




# Industrial Control Systems The “Other” Network And Cyber Security

Dated: March 7, 2019 – Davenport – GICSP 1848



## What are ICS Networks?

## What are ICS Networks?

- ICS, or Industrial Controls Systems, is a generic term referencing networks that manage, monitor, control, log and alert for trouble, automated processes conducted by machines for precision, accuracy and safety across a wide range of applications.
- ICS Networks are encountered every day, oftentimes overlooked or taken for granted, yet are vital to our society and our way of life.
- Systems generically referred to as ICS include SCADA, or Supervisory Control and Data Acquisition systems, PCS, or Process Controls Systems, DCS, or Digital Controls Systems, SiS, or Safety Instrumentation Systems, et al.
- Whether processes are Discrete, Batch or Continuous, ICS systems provide control and insight into these automated processes.
- Although these systems do have distinct differences between them, and related application for specific jobs, the purpose is pretty much the same – control of automated processes in a safe, efficient fashion.

## What are ICS Networks?

**Some examples of ICS in action include:**

**Energy Production** – Nuclear power plants, gas and oil production, oil refineries, even control of hydro-electric turbines, all leverage ICS networks.

**Manufacturing** – Be it automotive, chemical production, food processing, metal stamping, you name it, you will typically find process control systems in play.

**Energy Transmission and Management** – Grid operations are all about controls systems, as are pipelines transporting oil and natural gas from the wells to the homes and businesses, while allowing operators to know when to feed more power or oil into the delivery systems for consumption.

**Transportation** – Trains, subways, etc. are now mainly operated by ICS systems.

**Building Management Systems** – Believe it or not, any facility built within the last 25 years is maintained and controlled by an ICS network. From environmental controls, lighting, elevator operations, dehumidification and humidification, to physical access controls on doors, gates, elevators are all controlled by ICS networks. BMS systems are most often easily taken for granted as these systems are not seen as impacting an operations' bottom line.



## What are ICS Networks?

### ICS and Enterprise IT Network Similarities:

Certainly several similarities exist between traditional Enterprise IT networks and ICS/ OT (Operation Technologies) networks:

**Each network contains similar infrastructure** – switches, firewalls, network wiring and data closets

**Workstations/ Desktop Computers** – The devices humans interface with data/ information

**Servers** – Hosting central repositories for historical data, commonly used files, reporting tools, electronic communications hosts, etc.

**Some peripherals** – like printers, multi-function copiers, fax machines, modems, etc.



Enterprise IT vs. ICS  
Similar technologies – different purpose and  
priorities

## ICS Purpose and Priorities

### An ICS Network has a different purpose

Although we are still dealing with data, this data is used for a completely different purpose, and although we are not dealing with specific IP or PII, some sensitive information, such as floor plans, engineering documents, etc. certainly must be protected. However, the primary purpose for ICS networks is real-time operation of mechanical systems acting together in an automated process.

In an ICS system, confidentiality will take a back seat to SAFETY, and in the controls system world, real-time, or near real-time availability, 24/7/365, is of paramount importance.

Unfortunately, as technology and its application in everything has grown, hackers have evolved as well, and the attack surface has exploded exponentially.

Despite the surface similarities between Enterprise IT and ICS Networks, each network has vastly differing purposes, and with that priorities for IT professionals and Process Engineers to be well aware of.

### Enterprise IT purpose and Priorities

**Purpose:** Fast, efficient and reliable production, transformation and storage of business-critical information, communications, planning, analysis and forecasting impacting the viability and competitiveness of a business or organization

**Priorities:** Secure vital and proprietary information from unauthorized access, damage or theft, from threats both inside and outside the organization

### ICS Purpose and Priorities

**Purpose:** Control of automated processes/ jobs done by physical machines to assure safe, efficient and precise processes critical to that which is produced by the business, or operations of business assets

**Priorities:** Real-time insight and control of process machines to assure operations are safe from harming human life, physical assets and the environment, 24/7/365.

## ICS Purpose and Priorities

### Traditional IT - CIA

- 1 – Confidentiality
- 2 – Integrity
- 3 – Availability

- Confidentiality of data is the top concern for traditional IT. Protecting information from outside breach and from inside personnel accessing certain data, while keep other information confidential.
- Assuring the integrity of data for accuracy, against errors and packet corruption to assure all information is accurate and reliable.
- Availability is the final concern for IT, as if it requires a few minutes to access a report due to measures protecting the confidentiality and integrity of the data, or if the accounting platform is down for maintenance for a period of time during the day, that time trade off to ensure confidentiality is acceptable.

