SYSTEMINENCE

Implementing Dual Authorization in Avigilon for Enhanced Access Control

Background

A leading cybersecurity organization required a security enhancement for their access control system to introduce an additional layer of authorization when granting user access to critical areas. The customization aimed to ensure that an administrator alone could not grant access without approval from a higher-level authority, thus mitigating risks associated with unauthorized access.

Challenges

Avigilon's native access control system allowed administrators to create users and assign access rights without requiring secondary approval. This meant that once an admin provided access to a user for a specific area, that access was immediately effective, with no way to stop, review, or audit it before implementation.

However, the organization needed an additional security mechanism where any new access rights granted by an administrator would require explicit approval from a super admin before becoming active. This was particularly crucial for highly sensitive areas, such as rooms containing financial records, classified documents, or critical infrastructure.

The Solution

To meet this requirement, Systeminence developed a Dual Authorization mechanism using the Octopus middleware, integrating it with Avigilon's access control system.

The solution worked as follows:

- User Role Definition:
  - Super Admin: Highest privilege, responsible for approving or rejecting access requests.
  - Admin: Can create users and assign access but requires Super Admin approval.
  - Operator: Limited to monitoring events but cannot create or modify access rights.
- Access Request Workflow:
  - When an Admin assigns access rights to a user (e.g., allowing entry to a restricted area), the request does not take effect immediately.
  - Instead, a notification is sent to the Super Admin detailing the requested access changes.
  - If the Super Admin approves, the system enables the user and grants the requested access.
  - If the Super Admin rejects, the access request is canceled, and the user remains restricted.
- System Implementation in Avigilon:
  - Octopus was configured to track all user creation and access modifications within Avigilon.
  - Any change made by an Admin (add, edit, or delete access rights) was intercepted and paused until the Super Admin provided a decision.

  - If the Super Admin approved, the system executed the change; otherwise, the access remained disabled.
  - The system automatically disabled the user's access rights until approval was granted, ensuring that no unauthorized entry occurred during the approval process.

- System Implementation in Avigilon:
  - The dual authorization system ensured compliance with cybersecurity and security auditing standards.
  - Auditors reviewing access control logs could confirm that access rights were approved by a higher authority before being granted.
  - This prevented unauthorized personnel from gaining access to restricted areas without proper oversight.

Outcome

- Enhanced Security: No unauthorized access could be granted without dual approval, significantly reducing the risk of insider threats.
- Improved Compliance: The new workflow met the stringent security audit requirements, ensuring role-based access aligned with organizational policies.
- Accountability & Transparency: Every access request was logged, along with approval/rejection records, providing a clear audit trail.
- Seamless Integration: The solution was implemented without disrupting daily operations, and admins quickly adapted to the new workflow.

Why Octopus?

- Seamless Integration: Octopus enabled smooth middleware integration with Avigilon's access control system without requiring extensive modifications.
- Customizable Workflow: The flexibility of Octopus allowed the implementation of the dual authorization mechanism tailored to the organization's security policies.
- Centralized Control: The platform provided a centralized interface for managing access rights, improving overall security oversight.

Technologies Used

- Avigilon Access Control System – The foundation for user access management.
- Octopus Middleware – The core system handling the dual authorization process.
- Automated Notification System – Alerts Super Admins for approval or rejection of access requests.
- Audit Logging & Reporting – Ensures compliance and provides traceability for all access control modifications.

By implementing the Dual Authorization mechanism, the organization strengthened its security posture, ensuring that access control decisions were always reviewed by a higher authority before being enacted. This solution provided an effective way to enforce role-based access management, regulatory compliance, and security oversight within Avigilon's access control system.

About Systeminence

Systeminence is a software development company that specializes in designing, developing, and executing Computer Vision and software integration solutions for the security industry. We employ an agile and flexible software development approach to assist you in saving time when dealing with mission-critical situations and simplifying your day-to-day tasks, thereby making your business processes more intuitive, connected, and integrated.