IDC Technology Spotlight

Sponsored by **Kaspersky**

Authors:

Konstantin Rychkov

Christopher Kissel

August 2020

Battle for the Modern Security Operations Center

The Evolution of Security Operations and the Contemporary State of Play

Today more than ever, security is not about buying the latest security novelties; it is about building efficiencies into the processes that contribute to overall business priorities, without undermining key security prerequisites. Currently, over half of all global businesses with 2,500 or more employees already have a security operations center (SOC) in one form or another, and 72% of those have built these capabilities within the last five years. The most advanced organizations build their internal security operations centers so that they are integrated with overall IT governance and guided by strategic priorities on the horizon.

This change in approach is reflected in many layers:

- Cybersecurity automation intelligence response and orchestration technologies, which previously had an exclusive position at the core of the SOC, now compete with other technologies and/or have become inclusive components of detection and response technologies and services.
- SOCs have become collaborative projects, involving NetOps, SecOps, DevOps, and business contributors.
- The expansion of organizational perimeters has led to floods of alerts and masses of noise, thus encouraging greater use of:
  - Functional outsourcing, whereby organizations rely on managed security services (MSS) from select service providers or security vendors (with 85% of companies currently outsourcing at least part of their SOCs to MSS providers and 32% fully outsourcing their SOCs)
  - Research and triage augmentation with threat intelligence (TI), either through paid feeds or by building a TI practice and plugging it into a specialized platform (with overall spending on TI among North American organizations of over $1.2 billion)
  - Streamlining functions and SOC processes with automation and orchestration (with a 5-year CAGR for the SOAR market in North America of 7.4%, even when accounting for the impact of the COVID-19 crisis)

The modern SOC has evolved dramatically, as have requirements for its efficiency and effectiveness.

Challenges of the Modern SOCs

Increasing Volume of Alerts Compounded by the Skills Gap

Triaging and system maintenance eat up the time of resource-restricted security teams. This problem is not novel to the industry, and over 90% of teams are operating understaffed. Analysts' time would be better spent working on more sophisticated alerts that need human intervention, as well as proactively threat hunting to minimize the time from breach discovery to resolution.

Today, on average, a cybersecurity analyst stays in a company for 27 months, 4 months of which are spent on induction training.

Swiveling Chair Problem

A typical security operations center may use a combination of 20 or more technologies, which understandably can be difficult to monitor and manage individually. Triage can be hard across even two different dashboards, but normally we are looking at numbers well above three: network, security incident and event management (SIEM), TI, and so on.

A lack of integration between tools complicates the resolution push. Usually, we have separate endpoint, network, and web policies, and the situation is worsening due to the number of deployment environments in the cloud and on premises.[1]

Legal and Regulatory Compliance

Since the initial round of regulatory upheaval in 2016–2017, the importance of compliance for security operations has grown tremendously. Regulatory compliance is now among the top-five priorities for security leaders.

Despite the security industry's active progress in this direction, legal and security compliance are still unsolved issues. Even if we ignore the impact of numerous "tick-box compliance" exercises aimed at passing audits, issues such as regulatory overlaps for multinationals will remain. Moreover, this is yet another process, console, and/or tool to manage for the SOC team.

Budgets

Demonstrating immediate ROI for SOC tooling is almost impossible, but businesses still prefer this indicator for defining budget allocations. If we take the formula for ROI from the official guide to CISSP-ISSMP, the hardest to assess would be the monetary impact from applying countermeasures. And, yes, it still leans on a reactive approach to security.

While the long-term effects of COVID-19 are still to be determined, a global IDC survey of 880 IT professionals found that 54% of companies plan an increase in, or no change to, their IT budgets in 2020 and 2021. More companies were expected to have reduced their planned IT budgets than those planning to increase them, but IT has become an essential part of every business. With a greater shift to remote working and growing economic uncertainty, perhaps the case for getting a better performance out of the SOC is now stronger than ever.

