SentinelOne

Security Operations Checklist

Protecting your Business in the Age of AI

Is your organization ready for autonomous security operations? Security teams are under constant pressure to stay ahead of rapidly evolving threats, and the platforms they rely on are transforming rapidly in response. At the forefront of this movement is the shift of Artificial Intelligence (AI) technology from a tactical tool into a strategic advantage for defenders. Leading this wave is agentic AI: systems that not only analyze data but actively take initiative, make decisions, and act independently.

Security Operations Centers (SOCs) are adopting agentic AI to reduce complexity, increase precision, and respond faster than ever before. AI's capabilities offer the promise to transform nearly every workflow, from data ingestion and normalization to real-time threat analysis and response. Here are some ideas to get you thinking about how AI can help your organization transform security operations.

	SOC Platform Challenge	AI can help with...
Data Ingestion and Normalization Broad and deep telemetry is the lifeblood of detection and response workflows.	**Incomplete Visibility:** Is our SOC ingesting all the data and telemetry that we need in order to effectively identify, understand, and respond to threats?	**Autonomous Discovery:** AI can analyze incoming telemetry and other signals to uncover uncataloged devices and data sources, helping to ensure 100% coverage.
	Normalization: How can we reduce the engineering effort needed to parse and normalize new data sources in our SOC?	**Intelligent Parsing:** AI can analyze and interpret sample logs, immediately identifying key fields and creating parser logic, automating tasks that once took hours or days.
Automated Analysis SOCs rely on analytics engines to surface meaningful signals from massive telemetry.	**Anomaly Detection:** Can we identify unusual and potentially threatening behaviors across our network in real-time, at scale?	**Behavioral Analysis:** AI can learn "normal" behavior and flag deviations to analysts, increasing detection fidelity.
	Multi-signal Detection: Can detection logic incorporate insights across different data sources, to ensure maximum fidelity and accuracy?	**Automated Correlation:** AI can continuously correlate insights from diverse sources and surface threats with full context, helping analysts focus on high-impact events.
Investigation and Threat Hunting Security analysts need intuitive and friction-free tools to help them quickly understand the scale and scope of potential threats.	**Ambiguous Alerts:** How do we reduce the manual effort analysts expend in order to get the basic context necessary to understand a potential threat?	**Contextual Awareness:** AI can simplify reporting with automatically generated natural language summaries, enriched with context and threat intelligence, aiding in quicker and more accurate threat triage and investigation.
	Query Complexity: Can every analyst get fast answers to all the questions they may have in order to fully understand a potential threat quickly?	**Natural Language Queries:** Transitioning from highly technical query languages into natural language is a game changer, dramatically lowering the barrier to getting answers to critical questions out of your SOC platform.

	High Skill Threshold: How much experience and training does an analyst need in order to effectively investigate and understand an emerging threat?	**Guided Investigation:** Sometimes the toughest part of understanding a threat is knowing the next question to ask. AI systems can guide analysts down the optimal path.
	Poor Prioritization: How do we ensure that the most critical potential incidents are the ones at the top of the queue?	**Risk Assessment:** AI models can assess the risk level of various alerts, helping prioritize SOC investigation and response efforts.
	Limited Hunting: How can we democratize threat hunting and empower more staff to hunt for stealthy threats?	**Guided Hunts:** Agentic AI can launch hunts independently, proactively surfacing suspicious activity and empowering any analyst to become an expert threat hunter.
Decision and Action Once analysts have sufficient understanding of a threat, it's time to act. An effective SOC platform empowers defenders to disrupt attacks before a damaging breach can happen.	**Slow Response:** How can I empower more analysts to take fast and decisive action to neuter emerging threats in minutes without escalation?	**Decision Support:** AI can provide real-time response recommendations based on built-in expert knowledge and historical context.
	Limited Automation: Can I speed up response even more by taking the human out of the loop?	**Automated Response:** For incidents where the risk of false positives is low and the risk of damage is high, AI can automate response actions, speeding up the mitigation process dramatically.
Continuous Improvement Every encounter with an adversary creates opportunities to learn and improve results.	**Groundhog Day:** Once a threat is eradicated, how do we learn from the experience so we can deal with it more efficiently next time?	**Self-Improvement:** AI systems can continuously learn from new data, improving their accuracy and effectiveness over time.

AI is a foundational component of a SOC platform that can stand up to sophisticated threats of today and tomorrow. SentinelOne is leading the charge in agentic AI, empowering defenders with a platform that continuously learns, combines human intelligence with AI reasoning, and drives efficiency for the SOCs of tomorrow with a unified AI-powered control plane that scales autonomous protection across the enterprise.

Innovative. Trusted. Recognized.

Gartner

A Leader in the 2024 Magic Quadrant for Endpoint Protection Platforms

MITRE ENGENUITY

Industry-leading ATT&CK Evaluation

+ 100% Detections. 88% Less Noise
+ 100% Real-time with Zero Delays
+ Outstanding Analytic Coverage, 5 Years in a Row

Gartner Peer Insights

96% of Gartner Peer Insights™

EDR Reviewers Recommend SentinelOne Singularity

FedRAMP · TEVORA PCI DSS Attestation HIPAA Attestation · AICPA SOC · STAR Level One · Virus 100 · SE Labs Best Innovator Winner 2021 · SE Labs AAA · Cloud Security Alliance Trusted Cloud Provider CSA

About SentinelOne

SentinelOne is the world's most advanced cybersecurity platform. The SentinelOne Singularity™ Platform detects, prevents, and responds to cyber-attacks at machine speed, empowering organizations to secure endpoints, cloud workloads, containers, identities, and mobile and network-connected devices with intelligence, speed, accuracy, and simplicity. Over 11,500 customers—including Fortune 10, Fortune 500, and Global 2000 companies, as well as prominent governments—all trust SentinelOne to Secure Tomorrow.

sentinelone.com

sales@sentinelone.com
+1 855 868 3733