### OT – Operation Technology - AIC

- 1 – Availability/ Safety
- 2 – Integrity
- 3 – Confidentiality

- Availability is the number one priority for ICS. Any measures taken to secure ICS systems that negatively impact real-time or near real-time availability to the system and its process readings must be avoided. Oftentimes processes of a controls system demands millisecond responses to variable changes, otherwise problems can arise, which could result in catastrophic consequences if the system is unavailable, even for a very short period of time. Often, these systems run 24/7/365, and any interruptions unless meticulously scheduled, is considered unacceptable.
- Integrity of the data must be assured, as is similar to traditional IT. Readings and point values must be protected from error from malformed data packets, communications interruptions, etc.
- Confidentiality is not as critical in OT environments, as much of the information pertains to historical logging, although specific process controls programming does require defense. Since many ICS platforms use proprietary programming language, coupled with specific calls to differing types of field controls, even defending this data from snooping is not as critical as having these programs available for adjustment when needed.

## ICS Purpose and Priorities

### **Lifecycle differences between ICS and Enterprise IT and related vulnerabilities**

Traditional Enterprise IT networks have typical lifecycles of workstations and servers of @ 3-5 years.

- Driven by advances in computing capabilities
- More capable operating systems' releases requiring new hardware architecture to support the OS environment
- Third-party software solutions, such as ERP systems, evolve with operating systems and new features and security designs are included in these updated platforms
- Regular upgrading/ replacing old systems with new not only increases productivity and security (sometimes), but reduces the cost of infrequent upgrades when versions have advanced beyond upgrade paths built into new versions, requiring step-upgrades which cost more time and money

ICS networks typically have a lifecycle of 10-20 years, depending on devices

- Systems and process engineers are responsible for systems upgrades, rather than IT
- Operational integrity is more important than being on the "bleeding edge" – "if it ain't broke, don't fix it"
- Upgrades to ICS systems can result in significant down time that can impact production of goods the organization relies on for revenue
- The real time operating system controllers and field devices can be exponentially more costly to replace, based on location and accessibility of these devices, and compatibility concerns with the newer technologies can deter regular upgrades



## ICS Purpose and Priorities

### Real-time Operating System Devices – the true workhorses of ICS Networks

In the Enterprise IT environment, the workhorses are servers and workstations running information-delivering applications, increasing productivity, speed to discovery of trends, financials, etc. From electronic communications, to cloud-storage and services, the Enterprise IT edge has been extended, allowing great collaboration and productivity from anywhere, anytime.

However, in an ICS environment, the workhorses are not the workstations and servers, rather the network-connected devices running a real-time operating system, such as firmware or lightweight versions of operating systems such as LinuxRT, or other customized platforms.

In the old days, these devices are driven by straight C compiled firmware. Microprocessor architecture is limited, with dedicated processing power mainly focused on the controls duties themselves. Some processing power is dedicated for logging historical actions, and some for trouble faults and alarm detection and transmission to the HMI/ monitoring stations. However, the primary purpose is control of automated processes, and any additional duties, such as decrypting asymmetric encryption keys, or authorization lookups against roll based tables require processing resources – resources that often do not exist without sacrificing a critical operational and safety function.



## ICS Evolution, the Computing Revolution, and Impacts to Threat Landscape

### **ICS Evolution – History in brief**

- Networked controls systems began in the late-1970's, replacing manual facility controls systems
- Centralized controls increased efficiencies and reduced costs of facilities' labor liabilities
- Early ICS systems were 100% proprietary in nature, including computer systems employed as Human Machine Interfaces/ Engineering stations and DBMS/ Historian servers
- Communications protocols and network architecture was designed with speed and high-availability in mind
- Security was not built into these controls protocols, as no significant interconnected networks existed
- The first official controls system protocol was developed and launched in 1979 – MODBUS-IP
- Controls networks were separated physically/ air-gapped
- Controls Systems Security was done with the 3 G's – Gates, Guards and Guns

Due to the nature of these controls systems, be it SCADA (Supervisory Control and Data Acquisition systems), DCS (Digital Controls Systems), PCS (Distributed Digital Controls), or a variety of other acronyms lumped together as ICS (Industrial Controls Systems), the HMIs (Human Machine Interface) and Servers were typically expensive and proprietary, needing to be purchased from and supported by the controls vendor, resulting in very costly systems in total.


