Invensys Cyber Security

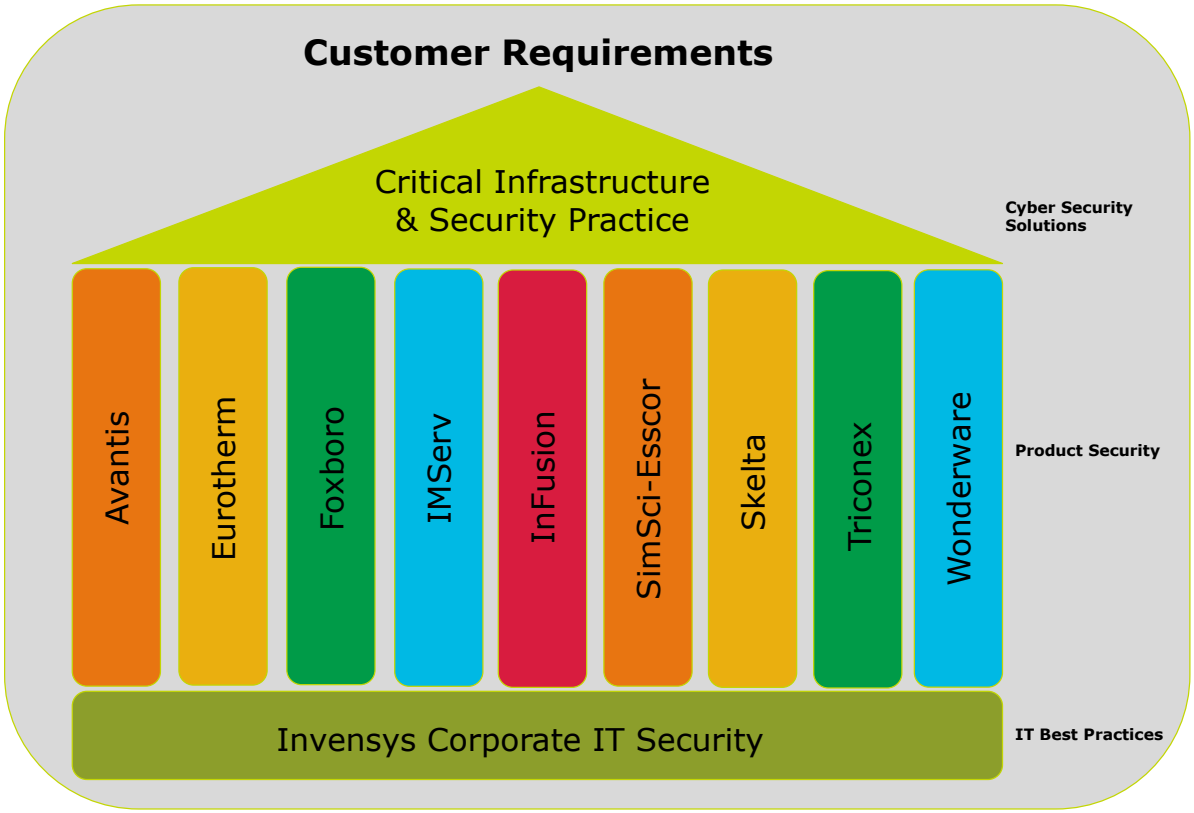
Cyber Security 'Best Practices' and Solutions

Table of Contents

1. Invensys Cyber Security

Cyber Security DNA

At Invensys, security is a primary focus in all development efforts to ensure that we meet our customer's requirements. The Invensys cyber security team builds on the firm corporate IT security practice and the cross portfolio product security development, delivering complete integrated security solutions and security programs for our client's entire plant and infrastructure. With this alignment, it ensures that our Cyber Security solutions reflect the best Invensys has to offer. The Invensys cyber security team has years of specialized Cyber Security experience and extensive industry knowledge. When combined, the Invensys cyber security team can deliver Cyber Security solutions for any regulatory or industry requirement facing customers today.



