within time period

2 evidence items • Last assessed: 2024-11-07

Evidence Trail: → Qualys + Wiz + CrowdStrike → SI-2 → NIST 800-53

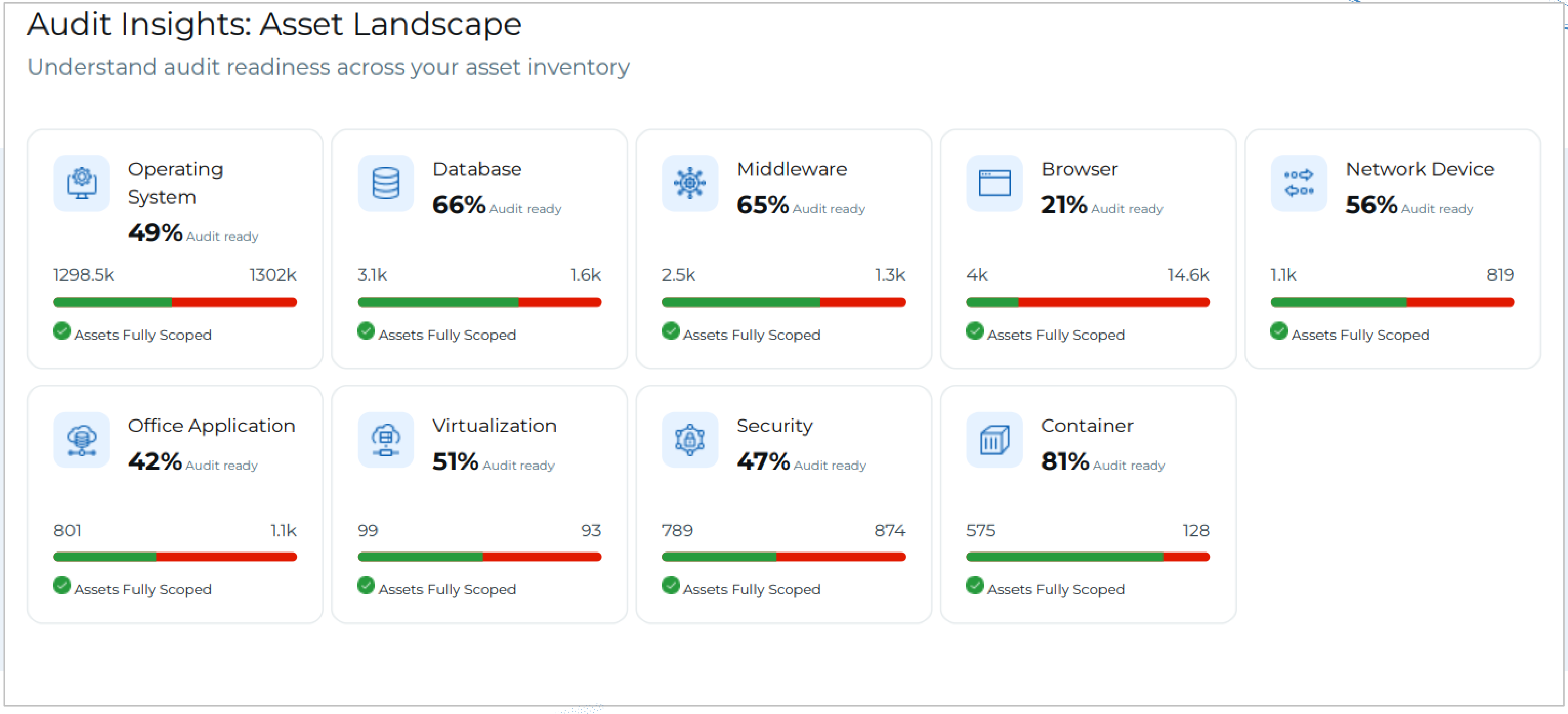
ISO 27001 A.12.6.1 COMPLIANT ✓

Timely information about technical vulnerabilities shall be obtained

3 evidence items • Last assessed: 2024-11-07

Evidence Trail: → Qualys + Wiz + CrowdStrike → → ISO 27001

Comprehensive Visibility across your Asset landscape: audit-readiness for your inventory



