A unified AI-powered threat intelligence workspace for SOC teams and threat analysts

Kaspersky Threat Intelligence Portal

kaspersky cybersecurity true to business

7

areas of CIS18 controls covered*

848%

potential ROI in the first year*

$2.3M

average cost of damage reduction in the first year of implementation*

№1

leader in APT Intelligence and Attribution**

FROST & SULLIVAN

The brain of your cybersecurity ecosystem

The Kaspersky Threat Intelligence Portal (TIP) is a centralized platform and investigation workspace that gives security teams a single access point to trusted, up-to-date cyberthreat intelligence.

It brings together Kaspersky's threat research, intelligence data, analysis technologies, and expert knowledge in one unified web interface and API, enabling organizations to investigate threats, enrich Indicators of Compromise (IOCs), analyze malware, track threat actors and campaigns and make faster, more precise security decisions.

Clear value for every security role

C-level

Gain a clearer view of external risk, justify security investment against the actual threat landscape and improve the effectiveness and value of your existing security stack.

SOC L1/L2

Instantly enrich every alert with relevant context, filter false positives automatically and accelerate triage – reducing repetitive workload and analyst fatigue.

SOC L3 and threat hunters

Investigate complex threats in greater depth, link activity to known APT groups, analyze suspicious samples securely in a sandbox and access unique research.

Your next security decision starts here

Understand faster

Our AI automation helps analysts focus on what matters by transforming large volumes of threat information into concise, actionable intelligence.

- Reduce analyst time spent reviewing and processing threat reports
- Accelerate triage and investigation workflows through AI-powered contextualization
- Improve SOC productivity without increasing headcount

See further

The Kaspersky Threat Landscape provides a continuously updated view of the threats, actors, industries, technologies and regions that matter most to your organization.

- Improve cyber risk prioritization by understanding emerging attacker activity and trends
- Strengthen cyber resilience through proactive threat awareness rather than reactive response
- See beyond your perimeter and build a strong cybersecurity strategy

Decide smarter

A powerful set of unique investigation tools helps analysts identify threats, attribute actors, validate findings, and accelerate response.

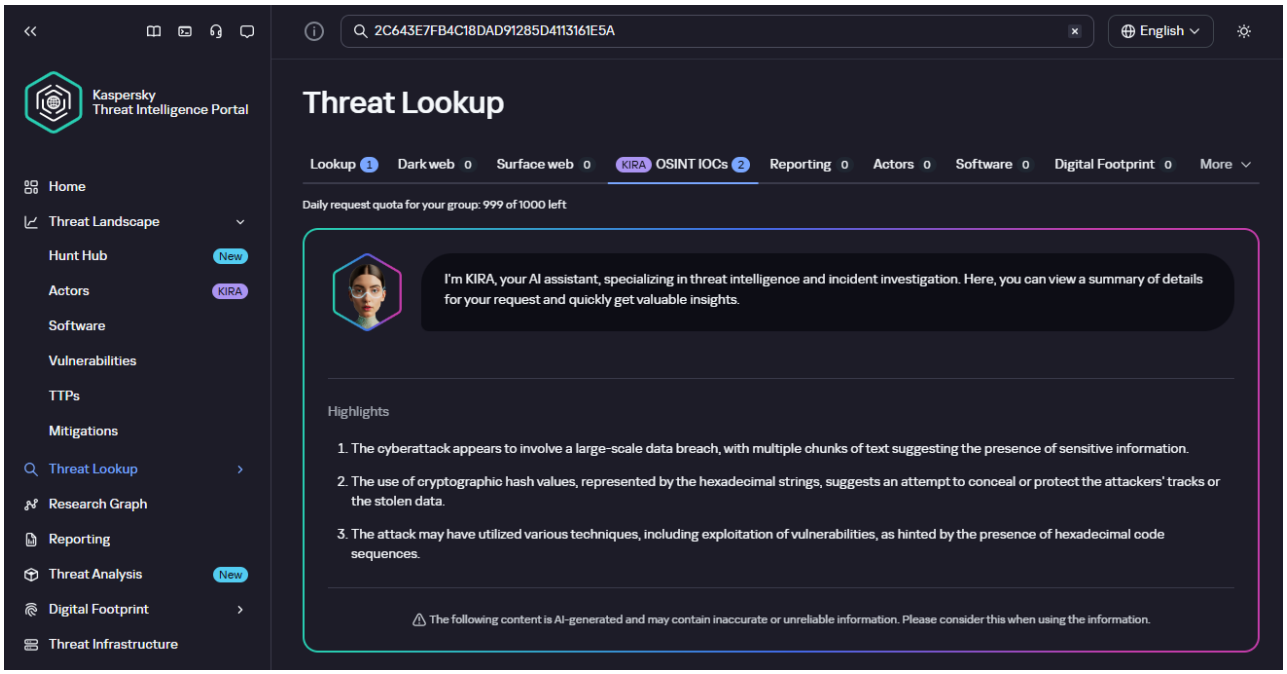
- Improve analyst confidence through attribution, analysis and correlation capabilities
- Gain access to detailed research on advanced campaigns, threat actors and emerging attack techniques
- Accelerate investigations with trusted context, threat validation and expert intelligence

