SIRP

DATASHEET

AI-DRIVEN.
AGENTIC BY DESIGN.

BUILT FOR THE NEXT GENERATION
OF SECURITY OPERATIONS.

OVERVIEW

SIRP is not just evolving; it's transforming.

Our platform is now a fully AI-powered, adaptive security operations ecosystem - built from the ground up on a distributed agentic mesh architecture.

This shift allows SIRP to operate beyond conventional security automation, moving toward a future where security becomes self-orchestrating, intelligent, and continually improving.

At the core of this transformation is OmniSense™, our proprietary intelligence engine that coordinates a growing network of specialized AI agents.

Each agent is purpose-built to tackle a distinct part of the incident lifecycle - correlation, triage, response, remediation, scoring, assignment, and playbook generation.

SIRP EMPOWERS ORGANIZATIONS TO:

Reduce Mean Time to Respond (MTTR) by up to 70%

Automate up to 80% of tier-1 analyst workflows

Increase alert triage speed by 5x

Minimize noise and false positives through intelligent correlation

With a cloud-native, microservices-based deployment model, SIRP supports unlimited scalability and seamless integration. AI is embedded at every layer - from enrichment and decision support to workflow generation and task orchestration.

THE AGENTIC MESH FRAMEWORK

Unlike monolithic AI, SIRP's Agentic Mesh is a modular, distributed system of collaborative AI agents, orchestrated by OmniSense™. OmniSense™ handles real-time task routing, agent coordination, and decision-making using shared context and system-wide memory.

As agents operate, they learn from user feedback. This fuels continuous retraining, aligning agent behavior with analyst decisions and organizational patterns. The result: an adaptive AI ecosystem tailored to your security posture and operational rhythm.

SPECIALIZED AI AGENTS IN THE MESH

AGENT	FUNCTION
RISK SCORING AGENT (S3)	Calculates real-time incident risk scores by analyzing alert metadata, asset sensitivity, threat intel, and business context
AUTO - ASSIGNMENT AGENT	Automatically assigns cases based on analyst availability, expertise, workload history, and SLA urgency
INCIDENT ANALYSIS AGENT	Extracts key artifacts and IOCs from raw alerts and enriches them with context-aware metadata for deeper analysis
INCIDENT REMEDIATION AGENT	Recommends targeted remediation actions by analyzing attack techniques, vulnerabilities, asset configurations, and past response outcomes
RESPONSE WORKFLOW AGENT	Auto-generates step-by-step workflows for resolving incidents, based on incident type, risk score, and organizational response history.
RESPONSE ACTIONS AGENT	Auto-generates step-by-step workflows for resolving incidents, based on the best way to remediate
RESPONSE PLAYBOOK AGENT	Enables security teams to trigger recommended actions with a single click

Each of these agents operates independently but communicates through shared context provided by OmniSense™, forming a highly coordinated, AI-native security infrastructure.

SARA:

YOUR TIRELESS TIER-1 ANALYST, WORKING AT 5X SPEED

Sara functions as your AI-powered Tier-1 analyst, built directly into the SIRP ecosystem. She handles high-volume, repetitive triage tasks 5x faster than a typical human analyst delivering measurable cost savings and freeing your team to focus on strategic decisions.

1 SARA = 5X THE SPEED OF A TRADITIONAL T1 ANALYST = 5X THE COST EFFICIENCY.

Today, SARA performs the essential functions of an entry-level analyst with speed and consistency:

01 **Generates real-time incident summaries** for immediate understanding

02 **Recommends remediation details** based on context and past outcomes

03 **Surfaces workflow actions** tailored to the incident

04 **Auto-assigns analysts** using intelligent routing logic from the Auto-Assignment Agent

But SARA isn't static. As she begins leveraging the broader **Agentic Mesh**, she will evolve into a more advanced operator, using the capabilities tof agents like the response actions agent, and response playbooks agent to **upgrade herself beyond Tier-1 boundaries.**

SECURITY & PRIVACY FIRST

CONTROL	FUNCTION
SELF-HOSTED	SIRP is hosting an internal, self-contained LLM for full privacy and data sovereignty
RBAC & ACCESS CONTROL	Granular permissioning at module, role, and case levels
IMMUTABLE AUDIT LOGS	All activities are logged and timestamped
OUR COMPLIANCES	SOC 2, ISO 27001

INCIDENT MANAGEMENT

STATE-OF-THE-ART RESPONSE, BUILT FOR THE REAL WORLD.

SIRP delivers next-gen incident management with built-in case management, enabling your SOC to manage the complete lifecycle of incidents from a single, unified console. Each case is enriched, correlated with relevant alerts, assigned based on role or severity, and progressed through customizable workflows.

With robust audit trails, collaborative tools, SLA tracking, and automated remediation steps, your team is always operating at peak efficiency.

VULNERABILITY MANAGEMENT

TURN GAPS INTO ACTIONABLE FIXES.

Take control of your entire vulnerability management program with SIRP, from executing manual and automated assessments to managing remediation processes end-to-end.

Gain real-time visibility into your attack surface through a centralized asset repository, vulnerability consolidation and prioritization, and integrated issue management workflows. Contextual risk scoring helps you focus on what matters most, while threat intelligence driven vulnerability monitoring ensures emerging risks don't go unnoticed.

THREAT INTELLIGENCE

ACTIONABLE INTEL AT YOUR FINGERTIPS.

Go beyond traditional threat feeds with visibility that fuses organizational context and risk posture into a dynamic, global threat outlook. SIRP provides a centralized platform for aggregating, normalizing, and operationalizing threat intelligence from multiple internal and external sources.

Get access to real-time cyber threat intelligence, tailored to your environment, with automated IOC enrichment, indicator lifecycle management, and correlation with active incidents. Feed intelligence directly into playbooks to enable rapid, automated responses—reducing noise and helping your team stay ahead of emerging threats with confidence and clarity.

S3 AND ASSET RISK MANAGEMENT

KNOW WHAT YOU HAVE.
SECURE WHAT MATTERS.

Maintain a real-time inventory of assets, including cloud buckets, endpoints, and applications, while continuously evaluating their risk posture. SIRP dynamically maps asset relationships, evaluates vulnerabilities, and surfaces misconfigurations. With asset-driven risk scoring and contextual enrichment, you can prioritize remediation and reduce the overall attack surface.

DASHBOARDS & REPORTS

FROM DATA TO DECISIONS — INSTANTLY.

Monitor, measure, and manage your security operations with real-time dashboards and reports powered by **pre-built widgets** and complete **data customization.**

SIRP gives you the flexibility to visualize any data point in the platform: incidents, vulnerabilities, asset risk, threat intelligence, and more by simply dragging and dropping widgets onto your dashboard. Whether you're tracking KPIs, SLA compliance, or operational trends, our **interactive dashboards** adapt to your team's specific needs.

SIRP