[1] IDC Technology Spotlight: Integrated Cybersecurity Delivers Efficiency and Effectiveness in a Challenging Environment

Knowledge Transfer and Talent Sourcing

The security talent sourcing problem is no surprise, but issues currently also exist around knowledge transfer for sophisticated enterprise systems, especially in connection to business routines.

Acquiring and raising talent internally costs money, but the time a tier-one analyst spends at a company is decreasing each year. Nowadays, on average, a cybersecurity analyst stays in a company for 27 months, 4 months of which are spent on induction training.

A lack of documented processes and procedures forces SOC leaders to start from scratch every time a shift in the team occurs. So, increasing turnover among analysts decreases the efficiency of the entire security program.

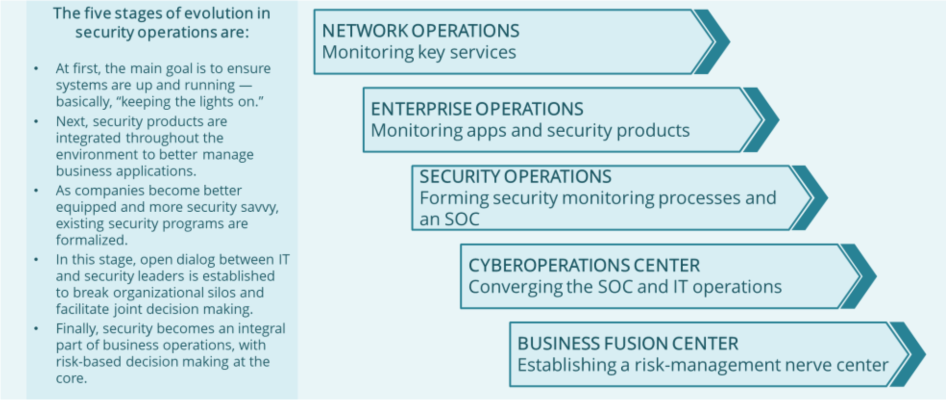
Human-less Technology's Impact on Operations

According to IDC research, the majority of CISOs find that time is wasted on routine tasks and maintenance when that time could be better spent on actual response. Building a “great filter” can help to prioritize real problems and resolve the basics much faster.

We can engage tier-one analysts, and, as we build in more automation and orchestration, our SOC will evolve along the maturity curve, as shown here:

Figure 1

Maturity Curve for Security Operations



The five stages of evolution in security operations are:

- At first, the main goal is to ensure systems are up and running — basically, “keeping the lights on.”
- Next, security products are integrated throughout the environment to better manage business applications.
- As companies become better equipped and more security savvy, existing security programs are formalized.
- In this stage, open dialog between IT and security leaders is established to break organizational silos and facilitate joint decision making.
- Finally, security becomes an integral part of business operations, with risk-based decision making at the core.

NETWORK OPERATIONS
Monitoring key services

ENTERPRISE OPERATIONS
Monitoring apps and security products

SECURITY OPERATIONS
Forming security monitoring processes and an SOC

CYBEROPERATIONS CENTER
Converging the SOC and IT operations

BUSINESS FUSION CENTER
Establishing a risk-management nerve center

Source: IDC

Progression through stages by using internal resources and only enhancing the SOC stack with technology is not feasible for most organizations. For that reason, the automation of security functions and the augmentation of the internal SOC with managed security services is inevitable and, in fact, recommended.

Progression through maturity stages by using internal resources and only enhancing the SOC stack with technology is not feasible for most organizations. For that reason, the automation of security functions and the augmentation of the internal SOC with managed security services are inevitable and, in fact, recommended.

Recently, security technology has leapfrogged the expected evolutionary stages to help practitioners with this problem. Automation and outsourcing help the security team speed through the traditional sequence of monitor, collect, correlate, analyze, detect, and report. Incident management automation builds an operational link between insight and action. Threat intelligence, in turn, helps in incident prioritization and preemption, guiding the team's efforts to maximize efficiency.

