



## Kyndryl Security Operations as a platform

Kyndryl's Security Operations as a platform is a dedicated and secure infrastructure hosted on the cloud and built on best-of-breed technology that customers can use for Security Operations. Expertise and support services to help customers build, deploy, manage, and secure enterprise systems.

### Introduction

Design and build the security architectural building blocks and connectors so that customers can improve their security posture and focus on managing their Security Operations. Kyndryl removes the burden of managing your platform, which includes various security technologies. Our Cyber Resilience experts manage the infrastructure and monitor the environment for any security events, allowing you to concentrate on the things that matter most – the security of your environment. Kyndryl Security Operations as a platform covers - SIEM, EDR, SOAR, and Vulnerability Management.

### Kyndryl's Point of View

In Kyndryl, we believe that security is about defense in depth. Hence, we need an integrated platform with security technology to cover core security controls. But it is not enough to manage the breadth and complexity of security operations or solution integration. The client needs something beyond the standard operation methodology. And that is well-defined, high-quality content to streamline their security operations. SOaap offers -

- An easily deployable, easily integrable platform with the promise of keeping your IP even if you decide to move away.
- Kyndryl integrates state-of-the-art technology products into a consumable Service and helps bring your security operations to a different level, regardless of your environment's complexity.
- Kyndryl power this with pre-configured, state-of-the-art rules, threat scenarios, playbooks, integrations, dashboards, and reports, continuously updated and refined for you.

### Highlights

#### Kyndryl Security Operations as a platform:

- Kyndryl SOaap platform includes SIEM, EDR, SOAR, and Vulnerability Management
- Freedom to select other vendor products to integrate with the SOaap platform and services.
- Retain the platform and content even if you decide to move away
- Service Capability Module as per the client's requirement

#### SOaap Delivery Services:

- Integrated threat detection and response with the combined capabilities of SIEM, SOAR, Vulnerability Management, EDR
- Centralized security management with a unified view of your organization's security posture
- Scalable and flexible security response
- Cloud-native-enabled deployment

# Kyndryl Security Operations as a platform

## Service Overview

Ongoing content updates (rules, threat scenarios, playbooks, integrations). A platform that will provide the retention of your content and gives flexibility to quickly lift and shift MSSPs using a fully built SOC platform ready for monitoring. Allow for different SOC models. It is a highly integrable platform. Move from bare metal hypervisor-based systems to more scalable, elastic platforms for operations (pay-as-you-go). Provide the ability for clients to Co-Create SOaap (add capability modules, rules, playbooks). SOaap enables clients to continue to focus on cybersecurity and not the overhead of managing operational and administrative tasks associated with SOC infrastructure and tools.

### Kyndryl Security Operations as a platform:

Pre-configured rules and threat scenarios - Malware Detection, Cloud Security Analytics, Endpoint Detection, Machine Learning Models, Threat Intelligence, User and Entity Behavior Analytics (UEBA)

Ready for customization Standard Operating Procedures, aligned with platform integrations, consistent and effective incident handling in your SOC.

Workflow integration and consistent workflows make it easier to add emerging technologies or swap out point products.

Modular design and flexibility to select modules.

Decide the Delivery Model, pair SOaap with your SOC, existing MSSP, or complement with Kyndryl SOC service.

## Kyndryl's Competitive Differentiators

- Simplify cloud complexity through end-to-end design, deployment, and integration of services, ensuring compliance visibility.
- Engage with deep industry expertise and thousands of person-years of.
- Modernize automation, operations, management, and governance.

## Target Audience

### Typical Sponsor

- CISO, CIO, CTO, COO, SOC executives and directors, etc.
- Companies of any size on a Zero or Cyber journey.
- Companies with a mobile workforce.

### Geographies

- Worldwide

### Target Industry

- All industries (especially those that are regulated and/or have experienced major security issues)

## For more information

To learn more about Kyndryl Security Operation Services please contact your Kyndryl representative or Kyndryl business partner or visit: [www.kyndryl.com](http://www.kyndryl.com).

## Why Kyndryl?

At Kyndryl, we understand the pros and cons of various cyber resilience strategy options and can help you navigate and select a strategy that is most capable of meeting your requirements and assumptions.

## Experience

Execute faster by leveraging the extensive skills and resources across Kyndryl and our broad partner ecosystem.

## Technology

More securely integrate emerging technologies across hybrid environments, benefiting from our decades of experience and patterns of success.

## Support

Manage the rapidly evolving operational risks, effectively protect business-critical infrastructure, and mitigate the business impact of security and resiliency incidents.



© Copyright Kyndryl, Inc. 2023.

*Kyndryl is a trademark or registered trademark of Kyndryl, Inc. in the United States and/or other countries. Other product and service names may be trademarks of Kyndryl, Inc. or other companies. This document is current as of the initial date of publication and may be changed by Kyndryl at any time without notice. Not all offerings are available in every country in which Kyndryl operates. Kyndryl products and services are warranted according to the terms and conditions of the agreements under which they are provided.*