VOLUME 7 NUMBER 2
AUGUST 2019

CSIAC JOURNAL
A Quarterly Publication of the Cyber Security & Information Systems Information Analysis Center

RESILIENT INDUSTRIAL CONTROL SYSTEMS & CYBER PHYSICAL SYSTEMS

The Growing Cyber-Kinetic Threats

CSIAC

Cyber Security & Information Systems
Information Analysis Center

ABOUT THE CSIAC

As one of three DoD Information Analysis Centers (IACs), sponsored by the Defense Technical Information Center (DTIC), CSIAC is the Center of Excellence in Cyber Security and Information Systems. CSIAC fulfills the Scientific and Technical Information (STI) needs of the Research and Development (R&D) and acquisition communities. This is accomplished by providing access to the vast knowledge repositories of existing STI as well as conducting novel core analysis tasks (CATs) to address current, customer focused technological shortfalls.

OUR MISSION

CSIAC is chartered to leverage the best practices and expertise from government, industry, and academia in order to promote technology domain awareness and solve the most critically challenging scientific and technical (S&T) problems in the following areas:

- Cybersecurity and Information Assurance
- Software Engineering
- Modeling and Simulation
- Knowledge Management/Information Sharing

The primary activities focus on the collection, analysis, synthesis, processing, production and dissemination of Scientific and Technical Information (STI).

OUR VISION

The goal of CSIAC is to facilitate the advancement of technological innovations and developments. This is achieved by conducting gap analyses and proactively performing research efforts to fill the voids in the knowledge bases that are vital to our nation. CSIAC provides access to a wealth of STI along with expert guidance in order to improve our strategic capabilities.

WHAT WE OFFER

We provide expert technical advice and assistance to our user community. CSIAC is a competitively procured, single award contract. The CSIAC contract vehicle has Indefinite Delivery/Indefinite Quantity (ID/IQ) provisions that allow us to rapidly respond to our users' most important needs and requirements.

Custom solutions are delivered by executing user defined and funded CAT projects.

CORE SERVICES

- Technical Inquiries: up to 4 hours free
- Extended Inquiries: 5 - 24 hours
- Search and Summary Inquiries
- STI Searches of DTIC and other repositories
- Workshops and Training Classes
- Subject Matter Expert (SME) Registry and Referrals
- Risk Management Framework (RMF) Assessment & Authorization (A&A) Assistance and Training
- Community of Interest (COI) and Practice Support
- Document Hosting and Blog Spaces
- Agile & Responsive Solutions to emerging trends/threats

PRODUCTS

- State-of-the-Art Reports (SOARs)
- Technical Journals (Quarterly)
- Cybersecurity Digest (Semimonthly)
- RMF A&A Information
- Critical Reviews and Technology Assessments (CR/TAs)
- Analytical Tools and Techniques
- Webinars & Podcasts
- Handbooks and Data Books
- DoD Cybersecurity Policy Chart

CORE ANALYSIS TASKS (CATS)

- Customer tailored R&D efforts performed to solve specific user defined problems
- Funded Studies - $1M ceiling
- Duration - 12 month maximum
- Lead time - on contract within as few as 6-8 weeks

CONTACT INFORMATION

266 Genesee Street
Utica, NY 13502

1 (800) 214-7921

info@csiac.org

/DoD_CSIAC

/CSIAC

/CSIAC

CSIAC is operated by Quanterion Solutions Inc and sponsored by the Defense Technical Information Center (DTIC)
266 Genesee Street Utica, NY 13502 | 1 (800) 214-7921 | info@csiac.org | https://www.csiac.org

ABOUT THE JOURNAL OF CYBER SECURITY AND INFORMATION SYSTEMS

ABOUT THIS PUBLICATION

The Journal of Cyber Security and Information Systems is published quarterly by the Cyber Security and Information Systems Information Analysis Center (CSIAC). The CSIAC is a Department of Defense (DoD) Information Analysis Center (IAC) sponsored by the Defense Technical Information Center (DTIC) and operated by Quanterion Solutions Incorporated in Utica, NY.

Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the CSIAC. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the CSIAC, and shall not be used for advertising or product endorsement purposes.

All article figures contained in this issue were provided directly by the respective author(s), unless specifically noted otherwise.

ARTICLE REPRODUCTION

Images and information presented in these articles may be reproduced as long as the following message is noted:

"This article was originally published in the CSIAC Journal of Cyber Security and Information Systems Vol.7, No 2"

In addition to this print message, we ask that you notify CSIAC regarding any document that references any article appearing in the CSIAC Journal.

Requests for copies of the referenced journal may be submitted to the following address:

Cyber Security and Information Systems
266 Genesee Street
Utica, NY 13502

Phone: 800-214-7921
Fax: 315-732-3261
E-mail: info@csiac.org

An archive of past newsletters is available at **https://www.csiac.org/journal/.**

*To unsubscribe from CSIAC Journal Mailings please email us at **info@csiac.org** and request that your address be removed from our distribution mailing database.*

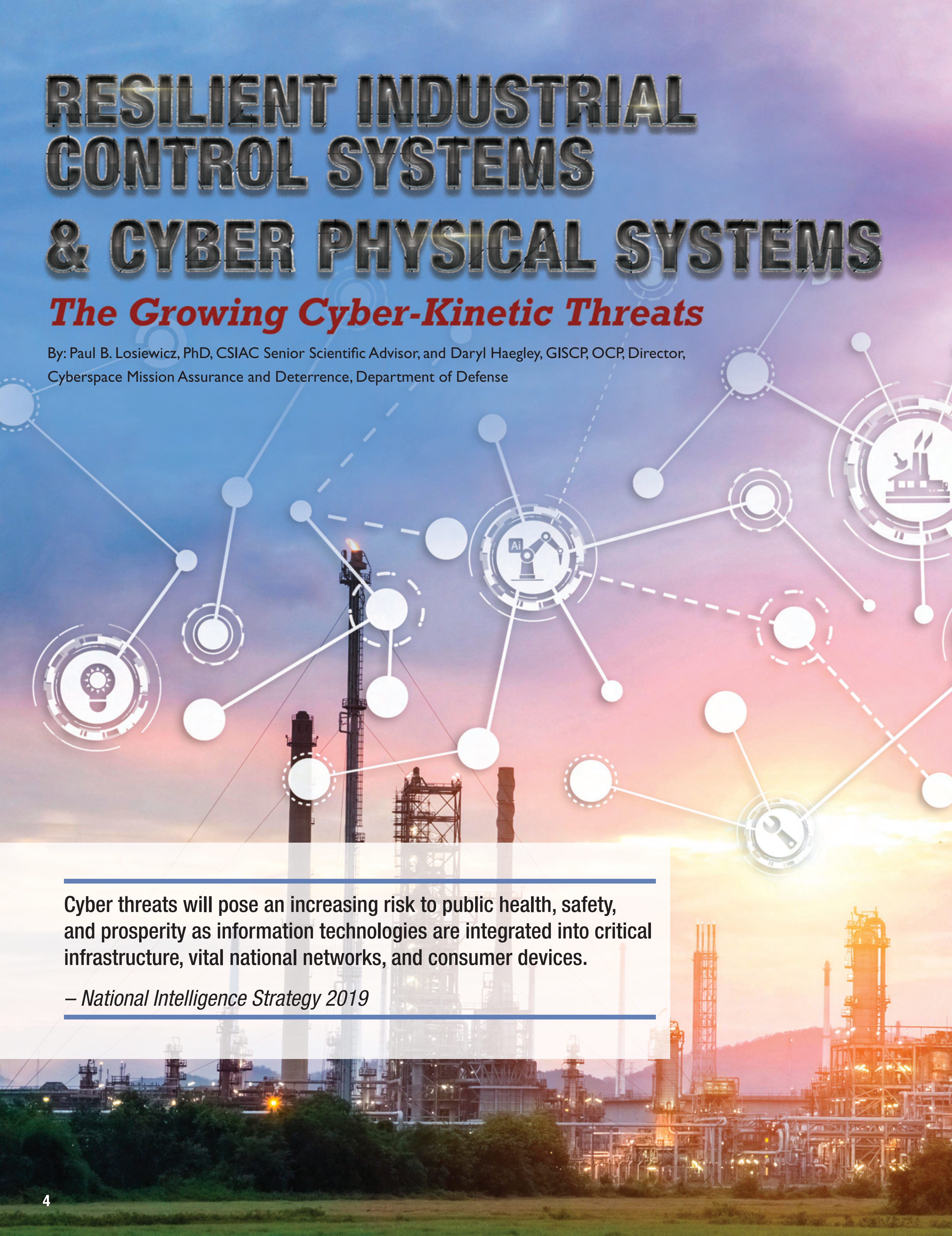
JOURNAL OF CYBER SECURITY AND INFORMATION SYSTEMS

Resilient Industrial Control Systems (ICS) & Cyber Physical Systems (CPS): The Growing Cyber-Kinetic Threats

RESILIENT INDUSTRIAL CONTROL SYSTEMS & CYBER PHYSICAL SYSTEMS

The Growing Cyber-Kinetic Threats

By: Paul B. Losiewicz, PhD, CSIAC Senior Scientific Advisor, and Daryl Haegley, GISCP, OCP, Director, Cyberspace Mission Assurance and Deterrence, Department of Defense



Cyber threats will pose an increasing risk to public health, safety, and prosperity as information technologies are integrated into critical infrastructure, vital national networks, and consumer devices.

– National Intelligence Strategy 2019

THIS EDITION OF THE CSIAC JOURNAL FOCUSES ON THE TOPIC OF CYBERSECURITY OF CYBER-PHYSICAL SYSTEMS (CPS), PARTICULARLY THOSE THAT MAKE UP CRITICAL INFRASTRUCTURE (CI).

Cyber-physical system attacks have crept from the theory to reality; 2017-2018 demonstrated the severity of the threat to Critical Infrastructure, hence to national security by way of coordinated cyber and physical attacks (CCPA). The most salient point about Cyber-Physical Systems is that they have their feet firmly planted in two worlds, the information systems enabling them and the Control Systems (CS) that execute physical effects. The understanding of a particular CPS' maintenance procedures, protections, indications and warnings, and response and recovery procedures require both technical and operational insight into the cyber and physical domains. There is huge variation across the CPS domain, and the challenges are significant. We will review here some of the most recent actions and recommendations by the U.S. Government to reduce the threat to Critical Infrastructure CPS, with a focus on Department of Defense (DoD) actions to secure its critical Infrastructure.

HOUSE ENERGY AND COMMERCE COMMITTEE REPORT

CSIAC will be examining current preparedness status in light of the most recent recommendations from the U.S. House Energy and Commerce Committee reviewing their priorities vis-à-vis 2018-19 government cyber strategies and budget authorizations.

The Oversight and Investigations Subcommittee of the House Energy and Commerce Committee released their December 7 2018 *Cybersecurity Strategy Report* (Committee on Energy and Commerce, 2018) after having spent several years analyzing cybersecurity issues with impacts across the 16 sectors defined in Presidential Policy Directive 21 ("PPD-21") *Critical Infrastructure Security and Resilience*. (The White House Office of the Press Secretary, 2013) The Subcommittee established six priorities:

PRIORITY 1: The widespread adoption of coordinated disclosure programs.

PRIORITY 2: The implementation of software bills of materials across connected technologies.

PRIORITY 3: The support and stability of the open-source software ecosystem.

PRIORITY 4: The health of the Common Vulnerabilities and Exposures (CVE) program.

PRIORITY 5: The implementation of supported lifetimes strategies for technologies.

PRIORITY 6: The strengthening of the public-private partnership model.

Of specific interest here will be the impact to the DoD and its Defense Industrial Base (DIB) of Priority 2, *implementation of software bills of materials (SBOM) across connected technologies*, Priority 5, *implementation of supported lifetimes strategies for technologies*, and Priority 6, *the strengthening of the public-private partnership model.*

A **software bill of materials** (SBOM) requirement for government acquisition is considered "key for organizations to manage their assets because they must first understand what they have on their systems before determining whether these technologies are impacted by a given threat or vulnerability" [p6]. This is essential to the effectiveness of an inventory of CS components in order to mitigate vulnerabilities. The importance of this to cyber-physical systems is that such systems are generally composed of off-the-shelf devices, many of which are replaced or upgraded piecemeal over the long life of an industrial plant or platform. They generally take on the character of a "black-box" from the operator's perspective. Provision of a "good faith" description of the software embedded in a device is key to ongoing vulnerability assessment.

The **implementation of supported lifetimes strategies for technologies** is going to have a much greater impact on the defense industrial base, as the requirement for adaptable modularity in the hitherto largely "designed for purpose" cyber-physical systems will increase component design and cost, with the added requirement that critical systems demand minimal or no system downtime.

Strengthening the public-private partnership model will certainly receive greater attention when it comes to Utilities Privatization of DoD critical infrastructure, in the face of recent criticism of the results of DoD's Privatization of military housing. Much greater oversight will be required over contract issuance, maintenance and operations, to include provision of procedures for Defense Support of Civilian Authorities (DSCA) in remediation of cyber-attacks on DoD CI that has been privatized.

THE 2018 NATIONAL CYBER STRATEGY

Following issuance of Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (Department of Homeland Security, 2017), the National Cyber Strategy for 2018 laid out priorities for the U.S. Government, to be coordinated for action by the National Security Council. (National Intelligence Strategy (NIS), 2019, p. 3) The following points are relevant to the above House Report:

- The United States Government will convene stakeholders to devise cross-sector solutions to challenges at the network, device, and gateway layers, and will encourage industry-driven certification regimes that ensure solutions can adapt in a rapidly evolving market and threat landscape [p.9]
- The United States Government will promote full-lifecycle cybersecurity, pressing for strong, default security settings, adaptable, upgradeable products, and other best practices built in at the time of product delivery [p.15]
- Capacity building allows for additional opportunities to share cyber threat information, enabling the United States Government and our partners to better defend domestic critical infrastructure and global supply chains, as well as focus whole-of-government cyber engagements [p.26]
- The United States will work with international partners, government, industry, civil society, technologists, and academics to improve the adoption and awareness of cybersecurity best practices worldwide [p. 26]

THE 2018 DOD CYBER STRATEGY

The DoD Cyber Strategy was released the same month as the National Cyber Strategy. (Department of Defense,

2018) Both documents addressed defense of Critical Infrastructure, but with more of a focus on Defense Support of Civil Authority (DSCA) via public-private partnership by DoD:

- "The Department must defend its own networks, systems, and information from malicious cyber activity and be prepared to defend, when directed, those networks and systems operated by non-DoD Defense Critical Infrastructure (DCI) and Defense Industrial Base (DIB) entities"
- "The Department seeks to preempt, defeat, or deter malicious cyber activity targeting U.S. critical infrastructure that could cause a significant cyber incident regardless of whether that incident would impact DoD's warfighting readiness or capability. Our primary role in this homeland defense mission is to defend forward by leveraging our focus outward to stop threats before they reach their targets. The Department also provides public and private sector partners with indications and warning (I&W) of malicious cyber activity, in coordination with other Federal departments and agencies". (Department of Defense, 2018, p. 2)

The obvious intersection with the House Report is the strengthening of the public-private partnership, as implied by defending non-DoD operated DCI and DIB entities, and providing the private sector military I&W. In addition, the DoD strategy requires increased practical activity in Cyber DSCA.

The summary goes on to affirm that the DoD is the Critical Infrastructure "Sector Specific Agency (SSA) for the DIB and a business partner with the DIB and DCI". (Department of Defense, 2018, p. 3) As we noted above, an SSA has clear responsibilities as laid out in PPD-21, which authorizes increased DoD interaction and oversight with industry, including utilities and vendors providing DCI services.

NATIONAL DEFENSE AUTHORIZATION ACT OF FY2019

The National Defense Authorization Act of FY 2019 (NDAA-19) addresses the DoD role in cybersecurity of Defense Critical Infrastructure (DCI) as well as national CI, and strengthening of corresponding public-private and multi-agency partnerships. In addition, it specifically calls out the cybersecurity of Facilities Related Control Systems (FRCS), a key element of CI security.

> *"DoD seeks to preempt, defeat, or deter malicious cyber activity targeting U.S. critical infrastructure"*

With respect to FRCS, the following was authorized:

- The Secretary of Defense shall designate one official to be responsible for matters relating to integrating cybersecurity and industrial control systems within the Department of Defense [FY19 NDAA SEC. 1643]

However, previous NDAAs had addressed FRCS in greater detail:

- The Secretary of Defense shall make such changes to the cybersecurity scorecard as are necessary to ensure that the Secretary measures the progress of each element of the Department of Defense in securing the industrial control systems of the Department against cyber threats, including such industrial control systems as supervisory control and data acquisition systems, distributed control systems, programmable logic controllers, and platform information technology [FY18 NDAA SEC. 1639]
- The Secretary of Defense shall, in coordination with the Director of National Intelligence, the Secretary of Energy, and the Secretary of Homeland Security, submit to Congress a report identifying significant security risks to defense critical electric infrastructure posed by malicious cyber-enabled activities [FY18 NDAA SEC. 11604]
- DoD shall issue a joint training and certification standard for the protection of control systems for use by all cyber operations forces within the Department of Defense [FY17 NDAA SEC. 1644]
- Initiate a pilot program under which the Secretary shall assess the feasibility and advisability of applying new, innovative methodologies or engineering approaches to improve the defense of control systems against cyber-attacks [FY17 NDAA SEC. 1650]
- Report the structural risks inherent in control systems and networks, assess the current vulnerabilities to cyber-attack initiated through Industrial Control Systems (ICS) at Department of Defense installations worldwide, propose a common, Department-wide implementation plan to upgrade and improve the security of control systems, assess the extent to which existing DoD military construction regulations require the consideration of cybersecurity vulnerabilities and cyber risk. The effort is to employ the capabilities of the Army Corps of Engineers, the Naval Facilities Engineering Command and the Air Force Civil Engineer Center [F17 NDAA Report 114-255]

With respect to Critical Infrastructure Cyber Defense Support for Civil Authorities (DSCA), NDAA-19 requires the following:

- A Tier 1 Exercise in Cyber Defense Support for Civil Authorities (DSCA) by U.S. Cyber Command and U.S. Northern Command [SEC. 1648]

- A pilot program in Modeling and Simulation for Cyber DSCA [SEC. 1649]
- A pilot training program for Guard elements [SEC. 1651]
- A study on the use of Reserve elements for cyber civil support [SEC. 1653]
- Immediate authorization for assignment of active duty military personnel to the DHS National Cybersecurity and Communications Integration Center (NCCIC) [SEC. 1650]

These are all significant, though overdue, preparations for DoD defense of national CI. Let us hope that the pilot programs and studies are not overcome by events. Congressional urgency was demonstrated in bill S. 79 introduced by Senator King called the "Securing Energy Infrastructure Act", which passed the Senate in December 2018. This bill includes the DoD in a multi-agency public-private pilot program headed by the Department of Energy (DOE) to "defend industrial control systems … from security vulnerabilities and exploits in the most critical systems …, including - (A) analog and non-digital control systems; (B) purpose-built control systems; and (C) physical controls". (S. 79, 2017) S.79 needs to now go to the House. However, as we see below, the DOE's National Laboratories are already working with the DoD on cybersecurity of CI.

> *"isolate and defend industrial control systems of covered entities from security vulnerabilities and exploits in the most critical systems of the covered entities."*
>
> *— Senator Angus S. King Jr (I-ME)*

MORE SITUATIONAL AWARENESS OF INDUSTRIAL CONTROL SYSTEMS (MOSAICS)

In April 2018, the Under Secretary of Defense for Research and Engineering (USD(R&E)) formally announced the approved Joint Technology Capability Demonstration (JCTD) program, which included the NORTHCOM-INDOPACOM sponsored "More Situational Awareness for Industrial Control Systems" (MOSAICS). The purpose is to enhance facilities control system situational awareness and protection via an integrated, semi-autonomous solution for situational awareness and defense of industrial control systems associated with task critical assets. The demonstration will provide an ability to semi-autonomously identify, respond to, and recover from asymmetric attacks on critical infrastructure in mission-relevant timeframes

The MOSAICS team includes NAVFAC EXWC, Sandia National Laboratories (SNL), Idaho National Laboratory (INL), and Pacific Northwest National Laboratory (PNNL).

ENHANCING PUBLIC PRIVATE PARTNERSHIPS TO CYBERSECURE CONTROL SYSTEMS

The National Security Council (NSC) has also taken steps to address "Enabling Cybersecurity through Information and Communications Technology Providers" described in the National Cyber Strategy and the lack of an effective inventory and cybersecurity training in cyber-physical system components installed in DCI systems. An industry and government working group defined priorities and the required action items to enhance security of DoD cyber-physical systems. The following were identified for action:

- Establish a program and processes for industry support of government [vulnerability] assessment and response teams through value-added augmentation of teams, participation in joint security/threat assessments of supplier control systems, and/or facilitation of incident response and forensic analysis
- Develop methods for determining the level and type of cybersecurity implemented by DoD suppliers and reporting this information to the DoD (while addressing liability and intellectual property concerns)
- Develop Information Sharing Agreement/Process/Technology for improved preparedness and response to threats and malicious activity that addresses liability and intellectual property concerns
- Develop end-to-end CS cybersecurity workforce development and training programs from secondary education through owner/operator roles

The recommendations above were submitted in December of 2018 to the Director for Critical Infrastructure Cybersecurity, of the National Security Council, with the goal of obtaining senior DHS, DoE and DoD support.

