OVERVIEW

THREAT INTELLIGENCE

Unique intelligence feeds and reports
from the industry's top professionals

Progress. Protected.

Why add ESET to your CTI stack?

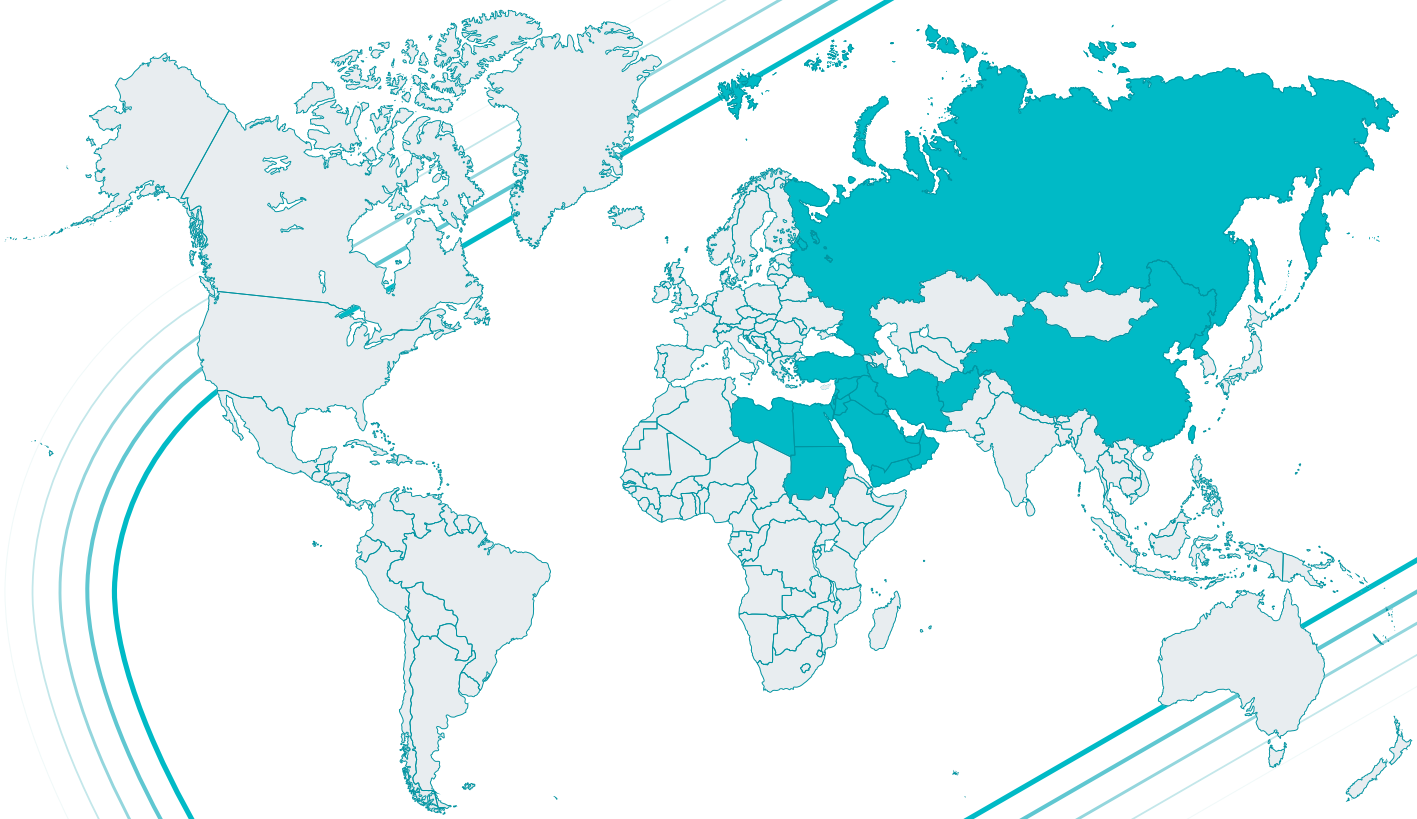
Understanding the current threat landscape and the tactics employed by cybercriminals provides a crucial knowledge advantage. This insight enables organizations to **fortify** their **internal defense systems effectively**. High-quality intelligence data is the cornerstone of any robust cyber threat intelligence (CTI) strategy.

