DARKNETSEARCH
BY KADUU

Attack Surface Report

acmesample.com

Attack surface observed: 2026-09-02 21:04 UTC

Report generated: 2026-09-16 17:15 UTC

SAMPLE REPORT — IDENTIFIERS ANONYMIZED

Executive Summary

Target Profile

Domain	acmesample.com
Organisation	Acme Sample GmbH
Type	Private Company
Industry	Industrial Manufacturing
Size	501-1000 employees
Headquarters	Sample City, United States
Operating In	United States, Canada

Acme Sample GmbH, a private North American company in the Industrial Manufacturing industry, faces moderate cyber targeting pressure. The industrial manufacturing sector is increasingly targeted by cyber threats, particularly ransomware and supply chain attacks, due to its reliance on technology and complex supply chains. Operating in Canada and the United States, both frequent targets for cybercrime, further increases the risk. With a company size of 501-1,000 employees, Acme Sample GmbH is a viable target for cybercriminals seeking financial gain through ransomware and other cyber threats.

About This Report

> This report provides a hacker's-eye view of your organization's attack surface, based on passive reconnaissance methods. By aggregating data from multiple intelligence sources, it reflects how an attacker could identify exposed assets, services, and potential risks — without conducting any intrusive scanning.

The scanned website domain **acmesample.com** uses a different domain for employee email: **acmesample.com, acmesample.net**. Credential leak searches covered all identified email domains.

Infrastructure Footprint Comparison

DOMAIN	EST. SUBDOMAINS
acmesample.com (initial input domain)	~54
acmesample.net	~1

Report Structure

This report is organised into five main chapters, each covering a distinct dimension of the attack surface:

CHAPTER	FOCUS	PAGE
Network	IP ranges, network neighbours, hosting, geographic distribution	14

CHAPTER	FOCUS	PAGE
Applications	Tech stack, DNS & email security, vulnerabilities, TLS, web app security	**49**
Infrastructure	Ports, subdomains, auth surface, software risk, admin panels, exposure	**68**
People	Credentials, breach content, email enumeration, VIP digital footprint	**18**
Threat Landscape	IP reputation, code exposure, Telegram/Discord/paste, social media, typosquatting	**82**

KEY SECURITY SCORES OVERVIEW

55 / 100

SECURITY POSTURE

FAIR

Composite across 12 assessment areas. Higher is better.

5.8 / 10

OPERATIONAL RISK

ELEVATED

Sensitive to active critical findings. Driven by worst-case hosts and urgent conditions.

The Attack Surface Monitoring report for Acme Sample GmbH encompasses a thorough evaluation of the organization's digital footprint, revealing a total of **54 hosts** and **25 resolved IPs**. The organization's Security Posture Score is **55/100** (FAIR) with an Operational Risk level of **5.8/10** (ELEVATED). The assessment utilized a combination of automated scanning and manual review to identify vulnerabilities and exposures across various domains.

Key findings indicate significant risks, including **26 credential leaks** and **11 cloud exposed files**, which heighten the organization's vulnerability to unauthorized access. Additionally, the presence of **372 typosquatting domains** with live DNS records poses a potential threat to brand integrity. The web application security posture score stands at **74**, with **3 high-severity issues** identified, necessitating immediate remediation.

To mitigate identified risks, it is recommended that Acme Sample GmbH conduct a separate scan of its email domain due to discrepancies between its website and email domains. Strengthening cloud security measures and addressing the high-severity vulnerabilities in web applications should be prioritized. Furthermore, implementing monitoring for typosquatting threats and enhancing email authentication protocols will bolster the organization's overall security posture.

Key Findings

- There are **26 credential leaks** associated with the organization.
- A total of **372 typosquatting domains** with live DNS records were identified.
- The web application security score is **74**, with **3 high-severity vulnerabilities**.
- Cloud exposure includes **11 files** that are publicly accessible.

- The organization’s email domain differs from its website domain, warranting a dedicated email domain scan.

SECURITY SCORES DETAILS

Scale: **0 = maximum exposure / worst**, **100 = best posture** — higher is better for every category below (e.g. a People Exposure score of 0/100 means the org is maximally exposed, not that nothing was found).

0 — **PEOPLE EXPOSURE** — CRITICAL
1 employee with stealer log exposure
Weight: 10%

50 — **BRAND PROTECTION** — POOR
362 typosquats with active web servers
Weight: 4%

53 — **VULNERABILITIES** — POOR
67 unverified critical/high CVEs (product-matched)
Weight: 20%

64 — **NETWORK** — FAIR
3 hosts with high-risk services, 5 unusual-port hosts
Weight: 11%

70 — **CREDENTIALS** — FAIR
9 critical-risk mailboxes
Weight: 20%

74 — **WEB APPLICATION SECURITY** — FAIR
3 high-severity web security issues
Weight: 10%

76 — **DNS & EMAIL** — GOOD
No critical DNS/email issues
Weight: 10%

79 — **THREAT ACTOR EXPOSURE** — GOOD
Moderate sector targeting pressure
Weight: 5%

80 — **SOCIAL MEDIA** — GOOD
1 impersonation risk found
Weight: 3%

82 — **INFRASTRUCTURE** — GOOD
1 authentication endpoint detected
Weight: 5%

90 — **HACKER CHANNEL EXPOSURE** — EXCELLENT
No hacker channel / paste site mentions detected
Weight: 5%

91 — **TLS / SSL** — EXCELLENT
2 weak protocol hosts
Weight: 10%

POSTURE SCORE GUARDRAILS ACTIVE

55 **Compound Risk:** 8 hosts with compound risk ≥ 8.0

HOW THIS SCORE IS CALCULATED

CATEGORY	WEIGHT	SCORE	CONTRIBUTION
DNS & Email	10%	76 / 100	7.6 pts
TLS / SSL	10%	91 / 100	9.1 pts
Vulnerabilities	20%	53 / 100	10.6 pts
Credentials	20%	70 / 100	14.0 pts

CATEGORY	WEIGHT	SCORE	CONTRIBUTION
Network	11%	64 / 100	7.0 pts
Infrastructure	5%	82 / 100	4.1 pts
Brand Protection	4%	50 / 100	2.0 pts
People Exposure	10%	0 / 100	0.0 pts
Social Media	3%	80 / 100	2.4 pts
Hacker Channel Exposure	5%	90 / 100	4.5 pts
Web Application Security	10%	74 / 100	7.4 pts
Threat Actor Exposure	5%	79 / 100	4.0 pts

Scoring methodology: Each category uses logarithmic scaling (not raw counts) with prevalence multipliers — widespread issues across many hosts are penalised more heavily than isolated findings. The legacy vulnerability model separates verified findings from passive/product-matched indicators but does not apply the DS-90 evidence-tier contribution multipliers. Prevalence multipliers of up to 1.75× still apply where supported. Business-critical hosts (auth endpoints, admin panels) amplify risk via cross-module correlation. The Posture Score is a weighted average with guardrail caps that prevent a misleadingly good overall score when any single area is critically compromised. The Operational Risk Score is driven by compound host risk — hosts where multiple risk factors overlap (e.g. admin panel + weak TLS + leaked credentials). (Scoring model: legacy.)

MOST IMPORTANT FINDINGS

6

HIGHEST ASSET RISK

6 / 10

Worst single host in this scan (0 = lowest).

CVE INSTANCES

245

From Shodan, Netlas, ZoomEye & CVEDB

VERIFICATION FINDINGS

2

Actionable · +397 informational

SECURITY POSTURE (AT A GLANCE)

CVE references are derived from **service banner analysis** (Shodan, Netlas, ZoomEye) and **product version matching** (CVEDB). These are indicators based on detected software versions — not confirmed exploits. Prioritize by severity, exposure, and business context; see the full Vulnerability Assessment section for confidence tiers.

SCOPE & FOOTPRINT

SUBDOMAINS FOUND
54
Unique FQDNs discovered

LIVE HOSTS
25
Resolved to an IP

IP RANGES
0
Owned network blocks (RIR)

OPEN PORTS (HOSTS)
22
Passive + Nmap confirmed

SENSITIVE HOST NAMES
9
Flagged subdomains

HOSTS W/ VULN SIGNALS
10
Any CVE-related signal

SCAN DURATION
91 min
Pipeline wall time

CLEAN HOSTS
6
Live hosts, risk score 0

THREAT INTELLIGENCE

LEAKED CREDENTIALS
26
Employee accounts on ext. services

BREACH DB RECORDS
2,038
Domain mentions (substring-matched)

CLOUD EXPOSURES
11
7 sensitive files

SHORTENED URLS
3,000
0 internal resources

SOCIAL MEDIA
192
1 impersonation risks

EMAIL EXPOSURE
498
14 critical, 61 high risk

CODE EXPOSURE
26
0 high risk on GitHub/ Gists

TG / DISCORD / PASTE
0
0 critical, 0 high risk

CRITICAL BUSINESS SYSTEMS
12
Internet-exposed critical functions

ATTACK PATHS
1
1 total pivot paths

INFRASTRUCTURE & APPLICATION SECURITY

ADMIN PANELS
0
Management interfaces exposed

TLS ISSUES
2
Cert / protocol / cipher

WEB APP SECURITY
74/100
3 high, 3 medium

TYPOSQUAT DOMAINS
372
0 phishing detected

AUTH ENDPOINTS
1
SSO, VPN, firewall panels

TOP RISKIEST ASSETS

The following systems represent the highest compound risk based on cross-module correlation. Each host was scored by combining individual risk factors — such as exposed admin panels, weak TLS, leaked credentials, and vulnerability signals — with business criticality multipliers. Systems where multiple risk factors overlap receive exponentially higher scores, as attackers can chain these weaknesses for maximum impact.

HOST	RISK	BUSINESS IMPACT	RISK FACTORS
asset-062.acmesample.com +1 alias on 192.0.2.178	10.0	Email System	13 high/crit CVEs, Flagged IP, Auth endpoint, 13 open ports
asset-166.acmesample.com	10.0	Website / Public-facing	37 high/crit CVEs, Flagged IP, Auth endpoint
asset-143.acmesample.com +1 alias on 192.0.2.27	10.0	Website / Public-facing — security weaknesses on authentication endpoint	32 high/crit CVEs, Weak TLS, Web app HIGH, Auth endpoint
www.acmesample.com +1 alias on 192.0.2.11	10.0	Website / Public-facing — security weaknesses on authentication endpoint	5 high/crit CVEs, Web app HIGH, Auth endpoint
asset-071.acmesample.com	8.8	Website / Public-facing	13 high/crit CVEs, Flagged IP, 13 open ports
asset-141.acmesample.com	7.5	API Infrastructure	2 high/crit CVEs, Sensitive subdomain
portal.acmesample.com	6.0	Customer Portal	Auth endpoint
asset-142.acmesample.com	5.0	API Infrastructure	2 high/crit CVEs
asset-064.acmesample.com	1.8	CRM / ERP	Auth endpoint, Sensitive subdomain
asset-055.acmesample.com	1.2	Internet-exposed system	Sensitive subdomain

TOP RISKIEST EMPLOYEES

High-value management-level personnel with the greatest exposure based on VIP intelligence (breach records, leaked passwords, account detections) and email enumeration data. These individuals represent priority targets for spear-phishing and credential-based attacks.

NAME	POSITION	RISK	BREACHES	PWD	RISK FACTORS
Executive012 Sample012	Vice President of Product Management	85	177	YES	177 breaches, Leaked passwords, MS recovery, Google ID found
Executive035 Sample035	Senior Director Strategic Accounts	80	79	YES	79 breaches, Leaked passwords, 1 online accounts, MS recovery
Executive020 Sample020	Senior Director, National Accounts	85	26	YES	26 breaches, Leaked passwords, 1 online accounts, MS recovery
Executive067 Sample067	Chief Financial Officer	85	10	YES	10 breaches, Leaked passwords, 4 online accounts, MS recovery
Executive040 Sample040	IT Technical Lead	80	11	YES	11 breaches, Leaked passwords, 5 online accounts, MS recovery
Executive041 Sample041	Chief Executive Officer	95	8	—	8 breaches, 5 web sources
Executive036 Sample036	Vice President of Distribution	80	8	—	8 breaches
Executive131 Sample131	Director of Human Resources	80	7	—	7 breaches

NAME	POSITION	RISK	BREACHES	PWD	RISK FACTORS
Executive005 Sample005	Chief Culture Officer	80	6	—	6 breaches
Executive078 Sample078	Product Marketing Manager	70	6	—	6 breaches, 4 web sources

TOP 10 PRIORITY ACTIONS

#	ACTION	TIMEFRAME	CATEGORY
1	**Review and patch 37 high/crit CVEs on asset-166.acmesample.com** Asset-166.acmesample.com has 37 high/critical CVEs that need immediate attention to secure the public-facing website. **Affected:** `asset-166.acmesample.com`	Immediate	VULNERABILITIES
2	**Review and patch 32 high/crit CVEs on asset-143.acmesample.com** Asset-143.acmesample.com is vulnerable with 32 high/critical CVEs. Immediate remediation is crucial for the website's authentication endpoint. **Affected:** `asset-143.acmesample.com`	Immediate	VULNERABILITIES
3	**Review and patch 5 high/crit CVEs on www.acmesample.com** The authentication endpoint on www.acmesample.com has 5 high/critical CVEs that require immediate remediation to protect user data. **Affected:** `www.acmesample.com`	Immediate	VULNERABILITIES
4	**Restrict admin-panel exposure on asset-062.acmesample.com** Asset-062.acmesample.com is flagged as an auth endpoint with high risk due to 13 open ports. Immediate restriction is necessary. **Affected:** `asset-062.acmesample.com`	This week	NETWORK
5	**Restrict access to auth endpoints on asset-071.acmesample.com** Asset-071.acmesample.com has 13 open ports and should have its auth endpoint access restricted to mitigate risks. **Affected:** `asset-071.acmesample.com`	This week	NETWORK
6	**Implement DMARC reject policy on acmesample.com** To enhance email security, implement a DMARC reject policy on the root domain acmesample.com to prevent spoofing.	Within 30 days	BRAND PROTECTION
7	**Review 26 credential leaks associated with acmesample.com** 26 employee mailboxes under acmesample.com were found in third-party breach datasets. Conduct a review for credential hygiene.	Within 30 days	CREDENTIALS
8	**Audit 372 typosquatting domains related to acmesample.com** There are 372 typosquatting domains that could pose a risk to brand integrity. An audit is necessary to mitigate potential phishing.	Within 30 days	BRAND PROTECTION
9	**Review and secure 7 cloud sensitive files** There are 7 sensitive files in the cloud that require review and security enhancements to prevent unauthorized access.	Within 90 days	INFRASTRUCTURE
10	**Conduct security assessment for 3 internet-exposed hosts** Three hosts are exposed to the internet and require a comprehensive security assessment to identify and mitigate risks.	Within 90 days	INFRASTRUCTURE

Scan Methodology & Coverage

DarknetSearch Attack Surface Enumeration uses an **8-phase automated pipeline** to map an organization's external digital footprint. Starting with the target domain, the system progressively discovers, enriches, and analyzes every externally-reachable asset — mirroring the same reconnaissance techniques used by real-world attackers.

1
Target analysis
Resolve IP, WHOIS/RDAP baseline.

2
Subdomain discovery
Up to 16 passive OSINT modules.

3
Infrastructure map
RIR ranges, same-IP, reverse WHOIS.

4
Passive intelligence
Shodan, Netlas, ZoomEye.

5 OPT-IN
Active scanning
Nmap on discovered ports.

6
Analysis & correlation
Risk scores, neighbours, CVEs.

7 OPT-IN
Active verification
Safe HTTP/SSL template scanning.

8
Report generation
Analysis, charts, PDF rendering.

Phase 1 — Target Analysis

The pipeline begins by resolving the target domain's primary IP address and querying WHOIS/RDAP registration databases to identify the domain owner, registrar, and registration history. This establishes the baseline identity for subsequent lookups.

Phase 2 — Subdomain Discovery

Up to 16 passive OSINT modules run in parallel — querying certificate transparency logs (crt.sh, Kaduu CT Monitor), search engine indexes (Shodan, ZoomEye, Google via SERPHouse/ScrapingBee), passive DNS databases (RapidDNS, DNSDumpster, SubdomainCenter, HackerTarget), web archive history (Wayback Machine), darknet credential leaks (Kaduu), headless browser scraping (Netcraft), and the target website itself via a concurrent BFS web crawler. When active DNS enumeration is enabled, a DNS brute-force module tests 5,000 common subdomain prefixes.

Phase 3 — Infrastructure Mapping

Four reverse IP lookup sources identify domains sharing the target's IP. RIR REST APIs (RIPE, ARIN) discover all IP ranges registered to the target organization. A GPT-enhanced pipeline identifies the company, generates normalized search names, and adjudicates which RIR registrations belong to the target. Reverse WHOIS lookups find all domains registered by the same entity.

Phase 4 — Passive Intelligence

For each discovered host, the system queries Shodan, Netlas, and ZoomEye for open ports, service banners, SSL certificates, CPE identifiers, and known vulnerabilities — without touching the target's infrastructure. Results are cached for 7 days per IP to optimize API usage.

Phase 5 — Active Scanning (opt-in)

When enabled, Nmap performs targeted TCP scanning with version detection (-sV) and NSE scripts (vulners for CVE lookup, ssl-enum-ciphers for TLS audit) on passively-discovered ports. If no ports are known, a fast scan of the top 100 TCP ports runs instead.

Phase 6 — Analysis & Correlation

Network neighbourhood analysis examines adjacent IPs for SSL certificate matches, PTR patterns, ASN comparison, and HTTP fingerprinting. CVEs are aggregated from 5 sources and cross-verified against Nmap service banners. Risk scores (0–10) are calculated per host based on vulnerabilities, unusual ports, and sensitive hostname patterns.

Phase 7 — Active Security Verification (opt-in)

When enabled, an automated security verification engine scans all discovered hosts with live HTTP/HTTPS endpoints using **4,000+ curated safe detection templates**. These templates use only GET/HEAD requests (no exploitation or payload injection) to detect exposed admin panels, security misconfigurations, sensitive file exposures, outdated software, and known CVE indicators. Additionally, SSL/TLS, DNS, and network-level checks run against all hosts with classified ports. Only hosts with open ports are tested; the engine first probes each URL for liveness before scanning.

Phase 8 — Report Generation

All scan results are deduplicated and consolidated. Enrichment counters are materialized, wildcard DNS entries detected, and risk scores finalized. The report generation pipeline then collects all data from the database, runs deterministic analysis (risk distribution, port/service frequency, technology stack, CVE landscape, network ownership), generates charts via matplotlib, obtains a GPT-powered executive summary, geolocates all resolved IPs, and renders the final PDF using WeasyPrint. Detailed CSV evidence is omitted from this public sample.

Module Summary

56 modules completed, **0** failed, **5** skipped. Full per-module breakdown available in `private evidence dataset` omitted from this public sample.

Modules not completed

The following modules failed or were skipped. Their findings may be absent from this report; a zero count must not be interpreted as a clean result.

MODULE	STATUS	DIAGNOSTIC
ip_range_discovery	Skipped	domain_mode=default (scoped) — additional-domain discovery off
reverse_dns	Skipped	Disabled by feature flag
reverse_whois	Skipped	domain_mode=default (scoped) — additional-domain discovery off
same_ip_domains	Skipped	domain_mode=default (scoped) — additional-domain discovery off
hackertarget_same_ns	Skipped	domain_mode=default (scoped) — same-NS apex discovery off

Attack Surface Overview

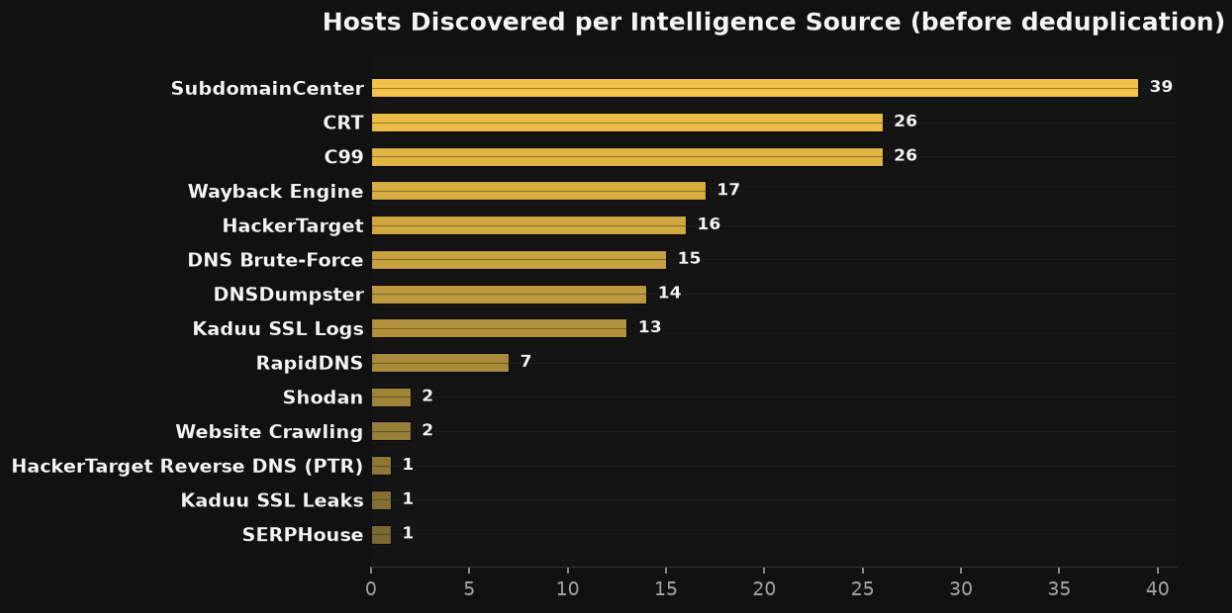
The attack surface represents all externally-reachable hosts, services, and digital assets associated with **acmesample.com**. Hosts were discovered through passive intelligence sources (certificate transparency, DNS databases, search engines, leaked credentials) and optionally confirmed through active scanning (Nmap, active verification).

Sensitive Host Names are hostnames containing patterns that suggest high-value or internal systems — such as admin, dev, staging, vpn, jenkins, grafana, or backup. These systems are often the first targets in real-world attacks. **Unusual Ports** are open TCP/UDP ports outside the standard set of common internet services (HTTP, HTTPS, SSH, DNS, SMTP, FTP). Their presence may indicate development servers, management interfaces, legacy applications, or misconfigured services.

54	54	9	5
SUBDOMAINS FOUND	CLIENT OWNED	SENSITIVE HOST NAMES	UNUSUAL PORTS

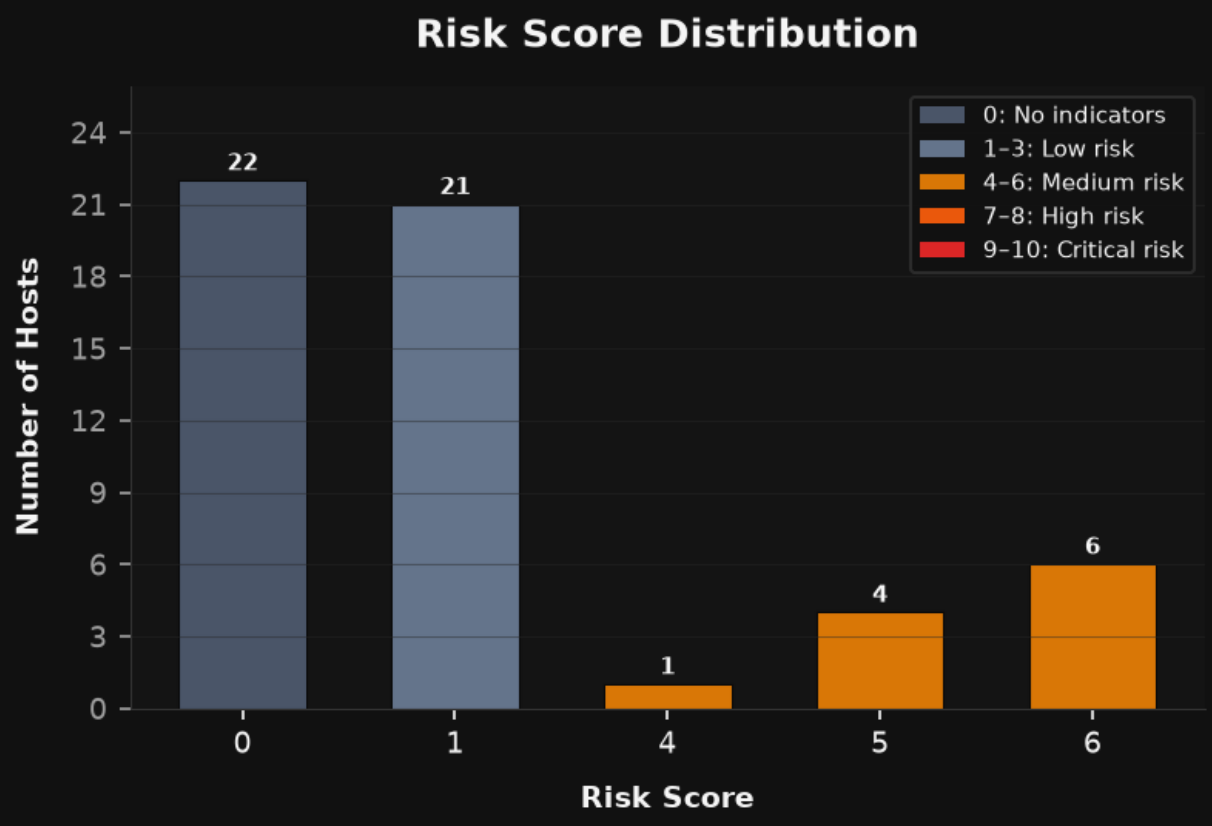
Discovery sources (before deduplication)

Bars use a **single gold ramp** by rank — easier to read than many unrelated colors. Each bar counts hosts contributed by that source (hosts may appear in multiple sources).



Risk score distribution

Scores 0–10 from CVE signals, unusual ports, port count, and sensitive hostname patterns. Chart legend matches bar colors.



NETWORK

Organisation Owned IP Ranges

IP range discovery identifies all network blocks registered to the target organization through Regional Internet Registries (RIPE for Europe/Middle East, ARIN for North America). A GPT-enhanced pipeline identifies the company behind the domain, generates search name variants (including ASCII-folded and legal-suffix-stripped forms), and validates which RIR registrations belong to the target. Large ranges (>/24, 256+ hosts) are listed as informational only.

Important: This analysis identifies which network blocks belong to the organization based on RIR registration data. **No hosts within these ranges were actively scanned, enumerated, or probed.** The ranges provide context about the organization's registered IP estate — any security assessment of individual hosts within these ranges would require a separate targeted scan.

No Registered IP Ranges Found

The RIR lookup (RIPE, ARIN) did not identify any IP ranges directly registered to this organization. This typically means the organization uses cloud-hosted or shared infrastructure (e.g. AWS, Azure, Cloudflare) rather than owning dedicated IP blocks. This is common for small-to-medium organizations and does not indicate a security issue — however, it means there is no additional IP estate to audit beyond the hosts discovered through subdomain enumeration.

Network Neighbour Analysis

For each discovered IP, the system examines neighbouring addresses in the same /24 subnet. Neighbours are evaluated through SSL certificate matching (CN/SAN comparison), PTR record patterns, ASN comparison, and HTTP content fingerprinting. Each neighbour receives a confidence score: **CONFIRMED** (IP falls within a registered client IP range), **HIGH** (2+ strong signals such as certificate or ASN match), **MEDIUM** (1 strong signal), **LOW** (weak signals only).

Important: Neighbouring IP addresses were only fingerprinted using passive techniques (certificate inspection, PTR lookup, HTTP headers). **No active scanning, penetration testing, or vulnerability assessment was performed on any neighbour IP.**

Analysed **20** IP neighbourhoods — **8** SSL certificate matches, **2** HTTP fingerprint matches, **0** RDAP-confirmed owned. Complete neighbour evidence is omitted from this public sample.

Sample Findings

TARGET IP	NEIGHBOUR IP	CONFIDENCE	MATCHING SIGNALS
192.0.2.182	192.0.2.183	MEDIUM	Ptr Match, Same Subnet
192.0.2.184	192.0.2.183	MEDIUM	Ptr Match, Same Subnet

Why Neighbouring IPs Matter

If the analysis above identified neighbouring IP addresses with **medium** or **high** confidence of belonging to your organization, these hosts were not included in the active scan scope and have not been tested for vulnerabilities. However, an attacker performing reconnaissance would also discover these neighbours and may investigate or attack them to gain a foothold into your network. We recommend verifying ownership of high-confidence neighbours and including them in future security assessments.

