WHITEPAPER

Industrial Control System (ICS) Security
INTRODUCTION

Industrial Control Systems (ICS) manage the industrial infrastructure on a global basis including water supplies, electric power generation and transmission, oil and gas refining and distribution, chemical manufacturing, pipelines, mining operations, transportation and a host of other manufacturing facilities. These systems are vital to the sustained operation, control, assessment as well as provide a view into the operations of industrial processes worldwide.

Industrial Control Systems can include any or all of the following components:

• Automated Control Systems (ACS)
• Distributed Control Systems (DCS)
• Programmable Logic Controllers (PLC)
• Supervisory Control and Data Acquisition (SCADA) Systems
• Intelligent Electronically Operated Field Devices (IED), such as valves, controllers, instrumentation
• Intelligent meters and other aspects of the Smart Grid
• Other networked-computing systems

These systems continue to be upgraded, improved and replaced, and the communications that exist between ICS components continue to change as well. In this modern age of telecommunications, these systems are being upgraded with advanced communication capabilities and are networked together just like any other Internet Protocol (IP) capable device. This represents an enormous challenge in securing these devices with regard to cyber threats, industrial espionage and other electronic threats.

In the world of Internet Technology, commonly referred to as IT, a system outage or infiltration can result in system downtime, loss of productivity and loss of revenue, as well as loss of confidentiality, integrity and availability. However in the world of ICS, system outage or infiltration could possibly result in loss of life often due to the critical nature of these devices. IT security is more concerned with integrity and confidentiality whereas ICS security is more concerned with system availability. Together, lack of access to critical ICS components and lack of visibility of the operational performance of these components can create a dire situation for those that are tasked with ensuring the safety of these systems.

UNDERSTANDING ICS ISSUES

As the convergence of Industrial Control Systems (ICS) and IT continues, often times physically across the same network infrastructure, ICS components today are most susceptible to the four types of issues below: (Weiss, 2010)

1. **Loss of View (LOV)** results in operators being “blind” to the system “state” and creates a risk of operators taking inappropriate or even harmful actions. Because of this, many plant operators are forced to shut down their facilities upon a Loss of View. In the past, LOV has caused power plant shutdowns due to Human Machine Interfaces (HMIs) that were infected by worms, such as Slammer and Blaster in the early 2000’s. For example, in January 2003 the Slammer worm disrupted systems at Ohio’s Davis-Besse nuclear power plant, but did not pose a safety risk because the plant had been offline since the prior year. However the incident did prompt a notice from the NRC warning all power plant operators to take such cyber risks into account.
UNDERSTANDING ICS ISSUES (cont.)

2. **Manipulation of View (MOV)** results in operators making the wrong decision based upon erroneous information of system state of operation. MOV can be caused by intentionally influencing the operator display to effectively cause the operator to be the hazardous component in the overall equation. For example, federal laboratories have demonstrated attacks whereby the displayed state of IEDs were changed from closed to open and forced the operator to perform dangerous actions causing the operator to act as an "attacker" due to the manipulation of the operators view.

3. **Denial of Control (DOC)** results in operators being denied access to critical systems. Unintentional denial of control includes hardware failures, network failures, and insufficient network capacity or even operator incidents. For example, in the Browns Ferry nuclear incident of 2006 a data storm was blamed for the Alabama nuclear-plant shutdown. The device responsible for flooding the network with data appeared to be a programmable logic controller (PLC) connected to the plant’s Ethernet network, according to an NRC information notice on the incident.

4. **Loss of Control (LOC)** results in a “sustained loss of control” and creates a situation whereby operators are unable to take alternate action before a potential catastrophic situation occurs. For example, the June 1999 Bellingham, Washington gasoline pipeline ruptured and the resulting fireball killed three people, including two 10 year old boys, and injured eight others. The broken pipeline spilled more than 230,000 gallons of gasoline into Whatcom and Hanna Creeks, scorched a 1.5 mile stretch of stream bank and damaged several buildings. According to the NTSB, the Olympic Pipe Line Company's practice of performing database development work on the supervisory control and data acquisition system (SCADA) while the system was being used to operate the pipeline, led to the system's becoming non-responsive at a critical time during pipeline operations.