For over 35 years, ESET has been a privately held, debt-free and consistently growing company. Our success is built on a "prevention-first" approach powered by AI and enhanced by human expertise. At the heart of our operations is our **unique Global Threat Intelligence, supported by an extensive R&D network led** by industry-acclaimed researchers. We take the time to truly understand cyber threats, enabling us to defend against them effectively.

No matter how advanced your current CTI solutions are, integrating **ESET into your stack will provide unparalleled value**. Our comprehensive threat intelligence feeds, APT reports and eCrime reports ensure you stay ahead of emerging threats, enhancing your existing defenses with actionable insights and cutting-edge research.

Leverage ESET's unique telemetry

ESET's global presence, built over decades, provides us with a **rich and diverse intelligence library** from millions of nodes. Unlike many competitors, our telemetry is particularly strong in regions considered **"more interesting" from a geopolitical point of view** in the cyber defense world. This unique coverage translates directly into superior intelligence. By leveraging ESET's telemetry, you **gain access to high-quality, actionable insights** that enhance your threat detection and response capabilities.

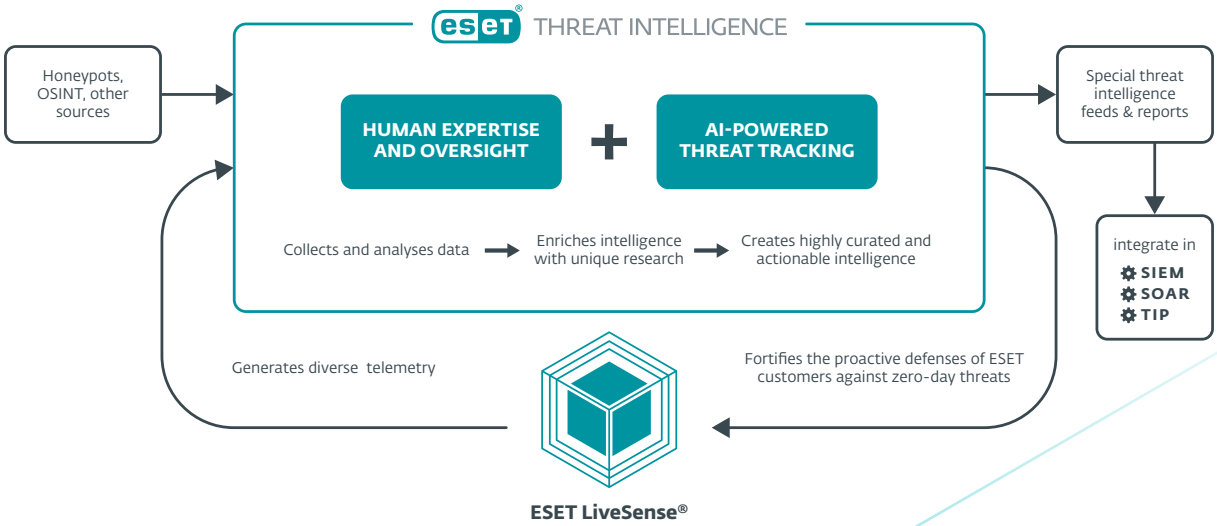


