CygniSoft Cybersecurity Audit Report

Formal Corporate Layout with Risk Heat Map and Visual Charts

Prepared for Orion Manufacturing Ltd.
Prepared by CygniSoft Cybersecurity Division
Report Version 3.0 • January 2025

Table of Contents

Executive Summary

CygniSoft performed a full-spectrum cybersecurity audit covering infrastructure, applications, networks, cloud posture, and employee security behaviour. The audit uncovered several high-risk and medium-risk findings, primarily related to outdated software, misconfigured access controls, and gaps in endpoint security. No active breaches were detected, but multiple vulnerabilities could lead to compromise if not addressed.

Overall Security Score: 72 out of 100
Industry Average (Manufacturing): 64 out of 100

Audit Scope

Assessed Areas

- Network and firewall architecture
- Cloud security posture (AWS)
- Web applications and APIs
- Identity and access management
- Endpoint protection and patch lifecycle
- Incident response maturity
- Social engineering risk
- Backup and recovery readiness

Assets Reviewed

- 42 servers
- 118 endpoints
- 37 cloud workloads
- 2 customer-facing applications
- 312 user accounts

Methodology

Include:

- Automated scanning tools
- Manual security review
- Penetration testing
- Configuration audits
- Social engineering simulations

Key Findings Overview

Summaries of critical, high and medium findings.
Examples:

- Outdated VPN service vulnerable to RCE
- Excessive admin accounts
- SQL injection vulnerability
- Weak passwords and compromised credentials
- Public S3 buckets with open read access

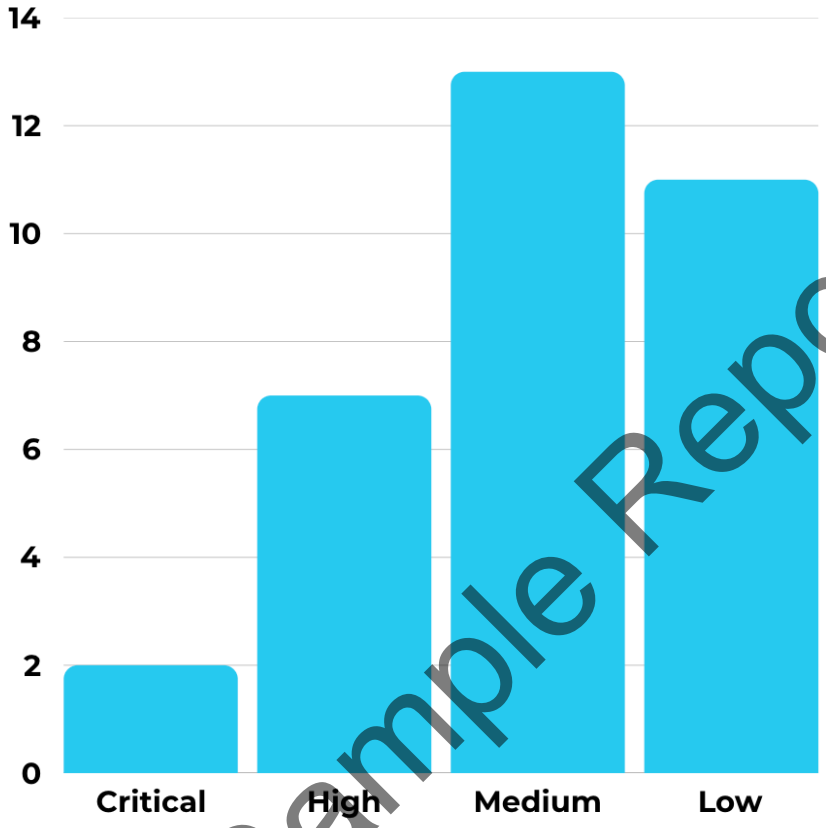
Risk Heat Map

Impact ↓ / Likelihood →	Low	Medium	High
High Impact	Moderate Risk	Significant Risk	**Critical Risk**
Medium Impact	Low Risk	Moderate Risk	Significant Risk
Low Impact	Minimal Risk	Low Risk	Moderate Risk

- **Critical Risk:**
  - Outdated VPN with RCE (High likelihood, High impact)
  - SQL injection vulnerability (High likelihood, High impact)
- **Significant Risk:**
  - Admin privilege excess
  - Missing endpoint patches
  - Over-permissive firewall rules
- **Moderate Risk:**
  - Weak password usage
  - MacOS unsupported versions
  - S3 logging disabled

Vulnerability Breakdown Chart

Bar Categories and Values:



Penetration Testing Results

1. External Attack Surface

- 4 high risk
- 6 medium
- 18 low

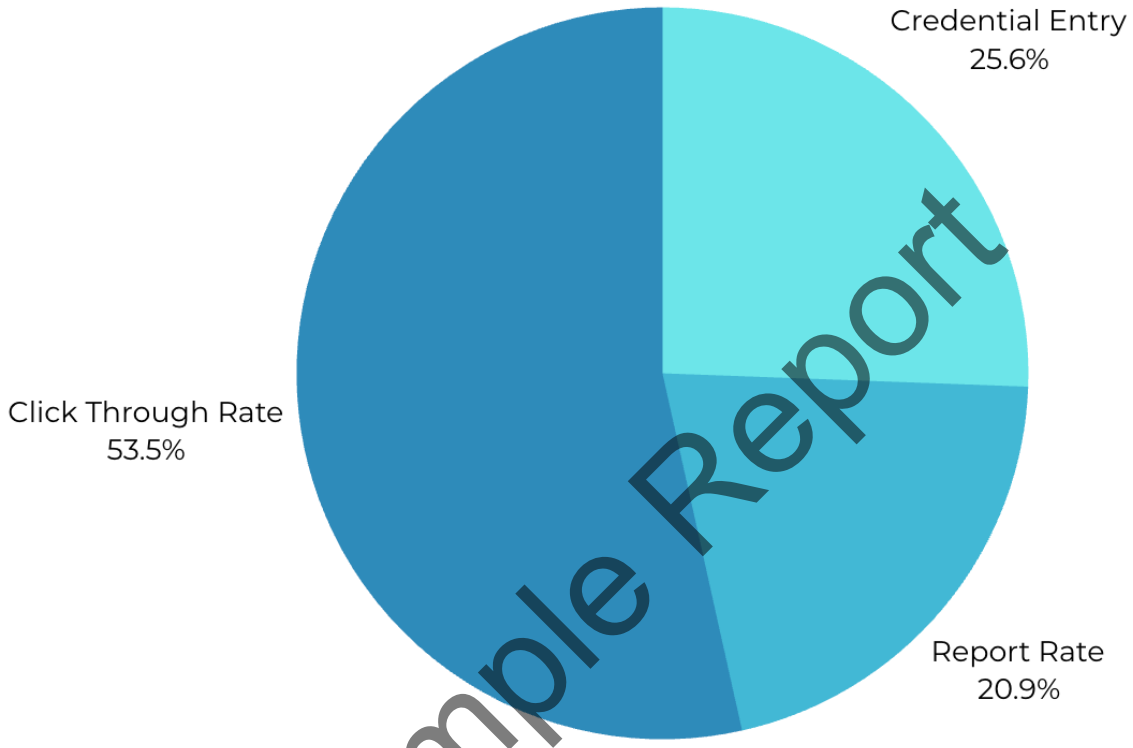
2. Internal Network Exposure Chart

List:

- Lateral movement possible: Yes
- Privilege escalation paths: 3 identified

- Misconfigured AD permissions: 7 instances

3. Phishing Simulation Result Chart



Infrastructure and Cloud Review

Network Summary

- 126 firewall rules
- 14 overly permissive inbound rules
- 6 legacy protocol rules

Endpoint Summary

- 7 devices missing real time protection
- 28 missing patches
- 4 outdated antivirus engines

Cloud Summary

- 11 roles violating least privilege
- MFA adoption: 92 percent for admins, 71 percent for others
- 5 buckets missing logging

Compliance Evaluation

ISO 27001 Alignment

- Access control: 68 percent
- Operations security: 74 percent
- Supplier relationships: 81 percent
- Cryptographic controls: 92 percent

NIST CSF Maturity

- Identify: Partial
- Protect: Adequate
- Detect: Developing
- Respond: Partial
- Recover: Adequate

Recommendations and Remediation Plan

Immediate (0 to 30 days)

- Patch VPN RCE vulnerability
- Fix SQL injection
- Disable unused admin accounts
- Reset weak credentials
- Enable MFA organization-wide

Short Term (30 to 90 days)

- OS and security patch lifecycle enforcement
- Centralized cloud logging
- Firewall rule cleanup
- Phishing training cycle

Long Term (90 to 180 days)

- Implement Zero Trust
- Deploy SIEM with continuous monitoring
- Annual penetration testing

- DR strategy upgrade with immutable backups

Final Rating and Conclusion

Current Score: 72
Projected Score Post Remediation: 88

CygniSoft is confident that with the remediation steps outlined in this report, Orion Manufacturing Ltd. can achieve a significantly stronger cybersecurity posture within a short timeframe. The organization already demonstrates a solid foundation, supported by structured IT processes, modern cloud tooling and well maintained core systems. The gaps identified during this audit are addressable through targeted and achievable improvements rather than large scale architectural changes.

By resolving the critical vulnerabilities, tightening identity and access controls, improving endpoint hygiene and implementing centralized monitoring, the company will reduce its exposure to external and internal threats. The combined effect of these enhancements directly strengthens the organization's resilience, lowers operational risk and improves overall compliance alignment.

Once the recommended actions are completed, CygniSoft projects an uplift of the security score from 72 to 88, representing a mature and defensible cybersecurity posture appropriate for modern threat landscapes. This improved posture will enable Orion Manufacturing Ltd. to operate with increased confidence, safeguard its operational continuity and better protect its customers, partners and intellectual property.

CygniSoft remains committed to supporting the organization through its remediation journey and stands ready to assist with implementation, validation and ongoing security improvement initiatives.