kyndryl

Kyndryl Security Information and Event Management Migration

Customer Presentation

May 2024

Contents

kyndryl

What sets Kyndryl Security & Resiliency apart:

- Extensive partner ecosystem to support best-in-class technology solutions
- Improved ability to identify and respond to security threats
- More efficient security teams with flexible, modular delivery models

Leader

NelsonHall Cyber Resiliency NEAT Leader for 2024 [1]
Cybersecurity Services 2022 RadarView Report by Avasant [2]

50+

Countries with Kyndryl Security and Resiliency presence

7500+

Skilled Security and Resiliency practitioners globally

6

Global Security Operations Centers

500+

Security and Resilience patents

40+

Security and Resiliency alliances and strategic partners

30+ years

Experience in IT services

NelsonHall NEAT Leader 2024 Report [1]
Avasant Cybersecurity Services 2022 RadarView [2]

kyndryl

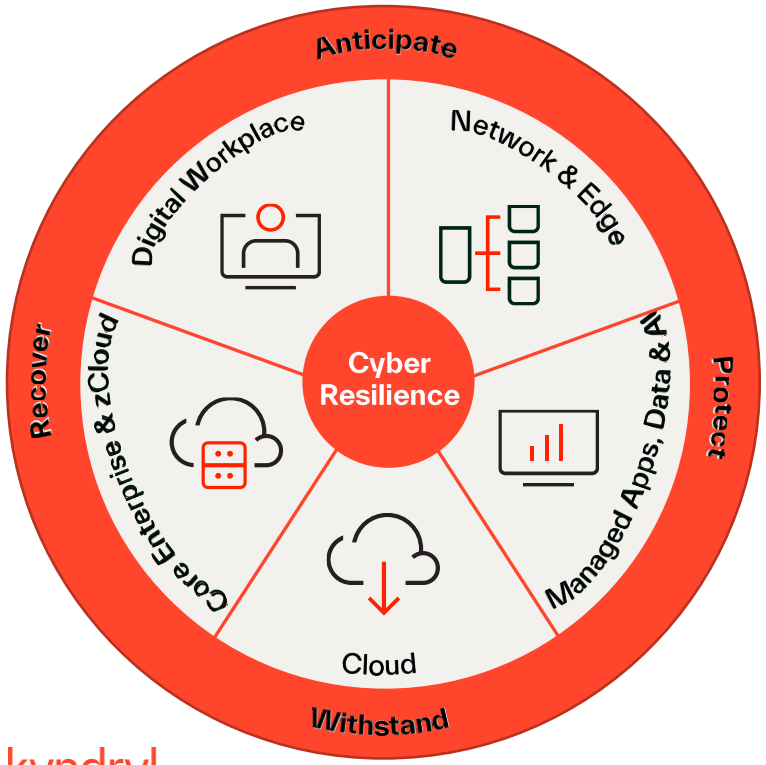
Kyndryl's Cyber Resilience Framework

cyber resilience

[**sahy**-ber ri-**zil**-y*uh*ns, -**zil**-ee-*uh*ns]

noun

The ability to anticipate, protect against, withstand and recover from adverse conditions, stresses, attacks and compromises of cyber-enabled business.



Security Assurance Services

Assess and benchmark resilience maturity, gain visibility into significant threats and vulnerabilities, manage compliance

- Risk Management
- Offensive Security Testing
- Compliance Management

Zero Trust Services

Protect critical business data and applications in a security-rich infrastructure

- Identity & Access Management
- Endpoint Security
- Network Security
- Data Protection & Privacy

Security Operations & Response Services

Discover and respond to a detected security incident

- Incident Response and Forensics
- Threat Detection & Response
- Vulnerability Management
- Security Operations Center (SOC) Services
- Security Operations as a platform

Incident Recovery Services

Mitigate impact of disruption with capabilities to automatically recover critical business processes and data

- Cyber Incident Recovery
- Managed Backup Services
- Hybrid Platform Recovery
- Data Center Design & Facilities

