Threat intelligence: which warnings deserve your time, and what do you do with them?

This month, write down the products, suppliers and sector you need warnings about, and subscribe to the free sources that cover them: CERT-Bund's WID, CISA's and ENISA's catalogs of exploited vulnerabilities and your vendors' advisories. Give every warning that matches your inventory an owner and a decision (patch, block, hunt or detect) within one working day, or the same day if it is exploited and exposed, and judge your intelligence by the actions it produced, not by what you read.

Reviewed **5 Nov 2026** | Next review **5 Dec 2026** | Version **1.1**

Written for
IT and security teams in EU organizations of any size, many in Germany, from teams without analysts to those with a small SOC

Latest version
sheets.einblick.dev/threat-intelligence/

If you only do five things

1. **Write down what you need to know.**
   List your internet-facing products and versions, critical suppliers, sector and countries. A warning that touches none of them is reading, not work.
2. **Subscribe to the free primary sources.**
   Follow CERT-Bund's WID, which publishes short advisories for organizations on its portal and by RSS[1]. Add CISA KEV[8], ENISA's EU KEV[9] and your vendors' advisories.
3. **Filter by your inventory, then act on every match.**
   WID lists 4,250 advisories first published in 2026 by 5 November, 55% more than in all of 2025[2]. CISA added 284 to KEV in the same period[8]: few enough to check each one.
4. **Detect techniques, not just indicators.**
   The NCSC warns that indicators from China-linked covert networks "disappear as quickly as they are discovered"[21]. Build lasting detections on the behavior an advisory describes[22].
5. **Join one sharing community.**
   In Germany, the Allianz für Cyber-Sicherheit is free[4] and passes on the BSI's confidential TLP-labeled warnings[3]. Elsewhere, ask your national CERT or your sector's ISAC.

Turn a warning into an action

1. **Does it touch something on your list?**
   Match product, version and exposure against the inventory. CSAF, the JSON format of CERT-Bund's feed[2], lets tools compare advisories with an asset database or SBOM[7].
2. **Is it being exploited?**
   Check KEV, EU KEV and the advisory. Verizon found the chance of renewed exploitation roughly halves 30 days after the last observed activity[23], so when you must choose, put recent activity first.
3. **Which action fits?**
   Patch or contain within the patching sheet's deadlines. Block indicators that are recent and specific. Hunt in your logs back to the first known exploitation. Add a detection when the advisory describes a technique your logs can show.
4. **Who does it, and did it hold?**
   Open a ticket with one owner and a due date. Close it with the outcome (patched, blocked, nothing found or not affected) once a check confirms it.

Decide what you need to know

- **Your technology.** Edge devices, identity, remote access and what suppliers run for you. ENISA knew the vector of only 5.2% of unauthorized access incidents in the EU in 2025; 60.4% of those used a vulnerability[24].
- **Your sector and region.** Public administration, business services, transport, manufacturing and finance were the most affected EU sectors in 2025, and ideology-driven operations made up 57.3% of incidents[24].
- **Your suppliers and your own alerts.** Add your MSP and cloud suppliers, and feed phishing reports and blocked sign-ins back in.
- **Strategic reports, once a year.** Read your sector's part of the ENISA Threat Landscape[24], the BSI's Lagebericht[25] and M-Trends or the DBIR. Take one or two changes in priority from each.

Free sources worth subscribing to

- **CERT-Bund's WID.** Short advisories for organizations on the portal and by RSS[1], and a CSAF feed for automated matching[2].
- **CISA KEV and ENISA's EU KEV.** KEV lists 1,768 exploited vulnerabilities[8], EU KEV those confirmed exploited against EU entities[9].
- **Vendor advisories** for every product on your list. NIS2's rules for digital providers name suppliers as a channel to monitor[11].
- **The BSI-Portal and the ACS.** Participants get BSI security notices (BITS), warnings and daily and monthly situation reports[5].
- **Microsoft Defender threat analytics.** Reports show exposed devices and recommended actions, with any Defender license except Endpoint P1[26].
- **Exposure alerts** about your own addresses: see the attack surface sheet.

Indicators, techniques and ATT&CK

- **Indicators expire.** Hashes, IP addresses and domains are the easiest things for an attacker to change; techniques are the costliest[20]. Give each blocked indicator an expiry date, such as 30 days for IP addresses.
- **Search the past.** When an advisory lists indicators, search your logs back to the campaign's start. A hit means incident response, not just a block.

Share what you see

- **EU law encourages it.** NIS2 Article 29 has member states let entities share indicators, TTPs and alerts voluntarily in sharing arrangements, including with suppliers[10]. DORA Article 45 covers financial entities[12].
- **Personal data needs a basis.** NIS2 recital 121 says legitimate interest under GDPR Article 6(1)(f) could cover sharing IP addresses and URLs[10].

- **Build lasting detections on behavior.** Mandiant advises it because attackers rapidly change infrastructure and run malware in memory[22].
- **Tag rules with ATT&CK technique IDs.** Start from the detection strategies MITRE has linked to techniques since v18[17], but don't chase 100% coverage[16].

Is it changing anything?

- **Actions per month.** Patches, blocks, hunts and detections that started from a warning. Review any source that produced none for two quarters.
- **Time from advisory to decision.** For warnings that match your list. Aim for one working day, the same day if exploited and exposed.
- **Learned too late.** Exploited flaws in your products you first heard about from a customer, supplier or the news.

