kyndryl

Kyndryl Security Operations Center

Index

Executive summary

Since our company's establishment, Kyndryl has entered the IT services market in the security and resiliency space, which today has an organization of 7500+cyber resilience professionals and 500+ patents. With our reference blueprint and operating model, Kyndryl Security and Resiliency excels in the competitive market with a broad level of certifications, established relationships with technology leaders, and an ecosystem of cloud providers, including AWS, Azure, Google Cloud Platform, and Oracle Cloud Infrastructure.

Kyndryl's strategic directive sees the role of security and resiliency as crucial to the modernization of legacy systems and services and successful IT transformations to the cloud. Among our centralized services is the Kyndryl Security Operations Center (SOC). This evolved, around-the-clock service offers threat intelligence and integrated automation systems. The portfolio of centralized services extends with additional opportunities for zero trust, incident response, and consulting services.

Today, many IT organizations have established or delegated a security monitoring facility through a security operations center with the primary goals of intercepting and responding to cyberattacks and mitigating security risks. Industry sectors are driven by increasingly strict regulations to prevent, monitor, and remediate possible cyberattacks. Companies are also subject to audits by cyber auditors from internal and external industry functions and must run periodic health checks through Red Team services.

In opposition to the security operations center, the Red Team consists of ethical hacking security experts who simulate external threat attacks to identify vulnerabilities and weak points in corporate security. These experts perform preventative activities like penetration testing, phishing, social engineering, and infrastructure and application attacks to help organizations improve their defenses and prevent actual attacks. Their job is to provide an independent, objective assessment of the security capabilities of the enterprise.

Kyndryl focuses at the ongoing challenges of CISOs, CIOs, and cybersecurity leaders in mitigating increased cyber risks, improving operational efficiency, complying with new security regulations, integrating with new technologies, handling increased workloads, responding to changing business needs, and managing increased attack surface and emerging threats, including the rise of digital services and the adoption of the cloud.

Companies are careful in assessing the actual performance and operating costs of their cyber operations center service, and are constantly preparing to evaluate alternatives when one or more factors are highlighted in service delivery:

1. Poor performance or ineffectiveness in service outcomes
2. High operating costs that do not match expectations
3. Inadequate technical and cyber engineering support
4. Lack of knowledge required for integration with other cybersecurity solutions
5. Use of technological infrastructures that are obsolete or difficult to integrate into the security ecosystem
6. Difficulty with the operational industrialization of the service
7. Insufficiency or lack of response to emerging capabilities

To face these scenarios, organizations must approach security defense in an extended mode, focusing not only on IT infrastructure but also on employees and business processes. It's vital to build a competent and collaborative team that is constantly updated and efficient in operations, equipped with state-of-the-art technological tools and timely, methodological service governance.

To accomplish all these goals on your own can be challenging and expensive, as it would impact the organization and require significant economic investments. In fact, companies today increasingly need to focus their workforce on the evolution of the core business rather than security management. Furthermore, the need to equip evolved software platforms to deliver operational activities and train and hire employees with up-to-date skills on evolving cyber threats has a significant impact on costs and, as a result, is often unsustainable for IT budgets.

In this regard, it is necessary to rely on the collaboration of experienced, credible, and industry-specific partners, known as Managed Security Service Providers (MSSPs), who can deliver evolved cybersecurity protection services and have the necessary experience and assets to help customers protect their organizations against security incidents and support overall infrastructure and data resilience.

Kyndryl Security and Resiliency offers skills, services, and technologies to help your company anticipate, protect, withstand, and recover from adverse conditions, stress, and compromised services due to cyberattacks. We provide coverage that is not only proactive (identify and protect) and reactive (detect and respond) but also adaptive to support rapid recovery following a security incident.

Introduction

Today, many companies and public administrations are involved in the ongoing digital transformation. To maximize benefits and quickly seize opportunities offered by the new market scenario, it's essential to address an insidious danger: the various kinds of sophisticated, diverse, and frequent digital threats to business and critical public and private services. No industry can be considered safe from this threat, with significant risk to a company's most vital assets: people, revenue, personal and operational data, and brand reputation.

