. Liste des Sources

1. **ENISA Threat Landscape 2025**, ENISA, 1 Octobre 2025, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025
2. **ENISA Threat Landscape 2025 - Full Report**, ENISA, Janvier 2026, https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf
3. **The State of AI Cybersecurity 2026**, Darktrace, Janvier 2026, https://www.darktrace.com/resource/the-state-of-ai-cybersecurity-2026
4. **2026 Public Sector Cyber Outlook**, Palo Alto Networks, 15 Janvier 2026, https://www.paloaltonetworks.com/blog/2026/01/public-sector-cyber-outlook/
5. **Model Context Protocol: Understanding MCP security risks**, Giskard AI, 20 Janvier 2026, https://www.giskard.ai/knowledge/model-context-protocol-understanding-mcp-security-risks-and-prevention-methods
6. **OWASP MCP Top 10: Key MCP Vulnerabilities**, MSSP Alert, 26 Décembre 2025, https://www.msspalert.com/native/owasp-mcp-10-external-aiexposures-you-must-prioritize-in-2026
7. **Gartner Identifies the Top Cybersecurity Trends for 2026**, Gartner Inc., 5 Février 2026, https://www.gartner.com/en/newsroom/press-releases/2026-02-05-gartner-identifies-the-top-cybersecurity-trends-for-2026
8. **2026 Predictions for Autonomous AI**, Palo Alto Networks, 20 Novembre 2025, https://www.paloaltonetworks.com/blog/2025/11/2026-predictions-for-autonomous-ai/
9. **L'Anssi publie son panorama de la cybermenace 2025**, InCyber, 2 Février 2026, https://incyber.org/article/anssi-publie-son-panorama-cybermenace-2025/
10. **Bizarre Bazaar campaign exploits exposed LLM endpoints**, Bleeping Computer / SC World, 29 Janvier 2026, https://www.scworld.com/brief/bizarre-bazaar-campaign-exploits-exposed-llm-endpoints
11. **The AI-fication of Cyberthreats: Trend Micro Predictions for 2026**, Trend Micro, Décembre 2025, https://documents.trendmicro.com/assets/research-reports/the-ai-fication-of-cyberthreats-trend-micro-security-predictions-for-2026.pdf
12. **Security Predictions 2026: Agentic AI in the SOC**, Splunk, Décembre 2025, https://www.splunk.com/en_us/blog/leadership/security-predictions-2026-what-agentic-ai-means-for-the-people-running-the-soc.html
13. **Architecture for the agentic era: How AI will reshape security**, Cribl, Novembre 2025, https://assets.ctfassets.net/xnqwd8kotbaj/6PYzA9LZXbMiy0kFGD1p6B/002d137c86cdb84962e7024c6d129689/RPT-0004_2026-trends-and-predictions-report_112025.pdf
14. **Agentic AI Security Threats in late 2026**, Stellar Cyber, Janvier 2026, https://stellarcyber.ai/learn/agentic-ai-securiry-threats/
15. **5 Realities for the 2026 AI SOC**, Laura Grace Ellis, Décembre 2025, https://www.littlemissdata.com/blog/aisoc2026

