kyndryl

Kyndryl Cyber Defense Operations Center

Highlights

Key capabilities (Design and Build)

- Architecture Design for Kyndryl Cyber Defense Operations Center
- Streamlined target operating model and operational workflow processes
- Develop and implement a plan for tools to reduce overlap, integrate to provide scalability future expansion
- Design, build, and deploy at least 5 playbooks (baseline)
- Perform acceptance testing for playbooks and establish regular reviews
- Configure analytics automation and machine learning to enhance threat detection and automate response capabilities
- User Acceptance Testing and Period Reviews
- Playbooks and Automation recommendations to implement for Proactive Incident and Threat Management
  - Modify existing or create new Kyndryl Cyber Defense Operations Center operations
  - SOPs, playbooks, and automations
  - Incident detection, evaluation & response across Kyndryl Cyber Defense Operations Center, develop a transition and steady state plan

Available services

- Advisory Services, Design Services, Implementation Services and Future expansion to Managed and Staff Augmentation

In today's increasingly complex and interconnected digital environments, organizations face significant challenges in maintaining the availability, performance, and security of their IT systems. Traditional NOC and SOC often operate in silos, leading to delayed incident response, fragmented visibility, and inefficient resource utilization. The absence of such a unified approach can result in increased downtime, data breaches, and operational inefficiencies, ultimately impacting business continuity and customer trust.

Introduction

Kyndryl provides a standard and consistent integrated approach to IT operations and security. This integration allows for seamless communication and collaboration between network and security teams, leading to more effective incident response and overall IT management.

While many organizations have established Security Operations Centers (SOC) and Network Operations Centers (NOC) to monitor their digital state, Kyndryl recognizes the interdependence of security and network functions and seeks to break down silos for a more holistic and responsive operational model. The integration of the SOC and the NOC into a unified Cybersecurity and Network Intelligence Operations Center is a strategic move designed to enhance operational efficiency, communication, and collaboration within an organization.

Kyndryl's Point of View

As per Kyndryl, we recognized the need for Collaborative Security and Network operations, which provides both sets of engineers comprehensive visibility through network traffic, system performance, endpoint activity & threads, security events correlation leveraging a single case management tool, and automated/integrated playbooks.

We believe that a key requirement for full realization of the benefits of this Kyndryl Cyber Defense Operations Center approach requires a suite of integrated tools and processes for unified Threat detection & Incident Response and better performance. This approach helps you achieve peak operational efficiency with optimized resource models and proactive, accurate issue identification. Combined uptime monitoring with proactive threat detection (availability and security) provides continuous service delivery through greatly minimized disruptions and downtime.

Integration will lead to accelerated, accurate decisive responses, amplify the visibility across the entire IT ecosystem, slash operational costs by harnessing automation and accurate threat/incident identification, and remediation all within a unified ecosystem. Finally, you will boost resilience through forward-thinking detection and automated countermeasures.

Kyndryl Consult Cyber Defense Operation Center (Design and Build)

Kyndryl will work with our customers to define which tools, functions, and responsibilities will be included in the unified Kyndryl Cyber Defense Operations Center. This includes assessing the current capabilities across existing SOC(s) and NOC(s), evaluating processes, procedures, workflows, existing playbooks, automation in place, and analyzing team structure and skills. Kyndryl will also perform a technology and architectural review of the current Infrastructure, including tools used, capabilities, scalability, integrability, and usability.

Kyndryl will collaborate with cross-functional teams to create a comprehensive roadmap and timeline for developing an effective Kyndryl Cyber Defense Operations Center. This process will involve integrating tools, making architectural changes, updating processes, redesigning the organizational structure, mapping required skills, integrating workflows, recommending key performance indicators (KPIs), generating base reports, identifying necessary cross-training, and suggesting a set of playbooks and automation strategies.

Kyndryl is exploring modern AI techniques while designing the Kyndryl Cyber Defense Operations Center process to provide richer probabilistic insights based on patterns, with a human in the loop to execute automation playbooks faster and drive towards a quicker response.

Kyndryl's Competitive Differentiators

Comprehensive and extensive experience in large scale security and network solutions, including assessments, design and build, and managed services.

- → Assessing, designing, and building a Kyndryl Cyber Defense Operations Center
- → Rationalizing existing tools and achieving better operational efficiency
- → Integrating tools with a reference architecture approach
- → Achieving cost savings through the consolidation of technology, infrastructure, and personnel
- → Reduce complexity and streamline threat detection and incident response
- → Automating playbooks leveraging our technology

Kyndryl's focus on playbook automation, combined with the use of AI and ML algorithms, enhances response times and preventive capabilities.

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 suitable to meeting your requirements.

Experience

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

Technology

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.

For more information

To learn more, Kyndryl Consult Cyber Defense Operation Center please contact your Kyndryl Representative or Kyndryl Business Partner, or visit www.kyndryl.com.

kyndryl