Practical Industrial Control System (ICS) Cybersecurity: IT and OT Have Converged - Discover and Defend Your Assets

The benefits derived from information technology (IT) and operational technology (OT) convergence are enabling more effective management of contemporary control systems. However, the unique challenges of IT/OT convergence make managing and securing an industrial control system (ICS) more difficult. This paper explores how industrial and information system administrators can build stronger cybersecurity programs to protect IT/OT systems.

A SANS Whitepaper

Practical Industrial Control System (ICS) Cybersecurity: IT and OT Have Converged—Discover and Defend Your Assets

Written by **Doug Wylie** and **Dean Parsons**

September 2018

Sponsored by:
Tenable

Introduction

More than half of respondents to a recent Industrial IoT security survey use connected devices in Industrial IoT systems:

- 71% actively collect and monitor process health data.
- 69% collect status, alarms and alerts.
- 56% feed predictive maintenance solutions and also control aspects of their operations and processes.[1]

Clearly, the use and benefits derived from information technology (IT) and operational technology (OT) convergence are growing and enabling more effective management and operation of contemporary control systems. Convergence improves uptimes, performance, quality and productivity, all of which lead to increased profits for those who adopt these solutions.

On the flipside, IT/OT convergence carries unique challenges that make managing and securing an industrial control system (ICS) more difficult. This is due to greater technical complexity, expanded risks and new threats to more than just business operations.

[1] The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns, www.sans.org/reading-room/whitepapers/analyst/2018-industrial-iot-security-survey-shaping-iiot-security-concerns-38505

Objective

This paper will explore the issues that arise with the blending of IT and OT into combined cyber-physical systems where risks must be identified and managed. Specifically, it will help you address these questions:

- Why are digital asset inventories critical for IT/OT security risk management?
- How does knowledge about risks and vulnerabilities to IT/OT systems lead to better risk management?
- Can applying even a few of Center for Internet Security (CIS) Controls make a marked difference in the security posture of today's control systems?

Equipped with answers to these questions, industrial and information system administrators can make more informed decisions about how to build stronger cybersecurity programs to protect IT/OT systems.

A Path Toward Better Cybersecurity Risk Mitigation

A company's security posture depends on many factors and will vary over time:

- Risks and threats emerge and evolve
- Unintentional and malicious behaviors affect risk exposure and impacts
- Policies and compliance pressures compel investments and actions
- The demands of markets, business partners and shareholders

Not all cybersecurity risks can be fully addressed, nor are all risks created equal. Although there is no one-size-fits-all approach for what steps and priorities to take to manage security risks, industry-accepted best practices and guidelines can help.

Cybersecurity Controls for Critical Systems

CIS produces and manages the CIS Controls, a prioritized set of practices that can mitigate risks to networked systems. Currently in Version 7,[2] the Controls are broadly accepted as a means to assess and address common risks to systems, providing steps that can notably reduce the likelihood of exposure and impacts. A community of experts—representing most industries—helps to manage these best practices. Because IT and OT domains share similarities yet also have key differences, the application of the Controls in each domain requires careful consideration, especially where IT/OT convergence is prevalent.

The CIS Controls include top-level controls categorized as Basic, Foundational and Organizational. They are ordered sequentially to prioritize those typically holding the greatest potential for reducing cybersecurity risk. By aligning investments to these CIS Controls, you can measurably improve the security posture of your organization. See Figure 1 on the next page.

[2] www.cisecurity.org/controls

While the Controls originated with a focus on information security for enterprise-level IT, CIS continues to expand its resources and tools to help companies implement them more broadly. This now includes the recently released "CIS Controls Implementation Guide for Industrial Control Systems" for Version 7.[3] Useful as a starting point for a security improvement assessment, these ICS Controls provide a road map for an organization embracing or moving toward converged IT/OT systems, including industrial IoT solutions spanning across domains and may reach outside of the organization's local network architecture.

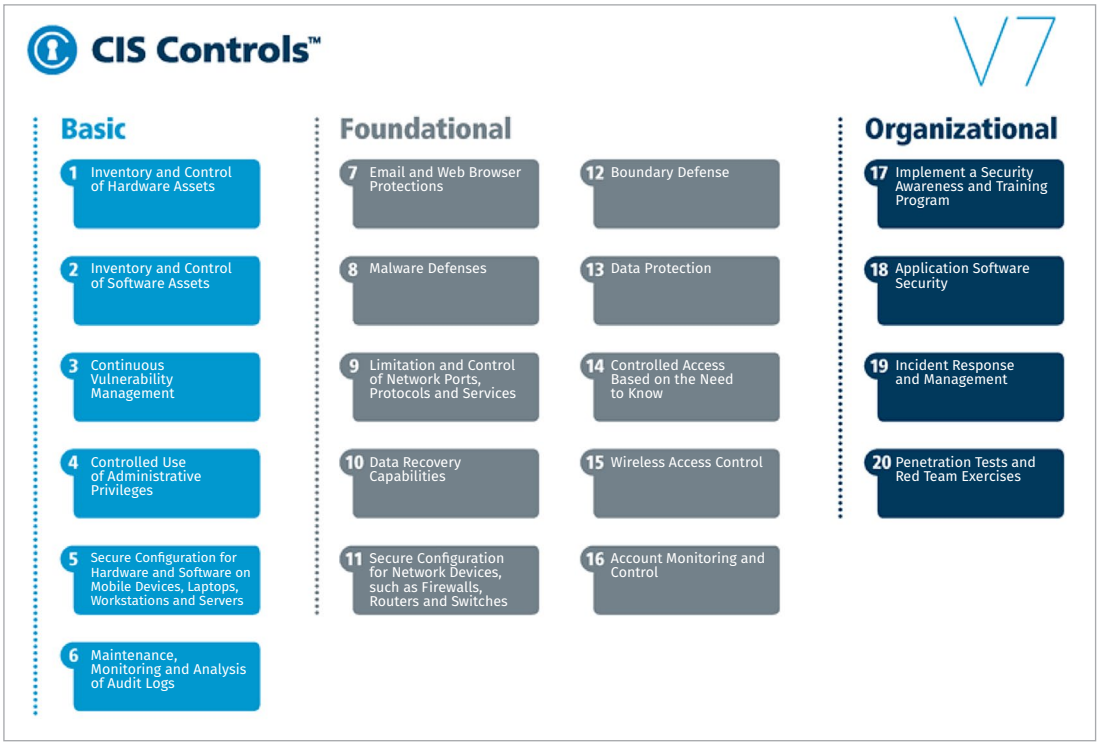

Figure 1. Center for Internet Security Controls Version 7

EXPERT ADVICE:

Per CIS, "While many of the core security concerns of enterprise IT systems are shared by ICS operators, the main challenge in applying best practices to ICS is tied to the fact that these systems typically operate software and hardware that directly control physical equipment or processes. Compounding this issue is the fact that many systems not only often have high availability requirements, but also are often the underpinning of critical infrastructure."[4]

The first three CIS Controls form the foundation for all the other controls and provide a comprehensive asset inventory spanning hardware and software, and the execution of a security vulnerability and product patch management program. See Figure 2.

