Establish your own Security Operations Center or enhance your current SOC

Kaspersky SOC Consulting services

kaspersky BRING ON THE FUTURE

Security Operations Center (SOC)

is a centralized command center that monitors, detects, analyzes, and responds to security incidents within an organization's network and systems.

Overview

By investing in the right resources, technology, and people, you can enhance your security posture, mitigate risks and protect sensitive data and business services — safeguarding your reputation and business continuity in an increasingly complex threat landscape.

Based on our experience in security operations and reflecting the latest security best practices, Kaspersky has developed a wide range of consulting services to help you establish your own SOC.

Kaspersky SOC Consulting Services can help you:

Build a SOC from scratch	Kaspersky will develop a comprehensive SOC framework for you, from creating a high-level SOC strategy to developing policies, procedures and guidelines.
Increase the maturity and capability of existing operations	
Identify gaps in security operations and opportunities for improvement	SOC Maturity Assessment covers the five main security operations domains: Business, People, Process, Technology, and Services.
Understand your potential threat landscape	The service is focused on building a company's own Cyber Threat Intelligence Program. This framework enables organizations to better understand the tactics, techniques, and procedures used by threat actors, to identify potential vulnerabilities, and to develop effective countermeasures and incident response strategies.
Increase the efficiency of your incident response activities	Kaspersky Incident Response Readiness (IRR) helps to identify and close gaps in your current incident response activities on multiple levels, from the interaction between different departments across the organization to the steps required to respond to specific threats.
Test the detection capabilities of your security team	Kaspersky Adversary Attack Emulation provides tests against different adversary techniques and analyzes blue team capabilities. The emulated tests are mapped to tactics and techniques in the MITRE ATT&CK framework.

Why Kaspersky SOC Consulting Services?

1

The World's Largest Independent Information Security Company

With a global presence focused on threat intelligence and technology leadership.

2

Hands-on experience in building SOCs

Our approach to organizing a SOC is based on practical experience, including operating our own SOC, providing security services to our clients, investigating APT campaigns and customer incidents, as well as conducting daily analysis of approximately 400,000 new malware samples.

3

Certified Cybersecurity Team

Our team consists of certified experts in areas including Information Security, Incident Management, Digital Forensics, Malware Analysis, Network Security and Risk Assessment. Our experts also leverage widely recognized best practices, such as methodologies from MITRE, NIST, SANS Institute, ENISA, FIRST and other professional communities.

Key project stages

Building a SOC is a major undertaking, and the business of improving and optimizing its operations, tools and pool of human expertise should be ongoing.

Our approach is based on identifying significant maturity levels, and achieving them in separate stages or through consecutive SOC development projects.

The average project covers four main steps:

Data collection

Understanding the current state of your security operations, and the future state that's our joint objective.

Framework development

Defining and developing a model of your SOC and assessment procedures, covering key security operations domains: people, processes and technologies.

Guidance with technologies & processes implementation

Consulting support for the implementation and deployment of technical solutions within the framework of the developed SOC project documentation. Coordination of the of teams implementing SOC solutions.

Continuous improvement and support

Additional training for your security teams, development of detection logic, dedicated threat intelligence or any other additional Kaspersky service to ensure your SOC's optimum efficiency.

Kaspersky SOC Consulting outcome

We take a comprehensive approach to SOC design, following best practice but adapted to your needs and resources.

Service	Description	Key Deliverables
SOC Framework Development	The goal of the service is to develop a consistent and complete SOC framework, which covers building, operation and further development of a SOC. The objectives of the service include but are not limited to: • Definition of SOC processes, procedures and policies • Definition of SOC staff roles, requirements and responsibilities • Definition of SOC organizational chart • Definition of SOC KPI • Technical architecture design • Developing the SOC strategy and roadmap • Developing SOC security use- cases • Developing incident response playbooks • Deployment and configuration of security tools • SOC staff training and knowledge transfer	• Full SOC design documentation for processes, architecture and team • SOC Use Cases • SOC Playbooks
SOC Maturity Assessment	Maturity measurements are a widely used tool for evaluating strengths and weaknesses. The SOC-CMM is an internationally-recognized capability maturity model that can be used to perform an assessment of the Security Operations Center (SOC). Because different kinds of security-related activities are aggregated into the SOC, determining the maturity level of the SOC as a whole requires determining the maturity level of each of its elements. This enables SOC management to make informed decisions about which elements of the SOC require additional attention and/or budget. By regularly assessing the SOC for maturity and capability, ongoing progress can be monitored. This tool is intended to be used by the customer's SOC to achieve the following goals: • Gain a formal understanding of the current security operations posture • Get insights into weak spots, and plan future resources and efforts for these areas • Assess the progress of security operations improvement activities	• Assessment Report with identified gaps and recommendations • SOC Roadmap to close identified gaps (optional)

