CYBER THREAT INTELLIGENCE

Daily CISO Threat Sweep — 2026-07-17

Board-ready daily situational awareness · Verified facts only · Action-forced

OVERALL POSTURE: SEVERE

Run date: 2026-07-17
Classification: Internal — Decision Support
Window: 24–48h critical · 7–14d blast-radius
Generated: 2026-07-17 15:55
Format: Full intelligence product (complete content)

This product prioritizes confirmed in-wild exploitation, supply-chain propagation, ransomware enablement, and identity/control-plane risk. Immediate mitigations and a confrontational action plan follow.

Classification: Internal — Decision Support Window: 24–48h critical · 7–14d blast-radius Date anchors: yesterday = 2026-07-16 · last_7_days = 2026-07-10 · last_14_days = 2026-07-03 Overall threat posture: **Severe**

1. Executive Summary

The enterprise threat picture on 2026-07-17 is **Severe**. The last 72 hours compressed multiple confirmed in-the-wild exploitation events into a single operational week: a dense Known Exploited Vulnerabilities (KEV) delta (17 July additions to date, with critical batches on 14–16 July), dual Microsoft zero-days in SharePoint and Active Directory Federation Services (AD FS) from the July Patch Tuesday cycle, unauthenticated remote code execution paths on FortiSandbox and SonicWall SMA1000 edge appliances, and a critical unauthenticated Oracle Payments takeover path now under active exploitation. Concurrently, the Miasma / Shai-Hulud npm worm lineage delivered a new canary wave (`miasma-train-p1`) on 14 July that abused trusted CI/CD publishing and **valid SLSA provenance**—a control-plane failure mode that bypasses many "provenance-only" supply-chain defenses. Ransomware-as-a-Service remains industrially active (The Gentlemen, Qilin, Akira and peers posting multi-sector claims), and a multi-agency joint advisory (AA26-194A, 13 July) re-confirmed long-running FSB Center 16 (Berserk Bear / Energetic Bear / Ghost Blizzard / Static Tundra lineage) exploitation of weak SNMP and edge routers across critical infrastructure.

What changed since yesterday (16 July): three additional KEV entries landed—SharePoint deserialization RCE (CVE-2026-58644) and two FortiSandbox OS command injection flaws (CVE-2026-39808, CVE-2026-25089)—all with federal due dates of 19 July. SharePoint now has a multi-CVE exploitation cluster (CVE-2026-45659 from 1 July, CVE-2026-56164 from 14 July, CVE-2026-58644 from 16 July). SonicWall SMA1000 and SharePoint Server KEV due dates for several entries fall on **today (17 July)** or **tomorrow (18 July for Oracle)**.

Top decisions required today

1. **Emergency patch / isolate** internet-facing SharePoint, SonicWall SMA1000, FortiSandbox, and Oracle E-Business Suite Payments surfaces; treat unpatched internet exposure as presumed compromise until forensically cleared.
2. **Force AD FS DKM ACL audit + remediation** and identity session/token review for any federated estate still on AD FS.
3. **Lockfile / SBOM sweep** for `@asyncapi/*` malicious versions and Miasma drop paths; rotate developer, CI, cloud, and registry credentials if any hit.
4. **Router hygiene sprint** per AA26-194A: kill SNMPv1/v2c defaults, Smart Install, and internet-exposed management planes.
5. **Ransomware readiness check**: immutable backup integrity + restore drill for high-value systems; edge VPN/RDP exposure inventory.

Explicit silence (last 48h — no new critical developments confirmed)

- No newly named nation-state campaign beyond the 13 July AA26-194A reaffirmation of ongoing FSB Center 16 router operations (no fresh APT28/APT29 mass-campaign disclosure in the 16–17 July window).
- No verified brand-new RaaS platform launch in the last 48 hours; activity is continuation/scale of existing groups (The Gentlemen, Qilin, Akira, and peers).
- No confirmed novel browser zero-day with enterprise mass exploitation in this 48h window.
- No high-confidence public underground marketplace listing inventable as "new IAB product line" beyond ongoing RDP/VPN access brokerage patterns already documented in mid-2026 reporting.