Combined, these three controls can provide valuable awareness and be used to effectively set priorities based on risk. Knowing what products are installed and keeping them up to date sounds simple, but carries a unique set of challenges.

Figure 2. The First Three CIS Controls

[3] www.cisecurity.org/white-papers/cis-controls-implementation-guide-for-industrial-control-systems

[4] www.cisecurity.org/webinar/cis-controls-implementation-guide-for-industrial-control-systems-launch-event

Asset Identification for IT/OT Converged Systems

Gone are the days when an IT or OT installed system closely matched its original engineering drawing. For OT systems especially, they are typically tailor-fit in situ to suit existing environments—and the activities required to manage and support architectures and cyber-physical processes are a lifecycle that rarely stops, as illustrated in Figure 3.

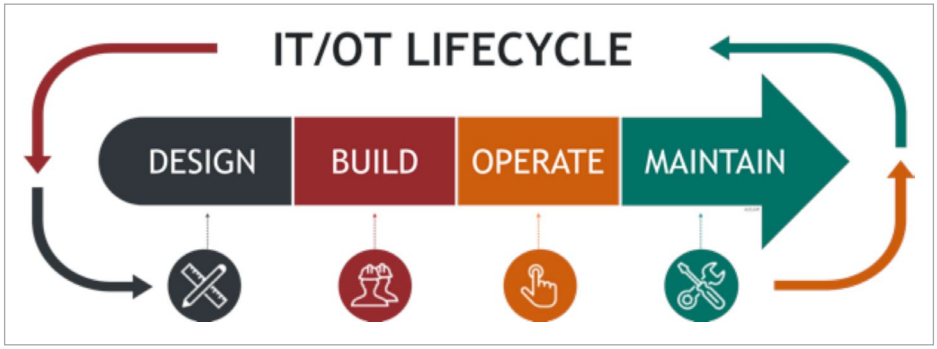

Figure 3. The IT/OT Lifecycle Process

It's a twofold problem:

- Engineering drawings are less accurate.
- Changes and customization activities are not well-documented (if documented at all).

Answering the seemingly simple question, "What is connected to a system?" can be far out of reach. Yet arguably, this may be the most essential information needed to safeguard IT and OT systems.

Ascertaining what is connected to a system and how current these devices are requires a combination of physical and logical approaches that ideally become ingrained into processes, policies and job duties. Asset discovery, inventories and comprehensive device identification processes are each crucial to help protect systems from security risks.

Physical Asset Inventory

While physical inventories are useful and important, they represent a version of what was known and accessible at a particular point in time. Thus, a physical inventory can miss some devices altogether—especially if sections of a system are inaccessible, network edges misidentified, cables cannot be traced, or wireless and mobile assets connect only periodically.

Manual inventories also can't see logical interrelationships among devices on the same or different networks, nor can they see network routing paths such as VLANs or WAN connections that may be critical parts of the same system. There are also contested spaces, such as an industrial demilitarized zone (DMZ), where it's not always clear if an asset is part of an IT or OT system, or both. In addition, physical inventories often miss off-premises infrastructures, assets and services.

The takeaway: Conduct a physical inventory, but treat this step as part of a larger asset discovery process.

Network-based Asset Inventory Methods

Network-based approaches can help verify and expand the asset discovery process for IT/OT systems. However, not all logical discovery approaches deliver the same results. Employing more than one approach helps ensure completeness, especially since elements in networks change over time. Figure 4 illustrates a recommended architecture for a secure network promoted by the US Department of Homeland Security NCCIC and its ICS-CERT branch.[5]