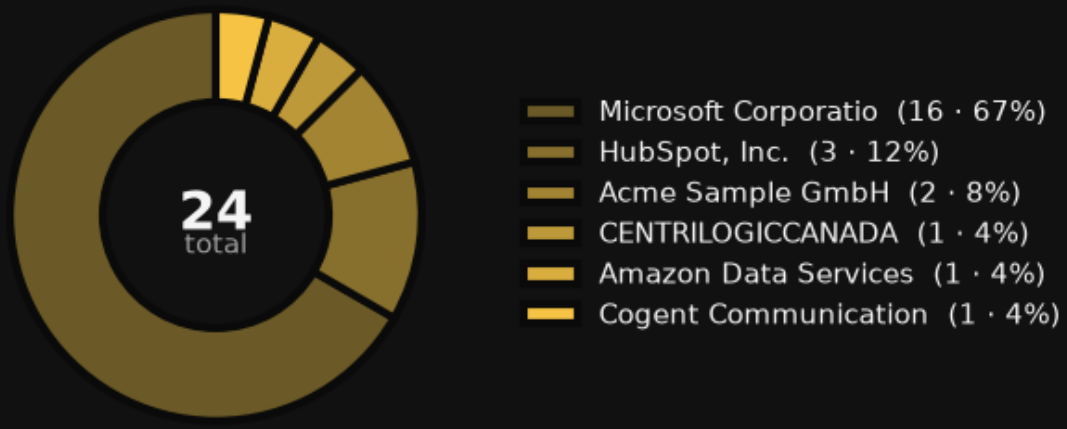
Hosting Providers & Distribution

Hosting provider distribution reveals the infrastructure diversity of the organization's attack surface. A concentrated hosting footprint (few providers) simplifies security monitoring but creates single points of failure. A highly distributed footprint increases management complexity and the risk of configuration drift across providers.

Assessment: 6 providers — moderate management complexity.

Distribution

Hosting Provider Distribution



Top providers

Microsoft Corporation	16
HubSpot, Inc.	3
Acme Sample GmbH	2
CENTRILOGICCANADA	1
Amazon Data Services Canada	1
Cogent Communications, LLC	1

Risk Assessment

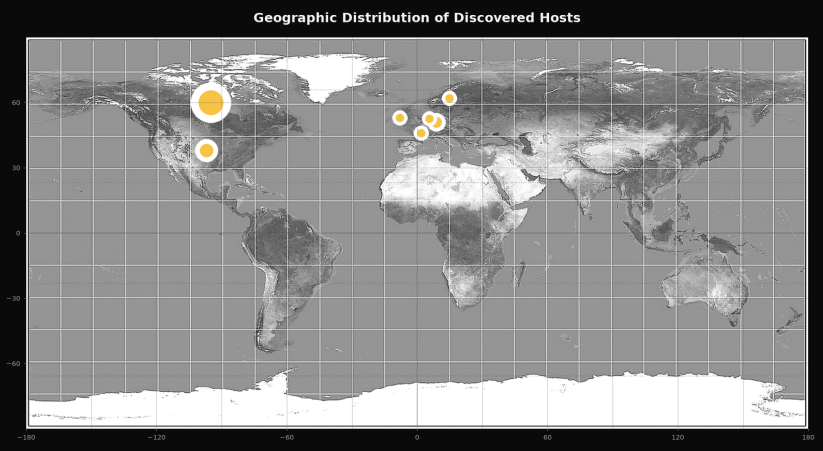
The organization relies heavily on third-party hosting, with 66.7% of its infrastructure provided by Microsoft Corporation, indicating a significant concentration risk. As the dominant provider is external and accounts for more than 70% of the hosted services, this poses a vulnerability where a regional outage could disrupt all operations. The resilience verdict is concerning due to this high dependency on a single provider. To mitigate this risk, the organization should implement a multi-provider strategy to enhance redundancy and ensure service continuity in the event of an outage.

PROVIDER	HOSTS
Microsoft Corporation	16
HubSpot, Inc.	3
Acme Sample GmbH	2
CENTRILOGICCANADA	1
Amazon Data Services Canada	1
Cogent Communications, LLC	1

Geographic Distribution

IP geolocation shows where discovered hosts are allocated (typically city/region accuracy). A wide spread may indicate CDN, multi-region cloud, or unexpected jurisdictions.

Note: Map uses an **equirectangular** projection (WGS-84). Bubble **position** is each country's standard map centroid (ISO); **size** reflects host count from geolocation. The legend lists every country with hosts.



CA	Canada	12
US	United States	3
DE	Germany	2
IE	Ireland	1
SE	Sweden	1
FR	France	1
NL	Netherlands	1

Bubble position = ISO country centroid (plate carrée); bubble size ∝ hosts geolocated to that country. Country codes match the legend. Base map: equirectangular projection (Wikimedia Commons, CC BY-SA).

PEOPLE

Leaked Credential Exposure

70
FAIR

Analysis of corporate credential exposure across breach databases and stealer log aggregators. Identifies employee accounts compromised on external services.

Validity of Breached Credential Data

Threat actors often recycle older data in so-called "combo lists," and breach data can sometimes be months or even years behind the original incident. Based on our experience, fewer than ~2% of the leaked credentials we index remain valid. That said, even a very small number of working credentials can still present a real risk. Preventing a breach may come down to just one compromised account out of hundreds.
It is also important to differentiate between data sources: the database search used in this report focuses on breached data that has already been shared publicly (often for free), whereas threat actors typically attempt to sell fresh data first. This more recent, higher-value data is usually found via live hacker forum searches (not part of this report).
Beyond credential validity, historical data still provides meaningful security insights. For example, it helps identify password reuse patterns across services — a key enabler of credential stuffing attacks — or cases where corporate email accounts are used on private platforms. These types of findings are particularly useful for targeted awareness training and strengthening internal security practices.

Multi-Domain Credential Search

The organisation uses multiple email domains. Credentials were searched across all identified domains:

DOMAIN	EMPLOYEE LEAKS	BREACH DB RECORDS	UNIQUE EMAILS
@acmesample.com	26	2,036	15
@acmesample.net	0	2	0

Summary

Searched website domain (acmesample.com) and email domain(s) (acmesample.net). @acmesample.com: 26 employee leaks, 2,036 breach DB records. @acmesample.net: 0 employee leaks, 2 breach DB records. 2,038 leaked account records found in breach databases. 26 employee credential exposures detected across 15 unique email addresses. 17 are rated high or critical risk (plaintext passwords present on external services).

26	388	2,038	17
EMPLOYEE CRED RECORDS	**BREACH-DERIVED MAILBOXES**	**BREACH DB RECORDS**	**HIGH/CRITICAL RISK**
login + password pairs	canonical breach union	domain mentions	cred records

Understanding the Numbers

Employee Cred Records counts distinct credential rows (login + password / hash pairs) after identical sightings from multiple leak sources are collapsed. **Breach-Derived Mailboxes** deduplicates breach evidence into distinct addresses and unions in any additional `@acmesample.com` mailboxes seen across the live breach DB (scanned in full), breach content samples, and Hunter.io public sources. Source breakdown (BEFORE deduplication): 15 from credentials, 383 from live breach search, 384 from breach content samples, 0 from Hunter.io. **Breach DB Records** counts every breach document (log files, database dumps, paste content) that mentions the domain in any field — a far broader measure that frequently exceeds the cred-record count by orders of magnitude because one leaked file can contain thousands of lines mentioning the domain.

How "17 critical findings" relates to the 388 breach-derived mailboxes: the High/Critical Risk count is the number of credential records rated critical by the source and risk model — typically recent stealer-log or plaintext-present evidence. Password validity was not tested. The same mailbox can have more than one distinct critical credential record, so this record count can exceed the mailbox count.

***Note on breach evidence:** These figures reflect historical breach databases and stealer-log aggregators. Identical sightings are deduplicated, but different credentials for one mailbox remain separate. Presence in a feed does not establish that an account or password is currently valid.

Raw vs. Deduplicated Records

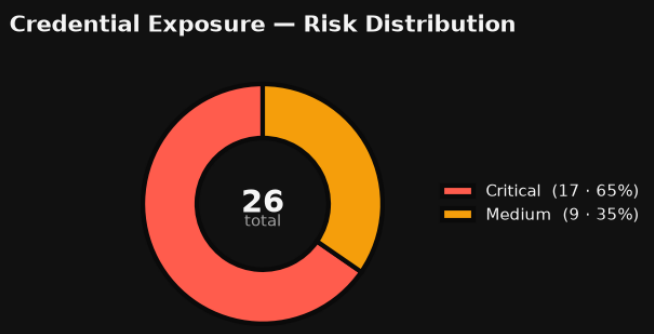
Across all in-scope domain searches the breach feeds returned **129** raw credential records. After deduplicating the same leaked mailbox/password pair re-surfaced by overlapping domain searches and multiple combo-lists, this reduces to **26** distinct records (103 duplicate records removed). The headline and score use the deduplicated figure; the raw subtotal is shown here for reconciliation against upstream feed counts. These records span **75** distinct leak sources.

Exposure Window (record age)

Breach data is historical — a record's presence does not mean the password is still valid. The distribution below buckets each dated record by how long ago it was first seen, so the report shows an exposure window rather than implying every leak is current:

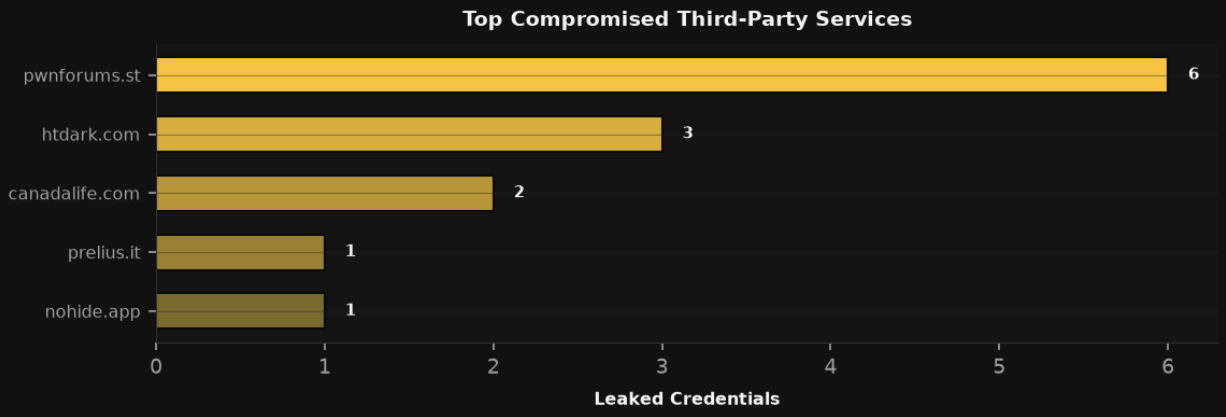
FIRST-SEEN AGE	RECORDS
Last 90 days	8
90 days – 1 year	18

This chart shows **distinct credential records** from the breach content search API — each record represents a distinct email + case-sensitive redacted-password + server combination. The feed returned 129 raw sightings; 103 duplicate sightings across leak sources were removed before charting.



Top Compromised Third-Party Services

These are **third-party** platforms (not owned by the organisation) where employee credentials were found in breach databases and stealer logs. This does not mean these platforms were compromised — rather, employees used their corporate email to register on these services, and those credentials were subsequently exposed in third-party data breaches. Login endpoints belonging to the organisation's own domains are listed separately below.



Credential Exposure Details (Redacted)

Showing 20 of 26 records (balanced — max 3 rows per email address so the table surfaces distinct affected users rather than repeating one heavily-breached mailbox). Complete data in `private evidence dataset` omitted from this public sample.

EMAIL	DOMAIN	SERVICE	PASSWORD	RISK	FIRST SEEN
employee125@acm...	acmesample.com	pwnforums.st	S***e (sample)	7.0	2026-08-18
employee155@acm...	acmesample.c	htdark.com	S***e (sample)	7.0	2026-01-06
employee044@acm...	acmesample.com	pwnforums.st	S***e (sample)	7.0	2026-08-18
employee088@acm...	acmesample.c	nohide.app	S***e (sample)	7.0	2026-07-31
employee058@acm...	acmesample.com		S***e (sample)	7.0	S***e (sam
employee136@acm...	acmesample.c	pwnforums.st	S***e (sample)	7.0	2026-08-18
employee498@acm...	acmesample.com	pwnforums.st	S***e (sample)	7.0	2026-08-18
employee192@acm...	acmesample.c	pwnforums.st	S***e (sample)	7.0	2026-08-18
employee158@acm...	acmesample.com	canadalife.com	S***e (sample)	4.0	2026-04-29
employee076@acm...	acmesample.c	canadalife.com	S***e (sample)	4.0	2026-04-29
employee024@acm...	acmesample.com		S***e (sample)	4.0	2026-04-15
employee264@acm...	acmesample.c		S***e (sample)	4.0	2025-12-27
employee341@acm...	acmesample.com		S***e (sample)	4.0	2026-01-05
employee395@acm...	acmesample.c		S***e (sample)	4.0	2026-01-05
employee374@acm...	acmesample.com		S***e (sample)	7.0	2025-12-25
employee125@acm...	acmesample.c	pwnforums.st		7.0	2026-08-18

EMAIL	DOMAIN	SERVICE	PASSWORD	RISK	FIRST SEEN
			S***e (sample)		
employee155@acm...	acmesample.com	htdark.com	S***e (sample)	7.0	2026-01-06
employee044@acm...	acmesample.c		S***e (sample)	7.0	2026-01-19
employee088@acm...	acmesample.com		S***e (sample)	4.0	2026-04-15
employee058@acm...	acmesample.c		S***e (sample)	4.0	2025-12-27

Breaches Overview

The website domain you submitted is **acmesample.com**, but the organisation's MX records resolve to a different registered apex used for employee email. The table below compares the **breach-database footprint** of each: the website apex covers everything indexed against the public-facing brand, while the email apex covers credential leaks tied to actual employee mailboxes — frequently a much larger footprint and the higher-priority cleanup target.

The alternate email apex was looked up in the leak.center breach database only — its subdomain inventory, port surface, vulnerabilities and so on were NOT enumerated by this scan. To run a full attack-surface analysis on the email apex, re-submit it as the primary target or select `domain_mode=all` on the next scan.

Source: leak.center distinct-leak API. Counts are aggregated resultCount values across all leaks where the domain appears in the indexed content. Substring matching by the upstream API can inflate counts when the domain registered name is a substring of another organisation's domain (e.g. `gilgen.ch` also matches `keller-gilgen.ch`) — values should be read as relative indicators of exposure pressure rather than exact unique-record totals.

2	284	2,038
DOMAINS SEARCHED	TOTAL DISTINCT LEAKS	TOTAL BREACH RECORDS

DOMAIN	DISTINCT LEAKS	TOTAL RECORDS	STEALER LOGS	COMBOLISTS	WEBSITE BREACHES	DB DUMPS	TOP TAGS / DATE RANGE
acmesample.com TARGET	282	2,036	33	55	48	17	account (222), email (215), password (159), username (122), url (79) 2008-07-01 → 2026-08-15
acmesample.net EMAIL APEX	2	2	—	—	2	—	ip (2), name (2), email (2), phone (2), dob (1) 2019-03-07 → 2020-01-01

How to Read This Chapter

Stealer logs indicate that infostealer malware compromised endpoints (employee or third-party) and exfiltrated saved-credential stores referencing this domain. **Combolists** are aggregated email/password recyclings — most pairs are credential-stuffed against this domain even if not directly breached. **Website breaches** mean the domain itself (or a closely related service) was compromised. **Database dumps** are full SQL/CSV exports leaked to the public.

Each subsequent chapter (Breach Content Risk Assessment, Known Breaches Involving This Organisation, Breach Data Intelligence) drills into the **target domain only** — the per-domain figures here are the only place where every analysed domain is compared side-by-side.

Breach Content Risk Assessment

Darknet Threat Intelligence Analysis

The organization has been identified in **282** distinct leak sources, with a total of **2036** records found mentioning the domain acmesample.com. The date range of exposure spans from **July 1, 2008** to **August 15, 2026**. This level of exposure is considered elevated for an organization of this type, indicating significant risks to its data integrity and security posture.

The main leak categories include stealer logs, which indicate malware on employee or customer devices that harvest sensitive information in real-time; combolists, which are collections of username and password pairs used for credential stuffing attacks; and website/database breaches, which represent direct compromises of specific services.

Key risks for the organization include credential stuffing attacks using the **159** password records found, session hijacking through stolen cookies from the **33** stealer logs, and potential phishing attacks leveraging the **215** email addresses exposed.

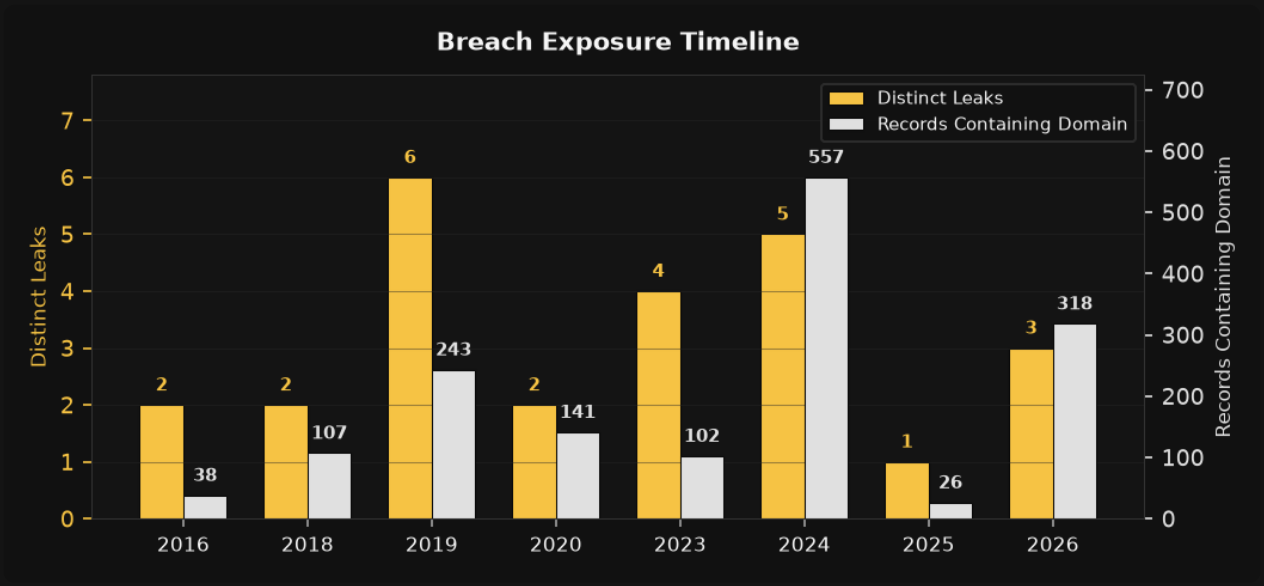
Given that stealer logs have been identified as recent as **August 15, 2026**, the organization must act urgently to reset passwords and enforce multi-factor authentication, as these credentials may still be active and pose an immediate threat.

Breach Content Risk Assessment

The organization faces significant exposure due to the discovery of **384** unique email addresses belonging to its domain. This represents a direct risk to the organization, as these email addresses can be leveraged for various malicious activities. Additionally, the breach data includes sensitive information such as **376** phone numbers, **48** IP addresses, and **315** URLs, which may provide insights into the organization’s internal infrastructure and operational details.

The attack risks stemming from this exposure are multifaceted. The presence of the organization's email addresses opens the door to credential stuffing attacks, where attackers may attempt to gain unauthorized access using previously leaked credentials. Furthermore, the availability of phone numbers increases the risk of spear-phishing and social engineering attacks, as attackers can impersonate trusted contacts to extract sensitive information. The **48** IP addresses found

could assist attackers in mapping the organization’s internal network, potentially leading to more sophisticated attacks. It is important to note that the breach data does not contain stealer logs or database dumps; rather, it appears to consist primarily of combolists, which further emphasizes the need for heightened vigilance in monitoring for suspicious activities related to the exposed email addresses and associated data.



Breach Trend Analysis

The analysis of breach timeline data reveals a fluctuating trend in the frequency of distinct data leaks associated with the organization. Over the years, the number of leaks varied, with a notable spike in 2019, where six distinct leaks were recorded. The volume of records, however, presents a more concerning picture, particularly in 2025, which saw an alarming peak of 557 records. This spike suggests a significant incident, likely a large-scale database breach, as opposed to numerous smaller leaks, indicating a potential vulnerability in the organization's data security posture. The total of 1,532 records across 25 leaks highlights a persistent risk that the organization must address.

From a risk perspective, the presence of stealer logs among the leak types indicates that recent and active malware threats are targeting the organization, which could lead to further data compromise. The exposure dates range from 2008 to the latest breach in August 2026, suggesting that while some leaks may be historical, the organization is still facing fresh threats. Given the current trend, it is imperative for the organization to prioritize enhancing its cybersecurity measures, particularly focusing on monitoring and mitigating threats from stealer logs, while also conducting thorough assessments of its data handling and storage practices to prevent future breaches.

Known Breaches Involving This Organisation

25 distinct leak sources containing 1,532 records mentioning the domain.

DATE	LEAK NAME	RECORDS	DATA TYPES
2026-08-09	zoominfo.com darkforums.ru 081220…	**155**	private, address, business, phone, name, email, url
2026-04-22	Pitney Bowes Inc. (pb.com)_shinyhun…	**46**	private, address, business, phone, identity, name, email, username
2026-02-16	CORPS Combolist_breachforums.as 1…	**117**	password, mix, email, username
2025-03-13	owcareers.com	**26**	password, private, address, dob, csv, name, email, hash, url, account, username
2024-09-23	xiqonline.com	**38**	private, address, business, name, email
2024-09-19	Unique emails by Addka72424 and Br…	**19**	email
2024-09-12	pureb2b.co.uk	**128**	password, private, address, business, phone, csv, ip, name, company, email, hash, account
2024-08-15	demandscience CSV 15 Aug 2024	**342**	password, address, business, phone, ip, name, email, account
2024-04-07	epa.gov	**30**	private, address, phone, csv, name, company, email
2023-06-11	Collection stealer logs and combolists…	**14**	password, private, business, email, hash, account
2023-05-29	"CORP APB" corporate credentials lea…	**18**	password, email, account
2023-03-18	Linkedin_darkforumns.su 18 February…	**38**	private, business, phone, identity, csv, name, url, username
2023-02-18	LinkedIn 18 February 2023	**32**	private, address, business, phone, csv, name, company, url, username
2020-12-14	Breach Compilation	**16**	account
2020-01-01	linkedin.com	**125**	password, private, business, name, email

Showing 15 most recent of 25 distinct leak sources. Full data available in `private evidence dataset`.

Breach Data Intelligence

Analysis of **2,036** sample breach records (out of **2,038** total — Elasticsearch limits per-query exports to 2,036) reveals the following exposed data types beyond credentials:

388 EMPLOYEE EMAILS	**376** PHONE NUMBERS	**661** LINKEDIN PROFILES	**284** PERSONAL NAMES
358 PHYSICAL ADDRESSES	**349** JOB TITLES	**315** URLS	**48** IP ADDRESSES

Why This Matters

Breach data containing personal names, physical addresses, phone numbers, and job titles enables highly targeted spear-phishing and social engineering attacks. Attackers can craft convincing pretexts using real employee details, significantly increasing the success rate of business email compromise (BEC) campaigns.

Raw Breach Evidence Samples

Excerpts from actual breach records where the organization's domain was found. Domain matches are highlighted.

BREACH RECORD
`[Anonymized breach record] acmesample.com [credential value removed from public sample]`

BREACH RECORD
`[Anonymized breach record] acmesample.com [credential value removed from public sample]`

BREACH RECORD
`[Anonymized breach record] acmesample.com [credential value removed from public sample]`

BREACH RECORD
`[Anonymized breach record] acmesample.com [credential value removed from public sample]`

BREACH RECORD
`[Anonymized breach record] acmesample.com [credential value removed from public sample]`

Email Enumeration & Exposure Analysis

Mailboxes belonging to `acmesample.com` discovered across four independent sources: data-breach databases, Hunter.io public-internet enumeration, RocketReach professional contact data (corporate addresses only), and the Central API `unique_domain_emails` registry. The **Identified Mailboxes** headline below is this chapter's broader deduplicated discovery union. Breach-focused chapters use their separately labelled canonical breach-derived mailbox population.

100
IDENTIFIED EMPLOYEES
VIA ROCKETREACH / APOLLO

498
IDENTIFIED MAILBOXES
DEDUPLICATED UNION

390
WITH BREACH EXPOSURE

75
HIGH / CRITICAL RISK

Source Breakdown

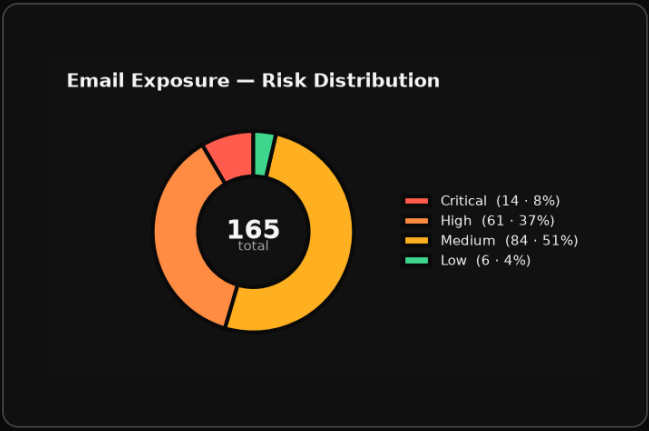
Each source is queried independently; the same mailbox can be discovered by more than one channel. The sum of the per-source rows is therefore typically larger than the deduplicated **498**-mailbox total.

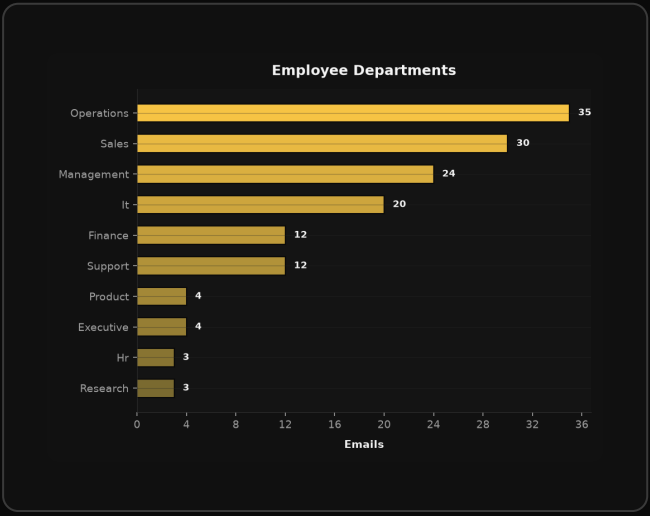
SOURCE	MAIL-BOXES	NOTES
Breach databases	390	Per-leak iteration of leak.center across the top 100 most data-rich leaks containing `@acmesample.com` (and any alternate email domains). Detail: `private evidence dataset`.
Hunter.io	165	Public-internet email discovery (Hunter `/v2/domain-search`). Detail: `private evidence dataset`.
RocketReach	15	Corporate-domain emails resolved via deep `/person/lookup` harvest over RocketReach's employee directory. Detail: `private evidence dataset`.
Central API registry	0	`unique_domain_emails` — a curated upstream registry. Often empty for very short domains (e.g. `tp.com`).
TOTAL (deduplicated)	**498**	Broader discovery union used by Email Enumeration (breach data, Hunter.io, RocketReach, and the Central API registry). Breach-focused chapters separately use the canonical breach-derived mailbox population. See `private evidence dataset` for the full audit trail.

How this relates to other chapters

We identified **100** people associated with `acmesample.com` via RocketReach professional-network data (titles, employer, location). RocketReach's `/person/search` endpoint returns metadata only — actually retrieving an email address requires a separate `/person/lookup` call per profile. The People Intelligence chapter additionally looks up the top 15 highest-value targets (executives) for the VIP Intelligence chapter; their corporate addresses contribute to the RocketReach row in the Source Breakdown. The **498** "Identified Mailboxes" headline is the broader discovery union for this chapter: addresses observed in breach data, Hunter.io, RocketReach lookups, or the Central API registry. Credential Exposure uses the narrower canonical breach-derived mailbox population, so the two totals are intentionally not interchangeable.

Of the **498** identified mailboxes, **390** were observed in at least one known data breach. Across those, we counted approximately **26** credential-leak records (login + password / hash pairs). The wider `acmesample.com` domain is mentioned across **2,038** breach records (any field — emails, URLs, hashes, attachments) spanning **282** distinct breach databases.





Dual Exposure

62 email addresses appear in both breach databases AND public internet sources. These individuals face the highest risk — attackers can combine leaked credentials with publicly available personal details (position, LinkedIn profile) for highly targeted spear-phishing and business email compromise (BEC) attacks.

Summary

498 unique employee emails discovered for acmesample.com. 390 appear in data breach databases. 165 are publicly visible on the internet. 62 emails found in both breaches and public sources represent the highest exposure.

Top 3 Most Exposed Employees

Selected based on organisational seniority (management, director, head-of roles) combined with public online visibility (number of websites where the email address was found via OSINT)

These individuals were selected because their senior role makes them attractive targets for business email compromise (BEC) and social engineering, while their high online visibility makes them easy to research and impersonate. The breach/data/access scores below reflect additional exposure from data breaches.

CRITICAL Vice President of Product Management with leaked password and device compromise

employee058@acmesample.com · Vice President of Product Management (product)

ONLINE PRESENCE	ORG. ROLE	BREACH EXPOSURE	DATA EXPOSURE	CRITICAL ACCESS
3 public websites	Executive — Vice President of Product Management (product)	5/5 — 43 breaches · stealer log · password leaked	1/5 — password	1/5 — no critical services

Breach / Data / Access gauges computed deterministically from the reconciled breach evidence (record count, leaked password/stealer presence, distinct PII categories, and credential-service criticality).