Dealing with the complexity of this danger requires a holistic approach to identifying the attack surfaces and the adoption of timely solutions that address all potential exposures—including employees—and compliance with relevant laws and regulations to prevent the situation from escalating with serious damage to the company.

When we analyze the causes of the rising threats, we can identify three main elements introduced by the digital transformation process:

1. **The evolution of IT infrastructures.** Technical environments are increasingly complex and embrace hybrid models (on-premises and cloud) to allow the integration of applications and data to support flexibility and scalability, making enterprises accessible from multiple sources at any time of day. The increasing use of infrastructure delivered by leading hyperscalers is driving organizations to reconsider cybersecurity practices and take full advantage of the technological opportunities offered by these hyperscalers to address their cloud security posture, the security of cloud workloads, and cloud-native applications.
2. **The new organizational models in companies.** Organizations are increasingly adopting these models to support the digital transformation of their workforce better, helping them become more fluid and agile to facilitate operations on the move (for example, smart working). The recent pandemic further accelerated this adoption.
3. **The development of cyber-crime business as a parallel business element.** The cyber-crime industry is made up of industrially well-structured organizations that can identify new vulnerabilities and prepare new attack techniques.

These elements have increased the type and number of accesses to a company's various services, as well as the risk of cybersecurity attacks by hackers. Let's consider the growing number of devices connected to the Internet today (smartphones, laptops, IoT devices, and more) and new malicious software (ransomware, cryptolockers, viruses, worms, and trojans). It is clear that the threats to IT security will continue to increase in number and sophistication, requiring immediate response to neutralize them before they become a serious danger to the business. The risk is equally complex to address because it constantly changes and evolves, making it difficult to predict.

Another critical aspect to consider is compliance with government regulations regarding the protection and integrity of data and infrastructures. Regulatory rules already require companies to take all possible precautions to protect sensitive information from cyberattacks. Still, as cyber threats grow, the regulatory scenario will also evolve and increasingly require the adoption of adequate countermeasures in terms of services and control and governance processes. For example, the upcoming European directives regarding cybersecurity (like the implementation of NIS2) will require companies and public administrations to enhance their reaction and response capacity through a new set of minimum cybersecurity standards that must be assimilated into the regulations of individual countries.

This evolving situation now requires IT security transformation processes and the continuous adoption of tailored IT security technologies and services to keep companies constantly aligned with the evolution of businesses and target markets, with proportionate economic investments.

The accelerated push towards digitization has introduced new priorities for CISOs and CTOs, such as cyber resilience, regulation, compliance, and labor market skills shortages. Organizations must be prepared in terms of operational resilience to ensure they can deliver critical business services during an outage.

Security operations centers are operational structures that work 24 hours a day and provide resources, skills, and experience in monitoring, identifying, and managing security incidents. Through the use of industry-leading technologies, monitoring open-source intelligence (OSINT) and closed-source intelligence (CLOSINT) threat intelligence feeds, and labs designed to test new attack techniques and replay incidents for root cause analysis, these centers can efficiently and effectively govern the security management of mission-critical infrastructure and services. It's also vital for organizations to participate and share data with Information Sharing and Analysis Centers (ISACs), such as the European Union Agency for Cybersecurity (ENISA) and the Center for Internet Security (CIS).

The expected benefits

In defining the value and benefits of the Kyndryl Security Operations Center, it's essential to pay particular attention to governing the cyber risk of the entire internal and external perimeter of the company, meeting security compliances with corporate and industry standards and regulations, identifying and quickly responding to possible threats, highlighting cybersecurity exposures, protecting sensitive data, developing plans to prevent future attacks, and having extreme effectiveness in managing security operations center activities.