Audit Insights: Asset Landscape

Understand audit readiness across your asset inventory

Operating System
49% Audit ready
1298.5k 1302k
✓ Assets Fully Scoped

Database
66% Audit ready
3.1k 1.6k
✓ Assets Fully Scoped

Middleware
65% Audit ready
2.5k 1.3k
✓ Assets Fully Scoped

Browser
21% Audit ready
4k 14.6k
✓ Assets Fully Scoped

Network Device
56% Audit ready
1.1k 819
✓ Assets Fully Scoped

Office Application
42% Audit ready
801 1.1k
✓ Assets Fully Scoped

Virtualization
51% Audit ready
99 93
✓ Assets Fully Scoped

Security
47% Audit ready
789 874
✓ Assets Fully Scoped

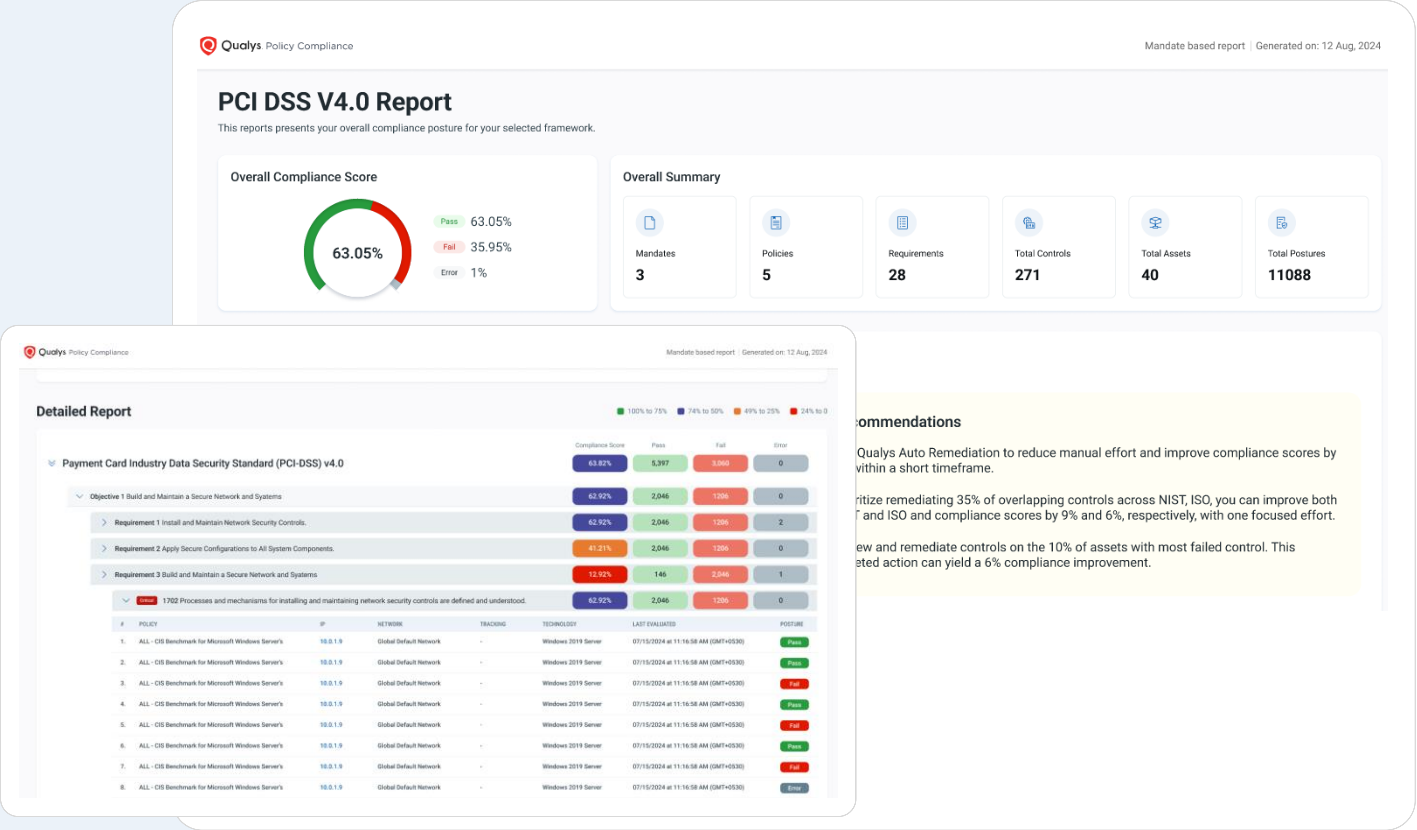
Container
81% Audit ready
575 128
✓ Assets Fully Scoped