Executive012 Sample012's email has appeared in 43 data breaches, with both a leaked password and evidence of device compromise through stealer logs. This makes him a prime target for credential stuffing attacks, potentially leading to account takeover. With his executive position, he is also at risk for Business Email Compromise (BEC) schemes, especially given that his email is publicly findable on 3 websites.

CRITICAL Senior Director, National Accounts with leaked password

employee074@acmesample.com · Senior Director, National Accounts (finance)

ONLINE PRESENCE	ORG. ROLE	BREACH EXPOSURE	DATA EXPOSURE	CRITICAL ACCESS
7 public websites	Executive — Senior Director, National Accounts (finance)	5/5 — 21 breaches · password leaked	3/5 — password, phone, address	1/5 — no critical services

Breach / Data / Access gauges computed deterministically from the reconciled breach evidence (record count, leaked password/stealer presence, distinct PII categories, and credential-service criticality).

Executive020 Sample020 has been exposed in 21 breaches, with a leaked password that could facilitate credential stuffing attacks. Additionally, his personal phone and address information are compromised, making him vulnerable to targeted social engineering attacks. As a senior director, he is a valuable target for attackers seeking to exploit his access, and his email is findable on 7 public websites.

CRITICAL **Chief Executive Officer with personal data exposure**

employee158@acmesample.com · Chief Executive Officer (executive)

ONLINE PRESENCE	ORG. ROLE	BREACH EXPOSURE	DATA EXPOSURE	CRITICAL ACCESS
5 public websites	**Executive** Chief Executive Officer (executive)	**4**/5 8 breaches	**3**/5 phone, address	**1**/5 no critical services

Breach / Data / Access gauges computed deterministically from the reconciled breach evidence (record count, leaked password/stealer presence, distinct PII categories, and credential-service criticality).

Executive041 Sample041's email has appeared in 8 breaches, but notably lacks a leaked password. However, his personal phone and address are exposed, making him susceptible to targeted social engineering attacks. As the CEO, he is a high-value target for attackers aiming for BEC, and his email is findable on 5 public websites, increasing the risk of tailored phishing attempts.

High-Value Targets

AI-prioritised from 100 employees discovered via OSINT (RocketReach / Apollo). GPT-4o evaluates role authority, system access potential, and targeting value to rank the highest-risk individuals.

100
EMPLOYEES DISCOVERED

10
HIGH-VALUE TARGETS

Out of **100** employees identified via OSINT, the following **10** individuals represent the highest-value targets for business email compromise (BEC), social engineering, and targeted phishing campaigns — selected based on organisational authority, system access privileges, and public visibility. The complete employee list with all 100 records is available in `private evidence dataset`.

E

MEDIUM **Executive144 Sample144**

Director, Quality, Inspections and Returns · 100 Market Street, Sample City

CORPORATE ✉ employee532@acmesample.com [A]

LinkedIn

As a Director overseeing quality and inspections, this individual may have access to sensitive operational data and quality assurance processes, making them a target for gaining insights into company vulnerabilities.

E

HIGH **Executive052 Sample052**

Executive Vice President, Operations · 100 Market Street, Sample City

CORPORATE ✉ employee250@acmesample.com [A]

LinkedIn

In the role of Executive Vice President of Operations, this individual holds significant decision-making authority and access to critical operational systems, presenting a valuable target for attackers seeking to disrupt business functions.

E

HIGH **Executive156 Sample156**

Senior Manager - Finance Services and Treasury · 100 Market Street, Sample City

CORPORATE ✉ employee565@acmesample.com [A]

LinkedIn

This individual manages finance services and treasury operations, granting them access to sensitive financial data and potential authority over financial transactions, making them a prime target for financial fraud.

E

HIGH **Executive035 Sample035**

Senior Director Strategic Accounts · 100 Market Street, Sample City

CORPORATE ✉ employee148@acmesample.com [A]

PERSONAL ✉ employee480@examplemail.com (consumer mail provider — not a target-domain leak)

LinkedIn Twitter

As a Senior Director managing strategic accounts, this person likely has access to key client information and contracts, making them a target for social engineering attacks aimed at compromising client relationships.

E

HIGH **Executive126 Sample126**

Director, Engineering · 100 Market Street, Sample City

CORPORATE ✉ employee484@acmesample.com [A]

LinkedIn

With a role in engineering, this director may possess technical access to critical systems and intellectual property, making them a valuable target for attackers seeking to exploit technical vulnerabilities.

E

MEDIUM **Executive005 Sample005**

Chief Culture Officer · 100 Market Street, Sample City

CORPORATE ✉ employee009@acmesample.com [A]

LinkedIn

As Chief Culture Officer, this individual may have access to sensitive employee data and organizational strategies, which could be leveraged for social engineering or insider threats.

E

CRITICAL **Executive083 Sample083**

Vice President Information Technology · 100 Market Street, Sample City

CORPORATE ✉ employee343@acmesample.com [A]

LinkedIn

In the role of VP of Information Technology, this individual has significant technical access and control over IT systems, making them a critical target for attackers aiming to compromise the organization's cybersecurity defenses.

E

MEDIUM **Executive039 Sample039**

Sales Director Strategic Accounts · 100 Market Street, Sample City

CORPORATE ✉ employee162@acmesample.com [A]

LinkedIn

This Sales Director manages strategic accounts, which may include access to sensitive client data and contracts, making them susceptible to social engineering attacks aimed at extracting confidential information.

E

MEDIUM **Executive003 Sample003**

Director Operational Excellence · 100 Market Street, Sample City

CORPORATE ✉ employee006@acmesample.com [A]

LinkedIn

As a Director focused on operational excellence, this individual may have access to process improvement data and operational strategies, which could be targeted for competitive intelligence.

E

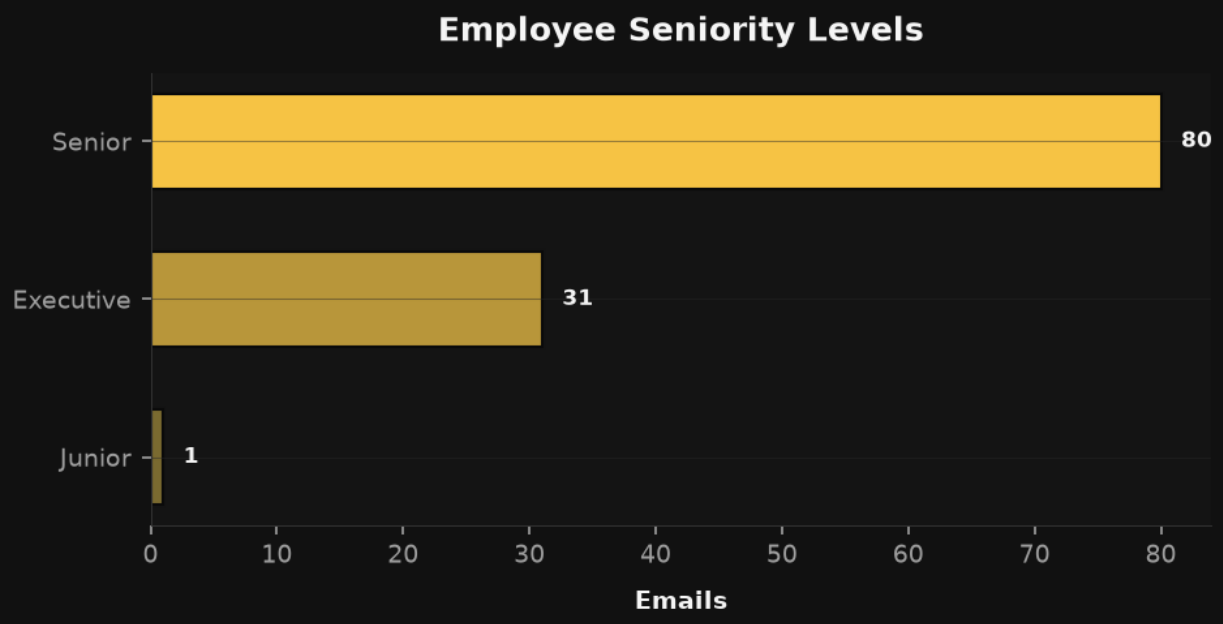
MEDIUM **Executive072 Sample072**

Director, People & Culture · 100 Market Street, Sample City

CORPORATE ✉ employee299@acmesample.com [A]

LinkedIn

This Director oversees people and culture initiatives, potentially granting access to sensitive employee information and organizational policies, making them a target for identity theft or insider threats.



Top Breach Sources

LEAK / BREACH	AFFECTED EMAILS
demandscience CSV 15 Aug 2024	41
pureb2b.co.uk	16
demandscience	12
CORPS Combolist_breachforums.as 16.02.2026	10

LEAK / BREACH	AFFECTED EMAILS
zoominfo.com darkforums.ru 08122026 (x)	8
zoominfo.com	7
xiqonline.com	6
Apollo.com	6
CORPS Combolist_breachforums.as	6
zoominfo.com darkforums.ru	6
linkedin.com	4
Pitney Bowes Inc. (pb.com)_shinyhunters	4
Pitney Bowes Inc. (pb.com)_shinyhunters FULL 22.04.2026 csv	2
canadalife.com_260429	2
UnderArmour_breachforums.bf 15.11.2025	2

Email Exposure — Sample Extract

Top 20 by risk score. Full dataset with all 100 records and detailed score breakdowns available in `private evidence dataset`.

EMAIL	NAME	POSITION	RISK	BREACHES	PWD	WEB SRC
employee074@acmesample.com	Executive020 Sample020	Senior Director, National Accounts	100	21	1	7
employee158@acmesample.com	Executive041 Sample041	Chief Executive Officer	95	8	—	5
employee058@acmesample.com	Executive012 Sample012	Vice President of Product Management	90	43	3	3
employee489@acmesample.com	Executive132 Sample131	Director of Human Resources	80	7	—	1
employee009@acmesample.com	Executive005 Sample005	Chief Culture Officer	80	6	—	1
employee163@acmesample.com	Executive036 Sample036	Vice President of Distribution	80	8	—	1
employee425@acmesample.com	Executive124 Sample124	Vice President Sales	70	2	—	5
employee220@acmesample.com	Executive050 Sample050	Quality Control Inspector	70	3	—	1
employee273@acmesample.com	Executive067 Sample067	Chief Financial Officer	70	5	—	1
employee324@acmesample.com		District Manager				

EMAIL	NAME	POSITION	RISK	BREACHES	PWD	WEB SRC
	Executive081 Sample081		70	4	—	6
employee437@acmesample.com	Executive121 Sample121	Executive Assistant	70	3	—	1
employee319@acmesample.com	Executive078 Sample078	Product Marketing Manager	70	6	—	4
employee533@acmesample.com	Executive146 Sample146	Regional Sales Manager	65	6	—	1
employee548@acmesample.com	Executive152 Sample152	Sales Manager	65	8	—	1
employee526@acmesample.com	Executive148 Sample148	Vice President of Sales	60	0	—	5
employee181@acmesample.com	Executive044 Sample044	Sales Director	60	0	—	6
employee148@acmesample.com	Executive035 Sample035	Senior Director of Strategic Accounts	60	0	—	6
employee162@acmesample.com	Executive039 Sample039	Sales Director	60	0	—	6
employee484@acmesample.com	Executive126 Sample126	Director of Engineering	60	2	—	1
employee160@acmesample.com	Executive037 Sample037	Quality Control Inspector	60	2	—	1

VIP Digital Footprint

OSINT intelligence on high-value targets — Google accounts, Microsoft recovery, account detection, breach exposure, password analysis

In this OSINT intelligence assessment, we evaluated 20 high-value corporate targets, including executives and senior management. Our analysis utilized multiple data sources, including Google account scans, Microsoft recovery checks, Holehe account detection, and breach databases. A total of 17 email accounts were tested, revealing 12 Google IDs and 9 Microsoft recovery accounts, with 360 total leak hits identified across the profiles. The key findings indicate significant vulnerabilities among the targets. Notably, all assessed individuals had leaked passwords, and personal accounts were exposed, including recovery email addresses and phone numbers. Additionally, location data was obtained from Google Maps reviews for some executives. These exposures create multiple attack vectors, enabling potential threats such as targeted phishing campaigns, credential stuffing attacks, and social engineering tactics. The overall risk level for the organization's leadership is high. An attacker could leverage the exposed data to impersonate executives, gain unauthorized access to sensitive information, and manipulate communications. Immediate action is recommended to enhance security measures, including implementing multi-factor authentication and conducting security awareness training for all high-value personnel.

17	12	9
EMAILS TESTED	GOOGLE IDS	MS RECOVERY

11	360
ACCOUNTS	BREACH RECORDS

ES

Executive012 Sample012

Vice President of Product Management

employee058@acmesample.com

Executive012 Sample012, Vice President of Product Management at Acme Sample GmbH, has a significant digital footprint with multiple breach records exposing corporate and personal credentials. The reuse of a weak password pattern across multiple sites and the exposure of personal data such as physical addresses and partial phone numbers heightens the risk of targeted attacks. This exposure could lead to unauthorized access to sensitive corporate systems and personal accounts, posing a critical risk to both personal and organizational security.

177	0	2	3
BREACH RECORDS	PLATFORMS	RECOVERY PROOFS	BREACH SOURCES

EXPOSURE SCORE

CRITICAL

85/100

Personalized attack potential · higher = more exposed

Based on 177 breach records · 2 recovery proofs · leaked password · password reuse
Model-assessed, bounded by deterministic evidence floors/caps

DIGITAL FOOTPRINT

Email Addresses

employee058@acmesample.com, employee059@examplemail.com, employee057@examplemail.com

Physical Address

100 Market Street, Sample City; 100 Market Street, Sample City

Phone Numbers

+1 202-555-1013

Recovery / Alt Emails

employee057@examplemail.com, email: employee058@acmesample.com, phone: (***) ***-**00

Observed Locations

Sample City, Canada; North York, Canada; Sample City, Canada; North York, Canada; North York, Canada

Google ID Confirmed

GAIA sample-45352... · 10 reviews

PASSWORD ANALYSIS

6	YES	WEAK	S***E (SAMPLE)
UNIQUE PASSWORDS	REUSE	STRENGTH	PREDICT.

S***e (sample)	S***E (SAMPLE)	S***e (sample)
S***e (sample)	S***E (SAMPLE)	S***e (sample)
S***e (sample)	S***E (SAMPLE)	S***e (sample)
S***e (sample)	S***E (SAMPLE)	S***e (sample)

- S***e (sample)
- S***e (sample)
- S***e (sample)

Reuse: S***e (sample) found on S***e (sample), S***e (sample)

Reuse: S***e (sample) found on S***e (sample), S***e (sample)

S***e (sample)

CRITICAL: Same password used on corporate AND personal email. The password 'S*e (sample)' was found under both corporate (employee058@acmesample.com) and personal (employee057@examplemail.com) emails, indicating critical reuse.**

PERSONAL INTELLIGENCE

Reviewed Linny's in Sample City, Canada on 2026-07-04 — likely leisure trip

Google Maps review · high

Reviewed Play It Again Sports in North York, Canada on 2026-05-04 — likely frequent visit

Google Maps review · high

Reviewed Enercare in Sample City, Canada on 2022-09-02 — likely service-related

Google Maps review · high

Works in industrial manufacturing aftermarket as Vice President of Product Management at Acme Sample GmbH

Linkedin_darkforumns.su 18 February 2023 · high

Phone area code suggests location: Sample City, Canada

Linkedin_darkforumns.su 18 February 2023 · medium

PERSONALITY

values quality service · appreciates helpful staff

INTERESTS

sports · dining

EMOTIONAL TRIGGERS

appreciates helpful service · values quality dining experiences

LIFESTYLE

frequent traveler · engages in leisure activities

ATTACK VECTORS

Credential Stuffing	HIGH
Spear Phishing - Corporate Credential Verification	HIGH
Spear Phishing - Social Media Security Alert	MEDIUM
Social Engineering - Dining Reward Scam	MEDIUM

CREDENTIAL RISK: Stuffing: **VIABLE** · Spray: **VIABLE**

SPEAR-PHISHING PRETEXTS — ONE SCENARIO PER OSINT DATA POINT

Each row below pairs ONE specific OSINT data point about this person (a breach record, a Holehe-detected account, a Google review, a password pattern, a corporate↔personal password reuse, or an enterprise service detected) with the concrete attack pretext an adversary could craft from that exact data. The “Source” column is the explicit citation that makes the pretext credible — it answers the question “why is this attack feasible?”. Yield is GPT’s estimate of how likely a real attack would succeed against this individual given that signal. Showing up to 6 of 6 pretexts derived for this profile (cap: 20).

TYPE	SERVICE / TOPIC	SOURCE — WHY THIS ATTACK IS FEASIBLE	PRETEXT & RATIONALE	YIELD
BREACH	**CORP APB** BREACH	CORP APB corporate credentials leaked May 2023	Acme Sample GmbH: Your corporate credentials may have been compromised. Verify your identity here. recent breach + corporate context	HIGH
BREACH	**Twitter** BREACH	1.5M Twitter Data Leak exposed email + password for employee057@examplemail.com	Twitter: Unusual login detected. Secure your account here. social media breach + personal email	MEDIUM
PATTERN	**S***e (sample)** PASSWORD	Password pattern 'S***e (sample)' observed across 10 breaches	Acme Sample GmbH IT: Weak password pattern detected. Update your password policy here. common password pattern + multiple breaches	MEDIUM

TYPE	SERVICE / TOPIC	SOURCE — WHY THIS ATTACK IS FEASIBLE	PRETEXT & RATIONALE	YIELD
REVIEW	**Linny's** REVIEW	Reviewed Linny's in Sample City, Canada on 2026-07-04 (5/5)	Linny's Sample City: Thank you for your recent visit! Claim your loyalty reward here. recent positive review + frequent dining	MEDIUM
REVIEW	**Play It Again Sports** REVIEW	Reviewed Play It Again Sports in North York, Canada on 2026-05-04 (5/5)	Play It Again Sports: We appreciate your feedback! Enjoy a 10% discount on your next purchase. positive review + sports interest	MEDIUM
REVIEW	**Enercare** REVIEW	Reviewed Enercare in Sample City, Canada on 2022-09-02 (5/5)	Enercare: Your service satisfaction is our priority. Claim your service voucher here. positive review + service satisfaction	MEDIUM

BEHAVIOUR & TRAVEL PATTERNS — FROM 10 GOOGLE REVIEWS

An attacker can craft personalised pretexts (false-event invitations, supplier-of-trust lures, family-context phishing) using the locations, businesses and timing visible in this person's public Google Maps activity. Each row below is a real review — the "exploit angle" column is the GPT-derived social-engineering hook.

BUSINESS / PLACE	LOCATION	RATING	DATE	EXPLOIT ANGLE
Linny's	100 Market Street, Sample City	5/5	—	Frequent visitor to quality dining spots — potential for dining-related pretexts.
Play It Again Sports	100 Market Street, Sample City	5/5	—	Engages in sports activities — potential for sports-related pretexts.
Enercare	100 Market Street, Sample City	5/5	—	Values efficient service — potential for service-related pretexts.
Rinx Sample City	100 Market Street, Sample City	4/5	—	Participates in recreational activities — potential for leisure-related pretexts.
Paramount Ice Complex	100 Market Street, Sample City	3/5	—	Visits ice complexes — potential for ice sports-related pretexts.
Turtle Jack's Winona	100 Market Street, Sample City	5/5	—	Enjoys dining at Turtle Jack's — potential for restaurant-related pretexts.
Victoria Village Arena	100 Market Street, Sample City	3/5	—	Frequent arena visitor — potential for sports event-related pretexts.
Y.O. Ranch Steakhouse	100 Market Street, Sample City	4/5	—	Dines at steakhouses — potential for steakhouse-related pretexts.
Don Mills Civitan Arena	100 Market Street, Sample City	1/5	—	Dissatisfied with arena conditions — potential for improvement-related pretexts.
The Venetian Las Vegas	100 Market Street, Sample City	5/5	—	Frequent traveler to Las Vegas — potential for travel-related pretexts.

ES

Executive020 Sample020

Senior Director, National Accounts

employee074@acmesample.com

Executive020 Sample020, a Senior Director at Acme Sample GmbH, has a high-risk exposure due to multiple data breaches involving leaked credentials. These breaches include significant platforms like LinkedIn and Trello, with evidence of password reuse patterns. The exposure of his physical address and partial phone number further elevates the risk, enabling potential targeted attacks. Immediate remediation is recommended to mitigate these risks.

26 BREACH RECORDS

1 PLATFORMS

2 RECOVERY PROOFS

6 BREACH SOURCES

EXPOSURE SCORE **HIGH**

85/100

Personalized attack potential · higher = more exposed

Based on 26 breach records · 1 account · 2 recovery proofs · leaked password
Model-assessed, bounded by deterministic evidence floors/caps

DIGITAL FOOTPRINT

@ Email Addresses
employee074@acmesample.com

A Physical Address
100 Market Street, Sample City

T Phone Numbers
+1 202-555-1015

R Recovery / Alt Emails
email: employee074@acmesample.com,
phone: ********68

W Detected Accounts
office365

P Observed Locations
Sample City, CA

G Google ID Confirmed
GAIA sample-19499...

PASSWORD ANALYSIS

5	NO	WEAK	S***E (SAMPLE)
UNIQUE PASSWORDS	REUSE	STRENGTH	PREDICT.

S***e (sample)	S***E (SAMPLE)	S***e (sample)
S***e (sample)	S***E (SAMPLE)	S***e (sample)
S***e (sample)	S***E (SAMPLE)	S***e (sample)
S***e (sample)	S***E (SAMPLE)	S***e (sample)

- S***e (sample)
- S***e (sample)
- S***e (sample)

S***e (sample)

PERSONAL INTELLIGENCE

i Works in Transportation as Business Analyst at Acme Sample GmbH (100-249 employees)
DemandScience CSV · high

i Revenue band of $50 - 99 Million
DemandScience CSV · high

ATTACK VECTORS

Credential Stuffing	HIGH
Spear Phishing	MEDIUM
Vishing	MEDIUM
Physical Access	LOW

CREDENTIAL RISK: Stuffing: VIABLE · Spray: VIABLE

SPEAR-PHISHING PRETEXTS — ONE SCENARIO PER OSINT DATA POINT

Each row below pairs ONE specific OSINT data point about this person (a breach record, a Holehe-detected account, a Google review, a password pattern, a corporate↔personal password reuse, or an enterprise service detected) with the concrete attack pretext an adversary could craft from that exact data. The “Source” column is the explicit citation that makes the pretext credible — it answers the question “why is this attack feasible?”. Yield is GPT’s estimate of how likely a real attack would succeed against this individual given that signal. Showing up to 5 of 5 pretexts derived for this profile (cap: 20).

TYPE	SERVICE / TOPIC	SOURCE — WHY THIS ATTACK IS FEASIBLE	PRETEXT & RATIONALE	YIELD
BREACH	**Zacks.com** FINANCE	Stealer log ULP 21.04.2025 captured employee074@acmesample.com on Zacks.com using password S***e (sample)	Unusual activity detected on your Zacks account. Confirm your recent transactions here. Stealer log provides direct credential capture with recent date.	HIGH
SERVICE	**Office365** PRODUCTIVITY	Holehe confirmed account exists at office365 for email employee074@acmesample.com	Your Office365 account requires immediate verification. Click here to secure your account. Confirmed account existence on a productivity platform.	MEDIUM
BREACH	**Trello.com** PRODUCTIVITY	Breach Compilation exposed email + password for Trello.com	Your Trello account was accessed from an unknown device. Verify your identity here. Breach data includes email and password for a productivity tool.	MEDIUM
BREACH	**xiqonline.com** OTHER	Breach Compilation exposed email + password for xiqonline.com	Your xiqonline account has been flagged for suspicious activity. Verify your account details here. Breach data includes email and password for a lesser-known service.	MEDIUM
PATTERN	**S***e (sample)** PASSWORD	Password pattern 'S***e (sample)' + numeric suffix observed in multiple breaches	Our system detected a weak-pattern match against your historical password (S***e (sample)). Update your password here. Reused weak password pattern across multiple breaches.	MEDIUM

ES

Executive040 Sample040

IT Technical Lead

employee157@acmesample.com

Executive040 Sample040, an IT Technical Lead at Acme Sample GmbH, has been exposed in multiple data breaches, including one that revealed full PII. This exposure includes email, password, phone, and address information, which could be leveraged for targeted attacks. The reuse of weak password patterns across different platforms further exacerbates the risk, making both personal and corporate accounts vulnerable to compromise.

11
BREACH RECORDS

5
PLATFORMS

1
RECOVERY PROOFS

2
BREACH SOURCES

EXPOSURE SCORE **HIGH**

80/100

Personalized attack potential · higher = more exposed

Based on 11 breach records · 5 accounts · 1 recovery proof · leaked password
Model-assessed, bounded by deterministic evidence floors/caps

DIGITAL FOOTPRINT

@ Email Addresses
employee157@acmesample.com, employee161@examplemail.com

A Physical Address
100 Market Street, Sample City; 100 Market Street, Sample City

T Phone Numbers
+1 202-555-1016, +1 202-555-1017

R Recovery / Alt Emails
phone: ********43

W Detected Accounts
hubspot, office365, gravatar, spotify

P Observed Locations
Sample City, Canada

G Google ID Confirmed
GAIA sample-69845...

PASSWORD ANALYSIS

1	NO	WEAK	S***E (SAMPLE)
UNIQUE PASSWORDS	REUSE	STRENGTH	PREDICT.

`S***e (sample)` `S***E (SAMPLE)` S***e (sample)

- S***e (sample)

S***e (sample)

PERSONAL INTELLIGENCE

Works in the IT industry as IT Technical Lead at Acme Sample GmbH

DemandScience CSV · high

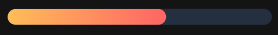
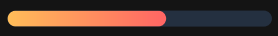
Browser/session traced to Sample City, Canada

Stealer log session · medium

Phone area code suggests location: Sample City, Canada

DemandScience CSV · high

ATTACK VECTORS

Spear Phishing via Pitney Bowes Breach		HIGH
Credential Stuffing on Office365		MEDIUM
Vishing using Exposed Phone Numbers		MEDIUM

CREDENTIAL RISK: Stuffing: **VIABLE** · Spray: **VIABLE**

SPEAR-PHISHING PRETEXTS — ONE SCENARIO PER OSINT DATA POINT

Each row below pairs ONE specific OSINT data point about this person (a breach record, a Holehe-detected account, a Google review, a password pattern, a corporate↔personal password reuse, or an enterprise service detected) with the concrete attack pretext an adversary could craft from that exact data. The “Source” column is the explicit citation that makes the pretext credible — it answers the question “why is this attack feasible?”. Yield is GPT’s estimate of how likely a real attack would succeed against this individual given that signal. Showing up to 3 of 3 pretexts derived for this profile (cap: 20).

TYPE	SERVICE / TOPIC	SOURCE — WHY THIS ATTACK IS FEASIBLE	PRETEXT & RATIONALE	YIELD
BREACH	**Pitney Bowes Inc. (pb.com)** BREACH	Pitney Bowes Inc. (pb.com)_ shinyhunters FULL 22.04.2026 csv exposed full PII (name, address, phone) for employee157@acmesample.com	Pitney Bowes security alert: Confirm your identity to secure your account. recent breach with full PII exposure	HIGH
SERVICE	**Office365** PRODUCTIVITY	Holehe confirmed account exists at Office365 for email employee157@acmesample.com	Your Office365 account was accessed from a new device. Click here to verify. corporate account confirmation	MEDIUM
PATTERN	**General** PASSWORD	Password pattern 'S***e (sample)' observed in xiqonline. com breach	Our system detected a weak-pattern match against your historical password. Update your credentials here. weak password pattern observed	MEDIUM

ES

Executive035 Sample035

Senior Director Strategic Accounts

employee148@acmesample.com

Executive035 Sample035, a Senior Director at Acme Sample GmbH, has been identified with multiple breached accounts, including Luxottica, Houzz, and AT&T, with exposed passwords. The reuse of similar password patterns across these breaches poses a critical risk to both personal and corporate security. Additionally, the presence of alternative emails and partial phone numbers increases the potential for targeted phishing and vishing attacks.

79 BREACH RECORDS

1 PLATFORMS

2 RECOVERY PROOFS

4 BREACH SOURCES

EXPOSURE SCORE **HIGH**

80/100

Personalized attack potential · higher = more exposed

Based on 79 breach records · 1 account · 2 recovery proofs · leaked password · password reuse

Model-assessed, bounded by deterministic evidence floors/caps

DIGITAL FOOTPRINT

@ Email Addresses

employee148@acmesample.com, employee480@examplemail.com, employee481@examplemail.com

T Phone Numbers

+1 202-555-1014

R Recovery / Alt Emails

employee480@examplemail.com, employee481@examplemail.com, email: employee480@examplemail.com, phone: ***-***-**76

W Detected Accounts

office365

G Google ID Confirmed

GAIA sample-95896...

