# Dashboard in Details

*Prepared by*

*Saiyeda Marzia*

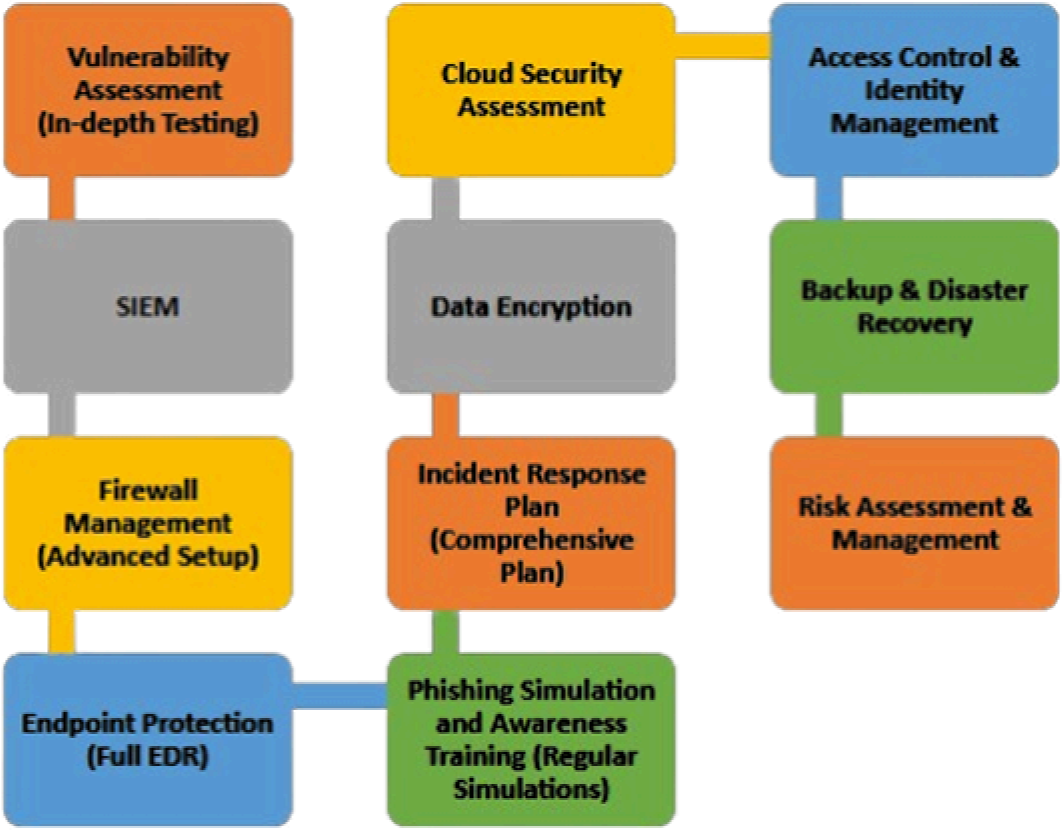
*SOC Engineer*

*@Cyberlog*

*20 September 2025*

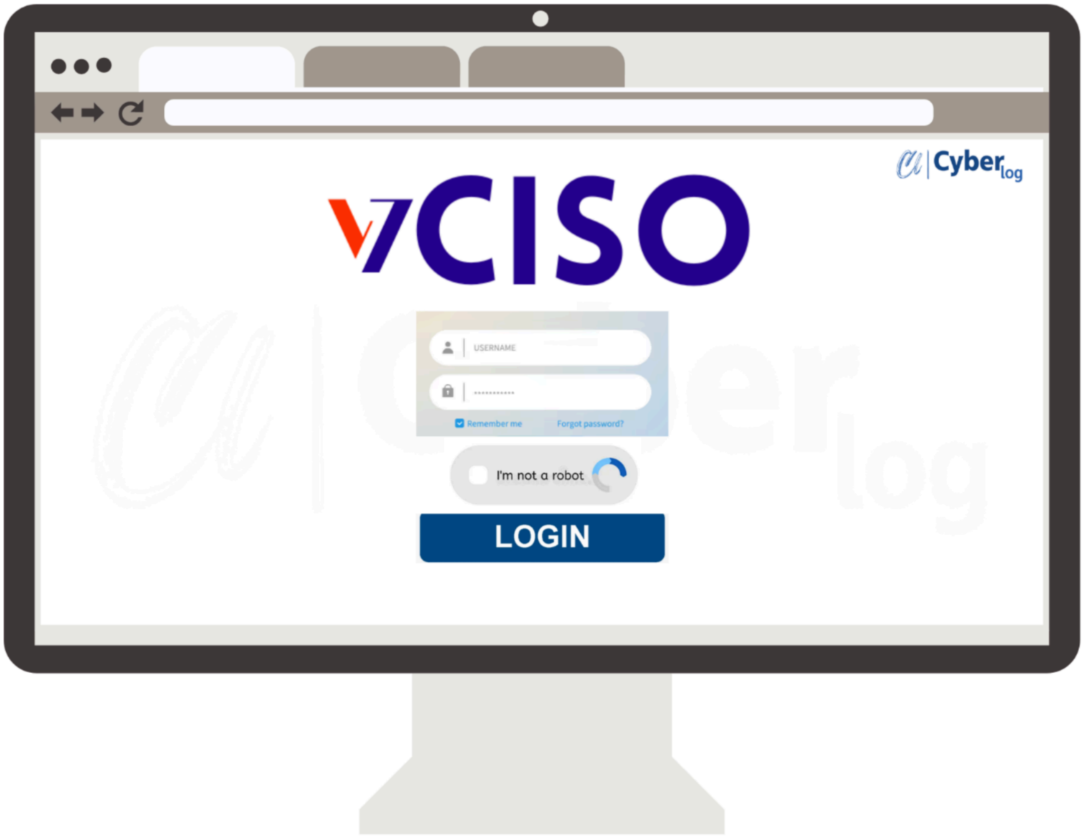
## Introduction

Cyberlog is launching vCISO service very soon for the first time in Bangladesh. The services we offer are given in the following figure. We want to have a dashboard of our vCISO service that will give not only our clients but also admin personnel a clear view of the ongoing status of the service at a glance. This report is the