Filling the Gaps in Your SOC

To overcome the challenges of building and running a security operations center, CISOs need a comprehensive solution that can enable the team to achieve the following:

- Build automation and transfer that knowledge into custom incident response playbooks, which can subsequently simplify dealing with similar incidents
- Enable expert teams to build a threat intelligence program to utilize TI information and maximize the output, demonstrating return on investment to the management (This use of TI has long been advocated in the market.)
- Proactively hunt threats to help prevent possible attacks and build defenses and a posture validation mechanism in accordance with the threat landscape that the enterprise faces
- Integrate the incident management toolkit with all systems that the computer security incident response team (CSIRT) requires for ticketing, runbook automation, collaboration channels, forensicating, and key performance indicator (KPI) monitoring (Agility in the response phase is essential for an effective SOC.)
- Establish a central console in which all sources of information from the web, networks, endpoints, email, and additional analytics are correlated and retained for investigation (This functionality becomes crucial to the SOC in the event of an advanced attack on the organization.)
- Dedicate resources to managing cloud architectures (In North America, the average business uses 1.63 cloud providers for hosting and IaaS, and roughly 55% of companies have more than half of their workloads in clouds.)
- Implement security and privacy guidelines from the very start of building the SOC plan, and focus on risk-driven governance
- Establish programs to retain and upskill personnel from the SOC's inception onward (Training should not only help in building essential knowledge in the team, but also facilitate effective knowledge-transfer processes. Security skills gaps exacerbated by turnover can interrupt and indefinitely delay the most well-structured SOC transformation plans.)

Considering Kaspersky Expert Framework and Toolset for SOC

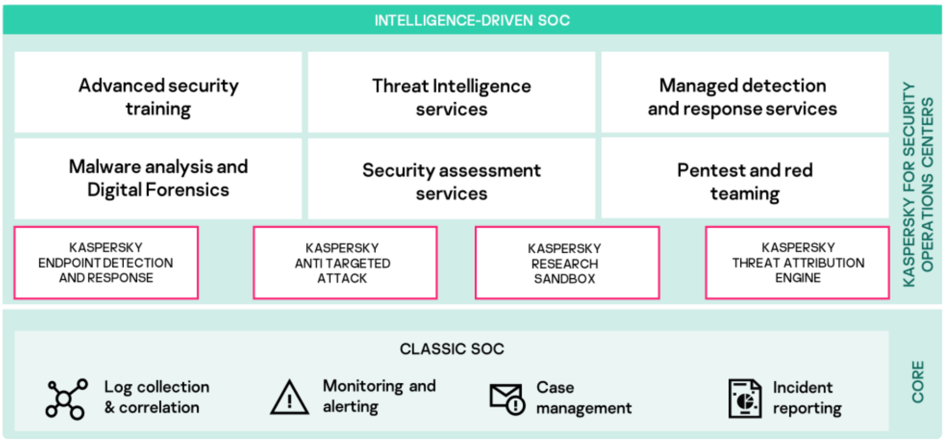
With the breadth and depth of problems that security leaders face en route to building a next-generation SOC, it is hard to imagine a single solution that can plug all the gaps and would fit any environment. Frankly speaking, it truly is not yet possible. Such a solution would need to include processes, people, and technology, with associated guidelines, wrapped into a comprehensive out-of-the-box operational framework and delivered as a platform or a managed service. While this is currently a tall order, transformation offerings exist on the market that can enhance the traditional SOC and facilitate the journey up the maturity curve.

To enable a next-generation SOC, a solution would need to include processes, people, and technology, with associated guidelines, wrapped into a comprehensive out-of-the-box operational framework and delivered as a platform or a managed service. While this is a tall order, transformational offerings exist that can enhance the traditional SOC and facilitate the journey up the maturity curve.

