

eSentire Threat Intelligence

Extend eSentire's threat intelligence expertise across your existing security tool stack to reduce false positive alerts and enhance your threat detection and response capabilities.

High Fidelity Indicators of Compromise (IOCs)

Get access to IOCs with 99% true positive rate or higher that have been verified by our Elite Threat Hunters and Threat Response Unit (TRU). Our threat feed is refreshed every 24 hours and every IOC in the feed has been observed in customer environments, significantly reducing the number of false positives.

Improved Threat Detection and Response Capabilities

Cover a broad spectrum of potential threats and malicious activities with multiple IOCs (i.e., IP addresses, domain names, file hashes) so your team can improve your detection accuracy and gain full context into the threat.

Seamless Integration with Your Existing Security Tools

Integrate our threat feed with your existing tools (e.g., firewalls, email servers, EDR) using the feed's STIX™ format for a cost-effective approach to operationalize threat intelligence and enhance detection capabilities.

Your Challenges

Mediocre threat intelligence has become a commodity in today's cybersecurity market. Many security leaders make the mistake of acquiring multiple threat feeds – which often have redundant, outdated data – believing that more data will equate to more actionable threat intelligence. Unfortunately, inaccurate threat intelligence can result in false positives, leading in-house security teams to divert valuable time and resources from genuine cyber threats.

Additionally, many threat feeds lack context around IOCs, leaving security teams unable to operationalize threat intelligence. Lastly, industry threat feeds are expensive, making it challenging for teams to operationalize threat intelligence when they're asked to do more with less.

Our Solution

eSentire Threat Intelligence offers a curated list of high-fidelity Indicators of Compromise (IOCs), meticulously vetted and approved by our Elite Threat Hunters and Threat Response Unit (TRU) based on positive Security Operations Center (SOC) investigations across our global customer base, so you can confidently integrate the actionable intelligence into your existing security tool stack (e.g., firewalls, endpoint agents, etc.). eSentire Threat Intelligence covers 71 industries and our IOCs have a 99% true positive rate.

By relying on high quality threat intelligence, your team can enhance your threat detection and response capabilities on real threats, not false positives. As a result, your team can reduce noise across your security tool stack and improve your automated blocking capabilities of known threats.

35%

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

12%

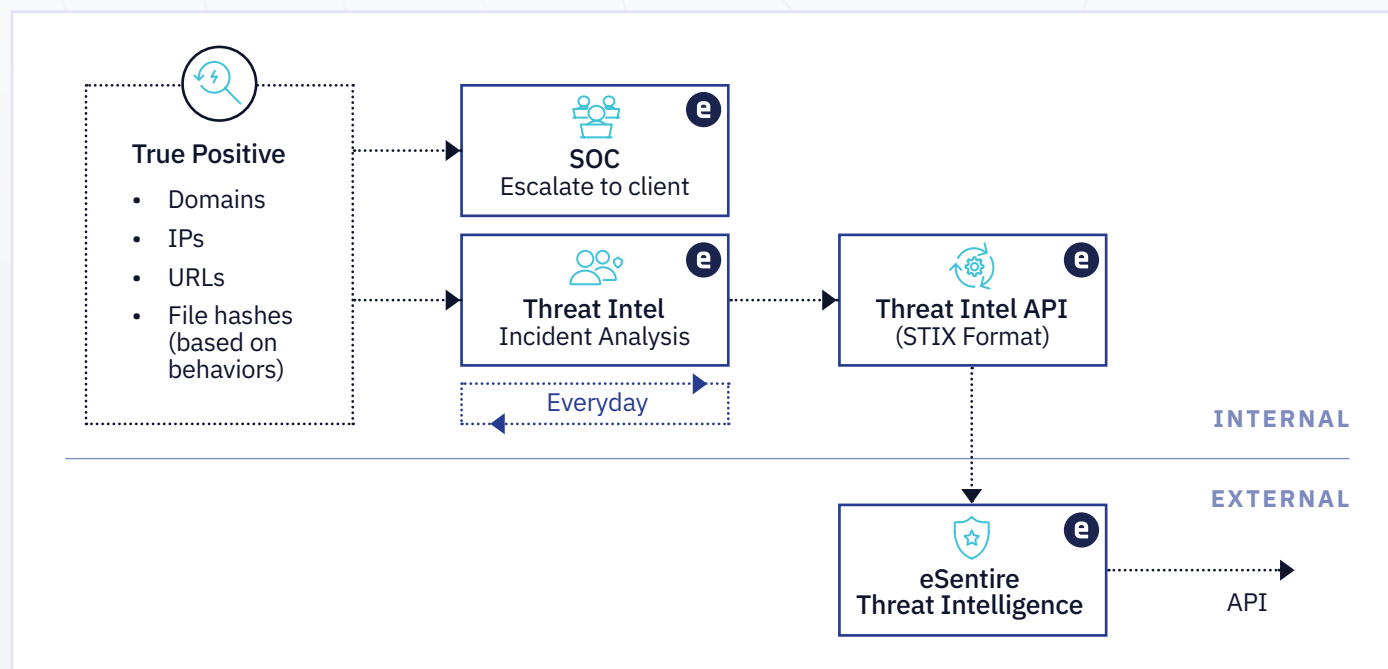
Of threats identified by TRU are *never* seen on commercial threat feeds.