CONCLUSION

As shown by the above, the preparedness status of Defense Critical Infrastructure and the role of DoD in the protection of national critical infrastructure are rapidly evolving. Many pilot programs, capability demonstrations, studies, multi-agency cooperation and information sharing initiatives have commenced. The concern is whether we will have made sufficient progress in these before they are required by actual events. With respect to Cyber DSCA, CSIAC has access to a July 2018 after-action report on a cyber-attack on the Colorado Department of Transportation by a SamSam ransomware malware variant. The attack persisted from February to March of 2018, and resulted in the Governor's call-out of the Colorado Army National Guard cyber team to assist the state and Federal agencies responding to the attack. The lessons learned identified areas of improvement within the integration of external assets. Recommendations included the observation that "future cyber response will require external support from vendors, the National Guard and federal assets". "Pre-incident planning and coordination will help ensure the right support is provided and integrated as rapidly as possible to facilitate a cohesive response effort that leverages the capabilities of each asset". (CDOT Cyber Incident After-Action Report, 2018) These lessons-learned requirements have already been anticipated by DoD and other Federal agencies, as shown above, but our preparations remain to be tested in *extremis* on the national scale. A recent article by private sector SMEs has argued that we are at significant national risk now, and ask for a much more urgent "moonshot" cyber defense of CI program by the Federal government. (Mroz & Kelly, 2019)

REFERENCES

National Intelligence Strategy (NIS). (2019). The National Intelligence Strategy of the United States of America. Retrieved from https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf

Committee on Energy and Commerce. (2018). (Rep.). Retrieved from https://energycommerce.house.gov/

Department of Defense. (2018). Department of Defense Cyber Strategy. Retrieved from https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

Department of Homeland Security. (2017, May 11). Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. Retrieved from https://www.dhs.gov/executive-order-strengthening-cybersecurity-federal-networks-and-critical-infrastructure

Mroz, R., & Kelly, S. (2019, February 26). Cybersecurity threats to US infrastructure warrant 'moonshot' response. Retrieved from https://thehill.com/opinion/cybersecurity/431079-cybersecurity-threats-to-us-infrastructure-warrant-moonshot

(2018, December 20). S.79 - 115th Congress (2017-2018): Securing Energy Infrastructure Act. Retrieved from https://www.congress.gov/bill/115th-congress/senate-bill/79

The White House. (2018). National Cyber Strategy of the United States of America . Retrieved from https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

The White House Office of the Press Secretary. (2013, February 12). Presidential Policy Directive -- Critical Infrastructure Security and Resilience. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

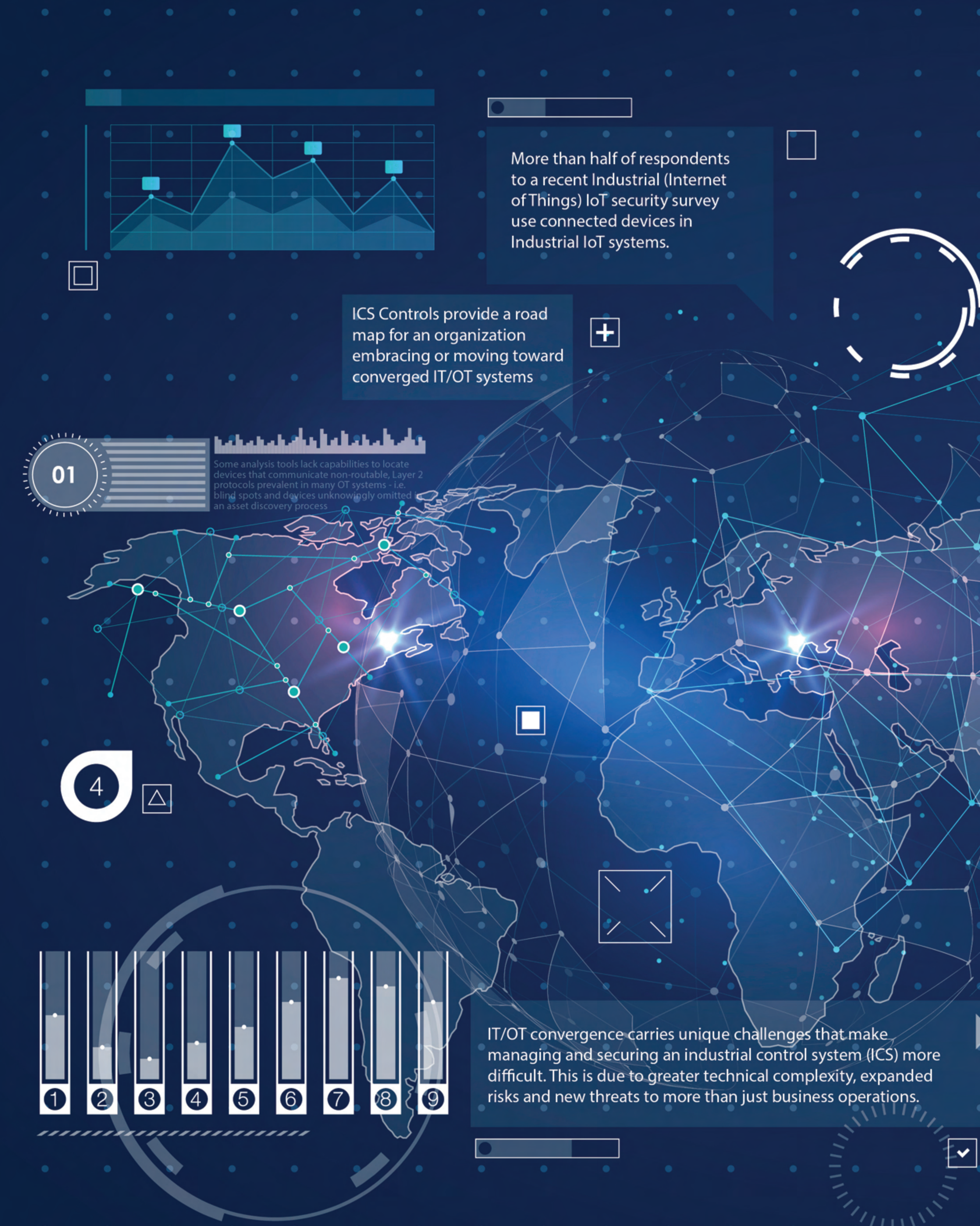
Willis, M. ***CDOT Cyber Incident After-Action Report.***

DR. PAUL B. LOSIEWICZ is Senior Scientific Advisor for the Cybersecurity and Information Systems Information Analysis Center (CSIAC), a DoD information analysis center operated by Quanterion Solutions Incorporated for the Defense Technical Information Center (DTIC), Ft Belvoir, MD. He has over 30 years of DoD RDT&E experience, including R&D for Navy Special Warfare, Air Force Research Laboratory, Air Force Office of Scientific Research, and Office of Naval Research Global (ONRG). Dr. Losiewicz has two patents.

Recent accomplishments include:

- Presented "Data Sets for Autonomous Intelligent Cyber-defense Agent Research" at the 1st NATO-Industry workshop on Autonomous Cyber Defence, Cranfield University, UK in March 2019
- Co-authorship of two papers on DoD Facilities Related Control Systems Cyber Security with Mr. Daryl Haegley, SECDEF Principle Cybersecurity Advisor, and one paper with Benoit LeBlanc and Sylvain Hourlier of L'Ecole Nationale Supérieure de Cognitique entitled "A Program for Effective and Secure Operations by Autonomous Agents and Human Operators in Communications-Constrained Tactical Environments"; ARL-SR-0395
- Served on the NATO Research Task Group (RTG) IST-152 "Intelligent Autonomous Agents for Cyber Defense and Resilience", chaired by Dr. Alexander Kott, Army Research Laboratory Chief Scientist
- Organized a DoD briefing Session on Industrial Control Systems Cybersecurity for Department of Homeland Security at the Industrial Control Systems Joint Working Group (ICSJWG) with representatives of OASD (E,I&E), INDO-PACOM and Sandia National Labs

MR. DARYL HAEGLEY has 30 years of military, federal civilian and commercial consulting experience, currently overseeing the cybersecurity effort to secure control systems / operational technology for the Department of Defense (DoD). He leads DoD policy, security assessments, cyber range capability developments, SECDEF scorecard requirements and Risk Management Framework (RMF) process improvements. Contributing author to NIST SP 800-82 R2 'Guide to Industrial Control Systems Security,' Unified Facilities Criteria 4-010-06 'Cybersecurity of Facility-Related Control Systems' and Springer publication 'Security of Industrial Control Systems.' He maintains four certifications, three Masters' degrees, two college loans & one patent.



More than half of respondents to a recent Industrial (Internet of Things) IoT security survey use connected devices in Industrial IoT systems.

ICS Controls provide a road map for an organization embracing or moving toward converged IT/OT systems

Some analysis tools lack capabilities to locate devices that communicate non-routable, Layer 2 protocols prevalent in many OT systems - i.e. blind spots and devices unknowingly omitted in an asset discovery process

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.

Practical Industrial Control System (ICS) Cybersecurity: IT AND OT HAVE CONVERGED—DISCOVER AND DEFEND YOUR ASSETS

By: Doug Wylie and Dean Parsons, SANS Technology Institute

MORE THAN HALF OF RESPONDENTS TO A RECENT INDUSTRIAL (INTERNET OF THINGS) 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. (Filkins, 2018)

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.

INTRODUCTION

This article 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

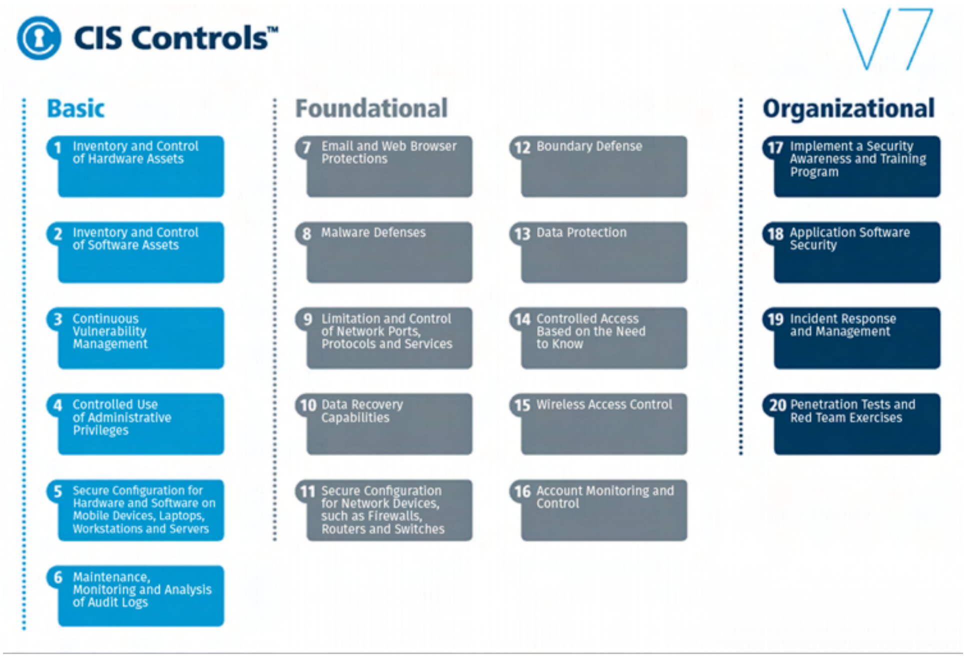
A company's security posture depends on many factors and will vary over time:

- 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.


CIS Controls™ V7

Basic
1 Inventory and Control of Hardware Assets
2 Inventory and Control of Software Assets
3 Continuous Vulnerability Management
4 Controlled Use of Administrative Privileges
5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational
7 Email and Web Browser Protections
8 Malware Defenses
9 Limitation and Control of Network Ports, Protocols and Services
10 Data Recovery Capabilities
11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12 Boundary Defense
13 Data Protection
14 Controlled Access Based on the Need to Know
15 Wireless Access Control
16 Account Monitoring and Control

Organizational
17 Implement a Security Awareness and Training Program
18 Application Software Security
19 Incident Response and Management
20 Penetration Tests and Red Team Exercises

Figure 1. Center for Internet Security Controls Version 7

Currently in Version 7[1], 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.

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. (Center for Internet Security, Inc (CIS), Williams, & Boeckman) 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.

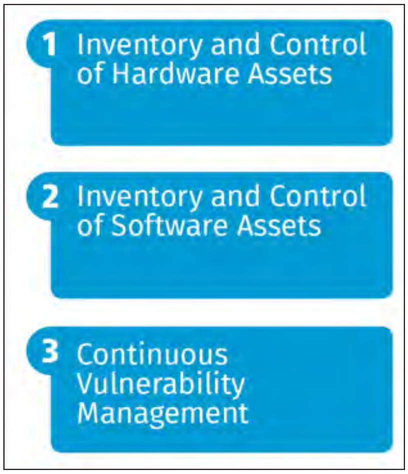

1 Inventory and Control of Hardware Assets
2 Inventory and Control of Software Assets
3 Continuous Vulnerability Management

Figure 2. The First Three CIS Controls

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

[1] https://www.cisecurity.org/controls/

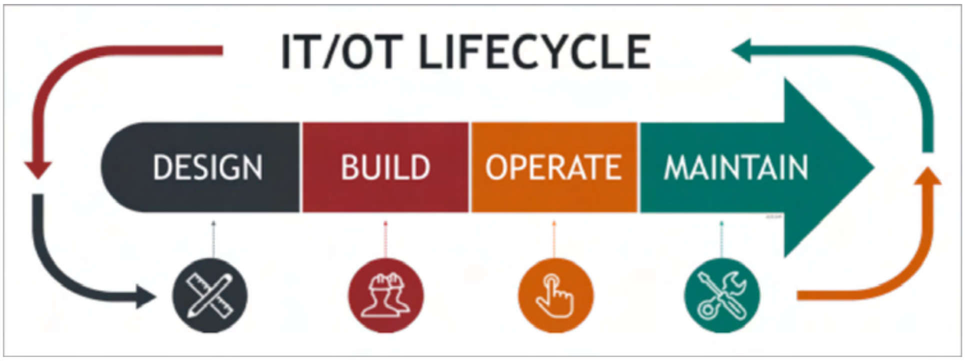


Figure 3. The IT/OT Lifecycle Process

> 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."("CIS Controls Implementation Guide for Industrial Control Systems Launch Event", 2018)

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.

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.

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.

"ICS Controls provide a road map for an organization embracing or moving toward converged IT/OT systems"

Physical Asset Inventory

While physical asset 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 not 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.

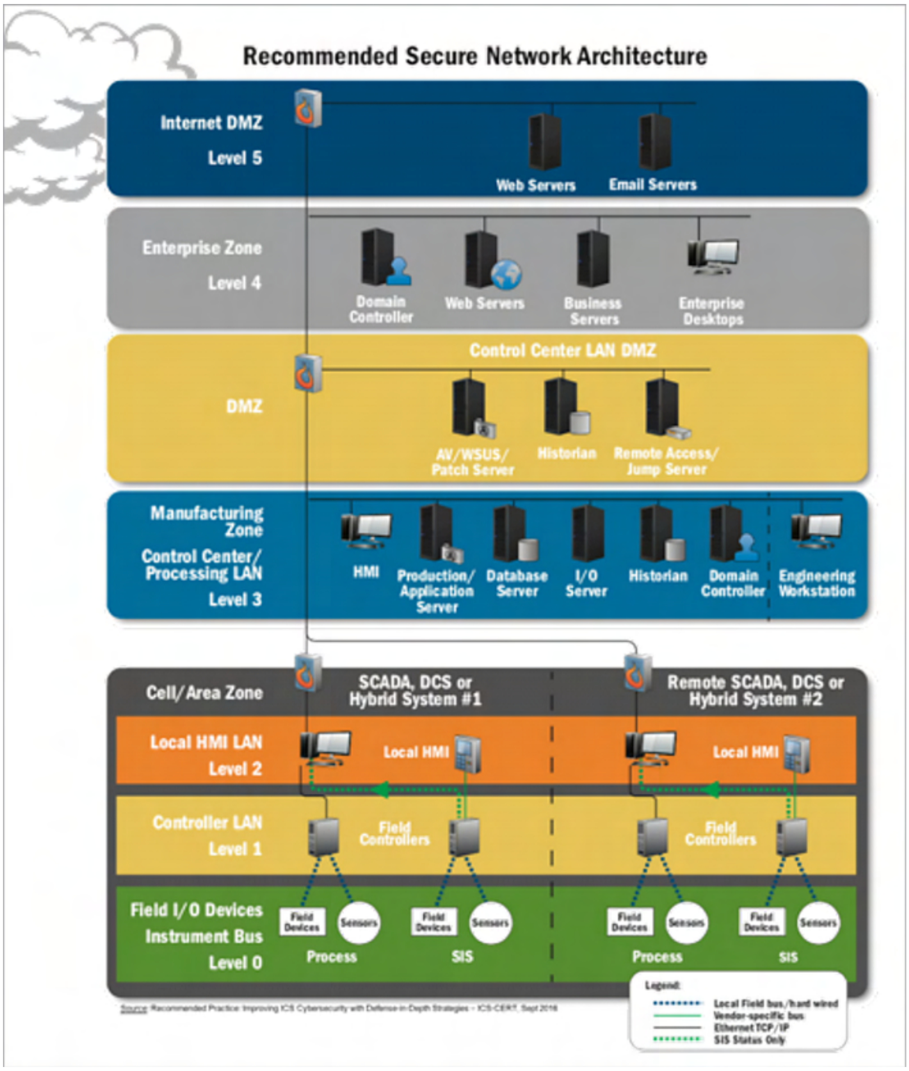
The takeaway: Conduct a physical inventory, but treat this step as part of a larger asset discovery process.

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. (Department of Homeland Security, 2019)

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



Source: Recommended Practice: Improving ICS Cybersecurity with Defense-in-Depth Strategies – ICS-CERT, Sept 2016

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

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 on 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).

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.

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

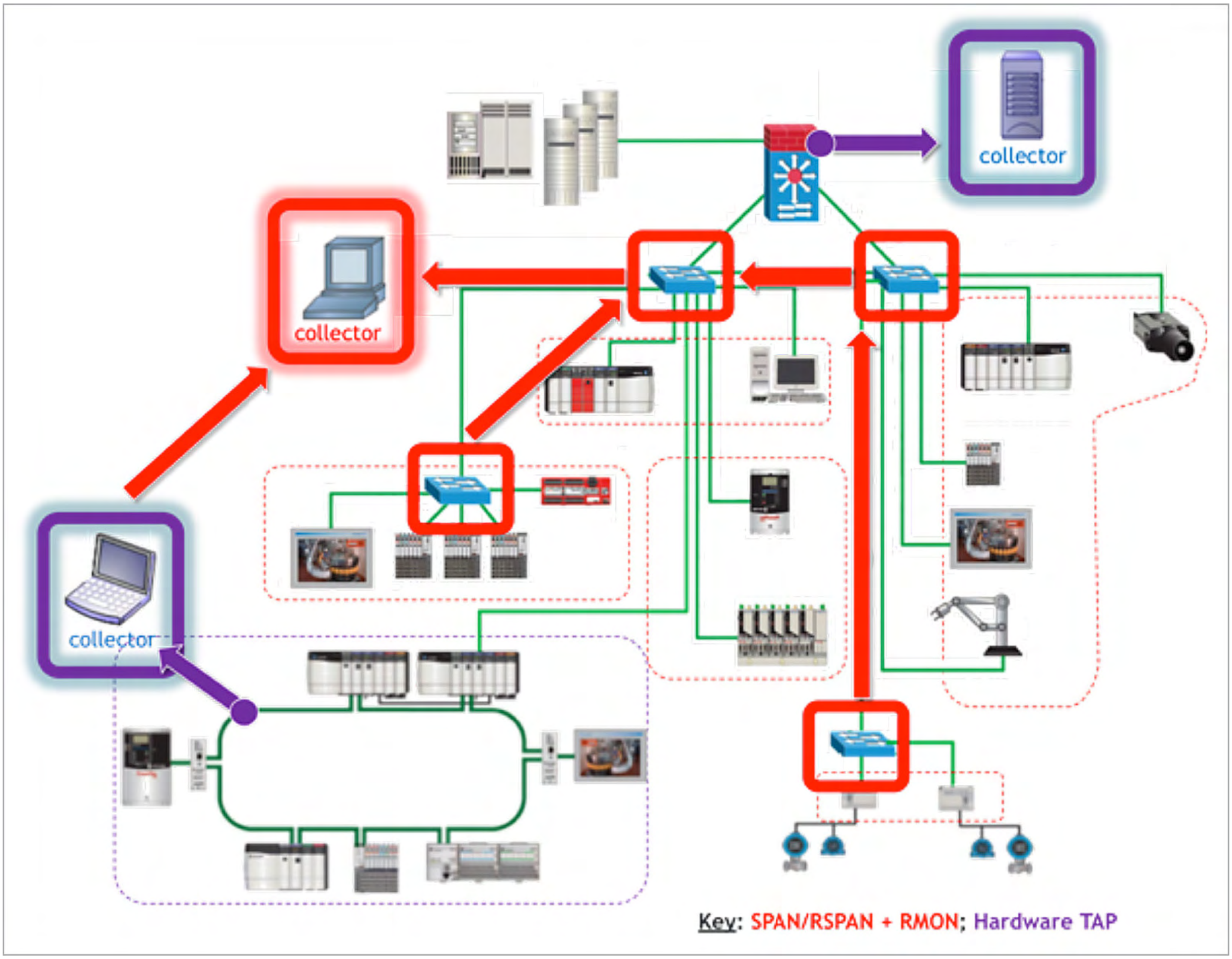
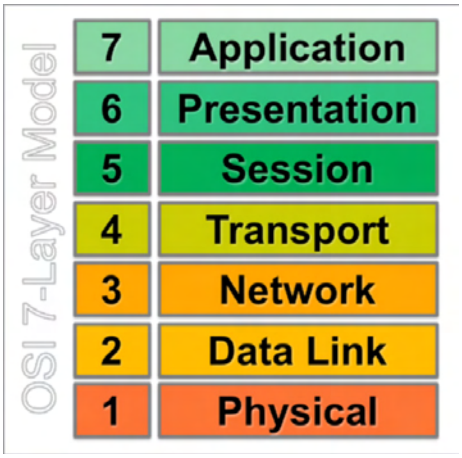


Figure 5. Network Architecture with Listening Points and Traffic Collectors

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[2]. 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 (International Organization for Standardization (ISO), ISO/IEC standard 7498-1:1994, 1996) is a useful reference when considering communication sources and information types to be evaluated via traffic capture, analysis and monitoring tools (see Figure 6).

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



7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical

Figure 6: ISO/OSI Basic Reference Model for Communications

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

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.

> *"Some analysis tools lack capabilities to locate devices that communicate non-routable, Layer 2 protocols prevalent in many OT systems - i.e. blind spots and devices unknowingly omitted in an asset discovery process"*

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.

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). (Lee, "ICS515: ICS Active Defense and Incident Response")

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).

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.

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.

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

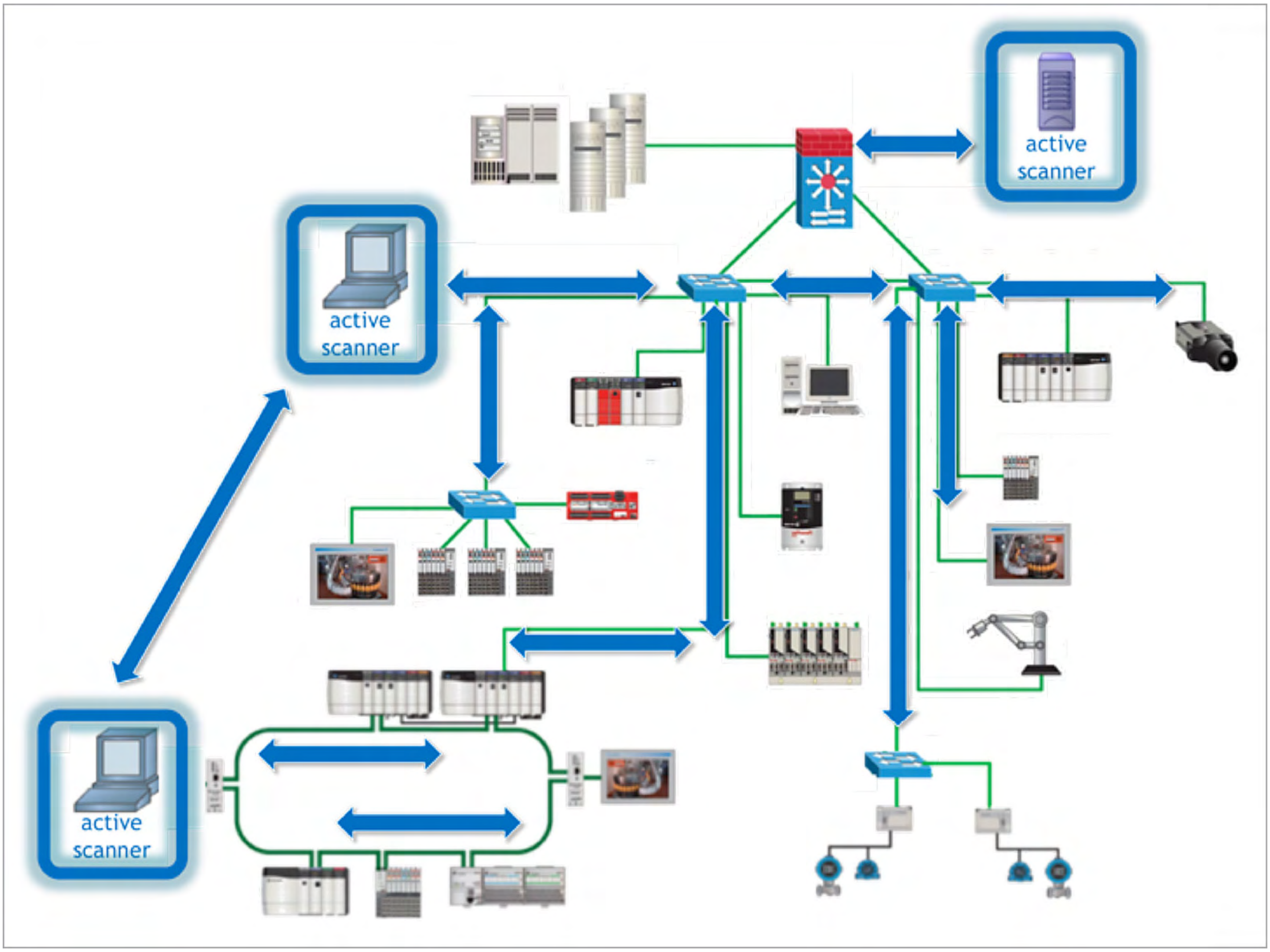


Figure 7. Network Architecture with Active Scanners

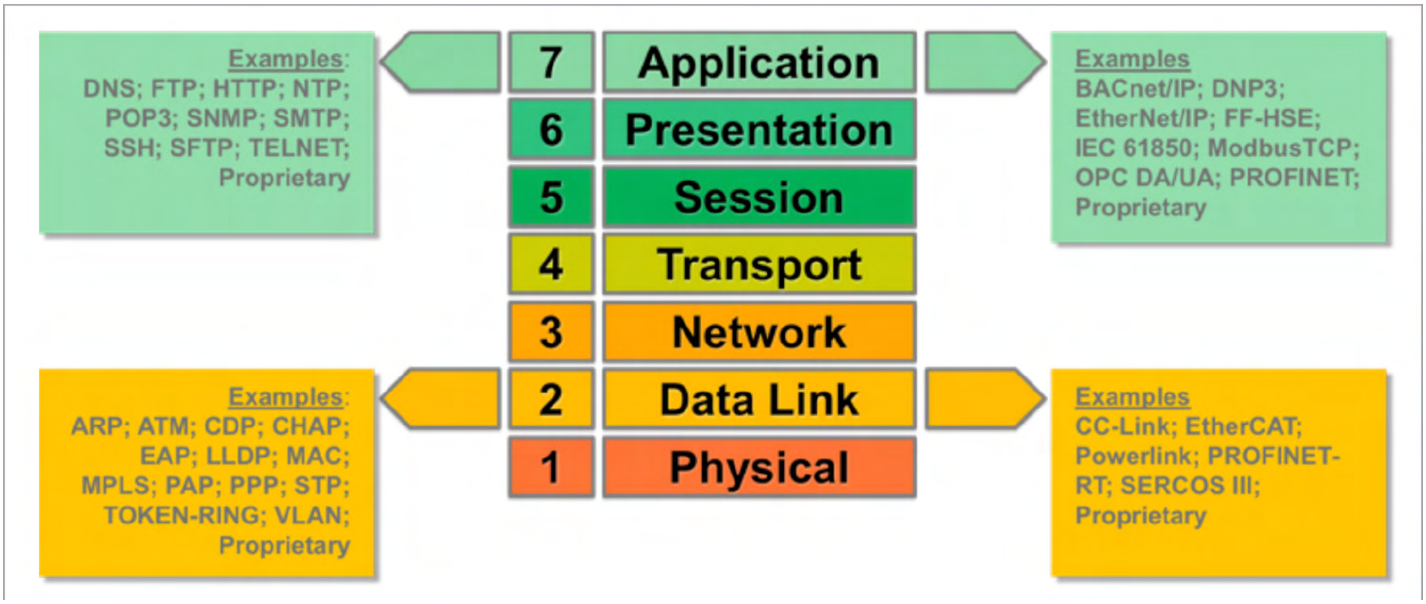


Figure 8. Popular IT and OT Protocols at OSI Layer 2 and Layer 7

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).