Audit-Ready Reports

Effortless audit ready reports with Pre-built library of 100+ mandates mapped to controls

- **Automatically generate multiple reports** from a **single data collection**
- **Custom reports** for on-demand audits
- Executive level and audit stakeholder ready reports to **prove compliance**

Reduce audit resources and costs by 50%



Qualys Policy Compliance

Mandate based report | Generated on: 12 Aug, 2024

PCI DSS V4.0 Report

This reports presents your overall compliance posture for your selected framework.

Overall Compliance Score

63.05%

Pass	63.05%
Fail	35.95%
Error	1%

Overall Summary

Mandates	Policies	Requirements	Total Controls	Total Assets	Total Postures
3	5	28	271	40	11088

ommendations

Qualys Auto Remediation to reduce manual effort and improve compliance scores by vithin a short timeframe.

ritize remediating 35% of overlapping controls across NIST, ISO, you can improve both T and ISO and compliance scores by 9% and 6%, respectively, with one focused effort.

ew and remediate controls on the 10% of assets with most failed control. This eted action can yield a 6% compliance improvement.

Qualys Policy Compliance

Mandate based report | Generated on: 12 Aug, 2024

Detailed Report

🟩 100% to 75% 🟦 74% to 50% 🟧 49% to 25% 🟥 24% to 0

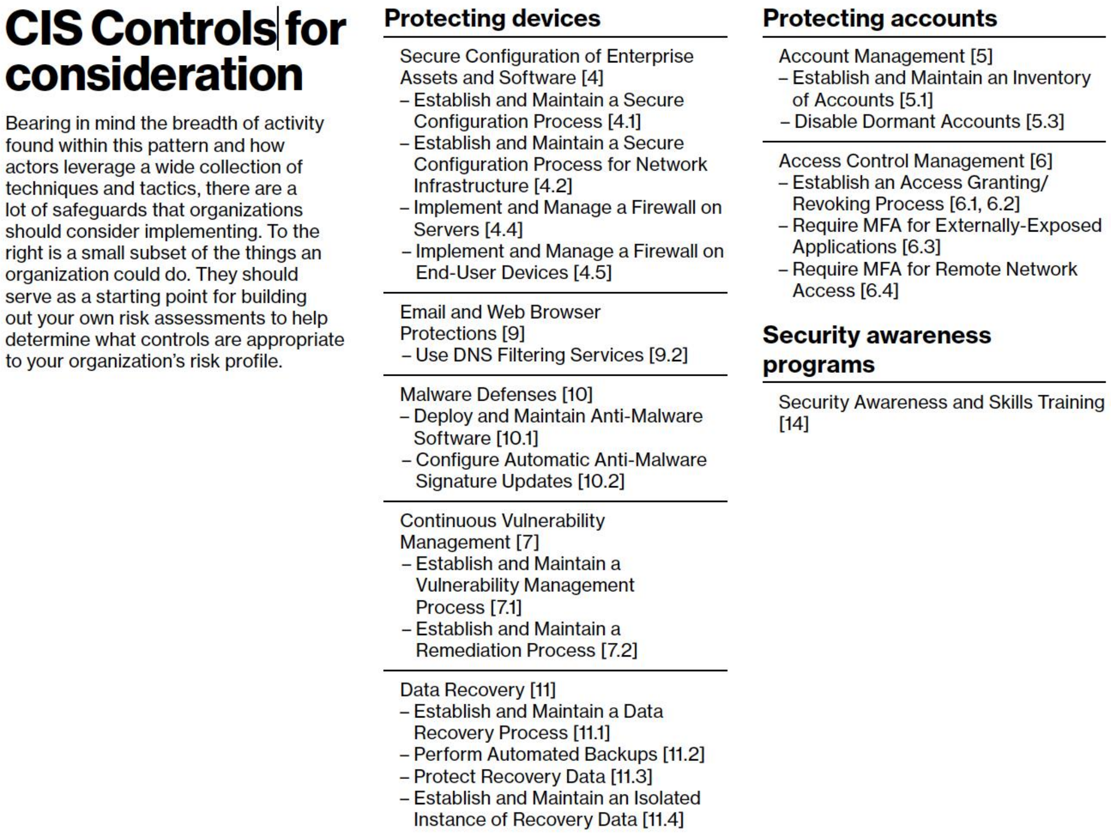
	Compliance Score	Pass	Fail	Error
Payment Card Industry Data Security Standard (PCI-DSS) v4.0	63.82%	5,397	3,060	0
Objective 1 Build and Maintain a Secure Network and Systems	62.92%	2,046	1206	0
Requirement 1 Install and Maintain Network Security Controls.	62.92%	2,046	1206	2
Requirement 2 Apply Secure Configurations to All System Components.	41.21%	2,046	1206	0
Requirement 3 Build and Maintain a Secure Network and Systems	12.92%	146	2,046	1
Critical 1702 Processes and mechanisms for installing and maintaining network security controls are defined and understood.	62.92%	2,046	1206	0