PASSWORD ANALYSIS

5	YES	WEAK	S***E (SAMPLE)
UNIQUE PASSWORDS	REUSE	STRENGTH	PREDICT.

S***e (sample)	S***E (SAMPLE)	S***e (sample)
S***e (sample)	S***E (SAMPLE)	S***e (sample)
S***e (sample)	S***E (SAMPLE)	S***e (sample)
S***e (sample)	S***E (SAMPLE)	S***e (sample)

- S***e (sample)
- S***e (sample)
- S***e (sample)

Reuse: S***e (sample) found on S***e (sample), S***e (sample)

Reuse: S***e (sample) found on S***e (sample), S***e (sample)

S***e (sample)

CRITICAL: Same password used on corporate AND personal email. The password 'S*e (sample)' was found under both the corporate email (employee148@acmesample.com) and personal email (employee481@examplemail.com), indicating a critical reuse issue.**

PERSONAL INTELLIGENCE

i Works in strategic accounts at Acme Sample GmbH

DemandScience CSV · high

i Browser session traced to USA

Stealer log session · medium

i Phone area code suggests location: USA

Stealer log session · medium

ATTACK VECTORS

Credential Stuffing	HIGH
Spear Phishing	MEDIUM
Vishing	MEDIUM

CREDENTIAL RISK: Stuffing: **VIABLE** · Spray: **VIABLE**

SPEAR-PHISHING PRETEXTS — ONE SCENARIO PER OSINT DATA POINT

Each row below pairs ONE specific OSINT data point about this person (a breach record, a Holehe-detected account, a Google review, a password pattern, a corporate↔personal password reuse, or an enterprise service detected) with the concrete attack pretext an adversary could craft from that exact data. The “Source” column is the explicit citation that makes the pretext credible — it answers the question “why is this attack feasible?”. Yield is GPT’s estimate of how likely a real attack would succeed against this individual given that signal. Showing up to 5 of 5 pretexts derived for this profile (cap: 20).

TYPE	SERVICE / TOPIC	SOURCE — WHY THIS ATTACK IS FEASIBLE	PRETEXT & RATIONALE	YIELD
SERVICE	**Office 365** PRODUCTIVITY	Holehe confirmed account exists at office365 for email employee148@acmesample.com	Your Office 365 account has unusual activity. Please verify your login here. corporate context confirmed	HIGH
BREACH	**Luxottica.com** BREACH	Breach data exposed email + password for Luxottica.com	Your Luxottica account was part of a data breach. Reset your password here. recent breach with password exposure	MEDIUM
BREACH	**houzz.com** BREACH	Breach data exposed email + password for houzz.com on S***e (sample)	Houzz security alert: Your account was accessed. Secure your account now. historical breach with password exposure	MEDIUM
BREACH	**AT&T** BREACH	Breach data exposed email + password for AT&T on S***e (sample)	AT&T account security: Unusual login detected. Verify your identity. recent breach with password exposure	MEDIUM
PATTERN	**Password Pattern** PASSWORD	Pattern r2****jf observed across multiple breaches	Our monitoring system detected a weak password pattern in your account. Update your password here. repeated pattern across breaches	MEDIUM

ES

Executive067 Sample067

Chief Financial Officer

employee273@acmesample.com

Executive067 Sample067, the CFO of Acme Sample GmbH, has a high-risk exposure due to multiple data breaches revealing sensitive information, including email, password, and full PII. The presence of weak password patterns and reuse across platforms increases the likelihood of successful credential attacks. This exposure poses a critical risk to both personal and corporate security, necessitating immediate remediation efforts.

10 BREACH RECORDS

4 PLATFORMS

2 RECOVERY PROOFS

3 BREACH SOURCES

EXPOSURE SCORE **HIGH**

85/100

Personalized attack potential · higher = more exposed

Based on 10 breach records · 4 accounts · 2 recovery proofs · leaked password

Model-assessed, bounded by deterministic evidence floors/caps

DIGITAL FOOTPRINT

@ Email Addresses

employee273@acmesample.com,

employee258@examplemail.com

A Physical Address

100 Market Street, Sample City

T Phone Numbers

+1 202-555-1019

R Recovery / Alt Emails

authenticator: TOTP, email: wi*****@gmail.com

W Detected Accounts

office365, spotify, xvideos

G Google ID Confirmed

GAIA sample-45583...

PASSWORD ANALYSIS

2	NO	WEAK	S***E (SAMPLE)
UNIQUE PASSWORDS	REUSE	STRENGTH	PREDICT.

S***e (sample) S***E (SAMPLE) S***e (sample)

S***e (sample) S***E (SAMPLE) S***e (sample)

• S***e (sample)

S***e (sample)

PERSONAL INTELLIGENCE

i Works in Manufacturing as Chief Financial Officer at Acme Sample GmbH (500-999 employees)

DemandScience CSV · high

i Company revenue is $10-49 Million

DemandScience CSV · high

ATTACK VECTORS

Credential Stuffing	HIGH
Spear Phishing via Office 365	HIGH
Vishing Attack	MEDIUM
Physical Access Exploitation	MEDIUM

CREDENTIAL RISK: Stuffing: VIABLE · Spray: VIABLE

SPEAR-PHISHING PRETEXTS — ONE SCENARIO PER OSINT DATA POINT

Each row below pairs ONE specific OSINT data point about this person (a breach record, a Holehe-detected account, a Google review, a password pattern, a corporate↔personal password reuse, or an enterprise service detected) with the concrete attack pretext an adversary could craft from that exact data. The “Source” column is the explicit citation that makes the pretext credible — it answers the question “why is this attack feasible?”. Yield is GPT’s estimate of how likely a real attack would succeed against this individual given that signal. Showing up to 5 of 5 pretexts derived for this profile (cap: 20).

TYPE	SERVICE / TOPIC	SOURCE — WHY THIS ATTACK IS FEASIBLE	PRETEXT & RATIONALE	YIELD
SERVICE	**Office 365** PRODUCTIVITY	Holehe confirmed account exists at Office 365 for email employee273@acmesample.com	Your Office 365 account requires verification due to unusual activity. Click here to secure your account. corporate account confirmation + high-value productivity platform	HIGH
BREACH	**xiqonline.com** BREACH	Breach record from xiqonline.com dated S***e (sample) exposed email employee273@acmesample.com with password S***e (sample)	We detected a login attempt on your xiqonline.com account. If this wasn't you, reset your password here. recent breach + password exposure	HIGH
BREACH	**DemandScience CSV** BREACH	DemandScience CSV breach exposed full PII (name, address, phone, role) for employee273@acmesample.com	AIRE Ancient Baths HR records — please confirm the address on file matches your current residence. full PII exposure + corporate context	HIGH
ACCOUNT	**Spotify** STREAMING	Holehe confirmed account exists at Spotify for email employee273@acmesample.com	Your Spotify account was accessed from a new device. Verify your identity here. personal account confirmation + streaming service	MEDIUM
PATTERN	**Password Pattern** PASSWORD	Pattern 'base word + numeric suffix S***e (sample)' observed in xiqonline.com breach	Our credential-monitoring system identified a weak-pattern match against your historical password (S***e (sample)). Read the updated password policy here. weak password pattern + potential for reuse	MEDIUM

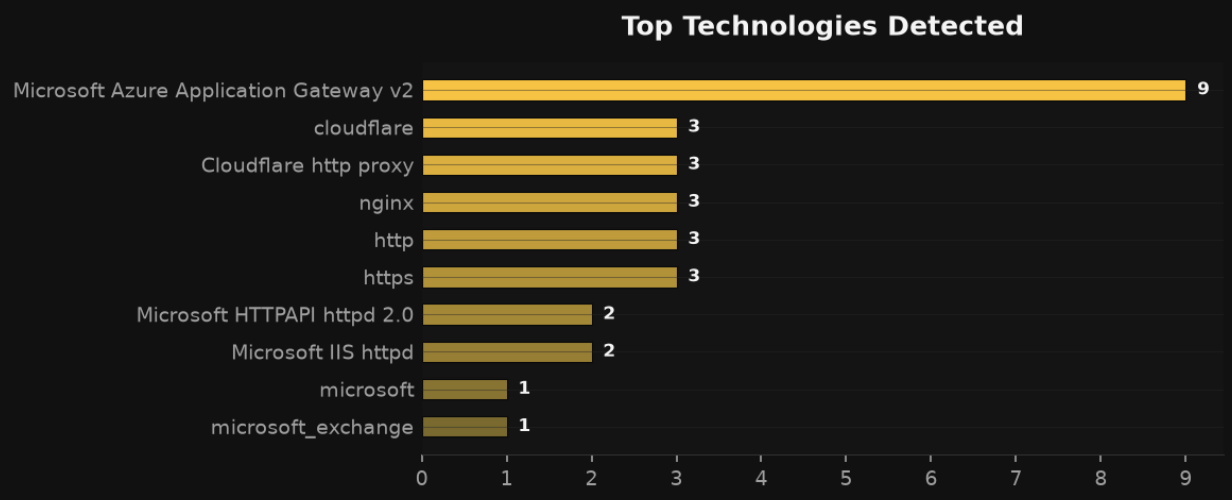
APPLICATIONS

Technology Stack

Technologies are detected through passive intelligence: Shodan service banners, Netlas domain fingerprinting, ZoomEye host analysis, and CPE (Common Platform Enumeration) identifiers extracted from banner data. Active port scanning (Nmap -sV) provided additional service version confirmation. Technology identification enables targeted vulnerability research and helps prioritize patching efforts.

Technologies detected on **21** of **54** hosts (18 unique technologies). Data sources: Shodan (service banners, CPE identifiers), Nmap (active service version detection).

Top technologies (single accent ramp)



Technology Risk Assessment

The organization’s technology stack shows a mix of modern and potentially outdated components, notably with the presence of Microsoft HTTPAPI httpd 2.0, which is no longer supported. Additionally, the use of Microsoft Exchange and IIS could pose risks if not regularly updated, given their historical vulnerabilities. It is recommended that the organization prioritize upgrading or replacing outdated software, particularly the Microsoft HTTPAPI, to mitigate security risks.

TECHNOLOGY	DESCRIPTION	HOSTS
Microsoft Azure Application Gateway v2		9
cloudflare	CDN / DDoS protection	3
Cloudflare http proxy	CDN / HTTP reverse proxy	3
nginx	Web server / reverse proxy	3
http	Hypertext Transfer Protocol	3
https	TLS-encrypted HTTP (port 443)	3
Microsoft HTTPAPI httpd 2.0		2
Microsoft IIS httpd	Microsoft web server (IIS)	2
microsoft	Microsoft web server (IIS)	1
microsoft_exchange	Mail & collaboration server	1
smtp		1
submission		1
microsoft_asp_net		1
kestrel		1
sfdcedge		1

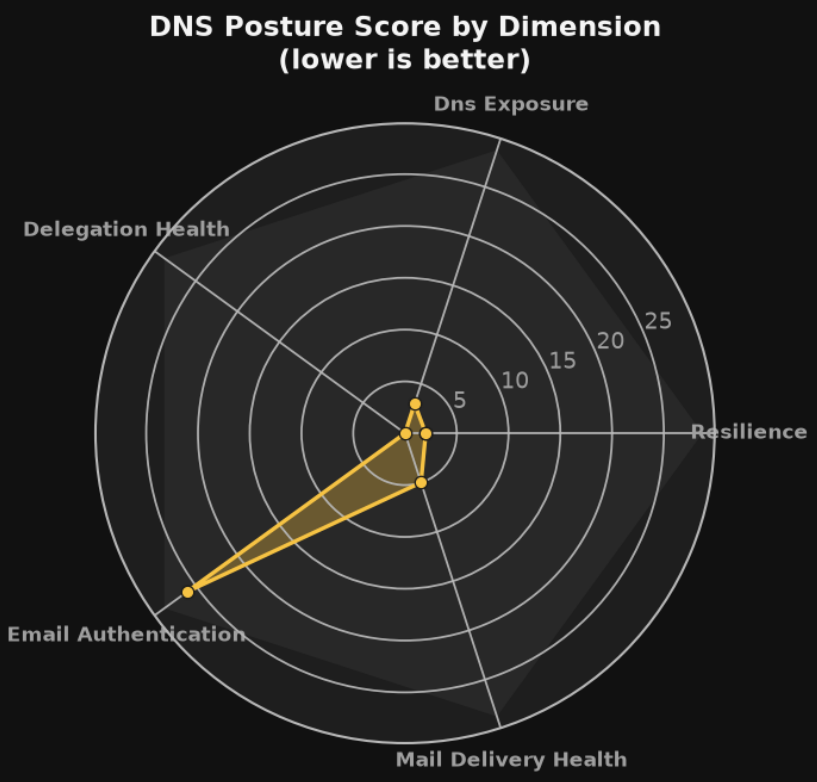
DNS & Email Security Posture

76
GOOD

The DNS posture assessment performed **39 automated checks** across five security dimensions: delegation health (NS presence, SOA validity, lame delegation), DNS exposure (zone transfer, open recursion, version disclosure), email authentication (SPF, DMARC, DKIM), mail delivery health (MX resolution, PTR alignment), and resilience (DNSSEC, CAA, NS diversity). Two complementary numbers are shown below: the **raw exposure score** (0 = none, 100 = critical — lower is better) and the **health score** (100 − exposure, higher is better) which is what feeds the overall Security Posture Score in the executive summary.

36/100	64/100	High	39
EXPOSURE SCORE (LOWER = BETTER)	HEALTH SCORE (HIGHER = BETTER)	OVERALL SEVERITY	CHECKS PERFORMED

Dimensions (lower is better)



DNS posture has gaps: DMARC Policy: Monitoring Only; No MTA-STS TXT Record. No critical exposures found.

Risk Findings (2)

SEVERITY	CHECK ID	RESULT
MEDIUM	MAIL_DMARC_POLICY	DMARC Policy: Monitoring Only
MEDIUM	MAIL_MTA_STS_TXT	No MTA-STS TXT Record

Complete check results (39 total) available in `private evidence dataset` omitted from this public sample.

Reverse DNS (PTR) Insights

For every IP address discovered during the scan, we perform a PTR (reverse DNS) lookup. PTR records map IPs back to hostnames and reveal naming conventions, infrastructure details, and potential misconfigurations that attackers use during reconnaissance.

21	2	19	3
IPS ANALYSED	VALID PTR RECORDS	MISSING PTR	RISK FINDINGS

SMTP Servers Without PTR (1)

Mail servers without PTR records face deliverability issues — many receiving servers reject or spam-filter mail from IPs lacking valid reverse DNS.

IP	HOSTNAME	SMTP PORTS	RISK
192.0.2.75	asset-166.acmesample.com	25, 587	HIGH

PTR Mismatches — Forward-Confirmed Reverse DNS Failures (1)

A PTR mismatch occurs when the reverse DNS name does not resolve back to the original IP. This is penalised by spam filters and indicates DNS configuration errors.

IP	PTR RECORD	RESOLVES TO	RISK
192.0.2.182	bl194.acmesample.com.11.164.2...	NXDOMAIN	MEDIUM

Third-Party / Shadow Infrastructure (1)

PTR records revealing cloud provider hostnames (e.g., ec2-*.amazonaws.com) may indicate unmanaged cloud assets or shadow IT — especially when the forward hostname belongs to the organization.

IP	HOSTNAME	PTR RECORD	CLOUD PRO-VIDER
192.0.2.33	asset-152.acmesample....	ec2-15-156-229-37.ca-central...	AWS

Email Authentication Security

This section evaluates whether the domain can be abused for email spoofing or phishing attacks based on SPF, DMARC, and DKIM configurations. Complete finding details including affected domains, evidence, and remediation steps is omitted from this public sample.

89/100	MEDIUM	MEDIUM	0
EMAIL AUTH SCORE	SPOOFING RISK	PHISHING RISK	CRITICAL / HIGH FINDINGS

Configuration Summary

PROTOCOL	STATUS	DETAILS
SPF	PRESENT	Policy: `-all` · 3 DNS lookups
DMARC	PRESENT	Policy: p=none
DKIM	1 SELECTOR(S)	Selectors: selector1
MX	PRESENT	2 record(s)

Key Findings

SEVERITY	FINDING	EVIDENCE
MEDIUM	**DMARC Policy: None (Monitoring)** p=none — no enforcement, monitoring only.	DMARC policy: p=none (monitoring only).

Findings Requiring Attention

RESULT	CHECK	DETAIL	RECOMMENDATION
WARN	**SPF Unknown Third-Party Includes**	SPF includes domains not recognized as standard email platforms.	Investigate unknown include: domains and remove if unused.
WARN	**DMARC Policy: None (Monitoring)**	p=none — no enforcement, monitoring only.	Progress to p=quarantine then p=reject after reviewing reports.
WARN	**DMARC Alignment Relaxed**	adkim=r or aspf=r — relaxed alignment may allow subdomain spoofing.	Set adkim=s and aspf=s for strict alignment.
N/A	**No BIMI Record**	BIMI is not configured.	Publish a BIMI TXT record at default._bimi.domain.
	No MTA-STS		

RESULT	CHECK	DETAIL	RECOMMENDATION
N/A		MTA-STS is not configured — email transport relies on opportunistic TLS.	Publish _mta-sts TXT record and host policy file.
N/A	**No TLS-RPT**	SMTP TLS Reporting not configured.	Publish _smtp._tls TXT record with rua= reporting URI.

Vulnerability Assessment

53
POOR

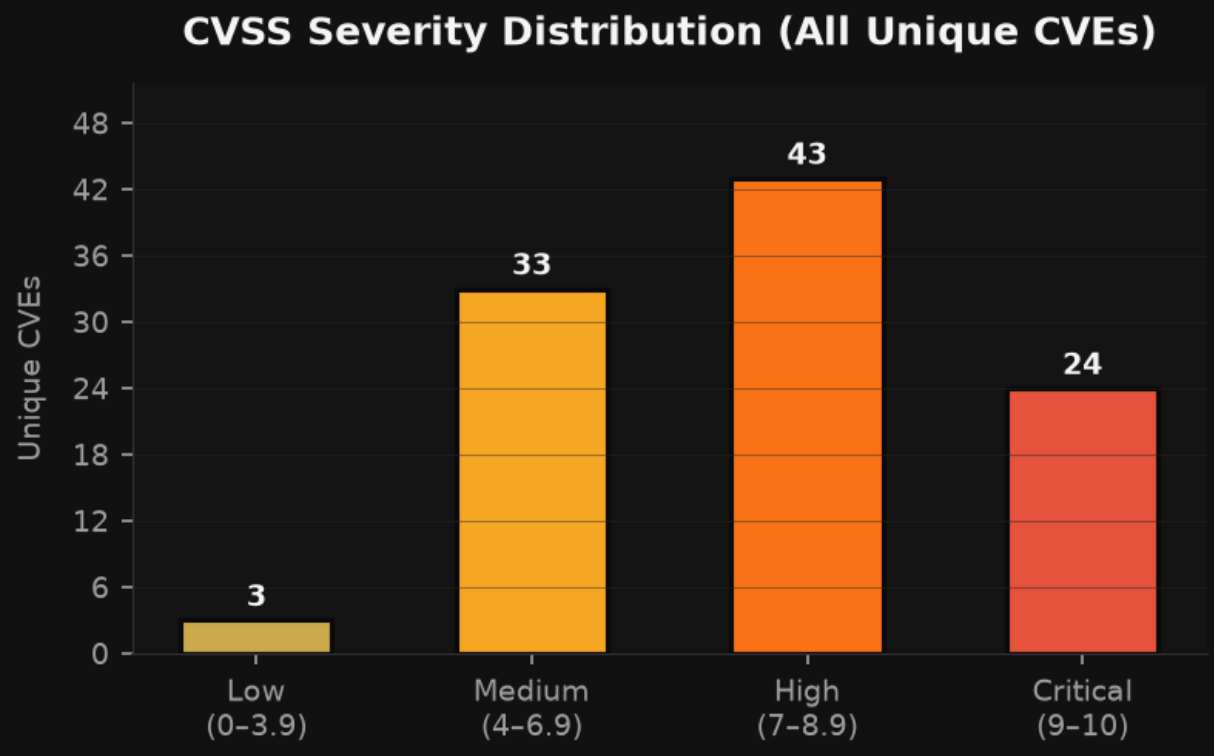
Vulnerabilities are aggregated from five sources in priority order: (1) Nmap vulners script — highest confidence, version-matched by live service detection, (2) Shodan, (3) Netlas, (4) ZoomEye passive intelligence, (5) Shodan CVEDB — free lookup by product name/version. Each CVE is cross-referenced against Nmap service banners; the **version-corroborated** flag indicates the product token and a version string both appeared in the detected service banner (a passive string match, not an active exploit-verification).

Disclaimer: All findings are based on **service banner and version matching** — no active exploitation or payload injection was performed. A CVE match means the detected version is known to be affected, not that it is exploitable in this configuration. Patches, WAFs, and compensating controls may mitigate the risk.

103	10	0	2
UNIQUE CVES	AFFECTED HOSTS	NMAP VERIFIED	VERIFICATION FINDINGS
			+397 INFORMATIONAL

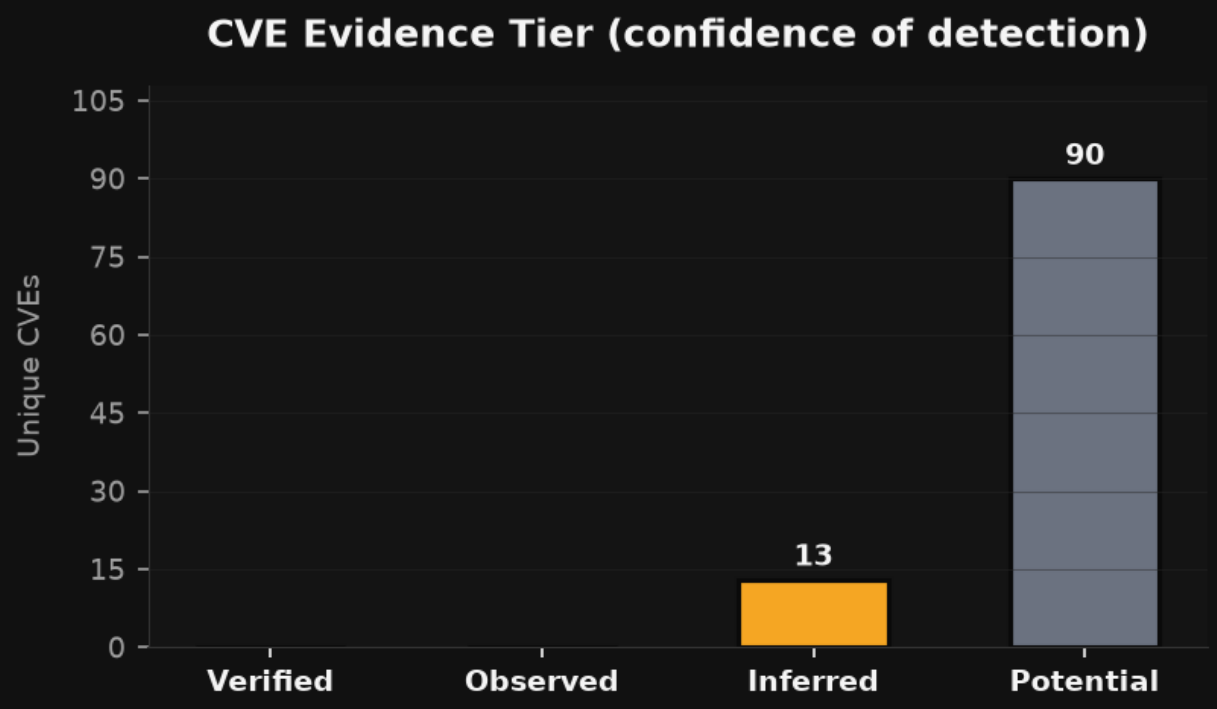
CVSS severity (unique CVEs)

Distribution of all 103 unique CVEs by CVSS v3 severity rating.

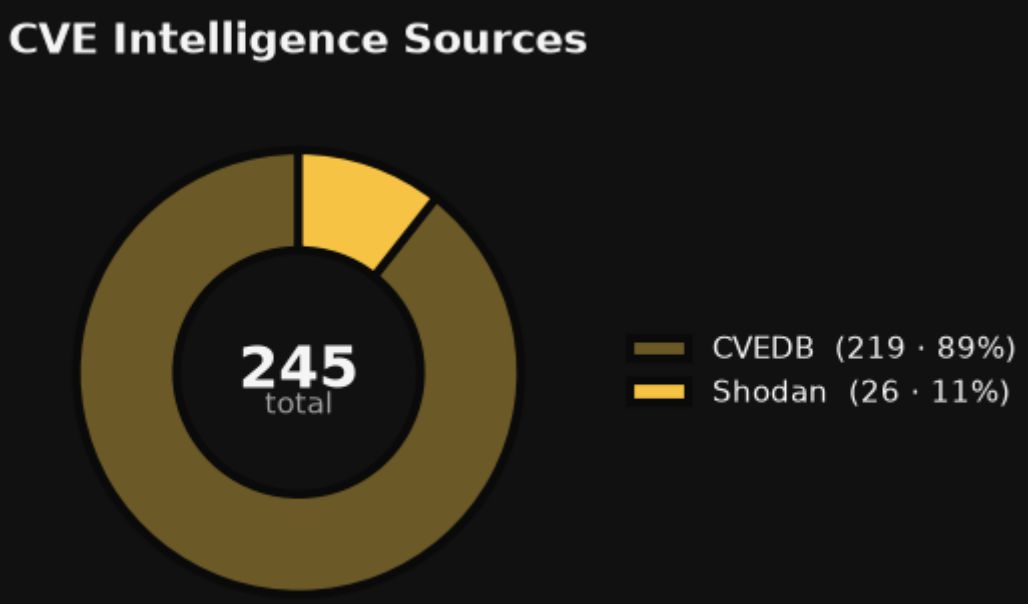


Evidence tier (unique CVEs)

The same CVEs graded by how strongly each was corroborated. **Verified** = exact Nuclei host/port/CVE match or operator-confirmed version; **Observed** = live Nmap service banner; **Inferred** = passive-intelligence or version-string corroboration; **Potential** = a single product-only signal, applicability unconfirmed.



CVE intelligence sources



Confidence levels

LEVEL	DESCRIPTION	CVES
Product Matched Unverified	Product matched via CPE/banner but version unconfirmed	**90**
Passive Intelligence	Reported by passive intelligence platforms (Shodan/Netlas/ZoomEye)	**13**

Evidence tiers

How strongly each CVE was corroborated, independent of its severity. Under the DS-90 v2 model this tier drives confidence-weighted vulnerability scoring. Evidence tiers are shown beside severity on CVE and CISA KEV surfaces where the underlying row supports the taxonomy.

TIER	MEANING	CVES
VERIFIED	Exact Nuclei host/port/CVE match, or confirmed against an operator-supplied version — highest confidence	**0**
OBSERVED	Corroborated by a live Nmap service banner on the affected host/port	**0**
INFERRED	Passive-intelligence report or version-string corroboration; not actively probed	**13**
POTENTIAL	A single product-only signal; the specific version and applicability are unconfirmed	**90**

Top CVEs by Severity

CVE	CVSS	EVIDENCE	SOURCES	HOSTS	CONFIDENCE
CVE-2004-0847	9.8	POTENTIAL	CVEDB	4	product matched unverified
CVE-2006-1364	7.5	POTENTIAL	CVEDB	4	product matched unverified
CVE-2003-0768	6.8	POTENTIAL	CVEDB	4	product matched unverified
CVE-2005-1664	6.4	POTENTIAL	CVEDB	4	product matched unverified
CVE-2005-1665	5.0	POTENTIAL	CVEDB	4	product matched unverified

CVE	CVSS	EVIDENCE	SOURCES	HOSTS	CONFIDENCE
CVE-2005-2224	5.0	POTENTIAL	CVEDB	4	product matched unverified
CVE-2005-0452	4.3	POTENTIAL	CVEDB	4	product matched unverified
CVE-2010-2084	4.3	POTENTIAL	CVEDB	4	product matched unverified
CVE-2010-2088	4.3	POTENTIAL	CVEDB	4	product matched unverified
CVE-2015-3105	10.0	POTENTIAL	CVEDB	3	product matched unverified
CVE-2014-0515	10.0	POTENTIAL	CVEDB	3	product matched unverified
CVE-2010-0425	10.0	POTENTIAL	CVEDB	3	product matched unverified
CVE-2015-0359	10.0	POTENTIAL	CVEDB	3	product matched unverified
CVE-2009-3555	9.8	POTENTIAL	CVEDB	3	product matched unverified
CVE-2024-4577	9.8	POTENTIAL	CVEDB	3	product matched unverified

Full vulnerability list (103 CVEs) available in Appendix B and in `private evidence dataset` omitted from this public sample.

Exploit Prioritization & Remediation Guidance

The following table enriches detected software components with exploit maturity intelligence to help prioritize remediation beyond CVSS severity alone. **Exploit Maturity** indicates how readily available working exploit code is — "Weaponized" means active exploitation in the wild, while "PoC" indicates proof-of-concept code exists. Components are sorted by remediation priority.