As convergence of both IT systems and ICS components continues to increase for the purpose of improving process efficiency, productivity, regulatory compliance and safety, any system, regardless of the type, is susceptible to Denial of Service (DoS) attacks, cyber threats and other malware-based attacks like Aurora and Stuxnet. For example, Stuxnet, discovered in June of 2010, is classified as a computer worm. The worm was reported to search for and specifically target ICS components manufactured by Siemens Corporation. The worm initially spread aimlessly, but included a highly specific malicious payload that was designed to target Siemens SCADA systems that control and monitor specific industrial processes. It is the first discovered malware that included a PLC rootkit.

Attackers, regardless of being internal, external or on the other side of the globe, understand the large number of vulnerabilities in ICS components and their underlying networks and, reminiscent of the Stuxnet worm, can easily develop targeted attack methodologies, techniques and payloads to:

- Force systems offline
- Force systems to provide erroneous information
- Force systems to create unsafe conditions
- Force systems to be purposely shut down

Many organizations that utilize ICS components within their industrial processes can be vulnerable to a host of attack vectors and this fact may have played a part in President Obama's signing of an executive order on Feb. 12, 2013. It calls on federal agencies to develop voluntary cyber security standards for critical parts of the private sector and to consider proposing new mandates where possible under existing law. Industrial control systems which manage large-scale processes like oil and gas production, power generation and water treatment, have increasingly become a point of concern for the White House as the systems are often older and in some cases are more vulnerable to attack.

A DEEPER UNDERSTANDING OF POORLY-TIMED UPDATES TO ICS COMPONENTS

There are many differences in the tactical approaches to securing IT systems and ICS components. For example, software and firmware updates are often applied to IT systems (PCs and servers) on regular bases and these systems being rebooted daily or within maintenance windows is quite common. However, with some ICS components, a simple operating system update could cause a host of problems.

Many times ICS systems run commercially available operating systems, but these operating systems and the applications that ride on them have been customized to the extent that a simple update can take a system offline for extended periods of time. This fact alone increases the risk to these systems because they are less likely to be updated at regular intervals like IT.
A DEEPER UNDERSTANDING OF POORLY-TIMED UPDATES TO ICS COMPONENTS (Cont.)

systems. Also, patching and updating these systems requires the system to either download an update from the outside world (for example Microsoft), or an update would have to be performed by inserting removable media (USB memory stick) which has been proven to be a very bad idea. For example, according to reports, an Iranian agent infected Iranian systems at the Natanz nuclear facility with the Stuxnet malware directly using a USB memory stick. The malware exploited a host of zero-day vulnerabilities to attack SCADA software.

VULNERABILITY ASSESSMENTS TESTS ON ICS COMPONENTS

It has also been shown that a simple vulnerability assessment test, often performed on IT systems without issue, could cause a host of issues for ICS components. Since patching to ICS components may be performed on an ad-hoc basis or since many of the ICS components potentially run old or even out-of-date operating systems, patches for these systems may not even be available from the manufacturer for the latest cyber threats.

ICS components traditionally require communication links that are more reliable in nature, not necessarily faster. High-speed links are not necessary because most systems’ messages are very small small exchanges of information at very consistent periods of time. For example, a simple port scan of an ICS component could create a denial of control condition due to fact that they are most often incapable of handling large numbers of connections and/or requests. They are very susceptible to information overload and denial of service attacks, which can cause ICS components to lock-up due to too many system messages. ICS components are quite durable with regards to mechanical breakdown and other electrical problems; however, they are very susceptible to electronic communication (broadcast) storms.

According to ICS-CERT (Industrial Control Systems Cyber Emergency Response Team) CSA-11-223-01—A SUMMARY OF REPORTED ISSUES AFFECTING SIEMENS SIMATIC PLCS, dated August 11, 2011, an attacker can craft a Denial of Service (DoS) attack against the built-in web server on the S7-1200 Programmable Logic Controller (PLC) that forces it into a “stop/defective” state.