#	POLICY	IP	NETWORK	TRACKING	TECHNOLOGY	LAST EVALUATED	POSTURE
1.	ALL - CIS Benchmark for Microsoft Windows Server's	10.0.1.9	Global Default Network	-	Windows 2019 Server	07/15/2024 at 11:16:58 AM (GMT+0530)	Pass
2.	ALL - CIS Benchmark for Microsoft Windows Server's	10.0.1.9	Global Default Network	-	Windows 2019 Server	07/15/2024 at 11:16:58 AM (GMT+0530)	Pass
3.	ALL - CIS Benchmark for Microsoft Windows Server's	10.0.1.9	Global Default Network	-	Windows 2019 Server	07/15/2024 at 11:16:58 AM (GMT+0530)	Fail
4.	ALL - CIS Benchmark for Microsoft Windows Server's	10.0.1.9	Global Default Network	-	Windows 2019 Server	07/15/2024 at 11:16:58 AM (GMT+0530)	Pass
5.	ALL - CIS Benchmark for Microsoft Windows Server's	10.0.1.9	Global Default Network	-	Windows 2019 Server	07/15/2024 at 11:16:58 AM (GMT+0530)	Fail
6.	ALL - CIS Benchmark for Microsoft Windows Server's	10.0.1.9	Global Default Network	-	Windows 2019 Server	07/15/2024 at 11:16:58 AM (GMT+0530)	Pass
7.	ALL - CIS Benchmark for Microsoft Windows Server's	10.0.1.9	Global Default Network	-	Windows 2019 Server	07/15/2024 at 11:16:58 AM (GMT+0530)	Fail
8.	ALL - CIS Benchmark for Microsoft Windows Server's	10.0.1.9	Global Default Network	-	Windows 2019 Server	07/15/2024 at 11:16:58 AM (GMT+0530)	Error

Moving From Configuration Assessment To Risk Management

Risk prioritization: Misconfigurations…

Assessing CIS/hardening benchmarks to prioritizing risk



CIS Controls for consideration

Bearing in mind the breadth of activity found within this pattern and how actors leverage a wide collection of techniques and tactics, there are a lot of safeguards that organizations should consider implementing. To the right is a small subset of the things an organization could do. They should serve as a starting point for building out your own risk assessments to help determine what controls are appropriate to your organization's risk profile.

Protecting devices

Secure Configuration of Enterprise Assets and Software [4]
- Establish and Maintain a Secure Configuration Process [4.1]
- Establish and Maintain a Secure Configuration Process for Network Infrastructure [4.2]
- Implement and Manage a Firewall on Servers [4.4]
- Implement and Manage a Firewall on End-User Devices [4.5]

Email and Web Browser Protections [9]
- Use DNS Filtering Services [9.2]

Malware Defenses [10]
- Deploy and Maintain Anti-Malware Software [10.1]
- Configure Automatic Anti-Malware Signature Updates [10.2]

Continuous Vulnerability Management [7]
- Establish and Maintain a Vulnerability Management Process [7.1]
- Establish and Maintain a Remediation Process [7.2]

Data Recovery [11]
- Establish and Maintain a Data Recovery Process [11.1]
- Perform Automated Backups [11.2]
- Protect Recovery Data [11.3]
- Establish and Maintain an Isolated Instance of Recovery Data [11.4]

Protecting accounts

Account Management [5]
- Establish and Maintain an Inventory of Accounts [5.1]
- Disable Dormant Accounts [5.3]