Cyber Security Portfolio

The Invensys cyber security team lifecycle approach ensures that the compliance solution is network and control system agnostic. The Invensys cyber security team divides the lifecycle of any network system into four distinct stages, explained below.

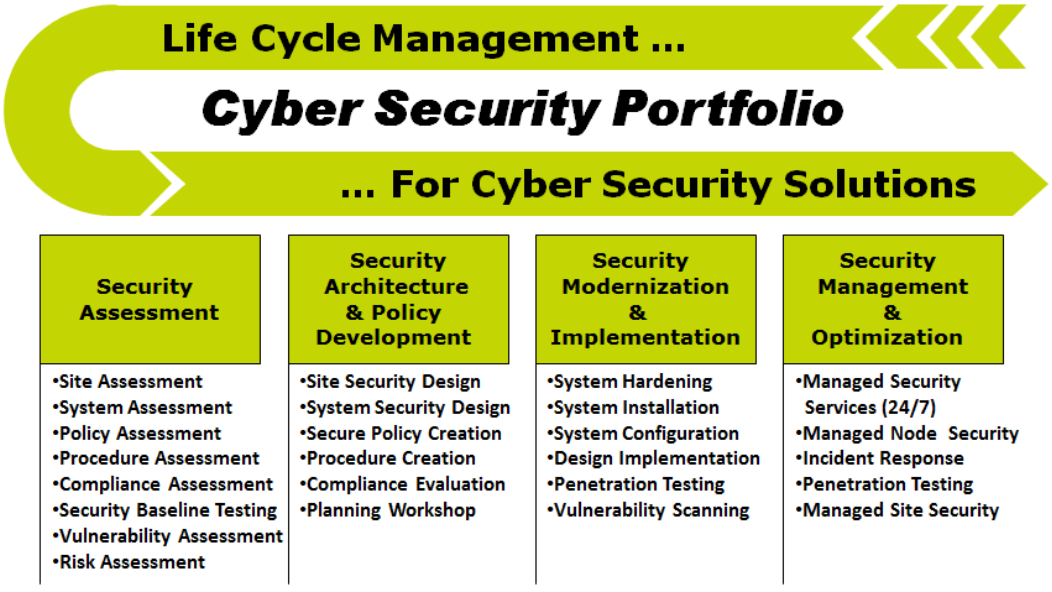
Stage 1: Assessment & Planning
The Invensys cyber security team reviews the current network, identifies any problems or issues, and suggests areas for improvement.

Stage 2: Development of Architecture & Design
Using an assessment or plan as a guideline, The Invensys cyber security team identifies what needs to be implemented and develops the detailed designs required to make it happen.

Stage 3: Implementation & Modernization
The Invensys cyber security team takes the network design and turns it into reality through the procurement, staging, and commissioning of the client's new or system upgrades.

Stage 4: Manage & Optimization
The Invensys cyber security team works closely with the management of the network, providing a mechanism to improve and optimize the continuously changing landscape of network usage.

The Invensys cyber security portfolio is flexible enough that it can be used in its entirety or implemented by any individual solution set, providing a comprehensive yet scalable solution to Cyber Security Compliance.



Please go to http://iom.invensys.com/CyberSecurity to learn more about the Invensys cyber security team and Cyber Security solutions.

2. Cyber Security Best Practices

Cyber security best practices are intended to provide guidelines on network security that will not only reduce external threat vectors, but also internal. Items are presented in order of priority.

- ☐ Always apply and maintain the latest Invensys-authorized Operating System (OS) and application patches.
  - Download updates directly from the patch source or via secure file server.
  - Assess which patches are required for each individual asset and apply as necessary, ensuring deployment does not impact operations.
  - Ensure all required patches have been successfully applied.
  - WITHOUT applying the current Invensys-authorized patches, individuals will be increasing the attackable surfaces of individual DCS workstations and servers.