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.

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.

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

Table 1: Asset Discovery Approaches and Their Attributes

Type	Risk	Target System Status	Speed	Accuracy	Coverage	Current and 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

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.

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.

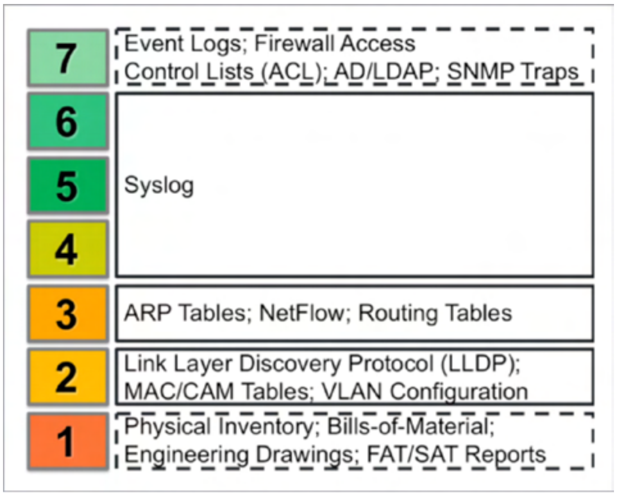
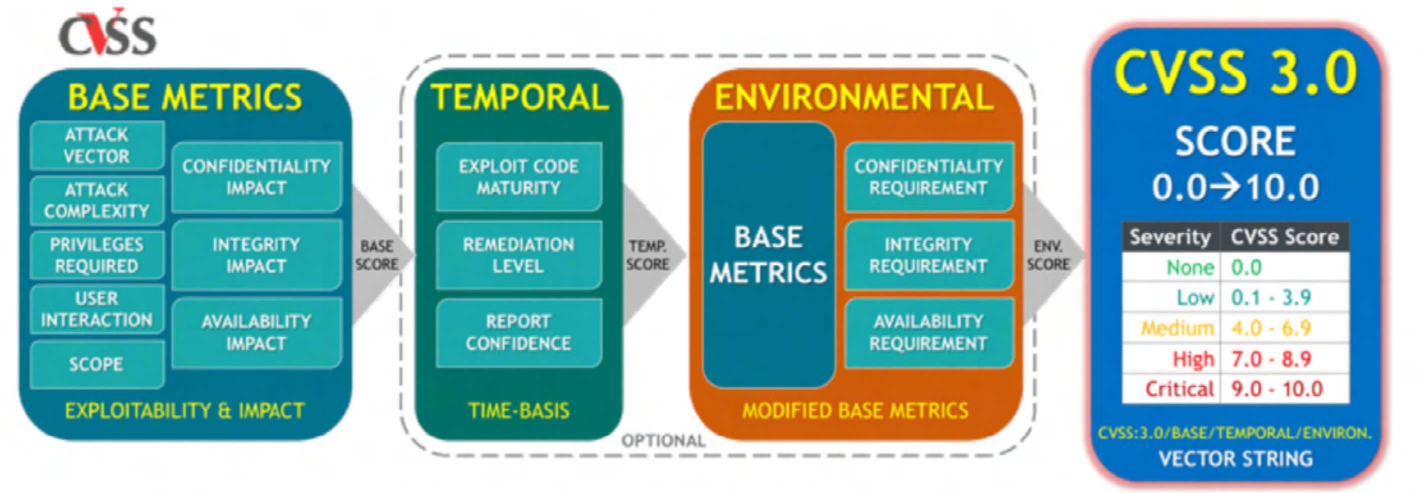

7
Event Logs; Firewall Access Control Lists (ACL); AD/LDAP; SNMP Traps
6
5
Syslog
4
3
ARP Tables; NetFlow; Routing Tables
2
Link Layer Discovery Protocol (LLDP); MAC/CAM Tables; VLAN Configuration
1
Physical Inventory; Bills-of-Material; Engineering Drawings; FAT/SAT Reports

Figure 9. Additive Information Sources from Devices

Because IT/OT converged systems can have tens, hundreds or even more connected devices to manage, the aforementioned manual process will



Severity	CVSS Score
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

Figure 10: CVSS 3.0 Base Score Calculation

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)[3], with input from industry contributors. CVSS v3.0[4] 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

[3] https://www.first.org
[4] https://www.first.org/cvss/

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.

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.

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.

REFERENCES

Center for Internet Security, Inc (CIS). CIS Controls™ Implementation Guide for Industrial Control Systems. Retrieved from https://www.cisecurity.org/white-papers/cis-controls-implementation-guide-for-industrial-control-systems/

Department of Homeland Security. (2019, June 5). National Cybersecurity & Communications Integration Center. Retrieved from http://www.dhs.gov/national-cybersecurity-and-communications-integration-center

Filkins, B. (2018, July 18). The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns. Retrieved from http://www.sans.org/reading-room/whitepapers/analyst/2018-industrial-iot-security-survey-shaping-iiot-security-concerns-38505

International Organization for Standardization (ISO). (1996, June 1). Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model. Retrieved from http://www.iso.org/standard/20269.html

Lee, R. M. ICS515: ICS Active Defense and Incident Response. Retrieved from https://www.sans.org/course/industrial-control-system-active-defense-and-incident-response

Wylie, D. (2018, June 28). Retrieved from https://www.cisecurity.org/webinar/cis-controls-implementation-guide-for-industrial-control-systems-launch-event/

RECOMMENDED READING

- 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 (https://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 (https://www.sans.org/summit-archives/file/summit-archive-1521575830.pdf)
- Webcast: ICS Network Hygiene www.sans.org/webcasts/ics-network-hygiene-108760

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. He also serves on the SANS Technology Institute advisory board for the Industrial Control Systems Security graduate certificate program. His lengthy career spans a wide array of industries. He formerly served as Rockwell Automation's global director of product security risk management, where he 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.

ADDRESSING BOTH SIDES OF THE CYBERSECURITY $\Sigma qu[a+10^{n}]$

By: Donnie W. Wendt

TODAY'S CYBER DEFENDERS FIND THEMSELVES AT A DISADVANTAGE DESPITE TECHNOLOGICAL ADVANCES IN CYBER DEFENSE. AMONG THE CHIEF CAUSES OF THIS DISADVANTAGE IS THE ASYMMETRY IN A CYBER CONFLICT THAT FAVORS THE ATTACKER.

On one side of the equation, defenders must improve detection and response times to avert or mitigate attacks. On the other side of the equation, defenders must slow the time to compromise by disrupting the attacker.

Under the assumption that increased cyberspace security is the main goal of cybersecurity policies, the current cybersecurity approach is not working. Cyberspace seems to have become less secure despite increasing expenditures on various aspects of cyber-security. The defenders continue to face significant challenges despite technological advances in security detection, prevention, and monitoring. Firewalls, vulnerability management, and intrusion prevention systems have proven ineffective against advanced threat actors. Attackers have successfully created attacks targeting vulnerabilities of which defenders are unaware, and the attackers have avoided detection through effective concealment. (Raymond, Conti, Cross, and Nowatkowski, 2014) Not only is detection failing, but the remediation time for cyber-attacks continues to increase. (Suby & Dickson, 2015)

THE ATTACKER'S ADVANTAGE

Cyber attackers have the advantage because the attackers need to exploit a single vulnerability whereas the defender has the much costlier task of mitigating all vulnerabilities. Attackers can choose the time and place of the attack which further disadvantages the defenders. The ease by which an attacker can acquire and use an exploit coupled with the low likelihood of detection favors the attackers. (Zheng & Lewis, 2015) Once inside a network, individual actors in the cyber domain can have an asymmetric advantage and possess highly dangerous capabilities.

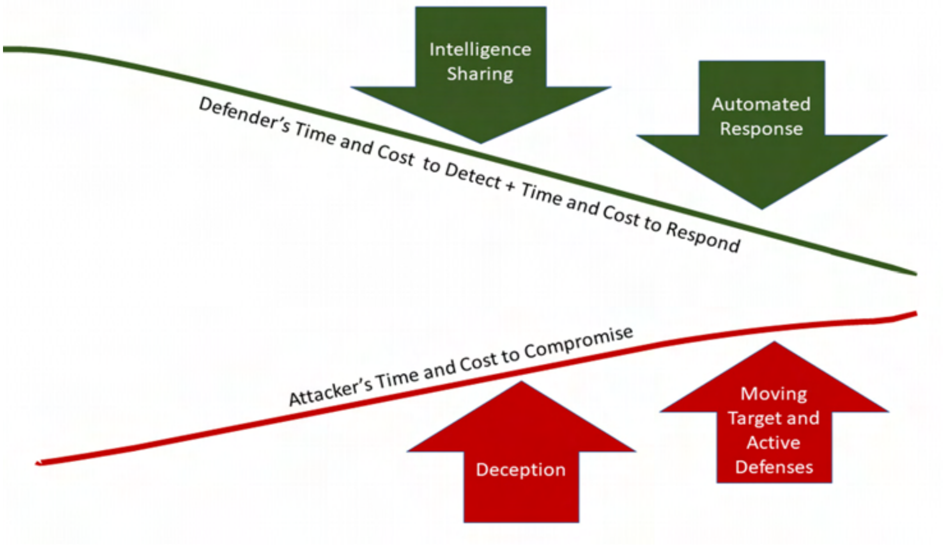

Intelligence Sharing
Automated Response
Defender's Time and Cost to Detect + Time and Cost to Respond
Attacker's Time and Cost to Compromise
Deception
Moving Target and Active Defenses

Figure 1: Addressing Both Sides of the Equation

An attack must first be detected before a response is possible. The increasing sophistication of attacks makes the identification of both successful and unsuccessful attacks more difficult. The detection of the attack should occur as early in the cyber-attack lifecycle, or cyber kill chain, as possible to minimize the ramifications of the attack. Many sophisticated attacks, known as advanced persistent threats (APT), seek to establish persistence from which to operate and call out to a command-and-control system. (Byrne, 2015) The attacker can establish this persistence because organizations are often unaware of what software products are installed on each device.

Attackers who invest in an APT are highly motivated and will devote significant time to compromise a target to achieve a specific goal. These threat actors will map out multiple paths to reach the target and pivot their attack as necessary to reach the end goal. (Byrne, 2015) With the expanding complexity of systems, organizations present an increasingly large attack surface. The greater the attack surface, the more opportunities the attacker has to penetrate the perimeter and establish a persistence within the environment. Detection of APTs by either signature or anomaly detection methods is challenging because APTs are crafted for a particular target and often use unique attack vectors. (Virvilis, Serrano & Vanautgaerden, 2014)

> *"Attackers who invest in an APT are highly motivated and will devote significant time to compromise a target to achieve a specific goal. "*

THE DEFENDER'S DISADVANTAGE

Organizations typically invest in point solutions to address cybersecurity issues. Such an approach results in organizations attempting to link together many disparate solutions into an architecture and framework unique to each organization. (Fonash & Schneck, 2015) Defenders must select and configure an increasing number of defenses of increasing complexity. Much of the configuring of defenses is conducted manually, and the defenders often do not have a full understanding of the integration points between the defenses or the associated risks with each defense. (Soule, Simidchieva, Yaman, Loyall, Atighetchi, Carvalho & Myers, 2015) Organizations may add defenses that provide little increase in security while introducing unacceptable costs and increasing the attack surface. New defenses may have adverse side effects when deployed in combination with existing defenses. Further, a fundamental limitation of reactive defense is that network connectivity automatically amplifies the effect of the attacks; however, reactive defenses are not so amplified.

Attackers can often reuse exploits due to a lack of effective, timely information sharing amongst defenders. If the community does not share information concerning cyber-attacks, the attackers can reuse the same attack methods on multiple organizations. Without information sharing, each organization is left to detect and analyze each attack. Organizations do not have the resources and knowledge to defend against the myriad of attacks when working independently.

Defenders also face a paradox of having too much data to deal with, while at the same time, missing critical data

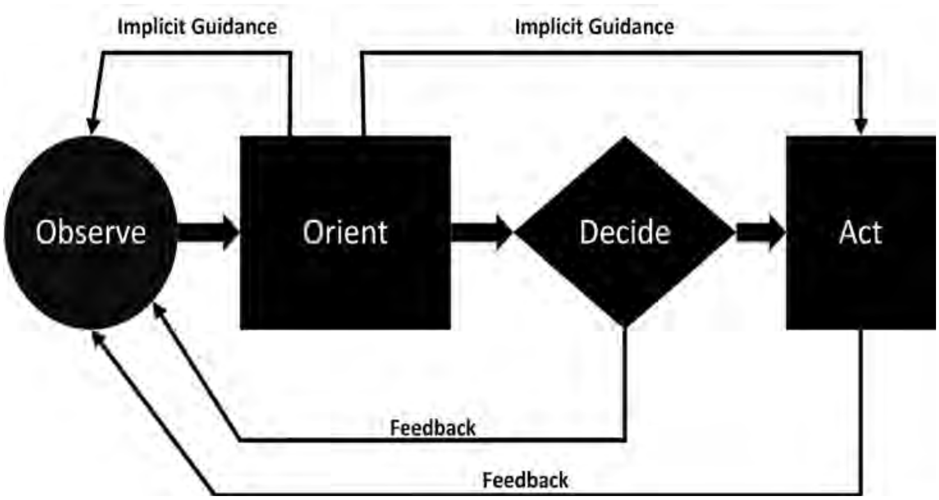


Figure 2: The OODA Loop

necessary to detect and analyze cyber attacks. (Brown, Gommers & Serrano, 2015) Cybersecurity operational environments are dynamic and can differ greatly between implementations. The vast volume of data and the wide variety of security devices challenge the analytical capabilities of human responders. (Lange, Kott, Ben-Asher, Mees, Baykal & Vidu, 2017) The rate of legitimate changes within large, complex enterprise systems makes the empirical validation and quantification of the attack surface prohibitively challenging. (Soule, Simidchieva, Yaman, Loyall, Atighetchi, Carvalho & Myers, 2015) Organizations require tools to manage the unlimited amounts of information they now collect from numerous sources. The knowledge tools must convert the information into actionable knowledge.

CLOSING THE GAP

Cyber defenders must address both sides of the equation to narrow the gap between the attackers' time to compromise and the defenders' time to respond. An integrated approach involving security orchestration, automated response, information sharing, and advanced defense methods can reduce the competitive gap between attackers and defenders. Figure 1 depicts intelligence sharing, automated response, deception techniques, and advanced defensive methods working together to reduce the gap between the time to compromise and the time to respond.

4.1 Boyd's OODA Loop

The *observe-orient-decide-act* (OODA) loop theory, developed by military strategist and Air Force pilot John Boyd, originally referred to gaining superiority in air combat. (Mepham, Ghinea, 2014)

> *"Changing the situation faster than the attacker could observe-orient-decide-act, lessening dwell time and giving the attacker less of a chance to Act."*

The concept behind the OODA loop was that completing an OODA loop quicker than the opponent prevented the opponent from gaining superiority in air combat [11]. Organizations can also apply the OODA loop to cyber-incident response. If the defender can respond quickly to the attacker's actions, before the attacker can complete the OODA loop, the defender can gain cyber superiority. (Mepham, Ghinea, 2014)

In Boyd's seminal presentation on air combat in which Boyd developed the OODA loop concept, Boyd suggested that to win it is necessary to get inside the adversary's OODA loop. Interrupting the adversary's OODA loop can cause confusion and disorder for the opponent. (Boyd, 1986) Changing the situation faster than the attacker could observe-orient-decide-act, lessening dwell time and giving the attacker less of a chance to "Act". Also, by inserting oneself into the opponent's OODA loop, a combatant can discover the strengths, weaknesses, tactics, and intent of the adversary. (Boyd, 1986)

The underlying goal of the OODA loop is to be faster than the enemy. This goal means that the cyber defender must streamline his command and control while also interfering with the attacker's command and control. In applying the OODA loop theory to cybersecurity, intelligence sharing and automated response help speed the defender's OODA loop. Whereas, deception and moving target defenses operate within the opponent's OODA loop, slowing and confusing the attacker.

Operating in the attacker's OODA loop using deceptions that disrupt the attacker's orientation will compromise the attacker's subsequent decisions and actions. (Almeshekah & Spafford, 2016 & Stech, Heckman & Strom, 2016) Deception-based defenses provide an advantage to the defenders as the deceptive information will affect the attacker's observation and orientation stages of the OODA loop. (Almeshekah & Spafford, 2016 & Stech, Heckman & Strom, 2016) Defensive deceptions can help consume the attacker's resources and disrupt decision-making by assigning additional tasks to the attacker. (Stech, Heckman & Strom, 2016) Also, by slowing the attacker, the defender gains more time to further orient, decide, and act. (Almeshekah & Spafford, 2016)

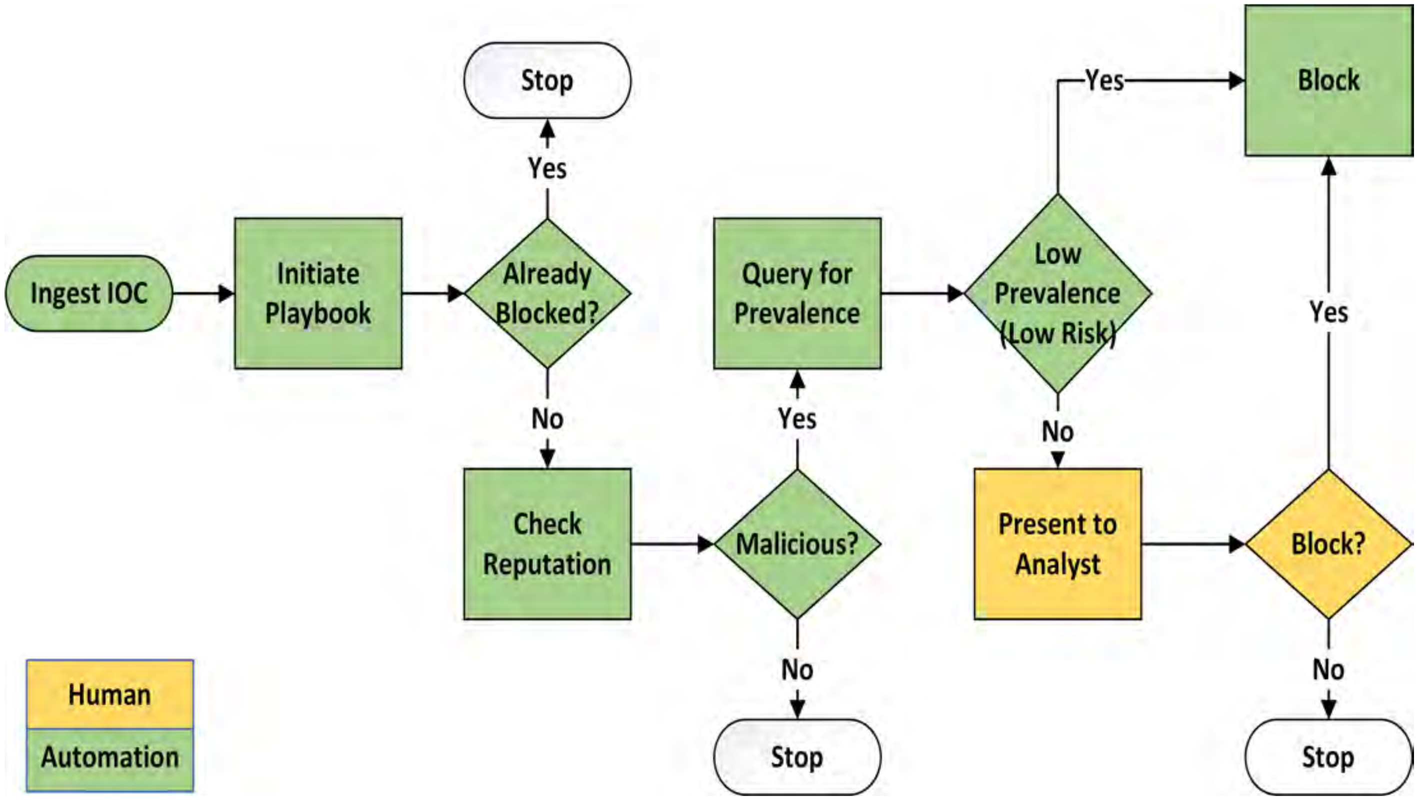


Figure 3: Example IOC Playbook

4.2 Automated Response

Current human-centered cyber defense practices cannot keep pace with the speed and pace of the threats targeting organizations. (Johns Hopkins Applied Physics Laboratory, 2016) There is a need to drastically increase the speed of both the detection of and response to cyber-attacks. Many risk-based decisions must be automated to facilitate this increase in detection and response speed. (Fonash & Schneck, 2015) Human involvement must become more oversight and less direct involvement. Increasing the speed and efficiency of detection and response requires rapid exchange of threat and incident detail among the automated defense systems. Such rapid exchange will require interoperability between systems at the technical, semantic and policy levels. (Fonash & Schneck, 2015)

The Department of Homeland Security (DHS), the National Security Agency (NSA), and Johns Hopkins University Applied Physics Lab (JHU-APL) jointly developed the Integrated Adaptive Cyber Defense (IACD) framework in collaboration with private industry leaders. (Johns Hopkins Applied Physics Laboratory, 2016) The DHS and the NSA started the effort in 2014 to help address the continued malicious cyber-attacks on government and private industry. Current human-centered cyber defense practices cannot keep up with the increasing volume and speed of cyber threats. The IACD framework seeks to close this gap by automating cyberdefense tasks and increasing information sharing between enterprises. (Walton, Watson, Kosecki, Mok & Burger, 2018) The IACD framework uses automation to increase the speed of detection of and response to cyber threats and relies on information sharing to limit the reusability of exploits against the community. (Johns Hopkins Applied Physics Laboratory, 2016) By implementing the traditional OODA loop at speed and scale, IACD seeks to decrease cyber operation timelines from months to milliseconds. (Johns Hopkins Applied Physics Laboratory, 2016)

In 2018, the Financial Services Information Sharing and Analysis Center (FS-ISAC) and JHU APL partnered with three financial institutions to pilot the IACD framework. (Walton, Watson, Kosecki, Mok & Burger, 2018) The financial sector IACD pilot was designed to demonstrate the deployment of the framework into production environments to foster adoption within the sector. The integrated pilot sought to understand how intelligence enrichment could assist different organizations with varying policies and risk tolerances to determine what action to take. The pilot focused on the ingestion of threat intelligence from the FS-ISAC at three financial institutions, Huntington Bank, Mastercard, and Regions Bank. Each pilot financial institution implemented the IACD framework to take automated action on the threat intelligence. The results of the pilot showed that automation decreased the average time for the FS-ISAC to generate an indicator of compromise (IOC) from nearly six hours to one minute. (Frick, 2018) Also, the automated receipt, enrichment, and triage of IOCs by the financial institutions were reduced from an average of four hours to three minutes. In total, the automation reduced the average time to produce an IOC, disseminate an IOC, and initiate a response from approximately 10 hours to 4 minutes.