Access Control Management [6]
- Establish an Access Granting/Revoking Process [6.1, 6.2]
- Require MFA for Externally-Exposed Applications [6.3]
- Require MFA for Remote Network Access [6.4]

Security awareness programs

Security Awareness and Skills Training [14]

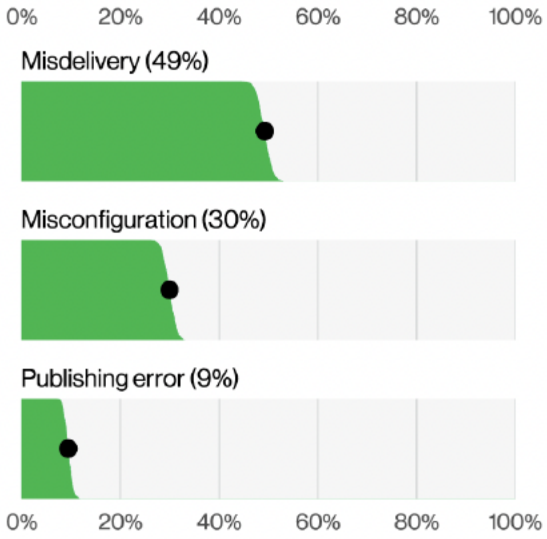


Figure 64. Top Action varieties in Miscellaneous Errors breaches (n=1,399)

Misconfigurations still one of the top vectors in breaches

DBIR report **2025**

Top Failing CIS Benchmarks	Technology	Technology Category
CIS Benchmark for IBM DB2 11.x Bennchmark	IBM DB2 11	Database
CIS Benchmark for Microsoft Windows 10 Benchmark	Microsoft Windows 10	Operating System
CIS Benchmark for Mozilla Firefox 102 ESR Benchmark	Mozilla Firefox	Browser
CIS Benchmark for Microsoft Internet Explorer 10 Benchmark	Microsoft Internet Explorer 10	Browser
CIS Benchmark for Microsoft Office Enterprise Benchmark	Microsoft Office Enterprise	Middleware
CIS Benchmark for Google Chrome Benchmark	Google Chrome	Browser
CIS Benchmark for Microsoft Windows 11 Stand-alone Benchmark	Microsoft Windows 11	Operating System
CIS Benchmark for Check Point Firewall Benchmark	Check Point Firewall	Network

40%

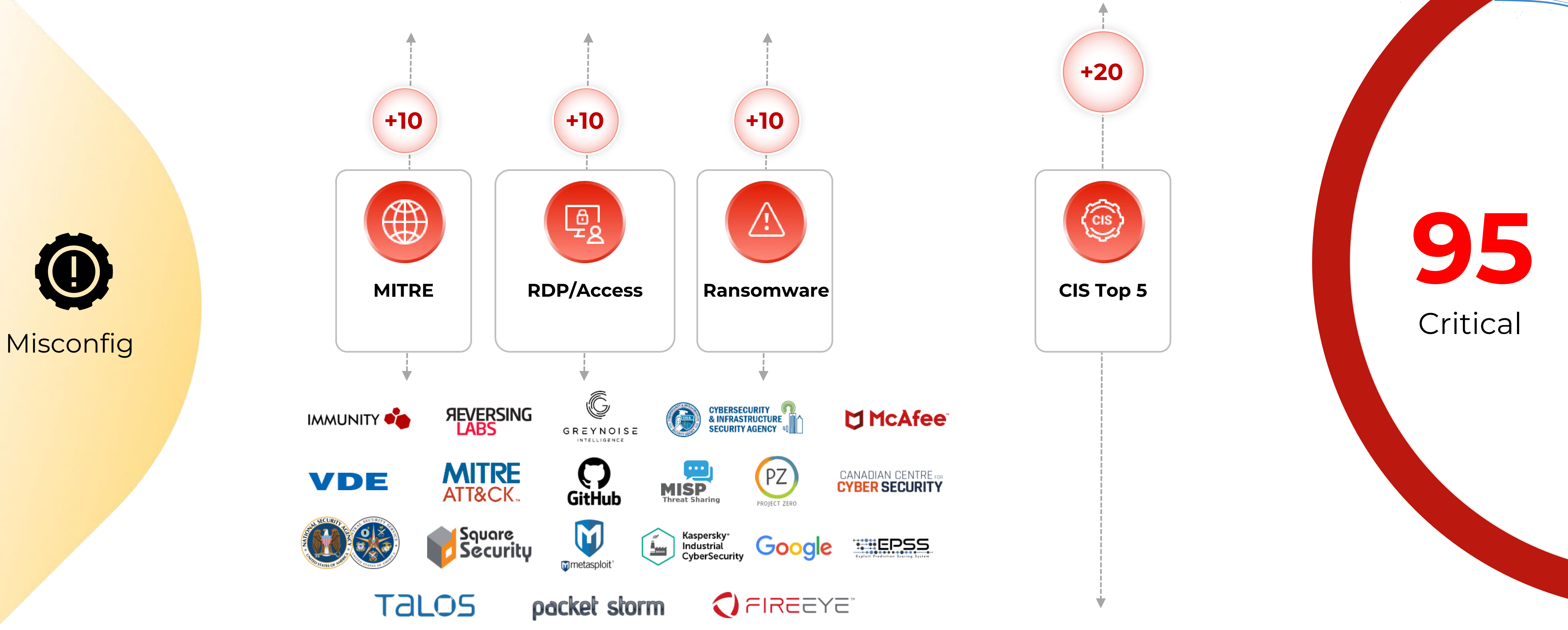
Avg. Misconfigurations from CIS benchmarks

