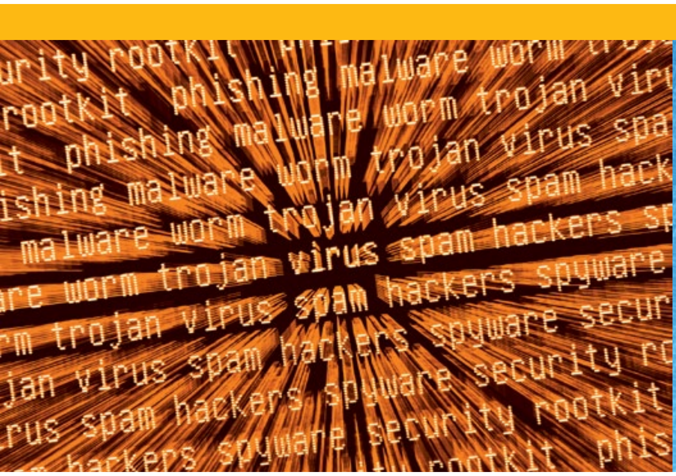
WHITE PAPER


phishing malware worm trojan virus spam hackers spyware security rootkit

Report from the Field: Seven Best Practices for Automation System Cyber Security and Compliance

INDUSTRIAL DEFENDER®

Industrial Defender, Inc.
16 Chestnut Street • Suite 300
Foxborough • MA • USA • 02035

Introduction

Stuxnet. Smart grid. Duqu. Advanced persistent threats. Industrial espionage. There's no shortage of discussion about the challenges critical infrastructure operators face as they modernize their automation systems and become a more visible target to attackers. What has received less attention though, are the underlying challenges organizations face in managing their automation and control systems in the midst of these market dynamics.

A recent study conducted by Industrial Defender has revealed that serious issues exist as these facilities strive to develop best-practice solutions for cyber security and compliance.

- The relationship between industrial operations and corporate IT continues to grow more complex. Substantial increases in connectivity between industrial and IT networks are expected over the next several years and there's a strong belief that industrial endpoint volume will grow significantly in the near term.
- On paper, responsibilities don't align with day-to-day activities. Industrial automation professionals have seen their responsibilities broaden from managing operations to managing security and, in some instances, managing compliance.
- Similar management requirements exist across security, compliance, and change management functions. The actions and activities necessary to support a security program may be strikingly similar to what's required for compliance management and operational management within critical infrastructure.
- Infrastructure operators are constrained in their ability to manage these overlapping requirements. This is particularly true when it comes to managing multi-vendor environments with assets from a mix of industrial automation suppliers.

These findings clearly point to important trends of blurring boundaries, increased complexity, overlapping responsibilities, and constrained resources. Thus, critical infrastructure owners should seek and embrace new, emerging administrative and technical best practices that respond to these trends by offering more effective and efficient management of the common elements underlying security, compliance, and operations.

Industrial Defender has performed over 100 security assessments of clients' mission-critical systems and networks. For the past 10 years, our professional services team has been focused on security issues relating to SCADA, EMS, DCS, and real-time process control systems.

This "Report from the Field" is the result of these hands-on, in-person consulting engagements and field deployments, vulnerability assessments, penetration testing, and compliance gap analyses.

Top Compliance Challenges and Best Practices

Through the many gap analyses we have conducted, Industrial Defender has identified seven major issues that appear more frequently across critical infrastructure facilities and the best practices required to solve them. These potential gaps in compliance arise from issues with personnel, access control devices such as firewalls, software patching practices, network isolation, access credentials, ports, and services, and unnecessary software.

1. **Inadequate Security/Compliance Staffing**

   Effectively addressing security and compliance standards requires dedicating adequate resources to the task.

   An essential first step that is often neglected is applying sufficient resources to successfully meet the goal. When a plant or enterprise commits to a rigorous cyber security program, the management work, such as coordinating gap analysis studies and managing technical feasibility exception (TFE) generation and submission, can be extremely labor intensive.