detailed discussion of what will be shown in the dashboard as per the Cyberlog vCISO service.


Vulnerability Assessment (In-depth Testing)
SIEM
Firewall Management (Advanced Setup)
Endpoint Protection (Full EDR)
Cloud Security Assessment
Data Encryption
Incident Response Plan (Comprehensive Plan)
Phishing Simulation and Awareness Training (Regular Simulations)
Access Control & Identity Management
Backup & Disaster Recovery
Risk Assessment & Management

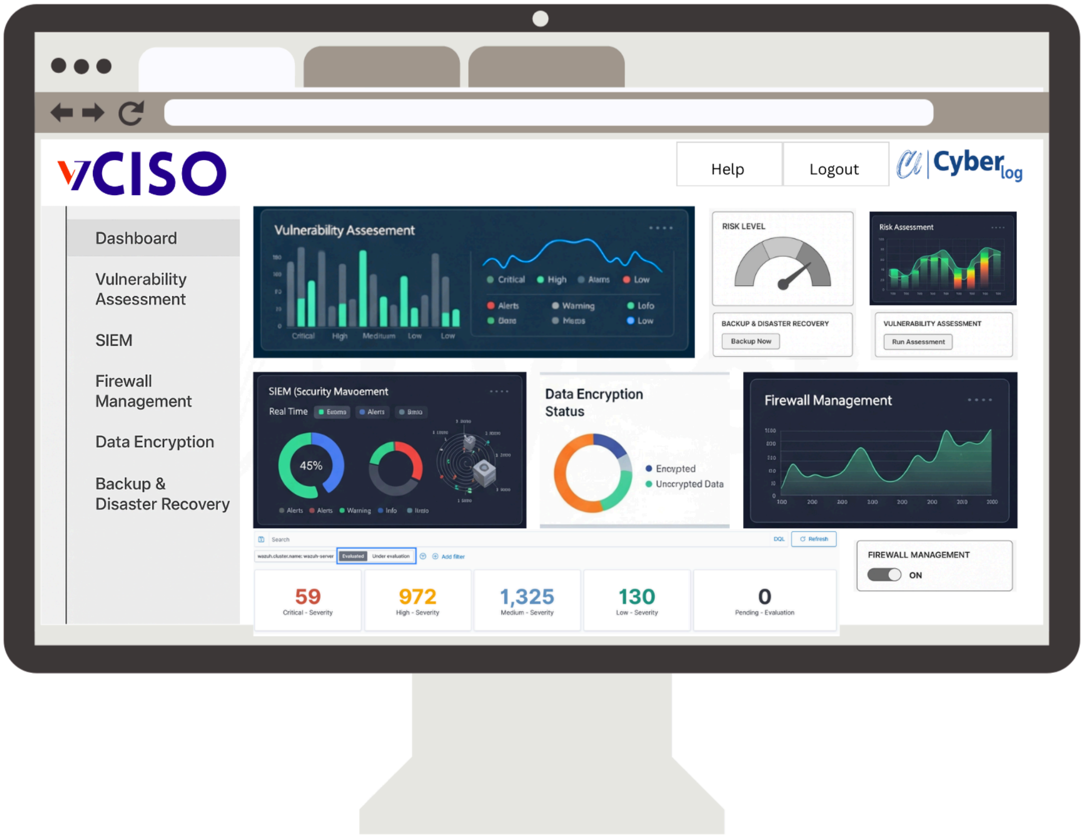
## Access Control and identity Management