2. Top Threats

#	Name	Atomic Risk	Business impact (one line)	Why it matters today
1	**Miasma / Shai-Hulud lineage — `miasma-train-p1` (AsyncAPI npm, 14 Jul)**	**10**	Developer workstation + CI secrets → cloud/identity takeover at worm scale	**High propagation.** Valid provenance + on-import RAT; credential harvest of 130+ secret types; AI-assistant poisoning.
2	**CVE-2026-58644 — SharePoint deserialization RCE**	**9**	Full on-prem collaboration server compromise; document/IP theft; ransomware staging	KEV 16 Jul; CVSS 9.8; SSVC active/automatable/total; due 19 Jul; part of SharePoint exploit cluster.
3	**CVE-2026-15409 / CVE-2026-15410 — SonicWall SMA1000 SSRF + code injection**	**9**	Remote access appliance foothold → credential/TOTP theft → lateral movement	Zero-day exploitation pre-disclosure; KEV 14 Jul; due **today 17 Jul**; CVSS 10.0 SSRF.
4	**CVE-2026-25089 / CVE-2026-39808 — FortiSandbox unauth OS command injection**	**9**	Security appliance RCE; sandbox evasion; pivot into security stack	KEV 16 Jul; CVSS 9.8 both; due 19 Jul; public PoC history; internet-facing management is catastrophic.
5	**CVE-2026-46817 — Oracle E-Business Suite Payments takeover**	**9**	Unauthenticated HTTP compromise of payment processing → financial fraud / data theft	KEV 15 Jul; CVSS 9.8; due **18 Jul**; exploitation observed since late June.
6	**CVE-2026-56164 + CVE-2026-45659 — SharePoint auth/deserialization cluster**	**8**	Privilege escalation / RCE chain on ubiquitous enterprise portals	Zero-day EoP (56164) + prior KEV RCE (45659); internet-facing farms highest risk.
7	**CVE-2026-56155 — AD FS DKM ACL privilege escalation**	**8**	Local EoP on identity issuer → token-signing key risk → federated impersonation	Zero-day; KEV 14 Jul; identity control-plane blast radius if AD FS still in production.
8	**The Gentlemen / Qilin / Akira RaaS double-extortion**	**8**	Revenue stop, data leak, regulatory exposure across healthcare/mfg/gov/services	Continuous leak-site claims mid-July; edge/VPN initial access patterns feed affiliates.
9	**FSB Center 16 (Berserk Bear / Energetic Bear / Ghost Blizzard / Static Tundra) — AA26-194A**	**7**	Router config theft, credential harvest, long-dwell critical-infra access	Joint multi-nation advisory 13 Jul; SNMP/TFTP/Smart Install; multi-year campaign still live.
10	**IAB remote-access brokerage (RDP/VPN/FortiGate-class footholds)**	**7**	Purchased domain-user/admin access short-circuits perimeter; enables RaaS	Mid-2026 market shift to higher-value targets; FortiBleed-class campaigns feed ransomware.

Items **1–5 and 8** are **bold-priority** for ransomware enablement and/or high propagation.

3. Comprehensive Threats Table

Wide table continues on landscape layout for board readability.

Item (CVE/Threat/Campaign)	Threat Actor / Campaign	CVSS	Exploit Status	Exploitation Maturity	Affected	Atomic Risk	Immediate Mitigation	Primary Defense Layer
miasma-train-p1 / Miasma v3 (AsyncAPI packages)	TeamPCP lineage / copycats (Medium–High conf. on lineage; Unattributed for exact operator of this wave)	N/A (malware)	Actively distributed (packages yanked same day)	Worm-capable credential stealer; this wave `propagate: false` canary	`@asyncapi/generator@3.1.1`, `generator-helpers@1.1.1`, `generator-components@0.7.1`, `specs@6.11.2` (+ alpha); transitive via `^6.11.1`	10	Lockfile purge; pin safe versions; rotate all secrets; hunt drop paths & C2	CI/CD & OSS Integrity
CVE-2026-58644 SharePoint deserialization	Unattributed (in-wild; Confirmed)	**9.8**	Actively exploited	Automatable (SSVC); Targeted→mass risk	On-prem SharePoint Server (2016/2019/Subscription)	9	Emergency July CU; remove internet exposure; AMSI; hunt webshells/machine keys	Endpoint Detection + Rapid Patch
CVE-2026-15409 SMA1000 SSRF	Unattributed (zero-day in-wild; Confirmed)	**10.0**	Actively exploited	Targeted appliance campaigns; chainable	SMA1000 (6210/7210/8200v) specific 12.4.3/12.5.0 builds	9	Hotfix to fixed builds; if IOC → re-image, reset admin/TOTP	Remote Access Hardening + Detection
CVE-2026-15410 SMA1000 code injection	Unattributed (chained with 15409; Confirmed)	**7.2**	Actively exploited	Post-auth RCE in chain	Same SMA1000 set	8	Same as above; treat admin compromise as full appliance loss	Remote Access Hardening + Detection
CVE-2026-25089 FortiSandbox cmd inject	Unattributed (Confirmed)	**9.8**	Actively exploited	PoC public; unauth HTTP	FortiSandbox 4.2/4.4.x/5.0.x + Cloud/PaaS affected builds	9	Upgrade to fixed (e.g. 4.4.9+, 5.0.6+); no internet mgmt UI	Network Edge Hardening
CVE-2026-39808 FortiSandbox cmd inject	Unattributed (Confirmed)	**9.8**	Actively exploited	PoC/public tooling history	FortiSandbox 4.4.0–4.4.8 (verify branch)	9	Same firmware upgrade; segment analysis plane	Network Edge Hardening
CVE-2026-46817 Oracle Payments	Unattributed (Confirmed; pattern similar to prior EBS mass-exploit waves)	**9.8**	Actively exploited	Network unauth; mass-scan capable	EBS 12.2.3–12.2.15 Payments / File Transmission	9	Apply May 2026 CPU; restrict HTTP to Payments; forensic review	Endpoint Detection + Rapid Patch
CVE-2026-56164 SharePoint missing auth	Unattributed zero-day (Confirmed)	**5.3** (base; high operational risk)	Actively exploited	Network unauth EoP; chain fuel	On-prem SharePoint 2016/2019/SE	8	July 2026 security updates; de-expose	Endpoint Detection + Rapid Patch
CVE-2026-45659 SharePoint deserialization	Unattributed (Confirmed KEV 1 Jul)	**8.8**	Actively exploited	Network RCE (auth'd low priv)	On-prem SharePoint Server	8	Confirm July/prior CUs applied; hunt residual	Endpoint Detection + Rapid Patch
CVE-2026-56155 AD FS DKM ACL	Unattributed zero-day (Confirmed)	**7.8**	Actively exploited	Local EoP; identity impact	AD FS on Server 2012–2025	8	July update + DKM ACL remediate (audit→enforce); monitor events 1132–1136	Cloud Identity & Control Plane