- ☐ Always use current anti-virus definitions.
  - Ensure that the latest anti-virus definition files have been downloaded and run from the Invensys Support Website.
  - Verify through the McAfee client that the update was successfully installed.
  - Test new DAT in a test bed environment, prior to release into production environment.
  - WITHOUT keeping anti-virus current, the servers and workstations will not have the current malware signatures, leaving the equipment vulnerable to current attacks.

- ☐ Update authorized application software.
  - Ensure application software such as Adobe, if authorized, is updated. File types such as *.pdf* are one of the top distributors of malware if not routinely updated.
  - WITHOUT updating third party software on the inventoried system, additional vulnerabilities will remain in place.

- ☐ Enable Network Anti-Virus / Intrusion Prevention System.
  - Ensure that the most current anti-virus definition files and Intrusion Prevention System policies are enabled on all capable network appliances protecting the second Ethernet networks.
  - WITHOUT using a device that incorporates intrusion detection system (IDS), you will not have a baseline of normal network activities versus an attack. Antivirus module will provide an alert and a secondary screen for network malware.

- ☐ Do not use a USB stick unless it has been scanned and confirmed that it is free of problems with the latest *dat* file.
  - Designate and use specific USB equipment where required.
  - If using USB equipment to bridge air-gaps, always use a specific designated station in conformance with DCS security policies.
  - WITHOUT restriction on USB devices, their portable nature can be used to compromise your security perimeter.

- ☐ Harden Servers and Workstations. Hardening Non-DCS assets is a requirement and typically will not have negative effects on the DCS. Hardening DCS assets may be performed and will vary from Non-DCS asset hardening.
  - Ensure all software and hardware patches and updates are current.
  - Run A/V scans.
  - Disable all unused ports and services.
  - Harden Bios.
  - Use static IP addresses, disable DHCP on the interfaces, and disable unused interfaces.
  - Disable NetBIOS, unless specifically mandated by the IT department; disable NetBIOS over TCIP/IP (via WINS tab).
  - WITHOUT hardening servers, there is greater risk for attacks. Hardening reduces the attackable profile of the system.

- ☐ Change default “admin” passwords.
  - Use strong passwords consisting of more than 6-8 characters using special characters when applicable.
  - WITHOUT policies to ensure that “admin” passwords are changed, individuals can use “admin” passwords to escalate their privilege levels. Automated attacks by malware using “admin” passwords are prevalent.

- ☐ Control User Rights.
  - Verify that **only** authorized accounts are members of the local system administrators group.
  - Do not use accounts across domains.
  - When applications cannot use special characters, a service account should be created with authentication compatible with the application.
  - Wherever Group Policies are in use:
    - Change local system administrator passwords.
    - Implement password aging, history, and complexity requirements.
    - Ensure that Restricted Groups policy is enabled and used.
  - WITHOUT policies that specify user privilege criteria, individuals can receive privileges beyond those required for the task at hand. If too many users have elevated privileges beyond their needs, malware can use this as threat vector.

- ☐ Always implement Backup and Restoration.
  - Use a network backup repository.
  - Back up the network repository to a geographically disperse secondary storage site for disaster recovery or to removable media that can be stored off site.
  - If removable media is elected, then a rotation policy should be implemented to ensure that multiple copies of the backup exist off site.
  - Periodically conduct recovery exercises using test bed equipment.
  - Determine relative storage capacity available and automated a backup schedule for individual workstations and servers.
  - WITHOUT implementing a back up policy, customers will have no recourse to restore to a condition prior to an attack date if required.

- ☐ Take inventory of network assets.

- Keep inventory current of all network assets and status.
- Update inventory as network changes are made to both hardware and software.
- Run network scans to collect asset information (log files, etc.) where authorized. Non-DCS assets typically may be scanned without issues but DCS asset scanning should incorporate a limited tuned methodology for scanning DCS assets.
- Run regular network audits to ensure all systems are up to date.
- WITHOUT a network inventory, you do not have a baseline of what normal network assets are and that goes towards the network scan, complicating what are known devices and what are known patches. Knowledge of what specific network firmware is running and what network security equipment is present can be critical in determining whether or not vulnerabilities exist.