- Have a login page with captcha
- Have the option to recover password (forgot password)
- Enter username and password
- Two types of login: admin and clients
- Admin can create client accounts.
- Admin will have access to all services and can edit or delete services of the clients



## Overall Dashboard

It will have a glimpse of all the services bought by the client according to the tier. If double-clicked on a specific service, it will take the client to its own vast dashboard.



## VAPT

- Total vulnerabilities vs. resolved (Trending graph showing vulnerabilities discovered vs. remediated over time)
- Total vulnerabilities (open, in-progress, closed)
- Severity breakdown (Critical, High, Medium, Low)
- Top 5–10 critical vulnerabilities
- Links to remediation guidance or tickets
- Number of assets scanned (web apps, servers, endpoints, cloud)
- Asset health status (secure, at risk, unknown)
- Exposure by asset type
- Pie or bar charts showing severity by:
  - Application/module
  - Location/department
  - CVSS score range
- Percentage of coverage vs. planned scope
- Timeline of recent scans
- SLA compliance for fixes (e.g., % of critical issues fixed within 7 days)
- Assigned teams or owners
- Status of patches
- Compliance gaps mapped to standards
- Compliance status (PCI DSS, ISO 27001, etc.)
- Export options for both technical and executive summaries, detailed reports, audit-ready PDFs
- List of services

## SOC (Security Operation Center)

- This section can be organized in two ways.
    1. We allow clients to access only specific pages of Wazuh (not all), such as Alerts, Threat Hunting, Agents Status, FIM, VirusTotal, and a Custom Dashboard
    2. Give the clients full access to the Wazuh dashboard (but not as admin) and have a separate section of at-a-glance services.

**Details of the second option:**

Two parts: one is the Wazuh dashboard, and the other is at-a-glance information

a) Wazuh dashboard (Full access to wazuh and all its services as a client user account)

b) At a glance -------------------------

- Overall risk/security score
- Total open incidents, with severity breakdown (Critical / High / Medium / Low)
- Percentage of incidents contained vs. resolved
- Latest alerts (sortable by time, source, severity)
- Incident trend graph (e.g., last 24h / 7d / 30d)
- Top unresolved incidents with SLA timers
- Drill-down links to investigation details
- Geo-location map of current attacks or suspicious IPs
- Emerging campaigns or malware families detected
- Number of endpoints monitored vs. unmonitored
- Compliance status (patching, EDR, antivirus)
- Bandwidth anomalies, unusual protocols, or traffic spikes

- IDS/IPS events by severity
- Firewall block vs. allow statistics
- Outstanding vulnerabilities (grouped by CVSS severity)
- Exposure of internet-facing assets
- Patch coverage percentage
- Suspicious login attempts (failed, from new geographies, MFA bypass)

- Privileged account activity summary
- Insider-threat indicators
- MTTR (Mean Time to Respond) & MTTD (Mean Time to Detect) trends
- Able to download reports