### **ICS Evolution continued...**

- The Personal Computer revolution in the 1990's completely altered Controls systems operation and affordability
- Computer systems proliferated with ease of use
- New commercially available server platforms increased business function extensions (Netware and Windows NT)
- Widespread availability reduced costs of ownership
- In response, controls vendors began development of ICS systems to leverage this new Computers Off The Shelf (COTS) option
- As proprietary computer systems were replaced with COTS, tremendous cost-savings were realized through widespread availability and reduced need for specialized support available only through the vendor
- The emerging IT profession viewed the common operating system designs as more efficient to service and maintain
- The age of COTS had arrived
- Ethernet communications development expanded networking capabilities and network performance
- Despite these evolutions, ICS protocols remained relatively unchanged
- Field devices remained unchanged, while field controls moved to Ethernet networks





# Evolution of Threats



## Evolution of Threats

### **Technical progress creating vastly larger attack surface.**

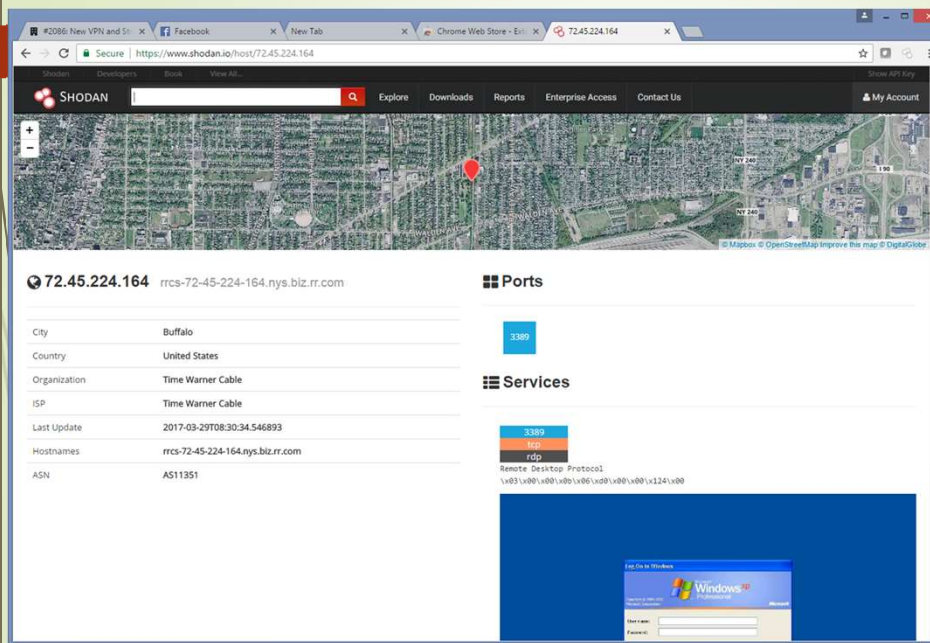
- Interconnectivity, both inside an organization and to the outside world.
- Employment of universally-available operating systems vs. proprietary – a vulnerability in one is a vulnerability in all systems.
- Networking device evolution incorporating more software and complexity creates more opportunity through coding mistakes. Increased communication features, such as the move from single-duty transmission (send or receive) to the full duplex, multitask (transmit and receive simultaneously) supports more data on the wire
- New IoT devices bring additional security and asset management concerns, opening another avenue of attack.
- Reliance upon discovery of vulnerabilities and identification of new malware signatures, creates reactionary conditions vs. proactive practices that are more desired.



## Evolution of Threats

### The Internet and Electronic Communications – The Double-Edge Sword

- The Internet has certainly opened up the world of information, as knowledge-base articles, technical documents, architecture recommendations are all available online from vendor websites and document-sharing communities. However, this same information used to help solve problems or streamline system design and deployments can be accessed and IS used by hackers to gain intelligence.
- Search engines, like Google, that help find the right information on the web, quickly, can also be used by hackers to discover vendor passwords and even identify poorly configured internet-facing devices and login pages to embedded web servers.
- Device search engines like SHODAN IO delivers great insight into how your own site is connected to the internet, and what is exposed, but this is also used by hackers to find specific targets.
- Electronic communications, such as email or SMS has extended alerting of critical equipment alarms, but also open the door for phishing campaigns, and expands opportunity for sideways moves from a vulnerable mail server to a vulnerable ICS HMI.



This particular SHODAN Search even shows us that an old Windows XP system is waiting on the other side of the firewall!

### **ISC Threat-scape Changed in 2010 - STUXNET**

The discovery of a virus called Stuxnet in 2010 sent shockwaves through the ICS community, as for the first time ever malware was discovered that could actually infect downstream attached Programmable Logic Controllers (PLCs) – something that up until the Stuxnet discovery, was thought impossible. Centering primarily in Iran within the Natanz Uranium enrichment facility, Stuxnet was later determined, and then confirmed, to be the work of military cyber personnel, delivering the first official cyber-warhead the world had known. It is noteworthy to mention that cyber security experts who discovered the Stuxnet virus estimate it's existence could have begun in 2005 – a full 5 years before it's code was identified.