SOFTWARE	DETECTED VER.	CURRENT VER.	TOP CVE	CVSS	EXPLOIT MATURITY	PRIORITY
windows	unknown	unknown	CVE-2010-0425	10.0	WEAPONIZED	CRITICAL
Critical CVEs with known exploits and multiple affected hosts necessitate immediate remediation. `cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*`						
internet_information_services	10.0	10.0	CVE-2000-0246	10.0	WEAPONIZED	LOW
Detected version matches the latest available release; the listed CVE typically requires a specific configuration or vulnerable build — verify patch level and exposure rather than performing a blind upgrade. Critical vulnerabilities with known exploits and significant host count require urgent attention. `cpe:2.3:a:microsoft:internet_information_services:10.0:*:*:*:*:*:*:*`						
nginx	unknown	unknown	CVE-2009-2629	9.8	WEAPONIZED	CRITICAL
High CVSS scores and known exploits across multiple vulnerabilities indicate critical risk. `cpe:2.3:a:nginx:nginx:*:*:*:*:*:*:*:*`						
asp.net	unknown	unknown	CVE-2005-1665	9.8	FUNCTIONAL	HIGH
High CVSS with reliable public exploits suggests significant risk, despite no known exploitation. `cpe:2.3:a:microsoft:asp.net:*:*:*:*:*:*:*:*`						
exchange_server	unknown	unknown	CVE-2021-26855	9.1	WEAPONIZED	CRITICAL
Critical vulnerabilities with known exploits and a single affected host necessitate immediate action. `cpe:2.3:a:microsoft:exchange_server:*:*:*:*:*:*:*:*`						
cloudflare	unknown	unknown	CVE-2024-0212	8.1	UNPROVEN	MEDIUM
Moderate CVSS with no known exploits and low host count suggests lower urgency for remediation.						

Exploit maturity is assessed using CVSS severity, software prevalence, and known exploit intelligence. "Weaponized" = active exploitation in the wild; "Functional" = reliable public exploits; "PoC" = proof-of-concept exists; "Unproven" = no known exploit code.

Active Security Verification

Scanned **22/22** unique IPs (46 live HTTP endpoints) in 36.2 minutes using 4,000+ curated safe templates (GET/HEAD only — no exploitation).

Why 22 IPs instead of 54 hostnames? The verification engine operates on unique IP addresses (not hostnames). 54 hostnames were discovered, of which **25** were successfully resolved to **21** unique IPs. Most IPs in this scan are dedicated to a single hostname — **17** of **21** IPs (81.0%) serve exactly one FQDN. A small number host multiple names (top shared IP: `192.0.2.178` with 2 FQDNs). The remaining 22 IPs entered the pipeline and were further filtered through: (1) a port classification whitelist (only web, SSL, DNS, and known network service ports qualify), (2) an httpx liveness check (only responding HTTP/HTTPS endpoints are tested with HTTP templates), and (3) the per-IP cache. Hosts with no qualifying ports or no live HTTP endpoint are still counted in the dispatch totals but produce no nuclei findings.

2 actionable security findings (critical/high/medium/low) and **397** informational detections (technology fingerprinting, environment metadata — not weaknesses by themselves).

CATEGORY	SEVERITY	FINDINGS
Actionable	LOW	**2**
Informational	INFO	**397**

Top Actionable Findings by Template

Informational templates are excluded from this table (full set in `private evidence dataset`).

FINDING	SEVERITY	HOSTS	SAMPLE URL
Weak Cipher Suites Detection	LOW	**2**	asset-188.acmesample.com:443

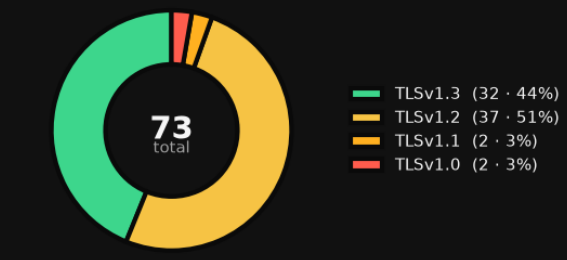
Showing top 1 actionable templates by occurrence. Full list (incl. informational) in Appendix B and `private evidence dataset`.

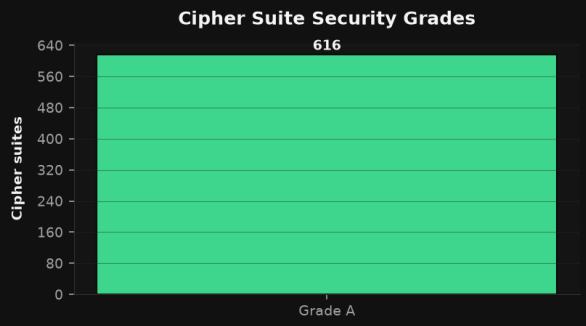
TLS/SSL Security Posture

91
EXCELLENT

Synthesised from nmap ssl-enum-ciphers, Shodan certificate data, and nuclei SSL templates. Identifies expired/self-signed certificates, deprecated protocols (TLS 1.0/1.1), weak cipher suites, and HTTP-only hosts missing HTTPS.

20 HOSTS WITH TLS	**0** EXPIRED CERTS	**0** SELF-SIGNED
2 WEAK PROTOCOLS	**0** WEAK CIPHERS	**90/100** RISK SCORE · HIGHER = WORSE (CRITICAL)





Summary

20 host(s) with TLS detected across the attack surface. 2 host(s) serve deprecated TLS protocols (1.0/1.1). 17 host(s) are on shared IPs where the default certificate belongs to a different domain (CN mismatch). 1 host(s) serve HTTP without detected TLS.

TLS Findings

HOST(S)	IP	HOSTS	AFFECTED PORTS	SEVERITY	ISSUE
asset-143.acmesample.com (+1 more)	192.0.2.27	**2**	443	HIGH	**TLSv1.0 enabled**
asset-143.acmesample.com (+1 more)	192.0.2.27	**2**	443	MEDIUM	**TLSv1.1 enabled**
asset-059.acmesample.com	192.0.2.10	**1**	443	MEDIUM	**Nmap cipher warning**
asset-146.acmesample.com	192.0.2.49	**1**	443	MEDIUM	**Nmap cipher warning**
asset-049.acmesample.com	192.0.2.63	**1**	80	INFO	**HTTP-only host (no TLS detected)**

Certificate Inventory

Showing top 15 certificates by expiry urgency. Complete inventory with all 26 hosts available in `private evidence dataset`.

HOST	CN	ISSUER	EXPIRES	DAYS	STATUS
asset-168.acmesample.com	*.acmesample.com	GoDaddy.com, Inc.	2026-12-22	**111**	VALID
asset-166.acmesample.com	outlook.com	DigiCert Inc	2027-01-10	**130**	VALID
asset-166.acmesample.com	outlook.com	DigiCert Inc	2027-01-10	**130**	VALID
asset-166.acmesample.com	outlook.com	DigiCert Inc	2027-01-10	**130**	VALID
asset-166.acmesample.com	outlook.com	DigiCert Inc	2027-01-10	**130**	VALID
asset-166.acmesample.com	outlook.com	DigiCert Inc	2027-01-10	**130**	VALID
asset-166.acmesample.com	outlook.com	DigiCert Inc	2027-01-10	**130**	VALID
asset-166.acmesample.com	outlook.com	DigiCert Inc	2027-01-10	**130**	VALID

HOST	CN	ISSUER	EXPIRES	DAYS	STATUS
asset-142.acmesample.com	*.acmesample.com	GoDaddy.com, Inc.	2026-12-22	**111**	VALID
www.acmesample.com	*.acmesample.com	GoDaddy.com, Inc.	2026-12-22	**111**	VALID
asset-141.acmesample.com	*.acmesample.com	GoDaddy.com, Inc.	2026-12-22	**111**	VALID
asset-146.acmesample.com	asset-146.acmesample.com	Let's Encrypt	2026-10-30	**57**	VALID
asset-169.acmesample.com	*.acmesample.com	GoDaddy.com, Inc.	2026-12-22	**111**	VALID
asset-059.acmesample.com	asset-059.acmesample.com	Let's Encrypt	2026-10-30	**57**	VALID
asset-170.acmesample.com	*.acmesample.com	GoDaddy.com, Inc.	2026-12-22	**111**	VALID

… and 11 more certificates (see `private evidence dataset` omitted from this public sample)

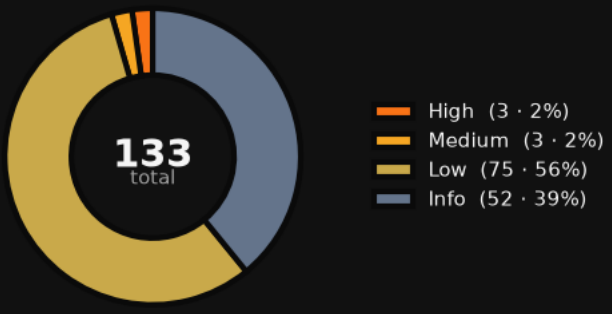
Web Application Security

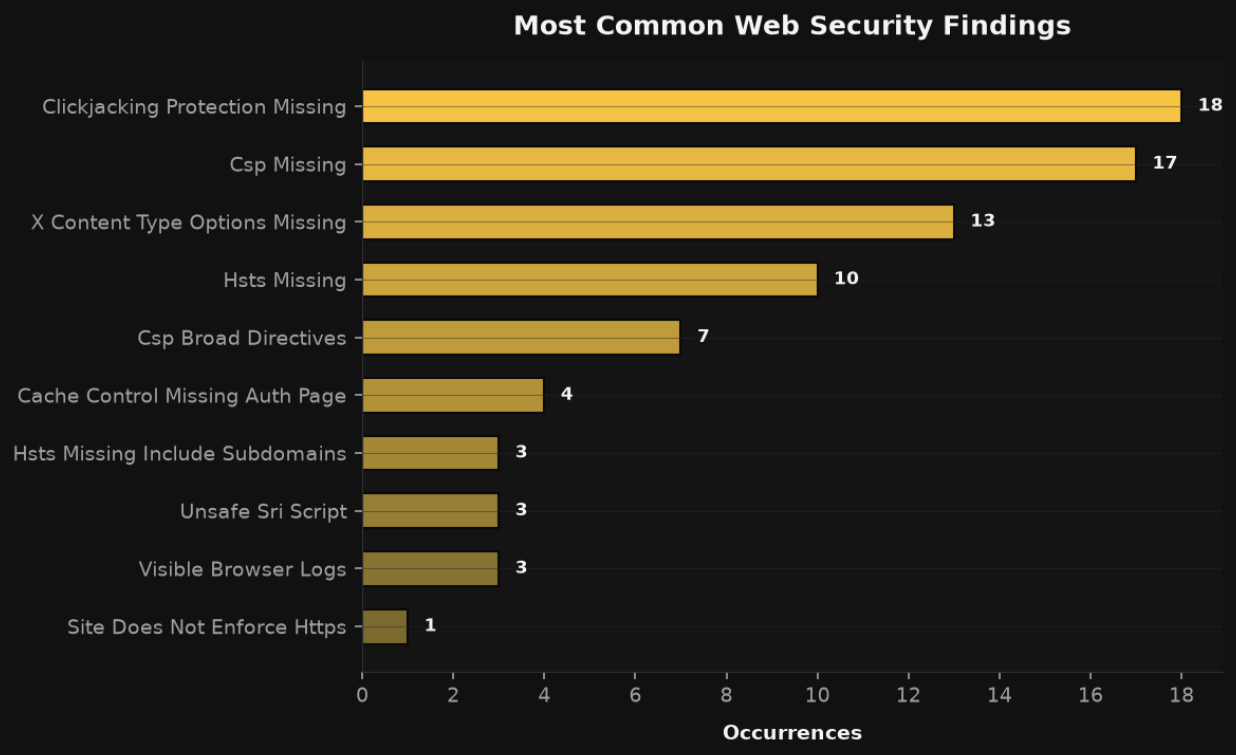
74
FAIR

Evaluates externally reachable web endpoints for non-intrusive HTTP security weaknesses using safe GET requests, redirect analysis, response header inspection, Set-Cookie analysis, and passive HTML parsing. Does not attempt exploitation, login, fuzzing, or payload injection.

74/100 SECURITY SCORE (FAIR)	**48** URLS SCANNED	**33** URLS WITH FINDINGS
3 HIGH SEVERITY	**3** MEDIUM SEVERITY	**75** LOW SEVERITY

Web App Findings by Severity





Summary

Web application security posture for acmesample.com was assessed across 48 URL(s), yielding an overall score of 74/100 (fair). 3 high-severity finding(s) were identified, including issues with session cookie security and/or insecure redirect chains. 3 medium-severity issue(s) require attention. 75 low-severity configuration weaknesses were noted (missing headers, weak CSP/HSTS settings).

Host Security Scores

HOST	SCORE	HIGH	MEDIUM	LOW	RATING
asset-064.acmesample.com	**61/100**	0	3	1	FAIR
www.acmesample.com	**70/100**	1	0	3	FAIR
asset-188.acmesample.com	**70/100**	1	0	3	FAIR
asset-143.acmesample.com	**70/100**	1	0	3	FAIR
192.0.2.68	**78/100**	0	0	8	GOOD
asset-065.acmesample.com	**82/100**	0	0	7	GOOD

HOST	SCORE	HIGH	MEDIUM	LOW	RATING
asset-134.acmesample.com	**85/100**	0	0	5	GOOD
asset-148.acmesample.com	**88/100**	0	0	4	GOOD
asset-142.acmesample.com	**88/100**	0	0	4	GOOD
asset-168.acmesample.com	**88/100**	0	0	4	GOOD

High-Risk Web Security Findings

HOST	CHECK	SEVERITY	EVIDENCE
www.acmesample.com	Unsafe Sri Script	HIGH	External script from hs-scripts.com lacks SRI integrity attribute
asset-188.acmesample.com	Unsafe Sri Script	HIGH	External script from hs-scripts.com lacks SRI integrity attribute
asset-064.acmesample.com	Insecure Https Redirect Pattern	MEDIUM	HTTP redirect to external domain microsoft.com
asset-064.acmesample.com	Csp Broad Directives	MEDIUM	CSP has 3 broad directive(s)
asset-064.acmesample.com	Csp Unsafe Directives	MEDIUM	CSP uses 1 unsafe directive(s)
asset-143.acmesample.com	Unsafe Sri Script	HIGH	External script from hs-scripts.com lacks SRI integrity attribute

Most Common Findings

CHECK	OCCURRENCES
Clickjacking Protection Missing	18
Csp Missing	17
X Content Type Options Missing	13
Hsts Missing	10
Csp Broad Directives	7
Cache Control Missing Auth Page	4
Hsts Missing Include Subdomains	3
Unsafe Sri Script	3
Visible Browser Logs	3
Site Does Not Enforce Https	1

Methodology. This chapter evaluates externally reachable web endpoints for non-intrusive HTTP security weaknesses using safe GET/HEAD requests, redirect analysis, response header inspection, Set-Cookie analysis, and passive HTML parsing. It does not attempt exploitation, login, fuzzing, or payload injection. Checks cover session cookie security, HTTPS enforcement, Content Security Policy, HSTS, clickjacking protection, subresource integrity, and more.

INFRASTRUCTURE

Port & Service Analysis

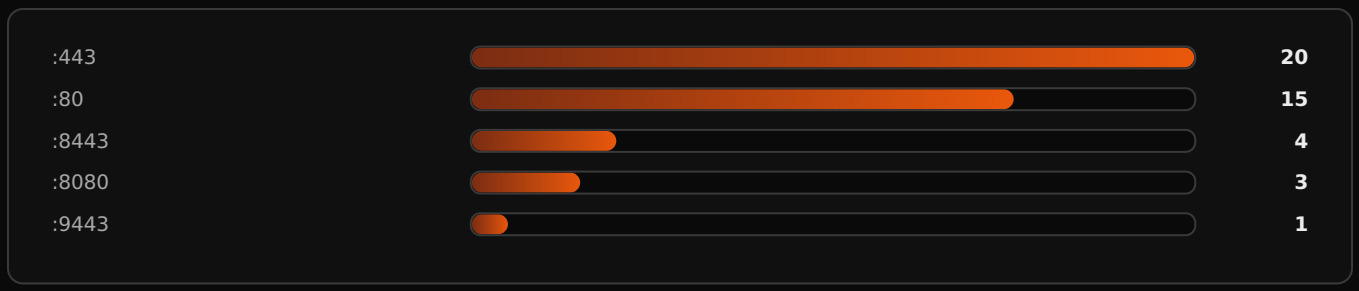
64
FAIR

Open ports are detected through a combination of **passive intelligence** (Shodan, Netlas, and ZoomEye continuously scan the internet and report open ports without touching the target) and **optional active scanning** (Nmap). Passive sources provide broad coverage but may report slightly stale data; active scanning confirms the current state.

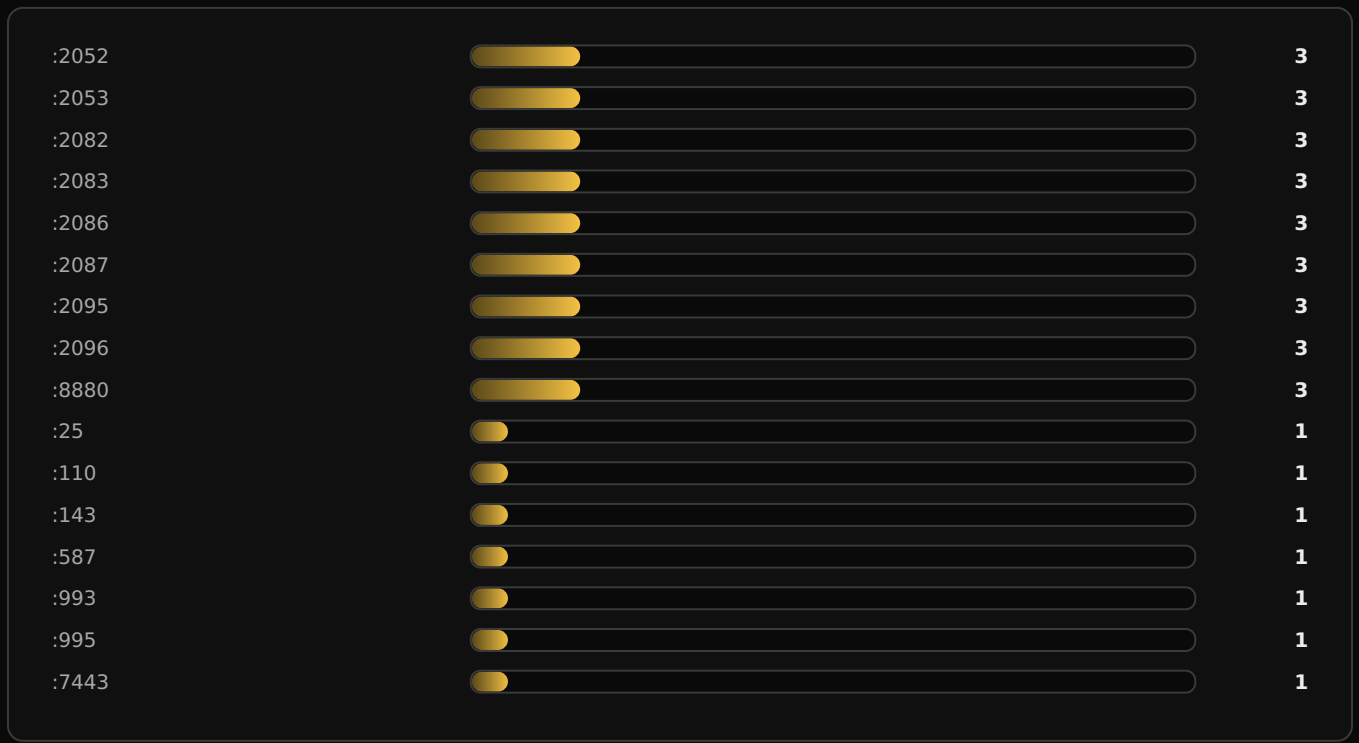
Coverage note: Active port scanning was enabled. Nmap verified all passively-discovered ports with service version detection (-sV) and scanned the top 100 TCP ports on hosts with no prior port data.

23 unique ports across **22** hosts.

Web-facing (typical)

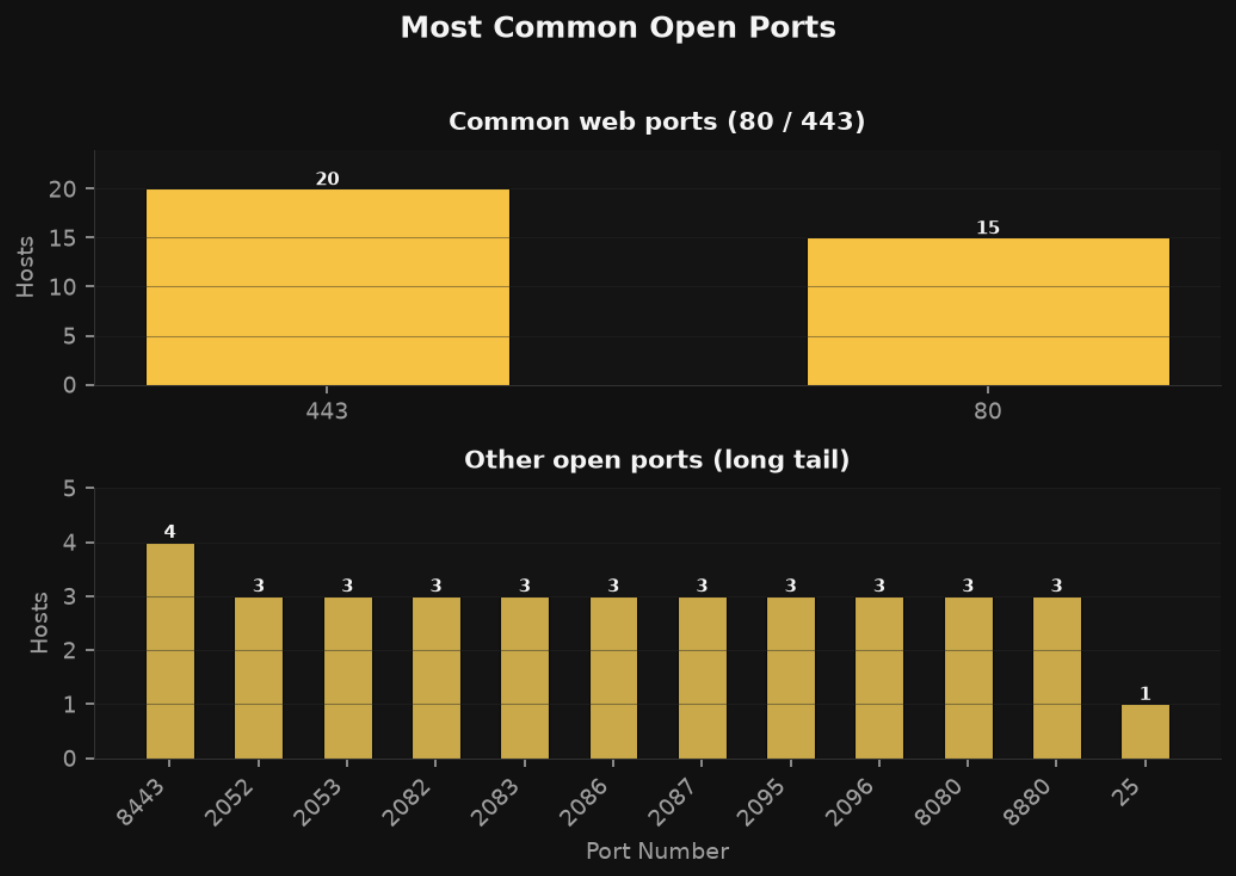


Other services (long tail)



Bars share one scale (max count across both groups).

All ports — top counts (chart)



SERVICE	HOSTS
http/Cloudflare http proxy	21
http/nginx	12
http/Microsoft Azure Application Gateway	11
upnp/Microsoft IIS httpd	4
https/cloudflare	3
https-alt/cloudflare	3
http	3
https	3
http/Microsoft HTTPAPI httpd	3
smtp	1
submission	1
http/sfdcedge	1

Internet-Exposed Backend Services

The following ports host **backend services** (databases, message brokers, management interfaces) that should **not be reachable from the public internet**. These services are designed for internal network access only — exposing them increases the risk of data exfiltration, brute-force attacks, and lateral movement. Each should be placed behind a firewall or VPN. For a detailed per-host breakdown, see `private evidence dataset` omitted from this public sample.

PORT	SERVICE	RISK	HOSTS	REASON
:8443	Plesk HTTPS	LOW	4	Hosting admin panel (HTTPS)
:2082	cPanel HTTP	MEDIUM	3	Hosting admin panel — brute-force if no IP restriction
:2083	cPanel HTTPS	MEDIUM	3	Hosting admin panel — brute-force if no IP restriction
:2086	WHM HTTP	HIGH	3	Server management panel — full server control if compromised
:2087	WHM HTTPS	HIGH	3	Server management panel — full server control if compromised
:2095	cPanel Webmail	MEDIUM	3	Webmail — credential brute-force vector

PORT	SERVICE	RISK	HOSTS	REASON
:8880	Plesk HTTP	MEDIUM	3	Hosting admin panel

Hosts with Unusual Ports

Unusual ports are any open TCP/UDP ports that fall **outside the standard set** of common internet services (HTTP/80, HTTPS/443, SSH/22, DNS/53, SMTP/25, FTP/21, etc.). The presence of unusual ports may indicate development servers, management interfaces, legacy applications, or misconfigured services — all of which expand the attack surface and warrant investigation.

HOST	IP	UNUSUAL PORTS	RISK
asset-047.acmesample.com	192.0.2.178	2052, 2053, 2082, 2083, 2086, 2087, 2095, 2096, 8880	6
asset-062.acmesample.com	192.0.2.178	2052, 2053, 2082, 2083, 2086, 2087, 2095, 2096, 8880	6
asset-071.acmesample.com	192.0.2.179	2052, 2053, 2082, 2083, 2086, 2087, 2095, 2096, 8880	6
portal.acmesample.com	192.0.2.137	7443, 9443, 10443	4
remote.acmesample.com	192.0.2.182	179	1

Sensitive Subdomains

Hostnames are analyzed for patterns that suggest sensitive or high-value systems. The scanner checks for **9** hostname patterns across 9 categories: administration panels (admin, backend, cpanel), development/staging environments (dev, staging, qa, sandbox), internal infrastructure (intranet, vpn, gateway), databases (mysql, redis, elastic), monitoring systems (grafana, prometheus, kibana), CI/CD infrastructure (jenkins, gitlab, docker-registry), authentication services (auth, sso, oauth), storage/backup systems, and legacy/migration endpoints. These systems are frequently the first targets in penetration tests and real-world attacks.

Sensitive Subdomain Categories

CATEGORY	HOSTS
Development & Staging	**3**

Sensitive Hosts (Top 9)

HOSTNAME	IP	CATEGORY	PORTS	RISK
asset-141.acmesample.com	192.0.2.45	Development & Staging	**1**	**6**
asset-168.acmesample.com	192.0.2.11	Other	**1**	**6**
asset-059.acmesample.com	192.0.2.10	Development & Staging	**2**	**1**
asset-064.acmesample.com	192.0.2.78	Other	**2**	**1**
asset-065.acmesample.com	192.0.2.66	Other	**2**	**1**
asset-148.acmesample.com	192.0.2.43	Development & Staging	**2**	**1**
asset-153.acmesample.com	192.0.2.184	Other	**0**	**1**
asset-169.acmesample.com	192.0.2.15	Other	**1**	**1**
asset-170.acmesample.com	192.0.2.15	Other	**1**	**1**

Authentication Surface

Authentication endpoints — SSO portals, VPN gateways, firewall panels, and remote access systems — are high-value targets. Compromising a single identity provider can grant access to all connected services. This section identifies all authentication-related systems in the attack surface.

