DEFINING 21ST-CENTURY CYBERSECURITY FOR ICS

Mario Chiock, CISSP, CISM, CISA, executive adviser
Cybersecurity & Disruptive Technology

Del Rodillas, GICSP, MSEE, MBA, director
Industrial Cybersecurity Product Marketing

Executive Summary

SCADA and Industrial Control Systems found in critical infrastructure and manufacturing industries have enjoyed unprecedented levels of agility, speed and cost savings with the pervasive adoption of information technology and increased connectivity to supporting networks. An industrial internet of things, or IIoT, is starting to emerge, enabling new capabilities, such as predictive maintenance and even new business models. However, with this modernization have also come undesired IT vulnerabilities and other threat vectors, which are increasingly being exploited by malicious actors, such as nation-states, cybercriminals and malicious insiders. Recent years have shown a concerning rise in the number and sophistication of attacks specifically targeting critical infrastructure and manufacturing asset owners. Real-world cases have shown disruption of critical processes and even destruction of ICS equipment. The need for improved security in ICS has never been higher and has become a board-level issue for many organizations.

While IT administrators have been quick to deploy the latest and greatest technologies and practices to secure corporate environments, operational technology – OT – administrators have not been as aggressive. The extreme sensitivity of ensuring availability and performance of the industrial process has led to a more conservative and rigorous approach to how security is deployed and maintained. For example, to minimize disruptions to the process – sometimes, because of the very nature of a process – it is not uncommon to have systems with maintenance cycles in excess of 12 months, with some even running multi-year cycles. Within this window, software cannot be patched, and AV signatures cannot be updated. Other times, administrators avoid in-line protection, such as network IPS or AV, because of the concern over accidental blocking or performance degradation. These products are put in detection-only mode or thrown out altogether. Even practices commonplace in IT environments, such as vulnerability scanning, can cause malfunctions or denial-of-service scenarios in industrial controllers that were not designed to deal with such events. These constraints make securing ICS/SCADA environments both unique and difficult.

The result is that many organizations are still working with a mixed bag of antiquated security technologies that operate in silos, are difficult to manage, provide limited situational awareness and do not provide the kind of preventive security required. Such organizations become prime targets for attackers who are likely using similar environments as quality assurance test beds for their sophisticated attacks. The bigger gap is the inability to address the constantly evolving threats that make use of never-before-seen attacks. Actions must be taken to build up the right capabilities to better protect ICS.

A new kind of platform – one built for 21st-century ICS – is required to properly secure control systems from the new threat landscape. This platform must consolidate different core technologies in a way that ensures prevention even against advanced attacks. The integration must also allow interfaces to alert and perform security actions in an automated way with its own services as well as other supporting technologies. It must also facilitate information sharing within the organization and with peer organizations. In the same way the bad guys collaborate to develop targeted attacks, so too must the good guys.

In this paper, we will look at the nine core capabilities that define such a security platform for industrial control systems. This platform:

1. Integrates network and endpoint security with a threat intelligence core.
2. Classifies traffic based on applications and users, not ports and IP.
3. Supports granular network segmentation, including role-based access.
4. Natively blocks known threats.
5. Detects and prevents attacks by unknown malware.
6. Stops zero-day attacks on endpoints.
7. Provides central management and reporting.
8. Secures the use of mobility and virtualization technologies.
9. Has a powerful API and industry-standard management interfaces.

With these capabilities in place, organizations are better able to deter advanced threats as well as adapt and scale as the threats evolve.

Introduction

The Evolution of Industrial Control Systems

The automation systems used to monitor and control industrial processes in factory floors and critical infrastructure, such as electrical substations and oil rigs, have many names: Industrial Control Systems, or ICS; Supervisory Control and Data Acquisition, or SCADA; and Distributed Control Systems, or DCS, to name a few. These systems, holistically referred to in this paper as "ICS," have evolved dramatically over recent decades. What once were isolated, proprietary systems interconnected by serial communications technologies are now highly interconnected and geographically distributed systems that utilize commercial off-the-shelf, or COTS, products and the Internet Protocol. This merging of information technology and operational technology – IT and OT – has allowed many critical infrastructure and manufacturing asset owners to enjoy tremendous productivity and cost savings. Further efficiencies are anticipated with the deployment of mobility, virtualization and even cloud-based components.

Economically, IT-OT integration has been very advantageous for many asset owners. However, along with these benefits has come a wider exposure to a variety of cyberthreats that could compromise availability, integrity and confidentiality. More than ever, organizations are being called out to revisit their control systems security posture to assess just how capable it is of preventing cyber incidents.