This malware effectively took over the process controls (Siemens systems) responsible for uranium enrichment centrifuge motors, spinning them at high speed, then abruptly stopping the motors, repeatedly, until the million dollar units burned out. At the HMI, however, operators noticed nothing but normal operations, and no alarms were detected until the motors themselves were destroyed.

Up until this point in history, it was thought impossible for PC-based and crafted malware to impact, let alone infect PLCs, but this is exactly what happened, like something out of a science fiction movie, and this new reality has changed the ICS landscape forever. Although this attack targeted centrifuge motors with specially crafted code suited for the devices controlling the motors, this event revealed how easy it could be to usurp control of devices, such as nuclear reactors, coal-fired turbines, water treatment controls, etc., and create conditions where physical destruction of such equipment could cause devastating damage to property and even human life. Unlike a conventional warhead, which carries tremendous expense and a "use once" condition, cyber warheads are relatively cheap to develop and deliver, and can be used over and over again, but the risk of the enemy securing the code also brings the reality of reverse-engineering and the weapon being turned on the originator. The threat-scape has indeed been altered forever.

### **Malware targeting ICS Systems on the rise**

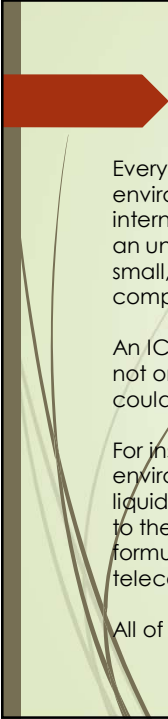
Since the discovery of STUXNET, and the related FLAME and DUQU malware, additional ICS-centric malware has been discovered, in addition to the reclassification of the Conficker virus to an ICS attack, based on the French Navy being hit by this malware, which prevented their planes from downloading specific flight plans.

Such ICS Attacks include, besides Conficker, STUXNET and its related malware:

- **Black Energy** – Ukraine – targeted electrical grid operations
- **Industroyer/ CrashOverride** – Ukraine – targeted electrical generation facilities
- **TRITON/ HATMAN** – Middle East and Ukraine – targeted Safety Instrumentation Systems (discovered 2017!)
- **ClearEnergy/ Scythe** – Ransomware specifically targeting ICS systems
- **HAVEX/ Dragonfly/ GRIZZLY STEPPE** – Europe and USA – appears to be reconnaissance malware against energy sector ICS
- **Irongate** – appears to be proof-of-concept malware



## Successful Attack Consequences



### Consequences of a successful ICS compromise

Every attack that succeeds brings with it the consequences of the successful attack. In a traditional IT environment, this could mean loss of data, or availability of applications, servers, network resources such as internet access, services such as electronic communications, or stolen data resulting in a competitor gaining an unfair advantage. In any of these scenarios, productivity takes a hit, sometimes small, sometimes not-so-small, but the impacts are typically limited to every day business functions and productivity, or market competitiveness.

An ICS attack on CIKR brings far different consequences, and a successful attack could be physically felt by not only the personnel onsite, but to the community at large directly, or through environmental damage that could linger, causing health issues, for decades.

For instance, a successful attack on a Chemical manufacturer could release highly toxic substances into the environment. An oil refinery could lose control of process tanks causing a serious explosion of flammable liquids. A successful attack on an electrical grid operator could result in widespread power outages, similar to the one experienced in 2003. A successful attack on a water treatment plant could result in the wrong formulation of treatment chemicals being used, resulting in water unsafe to drink. A compromise at a major telecommunications center could result in loss of telephone service, cell phone, service, internet service, etc.

All of the above carry downstream consequences as well, across multiple sectors, as we can well imagine.

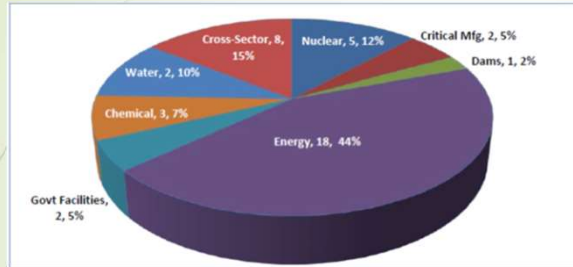
## Threat Intelligence and Awareness Assists in ICS Security

