AYI NEDJIMI Consultants

SOC augmenté par IA — SIEM, LLM

16 mai 2026 • Mis à jour le 17 mai 2026 • 20 min de lecture • 3063 mots •

Construisez un SOC augmenté par IA : architecture SIEM+LLM+SOAR, tria
par IA, métriques MTTD/MTTR. Guide complet pour SecOps 2026.

À RETENIR

A retenir -- SOC augmente par IA

Le **SOC augmente par IA** n'est plus une vision futuriste : en 2026, l'integratio
MTTD de 40 a 65% et divise par deux le taux de faux positifs traites manuell
(Splunk, OpenSearch) pour la correlation d'alertes, un LLM local pour la sum
l'execution automatisee des playbooks. Le human-in-the-loop reste indispen
succes : commencer par l'alert summarization, mesurer les gains, puis eten

La montee en puissance des cyberattaques sophistiquees -- rançongiciels a doub
chain attacks -- confronte les equipes SOC a un par l'alertes do
d'analystes qualifies stagne. Le **SOC augmente par** la reponse

integrant des LLM dans le pipeline d'analyse des alertes, les organisations pionniè
du MTTD (Mean Time to Detect) de 40 a 65%, division par 3 du cout de traitemen
couverture de detection. En 2026, les architectures de reference combinent des S
OpenSearch/Wazuh) avec des LLM locaux ou cloud pour la summarization intellig
Swimlane, Shuffle) pour l'execution automatisee des playbooks de remediation. C
l'implementation et la mesure d'un SOC augmente par IA, avec des benchmarks re
demarrer rapidement.

Architecture de reference SOC IA -- les trois couches

L'architecture d'un **SOC augmente par IA** efficace repose sur trois couches compl
pour maximiser les gains operationnels tout en maintenant la qualite de detection
critiques.

La **couche de collecte et correlation** (SIEM) reste le socle incontournable. Elle ing
de correlation (SIGMA, Elastic Detection Rules) pour generer des alertes, et enrich
MITRE ATT&CK, assets affectes). Les SIEM modernes integrent deja de l'apprentis
comportementales (UEBA).

La **couche d'intelligence IA** (LLM) recoit les alertes brutes du SIEM et les enrichit
comprehensible par un analyste L1, scoring de severite contextualise (pas seulem
next steps d'investigation, et correlation avec des incidents passes similaires stoc

La **couche d'execution automatisee** (SOAR) transforme les analyses du LLM en a
firewall, creer un ticket Jira, envoyer une notification Teams, ou escalader vers un
actions a fort impact (suppression de comptes, isolation de serveurs de productio

Réponse sous 24h

Devis gratuit →