



give some cyber and network security projects or research topic for an organization.latest and best novel topics

Here are high-impact, novel cybersecurity and network security project ideas for an organization in 2025, prioritized around current threats and emerging standards such as ENISA's threat landscape, NIST's PQC standards, and AI/LLM security guidance. Each idea is scoped so a security team can pilot, measure value, and scale across the enterprise while aligning to widely adopted frameworks. [\[1\]](#) [\[2\]](#) [\[3\]](#) [\[4\]](#) [\[5\]](#)

GenAI and LLM security

- Build an LLM security program aligned to OWASP Top 10 for LLM applications (prompt injection, insecure output handling, data poisoning, model theft) with automated red teaming, guardrails, and evaluation gates in CI/CD. [\[6\]](#)
- Operationalize NIST's Generative AI Risk Management Profile by mapping GenAI-specific risks to controls, validation tests, and residual risk reporting for business owners. [\[4\]](#) [\[5\]](#)
- Adopt MITRE ATLAS for threat-informed defense of AI systems; create purple-team playbooks for prompt injection, data poisoning, model evasion, and supply-chain compromise of AI components. [\[7\]](#) [\[8\]](#) [\[9\]](#)

Post-quantum cryptography (PQC) migration

- Launch a crypto modernization program to inventory, prioritize, and pilot FIPS-approved PQC algorithms ML-KEM (FIPS 203), ML-DSA (FIPS 204), and SLH-DSA (FIPS 205) in internal PKI, TLS, code signing, and firmware signing workflows. [\[3\]](#) [\[10\]](#)
- Evaluate performance, handshake sizes, and operational impacts of hybrid TLS with PQC in HTTP/3/QUIC environments to guide rollout plans and SLOs under real traffic. [\[11\]](#) [\[12\]](#) [\[3\]](#)
- Brief execs on migration roadmaps and standards outlook using authoritative updates from NIST and the PKI community to secure budget and timelines. [\[13\]](#) [\[14\]](#)

Software supply chain and transparency

- Achieve SLSA v1.0 Build Track provenance for critical CI/CD pipelines, with evidence verification at deployment and policy gates for artifact promotion. [\[15\]](#) [\[16\]](#)
- Implement NIST SSDF 1.1 across SDLC and extend with SP 800-218A GenAI profile for AI model development, linking artifacts to executive attestation expectations. [\[17\]](#) [\[18\]](#) [\[19\]](#)

- Prototype IETF SCITT-based transparency logs for signed attestations (builds, scans, models, datasets) to enable cross-vendor verification and auditability.[\[20\]](#)
- Conduct a response drill on open-source maintainer compromise using the XZ Utils backdoor as a scenario; validate detection, provenance, and supplier trust workflows.[\[2\]](#)

Memory safety and secure-by-design

- Create an organization-wide memory-safety roadmap (Rust/Go/Java adoption, wrappers for unsafe code, safe libraries) tied to measurable CVE-class reduction targets and engineering incentives.[\[21\]](#) [\[22\]](#)
- Harden legacy C/C++ through defense-in-depth (control-flow integrity, hardened allocators, sanitizer builds, fuzz coverage SLAs) while tracking defect trendlines as a KPI to leadership.[\[22\]](#) [\[21\]](#)

Next-gen transport security (HTTP/2, HTTP/3, QUIC)

- Build a lab and production detection for HTTP/2 Rapid Reset (CVE-2023-44487) with rate limiting, stream concurrency policies, and upstream vendor validation; rehearse emergency mitigations for volumetric events.[\[23\]](#) [\[24\]](#) [\[25\]](#)
- Develop an HTTP/3/QUIC security hardening guide covering fingerprinting defenses, traffic analysis risks, and operational configurations tied to recent survey insights and implementation studies.[\[12\]](#) [\[26\]](#) [\[11\]](#)
- Evaluate SSH over QUIC (SSH3) for internal admin access: latency, auth modernization (OIDC/OAuth), and stealth posture under scanning and middlebox constraints.[\[27\]](#)

WAF and HTTP parsing research

- Conduct differential parsing and spec-conformance testing across proxies/CDNs/app servers to surface request smuggling and parsing ambiguities from HTTP/1.1 through HTTP/2/3 and intermediaries.[\[28\]](#)
- Build and publish WAF bypass test suites derived from recent parsing discrepancy research, and benchmark mitigations against modern WAFs and cloud shields.[\[29\]](#)

eBPF-powered runtime security (cloud/Kubernetes)

