eSENTIRE
THREAT RESPONSE UNIT

GUIDE

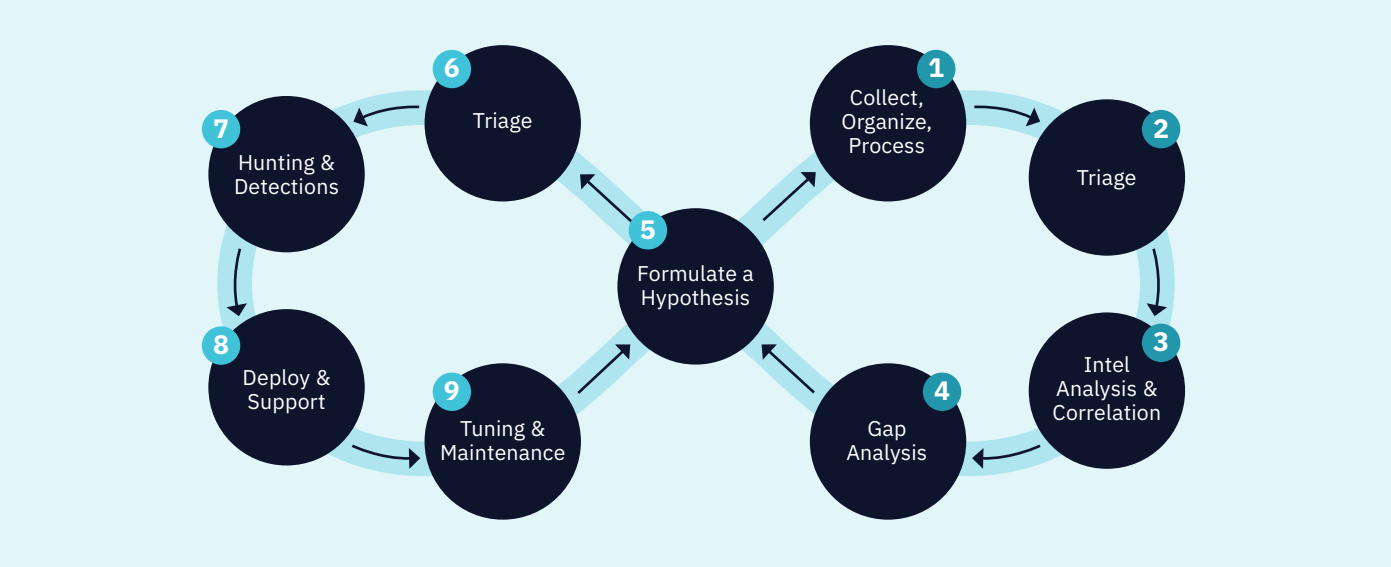
How eSentire Threat Response Unit (TRU) Conducts Proactive Threat Hunting with the Infinite Loop Threat Framework

Threat hunting is the practice of proactively searching for signs of malicious activities or indicators of compromise (IOCs) before threat actors gain a deep foothold within your organization's environment.

This involves observing both attacker behaviors (e.g., evidence of lateral movement, privilege escalation attempts, anomalous user activity) and indicators (e.g., presence of malware artifacts, unusual network traffic, command and control).

The eSentire Threat Response Unit (TRU) is an industry-leading threat research team that helps your organization become more resilient against modern sophisticated threats. This is an elite team of threat intelligence researchers and threat hunters that supports our 24/7 Security Operations Centers (SOCs), builds threat detection models across the eSentire XDR Cloud Platform, and works as an extension of your security team to continuously improve our MDR service.

At eSentire, TRU uses an Infinite Loop framework to gather threat intelligence, operationalize it to conduct hypothesis-driven threat hunts, and build detections for our team of 24/7 SOC Cyber Analysts:



Once a threat is discovered, eSentire's TRU team 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.