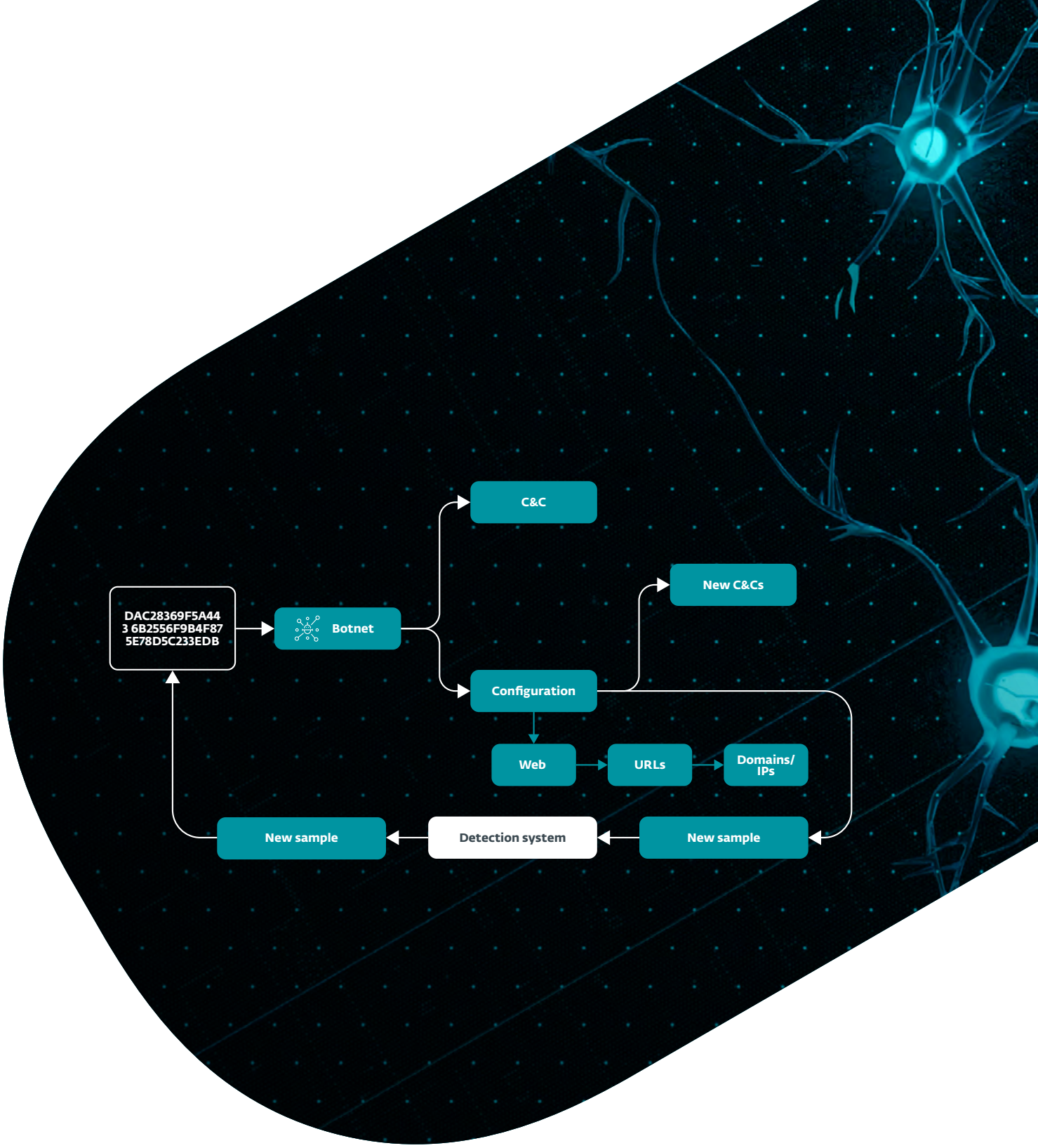
eset® Cybersecurity
Progress. Protected.

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:** Our intelligence starts with a wide range of telemetry generated by ESET LiveSense, our multilayered security technology integrated within the ESET PROTECT Platform. This ensures a broad and deep collection of data from diverse sources.
2. **Diverse Collection Methods:** In addition to LiveSense, we utilize various collection and monitoring methods, including honeypots, sensors, OSINT resources, web crawling (both clear and deep web), and Threat Tracking. This results in a significant volume of high-quality data.
3. **Advanced Processing:** Once collected, all data is processed through our robust backend systems, which leverage AI to classify and analyze the information automatically. This ensures that only the most relevant and actionable intelligence is surfaced.
4. **Expert Analysis:** Beyond automated processing, our skilled team of threat intelligence analysts and researchers plays a crucial role. They continuously study and analyze various threat actors, their motivations, TTPs (tactics, techniques, and procedures), and tools. This human verification adds an extra layer of depth and accuracy to our intelligence, going beyond what machine learning and automation alone can achieve.