What you can skip

- **Paid feeds before free ones turn into tickets.** Only 26% of KEV vulnerabilities in Verizon's data were fully fixed in 2025, and full fixes took a median of 43 days[23].
- **Indicator lists without context.** Without campaign, date and confidence you can't judge them, and IP lists go stale fast[21].
- **Tracking actor names.** Microsoft lists 12 other names for its Forest Blizzard, APT28 among them[27]. Track techniques instead.
- **A threat intelligence platform before a process.** A mailbox, a ticket queue and a one-page requirements list come first.

- **Check whether to tell the authority.** DORA requires it[12], and NIS2 asks member states to require it[10]. Under BSIG § 30(7), sharing on the BSI's platform adds no obligations[6].
- **Label with TLP 2.0.** CLEAR is public, GREEN stays in the community, AMBER in your organization and its clients, AMBER+STRICT in your organization, RED only with the individual recipients[13].

What changed in 2026

- **The ACS moved into the BSI-Portal in January 2026.** Existing participants must re-register there, with an ELSTER company login, by 31 January 2027 or lose their participation[5].
- **ATT&CK v19 split Defense Evasion** into Stealth and Defense Impairment in April[18]. Re-tag your rules. v20 added AI techniques in October[19].
- **EU KEV will add manufacturers' reports.** The CRA has required them since 11 September 2026[9].

Mistakes that cost the most

- **Reading without a ticket.** A warning that ends in a chat has no owner. Every match gets a ticket, even when the answer is "not affected".
- **Blocking feeds unfiltered.** Feeds can include public DNS resolvers, popular domains and scanners. Check them against MISP's warninglists[15].
- **Forwarding labeled warnings to suppliers.** TLP:AMBER covers your organization and its clients, not your MSP. Ask the source first[13].
- **Stale filters.** Update feed filters and subscriptions when you add a product. NIS2's rules for digital providers require reviewing these channels at planned intervals[11].

What this looks like at your size

Small team, no security staff

- Send WID's RSS feed and your vendors' advisories, filtered to your internet-facing products, to a mailbox two people read.
- Join the ACS, or ask your national CERT what it shares with companies.
- Ask your IT provider which advisories it acted on last month.

Growing, with IT or security staff

- Pull KEV, EU KEV and vendor CSAF feeds into tickets, matched against the inventory.
- Add one detection a month from an advisory relevant to your sector.
- Run MISP, which is free and open source[14], or use your ISAC's.

Enterprise or regulated

- Review intelligence requirements with risk owners every quarter.
- Keep a register of the sharing arrangements you join and the notifications you made.
- Put TLP handling in your MSSP contract and report the three measures to leadership.

Version history

5 Nov 2026, version 1.1	Reviewed for company readers: small teams outside Germany now ask their national CERT what it shares with companies, since some CERT communities serve only public bodies.

Sources

1. Technische Sicherheitshinweise (WID). BSI, checked 5 Nov 2026. bsi.bund.de
2. WID CSAF feeds. CERT-Bund, counted 5 Nov 2026. wid.cert-bund.de
3. BSI-IT-Security-Advisories. BSI, checked 5 Nov 2026. bsi.bund.de
4. Teilnehmer. ACS (BSI), checked 5 Nov 2026. allianz-fuer-cybersicherheit.de
5. Die ACS erweitert ihre Präsenz um das neue BSI-Portal. ACS (BSI), 6 Jan 2026. allianz-fuer-cybersicherheit.de
6. BSIG §§ 5, 6 and 30. BMJV, checked 5 Nov 2026. gesetze-im-internet.de
7. TR-03191: CSAF. BSI, checked 5 Nov 2026. bsi.bund.de
8. KEV catalog (JSON feed). CISA, version 2026.11.04. cisa.gov
9. Vulnerability Services. ENISA, checked 5 Nov 2026. enisa.europa.eu
10. NIS2 Directive, Article 29 and recital 121. EUR-Lex, 2022. eur-lex.europa.eu
11. Regulation 2024/2690, Annex 6.10. EUR-Lex, 2024. eur-lex.europa.eu
12. DORA Regulation, Article 45. EUR-Lex, 2022. eur-lex.europa.eu
13. Traffic Light Protocol 2.0. FIRST, Aug 2022. first.org
14. MISP. MISP Project, 2.5.50, 9 Oct 2026. misp-project.org
15. MISP warninglists. MISP Project, checked 5 Nov 2026. misp-project.org
16. ATT&CK resources. MITRE, checked 5 Nov 2026. attack.mitre.org
17. ATT&CK v18 release notes. MITRE, 28 Oct 2025. attack.mitre.org
18. ATT&CK v19 release notes. MITRE, 28 Apr 2026. attack.mitre.org
19. ATT&CK v20 release notes. MITRE, 13 Oct 2026. attack.mitre.org
20. The Pyramid of Pain. David Bianco, 1 Mar 2013, updated Jan 2014. detect-respond.blogspot.com
21. China-nexus covert networks. NCSC (UK), 23 Apr 2026. ncsc.gov.uk
22. M-Trends 2026. Google Cloud (Mandiant), 23 Mar 2026. cloud.google.com
23. 2026 DBIR. Verizon, 19 May 2026. verizon.com
24. ENISA Threat Landscape 2026. ENISA, Sep 2026. enisa.europa.eu
25. State of IT Security in Germany 2025. BSI, Nov 2025. medien.bsi.bund.de
26. Threat analytics. Microsoft Learn, 26 May 2026. learn.microsoft.com
27. Threat actor naming. Microsoft Learn, 21 Oct 2026. learn.microsoft.com