Item (CVE/Threat/Campaign)	Threat Actor / Campaign	CVSS	Exploit Status	Exploitation Maturity	Affected	Atomic Risk	Immediate Mitigation	Primary Defense Layer
The Gentlemen RaaS	The Gentlemen (aka Thegentlemen); High conf. as named RaaS	N/A	Active extortion ops	RaaS-integrated double extortion	Multi-OS (Win/Linux/ESXi/NAS); multi-sector	8	Patch edge; MFA; immutable backups; segment	Backup & Extortion Resilience
Qilin / Akira RaaS	Qilin (Agenda); Akira — High conf. as named groups	N/A	Active leak-site claims	RaaS / affiliate model	Manufacturing, services, construction, healthcare-adjacent	7	Same ransomware controls; credential hygiene	Backup & Extortion Resilience
AA26-194A FSB Center 16	FSB Center 16 (Berserk Bear / Energetic Bear / Dragonfly / Crouching Yeti / Ghost Blizzard / Static Tundra) — High conf. government attribution	N/A	Ongoing multi-year	Targeted opportunistic edge	Internet-exposed routers/SNMP/Smart Install	7	SNMPv3 authPriv; disable SMI; ACL mgmt; patch EOL	Network Edge Hardening
IAB RDP/VPN brokerage	Multiple brokers (e.g. FortiBleed-linked “SantaAd” lineage reported mid-2026; Medium conf. on specific handles)	N/A	Continuous marketplace	Access-as-a-service	Exposed RDP/VPN/edge	7	Kill internet RDP; phishing-resistant MFA; patch VPN	Remote Access Hardening + Detection
CVE-2023-4346 KNX protocol	Unattributed (KEV 15 Jul)	(legacy ICS)	Actively exploited	ICS-specific	KNX Connection Authorization Option 1	4	ICS advisory mitigations; segment OT	Network Edge Hardening
CVE-2008-4128 Cisco IOS CSRF	FSB Center 16 and others (overlap)	(legacy)	Actively exploited (EOL context)	Opportunistic on EOL	EOL Cisco IOS 12.4 class	5	Replace EOL; block management from internet	Network Edge Hardening

4. Detailed First-Principles Analysis (Top 6)

4.1 Miasma / Shai-Hulud — `miasma-train-p1` (AsyncAPI npm)

1. **Root cause (technical)** Compromised push access to unprotected release branches (`next` / `master`) in AsyncAPI GitHub repositories. Malicious commits triggered legitimate GitHub Actions that used OIDC trusted publishing to npm—producing packages with **valid SLSA provenance**. Payload executes on module `require()`/`import` (not only install lifecycle), spawning detached Node and fetching stage-2 from IPFS.