Gathering Threat Intelligence

Given the sheer volume of cyberattacks that occur daily, it's important to be able to direct threat intelligence activities on the right threat at the right time.

TRU collects and processes threat intelligence from **54 commercial threat feeds and 10+ proprietary intel sources**, the Dark Web, social media, security reports, positive SOC-driven threat investigations, and various third-party tools to conduct further investigations and identify potential Indicators of Compromise (IOCs).

STAGE 1: Collect, Organize, Process

TRU regularly collects threat intelligence data sourced from disclosures about new vulnerabilities or threats, threat landscape monitoring, and even observations of incidents occurring in customer environments so they can allocate resources on the most impactful threats first.

Often, they focus on ransomware or malware activities. However, they may also choose to focus on tangential activities, such as initial access brokers since these groups breach our customers' environments and sell this access on underground marketplaces.

TRU also has long-term projects to track down threat actors, using data collected from a myriad of sources like OSINT, commercial threat feeds, underground cybercrime forums on the Deep and Dark Web, and conducting malware reverse engineering. In practice, it means TRU can identify and understand new threats in near real time and validate our detection capabilities in response to evolving and emerging threats.

Next, they categorize the threats based on 'topics', such as initial access malware, ransomware, post-exploitation activity, etc.

STAGE 2: Triage Threats and Vulnerabilities

Once identified, the threats and vulnerabilities are prioritized based on their severity and potential impact on our customers. If TRU determines that mass exploitation and follow-on actions of malware are highly probable, those threats will be tagged as high severity events that require rapid response. This is most typically seen for zero-day attacks or vulnerabilities (e.g., the Log4j zero-day vulnerability) that are being actively exploited.

STAGE 3: Intelligence Analysis and Correlation

As part of this stage, TRU rigorously deep dives into the malware to find attack patterns, determine attacker tactics, techniques, and procedures (TTPs), gather Indicators or Compromise (IOCs) from public and private sources, understand the full scope of the attack, and more.

These analyses may also be performed by conducting malware reverse engineering to identify exactly how the malware was deployed, the impact of the malware execution, and how the threat actors were able to gain initial access in the first place. Based on the analysis, TRU evaluates the best course of action to detect, mitigate, or prevent threats and vulnerabilities.

STAGE 4: Conduct a Gap Analysis for Detections

Next, TRU conducts a gap analysis to determine whether we have existing detections for the threats in our detection library. If there is an existing detection in place, TRU will re-evaluate to ensure it's a robust, high-fidelity detection. They will also reference it in any security advisories or threat briefings for our customers.

If there are no existing detections, or if TRU determines that the detections need to be updated, the threat intelligence collected is passed over to our team of Elite Threat Hunters so they can conduct a proactive threat hunt and build novel detections.

Conducting Proactive, Hypothesis-Driven Threat Hunting

Operationalizing threat intelligence means transforming raw data about emerging or existing threat actors and their tactics, techniques, and procedures (TTPs) into actionable insights.

These insights not only enhance your organization's defensive capabilities but also empowers the threat hunting process, making it more efficient and effective. It does this by setting up a proactive, systematic approach to enable 24/7 threat detection and response for potential threats before they disrupt your business.

In fact, eSentire's TRU team has discovered some of the most dangerous cyber threats and nation-state attacks in our space. In 2023, TRU circulated 44 threat advisories, performed 1100+ hypothesis-based threat hunts, 200,000+ threat sweeps and built 520+ new detections to protect our customers.

STAGE 5: Formulate a Hypothesis

Once a detection gap is identified, our Elite Threat Hunters collect and analyze the threat intelligence data, in addition to collecting behavioural data from their own research, red team assessments, and third-party integrations (e.g., log sources) to formulate a hypothesis.

By building hypotheses based on the relevant data, Elite Threat Hunters can test their hypotheses in sandbox environments to predict malware activity, infer attacker TTPs, and use the findings to build novel detections.