Kaspersky's Expert framework links a vast portfolio of advanced tools with dedicated services and expert support. In its essence, Kaspersky's approach is to identify issues and oversights in both the process and the underlying technology, and then address them with comprehensive solutions and services to enable SOC transformation. A high-level overview of key components is shown in Figure 2, below.

Figure 2

Kaspersky for Security Operations Center


INTELLIGENCE-DRIVEN SOC
Advanced security training
Threat Intelligence services
Managed detection and response services
Malware analysis and Digital Forensics
Security assessment services
Pentest and red teaming
KASPERSKY ENDPOINT DETECTION AND RESPONSE
KASPERSKY ANTI TARGETED ATTACK
KASPERSKY RESEARCH SANDBOX
KASPERSKY THREAT ATTRIBUTION ENGINE
KASPERSKY FOR SECURITY OPERATIONS CENTERS
CLASSIC SOC
Log collection & correlation
Monitoring and alerting
Case management
Incident reporting
CORE

Source: Kaspersky

At the core of this offering sits a single technology platform comprising three key components:

- Kaspersky Anti Targeted Attack (KATA) platform
- Kaspersky Endpoint Detection and Response (KEDR) Expert offering
- Kaspersky Managed Detection and Response (MDR) Expert offering

Expert solutions are extended versions of the offering for the mainstream market, delivered within Kaspersky's Optimum framework. Kaspersky's Optimum framework includes Kaspersky EDR for anomalous detection across endpoints, Kaspersky Sandbox to convict individual files, and Kaspersky Threat Intelligence Portal.[2]

[2] This framework is discussed in more detail here: http://media.kaspersky.com/en/business-security/enterprise/endpoint-detection-and-response-optimum-whitepaper.pdf

The list of the Expert framework components for SOCs includes:

- Kaspersky TI and CyberTrace fusion tool
- Kaspersky cybersecurity training programs
- Enterprise-wide and industry-specific security assessment services
- Incident investigation and response services
- Professional services (e.g., SOC consulting and technical support)

Kaspersky Base Functionality for Mature SOCs

As discussed above, Kaspersky's security offering for mature clients includes additional features. The KEDR Expert offering shifts the focus to investigation automation for increased SOC efficiency. Alongside the full capabilities of the Optimum offering, SOC teams receive unique indicators of attack (IoAs) with MITRE ATT&CK mapping, a customizable research sandbox for on-demand deep analysis of suspicious samples in isolated simulation, and access to threat intelligence for investigations.

MDR, under the Kaspersky Expert framework, runs 24x7 monitoring, incident validation, and automated and managed threat hunting, with extended raw data storage terms for retrospective threat hunting. This service enables the outsourcing of tier-one functionalities and adds a direct communication channel to Kaspersky's SOC experts for assurance and validation. All raw and TI data is available for forensicating and internal investigations. The goal here is to lift the burden of time-consuming processes and ensure the true transience of externalized operations.

Mean time to resolution (MTTR) — which is the time from the automatic generation of an alert (from the automated analysis of events) to its resolution by Kaspersky experts — is 25 minutes on average.[3] Frankly, this metric for the industry varies from hour to days, or even weeks, especially when we consider breach remediation. Reaction time counted in minutes is essential in a modern and fast-moving SOC environment.

The most important component of functionality from Kaspersky for mature SOCs is the KATA platform, which centralizes operations in one web-based console for network traffic analysis, endpoint activity monitoring, and unified visibility and control. The platform automates collection, normalization, correlation, storage, and investigation across metadata from networks, email, the web, and endpoint telemetry. Semi-automated functionality includes root cause analysis (RCA), forensics, YARA detection, indicator of compromise (IoC)-based discovery, IoA mapping, querying for threat hunting, and integration with Kaspersky's TI portal.