☐ Use physical network isolation when possible
- WITHOUT using physical network isolation, cross contamination of the DCS platform is possible from the corporate system.

☐ Use logical network segmentation (secure zones) when possible with strict Firewall Rules.
- Isolate and control flow of information between Business Network(s) from PCN through use of firewalls.
- Require strict firewall rules with specific (/32) source, destination, port, and protocol.
- Use DMZs
- WITHOUT using a secure zone, there will be no buffer before the network traffic traverses into the DCS network.

☐ Enable Firewall Logging.
- Ensure that all firewall policies protecting the Process Control Networks (PCN) and supporting infrastructure have logging enabled.
- Monitor firewall logs as appropriate, paying special attention to locate potentially malicious or abnormal traffic.
- WITHOUT firewall logging, you will not have visibility into dropped traffic or attacked traffic.

☐ Use Network Management Systems (NMS).
- Implement NMS to provide system audit and logging.
- Monitor system logs for failed login attempts.
- Generate and review reports for abnormal events.
- WITHOUT using NMS, there will not be a consolidated location for viewing all logs. The NMS system reports provides consolidated insight to all systems, which is invaluable for day-to-day operations and in the event of a cyber attack.

☐ Don’t click links or files that aren’t verified.
- DCS assets should not have internet access; some Non-DCS assets may have outside DCS access to business network website interfaces. Even business networks could be compromised, so verify all access leaving the DCS network to un-trusted networks.

- Ideally, the DCS network should be isolated from internet connected networks.
- WITHOUT policies restricting web access, users can potentially comprise the security perimeter by clicking on malicious links and installing unauthorized software.

☐ In the event of a Cyber Incident:

- Create an Incident Response Plan before an Incident so that you are prepared in the event of an Incident. Steps that are typically part of incident response plans are:
  - *Do not* start updating anti-virus.
  - *Do not* start running anti-virus patches.
  - *Do* get a triage team together.
  - *Do* get copies of all the logs.
  - *Do* make a VM image of the affected system.
- WITHOUT an incident response team and procedures, the opportunities to collect the forensic evidence required to determine the attack vector and point of origin can be lost or compromised, depriving the client the opportunity to work with the antivirus vendor and other agencies.

☐ Download and run latest McAfee Stinger tool

- WITHOUT collecting the necessary forensic evidence to work with the antivirus vendor, the client may not detect the variant that was not completely remediated by the Stinger tool.

3. Cyber Security Solutions

3.2 Cyber Security Workshops

3.1.1 Active Directory Workshop

Active Directory (AD) is a technology which provides a central location for access to user information for a given network. Central user account information provides authentication, authorization, password management, and updates enforcing security policies for computers that are part of the active directory domains. The Active Directory workshop will provide a matrix of users and a check list for verification.

The following AD requirements will need to be addressed and/or implemented:

- Identify and document the client's user and security group requirements.
- Identify and document external network connectivity requirements (if any).
- Identify and document the client's corporate security requirements.
- Identify and document future I/A requirements or future additions.

3.1.2 Cyber Vulnerability Assessment

A cyber vulnerability assessment will identify attack vectors and risks associated with cyber attacks and provide a unique approach of reviewing particular site and system vulnerabilities.

The vulnerability assessment feature will perform numerous comprehensive checks on clients' systems and allow clients to analyze the state of their network security, what the risks are, how exposed their network is, and how to take action before it is compromised.

The vulnerability assessment must be run on offline systems and depends on the availability of the assets as granted by the client.

3.1.3 Electronic Security Perimeter (ESP) Definition Workshop

This workshop will help clients identify Critical Cyber Assets (CCA), CIP Protected Cyber Assets, and Non-CIP Protected Cyber Assets to limit the number of CCAs and reduce the size/number of NERC CIP Electronic Security Perimeters. Benefits from cyber security workshops not only include technical solutions but include bringing together stakeholders from various groups in an open forum to identify and resolve issues for multiple viewpoints.