- Stand up an eBPF-based runtime security stack for Kubernetes to detect process, syscall, file, and network anomalies with low overhead, and benchmark Tetragon/Falco/Tracee against use cases.[\[30\]](#) [\[31\]](#) [\[32\]](#)
- Map eBPF attack surface, verifier limitations, and kernel CVEs to hardening guidance (privilege scoping, program verification, kernel baseline) and blue-team detections.[\[33\]](#) [\[34\]](#) [\[35\]](#)
- Detect cryptojacking in containers using eBPF telemetry and ML classification; measure precision/recall and operational overhead before fleet rollout.[\[36\]](#)

Critical infrastructure and enterprise resilience

- Build a threat-driven resilience plan aligned with ENISA TL 2024's top threats (availability attacks/DDoS, ransomware, data threats, supply chain) including tabletop exercises and sector-tailored controls.[\[37\]](#) [\[1\]](#) [\[2\]](#)
- Elevate API security posture with discovery, inventory, and continuous testing governance, reflecting observed growth in API traffic and unmanaged endpoints in contemporary reports.[\[38\]](#)
- Test DNS resolver stacks against KeyTrap-style algorithmic complexity attacks and validate safe configs, vendor patch status, and fail-open/fail-closed behaviors.[\[39\]](#)

Threat intel, CTI-led risk, and measurement

- Integrate cyber threat intelligence into risk management to improve prioritization, bridging gaps between adversary TTPs and operational decision-making in critical infrastructure contexts.[\[40\]](#)
- Evaluate robust statistical methods to prioritize vulnerabilities under partial information conditions to better guide patching and exposure management at scale.[\[41\]](#)

Sector-specific and IoT/5G initiatives

- Develop AI-driven anomaly detection for connected vehicles and IoT fleets with domain-specific datasets and model evaluation, focusing on constrained devices and real-time constraints.[\[42\]](#)
- Review 5G threat models and controls drawing on ENISA material to align enterprise use of private 5G and network slicing with defensible architectures.[\[43\]](#) [\[44\]](#)

Program kickstart suggestions

- Start with two quick wins: HTTP/2 Rapid Reset detection-and-response runbook and organization-wide SSDF 1.1 baseline with artifact mapping, then fund PQC and eBPF pilots as Q2–Q3 strategic initiatives.[\[19\]](#) [\[3\]](#) [\[23\]](#)
- Establish a cross-functional AI security council to implement the NIST GenAI profile and OWASP LLM Top 10 across data, model, and application layers with quarterly risk reporting.[\[6\]](#) [\[4\]](#)

If desired, these can be packaged into a 12-month roadmap with measurable outcomes, executive reporting, and platform changes aligned to the cited standards and threat reports.[\[16\]](#)
[\[1\]](#) [\[3\]](#) [\[4\]](#)



more

Here are additional, high-impact 2025 cybersecurity and network security project ideas, tuned for enterprise adoption and regulatory alignment, with concrete scopes and outcomes for quick pilots and scale-up.[\[166\]](#) [\[167\]](#)

CRA, NIS2, DORA readiness labs

- Stand up a Cyber Resilience Act compliance lab to test “products with digital elements” against CRA obligations (secure by design/default, vulnerability handling, reporting) and build a gap remediation playbook before full applicability dates.[\[168\]](#) [\[169\]](#)
- Map NIS2 security measures using ENISA’s implementation guidance into concrete technical controls, evidence artifacts, and board reporting for essential/important entities.[\[170\]](#) [\[171\]](#)
- For financial services, run a DORA operational resilience program with adversarial scenario testing, third-party oversight drills, and incident/threat reporting workflows aligned to Jan 17, 2025 applicability.[\[172\]](#) [\[173\]](#)

Phishing-resistant MFA and passkeys at scale

- Launch a phishing-resistant MFA migration using FIDO2/passkeys with device analytics, pilot cohorts, helpdesk playbooks, and measurable ATO reduction targets.[\[174\]](#) [\[175\]](#)
- Pair passkeys with SSO hardening and “MFA fatigue” controls, implementing explicit user interaction and risk prompts to reduce relay/MITM exposure in high-risk flows.[\[176\]](#) [\[174\]](#)
- Publish enterprise UX and recovery standards for passkeys using current FIDO design guidance to keep friction low while maintaining phishing resistance.[\[175\]](#) [\[177\]](#)