1	1	0
AUTH ENDPOINTS	UNIQUE TYPES	HIGH CONFIDENCE

Authentication Surface by Type

SURFACE TYPE	COUNT
VPN Gateways	1

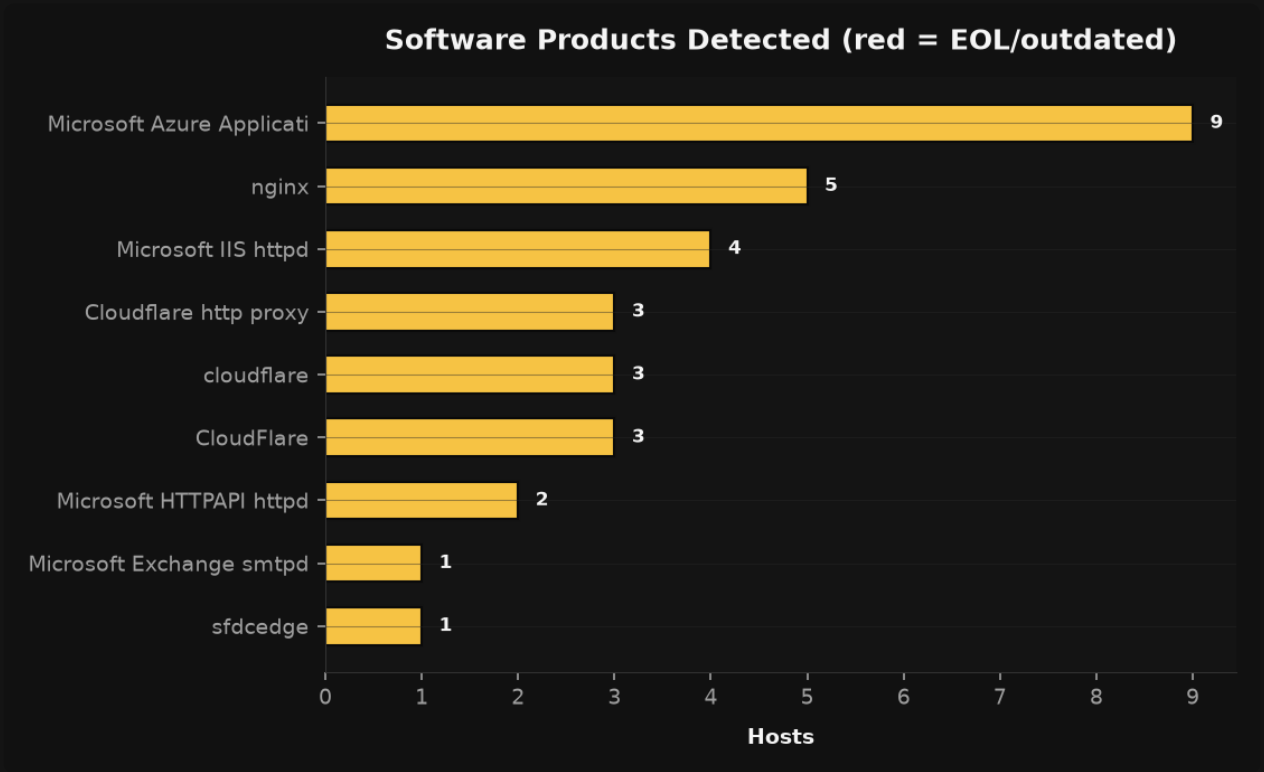
Detected Authentication Endpoints

HOSTNAME	IP	SURFACE TYPE	TECHNOLOGY	CONFIDENCE
remote.acmesample.com	192.0.2.182	VPN Gateways	Hostname pattern	medium

Software Version Risk

Software versions detected via nmap service scanning and Shodan CPE data are checked against known end-of-life (EOL) databases. Outdated software with known CVEs represents immediate patching priorities.

9	0	2
UNIQUE PRODUCTS	END-OF-LIFE	WITH KNOWN CVES



All Detected Products (Top 30)

PRODUCT	TOP VERSION	HOSTS	CVES	STATUS
Microsoft Azure Application Gateway	v2	9	0	CURRENT
nginx	—	5	60	NO VERSION
Microsoft IIS httpd	10.0	4	0	CURRENT
Cloudflare http proxy	—	3	0	NO VERSION

PRODUCT	TOP VERSION	HOSTS	CVES	STATUS
cloudflare	—	3	3	NO VERSION
CloudFlare	—	3	0	NO VERSION
Microsoft HTTPAPI httpd	2.0	2	0	CURRENT
Microsoft Exchange smtpd	—	1	0	NO VERSION
sfdcedge	—	1	0	NO VERSION

Attack Path & Pivot Risk Analysis

This section identifies potential lateral movement paths based on network co-location analysis. When hosts serving different business functions (e.g., development and production) share the same IP address or /24 subnet, attackers who compromise the less-secured system can potentially pivot to the more critical one.

1	1	0
CRITICAL PATHS	TOTAL PATHS	SINGLE POINTS OF FAILURE

Identified Attack Paths

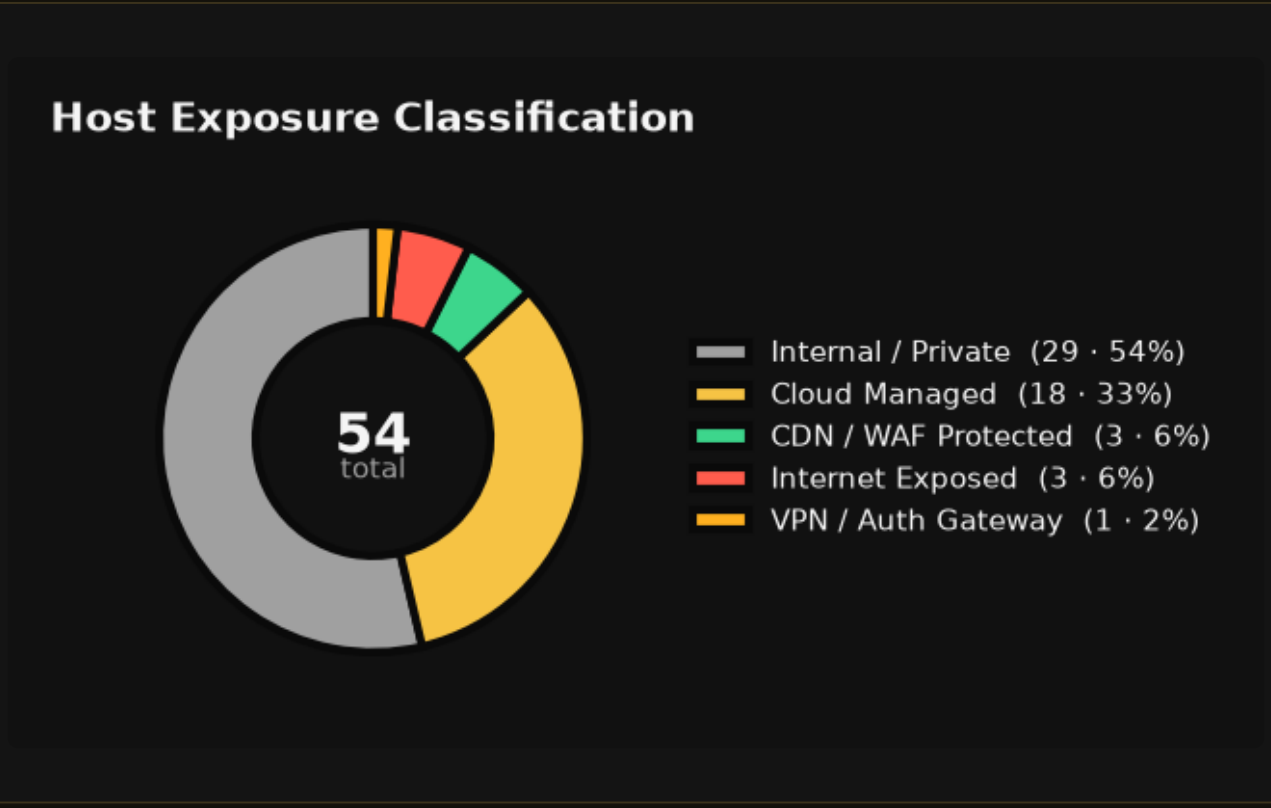
SOURCE HOST	TARGET HOST	PATH TYPE	PROXIMITY	RISK
asset-168.acmesample.com	www.acmesample.com	Development → Production	SAME IP	10

Exposure Classification

Each discovered host is classified by exposure type based on hosting provider, RDAP data, Shodan intelligence, and hostname patterns. This helps distinguish directly internet-exposed systems from those protected by CDN/WAF, managed in cloud platforms, or served by third-party SaaS providers.

3	3	18
INTERNET EXPOSED	CDN / WAF PROTECTED	CLOUD MANAGED

0	1	29
THIRD-PARTY SAAS	VPN / AUTH GATEWAY	INTERNAL / PRIVATE



Directly Internet-Exposed Hosts (Top 30)

HOSTNAME	IP	EXPOSURE TYPE	EVIDENCE
asset-153.acmesample.com	192.0.2.184	INTERNET EXPOSED	Acme Sample GmbH

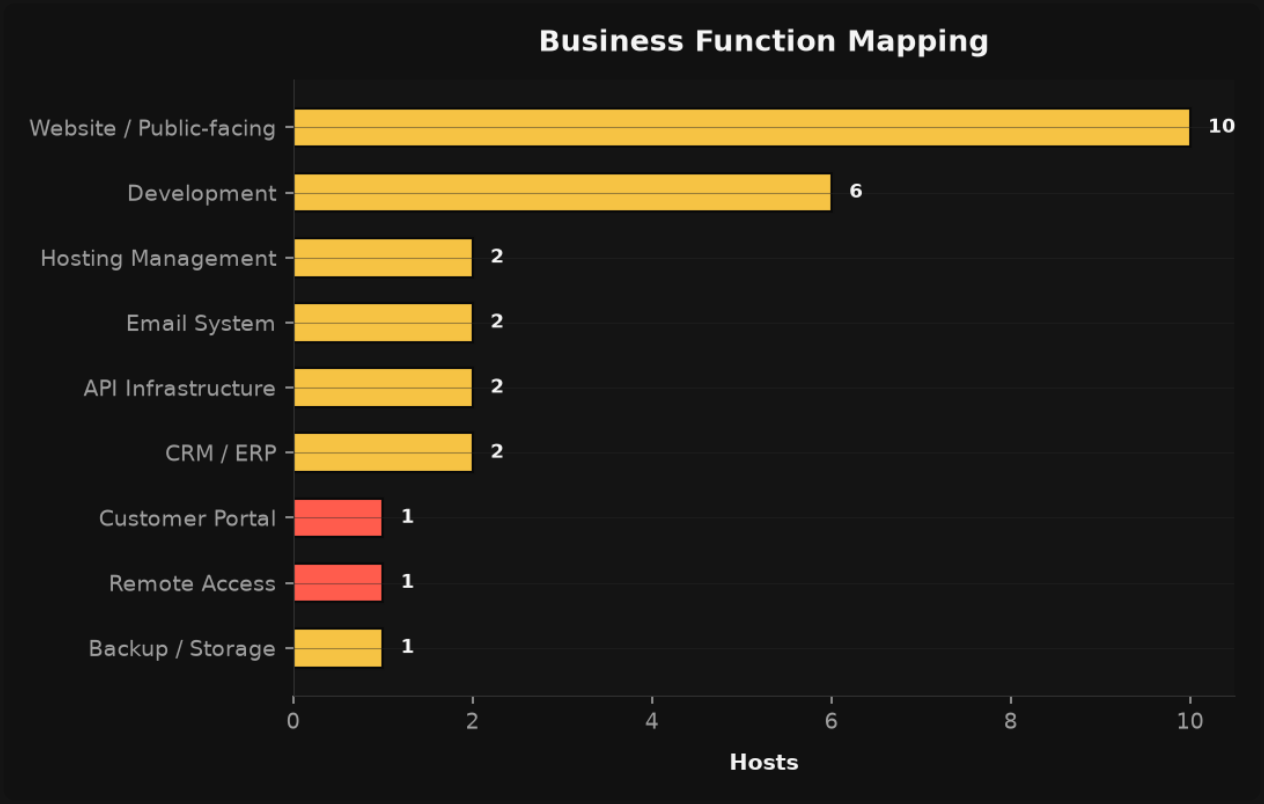
Business Impact Mapping

Discovered hosts are mapped to business functions based on hostname patterns. This classification helps prioritize remediation by identifying which critical business systems are exposed to the internet.

12
CRITICAL SYSTEMS

9
HIGH-IMPACT SYSTEMS

6
MEDIUM-IMPACT SYSTEMS



Business-Critical Hosts

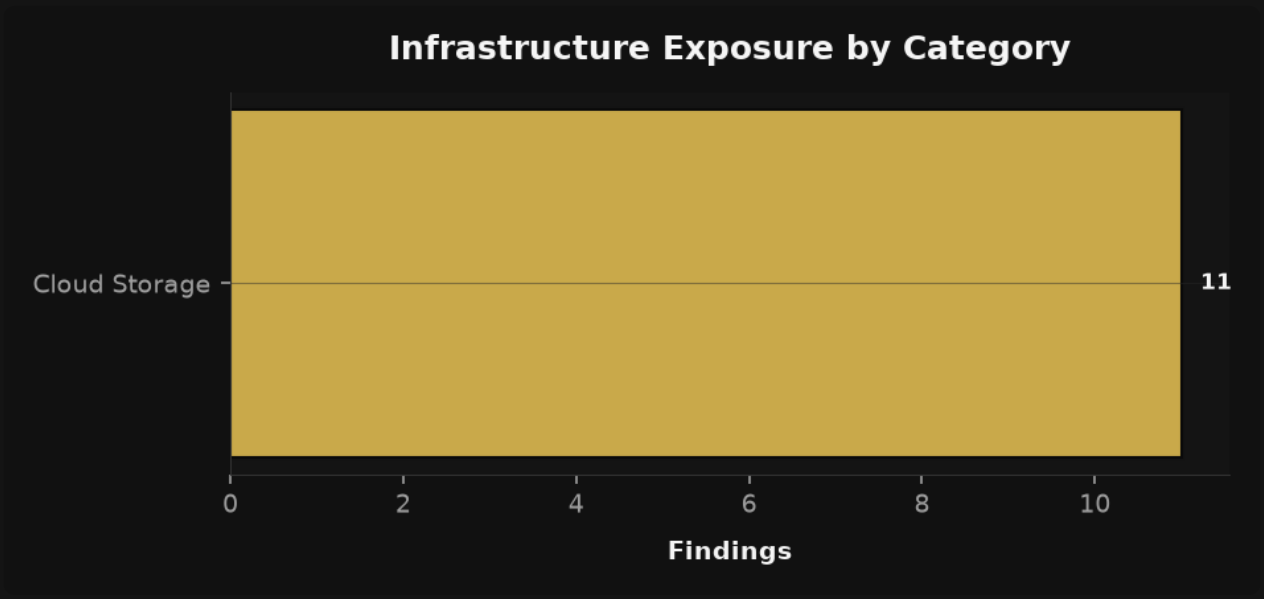
HOSTNAME	IP	BUSINESS FUNCTION	CRITICALITY	PORTS	RISK
asset-047.acmesample.com	192.0.2.178	Website / Public-facing	CRITICAL	13	6
asset-071.acmesample.com	192.0.2.179	Website / Public-facing	CRITICAL	13	6
asset-166.acmesample.com	192.0.2.75	Website / Public-facing	CRITICAL	8	6

HOSTNAME	IP	BUSINESS FUNCTION	CRITICALITY	PORTS	RISK
asset-143.acmesample.com	192.0.2.27	Website / Public-facing	CRITICAL	2	5
www.acmesample.com	192.0.2.11	Website / Public-facing	CRITICAL	1	5
asset-188.acmesample.com	192.0.2.27	Website / Public-facing	CRITICAL	2	5
portal.acmesample.com	192.0.2.137	Customer Portal	CRITICAL	6	4
remote.acmesample.com	192.0.2.182	Remote Access	CRITICAL	1	1
asset-049.acmesample.com	192.0.2.63	Website / Public-facing	CRITICAL	1	0
asset-134.acmesample.com	192.0.2.65	Website / Public-facing	CRITICAL	2	0
asset-146.acmesample.com	192.0.2.49	Website / Public-facing	CRITICAL	2	0
asset-174.acmesample.com	192.0.2.61	Website / Public-facing	CRITICAL	0	0
asset-062.acmesample.com	192.0.2.178	Email System	HIGH	13	6
asset-141.acmesample.com	192.0.2.45	API Infrastructure	HIGH	1	6
asset-142.acmesample.com	192.0.2.13	API Infrastructure	HIGH	1	5
asset-064.acmesample.com	192.0.2.78	CRM / ERP	HIGH	2	1
asset-065.acmesample.com	192.0.2.66	CRM / ERP	HIGH	2	1
asset-152.acmesample.com	192.0.2.33	Backup / Storage	HIGH	2	0
asset-168.acmesample.com	192.0.2.11	Development	MEDIUM	1	6
asset-059.acmesample.com	192.0.2.10	Development	MEDIUM	2	1
asset-148.acmesample.com	192.0.2.43	Development	MEDIUM	2	1
asset-169.acmesample.com	192.0.2.15	Development	MEDIUM	1	1
asset-170.acmesample.com	192.0.2.15	Development	MEDIUM	1	1

Cloud & Infrastructure Exposure

Infrastructure components detected through admin panel analysis, nuclei verification, and open port scanning. Exposed databases, container orchestration, CI/CD pipelines, and monitoring systems represent high-value targets for attackers.

11
CLOUD STORAGE



Infrastructure Findings

HOST	IP	CATEGORY	TYPE	SOURCE	SEVERITY
		Cloud Storage	11 exposed files	Cloud Exposure Scan	HIGH

Breaches Mentioning Your Servers

Our breach database was searched for all confirmed hostnames (FQDNs) discovered during this assessment. When a server hostname appears in breach data, it means that some record — such as a URL, login form, or user credential — references that server. **This does not necessarily mean the server itself was compromised.** Common explanations include:

- Users whose devices were infected with stealer malware had their browser-saved credentials for these servers captured and leaked
- Public databases or aggregated breach compilations that index URLs and login endpoints
- Third-party services that reference your infrastructure in their data

Servers with a high number of credential-type breach records deserve immediate attention, as they indicate that login credentials for those systems are actively circulating in threat actor channels.

How this compares to the wider breach exposure: the chapter below covers **17** breach records that explicitly reference one of your discovered server hostnames. The Leaked Credential Exposure chapter shows **2,038** breach records mentioning your domain in any field (URLs, emails, hashes, attachments) — a broader measure of how often your organisation appears in breach corpora. The server-specific number is a strict subset.

1
SERVERS IN BREACHES

26
SERVERS SEARCHED

17
SERVER-REFERENCE RECORDS
subset of 2,038 domain-wide

50
UNIQUE BREACH SOURCES

www.acmesample.com 192.0.2.11

17 records **17** breaches **1** credentials **1** emails **16** URLs

log (7) url (15) hash (7) name (8) email (16)

2021-08-18 — 2026-07-15 · CVSS avg 7.0

Server Breach Details

HOSTNAME	IP	RE-CORDS	BREACHES	CREDS	TOP DATA TYPES	DATE RANGE
www.acmesample.com	192.0.2.11	**17**	**17**	**1**	log, url, hash	2021-08-18 — 2026-07-15

THREAT LANDSCAPE

IP Reputation & Threat Intelligence

Each unique IP address in the attack surface is checked against multiple threat intelligence feeds: TOR exit node lists, the Spamhaus DROP (Don't Route Or Peer) list of criminal-controlled networks, AbuseIPDB abuse reports, AlienVault OTX threat pulses, and the C99 malicious IP database. Results are cached for 30 days to minimize API calls on repeat scans.

22	0	0
IPS CHECKED	TOR EXIT NODES	ON SPAMHAUS DROP
0	**4**	**0**
ABUSE REPORTS	IN THREAT FEEDS	C99 MALICIOUS

Summary

Checked 22 IPs. Flagged: 4 in threat feeds.

Flagged IPs (Top 30)

IP ADDRESS	HOSTNAMES	TOR	SPAMHAUS DROP	ABUSEIP-DB	OTX PULSES	C99
192.0.2.75	asset-166.acm…	—	Clean	0	6	Clean
192.0.2.178	asset-047.acm…	—	Clean	0	50	Clean
192.0.2.65	asset-134.acm…	—	Clean	15	3	Clean
192.0.2.179	asset-071.acm…	—	Clean	2	50	Clean

Code Exposure Analysis

82
GOOD

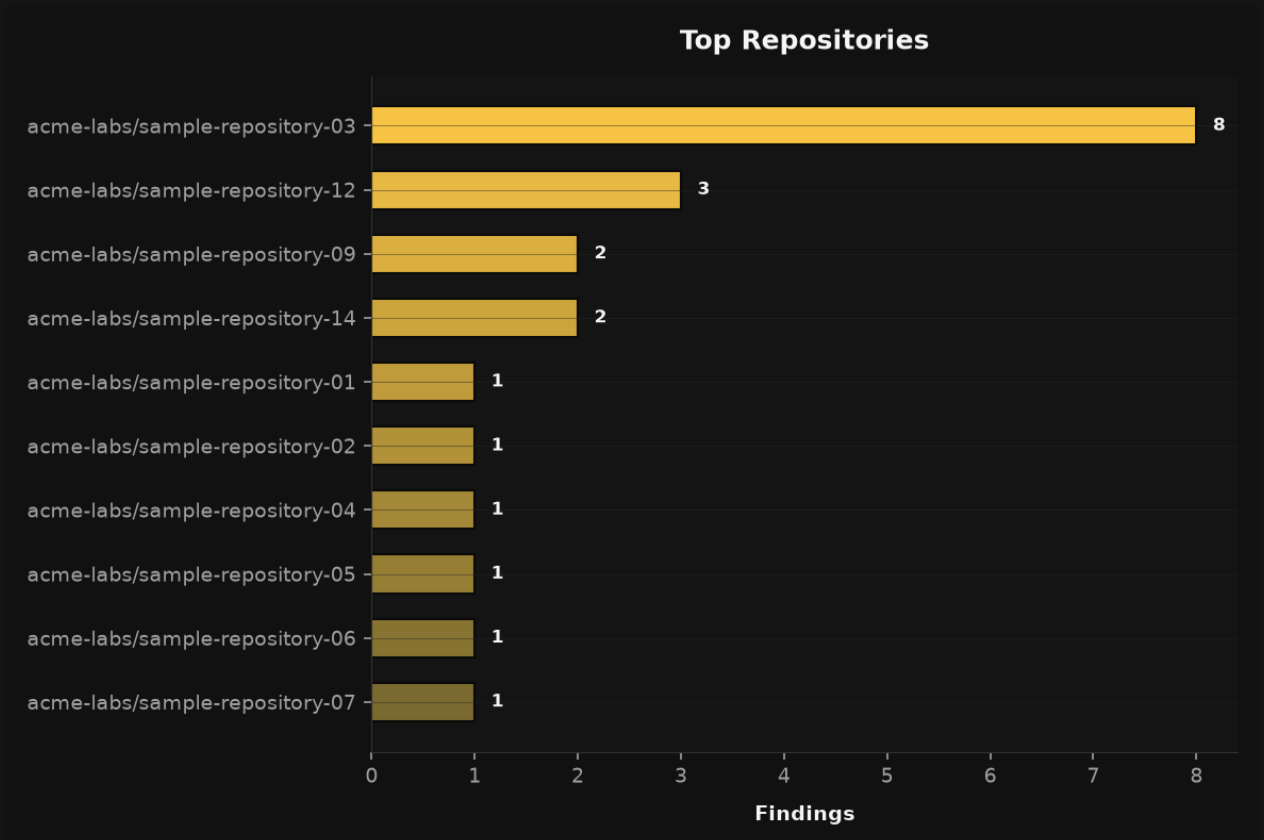
Searches GitHub repositories and Gists for exposed source code, secrets, API keys, and sensitive data mentioning **acmesample.com**. Each finding is scored 0-10 for risk by AI analysis and scanned against 150+ secret-detection patterns.

26	0	0
Total Findings	High Risk (7-10)	Medium Risk (4-6)

26
Low / Info

Summary

26 anonymized code-exposure findings were retained. Repository names, file paths, snippets, and third-party identities were replaced for this public sample.



Top Repositories by Finding Count

Top Findings

acme-labs/sample-repository-01 data/private evidence dataset **3/10**

```
# Anonymized public-code excerpt 01
TARGET_DOMAIN = "acmesample.com"
```

A public repository referenced the sample organization. The original excerpt and third-party identities were removed from this marketing copy.

acme-labs/sample-repository-02 src/sample-config-02.py **2/10**

```
# Anonymized public-code excerpt 02
TARGET_DOMAIN = "acmesample.com"
```

A public repository referenced the sample organization. The original excerpt and third-party identities were removed from this marketing copy.

acme-labs/sample-repository-03 data/private evidence dataset **1/10**

```
# Anonymized public-code excerpt 03
TARGET_DOMAIN = "acmesample.com"
```

A public repository referenced the sample organization. The original excerpt and third-party identities were removed from this marketing copy.

acme-labs/sample-repository-03 data/private evidence dataset **1/10**

```
# Anonymized public-code excerpt 04
TARGET_DOMAIN = "acmesample.com"
```

A public repository referenced the sample organization. The original excerpt and third-party identities were removed from this marketing copy.

acme-labs/sample-repository-04 src/sample-config-05.py **1/10**

```
# Anonymized public-code excerpt 05
TARGET_DOMAIN = "acmesample.com"
```

A public repository referenced the sample organization. The original excerpt and third-party identities were removed from this marketing copy.

Showing top 5 of 26 findings. The complete list is omitted from this public sample.

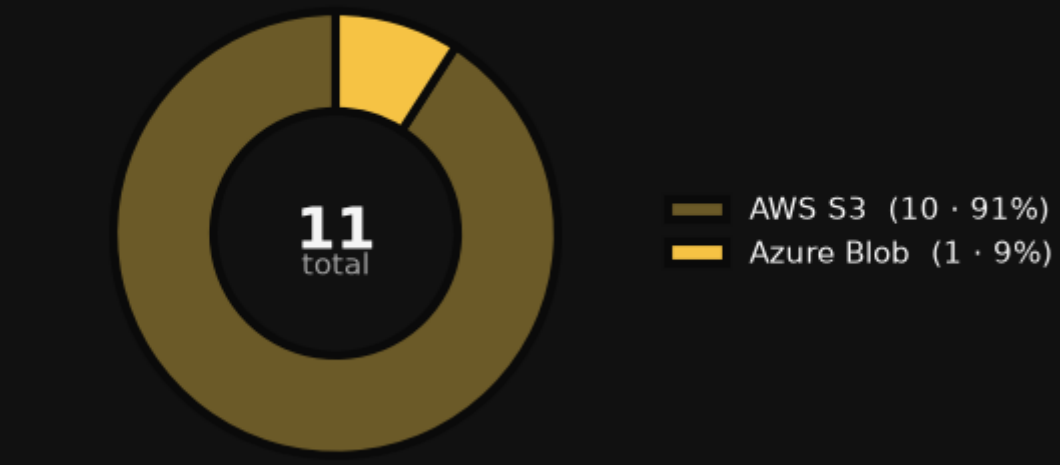
Cloud Storage Exposure

Exposed files discovered in public cloud storage buckets (AWS S3, Azure Blob Storage, Google Cloud Storage) matching the organization name.

11	7	2
FILES FOUND	SENSITIVE FILES	CLOUD PROVIDERS

Summary

11 files found in exposed cloud storage buckets. 7 are security-sensitive (configs, databases, archives, scripts). Cloud providers: AWS S3 (10), Azure Blob (1).



Exposed Files

FILE URL	PRO-VIDER	EXT	SIZE	SENSITIVE
https://sample-storage.invalid/redacted/sample-file-001.dat	AWS S3	pdf	**9214.4 KB**	—
https://sample-storage.invalid/redacted/sample-file-002.dat	AWS S3	pdf	**596.6 KB**	—
https://sample-storage.invalid/redacted/sample-file-003.dat	Azure Blob	pdf	**570.0 KB**	—
https://sample-storage.invalid/redacted/sample-file-004.dat	AWS S3	pdf	**223.1 KB**	—
https://sample-storage.invalid/redacted/sample-file-005.dat	AWS S3	xml	**0.3 KB**	DATA/ CONFIGURATION FILE
https://sample-storage.invalid/redacted/sample-file-006.dat	AWS S3	xml	**0.3 KB**	DATA/ CONFIGURATION FILE
https://sample-storage.invalid/redacted/sample-file-007.dat	AWS S3	xml	**0.3 KB**	DATA/ CONFIGURATION FILE
https://sample-storage.invalid/redacted/sample-file-008.dat	AWS S3	emb	**85.5 KB**	
https://sample-storage.invalid/redacted/sample-file-009.dat	AWS S3	emb	**84.5 KB**	
https://sample-storage.invalid/redacted/sample-file-010.dat	AWS S3		**81.1 KB**	
https://sample-storage.invalid/redacted/sample-file-011.dat	AWS S3	info	**0.2 KB**	

Shortened URL Exposure

Shortened URLs (goo.gl, bit.ly, tinyurl, ow.ly, etc.) that point to or reference the scanned domain. These links reveal internal resources shared externally, sensitive documents, and potential brand impersonation domains.

3,000	0	1	0
TOTAL LINKS	INTERNAL RESOURCES	NON-HTML FILES	PHISHING DOMAINS

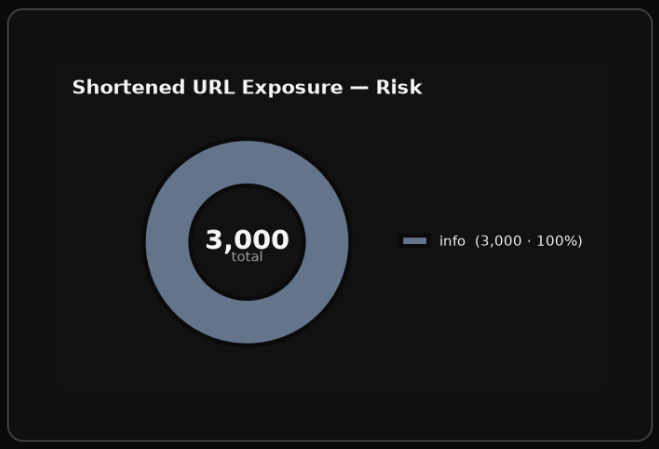
The headline counters summarize every valid link returned and classified by the scan. Detailed finding records are persisted for at most **5,000 links**. The PDF tables are smaller presentation samples, and `private evidence dataset` contains only the persisted findings that remain after any report exclusions; rows beyond the persistence cap are not available as detailed evidence.