ICS were not designed with speed in mind. They’re more concerned with integrity of the information, often times at very slow speeds. IT systems require faster and faster links due to the large amount of information being transferred between client and server and so on. This is not the case for ICS.

PASSWORD MANAGEMENT ON ICS COMPONENTS

IT systems password length and strength is critical to block brute force password guessing attacks. Password requirements continue to increase on IT systems and often times continuous password guessing would result in a user getting locked out of an IT system. In the world of ICS, default passwords are most often used due to the fact if an ICS component was reeling out of control creating an extremely dangerous situation, the last thing operators desire is extremely hard passwords to remember and enter or to get locked-out of a system due to entering the wrong password too many times. Loss of life is the primary concern for ICS. Nobody has ever reported a death because the mail server was offline or unable to access. Deaths have been reported when ICS components were inaccessible or provided erroneous information to the operators.

As we can see from just a few examples above, fundamentally ICS components and IT systems are very different in their operation, but on the other hand both are vulnerable to the same types of electronic threats. Often IT security professionals try to apply their security knowledge to protecting ICS components while at the same time possibly causing loss of view, denial of control and loss of control situations. For example, NIST demonstrated the effects of performing a simple anti-virus (AV) update on a typical control system processor. The testing showed that performing an AV update resulted in a 2- to 6-minute denial of service due to the slow speed and loading of the processor.

SECURING THE PERIMETERS OF ICS DEPLOYMENTS

Cyber threats to both IT systems and ICS components can come from and include the following: (Weiss, 2010)¹

- Insider - intentional threats
- Internal - unintentional threats
- External - nontargeted threats
- Unwanted traffic and other malicious attacks

¹ Industrial Control System (ICS) Security
SECURING THE PERIMETERS OF ICS DEPLOYMENTS (cont.)

In the early days of both IT networks and ICS networks there was little if any interconnectivity: this is the IT network, and this is the ICS network. However, as convergence continues, points of “demarcation” are beginning to arise which creates internal and external perimeters that must be identified and secured.

In today’s complex networking environments identifying who is an insider and who is an outsider, what is internal and what is external is not as easy as it sounds. Even identifying inside perimeters within the interworking of a network is no simple task.

The real key to understanding the perimeter has mostly to do with “how does traffic actually flow” from client-to-server, server-to-server and server-to-client with regard to IT systems and how does traffic flow between the various ICS components. A thorough understanding of the perimeters of a network allows network administrators and information security personnel the ability of determining if any backdoor into the network exists while providing the utmost security and control for ICS. Perimeters identify where separation and segmentation of traffic and devices must be controlled.

For example ACSs, DCSs, PLCs, HMIs, SCADA and other remote ICS components have no need to access the Internet in most cases. These systems not only need to be isolated from the Internet, but they also need to be completely isolated from the business and information network that exists within the constraints of the “internal network” as well. Today’s attacks on internal computing systems don’t always originate from outside the perimeter. Many of them are caused by users who, while casually surfing the Internet, unknowingly download malware from malware infected websites. Once the “PC” becomes infected, these internal computers are used to spread their infection to other internal systems or can be used to launch attacks from within, in the form of Advanced Persistent Threats (APT). There simply is a need to protect all ICS components not only from the Internet itself, but also from any computing device that has had access to the Internet. All internal systems that have Internet access are suspect, period.

Not only do organizations that utilize ICS components need to worry about the outsider threat, but they also need to worry about the insider threat as well. In July of 2011, an intelligence report from the Department of Homeland Security, titled Insider Threat to Utilities, warns “violent extremists have, in fact, obtained insider positions,” and that “outsiders have attempted to solicit utility-sector employees” for damaging physical and cyber-attacks. Never before have ICS networks been this vulnerable, not only to denial of service attacks and malware, but now ICS networks are also vulnerable to the insider threat as well.

OPEN STANDARDS AND COMMERCIAL SYSTEMS

The move to using open standards such as Ethernet, TCP/IP, and web-based technologies in Supervisory Control And Data Acquisition (SCADA) and other ICS components has begun to expose these systems to the same cyber-attacks that have plagued corporate IT systems and admins for years.

