

9/24/2025

# Cyber Intelligence Report

Level I

For Acme Group

## Overview

This Level 1 Cyber Intelligence Assessment delivers clear insights into your attack surface and potential data leaks. Each area is rated from Low to Critical using trusted industry frameworks and scoring models, with weightings applied to reflect both security posture and business impact. The result is an actionable snapshot to guide smarter decision-making, strategic planning, and budgeting. For a full 360° view of your company's cybersecurity readiness, we recommend upgrading to Levels 2 and 3.

## Executive Summary

### Analyst commentary



Medium

### Level 1 Cyber Risk Rating

Medium

Attack Surface Analysis L1: Rates your digital footprint from Low to Critical, indicating the exposure level across entry points attackers could exploit.

Low

Data & Email Credential Breach L1: Rates data leaks from Low to Critical, indicating levels of employee and customer data found in the dark web.

-

Financial Exposure L2: Rates your potential loss impact from Low to Critical, showing the monetary risk attackers could cause

-

Baseline Compliance L2: Rates your adherence from Low to Critical, showing gaps against essential cybersecurity standards and controls.

-

3rd Party Analysis L3: Rates external vendor and partner risks from Low to Critical, showing exposure inherited through your supply chain.

BREACH LIKELIHOOD  
- yearly

INDUSTRY ASM AVERAGE  
Medium

COMPLIANCE | ASM  
Pass -% | -%

TOTAL DOMAINS  
10

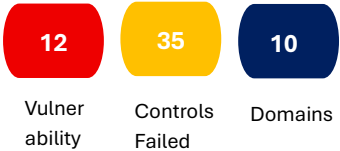
FINANCIAL EXPOSURE  
\$-m

DATA & EMAIL BREACH  
23

Attack Surface

CriticalD

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 Scope

www.domain.com, www.app.domain.com

FAILED CONTROL	CONTROL REMEDIATION	DOMAIN FAILED
CRITICAL VULNERABILITY	CVE-2021-3456: Please check <a href="https://nvd.nist.gov">https://nvd.nist.gov</a> for remediation of this code.	www.domain.com



WAN IP Compromised

High

WAN IP Compromise Analysis [L1] evaluates your public IP addresses to ensure they are not being exploited by attackers. The assessment checks for malware distribution, unauthorized proxy services, spam operations, and botnet activity originating from the IP. This helps ensure your network remains secure and prevents your infrastructure from being used for malicious activities.



Assessment Scope

234.445.65.33; 234.545.66.22

WAN IP	THREAT ID	THREAT REMEDIATION
234.445.65.33	Malware Distribution	Contact your system admin or hosting provider to alert them of this finding. Scan your server with the latest malware software. Consider rebuilding the server from last known good backup.

# Data Leak

Critical

Data Leak Checks [L1] identify exposed company, employee and customer information across multiple sources. The assessment scans code repositories, Google public shares, paste sites, and the deep web to detect sensitive data leaks. This helps prevent unauthorized access, protect intellectual property, and reduce the risk of data breaches.



## Assessment Scope

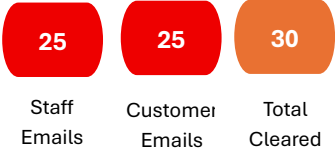
Company name searched here

SEARCH TERM	THREAT ID	URL THREAT ID
ACME	Paste Site	www.domain.com/data123

Email Credentials

High

Email Credential Checks [L1] identify if staff email accounts have been compromised, including stolen passwords. The assessment scans for exposures across external website registrations and customer accounts linked to your company domain. This helps prevent unauthorized access, phishing attacks, and potential business email compromise.



Assessment Scope

Acme.com; domain.com

USERNAME	DATE OF BREACH	WEBSITE BREACHED
STAFF EMAIL		
JOHN@DOMAIN.COM	12/12/25	www.domain.com
CUSTOMER EMAIL		
JANE@GMAIL.COM	12/12/25	www.acms.com



Thank You

Please contact  
[support@cygienic.com](mailto:support@cygienic.com)