Intrusion Detection and Prevention Systems in the Industrial Automation and Control Systems Environment

Chris Martin
Senior Director Product Strategy
Industrial Defender Inc.
Agenda

- Overview of IDS/IPS
- Planning for IDS/IPS
- Architecture and Design Selection
- Implementation Recommendations
- Supporting after Deployment

Presentation based on Chemical Sector Cyber Security Program white paper titled “Intrusion Detection and Prevention Systems in the Industrial Automation and Control Systems Environment”
Definitions

- **IDS**: Intrusion Detection System
- **IPS**: Intrusion Prevention System

IDS/IPS monitors and detects malicious behaviors and identify suspicious patterns that can compromise the security of a computer system/network.

- IDS is a passive system; the system detects a potential security breach, logs the information and signals an alert.
- IPS is a reactive system; responds to suspicious activity typically by reprogramming a firewall to block network traffic or dropping traffic on the network.
Components of the System

- **Sensors which monitor activity and generate security events**
- **Security Information & Event Management (SIEM) system (or Console) to receive security events and manage the sensors**
  - Updates rules/signatures, software updates
- **Rules Engine**
  - Records the events in a database
  - Compares events to a library of rules and generates alerts based on the output
Types of IDS/IPS

- **Host based (HIDS/HIPS)**
  - Small software programs (agents) that reside on a host
  - Monitor metrics such as access, file modification, removable media insertion, performance, etc.

- **Network-based (NIDS/NIPS)**
  - Separate appliance
  - Monitors network traffic, rogue devices, internal attacks

- **Protocol-based**
  - May reside on NIDS or host
  - Monitors use of communication protocol between systems

- **Application-based**
  - Reside on host
  - Monitors metrics such as process terminations, abnormal exits, message queues, etc.
Reasons for IDS/IPS

- Loss of Intellectual Property
- Industrial Espionage
- Loss of Process Control
- Loss of Data Integrity
- Sequence of Events Recording

➢ While not a silver bullet, properly configured IDS/IPS is an integral component of a defense-in-depth solution
Planning for IDS/IPS
Organizing for Success

**Corporate Stakeholders**
- Corporate Security
- Corporate Manufacturing
- Corporate IT
- Audit & Compliance

**Site Stakeholders**
- Someone who understands the current network architecture.
- Someone who understands the real-time control system.
- Someone who represents manufacturing, production or energy management.
- Someone who represents the site IT organization.

➤ Each company and site that is considering technology will be at different starting points with respect to process control architectures and the skill and staffing level of their process control and IT organizations. These two factors can significantly impact the cost of introducing IDPS technology.
Starting Point – Risk Assessment

- To examine the current risk state of the manufacturing control system and determine if IDS/IPS technology will significantly reduce the risk

- Steps in an Assessment
  - Network Architecture Review
  - Vulnerability Assessment
  - Penetration Testing
  - Red Team Testing
  - Compliance Gap Analysis
  - Disaster Recovery Plan Creation
  - Protection training
  - Cyber Forensics
Risk Assessment Steps

- **Network Architecture Review**
  - Determines what systems are in place in the control system environment and how they are integrated
  - Typically involves interviews and reviews of existing documentation
  - Critical step in achieving NERC CIP compliance for asset owners in the electric power sector
  - *Result*: Logical network diagram complete with security zones for each unique environment
Risk Assessment Steps

- **Vulnerability Assessment**
  - Must have knowledge of SCADA, DCS, PLC and other industrial control systems
  - Its possible mitigation of risks could turn out to be more disastrous than the risk itself due to unforeseen system impact
  - Balanced background in both operations and security
  - *Result*: Detailed Vulnerability Analysis with mitigation strategies, cost to repair, recommended next steps
Laptop Taped Under Server Cabinet to Sniff Passwords

Problem
In 2003, a N. A. power generation company performed a routine physical inventory of their control systems revealing one fewer machines than on the table of active IP addresses. A subsequent detailed search revealed a laptop taped under a server cabinet running password sniffing software. The laptop was traced to a returning contractor.

Consequences
Potential loss of confidentiality of control system passwords leading.
Potential misuse of control system and loss of production.

