SALT

IEC 62443 – Industrial API Security: Protecting Critical Infrastructure

IIEC 62443 targets the security of industrial automation and control systems (IACS), relying on APIs for communication. It promotes a zone and conduit model for network segmentation and secure communication to protect APIs. The standard requires strong authentication and precise access control to prevent unauthorized access and safeguard critical infrastructure. Following IEC 62443 ensures the safety and reliability of industrial operations.

- Zone and Conduit Model:
  - Segmentation of industrial networks into security zones.
  - Implementation of secure communication conduits between zones.
  - Control of network traffic to prevent unauthorized access.
- Authentication and Authorization:
  - Use of mutual TLS (mTLS) for strong authentication.
  - Implementation of role-based access control (RBAC) for granular access control.
  - Regular review of user access privileges.
- Operational Technology (OT) Security:
  - Addressing real-time constraints and legacy systems.
  - Implementing security measures to protect against OT-specific threats.
  - Ensuring the safety and reliability of industrial operations.

Why It Matters: IEC 62443 is crucial for protecting industrial automation and control systems (IACS), which are vital for critical infrastructure. Secure APIs prevent disruptions, ensure safety, and maintain the reliability of these systems, safeguarding essential services and preventing potential disasters.

API Security Requirements:

- Strong Authentication: Industrial APIs must use mutual TLS (mTLS) and certificate-based authentication.
- Access Restrictions: APIs should have network segmentation and zero trust policies.

Relevant Sections Referencing APIs:

- IEC 62443-4-2: APIs must be secured to prevent unauthorized access to industrial control systems.

How Salt Security Helps: Salt Security secures industrial APIs and aligns with IEC 62443 by providing API discovery, vulnerability assessment, and threat protection. Posture governance features help enforce secure configurations and monitor API activity, ensuring the ongoing security and compliance of industrial operations. Learn more about API Security and Compliance in our **White-paper.**