Discovery and investigation results on the KATA platform are set to trigger and execute a gateway-level auto-response based on customizable policies and thresholds. The KEDR and KATA products both have a Syslog API and support all SIEMs and security orchestration, automation, and response (SOAR) stacks that can work with Syslog CEF. This capability can tremendously decrease the level of "noise" and help to focus efforts on significant security events. With pre-filtered

[3] http://securelist.com/managed-detection-and-response-analytics-report/94076/

alerts, compute and storage in SIEM substantially decrease, subsequently reducing per-use fees and the overall cost of ownership.

In a nutshell, three components of the SOC Expert core offering can provide advanced and customizable tooling for the detection and prevention of both known and novel 0-day and advanced threats. The managed component eliminates the need for personnel to monitor, triage, and investigate ad-hoc incidents. On-demand components can support the most sophisticated cases with in-depth services and capabilities. All components are linked with the TI platform, providing context for actions and investigations.

In a nutshell, three core components of the SOC Expert offering can provide advanced and customizable tooling for detection and prevention of known and novel 0-day and advanced threats. All components are linked with the TI platform, providing context for actions and investigations.

Value-Add Components for SOC Programs

KATA, KEDR, and MDR are designed for the automation and orchestration of advanced investigations and response processes. Still, gaps remain in SOCs that currently cannot be fully covered by technology alone. For this reason, the Expert framework from Kaspersky includes a set of services and supporting tools to help identify and mitigate flaws in security setups.

SOC transformation is a complex process that requires a clear roadmap and continual verification of its execution. Security assessments, despite their snapshot nature, reveal major issues and inconsistencies within the security program and technology stack. The findings of penetration tests, red teaming, and software security assessments are key constituents of a changing blueprint and can help to assess progress as well as benchmark against peers.

Expert guidance, technical support, and consultancy services can help to build an SOC program that customizes best practices to align with organizational business objectives. Effective planning reduces costs and helps to make risk-based architecture decisions, as well as to demonstrate the security ROI to enterprise stakeholders.

As mentioned already, personnel are the most critical asset and the main issue for an SOC of any size. Training and upskilling analysts should be prioritized in a modern security operations strategy. Kaspersky has thus included education and training in the Expert framework for SOCs, listing courses for different levels of personnel, from security awareness basics for lines of business to incident response, malware analysis, and threat hunting for tier-three analysts.

With an evolution roadmap derived from realistic and critical assessments of the organization's posture — one that incorporates industry best practices for security operations augmented by trained personnel and backed up with technical support — we can embark on a journey to a modern SOC.

Fueling the SOC with Threat Intelligence

As much as a modern SOC relies on technology and processes, it also leans on contextualized insights for timely and informed decisions. Standalone components of the Expert framework can deliver value as purpose-built solutions, but we need a common information plane to connect them beyond technology integration.

The last major component of the value-add proposition from Kaspersky is its TI platform. Threat data feeds are layered over the enterprise threat profile to help triage and highlight the most relevant and impactful IoCs. The list of Kaspersky feeds includes, but is not limited to: URLs segmented by threat type (ransom, phishing, etc.) and targeted-environment type (IoT, mobile, etc.), IP reputations, APT IoCs, passive DNS resolutions, FQDNs, vulnerabilities and CVEs, C&C botnets, and MD5 hashes. TI also includes methods, techniques, and tactics from ATP research to keep defenders up to date with the threat landscape.

In the SOC Expert offering, KEDR and KATA support the import of IoCs for machine scanning. These solutions natively integrate with Kaspersky Security Network (cloud knowledge base), which sources TI from third-party vendors, partners, and open-source intelligence. Kaspersky's TI portal enables the looking up and matching of objects against feeds, with the subsequent alerting of incident-response teams. Finally, the CyberTrace TI fusion and analysis tool helps to merge feeds from all sources (in JSON, STIX, XML, and CSV formats, including custom internal feeds) and push them into SIEM or run correlations across logs.