Confidential computing for data-in-use

- Pilot confidential VMs/containers with attestation in analytics or AI workloads to protect data-in-use, measuring overhead, developer experience, and audit artifacts for regulated use cases.[\[178\]](#) [\[179\]](#)
- Build an attestation verification service and policy gates (admission controllers) that block workloads lacking verified TEE posture in sensitive namespaces.[\[180\]](#) [\[179\]](#)
- Create a business case and roadmap using market studies and CCC resources to prioritize the highest-ROI confidential computing use cases in the organization.[\[181\]](#) [\[178\]](#)

SBOM + VEX operations

- Operationalize SBOM ingestion at scale (SPDX/CycloneDX) with VEX processing to determine exploitability context, wired into vulnerability management SLAs and dashboards.[\[182\]](#) [\[183\]](#)
- Evaluate SBOM toolchain accuracy and completeness on a representative portfolio, referencing recent analyses of Python SBOM generators and VEX consistency pitfalls.[\[184\]](#) [\[185\]](#)

- Join SBOM community events to align internal minimum elements and automation plans with current US/EU practices and CRA-driven expectations.[\[169\]](#) [\[186\]](#)

CAASM and EASM exposure management

- Deploy External Attack Surface Management to continuously discover internet-facing assets, prioritize exposures by exploitability/KEV status, and validate fixes in rolling windows.[\[187\]](#) [\[188\]](#)
- Implement CAASM to unify internal asset inventories across endpoints, cloud, identities, and apps for a single security view that supports breach response and exposure trending.[\[189\]](#) [\[190\]](#)
- Tie EASM and CAASM outputs into zero-trust device posture and change-management alerts to cut unknown/unauthorized asset dwell time.[\[187\]](#) [\[189\]](#)

Cloud dangling resource abuse mitigation

- Scan for and eliminate dangling DNS/storage/identity references across cloud providers, then introduce pre-provisioning guardrails and continuous controls to block takeover paths.[\[191\]](#)
- Build detections for sudden ownership changes and unexpected CNAME or object reclamations tied to product subdomain inventories, with on-call runbooks for takedowns.[\[191\]](#)

NIS2 technical controls mapping program

- Use ENISA's NIS2 technical guidance to create a control-to-evidence matrix (logging, detection, incident response, vulnerability management, crypto, supply chain) with audit-ready artifacts.[\[171\]](#) [\[170\]](#)
- Run quarterly control effectiveness reviews simulating cross-border incident reporting timelines and regulator information requests for covered entities.[\[171\]](#)

Sectoral PQC transition for finance

- Establish a quantum-safe crypto working group in finance units to evaluate hybrid handshakes, signing, and data-at-rest protections in line with DORA's resilience posture.[\[192\]](#) [\[173\]](#)
- Produce a board-level PQC risk memo and pilot plan emphasizing long-lived secrets, archival data, and inter-bank dependencies under realistic performance constraints.[\[192\]](#)

Outcome-focused kickstarts

- 90-day CRA/NIS2 readiness sprint: compile an evidence catalog, run a product security gap analysis, and rehearse vulnerability handling and incident reporting with suppliers.[\[169\]](#) [\[171\]](#)
- 120-day identity modernization pilot: roll out passkeys to a high-risk cohort, benchmark ATO and helpdesk metrics, and document migration runbooks for enterprise-wide rollout.[\[174\]](#) [\[175\]](#)

If helpful, these can be packaged into a 12-month roadmap with pilots, metrics, and executive updates tied to the cited standards and frameworks for defensible investment decisions.^[169]
^[171]

