



Kyndryl Security Information and Event Management Advisory and Implementation

Security Information and Event Management (SIEM) is a software solution that aggregates and analyzes activity from many different resources across your entire IT infrastructure. SIEM collects security data from network devices, servers, domain controllers, and more.

Introduction

SIEM combines two functions: security information management and security event management. This combination provides real-time security monitoring, allowing teams to track and analyze events and maintain security data logs for auditing and compliance purposes.

SIEM offers a complete security solution to help organizations identify potential and real security vulnerabilities and threats before they disrupt operations or cause lasting damage to their business reputation. SIEM makes behavioral anomalies visible to security teams, enhancing the monitoring process with AI to automate incident detection and response processes. It has replaced many manual tasks, becoming a base tool for any security operation center (SOC).

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. This requires proven design and development methodologies for the creation of SIEM content. SIEM implementations have a tendency to far exceed project timelines and budgets.

The ability to access the right skillset at the right time and quick access to vendor expertise are crucial for delivering SIEM projects on time and on budget. Implementation of too many use case scenarios at once often leads to a significant increase in SOC analyst workload due to a high number of false positives. The ability to define a phased implementation plan that prioritizes use case scenarios according to business risk posture and industry knowledge is fundamental.

Highlights

Advisory for SIEM tool selection, integration of Log sources, use cases, identification and Defining support structure.

SIEM Deployment Services

- Deployment plan.
- SIEM Software deployment.
- Policy and Response defined use case.
- Initial baselining and tuning.
- SIEM Migration Services
- Migration from existing Client SIEM solution to selected provider.
- Support to migrate from On-premises to Cloud solutions.
- Current supported target SIEM technology: Sentinel, Splunk, IBM QRadar.

Kyndryl Security Information and Event Management

Service Overview

Kyndryl SIEM advisory and Implementation Services are designed to help customers select the tools and plan the implementation or migration. Kyndryl helps customers to identify appropriate processes, design, and configuration of data sources, define playbooks, well defined best practices, and arrange for integration with automation tools like (ITSM and SOAR).

Kyndryl not only manages the implementation but also plans in providing the migration plan, it's the timeline, training, and how to plan required support after handover, and even extends for the ongoing management of the SIEM infrastructure as a future roadmap.

Kyndryl SIEM Implementation Services assist customers in:

- Aligning SIEM strategy approach with business and security objectives.
- Environmental assessment.
- Definition of Client's current SIEM environment, goals, log source baseline, data source priority points, and definition of the implementation timeline.
- Architecture design and planning.
- Co-relation rules and use cases
- Integration of Log sources, Baseline reports.
- Log Source baselining and policy tuning.
- Real time event and incident reports for analysis

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 experience.
- Modernize automation, operations, management, and governance.

Target Audience

Typical Sponsor

- CISO, CIO, CTO, COO, SOC Executives / Directors, etc.
- Companies of any size on a Zero Trust/Cyber journey
- Companies with a mobile workforce

Geographies

- Worldwide

For more information

To learn more about SIEM Advisory and Implementation Services please contact your Kyndryl Representative or Kyndryl Business Partner or visit 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.

The Kyndryl logo is displayed in a bold, lowercase, sans-serif font. The letters are a dark red or maroon color. The 'y' has a distinctive shape with a long, curved tail that loops back towards the stem.

© 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.