### Some facts about cyber security compromises

- Average detection time in 2018 for a company or organization to identify a data breach/ network compromise has dropped to an average of 71 days<sup>4</sup>, a vast improvement over 2016 and the staggering 200+ days, or nearly 8 months! This is being driven from increased awareness and emphasis on Cyber Security, coupled with regulatory action such as GDPR. Remember, Stuxnet was discovered in 2010, but researchers believe it had been doing its thing for up to 5 years prior to its discovery!<sup>1</sup>
- Over 60% of successful cyber intrusions and security breaches result from internal threats rather than outside forces!<sup>2</sup> Small business are targeted with 43% of attacks, as hackers view these entities as weaker, and also offer "practice" for larger targets<sup>4</sup>.
- Human error/ unsecure practices, such as use of weak or default passwords is a top reason for ease of cyber security breaches<sup>3</sup>
- Although one can never truly stop a hacker from breaching your defenses, early detection is critical to mitigating any damage or loss of data, and is the best protection you can have in defending your critical IT and OT assets. Note that cyber attacks occur every 39 seconds, and approximately 230,000 NEW malware samples are detected EVERY DAY<sup>4</sup>!

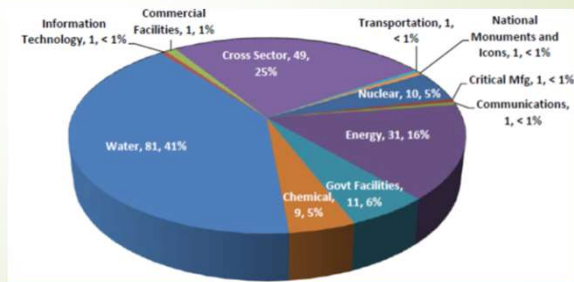
1 – InfoSecurity Magazine, February 24, 2015, "Hackers Spend 200+ Days Inside Systems Before Discovery"  
 2 – Harvard Business Report, September 19, 2016, "The Biggest Cybersecurity Threats Are Inside Your Company"  
 3 – CybersecurityTrend.com, June 6, 2016, "Human Error Is to Blame for Most Breaches"  
 4 – December 3, 2018/in Cybint News, Popular Posts

### Increased attacks of ICS systems detected since Stuxnet



In 2010, most activity reported centered on the Energy Sector

In 2011, reported number of attacks increased tremendously, with water treatment operations taking the top spot for number of reported incidents/ compromises



### Protecting ICS

As we have learned, despite many similarities between traditional IT domains and ICS domains, effective protection of ICS differs from traditional IT due to the necessity to limit impacts to availability, vs. assuring that data is kept confidential. Yet, threats to ICS and uninterrupted operations include malware and hacks targeting traditional IT which can spread across poorly configured networks, rendering operator systems and servers useless. The larger ICS-related attacks up the damage potentials and consequences of a successful breach.

A very important fact to know – **there exists no magic bullets**, nor are ICS defenses a “one-size fits all” endeavor.

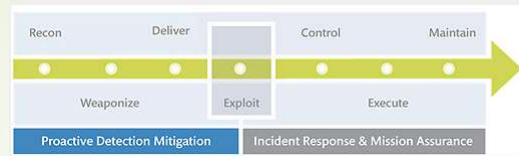
Defense-In-Depth means layers of defensive measures intended to minimize, if not eliminate the opportunity for an attack to be successful. Understanding the attack lifecycle assists strategy development and implementation of appropriate defensive measures. This also reveals the “Kill Chain” that exists with every attack.

After 9/11, Sec. of State Condoleezza Rice explained that to stop a terror attack from being successful, we have to be right all the time, whereas a terrorist only has to be right once. Understanding an attack lifecycle reveals the actual “Kill Chain” and how to properly strategize to defend against attack.

“Kill Chain” is a registered trademark term coined by Lockheed Martin



## Cyber Attack Lifecycle and the “Kill Chain”

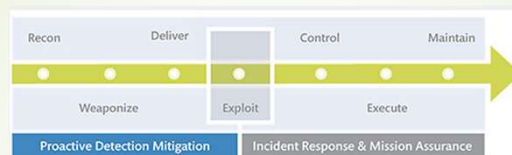


The graphic above illustrates a typical lifecycle of a cyber attack. Like in classic military combat, several elements must occur in advance of an attack being launched in order to assure the attacker achieves their goals. Knowing this very real process involved allows us to understand the proactive measures to take to discourage or prevent a successful breach from happening. Each of the 7 steps in this Life-cycle represents defensive opportunity, as if one of these 7 steps is disrupted or halted, the attack will fail.

**RECON** – Before any attack can happen, the attacker must know the vulnerabilities of a potential target or targets. This includes understanding network architecture, identifying vulnerabilities within assets of the system, whether access to the systems can be gained, and whether the presence of the breach can remain hidden and persist through system restarts or the like.