4.3 Intelligence Sharing

Reactive cyber defense strategies are insufficient to deal with the increasing persistence and agility of cyber attackers. (Zheng & Lewis, 2015) Information sharing amongst defenders can increase the efficiency in detecting and responding to cyber-attacks. When one organization detects an attack, collaborating organizations can use the information to take preventative measures. (Zheng & Lewis, 2015) Community sharing of attack intelligence fosters collective action. The number and sophistication of cyber-attacks require collective response action. Collective action requires that participants share and make use of information from attempted or successful attacks. For collective action to be effective, the other systems within the community must be informed of an attack before those systems are themselves attacked.

Intelligence sharing and automated response work together to reduce the defender's cost and time. Information sharing can increase efficiency in detecting and responding to cyber-attacks. Collaborating organizations can use the information shared by one organization to take preventative measures to thwart attacks. (Zheng & Lewis, 2015) Collective action, fostered by community sharing of intelligence can act as an immune system for the collaborating organizations. As shown in the FS-ISAC pilot, security automation can increase the speed of response to an attack and the speed of proactively applying intelligence.

Maintaining a secure and resilient cyber ecosystem requires more than the sharing of attack information. Organizations must use the shared information to assess the effectiveness of courses of actions taken and develop, evaluate, and implement alternative courses of action as needed. Cyber intelligence aims to support decision making regarding the detection of, prevention of, and response to cyber attacks by developing reliable conclusions based on facts. (Brown, Gommers & Serrano, 2015) Organizations need to move beyond creating interoperable systems to share data and develop methods to generate value from the shared information.

4.4 Deception

Defenders should consider using deception as a critical component of their defensive posture since attackers have repeatedly demonstrated the ability to subvert traditional defenses. (Raymond, Conti, Cross, and Nowatkowski, 2014) Conventional defensive tactics focus on detecting and preventing the attacker's actions while deception focuses on manipulating the attacker's perceptions. (Almeshekah & Spafford, 2016 & Stech, Heckman & Strom, 2016 & DeFaveri & Moreira, 2018) Deception can manipulate the attacker's thinking and cause the attacker to act in a way beneficial to the defender. (Rauti & Leppanen, 2017) The use of deception can also cause the attacker to expend resources and force the attacker to reveal the attacker's techniques and capabilities. (DeFaveri & Moreira, 2018 & Rauti & Leppanen, 2017 & Dewar, 2017) In addition to detecting intruders, deception methods can provide an effective means of identifying an internal threat. (Fraunholz, Krohmer, Pohl & Schotten, 2018)

> "Information sharing amongst defenders can increase the efficiency in detecting and responding to cyberattacks"

Cyberspace provides great potential for the practice of deception in cyber defense operations. (Raymond, Conti, Cross, and Nowatkowski, 2014) In the cyber realm, combatants can construct and move deceptive terrain with ease. Companies use the deceptive practice of honeypots and honeynets to divert attackers from valuable assets. A honeypot is designed as a decoy to entice attackers. In addition to slowing the attacker, honeypots allow defenders to gain knowledge of the attackers' tactics, techniques, and procedures. (Olagunju & Samu, 2016 & Saud & Islam, 2015) Engaging the attacker early and maintaining deception with a honeypot allows the defender to collect and record details about the attacker's attempts to compromise the system. Honeypots provide a versatile approach to network defenses. Defenders can deploy preventative and reactive honeypots in various network environments and situations. Also, honeypots can provide efficiencies over traditional intrusion detection systems. Honeypots generate far less logging data than traditional intrusion detection since the honeypots are not involved in normal operations. (Almeshekah & Spafford, 2016)

Deploying and maintaining honeypots requires expertise and ongoing maintenance to ensure the honeypot remains relevant. For a deception operation to be effective, it must present and maintain a plausible story to the attacker. (DeFaveri & Moreira, 2018) The honeypot must also be realistic enough that once it lures the attacker in, the honeypot continues to deceive the attacker. (Almeshekah & Spafford, 2016) Also, the honeypot must provide capabilities for the defender to detect and capture all actions taken by the attacker while in the honeypot.

Deception tactics are not limited to honeypots and honeynets. Defenders can deploy many types of deception, which can provide an early-warning system of possible intrusions. (Virvilis, Serrano & Vanautgaerden, 2014 & Rauti & Leppanen, 2017) Defenders can create a wide range of fake entities, including files, database entries, and passwords, which only a malicious attacker should access. (Rauti & Leppanen, 2017) Defensive systems monitor the fake entities and alert on any interactions with the bogus resources. Several of these methods are simple to implement and require no new technology. Organizations should consider combining techniques into a deception framework. The use of multiple techniques increases the effectiveness of the deception. For example, Fraunholz et al. developed a deception framework and a reference implementation that includes deceptive tokens for files, user accounts, database entries, and communication ports. (Fraunholz, Krohmer, Pohl & Schotten, 2018)

"Advanced defense methods, including MTD, active defenses, and deception can raise the cost of an attack and slow the attack"

Like with all approaches to cybersecurity, the use of fake entities for deception comes with challenges. False alarms, or false positives, can occur when an employee interacts with a fake entity on the system. However, the interaction with honeytokens by an employee may indicate an insider threat. Perhaps the biggest challenge with fake entities is creating them. Fake entities must look realistic to the attacker to be effective. (Virvilis, Serrano & Vanautgaerden, 2014 & Rauti & Leppanen, 2017)

4.5 Moving Target Defenses

Moving target defenses (MTD) diversify the critical components of homogeneous environments. (Winterrose, Carter, Wagner & Streilien, 2014 & Ge, Yu, Shen, Chen, Pham, Blasch & Lu, 2014) By diversifying the attack surface presented to the attacker, the defender can increase the operational costs of the attackers. Dynamically changing the attack surface at run-time can reduce the attacker's asymmetric advantage by complicating the attacker's reconnaissance and exploitation efforts. Moving target defenses encompass emerging methods that make it more difficult for attackers to detect entry points into a system, reduce vulnerabilities, make remaining vulnerability exposures more transient, and decrease the effectiveness of attacks. (Soule, Simidchieva, Yaman, Loyall, Atighetchi, Carvalho & Myers, 2015)

Most systems operate with a static configuration, including the network, operating system, and application configurations. An attacker can probe these static systems to locate specific vulnerabilities for which the attacker has an exploit. The static configurations provide the attacker with time to conduct reconnaissance, develop a plan, and launch an attack. (Ge, Yu, Shen, Chen, Pham, Blasch & Lu, 2014) Defenders use MTDs to make computer systems more dynamic, thus increasing the difficulty and the cost of cyber-attacks. Moving target defenses change the static nature of the system in various ways including changing properties over time, introducing randomness into the internals of a system to make them less deterministic, and increasing the diversity in the computing environment. (Okhravi, Streilein & Bauer, 2016) By dynamically changing the environment, MTDs increase the effort on the part of the attacker while decreasing the attacker's certainty of success. (Atighetchi, Benyo, Eskridge & Last, 2016)

Organizations may be reluctant to deploy MTD techniques because many MTD methods can potentially negatively impact the network's mission more than they positively impact security. (Zaffarano, Taylor & Hamilton, 2015) Many MTD techniques can have negative performance impacts that may be prohibitive. (Okhravi, Streilein & Bauer, 2016) Also, organizations must take care to avoid implementing security solutions, including MTD methods, which add little value, increase operational costs, expand the attack surface, or create issues with existing security components. (Atighetchi, Benyo, Eskridge & Last, 2016)

The inability of many proposed MTD techniques to guarantee that varying the attack surface will enhance security effectiveness presents a major roadblock to the adoption of MTD techniques. (Hong & Kim, 2015) Measuring an MTD's effectiveness, or the degree to which an MTD enhances security while minimizing defender effort is difficult. The evaluation of the effectiveness of MTD techniques is further complicated since the attackers need only to exploit the weakest link. (Okhravi, Streilein & Bauer, 2016)

4.6 Active Defenses

The active defense approach is based on countermeasures designed to detect and mitigate threats in real-time combined with the capability of taking offensive actions against threats both inside and outside of the defender's network. (Dewar, 2014) Active defense emphasizes proactive countermeasures aimed at counteracting the immediate effects of incidents. Active cyber defense counters an attack by detecting then stopping malware or through concealment of target devices to counter espionage. Examples of active cyber defense methods include white worms, hacking back, address hopping, and honeypots. (Dewar, 2017)

White worms are like computer viruses; however, the purpose of a white worm is to locate and destroy malicious software, identify system intrusions, or to perform recovery procedures. (Dewar, 2014) Defenders deploy white worms within their network to seek out malicious intrusions, much like the human body deploys white blood cells to attack infections. White worms can be designed to destroy malicious software once discovered or to analyze the software to assist in the attribution and location of the perpetrators. (Dewar, 2017) However, defenders rarely deploy white worms operationally due to significant drawbacks. (Dewar, 2017) Defenders may have difficulty controlling white worms especially if the white worms are self-propagating. There is a risk that a white worm will escape the network in which it was deployed, possibly through an internet connection or removable storage. After escaping the network, the white worm may continue to replicate and cause unintended collateral damage to external networks. The potential costs associated with a white worm going rogue will often outweigh any potential benefit.

Active defense employs two classes of methods. Within the defender's networks, active defenses detect and mitigate threats in real-time. (Dewar, 2014) With active defenses, the defender can also employ offensive countermeasures beyond the defender's network. Defenders can, after identifying the source devices of an attack, take aggressive, offensive action to disable the source devices. Such aggressive measures operate outside the defender's network. (Dewar, 2014) Many experts consider retaliatory actions or hacking back illegal as these methods require accessing systems of another organization without permission. (Heinl, 2014) Defenders who take offensive actions outside of the boundary of their network face legal implications. Further, the accessing of the command and control server of an attacker without permission may expose the company to criminal or civil actions. (Heinl, 2014) The ability to anonymize traffic on the Internet also complicates the use of offensive practices as the defender may not be able to attribute the incident to the perpetrator accurately. (Dewar, 2014)

CONCLUSION

The use of security automation and adaptive cyber defenses to combat cybercrime is an area of increasing research interest. Cyber attackers enjoy a significant advantage over the defenders in cyber conflict. The attackers' advantage stems from multiple issues including the asymmetry of cyber conflict (Winterrose, Carter, Wagner & Streilien, 2014), the increased sophistication of cyber attacks (Bryne, 2015), the speed and number of attacks (Fonash & Schneck, 2015), and a shortage of cybersecurity talent. (Suby & Dickson, 2015 & Morgan, 2017) Current human-centered cyber defense practices cannot keep pace with the threats targeting organizations.

An integrated approach that speeds detection and response while slowing the attack is required. Security automation and intelligence sharing work together to reduce the defender's cost and time. Information sharing can increase efficiency in detecting and responding to cyber-attacks. Collaborating organizations can use the information shared by one organization to take preventative measures to thwart attacks. Collective action, fostered by community sharing of intelligence can act as an immune system for the collaborating organizations. Security automation can increase the speed of response to an attack and the speed of proactively applying intelligence.

Cyber defenders can use many defensive methods to deter or delay attackers by operating within the attacker's OODA loop. Advanced defense methods, including MTD, active defenses, and deception can raise the cost of an attack and slow the attack. Moving target defenses seek to increase the operational costs of the attackers by diversifying the attack surface presented to the attacker. (Winterrose, Carter, Wagner & Streilien, 2014) Active cyber defense countermeasures detect and mitigate threats in real-time and can take offensive actions both inside and outside of the defender's network. (Dewar, 2014) Deception can accomplish two major objectives by disrupting the attacker's OODA loop. First, deception can confuse and slow the attacker, causing the attacker to expend resources. Second, deception can reveal the attacker's capabilities and techniques.

REFERENCES

Almeshekah, M. H., & Spafford, E. H. (2016). Cyber Security Deception. In S. Jajodia, V. Subrahmanian, V. Swarup, & C. Wang (Eds.), Cyber Deception (pp. 23-50). Switzerland: Springer. doi:10.1007/978-3-319-32699-3_2

Atighetchi, M., Benyo, B., Eskridge, T. c., & Last, D. (2016). A decision engine for configuration of proactive defenses: Challenges and concepts. Resilience Week (pp. 8-12). Chicago, IL: IEEE. doi:10.1109/RWEEK.2016.7573299.

Boyd, J. R. (1986). Patterns of conflict. Retrieved from http://dnipogo.org/john-r-boyd/

Brown, S., Gommers, J., & Serrano, O. (2015). From cyber security information sharing to threat management. Workshop on Information Sharing and Collaborative Security (pp. 43-49). Denver, CO: ACM. doi:10.1145/2808128.2808133.

Byrne, D. J. (2015). Cyber-attack methods, why they work on us, and what to do. AIAA SPACE 2015 Conference and Exposition (pp. 1-10). Pasadena, CA: American Institute of Aeronautics and Astronautics. doi:doi.org/10.2514/6.2015-4576.

De Faveri, C., & Moreira, A. (2018). A SPL framework for adaptive deception-based defense. 51st Hawaii International Conference on System Sciences, (pp. 5542-5551). Honolulu, HI. doi:10.24251/HICSS.2018.691

Dewar, R. S. (2014). The triptych of cyber security: A classification of active cyber defense. 6th International Conference on Cyber Conflict (pp. 7-22). Tallinn, Estonia: NATO CCD COE Publications. doi:10.1109/CYCON.2014.6916392

Dewar, R. S. (2017). Active cyber defense: Cyber defense trend analysis. Zurich, Switzerland: ETH Zurich.

Fonash, P., & Schneck, P. (2015, January). Cybersecurity: From months to milliseconds. Computer, 42-50. doi:10.1109/MC.2015.11.

Fraunholz, D., Krohmer, D., Pohl, F., & Schotten, H. D. (2018). On the detection and handling of security incidents and perimeter breaches: A modular and flexible honeytoken based framework. IFIP International Conference on New Technologies, Mobility and Security. Paris, France: IEEE. doi:10.1109/NTMS.2018.8328709

Frick, C. (2018). IACD & FS ISAC financial pilot results. Integrated Cyber October 2018 Conference (pp. 1-28). Laurel, MD: Johns Hopkins University Applied Physics Lab.

Ge, L., Yu, W., Shen, D., Chen, G., Pham, K., Blasch, E., & Lu, C. (2014). Toward effectiveness and agility of network security situational awareness using moving target defense (MTD). SPIE - The International Society for Optical Engineering (pp. 1-9). San Diego, CA: International Society for Optical Engineering. doi:10.1117/12.2050782

Heinl, C. H. (2014). Artificial (intelligent) agents and active cyber defence: policy implications. 6th International Conference on Cyber Conflict (pp. 53-66). Tallinn, Estonia: NATO CCD COE Publications. doi:10.1109/CYCON.2014.6916395.

Hong, J. B., & Kim, D. S. (2015). Assessing the effectiveness of moving target defenses using security models. IEEE Transactions on Dependable and Secure Computing, 13(2), 163-177. doi:10.1109/TDSC.2015.2443790

Johns Hopkins Applied Physics Laboratory. (2016). Integrated Adaptive Cyber Defense (IACD) Baseline Reference Architecture. Laurel, MD: Johns Hopkins Applied Physics Laboratory. Retrieved from https://secwww.jhuapl.edu.

Lange, M., Kott, A., Ben-Asher, N., Mees, W., Baykal, N., Vidu, C. M., et al. (2017). Recommendations for model-driven paradigms for integrated approaches to cyber defense. Adelphi, MD: US Army Research Laboratory. Retrieved from https://www.arl.army.mil.

Mepham, K., & Ghinea, G. (2014). Dynamic cyber-incident response. 6th International Conference on Cyber Conflict, 121-136. doi:10.1109/CYCON.2014.6916399.

Morgan, S. (2017). Cybersecurity Jobs Report: 2017 Edition. Herjavec Group. Retrieved from https://www.herjavecgroup.com.

Okhravi, H., Streilein, W. W., & Bauer, K. S. (2016). Moving target techniques: Leveraging uncertainty for cyber defense. Lincoln Laboratory Journal, vol. 22, pp. 100-109.

Olagunju, A. O., & Samu, F. (2016). In search of effective honeypot and honeynet systems for real-time intrusion detection and prevention. Proceedings of the 5th Annual Conference on Research in Information Technology (pp. 41-46). Boston, MA: ACM. doi:10.1145/2978178.2978184

Rauti, S., & Leppanen, V. (2017). A survey on fake entities as a method to detect and monitor malicious activity. Euromicro International Conference on Parallel, Distributed and Network-Based Processing (pp. 386-390). St. Petersburg, Russia: IEEE. doi:10.1109/PDP.2017.34

Raymond, D., Conti, G., Cross, T., & Nowatkowski, M. (2014). Key terrain in cyberspace: Seeking the higher ground. 6th International Conference on Cyber Conflict (pp. 287-300). Tallinn, Estonia: NATO CCD COE Publications. doi:10.1109/CYCON.2014.6916409.

Saud, Z., & Islam, M. H. (2015). Towards proactive detection of advanced persistent threat (APT) attacks using honeypots. Proceedings of the 8th International Conference on Security of Information and Networks (pp. 154-157). Sochi, Russia: ACM. doi:10.1145/2799979.2800042

Soule, N., Simidchieva, B., Yaman, F., Loyall, J., Atighetchi, M., Carvalho, M., . . . Myers, D. F. (2015). Quantifying & Minimizing attack surfaces containing moving target defenses. Resilience Week. Philadelphia, PA: IEEE. doi:10.1109/RWEEK.2015.7287449.

Stech, F. J., Heckman, K. E., & Strom, B. E. (2016). Integrating cyber-D&D into adversary modeling for active cyber defense. In S. Jajodia, V. S. Subrahmanian, V. Swarup, & C. Wang (Eds.), Cyber Deception (pp. 1-22). Switzerland: Springer. doi:10.1007/978-3-319-32699-3_1

Suby, M., & Dickson, F. (2015). The 2015 (ISC)2 Global Information Security Workforce Study. Mountain View, CA: Frost & Sullivan. Retrieved from https://www.boozallen.com.

Virvilis, N., Serrano, O. S., & Vanautgaerden, B. (2014). Changing the game: The art of deceiving sophisticated attackers. 6th International Conference on Cyber Conflict (pp. 87-97). Tallinn, Estonia: NATO CCD COE Publications. doi:10.1109/CYCON.2014.6916397.

Walton, T., Watson, K., Kosecki, C., Mok, J., & Burger, W. (2018). Piloting expanded threat enrichment and automation via the FS-ISAC feed. May 2018 Integrated Cyber. Laurel, MD: Johns Hopkins Applied Physics Lab. Retrieved from https://www.iacdautomate.org/may-2018-integrated-cyber

Winterrose, M. L., Carter, K. M., Wagner, N., & Streilien, W. W. (2014). Adaptive attacker strategy development against moving target cyber defenses. ModSim World (pp. 1-11). Hampton, VA: ModSim World.

Zaffarano, K., Taylor, J., & Hamilton, S. (2015). A quantitative framework for moving target defense effectiveness evaluation. MTD'15 (pp. 3-10). Denver, CO: Association for Computing Machinery. doi:10.1145/2808475.2808476

Zheng, D. E., & Lewis, J. A. (2015). Cyber Threat Information Sharing: Recommendations for Congress and the Administration. Washington, DC: Center for Strategic & International Studies. Retrieved from https://www.csis.org.

DONNIE WENDT has over 30 years in information technology, including in the defense, telecommunications, and finance industries. Mr. Wendt currently designs and implements security controls and monitoring solutions for Mastercard, where he has worked since 2004. Also, he is an adjunct professor of cybersecurity at Utica College. Currently pursuing a Doctorate of Science in Computer Science at Colorado Technical University, his research focuses on security automation and adaptive cyber defense in the financial services industry. He earned a CISSP certification, an MS in Cybersecurity from Utica College, and a BA in Business Administration from Webster University. You may contact Mr. Wendt at donnie@showmecyber.com or visit his website: www.showmecyber.com.

HERE TO SUPPORT YOUR MISSION.

Is your organization currently facing a challenging Information Technology oriented research and development problem that you need to have addressed in a timely, efficient and cost effective manner?

HOW CAN CSIAC HELP?

In a time of shrinking budgets and increasing responsibility, CSIAC is a valuable resource for accessing evaluated Scientific and Technical Information (STI) culled from efforts to solve new and historic challenges. Our CSIAC SME network includes experienced engineers and technical scientists, retired military leaders, information specialists, leading academic researchers, and industry experts who are readily available to help prepare timely and authoritative answers to complex technical inquiries.

Once submitted, the inquiry is sent directly to an analyst who then identifies the staff member, CSIAC team member, or SME that is best suited to answer the question. The completed response is then compiled and sent to the user. Responses can take up to 10 working days, though they are typically delivered sooner.

WANT TO SUBMIT A TECHNICAL INQUIRY?

The CSIAC provides up to **4 hours of Free Technical Inquiry research** to answer users' most pressing technical questions. Our subject matter experts can help find answers to even your most difficult questions.

Technical inquiries can be submitted to CSIAC via our csiac.org, or by email, phone or fax.

☎ CALL NOW! 800-214-7921

✉ EMAIL AT: INFO@CSIAC.ORG

Cyber Security & Information Systems
Information Analysis Center

FOR MORE INFO, GO TO:
https://www.csiac.org/free-inquiries/

GAINING ENDPOINT LOG VISIBILITY IN ICS ENVIRONMENTS

By: Michael Hoffman, Candidate, SANS Technology Institute, MS in Information Security Engineering.

SECURITY EVENT LOGGING IS A BASE IT SECURITY PRACTICE AND IS REFERENCED IN INDUSTRIAL CONTROL SECURITY (ICS) STANDARDS AND BEST PRACTICES.

Although there are many techniques and tools available to gather event logs and provide visibility to SOC analysis in the IT realm, there are limited resources available that discuss this topic specifically within the context of the ICS industry. As many in the ICS community struggle with gaining logging visibility in their environments and understanding collection methodologies, logging implementation guidance is further needed to address this concern. Logging methods used in ICS, such as WMI, Syslog, and Windows Event Forwarding (WEF), are common to the IT industry. This paper examines WEF in the context of Windows ICS environments to determine if WEF is better suited for ICS environments than WMI pulling regarding bandwidth, security, and deployment considerations. The comparison between the two logging methods is made in an ICS lab representing automation equipment commonly found in energy facilities.

INTRODUCTION

The monitoring and subsequent analysis of event logs is a foundational IT security activity and is listed as the sixth most important control in the Center for Internet Security (CIS) Version 7 Top 20 Controls (CIS, 2018). For Industrial Control Systems, log monitoring and analysis is just as important. The widely-adopted ICS Cyber Security Framework (CSF) Version 1.1 from NIST lists the category Anomalies and Events under the core Detect Function (NIST, 2018). Energy companies that operate ICS equipment under regulation of the North American Electric Reliability Corporation (NERC) standards specify logging in CIP-007-6 R4 as a requirement for asset owners to implement and review systems for events (NERC, 2016). Furthermore, NIST 800-82 (2015) states “the security architecture of an ICS must also incorporate mechanisms to monitor, log, and audit activities occurring on various systems and networks” (pp. 5-25).

As companies' operating ICS systems seek to comply with industry regulations, standards, and best practices, there often lacks detailed implementation guidance for establishing logging architectures, considering the diverse ICS install base.

ICS Logging Constraints

ICS devices and networks are purpose-built for the intended mission of monitoring and controlling a physical entity. Although ICS computers often share similar operating systems, applications, and hardware as their IT counterparts, the mission of ICS systems is to support physical entities. ICS systems are found in refineries, gas plants, power plants, water and wastewater facilities, and manufacturing floors. These systems have different uptime, integrity, and safety requirements that IT systems often do not. Also, ICS networks are often deployed for years without an upgrade and can be constrained by bandwidth or physical locations.

IT environments are fluid from a technology, connectivity, and security landscape perspective and prioritize data confidentiality above integrity and availability. In contrast, ICS environments are stable, deterministic, change infrequently and prioritize control (safety), integrity, and availability above confidentiality (Novotek, 2018). The differences between IT and OT, therefore, bring different logging restrictions and requirements. Nevertheless, due to defined architectures, connection pathways, and stable installations, ICS environments are more defensible than IT environments (Lee & Assante, 2015).