## Firewall Management

- Status of each firewall (online/offline, healthy, degraded)
- CPU / memory usage & uptime
- Firmware / OS version, update status
- Total traffic allowed vs. blocked (graph)
- Bandwidth utilization by interface or zone
- Top applications / services using bandwidth
- Geographic map of traffic sources & destinations
- ID, source/destination, service, action (allow/deny)
- Hit count (how often rules are used)
- Policy compliance score (e.g., following least-privilege)
- Denied connections by reason (geo-block, port scan, etc.)
- Malware or IPS alerts from firewall modules
- Top attack sources & destinations
- Current VPN sessions (site-to-site & client)
- Connection success/failure rates
- Bandwidth used by VPN tunnels
- Scheduled reports (e.g., daily traffic, monthly security events)
- Threshold-based alerts (e.g., CPU > 80%, session limit reached)
- Export options (CSV, PDF, syslog forwarding)

## Data Encryption

- Overall encryption compliance score (e.g., % of data protected)
- Quick view of:
  - Data at rest (disks, databases, backups)
  - Data in transit (TLS, VPNs, secure email)
  - Data in use (applications using encryption)
- List of systems & storage where data resides (servers, databases, cloud buckets, endpoints)
- Encryption status per asset:
  - Enabled / Not enabled / Partial
- Algorithm & key length (AES-256, RSA-2048, etc.)
- Alignment with standards (GDPR, HIPAA, PCI DSS, ISO 27001)
- Policy violations (e.g., unencrypted PII or payment data)
- Audit readiness indicator
- Number of files / databases encrypted in a period
- Failed or pending encryption jobs
- Alerts:
  - Key compromise
  - Unsupported cipher detected
  - Data stored in plaintext
- Overhead from encryption on CPU / memory
- Throughput for bulk encryption tasks
- Key rotation success rates
- Integration with DLP, SIEM, or backup systems
- Quick actions: (presented in buttons)
  - Rotate keys
  - Enable encryption on an asset
  - Export compliance report

## Risk Assessment and Management

- The overall risk score shows the total enterprise risk level, for example, 72 out of 100, or “Medium.”
- The Risk Register Summary lists the number of risks by status, such as Open, Mitigated, or Accepted.
- Top Risks includes the highest-ranked risks with their severity and trend.
- The risk heat map displays a likelihood versus impact matrix with color coding.
- Control effectiveness indicates how well controls reduce risk in percentage.
- Residual risk represents the risk remaining after controls, shown per asset or department.
- Compliance and framework mapping show risks tied to standards like ISO 27001, NIST, or CIS.
- Remediation Progress tracks open versus closed mitigation tasks and SLA adherence.
- Audit and review dates provide information on the next assessment, last update, and owner of each risk.

## Incident Response plan

- Active Incidents: Number of ongoing incidents with severity levels (High, Medium, Low).
- Incident Status: Breakdown of incidents by status, such as New, In Progress, Contained, Resolved, or Closed.
- Incident Type Distribution: Categorization of incidents (e.g., malware, phishing, insider threat, DDoS, data breach).

- Mean Time to Detect (MTTD): Average time taken to detect incidents.
- Mean Time to Respond (MTTR): Average time taken to contain and remediate incidents.
- Top Incident Sources: Sources or systems where incidents are most frequently detected.
- Trend Over Time: Graph showing incidents over days, weeks, or months to identify patterns.
- Impact Analysis: Estimated impact per incident in terms of business, financial, or operational loss.
- Response Team Activity: Actions taken by the response team per incident, including task completion and ownership.
- Remediation Progress: Percentage of incidents mitigated versus pending mitigation.
- Compliance & Reporting: Incidents tied to compliance frameworks like ISO 27001, NIST, or GDPR reporting requirements.
- Lessons Learned / Post-Mortem: Summary of incident outcomes, root causes, and recommended preventive measures.

## Backup and Disaster Recovery

- Backup job success/failure status
- Recovery Point Objective (RPO) and Recovery Time Objective (RTO) metrics
- Storage utilization (local/cloud/immutable)
- Recent restore tests and their results
- Active alerts (e.g., failed backup, nearing capacity)
- Replication status between sites or clouds
- Version history and retention periods
- Graph of backup trends over time

## Security Training

- Total Employees enrolled in training
- Training Completion Rate (%)
- Pending Training count
- Progress by Department
- Training Type Breakdown
- Assessment Scores / Pass-Fail Rate
- Top Performers
- Training Frequency over time
- Compliance Status (ISO, GDPR, HIPAA)
- Upcoming Training Schedule
- Phishing Simulation Results
- Feedback / Ratings

# Thank You