Some of these threats are unique to ICS components and others relevant to both IT and OT products. In addition, these threats could originate from within the ICS or originate from extraneous locations. Finally, cyberthreats to ICS could be malicious or accidental in nature. Figure 1 shows the most concerning ICS threat vectors as identified by the respondents in the SANS Institute's 2016 State of ICS Security Survey.[1]

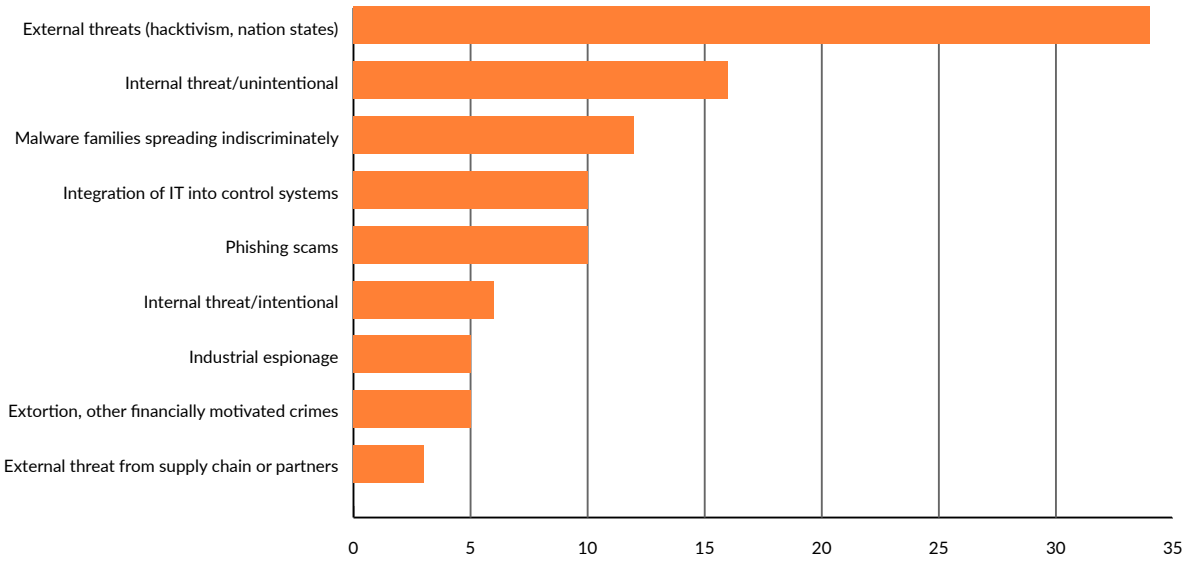

Figure 1: Top threat vectors of concern in ICS

In terms of the first category of external threats, Stuxnet was the first publicly disclosed cyberattack targeting ICS specifically. It exploited applications, files and vulnerabilities in COTS and ICS software to achieve its goal of disrupting Iran's uranium enrichment program. In this case, ICS equipment – the centrifuges themselves – were reported to have been damaged, highlighting the reality of cyber-physical consequences. Since then, we have seen an increased sophistication of the techniques used by targeted attacks to ICS. Reports for 2014's Energetic Bear campaign revealed its use of malware hidden in the ICS software packages downloaded from vendor websites.[2] It also utilized ICS protocols to learn about the affected organization's environment. And more recently, the Ukraine grid attacks of 2015 and 2016,[10] which were also successful cyber-physical campaigns, exposed how attackers have developed malware payloads that utilize ICS protocols themselves. This is an indicator of just how sophisticated attacks on ICS have become.

The next category is spear phishing attacks, or to be more general, social engineering techniques, which can include watering hole attacks or something as simple as leaving a malware-infected USB thumb drive in a target organization's parking lot as bait. Virtually all targeted attacks involve the compromise of the endpoint at some point via social engineering. For example, Stuxnet purportedly utilized USB drives to infect laptops used by support personnel, and Energetic Bear applied a combination of spear phishing, watering hole and Trojanized malware attacks. The concentrated spear phishing campaign to Norwegian oil and gas companies around August 2014,[3] where there were 50 confirmed attacks on organizations, including Statoil®, highlights how this has become a staple method for hackers trying to breach networks of critical infrastructure operators. The Ukraine grid attacks also utilized spear phishing, using Microsoft® Office documents with macros, to gain an initial foothold on the utility organization's IT network.

Another major concern is the introduction of malware into the ICS. This is often done by accident through infected mobile computing devices or removable media used by personnel with access to the ICS. Worms may also sneak into the ICS via "trusted" vendor and partner networks. Whether malicious or unintentional in nature, malware can lead to costly downtime and potential safety issues. These often do not make the news, but they can result in multimillion-dollar losses due to lost production, remediation costs and perhaps legal fees when incidents involve injury, death or environmental damage.