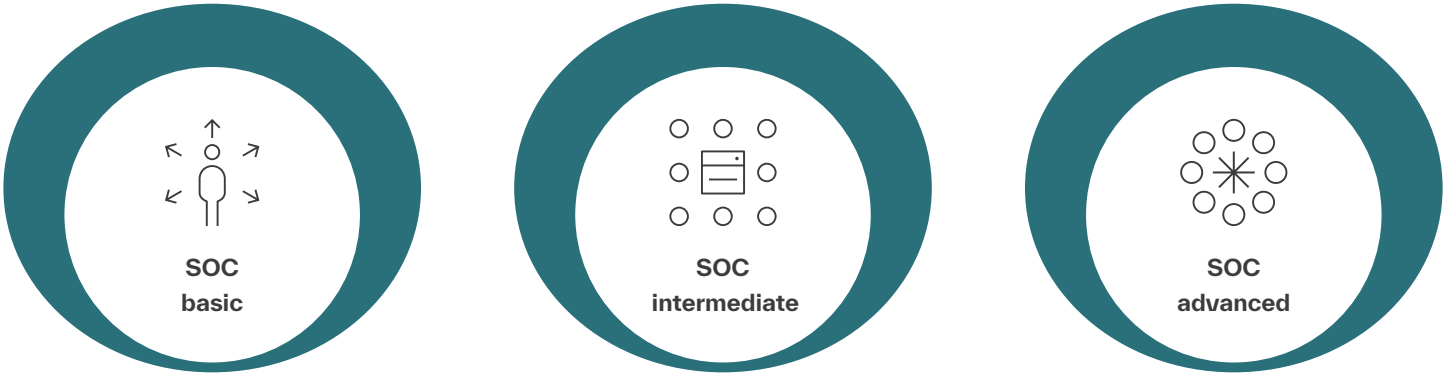
The performance and effectiveness of a security operations center are measured according to three guidelines:

1. **Organizations must have appropriate technology** to collect, monitor, and correlate security events around the entire IT perimeter, commonly known as security information and event management (SIEM). The latest-generation SIEMs use artificial intelligence (AI) and machine learning (ML) modules to anticipate malicious intentions as early as the interception of seemingly weak signals. Evolved facilities make complementary technologies for orchestration and the automation of potential incidents available through security orchestration and automation response (SOAR) platforms. Recent and progressively adopted technologies include extended detection and response (XDR) platforms that can collect and compare telemetry across the entire IT environment and exchange data between endpoints, e-mail, networks, servers, identity parameters, access, and cloud environments. XDR platforms are designed to detect, correlate, contextualize, and prioritize data and alerts collected through AI, ML, and behavioral analysis to provide an effective cyber response.
2. **High-level cyber engineering** is critical to analyze impact and consider the evolution of compromise indicators, which attackers can easily change. Cyber engineering drives the adoption of detection techniques based on tactics, techniques, and procedures to empower a company's defense. It also provides continuous integration of internal and external data sources to increase threat awareness and the ability to respond. Cyber engineering can also respond to changing rules and correlations to account for adjustments in business applications, integration of new technologies, and cloud adoption, as well as maintain and develop playbooks for managing cyber threats.
3. **Establish an excellent working machine** to support 24×7 service that includes Level 1 (L1) operational functions for analysis and monitoring (incident triage), Level 2 (L2) functions for analyzing incidents processed by L1 and identifying remedial actions (incident containment), and Level 3 (L3) functions for responding in the wake of an attack (incident response), with deep and specialized analysis capabilities in security monitoring (malware analysis, packet capture analysis, and deep complex threat hunting for advanced threats). In terms of organization, processes, and reporting, the effectiveness of operations is orchestrated and automated by SOAR platforms. These advanced centers are designed to take over conventionally coordinated functions and activities and are supervised by other cybersecurity bodies like the Computer Security Incident Response Team (CSIRT) or the Computer Emergency Response Team (CERT).

Kyndryl's vision of the market

The Kyndryl Security Operations Center observes different levels of adoption in the market with varying degrees of maturity, relative operational performance, and functional complexity to provide a three-dimensional view of the service. By convention and simplification, we've identified three degrees of adoption (basic, intermediate, and advanced) that can address temporary or current needs and are evolving to meet a continuing need to mitigate security risk.