The samples we receive via telemetry undergo in-depth behavioral and structural analysis. This process yields additional useful indicators, further enriching our threat intelligence. By meticulously examining each sample, we extract valuable insights that enhance the overall quality and effectiveness of our intelligence, providing you with a more comprehensive understanding of the threat landscape.

Superior security via detailed APT Reports

Written in concise, actionable language to improve your organization's security posture, our APT reports provide detailed insights into malware campaigns, distribution, and actors involved. Access our MISP server and AI advisor, and book live sessions with ESET's top threat intelligence experts for comprehensive, actionable intelligence.

PUTTING OUR BEST RESEARCH AT YOUR FINGERTIPS

Our research team is well known in the digital security industry, thanks to our award-winning WeLiveSecurity blog. The team's excellent research and APT activity summaries are available, along with much more detailed information. ESET customers get an exclusive early preview of all WeLiveSecurity content.

ACTIONABLE, CURATED CONTENT

Reports provide a great deal of context for what is going on and why. Thanks to this, organizations can prepare in advance for what might be coming. Importantly, our experts make sure the content is easy to understand.

MAKE CRUCIAL DECISIONS FAST

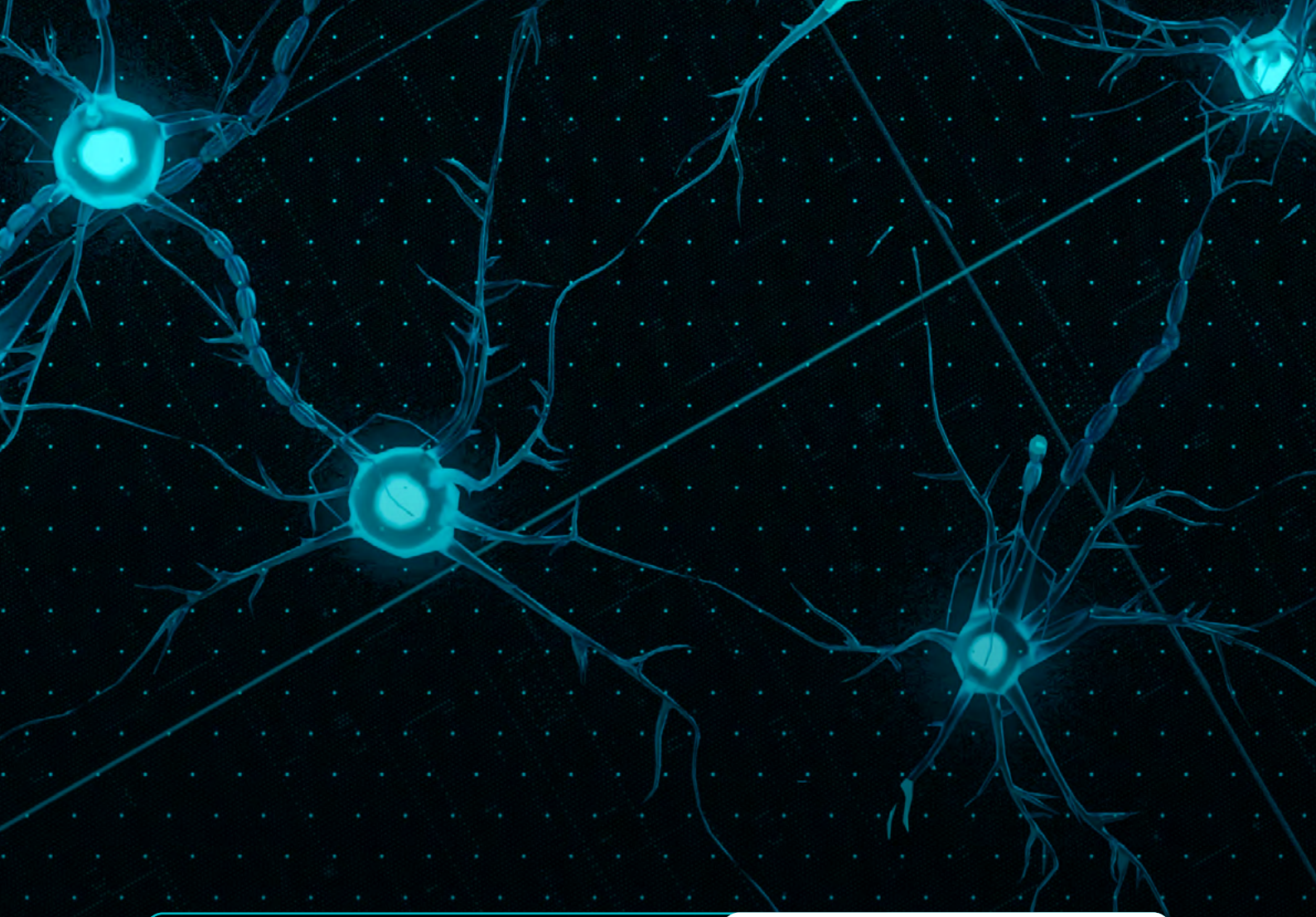
All this helps organizations make crucial decisions and provides a strategic advantage in the fight against digital crime. It brings an understanding of what is happening on the 'bad side of the internet' and provides crucial context, so that your organization can make internal preparations quickly.

