TUSKIRA BUYER'S SHEET · NOVEMBER 2026

AI SOC Platforms Compared

12 platforms by type, data reach, response model, best fit and main caveat.

Tuskira™

Platform	Type	Data reach	Response model	Best fit	Main caveat
Tuskira	AI SOC plus exposure management	200+ integrations, queried in place	Proposes containment through existing controls, inside autonomy limits you set	Teams that want investigations to see breach paths and exposure	More platform than you need if alert triage is the only goal
7AI	Standalone agent platform	Federated SIEM that queries data in place	Agents across cloud, email, identity and EDR	Teams that want whole-SOC coverage sold as a service	Autonomy levels aren't specified publicly
Conifers.ai	Standalone agent platform	90+ integrations	Graduated autonomy with an Act function	MSSPs and multi-tenant operations	Built first for providers, not single enterprises
Prophet Security	Standalone agent platform	200+ integrations	Scoped Agent Actions, autonomous or with sign-off	Teams that want analyst, hunter and detection engineer agents in one place	Specific response actions aren't documented publicly
UnderDefense Agentic AI SOC	Standalone agent platform with managed analysts	250+ integrations; SaaS, on-prem or air-gapped	Agents triage and investigate, analysts take critical alerts within a 20-minute SLA	Teams that want agents plus 24/7 human coverage on their existing stack	Sold with a managed analyst service, so it's more than software-only teams need
Dropzone AI	Standalone investigation layer	90+ integrations queried by API	Analyst-authorized, or handed to SOAR	Teams that want every alert investigated without changing their stack	Response is mostly left to analysts or SOAR
D3 Morpheus	Automation platform with agents	800+ integrations	Four autonomy modes, approval gates and rollback	Teams that want governed, deterministic autonomy	Onboarding is a scoped project, with a 60 to 90 day ramp
Torq HyperSOC	Automation platform with agents	300 integrations	Agent-run cases plus hyperautomation steps	Teams with SOAR maturity that want agents on top	Value assumes investment in building workflows
Exaforce	SIEM replacement with agents	Its own data platform, 100+ sources	Agents across detect, triage, investigate and respond	Cloud and SaaS-heavy teams ready to replace the SIEM	A bigger commitment than an overlay
CrowdStrike Charlotte AI	Platform-native	Falcon telemetry, third-party data through Next-Gen SIEM	Recommends by default, actions need approval	Falcon-committed shops	Strongest where Falcon's data reaches
Google SecOps	Platform-native	Google SecOps data	Triage agent generally available, response agents in preview	Teams already running Google SecOps	Response capabilities are still in preview
Microsoft Security Copilot	Platform-native	Microsoft security products	Prebuilt agents per Microsoft product	Microsoft-centric estates, especially on E5	Agents are tied to individual Microsoft products

Questions to ask every vendor in a bake-off

1. Run the evaluation on **a week of your own alerts**, and compare verdicts with what your analysts decided.
2. Show a **false positive it closed**, and the evidence it used.
3. Show an **escalation it got right** that a person missed.
4. Show a **verdict it got wrong**, and how you'd have caught it.
5. Open the **audit trail** for one verdict. Can an analyst check the reasoning?
6. What can the agent do **without approval**, and can you undo it?
7. Whose data can it reason over: your whole stack, or one vendor's?
8. What does the **bill look like at your real alert volume** over two years?

Descriptions reflect public vendor information as of October and November 2026. Performance figures are vendor-reported; verify current capabilities with each vendor. Tuskira is one of the platforms listed. Platforms are grouped by type after Tuskira and listed alphabetically within each group, not ranked. Full guide, with each platform's details and FAQ, at **tuskira.ai/blog/best-ai-soc-platforms**