Sentinelcore-Ai

WHITEPAPER · EASM · TPRM



Outside-In: Attack Surface and Third-Party Risk

What attackers can see about you and your suppliers, and how to turn outside-in signals into supply-chain controls that hold up under NIS2 and DORA.

By Harsukh Singh

Eight years in security engineering, information security governance and identity

September 2026 · sentinelcore-ai.com

Free to share with attribution

EXECUTIVE SUMMARY

Attackers start from the outside. So should you.

Before an attacker touches your network, they look at what's public: every subdomain in certificate logs, every exposed service indexed by internet-wide scanners, every lookalike domain they could register, and the same for your suppliers. Most of this is visible to anyone, yet many organisations have never looked at it systematically.

This paper covers three outside-in disciplines: external attack surface management (EASM) for your own domains, brand protection against lookalike domains and rogue apps, and outside-in security ratings for your vendors. It closes with how to wire them into supply-chain controls required by NIS2 Article 21(2)(d) and DORA Chapter V.

1. Your external attack surface

Discovery without touching anything

- **Certificate Transparency logs** (RFC 6962 / RFC 9162) publicly record every TLS certificate issued by trusted CAs, and with it most subdomains you have ever secured.
- **DNS** reveals which of those names still resolve, and where CNAME records point.
- **Internet-wide scan data**, collected continuously by research projects and commercial scanners, shows which ports are open on your IP addresses and which software versions they announce.

Together these give a live inventory of internet-facing assets without sending a single packet to your own systems. Limit monitoring to domains you have proven you own, typically with a DNS TXT record, so the capability cannot be pointed at someone else's infrastructure.

What to check on each host

Area	Checks	Typical ISO 27001 control
Exposure	Remote access (RDP, SSH), databases, file sharing and admin consoles reachable from the internet	8.20 Networks security, 8.22 Segregation
Takeover	CNAMEs pointing at deleted cloud or SaaS resources (dangling DNS)	8.20, 5.9 Inventory
TLS	Expired, expiring or untrusted certificates; TLS 1.0/1.1 still enabled (deprecated by RFC 8996)	8.24 Use of cryptography
Web	HTTPS enforced, HSTS (RFC 6797), security headers, version banners	8.26 Application security requirements
Email	SPF (RFC 7208), DMARC (RFC 7489) at enforcement, CAA (RFC 8659)	5.14 Information transfer
Hygiene	Development, test and admin hosts that answer publicly	8.31 Separation of environments

Area	Checks	Typical ISO 27001 control
Vulnerabilities	Version-based CVE matches, prioritised with CISA KEV and EPSS	8.8 Technical vulnerabilities

> **Only resolve what a complete scan confirms**
> When a data source is unavailable, a scan is incomplete. Findings should only be marked fixed after a complete pass no longer sees them; otherwise an outage at a data provider looks like a security improvement.

2. Brand protection

Lookalike domains

Phishing and invoice fraud rely on domains that look like yours: a missing letter, swapped letters, look-alike characters (rn for m, 0 for o), another top-level domain, or your brand plus a word such as login, secure or support. Generating these variants and checking DNS daily shows which have been registered, and which have **mail servers**. A lookalike with MX records can send and receive email today, making it the highest-priority signal.

- Block high-risk lookalikes at your email gateway and web proxy as soon as they appear.
- Report active phishing to the registrar's abuse contact, the hosting provider, browser safe-browsing services and your national CERT.
- Defensively register the variants most likely to fool your customers, and mark them as yours so they don't raise alerts.
- Enforce DMARC on your real domain: it doesn't stop lookalikes, but it stops exact-domain spoofing and makes lookalikes easier to spot.

Rogue and leaky mobile apps

Mobile app intelligence services index public Android apps and the domains, keys and endpoints embedded in them. Apps that reference your domains but aren't yours may be partners, SDKs, or impersonation. For your own apps, the same analysis finds hard-coded secrets and insecure configurations before an attacker does.

3. Outside-in vendor ratings

Questionnaires tell you what a supplier says; outside-in ratings show what anyone can see about their public infrastructure. Applied politely, looking only at the vendor's main domain like a browser visit, using DNS and pre-collected scan data, and never probing further, ratings are a cheap, continuous signal across your whole vendor base.