Within the interworking of SCADA the term supervisory station refers to the servers and software responsible for communicating with the field equipment (RTUs, PLCs, etc.) and then to the HMI software running on workstations in the control room or elsewhere. In larger SCADA deployments, the “master station” may include multiple servers, distributed software applications, and disaster recovery sites. More components equate to more security related vulnerabilities.

For example, HMIs and other SCADA components are vulnerable to denial of service attacks, specially crafted packet attacks, malware, exploits, compromise and a host of other attack vectors. A search of cve.mitre.org related to the keyword “SCADA” returns over 202 vulnerabilities reported for SCADA software and hardware systems. Often times these systems have been excessively customized by the individual software/hardware vendors and these systems most often cannot be updated in the same fashion as any other business related IT system; this makes SCADA systems even more vulnerable to mainstream exploits, attack tools and methodologies.

Today there is a requirement for the business and information network to also have access to the certain ICS components for reporting, compliance, planning and improving safety, not to mention reducing cost and improving efficiency. Simply put there is no longer a way to completely isolate these ICS components from the rest of the network.

PERDUE REFERENCE MODEL – LAYERS OF INTERNAL SEGMENTATION

As shown in Figure 1 on the following page, the “levels” of the network are separated using traditional firewalls. According to the Perdue Reference Model (non-nuclear), points of demarcation exist and various parts of business and ICS networks must be physically and/or logically separated. Of course we understand that Figure 1 is only a “conceptual diagram”
PERDUE REFERENCE MODEL – LAYERS OF INTERNAL SEGMENTATION

and no two networks are built exactly in the same fashion. The Perdue Reference Model is not to be used as a network design tool but more of a “high-level” portrayal of where the various levels exist and how to create segmentation via points of demarcation between each level as necessary.

The recommendation here is to separate the levels of the networks using traditional 1st generation or even next-generation firewall technology, which may not be the best recommendation with regard to today’s cyber-security threat landscape.

PERDUE REFERENCE MODEL DISCUSSION

As shown in (Figure 1) working from the top (Internet) downward and not necessarily focusing on the Internet Perimeter but more, focusing on the “Internal Perimeters”, let’s take a closer look at the intercommunications that most likely exist between each level as shown above.

(Figure 1) (Weiss, 2010)"
Example 1 - Since the Business and Information network (Level 4) may need to have access to the ICS Operations (Level 3) for access to the Control Network one level below (to access the Process History or Advanced Control), inbound (downward) holes will have to be opened on the firewall to allow any communications between them to exist. Firewalls have a concept of untrusted and trusted. For any device that needs to communicate from the untrusted side of a firewall to the trusted side, downward holes must be opened for this communication to exist.

This opens up the lower levels to attacks coming from the higher Levels in the model shown. If any TCP or UDP port is allowed inbound (downward), then any device that has access to the Internet might also be allowed access to the ICS Operations at a lower Level.

Example 2 - Since SCADA HMIs today often use web-based interfaces, TCP port 80 and/or port 443 in most cases will naturally need to be opened inbound (downward) on the firewall between the two levels if any device in the ICS operations (Level 3) needs access to the HMIs located in Level 2.

Example 3 – Finally, if the Supervisory Control in Level 2 needs access to the Regulatory Control (PLCs, RTUs, etc.) devices located in Level 1, often times that communication will utilize very specific TCP/UDP ports which again will need be opened up inbound (downward) on the firewalls between the two levels, as shown.

The Perdue Reference Model advocates that segmentation is a good design, especially between the Business and Information Network, the ICS Operations network and the Operational Interface and Supervisor Control network; however, the recommended technology—firewalls—are not necessarily the best technology to provide the recommended segmentation. Stateful Packet Inspection (SPI), which has been in existence since the late 1980’s and which all firewalls in existence depend on to perform “allows and blocks”, only has the ability to inspect traffic headers, and not traffic payloads. SPI simply does not have the ability to block today’s attacks and overall threat landscape. Firewalls were intended to block devices (IP addresses) and control access, not block malware and other intentional or unintentional attacks.
PERDUE REFERENCE MODEL DISCUSSION (cont.)

Because unlimited types of attacks against any computing and/or control systems exist today and firewalls offer little protection for today’s attack vectors, the above design must be questioned. Certainly, “inline technology” makes the most sense to block Denial of Service attacks, unwanted traffic and malware; however, first generation or even next-generation firewall technologies are simply not up to the task of blocking all the attacks that ICS components may experience—now and well into the future.

As explained earlier in this white paper, it is very simple to perform a Denial of Service attack on many ICS components by simply accessing the device repeatedly at even moderate speeds. Many ICS components were never designed to be accessed at high rates and/or to receive high levels of control signals and/or commands in a short period of time. Even polling these devices too often for system status can cause them to become unstable, resulting in a possible Loss of View or even a Loss of Control over the ICS component. Therefore, another system of protection must be implemented beyond firewalls that can control the “rate” at which communications to the ICS components are permitted. Firewalls normally have few, if any, features with regard to controlling rates of information and traffic flow.

Exploits, malware and Denial of Service attacks will easily pass right through the firewall but not because the firewall is ineffectual at blocking traffic. It’s due to the usage of the firewall in general that represents the primary issue. Inbound (downward) holes in firewalls provide no protection whatsoever, and malware, Denial of Service attacks and other application abuses take advantage of inbound holes on firewalls. Additionally, cyber attackers understand the vulnerabilities firewalls possess as well.

NOTHING MORE THAN SPEED BUMPS

Simply put, there must be something better than commercially available firewall technology that can be used to protect ICS systems against Denial of Service attacks, undesired access and malware. Security experts are implicitly recommending that segmentation must exist between the business computing systems and the ICS computers and other industrial related components like PLCs and DCSs. The recommendation of segmenting the network is a good idea; however many experts are still recommending firewalls that are simply not up to the task with regard to today’s attack vectors.

FIREWALL PROOF POINTS:

In the past, several demonstrations of ICS component cyber-attacks have been provided by US national laboratories. For example:

1. Idaho National Laboratory
   a. Remote Supervisory Control And Data Acquisition Hack – a buffer overflow vulnerability in the Apache software the SCADA system was using
   b. Aurora demonstration that malware could damage rotating equipment

2. Pacific Northwest National Laboratory
   a. Man-in-the-Middle Attack on a SCADA system and an Intelligent Electronic Device (IED)

In all three of these cases demonstrated by the two national laboratories listed above, **firewalls would not have blocked these attacks, period.** A well-known analogy used often in the world of the hacker underground is that firewalls are nothing more than speed bumps to the seasoned professional.

THE ADVANCED TARGETED ATTACK

Beyond the conversation of segmentation within the internal network, it is well known that hackers do not have to be located near their victims to achieve their desired results, and many of the recently recorded industrial cyber-attacks were not performed over the Internet. Often they were performed by attackers having access to internal systems, remotely via the Internet, or other means of access like a modern or even from an insider threat that had authorization to a victim device.
THE ADVANCED TARGETED ATTACK (cont.)

In today’s threat landscape, compromising (taking control of) a computer system is nothing more than a click away. All an attacker needs is an HMI operator to simply click on a link that goes to any attacking device on the Internet or on the inside of a network. The attacking device responds with a number of browser and/or other application exploits, inserts some remote code that the victim computer (HMI in this case) executes, and the backdoor is easily established right through the several layers of perimeter firewalls, regardless of where they are deployed. Exploits easily pass through any firewall due to the nature of Stateful Packet Inspection, how it operates and who initiated the conversation.

Hackers take advantage of human nature and not only do they socially engineer their victims, but also today there is even proof of social profiling the victim first, then socially engineering them and phishing them into clicking on a web link. There are thousands of examples of this attack “vector” being quite successful, and SANS reports it to be the number one attack vector in use today. One single click on a web link can open backdoors into any network and often times these covert channels are nearly impossible to find.

An Advanced Persistent Threat (APT), for example, has an established backdoor into the network whereby the communications between hacker and compromised computer system often looks like normal everyday traffic to the average security team. Firewall logs look normal; intrusion detection systems are not alerting to the presence of a covert channel; and anti-virus software operating on the computing system does not alert on anything unusual. However, the Advanced Persistent Threat is active and real and results in an internal trusted computer being run remotely providing an open doorway into the victim’s infrastructure.

INDUSTRY RECOMMENDATIONS FOR SECURING ICS

Because the consensus today in information security circles is that firewall technology is limited at best and offers little protection against the plethora of possible attack vectors, there again must be a better way of providing segmentation via a “new” First Line of Defense. If communication must exist between the various levels and “holes” must be opened on the firewalls between the levels, the principal recommendation would be to utilize a technology that is capable of not only acting as a firewall but the technology must go beyond the capabilities of first- and next-generation firewall technology.

SOLUTION: THE CORERO FIRST LINE OF DEFENSE

Instead of deploying firewall technology, which literally addresses a very limited subset of possible attack vectors, deploying the Corero First Line of Defense addresses the broadest spectrum of unwanted traffic. The Corero technology not only meets the industry’s recommendations, but it also exceeds them on all fronts. Simply put, communications often must exist between the levels as previously discussed, but Corero offers a comprehensive solution like no other in existence today.

In a good network design natural “collapsed inspection points” are created inherently by the devices that provide the segmentation between the levels previously discussed. Instead of deploying first- or even next-generation firewall technology between the levels (Figure 1), transparent inspection technology is imperative to protect against the wide array of electronic threats facing ICS components today. The Corero technology can be easily deployed between the layers, creating the required segmentation whereby all:

1. Traffic regardless of type is “funneled” and fully inspected
2. Computing devices and all protocols are either allowed or blocked
3. Allowed traffic is thoroughly scrutinized, inspected and controlled
4. Covert channels, backdoor communications or APTs are easily identified and blocked
5. Attackers, regardless of location, and malware, regardless of type is blocked
SOLUTION: THE CORERO FIRST LINE OF DEFENSE

6. Security policy violations are logged, recorded and stored for further analysis
7. Security related events and alerts are generated, recorded and stored long-term
8. Reports, regardless of type or purpose, are generated, delivered and cataloged
9. Traffic is capable of being copied and directed to storage for required forensics analysis (PCAP)
10. Industry recommendations for securing ICS components and other systems are achieved

The Corero First Line of Defense eliminates unwanted traffic through a systematic approach called the:

Five Key Steps of Protection

1. **Restrict Access ------ Allow only the EXPECTED traffic**
2. **Limit Rates  ----------- Evaluate the AMOUNT of traffic**
3. **Enforce Protocol ----- Enforce the CORRECTNESS of traffic**
4. **Prevent Intrusions --- Analyze the INTEGRITY of traffic**
5. **Increase Visibility ---- Provide VISIBILITY into unwanted traffic and attacks**

- The first step above (Restrict Access) revolves around allowing only expected traffic and restricting access of known attackers, via IP Reputation, Geolocation or other intelligence gained from internal and/or external logging systems and regulatory agencies.
- The second step (Limit Rates) prevents attacks based upon clients’ individual traffic behaviors and controls the amount of traffic from any single source. For example, blocking is performed against sources that transmit volumes of traffic toward your ICS components, and just as bad, those that open excessive number of connections, keeping vital resources tied up and potentially forcing systems offline.
- The third (Enforce Protocol) ensures all allowed traffic conforms to RFC specifications and de facto standards, thereby enforcing the correctness of traffic. Any traffic not conforming to standards and/or case-by-case whitelisting is simply discarded.
- The fourth (Prevent Intrusions) analyzes the integrity or goodness of traffic and detects known, and possibly unknown, buffer overflows, code injections, malware and other targeted attacks. Through extremely high-speed deep packet inspection capabilities, additional unwanted traffic is quickly and easily eliminated.
- The fifth (Increase Visibility) provides operators and security personnel insight into what is happening on their networks. It includes the ability to collate data from “syslog” events, SNMP polls and traps, and proprietary APIs, enabling meaningful visibility and a stream of potentially critical information.