70%

Misconfigurations mapped to Ransomware Risks

Control ID	Statement	Criticality	Ransomware Risk	Remote Risk	Risk Explanation
2181	Current list of Groups and User Accounts granted the 'Access this computer from the network' right	URGENT	✅	✅	Allows lateral movement and unauthorized remote access.
2196	Current list of Groups and User Accounts granted the 'Deny Access to this computer from the network' right	CRITICAL	✅	✅	Unauthorized users may access the system remotely.
2200	Current list of Groups and User Accounts granted the 'Deny logon through terminal (Remote Desktop) service' right	CRITICAL	✅	✅	Attackers can exploit RDP to gain remote access and deploy ransomware.
9830	Status of the 'Prevent users from sharing files within their profile' setting	CRITICAL	✅	❌	Ransomware can spread through user-shared folders.
9304	Status of the "Do not preserve zone information in file attachments" setting for Windows users	CRITICAL	✅	❌	Downloaded files lack zone info, allowing ransomware to run without warnings.
1318	Status of the 'Enforce password history' setting	URGENT	✅ (Indirectly)	✅	Users may reuse weak or old passwords, aiding brute-force or credential stuffing attacks.
13924	Status of 'Block all Office applications from creating child processes' ASR rule (D4F940AB-401B-4EFC-AADC-AD5F3C50688A)	CRITICAL	✅	❌	Ransomware can use malicious Office macros to spawn additional malware.