Insider exploits are also high on the list. A good publicly disclosed example is the Maroochy Shire incident.[4] In this case, a disgruntled employee of an ICS vendor supporting the Shire's sewage treatment works took vengeance after an employment-related disagreement. Using his deep knowledge of the Shire's sewage treatment control systems, including an unsecured wireless network, he released 800,000 liters of sewage into the local parks, rivers and hotel grounds, causing significant environmental damage.

While not a cyberthreat per se, the risk of failing a regulatory audit has increased the pressure on security organizations. Several countries have adopted regulations around controls systems security that could lead to severe fines for noncompliant organizations. In the U.S. and Canada, the NERC CIP standard has been adopted in the Electric Utilities industry. For chemical facilities in the U.S., the CFATS standard serves a similar purpose of enforcing cybersecurity compliance. The National Institute of Standards and Technology's Cybersecurity Framework, or NIST CSF, is a more recent standard with which government agencies must be compliant, and which also serves as a best practices reference for other ICS asset owners.

Is Your Organization Equipped to Deal With These Threats?

Discussing the different types of cyberthreats raises some very important questions organizations need to ask themselves in terms of their ability to defend their ICS.

- Do you have the right level of traffic visibility to validate proper use of the ICS and, more importantly, quickly detect improper use? How easy is it to extract this information?
- Can you enforce sufficient access controls that align to business policies and effectively limit extraneous and internal attack vectors while meeting stringent performance requirements? How easy is it to deploy and maintain the controls?
- Are your unpatched or possibly unpatchable legacy systems protected from exploits and malware? Could you further reduce downtime due to cyber incidents or patch maintenance?
- If faced with a targeted cyberattack that utilized methods and malware never before seen in the wild, would you be able to prevent the attack?
- Do your network and endpoint security solutions work together to support the goal of prevention, or are they disjointed? Can you manage them centrally across a large, geographically distributed operation?
- Do your security solutions facilitate or increase the burden of meeting regulatory standards?
- If you are using advanced technologies, such as virtualization or mobile devices, is your security implementation consistent or might these serve as vulnerabilities?

The ICS Security Gap

Most critical infrastructure and manufacturing organizations have some level of cybersecurity today. However, a good portion of organizations – especially in less heavily regulated industries – still use legacy technologies that are inadequate at addressing modern ICS cybersecurity challenges. Figure 2 shows a typical legacy security configuration found in many ICS environments today:

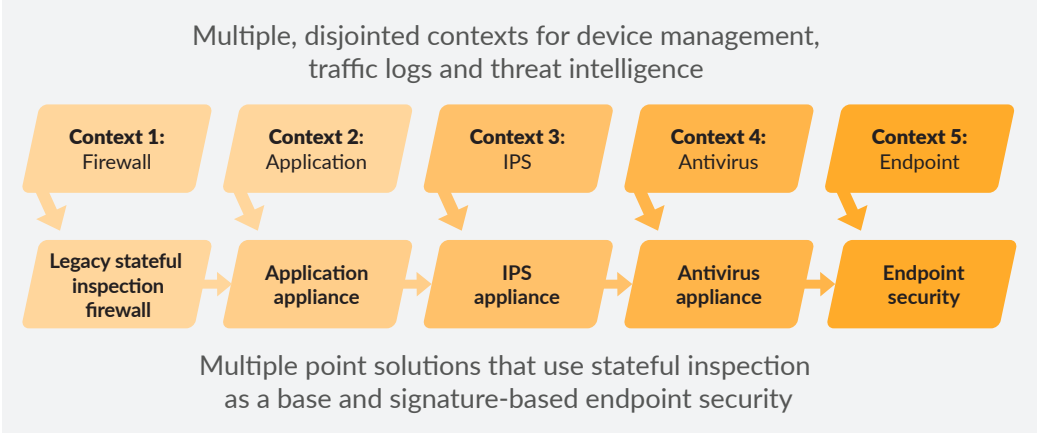

Figure 2: Typical legacy security

From a network security standpoint, legacy solutions are often based on stateful inspection firewalls, which do not provide the Layer 7 visibility and user-based access controls required to effectively detect anomalies and minimize exposure. Organizations try to fill the gap by deploying multiple disjointed solutions, such as application, IPS and AV appliances, but this typically results in increased risk of misconfiguration, silos of uncorrelated information, performance degradation and increased costs in terms of capital and operational expenditures. To add to the difficulties, existing endpoint security products operate separately from the network security, but of greater concern is how they can only address threats that have known signatures, strings and behaviors. They are unable to prevent attacks that use never-before-seen exploits and malware. Given the high risks involved in protecting ICS environments, security solutions must be able to prevent attacks – even zero-day attacks. Furthermore, the proliferation of point solutions has increased the load on organizations and made the job of securing ICS very complex.

