



Company OSINT Exposure Checklist

CM-SEC • UNCLASSIFIED • FOR PUBLIC USE

This checklist helps organizations identify OSINT-visible exposure across public web presence, external assets, third-party services, and leaked data sources. It reflects what an external party can learn without privileged access, and it is intended to support practical exposure reduction and monitoring.

How to use: Review each item, mark Priority (H/M/L) based on potential impact, and mark Status (OK/Fix/N/A) based on current state. Keep evidence (URLs, screenshots, notes) in your internal case file.

Organization Name: **Assessment Date:**

Primary Domain(s): **Industry / Sector:**

HQ Location (City/State): **Reviewer / Assessor:**

Engagement Type: **Scope Notes (optional):**

1) Asset Discovery and External Footprint

Focus: what can be enumerated publicly (domains, subdomains, hosting, exposed services, and technology stack signals).

Primary domains, brand domains, and common name variants are inventoried (including country/region domains).

Priority: H M L

Status: OK Fix N/A

Subdomains are reviewed for unexpected systems (staging, dev, admin, legacy, vendor portals).

Priority: H M L

Status: OK Fix N/A

Public IP ranges and hosting providers are documented (cloud, colocation, CDN, third-party).

Priority: H M L

Status: OK Fix N/A

Externally visible services are cataloged at a high level (web, email, VPN, remote access gateways, portals).

Priority: H M L

Status: OK Fix N/A

Technology stack signals are reviewed (CMS, frameworks, analytics, WAF/CDN) for risk implications.

Priority: H M L

Status: OK Fix N/A

Forgotten/abandoned assets are identified (old microsites, campaign pages, deprecated products).

Priority: H M L

Status: OK Fix N/A

External certificates are reviewed for naming patterns and unexpected hostnames (risk-based).

Priority: H M L

Status: OK Fix N/A

Public "status" pages and incident history are reviewed for operational and dependency clues.

Priority: H M L

Status: OK Fix N/A



Company OSINT Exposure Checklist

CM-SEC • UNCLASSIFIED • FOR PUBLIC USE

2) DNS and Email Authentication Signals

Focus: DNS records that reveal infrastructure and misconfigurations that enable impersonation or spoofing.

DNS records do not expose unnecessary internal naming conventions or sensitive host patterns.

Priority: H M L

Status: OK Fix N/A

SPF is present and appropriately restrictive for authorized mail sources.

Priority: H M L

Status: OK Fix N/A

DKIM is enabled for primary mail platforms and key sending services (marketing, ticketing, etc.).

Priority: H M L

Status: OK Fix N/A

DMARC is enabled with a policy appropriate for the organization's risk appetite (monitoring to enforcement).

Priority: H M L

Status: OK Fix N/A

Email subdomains used for third-party mailers are tracked and governed (so they cannot be abused).

Priority: H M L

Status: OK Fix N/A

MTA-STX / TLS reporting is implemented where appropriate (reduces downgrade and misdelivery risk).

Priority: H M L

Status: OK Fix N/A

Common typo domains are evaluated for mail spoofing risk (unprotected lookalikes).

Priority: H M L

Status: OK Fix N/A

Public mail routing and MX records align with intended platforms (no unexpected third-party routing).

Priority: H M L

Status: OK Fix N/A

3) Web Presence and Public-Facing Applications

Focus: public web apps, portals, and management interfaces that expose sensitive data or expand attack paths.

Public websites avoid disclosing sensitive internal details (staff emails, direct numbers, internal tools).

Priority: H M L

Status: OK Fix N/A

Staging/test environments are not publicly accessible, or are clearly controlled and sanitized.

Priority: H M L

Status: OK Fix N/A

Administrative login pages are minimized and protected (no exposed default paths where avoidable).

Priority: H M L

Status: OK Fix N/A



Company OSINT Exposure Checklist

CM-SEC • UNCLASSIFIED • FOR PUBLIC USE

Robots.txt and publicly accessible sitemaps do not reveal sensitive directories or endpoints.

Priority: H M L

Status: OK Fix N/A

Directory listing is disabled and “debug” pages are not publicly accessible.

Priority: H M L

Status: OK Fix N/A

Public error messages do not leak stack traces, internal hostnames, or file paths.

Priority: H M L

Status: OK Fix N/A

Public-facing forms and uploads are assessed for data handling risks (PII exposure, public storage links).

Priority: H M L

Status: OK Fix N/A

Third-party widgets and embedded tools are reviewed for privacy and exposure implications.

Priority: H M L

Status: OK Fix N/A

4) Cloud Storage, Public File Shares, and Exposed Data

Focus: accidental exposure of documents, backups, data exports, or internal material through public storage or sharing.

Cloud storage endpoints are checked for public read/list access (buckets, blobs, object stores).