**WEAPONIZE** – Once reconnaissance has been completed, and systems have been successfully compromised, **DELIVERY** of the exploit kit can occur – but attackers will only move if the opportunity for success exists.

## Cyber Attack Lifecycle and the “Kill Chain”, continued...



At the point of exploit, prevention turns to mitigation. A determined and well-financed attacker cannot be stopped, but proper network configurations, secure communications conduits between non-related domains (corporate network to ICS network) and detection tools such as Network Intrusion Detection Systems (NIDS) can make accessing targeted systems difficult, and behavioral monitoring of the ICS network can help spot abnormal and dangerous network traffic as it begins. It is important to note that with this knowledge, we flip the tables on the bad actors. Rather than always needing to be right, defenders need only interrupt one of the 7 steps to stop an attack, whereas the hacker has to be right in all 7 phases to succeed!

Although ICS systems, due to age, unsecure protocols, and COTS introducing myriad of common vulnerabilities between traditional IT and ICS computers offering a potential wide range of exploitable vulnerabilities, an attacker nevertheless needs opportunity to succeed to launch the attack. Despite many challenging factors in ICS, driven by availability as the number one priority, ICS networks are fairly predictable in terms of network traffic, making NIDS/network behavior, a reality as part of a defense-in-depth approach.

### **Defense-in-Depth**

On order to develop a proper Defense-In-Depth strategy, we also need to conduct our own reconnaissance in several areas, as follows:

- 1 – Asset Management and Discovery – understanding what devices and systems are in the ICS domain, and what vulnerabilities may exist, and whether an opportunity exists to exploit vulnerabilities.
- 2 – Network Configurations – Is the network air-gapped? Properly segregated/ segmented to carve controls and/ or camera networks off the business domain?
- 3 – Firewall Configurations – Are trusted connections properly configured? Are ACL being leveraged to further limit authorized connections?
- 4 – Remote Access – Is remote access configured with a secure connection? Is the connection port-forward? VPN with limited access rules? Are connections encrypted?
- 5 – Device configuration – Are field controllers configured with strong passwords? Are default from factory passwords still in play?
- 6 – Human – Most vulnerabilities occur due to human error/ human permission. Like vampires of old, most attackers must be “invited in”. Are users security aware? Do we, as integrators, provide information to help make clients more security conscious? Is a security culture beginning to take shape?
- 7 – Is the existing network clean or already compromised?

### **ICS Security Summary**

Challenges in securing ICS with IT approaches being identified, a multi-layer, defense-in-depth approach is best:

- Human security awareness training
  - Network design and limited egress to the ICS networks
  - Accurate asset discovery, management and monitoring for state changes
  - Network Behavioral monitoring for fast detection of intrusions
  - Network segmentation with flow control for containment capabilities in the event of an attack
- Patching when possible  
Use the static nature of controls systems workstations and servers to your advantage
- Periodic vulnerability and penetration testing to identify the “weak links” and mitigate based on likelihood of exploit, not the fact the vulnerability exists alone





### Network architecture re-design

Recommended ICS and Enterprise IT network design is to follow the ISA-99, or Perdue Enterprise Reference Architecture (PERA), or simply the Perdue model, for strong segmentation with flow control.

Containment and true segmentation is the goal

If internal firewalls to create enforcement zones is not possible due to budget limitations, at minimum the implementation of VLANs is in order. However, we must not intermingle Controls and Enterprise IT VLANs in the same switch, as Application layer header data can override the layer 3 VLAN rules allowing transversal of malware across segmented switches.

Additional engagement and consultation to achieve the best architecture to assure segmentation and outbreak containment capabilities is a priority for U&S Services.



