Nozomi Networks CMC (Central Management Console) – Operations & Administration

Duration: 3 Days

Module 1: Introduction to Nozomi Networks

- Overview of Nozomi Networks and its cybersecurity ecosystem
- Understanding industrial cybersecurity and the role of CMC
- Nozomi Guardian vs. Nozomi CMC – Key differences

Module 2: CMC Architecture and Deployment

- CMC architecture and communication model
- Deployment models (cloud, on-premises, hybrid)
- System requirements and installation steps
- Integrating multiple Guardian sensors

Module 3: User Interface and Navigation

- Dashboard overview and user interface walkthrough
- User roles and access control
- Overview of key menus: Alerts, Assets, Map, Reports

Module 4: Asset and Network Visibility

- Asset discovery and classification
- Network topology mapping
- Managing asset inventory across multiple sites
- CMC’s role in centralized monitoring

Module 5: Threat Detection and Alerts Management

- Understanding alert types and severities
- Correlating alerts from different Guardians
- Alert workflow: acknowledgment, investigation, and resolution
- Alert suppression and tuning

Module 6: Configuration and Policy Management

- Centralized configuration of Guardians
- Managing baselines, rules, and policies
- Using templates for consistent deployment

Module 7: Reporting and Compliance

- Generating and scheduling reports
- Overview of compliance-oriented reporting (NIST, IEC 62443)
- Exporting logs and alerts for audit purposes

Module 8: Integrations and API Use

- Integrating with SIEM, SOAR, and ticketing systems
- Syslog, SNMP, and email alert configuration
- Overview of Nozomi API and its use cases

Module 9: Maintenance and Troubleshooting

- CMC logs and health monitoring
- Upgrades and backup procedures
- Common issues and troubleshooting tips

Module 10: Hands-on Labs (Optional)

- Deploying and configuring CMC
- Simulating alerts and policy changes
- Centralized management of Guardian appliances