securonix DATASHEET

MEET SAM

YOUR ALWAYS-ON AI SOC ANALYST

Trusted AI that Scales Modern Security Operations

Sam, the Securonix AI SOC Analyst, is your always-on digital co-pilot and tireless SOC teammate. Natively embedded within the Securonix Unified Defense SIEM and powered by the Securonix Agentic Mesh, Sam orchestrates specialized AI agents into a single, governed system that accelerates investigations, reduces analyst fatigue, and delivers explainable audit ready outcomes.

Sam helps security teams modernize SOC operations by combining AI-driven scale with human oversight, policy-alignment, and full transparency. Every action is auditable, every recommendation explainable, and every outcome measurable.

- **Automate with confidence** — Explainable, governed AI automates Tier 1 and Tier 2 tasks while maintaining full compliance.
- **Reduce manual work** — Up to 60% less investigation time through intelligent triage and contextual insight.
- **Accelerate response** — 3× faster incident resolution using adaptive AI Agents that correlate data and context.
- **Deliver measurable savings** — Organizations using Sam have achieved up to $2M annual savings through reduced labor costs, optimized data ingestion, and lower analyst fatigue.

Transform Your SOC Operations

See how Sam enhances productivity, compliance, and visibility across your SOC.

Alert Triage Automation

Automates enrichment, contextualization, and correlation to reduce Tier 1 workloads by up to 80%.

Compliance and Audit Reporting

Delivers explainable, traceable investigations aligned with NIST, ISO 27001, and enterprise frameworks.

Incident Correlation & Summarization

Links related events, adds deep investigative context and produces clear, actionable summaries.

Executive Threat Briefings

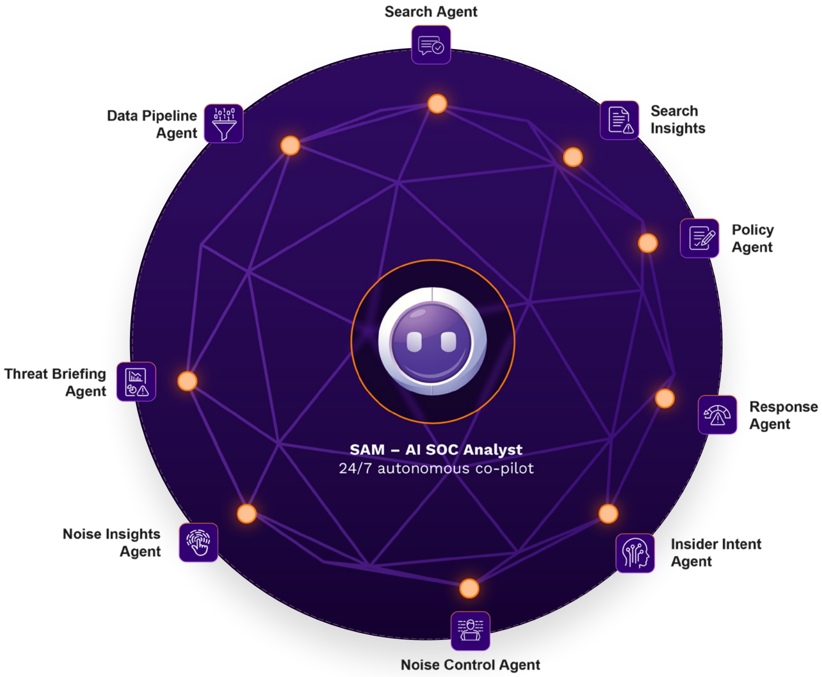
Generates plain-language reports that translate SOC activity into business-relevant risk insights for technical and non-technical stakeholders.

60% less manual investigation time

80% reduction in Tier 1 workloads

How Sam Works

Sam operates as part of the Securonix Agentic Mesh, a governed orchestration layer that coordinates users, data, and AI agents across SOC workflows. Rather than acting as a black box, Sam exposes its reasoning, maintains human-in-the-loop control, and enforces policy at every step. Sam brings together a modular ecosystem of AI agents, from reducing alert noise to generating board-ready threat briefings, every agent contributes to measurable outcomes in speed, clarity, and risk reduction. Here's how each Agent adds value across the SOC:



Noise Control Agent

REDUCE ALERT FATIGUE

Removes duplicates and false positives to deliver a cleaner, more actionable alert queue.

Insider Intent Agent*

PROACTIVELY IDENTIFY INSIDER THREATS

Applies behavioral analysis to surface potential malicious or negligent activity before it causes harm.

**Licensed separately*

Search Agent (NLP)

SIMPLIFY INVESTIGATIONS

Enables natural-language search to quickly find, correlate, and explore security data.