1. **Basic SOCs** predominantly use a SIEM platform that integrates events and security logs from primary IT sources, such as servers, network security, intrusion prevention systems (IPS) and intrusion detection systems (IDS), identity systems, databases, applications, antivirus software, and more. These operations are typically L1 and L2, with daily and escalation monitoring for times outside business hours and holidays. Incident response forensic activity tends to occur on demand when necessary.
2. **Intermediate SOCs** predominantly use a SIEM platform that, in addition to the base model, integrates threat intelligence, works with behavioral analysis systems, and enhances the overall cyber view with endpoint detection and response (EDR) and network detection and response (NDR) sources. L1 and L2 operations have 24×7 characteristics with the adoption of a threat-hunting framework. Incident response forensics activity is generally provided by entities outside the SOC.
3. **Advanced SOCs** predominantly use an evolved SIEM platform with AI and ML capabilities that, in addition to the intermediate model, integrate orchestration and operational automation through SOAR platforms with further XDR enrichment for high-performance response and recovery. Operations are elevated with L1, L2, and L3 services with 24×7 features and more mature threat-hunting framework. The advanced service also offers a possible diversification of priorities based on the application, business line, or legal entity context for mitigating the impact of an incident. In addition to threat intelligence integration, early warning proactive analysis tasks and simulated attack campaign executions (simulation attacks) are also performed. Incident response forensics activity is also offered in the advanced service.



SOC basic		SOC intermediate		SOC advanced	
Adopted technology	**Operations**	**Adopted technology**	**Operation**	**Technology**	**Operation**
SIEM	L1 and L2 basic support during prime time, 24x7 availability for escalation	SIEM, User and entity behavior analytics (UEBA), EDR	L1 and L2 24x7 support, L3 with basic threat-hunting capabilities	SIEM, Comprehensive SOAR, XDR	L1 and L2 24x7 support L3 advanced threat-hunting capabilities, advanced threat intelligence, Red Teaming exercise

SOC complexity management indicators apply to these three adoption models, with a derived differentiation of the overall weight.

Key performance indicators (KPIs) of security operations center complexity include:

KPIs

Incident analysis rules and correlations

Playbooks
False positives
Detected incidents

Infrastructure perimeter cyber use cases

Variety of data sources
Variety of managed environments (Legacy, distributed, cloud)

Security operations (SecOps)

Operational relationship between L1, L2, and L3 support

Service-level agreement (SLA) and reporting

Stipulation of SLAs in the contract
Degree of reporting

Kyndryl's Security Operations Centers uses the advanced mode, combining advanced technologies, high-profile cyber engineering, and 24×7 operational capacity to respond to the current and future challenges of integrating cloud environments and digital transformation.

The Kyndryl approach

Kyndryl Security and Resiliency is entirely dedicated to cyber resilience solutions that can provide support and protection across the entire threat lifecycle: risk identification, AI-driven threat intelligence, vulnerability management, incident detection, identifying appropriate response and mitigation strategies, and data protection and recovery in emergency conditions. We continue to invest in training professional resources for cyber engineering and day-to-day operations.

Our broad portfolio of services aims not only to anticipate, protect, withstand, and respond to cyberattacks that can impact and compromise the delivery of IT services, but also to safeguard your business by supporting the recovery of conditions before the attack.

Kyndryl is proud to be an MSSP of choice for companies and public administrators around the world.

Global experience

Kyndryl Security Operations Center benefits from our global experiences in managing cyberattacks and implementing incident management best practices.

Extended portfolio of services

Our extensive security services are designed to help companies anticipate, protect, withstand, and recover quickly from cyber incidents.

- Security Assurance Services
- Zero Trust Services
- Security Operations and Response Services
- Incident Recovery Services

Automation

Our service portfolio uses SOAR technology to increase the productivity and efficiency of security analysts in incident management.