Establishing a standardized logging architecture across these environments is difficult considering ICS vendor restrictions, where support contracts are often voided if unapproved software, such as a software logging agent, is installed (Miller, 2017). The limitation of third-party tools and applications that are approved by respective ICS vendors restricts options for log gathering to the embedded functionality of the operating system itself.

> *"Logs represent a component of Passive Defense and play a foundational role in Active Defense"*

ICS Log type review

Syslog is a commonly-used logging protocol for network routers, switches, firewalls, and Unix or Linux operating systems. Syslog can also be used to gather logs from Programmable Logic Controllers (PLC), Remote Terminal Units (RTU), Intelligent Electronic Devices (IED) and other ICS devices, given they support Syslog logging functionality.

Nevertheless, Windows clients and servers are used extensively in ICS environments as part of an overall Distributed Control System (DCS) or Supervisory Control and Data Acquisition (SCADA) system. Gaining centralized log visibility with these systems is often performed through Windows Management Instrumentation (WMI), which has been available in Windows since NT 4.0, and can be used to pull security event logs over DCOM or Windows Remote Management (WinRM) (Graeber, 2015). Many IT administration and security vendors, such as Splunk and SolarWinds, have implemented event log pulling using WMI as an option. Starting in Windows Vista and Server 2008, however, Microsoft introduced WinRM and the capability to enable Windows Event Forwarding and Collection (Helweg, 2008). WinRM is backward compatible on Windows XP SP2+ and Server 2003 SP1+ systems by installing the WS-Management patch.

When an ICS security group considers whether to use WEF or WMI with DCOM in an ICS environment, WEF appears the preferred choice with built-in Kerberos authentication and encryption, firewall-friendly protocol, and domain enrollment and deployment. Additionally, WEF allows forwarding interval modification that reduces bandwidth spikes unlike WMI with DCOM pulling. The remainder of this paper will review WEF and WMI/DCOM in an ICS lab to determine if WEF is better suited for constrained ICS environments to support ICS owners and operator's adherence to industry regulations, standards, and best practices.

RESEARCH METHOD

An operational ICS lab, which contains three ICS DCS vendors, was utilized to establish the nuances between WMI and WEF logging in an ICS environment. Both WEF and WMI over DCOM was deployed to determine performance and deployment aspects of the two Windows logging protocols. To determine network

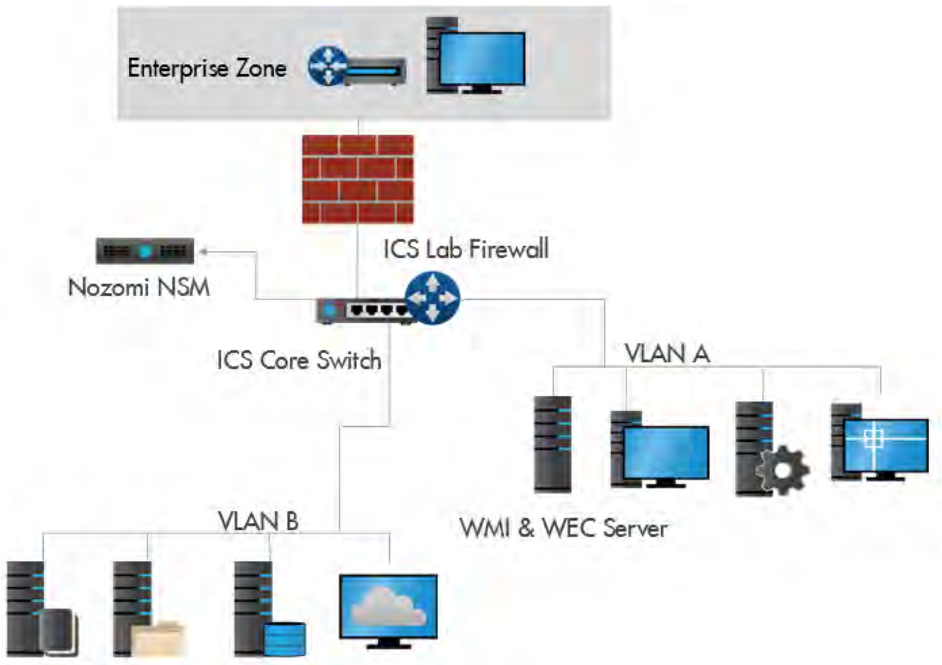


Figure 1. Test ICS Lab network layout.

traffic and bandwidth consumption logging measurements, a Nozomi ICS Network Security Monitoring (NSM) appliance was utilized to capture all network packets passing through the ICS network core switch, as illustrated in Figure 1.

The ICS environment lab environment consisted of ICS devices and systems ranging from Windows 2000 to Windows 2016 server, and Windows NT 4.0 to Windows 10 client OS versions. The Windows forest and domain levels were upgraded to the maximum level of 2008R2 for the assessment to allow backward compatibility with the older Windows 2000 hosts, and yet to still provide WinRM and WEF Group Policy Object (GPO) capability. A 2012R2 Windows VM was deployed to consume WEF logs from the ICS domain hosts. The same server also had a trial version of Splunk Enterprise to pull security logs using WMI with DCOM, which helped rule out network path and latency testing concerns using different physical or virtual logging servers. Only Windows Vista and Server 2008 operating systems and above were tested due to OS restrictions with WEF as WS-Management was not deployed. The same computers' forwarding logs using WEF were also pulled with WMI, which consisted of 40 Windows client and servers in total having both virtual and physical installations.

FINDINGS AND DISCUSSION

Gaining access to ICS systems security logs is an essential step for organizations. Logs represent a component of Passive Defense and play a foundational role in Active Defense, which Lee (2015) describes as "the process of analysts monitoring for, responding to, and learning from adversaries internal to the network" (p. 10).

Unfortunately, obtaining logs from ICS environments for Security Information and Event Management (SIEM) consumption, and ultimately by ICS and IT security engineers and analysts is difficult. Many security logging and monitoring vendors offer software agents to install on end-point systems that allow log collection and log forwarding to a SIEM, which can even provide interactive queries. However, as mentioned previously, adding unapproved or untested software to ICS vendor systems often voids warranties or service contracts. Software agents also add a burden to the available compute and memory resources on what are often constrained ICS systems and are generally only available for supported operating systems. Therefore, utilizing existing OS platform tooling in ICS environments is much preferred over adding third-party products and applications.

Another requirement when rolling out logging infrastructure, or any security tooling in an ICS environment, is to limit the necessary physical presence required. Depending on the industry and environment, ICS systems are often spread across hundreds of miles of land or water, so reducing physical deployment presence requirements is a must. Furthermore, reducing or eliminating end-point reboots is a high priority, as reboots can cause loss of process view, process disruption, or even process downtime — depending on the underlying design of the ICS system and built-in component redundancy. Therefore, leveraging GPO settings, VB scripts or PowerShell scripts that require reboots to take effect are less preferred versus using scripts or GPO settings that take effect on the target system(s) immediately.

Furthermore, Security Operation Center (SOC) use-cases also need to be understood and documented before determining logging settings on end-points. Logging for the sake of logging will not assist cyber defenders in detecting an incident or supporting threat hunts if the logs do not add value. Use-cases are required to determine what to log and what to collect from a centralized perspective. Excessive logging settings can overwhelm endpoints, consume valuable LAN or WAN network bandwidth, and ultimately cause more harm than good to the ICS environment. Therefore, planning and mapping logging settings in the environment to match pre-defined use-cases is a critical step. Murdoch (2018) describes building use-cases for SOC teams and gives exceptional coverage of Windows security events in the Blue Team Handbook that ICS asset owners and operators can leverage.

Table 1: Event Log GPO.

Local Policies/Audit Policy	Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Success, Failure
Audit logon events	Success, Failure
Audit object access	Failure
Audit policy change	Success, Failure
Audit privilege use	Failure
Audit system events	Success, Failure
Local Policies/Security Options	
Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings	Enabled
Advanced Audit Configuration	
Account Management	
Audit Computer Account Management	Success, Failure
Audit Other Account Management Events	Success, Failure
Audit Security Group Management	Success, Failure
Audit User Account Management	Success, Failure
Detailed Tracking	
Audit Process Creation	Success
Audit Process Termination	Success
Logon/Logoff	
Audit Account Lockout	Success
Audit Logoff	Success
Audit Logon	Success, Failure
Audit Other Logon/Logoff Events	Success, Failure
Audit Special Logon	Success, Failure
Object Access	
Audit Other Object Access Events	Success, Failure
Policy Change	
Audit Audit Policy Change	Success, Failure
Audit Other Policy Change Events	Success, Failure
System	
Audit System Integrity	Success, Failure
Administrative Templates	
System/Audit Process Creation	
Include command line in process creation events	Enabled

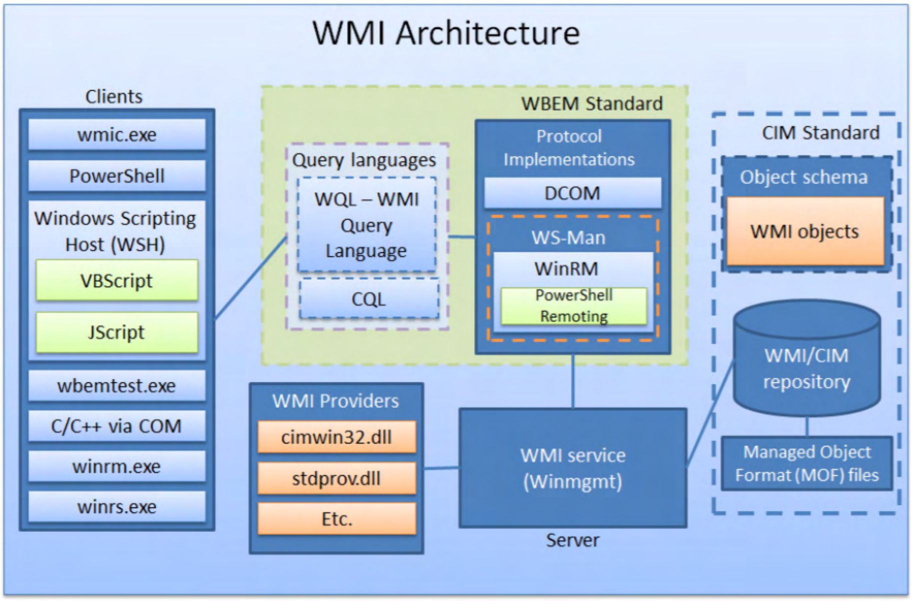


Figure 2: Windows WMI Architecture (Graeber, 2015).

Logging configuration

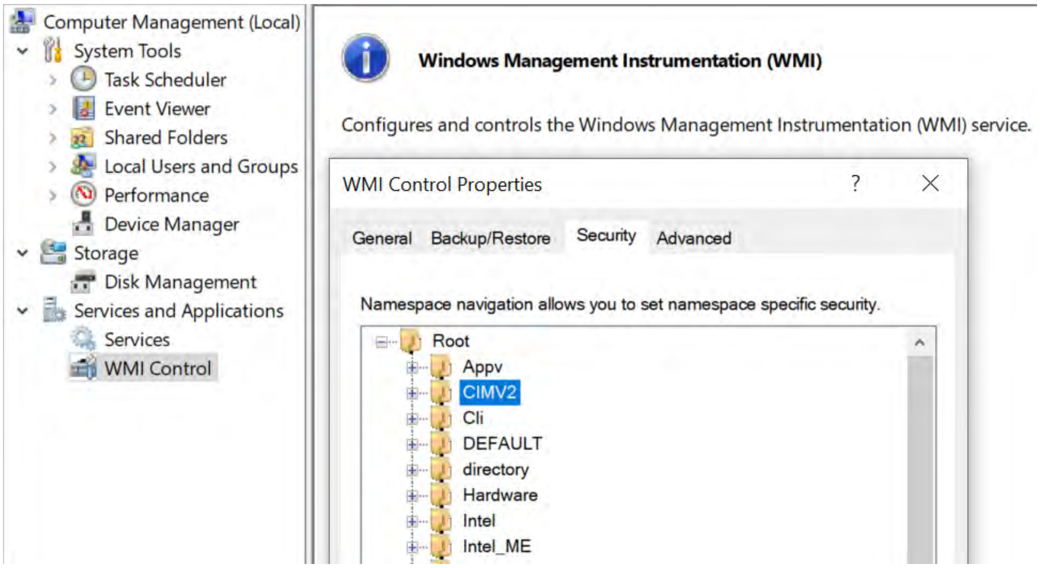
An essential element for testing logging protocols in the ICS lab is to have consistent audit policy settings across the endpoints and is achieved by creating a domain-wide audit policy GPO. The GPO created for the assessment leveraged event logging recommendations from the SANS ICS410 course (Searle, 2017). Recommendations from the Australian Cyber Security Center were used for Vista and above OS with Advance Audit Configuration capability in the GPO (ACSC, 2018). Between SANS and ACSC recommendations, the audit settings ensured adequate log coverage and traffic required for WEF and WMI protocol testing. It is worth noting that enabling *Force audit policy subcategory settings* in the GPO causes Vista/2008 and above OS's to disregard the Local Audit Policies in favor of the Advanced Audit Policies. The combined GPO settings for both Local and Advanced auditing are shown in Table 1.

Advanced audit policies can generate a considerable amount of logging activity depending on the environment. With an application that performs pulling, each WMI query will generate a process creation, process termination, login and logoff events. The events count scales linearly with the number of computers pulled in the environment, so just the operation of log querying can be a significant source of logs. With this in consideration, it would be prudent to target logging GPO's per use-case covering clients and servers located in their respective Active Directory organization units in the domain, instead of deploying one GPO domain logging policy across the environment.

WMI and DCOM Log Pulling

Windows Management Instrumentation (WMI) is a standard method of administrating Windows systems and viewing configuration settings of both standalone and networked-based machines. WMI is a collection of namespaces that can be queried to obtain system information. As discussed by Graber (2015), and as shown in Figure 2, WMI can be quired scrabble locally or remotely.

The transport mechanism for remote WMI queries is WS-Man (WinRM) or DCOM. WinRM is Microsoft's implementation of WS-Management Protocol and uses XML tags with Simple Object Access Protocol (SOAP) to describe and transfer management communications between endpoints. WinRM uses port 5985 for HTTP and 5986 for https communications, respectively.



Windows Management Instrumentation (WMI)

Configures and controls the Windows Management Instrumentation (WMI) service.

WMI Control Properties

Namespace navigation allows you to set namespace specific security.

Figure 3. Windows WMI security settings configuration screen.

DCOM is Distributed Component Object Model and uses Remote Procedure Call (RPC) well-known TCP port 135 to establish initial communication, and then negotiates a dynamic port number from an available dynamic upper port range to continue the communication. Dynamic port ranges have not been consistent throughout the history of Windows client and server operating systems. Windows 2000 to 2003 servers' dynamic port ranges are between 1024 through 5000, while newer client and server operating systems' dynamic port ranges fall between 49152 and 65535. However, for DCOM specifically, Microsoft suggests setting a firewall port range from 1024 to 65535 for XP and 2003 systems and 49152 to 65353 for systems newer than XP/2003 (2018). Therefore, DCOM is not firewall friendly and requires opening a significant block of dynamic ports. It may also require a firewall capable of understanding DCE-RPC protocol to configure session by session rules upon TCP connection establishment. Cisco (nd), for example, implements dynamic RPC session rule creation in their ASA firewall product line using DCE-RPC Inspection.

A dedicated high range DCOM port or reduced port range is configured using dcomcnfg.exe, but the configuration does require a system reboot to take effect and can have negative consequences to other ICS critical DCOM communications. Therefore, WinRM is much easier to configure across firewalls than DCOM. However, DCOM is used heavily in the ICS sector with OPC Classic specification communications.

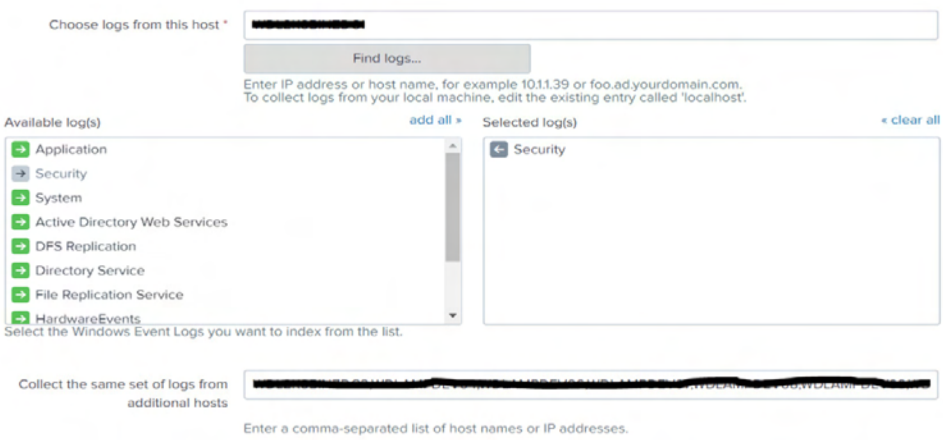
Configuration – domain and network requirements

Pulling windows security logs using WMI with DCOM is configured in multiple steps and can be accomplished in a domain or workgroup environment. In a workgroup environment, a user account with the same password is created in every computer and linked to the Distributed COM user's group, Event Log Readers, and WMI providers. For a domain scenario, an administrator must create a named service account in Active Directory. Linking the user to the targeted domain computers' Event Log Readers group and Distributed COM Users is accomplished by adding the account to a GPO preference in a domain. However, access to WMI providers cannot be performed by this method as there are no available WMI settings available in a GPO template to change security access settings to root/CIMV2 settings for WMI, as shown in Figure 3.

Therefore, other means such as login scripts, scheduled tasks, PowerShell remoting, or VB scripts with PsExec utility are required to configure WMI providers security settings remotely. PowerShell is an excellent method but requires PowerShell Remoting and passing administrative credentials using the Invoke-Command to modify WMI settings on remote computers. PowerShell Remoting, therefore, poses a challenge when configuring the environment if it is using older versions of PowerShell below 4.0, which is common to ICS environments.

> *"Advanced audit policies can generate a considerable amount of logging activity depending on the environment."*

A workaround to the problem of granting a local user account, or a domain user account, access privileges to WMI providers, is to configure a named domain service account and link the account to



Choose logs from this host * [redacted]

Enter IP address or host name, for example 10.1.1.39 or foo.ad.yourdomain.com.
To collect logs from your local machine, edit the existing entry called 'localhost'.

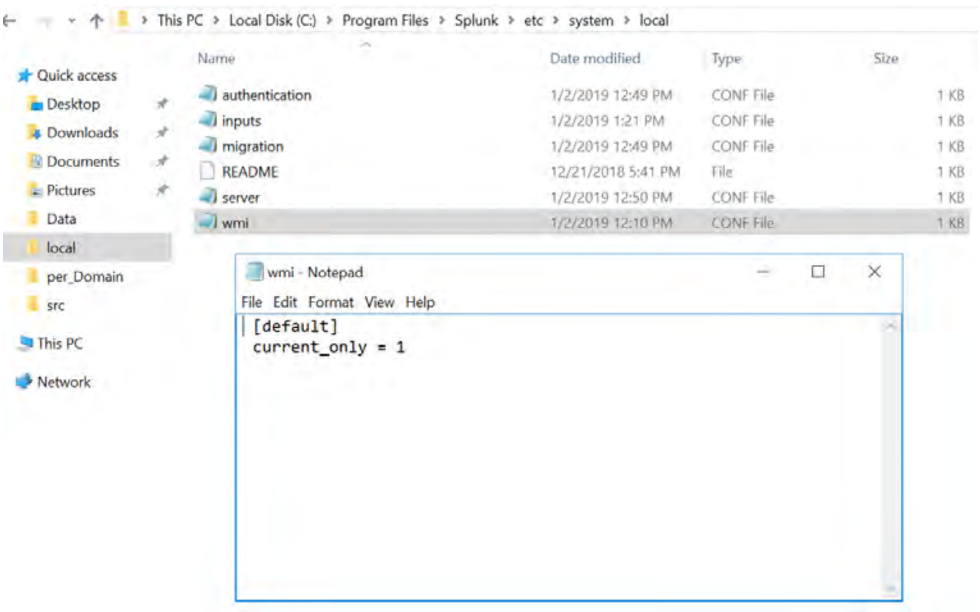
Available log(s) add all »	Selected log(s) « clear all
Application Security System Active Directory Web Services DFS Replication Directory Service File Replication Service HardwareEvents	Security

Select the Windows Event Logs you want to index from the list.

Collect the same set of logs from additional hosts [redacted]

Enter a comma-separated list of host names or IP addresses.

Figure 4. Splunk WMI remote data source configuration.



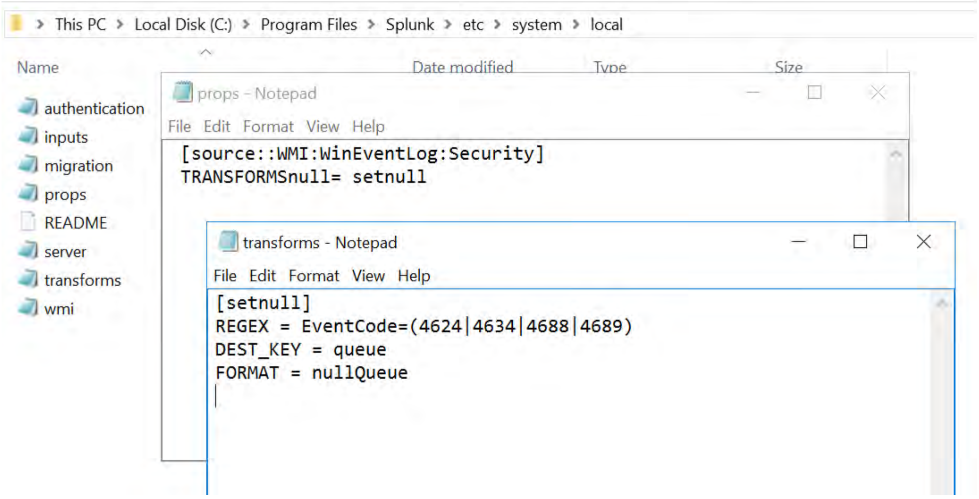
This PC › Local Disk (C:) › Program Files › Splunk › etc › system › local

Name	Date modified	Type	Size
authentication	1/2/2019 12:49 PM	CONF File	1 KB
inputs	1/2/2019 1:21 PM	CONF File	1 KB
migration	1/2/2019 12:49 PM	CONF File	1 KB
README	12/21/2018 5:41 PM	File	1 KB
server	1/2/2019 12:50 PM	CONF File	1 KB
wmi	1/2/2019 12:10 PM	CONF File	1 KB

wmi - Notepad

```
[default]
current_only = 1
```

Figure 5. Splunk WMI override configuration file for current only log collection.



This PC › Local Disk (C:) › Program Files › Splunk › etc › system › local

props - Notepad

```
[source::WMI:WinEventLog:Security]
TRANSFORMSnull= setnull
```

transforms - Notepad

```
[setnull]
REGEX = EventCode=(4624|4634|4688|4689)
DEST_KEY = queue
FORMAT = nullQueue
```

Figure 6. Splunk WMI settings to discard events before they are indexed.

the Domain Admins group. By default, the Domain Admins group is linked to the local Administrators group when a computer joins the respective domain. Thus, the Domain Admins Group obtains full local computer access. Although it is an administratively easy solution, granting the WMI service account Domain Admin privileges does not abide by the principle of least-privilege and creates significant weakness in the security of the deployment.

A Windows domain administrative level account was not used in the ICS lab and solutions were explored to use a restricted account. Due to uptime availability requirements, login scripts or other means of deployment to configure WMI provider security settings that required rebooting were not suitable. The next option was to use PowerShell Remoting to iterate through the test list of computers and remotely connect to each using the Invoke-Command and modify the WMI settings. Using PowerShell Remoting is challenging in environments that use older versions of PowerShell because of the requirement that the remote PowerShell Session be "run as administrator" to modify the remote computers' WMI security settings. One option, among many, is to run Invoke-Command on the remote computer, launch a new PS-Session with the admin credentials, step into the remote session, and then pass long the PS code to modify the WMI provider settings. After multiple failed iterations of PowerShell Remoting, the WMI provider security settings were successfully set by a VB script. The script leveraged a combination of Microsoft's Sysinternals PsExec utility for remote system configuration and wmisecurity.exe application for WMI providers security, as described and developed by Madden (2006).