* Kaspersky ROI Calculation Analysis Report, 2026

** Frost & Sullivan Global Company of the Year award in the APT Intelligence & Attribution industry, 2026

Your AI-powered Threat Intelligence Assistant

KIRA, Kaspersky's Investigation and Response Assistant, helps security teams work faster and more efficiently by bringing AI-powered assistance directly into your daily cybersecurity workflows. For specific use cases, you can connect your preferred third-party AI models.



AI summarization

When searching for any object, AI automatically traces its relationships across multiple levels, aggregates the results, and produces a simple, human-readable verdict explaining what was found and why the object was classified in that way.

AI-powered OSINT search

Transforms data collected from publicly available sources into clear, actionable threat intelligence. Type a query and get a synthesized summary of what the security community already knows.

Expanded actor profiles

When a new Kaspersky Threat Intelligence report is published on a specific subject, new TTPs, recent campaigns, and updated technical indicators are automatically linked to the profile.

Third-party AI models

Remote MCP support for Kaspersky Threat Intelligence Portal lets you connect any compatible AI assistant: Claude, ChatGPT or any other MCP-enabled tool. Threat Intelligence Portal data becomes available as live tools inside the AI environment of your choice.

Become a threat hunter with advanced tools

Every service in the Kaspersky Threat Intelligence Portal is powered by the Kaspersky Threat Landscape, providing complete, continuously updated visibility into global and company-specific threat environments.

Tactical
Perishable data to support security operations and incident response

Operational
A clear view of specific threat actor attributes, including their capabilities, behaviors and intent

Strategic
Trends, actor motivations and their classifications, supporting C-level executives in making critical decisions

---

Kaspersky Threat Lookup

Access Kaspersky's complete body of cyberthreat knowledge, along with the connections between related threats

- Threat Hunting
- Incident Response
- Monitoring

Best fit for SOC Analysts

Kaspersky Threat Analysis

Go beyond surface-level analysis with flexible, multi-layered analysis to detect previously unknown threats in suspicious files

- Threat Hunting
- Incident Response

Best fit for SOC L3 and DFIR/IR Analysts

Kaspersky Threat Intelligence Reporting

Stay ahead of the most relevant, dangerous threats with exclusive access to Kaspersky research and expert threat intelligence

- Threat Hunting
- Incident Response
- Building Strategy
- Raising Awareness
- Monitoring

Best fit for SOC and DFIR/IR Analysts as well as for C-Level

Kaspersky Digital Footprint Intelligence

Comprehensive monitoring of your corporate digital assets to detect threats to your organization from the surface, deep and dark web

- Threat Hunting
- Incident Response
- Building Strategy
- Raising Awareness

Best fit for SOC L3 and DFIR/IR Analysts as well as for C-Level

Kaspersky Brand Monitoring

Detect and mitigate brand abuse, impersonation and other online threats with advanced brand monitoring backed by unique expertise

- Threat Hunting
- Incident Response
- Building Strategy
- Raising Awareness

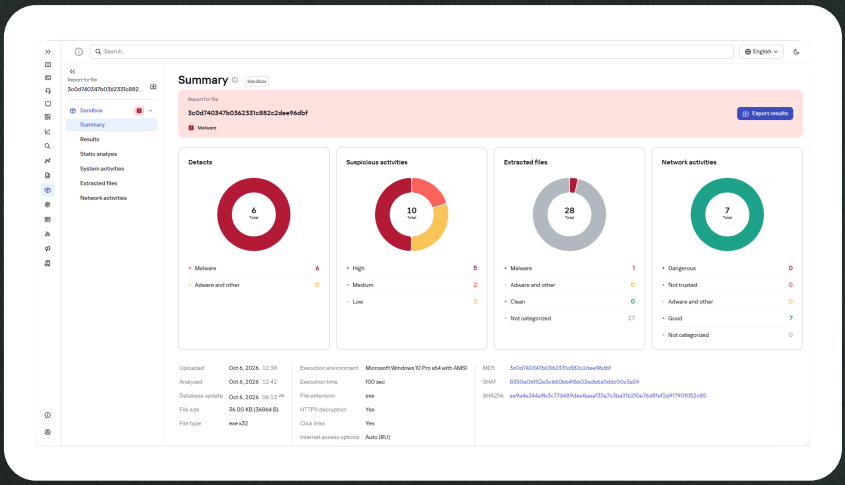
Best fit for SOC L3 and DFIR/IR Analysts as well as for C-Level

A Unified Threat Intelligence workflow

Incident Response

Investigate security incidents faster and understand the full context needed to respond effectively.

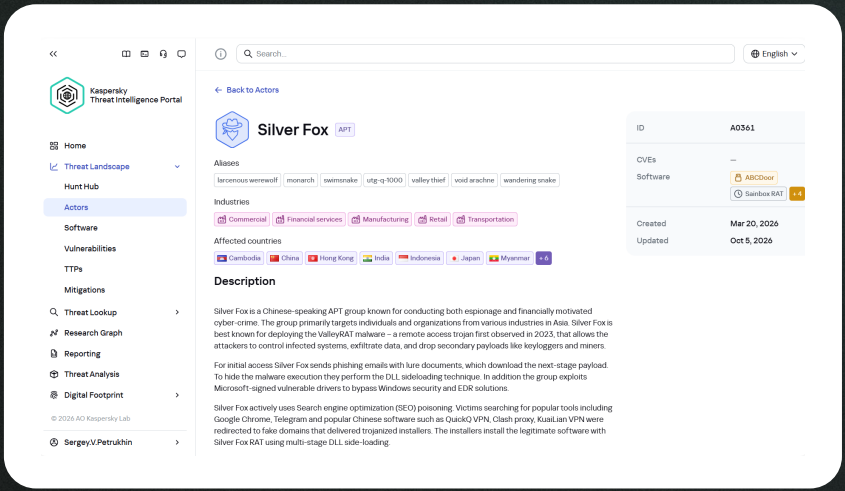
- Investigate IOCs
- Analyze suspicious files
- Reconstruct the incident
- Prioritize the response
- Get expert context



Adversary Tracking

Understand which threat actors are most relevant to your organization and track their activity, capabilities and campaigns.

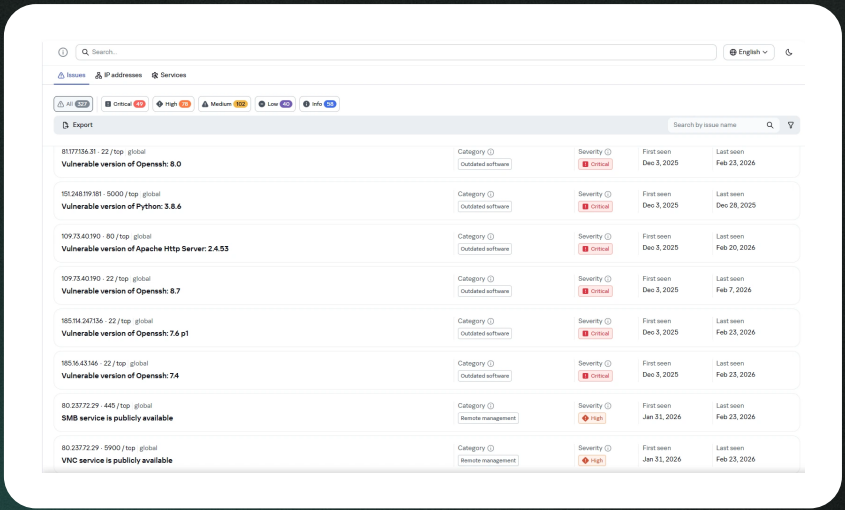
- Identify relevant adversaries – discover threat actors and campaigns targeting your industry and region
- Track attacker activity – follow related infrastructure, malware and indicators
- Capabilities and intent – access expert analysis of APT, crimeware and other sophisticated threat actors
- Build an adversary view – connect campaigns and attacker activity to your organization's specific threat environment



Digital Risk & Brand Protection

Discover and investigate threats targeting your digital presence, brand and externally exposed assets.

- Discover exposed assets – identify external assets, misconfigurations and exposed services
- Find compromised data and accounts – monitor the deep and dark web for leaked data and compromised credentials
- Detect brand abuse – identify impersonation, phishing, fraudulent resources and unauthorized use of your brand

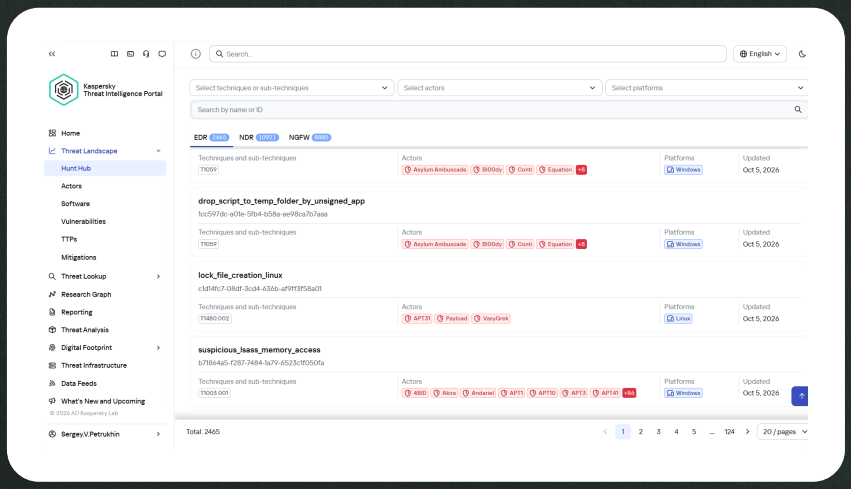


A Unified Threat Intelligence workflow

Threat Hunting

Proactively search for hidden threats and uncover malicious activity that may have bypassed existing defenses.

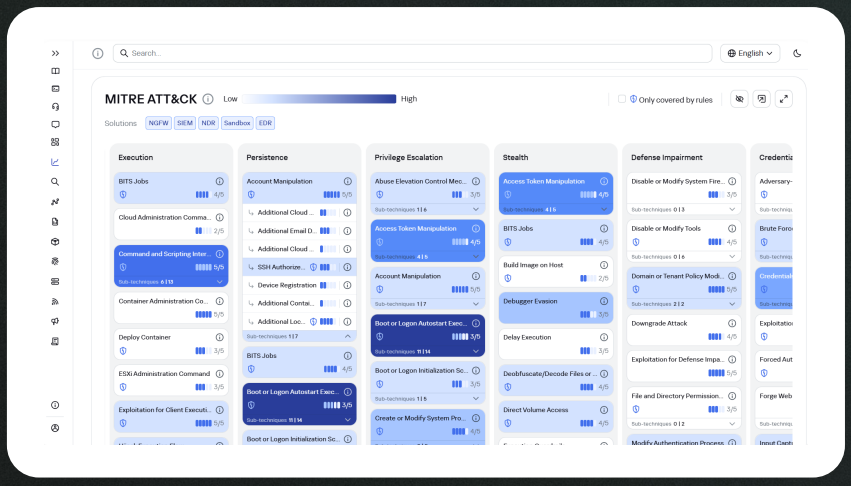
- Search for unknown connections – explore relationships between indicators, infrastructure and threat artifacts
- Validate hunting hypotheses – investigate suspicious files and related samples
- Hunt for emerging threats – identify new threats and activity relevant to your industry and organization
- Extend the hunt externally – investigate exposed assets and compromised accounts



Strategic Decision Support

Turn threat intelligence into strategic insight to help prioritize risk, investment and security initiatives.

- Define your threat environment – understand the threats and adversaries most relevant to your organization
- Identify emerging risks – track trends, attacker activity and developments that could affect your industry
- Understand sophisticated threats – access expert analysis of major APT, crimeware and ICS campaigns
- Validate strategic concerns – conduct deeper investigations into specific threats when needed
- Assess broader business exposure – incorporate external and reputational risks into your security decisions



Why organizations worldwide choose the Kaspersky Threat Intelligence Portal

Unique Threat Intelligence infrastructure

200+ million sensors

around the world

170,000 indicators

of compromise linked to TI reports

130,000+ samples

make Kaspersky's APT file collection the largest in the industry

Research lab

30 years

of unique historical threat data, research and expertise

Kaspersky researchers

are invariably the first to expose major threats including Stuxnet and Operation Triangulation

200+ certified specialists

work across five internationally recognized centers of expertise

200+ unique private reports

published by our experts each year

Proprietary technologies

Extensive repositories

of malicious and legitimate files, darknet resources, web scanners and spam traps provide comprehensive intelligence coverage

AI and proprietary technologies

support threat detection, analysis and attribution

Defined SLAs

support timely threat intelligence updates following the detection of critical threats

Expertise

900+ hacker groups

and operations constantly monitored by our experts

200+ countries

from where we collect unique threat intelligence

500,000+ new unique malicious files

detected by us every day

Most trusted. Most awarded.

INTERPOL

AFRIPOL

QKS Group

FORRESTER®

FROST & SULLIVAN

Kaspersky Threat Intelligence Portal

Request a demo

www.kaspersky.com

© 2026 AO Kaspersky Lab.
Registered trademarks and service marks
are the property of their respective owners.

#kaspersky
#truetobusiness