Integration between security and resiliency

Combining security and resiliency capabilities helps address end-to-end cyber threats.

- Preventive (identify and protect)
- Reactive (detect and respond)
- Adaptive (recover)

1. **Global presence and experience:** Kyndryl has a global presence with its professionals focused on security and resiliency services and managing thousands of customers across various industries (automotive, banking and insurance, manufacturing, public administration, retail, large-scale retail trade, healthcare, and transport). This presence allows us to take advantage of daily practical experience gained from managing cyberattacks, developing and implementing best practices to manage incident monitoring and classification activities and prepare attack response and mitigation strategies, collecting feeds and context information related to threats and potential attacks through the analysis of threat intelligence OSINT and CLOSINT sources, and developing automation solutions (playbooks) with appropriate orchestration and automation technologies.
2. **Extended portfolio of services:** Our Security Operations Center is designed to be a cyber defense center with an extensive portfolio of services that cover all five phases of the National Institute of Standards and Technology (NIST) reference security framework: identify, protect, detect, respond, and recover.

   - **Security Assurance Services:** Our assessment services are designed to evaluate the maturity and completeness of adopted solutions, compare a service's maturity level against models and best practices, and provide support for compliance management—security, strategy and risk management, offensive security testing, and compliance management.
   - **Zero Trust Services:** Kyndryl adopts the zero-trust methodology based on its fundamental principles: "never trust, always verify" and "always apply least privilege." These services continuously evaluate parameters that are functional to the security posture—identity and access management, endpoint security, network security, application and workload security, and data protection and privacy services (MDR, XDR, NDR, microsegmentation, identity management, privileged access management, zero-trust network access).
   - **Security Operations and Response Services:** This portfolio includes all our security incident monitoring and management services and threat response services—event monitoring, incident detection and investigation, incident triage, incident management, and threat intelligence.
   - **Incident Recovery Services:** Drawing upon our experience managing complex and critical IT infrastructures, Kyndryl has developed a set of skills and effective methodologies to mitigate the impact of an incident and help restore critical business data, applications, and infrastructure as soon as possible—cyber incident recovery, managed backup services, hybrid platform recovery services, and data center services. These services support the resilience of our customers' physical and logical infrastructures.
3. **Automation and orchestration:** The analysis and mitigation of processes is a key step to support proactive security management. Automation and orchestration make the analysis and classification of incident-related tasks more efficient for operations personnel and provide automatic responses to actions that compromise company infrastructures. We've developed our own operations structure by placing a powerful, flexible orchestration and automation platform at the core of our architecture, programmed using playbooks developed with in-house expertise.
4. **Integration between security and resiliency:** Combining cybersecurity and resiliency positions Kyndryl distinctively from current leading MSSPs, with capabilities to address cyber threats not only in a preventive and reactive way, but also from an adaptive perspective to recover quickly following a security incident. Kyndryl Cyber Incident Recovery (CIR) services support rapid response to ransomware and other cyberattacks that cause damage to data and systems, helping restart vital systems operations in the wake of an attack.