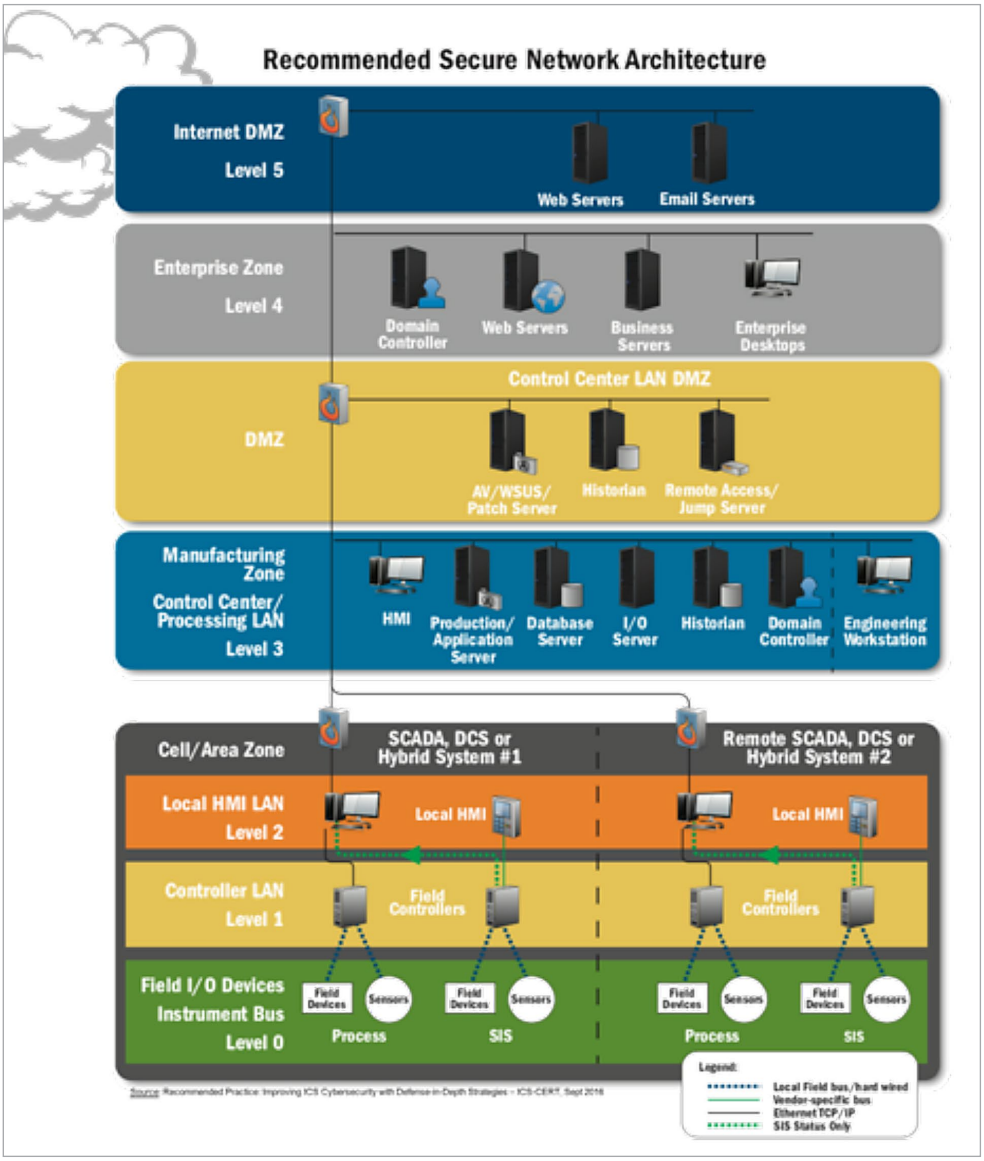

Figure 4. DHS NCCIC/ICS-CERT Recommended Secure Network Architecture

Passive Monitoring: A "Listen, Don't Touch" Approach

One approach to network-based asset discovery is passive monitoring. This is especially fitting for antiquated, fragile OT systems as it does not interact with connected devices, nor does it change the network's performance. Passive monitoring can also be especially important when you don't know how devices will react to a particular asset discovery approach.

Passive monitoring capabilities need raw network traffic to analyze, and this data is most often gathered from strategic listening points in a system capturing data for analysis. This can include network appliances, such as routers and firewalls, which operate at the edge of a network and route information between systems. Also, it can include the uplink of managed switches and routers where lower-level network communication can be actively exchanged with other peer or higher-level systems.

When used for asset discovery, passive monitoring techniques analyze a mirror image of raw traffic from a system and identify connected devices based analyzing attributes stored within the network traffic. As an added benefit, you can use this same data to determine device-to-device communication paths, or potential abnormal communication activities. Properly installed, passive monitoring solutions can also be stealthy and difficult for an adversary to discover, making this data mirroring approach useful for a network intrusion detection system (NIDS).

[5] www.dhs.gov/national-cybersecurity-and-communications-integration-center

Passive Monitoring: Infrastructure Requirements

Security architects should consider the potential to make use of existing network capabilities where possible and appropriate when implementing passive monitoring. Where available, managed network appliances such as Layer 3 (L3) switches, routers and firewalls can usually be configured to route raw network packet streams to supply a network monitoring process. Network services like port mirroring/switched-port analyzer (SPAN) configurations, remote monitoring (RMON) services and network trunking capabilities can combine to help provide a central view of a given IT/OT system's connected devices. Ideally, a network architecture would already include listening points in its infrastructure or some capability to enable such services (see Figure 5)—but not all do.