21st-Century Security for ICS

Organizations can no longer rely on disjointed and ineffective legacy point solutions to defend critical infrastructure. The stakes are just too high. They need a 21st-century cybersecurity platform with a complete, tightly integrated set of capabilities to prevent threats while reducing the burden on organizations in deploying and maintaining security. When selecting the ideal security platform, you must look for one that:

1. Integrates network and endpoint security with a threat intelligence core.
2. Classifies traffic based on applications and users, not ports and IP.
3. Supports granular network segmentation, including role-based access.
4. Natively blocks known threats.
5. Detects and prevents attacks by unknown malware.
6. Stops zero-day attacks on endpoints.
7. Provides central management and reporting.
8. Secures the use of mobility and virtualization technologies.
9. Has a powerful API and industry-standard management interfaces.

1. Integrates network and endpoint security with a threat intelligence core

Your network can be compromised directly at hosts on the network, such as human-machine interfaces – HMIs – or automation servers, or from other hosts, such as third-party vendors' laptops or adjacent networks. It is very clear today that attackers will exploit weaknesses on both the network and hosts in a highly orchestrated fashion to achieve their agendas. Organizations must be aware of this and have provisions that can stop threats across the attack lifecycle. Besides just having this preventive toolbox as individual parts, the new requirement is that the preventive mechanisms must work collaboratively and share threat intelligence amongst each other.

Organizations can derive at least two powerful benefits from adopting such a platform. The knowledge gained about threats collected at endpoints can now be correlated with knowledge gained about threats traversing the network. Organizations can better understand and cyberattacks, especially targeted attacks, when they are able to view these repositories of threat intelligence with shared context. Secondly, protections for threats discovered on endpoints can be quickly sent to the network to prevent threats from propagating, and protections for threats discovered at the network can also be distributed to stop attacks at endpoints. The two work hand in hand to prevent threats while the threat intelligence core provides centralized, automated intelligence. The challenge with most existing solutions is that endpoint and network security operate in separate silos. However, newer technologies have begun to tightly integrate these capabilities along with shared, automated threat intelligence and dissemination of protections.[5]

Figure 3 shows the concept of integration of endpoint, network and a threat intelligence core to protect the process. The red arrows represent areas where advanced threats could initiate their attacks and the blue arrows capture the interaction of the network and endpoint security with the threat intelligence core or cloud. This is the basis of the 21st-century security platform.

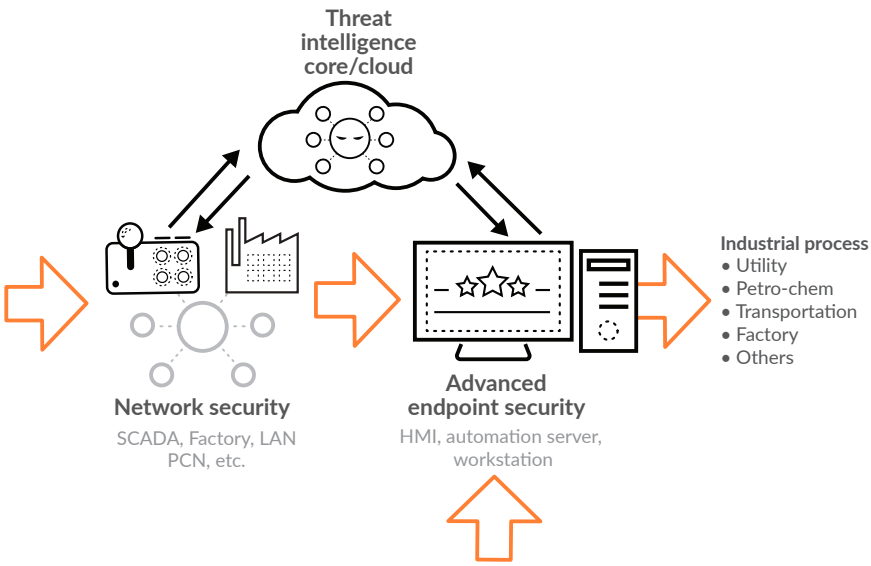

Figure 3: Endpoint and network protection with a threat intelligence core as the basis for a 21st-century security platform

2. Classifies traffic based on applications and users, not ports and IP

Drilling down into requirements for network security, two frequently discussed areas are Layer 7 and Layer 8 visibility – application and user, respectively. Although these may have been nice-to-haves in the past, both are now essential to enable the level of visibility required to detect anomalous use. Rather than being add-ons, these capabilities need to be intrinsic to the technology at a high level of performance. Here are several reasons why these are essential capabilities:

1. **Advanced threats cleverly use open ports.** Targeted attacks are likely to exploit ports open in the ICS environment, for example, as channels for command and control. By classifying traffic at the application layer, the platform enables your security team to better distinguish between expected traffic and potential malicious traffic exploiting open ports.
2. **Applications hop ports.** Aside from malicious traffic, other risky or bandwidth-hogging applications are introduced by personnel to improve productivity or provide leisure. These applications often port hop to avoid detection. By identifying applications, your security team is better able to detect such undesired applications that could hinder process availability.
3. **Some protocol functions are more "interesting" than others.** ICS protocols, such as Modbus and DNP3, have read and write functional variants. As write commands have the ability to alter the state of a programmable logic controller, or PLC, and potentially take down the process, one will want to have visibility to functional variants to increase intelligence on the nature of control systems traffic.
4. **Adding user and user group visibility broadens intelligence.** In all three scenarios, adding the context of user or user group to the application and protocol traffic allows one to detect anomalies based on role.

When selecting your platform, ensure it supports native application visibility and integration of user-IP mapping repositories, as the latter can be contextually linked to application/protocol traffic.

3. Supports granular network segmentation, including role-based access

There is a common misconception that perimeter-based security is enough to protect control systems from cyberthreats. As shown in our discussion of threats, separating SCADA from the business network, for example, is not enough to stop cyberthreats. Targeted attacks will find a way into the ICS: malicious insiders leverage their inside knowledge, well-meaning engineers unintentionally introduce risks, and malware jumps from "trusted" partner/vendor networks. More granular security zones interconnected by more intelligent segmentation gateways are required to ensure users get just enough access to do their jobs. This is the so-called least-privilege approach described in ISA 62443[6] or the Zero Trust model developed by Forrester® Research.[7]

A next-generation security platform for ICS should provide highly granular visibility into traffic at the application and user levels as well as be able to apply these parameters in policy. By segmenting the network by applications and users, the concept of role-based access control can be applied between security zones. The platform must make it very easy and intuitive to apply application/protocol control by user and not require multiple policies to realize the desired access control. This reduces administrative burden and the likelihood of mistakes. Figure 4 shows this important first step of reducing one's attack footprint by controlling the use of protocols, applications and other potential vectors.

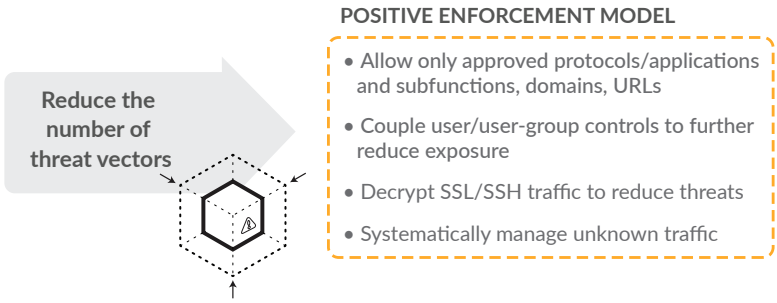

Figure 4: Applying segmentation to reduce the number of threat vectors

Some powerful use cases can now be considered with this capability to whitelist protocols and applications as well as how individual users or user groups use them:

- Allow third-party vendors access to Modbus reads from a DMZ into a PLC zone. If they need to make any write changes, a ticket would need to be opened to allow Modbus programming commands.
- Allow only certain business users access to a historian server in the process control network, which may be using OSIsoft® PI or other ERP/database applications.
- Limit the use of administrative applications, such as SSH, RPC and RDP, to only approved SCADA admins who understand the risks involved with maintaining critical infrastructure assets.

It is interesting to note that some technologies, like data diodes, were created to address the access control and security limitations of stateful inspection firewalls. Data diodes limit traffic to one direction at the IT-OT perimeter, for example, to allow data flow only from the ICS environment to the business network. However many applications still require bidirectional communications leading organizations to have a pair of data diodes. With the advanced segmentation and access controls described above, one can use the same device that provides fine-grained micro-segmentation within the control systems to manage the perimeter.

4. Natively blocks known threats

Also part of the network security discussion is the capability to stop known threats. There is a universe of known threats to ICS, including:

- Exploits to ICS-specific products, such as the controllers (PLCs, RTUs, IEDs) or SCADA software packages.
- Exploits to IT products used in ICS, such as operating systems, browsers and specific modules, including OpenSSL and the Unix BASH shell.
- Protocol functions risky enough to warrant treatment as exploits despite being normal features, such as DNP3 warm restarts.
- Run-of-the-mill viruses that, even if introduced by accident, could still take down hosts and cause downtime.
- Known bad domains/URLs used by malware for command and control as well as watering hole attacks.