### Endpoint Protection – Shift to White Listing solutions

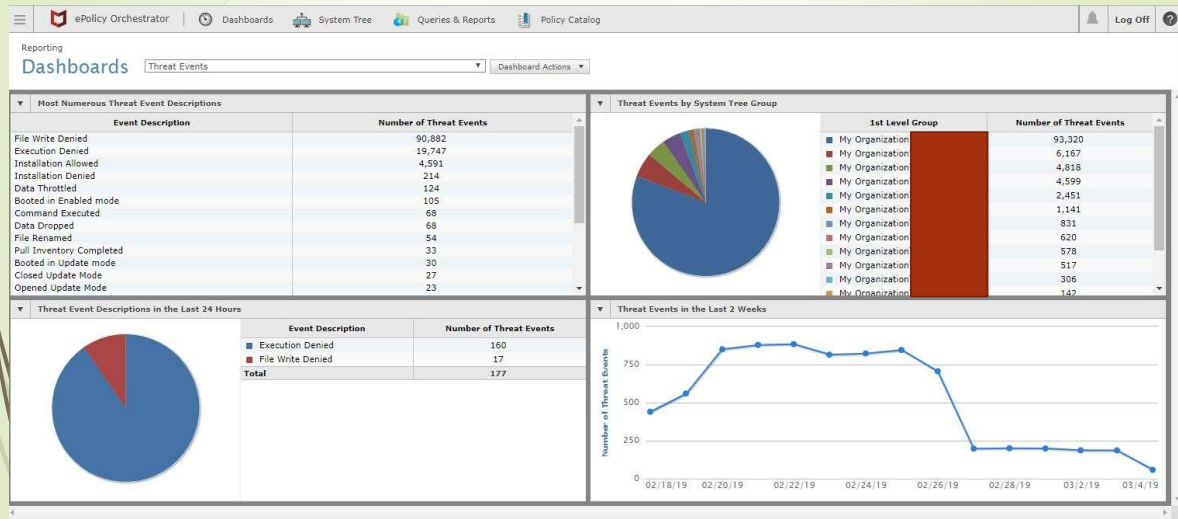
U&S Services now is offering end point protection for Windows systems, workstations and servers, to better defend your ICS IT assets.

We have a central threat management server to manage whitelisting and threats, which does mean firewall rule adjustments are needed, if this option is desired

Several clients have taken advantage of this solution, which is working well to keep malware from executing onto the systems.

With ICS systems being inherently vulnerable, a white list solution to lock the systems down in time is the best practice, and is recommended by US/ ICS-CERT for ICS environments.

## Endpoint Monitoring Threat Dashboard



## Top line threat report – per specific client – all threats

The report shows a list of threat events for 'My Organization'. The columns are:

- Event Generated Time:** A list of timestamps from 2/19/19 12:40:26 PM EST to 2/19/19 1:00:41 PM EST.
- Threat Target Host Name:** A column containing redacted host names.
- Threat Name:** A column containing the text 'EXECUTION\_DENIED' for all events.

At the bottom, there are controls for actions, showing 4599 items, and options to show source or target systems.

### Top line threat report – per specific client – filtered

Reporting Dashboards

Threat Events by System Tree Group -> My Organization

Custom: [Event20720] ☐ Show selected rows

| Event Generated Time    | Threat Target Host Name | Threat Name      |
|-------------------------|-------------------------|------------------|
| 2/18/19 12:40:26 PM EST |                         | EXECUTION_DENIED |
| 2/18/19 1:00:26 PM EST  |                         | EXECUTION_DENIED |
| 2/18/19 1:20:26 PM EST  |                         | EXECUTION_DENIED |
| 2/18/19 1:40:26 PM EST  |                         | EXECUTION_DENIED |
| 2/18/19 2:00:27 PM EST  |                         | EXECUTION_DENIED |
| 2/18/19 2:20:28 PM EST  |                         | EXECUTION_DENIED |
| 2/18/19 2:40:27 PM EST  |                         | EXECUTION_DENIED |
| 2/18/19 3:00:27 PM EST  |                         | EXECUTION_DENIED |
| 2/18/19 3:20:28 PM EST  |                         | EXECUTION_DENIED |
| 2/18/19 3:40:28 PM EST  |                         | EXECUTION_DENIED |
| 2/18/19 4:00:29 PM EST  |                         | EXECUTION_DENIED |
| 2/18/19 4:20:29 PM EST  |                         | EXECUTION_DENIED |
| 2/18/19 4:40:29 PM EST  |                         | EXECUTION_DENIED |
| 2/18/19 5:00:30 PM EST  |                         | EXECUTION_DENIED |
| 2/18/19 5:20:30 PM EST  |                         | EXECUTION_DENIED |
| 2/18/19 5:40:30 PM EST  |                         | EXECUTION_DENIED |
| 2/18/19 6:00:31 PM EST  |                         | EXECUTION_DENIED |
| 2/18/19 6:20:32 PM EST  |                         | EXECUTION_DENIED |
| 2/18/19 6:40:31 PM EST  |                         | EXECUTION_DENIED |
| 2/18/19 7:00:32 PM EST  |                         | EXECUTION_DENIED |
| 2/18/19 7:20:32 PM EST  |                         | EXECUTION_DENIED |
| 2/18/19 7:40:32 PM EST  |                         | EXECUTION_DENIED |
| 2/18/19 8:00:33 PM EST  |                         | EXECUTION_DENIED |
| 2/18/19 8:20:33 PM EST  |                         | EXECUTION_DENIED |
| 2/18/19 8:40:33 PM EST  |                         | EXECUTION_DENIED |
| 2/18/19 9:00:34 PM EST  |                         | EXECUTION_DENIED |
| 2/18/19 9:20:34 PM EST  |                         | EXECUTION_DENIED |