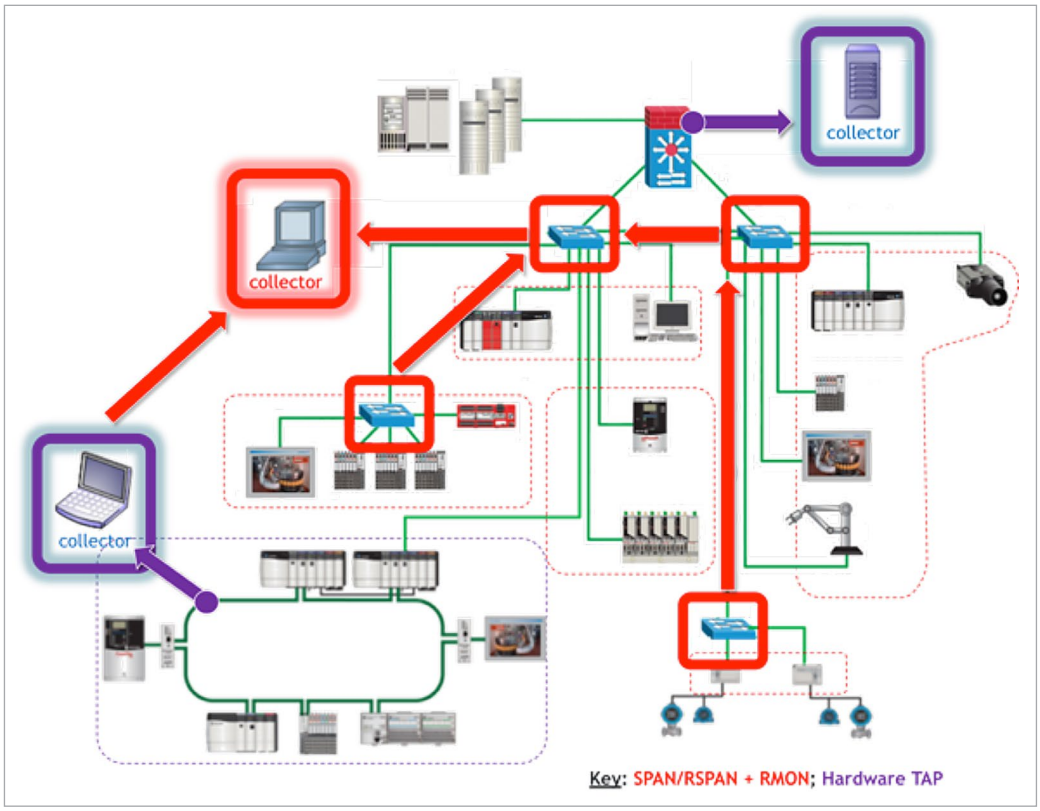

Figure 5. Network Architecture with Listening Points and Traffic Collectors

For a variety of reasons, many OT systems might have a limited number, or might be altogether lacking, managed network infrastructure devices such as L3 switches and routers. For those who do have these products, it's not uncommon to find these appliances installed at locations in a system that are less- than-ideal to support broad, ready access to network traffic to be analyzed. Some infrastructures are built around products limited in their performance and availability to service higher-traffic applications. Some purported L3-managed devices may even lack basic port mirroring, trunking and RMON services commonly found in most medium and high-end products. These are just some of the reasons why it's a good practice to invest for the future during network design, procurement, system retrofits and upgrades. Include products with these capabilities, while also balancing these decisions with consideration of how these software-configured services will be responsibly managed, and by whom.

To help reduce the administrative challenges and associated risk with such software-configured services, packet captures can be taken from a network interface card (NIC) operating as a network sniffer. This approach yields a wealth of information valuable for asset discovery and deeper packet-analysis activities. Be sure to configure the NIC in promiscuous mode and offload the recorded data into a packet capture file, typically a PCAP or PCAP-NG format, since these files are widely compatible with network

analysis tools. Such files can be easily created and replayed via Unix/Linux command-line services **`tcpdump`** and **`tcpreplay`** respectively.[6] For added assurance, many practitioners will move the analysis process to devices completely disconnected from a target system running specialized software.

The ISO Open Systems Interconnection (OSI) model for communication (ISO/IEC standard 7498-1:1994[7]) is a useful reference when considering communication sources and information types to be evaluated via traffic capture, analysis and monitoring tools (see Figure 6).

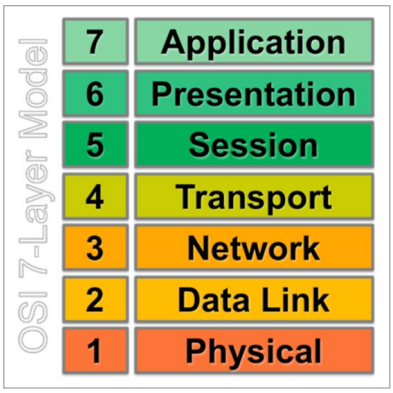

Figure 6. ISO/OSI Basic Reference Model for Communications

EXPERT ADVICE:

For some advanced users, it can be useful to perform a preliminary review of a traffic capture and focus on what's known as a 5-Tuple—a method grouping packets by source IP, source port, destination IP, destination port and OSI Layer 3/4 (network and transmission layer) protocols. This approach ignores packet payload analysis and can speed an ad-hoc discovery process. However, the approach does not display OSI Layer 2 (data-link layer) devices often at the core of many OT systems. Time and expertise are also needed to work with such an approach, but with a permanent solution a 5-Tuple can avoid some of the risks that could be introduced if point solutions are used.

As an alternative, advanced automated network analysis products can provide tailored and targeted asset discovery capabilities, producing more complete inventories and more detailed views of device identity information. There are added benefits with such products since they can often be installed as a permanent addition to a system to streamline workflows and establish asset discovery as a sustainable, continuous process within a system.

To remove the risk of affecting network communication altogether, install a physical hardware test/terminal access point (TAP) in-line with the network to electrically, not logically, transfer bit-level information (Layer 1) to a downstream NIC. The installation of such a TAP will require a temporary physical break to a network, so only install it once you confirm the system is not operational.

For a growing number of IT/OT converged systems, some combination of configured port mirroring, SPAN, RSPAN via network trunking and hardware network TAPs are employed. Some also now include a separate management network as a backhaul to move and aggregate packet streams for centralized monitoring. Designing and implementing these sorts of network enhancements is an area in particular where IT personnel can share technical expertise with OT teams.

Point-level and broad-scope traffic mirroring capabilities allow you to consider adding automated network monitoring products as an integral part of IT, OT and converged systems. Some advanced products provide capabilities extending far beyond the manual, command-line packet capture and replay services. They may even feature tailored product discovery, tracking and analysis tools specifically intended to operate as persistent devices for continuous traffic capture and data analysis.

[6] https://danielmiessler.com/study/tcpdump/#protocol, http://tcpreplay.synfin.net/wiki/tcpreplay

[7] www.iso.org/standard/20269.html

What Is Visible from Passive Monitoring

When analyzed with capable passive monitoring solutions, live or recorded packet captures (PCAPs) can reveal a range of helpful information to expand upon a physical asset inventory—hardware MAC addresses for devices that may communicate at only Layer 2 (data-link layer) can be evaluated, as well as IP-based devices that communicate Layer 3 (network layer) and above. This comprehensive coverage is necessary because some analysis tools lack capabilities to locate devices that communicate non-routable, Layer 2 protocols prevalent in many OT systems. This can lead to blind spots and devices unknowingly omitted in an asset discovery process. Not all network monitoring solutions are equal. More capable products can analyze Layer 2 communication and may even depict device-to-device interactions. Some are able to correlate device information to known product vulnerabilities. Products with such capabilities can be valuable for patch management and incident response processes, as well as network security monitoring teams following an Active Cyber Defense Cycle (ACDC).[8]

EXPERT ADVICE:

When capturing packet streams, ensure the window for packet capture is long enough for most events and communication to occur at least once. A window of 24 to 72 hours is usually sufficient to locate most connected assets, but certain devices or events may not necessarily communicate all the time, nor will they send the same data all the time. For instance, Address-Resolution Protocol (ARP) messages may be produced only once by a device as it connects to a system or inconsistently by a device that periodically sends Gratuitous ARPs (GARPs). For this reason, even PCAPs taken from the same system over time can be different. To help avoid missing assets, start traffic captures from a time just prior to the start of a process and during periods of high or unusual activity.

Passive monitoring can also begin to build time-based inventory tables of communication ports, protocols, device host names and packet payloads. In some cases, it can even build time-based inventory tables for specific device identity information and network commands used to perform tasks (e.g. device configuration and control, data collection services for network and endpoint diagnostics).

