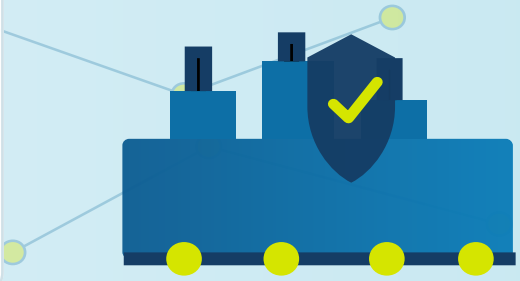
Steel Industry Vulnerability Management and Compliance at Scale

Continuous vulnerability assessment for a leading Indian steel manufacturer

EXECUTIVE CONTEXT

COMnet strengthened cyber-risk visibility for one of India's leading steel manufacturers by deploying the Qualys vulnerability management platform across 200 server and endpoint assets. The engagement introduced weekly vulnerability scanning, centralized asset visibility, CIS benchmark compliance reporting, prioritized remediation support, and 24/7 remote assistance under one managed delivery model.



200 — **Assets Covered**
Qualys visibility across server and endpoint assets.

7D — **Weekly Scanning**
Repeatable vulnerability assessment and reporting cadence.

CIS — **Compliance Reporting**
Benchmark-aligned posture visibility for audit readiness.

IMPACT

- Established centralized visibility of approximately 200 server and endpoint assets through the Qualys platform.
- Introduced weekly vulnerability scanning to identify new exposures and track remediation progress consistently.
- Improved risk prioritization by consolidating vulnerability findings, asset context, and severity information.
- Enabled CIS benchmark compliance reporting to strengthen regulatory, audit, and internal governance readiness.
- Reduced organizational cyber risk through structured remediation coordination and continuous 24/7 remote support.

MAJOR ISSUES

- The organization required a repeatable weekly scanning process across a mixed server and endpoint estate.
- Limited IT asset visibility made it difficult to maintain an accurate view of systems, ownership, and exposure.
- Vulnerability data needed to be consolidated and prioritized to support timely remediation by technical teams.
- Compliance stakeholders required benchmark-aligned reporting, particularly against CIS security controls.
- The client needed dependable post-deployment support, escalation, and platform assistance around the clock.

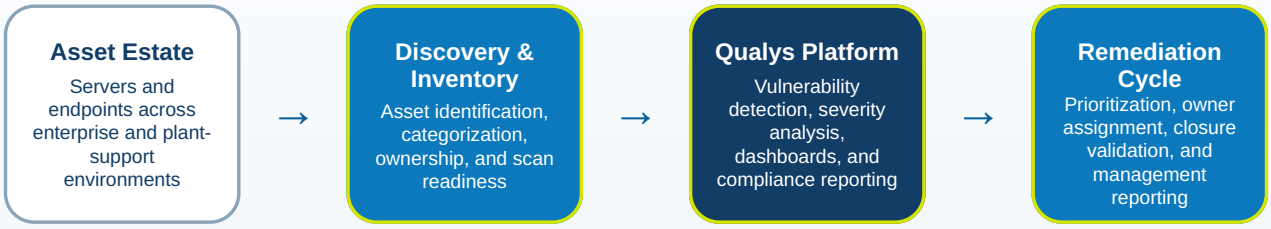
Steel Industry Vulnerability Management and Compliance at Scale

Continuous vulnerability assessment for a leading Indian steel manufacturer

HIGHLIGHTS

ARCHITECTURE AND DEPLOYMENT SCOPE

Continuous Vulnerability and Compliance Management Model



SRV — **Server Vulnerability Coverage**

Scheduled scanning and remediation visibility for business-critical server assets.

END — **Endpoint Vulnerability Coverage**

Consistent detection and reporting across managed user endpoint assets.

Engagement Highlights

- Assessed the server and endpoint estate, asset visibility gaps, scanning requirements, and compliance objectives.
- Designed and deployed the Qualys vulnerability management solution for approximately 200 assets.
- Established a weekly scanning cycle with repeatable reporting and remediation follow-up.
- Configured CIS benchmark-aligned compliance reports for audit and governance stakeholders.
- Implemented 24/7 remote support, incident handling, escalation, and platform assistance.

Technical Deployment Scope

- **Asset Discovery and Baseline:** Identified in-scope servers and endpoints, organized asset groups, and established a centralized inventory baseline.
- **Scanner and Platform Configuration:** Configured the Qualys environment, scanning profiles, schedules, credentials where applicable, dashboards, and reporting views.
- **Weekly Vulnerability Assessment:** Implemented scheduled scans to detect newly disclosed vulnerabilities, configuration weaknesses, and changes in exposure.
- **Risk Prioritization:** Structured findings by severity, asset criticality, and remediation ownership to focus technical teams on the highest-risk issues.
- **CIS Compliance Reporting:** Enabled benchmark-aligned reports to provide measurable visibility into configuration posture and control gaps.
- **Remediation Validation:** Supported rescans and closure verification after fixes were applied, improving accountability and evidence of risk reduction.
- **Managed Support Integration:** Provided 24/7 remote support, troubleshooting, reporting assistance, escalation coordination, and ongoing operational guidance.

Steel Industry Vulnerability Management and Compliance at Scale

Continuous vulnerability assessment for a leading Indian steel manufacturer

KEY STRATEGIES

OPERATIONS ASSURANCE MODEL

Continuous Vulnerability and Compliance Operations

Weekly scanning, risk prioritization, CIS benchmark reporting, remediation validation, SLA governance, and 24/7 remote support.

200	Weekly	CIS	24x7
Assets covered	Assessment cadence	Compliance reporting	Remote support

- **Asset-Visibility First:** A centralized inventory baseline was established so vulnerability findings could be tied to known servers, endpoints, owners, and business context.
- **Scheduled Assessment:** Weekly scanning created a dependable operating rhythm for discovering new exposures and monitoring changes in the environment.
- **Risk-Based Prioritization:** Findings were organized by severity and asset relevance to help technical teams focus remediation effort on the most material risks.
- **Compliance-by-Design:** CIS benchmark reporting was embedded into the operating model to support measurable governance and audit readiness.
- **Closed-Loop Remediation:** Scan, assign, remediate, rescan, and validate steps improved accountability and evidence of closure.
- **Operational Continuity:** Scheduled activities and support processes were structured to minimize disruption to business and production-support environments.
- **Managed Service Governance:** 24/7 support, escalation paths, reporting assistance, and periodic review strengthened platform reliability and operational consistency.

Solution Model

- **Qualys Vulnerability Management:** Central platform for detection, asset visibility, dashboards, and reporting.
- **200-Asset Coverage:** Server and endpoint assessment under a common governance model.
- **Weekly Scan Program:** Repeatable scheduling, reporting, and exposure tracking.
- **CIS Compliance:** Benchmark-aligned configuration posture and gap reporting.
- **Managed Services:** 24/7 remote support, troubleshooting, escalation, and operational guidance.

OK

EXECUTIVE OUTCOME

COMnet established a continuous vulnerability and compliance management foundation across approximately 200 server and endpoint assets, improving IT asset visibility, reducing cyber risk, strengthening CIS-aligned compliance reporting, and sustaining operations through 24/7 Qualys support.