Measuring Risk of Misconfiguration



Misconfig

+10

MITRE

+10

RDP/Access

+10

Ransomware

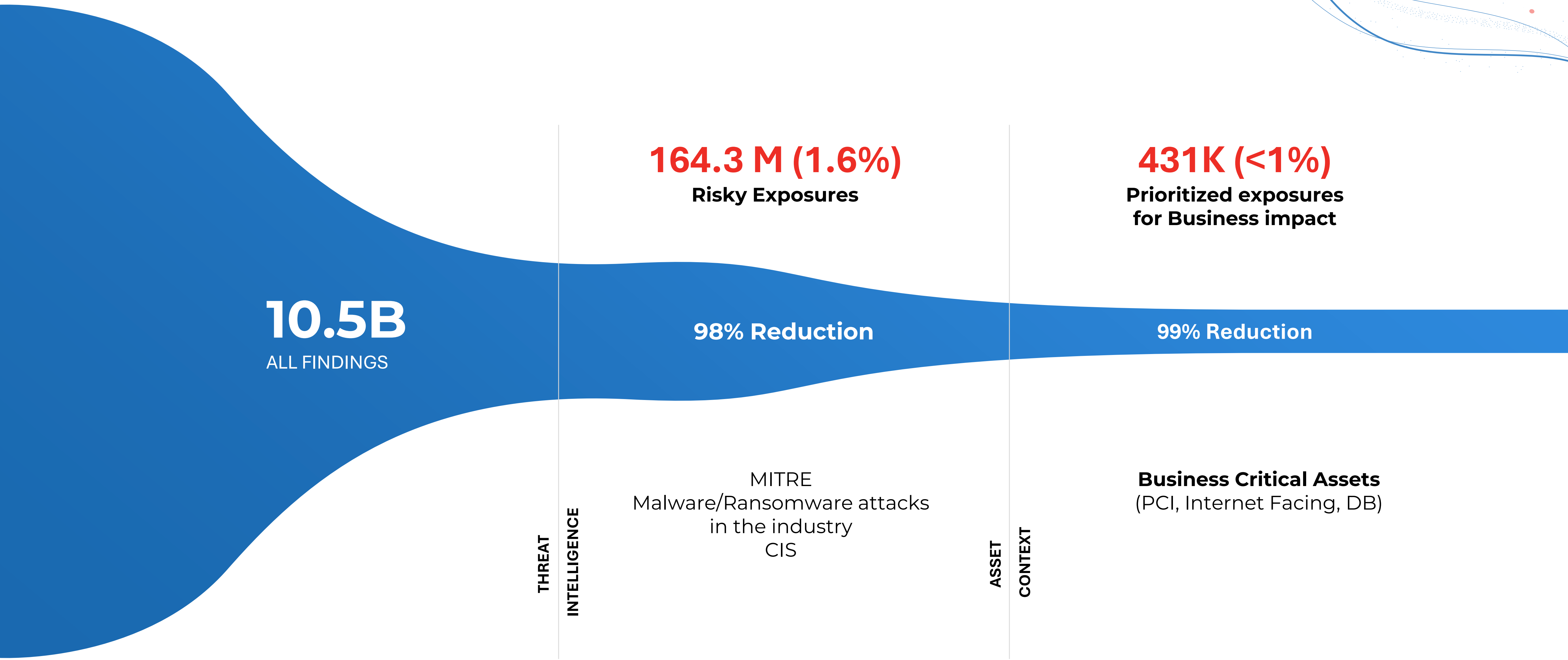
+20

CIS Top 5

95

Critical

Prioritizing Risk of Misconfigurations



10.5B
ALL FINDINGS

THREAT INTELLIGENCE

164.3 M (1.6%)
Risky Exposures

98% Reduction

MITRE
Malware/Ransomware attacks
in the industry
CIS

ASSET CONTEXT

431K (<1%)
**Prioritized exposures
for Business impact**

99% Reduction

Business Critical Assets
(PCI, Internet Facing, DB)

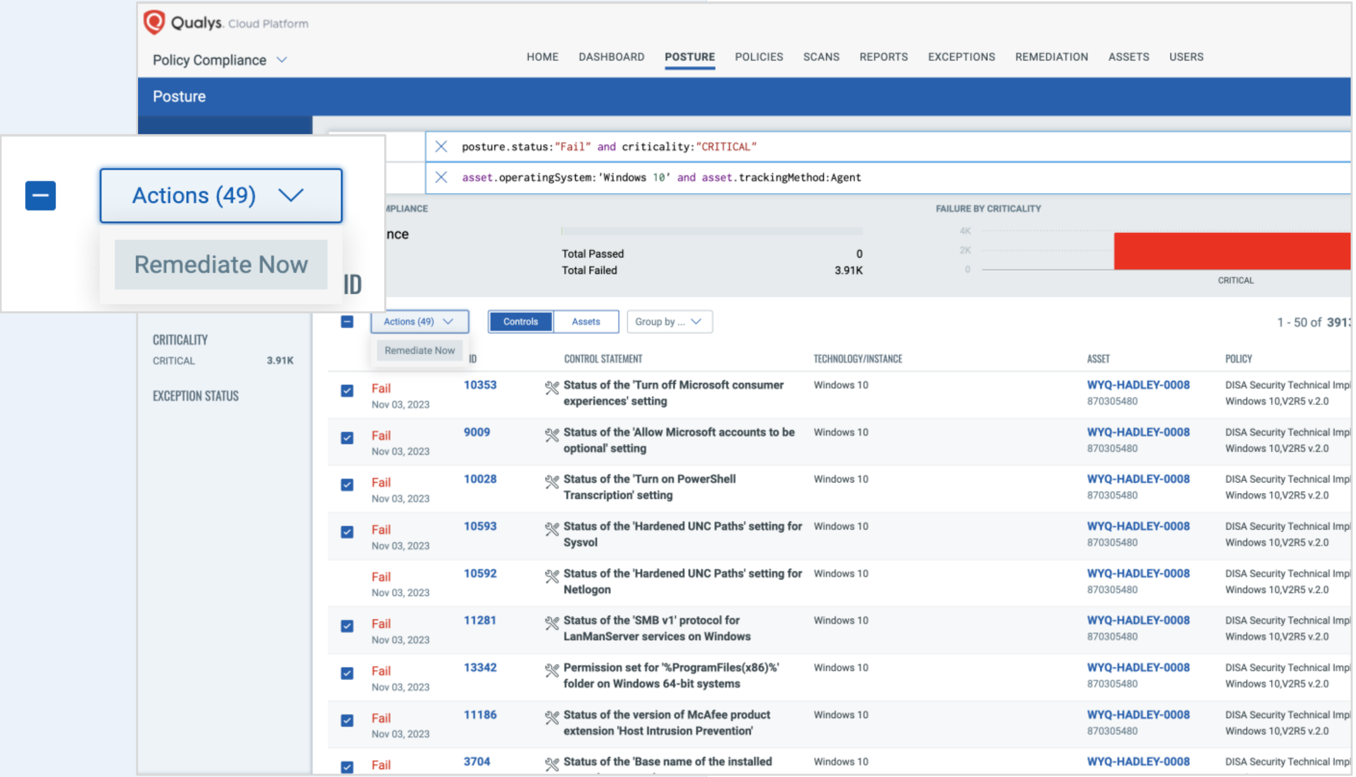
Audit Fix - Automated Remediation Workflows