With WMI services privileges set, the next step was to install a trial version of Splunk Enterprise on the VM logging server. During Splunk Enterprise installation, the custom option must be selected to allow domain authentication

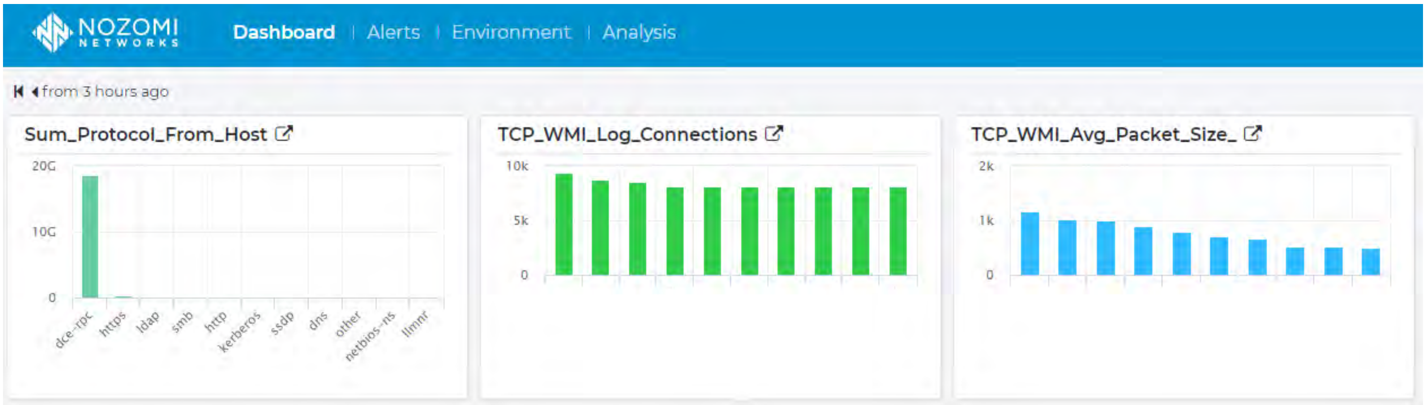


Figure 7. WMI network statistics measured by the NSM over six days of testing.

necessary for WMI collection. The domain WMI account, already created, was added to the installation configuration. Next, an external event log collection was created to pull the Security event log from 40 systems in the ICS lab, which were the same systems being pulled using WEF. Data collections require one Windows host to configure, and an optional comma-separated list of computers for the additional computers, as shown in Figure 4.

The default Splunk configuration will pull all security logs from all hosts, which can saturate network connections and exceed the 500 MB trial Splunk license. During testing, excessive bandwidth and network traffic was observed, and the puller was disabled to determine configuration options. After some additional research, Splunk can be configured only to pull the most recent logs. Creating a WMI. conf file in the %$SPLUNK_HOME%/ etc/system/local file path and adding **current_only = 1**, as shown in Figure 5, achieved the expected results and was used throughout WMI testing.

With the Splunk WMI system working, it was also observed that the logging GPO was generating a considerable number of logins, logoffs, process creations, and process termination logs, which exceeded the 500 MB limit. To tune these out for the assessment, Splunk offers a way to select specific events and forward them to a null Index, which is the same as permanently discarding the logs at the Splunk Server. This setting does not filter logs in the WMI query, so the amount of traffic is not reduced by this method, but rather, only the logging, and indexing of logs is reduced. In a production environment, this method would help to remove specific logs are not part of targeted use-cases, but caution should be used, nonetheless, when discarding logs as regulatory requirements may dictate maintaining all logs for a given period. The specific log files and configurations are shown in Figure 6.

WMI Bandwidth Consumed

After six days of WMI log collection, Figure 7 shows the Nozomi NSM appliance registered 17GB of logging traffic transferred between the log puller server and hosts in the ICS lab. (This traffic does not represent all bytes transferred with WMI due to the location of the IDS appliance but does represent 32 systems.)

As DCOM uses DCE-RPC protocol, all WMI traffic is labeled as DCE-RPC in the Nozomi appliance. The log server did not have any other service that was using DCE-RPC during the test, so the entire traffic captured is from WMI pulling activities. The number of connections and the average packet size is also captured. The number of connections is caused by the pulling cycle in Splunk and is a function of log pulls per time, which is relatively consistent across the environment and registered over 9,000 pulls across six days. The average packet size, however, is not consistent across the pulls and may be an indication that some systems, such as domain controllers, have logs available every pull, which maintains a higher average packet size. Other systems that generate fewer logs will also have less data to transfer. This behavior may indicate that WMI pulling is less efficient than other means of log gathering if systems are being pulled with few or no logs to provide the log server.

Windows Event Forwarding

One of the features of Windows Remote Management (WinRM) is the ability to use the underlying framework to establish a fully functional log querying or forwarding environment between network clients and one or more log collectors. WEF is not a replacement for a SIEM, but a method to transfer logs from an ICS environment to a SIEM. Windows Event Forwarding (WEF) is set up either in a push or pull configuration. In the push configuration, which, according to Microsoft, is the recommended configuration, clients push their logs to one or more servers operating as a Windows Event Collector (WEC) (ACSC, 2018). The pull configuration is the opposite, where the WEC server pulls logs from the clients. Another feature is to chain WEC servers together for log aggregation in large environments or across multiple windows domains. As shown in Figure

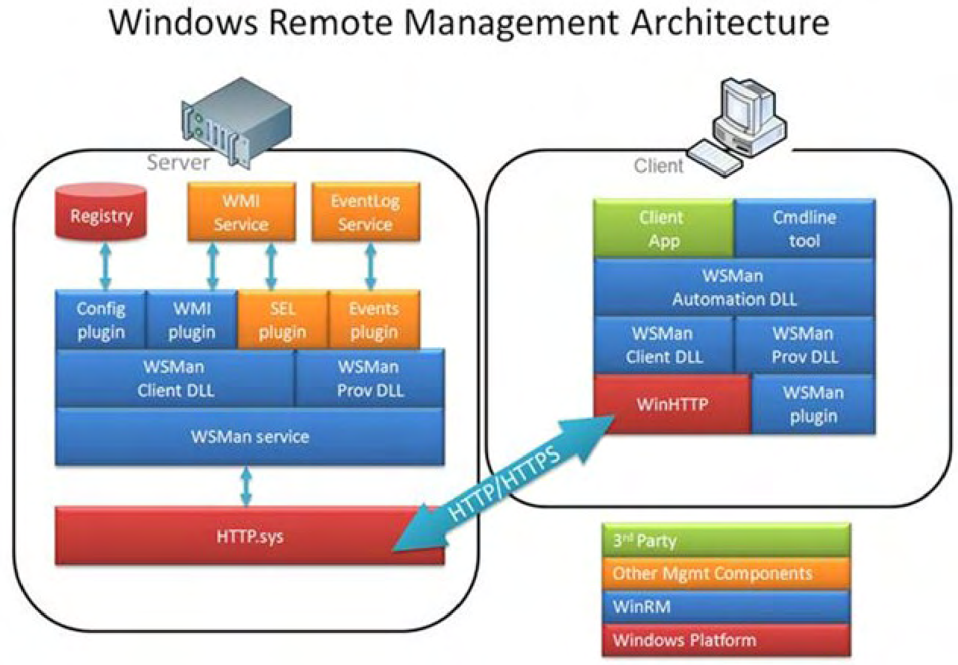
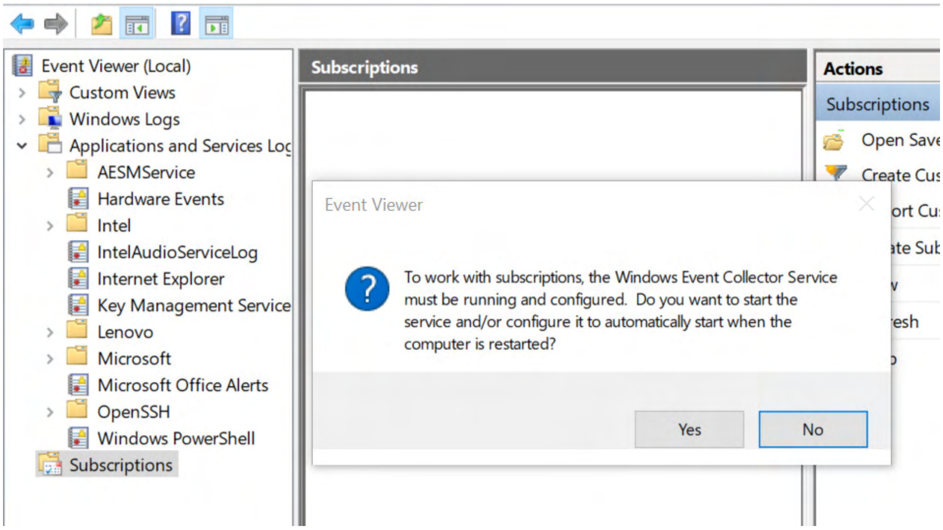


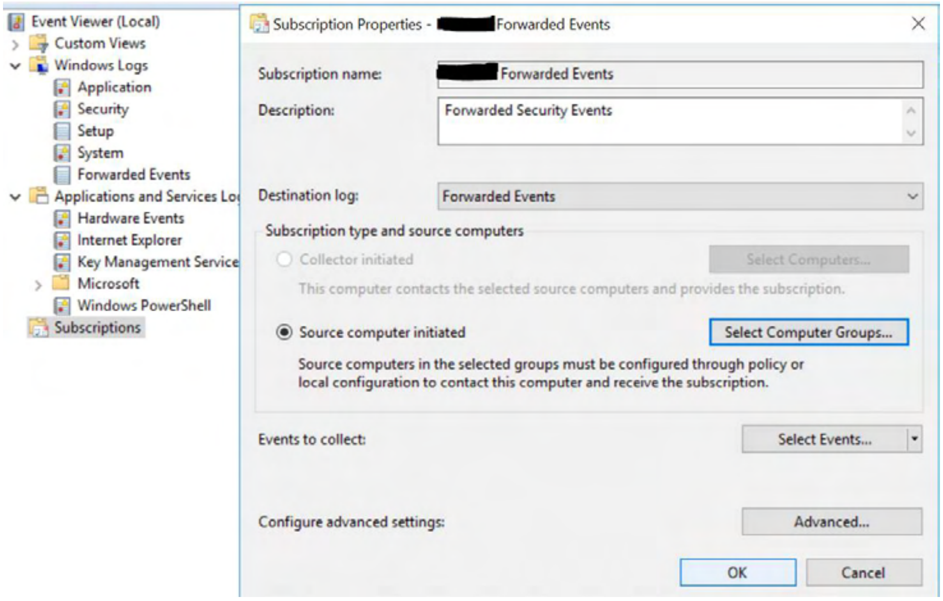
Figure 8. Microsoft WinRM components and communication protocol (Jonathan, 2009).



Event Viewer

To work with subscriptions, the Windows Event Collector Service must be running and configured. Do you want to start the service and/or configure it to automatically start when the computer is restarted?

Figure 9. WEC Server initial subscription configuration.



Subscription Properties - [redacted] Forwarded Events

Subscription name: [redacted] Forwarded Events

Description: Forwarded Security Events

Destination log: Forwarded Events

Subscription type and source computers

○ Collector initiated

This computer contacts the selected source computers and provides the subscription.

● Source computer initiated

Source computers in the selected groups must be configured through policy or local configuration to contact this computer and receive the subscription.

Events to collect:

Configure advanced settings:

Figure 10. WEC new subscription properties panel.

8, WinRM uses HTTP or HTTPS protocol across the network medium.

For WinRM, however, HTTP communicates over TCP 5985 and uses TCP port 5986 for HTTPS. Despite using HTTP as the default protocol, WEF uses Kerberos authentication and encrypts communication by default. HTTPS requires a trusted certificate for operating but allows cross domain and workgroup deployment options. Additionally, because WinRM uses only one TCP port, host-based and ICS zone firewall rules are straightforward to both configure and implement across the environment.

Configuration – domain and network requirements

Configuring WEF is accomplished first by ensuring that WinRM service is running and listening for requests on all machines in the domain. Running **WinRM -quickconf** on each computer accomplishes the prerequisite. Domain-based GPOs are a second way, but the domain computer would require a reboot to prompt the service to run. A third way is to leverage free tools, such as **SolarWinds Remote Execution Enabler for PowerShell** that can enable based on computer names, IP addresses or ranges.

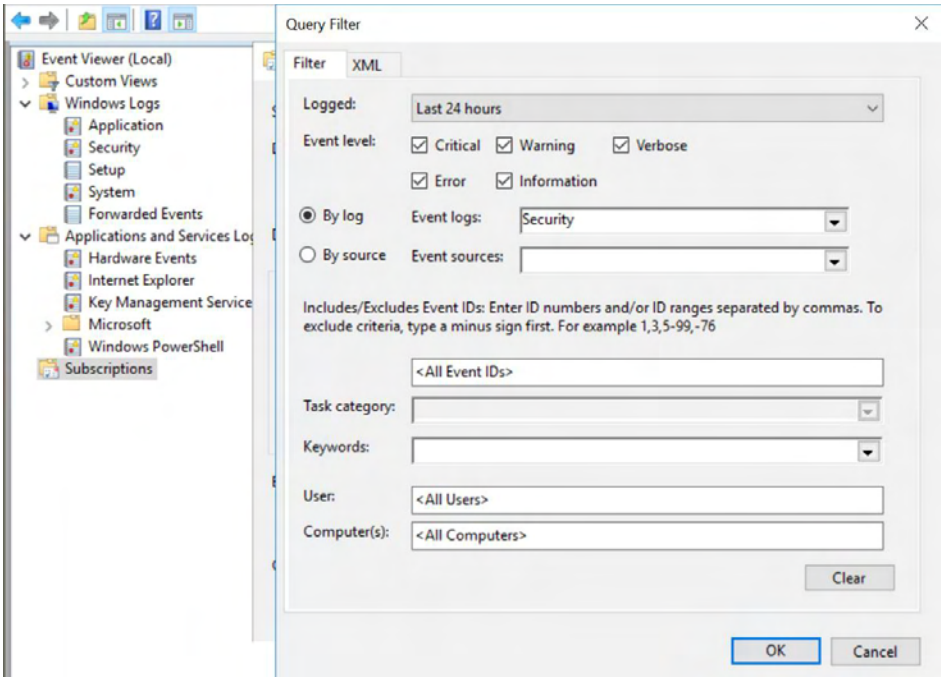
Configuring the WEC requires a few more steps to set up the listener and configure the subscription. Issuing **wecutil.exe quickconfig** at an elevated command prompt is one way, but the other is to open **eventvwr.msc** and click 'Yes' on the prompt and then reboot the WEC server, as shown in Figure 9.

With the WEC service running and listening for connection attempts, the next steps are to set up the Domain GPO to allow the WEC server access to the domain computers' security event logs, set the WEC subscription path, enable WinRM service, and restrict access to WinRM. Out of these, the most intrusive task is allowing the forwarding service access to the security event logs. Although an administrator can link the Network Service group to the local Event Log Readers group, doing so requires a reboot to each computer in the environment for settings to take effect. An alternative option is to run the command s**c config wecsvc type=own && sc stop wecsvc && sc start wecsvc** on each computer (ACSC, 2018). There is a third solution to this problem according to Payne (2015). The Security ID for the Event Log readers group can be obtained by running **wevtutil gl security** command on a domain host and copying the SID output to Notepad, appending the following ID **(A;;0x1;;;NS)**, and placing the complete string into a GPO under **Log Access**. This method ensures the forwarding service can immediately gain access to the security event log without requiring the reboot of each computer when the computer pulls the GPO from the domain controller. For the ICS lab, Table 2 shows the following GPO that was configured and distributed across the environment.

The **Configure target Subscription Manager** setting in the domain logging GPO tells domain clients where to push their logs, which can be to one or more WEC servers. The next step is to configure a forwarding subscription on the WEC server to retrieve the targeted hosts' logs. A new subscription is configured by opening Event Viewer on the WEC server and creating a new subscription under Subscriptions, as shown in Figure 10.

The subscription is either source computer- initiated (push) or collector-initiated (pull). With the subscription type configured, there are three other steps to get the collector running. The next step is to select what events to collect. As no event filtering took place in the Splunk WMI data source, the subscription configuration did not perform any log filtering and, thus, all security event logs were pushed from the clients to the WEC, as shown in Figure 11.

Microsoft provides significant flexibility in the configuration by being able to only subscribe to logs by event ID or event



Logged: Last 24 hours

Event level: ☑ Critical ☑ Warning ☑ Verbose ☑ Error ☑ Information

● By log Event logs: Security

○ By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

<All Event IDs>

Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers>

Figure 11. WEC subscription source type and filter configuration.

Table 2: WEF GPO as deployed in the ICS lab.

Windows Components/Event Forwarding Policy	Setting
Configure target Subscription Manager	Enabled
SubscriptionManagers	
Server=http://WECServer.icsdomain.local:5985/wsman/SubscriptionManager/WEC	
Windows Components/Event Log Service/Security Policy	**Setting**
Configure log access	Enabled
Log Access	O:BAG:SYD:(A;;0xf0005;;;SY)(A;;0x5;;;BA)(A;;0x1;;;S-1-5-32-573)(A;;0x1;;;NS)
Windows Components/Windows Remote Management (WinRM)/WinRM Client Policy	**Setting**
Trusted Hosts	Enabled
TrustedHostsList:	*icsdomain.local
Windows Components/Windows Remote Management (WinRM)/WinRM Service Policy	**Setting**
Allow remote server management through WinRM	Enabled
IPv4 filter:	IPWECserver
Preferences	
Control Panel Settings	
Services	
Service (Name: WinRM)	
Service name	WinRM
Action	Start service
Startup type:	Automatic (Delayed Start)
Wait timeout if service is locked:	30 seconds

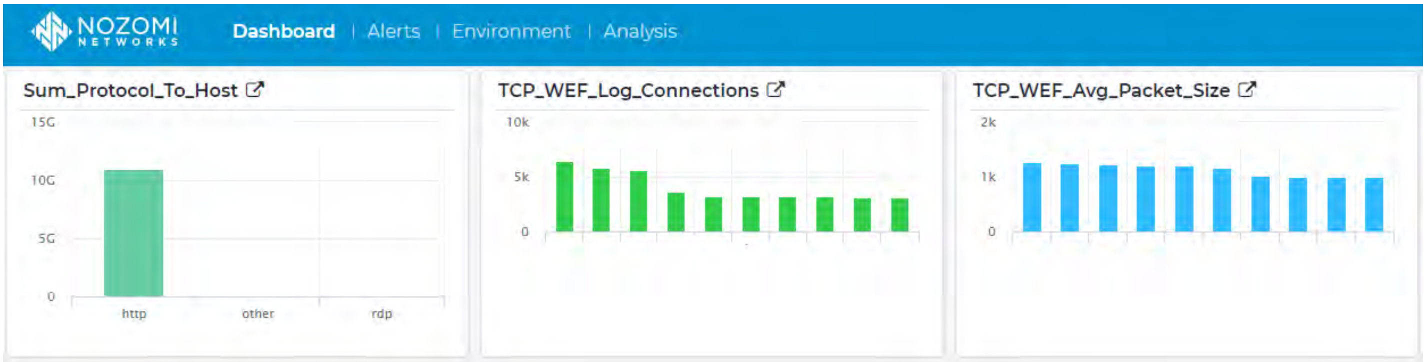


Figure 12. WEF network statistics measured by the NSM over six days of testing.

ID range. Subscriptions, therefore, can match use-cases defined by monitoring teams. Additionally, limiting logging activity to what is vital for incident analysis is an excellent way to reduce network traffic, log storage capacity, and minimize SIEM alerts. This is far more efficient than ingesting everything and filtering out what is critical in the SIEM.

Under advanced subscription settings, options include subscription protocol and latency requirements. Protocol selected is either HTTP or HTTPS and must match the target subscription managers' setting in the domain GPO. Latency can be set to Normal, Minimize Bandwidth, or Minimize Latency. Minimize latency sets a batch timeout of 30 seconds to push events to the WEC server, while Normal has a timeout of 15 minutes and the Minimize Bandwidth batch timeout is six hours (Halfin, Hardy, Mackenzie, Bichsel, & Justin, 2018). It is also possible to customize batch timeouts and heartbeat intervals beyond the three default settings to match network and ICS systems constraints.

> *"Bandwidth restrictions in ICS environments play a critical role in technology deployment and configuration"*

With latency configured, the final step is to select the individual computers or groups to join the subscription. Computers are individually added to the subscription by searching for and selecting the respective computer from the domain. However, a more efficient method is to utilize the built-in Domain Computers' group and the Domain Controllers' group. By default, when a computer joins a domain, it is automatically added to the Domain Computers' group. Therefore, this group contains all computers in the respective domain. Domain Controllers are added to the Domain Controllers' group as they have a unique responsibility in the domain. Therefore, between these two group objects, all computers are targeted. This method ensures that as computers are added or removed from the domain, they are automatically added or removed from the event log subscription.

WEF Bandwidth consumed

With six days of log collection, Figure 13 shows that WEF logging activities consumed a little over 10GB of network resources, which is 40 percent less than measured with WMI. As with WMI, this was not the full amount of bandwidth used but rather what was visible to the Nozomi NSM appliance. Since WEF uses HTTP as the outer protocol on TCP port 5985, the NSM appliance protocol inspection engine identifies WEF as HTTP and is displayed accordingly in Figure 12.

As with WMI, the graph shows the top 10 highest number of TCP connections and average packet sizes. The highest number of TCP connections in WEF push mode was over 6,000 and came from a domain controller. The second, and third, highest number of TCP connection also came from domain controllers. Numbers fell quickly with the remaining ICS servers in the lab, having less than 3,000 TCP connections during the test duration. The average packet size, however, for the WEF sessions hovered around 1KB. The consistent packet size could be attributed to higher overhead for WEF packets, such as encryption, but could also indicate that when hosts push their logs, they only do so when the log queue is full. Continuing this reasoning, WEF is utilizing the packet payload and network resources more efficiently than WMI is over DCOM.

RECOMMENDATIONS AND IMPLICATIONS

ICS owners and operators need a method to log host-based events in their environment and feed IT/OT SIEM systems for event reviewing, alerting, and analysis as part of ICS security standards and best practices. Historically, Windows systems used in ICS utilize WMI log methods as WMI is built into Windows and does not require log agents. However, WEF is a newer, alternative method, and options are available for complete domain configuration. WEF also does not require client system reboots and uses less bandwidth than WMI.

Recommendations for Practice

From the results of the WEF and WMI assessment in an ICS lab, the following recommendations should be considered for ICS owners and operators.

- Utilize WEF for newer client and server operating systems that support WinRM, which are Windows Vista or Server 2008 systems and newer. (Windows XP and Server 2003 operating systems will need a Windows patch to support WinRM.)
- Configure WEF push method with subscriptions targeted for domain computers and servers.
- Optimize subscription event filtering to support use-cases mapped to cyber defense activities and active defense programs in the ICS.
- Optimize subscription latency settings for the environment to ensure logs are forwarded quickly enough for SOC monitoring teams but are not consuming more network resources than needed for the use-cases.
- Consider one or two log collectors for each Windows domain and forward logs across domains to a centralized WEC using HTTPS protocol and certificates in the subscription settings.

One issue with WEF, which is a limitation with Windows event log 4GB size restriction, is that although multiple WEC servers can forward to a central WEC server, there is a limitation for log capacity without log archiving and rotation. Another option is to install a SIEM log forwarding agent on the WEC servers in the environment, such as a Splunk Forwarder used with a Splunk SIEM, to move logs off the WEC servers in the ICS environment to an OT or IT/OT SIEM.

Implications for Future Research

Bandwidth restrictions in ICS environments play a critical role in technology deployment and configuration. With regards to WEF, further research that focuses on subscription settings between Low Latency, Low Bandwidth, and Normal -- and their effects on both LAN and WAN networks -- would be beneficial. Additionally, understanding network resource requirements between HTTP and HTTPS and research regarding Public Key Infrastructure (PKI) certificate deployment to enable HTTPS within the constraints of ICS environments would also be worthwhile to the ICS community.