Priority: H M L

Status: OK Fix N/A

Public file sharing platforms are reviewed for overly broad links (“anyone with the link”).

Priority: H M L

Status: OK Fix N/A

Shared folders are reviewed for sensitive materials (contracts, HR, finance, roadmaps, credentials).

Priority: H M L

Status: OK Fix N/A

Backups or exports are not publicly accessible (database dumps, logs, config archives).

Priority: H M L

Status: OK Fix N/A

Publicly accessible collaboration spaces are reviewed (wikis, knowledge bases, project hubs).

Priority: H M L

Status: OK Fix N/A

Publicly reachable camera feeds, dashboards, or IoT/OT interfaces are not exposed to the internet.

Priority: H M L

Status: OK Fix N/A

Public documents do not contain embedded secrets (API keys, tokens, passwords) in text or metadata.

Priority: H M L

Status: OK Fix N/A



Company OSINT Exposure Checklist

CM-SEC • UNCLASSIFIED • FOR PUBLIC USE

Public sample data and demo environments do not contain real customer or employee information.

Priority: H M L

Status: OK Fix N/A

5) Leaked Credentials, Breach Data, and Paste Exposure

Focus: OSINT-visible evidence of compromise or weak identity hygiene that enables account takeover and phishing.

Known credential leaks are reviewed for organization domains and brand identifiers.

Priority: H M L

Status: OK Fix N/A

Credential reuse risk is addressed through enforced policies and MFA coverage on high-risk accounts.

Priority: H M L

Status: OK Fix N/A

Leaked password hashes or credential material are treated as incident signals and tracked to remediation.

Priority: H M L

Status: OK Fix N/A

Paste sites and public dumps are monitored for organization names, domains, and key product terms.

Priority: H M L

Status: OK Fix N/A

Exposed customer data indicators are tracked (sample files, screenshots, database snippets).

Priority: H M L

Status: OK Fix N/A

Leaked internal documents or screenshots are escalated with evidence preservation procedures.

Priority: H M L

Status: OK Fix N/A

Accounts and access recovered after exposure are verified for recovery-channel security.

Priority: H M L

Status: OK Fix N/A

High-risk user populations are tracked (support, finance, IT admins, HR, executives).

Priority: H M L

Status: OK Fix N/A

6) Dark Web and Threat Actor Chatter Monitoring

Focus: early warning signals from criminal forums, marketplaces, and chatter that reference the organization.

Watchlist terms are established (domain, brand, product names, key executives, critical vendors).

Priority: H M L

Status: OK Fix N/A

Monitoring includes credentials, access sales, data listings, and impersonation attempts (risk-based).

Priority: H M L

Status: OK Fix N/A



Company OSINT Exposure Checklist

CM-SEC • UNCLASSIFIED • FOR PUBLIC USE

Triage criteria exist for credibility (proof samples, reputation, cross-source confirmation).

Priority: H M L

Status: OK Fix N/A

Escalation paths are defined for credible listings (security, legal, PR, leadership).

Priority: H M L

Status: OK Fix N/A

Evidence handling is documented (timestamps, screenshots, source context, preservation notes).

Priority: H M L

Status: OK Fix N/A

Notification cadence is defined (immediate for critical, weekly/monthly summaries for low-risk mentions).

Priority: H M L

Status: OK Fix N/A

Monitoring includes brand-abuse signals (fake support, fake recruiting, fake invoices).

Priority: H M L

Status: OK Fix N/A

Coverage includes common executive and finance fraud patterns (invoice change, wire diversion, gift cards).

Priority: H M L

Status: OK Fix N/A

7) Public Documents, Metadata, and Sensitive Content

Focus: what can be extracted from public PDFs, presentations, images, and repositories without "hacking" anything.

Public PDFs and documents are reviewed for metadata (authors, usernames, internal paths, revision history).

Priority: H M L

Status: OK Fix N/A

Press kits, brochures, and marketing materials do not reveal sensitive operational details.

Priority: H M L

Status: OK Fix N/A

Job postings are reviewed for excessive disclosure (internal tools, security controls, network details).

Priority: H M L

Status: OK Fix N/A

Presentations and webinars are reviewed for accidental leakage (screenshares, URLs, internal dashboards).

Priority: H M L

Status: OK Fix N/A

Images posted publicly are reviewed for sensitive background content (badges, floorplans, whiteboards).

Priority: H M L

Status: OK Fix N/A

Publicly indexed documents (search engines) are checked for inadvertent disclosure of internal material.

Priority: H M L

Status: OK Fix N/A



Company OSINT Exposure Checklist

CM-SEC • UNCLASSIFIED • FOR PUBLIC USE

Public repository documentation does not include environment URLs, admin paths, or secret values.

Priority: H M L

Status: OK Fix N/A

Contracts and legal documents posted publicly are reviewed for redaction quality and hidden layers.