Key Control System Recommendations
Technology - Network device change detection
Policy - Equipment check-in/check-out policy

Source: Industrial Defender Contact
Risk Assessment Steps

- **Penetration Testing**
  - Use goal-oriented testing on only individual systems of interest
  - Use the same techniques as a hacker would use
  - Result: Proof-of-Concept of specific vulnerabilities with counter measure options
Architecture and Design
Initial Design Considerations

- Have network as-built diagrams available
  - Can be verified during an assessment

- Logical segmentation of networks and user authentication should already be in place

- Fundamental Decision: Proactive or Reactive system?
  - Is timely detection, alarming and an audit trail sufficient?
  - If proactive, need to consider consequences of false positives

- Impact of monitoring, managing and supporting the system
  - Different design approaches are likely to require different openings through segmentation firewalls
Architecture
Methods of Detection

- **Misuse of System Protocol**
  - Misuse detection monitors for deviations in normal protocol.
  - This method is useful to detect attempts by a user or application attempting to gain unauthorized access to a system.

- **Signature-Based Detection**
  - A basic form of network intrusion detection is based on pre-identified attack signatures.

- **Anomaly-Based Detection**
  - By using base lining and statistical methods, anomaly detection finds irregular activities that differ from the normal baseline pattern.
Host versus Network-Based IDS/IPS

**Host-Based**
- Two common methods of implementing are agent-based and logging analysis
- Agent-based deployment requires specialized programs to be installed on the host system
- Logging analysis implementation relies on host logs being pulled or pushed to a logging system

**Network-Based**
- Placed on one or multiple points across the network
- Sniffer agent analyzes network packets that contain data, including the message and header that identify the sending and receiving parties
- Network attacks such as IP spoofing, packet floods, and denial of service, are better detected through packet examination than host-based IDS
HIDS: Host Intrusion Detection Sensors

- Soft sensors should allow fine grained monitoring of both control applications and host
- Detect any unusual activity on the host
- Purposed built for control environments
  - Unidirectional communication
  - Totally passive
  - Low impact on *legacy* platforms
  - Tunable, with up to 8 priority categories
  - Proven track record of installation on live production systems with no impact
- Redundant path support
- Can be locally or remotely installed
For Security and Performance Monitoring

**Security**

- **Control intrusion detection**
  - Large # of signatures

- **Control system integrity**
  - Device addition
  - Device masquerading
  - Device continuity
  - Network equipment status

- **Host access monitoring**
  - Failed log-in attempts
  - Failed password change attempts
  - Password age status
  - Root user count
  - Total user count

- **Host file monitoring**
  - File deletion, modification
  - File permission changes
  - File checksum mismatch
  - Removable media detection

**Performance & Integrity**

- **Host performance**
  - Resource usage (CPU, disk space swap space)
  - Network traffic counts
  - System uptime
  - Identification (name, OS version, hardware type, IP address)
  - Event log status

- **Control application integrity**
  - Abnormal program exits
  - Control application shutdown
  - Process terminations
  - Watchdog status
  - Message queue status

- **Soft sensor heartbeats**
Industrial HIDS Functionality

- Array of subagents can detect virtually any dangerous or suspicious behavior
- Rules engine allows normal and required behavior to be specified
  - Alarms only raised on abnormal behavior
  - Minimizes network traffic
Anomaly Detection Examples

- Disgruntled Employee
- Trojan
- Virus
- Illegal Software
- Vendor modification
- Software malfunction

- New file
- New socket
- New process
- Removable media insertion
- File modification
- Socket disappearance
Host-Based IPS Differences

- Preventative measures can be enabled or disabled as needed
- Installed on each local host, with locally stored policies and rule sets, in order to prevent real time events
  - each host agent will require some tuning within an industrial control system
- Based on a company’s needs, the agents will need to send the activities of the host and actions of the agent back to the manager
Host Security and Performance Monitoring

Comprehensive security and performance metric monitoring
Hacked Historian becomes Spam Server

Problem

In 2004, a power generation company in the U.S. had a historian connected to the Internet to receive time syncing data (NTP). The server was compromised and used as a spam relay and a file server.

Consequences

Operators had slow display refresh rates and there was a huge bandwidth usage increase. Additionally, spam servers eventually become blacklisted in the Internet community. Valid emails from that company could be rejected by other companies subscribing to blacklisting services.

Key Control System Recommendations

Technology: Firewall, IDS/IPS, and file, process and bandwidth monitoring

Policy: Have dedicated NTP servers

: Put historians in a DMZ

Source: Industrial Defender contact
Laptop Infects Power Generation Company

Problem
In 2005, an employee of a European power generation company bypassed corporate firewall security and brought a laptop infected from home into work. The laptop spread a worm throughout the network. IT attempted to remove the worm, but when HIDS was installed to control system, additional instances of the worm were detected.

