eSENTIRE

DATA SHEET

eSentire Security Operations Center (SOC)

eSentire MDR provides SOC-as-a-Service with the 24/7 coverage you need to investigate and respond to threats before they impact your business.

24/7 Live SOC Cyber Analyst Support

Get immediate support and expertise from our SOC team 24/7. Speak with a live analyst who is already engaged and initiate expert-level response as an extension of your team.

Incident Handlers and Threat Hunters on Every Shift

Each SOC shift is supported by senior technical experts who perform global threat sweeps and proactively hunt threats based on the latest intelligence from our Threat Response Unit (TRU).

Advanced Certification and Training Program

With an average tenure of 6 years and a 95%+ retention rate, our team proudly holds advanced certs including SSCP, CSAP, CISSP, Security+, Network+, Linux+, Server+, and more.

Powerful Open XDR Cloud Platform Support

If an orchestrated response isn't possible, our XDR platform equips our SOC team with the insights they need to perform deep threat investigations and execute manual containment.

Industry-Leading Research and Models from TRU

Our SOC-as-a-Service is supported by top research and machine learning experts, so you benefit from improved detection, response, and timely threat advisories.

Our SOC Team Stands Guard 24/7 So You Don't Have To

Given that a single successful attempt is all that a cybercriminal needs, your defenses must be foolproof. It's vital to have a dedicated SOC team at your disposal 24/7 who can spring into action without hesitation to manage active threats, efficiently manage escalations, and intervene to prevent further spread.

Our open XDR cloud platform automatically disrupts high fidelity threats known to eSentire, enabling our 24/7 SOC - staffed with Elite Threat Hunters and experienced Cyber Analysts - to focus on multi-signal investigation, threat containment and response. Backed by our industry-renowned Threat Response Unit (TRU), we offer around the clock security monitoring, unlimited threat hunting, threat disruption, containment, and unlimited incident handling and remediation.

15 Minutes Mean Time to Contain

Initial Response in Seconds and Containment in Minutes

The time from alert to action is critical to prevent disruption across your business. eSentire SOC-as-a-Service provides initial threat response in seconds and contains threats with a 15-minute Mean Time to Contain.

How We Do It

Detect

A SOC Analyst receives an XDR-enriched output and cross-references detection and signal properties for event validation. They conduct a comprehensive review of the metadata, including endpoint processes, file downloads, and network traffic summaries related to the event.

Next, they conduct a preliminary investigation by using various tools to establish data points and assessing the domains leveraging the IP for hosting purposes.

Evaluate

The SOC Analyst then examines business-specific information (e.g., work-flow handling notations, IP notations, and common knowledge notes) to determine if there are any considerations that could influence how the investigation should be handled.

Investigate

The SOC Analyst will investigate to determine if the detection triggered was rule noise, a malicious attack, a suspicious incident, or initiated by a benign actor. The success of the attack is determined based on:

- IOCs and/or IOAs for the intrusion
- Details of the intrusion
- Level of access the attacker achieved
- Related malicious activity
- Indications of lateral movement

Inform, Respond & Remediate

The SOC Analyst will determine if the incident requires customer notification, complying with the documented escalation and containment procedures for email and phone call communication. Simultaneously, our SOC team will isolate and contain the threat, and initiate threat response measures, which align with our response processes based on signal type and customer preference.

* *If the SOC Analyst determines there is a hands-on-keyboard attacker or ransomware attack unfolding, the analyst will engage our Incident Handling team that is on staff for every shift. They will take command of the incident at that point, and they become the main point of contact for the customer. Our Incident Handling team will also work cross-functionally with eSentire's Threat Response Unit to scope the intrusion, identify threat actor activity in the environment and to ensure full remediation.*

Continuously Improve

Our SOC team collaboratively enhances your overall security posture over time and becomes an extension of your security team. We leverage insights gained from each investigation in our SOC, providing ongoing improvements in your MDR service to bolster your organization's cyber resilience.