Qualys. ROCon 25 The Risk Operations Conference APAC

Regulatory Alignment & Flexibility

- **Fix your Audit findings** before they become audit issues with Automated Remediation
- **Pre-defined library** of out of the box scripts
- **Customizable remediation**

Significantly Reduce Breach Exposure



```
posture.status:"Fail" and criticality:"CRITICAL"
asset.operatingSystem:'Windows 10' and asset.trackingMethod:Agent
```

MPLIANCE
nce

Total Passed	0
Total Failed	3.91K

CRITICALITY

CRITICAL	3.91K

EXCEPTION STATUS

1 - 50 of 391

		ID	CONTROL STATEMENT	TECHNOLOGY/INSTANCE	ASSET	POLICY
☑	Fail Nov 03, 2023	10353	Status of the 'Turn off Microsoft consumer experiences' setting	Windows 10	WYQ-HADLEY-0008 870305480	DISA Security Technical Impl Windows 10,V2R5 v.2.0
☑	Fail Nov 03, 2023	9009	Status of the 'Allow Microsoft accounts to be optional' setting	Windows 10	WYQ-HADLEY-0008 870305480	DISA Security Technical Impl Windows 10,V2R5 v.2.0
☑	Fail Nov 03, 2023	10028	Status of the 'Turn on PowerShell Transcription' setting	Windows 10	WYQ-HADLEY-0008 870305480	DISA Security Technical Impl Windows 10,V2R5 v.2.0
☑	Fail Nov 03, 2023	10593	Status of the 'Hardened UNC Paths' setting for Sysvol	Windows 10	WYQ-HADLEY-0008 870305480	DISA Security Technical Impl Windows 10,V2R5 v.2.0
	Fail Nov 03, 2023	10592	Status of the 'Hardened UNC Paths' setting for Netlogon	Windows 10	WYQ-HADLEY-0008 870305480	DISA Security Technical Impl Windows 10,V2R5 v.2.0
☑	Fail Nov 03, 2023	11281	Status of the 'SMB v1' protocol for LanManServer services on Windows	Windows 10	WYQ-HADLEY-0008 870305480	DISA Security Technical Impl Windows 10,V2R5 v.2.0
☑	Fail Nov 03, 2023	13342	Permission set for '%ProgramFiles(x86)%' folder on Windows 64-bit systems	Windows 10	WYQ-HADLEY-0008 870305480	DISA Security Technical Impl Windows 10,V2R5 v.2.0
☑	Fail Nov 03, 2023	11186	Status of the version of McAfee product extension 'Host Intrusion Prevention'	Windows 10	WYQ-HADLEY-0008 870305480	DISA Security Technical Impl Windows 10,V2R5 v.2.0
☑	Fail	3704	Status of the 'Base name of the installed	Windows 10	WYQ-HADLEY-0008	DISA Security Technical Impl

Demo

Qualys®

ROCon 25

The Risk Operations Conference

APAC