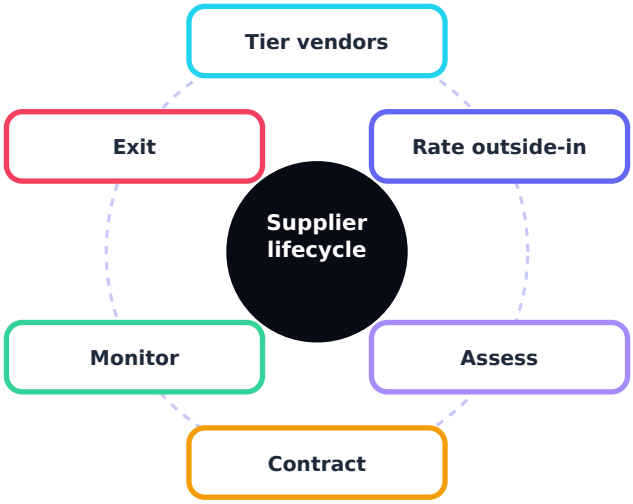
Category	What is observed	Why it matters
Email security	SPF and DMARC policy	Spoofed invoices from a supplier's domain are a leading fraud route
Website & TLS	Certificate validity, TLS versions, HTTPS and headers	A proxy for operational hygiene

Category	What is observed	Why it matters
Network exposure	Remote access and databases open to the internet	Direct entry points to systems that may hold your data
Known vulnerabilities	Version-based CVEs, KEV-listed issues	Exploitable weaknesses in the supplier's perimeter

Treat the rating as a **trigger**, not a verdict. A critical supplier with a failing grade or a sharp drop should prompt a conversation, a targeted questionnaire or a contractual remediation request. It does not replace due diligence, and it says nothing about controls that aren't visible from outside.

Wiring it into supply-chain controls

NIS2 Article 21(2)(d) requires supply-chain security, including security-related aspects of relationships with direct suppliers and service providers, and Article 21(3) asks entities to take into account suppliers' vulnerabilities and the overall quality of their products and cybersecurity practices. DORA Chapter V requires a register of ICT third-party arrangements, risk assessment before contracting, and ongoing monitoring. ISO/IEC 27001:2022 covers the same ground in Annex A 5.19 to 5.22.



- ☐ Tier suppliers by the data they access and how critical their service is.
- ☐ Record each supplier's primary domain so outside-in ratings run automatically.
- ☐ Re-rate weekly; alert on grade drops for critical suppliers.
- ☐ Use rating issues to focus questionnaires on what's actually observed.
- ☐ Include remediation and notification clauses in contracts for critical suppliers.
- ☐ Review ratings and assessments together in the management review.

How Sentinelcore-Ai helps

Sentinelcore-Ai's Attack Surface module monitors DNS-verified domains using certificate transparency, DNS and internet-wide scan data, with light browser-like TLS and HTTP checks. It detects lookalike domains, flags AI exposure and employee credentials stolen by infostealer malware, and can add mobile-app intelligence. Vendor Ratings grade every supplier's public domain A to F weekly, next to their questionnaire and contract data, and findings flow into corrective actions.

References

Directive (EU) 2022/2555 (NIS2), Article 21 · Regulation (EU) 2022/2554 (DORA), Chapter V · ISO/IEC 27001:2022, Annex A 5.19–5.22, 8.20–8.26 · RFC 6962 and RFC 9162 (Certificate Transparency), RFC 7208 (SPF), RFC 7489 (DMARC), RFC 8659 (CAA), RFC 6797 (HSTS), RFC 8996 (deprecating TLS 1.0 and 1.1) · CISA Known Exploited Vulnerabilities catalog · FIRST EPSS.

About the author

Harsukh Singh has spent eight years in hands-on cybersecurity work across security engineering, information security governance, and identity and access management. That work has meant building and running information security management systems to ISO/IEC 27001:2022, auditing them against the standard, and designing identity and access controls on Microsoft Entra ID, from conditional access and privileged roles to access reviews. Harsukh founded Sentinelcore-Ai to give security and compliance teams the tooling that work called for: posture measured against vendor baselines, findings tied to risks and corrective actions, and evidence an auditor can follow.