   This is addressed to some degree by the standard audit process that requires the participation of subject-matter experts (SMEs). The SME for physical security is typically not the SME for configuration management, and neither of those is the SME for personnel training, and so forth. Industrial Defender has repeatedly found that the amount of daily work to ensure success is underestimated and, thus, proves too large a task for the resources assigned at the start. A large portion of this work involves data collection and detailed report generation. Other notable tasks include TFE development and submission, hosting auditors, and more.

   Best Practice
   To address this issue, organizations should carefully consider the work needed to prepare for a gap analysis program. They should then assign an appropriate number of people, perhaps drawing from Corporate IT resources temporarily or by hiring more control system IT resources.

   In addition, critical infrastructure operators should investigate work-saving data collection, measurement, and reporting solutions, and then select one that meets their particular requirements. Such a solution can greatly reduce the data collection and compliance assessment work load.

2. **Insecure Perimeter Firewall and Router Configurations**

   Discouraging unauthorized access to your electronic security perimeter (ESP) requires secure firewall configurations and rules.

   Firewalls and routers are typically the access points to an organization’s ESP. The rules for routing traffic and the transparency of the traffic must be examined. For example, some organizations have not confirmed that the firewalls and routers are configured such that rules deny and log the traffic that is not predefined. While these rules should be documented and stored, many older firewalls typically lack the audit capabilities needed for security and compliance.

In addition, router access control lists (ACLs) — and the ports and services they enable — often allow all traffic from various devices, network groups, and object groups that reside outside of the ESP into the ESP. We have found that ACLs are often too permissive and should be restricted as much as possible to only the required hosts, ports, and services.

A third perimeter security consideration is the degree of transparency of traffic passing through access points. Many organizations, for example, allow clear-text traffic, such as telnet, rcp, rlogin, tftp, and ftp traffic, through ESP network firewalls, switches, or routers. Clear-text services could also allow an attacker to easily obtain credentials and other information through packet capture. The attacker could then use these valid credentials to further exploit the system perhaps using a man-in-the-middle attack.

Best Practice

The control staff should be able to generate reports of the firewall rules and the ACLs of the internal routers at any time and review them on a regular basis. This report will help achieve compliance by documenting the access allowed across the ESP. The report should include the source and destination IP information, the ports allowed, any time parameters and an easily understood description of the access. It can also include the approval of the access request. One of the biggest challenges for many organizations is to document the existing rules. Be sure to allow sufficient time for this review.

"All" or "any" type rules should be reviewed and pared down to the essential ports and services that are required for system operation. While it is possible that all ports and services are required, experience and practice suggests that the number of actual ports and services needed are a very small subset of the possible 65,535 TCP or UDP values. In addition, the rules should specifically state the ports and services that are required.

Regarding clear-text protocols, such as telnet, rcp, and rlogin, any unencrypted protocols should be phased out and replaced with secure administration protocols such as HTTPS, SSH, or SCP. With wireless, all traffic should be at least encrypted with WPA2 AES-based encryption with a strong key on wireless network devices used to bridge physical network segments. The network name should not be broadcast in order to make network discovery harder for an attacker. Disabling SSID broadcasts will not completely prevent an attacker from discovering the network name, but it will require more time and effort to discover it.

Here also, a compliance management tool that collects and reports on firewall data can save significant time and improve data accuracy. Such reports should list the firewall rules for a given device, on different devices, and at two different times. It should also support configuration and control management to aid in the timely review and tracking of firewall rules.

3. **Insufficient Patching**

Assessment and implementation of the latest software patches are required to help prevent malicious, unauthorized incursion into your ESPs and CCAs. This is particularly challenging for automation systems environments.

Vendor-supplied software patches frequently fix security vulnerabilities and improve usability or performance. Through our assessments, we frequently identified numerous missing service packs and patches on control system workstations and servers. In fact, the number of missing patches averaged over 20 per site. Patches for network devices and third-party applications are equally important to the security posture of SCADA networks.