1. **Attack mechanism + TTPs + kill-chain position** Initial access: repo/CI compromise → supply-chain distribution → developer/CI execution → mass credential theft → optional worm republish (disabled in this canary: `propagate:false`, `safeMode:true`, campaign id `miasma-train-p1`). Kill-chain: **supply chain** → **execution** → **credential access** → **persistence** → **C2** → **lateral (LAN/mDNS)**.

1. **MITRE ATT&CK** - Initial Access: T1195.001/002 (Compromise Software Dependencies / Supply Chain) - Execution: T1059.007 (JavaScript) - Persistence: T1543 / T1053 / T1547 (service/cron/launchd/Run keys) - Credential Access: T1555, T1552 (credentials from stores/files) - C2: T1071, T1102 (web + decentralized channels: Nostr, BitTorrent DHT, Ethereum dead-drop) - Discovery/Lateral: T1046, T1016

1. **Blast radius + propagation** Any org installing affected versions (including transitive `@asyncapi/specs@^6.11.1` → 6.11.2) risks workstation and pipeline secret loss. Family history includes self-replication across maintainer packages; this wave is a **training/canary** but capability remains worm-class. Downstream: cloud accounts, registries, production deploy keys.

1. **Exploitation maturity & attacker ease** High. No exploit skill required for victims—`npm install` / import is enough. Provenance trust is weaponized.

1. **Why it matters right now** Incident is 72 hours old; many lockfiles may still pin malicious versions; secret rotation windows are closing while stolen tokens remain valid.

1. **Confrontational control gaps** Branch protection gaps, over-trusted OIDC publish, provenance-as-sole-trust, no install-time behavioral block, long-lived developer PATs, AI coding tools as secondary infection surface.

4.2 CVE-2026-58644 — SharePoint Deserialization RCE

1. **Root cause** Deserialization of untrusted data (CWE-502) in on-premises SharePoint Server processing paths.

1. **Mechanism + kill-chain** Network attacker triggers unsafe deserialization → arbitrary code execution on SharePoint host. Position: **initial access / execution** on collaboration tier; often followed by webshells, IIS machine-key theft, lateral to AD.

1. **MITRE ATT&CK** T1190 (Exploit Public-Facing Application), T1059, T1505.003 (webshell), T1003 (credential dump post-exploit).

1. **Blast radius** Document stores, service accounts, intranet SSO integrations, potential domain pivot. SharePoint Online not indicated as affected; on-prem farms—especially internet-facing—are critical.

1. **Maturity** Confirmed active exploitation; SSVC: exploitation=active, automatable=yes, technicalImpact=total. KEV due 2026-07-19.

1. **Why now** Added to KEV **yesterday (16 Jul)** amid an already-active SharePoint multi-CVE cluster.

1. **Control gaps** Internet-exposed SharePoint, delayed CU deployment, missing AMSI integration, weak post-exploit hunting for machine keys and webshells.

4.3 CVE-2026-15409 / 15410 — SonicWall SMA1000

1. **Root cause** Unauthenticated SSRF (CWE-918) in Work Place interface (15409, CVSS 10.0) plus post-auth code injection in management console (15410, CVSS 7.2).

1. **Mechanism + kill-chain** Pre-auth SSRF abused for internal request forging and foothold; chained with admin-context code execution for OS command control. Observed outcomes: session/credential/TOTP seed theft, anomalous auth from appliance IP. Position: **initial access on remote-access edge**.

1. **MITRE ATT&CK** T1190, T1133 (External Remote Services), T1059, T1003/T1555 (credential theft), T1078 (valid accounts post-theft).

1. **Blast radius** Entire remote workforce path; MFA seed theft defeats weak second factors; pivot into internal AD/apps.

1. **Maturity** Zero-day exploitation before public advisory; KEV 14 Jul; due **2026-07-17 (today)**. Fixed builds: 12.4.3-03453+ / 12.5.0-02835+.

1. **Why now** Federal/enterprise SLA clocks expire today; unpatched internet SMA1000 should be treated as emergency.

1. **Control gaps** Internet management exposure, slow hotfix process, “patch-only” without re-image after compromise, weak appliance log review.

4.4 CVE-2026-25089 / 39808 — FortiSandbox

1. **Root cause** OS command injection (CWE-78) via crafted HTTP (API / UI features including VNC-related paths). Unauthenticated.

1. **Mechanism + kill-chain** Unauth HTTP → command execution on malware analysis platform. Position: **initial access into security infrastructure**—ironic and high-value for evasion and sample theft.

1. **MITRE ATT&CK** T1190, T1059, T1562 (impair defenses if sandbox is subverted).

