

# Threat Intelligence for the Energy Sector

The energy sector remains a prime target for cyberattacks and hacking incidents—a US presidential directive has identified the sector as “uniquely critical.” To prevent disruptions to essential energy services, providers need real-time threat intelligence that informs threat detection and incident response.

By leveraging unique proprietary telemetry, energy companies can detect and respond to threats more quickly and accurately, reducing the time that attackers have to cause damage and helping maintain operational continuity. Critical energy infrastructure can be proactively hardened using curated threat intelligence to anticipate and mitigate potential threats before they materialize.

Up-to-the-minute threat intelligence reports provide comprehensive insights into attack vectors, malware behavior, and indicators of compromise. Meanwhile, access to high-quality threat analysis allows energy sector leaders to make informed decisions about cybersecurity investments and strategies, ensuring that resources are allocated efficiently to areas of highest risk.

## THE MAIN CONCERNS OF ENERGY PROVIDERS

- ✓ Maintaining the energy supply chain, including generation and distribution
- ✓ Ransomware and other malware threats that can interrupt energy supply
- ✓ Targeted APT attacks that represent an invasive threat to systems

## THEIR CRITICAL NEEDS

- ✓ Protection of critical infrastructure and operational technology (OT)
- ✓ Real-time threat detection and incident response capability
- ✓ Compliance with industry-specific cybersecurity regulations

## HOW CAN ESET THREAT INTELLIGENCE HELP?

ESET is a trusted provider of cyber threat intelligence in the energy sector, with 38 years of cybersecurity expertise. Our global presence, built up over decades, provides us with a rich and diverse intelligence library drawn from over 100 million nodes.

By leveraging ESET's Data Feeds and APT Reports, you gain access to high-quality, actionable insights that enhance your threat detection and response capabilities. ESET goes well beyond just collecting indicators—we employ advanced AI technology and expertise to provide your organization with real added value.



We deliver actionable intelligence that leads to faster, better decisions



We provide unique insights that enable a profound understanding of the threat landscape



We allow you to proactively zoom in on new and emerging threats

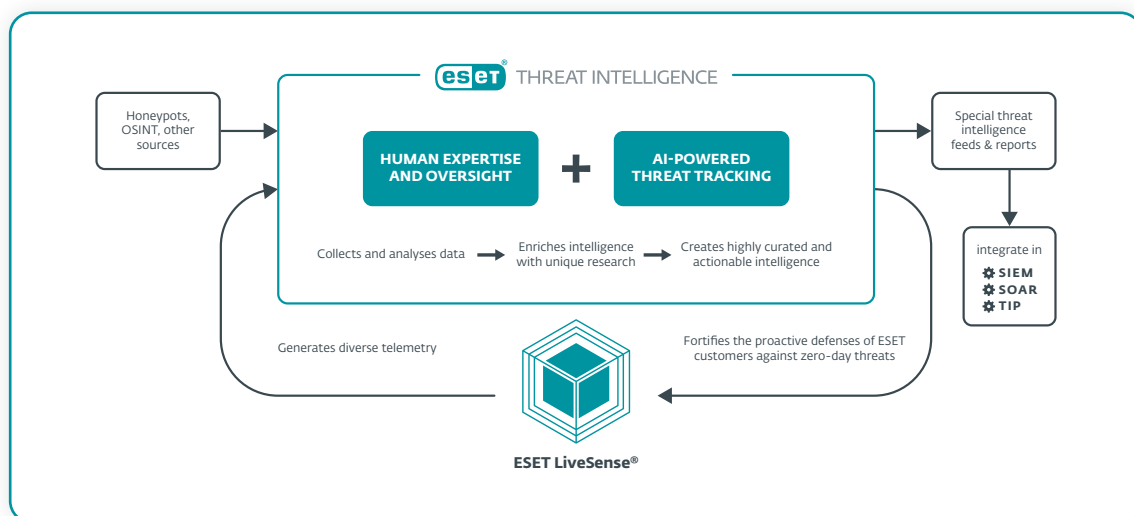


We enable you to prioritize threat investigation, and thus minimize impact

# Unique, Enriched Intel for Actionable Insights

Threat intelligence is not just about collecting indicators and wrapping them up—ESET goes well beyond that. We employ advanced technology and extensive expertise to process and enrich our intelligence, ensuring it provides real value to your business.

- 1. Comprehensive Telemetry:** ESET LiveSense, integrated within the ESET PROTECT Platform, delivers a broad and deep collection of data from a hugely diverse range of telemetry.
- 2. Diverse Collection Methods:** We also utilize diverse collection and monitoring methods—including honeypots, sensors, OSINT, and more—to gather large volumes of quality data.
- 3. Advanced Processing:** All data is processed through our robust backend systems, which leverage AI to classify and analyze intel so that only the most relevant and actionable data is surfaced.
- 4. Expert Analysis:** Beyond automated processing, our skilled threat intelligence analysts and researchers play a crucial role, going beyond what machine learning and automation alone can achieve.



## ESET Threat Intelligence, Tailored for Energy Providers

ESET Threat Intelligence is designed to help protect energy producers and distributors against ransomware, data breaches, and other cyber threats. Our Data Feeds and APT Reports are tailored to protect critical infrastructure and operational technology (OT) from sophisticated cyber threats. ESET's unique telemetry and advanced processing deliver real-time threat intelligence, helping you prevent disruptions and comply with industry-specific regulations.

### MALICIOUS DATA FEED

Gain valuable insights from this real-time feed, which provides information on newly discovered malware samples, their characteristics, and IoCs. The feed includes details such as file hashes, timestamps, and identified threat types.

### RANSOMWARE FEED

Combat ransomware with real-time data on prevalent samples. Our feed provides insights into active ransomware families, enabling proactive blocking. Stay ahead of threats and protect your organization from data breaches and costly disruptions.

### BOTNET FEED

Leverage insights from ESET's proprietary botnet tracker network with our Botnet Feed. This feed comprises three sub-feeds: botnet, command and control (C&C), and targets. It provides crucial data, including detection details, file hashes, IP addresses, and more.

### APT IOC

Benefit from valuable information from ESET's proprietary APT Feed, which provides insights into advanced persistent threats (APTs) based on ESET's meticulous research and long experience of APT detection and remediation.