Anticipate → Protect → Withstand → Recover

Cybersecurity + Recovery

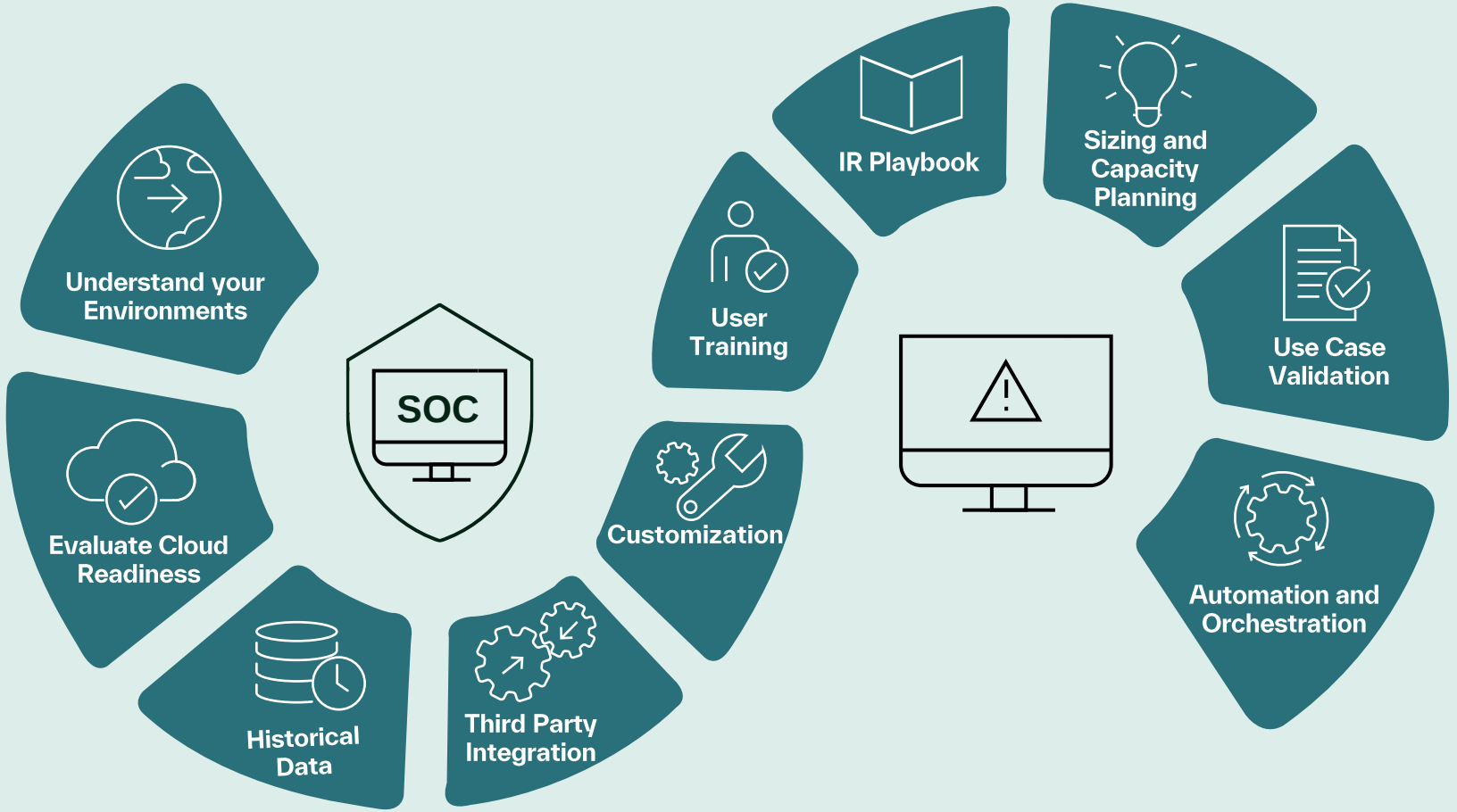
Deep expertise | Proven Processes | Intelligent automation

kyndryl

Key Findings

- **Slow response to threats:** legacy SIEMs use correlation rules, which are difficult to maintain and ineffective for identifying emerging threats. SOC analysts are faced with large amounts of false positives.
- **Scaling challenges:** as data ingestion rates grow, SOC teams are challenged with scaling their SIEM instead of focusing on protecting the organization.
- **Manual process**: SOC teams need highly skilled analysts to manually process large amounts of alerts**.** SOC teams are overworked, and new analysts are difficult to find.
- **Complex and inefficient management:** SOC teams typically oversee orchestration and infrastructure, manage connections between the SIEM and various data sources, and perform updates and patches. These tasks are often at the expense of critical triage and analysis.

Challenges and Complexities



kyndryl

The rapidly evolving IT environment and threat landscape continues to bring an increase in attacks and digital vulnerabilities

Risks to customers are increasing and are costly to resolve.

