SIRP

WHITEPAPER|2025

DISRUPTING L1 INCIDENT RESPONSE WITH OMNISENSE™ AND SARA

EXECUTIVE SUMMARY

Security operations centers (SOCs) world-wide struggle to handle an exploding volume of alerts and incidents, typically relying on expensive and hard-to-train Level 1 (L1) analysts. **SIRP** has redefined the game by introducing **Omnisense™** - our intelligence engine built on an **Agentic Mesh** - and **Sara**, the AI-driven L1 analyst who processes, investigates, and remediates routine incidents at machine speed

With **Omnisense™** powering continuous learning at a pace beyond any human analyst, Sara seamlessly automates up to 90% of Tier-1 tasks and can autoremediate 95% of security cases. In a field where time is everything, this level of automation translates directly into significant cost savings, faster resolution, and unmatched scalability

> **I saw it in action and can only imagine the disruption it's going to cause in the cybersecurity world. Handling 50 times the work of a single analyst is just wild**
>
> *— Beta Tester from SIRP's Early Access Program*

KEY REASONS TO READ ON

- Discover how Omnisense's interconnected AI framework delivers hyper-accurate, proactive threat detection
- Understand how Sara frees your skilled analysts from repetitive tasks, cutting mean time to resolution (MTTR)
- Learn how automating L1 tasks can yield massive ROI through reduced hiring and training overhead

INTRODUCING OMNISENSE™

Typical AI solutions rely on a single, isolated agent. Omnisense™ takes a radically different approach with its Agentic Mesh architecture

- **Interconnected Specialized Agents**

  Each agent focuses on a different dimension of security (network traffic, endpoint behavior, user access patterns, and more), sharing insights with the mesh in real time

- **Continuous, Accelerated Learning**

  Unlike human analysts - who need months of expensive training - Omnisense™ scales its knowledge base at exponential rates, absorbing new threat intelligence and refining detection algorithms instantly

- **Adaptive Collaboration**

  Information from one agent instantly enhances the decision-making across all agents, enabling unprecedented precision in triage and remediation

  This unique ecosystem approach fuels Sara, ensuring that every incident response workflow benefits from deeply contextual, always-updating intelligence

MEET SARA: THE AI L1 ANALYST

Sara is the AI-driven centerpiece of the Omnisense™ ecosystem, dedicated to elevating **Level 1 (L1) incident response**. At present, she excels at delivering comprehensive **case analysis summaries**, identifying **potential vulnerabilities**, and **recommending remediation steps** - all within a single, unified interface. By synthesizing relevant data such as threat status, historical context, and recommended next steps, Sara helps security teams see the entire picture at a glance. This clarity enables analysts to make decisions faster and more confidently, reducing both human error and the need for repetitive manual tasks

One of Sara's most compelling features is her capacity to transform case summaries into **directly actionable tasks**. Instead of leaving teams to piece together complex instructions from different tools, Sara presents analysts with a succinct, **prioritized list of steps** that can be executed on the spot. Beyond simply informing analysts of what needs to be done, Sara also takes on the responsibility of **auto-assigning tasks** based on each team member's workload, skill set, and availability. This real-time routing ensures incidents are managed by the most qualified person without administrative bottlenecks, expediting the entire remediation process

But Sara's journey doesn't end there. We're currently training her to expand from her L1 roots into **new levels of operational autonomy**. Soon, she will not only provide robust investigative insights and workflow actions but also have the capability to **propose and build full-fledged playbooks**. These playbooks serve as dynamic, step-by-step guides that unify best practices, corporate policies, and threat intelligence into a coherent response strategy. By developing this capacity, Sara is set to reduce the burden on human analysts even further, bridging the gap between detection and resolution with **minimal need for manual oversight**

In a world where cybersecurity talent is in short supply and the stakes are high, Sara's ability to operate continuously- without fatigue, shift changes, or inconsistency - gives organizations a critical advantage. By offloading routine tasks and enhancing response quality, Sara frees up your most skilled security professionals to concentrate on complex or high-impact threats. This combination of tireless automation and intelligent, context-aware decision-making allows businesses to strengthen their security posture while containing labor costs. As Sara continues to evolve, so too does the promise of a more adaptive, **truly autonomous**, resilient, and forward-looking cybersecurity operation- one that grows hand in hand with the ever-shifting threat landscape