1. **Blast radius** Sandbox host, submitted malware corpus, integrations with gateways/EDR, potential lateral from security VLAN if poorly segmented.

1. **Maturity** Active exploitation since mid-June reporting; PoC circulation; KEV 16 Jul; CVSS 9.8; due 19 Jul.

1. **Why now** Fresh KEV elevation forces 72-hour remediation for many governance programs.

1. **Control gaps** Public management interfaces, delayed firmware, security tools treated as “trusted” without same patch SLA as user endpoints.

4.5 CVE-2026-46817 — Oracle E-Business Suite Payments

1. **Root cause** Improper privilege management / missing authentication on critical Payments (File Transmission / `ibytransmit`-class) HTTP functions (CWE-269/287/306).

1. **Mechanism + kill-chain** Unauthenticated network HTTP → compromise/takeover of Oracle Payments. Position: **initial access into ERP/finance control plane**.

1. **MITRE ATT&CK** T1190, T1078, T1005/T1530 (sensitive financial data), potential T1657 (financial theft).

1. **Blast radius** Payment processor keys, DB credentials, PII/financial records, regulatory (SOX/PCI) exposure.

1. **Maturity** Exploitation observed late June; KEV 15 Jul; CVSS 9.8; due **18 Jul**.

1. **Why now** 24-hour remediation window for many orgs; finance systems often change-controlled slowly—unacceptable here.

1. **Control gaps** Internet-reachable EBS, lagging CPU application, insufficient WAF/allowlisting on Payments endpoints, weak ERP logging.

4.6 CVE-2026-56155 — AD FS DKM ACL Elevation

1. **Root cause** Insufficient granularity of access control (CWE-1220) on AD FS Distributed Key Manager (DKM) container ACLs protecting token-signing/decryption key material.

1. **Mechanism + kill-chain** Low-priv authorized local attacker escalates on AD FS server via DKM ACL weakness → path toward token key material abuse and federated impersonation. Position: **privilege escalation on identity issuer**.

1. **MITRE ATT&CK** T1068 (Exploitation for Privilege Escalation), T1550 (Use Alternate Authentication Material), T1078.004 (Cloud Accounts) in federated scenarios.

1. **Blast radius** Any relying party trusting AD FS-issued tokens (on-prem apps, hybrid Entra, SaaS federation).

1. **Maturity** Zero-day discovered in IR; KEV 14 Jul; CVSS 7.8; due 28 Jul—but identity risk warrants faster action. Vendor path: audit mode → opt-in remediation → enforced later (Oct 2026).

1. **Why now** Patch Tuesday zero-day with identity control-plane implications; many enterprises still run AD FS.

1. **Control gaps** Lingering AD FS without decommission plan, unmonitored DKM ACLs, no event 1132 alerting, broad local admin on federation servers.

5. Emerging Signals & Watch Items

Signal	Confidence	Notes
SharePoint multi-CVE chaining (45659 + 56164 + 58644) into automated kits	**High**	Cluster behavior elevates residual risk even after single-CVE patch
Miasma family next wave with `propagate:true`	**Moderate**	This wave explicitly canary; family history supports re-enablement
FortiBleed-class IAB → Inc Ransom / Lynx-style deployments	**Moderate**	Mid-2026 reporting; watch VPN appliance compromise → RaaS
APT28 Office/document tradecraft (CVE-2026-21509 lineage, stego/cloud C2)	**Moderate**	Ongoing 2026 espionage; not a fresh 48h mass event
APT29 / Midnight Blizzard identity & Golden SAML-style tradecraft	**Moderate**	Q1 2026 patterns remain strategically relevant; quiet in last 48h for new public campaigns
xpl0itrs-style mid-July access advertisements	**Low–Moderate**	Early-warning only; treat as watch, not confirmed enterprise hit
KNX ICS KEV addition (CVE-2023-4346)	**Confirmed KEV / niche impact**	OT environments only unless building automation is in scope

6. Broader Signals & Threat Actor Landscape

Ransomware / extortion: Public leak-site aggregation for mid-July shows continued high claim volume. **The Gentlemen** remains among the most prolific posters (multi-country, multi-sector claims including healthcare, manufacturing, municipal, and high-profile organizational names). **Qilin** and **Akira** continue steady affiliate-style claims. July YTD claim volume remains elevated versus prior-year baselines in public trackers; no evidence of ecosystem collapse after earlier 2026 internal leaks affecting some groups.