The number of common IT security vulnerabilities and exposures (CVEs) discovered worldwide has increased by **449%** in the past 10 years.[1]

49% of IT and security professionals believe their company's current patch management protocols fail to mitigate risk effectively, and **71%** see patching as overly complex, cumbersome, and time-consuming.[2]

By 2026, organizations prioritizing their security investments based on a continuous threat exposure management program will realize a two-third reduction in breaches.[3]

80% of applications contain at least one security vulnerability. Among the most common are vulnerabilities related to outdated components, security logging and monitoring failures, injection flaws, broken access controls, and cryptographic failures.[4]

Sources: https://nvd.nist.gov/general/nvd-dashboard
[1] https://www.statista.com/statistics/500755/worldwide-common-vulnerabilities-and-exposures/
[2] VentureBeat
[3] https://www.gartner.com/en/newsroom/press-releases/2024-02-22-gartner-identifies-top-cybersecurity-trends-for-2024
[4] State of Software Security 2024

kyndryl

Kyndryl's Approach to Security Information and Event Management (SIEM) Migration Services

Challenges

Coverage for Cloud Assets: legacy SIEMs often struggle to provide comprehensive coverage for cloud assets such as those in Azure, Microsoft 365, AWS, and Google Cloud Platform.

Slow Response to Threats: legacy SIEMs rely on correlation rules, which can be difficult to maintain and are often ineffective at identifying emerging threats. Microsoft Sentinel delivers intelligent security analytics, threat visibility, proactive hunting, and efficient threat response.

False Positives and Alert Overload: SOC analysts face challenges due to large volumes of false positives and alerts from various security components. Microsoft Sentinel provides signal-to-noise ratio and reduces alert fatigue.

52% of businesses report a security skills gap in their workforce.[1]

Migration Complexity: organizations may hesitate to migrate due to perceived risks of vendor lock-in, integration complexity, and data migration challenges.

- Microsoft Sentinel delivers intelligent security analytics and threat intelligence across the enterprise. It provides a single solution for attack detection, threat visibility, proactive hunting, and threat response.
- Microsoft Sentinel is your bird's eye view across the enterprise alleviating the stress of increasingly sophisticated attacks, increasing volumes of alerts, and long resolution timeframes.

Collect data at cloud scale across all users, devices, applications, and infrastructure, both on premise and in multiple clouds.

Detect previously undetected threats and minimize false positives using Microsoft's analytics and unparalleled threat intelligence.

Investigate threats with artificial intelligence, and hunt for suspicious activities at scale, tapping into years of cybersecurity work at Microsoft.

Respond to incidents rapidly with built-in orchestration and automation of common tasks.