Typically, systems are brought up to date when deployed. Ensuing patches are reviewed for applicability and compatibility, and are then applied as necessary. Some of the unapplied patches have been critical in nature and could allow an attacker who gets past the first line of defense to easily gain access to the control network. By taking advantage of an inconsistent patch policy, an attacker would be free to leverage gained access and use any number of easily obtainable, reliable exploits to take control of unpatched machines. This ultimately enables the attacker to gain the same privileges as the very people who provide technical support or have access to the control system from the corporate network.

Best Practice

Critical infrastructure operators should review their patch policy with an eye towards improving timeliness, regularity, and testing. These issues are critical because of the vulnerability of unpatched systems. Testing also is important because the systems being patched are critical control systems and should remain stable and available through the patching process.

We recommend that organizations work with their SCADA, DCS, and EMS system vendors on a regular basis to determine the patches that can be applied. These patches should be tested in a development or test environment prior to implementation on production systems.

One way to gain the advantage of a test environment without having to duplicate all existing hardware is to use virtualization. In a virtualized environment, patches can be deployed, tested, and reverted easily and quickly if trouble arises.

Monitoring the patch level of systems on a regular basis becomes significantly simpler and more accurate with a compliance tool that collects and reports on patch inventory. Additional security and compliance benefits accrue if the compliance tool can compare actual patch levels on a device to levels on a baseline or "gold standard" device.

Best Practice

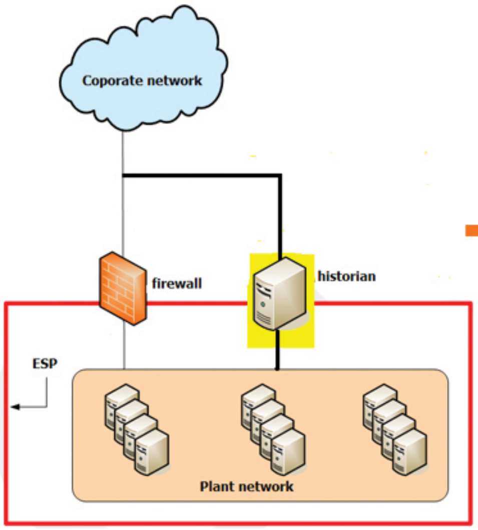
Despite best efforts, there may be times where patches cannot be realistically applied until months after the patch has been released. In this case, whitelisting can be used as a mitigation to reduce the possibility of malicious code from executing on unpatched machines. Whitelisting identifies all of the approved applications on a machine and then monitors the machine to ensure that only those applications execute. Reducing the number of allowed executables to only those required for normal operation allows an operator to more easily detect when anomalous behavior occurs.

4. Inadequate Separation Between Corporate and Plant Control Networks

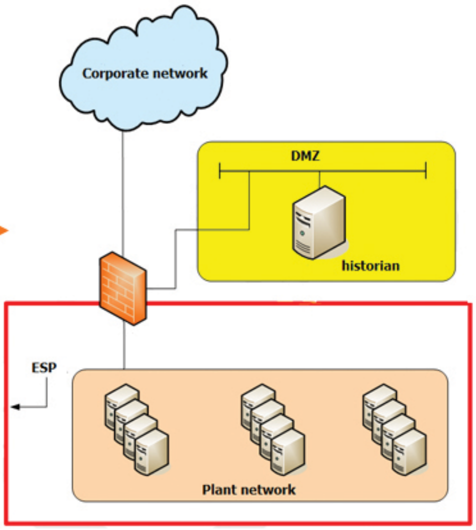
Keeping skilled attackers from traversing from a corporate network to a control network requires a strong network architecture that includes a control DMZ and re-architecting, dual-homed hosts so that they do not bridge disparate networks.

Many of our clients have implemented plant information systems (PIS) and historians. These systems aggregate control system information so the business can better direct operations toward increased profitability and productivity, and to conduct effective business planning. They also represent paths between the corporate and control system networks.

Upon closer examination of these systems, we have found host systems with more than one network card connecting the host directly to more than one network at a time (dual-homed; shown below left).



Dual-homed



With DMZ

A vulnerability in a dual-homed machine can offer an attacker direct access from the corporate network to the control network. Furthermore, these connections are often not audited since they do not traverse normal network infrastructure devices.