Having TI is less important than being able to use and apply it. In its early days, security teams piled up intelligence, but, without process integration, it was doomed to become shelfware. Actionable and company-/industry-specific intelligence must become an integral part of operations and feed into investigations.

Challenges & Outlook

Kaspersky's Expert framework and toolset for SOCs is a highly detailed and specialized offering designed to cover gaps in security operations from people, process, and technology perspectives. The chosen approach uniquely bonds together service and technology to enhance the capabilities of SOC analysts, retain and increase knowledge, retain and train talent, and enrich security functionality. Nonetheless, as is the case with any solution, this offering has its limitations.

The sophistication of components requires SOC leads to have an advanced skills set at their disposal. The Expert framework from Kaspersky targets very mature environments and teams in which many components are already in place and that operate under a detailed governance framework. The standalone components of the Expert offering can fit a mature environment with minimal adjustment, yet a full framework may require the restructuring of processes and integration with existing tools, especially custom ones. A detailed assessment of requirements at the proof-of-concept stage is advisable. Assessment services can support this analysis to a degree, leaving the decisions to SOC leads and the CISO.

The cost associated with entire-stack implementation can be prohibitive for some organizations, especially when Kaspersky solutions will be replacing products under terminal licenses. ROI evaluations in such projects should be among the first steps. Alternatively, components can be acquired separately, but the cost of integrating these with in-house inventory must be verified.

The core technology stack of Kaspersky's Expert framework is fit to combat threats across the estate. The functionality and effectiveness of KEDR and KATA are rated highly by industry experts and practitioners, but some limitations apply here, as well. KATA's traffic throughput is limited by the machine setup; it requires the well-thought-out design and architecture of data-flow processing to sustain performance. KEDR is lightweight and can run alongside non-Kaspersky endpoint protection tools. But, to deploy it, the organization will need a dedicated KEDR server and Kaspersky Security Console (KSC) server to manage installation, update, removal, and agent-related scenarios. In some implementations, the automatic forwarding of suspicious objects from KEDR to a sandbox is not possible; it requires validation.

From the architecture perspective, both KEDR and KATA can run on physical machines or virtual servers, and some limited functionality can be deployed in the public cloud of choice. Currently, the biggest limitation for the KEDR component is the OS on which agents can be deployed. Currently, that only includes Windows-based devices, but the product development roadmap includes plans for Linux and macOS support in 2021.

KATA's advanced web and email analysis features reportedly work best with the Kaspersky stack. Deployments in heterogenous environments will require full-stack integration to map the metadata for analysis.

Kaspersky's threat intelligence suite, like KATA, has a dedicated server as a prerequisite. Log correlation may require forwarding from SIEM and back, generating additional network footprint. A new release of CyberTrace is planned for 2021, which may partially solve related issues.

On a higher level, Kaspersky's Expert offering requires a deep understanding of technology; it is not a simple one-size-fits-all solution. Out-of-the-box capabilities that can be customized and integrated flexibly can be invaluable for a modern SOC, but maximizing the value of Kaspersky's suite without Kaspersky's Expert services would not be a trivial task. The complexity and the number of components require a clear vision and professional support from the vendor. Ideally, this offering should come with reference architecture and a use-case portal to simplify its operationalization.

Finally, Kaspersky's Expert framework and toolkit for SOCs is a unique offering that continuously evolves with the addition of new features and integrations. Its sole purpose is to help mature SOCs maximize the efficiency of security operations and the level of protection provided to the enterprise. As it evolves with MDR and people-centric services, such a framework can become a cornerstone of transformation from a traditional to a modern SOC.

Kaspersky's Expert framework and toolkit for SOCs is a unique offering with the sole purpose of helping mature SOCs maximize the efficiency of security operations and the level of protection provided to the enterprise. As it evolves, such a framework can become a cornerstone of the modern SOC.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC UK

5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com

Copyright and Restrictions:

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com.