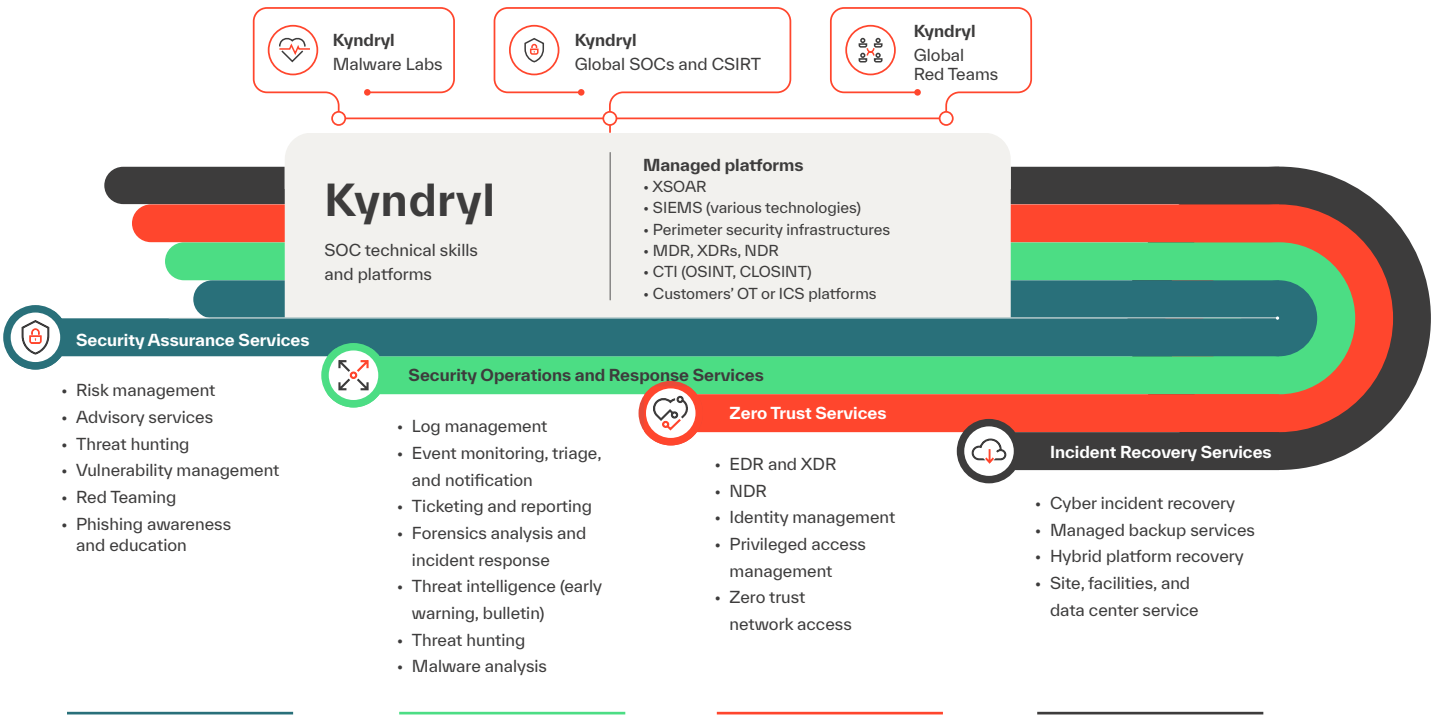
Through our global agreements with leading alliances (AWS, Google Cloud, Microsoft Azure, Oracle, and VMware), infrastructure solution providers, and a broad ecosystem of security and data protection technology vendors, we advise and support our customers in their end-to-end transition journeys to elevate cybersecurity control and management with state-of-the-art technologies.

The Kyndryl Security Operations Center is designed to provide a center of excellence for cybersecurity management with specialized skills, certifications, and experience in cybersecurity platform management and technologies to support security events, operational management, and monitoring. (SIEM, SOAR, MDR, XDR, NDR, perimeter security, OSINT and CLOSINT threat intelligence sources, and more).

Our Security Operations Center draws upon deep experience in security incident management across a wide range of medium- and large-scale customers (measured in terms of the number of infrastructure elements managed and revenue on a global scale) operating in all industries, supported by a Kyndryl computer security incident response team (CSIRT) that—in addition to providing evidence on key threats and guidelines to follow—can also provide operational guidance on incident response activities. This guidance helps support governance over security incident management in accordance with Kyndryl policies and best practices. Furthermore, our center uses a global Red Team distributed across several countries, with specific skills and methodologies in conducting simulated attacks on customer infrastructures to verify robustness and identify potential vulnerability points.

Security research is another important asset of the Security Operations Center, supporting the continuous development of skills and experience. This research nurtures not only the practical knowledge of professionals working in design, delivery, and operations, but also the ability to quickly interpret critical phenomena and develop technological assets to make the response faster and more effective.

Kyndryl Security Operations Center Services



kyndryl