How It Works

Unlike other commercial threat feed providers that use threat intelligence from open source and publicly available feeds, eSentire uses a human-driven approach to provide the most updated threat feed with the least number of false positive alerts.

Every IOC in our threat feed is observed by our 24/7 SOC Cyber Analysts during threat investigations around true positive threats. These IOCs are then reviewed further by our team of Elite Threat Hunters, who provide additional context to the indicators. Finally, these IOCs are then shared with you in STIX format as the eSentire Threat Intelligence offering.

eSentire Threat Intelligence is available a la carte or as part of our eSentire Atlas MDR packages.



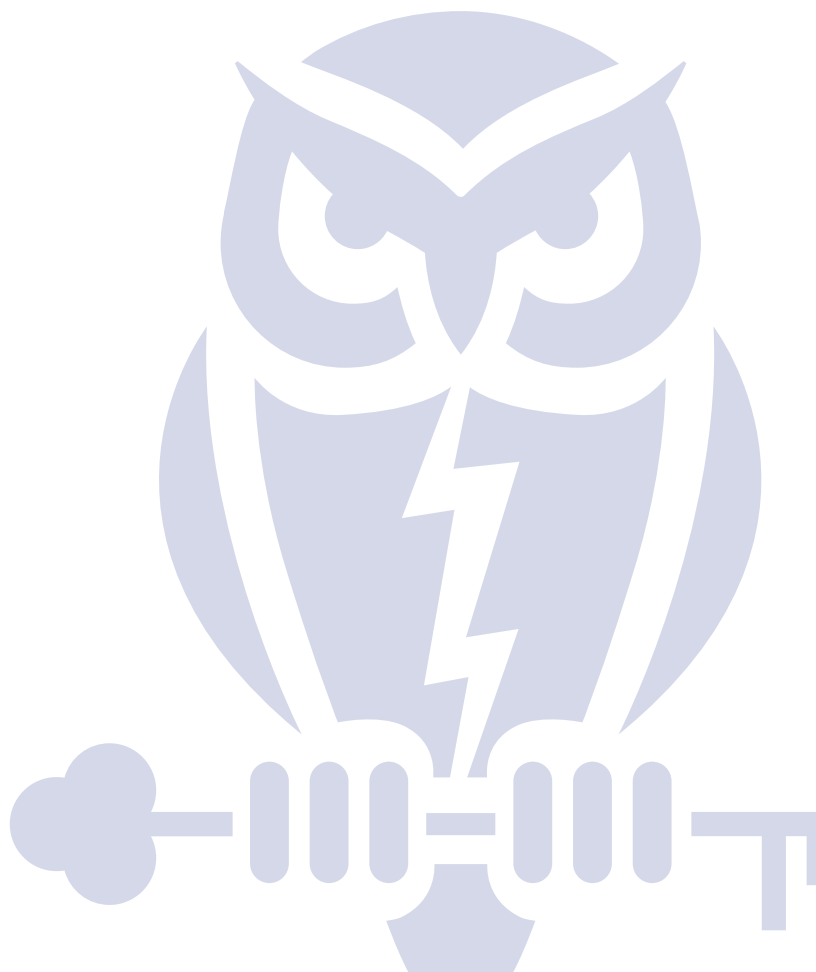
Why Choose eSentire for Threat Intelligence

- ✓ **High Fidelity Threat Feed from a Proven Managed Detection and Response (MDR) Leader**
With a false positive rate of <1%, we use collective threat intelligence from 2000+ customers across 71 industries to only add high fidelity IOCs observed across customer environments. All IOCs are refreshed every 24 hours, and we continuously remove old IOCs, so you only focus on critical threats that matter.
- ✓ **Easy Integration with Existing Security Tools**
We use Structured Threat Information Expression (STIX™) format to exchange cyber threat intelligence (CTI), allowing for easy integration across different security tools. Using a standardized format like STIX helps improve interoperability and collaboration among different organizations and security teams.
- ✓ **Rich Context Around Threats**
The STIX format enables us to provide rich context around IOCs, including threat actors involved, malware campaigns, targeted assets, attacker tactics, techniques, and procedures (TTPs) and more.
- ✓ **Security Expertise from Industry-leading 24/7 SOC Cyber Analysts and Elite Threat Hunters**
Every IOC added to the threat feed is thoroughly vetted by our SOC and Threat Response Unit (TRU). With an average tenure of 6 years, our SOC Cyber Analysts and Threat Response Unit (TRU) are highly certified, seasoned industry veterans who hold advanced credentials, share their expertise with industry publications, and are trusted sources for global law enforcement agencies.

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

Our TRU team hold 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](https://twitter.com/eSentire).