Despite knowledge of these risks, many organizations leave devices in ICS unpatched and unprotected against these threats for extended periods. This could be because the product vendor has not yet made a patch available or because the operator needs to wait for a maintenance window before taking the device offline for patching. It is not uncommon for the systems to never be patched due to product end-of-life. It is therefore critical to have compensating protections for these devices while they are left vulnerable.

Preventing known threats is part and parcel of a next-generation security platform. Unlike legacy systems that analyze threat information separately from application or user information, the platform must analyze threat information at the same time as application and user information to improve performance and ensure shared context between repositories. Shared context allows increased intelligence in terms of recognizing the nature of a threat with respect to the originating application and users as well as affected assets. Furthermore, it allows much easier creation of policies. The platform must analyze threat information at the same time as application and user information to improve performance and ensure shared context between repositories, based on a more effective approach of allowing legitimate applications/protocols between security zone according to role while blocking known threats that may be using the channel to propagate. Figure 5 shows the concept of blocking known threats that may have come in via whitelisted traffic.

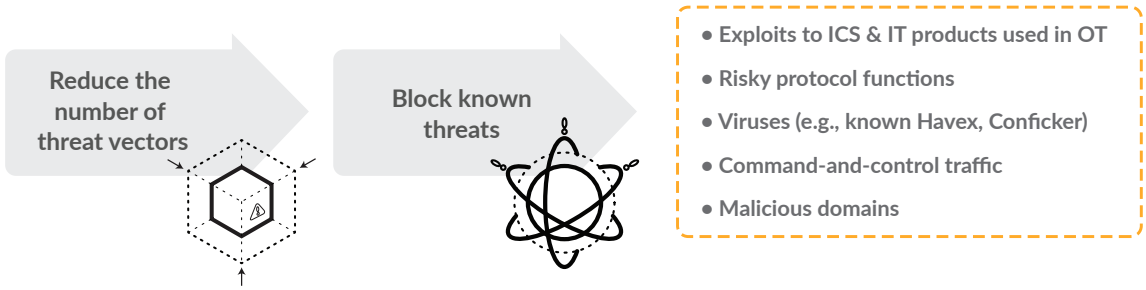

Figure 5: Block known threats natively after reducing potential attack vectors

5. Detects and prevents attacks by unknown malware

The question then arises of how to deal with unknown malware that passes through the network. This is where shared threat intelligence comes in. A next-generation security platform must be able to isolate suspicious network-borne payloads and send them to a threat intelligence "core" for rapid, automated analysis and dissemination of protections such as antivirus, exploit, and command-and-control signatures. While solutions exist for this functionality as a stand-alone sandboxing appliance, this capability must be native to the platform so that the protections can be quickly and automatically provided to the enforcing device, the firewall. Detection is helpful, but there must be a closed loop to ensure prevention in a timely manner. Furthermore, because of the shared context, more intelligence could be collected in terms of the relationship of the zero-day malware with the application and user information. When selecting your platform, be cautious of stand-alone sandboxing solutions that only alert you to a problem, yet do nothing in terms of offering protection. Figure 6 shows the process of converting unknown threats to known threats that can be stopped. Asset owners sensitive to sharing files outside of their organizations should look for a platform that supports local sandboxing and signature generation.

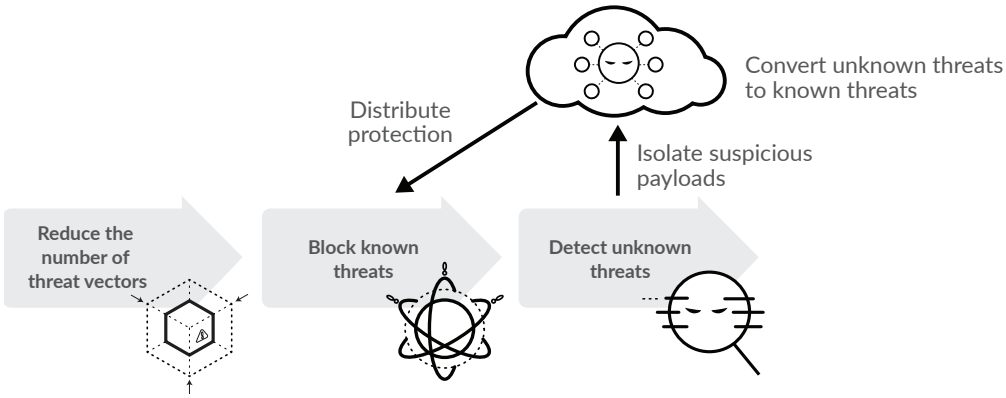

Figure 6: Native sandboxing capabilities detect unknown threats and make them known

6. Stops zero-day attacks on endpoints

Let's shift our attention to the protection of hosts, such as HMIs, automation servers, workstations and even those belonging to managers/admins with privileged access. These systems run software that may have remotely exploitable vulnerabilities. Furthermore, users can be tricked into running malware directly. Traditional endpoint security has been focused on looking at known malicious signatures, strings and behaviors to stop such endpoint-based attacks, but this approach has proven ineffective and operationally burdensome. It only stops known threats, and the moment you block a known threat with a signature, several new exploits or malware variants crop up that do not match the signature used. ICS endpoints are highly exposed to zero-day attacks, but they may not even be protected against known attacks, owing to their long patch/update cycles, which can span months or years.