*

1. https://securitydelta.nl/media/com_hsd/report/690/document/ENISA-Threat-Landscape-2024.pdf
2. <https://industrialcyber.co/reports/enisa-threat-landscape-2024-identifies-availability-ransomware-data-attacks-as-key-cybersecurity-threats/>
3. <https://csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved>
4. <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf>
5. <https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-generative-artificial-intelligence>
6. <https://owasp.org/www-project-top-10-for-large-language-model-applications/>
7. <https://atlas.mitre.org>
8. <https://ctid.mitre.org/blog/2024/09/30/threat-informed-defense-to-secure-ai/>
9. https://atlas.mitre.org/pdf-files/SAFEAI_Full_Report.pdf
10. <https://csrc.nist.gov/projects/post-quantum-cryptography>
11. <https://arxiv.org/html/2401.06657v3>
12. <https://ieeexplore.ieee.org/document/10677379/>
13. https://en.wikipedia.org/wiki/NIST_Post-Quantum_Cryptography_Standardization
14. https://pkic.org/events/2025/pqc-conference-austin-us/WED_PLENARY_1000_Bill-NAndrew-R_NIST-P_Q-Crypto-Update.pdf
15. <https://cycode.com/blog/slsa-1-0-improving-software-supply-chain-security/>
16. <https://slsa.dev/spec/v1.0/>
17. <https://www.sonatype.com/resources/guides/stay-compliant-nist-sp-800-218-cisa-requirements>
18. <https://csrc.nist.gov/news/2024/nist-publishes-sp-800-218a>
19. <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-218.pdf>
20. <https://datatracker.ietf.org/group/scitt/about/>
21. https://media.defense.gov/2025/Jun/23/2003742198/-1/-1/0/CSI_MEMORY_SAFE_LANGUAGES_REDUCING_VULNERABILITIES_IN_MODERN_SOFTWARE_DEVELOPMENT.PDF
22. <https://www.ic3.gov/CSA/2025/250212.pdf>
23. <https://blog.cloudflare.com/technical-breakdown-http2-rapid-reset-ddos-attack/>
24. <https://blog.cloudflare.com/zero-day-rapid-reset-http2-record-breaking-ddos-attack/>
25. <https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-http2-reset-d8Kf32vZ.html>
26. <https://ieeexplore.ieee.org/document/10585883/>
27. <https://blog.apnic.net/2024/02/02/towards-ssh3-how-http-3-improves-secure-shells/>
28. https://figshare.com/articles/conference_contribution/Who_s_Breaking_the_Rules_Studying_Conformance_to_the_HTTP_Specifications_and_its_Security_Impact/25826629/1/files/46339027.pdf
29. <https://arxiv.org/pdf/2503.10846.pdf>
30. <https://ieeexplore.ieee.org/document/11146725/>

31. <https://tetragon.io/docs/resources/>
32. <https://cilium.io/blog/2024/12/31/tetragon-2024-year-in-review/>
33. <http://arxiv.org/pdf/2409.07508.pdf>
34. <https://github.com/google/security-research/security/advisories/GHSA-hfqc-63c7-rj9f>
35. <https://www.linuxfoundation.org/hubfs/eBPF/ControlPlane — eBPF Security Threat Model.pdf>
36. <https://www.mdpi.com/2079-9292/14/6/1208>
37. <https://ec.europa.eu/newsroom/cipr/items/859770/en>
38. <https://ieeexplore.ieee.org/document/10866301/>
39. <https://arxiv.org/html/2406.03133v1>
40. <https://www.mdpi.com/2624-800X/4/2/18/pdf?version=1717938907>
41. <https://arxiv.org/pdf/2302.08348.pdf>
42. <https://www.mdpi.com/2673-2688/5/4/112>
43. <https://open-research-europe.ec.europa.eu/articles/2-125/v3>
44. <https://pmc.ncbi.nlm.nih.gov/articles/PMC10446063/>
45. <https://www.semanticscholar.org/paper/cba661c34afae4a0202d5366768ba6baba956db0>
46. <https://arxiv.org/abs/2405.08762>
47. <https://www.bussecon.com/ojs/index.php/ijbes/article/view/539>
48. <https://www.bussecon.com/ojs/index.php/ijbes/article/view/504>
49. <https://ieeexplore.ieee.org/document/10571373/>
50. <https://journal.uitm.edu.my/ojs/index.php/BEJ/article/view/976>
51. <https://www.linuxfoundation.org/research/software-security-education-study>
52. <https://www.linuxfoundation.org/research/2024-open-source-congress>
53. <https://ejbmr.org/index.php/ejbmr/article/view/2386>
54. <https://dl.acm.org/doi/10.1145/3708036.3708109>
55. <https://linkinghub.elsevier.com/retrieve/pii/S0959652621039536>
56. <http://arxiv.org/pdf/2310.06300.pdf>
57. <https://arxiv.org/pdf/2409.05014.pdf>
58. [https://zenodo.org/record/4428991/files/Transport Network Slices with Security.pdf](https://zenodo.org/record/4428991/files/Transport%20Network%20Slices%20with%20Security.pdf)
59. <http://arxiv.org/pdf/2407.13785.pdf>
60. <https://arxiv.org/pdf/2404.12300.pdf>
61. <https://arxiv.org/abs/2210.05813>
62. <http://arxiv.org/pdf/2408.02876.pdf>
63. <https://slsa.dev>
64. <https://openssf.org/press-release/2023/04/19/openssf-announces-slsa-version-1-0-release/>
65. <https://community.ibm.com/community/user/blogs/steve-weaver1/2024/01/11/secure-your-software-supply-chain-with-slsa-level>
66. <https://www.cbtnuggets.com/blog/technology/devops/is-slsa-the-best-standard-for-ci-ci-pipelines>
67. <https://datatracker.ietf.org/doc/draft-ietf-scitt-architecture/>
68. https://data.aclum.org/storage/2025/01/NIST_csrc_nist_gov_projects_ssdf.pdf

