



LLM Enhanced Threats SOC Update Checklist



Sandy Dunn

Recognize generative AI as both a tool that adversaries will weaponize and a potential attack surface in your systems.

LLM-Enhanced Threat TTPs (Microsoft's Framework): Tactics where threat actors leverage AI to enhance traditional attack techniques.

Who Should Use This Checklist?

- ★ **CISOs:** Track threat actor trends and align with strategic risk decisions
- ★ **Cyber Threat Intelligence:** Map actors / campaigns to profiles
- ★ **Threat Hunters:** Look for behavioral patterns tied to known TTPs
- ★ **SOC Analysts:** Prioritize threats and response
- ★ **Red Team / Offensive Sec:** Emulate adversary TTPs during testing

General: Security Operations Center

- ☐ Update SIEM rules to alert for both traditional and AI enhanced attacker capabilities.
- ☐ Prioritize mitigations in high probability target areas using LLM enhanced tooling

Add SIEM Rules For

- ☐ LLM-informed Reconnaissance
- ☐ LLM-enhanced Scripting Techniques
- ☐ LLM-aided Development
- ☐ LLM-supported Social Engineering
- ☐ LLM-assisted Vulnerability Research
- ☐ LLM-optimized Payload Crafting
- ☐ LLM-enhanced Anomaly Detection Evasion
- ☐ LLM-directed Security Feature Bypass
- ☐ LLM-advised Resource Development

SIEM: What to Log / Alert Conditions / Log Source

TTP	What to Log	Alert Conditions	Log Sources
LLM-informed Reconnaissance	Web traffic logs (URLs, queries) API access logs (LLM API usage) OSINT scraping activities	Abnormal access to tech/vendor docs burst of reconnaissance-related queries unusual LLM API key exhaustion or traffic spike	Web Proxies API Gateways DNS Logs Cloud SaaS Monitoring

LLM-enhanced Scripting Techniques	Script execution logs File creation logs (scripts) LLM API prompts	New script files with LLM generation patterns Sudden script usage from non-developer endpoints Excessive PowerShell/Bash/CMD command activity	EDR/AV Logs Endpoint Process Logs Cloud IDE/Developer Tool Logs
LLM-aided Development	Source code repository access Compile/build logs Malware sandbox submission logs	Source code uploads with AI-generated traits Low-reputation binaries matching GPT-style structures	DevOps Tooling (GitHub, GitLab Audit Logs) Sandbox/Threat Intel Feeds Source Code Management (SCM) Logs
LLM-supported Social Engineering	Email gateway logs Messaging app logs (Teams, Slack) Content scanning for language patterns	Spike in multilingual emails Emails with AI-optimized social engineering phrases	Email Security Gateway (SEG) Logs Messaging Security Logs DLP Tools
LLM-assisted Vulnerability Research	Vulnerability scanning logs API usage for vuln queries Web application firewall (WAF) logs	High-frequency vulnerability scans Novel scan signatures (non-standard nmap, burp scans) Prompt logs querying for CVEs	Vulnerability Scanner Logs (Qualys, Nessus) WAF Logs API Gateway Monitoring
LLM-optimized Payload Crafting	Malware detection logs E-mail attachment scans File integrity monitoring (FIM) logs	New payloads bypassing signatures Evasive payload delivery attempts	AV/EDR Logs Sandbox Analysis Email Security Logs
LLM-enhanced Anomaly Detection Evasion	User behavior analytics (UBA) Network traffic logs Process injection/evading behaviors	Synthetic login behaviors Unusual low and slow traffic Log tampering or deletion attempts	UEBA Tools (User and Entity Behavior Analytics) SIEM Native Analytics Network Traffic Analytics (NTA)






LLM-directed Security Feature Bypass	Authentication logs (SSO, MFA events) CAPTCHA challenge/response logs Brute force detection logs	Failed login surges followed by success CAPTCHA bypass anomalies impossible travel detections	IAM Logs (Okta, Azure AD) Web Application Logs Bot Detection Systems
LLM-advised Resource Development	Build server logs code repository access malware deployment attempts	Rapid dev cycles new C2 infrastructures or unusual tool uploads	DevSecOps Logs Threat Intelligence Feeds Build Server Logs (Jenkins, CircleCI)

MITRE ATT&CK / ATLAS ID and Example IOC

LLM TTP	Description	ATT&CK ID	ATLAS ID	Sample IOCs
LLM-informed reconnaissance	Using LLMs to gather actionable intelligence on technologies & potential vulnerabilities	T1592, T1595	TA0031	Suspicious OSINT scraping, abnormal LLM API usage
LLM-enhanced scripting techniques	Using LLMs to generate or refine scripts to use in cyberattacks	T1059	TA0002	High rate of script generation, AI-generated code artifacts
LLM-aided development	Using LLMs in the development lifecycle of tools and programs, including those with malicious intent, such as malware.	T1587	TA0002	AI-style malware source code, fast tool iteration
LLM-supported social engineering	Leveraging LLMs for assistance with translations & communication, likely to establish connections or manipulate targets.	T1566	TA0003	Sophisticated phishing emails, multilingual spear-phishing
LLM-assisted vulnerability research	Using LLMs to understand & identify potential vulnerabilities in software & systems, which could be targeted for exploitation.	T1595.002	TA0032	Abnormal vuln search patterns, AI-model queries

LLM-optimized payload crafting	Using LLMs to assist in creating & refining payloads for deployment in cyberattacks.	T1203	TA0002	Fast-evolving obfuscated payloads
LLM-enhanced anomaly detection evasion	Leveraging LLMs to develop methods that help malicious activities blend in with normal behavior or traffic to evade detection systems.	T1070, T1562	TA0005	Synthetic user behavior, adversarial noise injection
LLM-directed security feature bypass	Using LLMs to find ways to circumvent security features, such as two-factor authentication, CAPTCHA, or other access controls.	T1556, T1110	TA0035	MFA bypass attempts, CAPTCHA solving patterns
LLM-advised resource development	Using LLMs in tool development, tool modifications, and strategic operational planning.	T1587	TA0002	Rapid tool iteration, playbooks with perfect grammar

QR Link for additional Checklists

- ★  Organization AI Security Preparedness Short List
- ★  AI System Card Review Checklist
- ★  2025 IR Update Checklist AI Incident Response
- ★  2025 SIEM Run book for GenAI Incident Investigation
- ★  AI Updates for Organization's Enterprise Risk Register

