kyndryl

Kyndryl Managed Extended Detection and Response with Microsoft Defender XDR

Cyber attacks have become more frequent and sophisticated crossing multiple security domains including human-operated ransomware campaigns, business email compromise campaigns, and data exfiltration attacks.

Determining the full scope and impact of these attacks is one the most critical, but often most challenging, parts of security operations. Defending against these modern attacks is exponentially harder for Security Operations Center (SOC) teams who do not have visibility across the full attack chain because they are working with multiple siloed tools.

To tackle the nature of modern attacks crossing multiple domains and close security gaps, security teams need a unified solution that allows them to detect and respond to threats more efficiently across an organization's entire digital estate.

Highlights

Architecture Details

- Kyndryl will migrate an organization's existing XDR solution to Microsoft Defender XDR.
- Microsoft Defender XDR protects organizations from attacks on devices, identities, and cloud-based applications.
  - Microsoft Defender for Endpoint
  - Microsoft Defender for Office 365
  - Microsoft Defender for Identity
  - Microsoft Defender for Cloud Apps

Introduction

Kyndryl Managed Extended Detection provides organizations with the holistic view and response capabilities they need to effectively anticipate, protect, withstand, and recover from cyber attacks.
We help customers move beyond solely endpoint protection to all assets – including everything from email, identities, SaaS applications, cloud infrastructure, and data.

We protect a customer's endpoints detecting malware, including ransomware variants, zero-days, non-malware, and file-less attacks by leveraging the customer's tool of choice and by configuring and managing it in accordance with industry best practices and the customer's business needs.

Kyndryl Managed Extended Detection and Response provides complete extended detection and response (XDR) design, planning, migration, and managed services including 24×7 incident and alert investigation, and response services.

Kyndryl Managed Extended Detection and Response

Service Overview

Kyndryl Managed Extended Detection and Response correlates native signals across multi-platform endpoints, hybrid identities, email and collaboration tools, SaaS applications, data insights, and cloud workloads to provide a complete view of the kill chain. This deep context allows SOC teams to investigate and respond at the incident level, making prioritization easy and remediation faster.

Capabilities and Benefits

- Complete XDR design, planning, migration, and managed services
- Risk-based delivery model with a Zero Trust lens
- Standard framework to onboard and manage endpoints agent and XDR console
- Policy design, continuous review and tuning in accordance with best practices and customer needs
- Console and agent health and status management
- Threat hunting via additional detection capabilities and techniques to identify adversary activity
- Enhanced threat detection and response by breaking down silos, improving visibility, and streamlining security operations
- Architecture design for migration that includes detection rules, playbooks, historical data, dashboarding, and other processes
- Architecture planning and support
- Continuous XDR secure configuration, users, and privileges management
- 24×7 incident and alert investigation, and response services
- More efficient prioritization of cybersecurity alerts and notifications
- Holistic security and signal correlation across identity, email, endpoint, SaaS application, data, and cloud
- Helps protect against advanced attacks such as ransomware, business email compromise (BEC), and adversary in the middle (AiTM)

Kyndryl's Competitive Differentiators

- Holistic, end-to-end approach to security risk and compliance consulting
- Extensive experience managing complex policy sets for dozens of customers globally
- Over 30 years of mission-critical service experience with extensive focus on assessment insights and remediation activities
- Security consulting expertise and technology mastery
- Proven expertise serving customers across various industries including complex, highly regulated industries

For more information

To learn more about Kyndryl Managed Extended Detection and Response please contact your Kyndryl Representative or visit www.kyndryl.com.

kyndryl