Search Insights Agent

STRENGTHEN CONTEXT

Interprets search results and highlights anomalies or emerging risks to guide faster decision-making.

Response Agent

ACCELERATE DECISION-MAKING

Correlates related incidents and provides next-step recommendations with business-aware reasoning.

Policy Agent

ACCELERATE DETECTION RULE CREATION

Translates analyst intent into accurate, AI-generated detection logic, reducing manual effort.

Threat Briefing Agent

COMMUNICATE CLEARLY

Converts technical threat data, TTPs and campaigns to help CISOs communicate risk credibility to executives and boards.

Data Pipeline Agent

OPTIMIZE DATA FLOW

Routes telemetry to improve visibility, control ingestion costs, and meet compliance needs.

Global Energy Company Boosts SOC Efficiency and Governance

A global energy provider deployed Sam across its hybrid SOC to unify triage, investigation, and reporting.

Before Sam, each incident correlation took an average of 40 minutes and required multiple tools.

AFTER SIX MONTHS:

- Investigation time dropped to **4 minutes per case**
- Tier 1 triage became **80% automated**
- Audit readiness improved with real-time compliance dashboards
- **Annual operational savings exceeded $2 million**
- Executives gained real-time visibility into SOC performance and risk posture

This deployment demonstrated how explainable AI can drive measurable ROI while improving governance and trust.

Sam operates within Securonix Unified Defense SIEM, featuring:

- Explainable AI Guardrails
- 24/7 automation and visibility
- Full human oversight
- Flexible usage and overage options

Transparent, Value-Based Pricing

Sam's pricing is simple, predictable, and directly tied to measurable analyst productivity. Every AI Agent interaction tracks time saved and time billed. Billed time is deducted from Sam's 250-hours per 30-day billing cycle, visible in the Securonix Operations Center for complete transparency.

Concept	Description
1 Sam = 250 hours/month	Each Sam delivers up to 500 minutes of productive work per day. Time saved and time billed are fully visible.
List Price	$15,000 per AI SOC Analyst per year
Complementary Allocation	Customers receive 1–7 Sam units based on their licensed GB/day tier.

Turning Reactive Defense Into Proactive Intelligence

The SOC of the future is explainable, governed, and outcome-driven. Sam bridges the gap between data and decisions by uniting automation, analytics, and governance within a single framework.

- ✓ For **CISOs**, Sam builds measurable ROI, trust, and compliance.
- ✓ For **analysts**, it eliminates repetitive tasks and accelerates insight.
- ✓ For **executives**, it delivers transparent metrics that prove the business value of cybersecurity operations.

Sam brings structure to complexity, connecting the dots between raw telemetry and trusted action. By combining automation with analyst intent and enterprise governance, Sam empowers SOC teams to move with speed and confidence, knowing every decision is backed by context, transparency, and control.

Compare Sam

Sam combines human expertise with the speed and scale of AI, delivering decisions that are transparent, explainable, and fully auditable. It's never a black box, and never left to guesswork.

Capability	Sam (AI SOC Analyst)	Traditional SOC	Legacy Automation Tools
Continuous 24/7 Analysis	✓ Yes	✗ No	! Partial
Explainable AI Actions	✓ Full traceability	✗ None	! Limited
Compliance Validation	✓ Agentic Guardrails	✗ Manual	! Add-on only
Human Oversight	✓ Built in	✓ Manual	✗ Absent
Time Saved per Month	**250 hours**	0	~20% efficiency gain

Specifications

Specification	Function
AI	1 Sam = 250 hours per month (500 minutes per day).
Consumption Model	Monthly reset of time; no rollover.
Integration	Native to Securonix Unified Defense SIEM.
Compliance	Governed by Agentic Guardrails and audit logs.

Built on Trusted Data.

Effective AI requires high-quality, governed data. Sam operates directly on telemetry already ingested, normalized, and enriched within the Securonix platform, including identity, endpoint, network, cloud, and application data.

This native, data-first architecture ensures:

- Accurate cross-domain correlation
- Explainable and auditable AI outcomes
- Policy-controlled data handling
- Cost-aware ingestion and routing

Governance, Trust, and Explainability

Sam is designed for regulated and risk-averse environments:

- Human oversight is enforced by default
- All AI actions are logged and auditable
- Enterprise policies are enforced through Agentic Guardrails
- Explainable reasoning is visible within investigations

Sam is never autonomous. Analysts retain decision authority while AI accelerates the work.

securonix

Explore the Impact of Sam on Your Security Operations

To learn more about Sam, the AI SOC Analyst, visit

www.securonix.com/Sam