THE CYBERSECURITY CHALLENGE

Sara's prime advantage is its ability to run continuously without the downtime or human error inherent to manual labor - particularly valuable for organizations dealing with a worldwide shortage of qualified security analysts

- **Command High Salaries**

  In the U.S., an entry-level L1 analyst can range from **$60,000 to $85,000** per year, excluding overhead costs

- **Require Lengthy Training**

  Junior hires spend weeks to months mastering internal tools, policies, and playbooks

- **Demand Constant Supervision**

  Mistakes can lead to overlooked incidents or delayed response times

This model is both expensive and slow to adapt. As alert volumes spike, organizations scramble to hire, train, and retain more L1 analysts - an uphill battle in a hyper-competitive talent market

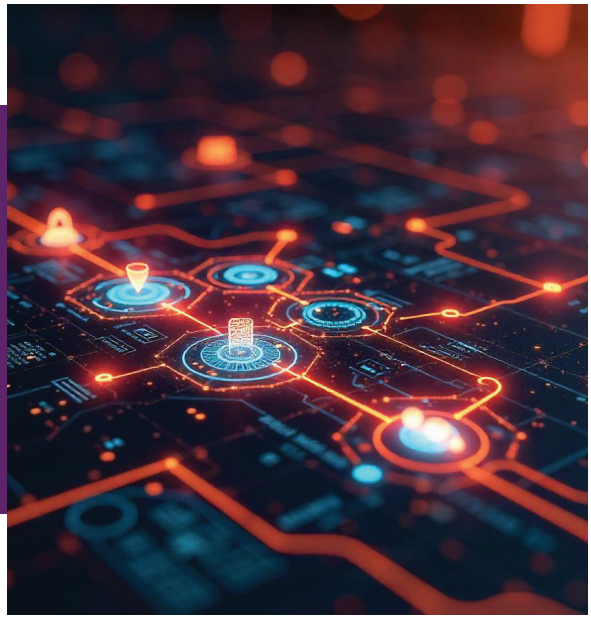
Sara solves this by taking over repetitive alert-handling, letting senior analysts focus on complex scenarios where human intuition truly excels. This frees resources, accelerates response, and curbs the operational cost of continuous recruitment and training

BENEFITS & ROI: REAL METRICS THAT MATTER

Powered by Omnisense™, Sara delivers tangible results that align with key priorities for CISOs and IT managers

1 AUTOMATE UP TO 90% OF TIER-1 TASKS

- **Time Savings:** Converts natural language queries into easy-to-execute task
- **Lower Risk of Burnout:** Relieves human analysts from mind-numbing tasks, boosting morale



1 AUTOREMEDIATE UP TO 95% OF SECURITY CASES

- **Speed & Accuracy:** Quick containment of threats within minutes, drastically reducing the mean time to resolution (MTTR)task
- **Standardized, Error-Free Responses:** SOC-defined runbooks guide every remediation, maintaining consistency and compliance

1 AUGMENT HUMAN EXPERTISE

- **Machine-Speed Analysis:** Even entry-level analysts can achieve advanced results, backed by Omnisense's integrated intelligenceeasy-to-execute task
- **Continuous Upskilling:** L1 analysts learn from Sara's investigations, elevating overall team proficiency

> **If we don't incorporate AI like Omnisense™ into our day-to-day security processes, we'll stagnate in a world that's accelerating at breakneck speed**
>
> *— Concerned CISO at a Major Financial Institution*

1 SAVE ON HIRING & TRAINING COSTS

- **Reduced Analyst Headcount:** Scaling automated L1 functions means organizations can do more with fewer staff

- **Instant Onboarding:** Omnisense™ doesn't need months of orientation - it's ready from day one, reducing dependencies on new hires

SCHEDULE A DEMO

Experience firsthand how quickly and accurately Sara identifies threats, executes remediation, and learns continuously from each case. Your L1 incident response could soon be handling **50 times** the workload of a single analyst, without compromising on quality or speed

CONCLUSION: ADAPT OR RISK OBSOLESCENCE

Cyber threats are evolving faster than ever, making real-time, AI-driven defense essential to staying ahead. **Sara**, powered by Omnisense™, does precisely that - enabling your SOC to investigate, triage, and remediate at lightning speed while saving significantly on operational overhead