360° Business Cyber Intelligence

For: Company Name

Date: 06/10/25

Report Overview

360° Business Cyber Intelligence provides a comprehensive view of your organisation's cybersecurity posture — analysing your digital footprint, identifying data leaks, assessing compliance levels, evaluating financial exposure, and uncovering potential vulnerabilities or entry points that could be exploited

Each assessment is evaluated using an industry-recognized scoring framework with defined weightings to provide an objective and balanced view of the organization's overall security posture. The findings are intended to inform decision-making, guide strategic planning, and support cybersecurity budgeting and investment priorities.

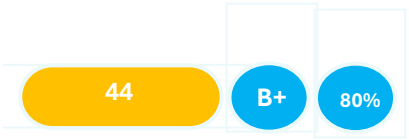
Results Summary

Open Risks Level

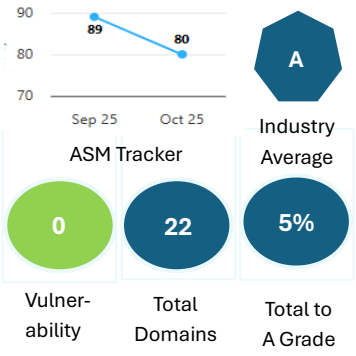
44	**Attack Surface Analysis Level1**: Severe impact. Immediate action required within days Please refer to page 2 for action details.
2	**WAN IP Compromised Level1**. Moderate impact. Needs remediation within a reasonable timeframe Please refer to page 3 for action details
5	**Data Leaks Level2:** Minimal impact. No immediate action is required. Please refer to page 4 for action details.
2	**Email Credential Leaks Level2**: Moderate impact. Needs remediation within a reasonable timeframe Please refer to page 5 for action details
11	**Baseline Compliance Level3:** Moderate impact. Needs remediation within a reasonable timeframe Please refer to page 6 for action details.
	Financial Exposure Level3: Minimal impact. No immediate action is required. Please refer to page 7 for action details.
-	**3rd Party Analysis Level4:** - Not tested

BREACH LIKELIHOOD < Once Yearly	INDUSTRY ASM AVERAGE Medium	COMPLIANCE | ASM Pass 73% | 80%
DOMAINS DISCOVERED 6	FINANCIAL EXPOSURE $1.5m	TOTAL OPEN RISKS 55

Attack Surface



Attack Surface Analysis [L1] evaluates your organization's digital footprint to identify potential entry points that attackers could exploit. It includes assessments of email and website security configurations, checks for known vulnerabilities, and identifies compromised systems or exposed data. The analysis also covers data privacy risks and open network ports, providing a comprehensive view of areas that require remediation to reduce overall cyber risk.



Assessment Summary

Domain in Scope [Domain [Grade], Last Scanned [Date] By [User]

Failed Control	Threat Severity	Domain Failed For remediation refer to Cygienic.com/login	Control Checked
SPF-Email		Domain.com	No
Email SPF Treatment		Domain.com	No
DMARC Authentication		Domain.com	No
HSTS-Enabled		Domain.com	No
XFrame-Option		Domain.com	No
XSS-Protection		Domain.com	No
MIME X-Content		Domain.com	No
Content Security Policy		Domain.com	No
Referrer Policy		Domain.com	No
Cache-Control		Domain.com	No
X Domain permission		Domain.com	No
Except-CT TLS		Domain.com	No
Open Proxy Services		Domain.com	No
Malware Hosting		Domain.com	No
SSL Renegotiation		Domain.com	No
Remaining ASM Passed			

REMAINING REPORT REDACTED

Redacted -WAN IP

Redacted -DATA LEAKS

Redacted -EMAIL CREDENTIALS

Redacted -BASELINE COMPLIANCE

Redacted -FINANCIAL EXPOSURE