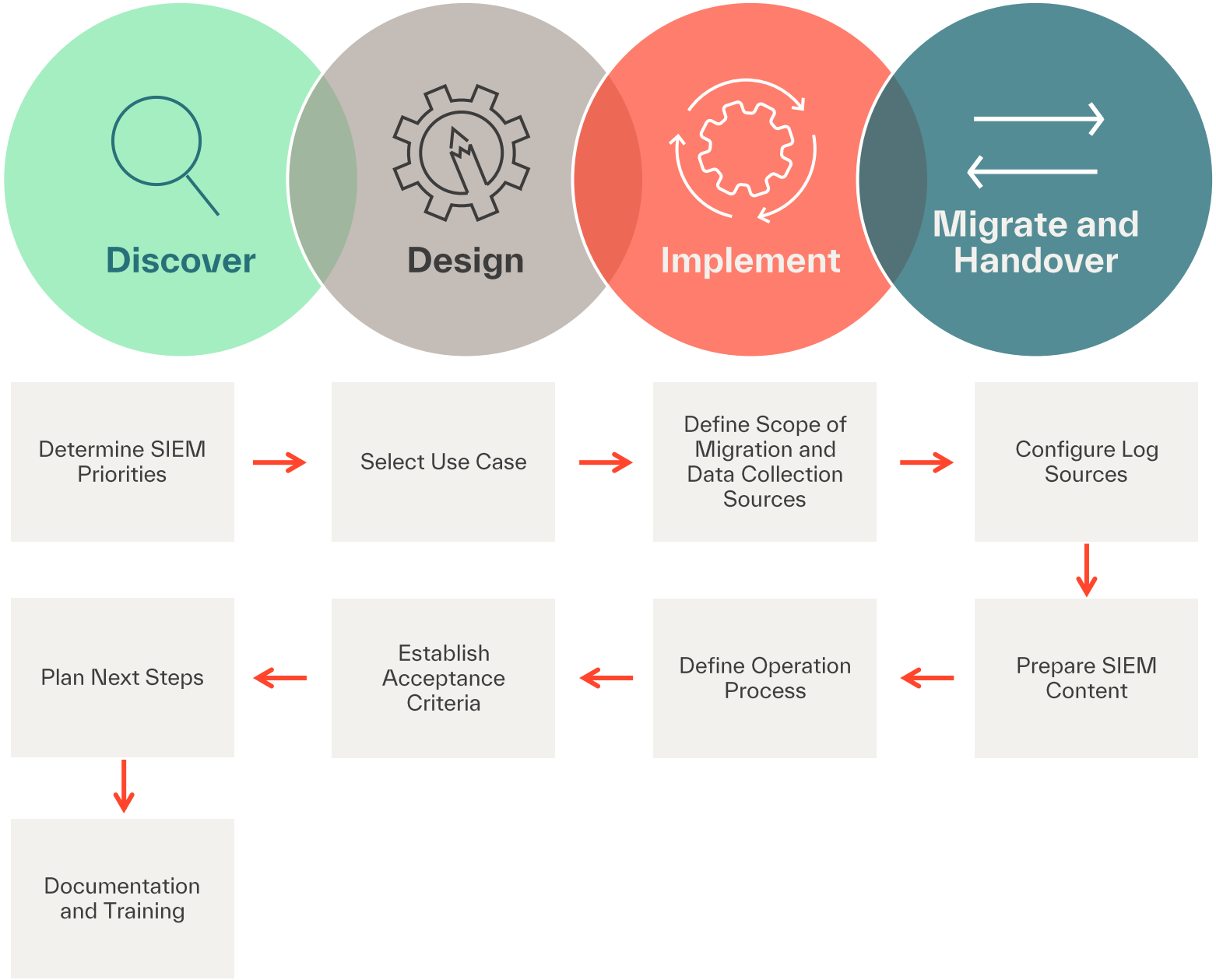
kyndryl

Source: [1] 2023 ISC2 Cybersecurity Workforce Study

Kyndryl's Approach

ROI of 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 with Sentinel migration.
- Azure Integration: Works seamlessly with Azure services.
- Delivery on time and within budget using well-defined processes and methodologies



kyndryl

Kyndryl Security Information and Event Management Migration

- Project management
- Assessment and planning
- Deployment
- Use case and Data migration
- Performance and scalability planning
- Integration and customization
- Define a plan to build a required support system

Identify requirements, business case and use cases

Documentation for data source integration and automation

Microsoft Sentinel implementation

Create Sentinel rules, Deploy, and create playbooks. Integrate with SOAR, ITSM

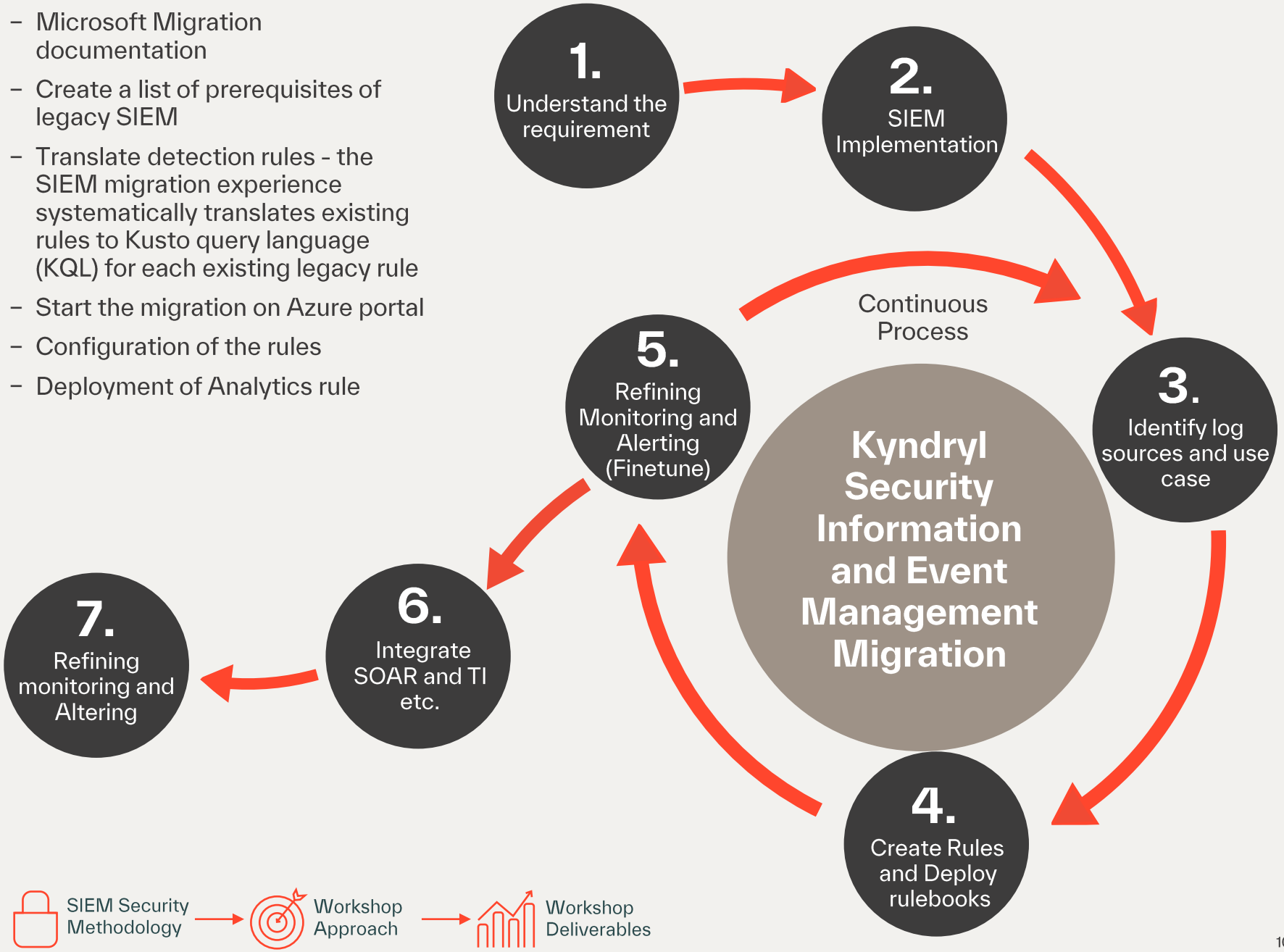
Deploy dashboards and refine monitoring and altering