About Our 24/7 Security Operation Centers (SOCs)

Two Security Operations Centers

Waterloo, ON, Canada

Cork, Ireland

Additional analysts operating across the US, EMEA, and APAC.

Mature Operations

We are PCI compliant, SOC 2 and ISO27001 certified. We deliver cutting-edge SecOps capabilities, optimized staffing and workload management, quality assurance, and complete 24/7 support.

SOC Support Satisfaction

- 100% Deployment Satisfaction
- 99% Ongoing Operations and Tuning Satisfaction
- 99% Threat Detection and Response Satisfaction

2000+ Companies Trust the eSentire SOC

eSentire in Action:

Citrix Vulnerability Case Study

In this incident our SOC Cyber Analysts on shift detected internal systems downloading malicious payloads from external sources, prompting the team to engage our customer about the activity. The malicious infrastructure was added to our global deny list and the SOC Incident Handling team was quickly engaged to provide containment and remediation recommendations, including resetting multiple compromised accounts, blocking malicious IP addresses on the firewalls, and isolating impacted systems.

The customer actioned SOC recommendations while the Incident Handling team continued their investigation where the attack source was traced to a threat actor-controlled host connected to the corporate VPN.

After containment actions were taken, the Incident Handling team joined a call with the customer. The root cause was identified as the Citrix vulnerability tracked in CVE-2023-4966, and the customer proceeded to rebuild vulnerable systems with patched software in accordance with Citrix advisories. As a continuation of the efforts, the Incident Handler requested logs and identified additional threat actor details, and searched for evidence of data exfiltration and confirmed that none was identified.

Ultimately, the actions taken by our SOC in this situation and other daily attacks ensure our 2000+ customers are protected from business disruption.

> *We received an urgent alert about a compromise on our network due to speed of patching across our environment. eSentire's 24/7 SOC includes incident handling expertise so we were able to partner to narrow the threat immediately, contain it in minutes, and remediate fully. The Analyst was able to demonstrate exactly how the threat actors took advantage of our network, and stayed on with us past the end of his shift to ensure we had no further questions or concerns. He showcased with confidence that no data was exfiltrated or system compromised. eSentire's SOC is so much more than alerting. The depth of analyst knowledge, expertise and 24/7 support is truly impressive."*
>
> **- CIO, Global Asset Management Firm**

"I like the fact that we can engage at anytime throughout the day with the SOC team and they are always ready to help with whatever security issues we are facing."

BYRON S.

READ THE FULL REVIEW →

"eSentire provides a comprehensive MDR solution that is scalable for companies of any size. Their SOC is incredibly responsive and gives us near-instant insight into suspicious activity on endpoints and network assets. Of late, eSentire has been closely partnering with Microsoft, aligning well with our increased leverage of Azure resources."

JORDAN F.
Director of Technology | Mid-Market

READ THE FULL REVIEW →

"I like that they are responsible for funneling the thousands of alerts through their SOC and only escalating to us when appropriate."

VERIFIED CUSTOMER
Financial Services

READ THE FULL REVIEW →

You Should Be Protected by the Best SOC in the Business

Submit your information and an eSentire representative will be in touch to help you reduce your risks and build a more resilient security operation today with eSentire MDR and SOC-as-as-Service.

GET STARTED

IF YOU'RE EXPERIENCING A SECURITY INCIDENT OR BREACH CONTACT US 1-866-579-2200

eSENTIRE

eSentire, Inc., the Authority in Managed Detection and Response (MDR), protects the critical data and applications of 2000+ organizations in 80+ countries, across 35 industries from known and unknown cyber threats by providing Exposure Management, Managed Detection and Response and Incident Response services designed to build an organization's cyber resilience & prevent business disruption. Founded in 2001, eSentire protects the world's most targeted organizations with 65% of its global base recognized as critical infrastructure, vital to economic health and stability. By combining open XDR platform technology, 24/7 threat hunting, and proven security operations leadership, eSentire's award-winning MDR services and team of experts help organizations anticipate, withstand and recover from cyberattacks. For more information, visit **www.esentire.com** and follow **@eSentire**.