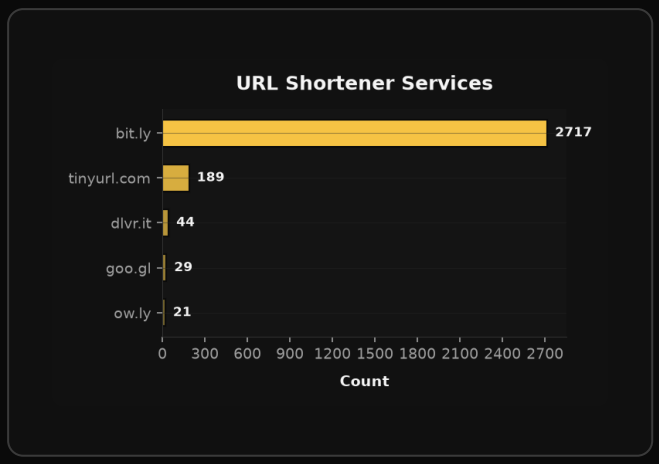
Summary

3000 shortened URLs found pointing to or referencing acmesample.com. 1 point directly to own-domain resources. 1 link to non-HTML files (PDFs, documents, archives).

Why shortened URLs matter for security
URL shorteners hide the true destination, making them popular for sharing internal resources (SharePoint, Google Drive, Dropbox). When employees share shortened links publicly, these internal resources become discoverable. Embedded access tokens in shortened URLs may still be valid, granting direct access to corporate files. Phishing campaigns also use shortened URLs with brand-similar domains to bypass email filters.

1	2,999
OWN-DOMAIN LINKS	THIRD-PARTY REFERENCES


Shortened URL Exposure — Risk
3,000
total
info (3,000 · 100%)


URL Shortener Services
bit.ly
tinyurl.com
dlvr.it
goo.gl
ow.ly
2717
189
44
29
21
0 300 600 900 1200 1500 1800 2100 2400 2700
Count

Social Media Exposure

80
GOOD

Brand exposure analysis across YouTube, Twitter/X, Facebook, LinkedIn, Reddit, and Google-indexed social platforms. Findings include brand impersonation detection, fake profiles, and phishing mentions.

192
TOTAL FINDINGS

3
OFFICIAL PROFILES

1
IMPERSONATION RISKS

0
PHISHING MENTIONS

192 social media mentions analyzed across **7** platforms. **3** classified as actionable risks, **112** as unrelated brand-name matches, **80** as official or benign.

Verified Official Channels

Official social media profiles identified from the company's website metadata, DNS records, structured data, and social media scanning. These are **excluded** from impersonation findings below.

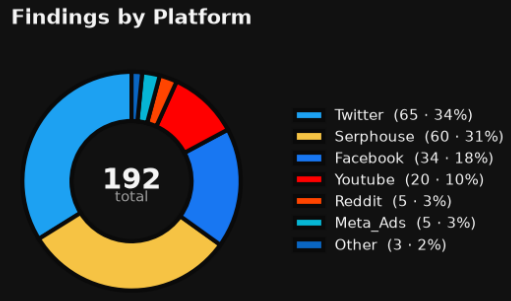
PLAT-FORM	HANDLE / NAME	URL	SOURCE
Twitter	Acme Sample GmbH	https://x.com/Acme Sample GmbH	Company metadata
Facebook	Acme Sample GmbH	https://facebook.com/Acme Sample G...	Company metadata
Linkedin	company/Acme Sample GmbH	https://linkedin.com/company/Acme S...	Company metadata
Youtube	Sample public mention of Acme Sample GmbH; original account and copy anonymized.	https://social.invalid/sample-account-...	Social media scan

Summary

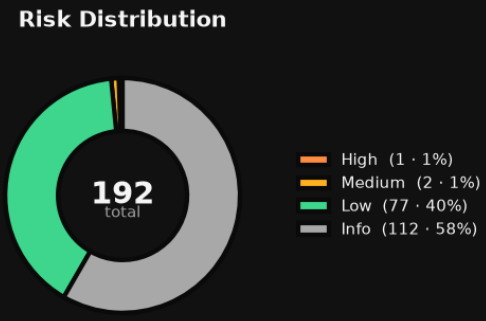
Found 192 social media mentions for acmesample.com across 7 platforms. 3 confirmed official profiles found. 1 potential brand impersonation risks detected.

AI Risk Assessment

The findings primarily consist of benign mentions and discussions about Acme Sample GmbH products across various platforms. There are no indications of critical or high-risk impersonation or fraudulent activity related to the brand.



Findings by Platform



Risk Distribution

Potentially Fraudulent Advertisement

Analysis of paid advertisements on LinkedIn Ad Library, Meta Ad Library, and TikTok Ad Library mentioning the brand. Ads are classified by threat level: phishing/scam ads that impersonate the brand, competitor ads exploiting the brand name, and legitimate/neutral advertisements. Classification confidence indicates how certain the AI assessment is about the assigned category.

> Classification retained from the source assessment; identifying account details were removed.

All 5 ads appear to be legitimate or official. No fraudulent advertisements were detected.

PLAT-FORM	ADVERT-ISER	AD CONTENT	RISK	CER-TAIN TY	CLASSIFICATION
Meta	Sample Account 670	Sample public mention of Acme Sample GmbH; original account and copy anonymized. — Sample public mention of Acme Sample GmbH; original account and...	LOW	85%	Classification retained from the source assessment;...
Meta	Sample Account 670	Sample public mention of Acme Sample GmbH; original account and copy anonymized. — Sample public mention of Acme Sample GmbH; original account and...	LOW	85%	Classification retained from the source assessment;...
Meta	Sample Account 304	Sample public mention of Acme Sample GmbH; original account and copy anonymized. — Sample public mention of Acme Sample GmbH; original account and...	LOW	85%	Classification retained from the source assessment;...
Meta	Sample Account 011	Sample public mention of Acme Sample GmbH; original account and copy anonymized. — Sample public mention of Acme Sample GmbH; original account and...	INFO	—	Classification retained from the source assessment;...
Meta	Sample Account 789	Sample public mention of Acme Sample GmbH; original account and copy anonymized. — Sample public mention of Acme Sample GmbH; original account and...	INFO	—	Classification retained from the source assessment;...

Twitter — 65 findings (2 medium, 55 low, 8 info)

RISK	TITLE	URL	REASON
MEDIUM	Sample public mention of Acme Sample GmbH; original account and copy anonymized.	https://social.invalid/sample-account...	Classification retained from the source assessment; identifying account...
MEDIUM	Sample public mention of Acme Sample GmbH; original account and copy anonymized.	https://social.invalid/sample-account...	Classification retained from the source assessment; identifying account...
LOW	Sample public mention of Acme Sample GmbH; original account and copy anonymized.	https://social.invalid/sample-account...	Classification retained from the source assessment; identifying account...
LOW	Sample public mention of Acme Sample GmbH; original account and copy anonymized.	https://social.invalid/sample-account...	Classification retained from the source assessment; identifying account...
LOW	Sample public mention of Acme Sample GmbH; original account and copy anonymized.	https://social.invalid/sample-account...	Classification retained from the source assessment; identifying account...

Showing top 5 of 65. Full evidence omitted from this public sample.

Serphouse — 60 findings (60 info)

RISK	TITLE	URL	REASON
INFO	Sample public mention of Acme Sample GmbH; original account and copy anonymized.	https://social.invalid/sample-account...	Classification retained from the source assessment; identifying account...
INFO	Sample public mention of Acme Sample GmbH; original account and copy anonymized.	https://social.invalid/sample-account...	Classification retained from the source assessment; identifying account...
INFO	Sample public mention of Acme Sample GmbH; original account and copy anonymized.	https://social.invalid/sample-account...	Classification retained from the source assessment; identifying account...
INFO	Sample public mention of Acme Sample GmbH; original account and copy anonymized.	https://social.invalid/sample-account...	Classification retained from the source assessment; identifying account...
INFO	Sample public mention of Acme Sample GmbH; original account and copy anonymized.	https://social.invalid/sample-account...	Classification retained from the source assessment; identifying account...

Showing top 5 of 60. Full evidence omitted from this public sample.

Facebook — 34 findings (1 high, 33 info)

All links relative to `https://social.invalid/`

RISK	TITLE	URL	REASON
HIGH	Sample public mention of Acme Sample GmbH; original account and copy anonymized.	../sample-account-0008	Classification retained from the source assessment; identifying account...
INFO	Sample public mention of Acme Sample GmbH; original account and copy anonymized.	../sample-account-0241	Classification retained from the source assessment; identifying account...
INFO	Sample public mention of Acme Sample GmbH; original account and copy anonymized.	../sample-account-0243	Classification retained from the source assessment; identifying account...
INFO	Sample public mention of Acme Sample GmbH; original account and copy anonymized.	../sample-account-0245	Classification retained from the source assessment; identifying account...
INFO	Sample public mention of Acme Sample GmbH; original account and copy anonymized.	../sample-account-0247	Classification retained from the source assessment; identifying account...

Showing top 5 of 34. Full evidence omitted from this public sample.

Youtube — 20 findings (19 low, 1 info)

All links relative to `https://social.invalid/`

RISK	TITLE	URL	REASON
LOW	Sample public mention of Acme Sample GmbH; original account and copy anonymized.	../sample-account-0016	Classification retained from the source assessment; identifying account...
LOW	Sample public mention of Acme Sample GmbH; original account and copy anonymized.	../sample-account-0020	Classification retained from the source assessment; identifying account...
LOW	Sample public mention of Acme Sample GmbH; original account and copy anonymized.	../sample-account-0024	Classification retained from the source assessment; identifying account...
LOW	Sample public mention of Acme Sample GmbH; original account and copy anonymized.	../sample-account-0028	Classification retained from the source assessment; identifying account...
LOW	Sample public mention of Acme Sample GmbH; original account and copy anonymized.	../sample-account-0032	Classification retained from the source assessment; identifying account...

Showing top 5 of 20. Full evidence omitted from this public sample.

Reddit — 5 findings (5 info)

RISK	TITLE	URL	REASON
INFO	Sample public mention of Acme Sample GmbH; original account and copy anonymized.	https://social.invalid/sample-account...	Classification retained from the source assessment; identifying account...
INFO	Sample public mention of Acme Sample GmbH; original account and copy anonymized.	https://social.invalid/sample-account...	Classification retained from the source assessment; identifying account...
INFO	Sample public mention of Acme Sample GmbH; original account and copy anonymized.	https://social.invalid/sample-account...	Classification retained from the source assessment; identifying account...
INFO	Sample public mention of Acme Sample GmbH; original account and copy anonymized.	https://social.invalid/sample-account...	Classification retained from the source assessment; identifying account...
INFO	Sample public mention of Acme Sample GmbH; original account and copy anonymized.	https://social.invalid/sample-account...	Classification retained from the source assessment; identifying account...

Linkedin — 3 findings (3 info)

All links relative to `https://social.invalid/`

RISK	TITLE	URL	REASON
INFO	Sample public mention of Acme Sample GmbH; original account and copy anonymized.	../sample-account-0307	Classification retained from the source assessment; identifying account...
INFO	Sample public mention of Acme Sample GmbH; original account and copy anonymized.	../sample-account-0309	Classification retained from the source assessment; identifying account...
INFO	Sample public mention of Acme Sample GmbH; original account and copy anonymized.	../sample-account-0313	Classification retained from the source assessment; identifying account...

Domain Typosquatting Analysis

50
POOR

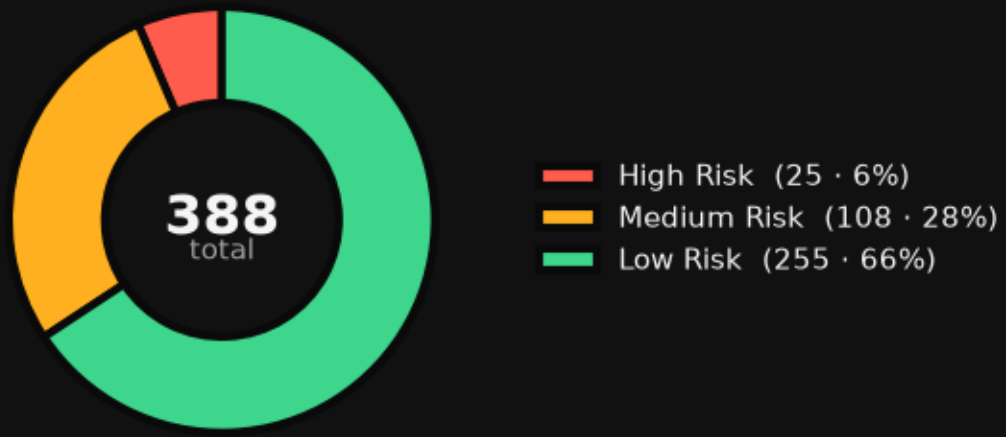
Domain variation analysis powered by SpoofGuard. Generates typosquats, homoglyphs, bit-squatting, TLD swaps, and other lookalike domains, then checks each for DNS records, active web servers, and phishing indicators.

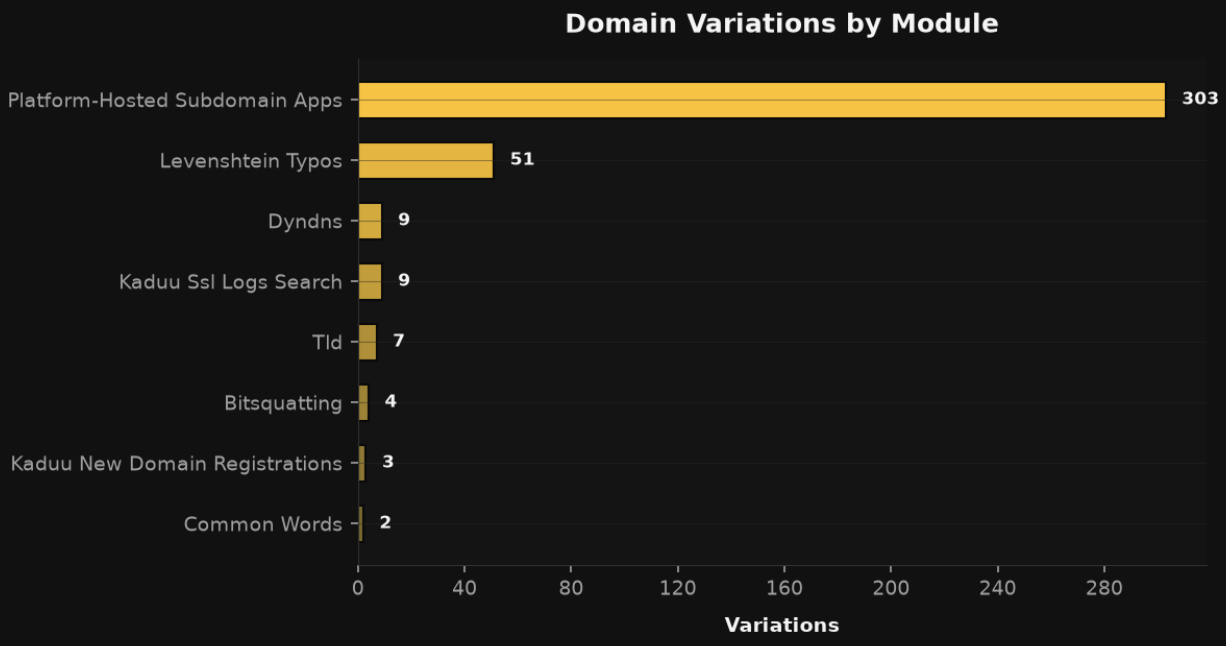
96,461	372	362	0
TOTAL VARIATIONS	WITH DNS RECORDS	ACTIVE WEB SERVERS	PHISHING DETECTED

Summary

SpoofGuard generated 96,461 look-alike variations for acmesample.com. 372 resolve in DNS; after active liveness checks, 59 actually serve live content (the rest are parked, unclaimed platform sub-domains, or return errors). 26 are rated High risk — confirmed brand/visual spoofing, a phishing-feed hit, or a malicious GPT vision verdict. 109 more are Medium (active look-alikes not yet confirmed malicious).

Typosquatting — Risk Distribution





Domain Variations — High & Medium Risk

Showing top 30 of 100 entries. Complete data in `private evidence dataset` omitted from this public sample.

DOMAIN	MODULE	A RECORD	WEB	RELEV-ANCE	RISK
acmesampl3.com		192.0.2.114	–	HIGH	HIGH

DOMAIN	MODULE	A RECORD	WEB	RELEV-ANCE	RISK
	Levenshtein Typos				
acme-sample-login.net	Levenshtein Typos	192.0.2.187	–	HIGH	HIGH
acmesample.dnsdyn.net	Dyndns	192.0.2.1	–	HIGH	HIGH
acmesample.now-dns.org	Dyndns	192.0.2.1	–	HIGH	HIGH
acmesample.dynserv.org	Dyndns	192.0.2.1	–	HIGH	HIGH
acmesample.tcp4.me	Dyndns	192.0.2.1	–	HIGH	HIGH
acmesample.dnsup.net	Dyndns	192.0.2.1	–	HIGH	HIGH
acmesample.mypi.co	Dyndns	192.0.2.1	–	HIGH	HIGH
acmesample.cn	Tld	–	–	HIGH	HIGH
acmesample-alert-010.inv…	Levenshtein Typos	–	–	HIGH	HIGH
acmesample-alert-011.inv…	Levenshtein Typos	–	–	HIGH	HIGH
acmesamplelp.com	Kaduu New Domain Registrations	–	–	HIGH	HIGH
acmesample.com.br	Tld	–	–	MED	HIGH
acmesample.biz	Tld	–	–	MED	HIGH
teaacmesample.com	Kaduu New Domain Registrations	–	–	MED	HIGH
acmesamplestore.com	Common Words	–	–	MED	HIGH
acmesample.info	Tld	192.0.2.93	HTTPS	HIGH	MEDIUM
acmesample.net	Tld	192.0.2.93	HTTPS	HIGH	MEDIUM
acmesample.org	Tld	192.0.2.93	HTTPS	HIGH	MEDIUM
acmesample.xxxy.biz	Dyndns	192.0.2.55	HTTPS	HIGH	MEDIUM
acmesample.ghe.com	Kaduu Ssl Logs Search	192.0.2.71	HTTPS	HIGH	MEDIUM

DOMAIN	MODULE	A RECORD	WEB	RELEV-ANCE	RISK
acmesample.arrivalsdepar…	Kaduu Ssl Logs Search	192.0.2.168	HTTPS	HIGH	MEDIUM
testing.acmesample-tor.com	Kaduu Ssl Logs Search	192.0.2.77	HTTPS	HIGH	MEDIUM
acmesample.atwater.dev	Kaduu Ssl Logs Search	192.0.2.79	HTTPS	HIGH	MEDIUM
acmesamplettx.com	Kaduu New Domain Registrations	192.0.2.93	HTTPS	HIGH	MEDIUM
acmesample.deckerdevs.c…	Kaduu Ssl Logs Search	192.0.2.149	HTTPS	HIGH	MEDIUM
acmesample-marketing.com	Common Words	192.0.2.167	HTTP	HIGH	MEDIUM
l-acmesample.art.pl	Platform-Hosted Subdomain Apps	192.0.2.138	HTTPS	HIGH	MEDIUM
acmesample.aquila.it	Tld	192.0.2.155	HTTPS	MED	MEDIUM
acmesample-alert-030.inv…	Levenshtein Typos	192.0.2.108	–	LOW	MEDIUM

Visual Verdict — Top 2 Most Suspicious Look-Alikes

A real headless browser was opened on each look-alike to render the page (catching JS-driven redirects to parking pages, ad networks, or impersonation sites that simple HTTP probes miss). GPT-4o analysed each screenshot together with the redirect chain and the target organisation context to produce a verdict.

Showing the 2 highest-priority look-alikes. **Verdicts, final URLs, redirect chains and screenshot links for ALL 10 enriched look-alikes are in `private evidence dataset`** (columns: `Final URL`, `Verdict Category`, `Verdict Severity`, `Verdict One-Liner`, `Verdict Evidence`, `Local Screenshot URL`).



l-acmesample.art.pl

MEDIUM RISK · REDIRECT TO UNRELATED · MEDIUM

Redirects to an unrelated domain, posing a risk of misleading users away from the intended site.

JS redirect → https://domeny.art.pl/

- Final URL is domeny.art.pl, unrelated to Acme Sample GmbH.
- JS-driven cross-host redirect detected.



acmesample-alert-042.invalid

MEDIUM RISK · REDIRECT TO UNRELATED · LOW

The domain redirects to an unrelated legitimate business, posing no threat to Acme Sample GmbH.

JS redirect → https://www.themetrocompanies.com/

- Final URL is themetrocompanies.com, unrelated to Acme Sample GmbH.
- Page title indicates a different industry: Card Manufacturing.

Threat Actor Cyber Exposure

79
GOOD

Threat actors — most notably **ransomware groups** — are organised cybercriminal operations that breach organisations, encrypt their data, and extort payment for its release. Many operate under a “Ransomware-as-a-Service” (RaaS) model and maintain public leak sites where they list victims who refuse to pay. These groups continuously scan the internet for vulnerable targets, making every exposed service a potential entry point.

This chapter assesses your organisation’s exposure to these threat actors based on industry, geography, organisation size, and publicly available ransomware intelligence data.

TARGETING PRESSURE
Moderate
Overall threat exposure

SECTOR EXPOSURE
Moderate
Industry-driven risk

COUNTRY MODIFIER
Increases Risk
Geography-based modifier

YOUR ORGANISATION
High Risk
Country (#1) & industry (#20) both in top 20 targeted

Most Relevant Threats

Ransomware	High	Ransomware is a significant threat to manufacturing sectors due to potential operational disruptions.
Supply Chain Attacks	Moderate	The reliance on complex supply chains in industrial manufacturing manufacturing makes it vulnerable to supply chain atta
Data Breaches	Moderate	Data breaches can expose sensitive information, impacting business operations and reputation.

Estimated Costs of a Successful Ransomware Attack

Based on the identified organisation size of **501-1000 employees** (Upper Mid-Market), industry research estimates the following financial impact if the organisation were to be hit by a ransomware attack:

METRIC	ESTIMATED VALUE
Average Total Cost	**$1,300,000**
Average Recovery Cost	$1,300,000
Average Ransom Paid	$300,000
Estimated Payment Rate	40%

Based on Sophos 251–1,000 employee bands; ransom varies by impact severity rather than organisation size alone.

Sources: Sophos State of Ransomware 2025; Coveware Quarterly Report; Verizon DBIR

Why Attack Surface Monitoring May Prevent Ransomware Attacks

Attackers often exploit exposed attack surfaces first.

Cybercriminals continuously scan the internet for open services, weak passwords, and leaked credentials. If something is exposed, it will be found — often automatically.

Two typical examples:

- **Exposed RDP/VPN:** attackers find an open remote access service and log in using brute force or stolen credentials.
- **Password reuse:** leaked credentials are reused to access corporate systems via password stuffing.

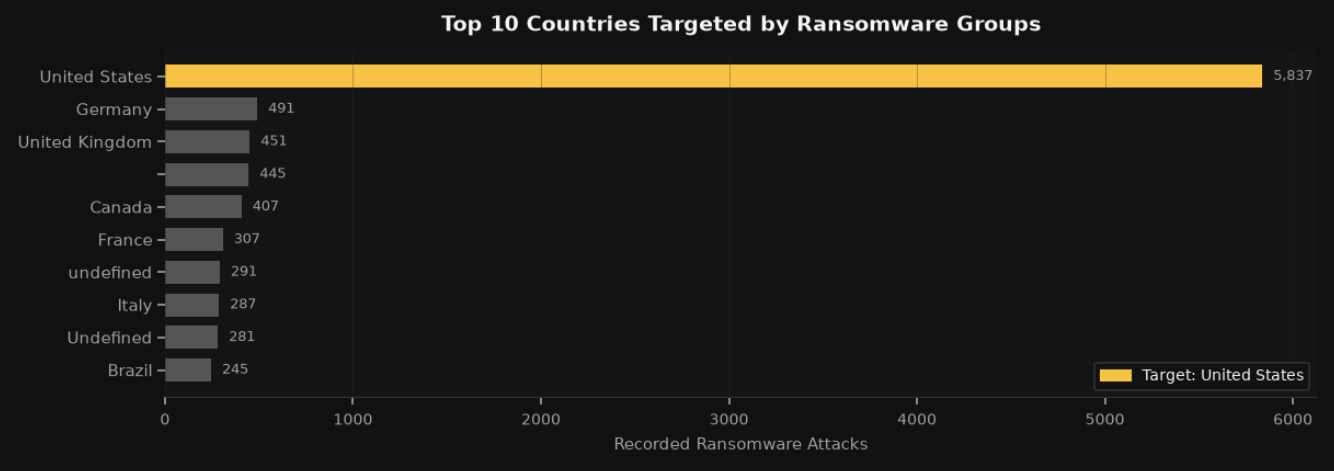
Attack surface monitoring is critical because it shows you what attackers can already see and exploit. If you reduce that visibility — by closing ports, securing access, and detecting compromised credentials — you significantly lower the risk of ransomware before it even starts.

Is Your Organisation Listed on a Threat Actor Website?

Ransomware groups operate public “leak sites” on the dark web where they list organisations that have been compromised and refused to pay. Being listed on such a site is a strong indicator that the organisation has been breached and sensitive data may have been exfiltrated. Our database continuously monitors these sites and currently tracks **12,972** victim records across all known ransomware groups.

No matches found. After analysing **12,972** ransomware victim records, your organisation does not appear on any known threat actor leak site. This is a positive indicator, but does not guarantee the organisation has never been targeted — not all incidents are publicly disclosed.

Ransomware Threat Landscape



COUNTRIES ATTACKED

179

With recorded ransomware incidents

MOST TARGETED

United States

5,837 recorded attacks

TOP INDUSTRY

Industrial Manufacturing

1,744 attacks

United States ranks **#1** globally for ransomware attacks with **5,837** recorded incidents. The **Industrial Manufacturing** sector ranks **#20** among targeted industries with **158** attacks. As a top-5 targeted country, organisations headquartered in United States face significantly elevated ransomware exposure.

Ransomware-Exploited Vulnerabilities

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) maintains the **Known Exploited Vulnerabilities (KEV)** catalogue — a curated list of vulnerabilities that have been actively used in real-world attacks. Many entries are explicitly tagged as used in ransomware campaigns. We cross-reference every CVE detected on your assets and every product / vendor in your tech stack against the current catalogue (1,709 entries). When a match exists, your environment is running software with a known, weaponised exploit path that ransomware operators are documented to exploit.

⚠ 3 matches against CISA's Known Exploited Vulnerabilities catalogue.

3 product / vendor co-occurrences (your stack runs the product; version-specific exposure should be verified).

Products in Your Stack with KEV-Listed Vulnerabilities

These products appear in your detected tech stack and have one or more CISA-KEV entries. Whether your specific deployed version is exposed depends on the patch level; treat each row as "verify your version".

VENDOR / PRODUCT	HOSTS	KEV CVES	TOP CVES	EVIDENCE	RANSOMWARE?
Microsoft — Exchange	1	1	CVE-2021-42321	POTENTIAL	KNOWN · VERSION UNCONFIRMED
Microsoft — Microsoft	16	1	CVE-2026-42897	POTENTIAL	UNKNOWN
Microsoft — Word	2	4	CVE-2006-2492, CVE-2012-2539, CVE-2014-1761 …	POTENTIAL	UNKNOWN

Appendix — Other Domains Discovered (Not Scanned)

This scan was configured in **DOMAIN ONLY** mode, so only the submitted target **acmesample.com** was assessed. During reconnaissance we observed the 1 additional registered domain below — co-hosted on the same infrastructure, sharing nameservers, or surfaced via reverse WHOIS. They were **not scanned**. To include them, re-run the scan with a broader domain mode.

DOMAIN	HOSTS SEEN	DISCOVERY METHOD
192.0.2.68	**1**	Subdomain enumeration

Appendix A — Full Asset Inventory

54 hosts sorted by risk score (top 200 shown). Complete data for all hosts is available in `private evidence dataset` omitted from this public sample.