Handover and Training

SIEM Migration is part of the Kyndryl Security Operation and Response Service

- The following diagram explains the Kyndryl methodology for SIEM Migration.
- It starts with SIEM deployment, migration of use cases, log ingestion, and finetuning before handover.
- Point 5 is feedback to point 3, which is a continuous process covered in managed and operation services.

- Microsoft Migration documentation
- Create a list of prerequisites of legacy SIEM
- Translate detection rules - the SIEM migration experience systematically translates existing rules to Kusto query language (KQL) for each existing legacy rule
- Start the migration on Azure portal
- Configuration of the rules
- Deployment of Analytics rule



kyndryl

Kyndryl Security Information and Event Management Migration

Overview

Security Information and Event Management (SIEM) is a comprehensive approach to security management that combines real-time event monitoring, log analysis, and incident response. It helps organizations detect and respond to security incidents by collecting, correlating, and analyzing data from various sources such as logs, network traffic, and security devices.

Legacy system: the existing SIEM may be outdated or no longer supported. Scalability: the current solution may not scale well with growing data volumes. Advanced features: a new SIEM may offer better features, threat intelligence, or automation capabilities. Cost efficiency: migrating to a more cost-effective solution. Vendor changes: organizations may switch vendors due to strategic decisions or mergers.

Capabilities

- Architecture planning and support
- Environmental assessment
- Complete SIEM design, planning, implementation, and handover planning for Operate-Manage
- Create an architecture design for migration that includes detection rules, playbooks, historical data, dashboarding, and other processes
- Timely delivery and a well-defined process
- Definition and onboarding of the customer's current SIEM environment, goals, log source baseline, data source priority points, and definition of the implementation timeline

Supported Vendor Products

- SIEM – Sentinel (Migration from QRadar, Splunk, ArcSight, and any other legacy SIEM solution)

Service Modules

- Assessment: evaluate the existing SIEM deployment, including data sources, use cases, and performance
- Planning: define migration goals, select the new SIEM, and plan the transition
- Data Migration: transfer historical data from the old SIEM to the new one
- Configuration: set up the new SIEM, and configure data sources, rules, alerts, and dashboards
- Testing: validate the new SIEM's functionality and performance
- Deployment: gradually switch over to the new SIEM while monitoring for any issues
- Training: train security analysts and SOC teams on the new system
- Optimization: continuously fine tune the new SIEM based on feedback and requirements

Thank You

Notices and Disclosures

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.

The performance data and client examples cited are presented for illustrative purposes only.
Actual performance results may vary depending on specific configurations and operating conditions.