CONCLUSION

ICS owners and operators have increasing demands to comply with regulations, standards and recommended practices regarding security event monitoring, and this paper has shown that WEF is the preferred logging aggregation technology over WMI in Windows-based ICS environments. Although both WMI and WEF require Microsoft OS and domain administrative knowledge, WEF was found to be easier to deploy in ICS environments and brought features such as domain deployment, simplified firewall configuration, push subscriptions, and event ID filtering. More importantly, WEF utilized fewer network resources than WMI. To better understand WMI and WEF, both logging methods were deployed in an ICS lab and assessed for ease of deployment, configuration options, and network bandwidth consumption. ICS vendor restrictions on third-party log agents were taken into consideration, from the reality that owners and operators are frequently left to use native operating system functionality for host event logging. Ultimately ICS owners and operators must decide on the logging techniques and technologies that are tailored for their unique deployment but may wish to review and leverage inherent OS capabilities to accomplish the critical task of gaining endpoint log visibility in ICS environments.

REFERENCES

ACSC. (2018, July). ***Publications***. Retrieved from ACSC: https://www.acsc.gov.au/publications/protect/windows-event-logging-technical-guidance.htm

CIS. (2018, March 19). ***Controls***. Retrieved from CIS Center for Internet Security: https://www.cisecurity.org/controls/

Cisco. (nd). ***Configuring Inspection of Management Application Protocols***. Retrieved from Cisco: https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/tsd-products-support-series-home.html

Graeber, M. (2015). ***Briefings***. Retrieved from Black Hat: https://www.blackhat.com/docs/us-15/materials/us-15-Graeber-Abusing-Windows-Management-Instrumentation-WMI-To-Build-A-Persistent%20Asynchronous-And-Fileless-Backdoor-wp.pdf

Halfin, D., Hardy, T., MacKenzie, D., Bichsel, A., & Justin. (2018, February 15). ***Use Windows Event Forwarding to help with intrusion detection***. Retrieved from Windows IT Pro: https://docs.microsoft.com/en-us/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection

Helweg, O. (2008, August 11). ***Quick and Dirty Large Scale Eventing for Windows***. Retrieved from Microsoft TechNet: https://blogs.technet.microsoft.com/wincat/2008/08/11/quick-and-dirty-large-scale-eventing-for-windows/

Jonathan. (2009, January 9). ***WinRM (Windows Remote Management) Troubleshooting***. Retrieved from Microsoft TechNet: https://blogs.technet.microsoft.com/jonjor/2009/01/09/winrm-windows-remote-management-troubleshooting/

Keith Stouffer (NIST), S. L. (2015, May). ***Publications***. Retrieved from NIST: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Lee, R. M. (2015, August 5). ***The Sliding Scale of Cyber Security.*** Retrieved from SANS: https://www.sans.org/reading-room/whitepapers/ActiveDefense/sliding-scale-cyber-security-36240

Lee, R. M., & Assante, M. J. (2015, October). ***The Industrial Control System Cyber Kill Chain.*** Retrieved from SANS: https://www.sans.org/reading-room/whitepapers/ICS/paper/36297

Madden. (2006, December 4). ***WMI-Namespace-Security.*** Retrieved from Code Project: https://www.codeproject.com/Articles/15848/WMI-Namespace-Security

Microsoft. (2018, October 2). ***Service overview and network port requirements for Windows.*** Retrieved from Microsoft Support: https://support.microsoft.com/en-us/help/832017/service-overview-and-network-port-requirements-for-windows

Miller, B. (2017). ***Media***. Retrieved from Dragos: https://dragos.com/media/2017-Review-Hunting-and-Responding-to-Industrial-Intrusions.pdf

Murdoch, D. (2018). ***Blue Team Handbook: SOC, SIEM, and Threat Hunting Use Cases Notes from the Field.*** San Bernardino, CA: CreateSpace Independent Publishing Platform.

NERC. (2016, July 1). ***United States Mandatory Standards Subject to Enforcement.*** Retrieved from NERC: https://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-007-6&title=Cyber%20Security%20-%20System%20Security%20Management

NIST. (2018, April 16). ***Cybersecurity Framework***. Retrieved from NIST: https://doi.org/10.6028/NIST.CSWP.04162018

Novotek. (2018). ***Vast Differences Between IT and OT Cyber Security.*** Retrieved from Novotek: https://www.novotek.com/en/solutions/cyber-security-for-production-and-process-networks/vast-differences-between-it-and-ot-cyber-security

Payne, J. (2015, November 23). ***Monitoring what matters – Windows Event Forwarding for everyone (even if you already have a SIEM.).*** Retrieved from Microsoft TechNet: https://blogs.technet.microsoft.com/jepayne/2015/11/23/monitoring-what-matters-windows-event-forwarding-for-everyone-even-if-you-already-have-a-siem/

Searle, J. (2017). Log Management. In J. Searle, 410.3, ***Defending ICS Servers and Workstations*** (pp. 150-154). SANS Institute.

MICHAEL HOFFMAN is currently the global Principle ICS Security SME for Shell Downstream and has over 19 years of combined experience in ICS Security, Controls and Automation, and Instrumentation. Past roles have included Instrumentation & Analyzer Specialist in Downstream, Controls & Automation Specialist in Upstream, and ICS Security Engineer in Downstream.

Michael desires to continuously learn and give back to the ICS community by training the next generation of ICS security experts. He is currently pursuing a Master of Science in Information Security Engineering from the SANS Technology Institute and holds the following certifications: CISSP, GSTRT, GICSP, GCIP, GCIH, GCIA, GPYC, GSEC, CCNA, and MCSA.

Call for Papers for Publication

CSIAC JOURNAL
ARMY RESEARCH LABORATORY (ARL)
CYBER SCIENCE & TECHNOLOGY
SERIOUS GAMES TO ENHANCE DEFENSE CAPABILITIES
TOOLS & TESTING TECHNIQUES
ASSURED SOFTWARE

CSIAC is chartered to ***leverage the best practices and expertise from government, industry and academia*** in order ***to promote technology domain awareness and solve the most critically challenging scientific and technical (S&T) problems.***

As part of that mission, CSIAC publishes the *Journal of Cyber Security and Information Systems,* focusing on scientific and technical research & development, methods and processes, policies and standards, security, reliability, quality, and lessons learned case histories. Contributing authors realize the benefits of being published in a highly-respected resource within the technical community, with an enormous reach across the Department of Defense and the broader scientific community (23k+ subscribers). Demonstrate your expertise and accomplishments or pose the challenging questions for further thought in the resource that reaches fellow Subject Matter Experts (SMEs) developing the solutions to support the warfighter.

To Submit an Article

Visit: **https://www.csiac.org/csiac-journal-article-submission-policy/**

CSIAC is currently accepting articles submitted by the professional community for consideration in the following topic areas:

- › Advances in AI and machine learning, deep learning, cognitive computing, intelligent agent, chatbot
- › AI applications in industry, business, healthcare, and education and training
- › Biometric Identity Management
- › Trust, resilience, privacy and security issues in AI applications
- › Testing and validation of AI and ML applications
- › Security automation techniques/real-time incident response
- › IoT, Smart Cities, Connected & Autonomous Vehicles (CAV)
- › Data-Centric Security
- › Data Loss Prevention (DLP)
- › Endpoint Security Risk
- › DevOps/DevSecOps

(A non-exhaustive set of topics)

Transform your Knowledge of the Research Development Test and Evaluation (RDT&E) Budget Process by...

Quickly search, connect and analyze multiple RDT&E budget datasets, such as:

- President's Budget (PB)
- R2s and P40s
- Research Projects (URED)
- Congressional Budget Marks

START TODAY! Visit DTIC's New Research Budget and Project Information (RPBI) tool at https://www.dtic.mil/bt/ui

R&E Gateway Powered by DTIC

https://discover.dtic.mil (Public) | https://www.dtic.mil (NIPR) | https://www.dtic.smil.mil (SIPR)
Defense Technical Information Center (DTIC) | Fort Belvoir, Virginia 22060

APPLYING CYBER THREAT INTELLIGENCE TO INDUSTRIAL CONTROL SYSTEMS

By: Matthew Sibiga, Robert Mills, Mason Rice, and Stephen Dunlap

THE PURPOSE OF CYBER THREAT INTELLIGENCE (CTI) IS TO HELP PROTECT NETWORK INFRASTRUCTURES.

Threat intelligence platforms (TIPs) have been created to help facilitate CTI effectiveness within organizations employing traditional information technology networks. The industrial control system (ICS) sector can benefit from these technologies since most ICS networks are connected to IT networks. In this paper, we provide a high-level overview of CTI and TIP capabilities and show how they can directly support ICS security. We also discuss a prototype solution using a commercially available TIP in conjunction with a standard open source intrusion detection system to mitigate a well-known ICS attack, BlackEnergy.

INTRODUCTION

Industrial control system (ICS) networks have historically operated without much regard to security (compared to traditional IT) due to their proprietary properties and lack of external connectivity. However, with the evolution of the Internet and organizations looking for the most efficient way to do business, ICS and IT networks have become interconnected and in some ways indistinguishable.

The challenge with this new environment is that both types of networks have fundamental differences regarding their operational and security goals. An ICS network's main objectives are usually focused on integrity and availability, while IT networks tend to be more concerned about confidentiality. Further, there are safety and revenue implications that can arise from the lack of availability to ICS devices. ICS and IT network operators therefore have different risk tolerances and perspectives regarding security. The ICS sector also does not tend to have as many security and defense tools as found in the traditional IT area.

Improvements in cyber threat intelligence (CTI) are showing great benefits in cybersecurity. CTI is based on traditional intelligence gathering and processing activities and produces actionable information products that allow decision makers to understand their operational risks and better prioritize and allocate resources.

"CTI is much more than simply collecting and sharing data—its true value derives from putting threat information into context that is more meaningful for the end-user"

Although CTI has primarily focused on traditional IT systems, we believe ICS network operators can also derive benefit from this capability, because many of the threats to ICS actually come through traditional IT networks (e.g., business networks, billing systems, remote monitoring, etc.). In this paper, we provide a brief overview of CTI and its benefits. We then discuss threat intelligence platforms (TIPs) as an emerging technology used to better deal with the vast (and growing) amount of CTI data. We then discuss a notional scenario in which an ICS network connects to a larger enterprise network and show how CTI and TIP tools can be used in conjunction with standard IT security tools to improve the overall security posture of the ICS network. We conclude with an example implementation use case for the BlackEnergy ICS attack against Ukrainian energy companies.

CYBER THREAT INTELLIGENCE

In 2015, the Cyber Threat Intelligence Integration Center (CTIIC) was created with the mission of determining connections among malicious cyber incidents (The White House, 2015). A major thrust of this initiative was to promote development and sharing of CTI data throughout the public and private sectors.

Benefits of CTI. There are tactical, operational, and strategic benefits of CTI, as shown in Table 1. Tactical benefits will be seen instantly, and operational benefits will begin to form as the context of an attack becomes apparent. Strategic benefits result in an organizational situational awareness that will help current and future security initiatives (Shackleford, 2015 & Friedman & Bouchard, 2015).

Used effectively, CTI offers significant added value because threat information can be shared quickly, often in machine-readable formats that can be readily ingested by security incident and event management (SIEM) tools and increasingly capable threat intelligence platforms (TIPs). But CTI is much more than simply collecting and sharing data—its true value derives from putting threat information into context that is more meaningful for the end-user. This reduces uncertainty, improves situational awareness, and leads to more informed risk management and security investment.

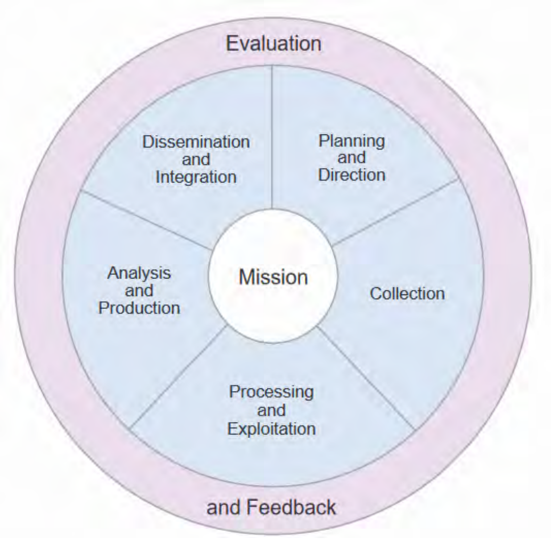


Figure 1: The Intelligence Cycle [4]

CTI Production Process. Development of CTI is similar to other forms of intelligence products and follows a traditional intelligence cycle (Figure 1) and as described in Joint Publication 2-0, *Joint Intelligence* (Deparptment of Defense, 2013).

The production cycle begins with requirements or questions that need to be answered, such as "What are the most significant threats to our organization?" or "Given our network maintenance posture, what kinds of attack techniques are we most vulnerable to?" Note that these questions are unique to the end-user and are not the same for everyone. There are no short cuts or technical solutions to replace the amount of introspection required to support a good risk management program. CTI is also adversary-based, because by knowing details about an adversary, an organization can enhance its protection against specific attack methods known to be used by that adversary.

Once the CTI requirements have been identified and prioritized, a data collection plan is developed (to include identification and evaluation of information sources), followed by data processing and exploitation. Analysis generates intelligence products (answers to the questions posed earlier), followed by timely dissemination to internal and external customers. The entire cycle includes ongoing evaluation and feedback to ensure that new information can be taken into account and to ensure that the original questions are being answered effectively.

Table 1: Benefits of CTI

Tactical	» Swift response to new indicators » Prioritize maintenance actions » Connect details associated with attacks quickly and accurately
Operational	» See attacks in larger context » Faster detection & remediation » Prevent future incidents
Strategic	» Broader situational awareness » Understand difference between real threats and hype » Allocate investments based on actual risk and adversary threats

Data Sources. Examples of CTI data sources include traditional SIEM tools (e.g., network monitors, firewalls, intrusion detection systems), dedicated CTI data feeds, vulnerability and malware databases, and the system users. The data collection must be timely and accurate, in addition to being relevant to address incidents that are likely to happen, are happening, or may be likely to happen. The data collected should also be meaningful to the organization and help answer the original CTI requirements.

From these sources, indicators of compromise (IOCs) can be identified, documented, and further analyzed. An IOC is a forensic artifact of an intrusion that can be identified on a host or network device. They are tied to observables and related to measurable events and can be categorized as either network-based or host-based. Network-based IOCs include email addresses, subject line and attachments, connections to specific IP addresses or web sites, and fully qualified domain names (FQDNs) used for botnet command and control (C2) server connections. Host-based IOCs may include the presence of filenames on a local drive, programs and processes that are running on a machine, and creation or manipulation of dynamic link libraries (DLLs) and registry keys.

The crux of CTI is the contextual information surrounding attacks. This is the comprehension of the past, present, and future tactics, techniques and procedures (TTPs) of an extensive range of adversaries. Included in this analysis should be the connection between the technical indicators, adversaries, their incentives and objectives and information about the target (Shackleford, 2015 & Deparptment of Defense, 2013). This should lead to informative and proactive decision-making.

"Analysts should be aware of and minimize internal biases and strive to manage and address uncertainty (e.g., known knowns, unknown knowns, etc.)."

Many CTI feeds exist, and the number is growing. Originators include private companies, government agencies, and non-profit group or open-source groups. Open Source feeds[1,2,3,4] are free to use, but they provide only basic IOC data with limited context, and the end-users need to perform more of the analysis to meet their specific needs. Commercial feeds[5,6,7,8] are richer and provide more actionable intelligence.

CTI data collection and analysis processes must be well-documented and efficiently executed, enabling organizations to think systematically on how to effectively use the collected information. Analysts should be aware of and minimize internal biases and strive to manage and address uncertainty (e.g., known knowns, unknown knowns, etc.). This includes keeping track of how answers are developed (traceability) and not just focusing on the answers themselves.

CTI products should also be customizable to meet the needs of different decision-makers. People consume and act on information differently depending on their role within the organization. An analyst will need just enough context to determine if further investigation is needed, whereas an incident responder may require extensive details to track down and assess related incidents. Finally, the chief security officer needs information to evaluate threats in a more global context (Friedman & Bouchard, 2015).

THREAT INTELLIGENCE PLATFORMS

A Threat Intelligence Platform (TIP) is a resourceful way to manage and automate CTI feeds, provide organizational-wide situational awareness, and integrate

[1] US Computer Emergency Readiness Team, "Automated Indicator Sharing," https://www.us-cert.gov/ais.
[2] Hail A TAXII, http://hailataxii.com/
[3] ThreatCrowd, https://www.threatcrowd.org/
[4] "Awesome Threat Intelligence," https://github.com/hslatman/awesome-threat-intelligence
[5] FireEye, "Cyber Threat Intelligence Services," https://www.fireeye.com/services/cyber-threat-intelligence-services.html.
[6] Symantec, "DeepSight Intelligence," https://www.symantec.com/services/cyber-security-services/deepsight-intelligence.
[7] Recorded Future, https://www.recordedfuture.com/.
[8] Verisign, https://www.verisign.com/en_US/security-services/index.xhtml.

with existing SIEM tools. Some well-known examples include AlienVault[9], ThreatStream[10], Recorded Future[7], and ThreatConnect[11]. Their capabilities vary, but successful integration can support timely analysis and visualization of intelligence from a wide range of sources. A TIP will also allow for concurrent access making existing network tools stronger and more integrated throughout the enterprise.

TIP employment is most beneficial within a Security Operations Center (SOC). The SOC (which could be a virtual organization) has teams which are responsible for IT control, monitoring and operations (e.g., analysts, incident responders, and Chief Security Officer). Key features are highlighted in Table 2 (Lawson & McMillan, 2014).

A general scenario showing how CTI and TIP technologies can be used within an organization is discussed below and illustrated in Figure 2. Detailed whitepapers are available to provide much more detail (Trost, 2016).

The process begins with ingesting CTI feeds, user input data, and local defensive network data. CTI feeds include commercial and open source feeds, whitepapers, government reports, technical reports, emails, SIEM logs, etc. A parser will extract, store, standardize, categorize, display and archive incoming data from the multiple sources. The SOC monitors the process to ensure proper operations and perform further research on the data to identify additional IOCs for inclusion in the TIP database.

As IOCs are incorporated into the TIP, they are classified with a status of Review or Active. Items labeled as Review are periodically analyzed for validity, and a human analyst may decide final approval of a data element. Some TIPs may be configured to automatically approve data that comes from certain sources. In some cases, IOCs may be deemed irrelevant, perhaps because of how the local network is configured, or because the risk is perceived as being low. The TIP will keep a record of these decisions, which duplication of effort and documents the approving authority's tolerance of risk when evaluating future IOCs. Once IOCs are validated for distribution, a TIP can automatically format the data for use with the organization's SIEM tools (e.g., IDS/IPS).

APPLYING CTI IN ICS NETWORKS

ICS networks generally do not have the same scope and breadth of security and SIEM tools as traditional IT networks. However, because most ICS networks connect to an IT network, some common IT security tools are applicable. Research has shown that using a standard IDS, such as SNORT, will improve security of ICS networks (Bartman & Kraft, 2016 & Horkan, 2015). SNORT's open source nature coupled with its vast IT security industry-wide adaptability make it highly recommendable for IDS purposes. In recent years, ICS and SCADA rule development has led to key enhancements for ICS infrastructures, to include specific SNORT rule sets for ICS security (Marshall, 2016 & Digital Bond). Similarly, ICS stakeholders wishing to increase their ability to prevent, detect, and remediate attacks would likely see benefit in adopting CTI and TIP solutions.

Table 2: TIP Capabilities

Collect	» Standardize ingestible threat data for analysts into one platform » Import and parse dedicated feeds and unstructured formats (e.g., email, webpages, and social media)
Act	» Activate tasks for teams (e.g., IDS signature updates and IOC analysis) » Create reports to distribute content and alerts to organizational wide users or a specific audience
Correlate	» Provide enrichment and pivoting data to find connections among IOCs » Produce threat landscape based on authoritative context
Integrate	» Transform higher level data to use with lower level tools and SIEMs » Develop signatures and data points for compatible IDS/IPS and firewalls » Create appropriate inputs for use in help desk tracking system
Categorize	» Organize IOCs by threat actor, country, severity, etc. » Gain insight into threat actor TTPs » Mark and refine IOCs to offer additional context and relevance
Share	» Support collaboration and sharing » Provide workflow coordination among organizational teams » Export data in a sharable format

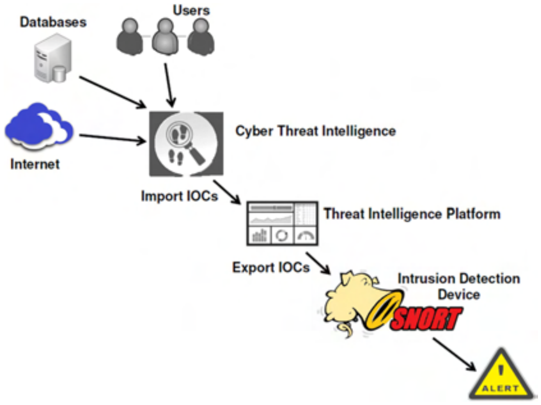

Databases
Users
Internet
Cyber Threat Intelligence
Import IOCs
Threat Intelligence Platform
Export IOCs
Intrusion Detection Device
SNORT
ALERT

Figure 2: Overview of CTI and TIP

Kill Chain and Indicators of Compromise. The two main stages of an ICS attack are gaining access (intrusion) and creating the effect itself (Lee, Assante & Conway, 2016). The intrusion stage will produce the most prevalent IOCs associated and can be studied using three zones as shown in Figure 3. In the *Internet* zone, threat actors conduct reconnaissance operations and decide where to probe further. The *Enterprise Network* zone is where threat actors either attempt to gain access to the internal network. IOCs associated with this could be spear-phishing email details, malicious files being delivered or downloaded.

[9] AlienVault, https://www.alienvault.com/.
[10] ThreatStream, https://www.anomali.com/.
[11] ThreatConnect, https://www.threatconnect.com/.

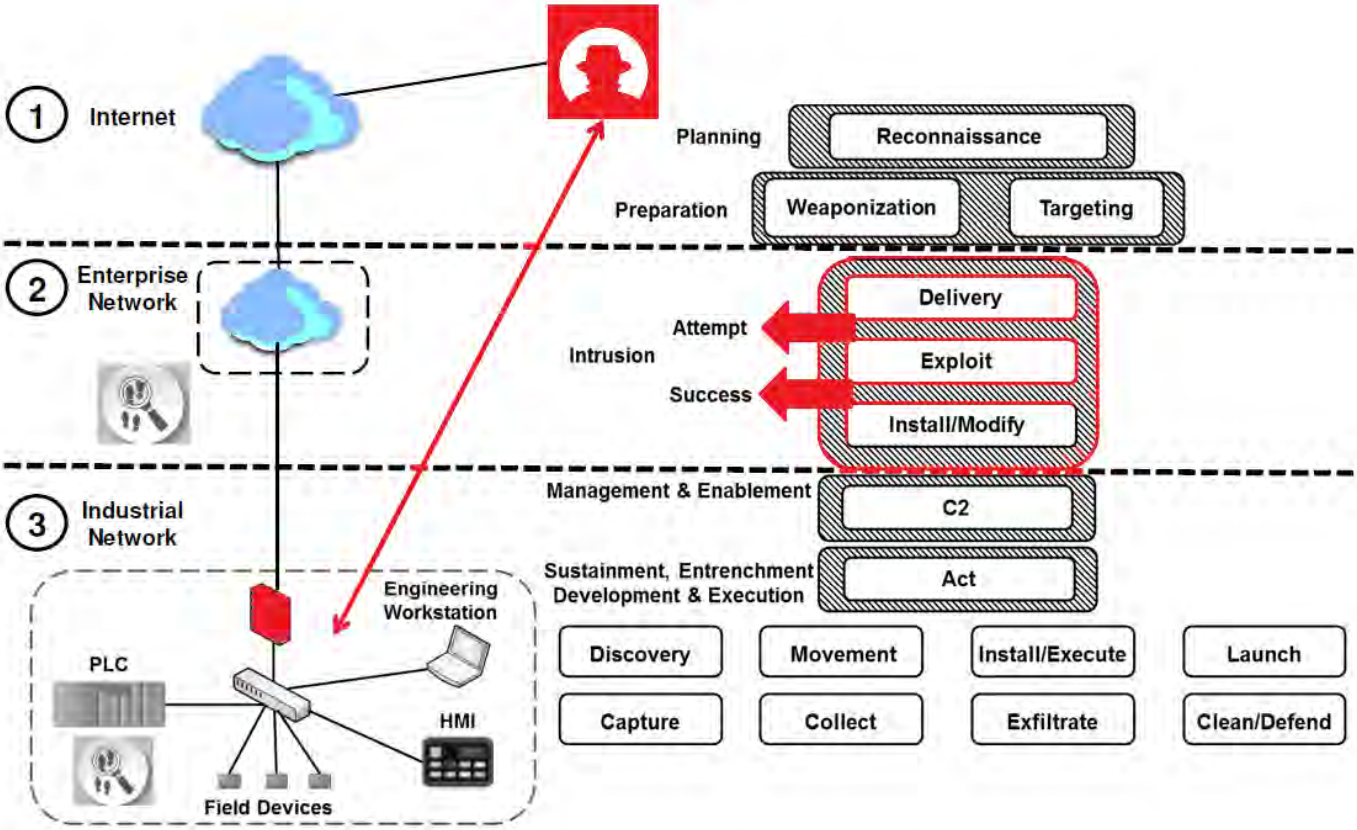


Figure 3: ICS Intrusion and Identifying Potential IOCs

Finally, the internal *Industrial Network* zone is where threat actors conduct C2 operations, maintain access, and prepare for future activity. IOCs associated with this could be unknown connections to external IP addresses and FQDNs, unrecognized programs, and any mutual exclusion or registry key creation.