Priority: H M L

Status: OK Fix N/A

8) Source Code, DevOps, and CI/CD Exposure

Focus: public code hosting, exposed repositories, and developer artifacts that leak secrets or internal architecture.

Public repositories are inventoried and reviewed for sensitive files and history (config, keys, dumps).

Priority: H M L

Status: OK Fix N/A

Secrets scanning is used to detect accidental exposure (tokens, credentials, API keys).

Priority: H M L

Status: OK Fix N/A

Exposed build artifacts are reviewed (logs, pipeline outputs, packaged configs).

Priority: H M L

Status: OK Fix N/A

Container images and registries are reviewed for public exposure and embedded secrets.

Priority: H M L

Status: OK Fix N/A

Public issue trackers and project boards are reviewed for sensitive operational details.

Priority: H M L

Status: OK Fix N/A

Documentation sites are reviewed for environment details that should not be public (internal endpoints).

Priority: H M L

Status: OK Fix N/A

Developer domains/subdomains are reviewed (git, ci, artifacts) to ensure they are appropriately controlled.

Priority: H M L

Status: OK Fix N/A

Access to public repos is governed (no abandoned personal accounts controlling critical organization repos).

Priority: H M L

Status: OK Fix N/A



Company OSINT Exposure Checklist

CM-SEC • UNCLASSIFIED • FOR PUBLIC USE

9) People, Social, and Organizational Intelligence

Focus: publicly observable human signals that enable spearphishing, social engineering, and physical approach.

Employee directory exposure is understood (LinkedIn, “meet the team” pages, org charts).

Priority: H M L

Status: OK Fix N/A

High-value teams are identifiable (IT, security, finance, payroll, support) and receive heightened awareness.

Priority: H M L

Status: OK Fix N/A

Public email patterns and naming conventions are documented and protected against spoofing.

Priority: H M L

Status: OK Fix N/A

Recruiting and HR processes are reviewed for impersonation risk (fake job offers, fake interviews).

Priority: H M L

Status: OK Fix N/A

Public posts do not disclose sensitive internal projects, customer incidents, or access methods.

Priority: H M L

Status: OK Fix N/A

Conference speaker bios and event listings are reviewed for personal contact and travel disclosure.

Priority: H M L

Status: OK Fix N/A

Brand ambassadors and executives have hardened profiles to reduce impersonation and doxxing risk.

Priority: H M L

Status: OK Fix N/A

Public support channels are validated to prevent fake “support” lookalikes (social, chat, phone).

Priority: H M L

Status: OK Fix N/A

10) Third-Party, Vendor, and Supply Chain OSINT Signals

Focus: exposures introduced by partners, vendors, and outsourced services that can become your problem.

Critical vendors and platforms are inventoried with publicly visible touchpoints (portals, integrations).

Priority: H M L

Status: OK Fix N/A

Vendor portals that reference the organization are reviewed for unintended disclosure.

Priority: H M L

Status: OK Fix N/A



Company OSINT Exposure Checklist

CM-SEC • UNCLASSIFIED • FOR PUBLIC USE

Public vendor incidents are tracked where they materially affect your risk posture (dependency awareness).

Priority: H M L

Status: OK Fix N/A

Third-party marketing, PR, or event sites do not inadvertently expose internal contacts or documents.

Priority: H M L

Status: OK Fix N/A

SSO and login pages are reviewed for brand abuse risk (phishing lookalikes).

Priority: H M L

Status: OK Fix N/A

Customer portals and help desks are reviewed for data handling exposure (public ticket links, indexing).

Priority: H M L

Status: OK Fix N/A

Publicly visible integrations are reviewed for oversharing (status pages, embedded widgets).

Priority: H M L

Status: OK Fix N/A

Offboarding processes exist for vendors and contractors to reduce lingering exposure.

Priority: H M L

Status: OK Fix N/A

11) Monitoring, Takedown, and Response Readiness

Focus: continuous visibility, clear ownership, and fast response when public exposure is discovered.

Alerting is configured for domains, brand terms, and key infrastructure indicators (risk-based).

Priority: H M L

Status: OK Fix N/A

Lookalike domain monitoring is in place (typosquats, homoglyphs, suspicious registrations).

Priority: H M L

Status: OK Fix N/A

Impersonation monitoring is in place (social profiles, ads, fake recruiting, fake support).

Priority: H M L

Status: OK Fix N/A

A takedown process exists (who files, where, required evidence, legal/PR coordination).

Priority: H M L

Status: OK Fix N/A

Incident response playbooks include OSINT-discovered exposures (leaks, credentials, public files).

Priority: H M L

Status: OK Fix N/A

Evidence preservation steps are documented (screenshots, hashing, timestamps, chain-of-custody as needed).

Priority: H M L

Status: OK Fix N/A