For many years, an approach based on known signatures was the only available option, but technologies have emerged to prevent even unknown attacks by stopping the underlying attack techniques used by exploits and malware, which change very infrequently.[8] Most exploits and malware use more than one technique in their attack sequence, but stopping the attack at any point in this sequence will prevent the attack from completing. By focusing on stopping techniques rather than focusing on known signatures, the endpoint security can be much more effective at preventing attacks. Such technology could also be used to validate installation packages from software vendors to check for Trojans. It can also be used to prevent and receive notifications for unauthorized installation of applications, giving organizations a way to take a more regimented, audit-friendly approach to application deployment at endpoints.

In addition to utilizing this disruptive, technique-based approach to stopping zero-day exploits and malware, the endpoint protection and network security components must interact with the threat intelligence cloud to make use of and contribute to centralized and automated threat intelligence. Figure 7 shows the concept of advanced endpoint protection and its interaction with the threat intelligence cloud.

7. Provides central management and reporting

Given how highly distributed ICS tends to be – whether across multiple plants on a campus or across multiple remote facilities, such as substations or production facilities – a next-generation security platform must provide a means for centrally managing the platform. Rather than having a separate central management device for application policy, threat prevention, URL filtering and other functions, these should all be administered via a single management device. Furthermore, the platform must be able to efficiently aggregate the local information from each of the remote devices to create a consolidated view of the operations, which may be global. This capability helps dramatically in terms of being able to perform forensics and is indispensable when creating supporting documents required in regulatory audits.

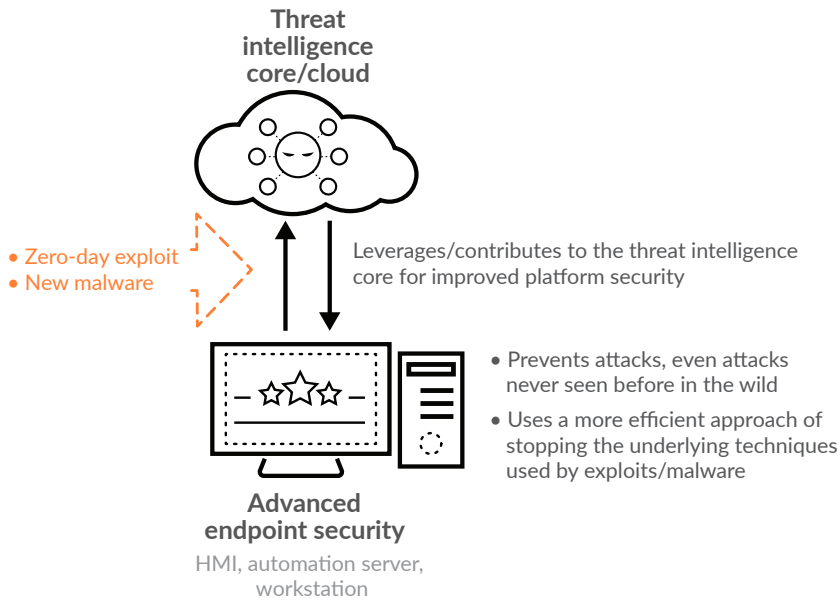

Figure 7: Advanced endpoint security stops attacks on the host and shares intel

8. Secures the use of mobility and virtualization technologies

Although mobile devices and virtualized operational data centers are not yet in common use and are often intentionally avoided, in ICS environments, some front-running organizations are already leveraging these technologies to further improve operational efficiencies and reduce costs. For example, some organizations have started to deploy mobile HMIs on tablet devices used in the field and on the factory floor. A next-generation platform must be able to ensure security policies are consistently enforced on such mobile devices to ensure safe use, even outside the walls of the control center or plant.

Some organizations have started to consolidate physical servers running historian, SCADA and other application servers onto several virtual machines residing on the same hypervisor. Most ICS asset owners are hesitant to adopt such technologies, preferring fixed assets and non-virtualized servers. This is justifiable – there are new security considerations with virtualized environments, such as securing east-west traffic between machines and ensuring consistent security when moving virtual machines around. Whatever their stance on virtualization technology, organizations must consider that strong economic drivers often compel migration to advanced technologies – especially once the technologies are proven. To set themselves up for the future, it would therefore be wise for organizations to select a security platform that also supports securing virtualized environments.