ACCESS TO AN ESET ANALYST

Every customer ordering the APT Reports Premium package will also have access to an ESET analyst for up to four hours each month. This provides the opportunity to discuss topics in greater detail and help resolve any outstanding issues.

ESET AI ADVISOR

ESET AI Advisor uses advanced AI and APT expertise to provide on-demand insights and protective measures against cyberattacks. Available as a chatbot, it addresses security inquiries, offers APT summaries, compiles IoCs and TTPs, and generates YARA rules for swift threat understanding and prevention.



		APT Reports	APT Reports Advanced	APT Reports Ultimate
Bi-weekly Activity Summary	Reports summarizing the activity of all covered APT Groups as detailed above (two reports per month)	✓	✓	✓
Threat Analysis Reports	Customized or regular technical analysis of prevalent threats (~30 per year)	✓	✓	✓
Monthly Overview	Monthly compilation of information with an executive overview of threats	✓	✓	✓
Monthly Digest	Index and executive summary of the month's reports and events	✓	✓	✓
Pre-access to WeLiveSecurity	Pre-access to Threat reports and selected WeLiveSecurity articles	✓	✓	✓
APT IOC Feed	Full access to STIX/TAXII feed containing IOCs from the reports	✓	✓	✓
MISP Server Access	Full access to ESET MISP server containing all the information available in the reports	✗	✓	✓
ESET AI Advisor	Access to ESET AI Advisor providing insights and summaries of available APT reports	✗	✓	✓
Analyst Access	Analyst access via various platforms such as MS Teams and email, limited to four hours per month (non-cumulative, including preparation time)	✗	✗	✓

From indicators to intelligence: Outsmart eCrime

ESET Threat Intelligence eCrime Reports deliver deep insights into ransomware and broader cybercrime operations. Gain visibility into attacker tooling, infrastructure and monetization strategies, backed by ESET's global research and telemetry. Move beyond IoCs to access contextual intelligence that strengthens proactive defense and strategic decision-making.

What sets ESET eCrime Reports apart

PROACTIVE DEFENSE

Gain intel not just into eCrime groups, but into the affiliates who actually run the attacks. See how they work and anticipate what they try next to stay ahead.

OPERATIONAL EFFICIENCY

Use clear, curated insights from real incidents to cut through the noise. Make it easier for your team to detect threats, respond faster and focus hunts where it matters most.