A typical response to this network configuration risk is to implement a control systems DMZ (shown above). However, the control system's ESP may well need to incorporate some DMZ devices.

Best Practice
Industrial Defender typically recommends that clients reposition dual-homed devices in the network or consider the implementation of a control systems DMZ to provide greater access control and auditing of the connections into and out of the device. The DMZ allows access from corporate, but maintains a level of separation from the control network. This separation will help prevent an attacker from freely accessing the control network in the event they find a security hole in the PI server or in Terminal Services.

If systems and data network machines exist with interfaces on the business network, they should be placed in a DMZ, which serves as the only gateway to the rest of the CCA devices. A control systems DMZ is considered security best practice and is recommended by NIST SP 800-82.

Reviewing network diagrams is the obvious way to identify network configuration issues, but larger networks change frequently making network diagram accuracy short lived. Maintaining current network diagrams manually is unnecessarily laborious and error-prone. Much greater efficiency, cost effectiveness, and accuracy would accrue from the deployment of a compliance management tool. This will automatically track device configurations (including network interfaces), periodically compare them with a baseline, and then issue an alert when actual data deviates from the desired baseline configuration.

5. Weak Passwords

Authorized access to accounts in the ESP must require strong passwords.

Weak passwords represent a common and severe vulnerability. We frequently find that weak passwords are in effect across systems and network devices that can be exploited to gain access. The overall use of weak passwords is usually discovered after successfully compromising the directory service domain controller and cracking the hashed passwords of nearly all the domain accounts (including administrator-level accounts). Additionally, weak passwords are found when default credentials, often deployed by a vendor on a vendor system or piece of software, are left in their default state.

Best Practice

Implementing and enforcing robust password policies across all environments will help ensure strong security. Rigorous password policies should be applied at the host and server level with local security policies on Windows and by configuring the Pluggable Authentication Modules (PAM) on UNIX variants. In addition, a centralized authentication solution such as Active Directory or LDAP should be considered to help enforce password policies and log access.

With respect to strength, passwords should be a minimum of eight characters long; consist of a combination of alpha, numeric, and special characters; and be changed at least annually, or more frequently based on risk. Some security experts advocate for even stronger passwords that are 12 to 14 characters, if permitted, and that mix upper- and lower-case letters if recognized by the system.

Regardless of password policies, a system that monitors and reports on the implementation of those policies adds significant value. A compliance system that actually examines the strength of individual passwords may be more intrusive than desired. However, one that at least automatically verifies that a given password policy has been implemented on a device is probably sufficient to determine compliance posture vis-a-vis password policies.

6. **Unnecessary Third-Party Products Installed with Weak Default Configurations**

Unauthorized traversal across an internal network is greatly hindered if unnecessary, weakly protected applications do not exist.

Accounts are considered default accounts if they were created by a vendor for maintenance or startup purposes. If left installed and available, these accounts can be used to access CCAs within a client's ESP. Industrial Defender has often found applications, database platforms, or other third-party software or firmware installed and running in default configurations with default accounts and default passwords still in place.

Microsoft, for example, creates a default administrator account automatically that is both the most powerful and most risky account on a system. The password lockout policy does not apply to the administrator and it is most likely to be the first account an attacker would attempt to crack. An attacker who successfully cracks the administrator password could take complete control of the affected system and possibly the network.

In another example, numerous machines in an Active Directory domain within the ESP have been found to be running the MS SQL Server services listening on port TCP 1433. These machines were also found to have the MS SQL Server `sa' account with a blank password. Such security oversights have been leveraged in penetration testing to execute administrator-level commands on various machines in order to gain administrative access.

Best Practice

The action for mitigating this compliance gap is clear: change any default user names to unique user names and change default passwords to appropriately complex unique passwords. With the Microsoft Administrator and Guest accounts, however, renaming the original accounts and changing the text in the description to eliminate anything that indicates that these are the Administrator and Guest accounts are insufficient. Default Administrator and Guest accounts can be discovered regardless of renaming because the underlying SIDs of the accounts remain the same. Thus, best practice here is to add a customer-specific administrative level account for each administrative user and disable both Administrator and Guest default accounts, where possible.