CIP002 R1, R2, and R3 call for the identification of Critical Assets and Critical Cyber Assets which sets the stage for all subsequent parts of NERC CIP standards. Therefore, mistakes in identifying the CIP Protected Cyber Assets can have a drastic impact in accurately identifying the ESP, and ultimately meeting compliance.

Invensys cyber security consultants will work with client-designated staff to establish a list of CCAs, CIP Protected Cyber Assets, and preliminary Electronic Security Perimeters limiting the number of Cyber Assets located in the ESP.

3.1.4 Site Assessment

A Site Assessment will establish the current architecture, security posture, and profile of all assets to be assessed within the systems network and will result in a network drawing with a system baseline scan.

In order to ensure optimal network performance, the Invensys cyber security team will submit a budgetary proposal to perform an assessment of the Process Control Network (PCN) at the client's site. Consultants will conduct a comprehensive technical network review of the current PCN infrastructure, which will provide the client with necessary information to make decisions relative to critical network management changes, including future growth requirements (both hardware and software), expense control, technology enhancements, configuration control, and proactive network maintenance.

3.1.5 Technology Assessment

The Technology Assessment workshop will help the client develop a roadmap for the secure network support of current and future business and industrial control system requirements. A secondary network is essential in providing an infrastructure to host the security solutions detailed in this document.

Users will be able to design a secondary network in support of cyber security management requirements for centralized management of:

- Backups
- Anti-virus management
- Patch management
- Event management
- Network performance monitoring and historical data reporting
- Security event historical data and reporting
- Active directory access controls
- Secure remote access relay server
- Plus support of future requirements

Consultants will establish the current architecture, define the desired security posture, design the required architecture to achieve the desired security posture, and outline a migration path in conjunction with the client's constraints.

3.2 Cyber Security Solutions

3.2.1 Hardening Services

System hardening documentation is a systematic process of documenting the secure configuration of systems for protection against unauthorized access while making systems more reliable.

Hardening is a procedure that updates patches and anti-virus software and disables unused ports and services. System hardening is necessary because default operating system installations focus more on ease of use rather than security. Most systems can have security measures enabled that will make them suitable for high security and high reliability environments.

3.2.2 NERC GAP Analysis

The NERC GAP Analysis includes a review of the client's current system in accordance with NERC CIP compliance guidelines and will result in a GAP analysis document that will aid in further defining the NERC compliance program.

The Invensys cyber security team will review the client's NERC CIP program, document the gaps between current state and compliant state, and suggest a remediation plan to bring identified gaps into compliance.

3.2.3 Event Logging

The ability to log events on the network is a critical tool for tracking and analyzing cyber security events for troubleshooting, remediation, and analysis. I/A Cyber Assets (Workstations and Switches) will forward security events to a central monitoring server. The central monitoring server will collect data from the various systems, provide notification on selected events, and act as a repository to allow the data to be analyzed at a later date. In addition, system logging will accommodate SYSLOG, SNMP TRAPS, and Windows Events.
Implementing logging requires the following actions:

- Invensys cyber security consultants will meet with designated customer staff to determine logging requirements for Cyber Assets (Workstations and Switches) and create a logging plan for implementation.
- A central monitoring server will be implemented for:
    - Assets supporting the sending of SNMP and SYSLOG messages to send various authentication, access, and log messages to this server
    - Windows events collection for Windows OS systems

3.2.4 Patch Management

Patch management is an important feature because missing security patches are one of the main reasons for network security breaches. The Invensys cyber security team eliminates this risk by providing on-demand or fully automated detection and installation of missing patches.

Patch management enables administrators to manage Industrial Control Systems and Microsoft patches and service packs for all languages supported by Microsoft. Patch Management also provides features like patch rollback and uses an existing WSUS patch repository.

Invensys cyber security consultants will work with client-designated staff to integrate the patching solution into an ongoing Cyber Asset patching program for I/A Windows Cyber Assets as well as create and update custom patch scanning profiles, perform training sessions, and document the patch management solution.