69. <https://buildkite.com/resources/blog/understanding-the-slsa-framework/>
70. <https://github.com/ietf-wg-scitt>
71. <https://arxiv.org/html/2409.05014v1>
72. <https://www.youtube.com/watch?v=1EQCTediRWI>
73. <https://scitt.io/community>
74. <https://dpo-india.com/Resources/NIST/Secure-Software-Development-Practices-Generative-AI-and-Du al-Use-Foundation-Models-NIST.pdf>
75. <https://blog.gitguardian.com/spice-wimse-and-scitt/>
76. <https://checkmarx.com/blog/what-you-need-to-know-about-nist-800-218-the-secure-software-develo pment-framework/>
77. <https://journals.library.columbia.edu/index.php/bioethics/article/view/10953>
78. <https://www.semanticscholar.org/paper/13abbdadcd5160efabba616786b22639db7b1069>
79. <http://medrxiv.org/lookup/doi/10.1101/2025.05.15.25327687>
80. <https://ojs.lifescience.org/index.php/life-and-science/article/view/875>
81. <https://www.aseansocialwork.com/index.php/asw/article/view/117>
82. <https://invergejournals.com/index.php/ijss/article/view/172>
83. <https://invergejournals.com/index.php/ijss/article/view/179>
84. <https://journal-buildingscities.org/articles/10.5334/bc.514/>
85. <https://bmjopen.bmj.com/lookup/doi/10.1136/bmjopen-2025-102723>
86. http://www.diw.de/de/diw_01.c.825124.de/publikationen/weekly_reports/2021_37_1/global_economy_retu rning_to_its_recovery_course_after_summer_setbacks_diw_economic_outlook_autumn_2021.html
87. <http://arxiv.org/pdf/2403.19368.pdf>
88. <http://arxiv.org/pdf/2305.01249.pdf>
89. <http://arxiv.org/pdf/2504.07634.pdf>
90. <https://arxiv.org/pdf/2208.06722.pdf>
91. <https://arxiv.org/html/2411.09895v1>
92. <https://blog.cloudflare.com/madeyoureset-an-http-2-vulnerability-thwarted-by-rapid-reset-mitigation s/>
93. <https://blog.qualys.com/vulnerabilities-threat-research/2023/10/10/cve-2023-44487-http-2-rapid-rese t-attack>
94. <https://www.cloudflare.com/the-net/rapid-reset-ddos/>
95. <https://arxiv.org/html/2409.16267v1>
96. <https://www.openlogic.com/blog/cve-2023-44487-http-2-rapid-reset>
97. <https://dl.acm.org/doi/abs/10.1109/TNSM.2024.3457858>
98. <https://www.haproxy.com/glossary/what-is-http2-rapid-reset>
99. <https://vaibhavbajpai.com/documents/papers/preprints/2024-arxiv-quic.pdf>
100. <https://dl.acm.org/doi/10.1145/3623565.3623757>
101. <https://gist.github.com/adulau/7c2bfb8e9cdbe4b35a5e131c66a0c088>
102. <https://www.scribd.com/document/727403344/A-Survey-on-the-Security-Issues-of-QUIC>
103. <https://vaibhavbajpai.com/documents/papers/proceedings/quic-tnsm-2024.pdf>

104. <https://www.sciencedirect.com/science/article/abs/pii/S016740482500152X>
105. <https://dl.acm.org/doi/10.1145/3658644.3691548>
106. <https://journaljsra.com/node/1083>
107. <https://arxiv.org/pdf/2102.09980.pdf>
108. <https://arxiv.org/pdf/2308.01983.pdf>
109. <http://arxiv.org/pdf/2406.14020.pdf>
110. <http://arxiv.org/pdf/1810.10260.pdf>
111. <https://ieeexplore.ieee.org/document/10619896/>
112. <https://www.acigjournal.com/Vulnerability-of-Students-of-Masaryk-University-to-Two-Different-Types-of-Phishing,190268,0,2.html>
113. <https://dl.acm.org/doi/10.1145/3646547.3688409>
114. <https://doi.ub.kg.ac.rs/2024/10-46793-arheon7-173k/>
115. <https://gsconlinepress.com/journals/gscarr/node/2666>
116. <https://gjeta.com/node/1797>
117. <https://fetbl.com/index.php/csitrj/article/view/1115>
118. <https://journals.sagepub.com/doi/10.1177/20552076241257146>
119. <https://www.frontiersin.org/articles/10.3389/fdata.2024.1381163/pdf?isPublishedV2=False>
120. <https://www.mdpi.com/1424-8220/23/8/4060/pdf?version=1681731584>
121. <https://www.mdpi.com/2227-7080/11/6/161/pdf?version=1699860751>
122. <https://www.mdpi.com/1424-8220/21/15/5189/pdf>
123. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>
124. <https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape>
125. <https://www.deloitte.com/ro/en/our-thinking/articles/raportul-enisa-threat-landscape-2024-peisajul-am-enintarilor-cibernetice-sectorul-financiar.html>
126. <https://industrialcyber.co/secure-by-design/nsa-cisa-guidance-push-for-adoption-of-memory-safe-languages-in-software-development-to-boost-resilience/>
127. <https://www.enisa.europa.eu/publications>
128. <https://gbhackers.com/cisa-publishes-guide-to-address-memory-safety-vulnerabilities/>
129. https://www.enisa.europa.eu/sites/default/files/2025-02/Finance TL 2024_Final.pdf
130. <https://www.damovo.com/blog/enisa-threat-landscape-2024-report/>
131. <https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards>
132. <https://www.devopsdigest.com/fix-it-or-face-the-consequences-cisas-memory-safe-muster>
133. <https://www.digicert.com/blog/nist-standards-for-quantum-safe-cryptography>
134. <https://ieeexplore.ieee.org/document/10532874/>
135. https://link.springer.com/10.1007/978-3-031-85593-1_9
136. <https://paperssds.eu/index.php/JSPSDS/article/view/760>
137. <https://arxiv.org/abs/2412.16089>
138. <https://dl.acm.org/doi/10.1145/3655693.3655701>

139. <https://ieeexplore.ieee.org/document/10932131/>
140. <https://ieeexplore.ieee.org/document/10779256/>
141. <https://dl.acm.org/doi/10.1145/3691620.3694982>
142. <https://lib.jucs.org/article/134739/>
143. <https://jcosine.if.unram.ac.id/index.php/jcosine/article/view/624>
144. <https://arxiv.org/pdf/2409.10490.pdf>
145. <http://arxiv.org/pdf/2406.18894.pdf>
146. <https://arxiv.org/pdf/2411.16239.pdf>
147. <http://arxiv.org/pdf/2501.17539.pdf>
148. <http://arxiv.org/pdf/2405.20441.pdf>
149. <https://arxiv.org/pdf/2404.13161.pdf>
150. <https://arxiv.org/pdf/2405.04760.pdf>
151. <http://arxiv.org/pdf/2410.16527.pdf>
152. https://owaspla.owasp.org/assets/prez/OWASPLA_pres_2024_05.pdf
153. <https://www.confident-ai.com/blog/owasp-top-10-2025-for-llm-applications-risks-and-mitigation-techniques>
154. <https://genai.owasp.org/resource/llm-top-10-for-llms-v1-1/>
155. <https://www.lasso.security/blog/owasp-top-10-for-llm-applications-generative-ai-key-updates-for-2025>
156. <https://www.dlapiper.com/en/insights/publications/ai-outlook/2024/nist-releases-its-generative-artificial-intelligence-profile>
157. <https://www.chaossearch.io/blog/mlops-monitoring-mitre-atlas>
158. <https://github.com/OWASP/www-project-top-10-for-large-language-model-applications>
159. <https://babl.ai/nist-releases-new-framework-to-address-risks-of-generative-ai/>
160. <https://www.cloudsine.tech/making-sense-of-ai-security-frameworks-owasp-mitre-atlas-and-the-nist-rmf/>
161. <https://www.securecodewarrior.com/article/owasp-top-10-for-llm-applications-whats-new-changed-and-how-to-stay-secure>
162. <https://www.holisticai.com/blog/nist-ai-rmf-generative-ai-use-case-profiles>
163. <https://www.youtube.com/watch?v=de9UPN7yD5U>
164. <https://www.nist.gov/itl/ai-risk-management-framework>
165. <https://www.sysdig.com/blog/understand-ai-threats-with-mitre-atlas>
166. https://securitydelta.nl/media/com_hsd/report/690/document/ENISA-Threat-Landscape-2024.pdf
167. <https://csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved>
168. https://www.european-cyber-resilience-act.com/Cyber_Resilience_Act_Links.html
169. https://en.wikipedia.org/wiki/Cyber_Resilience_Act
170. https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf
171. https://www.enisa.europa.eu/sites/default/files/2024-11/Implementation_guidance_on_security_measures_FOR_PUBLIC CONSULTATION.pdf