Consequences
Worm cleanup efforts sapped productivity from both IT staff and users. Control system integrity was at risk.

Key Control System Recommendations
- Technology - IPS, IDS and network segmentation
- Policy - Secure policy for portable machine connection to network
  - Up to date patching policy

Source: Industrial Defender Contact
Network Intrusion Detection System (NIDS)

- Monitor networks for malicious activity
  - Internally launched attacks
  - Unauthorized traffic
  - Detect additions and changes to devices on the network
  - Identify rogue devices
  - Secure authorized devices
  - Extensive signature library identifies broad range of attacks

- Uses include:
  - Security
  - Performance
  - Compliance
Industrial Protocol Signatures

● Malformed Packet Attacks
  - One of the most common form of attacks, attacker can send non-standard packets to crash or even take over a control system host or PLC
  - One form of this type of attack, buffer overflow, responsible for many worms
  - NIDS checks for malformed packets by checking that field structures and data values conform to protocol standards

● Denial of Service Attack
  - Prevent controller or PLC from performing normal operations
    - Ex. LAND attack: TCP/IP packet sent with same destination/source, thus PLC will try to respond to itself

● Replay Attacks
  - Requires no knowledge of protocol; copy of control traffic continuously rebroadcast over control network
NIDS also used for Performance Monitoring

- **Protocol Faults**
  - Many protocols give standard fault responses
  - NIDS generates alarms on common industrial protocols
  - All alarms logs and can be used to locate source of faults

- **Controller Resets**
  - Typically within control protocols in LANs, connection started and maintained indefinitely
  - Reset packets or new connections can indicate instability of control protocol
  - NIDS can actively monitor presence of reset packets or new connections

- **Invalid Configurations**
  - Configurations can become outdated, such as when packets sent to non-existent addresses
  - When OEM does not implement the full range of commands
  - NIDS can alarm on valid but unsupported commands
NIDS used to ensure Compliance to Standards

- **Configuration File Activity**
  - Often configuration file changes force reboots to controllers
  - NIDS can detect upload/download events and is recorded in a SEM database

- **Control Command Enforcement**
  - Many sites restrict PLC register reads/writes
  - NIDS can monitor Modbus, OPC or other protocols and report on disallowed read/writes

- **Login Recording**
  - Logins/Logouts/Failed Logins are recorded and optionally alerted

- **Default Password Usage**
  - Many control systems installed with default passwords
  - Optionally alert on their use either locally or via remote access protocols such as ftp, telnet, etc.
Control Network Security and Performance Monitoring

Protocol and Network Device Monitoring with No Network Latency
Network-based IPS

- Quite different from NIDS
- When in prevention mode, will drop suspicious traffic
  - Need to consider the ramifications of false positives, which could potentially drop valid control signals
Plant Perimeter Protection

Firewall, VPN, Antivirus, Intrusion Prevention in a Single Device
Worm Introduced by VPN

Problem
In 2004, while pilot testing a SEM and NIDS sensor in a large US power generation company, the Nachi/Welchia worm was detected scanning the control network. Using information from NIDS, the source of the infection was tracked to an infected home laptop. The user had valid privileges to use the VPN to bypass the firewall. The worm passed over the VPN, past the firewall into the control system.

Consequences
Corporate IT had been aware of the worm, but had not informed the control system staff. It took several days to eradicate the infection.

Key Control System Recommendations
Technology: IDS, perimeter/subsystem IPS
Policy: Prevent VPN access to control system with IPS/AV scanning

Source: Industrial Defender Contact
Host Antivirus Crashes SCADA System

Problem

In 2006, an AsiaPac city rail system installed McAfee antivirus on its SCADA servers. McAfee automatically enabled Windows firewall on both machines. This stopped SCADA synchronization packets between the redundant servers.

Consequences

Buffers built up over several months until the primary server failed and the redundant server came online with an unsynchronized configuration. City rail stopped for several hours. 4 people spent a full week trying to track down the problem. The organization was forced to put out a press release on the incident.