STAGE 6: Triage

The Elite Threat Hunters evaluate all the different threats and vulnerabilities passed by the threat intelligence researchers and triage based on the severity. They determine whether the threat requires rapid response, which is typically seen for the most critical threats like zero-day exploits and vulnerabilities with a CVS score of 10.

On the other hand, other threats get assigned as high-, medium-, and low-priority events that can be monitored over time.

STAGE 7: Threat Hunting and Detection Development

This stage involves conducting proactive threat hunts and converting the prioritized threat intelligence into detections that can be used to identify malicious activity within your environment. Detection development requires a deep understanding of the threat landscape and how specific threats may manifest in your network.

During this phase, TRU continues to research the potential threat to prototype a detection and perform a systematic threat hunt across our global customer base. The result is what we deem the 'eSentire Security Network Effect', wherein all our customers derive benefits from these proactive threat hunts.

The findings of the threat hunt are reviewed and analyzed further to determine whether the detection should be refined or updated.

STAGE 8: Deploy Detections and Support

After developing the detectors, the next step is to deploy them within your security infrastructure. This includes integrating them into existing security tools and ensuring they are properly configured to detect threats effectively.

Supporting the deployed detectors involves regular monitoring and updates to ensure they continue to function as intended. It also includes providing the threat hunting team with the necessary tools and information to respond to any detections.

Next, the Elite Threat Hunters create detailed runbooks for each detection they've developed. A runbook is a document that contains the description, references, detection query, and investigation steps for a specific threat behavior. The runbooks are then provided to our 24/7 SOC Analysts to use when they a security incident alert is triggered.

The detections queries are also deployed across all our customer environments and ran on a scheduled basis to generate alerts when suspicious or malicious activity is found.

STAGE 9: Tuning and Maintenance

In the last stage, TRU monitors the performance and quality of the detections and updates them as needed based on feedback from the SOC or their own analysis. They also report on the state of every detection and looks for surges or false positives that might indicate a need for tuning the detection.

Sometimes, they may decommission a detection if it is no longer relevant or effective. Tuning and maintenance is an ongoing process that ensures the detections are high fidelity and up to date.

How eSentire's Threat Response Unit (TRU) Helps You Build Resilience and Prevent Disruption

At eSentire, we believe that threat hunting and threat intelligence are foundational to a strong Managed Detection and Response (MDR) program and should never be an "add-on" or optional service.

By providing complete visibility across your attack surface and performing global threat sweeps as well as proactive hypothesis-driven threat hunts augmented by original threat research, TRU is laser-focused on defending your organization against known and unknown threats.

TRU acts as an extension of your security team to build your cyber resilience and prevent business disruption. With TRU by your side, you can rest easy knowing that you're protected by an MDR provider that law enforcement agencies rely on to identify threat actors and collaborate on threat intelligence.

Why Choose eSentire's Threat Response Unit (TRU)

- **Prepare and react to emerging, unknown cyber threats to prevent business disruption**

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

- **Harden your toolkit with novel threat detection rules and advanced ML models**

  As a foundational component of the eSentire MDR service, TRU constantly builds and updates new threat 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**

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

35% of our intel is distributed ahead of commercial feeds

12% of our intel is never seen in commercial feeds

200+ IoCs per day from positive SOC investigations

300+ security incidents identified per quarter through threat hunting process

In **2023**

1,100+ hypothesis-based hunts

200,000+ global threat sweeps

500+ novel detections and runbooks to improve security

Stay Up to Date with the Latest Threat Intelligence from our Threat Response Unit (TRU)

Our TRU team holds monthly threat intelligence briefings and regularly publishes threat advisories, security bulletins, and original threat research on emerging threats to help you stay ahead of the threat curve, reduce your cyber risks, and build a more resilient security operation.

LEARN MORE

Ready to get started?

Connect with an eSentire Security Specialist to learn how you can reduce your cyber risks, build resilience, and prevent disruption.

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**.