kyndryl

Security Operations as a Platform

Case Studies

July 2023

Endpoint Detection and Response

Protect endpoints by detecting malware with your tool of choice. Configure and manage it according to industry best practice and support by of Kyndryl's resources

Services

Kyndryl Endpoint Detection and Response (EDR) Advisory

- True end-to-end clarity into security management and performance of your endpoints
- Clear visibility into risks and threats with real-time analysis and detection
- Improve cyber resilience and reduce data breach risks

Kyndryl Endpoint Detection and Response (EDR) Managed Services

- Defining use cases and playbooks
- Integration and baseline tuning of EDR tools
- Continuous monitoring and support
- Dashboard for EDR and external attack surfaces
- Proactive identification of adversary activity based on various data sources and threat intelligence

Service Capabilities

EDR and EPP Managed Services (8x5)

- Console health management and upgrade coordination.
- Policy configuration and continuous tuning in accordance with best practice policy and alert recommendations.
- Quarterly audit and reconciliation reporting.
- Continuous EDR secure configuration, users, and privileges management.
- Threat Detection and Standard Reports with Daily Notification of Infections
- 8x5 Alerts: monitoring, triage, investigation, notification, or endpoint response with remediation direction.

24x7 MDR (Managed Detection and Response Services)

- Everything included in the 8x5 EDR Managed Services plus 24x7 eyes-on monitoring, investigation, notification, or endpoint response with remediation direction.

Case Study

Customer

Financial Institution

Situation

Customer desired to increase its security for Endpoint devices against Malware detection and Policy management for Windows and Linux virtual machines and provide Antivirus support to the workstations (desktops, laptops, Virtual machines, and servers).

Approach

Blended approach with proactive monitoring and maintenance of protection software, daily system health checks, monitoring endpoint devices, analyzing malware incidents with actions to address, access to anti-malware definitions and updates (e.g., products).

Results

Increased endpoint detection capabilities supported with policy change request processes, agreed IT security control document, and 24x7 monitoring.

Security Information and Event Management

Continuously collect, aggregate, and analyze data to detect, protect, and respond to cyber events

Services

Kyndryl System Information and Even Management (SIEM) Advisory

- Assist customers in the selection of the tools and the planning of the implementation or migration
- Identify appropriate processes, design and configure data sources, define paybooks, use best practices, and arrange for required support integration
- Provide migration plan, timeline, training, and even ongoing management of the SIEM infrastructure

Kyndryl SIEM Managed Services

- Holistic management of customer security logs
- Flexibility to use vendor and solutions of choice and to meet business needs
- Experienced teams help to plan, implement, manage, and monitory SIEM system based on your business requirements
- Managed detection of threats and investigation attacks through event management, event correlation, incident monitoring, and response

Service Capabilities

SIEM Managed Services Capabilities

- Kyndryl Managed SIEM Services are designed to help clients manage use cases and adapt to continuously changing threat environments, streamlining the log sources for better event management and correlation.
- Managed service delivery uses well-defined processes and methodologies to cover client objectives.
- Kyndryl provides highly skilled resources and expertise supported by a broad ecosystem to have minimum impact on business.
- SIEM tool management briefly covers:
  - Create policies to monitor the console, log sources (collection, parsing, and continuity), and policies.
  - Create processes to monitor the overall health of the SIEM environment.
  - Continuous console and patch upgrades.
  - Continuous data flow review.
  - Configuring co-relation rules if required.
  - Event analytics services, fine-tuning.

Case Study

Customer

Government Organization

Situation

Customer sought improvement of security incident monitoring of its public administration including a threat impact analysis on its IT infrastructure and continuous reporting of security incidents, threats, and vulnerabilities.

Approach

Centralize security management with a unified view of client's security posture, automated deployments, and hybrid operational models. All of these are supported by continuously updated rules, scenarios, playbooks and integrations.

Results

Synergy between the on-premise and SOC teams. Services provided both on-prem and in cloud. Other results include 13 types of integrated log sources, 146 offenses analyzed and mitigated, and 212 million security events with 100% of tickets closed.

Managed Detection and Response Services

Kyndryl's security services can be stand alone or integrated onto the Security Operations as a platform as a full spectrum Managed Detection and Response capability

Services Overview

Kyndryl Managed Endpoint Detection and Response

– True end-to-end clarity into security management and performance of your endpoints

Kyndryl SIEM Managed Services

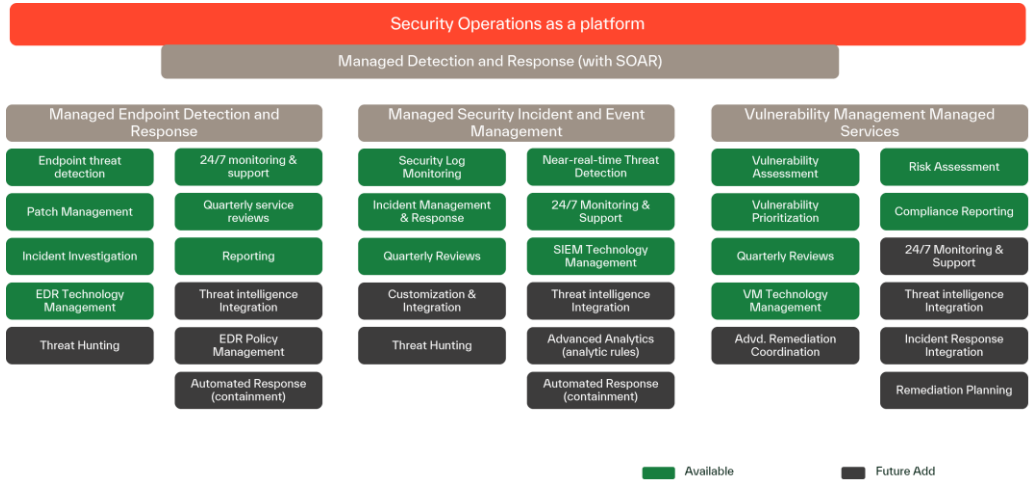
– Holistic management of customer security logs

Kyndryl Vulnerability Management Managed Services

– Modernize patch and vulnerability management to decrease response time to threats

Kyndryl Security Operations as a platform

– Kyndryl Security Operations as a platform allows organizations to consolidate security vendors while allowing the flexibility to scale their managed security capabilities. The platform consolidates EDR, SIEM, Automation and Response (SOAR), vulnerability management, and other features, to provide increased monitoring and response capabilities.



Win Story

Customer

Singapore Aero Engine Services Private Limited (SAESL)

Situation

SAESL, the world's largest Maintenance, Repair and Overhaul (MRO) facility for the Rolls-Royce Trent engines, appointed Kyndryl as it's new managed service partner to transform IT services.

Proposed Approach

Through this collaboration, Kyndryl will empower SAESL in modernizing its digital infrastructure, delivering automated service desk management across the multichannel, and integrating comprehensive security solutions to enhance organization-wide cybersecurity and resilience.

Press Release

Singapore Aero Engine Services Private Limited Appoints Kyndryl as Its New Managed Services Partner to Transform IT Services