The Invensys cyber security team will set up and verify scanning host files for patching Foxboro I/A workstations by creating:

- scanning host files according to I/A Windows Cyber Assets by unit number, operating system, and Service Pack (i.e. Unit 1 Windows XP SP2)
- scanning host files listing I/A Windows Cyber Assets by unit number
- creating scanning host files listing I/A Windows Cyber Assets by operating system and Service Pack number

3.2.5 Remote Relay Access Server

A Remote Relay Access Server will secure Remote Access associated with remote I/A views, remote HMI access, and Compliance/History Cyber Assets located in the Electronic Security Perimeter Zone.

To protect Cyber Assets located in the ESP Zone from Business Network access, Invensys cyber security consultants will deploy an intermediate access platform as a relay server (Remote Relay Access Server). Deploying a Remote Relay Access Server prevents direct access to the Data Acquisition, Compliance/History, and DCS secure zones.

Remote access may be required to do the following:

- Perform administration functions
- Run diagnostics
- Perform configurations
- Allow for non-operator observation and non-routine or infrequent control

3.2.6 Access Control Firewall

Cyber assets associated with process control are often required to share information with assets on both trusted and untrusted networks. To prevent cyber attacks, our cyber security solution will implement a zoned network approach, which means assets with similar roles and security will be grouped together to form Secure Zones. Using least privilege rule sets, firewalls will control access between Secure Zones. Secure Zones will allow the client to create independent security zones that limit inbound and outbound access to their assets.

The items below are associated with cyber security and must be addressed in the design of the Plant Control Network (PCN) Secure Zone:

- Controls for restricting access to PCN assets from Corporate Network assets, including Port and IP restrictions for source and destination
- Controls restricting access to Corporate Network assets from PCN assets, including Port and IP restrictions for source and destination
- Network Address Translation (if required)

3.2.7 Managed Security Services

Process control networks are specialized environments that require mission-built solutions and widely-used solutions for securing IT systems that are typically inappropriate for the process control environments. While some standard security tools and techniques can be used to protect process control systems, careful deployment or tailoring is necessary. In response to these threats, the Invensys cyber security team has taken its industry experience and market-leading Managed Security Service services from Integralis to create a Industrial Security Monitoring Solution that is built from the ground up to meet the needs of Process Control Systems.

The following items are examples of why Managed Security Services are required:

- Co-managed security monitoring solutions augment existing staff and provide 24/7/365 security professionals for monitoring, reporting and critical event alerting.
- Health monitoring and reporting of all firewalls within the DCS network help ensure systems are protected.
- Intrusion detection capability detects intrusions and intrusion attempts at the electronic security perimeter.

3.2.8 Standard Operating Procedures

The cyber security standard operating procedures serve many roles in a successful cyber security program, including:

- Establishing the purpose for deployment
- Defining expectations
- Defining the scope of systems to be included
- Identifying the controls and procedures necessary to achieve the desired expectations

The standard operating procedures serve as the basis for design and deployment of a cyber security program and all associated works.

3.2.9 Policy and Procedure Development

Invensys cyber security consultants will interview designated client staff, review relevant documents, and use security best practices to create cyber security policies and procedures for the client's cyber security program. Creating cyber security policies and procedures will use the following work flow:

1. The client will securely transmit all available system information, policy information, and cyber security documentation for Invensys cyber security consultants to become familiar with the environment before arriving onsite.
2. A team of two Invensys cyber security consultants will travel to the site for a period of one week to initiate the project and begin the data review and initial draft of the cyber security policies and procedures.
3. Invensys cyber security consultants may need to interview members of various departments to determine the extent and content of the cyber security policies and procedures. Consultants may need access to operations, maintenance, I&C, HR, local plant management, and senior management.
4. Invensys cyber security consultants will review the final draft of the cyber security policies and procedures with designated personnel for acceptance and approval (these reviews may be via phone conference or onsite). Consultants and client site personnel will determine which delivery method may be required as cyber security policies and procedures are delivered.