Collecting the current software inventory on a device could be done by running an installed applications report, but significant efficiencies can be realized with the use of a compliance management tool that automatically runs a device software inventory report on a predetermined schedule. The report would compare the actual software inventory on the device with a baseline inventory, highlight differences from the baseline, and then issue an alert.

7. Inadequate Ports and Services Documentation

Documentation showing that only necessary ports and services are open on a CCA demonstrates commitment to compliance and to reducing the penetration opportunities for an attacker.

An auditor will expect open ports and services on CCAs to be documented so that compliance with the requirement to close unnecessary ports and services can be determined. As previously mentioned, unnecessary ports and services are often enabled by default when devices ship from vendors. It is not uncommon to find services such as name, comsat, talk, uucp, finger, time, echo, discard, daytime, chargen, rquotad, ruserd, spray, walld, and rstatd enabled by default. Any unnecessary services expose a device to vulnerabilities and attacks that would normally not be available if the services were not enabled.

Leaving unnecessary services running provides a potential path for an attacker attempting to compromise the system. So, by only running services and software required to run the control system, the risk of attack is reduced. Critical infrastructure owners should work with their vendors to identify the ports and services required for operation and disable unnecessary services. Unfortunately, it is frequently very difficult to clearly document which ports and services are really necessary.

Best Practice

Inadequate ports and services documentation can be mitigated by identifying all ports and services necessary for the normal operation of each server and applying them to all hosts that need access. Next, disable all services that are unnecessary for normal operations to reduce the attack surface of a device. This hardening process is industry best practice for securing critical systems.

Once ports and services are reduced to those required for normal and/or emergency operations, customers need to frequently review ports and services to ensure that compliance is sustained. A compliance management solution that periodically collects data on the open ports and services on a given device and then compares that data with a desired baseline will dramatically improve security and compliance sustainability.

Conclusion

In this paper, we have presented a compilation of the most common threats to critical infrastructure security and compliance and, in each case, discussed best practices that will help mitigate those threats.

The report also highlights where and how an automated compliance and change management tool can help protect against attacks. Organizations can continue to correct cyber security and compliance issues the old-fashioned way with high labor and expense, or they can address these problems more rapidly, efficiently, and accurately with a tool, such as Industrial Defender's Automation Systems Manager (ASM), that can be customized to meet specific requirements and environments. In short, achieving and sustaining security and compliance, while managing the complexity and frequently changing automation system environment can be fast, efficient, and cost-effective with a minimal investment.

ASM consists of Monitor, Manage, and Protect solutions that address the change management, security, and compliance issues operators typically face. Each solution includes a comprehensive suite of software applications, infrastructure, and services to specifically address automation systems.

- **Monitor** collects event data from industrial endpoints and provides centralized event logging, correlation and archiving, and consolidation of log data for analysis and forensics.
- **Manage** builds on Monitor and offers capabilities for data capture from automation systems that are unmatched in the industry. It automatically collects configuration data from heterogeneous industrial endpoints, tracks changes to configurations, software, patches, and user accounts, and provides automated policy management and exception identification.
- **Protect** includes all of the functionality of the Monitor and Manage solutions, plus provides policy enforcement to prevent rogue applications, malware, memory exploits, and attacks that originate from removable media.

ASM helps critical infrastructure operators ensure the reliability and availability of their automation systems and by extension, their key industrial processes. We enable these benefits through our considerable domain knowledge and by capturing and leveraging commonalities in data, processes, and technologies that exist across security, compliance, and change management activities.

Whether through manual labor, automation with multiple tools, or automation with a single solution, the threats to security, compliance, and change management and, therefore, to critical infrastructure reliability and availability, must be addressed. These best practices will give organizations more efficient, effective, and unified ways to meet growing cyber security attacks as their asset bases grow and become more connected.

INDUSTRIAL DEFENDER®

Industrial Defender, Inc.
16 Chestnut Street • Suite 300
Foxborough • MA • USA • 02035

T: +1•508•718•6700
F: +1•508•718•6701

Email: Sales@industrialdefender.com

www.IndustrialDefender.com