EXCLUSIVE VISIBILITY

Go beyond public threat feeds with deeper insight into monetization tactics, infrastructure and affiliate behavior in practice – all backed by ESET's global telemetry and research.

		eCrime Reports	eCrime Reports Advanced
Activity Summary MONTHLY	○ Latest ransomware and infostealer campaigns distilled into clear, strategic insights ○ Who is targeted, how attacks unfold, what went wrong ○ Key lessons, IOCs and guidance to strengthen resilience	✓	✓
Technical Analysis MONTHLY	○ Deep dives into specific threat actors (e.g. FIN7) ○ Full attack chain: initial access to data theft ○ Attacker tactics, tools, infrastructure, MITRE ATT&CK® mapping, IOCs	✓	✓
Monthly Digest PERIODICALLY	○ Executive-ready overview of recent ransomware/ infostealer activity ○ Key trends, notable incidents, emerging threats ○ Helps leadership assess risk and set priorities without technical complexity	✓	✓
eCrime Feed	○ Fresh and curated IoCs on ransomware gangs, their affiliates and infostealer campaigns ○ Available in the standard STIX/TAXII format	✓	✓
ESET AI Advisor	○ Uses eCrime insights to answer threat-related questions ○ Helps interpret incidents and attacker behavior ○ Makes threat intelligence instantly accessible for teams and decision-makers	✗	✓
Access to MISP Server	○ Direct integration with curated threat intelligence ○ Automatic IOC ingestion to enrich defenses ○ Streamlines workflows, speeds detection and supports incident response	✗	✓

Clear and concise data feeds

Enhance your threat landscape view with ESET's unique telemetry. We provide highly curated data feeds in JSON and STIX 2.1, seamlessly integrating into SIEM, TIP, or SOAR tools. Unlike many TI vendors, we pay really close attention so that **our feeds are meticulously filtered and assessed** to ensure their relevance. This enables automatic actions by existing security systems when needed, empowering threat intelligence analysts with a comprehensive view of the global threat landscape.

- Metadata-rich, detailed and curated data with very low false positives
- We ensure data is low size, high relevancy, deduplicated, with confidence-scoring
- The result of advanced filtering, with insights by ESET researchers
- Market-leading, especially with botnet data
- Low maintenance requirements due to properly curated content
- Real-time feeds – only fresh and prevalent IoCs (Indicators of Compromise)

MALICIOUS DATA FEED

Real-time insights on newly discovered malware samples, their characteristics and IoCs. Includes file hashes timestamps and threat types to help you block malicious files before they cause harm.

RANSOMWARE FEED

Real-time data on active ransomware families and prevalent samples. Enables proactive blocking to prevent breaches and costly disruptions.

BOTNET FEED

Powered by ESET's botnet tracker, this feed includes three sub-feeds: botnet, C&C and targets. Provides detection details, file hashes, last communication timestamps, downloaded files, IPs, protocols and target information.

APT IOC FEED

Insights into Advanced Persistent Threats based on ESET research. Exported from ESET's internal MISP server and aligned with APT reports. Available as part of reports or as a standalone feed.

PUA ADWARE FEED

ESET has over two decades of experience classifying PUAs (Potentially Unwanted Applications), giving its intelligence unmatched depth and precision. Adware feeds deliver real-time insight into active adware and similar threats, enabling proactive blocking before impact.

PUA DUAL-USE APP FEED

Tracks legitimate tools (e.g., RMMs) misused by attackers, helping you stay ahead of abuse while reducing noise through tailored, low-redundancy data.

DOMAIN FEED

Provides data on malicious domains, including domain name, IP address and associated date. Domains are ranked by severity, allowing you to prioritize actions such as blocking high-risk domains.

URL FEED

A curated feed of specific URLs with detailed information on each address and its hosting domains. Includes only high-confidence findings, supported by clear, human-readable explanations for flagged URLs.

IP FEED

Receive actionable data on malicious IPs. The structure mirrors domain and URL feeds. Use it to identify common threats, block high-severity IPs, monitor lower-risk ones and investigate further using additional data to assess potential harm.