9. Has a powerful API and industry-standard management interfaces

A platform with all these core features will cover many of the bases, but there must be a provision to accommodate additional products that can address unforeseen needs or provide added value. To achieve this, the platform must support industry-standard management interfaces and an open API. Together, these capabilities allow integration with third-party solutions to, for example, improve policy/configuration management, log analysis, reporting and other important security functions. Security Information and Event Management, or SIEM, devices, in particular, are powerful platforms for aggregating data from many sources, including networks, servers, databases and, of course, security products.

Alignment With Industry Standards

Several cybersecurity standards specifically focused on critical infrastructure and ICS have been developed in recent years. Some, like NERC CIP and CFATS, are regulated while others, such as ISA 62443 and NIST Special Publication 800-82, serve as guidelines. The NIST Cybersecurity Framework is a more recent standard that calls for mandatory compliance for U.S. government agencies and serves as a best practice reference for other critical infrastructure asset owners.[9] With a next-generation security platform in place, organizations should be able to better address the requirements set forth by these standards and respond more efficiently during cyber incidents and compliance audits. Although an exhaustive mapping of capabilities to the NIST CSF is beyond the scope of this paper, it useful to discuss at a high level how some of the capabilities described above map back to the NIST CSF's functional areas, as follows:

NIST CSF Functional Area	Supporting Capabilities of a Next-Generation Security Platform
IDENTIFY	▪ Identify network traffic and usage at granular levels ▪ Applications, ICS protocols, protocol functions ▪ Users and user groups, IP address, countries ▪ Files, data strings, URLs, domains
PROTECT	▪ Reduce the number of attack vectors, including applications, protocols, domains/URLs, user and other segmentation ▪ Protect unpatched systems from zero-day exploits and never-before-seen malware ▪ Prevent malicious use of ICS protocols ▪ Secure mobile and virtualized environments ▪ Prevent data exfiltration
DETECT	▪ Detect unauthorized use, whether malicious or benign ▪ Decrypt encrypted traffic to identify stealthy malicious traffic ▪ Detect known and unknown threats (IPS, AV, malicious domains/URL, command and control, "Son of Stuxnet" attacks) ▪ Detection can be performed at the network or at endpoints
RESPOND	▪ Shared context between application, user and threat/content information increases intelligence, which simplifies forensics process ▪ Threat intelligence cloud provides automated threat analysis and protections for both endpoints and the network ▪ Integration with other security devices, such as real-time SIEMs, enriches the analytics
RECOVER	▪ Protections from threat intelligence cloud are automatically disseminated to endpoints to prevent attacks ▪ Knowledge of any impacted devices are provided back to centralized management and can be remediated ▪ Easy deployment of any additional policies/segmentation to improve security posture

Summary

The ICS threat landscape has escalated such that legacy technologies are no longer effective at stopping modern cyberthreats. A next-generation security platform is required to effectively combat cyberthreats and achieve the all-important goal of keeping the process available. The platform must combine the benefits of network security and endpoint security while leveraging a threat intelligence cloud to ensure attacks are prevented wherever they originate. Furthermore, it must provide granular visibility and control at the application and user levels to allow for network segmentation that better aligns with business needs. The platform must do more than just detect threats and attacks; it must prevent them, even if they have never been seen before. The risks involved in securing critical infrastructure and manufacturing assets are too great to rely on anything but prevention of cyberattacks. Finally, the platform must be easy to deploy and maintain, and should be able to interoperate with other security products. With such a platform in place, organizations will have what is required to secure modern ICS while maintaining high uptime and operational efficiency.

1. Report "2014 Survey on Industrial Control Systems Security," SANS Institute
2. Article "Havex Hunts for ICS/SCADA Systems," F-Secure, http://www.f-secure.com/weblog/archives/00002718.html
3. Article "Oil Industry Under Attack by Hackers," NewsInEnglish.no, http://www.newsinenglish.no/2014/08/27/oil-industry-under-attack-by-hackers/
4. Report "Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia," Joe Weiss and Marshall Abrams
5. Video "Enterprise Security Platform," Palo Alto Networks https://www.paloaltonetworks.com/products/platforms.html
6. Standard "ISA-62443-1-1 Security for Industrial Automation and Control Systems Models and Concepts," ISA99
7. Report "Developing a Framework to Improve Critical Infrastructure Cybersecurity," Forrester Research
8. Brief "Traps: Advanced Endpoint Protection," Palo Alto Networks, https://www.paloaltonetworks.com/products/secure-the-endpoint/traps
9. Standard "Framework for Improving Critical Infrastructure Cybersecurity," National Institute of Standards and Technology

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com