Service	Description	Key Deliverables
IR Readiness Assessment	Incident response readiness is a set of capabilities (people, processes, technology, etc. that provide an ability or capacity to perform incident response tasks) that are considered essential to protecting, detecting, and responding to cyber security incidents, as well as to sustaining the overall incident handling and response function. The key goal of the IRR Assessment Service is to assess current IR activities in the organization and provide a detailed report highlighting gaps and recommendations for improvement. The IRR Assessment Service typically covers a review of customers' IR plans, IR processes, IR procedures, response playbooks, the external and internal participants involved based on incident severity, the communications matrix, and technical solutions used for incident detection, management, and response.	Assessment Report with identified gaps and recommendations
IR Readiness	The key goal of the IR Readiness Service is to assess current IR activities in the organization and define a draft Incident Response Plan that covers the following topics: • IR Policy • IR Methodology • IR Process and Procedures This draft will consider the current organizational structure, internal processes and available resources. IR methodology is based on the NIST staged approach for Incident Handling. These stages are structured in seven phases derived from NIST (SP 800-61r2). They support the customer in maintaining consistency in incident tracking and reporting throughout the security incident lifecycle. IR stages provide a defined, repeatable, and measurable process by which customers can effectively respond and handle cybersecurity incidents originating from inside or outside of the organization.	• Incident Response Plan • IR Playbooks
CTI Framework	Threat intelligence is a crucial piece of any cybersecurity ecosystem. With a well-defined cyber threat intelligence program, your company can predict threats, prevent attacks, detect breaches and respond to incidents using the right processes, technologies and cybersecurity services. The CTI program also supports cybersecurity operations at a strategic level and helps the organization put the right security measures in place to safeguard against future attacks based on information about tactics, techniques and procedures used by cybercriminals. The CTI Framework project is focused on the assessment of existing CTI practices and operations and the development of a set of documents required to establish and	Design of corporate CTI program, including, processes, procedures, guidelines, architecture etc.

Service	Description	Key Deliverables
CTI Framework	improve CTI capabilities, which will include: • Cyber Threat Intelligence Assessment to understand the state of current CTI capabilities and identify gaps to plan further improvements • Cyber Threat Intelligence Capability Program to set out the strategic objectives and steps recommended for establishing CTI capabilities as well as a roadmap with necessary changes and steps for improvement • Cyber Threat Intelligence Framework with a set of documents to enable your organization to manage the CTI service on a day-to-day basis • Cyber Threat Intelligence Workshops to provide knowledge transfer sessions for staff involved in CTI operations.	
Adversary Attack Emulation	While Red Teaming is a good solution to check the company's resistance against real attacks, including prevention, detection and incident response capabilities, the red teaming service is very time consuming and can't be conducted very often (e.g. quarterly). Furthermore, as the red team targets critical systems only and performs the service as stealthily as possible, multiple attack techniques might not be covered. The missed techniques may then be used by other threat actors, including non-public APTs, malware or widespread ransomware attacks. The Kaspersky Adversary Attack Emulation Service closes this gap with a detailed assessment of a company's detection capabilities by emulating techniques of various threat actors on every stage of the cyber killchain. This service has the following objectives: • Analyze the coverage of the collected telemetry • Assess the customer's detection capabilities for each test in the scope of assessment • Identify gaps in detection security controls • Provide recommendations to fix these gaps. The Adversary Attack Emulation Service covers key stages of the cyber kill chain related to the internal infrastructure. The emulated tests are mapped to tactics and techniques of the MITRE ATT&CK framework. Based on different sets of chosen tests, the service can focus on specific goals. Choosing the tests for the Adversary Attack Emulation Service can be based on: • Techniques used by specific APT groups • Techniques used by region-specific or industry-specific APT groups • The most popular techniques used by all APT groups according to MITRE ATT&CK • The most popular techniques seen by Kaspersky MDR (Managed Detection and Response).	• Incident Response Plan • IR Playbooks

You may also be interested in

Kaspersky CyberTrace

Enabling effective threat intelligence management

Learn more

Kaspersky Endpoint Detection and Response Expert

Build defense-in-depth and boost security efficiency with automated responses and simple root cause analysis

Learn more

Kaspersky Threat Intelligence

For instant access to tactical, operational and strategic TI

Learn more

Improve your team's skills with Kaspersky training programs

1

Security Operations and Threat Hunting

During your time on the course, you will learn about the different roles within a SOC, its services and use cases, modern attack tactics, techniques and procedures, and how the SOC can help you deal with them. You'll have the opportunity to develop your incident detection and investigation skills through a series of in-depth lab sessions in the restricted areas of the virtual labs.

Course program

2

Suricata for Incident Response and Threat Hunting

Learn how to write and implement Suricata rules to detect and block even the most advanced threats. Gain a deep understanding of how the framework works and how to use it to detect and respond to attacks in real time. Get hands-on experience to improve your network security through practical exercises and various real-world scenarios.

Course program

3

Hunt APTs with Yara like a GReAT ninja

Our Threat Hunting with Yara online course draws on years of experience from the high-profile cases our specialists have worked on. Course instructor Costin Raiu, a 25-year veteran of the threat hunting industry, will teach you the unconventional ways of working with Yara so you can find threats on the same scale as his team.

Course program

Kaspersky SOC Consulting

Learn more

www.kaspersky.com

#kaspersky
#bringonthefuture