EXPERT ADVICE:

PCAPs acquired during passive monitoring can provide even deeper insights into the potential for serial devices not networked to also connect to a system via a gateway product. For instance, if Modbus TCP protocol is seen, the payload for a packet can reveal a Unit Identifier flag. When the flag is set to a value of 0, it indicates no serial devices are connected to the IP-connected device. If the flag is a value of 1–254, there is a potential for a serial device to be connected, prompting an added physical inspection to identify these added devices in a network architecture.

[8] Reference SANS ICS515: ICS Active Defense and Incident Response

Some advanced automated passive monitoring products have the capability to go beyond simply identifying the presence of a device and 5-Tuple information. They may have capabilities to also display detailed asset identity information such as device manufacturer, device type and model number, firmware/software revisions or even more, all by analyzing packet headers and payloads. Unavoidably though, passive monitoring has its limitations. You can only discover devices and have an opportunity to discern their respective device-level details if such data is produced and captured within a given window. Also, if data is encrypted, passive monitoring will be unable to show details much beyond a device MACID and 5-Tuple attributes. Like a physical inventory, passive monitoring can still have blind spots.

Active Scanning: Asset Identification for IT and OT systems

Active scanning is a complementary approach initiated by a product connected directly to the network it is monitoring. There are two basic types:

- Unauthenticated, a method to search for indicators of connected devices via port scanning
- Authenticated, a method to connect to devices and then access and obtain privileged device information

Authenticated scanning uses carefully engineered approaches to request asset identity information from other connected devices via structured messages to which other connected devices will reply. It has the capability to deduce deeper information too, such as installed software, user accounts, device networks hardening status and—in some cases—even indicators of known malware.

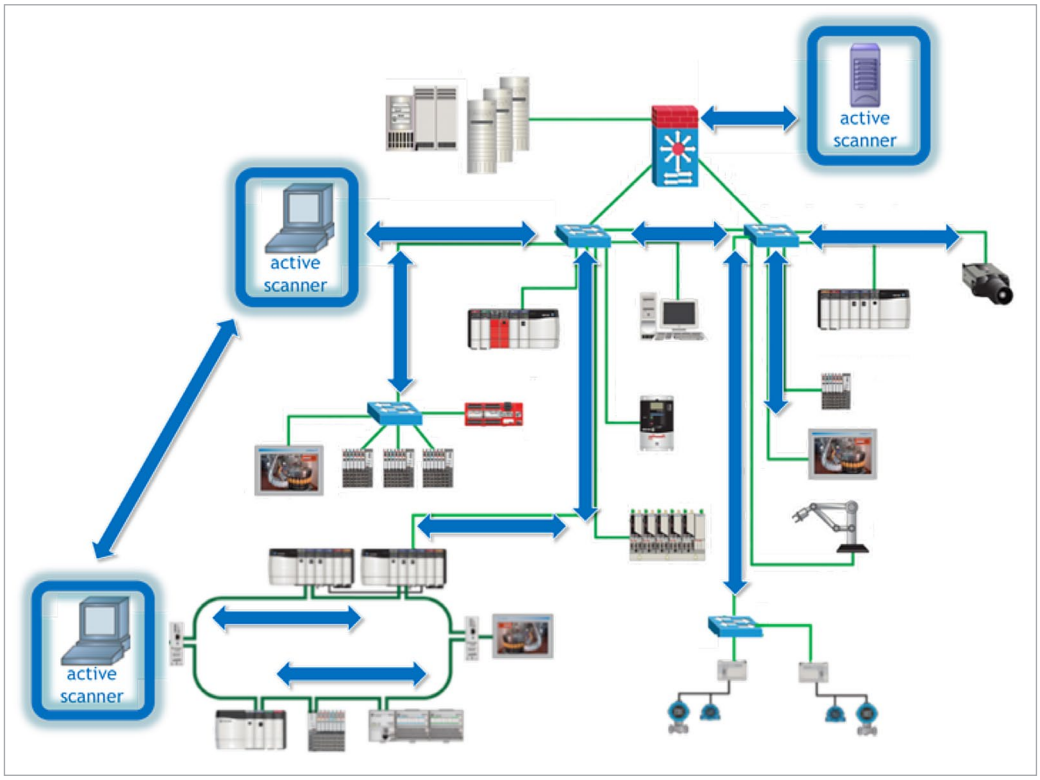

Figure 7. Network Architecture with Active Scanners

Most IT systems are comprised of IT-oriented products well suited to respond to both unauthenticated and authenticated active scanning. In fact, many IT devices are designed with hardened, resilient network interfaces, communication stacks and services that inherently expect to encounter such requests during daily operation. This is a hallmark of IT product security maturity—but it's often lacking in many application-specific embedded OT products. Figure 7 depicts active scanners directly interacting with network appliances and end-point devices to gather information. Multiple active scanners may be required when systems are well-segmented with limitations on network routing.

Many OT products are fragile in comparison to IT products. It's still not uncommon to find OT products unable to withstand active network scanning because product designers did not plan for the device to encounter such communications. Even worse, the precise device failure-modes may be unknown if the product should become confused or overwhelmed. For these reasons, it is prudent to be extremely cautious with anything connecting to an OT system, especially if it is intended to exercise communication services of other devices. Fortunately, the industry continues to mature, and a growing class of OT-oriented network monitoring products—with carefully engineered capabilities to discover IT and OT protocols and devices—is emerging (see Figure 8 for examples of popular IT and OT protocols).

