

Custom detections for Kaspersky SIEM and Kaspersky Next XDR

Reduce the risk of undetected cyberattacks with Kaspersky Detection Engineering

kaspersky

Threats evolve. Detection must keep pace.

Attackers use increasingly sophisticated techniques, combining multi-stage attack chains, defense evasion and constantly changing toolsets. At the same time, every organization has a different infrastructure, with different sources and volumes of security data. Out-of-the-box rules and basic monitoring alone are therefore not enough to detect many of today's threats.

Effective detection requires continuous development: expanding coverage, adapting detection use cases to the organization's infrastructure and available data, and regularly testing and fine-tuning detection logic. But not every security team has the time, resources or specialist expertise to do this effectively.

43%

of event sources covered by correlation rules on average[1]

Detection use case development helps organizations make better use of available telemetry to detect threats.

50%

of SOCs rely primarily on prebuilt rules supplied by vendors[1]

Tailoring detection rules to an organization's environment helps reduce false positives and close gaps in threat detection.

41%

of respondents struggle to find qualified specialists in detection use case development[2]

Bringing in external expertise helps advance detection capabilities without expanding the in-house team.

What is Kaspersky Detection Engineering?

Kaspersky Detection Engineering is an expert-led service for developing, testing, deploying and tuning detection use cases for Kaspersky SIEM and Kaspersky Next XDR.

Kaspersky experts identify the customer's priority detection needs, assess the organization's infrastructure and available telemetry, and develop use cases tailored to its environment. These use cases are then integrated into SOC workflows and delivered with supporting documentation and recommendations for ongoing use.



Kaspersky SIEM

A SIEM platform for centrally collecting, analyzing and correlating security events.

Learn more



Kaspersky Next XDR Expert

An XDR platform for multi-layered detection, monitoring, investigation and response across complex attacks and security incidents.

Learn more

1 Global Report Kaspersky Security Services, 2026

2 SANS Detection Engineering Survey, 2025

Where Kaspersky Detection Engineering helps

Kaspersky Detection Engineering helps establish detection capabilities for a new SOC or strengthen those already in place.

Strengthen SOC detection capabilities

Expand detection coverage based on the organization's infrastructure and changing threat landscape.

Bring new systems into monitoring

Develop detection use cases for newly connected systems and data sources.

Migrate detection content to Kaspersky SIEM and XDR

Transfer and adapt detection content from other platforms and solutions for use within Kaspersky SIEM and Kaspersky XDR.

Meet regulatory detection requirements

Develop and adapt detection use cases to address applicable regulatory requirements.

Apply lessons from incidents and cyber exercises

Create new detection use cases and update existing ones based on observed attacks, incident investigation findings and cyber exercise results.

Develop detection content with Kaspersky experts

Work with Kaspersky experts to develop, test and tune detection use cases and prepare them for operational use.

Kaspersky expertise

At the core of the service

Kaspersky Detection Engineering draws on global telemetry from Kaspersky MDR, Kaspersky Threat Intelligence data and analysis, extensive threat research, incident response experience and in-depth knowledge of Kaspersky SIEM and Kaspersky Next XDR architecture.

These capabilities enable Kaspersky experts to develop detection use cases based on real-world threats and adapted to the customer's infrastructure and technical capabilities.

Kaspersky was named a Leader in the Frost Radar™: Cyber Threat Intelligence, 2024 report, recognized for its innovation and strong position in the Cyber Threat Intelligence market.

Learn more



How we develop detection use cases

The scope of work depends on the project objectives, target systems and available telemetry.

1

Define objectives and priorities

Clarify the project objectives, assess the current threat landscape and identify the systems and attack scenarios that detection needs to cover.

2

Assess infrastructure and telemetry

Examine the target systems, data sources and event types to determine whether the available telemetry can support the required detection use cases. Where gaps exist, recommend improvements to data collection.

3

Design detection logic

Define the threat activity each use case needs to identify and the telemetry required to detect it. Where relevant, map the use cases to MITRE ATT&CK or another applicable threat classification framework.

4

Develop and deploy detection use cases

Build the detection use cases based on the approved logic and deploy them in Kaspersky SIEM and/or Kaspersky XDR.

5

Test and fine-tune

Validate that each use case works as intended, refine its triggering conditions and tune it to reduce false positives.

6

Document and transfer knowledge

Provide documentation and operational guidance for the developed use cases, followed by a knowledge transfer session with the customer's team.



MITRE ATT&CK is a globally recognized knowledge base of adversary tactics and techniques.

Detection use cases are mapped to MITRE ATT&CK or another classification framework used by the customer's SOC.

Business and SOC team outcomes

Business outcomes

- Reduced risk of attacks going undetected through broader, more effective detection coverage.
- Better support for regulatory requirements related to security monitoring and threat detection.
- Continued development of SOC detection capabilities with ongoing support from Kaspersky experts.

Impact on SOC operations

- New detection use cases become part of day-to-day security monitoring.
- Your SOC teams receives practical guidance for maintaining and further developing detection content.
- Your SOC specialists understand the logic behind each use case through dedicated knowledge transfer.

What your SOC team receives

Developed and tested detection use cases

A set of detection use cases developed and tested for Kaspersky SIEM and/or Kaspersky Next XDR.

Operational guidance

Recommendations for maintaining, operating and fine-tuning the developed detection rules.

Documentation for each detection use case, including:

- Purpose
- Required data sources and event types
- Fields used
- Mapping to MITRE ATT&CK or another framework used by the customer's SOC
- Detection logic
- Audit configuration requirements
- Enrichments used

Strengthen your SOC's detection capabilities

Talk to a Kaspersky expert about your priority detection use cases, telemetry requirements and plans for developing detection content.

Get in touch

Kaspersky Detection Engineering

www.kaspersky.com

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

#kaspersky
#truetobusiness