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) has abundant information that can be used to support an ICS CTI program. Other sources for CTI include reputable security firms and credible ICS-related open source websites[12]. Published alerts, advisories, bulletins, security blogs, reports, and white papers are all excellent sources for gathering appropriate data.

Example ICS Attacks. We now introduce three well-known attacks (BlackEnergy, Duqu, and Havex) to further illustrate the utility of CTI and TIPs in ICS networks. The Dragonfly campaign against the Ukraine power companies used a variant of BlackEnergy malware, resulting in successful attacks with physical impact. Duqu and Havex were used to perform reconnaissance of ICS networks. Technical reports describe these attacks in great detail (Lee, Assante & Conway, 2016 & Symantec Security Response, 2011 & Belden), and in each case, the attack vectors came through a traditional IT infrastructure, so there will be IOCs related to IT systems.

BlackEnergy. In 2015, a Ukrainian power company, Kylvoblenergo, suffered power outages related to a cyber-attack. A use case was generated (Lee, Assante & Conway, 2016) to better educate ICS stake-holders about security threats, vulnerabilities, and adversary TTPs. The attackers used spear-phishing to obtain valid credentials to gain initial access to the targeted networks. This included emailing infected Microsoft Office attachments which then allowed the malware to establish contact with its C2 system. Using stolen credentials, attackers mapped the victim network, pivoted through the infrastructure, and elevated privileges. Gaining persistent access, they abandoned the original access point and used virtual private networks (VPNs) to access devices controlling electrical power breakers, and about 27 substations were brought offline. Potential IOCs associated with this ICS attack include email (subject and to/from addresses), attachment file names, and traffic associated with in- and outbound C2 connections.

Duqu. Duqu was documented in a technical report in 2011 (Symantec Security Response, 2011). Nearly equivalent to Stuxnet, Duqu's intent was not to cause physical damage but to gather intelligence on the victim's assets and infrastructure, possibly to facilitate a future attack. It is primarily a remote access Trojan (RAT) and does not have any code specifically related to ICS. It contains three files: a driver, a main dynamic linked library (DLL), and an encrypted configuration file. In one reported case, the malware was delivered as a Microsoft Word email attachment containing a zero-

[12] SCADAHacker, "Think Like a Hacker to Secure Industrial Control Systems," https://scadahacker.com/

day exploit. The infection process for the malware is beyond the scope of the paper, but essentially an installer injects the main DLL into the core operating system begins a process of extracting other harmful components, which are then injected into other processes allowing security products to be avoided. One component is responsible for establishing C2 connections outside the target network using web requests. Attackers enumerated the network, logged keystrokes, and gathered system details. Duqu also propagates using network shares and peer-to-peer connections. Potential IOCs would include filenames and hashes of the malicious files and IP addresses of the C2 connections.

Havex. The Dragonfly attacks included multiple forms of malware, such as the Havex RAT, to conduct espionage and reconnoiter ICS networks (Belden & Kaspersky Lab, 2014 & Nelson, 2016). Threat actors planted malware on targeted machines using spear-phishing emails, watering hole attacks, and trojanized software downloads from compromised ICS vendor websites. All three methods required user action to trigger the malware installation, and upon installation the malware would establish contact with a C2 web server. Multiple modules were embedded in the reply message and installed on the target machine. Havex would then embed itself into the Windows Registry and maintain persistent presence. Havex also highlighted the vulnerabilities to so-called air-gapped networks that rely on engineering workstations moving from the main IT network to isolated ICS worksites. Potential IOCs from this attack include FQDN, filename's along with their respective hashes and registry entries.

> *"CTI is much more than simply collecting and sharing data—its true value derives from putting threat information into context that is more meaningful for the end-user"*

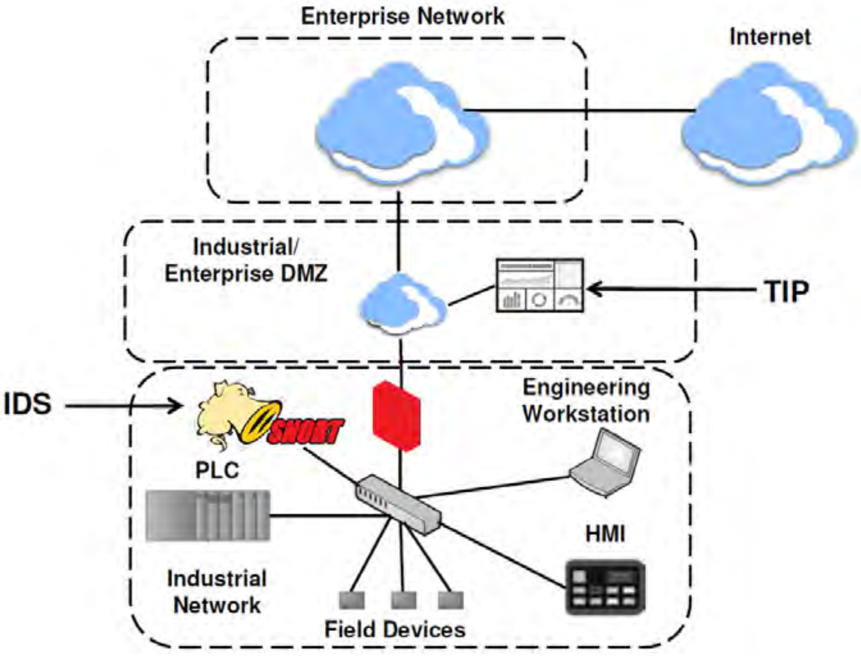


Figure 4: IT and ICS Sample Network

EXAMPLE IMPLEMENTATION

In this section, we present complete solution for using CTI and TIP in order to improve security against the BlackEnergy threat to ICS networks. Our demonstration used ThreatQ [13] as a TIP solution employed in the DMZ as shown in Figure 4, and we used SNORT for the internal network.

Virtual machines (VMs) were used to emulate most of the devices, to include two engineering workstations (Ubuntu and Windows 7) and a human machine interface machine (Windows XP). Figure 5 shows the general flow (which parallels Table 2) of information used to obtain pertinent CTI and ultimately generate signatures for SNORT IDS alerts.

ThreatQ offers great flexibility in importing and exporting data. While there are pre-programmed export options, it is highly tailorable to a wide variety of implementations. Open source data from ICS-CERT, Symantec, SCADAHacker[14], and IOC Bucket[15] were used to gather general CTI. The primary source for this example was an alert document regarding Ukraine's power outages[16]. This document was obtained from the ICS-CERT secure portal document library and outlines the IOCs associated with this particular attack, such as FQDNs, email headers, IP addresses, URLs and filenames. Six pages of the document were exported to a PDF file that was imported into ThreatQ. Other CTI sources could also be used in a similar manner.

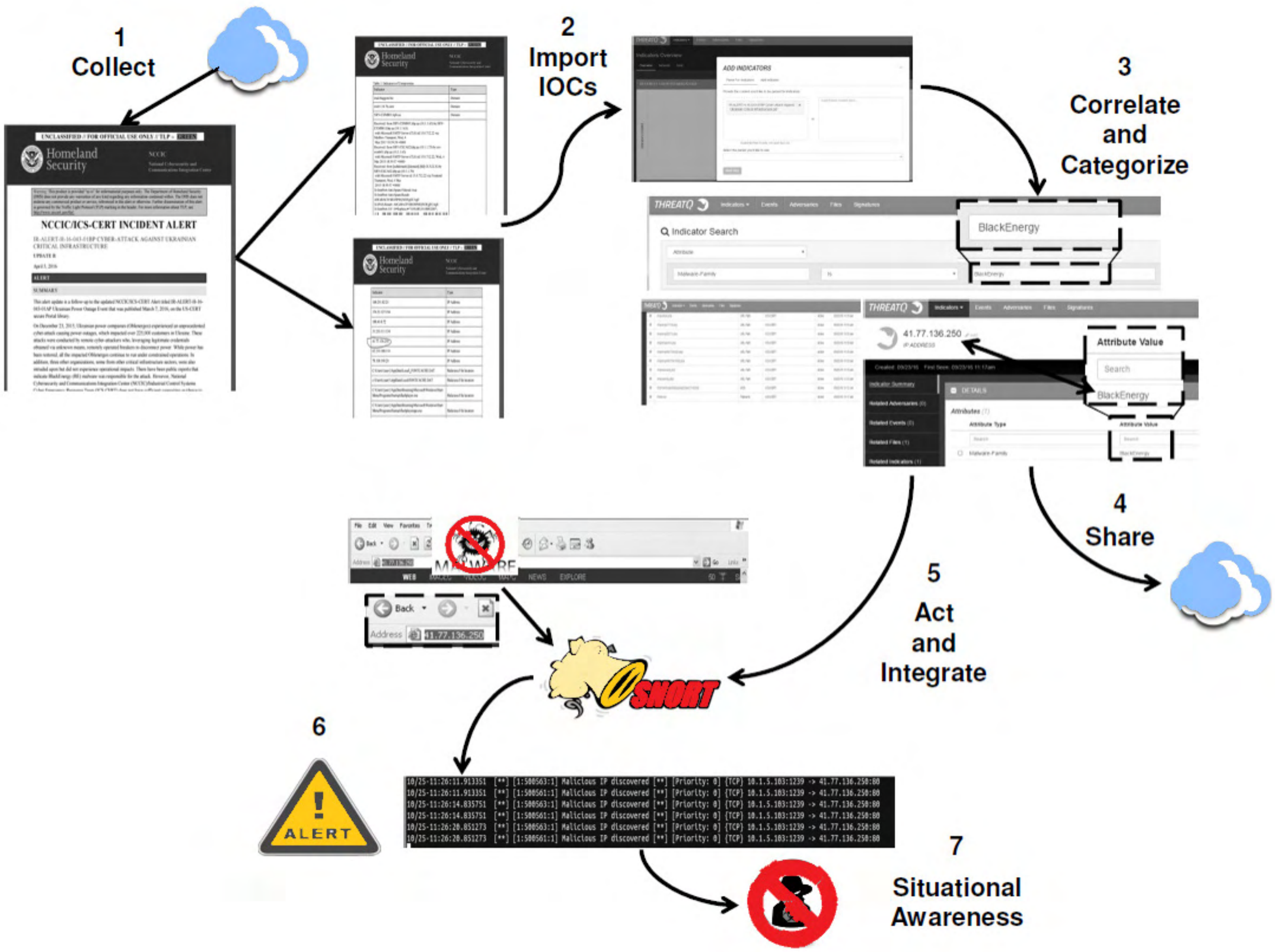
Once imported into ThreatQ, the information was correlated and categorized as part of the BlackEnergy malware family. At this point, the using organization could also share this intelligence with outside entities using a simple export operation provided by ThreatQ.

[13] ThreatQuotient, "ThreatQ Threat Intelligence Platform," https://www.threatq.com/threat-intelligence-platform/.

[14] SCADAHacker, "Think Like a Hacker to Secure Industrial Control Systems," https://scadahacker.com/.

[15] IOC Bucket, "Community Supported Threat Intelligence," https://www.iocbucket.com/

[16] Industrial Control Systems Cyber Emergency Response Team, "Cyber-Attack Against Ukrainian Critical Infrastructure," https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01



```
10/25-11:26:11.913351  [**] [1:500563:1] Malicious IP discovered [**] [Priority: 0] {TCP} 10.1.5.103:1239 -> 41.77.136.250:80
10/25-11:26:11.913351  [**] [1:500561:1] Malicious IP discovered [**] [Priority: 0] {TCP} 10.1.5.103:1239 -> 41.77.136.250:80
10/25-11:26:14.835751  [**] [1:500563:1] Malicious IP discovered [**] [Priority: 0] {TCP} 10.1.5.103:1239 -> 41.77.136.250:80
10/25-11:26:14.835751  [**] [1:500561:1] Malicious IP discovered [**] [Priority: 0] {TCP} 10.1.5.103:1239 -> 41.77.136.250:80
10/25-11:26:20.851273  [**] [1:500563:1] Malicious IP discovered [**] [Priority: 0] {TCP} 10.1.5.103:1239 -> 41.77.136.250:80
10/25-11:26:20.851273  [**] [1:500561:1] Malicious IP discovered [**] [Priority: 0] {TCP} 10.1.5.103:1239 -> 41.77.136.250:80
```

Figure 5: CTI and TIP for BlackEnergy Use Case

SNORT was initially configured using prevalent ICS rules from ICS-CERT[17], Emerging Threats[18], and Digital Bond[19]. The IDS host also included user-developed python scripts to create additional SNORT rules based on information provided by ThreatQ, such as malicious IP addresses, filenames, MD5 hashes, and DNS queries.

A scenario was then constructed to test the rules generated from ThreatQ. In the scenario, the HMI machine opens an Internet Explorer window and attempts to visit an IP address (41.77.136.250). This address had been correlated to BlackEnergy by ThreatQ, and an alert rule was automatically configured for SNORT. The IDS successfully alerted that a malicious IP address was being accessed within the network. As a result, improved situational awareness was obtained to stop and prevent future attacks.

While this example focused on BlackEnergy, the same approach works equally well for Duqu, Havex, and other ICS threats.

TECHNOLOGY LIMITATIONS

CTI and TIP may not be mature enough for most organizations to fully and successfully implement without signification customization. The standards for the data structure and sharing CTI are evolving. The MITRE corporation started an initiative that created the Structured Threat Information eXpression (STIX) language and Trusted Automated eXchange of Indicator Information (TAXII) delivery protocol for CTI. However, these are now being transferred to another standard, OASIS[20]. Because of these evolving standards, organizations using CTI may have to invest additional time and resources to stay abreast and perhaps revisit their implementation.

Additionally, commercial feeds operated by vendors use proprietary methods for delivery, thereby complicating their integration into a larger TIP solution. Offerings by vendors are still

[17] ICS-CERT, "Industrial Control Systems Cyber Emergency Response Team," https://ics-cert.us-cert.gov/.

[18] Emerging Threats, "Emerging Threats Rule Documentation," http://doc.emergingthreats.net/

[19] Digital Bond, "Snort IDS/IPS rules for ICS and ICS Protocols," https://github.com/digitalbond/Quickdraw-Snort

[20] "OASIS Cyber Threat Intelligence (CTI) Technical Committee," https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti.

somewhat vague, leading to confusion as to which intelligence is actionable compared to second-rate information. Over time, the CTI community will be better able to determine what intelligence is actually useful and provide better tools for effectiveness.

Finally, IOC data that is specific to ICS threats is quite limited. ICS-CERT hosts an advisory website that lists specific known vulnerabilities in ICS systems categorized by vendor. At the time of this writing there were numerous advisories related to buffer overflows, but CTI and TIPs will not account for this type of attack because they are not considered IOCs but rather flaws in software and/or firmware designs. Attackers can also use a variety of exploits (cross site scripting or structured query language injection) to obtain unauthorized access without leaving observable or measurable artifacts to support CTI.

CONCLUSION

The capabilities of cyber threat intelligence and threat intelligence platforms show significant potential in cybersecurity for industrial control systems and critical infrastructure. These technologies benefit IT and ICS infrastructures because of the connections these environments directly have in this ever-connected world. Capabilities and standards are still evolving, but as the community grows, information sharing should improve, yielding greater benefits over time.

The views expressed in this document are those of the author and do not reflect the official policy or position of the United States Air Force, the United States Department of Defense, or the United States Government.

REFERENCES

The White House, "Fact Sheet: Cyber Threat Intelligence Integration Center," https://obamawhitehouse.archives.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center.

D. Shackleford, "Who's Using Cyberthreat Intelligence and How?," 2015, https://www.sans.org/reading-room/whitepapers/analyst/who-039-s-cyberthreat-intelligence-how-35767.

J. Friedman and M. Bouchard, "Definitive Guide to Cyber Threat Intelligence," 2015, http://cryptome.org/2015/09/cti-guide.pdf.

Department of Defense, "Joint Publication 2-0, Joint Intelligence," 2013, http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_0.pdf.

US Computer Emergency Readiness Team, "Automated Indicator Sharing," https://www.us-cert.gov/ais.

Hail A TAXII, http://hailataxii.com/.

ThreatCrowd, https://www.threatcrowd.org/.

"Awesome Threat Intelligence," https://github.com/hslatman/awesome-threat-intelligence.

FireEye, "Cyber Threat Intelligence Services," https://www.fireeye.com/services/cyber-threat-intelligence-services.html.

Symantec, "DeepSight Intelligence," https://www.symantec.com/services/cyber-security-services/deepsight-intelligence.

Recorded Future, https://www.recordedfuture.com/.

Verisign, https://www.verisign.com/en_US/security-services/index.xhtml.

AlienVault, https://www.alienvault.com/.

ThreatStream, https://www.anomali.com/.

ThreatConnect, https://www.threatconnect.com/.

C. Lawson and R. McMillan, "Technology Overview for Threat Intelligence Platforms" https://www.gartner.com/doc/2941522/technology-overview-threat-intelligence-platforms.

R. Trost, "ThreatQ's Instant ROI to Standardize Intelligence Workflows in the Enterprise," 2016, http://www.infosecurityeurope.com/__novadocuments/242948.

T. Bartman and J. Kraft, "An Introduction to Applying Network Intrusion Detection for Industrial Control Systems," in The Iron & Steel Technology Conference and Exposition (AISTech), Pittsburgh PA, 2016.

M. Horkan, "Challenges for IDS/IPS Deployment in Industrial Control Systems," 2015, https://www.sans.org/reading-room/whitepapers/ICS/challenges-ids-ips-deployment-industrial-control-systems-36127.

C. Marshall, "IEC60870-5-104 Protocol Detection Rules," https://blog.snort.org/2016/12/iec60870-5-104-protocol-detection-rules.html.

Digital Bond, "Snort IDS/IPS rules for ICS and ICS Protocols," https://github.com/digitalbond/Quickdraw-Snort.

M. Assante and R. Lee, "The Industrial Control System Cyber Kill Chain," 2015, https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297.

SCADAHacker, "Think Like a Hacker to Secure Industrial Control Systems," https://scadahacker.com/.

R. Lee, M. Assante and T. Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid," 2016, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

Symantec Security Response, "W32.Duqu -The Precursor to the Next Stuxnet," 2011,http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet_research.pdf.

Belden, "Defending Againsts the Dragonfly Cyber Security Attacks," https://info.belden.com/ab-cyber-security-dragonfly-bc-lp.

Kaspersky Lab, "Energetic Bear -- Crouching Yeti," July 2014, https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08080817/EB-YetiJuly2014-Public.pdf.

N. Nelson, "The Impact of Dragonfly Malware on Industrial Control Systems," 2016, https://www.sans.org/reading-room/whitepapers/ICS/impact-dragonfly-malware-industrial-control-systems-36672.

ThreatQuotient, "ThreatQ Threat Intelligence Platform," https://www.threatq.com/threat-intelligence-platform/.

IOC Bucket, "Community Supported Threat Intelligence," https://www.iocbucket.com/.

Industrial Control Systems Cyber Emergency Response Team, "Cyber-Attack Against Ukrainian Critical Infrastructure," https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

ICS-CERT, "Industrial Control Systems Cyber Emergency Response Team," https://ics-cert.us-cert.gov/.

Emerging Threats, "Emerging Threats Rule Documentation," http://doc.emergingthreats.net/.

"OASIS Cyber Threat Intelligence (CTI) Technical Committee," https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti.

Cyber Security & Information Systems
Information Analysis Center

Need Specialized Technical Support with Easy Contract Terms?

Core Analysis Task (CAT) Program

A Pre-Awarded, Pre-Competed Contract Vehicle.

CSIAC provides Subject Matter Expert (SME) support on an as-needed basis to quickly address technical requirements with minimal contracting effort. CSIAC provides such solutions via the utilization of our Core Analysis Task (CAT) service/capability. CSIAC is a competitively awarded contract with Indefinite Delivery/Indefinite Quantity (ID/IQ) provisions that allow us to rapidly respond to our users' most important needs and requirements. Custom solutions are delivered by executing user-defined and funded CAT projects without the need for further competition.

Through the CAT program, CSIAC is a pre-competed contracting vehicle, enabling the DoD and other agencies to obtain technical support for specific projects/programs that fall within one of the CSIAC technology areas. As with any inquiry, the first four hours are free. If the scope requires a CAT, CSIAC will assist with the development of a Performance of Work Statement (PWS) to be approved by the Contracting Officer's Representative (COR).

Key Advantages of working with CSIAC:

Expansive Technical Domain
The CSIAC's broad technical scope provides numerous pre-qualified resources for potential projects, and is especially valuable for today's information system challenges that frequently cross multiple domains.

Comprehensive STI Repositories
As a consolidation of three predecessor Information Analysis Centers (IACs), CSIAC has a wealth of expertise, data and information to support the successful completion of CATs.

Expansive Subject Matter Expert Network
CSIAC is able to leverage reach-back support from its expansive SME Network, including technical experts from the CSIAC staff, team members, or the greater community, to complete CATs.

Minimal Start-Work Delay
Not only does CSIAC provide DoD and other government agencies with a contract vehicle, but as a pre-competed single award CPFF IDIQ, work can begin in just a matter of weeks.

Apply the Latest Research Findings
CSIAC draws from the most recent studies performed by agencies across the DoD, leveraging the STI holdings of the Defense Technical Information Center (DTIC). The results of all CSIAC CATs and other DoD-funded efforts are collected and stored in DTIC's STI repository to support future efforts by the CSIAC and others.

How To Get Started

If you have a need for CSIAC technical support, the first step is to contact us. All Technical Inquiries are free to the customer for up to four hours of service. If the scope of the support is more extensive and requires a CAT, CSIAC will assist with the development and submission of the task description and related contract documents. CATs may be awarded as either Cost Plus Fixed Fee (CPFF) or Firm Fixed Price (FFP) delivery orders.

Inquiries may be submitted by email to **info@csiac.org**,
or by phone at **1-800-214-7921**.

Please visit our website for more information:
https://www.csiac.org/services/core-analysis-task-cat-program/

Who We Are

The Cyber Security Information Systems Information Analysis Center (CSIAC) is the DoD's Center of Excellence in Cyber Security and Information Systems, covering the following technical domains:

- Cybersecurity
- Software Engineering
- Modeling and Simulation
- Knowledge Management/ Information Sharing

CSIAC is chartered to leverage best practices and expertise from government, industry, and academia to solve the most challenging scientific and technical problems. The Center specializes in the collection, analysis, synthesis, and dissemination of Scientific and Technical Information (STI) to produce solutions in support of the defense community.

Our Team

Quanterion Solutions Incorporated is the prime contractor responsible for operating the CSIAC. In addition to Quanterion, customers also have access to the other members of the CSIAC team which include leading technology corporations as well as prestigious academic institutions that perform cutting edge research activities to expand our knowledge base.

266 Genesee Street
Utica, NY 13502

1-800-214-7921
https://www.csiac.org

Cyber Security and Information Systems
Information Analysis Center
266 Genesee Street
Utica, NY 13502

THE CENTER OF EXCELLENCE IN CYBER SECURITY AND INFORMATION SYSTEMS

Leveraging the best practices and expertise from government, industry, and academia in order to solve your scientific and technical problems

CSIAC
Design and Development Process for Assured Software – Volume 1
Journal of Cyber Security & Information Systems
Read the Journal
Upcoming Events
Share and Invite
Read the Latest Journal

https://www.csiac.org/journal/

To unsubscribe from CSIAC Journal Mailings please email us at ***info@csiac.org***
and request that your address be removed from our distribution mailing database.