Kyndryl Security Information and Event Management Migration

Migrating your Security Information and Event Management solution is a strategic decision that requires careful planning, collaboration, and thorough testing. Whether you are moving from an existing Security Information and Event Management (SIEM) to a next-generation platform or transitioning to a cloud-native environment, a well-defined migration process is essential.

Highlights

Advisory for Security Information and Event Management (SIEM) tool selection, integration of log sources, use cases, identification and defining support structure.

SIEM Deployment Services

- Deployment plan
- SIEM software deployment

SIEM Migration Services

- Migration from customer's existing SIEM solution to selected provider
- Policy and response defined use case
- Migration support from on-premises to cloud solutions
- Current supported target SIEM technology: Microsoft Sentinel

Introduction

As organizations adapt to an increasingly decentralized digital landscape, migrating from legacy SIEM solutions becomes crucial. Microsoft Sentinel, a cloud native SIEM and Inbuilt Security Orchestration, Automation, and Response (SOAR) solution, offers several advantages over traditional SIEMs.

Legacy SIEMs may lack sufficient coverage for cloud assets like Azure Cloud infrastructure. Microsoft Sentinel ingests data from both on-premises and cloud environments, enabling comprehensive coverage.

Kyndryl's Point of View

The ROI of a SIEM is measured in the effectiveness and ease of management for the detection and prevention of security incidents. Kyndryl's approach to migration includes:

- Scalability: cloud-native architecture allows seamless scaling
- Intelligent analytics: detect threats, hunt for anomalies, and respond effectively
- Single solution: attack detection, threat visibility, and proactive response
- Azure integration: works seamlessly with Azure services
- Guided migration: join the Kyndryl and Microsoft Sentinel Migration and Modernization Program for expert assistance
- Delivery on time and within budget using well-defined processes and methodologies

Kyndryl Security Information and Event Management Migration

Service Overview

Kyndryl Security Information and Event Management (SIEM) Migration is designed to help customers select appropriate tools and plan for implementation or migration. Kyndryl helps customers to identify processes, design and configure data sources, and define playbooks and best practices.

Kyndryl's capabilities include defining and onboarding the customer's current SIEM environment, goals, log source baseline, data source priority points, and implementation timeline. We provide architecture design for migration that includes detection rules, playbooks, historical data, dashboards, and other processes.

Our experience and expertise are supported by a wide partner ecosystem which supports no or minimal impact to the customer's business during deployment and operation.

Kyndryl Security Information and Event Management Migration assists customers:

- Plan your migration: understand processes and phases
- Track migration: use workbooks to monitor progress
- Migrate detection rules and SOAR automation: transition your rules and automation
- Export historical data: preserve historical context
- Ingest historical data: choose an Azure platform and ingestion tool
- Convert dashboards to workbooks: adapt your visualizations
- Update SOC processes: align with Microsoft Sentinel capabilities

Competitive Differentiators

- Holistic, end-to-end approach to security risk and compliance consulting
- Extensive experience managing complex policy sets for dozens of customers globally
- Kyndryl leverages over 30 years of mission-critical service experience and has developed an extensive ability to focus on assessment insights and remediation activities
- Security consulting expertise and technology mastery
- Innovation and co-creation of risk and compliance solutions with industry leading partners
- Proven expertise to serve customers in complex, highly regulated industries
- Broad experience supporting customers from various industries

For more information

To learn more about Kyndryl Security Information and Event Management Migration please contact your Kyndryl Representative, Kyndryl Business Partner or visit www.kyndryl.com.

Why Kyndryl?

According to ISC2 there is a gap of 4 million individuals in the cybersecurity workforce worldwide.[1] At Kyndryl, we understand the pros and cons of various cyber resilience strategy options and can help you navigate and select a strategy that meets your requirements and assumptions.

Experience

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

Technology

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

Support

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

Source: [1] 2023 ISC2 Cybersecurity Workforce Study

kyndryl

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.