172. <https://fortifydata.com/blog/dora-implementation-date/>
173. https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en
174. <https://fidoalliance.org/cisa-secure-by-demand-guide-phishing-resistant-authentication-passkeys-by-default/>
175. <https://fidoalliance.org/white-paper-fido-deploying-passkeys-in-the-enterprise-introduction/>
176. <http://arxiv.org/pdf/2401.11599.pdf>
177. <https://www.passkeycentral.org/design-guidelines/>
178. <https://confidentialcomputing.io/resources/white-papers-reports/>
179. <https://confidentialcomputing.io>
180. https://archive.fosdem.org/2025/events/attachments/fosdem-2025-5002-confidential-computing-s-recent-past-emerging-present-and-long-lasting-future/slides/237828/Confident_fRySvCW.pdf
181. <https://confidentialcomputing.io/2024/03/27/march-2024-newsletter/>
182. <https://media.defense.gov/2023/Dec/14/2003359097/-1/-1/0/CSI-SCRM-SBOM-MANAGEMENT.PDF>
183. <https://english.ncsc.nl/binaries/ncsc-en/documenten/publications/2024/july/30/software-bill-of-materials-starter-guide/Software+Bill+of+Materials+Starter+Guide.pdf>
184. <https://arxiv.org/pdf/2503.14388.pdf>
185. <https://arxiv.org/html/2409.01214v1>
186. <https://www.federalregister.gov/documents/2024/02/29/2024-04235/winter-2024-cisa-sbom-a-rama>
187. <https://www.zerofox.com/blog/what-is-easm-external-attack-surface-management/>
188. <https://blog.qualys.com/product-tech/2024/03/26/meeting-fisma-m-24-04-requirements-with-a-unified-attack-surface-management-strategy>
189. <https://www.runzero.com/gartner-customer-choice-2024/>
190. <https://cyberstrategyinstitute.com/gartner-analysis-of-security-operations-centers-sochs-in-2024-understanding-the-hype-cycle-for-security-operations/>
191. <http://arxiv.org/pdf/2403.19368.pdf>
192. <https://link.springer.com/10.1365/s43439-025-00135-7>
193. <https://drops.dagstuhl.de/entities/document/10.4230/DagRep.14.3.52>
194. <https://www.tandfonline.com/doi/full/10.1080/13511610.2024.2349626>
195. <https://www.nature.com/articles/s41746-024-01116-6>
196. <https://journals.sagepub.com/doi/10.1177/17816858241288397>
197. <https://irek.ase.md/xmlui/handle/123456789/3147>
198. https://www.cambridge.org/core/product/identifier/S1867299X25000091/type/journal_article
199. <https://dl.acm.org/doi/10.1145/3715275.3732032>
200. <https://link.springer.com/10.1365/s43439-022-00067-6>
201. <https://intern.bulletin.knu.ua/article/view/3570>
202. <http://arxiv.org/pdf/2412.06261.pdf>
203. <https://arxiv.org/html/2502.10281v2>
204. <https://arxiv.org/pdf/2205.13196.pdf>
205. <https://www.tandfonline.com/doi/pdf/10.1080/13501763.2023.2295523?needAccess=true>
206. <https://arxiv.org/pdf/2203.04887.pdf>