Nation-state: AA26-194A (13 July) is the dominant public nation-state product this window—FSB Center 16 opportunistic router compromise via weak SNMP community strings, spoofed SNMP Set, TFTP config exfil, occasional Cisco CVE/Smart Install abuse. Targets span communications, DIB, energy, finance, government (esp. state/local), and healthcare. Overlap noted with other edge-focused actors (e.g., Salt Typhoon-class TTPs). APT28 and APT29 remain strategically active in 2026 reporting but without a newly confirmed joint mass campaign in the last 48 hours.

IAB: Market continues to monetize RDP, VPN, and RDWeb access with premium pricing for high-revenue targets. Edge appliance compromise campaigns remain a primary feedstock for ransomware affiliates.

Social / early-warning tone (qualitative): Elevated discussion around Patch Tuesday zero-days, KEV batching, npm worm recurrence, and edge appliance emergencies. Treat social volume as corroborative only; all Top Threats above are grounded in primary technical/catalog confirmation.

Developer ecosystem: Provenance-signed malicious packages are now a demonstrated reality—trust models must move beyond “attestation present” to “attestation + behavioral + allowlist + least-privilege tokens.”

7. Coverage Self-Audit & Completeness Confirmation

Domain reviewed	Status
New/exploited CVEs & zero-days	**Covered** — KEV CSV verified (17 July 2026 additions); NVD CVSS pulled for priority CVEs
Supply-chain worms & malicious OSS	**Covered** — Miasma/Shai-Hulud `miasma-train-p1` AsyncAPI wave (14 Jul)
Ransomware / RaaS / infrastructure	**Covered** — The Gentlemen, Qilin, Akira activity via public leak aggregation
APT / nation-state / IAB	**Covered** — AA26-194A FSB Center 16; IAB RDP/VPN market; APT28/29 strategic notes
Underground/extortion (public trackers only)	**Covered** — leak-site claims; no fabricated marketplace listings
Cloud / identity control plane	**Covered** — AD FS CVE-2026-56155; federation/token risk
CI/CD & developer tooling	**Covered** — OIDC trusted publish abuse, GitHub Actions release path
Network edge / VPN / appliances	**Covered** — SonicWall SMA1000, FortiSandbox, SNMP/router hygiene
Browsers & client software	**Quiet** — no critical new 48h mass-exploit browser zero-day confirmed
Endpoint OS/kernel/firmware	**Secondary** — addressed via Patch Tuesday identity/collab patches; no separate kernel zero-day elevated today

Unusually silent major categories (last 48h): brand-new RaaS platform launches; brand-new APT campaign names beyond AA26-194A reaffirmation; browser zero-day mass exploitation.

Tool/search limitations: Parallel web search hit rate limits mid-collection; mitigated via sequential queries, direct KEV CSV download, NVD API CVSS pulls, and primary advisory fetches. No direct dark-web access—underground statements limited to reputable public reporting. Social “Latest” keyword tools were not available in this runtime; early-warning relied on search aggregation.

8. Category-Based Defensive Recommendations

A. Supply Chain / CI/CD / OSS

- **Threats:** Miasma `miasma-train-p1`, provenance-abusing publish path
- **Why:** Worm-class credential theft with trusted pipeline abuse
- **Action:** Org-wide lockfile/SBOM search for listed `@asyncapi/*` versions; enforce branch protection + required reviews on release branches; pin exact versions; prefer install with script restrictions where feasible; block unexpected egress from CI
- **Primary defense layer:** CI/CD & OSS Integrity
- **Leadership implication:** Fund continuous SCA + pipeline hardening; accept short-term developer friction

B. Collaboration / Web Apps (SharePoint)

- **Threats:** CVE-2026-58644, 56164, 45659
- **Why:** Confirmed in-wild cluster on ubiquitous on-prem product
- **Action:** Emergency CU deployment; remove internet exposure; enable AMSI; hunt webshells and IIS machine-key theft

- **Primary defense layer:** Endpoint Detection + Rapid Patch
- **Leadership implication:** Accept emergency change windows; no CAB delay for internet-facing farms

C. Remote Access / Edge Appliances

- **Threats:** SonicWall SMA1000 15409/15410; FortiSandbox 25089/39808; IAB VPN sales
- **Why:** Pre-auth RCE/SSRF on security and remote-access gear
- **Action:** Inventory + patch/hotfix today; if SMA IOC → re-image and rotate TOTP/admin; never expose management to internet
- **Primary defense layer:** Remote Access Hardening + Detection / Network Edge Hardening
- **Leadership implication:** Budget appliance replacement for EOL; mandate management-plane zero-trust