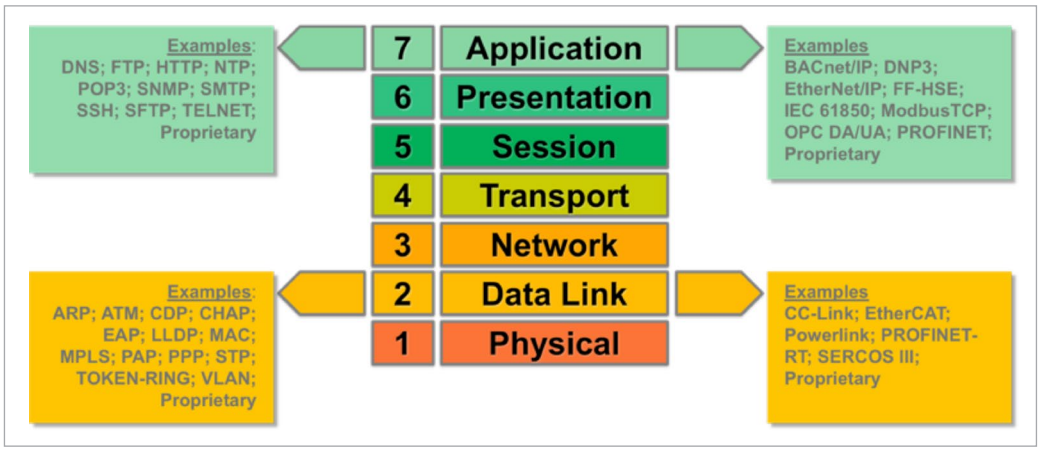

Figure 8. Popular IT and OT Protocols at OSI Layer 2 and Layer 7

A responsible active-scanning approach for OT systems exclusively uses tested and approved networking communication standards and protocols, covering OSI Layer 2 and higher for device discovery to build a view of what is connected to a given network. It offers the added benefit of requesting and collecting asset identity details that can include:

- Manufacturer information
- Device type
- Model number
- Firmware/software revision
- Configured and active services
- Device-level diagnostic and prognostic details
- Performance data
- Event logs

This type of information is needed during device and ICS commissioning, and typically for device replacement too. It's also widely used for asset management solutions, including backups and system recovery planning. By gathering this information, you can achieve an even more complete network inventory of a system.

EXPERT ADVICE:

You should conduct active scanning of OT systems using only tools specifically designed and confirmed to follow strict OT protocol and product implementation standards. Control systems often rely on time-critical communications and device availability. Otherwise, a system can become unstable or even unsafe. If a network disruption causes an unplanned failure mode, severe consequences may result, including possible loss of life, impacts to machinery, degraded performance, and loss of quality and productivity.

Additive Sources for Asset Inventories

Many network appliances such as managed switches, routers, firewalls and some endpoint devices also contain a bevy of information to add even more detail to a network inventory of a converged IT/OT system.

Collect and aggregate these additive sources to form a truth table to help further identify what is and should be connected. Since many of these services include timestamp information, they are also useful to track mobile assets and for digital forensics, too. Figure 9 highlights a number of these specific sources of information.

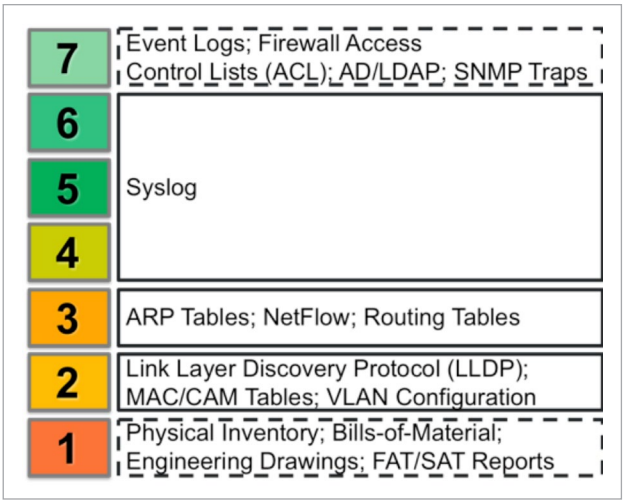

Figure 9. Additive Information Sources from Devices

EXPERT ADVICE:

LLDP is a service for active asset discovery that some network appliances support. The service is designed to help locate connected devices at Layer 2. It can also help create a map of a system. While it is sometimes enabled by default in a system to aid troubleshooting activities, it is best to disable LLDP when it is not needed. Otherwise, it could potentially be used by an attacker to gather intelligence in a manner likely to go undetected by most network monitoring tools.

Summary of Asset Discovery Methods

You may also want to consider key attributes of each asset discovery approach to establish appropriate expectations for level of risk, completeness and level of effort required. See Table 1.

Table 1. Asset Discovery Approaches and Their Attributes

Type	Risk	Target System Status	Speed	Accuracy	Coverage	Current & Up to Date
Physical Asset Inventory	**Low**	**Operational** Includes safety precautions	**Very Slow** Labor-intensive; schedule dependent	**Moderate** When assets are accessible	**High** When assets are accessible	**Low** Labor-intensive; scheduled activity
Passive Monitoring	**Low**	**Operational** Downtime may be required to set up monitoring in absence of TAPs, or if port mirror/ SPAN capabilities not available.	**Fast** Yet varies based on desired level of detail	**High** Improves with time; depends on packet stream	**Medium** Improves with time; depends on network access	**High** Can operate as a continuous process
Active Scanning	**High** Without ample planning and precautions	**Non-operational advised** Limit use on operational systems; only with precautions and when trusted methods are assured	**Fast** Yet varies based on desired level of detail	**High** Improves with time; depends on device capabilities	**Medium** Improves with time; depends on network access	**Medium** Often depends on execution schedule
Additive Data Sources	**Low**	**Operational** Downtime advisable to set up services	**Slow** Need to harmonize and interpret sources	**High** When information sources are accessible	**High** When information sources are accessible	**High** Inherently up to date

A Comprehensive Asset Inventory Can Lead to Risk Reduction

Each asset discovery approach can provide key asset data to help you make informed decisions about how to manage devices connected to a system. With added details about each device, you can also determine whether it is properly configured and current with the latest software updates. Some advanced passive monitoring solutions include these capabilities as part of a feature set enabling vulnerability analysis, management and reporting, but the industry's use of these products remains low even though their value proposition is high. Without the aid of automated tools, for many, the prospect of evaluating whether each connected device is up to date is daunting, especially when new product releases often outpace the practical speed at which devices can be updated. Even a single product update can be significantly time-consuming.

The product update procedure usually goes like this:

1. Test and verify updates only in a non-production environment.
2. Where possible, test the update on a product that mirrors the target device.
3. Ensure updates are obtained only from reliable sources, and integrity is maintained.
4. Establish and test a backup and recovery plan for the target device and system.
5. Prior to applying any updates to a target system, ensure it is in a non-operating state.
6. Take precautions to protect personnel, machinery and property from potential damage.
7. Cautiously apply the product update under controlled conditions to help ensure safety.
8. Reapply appropriate configurations, logic and safety and security precautions.
9. Reaffirm the safety of all potentially affected personnel and equipment.
10. Cautiously return the device and system to its operational state and verify operations.

