eSENTIRE

DATA SHEET

# eSentire Threat Response Unit (TRU)

*Stay ahead of sophisticated known and unknown cyber threats with proactive threat intelligence, original threat research, and a world-class team of seasoned industry veterans*

### Prepare and react to emerging, unknown threats

TRU continuously monitors the threat landscape, publishes regular threat advisories, security bulletins, and threat intelligence reports, and conducts proactive real-time threat hunts so you can stay ahead of the latest emerging threats and prevent business disruption.

### Harden your toolkit with novel detection rules and advanced machine learning (ML) models

As an integral part of the eSentire MDR service, TRU constantly builds and updates new detection rules and ML models across our eSentire XDR platform. These detections are further strengthened by robust investigative runbooks to support our SOC Cyber Analysts in their investigation and containment actions – on your behalf.

### Go into battle with a team of industry veterans with real-world experience

TRU has discovered dangerous threats and nation-state attacks, such as the Kaseya MSP breach and uncovered the identities of hackers behind the malicious more_eggs malware, and more. TRU acts as an extension of your team so you can do more with less.

With a 95% employee retention rate, TRU consists of highly certified, seasoned industry veterans who regularly hold interactive threat briefings, share their expertise with industry publications, and have proven to be trusted sources for global law enforcement agencies to track down cybercriminals.

## Your Challenges

As cyber threats rise in number and complexity, security leaders are grappling with the pressure of doing more with less while trying to keep up with the threat landscape. Unfortunately, many in-house security teams don't have the bandwidth or expertise to perform proactive threat hunting, conduct original threat research, develop, or deploy new detection rules to strengthen their cyber defense strategy. In addition, security leaders are also looking for actionable intelligence to protect their critical systems, applications, and data assets to further their defensive strategies against industry-specific threats.

Modern threat response requires the ability to collect unstructured data from disparate sources associated with attacker tactics, techniques, and procedures (TTPs) and operationalize global protections – **all in a timely manner.** While security tools that leverage automation may be sufficient at containing, and remediating most low-severity threats, manual human intervention will be required to defend your organization from sophisticated threats.

Therefore, you need access to a team of industry-renowned experts with real-world experience who are battle-tested to protect you against the most advanced cyber threats.

# Introducing the eSentire Threat Response Unit (TRU)

The eSentire Threat Response Unit (TRU) is an industry-leading threat research team that is committed to helping your organization become more resilient. By providing complete visibility across your attack surface and performing global threat sweeps and proactive hypothesis-driven threat hunts augmented by original threat research, we are laser-focused on defending your organization against known and unknown threats.

We prioritize creating and updating our detection rules and ML models regularly, so your security posture is hardened against the evolving threat landscape. Our content development is built upon the MITRE ATT&CK Framework and is constantly fine-tuned for efficacy to reduce false positives.

With TRU by your side, you can rest easy knowing that you're protected by a team of seasoned industry veterans and an MDR provider that law enforcement agencies rely on to identify threat actors and collaborate on threat intelligence.

eSENTIRE
Threat Response Unit

## How TRU Proactively Protects Your Organization

By leveraging contextualized human-driven threat intelligence, original content on emerging threats, 24/7 availability of Elite Threat Hunters, and advanced analytics based on the latest TTPs, TRU is committed to delivering the strongest MDR offering from eSentire.

eSentire's Threat Response Unit (TRU) is foundational to our MDR service – no add-ons or additional costs required. You benefit from:

- **Curated Threat Intelligence:** TRU collects and processes intel from 37+ commercial threat feeds and 10+ proprietary intel sources, relevant trending threats from the Dark Web and social media, security reports, positive SOC-driven threat investigations, and various third-party tools. This data is used to conduct further investigations to determine potential Indicators of Compromise (IOCs).

**35%** Of threats are identified by TRU before they appear on commercial threat feeds.

**12%** Of threats identified by TRU that are never seen in the commercial feeds we manage.

- **Proactive and Reactive Threat Sweeps:** Our Elite Threat Hunters conduct global threat sweeps across our customer base if an IOC is identified. As a result, eSentire MDR customers experience the benefit of the collective threat intelligence through Security Network Effects from our 2000+ customers.
- **Threat Hunting:** We continuously look for potential IOCs and develop novel detection rules for the latest cyber threats. These detection rules are published to the eSentire XDR Platform to strengthen automated threat detection and containment capabilities.
- **Live Defense Against Attackers:** Adversaries don't work 9-5, neither do we. Our team of 24/7 SOC Cyber Analysts, TRU, and Incident Handlers are battle-tested and ready to actively defend your organization against hands-on cybercriminals in real-time.

- **Mitigation Support for Zero Day Threats:** We identify customers who are vulnerable to zero-day threats and provide mitigation support for critical zero-day vulnerabilities until a security patch is published by the technology vendor.
- **Updated Detection Rules:** We regularly update your toolkit by building advanced machine learning models to detect anomalies in unstructured telemetry data that traditional security tools miss.
- **Original Research:** We publish threat advisories, security bulletins, and original threat research on emerging threats to arm our customers with the latest intel, so they know how to make informed decisions that evolve with the threat landscape. TRU's research routinely supports law enforcement agencies in their mission to unmask threat actors and stop cybercrime.
- **Monthly TRU Intelligence Briefings:** We hold monthly threat briefings to keep your team apprised of the latest emerging threats and new TTPs observed to help you stay ahead of the threat curve and build a more resilient security operation.
- **No Additional Cost:** Unlike most MDR providers, TRU's threat hunting and proactive detection rule development capabilities are built into your eSentire MDR service at no extra cost.

# Ready to get started?

We're here to help! Submit your information and an eSentire representative will be in touch to help you build a more resilient security operation today.

**Contact Us**

**If you're experiencing a security incident or breach contact us**  **1-866-579-2200**

eSENTIRE

eSentire, Inc. is the Authority in Managed Detection and Response, protecting the critical data and applications of 2000+ organizations in 80+ countries, representing 35 industries from known and unknown cyber threats. Founded in 2001, the company's mission is to hunt, investigate and stop cyber threats before they become business disrupting events. Combining cutting-edge machine learning XDR technology, 24/7 Threat Hunting, and proven security operations leadership, eSentire mitigates business risk, and enables security at scale. The Team eSentire difference means enterprises are protected by the best in the business with a named Cyber Risk Advisor, 24/7 access to SOC Cyber Analysts, Elite Threat Hunters, and industry-leading threat intelligence research from eSentire's Threat Response Unit (TRU). eSentire provides Managed Risk, Managed Detection and Response and Incident Response services. For more information, visit **www.esentire.com** and follow **@eSentire**.