D. ERP / Finance

- **Threats:** CVE-2026-46817 Oracle Payments
- **Why:** Unauth takeover of payment component
- **Action:** Apply May 2026 CPU; restrict network path; forensic review of Payments endpoints
- **Primary defense layer:** Endpoint Detection + Rapid Patch
- **Leadership implication:** CFO/CISO joint ownership; regulatory notification readiness

E. Identity / Federation

- **Threats:** CVE-2026-56155 AD FS
- **Why:** Identity issuer EoP → token trust collapse risk
- **Action:** Patch; remediate DKM ACLs; alert on AD FS events 1132–1136; accelerate AD FS decommission where possible
- **Primary defense layer:** Cloud Identity & Control Plane
- **Leadership implication:** Prioritize phishing-resistant MFA and federation modernization funding

F. Ransomware / Extortion Resilience

- **Threats:** The Gentlemen, Qilin, Akira
- **Why:** Continuous double-extortion industrial ops
- **Action:** Immutable backups + restore test this week; privileged access review; edge exposure kill
- **Primary defense layer:** Backup & Extortion Resilience
- **Leadership implication:** Board-level residual risk if restore untested

G. Network Infrastructure / Nation-State Edge

- **Threats:** FSB Center 16 SNMP/TFTP/Smart Install
- **Why:** Multi-year critical-infra campaign reaffirmed 13 Jul
- **Action:** Disable SNMPv1/v2c defaults; SNMPv3 authPriv; disable Smart Install; ACL management; replace EOL Cisco
- **Primary defense layer:** Network Edge Hardening
- **Leadership implication:** OT/IT joint program; attack-surface management subscription

---

9. Prioritized Action Plan (CISO Confrontational)

Bold = top mandatory actions. Deadlines relative to Run Date 2026-07-17 00:00 local ops clock.

Wide table continues on landscape layout for board readability.

Priority	Action	Owner	Deadline	Steps	Success metric	Residual risk if deferred
1	**Emergency patch & exposure kill for SharePoint cluster (CVE-2026-58644, 56164, 45659)**	IT Ops + AppSec	**T+4h** inventory / **T+24h** internet-facing patched / **T+72h** all on-prem	1) Inventory all on-prem farms & exposure 2) Apply July 2026 CUs 3) Block external access to Central Admin 4) Enable AMSI 5) Hunt webshells, anomalous w3wp children, machine-key changes	100% internet-facing patched or offline; hunt closed with findings ticketed	Active RCE/EoP on collaboration core; ransomware staging; data theft
2	**SonicWall SMA1000 hotfix + compromise assumption workflow (CVE-2026-15409/15410)**	Network Eng + SOC	**T+4h**	1) Identify SMA1000 models/firmware 2) Upgrade to 12.4.3-03453+ or 12.5.0-02835+ 3) Review vendor IOC paths in logs 4) If any IOC: re-image, reset admin passwords & TOTP seeds, review auth from appliance IP	All appliances fixed or removed from internet; IOC review signed by SOC lead	Pre-auth edge foothold; MFA seed theft; full remote-access takeover
3	**Miasma lockfile/SBOM sweep + secret rotation**	AppSec + Eng + IAM	**T+4h** scan / **T+24h** rotations complete	1) Search all repos/CI for malicious `@asyncapi/*` versions 2) Force safe pins (`generator@3.3.0`, `helpers@1.1.0`, `components@0.7.0`, `specs@6.11.1`) 3) Hunt `NodeJS` drop dirs, `miasma-monitor`, detached `node -e` 4) Rotate npm/GitHub/cloud/SSH/CI secrets for any hit or uncertain install since 14 Jul 5) Review AI assistant configs for poisoning	Zero malicious versions in prod lockfiles; rotation attestation filed	Persistent cloud/identity compromise via stolen tokens; worm re-entry
4	**FortiSandbox firmware emergency (CVE-2026-25089/39808)**	SecEng + Network	**T+24h**	1) Inventory FortiSandbox/Cloud/PaaS 2) Upgrade to fixed builds (4.4.9+ / 5.0.6+ per advisory) 3) Remove internet exposure of UI/API 4) Review logs for anomalous HTTP to analysis APIs	All instances patched or isolated; no public mgmt	Security-stack RCE; sandbox evasion; sample/data theft
5	**Oracle EBS Payments CPU + network restrict (CVE-2026-46817)**	ERP Owners + IT Ops	**T+24h** (due 18 Jul)	1) Confirm EBS 12.2.3–12.2.15 scope 2) Apply May 2026 CPU 3) Restrict HTTP to Payments/File Transmission 4) Forensic review for unusual `ibytransmit`/Payments access	Patched + access-restricted; IR note if anomalies	Payment fraud, credential/key theft, regulatory incident