Because IT/OT converged systems can have tens, hundreds or even more connected devices to manage, the aforementioned manual process will almost always lead to out-of-date devices and unaddressed risks. As an alternative to a blindly patching all products, consider a risk-based approach.

Risk-Based Product Update Approach

A risk-based product update strategy offers a more structured process to streamline and deliver more effective results to logically mitigate risk:

1. Determine which products are not running their most current version of software.
2. Determine which products are affected by known/reported safety or security issues.

3. Consider the products' criticality to the system and other dependent systems.
4. Consider risk exposure in context of local or remote accessibility to set priorities.
5. Evaluate each product update to determine relevance of corrective measures or actions.
6. Consult and regularly monitor threat intelligence resources for known exploitation (i.e., tactics, techniques and procedures (TTPs) relating to vulnerabilities and indicators of compromise).
7. Evaluate if risks warrant immediate update or if compensating controls are adequate.
8. Consider how disruptive an update may be to the system and the business. Give particular consideration to potential impacts to operational safety, downtime, recovery, compliance, etc.
9. Consider the order and priority to apply necessary updates—and which should wait.
10. Next, follow the above "step-by-step" process for this refined subset of product-level patches.

In concert with this process, continuous monitoring and the ongoing gathering of threat intelligence to support active defenders of IT and OT systems is imperative. This value only grows in importance when security patching is intentionally delayed or not possible, since well-informed defenders can take other precautions to monitor and mitigate unaddressed risks.

Product Vulnerability Analysis, Management and Reporting

A comprehensive asset inventory helps fulfill the objectives of CIS Control #3, continuous vulnerability management:

- Physical asset inventory, passive monitoring and active scanning activities can collect device details needed to more quickly identify which assets command attention.
- Detailed device-level information about product identities and versions can provide an even more refined list of assets needing attention.
- If automated passive and active network monitoring products are used, the workflows to track devices can be further streamlined and inventories can be kept more current and complete.

Added device details from the discovery process can also help identify connected assets most susceptible to known risks well in advance of planned maintenance windows. This information can feed into risk-based product update decisions to establish an appropriate timeline for patching. The prioritization for product-specific patching can be refined even further when known product vulnerabilities and associated risks are looked at more closely.

CVSS Breakdown: Extending Logic Even Further to Product Updates

The Common Vulnerability Scoring System (CVSS), an open, industry-standardized and accepted approach to assess the severity of security vulnerabilities to network-connected devices, produces a numerical score and qualitative results for level of risk (e.g., low, medium, high and critical). It is managed by the Forum of Incident Response and Security Teams (FIRST),[9] with input from industry contributors. CVSS v3.0[10] is the current version of the scoring system, and many companies actively use it to prioritize decisions about addressing known product-level vulnerabilities.

CVSS base scores are often listed in product vulnerability disclosures and advisories. When these disclosures are cross-referenced to a specific system's asset inventory, CVSS scores are useful to help characterize the amount of risk an affected product may potentially bring to a system at a high level, albeit every system is unique. For instance, if a product vulnerability allows for the remote execution of arbitrary code, a high CVSS base score alone might be enough of an indicator to prioritize remediation of the associated vulnerability

CVSS is based on a formula that adds specific values together to create an overall score based on severity. For asset owners seeking to determine their level of risk and remediation strategies, greater value can often be had from considering more carefully the parts compromising a CVSS score—rather than just focusing on the base score itself. See Figure 10.

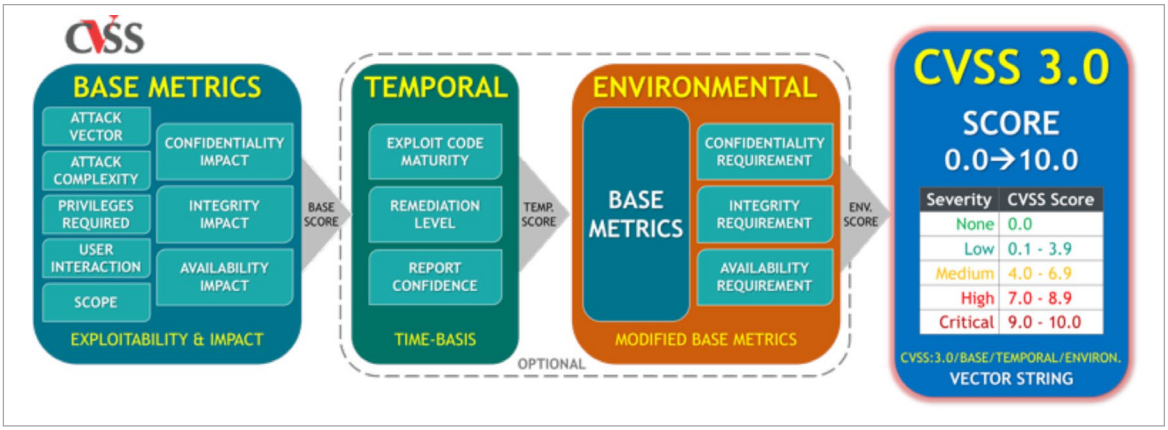

Figure 10. CVSS 3.0 Base Score Calculation

A threat = intent + opportunity + capability to cause harm. The values of the components that make up a CVSS base score provide useful guidance to a company to decide where to focus and likely where the most effective investments can be made to mitigate an associated risk. Looking more deeply into the score can help with planning and prioritization at a more granular level. For example, if the vulnerability cannot be patched in a timely fashion, it may be possible to strengthen event monitoring rules to identify any suspicious behavior associated with the asset.

The takeaway with this model: With a comprehensive asset inventory and this granular CVSS information in hand, system owners can begin to take a more calculated approach to risk management and more rationally improve the security posture of both IT and OT systems.

[9] www.first.org

[10] www.first.org/cvss

Conclusion

Unfortunately, no one can choose if they are a target or not. Adversaries make this choice for us. Today's cyber attackers seek not only financial gain, but also continue to demonstrate capabilities causing disruption, damage and even the growing likelihood for personal and widespread harm from their actions. For this reason, it's incumbent on companies to actively invest to maintain and manage risks to their critical systems, OT and IT alike.