16. **Cyber Insights 2026: API Security and Agentic AI**, SecurityWeek, Janvier 2026, https://www.securityweek.com/cyber-insights-2026-api-security/
17. **Geopolitical OSINT Threat Assessment Report (GOTAR) 2026**, DebugLies, 5 Février 2026, https://debuglies.com/2026/02/05/geopolitical-osint-threat-assessment-report-gotar-ai-driven-cyber-threats-and-risks-in-2026-agentic-ai-ransomware-apt-convergence-and-geopolitical-escalation-vectors/
18. **The Hidden Dangers of MCP: Emerging Threats**, Jit.io, Janvier 2026, https://www.jit.io/resources/app-security/the-hidden-dangers-of-mcp-emerging-threats-for-the-novel-protocol
19. **ENISA NIS Investments 2025**, ComplexDiscovery, Novembre 2025, https://complexdiscovery.com/enisa-2025-nis-investments-report-technology-prioritized-as-cyber-talent-pools-contract/
20. **ETL 2025: Key takeaways for SMEs**, Digital SME Alliance, Octobre 2025, https://www.digitalsme.eu/enisa-cybersecurity-threat-landscape-report-2025-key-takeaways-for-smes/
21. **CrowdStrike 2026 Global Threat Report (Preview)**, Make It Simple, 19 Janvier 2026, https://www.makeitsimple.co.uk/blog/saas-development-framework
22. **DockerDash: Vulnerability in MCP Gateway contextual trust**, The Hacker News, 2 Février 2026, http://thehackernews.com/2026/02/weekly-recap-ai-skill-malware-31tbps.html
23. **Model Context Protocol Security Best Practices**, ModelContextProtocol.io, Janvier 2026, https://modelcontextprotocol.io/specification/draft/basic/security_best_practices
24. **NTT DATA Technology Foresight Report 2026**, IT Brief UK, Janvier 2026, https://itbrief.co.uk/story/ntt-data-maps-six-ai-trends-shaping-mass-intelligence
25. **La sécurité du cloud : sept tendances structurantes pour 2026**, IT Social, 4 Février 2026, https://itsocial.fr/cybersecurite/cybersecurite-articles/la-securite-du-cloud-a-lere-des-architectures-hybrides-sept-tendances-structurantes-pour-2026/
26. **MITRE ATLAS Updates and Case Studies**, Vectra AI, Octobre 2025, https://www.vectra.ai/topics/mitre-atlas
27. **Threat Briefing 30 January 2026**, Black Arrow Cyber, 30 Janvier 2026, https://www.blackarrowcyber.com/blog/threat-briefing-30-january-2026
28. **TriZetto Data Breach and anomalous behavior detection**, SANS NewsBites, 30 Janvier 2026, https://www.sans.org/newsletters/newsbites/xxviii-08
29. **June 2025 MCP Content Round-up**, Pomerium, Janvier 2026, https://www.pomerium.com/blog/june-2025-mcp-content-round-up
30. **Stratégie nationale de cybersécurité en santé 2026**, E-santé.gouv.fr, Janvier 2026, https://esante.gouv.fr/strategie-nationale/cybersecurite
31. **Cybersecurity Trends shaping governance in 2026**, Economy Middle East, Février 2026, https://economymiddleeast.com/news/6-cybersecurity-trends-shaping-governance-and-ai-adoption-in-2026/
32. **Deepfake incidents surge 10x year-over-year**, Integrate.io, Janvier 2026,

https://www.integrate.io/blog/b2b-data-sharing-security-statistics/

33. **Critical React Native bug (Metro4Shell) targets Windows and Linux**, SC World, 4 Février 2026, https://www.scworld.com/brief/attacks-involving-critical-react-native-bug-target-windows-linux-systems

Sources des citations

1. The State of AI Cybersecurity 2026 | Insights from 1,500+ Leaders, consulté le février 10, 2026, https://www.darktrace.com/blog/the-state-of-ai-cybersecurity-2026
2. 2026 Predictions for Autonomous AI - Palo Alto Networks, consulté le février 10, 2026, https://www.paloaltonetworks.com/blog/2025/11/2026-predictions-for-autonomous-ai/
3. Experts Weigh In: AI Trends for the IT Channel in 2026, consulté le février 10, 2026, https://www.channelinsider.com/ai/ai-trend-predictions-2026/
4. 6 cybersecurity trends shaping governance and AI adoption in 2026, consulté le février 10, 2026, https://economymiddleeast.com/news/6-cybersecurity-trends-shaping-governance-and-ai-adoption-in-2026/
5. the ai-fication of cyberthreats: trend micro security predictions for 2026, consulté le février 10, 2026, https://documents.trendmicro.com/assets/research-reports/the-ai-fication-of-cyberthreats-trend-micro-security-predictions-for-2026.pdf
6. Model Context Protocol: Understanding MCP security risks and prevention methods, consulté le février 10, 2026, https://www.giskard.ai/knowledge/model-context-protocol-understanding-mcp-security-risks-and-prevention-methods
7. OWASP MCP 10: External AIExposures You Must Prioritize in 2026 ..., consulté le février 10, 2026, https://www.msspalert.com/native/owasp-mcp-10-external-aiexposures-you-must-prioritize-in-2026
8. 2026 Public Sector Cyber Outlook: Identity, AI and the Fight for Trust - Palo Alto Networks, consulté le février 10, 2026, https://www.paloaltonetworks.com/blog/2026/01/public-sector-cyber-outlook/
9. Security Predictions 2026: What Agentic AI Means for the People Running the SOC | Splunk, consulté le février 10, 2026, https://www.splunk.com/en_us/blog/leadership/security-predictions-2026-what-agentic-ai-means-for-the-people-running-the-soc.html
10. The AI SOC is Here. Now What? 5 Rules for 2026 - Little Miss Data, consulté le février 10, 2026, https://www.littlemissdata.com/blog/aisoc2026
11. Geopolitical OSINT Threat Assessment Report (GOTAR): AI-Driven Cyber Threats and Risks in 2026 – Agentic AI, Ransomware, APT Convergence and Geopolitical Escalation Vectors - https://debuglies.com, consulté le février 10, 2026, https://debuglies.com/2026/02/05/geopolitical-osint-threat-assessment-report-gotar-ai-driven-cyber-threats-and-risks-in-2026-agentic-ai-ransomware-apt-convergence-and-geopolitical-escalation-vectors/

