How Xage Security Supports The Saudi Arabia NCA OTCC-1:2022 Cybersecurity Mandates

Introduction

The Saudi Arabia National Cybersecurity Authority's (NCA) Operational Technology Cybersecurity Controls (OTCC-1:2022) framework aims to enhance the protection of industrial control systems (ICS) and operational technology (OT) environments. The framework outlines a set of cybersecurity controls specifically designed for ICS, focusing on mitigating cyber threats and ensuring compliance with international best practices. It plays a crucial role in securing critical infrastructures that operate or depend on ICS and OT systems.

The Xage Fabric is a comprehensive cybersecurity platform engineered to safeguard and manage OT and ICS environments by employing zero-trust principles. Through its decentralized architecture, the Fabric delivers robust security, identity and access management (IAM), and policy enforcement across a wide range of ICS and OT devices. This end-to-end protection solution empowers organizations to preserve the integrity and security of their critical operations without disruption or down time.

Overview of NCA's OTCC-1:2022

The NCA's OTCC-1:2022 framework consists of four key domains, each with a set of sub-domains and controls, summarized here. For a deeper dive into each domain and control, please request our extended NCA OTCC White Paper.

Cybersecurity Governance

- 8 Sub-domains
- 18 controls

Cybersecurity Defense

- 13 sub-domains
- 26 controls

Cybersecurity Resilience

- 1 sub-domain
- 2 controls

Third Party Cybersecurity

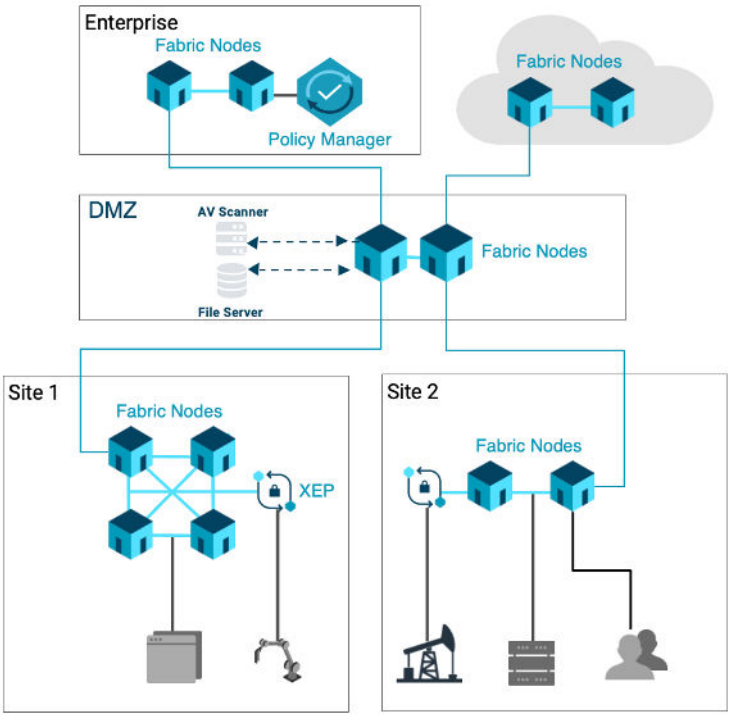
- 1 sub domain
- 2 controls

Compliance with OTCC-1:2022 is essential for organizations operating within Saudi Arabia's ICS and OT sectors. Adhering to the framework helps organizations proactively identify and manage potential risks, maintain the security and resilience of their systems, and uphold their reputation in the industry. Non-compliance with the OTCC-1:2022 framework can result in various consequences, including regulatory penalties, increased vulnerability to cyberattacks, loss of valuable data, and damage to critical infrastructure.

Overview of Xage Security Platform

Xage Security Platform is a comprehensive cybersecurity solution specifically designed to address the challenges faced by industrial control systems (ICS) and operational technology (OT) environments. The platform offers a wide range of features and capabilities to ensure robust protection and efficient management of ICS and OT assets.

Key security features and capabilities of the Xage Fabric Platform include:



1. **Zero Trust security:** Xage implements the Zero Trust security model, which mandates continuous validation of user and device identities, as well as the context of each access request, minimizing the risk of unauthorized access.
2. **Policy enforcement and automation:** Xage allows organizations to define and enforce security policies consistently across their ICS and OT environment, automating compliance and risk management processes.
3. **Decentralized architecture:** Leveraging distributed ledger technology, Xage ensures data integrity, tamper-proof protection, and resilient communication across various ICS and OT devices.
4. **Identity and Access Management (IAM):** The Xage Fabric platform offers granular access control, ensuring that only authorized personnel can access the systems and assets they require, following the principle of least privilege.

The benefits of using the Xage Security Platform are numerous, addressing many common cybersecurity challenges faced by organizations with OT landscape:

1. **Enhanced security:** Xage provides end-to-end protection for ICS and OT systems, mitigating the risk of cyberattacks and ensuring the continuity of critical operations.
2. **Scalability:** The decentralized architecture enables Xage to scale across vast and complex OT environments seamlessly, ensuring consistent security across various devices, systems, and networks.
3. **Streamlined compliance:** The platform's policy enforcement and automation capabilities simplify the process of adhering to industry regulations and standards, such as the NCA's OTCC-1:2022 framework.
4. **Reduced complexity:** Xage consolidates multiple security functions within a single platform, simplifying the management and maintenance of cybersecurity measures in the OT landscape.

Mapping NCA OTCC-1:2022 Technical Requirements to Xage Fabric Platform Capabilities

The 2nd domain of NCA OTCC-1:2022, Cybersecurity Defense, focuses on enhancing the security posture of ICS and OT environments by implementing a comprehensive set of controls to protect against cyber threats. The domain is divided into several sub-domains, each addressing specific aspects of cybersecurity defense. Xage Security Platform aligns well with the requirements of this domain, offering various capabilities that address the respective sub-domains and control numbers.

Below is a comprehensive mapping of Xage capabilities with the Cybersecurity Defence Domain and its respective sub-domains and controls that the Xage Fabric satisfies:

SN	Xage Capability	Xage Capability Details	OTCC Sub-Domain	Control Number
1	**Decentralized Identity and Access Management**	Provides role-based access control, secure authentication, and authorization for users and devices across the OT landscape.	• Access Control	• 2.1.1 - 2.1.6
2	**Zero Trust Architecture**	Ensures that all network communications are authenticated, encrypted, and authorized, significantly reducing the attack surface.	• Network Security	• 2.2.1 - 2.2.6
3	**Secure Remote Access**	Enables secure remote access for maintenance and support activities while maintaining a strong security posture.	• Access Control • Remote Access	• 2.1.6 • 2.3.1 - 2.3.5
4	**Data Security and Integrity**	Provides end-to-end data protection by encrypting and securing data at rest and in transit.	• Data Security	• 2.4.1 - 2.4.3
5	**Policy Enforcement**	Ensures that security policies are consistently applied across the OT landscape, enhancing the overall security posture.	• Configuration Management • Incident Response	• 2.5.1 - 2.5.4 • 2.6.1 - 2.6.4
6	**Automated Device and User Management**	Streamlines the process of adding, updating, and removing devices and users, ensuring consistent security configurations and adherence to security policies.	• Asset Management • Configuration Management	• 2.7.1 - 2.7.3 • 2.5.1 - 2.5.4

SN	Xage Capability	Xage Capability Details	OTCC Sub-Domain	Control Number
7	**Segmentation and Micro-segmentation**	Reduces the attack surface by isolating critical systems and devices, preventing lateral movement in case of a security breach.	• Network Security	• 2.2.1 - 2.2.6
8	**Scalable and Resilient Architecture**	Provides a highly scalable and fault-tolerant architecture capable of supporting large-scale deployments, ensuring continuous security operations in the face of infrastructure changes or failures.	• System Resiliency	• 2.8.1 - 2.8.3
9	**Tamper-proof Audit Trail and Security Reporting**	Ensures the integrity of audit logs and security reporting, providing a reliable source of information for incident response, compliance audits, and forensic investigations.	• Logging and Monitoring	• 2.9.1 - 2.9.5

Conclusion

Xage Security Fabric effectively addresses the key technical requirements of the NCA OTCC-1:2022 framework, providing comprehensive protection for ICS and OT environments. The Fabric's innovative features and alignment with the framework's sub-domains and controls ensure compliance and robust security. By choosing Xage Fabric, organizations can achieve both compliance and enhanced protection for their critical operations and infrastructures.

For a deeper understanding of how Xage covers the full range of requirements in the NCA OTCC-1:2022 mandate, please request our extended white paper.