ANDROID THREATS FEED

Provides real-time information on prevalent Android threats and their IoCs, enabling proactive blocking. Created from ESET telemetry, it updates in near real-time with daily deduplication.

ANDROID INFOSTEALER FEED

A specialized feed within Android threats, offering details on current infostealer samples and related data. Gain insight into active families and proactively block them before they cause harm.

SCAM URL FEED

Stay ahead of scams with real-time data on fraudulent URLs. It covers electronic shops, investment scams, dating scams and cryptocurrency scams. Created from all ESET URL sources in near real-time; deduplication happens every 24 hours.

CRYPTOSCAM FEED

Stay ahead of crypto scams with real-time updates on scam domains, URLs, and associated data. Sourced from ESET's extensive telemetry, it provides early, targeted information to help you proactively block threats and protect your assets.

MALICIOUS EMAIL ATTACHMENTS FEED

Email is a prime target for attacks. The feed provides real-time data on malicious email attachments sourced from ESET's extensive email scanning telemetry.

PHISHING URL FEED

Delivers real-time intelligence on active phishing URLs from ESET's dedicated database. Updated continuously with daily deduplication, this feed helps you detect and block fraudulent sites before they compromise sensitive data.

SMISHING FEED

Provides timely insights into SMS-based phishing (smishing), including domains, URLs and related indicators. Sourced from ESET's extensive telemetry, it updates in near real time with daily deduplication.

SMS SCAM FEED

Protect against SMS scams with real-time feed on malicious domains and URLs. Updated near real-time from ESET's extensive telemetry and deduplicated daily, it helps you identify and block sophisticated threats.

ECRIME FEED

Get clear, actionable data on cybercrime operations and malware-enabled eCrime, monitoring everything from ransomware gangs and their affiliates to infostealer campaigns, so your team can move from reacting to proactively defending your organization.

Experience the power of ESET Threat Intelligence

Schedule a demo with us today and discover the unparalleled value ESET Threat Intelligence can bring to your organization. With a 100% renewal rate, our satisfied customers are a testament to the effectiveness of our solutions. Let us show you how we can enhance your cybersecurity defenses.

Not ready for a demo call yet?

Start by creating a preview account in the ESET Threat Intelligence portal to explore feeds and APT reports.

This is ESET

Proactive defense. Minimize risks with prevention.

Stay one step ahead of known and emerging cyber threats—targeted attacks, zero-day threats, ransomware, phishing, and more—with our AI-Native, prevention-first approach. ESET combines the power of AI and human expertise to deliver easy and effective protection.

Experience best-in-class, science-driven security, backed by over 30 years of in-house global cyber threat intelligence. Our extensive R&D network, led by industry-acclaimed researchers, powers our award-winning, cloud-first cybersecurity platform. ESET solutions are highly customizable, include local support, and have minimal impact on performance.

ESET protects your business so you can unlock the full potential of technology.

ESET IN NUMBERS

1bn+
protected internet users

500k+
business customers

178
countries

11
global R&D centers

SOME OF OUR CUSTOMERS

MITSUBISHI MOTORS
Drive your Ambition

protected by ESET since 2017
more than 9,500 endpoints

Allianz Suisse

protected by ESET since 2016
more than 4,000 mailboxes

Canon Marketing Japan Group

protected by ESET since 2016
more than 23,000 endpoints

ISP security partner since
2008 2 million customer base

RECOGNITION

SE LABS® AWARDS Enterprise Endpoint (Windows) WINNER 2025

Winner of the **Best Enterprise Endpoint** and **Best Small Business Endpoint** awards at the SE LABS Awards 2025

Gartner Peer Insights **Customers' Choice** 2026

Named a **Customers' Choice** in Gartner® Peer Insights™ **"Voice of the Customer" Endpoint Protection Platforms** report 2026

FROST & SULLIVAN

Named a **Leader** in Frost Radar: Endpoint Security 2025, demonstrating excellence in growth & innovation