12. 9 AI Cybersecurity Trends to Watch in 2026 - SentinelOne, consulté le février 10, 2026, https://www.sentinelone.com/cybersecurity-101/data-and-ai/ai-cybersecurity-trends/
13. Gartner Identifies the Top Cybersecurity Trends for 2026, consulté le février 10, 2026, https://www.gartner.com/en/newsroom/press-releases/2026-02-05-gartner-identifies-the-top-cybersecurity-trends-for-2026
14. MITRE ATLAS: 15 tactics and 66 techniques for AI security - Vectra AI, consulté le février 10, 2026, https://www.vectra.ai/topics/mitre-atlas
15. The State of AI Cybersecurity 2026 - Darktrace, consulté le février 10, 2026, https://www.darktrace.com/resource/the-state-of-ai-cybersecurity-2026
16. June 2025 MCP Content Round-Up: Incidents, Updates, Releases, and more! - Pomerium, consulté le février 10, 2026, https://www.pomerium.com/blog/june-2025-mcp-content-round-up
17. Weekly Recap: AI Skill Malware, 31Tbps DDoS, Notepad++ Hack, LLM Backdoors and More - The Hacker News, consulté le février 10, 2026, http://thehackernews.com/2026/02/weekly-recap-ai-skill-malware-31tbps.html
18. B2B Data Sharing Security: 40 Critical Statistics for 2026-2026 | Integrate.io, consulté le février 10, 2026, https://www.integrate.io/blog/b2b-data-sharing-security-statistics/
19. ENISA THREAT LANDSCAPE 2025, consulté le février 10, 2026, https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf
20. ENISA Cybersecurity Threat Landscape Report 2025: Key takeaways for SMEs, consulté le février 10, 2026, https://www.digitalsme.eu/enisa-cybersecurity-threat-landscape-report-2025-key-takeaways-for-smes/
21. 'Bizarre Bazaar' campaign exploits exposed LLM endpoints | SC ..., consulté le février 10, 2026, https://www.scworld.com/brief/bizarre-bazaar-campaign-exploits-exposed-llm-endpoints
22. Canary Trap's Bi-Weekly Cyber Roundup, consulté le février 10, 2026, https://canarytrap.com/cyber-roundup-february-4/
23. 10 Hot Agentic SOC Tools In 2026, consulté le février 10, 2026, https://www.crn.com/news/security/2026/10-hot-agentic-soc-tools-in-2026
24. 2026 trends and predictions report, consulté le février 10, 2026, https://assets.ctfassets.net/xnqwd8kotbaj/6PYzA9LZXbMiy0kFGD1p6B/002d137c86cdb84962e7024c6d129689/RPT-0004_2026-trends-and-predictions-report_112025.pdf
25. ENISA 2025 NIS Investments Report: Technology Prioritized as Cyber Talent Pools Contract, consulté le février 10, 2026, https://complexdiscovery.com/enisa-2025-nis-investments-report-technology-prioritized-as-cyber-talent-pools-contract/
26. Projet de loi de finances pour 2025 : Direction de l'action du Gouvernement : Coordination du travail gouvernemental - Sénat, consulté le février 10, 2026, https://www.senat.fr/rap/a24-146-9/a24-146-9_mono.html
27. Cybersécurité : les attaques par rançongiciels en baisse chez les collectivités,

selon l'Anssi, consulté le février 10, 2026, https://www.banquedesterritoires.fr/cybersecurite-les-attaques-par-rancongiciels-des-logiciels-malveillants-en-baisse-chez-les

28. EU consistently targeted by diverse yet convergent threat groups - ENISA - European Union, consulté le février 10, 2026, https://www.enisa.europa.eu/news/etl-2025-eu-consistently-targeted-by-diverse-yet-convergent-threat-groups
29. The Hidden Dangers of MCP: Emerging Threats for the Novel Protocol - Jit.io, consulté le février 10, 2026, https://www.jit.io/resources/app-security/the-hidden-dangers-of-mcp-emerging-threats-for-the-novel-protocol