207. <https://www.jifmr.com/papers/2023/6/10726.pdf>
208. <https://www.tandfonline.com/doi/pdf/10.1080/13600869.2022.2060468?needAccess=true>
209. <https://www.tandfonline.com/doi/full/10.1080/07036337.2024.2411240>
210. https://www.europarl.europa.eu/doceo/document/TA-9-2024-0130_EN.html
211. https://www.cybercertlabs.com/case_studies/cyber-resilience-act-adopted/
212. <https://www.legitsecurity.com/blog/what-you-need-to-know-about-the-eu-cyber-resilience-act>
213. <https://www.nis-2-directive.com>
214. <https://digitalpolicyalert.org/change/2075>
215. <https://privacymatters.dlapiper.com/2025/08/eu-enisa-guidelines-on-compliance-with-nis-2-directive-published/>
216. <https://n2ws.com/blog/dora-regulation>
217. <https://www.whitecase.com/insight-alert/cyber-resilience-act-clock-ticking-compliance>
218. <https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance>
219. <https://www.cutover.com/blog/achieving-digital-operational-resilience-testing-compliance-dora-law>
220. <https://www.sgs.com/en/news/2025/09/safeguards-13125-update-on-developments-relating-to-the-eu-cyber-resilience-act>
221. <https://www.digital-operational-resilience-act.com>
222. <https://cyberhubs.eu/enisa-publishes-practical-guidance-on-mapping-nis2-obligations-to-cybersecurity-role-profiles/>
223. <https://www.cssf.lu/en/2025/01/entry-in-application-of-dora-regulation-on-17-january-2025/>
224. <https://www.mdpi.com/2410-387X/3/3/24/pdf?version=1568960031>
225. <http://arxiv.org/pdf/2407.20459.pdf>
226. https://zenodo.org/record/6038478/files/Practical_Threshold_Multi-Factor_Authentication.pdf
227. <http://arxiv.org/pdf/2412.12324.pdf>
228. <https://arxiv.org/html/2406.09000v1>
229. <https://arxiv.org/pdf/2312.04100.pdf>
230. <https://arxiv.org/ftp/arxiv/papers/2401/2401.06612.pdf>
231. <https://doubleoctopus.com/blog/general/phishing-resistant-mfa-guide/>
232. <https://tokenring.com/hubfs/Collateral/CISO-Guide-Stopping-Ransomware-with-Phishing-Resistant-MFA-eBook.pdf?hsCtaAttrib=185453357750>
233. <https://blog.hypr.com/what-is-phishing-resistant-mfa>
234. <https://thehackernews.com/2024/10/why-phishing-resistant-mfa-is-no-longer.html>
235. <https://www.corbado.com/blog/introducing-passkeys-large-scale-overview>
236. <https://www.iddataweb.com/inside-cisas-phishing-resistant-mfa-playbook/>
237. <https://fidoalliance.org/passkeys/>
238. <https://cpl.thalesgroup.com/resources/access-management/state-passkey-deployment-enterprise-fido-report>
239. <https://www.linuxfoundation.org/research/confidential-computing-use-case-study>
240. https://authenticatecon.com/wp-content/uploads/2024/04/Authenticate_Agenda_2024_AUG13.pdf
241. <https://confidentialcomputing.io/author/hlau/>

- 242. <https://www.swissbit.com/en/blog/post/authentication-101-passkeys-for-enterprises/>
- 243. <https://www.anjuna.io/blog/confidential-computing-wrapped-your-industry-update-as-we-enter-2025>
- 244. <https://arxiv.org/pdf/2301.05362.pdf>
- 245. <https://www.mdpi.com/1424-8220/23/4/1802/pdf?version=1675666303>
- 246. <https://arxiv.org/pdf/2503.13998.pdf>
- 247. <http://arxiv.org/pdf/2407.00246.pdf>
- 248. <https://www.mdpi.com/1424-8220/23/8/4060/pdf?version=1681731584>
- 249. <https://www.mdpi.com/2624-6511/7/4/72/pdf?version=1721631633>
- 250. <https://openssf.org/blog/2025/10/22/sboms-in-the-era-of-the-cra-toward-a-unified-and-actionable-framework/>
- 251. <https://cybellum.com/blog/breaking-down-cisas-minimum-vex-requirements/>
- 252. <https://www.packetlabs.net/posts/cisa-releases-software-bill-of-materials-guidance/>
- 253. <https://cymulate.com/blog/the-caasm-between-asset-management-and-attackers-view/>
- 254. <https://www.sygnia.co/gartner-market-guide/>
- 255. <https://www.wiz.io/academy/external-attack-surface-management-easm>
- 256. <https://www.sysdig.com/blog/gartner-runtime-insights-is-a-core-pillar-of-cnapp>
- 257. <https://brandefense.io/blog/cisa-cybersecurity-roadmap-2024-2026/>
- 258. <https://www.patrowl.io/en/external-attack-surface-management-easm>
- 259. <https://www.01net.it/runzero-recognized-as-a-customers-choice-in-2024-gartner-peer-insightsm-report-for-cyber-asset-attack-surface-management-caasm/>
- 260. <https://www.intruder.io/blog/cyber-security-trends>
- 261. <https://www.scribd.com/document/872148658/Market-Guide-for-MDMS-Gartner>
- 262. <https://learn.microsoft.com/en-us/security/zero-trust/cisa-zero-trust-maturity-model-devices>