Key Control System Recommendations

Technology : Network antivirus, non-intrusive monitoring.
Policy : Use control specific technology
: Fully test changes before implementation

Source: Industrial Defender Contact
Closing Caveat on IDS

- Although IDS may be an integral part of a plant’s overall system security, they do not provide complete protection from previously unknown threats or vulnerabilities.
  - Still need strong perimeter protection; complements firewalls but does not replace them
  - Can’t compensate for weak authentication procedures

- **IDS capabilities are highly dynamic, and continue to evolve**
  - Prudent to consider flexible IDS solutions that can be upgraded
  - Need to have a management system in place

- **Availability of control systems is of the utmost priority, trumping confidentiality and integrity**
  - Response procedures will vary, based on the value the organization places on each manufacturing asset
Other Planning Considerations

- Continuity of Business
- Self Audits
- Data Retention
- Classification of Date
- Chain of Custody
- Authentication
Implementation Recommendations
Design Decisions for Network Monitoring

- **Prevention versus detection?**
  - If prevention then IPS device is deployed in-line
  - Some IPS devices can fail open thus allowing traffic to pass
  - if feature not utilized, then failure will prevent traffic to pass through

- **Type of traffic to be monitored?**
  - Control network? Corporate network/internet facing? Both?
  - Typically recommend NIDS to passively monitor PCN, NIPS on the firewall at the plant perimeter/corporate side
Sensor Sizing

- To be effective, the IDS/IPS sensor needs to be sized appropriately.

- Size network sensors based on the current network utilization statistics.

- Several aspects of the network architecture that should be considered are:
  - Overall network baselines, such as total packets/sec.
  - Network segments to account for the case of load balanced or multi-path circuits.
  - Making sure the sensor has enough ports to be operated on the managed network segment, whether it is a dedicated or shared VLAN.
Host IDS/IPS Design

- Again, prevention or detection?
  - Must consider false positives such as processes starting or sockets opening

- Which Hosts to monitor? Risk assessment will help in the determination.

- What metrics to monitor?
  - Temptation to monitor all, but can introduce operational implications
  - Network bandwidth utilization must be considered for logging based HIDS which send events to the SIEM
Network Access Recommendation for NIDS

- In a switch network, typically connect IDS sensor through a network tap or mirror port

- Diagram below is a generic example of port mirror implementation. Tap placement is typically between the switch and the PCN firewall
Sensor Placement

• As a general rule of thumb, placing the sensor as close as possible to the assets it is protecting can provide several benefits
  – it can reduce the amount of changes and tuning needed
  – decrease the analysis overhead
  – lower the complexity of configuration
  – potentially decrease the amount of false positives
Placement of Management System

- Typical NIDS implementations will often have a dedicated network interface for management
  - used for managing the system
  - sending events if a central console (SIEM) is used

- Basically 3 choices on where to locate the management
  - On the corporate network
  - On the process control network segment
  - On a DMZ segment on the process network
Management Interface on Corporate Network

- The least appealing option
- Alternate path to the process control area
Management Interface on Monitored Segment

- Less than optimal for several reasons
  - Sensor may require additional tuning to filter management traffic
  - Ports may need to be opened to support signature updates
  - The sensor may require additional access controls
Management Interface on DMZ

- Optimal placement but does add some complexity
  - an additional network may need to be added to the process control firewall
  - Additional rules for management access, signature updates, etc. may also be required to access the management interface from the corporate network
Supporting after Deployment
System Operations

- **Tuning**
  - Not an installation event but a lifecycle
  - Small environment changes can precipitate need to tune
  - Can range from editing a file to point-and-click via a GUI

- **Signature Updates**
  - Typically requires internet access (Alternate approach: “store-test-forward”)
  - Since protecting control systems, have the opportunity to filter out some to accommodate system capacity
Event Management

- **Aggregation:** Events come from many sources such as IDS, IPS, firewalls, syslogs
  - Support team should consider maintaining a process to support secure receipt, tracking, escalating, and addressing these events on a 24x7 basis

- **Correlation:** Not all events generated are meaningful by themselves
  - Technology exists to establish relationships from multiple events to establish a single significant event
  - “Thresholding” should exist to create alarms based on a number of individual events
Response Plans

- Acquire and inventory the tools needed for intrusion detection, including ID software, backups and file system recovery tools
- Train staff on how to deal with intrusions. This can be through SANS courses, CERT training, vendor courses
- Form a response team
- Build an offline kit of standard system utilities
- Document all incidents carefully; incident reporting should include:
  - person discovering,
  - target systems,
  - purpose of attack
  - Parties notified
Any Questions?