In the figure on the next page (figure 2) notice how the firewalls in (figure 1) were replaced by the Corero First Line of Defense technology.
SOLUTION: THE CORERO FIRST LINE OF DEFENSE (cont.)

Why? Simple... Firewalls do not address the most common industry recommendations for securing ICS components whereas the Corero Technology provides a more comprehensive defense against the broadest spectrum of attacks ICS components and other network devices may come under.

(Figure 2)
For example, let’s take a look once again at the communications that exist between the two layers previously discussed, as shown below.
SOLUTION: THE CORERO FIRST LINE OF DEFENSE (cont.)

The Corero First Line of Defense has replaced the traditional first-generation firewall technology, as shown. If a firewall were used, inbound holes would have to be opened by using Port Forwarding, Static NAT or some other technique to allow incoming traffic to be directed to the downstream devices.

For example, if the ICS Operation Staff at Level 3 needed access to the HMIs on Level 2, TCP port 80 and/or TCP port 443 would have to be opened on the firewall to allow access the HMI’s web interface, and only packet headers would be inspected by the firewall technology.

With the Corero technology, TCP port 80 and/or TCP port 443 would be allowed and not only would the packet headers be inspected, but also entire contents of every packet’s payload would be thoroughly scrubbed for malware and for any information overload (Denial of Service) attacks. Any protocol anomaly would be detected and any covert channels would be identified. If the Corero technology is deployed appropriately, it is most often completely impenetrable.

PROTECTING INDUSTRIAL CONTROL SYSTEMS WITH FIVE KEY STEPS OF PROTECTION

In order to best combat the broadest range of threats, organizations who utilize ICS should consider selection and deployment of solutions that address as many threats as possible in a tightly integrated, mutually reinforcing fashion—as Corero Network Security provides with its First Line of Defense technology. The defense mechanisms that address the five key steps of protection are displayed below.
RETURN ON INVESTMENT

Customers who purchase the Corero First Line of Defense technology to protect their Industrial Control System networks have reported that the return on their investment is almost immediate, citing:

- Protection for mission-critical ICS components and reducing attacks on operating systems and ICS components from:
  - Insider - intentional threats
  - Internal - unintentional threats
  - External - nontargeted threats
  - Unwanted traffic and other malicious attacks

- Improvement of network performance by eliminating unwanted traffic, undesired access and Denial of Service attacks from impacting the network and ICS components

- The ability to identify compromised systems and provide increased visibility while remediation efforts of compromised systems are underway

- Protection for unpatched IP-based devices from remote exploits of known and unknown system, protocol and application vulnerabilities

- Reduction in operating expenses incurred by maintaining and running older, resource-intensive, ineffective security solutions

- Reduced risks and improved compliance by following recommended industry standards and best practices for protection of ICS network components and other IT resources

CONCLUSION

Organizations which utilize Industrial Control Systems face a significant paradox based on the requirement to further improve process efficiency, productivity, regulatory compliance and safety while also providing security as the convergence of both IT systems and ICS components continues to increase.

Corero Network Security has the best technology for offering protection from unwanted traffic, undesired access and rate-based Denial of Service attacks that target ICS components and devices. Corero also provides ICS security administrators the utmost peace of mind with fast response and timely updates to protect against new exploits of known and unknown vulnerabilities. The Corero technology is a high-performance, scalable and reliable solution that has been designed from the ground up to offer the best protection mechanisms and performance for detecting and eliminating cyber threats that target mission-critical ICS components.

REFERENCES:


ABOUT CORERO NETWORK SECURITY

Corero Network Security, an organization’s First Line of Defense® against DDoS attacks and cyber threats, is a pioneer in global network security. Corero products and services provide online enterprises, service providers, hosting providers, and Managed Security Service Providers with an additional layer of security capable of inspecting Internet traffic and enforcing real-time access and monitoring policies designed to match the needs of the protected business. Corero technology enhances any defense-in-depth security architecture with a scalable, flexible and responsive defense against DDoS attacks and cyber threats before they reach the targeted IT infrastructure allowing online services to perform as intended. For more information, visit www.corero.com.