Priority	Action	Owner	Deadline	Steps	Success metric	Residual risk if deferred
6	AD FS July update + DKM ACL remediation (CVE-2026-56155)	IAM + Windows Eng	**T+24h** patch / **T+72h** ACL remediate	1) Deploy July security update 2) Monitor events 1132–1136 3) Set RemediateDkmAcl=1 per guidance after backup 4) Review federation sign-in anomalies	No 1132 warnings remaining; patch compliance 100%	Token-signing key risk; federated impersonation
7	Router hygiene sprint (AA26-194A)	Network Eng	**T+72h**	1) Disable Smart Install 2) Kill SNMPv1/v2c or lock to RO + non-default 3) Prefer SNMPv3 authPriv 4) ACL mgmt planes; block UDP 69/161/162 & TCP 4786 from internet 5) Alert on SNMP Set to config-copy OIDs	Internet SNMP/SMI exposure = 0; monitoring rules live	Nation-state config theft and long-dwell edge access
8	Ransomware readiness: immutable backup verify + restore drill	IT Ops + CISO	**T+72h**	1) Confirm immutability/off-line copies 2) Restore one tier-0 and one tier-1 system 3) Document RTO/RPO actuals 4) Privileged account review	Successful restore evidence attached to ticket	Extortion without recovery option; board-level failure
9	Identity hardening: phishing-resistant MFA + session revoke for admin	IAM	**T+72h**	1) Enforce phishing-resistant MFA on all admin 2) Revoke stale refresh tokens 3) Audit new service principals / OAuth grants (30d)	Admin MFA compliance ≥99%; anomaly report delivered	Token replay / IAB-purchased account abuse
10	Threat hunts (defensive only)	SOC	**T+24h** start / **T+72h** close	Hunts: SharePoint webshells; SMA IOC paths; FortiSandbox anomalous HTTP; Miasma drop paths & egress to known C2 patterns; SNMP Set anomalies; impossible-travel VPN	Hunt report with true/false positives	Silent breach dwell
11	Vendor/third-party notification if AsyncAPI or shared CI used by suppliers	Procurement + Legal + AppSec	**T+72h**	Notify critical suppliers using shared npm pipelines; request attestation of lockfile clean + rotation	Supplier attestations received or risk accepted in writing	Downstream supply-chain reinfection
12	Comms readiness if customer data exposure plausible	Comms + Legal + CISO	**T+72h**	Draft holding statements for SharePoint/ERP/edge incidents; map regulatory clocks	Draft approved by Legal	Botched disclosure; regulatory penalty

10. Strategic Continuity Notes

• **Shai-Hulud** → **Mini Shai-Hulud** → **Miasma** remains the defining npm worm lineage of 2025–2026; treat any “quiet week” as temporary. Provenance abuse is now table stakes for attackers.

• **SharePoint on-prem** has entered a multi-CVE exploitation era in July 2026; long-term strategy should reassess internet exposure and migration off vulnerable on-prem farms.

• **Edge appliances (VPN/SMA/sandbox/firewall)** continue as the preferred ransomware and IAB initial-access commodity—patch SLAs must match endpoint criticality, not “network gear quarterly.”

• **AD FS** is a declining but high-impact identity plane; every zero-day argues for accelerated decommission to modern IdP with phishing-resistant MFA.

• **FSB Center 16 router operations** are multi-year; hygiene is continuous control, not a one-time project.

• **The Gentlemen / Qilin / Akira** double-extortion economics remain intact; backup immutability and identity quality are the durable counters.

11. Limitations

This briefing is grounded in tool-verified primary catalogs (KEV CSV), NVD CVSS/SSVC data, and multi-source technical reporting collected on 2026-07-17. Rate limits constrained some parallel search waves; social real-time keyword tooling was unavailable in-session, so early-warning coverage is partial. Underground statements are limited to public tracker/aggregator reporting—no direct dark-web observation was performed, and no marketplace listings were fabricated. Victim counts and leak-site claims are **claims**, not independently confirmed breaches. CVSS base scores can understate operational risk (e.g., CVE-2026-56164 at 5.3 with confirmed exploitation). Attribution for unattributed in-wild exploitation remains **Unattributed** unless multi-agency naming exists (FSB Center 16 / AA26-194A). Exploit code and offensive reproduction steps are intentionally omitted.

End of Daily CISO Threat Sweep — 2026-07-17 Classification: Internal — Decision Support · Source-opaque delivery

---

End of briefing. This document is a complete export of the daily CISO threat intelligence product. Intelligence sources are intentionally omitted from the deliverable. Actions are time-bound decision support — verify against your environment before execution.