FQDN	IP	RISK	PORTS	SOURCE	CVES
asset-047.acmesample.com	192.0.2.178	6	80, 443, 2052, 2053, 2082…	crt	21
asset-062.acmesample.com	192.0.2.178	6	80, 443, 2052, 2053, 2082…	crt	21
asset-071.acmesample.com	192.0.2.179	6	80, 443, 2052, 2053, 2082…	crt	21
asset-141.acmesample.com	192.0.2.45	6	443	crt	9
asset-166.acmesample.com	192.0.2.75	6	25, 80, 110, 143, 443…	crt	40
asset-168.acmesample.com	192.0.2.11	6	443	crt	13
asset-142.acmesample.com	192.0.2.13	5	443	crt	9
asset-143.acmesample.com	192.0.2.27	5	80, 443	subdomaincenter	49
www.acmesample.com	192.0.2.11	5	443	crt	13
asset-188.acmesample.com	192.0.2.27	5	80, 443	subdomaincenter	49
portal.acmesample.com	192.0.2.137	4	80, 443, 7443, 8443, 9443…	dns_bruteforce	0
asset-055.acmesample.com	–	1	—	crt	0
asset-059.acmesample.com	192.0.2.10	1	80, 443	crt	0
asset-060.acmesample.com	–	1	—	subdomaincenter	0
asset-064.acmesample.com	192.0.2.78	1	80, 443	dns_bruteforce	0
asset-065.acmesample.com	192.0.2.66	1	80, 443	dns_bruteforce	0
asset-148.acmesample.com	192.0.2.43	1	80, 443	crt	0
remote.acmesample.com	192.0.2.182	1	179	crt	0
asset-153.acmesample.com	192.0.2.184	1	—	subdomaincenter	0

FQDN	IP	RISK	PORTS	SOURCE	CVES
asset-158.acmesample.com	–	1	—	crt	0
asset-157.acmesample.com	–	1	—	crt	0
asset-156.acmesample.com	–	1	—	crt	0
asset-169.acmesample.com	192.0.2.15	1	443	crt	0
asset-170.acmesample.com	192.0.2.15	1	443	crt	0
asset-175.acmesample.com	–	1	—	waybackengine	0
asset-183.acmesample.com	–	1	—	subdomaincenter	0
asset-186.acmesample.com	–	1	—	subdomaincenter	0
asset-190.acmesample.com	–	1	—	subdomaincenter	0
asset-192.acmesample.com	–	1	—	subdomaincenter	0
asset-193.acmesample.com	–	1	—	subdomaincenter	0
asset-194.acmesample.com	–	1	—	subdomaincenter	0
asset-195.acmesample.com	–	1	—	subdomaincenter	0
asset-048.acmesample.com	–	0	—	subdomaincenter	0
asset-049.acmesample.com	192.0.2.63	0	80	crt	0
asset-050.acmesample.com	192.0.2.154	0	—	crt	0
asset-051.acmesample.com	–	0	—	subdomaincenter	0
asset-056.acmesample.com	–	0	—	crt	0
asset-057.acmesample.com	–	0	—	crt	0
asset-063.acmesample.com	–	0	—	subdomaincenter	0
mail.acmesample.com	–	0	—	crt	0
asset-134.acmesample.com	192.0.2.65	0	80, 443	dns_bruteforce	0
asset-144.acmesample.com	–	0	—	waybackengine	0
asset-146.acmesample.com	192.0.2.49	0	80, 443	crt	0
asset-152.acmesample.com	192.0.2.33	0	80, 443	dns_bruteforce	0
asset-165.acmesample.com	–	0	—	crt	0

FQDN	IP	RISK	PORTS	SOURCE	CVES
asset-174.acmesample.com	192.0.2.61	0	—	dns_bruteforce	0
asset-180.acmesample.com	–	0	—	subdomaincenter	0
asset-181.acmesample.com	–	0	—	crt	0
asset-182.acmesample.com	–	0	—	subdomaincenter	0
asset-184.acmesample.com	–	0	—	subdomaincenter	0
asset-185.acmesample.com	–	0	—	subdomaincenter	0
asset-187.acmesample.com	–	0	—	subdomaincenter	0
asset-189.acmesample.com	–	0	—	subdomaincenter	0
www.remote.acmesample.com	–	0	—	crt	0

All 39 DNS checks are available in `private evidence dataset` omitted from this public sample.

Appendix B — Complete Vulnerability List

All 103 unique CVEs and 399 verification findings. Complete data is available in `private evidence dataset`, `private evidence dataset`, and `private evidence dataset` omitted from this public sample.

All CVEs (103)

CVE	CVSS	SOURCES	HOSTS	CONFIDENCE
CVE-2004-0847	9.8	CVEDB	4	product matched unverified
CVE-2006-1364	7.5	CVEDB	4	product matched unverified
CVE-2003-0768	6.8	CVEDB	4	product matched unverified
CVE-2005-1664	6.4	CVEDB	4	product matched unverified
CVE-2005-1665	5.0	CVEDB	4	product matched unverified
CVE-2005-2224	5.0	CVEDB	4	product matched unverified
CVE-2005-0452	4.3	CVEDB	4	product matched unverified
CVE-2010-2084	4.3	CVEDB	4	product matched unverified
CVE-2010-2088	4.3	CVEDB	4	product matched unverified
CVE-2015-3105	10.0	CVEDB	3	product matched unverified
CVE-2014-0515	10.0	CVEDB	3	product matched unverified
CVE-2010-0425	10.0	CVEDB	3	product matched unverified
CVE-2015-0359	10.0	CVEDB	3	product matched unverified
CVE-2009-3555	9.8	CVEDB	3	product matched unverified
CVE-2024-4577	9.8	CVEDB	3	product matched unverified
CVE-2022-47986	9.8	CVEDB	3	product matched unverified
CVE-2015-3113	9.8	CVEDB	3	product matched unverified
CVE-2014-0497	9.8	CVEDB	3	product matched unverified
CVE-2015-5119	9.8	CVEDB	3	product matched unverified

CVE	CVSS	SOURCES	HOSTS	CONFIDENCE
CVE-2015-0313	9.8	CVEDB	3	product matched unverified
CVE-2013-0625	9.8	CVEDB	3	product matched unverified
CVE-2015-5122	9.8	CVEDB	3	product matched unverified
CVE-2025-34028	9.3	CVEDB	3	product matched unverified
CVE-2014-0569	9.3	CVEDB	3	product matched unverified
CVE-2011-0611	8.8	CVEDB	3	product matched unverified
CVE-2025-8088	8.4	CVEDB	3	product matched unverified
CVE-2024-0212	8.1	CVEDB	3	product matched unverified
CVE-2019-0232	8.1	CVEDB	3	product matched unverified
CVE-2017-12615	8.1	CVEDB	3	product matched unverified
CVE-2012-0754	8.1	CVEDB	3	product matched unverified
CVE-2021-34833	7.8	CVEDB	3	product matched unverified
CVE-2021-23017	7.7	CVEDB	3	product matched unverified
CVE-2023-44487	7.5	CVEDB	3	product matched unverified
CVE-2013-2028	7.5	CVEDB	3	product matched unverified
CVE-2016-0742	7.5	CVEDB	3	product matched unverified
CVE-2019-9513	7.5	CVEDB	3	product matched unverified
CVE-2009-2629	7.5	CVEDB	3	product matched unverified
CVE-2013-4547	7.5	CVEDB	3	product matched unverified
CVE-2017-7529	7.5	CVEDB	3	product matched unverified
CVE-2019-9511	7.5	CVEDB	3	product matched unverified
CVE-2019-9516	7.5	CVEDB	3	product matched unverified
CVE-2016-4450	7.5	CVEDB	3	product matched unverified
CVE-2009-4487	6.8	CVEDB	3	product matched unverified
CVE-2013-2070	5.8	CVEDB	3	product matched unverified
CVE-2018-16843	5.3	CVEDB	3	product matched unverified

CVE	CVSS	SOURCES	HOSTS	CONFIDENCE
CVE-2019-20372	5.3	CVEDB	3	product matched unverified
CVE-2018-16844	5.3	CVEDB	3	product matched unverified
CVE-2010-2263	5.0	CVEDB	3	product matched unverified
CVE-2010-2266	5.0	CVEDB	3	product matched unverified
CVE-2009-3898	4.9	CVEDB	3	product matched unverified
CVE-2010-3972	10.0	CVEDB	2	product matched unverified
CVE-2007-2815	10.0	CVEDB	2	product matched unverified
CVE-2017-7269	9.8	CVEDB	2	product matched unverified
CVE-2005-4360	7.8	CVEDB	2	product matched unverified
CVE-2009-1122	7.5	CVEDB	2	product matched unverified
CVE-2009-1535	7.5	CVEDB	2	product matched unverified
CVE-2002-0079	7.5	CVEDB	2	product matched unverified
CVE-2000-0884	7.5	CVEDB	2	product matched unverified
CVE-2000-0886	7.5	CVEDB	2	product matched unverified
CVE-2001-0506	7.2	CVEDB	2	product matched unverified
CVE-2006-0026	6.5	CVEDB	2	product matched unverified
CVE-2010-3332	6.4	CVEDB	2	product matched unverified
CVE-2003-0718	5.0	CVEDB	2	product matched unverified
CVE-2000-0778	5.0	CVEDB	2	product matched unverified
CVE-2009-2521	5.0	CVEDB	2	product matched unverified
CVE-2000-0246	5.0	CVEDB	2	product matched unverified
CVE-2001-1243	5.0	CVEDB	2	product matched unverified
CVE-2000-0630	5.0	CVEDB	2	product matched unverified
CVE-2001-0151	5.0	CVEDB	2	product matched unverified
CVE-2000-0649	2.6	CVEDB	2	product matched unverified
CVE-2021-34473	9.1	CVEDB	1	product matched unverified

CVE	CVSS	SOURCES	HOSTS	CONFIDENCE
CVE-2021-26855	9.1	CVEDB	1	product matched unverified
CVE-2020-17132	9.1	CVEDB	1	product matched unverified
CVE-2021-34523	9.0	CVEDB	1	product matched unverified
CVE-2020-0688	8.8	CVEDB	1	product matched unverified
CVE-2022-41040	8.8	CVEDB	1	product matched unverified
CVE-2021-42321	8.8	CVEDB	1	product matched unverified
CVE-2021-28482	8.8	CVEDB	1	product matched unverified
CVE-2023-21707	8.8	CVEDB	1	product matched unverified
CVE-2023-32031	8.8	CVEDB	1	product matched unverified
CVE-2022-41082	8.0	CVEDB	1	product matched unverified
CVE-2023-36035	8.0	CVEDB	1	product matched unverified
CVE-2023-36744	8.0	CVEDB	1	product matched unverified
CVE-2021-27065	7.8	CVEDB	1	product matched unverified
CVE-2021-26857	7.8	CVEDB	1	product matched unverified
CVE-2021-26858	7.8	CVEDB	1	product matched unverified
CVE-2021-33766	7.3	CVEDB	1	product matched unverified
CVE-2021-31207	6.6	CVEDB	1	product matched unverified
CVE-2021-41349	6.5	CVEDB	1	product matched unverified
CVE-2023-36777	5.7	CVEDB	1	product matched unverified
CVE-2026-6722	9.5	Shodan	2	passive intelligence
CVE-2026-17543	8.1	Shodan	2	passive intelligence
CVE-2013-2220	7.5	Shodan	2	passive intelligence
CVE-2025-14179	7.4	Shodan	2	passive intelligence
CVE-2026-6735	7.3	Shodan	2	passive intelligence
CVE-2026-7258	6.3	Shodan	2	passive intelligence
CVE-2026-7261	6.3	Shodan	2	passive intelligence

CVE	CVSS	SOURCES	HOSTS	CONFIDENCE
CVE-2026-7568	6.3	Shodan	2	passive intelligence
CVE-2026-14355	5.6	Shodan	2	passive intelligence
CVE-2026-7260	5.4	Shodan	2	passive intelligence

... and 3 more CVEs (see private evidence dataset omitted from this public sample)

All Nuclei Findings by Template

TEMPLATE	SEVERITY	COUNT
Weak Cipher Suites Detection	LOW	2
AspNet Version Disclosure - Detect	INFO	2
Content-Security-Policy "script-src" Wildcard Detected	INFO	2
Deprecated TLS Detection	INFO	1
HTTP Missing Security Headers	INFO	215
Keycloak OpenID Configuration - Detect	INFO	2
Microsoft IIS version detect	INFO	2
Mismatched SSL Certificate	INFO	5
Missing Cookie SameSite Strict	INFO	27
Missing Subresource Integrity	INFO	2
Microsoft Exchange Autodiscover - Local Domain Exposure	INFO	1
Detect OpenID Connect provider	INFO	2
POP3 Protocol - Detect	INFO	1
SMTP Detection	INFO	2
SSL DNS Names	INFO	28
Detect SSL Certificate Issuer	INFO	28
TLS Version - Detect	INFO	28
WAF Detection	INFO	31

TEMPLATE	SEVERITY	COUNT
Weak Content Security Policy - Detect	INFO	4
Wildcard TLS Certificate	INFO	14

Appendix D — Methodology & Definitions

Risk Score (0–10)

SCORE	LEVEL	DESCRIPTION
0	NONE	No IP resolved, no ports, no indicators
1–3	LOW	Resolved IP, standard web ports, sensitive subdomain names
4–6	MEDIUM	Multiple open ports, non-standard services, development endpoints
7–8	HIGH	Many open ports, file transfer services, known-vulnerable software
9–10	CRITICAL	Exposed admin panels, unprotected databases, critical vulnerabilities

CVE Intelligence Tiers

SOURCE	METHOD	CONFIDENCE
Nmap vulners	Active service version detection + vulners.com lookup	HIGH
Shodan / Netlas / ZoomEye	Passive intelligence from internet-wide scans	MEDIUM
CVEDB	Product name match via Shodan's free CVEDB API	LOW

Pipeline Phases

PHASE	DESCRIPTION
Target Analysis	Resolve the target domain IP and gather WHOIS registration data.
Subdomain Discovery	Discover all subdomains using 17 OSINT sources: certificate transparency, search engines, DNS databases, leaked credentials, reverse DNS (PTR), and web crawling.
Infrastructure Mapping	Identify shared hosting, IP ranges owned by the target, and domains registered by the same entity. Uses RIR REST APIs (RIPE, ARIN) and GPT-enhanced company identification.
Passive Intelligence	Gather port, service, technology, and vulnerability data from Shodan, ZoomEye, Netlas, and CVEDB without touching the target.
Active Scanning	Confirm open ports and identify exact service versions using Nmap. Passively-discovered ports are verified first.
Analysis & Correlation	Analyze network neighbourhoods, compare SSL certificates, verify CVEs against service versions, and calculate risk scores.
Nuclei Verification	Run 4,000+ curated nuclei templates against discovered hosts to detect exposed panels, misconfigurations, technology fingerprints, and safe CVE checks. Only triggers when active_vuln_scan=true.
Threat Intelligence	Automated querying of breach databases, cloud storage search engines, and passive banner analysis to identify credential leaks, exposed cloud files, and management interfaces.
Completion	Finalize results, deduplicate findings, materialize enrichment counters, and make the full report available.

Module Descriptions

Detailed explanation of each module that ran during this scan.

MODULE	DESCRIPTION
admin_panels	Detects admin panels and management interfaces from existing Shodan, Netlas, and nmap banner data. 55+ signatures including WordPress, Jenkins, Grafana, phpMyAdmin, Fortinet, and more. Zero additional HTTP requests.
cloud_exposure	Searches for exposed files in public cloud storage (AWS S3, Azure Blob, GCS) matching the organization name. Filters out noise (images, fonts) and classifies sensitive files (configs, databases, archives, scripts, keys).

MODULE	DESCRIPTION
code_exposure	Searches GitHub repositories and Gists for exposed source code, secrets, API keys, and sensitive data mentioning the target domain. Uses the Codewatcher API with exact-phrase matching. Each finding is scored 0-10 by GPT for risk and scanned against 150+ secret-detection regex patterns (gitleaks rules).
credential_exposure	Queries breach databases and stealer log aggregators for corporate email credentials found on external services. Returns risk-scored, deduplicated records with redacted passwords.
dns_asm	Comprehensive DNS attack surface assessment: 37 checks covering delegation health (NS presence, SOA, lame delegation, consistency), DNS exposure (AXFR zone transfer, open recursion, CHAOS version disclosure), email authentication (SPF, DMARC, DKIM), mail delivery health (MX resolution, PTR alignment), and resilience (NS diversity, DNSSEC, CAA, TCP/53, EDNS, IPv6). Tests the apex domain, each authoritative NS, and each MX host. Produces per-finding severity ratings and 5-dimension posture scores.
domain_exposure	Reverse-IP domain discovery via C99 ip2domains for every client-owned IP with web services (port 80/443), followed by RDAP domain expiry checking for all discovered domains. Identifies forgotten, expired, or soon-to-expire domains that could be hijacked for phishing or brand impersonation. Results are cached for 30 days per IP to minimize API usage.
email_auth	Evaluates DNS-based email security posture: SPF record analysis (presence, syntax, policy strength, include overflow, third-party exposure, wildcard risk), DMARC policy assessment (presence, enforcement level, percentage, alignment, reporting), DKIM selector discovery with key strength analysis (40 common selectors), and MX record validation (resolution, private IP detection, provider identification). Also checks BIMI, MTA-STS, and TLS-RPT presence. Scoring: 100-based with penalty deductions and guardrails for critical misconfigurations.
email_enumeration	Discovers employee emails via breach databases (Central API) and public internet sources (Hunter.io). Merges both data sets and scores each email across three risk dimensions: breach exposure, seniority/position risk, and public visibility.
enrichment_dns_resolve	Resolves each discovered subdomain to its IPv4 address via DNS A record lookup. Subdomains without an IP are marked as unresolvable (likely decommissioned or internal-only).
enrichment_mx_record	Discovers mail exchange (MX) records for each domain, revealing email infrastructure including cloud providers (Google Workspace, Microsoft 365) and self-hosted mail servers.
enrichment_netlas	Queries Netlas for each host's IP and domain to identify software technologies, frameworks, web server details, and open ports.

MODULE	DESCRIPTION
	Makes 2 API calls per host (IP info + domain info). Results cached for 7 days.
enrichment_network_discovery	Analyzes neighbouring IPs in the same /24 subnet. For each neighbour, checks SSL certificates (CN/SAN match, issuer match), PTR records, ASN comparison, HTTP content fingerprinting, and /24 subnet colocation. Assigns confidence scores (HIGH/MEDIUM/LOW) based on the number and strength of matching signals.
enrichment_nmap	Active TCP port scanning with intelligent targeting. When passive sources (Shodan/Netlas/ZoomEye) have identified ports, nmap performs targeted version detection (-sV) with NSE scripts (vulners for CVE lookup, ssl-enum-ciphers for TLS audit). When no ports are known, runs a fast scan (-F, top 100 ports). UDP scanning is disabled (requires root). Results include service name, product, version, and script output per port.
enrichment_shodan	Queries Shodan for each host's IP to get open ports, service banners, SSL certificate details, CPE identifiers, operating system detection, and organisation info. Results cached for 7 days per IP.
enrichment_whois	Fetches WHOIS registration data for each discovered subdomain, including registrar, creation/expiry dates, and registrant details.
enrichment_zoomeye	Queries ZoomEye for each host's IP to get SSL certificate chains, device fingerprints, port information, and vulnerability references. Results cached for 7 days.
entity_intelligence	Uses GPT with web search to identify the organisation behind the domain, classify its type, size, industry, and operating countries, then assess sector- and geography-based cyber targeting pressure. Also fetches current ransomware threat landscape data.
people_intelligence	Identifies high-value targets (C-suite, VPs, Directors) via RocketReach and enriches company data (official social media, tech stack) via Hunter.io. Produces employee profiles with contact details, career history, and social links for attack surface context.
phishing_exposure	Searches phishing intelligence databases (PhishTank, OpenPhish) via the Central API for known phishing campaigns targeting the organisation's brand name. Identifies active and historical phishing URLs impersonating the target.
server_breach_exposure	Searches the Kaduu breach database for all discovered FQDNs to identify servers mentioned in credential leaks, stealer logs, and data breaches. Results are attributed per-host with data type classification.
shortener_exposure	Searches for shortened URLs (goo.gl, bit.ly, tinyurl, ow.ly, etc.) that point to or reference the scanned domain. Detects internal corporate resources shared via shorteners, sensitive files (PDFs, spreadsheets), and suspected brand impersonation domains.

MODULE	DESCRIPTION
social_media	Searches YouTube, Twitter/X, Facebook, LinkedIn, Reddit, and Google-indexed social platforms for brand impersonation, fake profiles, and phishing mentions related to the scanned domain.
spoofguard	SpoofGuard generates thousands of domain variations (typosquats, homoglyphs, bit-squatting, TLD swaps, punycode, keyboard proximity, etc.), performs DNS lookups on all of them, checks for active web servers, detects phishing pages via multiple detection engines, and captures screenshots.
tg_discord_paste	Searches Telegram hacker channels, Discord cybersecurity servers, and paste sites (Pastebin, dpaste, ideone, etc.) for mentions of the target brand or domain. Findings are analyzed by GPT-4o-mini to filter noise and rate security relevance. Optional live Google search across 76 paste sites.
tls_posture	Synthesises TLS/SSL security posture from nmap ssl-enum-ciphers, Shodan certificate data, and nuclei SSL findings. Detects expired/self-signed certificates, weak protocols (TLS 1.0/1.1), weak ciphers (grade C-F), and HTTP-only hosts missing HTTPS.
vip_intelligence	Enumerates high-value targets (executives, directors, managers) across Google accounts, Microsoft account recovery, Holehe account detection (120+ sites), and breach databases. Produces GPT-powered risk profiles with attack vector assessment per person.
vuln_nuclei	Runs 4,000+ curated nuclei templates against discovered hosts, dynamically selected by open port type. HTTP templates (technologies, exposed panels, misconfigurations, sensitive file exposures, safe CVE detection) target live web endpoints. SSL templates check certificate and cipher configuration. DNS templates test zone transfer and configuration issues. Network templates fingerprint non-HTTP services (SSH, FTP, SMTP, databases). All templates are read-only (GET/HEAD only) — no exploitation or payload injection.
web_app_security	Evaluates externally reachable web endpoints for HTTP security weaknesses using safe GET requests, redirect analysis, response header inspection, Set-Cookie analysis, CSP/HSTS evaluation, and passive HTML parsing. 20+ checks covering session cookie security, HTTPS enforcement, security headers, subresource integrity, and clickjacking protection.
ip_range_discovery	Identifies IP ranges owned by the target organisation via RIR REST APIs (RIPE, ARIN, APNIC/AFRINIC RDAP). Uses GPT-enhanced company name identification to query registries and discover network blocks assigned to the target.
resolve_ip	Resolves the target domain to its primary IPv4 address via DNS A record lookup. This IP becomes the anchor for IP range discovery and ARIN/RIPE lookups.

MODULE	DESCRIPTION
reverse_dns	Performs reverse DNS lookups via ViewDNS to discover additional domains and hostnames associated with the target's IP addresses. Reveals PTR records and reverse DNS mappings.
reverse_whois	Finds other domains registered by the same entity using reverse WHOIS lookups (ViewDNS). Only runs when the domain is self-registered (not privacy-protected or provider-registered). Discovers shadow domains and brand-related assets.
same_ip_domains	Discovers other domains hosted on the same IP address(es) as the target using four reverse-IP sources (C99, RapidDNS, HackerTarget, ViewDNS). Shared-hosting neighbours may expose lateral-movement paths.
subdomain_discovery	Discover all subdomains using 17 OSINT sources: certificate transparency, search engines, DNS databases, leaked credentials, reverse DNS (PTR), and web crawling.
vuln_verification	Runs 4,000+ curated nuclei templates against discovered hosts to detect exposed panels, misconfigurations, technology fingerprints, and safe CVE checks. Templates are dynamically selected based on open ports.
whois	Fetches WHOIS/RDAP registration data for the main domain including registrar, creation date, expiry date, and registrant organisation.
c99	Queries C99's comprehensive passive DNS database for known subdomains of the target domain.
crt	Searches Certificate Transparency logs via crt.sh for all SSL/TLS certificates ever issued to subdomains of the target. Uses JSON API as primary, HTML scraping as fallback for large domains.
dns_bruteforce	Tries 5,000 common subdomain prefixes (www, mail, ftp, vpn, dev, staging, etc.) against the target domain using 12 public DNS resolvers in round-robin. Finds subdomains not visible in any passive source.
dnsdumpster	DNS reconnaissance tool that maps domain infrastructure. Returns subdomains from A, MX, NS, and TXT records discovered through passive DNS collection.
hackertarget	Searches HackerTarget's DNS database for known host records (A records) associated with the target domain.
hackertarget_ptr	Queries HackerTarget's reversedns API to find PTR records pointing back to the target domain. Discovers internal-facing hostnames (mail gateways, staging servers, log collectors) that are only visible via reverse DNS.
hackertarget_same_ns	

MODULE	DESCRIPTION
	Resolves the target's NS records, then queries HackerTarget's findshareddns API for every domain sharing those nameservers. Reveals organisationally-related domains.
kaduuleaks	Extracts hostnames from leaked credentials in Kaduu's darknet monitoring database. Parses credential dump lines (e.g. user@host:password) to discover subdomains that appear in breach data.
kaduulogs	Monitors SSL certificate transparency logs via Kaduu's proprietary darknet intelligence platform. Discovers subdomains from newly issued certificates in real-time.
netcraft	Queries Netcraft's internet survey database via Selenium headless Chrome to discover subdomains from their 30-year web survey archive.
rapiddns	Searches RapidDNS.io's passive DNS database for historical and current DNS records. Paginates through results to find all known subdomains.
scrapingbee	Uses ScrapingBee's anti-bot bypass to scrape Google search results for subdomain references. Runs 3 pages in parallel with a 60-second wall clock cap.
serphouse	Scrapes Google search results for references to subdomains that appear in indexed web pages. Uses the query site:{domain} to find indexed subdomains.
shodan	Discovers subdomains from Shodan's internet-wide scan data. Searches for hostname:{domain} and extracts hostnames from SSL certificates, reverse DNS, and HTTP banners.
subdomaincenter	Meta-aggregation service that combines subdomain data from dozens of underlying sources into a single query.
waybackengine	Queries the Internet Archive's CDX API for all historical URLs matching *.{domain}/*, extracting unique subdomains from archived pages. HTTPS primary, HTTP fallback.
webcrawl	Crawls the target website using 5 parallel HTTP workers (BFS, max 200 pages, depth 8, 10-minute wall clock). Extracts domains from <a>, <script src>, <link href>, <img src/srcset>, <iframe>, <form action>, <meta refresh>, inline JavaScript URL regex, and HTTP headers (CSP, Location, CORS, Link).
zoomeye	Chinese cyberspace search engine that indexes internet-connected devices and services. Searches v2 site="{domain}" (web subtype) and extracts hostnames from domain/rdns/hostname fields.

DarknetSearch is an Attack Surface Monitoring platform by Kaduu AG (Switzerland). The platform uses 49 modules across 8 pipeline phases to discover, enumerate, and analyze an organization's external digital footprint. This report was generated automatically from scan data. For questions about this report, contact support@kaduu.io.

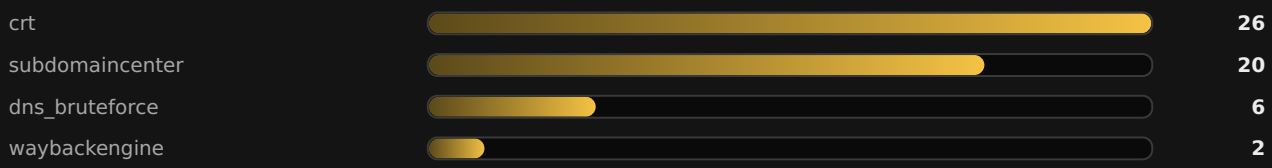
Appendix E — Intelligence Source Contribution

Intelligence Source Contribution

How each intelligence source contributed to the three pillars of asset discovery: **hostname enumeration** (finding subdomains/hosts), **open port detection** (identifying services), and **vulnerability intelligence** (CVE references).

Hostname Discovery

Unique hosts contributed by each OSINT module (before deduplication).



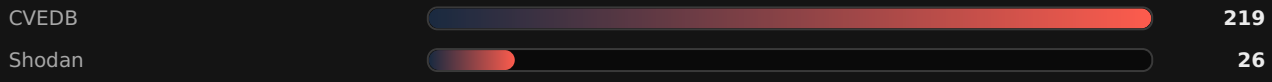
Open Port Detection

Hosts with port data from each source.



Vulnerability Intelligence

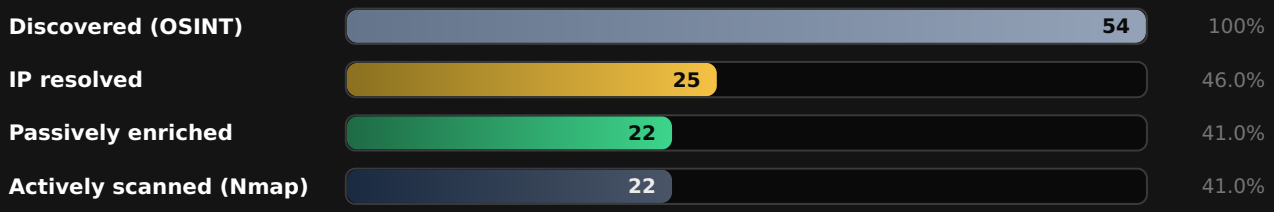
CVE references by intelligence source.



Additional threat intelligence: **Credential Exposure** (breach databases & stealer logs), **Cloud Storage Exposure** (S3/Azure/GCS bucket search), **Shortened URL Exposure** (goo.gl, bit.ly, tinyurl intelligence), **Admin Panel Detection** (passive banner analysis), **TLS/SSL Posture** (certificate & cipher analysis), **Domain Exposure & Expiry Risk** (reverse-IP discovery + RDAP expiry monitoring), **Code Exposure Analysis** (GitHub/Gist secret & source code detection via Codewatcher).

Enrichment Funnel

The scan works in stages like a funnel. First, we collect as many domain names as possible from passive OSINT sources (certificate logs, search engines, DNS databases). Next, we check which of those domains actually resolve to an IP address — many may be historical or inactive. For each host with a confirmed IP, we then run enrichment: querying Shodan, Netlas, and ZoomEye for port/service data, performing WHOIS lookups, checking MX records, and optionally running active Nmap scans. Each stage naturally filters down, which is why the bar narrows at each step.



Not resolved: 29 hosts (no DNS A record in scan window).