Actions 907 items

### Threat log event detail report – per specific client – filtered threats

Reporting Dashboards

Threat Event Log Details

|                                 |   |
|---------------------------------|---|
| Detecting Product Version:      | 8.1.0.179   |
| Detecting Product Host Name:    |   |
| Detecting Product IPv4 Address: | 10.1.230.1  |
| Detecting Product IP address:   | 10.1.230.1  |
| Detecting Product MAC Address:  | 54B64603640   |
| DAT Version:                    |   |
| Engine Version:                 |   |
| Threat Source Host Name:        |   |
| Threat Source IPv4 Address:     | 10.1.230.1  |
| Threat Source IP address:       | 10.1.230.1  |
| Threat Source MAC Address:      |   |
| Threat Source User Name:        |   |
| Threat Source Process Name:     |   |
| Threat Source URL:              |   |
| Threat Target Host Name:        |   |
| Threat Target IPv4 Address:     | 10.1.230.1  |
| Threat Target IP address:       | 10.1.230.1  |
| Threat Target MAC Address:      | 54B64603640   |
| Threat Target User Name:        | NT AUTHORITY\SYSTEM                                       |
| Threat Target Port Number:      |   |
| Threat Target Network Protocol: |   |
| Threat Target Process Name:     | C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe |
| Threat Target File Path:        | C:\Windows\TEMP\_psScriptPolicyTest_juu3vrip.hdd.pas      |
| Event Category:                 | Application Blocked                                       |
| Event ID:                       | 20720   |
| Threat Severity:                | Error   |
| Threat Name:                    | EXECUTION_DENIED  |
| Threat Type:                    | None  |
| Action Taken:                   | deny execute  |
| Threat Handled:                 | True  |
| Analyzer Detection Method:      |   |

Actions


## The previous slides are an actual Cyber Event currently under investigation

Steps taken thus far;

- 1 – Collection of log information and research concerning random powershell scripts
- 2 – Some information indicates a potential for system misconfiguration with App Locker – but this product is not used at this site, and the file path also differs from legitimate powershell activity
- 3 – Log sample sent to security vendor for additional opinion – the opinion was a powershell malware attack
- 4 – Additional findings show a discernable pattern to the behavior – every 20 minutes powershell is running a new, random powershell script.
- 5 – Other Windows 10 systems under threat management are not exhibiting this behavior
- 6 – Exam of system for the existence of these scripts show these scripts do not reside in the Windows\Temp directory, not even as hidden files
- 7 – View through our remote management utilities confirms the files do not exist on the system
- 8 – The threat is being properly and successfully handled – meaning no breach has occurred
- 9 – Collection of running config, memory dump and file analysis for evidence and deeper forensic analysis

## A bit about file-less memory attacks

- Recent article released by IBM indicate that today 57% of new attacks are leveraging powershell scripts, rather than traditional malware
- Powershell, since Windows 7, has become the powerful information collection tool of choice for network and system admins
- Since this tool is foundational to Windows 7, with insight into .NET and WMI, powershell activity is "expected" and not something (traffic) that is currently under watch
- No signatures for traditional anti-malware products to detect and stop
- Attack is very well obfuscated, difficult to detect where the attack is coming from
- Once a system is restarted, remnants of the attack are gone as this is a memory attack
- Use of malicious powershell scripts now being seen in the following attacks:
  - ❖ Information stealing – domain accounts/ email addresses, job titles, et al, via DNS query leveraging powershell – excellent for user recon to pick some likely targets
  - ❖ Network Mapping – collection of asset information and network information on the wire, again, recon
  - ❖ Crypto Coin Mining – cryptominers are starting to leverage powershell to bring down malicious applications, while shutting down "competing" cryptominers to focus CPU usage towards the new attacker.
  - ❖ Symantec reporting in 2018 showed an increase in malicious powershell script usage from 2017 to 2018 of @ 661%. Two known attacks are GhostMiner and Bluwimps, which are crypto-coin miners injected into memory to avoid detection and evade scanners.



Below are links to some videos that illustrate the consequences of a successful ICS attack, and some insight into how hackers breach an organization:

2007 – DHS-sponsored simulated cyber attack on a generator:

<https://www.youtube.com/watch?v=fJyWngDco3g>

An inside look at a white hack hacking team and the TTPs used to breach an organization

<https://www.youtube.com/watch?v=pL9q2lOZ1Fw>