A sustainable program, one combining physical asset inventories with network-based passive monitoring, active scanning and a risk-based approach to product patching, can be invaluable for helping companies manage risks and focus on their business imperatives. Knowing which devices are connected and managing them throughout their lifecycles is a good place to start to decide where to invest time and energy to safeguard your systems. Such inventories are critical to risk management, especially for the converged IT/OT systems of today and tomorrow.

Recommended References

- Know Thyself Better Than the Adversary – ICS Asset Identification and Tracking
  https://ics.sans.org/blog/2018/02/22/know-thyself-better-than-the-adversary-ics-asset-identification-and-tracking
- ICS Defense: It's Not a "Copy-paste" From an IT Playbook
  https://ics.sans.org/blog/2018/04/17/ics-defense-its-not-a-copy-paste-from-an-it-playbook
- Webcast: Canadian Webcast Series Part 3: ICS Defense: It's Not a "Copy-Paste" From an IT Playbook
  www.sans.org/webcasts/canadian-webcast-series-3-ics-defense-its-copy-paste-playbook-importance-intrusion-detection-compromised-prone-world-106775
- Adventures in ICS Asset Identification: Physical Inspection Style
  www.sans.org/summit-archives/file/summit-archive-1521575830.pdf
- Webcast: ICS Network Hygiene
  www.sans.org/webcasts/ics-network-hygiene-108760

About the Authors

Doug Wylie directs the SANS Industrials and Infrastructure business portfolio, helping companies fulfill business objectives to manage security risks and develop a security-effective workforce. His lengthy career spans a wide array of industries. He served as Rockwell Automation's director of product security risk management, where he founded and led its industrial cybersecurity and risk management program. Doug works around the world with companies, industry and standards bodies, and government entities to help safeguard converged IT-OT systems from contemporary cybersecurity threats. He holds the CISSP certification and numerous patents, as well as being an accomplished writer, speaker and presenter.

Dean Parsons is a SANS instructor for ICS515: ICS Active Defense and Incident Response, a member of the SANS/GIAC advisory board, and an active member of the cybersecurity community who works at both the packet and policy level. He is dedicated to educating others while helping companies address contemporary risks to business operations that stem from ever-changing threats. He is an ISO in the energy sector, security practitioner and frequent speaker at high-profile cybersecurity events. Dean earned a bachelor's degree in computer science from Memorial University of Newfoundland and holds the CISSP, GSLC, GCIA and GRID accreditations.

Sponsor

SANS would like to thank this paper's sponsor:

Last Updated: October 15th, 2018

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Houston 2018	Houston, TXUS	Oct 29, 2018 - Nov 03, 2018	Live Event
SANS Gulf Region 2018	Dubai, AE	Nov 03, 2018 - Nov 15, 2018	Live Event
SANS Sydney 2018	Sydney, AU	Nov 05, 2018 - Nov 17, 2018	Live Event
SANS DFIRCON Miami 2018	Miami, FLUS	Nov 05, 2018 - Nov 10, 2018	Live Event
SANS London November 2018	London, GB	Nov 05, 2018 - Nov 10, 2018	Live Event
SANS Dallas Fall 2018	Dallas, TXUS	Nov 05, 2018 - Nov 10, 2018	Live Event
Pen Test HackFest Summit & Training 2018	Bethesda, MDUS	Nov 12, 2018 - Nov 19, 2018	Live Event
SANS Mumbai 2018	Mumbai, IN	Nov 12, 2018 - Nov 17, 2018	Live Event
SANS Rome 2018	Rome, IT	Nov 12, 2018 - Nov 17, 2018	Live Event
SANS Osaka 2018	Osaka, JP	Nov 12, 2018 - Nov 17, 2018	Live Event
SANS San Diego Fall 2018	San Diego, CAUS	Nov 12, 2018 - Nov 17, 2018	Live Event
SANS November Singapore 2018	Singapore, SG	Nov 19, 2018 - Nov 24, 2018	Live Event
SANS ICS410 Perth 2018	Perth, AU	Nov 19, 2018 - Nov 23, 2018	Live Event
SANS Paris November 2018	Paris, FR	Nov 19, 2018 - Nov 24, 2018	Live Event
SANS Stockholm 2018	Stockholm, SE	Nov 26, 2018 - Dec 01, 2018	Live Event
SANS Austin 2018	Austin, TXUS	Nov 26, 2018 - Dec 01, 2018	Live Event
SANS San Francisco Fall 2018	San Francisco, CAUS	Nov 26, 2018 - Dec 01, 2018	Live Event
European Security Awareness Summit 2018	London, GB	Nov 26, 2018 - Nov 29, 2018	Live Event
SANS Khobar 2018	Khobar, SA	Dec 01, 2018 - Dec 06, 2018	Live Event
SANS Dublin 2018	Dublin, IE	Dec 03, 2018 - Dec 08, 2018	Live Event
SANS Santa Monica 2018	Santa Monica, CAUS	Dec 03, 2018 - Dec 08, 2018	Live Event
SANS Nashville 2018	Nashville, TNUS	Dec 03, 2018 - Dec 08, 2018	Live Event
Tactical Detection & Data Analytics Summit & Training 2018	Scottsdale, AZUS	Dec 04, 2018 - Dec 11, 2018	Live Event
SANS Frankfurt 2018	Frankfurt, DE	Dec 10, 2018 - Dec 15, 2018	Live Event
SANS Cyber Defense Initiative 2018	Washington, DCUS	Dec 11, 2018 - Dec 18, 2018	Live Event
SANS Bangalore January 2019	Bangalore, IN	Jan 07, 2019 - Jan 19, 2019	Live Event
SANS Sonoma 2019	Santa Rosa, CAUS	Jan 14, 2019 - Jan 19, 2019	Live Event
SANS Amsterdam January 2019	Amsterdam, NL	Jan 14, 2019 - Jan 19, 2019	Live Event
SANS Threat Hunting London 2019	London, GB	Jan 14, 2019 - Jan 19, 2019	Live Event
Secure DevOps Summit & Training 2018	OnlineCOUS	Oct 22, 2018 - Oct 29, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced