Xage Security enables NERC-CIP compliance for utility customers

Over the last few years the scale and severity of cybersecurity attacks has increased significantly. Incidents ranged from attacks on utility grids resulting in widespread power outages, exploits on aircraft changing their flight patterns, remote commandeering of vehicles, and an attack that turned the Internet-of-Things into the Army-of-Things launching the largest DDoS attack at the time. Such exploits have exposed systemic weaknesses with current cyber-security access control approaches like permanent certificates and hardcoded passwords. Lack of effective cybersecurity controls and policies at the edge is a big hurdle in converging industrial & commercial operations and scaling IoT adoption.

The North American Electric Reliability Corporation (NERC) is the regulatory body that puts together guidelines for assuring reliability and security of the power delivery networks in North America. The Critical Infrastructure Protection (CIP) standards are designed to address cybersecurity concerns of the North American power grids.

Xage Security delivers decentralized identity and access management services for heterogeneous IoT operations with centralized control, policy management & compliance. Xage enables industrial and commercial operators to control access between users, devices, applications, and data by hosting information security services within their operating environments. Xage's distributed consensus protocol builds high levels of tamper-resistance into these services in conjunction with industrial-scale control of policies & compliance assuring business continuity across all managed sites. Xage has partnered with industrial vendors & operators across verticals like energy, aviation, building management, and transportation.

Xage delivers enterprise class security services to the edges of large scale industrial & commercial operations. Xage's technology provides role based identity and access management for users, devices, applications, and data at the edge. Xage's policy management platform enables centralized creation of sophisticated access control policies and policy distribution to a network of edge nodes for decentralized enforcement delivering uninterrupted service over intermittent and offline connections.

Xage enables utilities to meet NERC-CIP requirements, maintain their service delivery standards, and avoiding potential large liabilities. This paper summarizes how Xage's products and technology uniquely address NERC-CIP challenges for our utility customers.

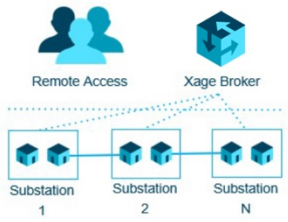
Xage System Architecture

Simplify Access Control & SDN deployments

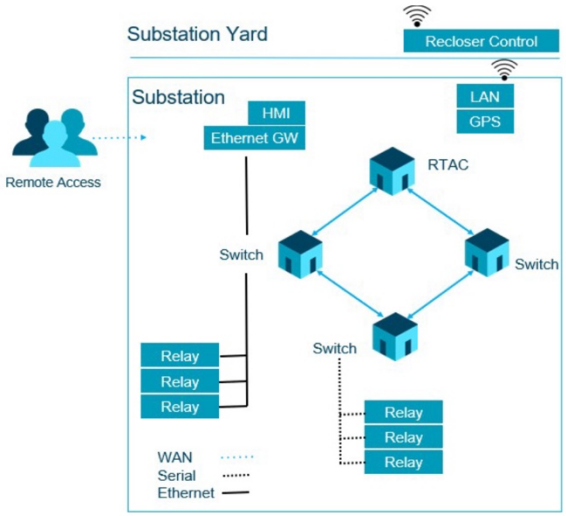
Eliminate single point of failure

Eliminate VLAN and ACL complexity

Eliminate single use or specialized gateways



Centralized operations and maintenance policy automatically replicated across all substations



Xage Security Suite Map for NERC CIP Requirements

CIP-004	CIP-005	CIP-007	CIP-011
Training & Personnel Security	**Electronic Security Perimeter**	**Systems Security Management**	**Information Protection**
4.2 - Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	1.3 - Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	1.1 - Where technically feasible, enable only logical network accessible ports that have been determined to be needed.	1.2 - Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.
4.3 - For electronic access, verify at least once every 15 calendar months that all user Accounts & associated privileges are correct.	1.5 - Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	3.1 - Deploy method(s) to deter, detect, or prevent malicious code.	
4.4 - Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System are correct.	2.1 - Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	3.2 - Mitigate the threat of detected malicious code.	

5.1 - A process to initiate removal of an individual's ability for physical access and Interactive Remote Access upon a termination action	2.2 - For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	4.1 - Event logging at the BES Cyber System or at the Cyber Asset Levels.	
5.3 - For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information.	2.3 - Require multi-factor authentication for all Interactive Remote Access sessions.	4.3 - Retain applicable event logs for at least 90 consecutive calendar days.	
5.4 - For termination actions, revoke the individual's non-shared user accounts.		4.4 - Review a summarization or sampling of logged events as determined by the Responsible Entity.	
5.5 - For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action.		5.1 - Have a method(s) to enforce authentication of interactive user access, where technically feasible.	
		5.2 - Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	
		5.3 - Identify individuals who have authorized access to shared accounts.	
		5.4 - Change known default passwords, per Cyber Asset capability.	
		5.5 - For password-only authentication for interactive user access, either technically or procedurally enforce complexity parameters.	
		5.6 - Where technically feasible, enforce password changes or an obligation to change the password at least once every 15 calendar months.	

		5.7 – Either limit the number of unsuccessful authentication attempts or Generate alerts after a define threshold of unsuccessful attempts.	

CIP-004-6 Training & Personnel Security

ID	NERC-CIP Requirements	Xage Response
4.2	Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	In Xage Audit log, all the authorization records could be viewed across all systems.
4.3	For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	User accounts, groups, and roles, as well as policies are managed in a central location. This makes this very easy to validate and change if needed.
4.4	Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	User accounts, groups, and roles, as well as policies are managed in a central location. This makes this very easy to validate and change if needed.
5.1	A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights)	A single policy is required to revoke the terminated user access rights. This policy change can also be automated completely using Xage REST API and integrated into existing workflows.

5.2	Foor reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	See 5.1
5.3	For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.	See 5.1
5.4	For termination actions, revoke the individual's non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	See 5.1
5.5	For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access. If the Responsible Entity determines and documents that extenuating operating circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the operating circumstances.	Xage eliminates the use of a shared account (which is a security hole by itself).

CIP-005-6 Electronic Security Perimeter

ID	NERC-CIP Requirements	Xage Response
1.3	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.	Xage enforces user-based policy over both inbound and outbound traffic and denies all other access.
1.5	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications.	Any login attempt, successful or not, is logged and monitored. Malicious or abnormal patterns will show up on the dashboard.
2.1	Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.	Xage acts as such an intermediate system which denies direct access between the two without authentication.
2.2	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	Xage fully encrypts the entire traffic end to end (as well as tamperproofing the traffic). This includes remote access sessions.
2.3	Require multi-factor authentication for all Interactive Remote Access sessions.	Xage enables MFA for every device.

CIP-007-6 System Access Control

ID	NERC-CIP Requirements	Xage Response
1.1	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	This requirement is trying to minimize Cyber risk ("closing ports" is reducing the attack surface). However, Xage reduces the attack surface even further than simply closing unused ports and leaving the "needed" ports open, by closing those ports as well and allowing access to those ports only based on user authentication.

3.1	Deploy method(s) to deter, detect, or prevent malicious code.	Xage monitors login attempts - This enables the detection of brute-forcing attacks or the use of common passwords by attackers. This also helps with detecting lateral movement. The policy enforcement makes it harder for malware to propagate in the network (for example, if a policy is set to not enable a device to connect to other devices which he should not access - they won't be infected).
4.1	Log events at the BES Cyber System level or at the Cyber Asset level for identification of, and after-the-fact investigation of, Cyber Security Incidents that includes, as a minimum: 4.1.1. Detected successful login attempts 4.1.2. Detected failed access and failed login attempts 4.1.3 Detected malicious code	Xage Nodes track all access attempts and transactions performed by users, devices, and applications across the entire field area network. These transactions along with source and destinations fields are sent up to the control center with signatures stored in the Xage Nodes such that audit trails cannot be compromised.
4.2	Generate alerts for security events that the Responsible Entity determines necessitate an alert, that includes, as a minimum, each of the types of events: 4.2.1.Detected malicious code from Part 4.1 Detected failure of Part 4.1 event logging.	Event and Alarm settings can be configured on the Xage Brokers and applied to the entire field of Xage Node on granular basis. Here is a sampling of supported events and alarms: rogue device detected and blacklisted, too many invalid login attempts, expired or revoked certificate is detected
4.3	Where technically feasible, retain applicable event logs identified in Part 4.1 for at least the last 90 consecutive calendar days except under CIP Exceptional Circumstances.	Xage Node stores unique log signatures in the distributed database. The audit trail is in the Common Event Format (CEF) and easily integrates with any security information and event management (SIEM) software products.
4.4	Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 calendar days to identify undetected Cyber Security Incidents.	With Xage audit logs this is easily doable - it is even possible to automate this process with REST API.
5.1	Have a method(s) to enforce authentication of interactive user access, where technically feasible.	Xage Nodes enables users to authenticate with field devices using enterprises credentials instead of devices specific credentials. Xage integrates with enterprise services such as LDAP, Active Directory, RADIUS, TACACS, and Certificate Authorities and makes their services available at the edge for authentication with field devices.

5.2	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).	Xage discovers all field device access methods, whether through management interfaces or industrial control protocols. Xage identifies all devices specific credentials, rotates them, and integrates identities and credentials with enterprise systems such Active Directory, LDAP, and Certificate Authorities.
5.3	Identify individuals who have authorized access to shared accounts.	Xage enables utilities to track all permissions and authorizations for field devices using enterprise management systems.
5.4	Change known default passwords, per Cyber Asset capability.	Xage Nodes deployed at the edge can update and rotate passwords for devices in the network based on schedule or on-demand using a specified password policy.
5.5	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1.Password length that is, at least, the lesser of eight characters Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase, lowercase, numeric, non-alphanumeric)	All interactive user access password policies can be centrally created using enterprise class access and identity management services (IAMs). Password policies can be created centrally and enforced at the edge using Xage Nodes.
5.6	Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.	Xage Nodes support password rotation and certificate enrollment for a variety of different devices such as smart meters, distribution automation controllers, relays, RTUs and PLCs. Credential rotation schedules can be specified centrally using Xage Brokers and are enforced at the edge through Xage Nodes.
5.7	Where technically feasible, either: • Limit the number of unsuccessful authentication attempts; or Generate alerts after a threshold of unsuccessful authentication attempts.	Xage Nodes can limit unsuccessful access attempts and generate alerts for greenfield and brownfield devices in the utility network that do not currently support this capability. In addition, Xage can identify all access transactions in the field network and provide detailed access logs to the operators.

CIP-011-6 Information Protection

ID	NERC-CIP Requirements	Xage Response
1.2	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	Xage secures the information exchanged between different BES by encryption and tamperproofing the information in transit. In the future, Xage will allow to store that data in a secure manner (encrypted with access controls, as well as tamper proof).

About Xage

The Xage Security Suite is the first and only blockchain-protected security platform for the Industrial Internet of Things (IIOT). Xage creates the essential trusted foundation for secure interactions between machines, people, and data. Advancing beyond traditional security models, Xage distributes authentication and private data across the network of devices, creating a tamper-proof "fabric" for communication, authentication and trust that ensures security at scale. Xage supports any-to-any communication, secures access to existing industrial systems, underpins continuous edge-computing operations even in the face of irregular connectivity, and gets stronger and stronger with every device added to the network. Xage customers include leaders in the largest industries, spanning energy, utilities, transportation and manufacturing