DEFENDING INDUSTRIAL CONTROL SYSTEMS WITH TRIPWIRE

USING TRIPWIRE TO IMPLEMENT THE DHS *SEVEN STEPS TO EFFECTIVELY DEFEND INDUSTRIAL CONTROL SYSTEMS*

ADVANCED THREAT PROTECTION, SECURITY AND COMPLIANCE

INTRODUCTION

Threats to Industrial Control Systems (ICS) are unique. Industries from energy to manufacturing rely on ICSs to drive their business forward and provide invaluable services to people. Industrial Control Systems are responsible for everything from energy production to manufacturing, and their connected ability to make physical changes in the world are what defines the Industrial Internet of Things.

And threats to Industrial Control Systems are increasing. Most industry professionals are familiar with the Stuxnet attack against Iran in late 2007[1]. More recently, reported in early 2015, a German steel mill experienced a significant fire after safety systems were disabled by a cyber attack[2]. In December 2015, the Ukraine suffered the first documented customer outage directly caused by a cyber attack[3]. While these three incidents do not represent a comprehensive timeline, they underscore the growing impact of cyberattacks on Industrial Control Systems.

It's a reality that ICS-centric industries are beginning to recognize. In late 2015, Tripwire conducted a survey of 150 IT professionals across energy, utilities and oil and gas industries[4]. The responses provide evidence for the conclusions we draw from the media-reported incidents. Cyber attacks against these industries are increasing, and more attacks are successful than ever before. At the same time, industry professionals indicate that their ability to detect successful attacks is poor, with 69% of oil and gas respondents saying they were "not confident" in their organization's ability to detect all cyberattacks.

The growing threat to Industrial Control Systems has not been without response. This whitepaper will explore how the U.S. federal government has responded to this threat with recommendations for defending Industrial Control Systems, along with how Tripwire products can specifically address those recommendations.

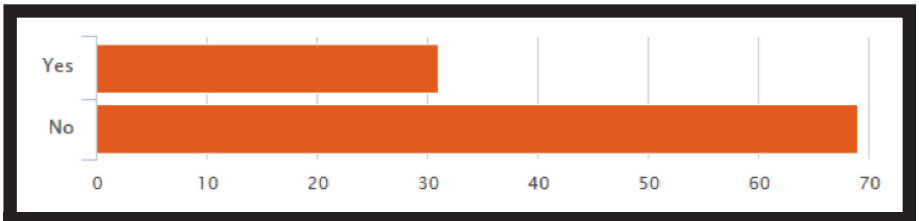

FIG. 1 *Oil and Gas Respondants: Are you confident your organization detects all cyberattacks?*

THE SEVEN STEPS

As a response to the growing need to protect Industrial Control Systems from cyberattack, the Department of Homeland Security (DHS) and the National Cybersecurity and Communications Integration Center (NCCIC) and the National Security Agency (NSA) have jointly published a paper aimed at providing practical steps organizations can take to protect their infrastructure. Titled *Seven Steps to Effectively Defend Industrial Control Systems*,[5] this paper outlines core best practices that should be applied to ICS environments, along with examples of real world incidents that could have been prevented by each step.

The seven steps are:

1. Implement Application Whitelisting
2. Ensure Proper Configuration/Patch Management
3. Reduce Your Attack Surface
4. Build a Defendable Environment
5. Manage Authentication
6. Implement Secure Remote Access
7. Monitor and Respond

These seven steps are sorted by the percentage of attacks they will help mitigate, with Application Whitelisting being the most effective.

ADDRESSING THE SEVEN STEPS WITH TRIPWIRE

Tripwire is uniquely positioned to help organizations defend their Industrial Control Systems. While no single company offers a silver bullet for cyber-defense, Tripwire products provide controls to meet the seven steps, or provide complementary capabilities to help ensure other controls are functioning as desired. In this whitepaper, we'll address each of the seven steps individually, and discuss how Tripwire products can assist customers.

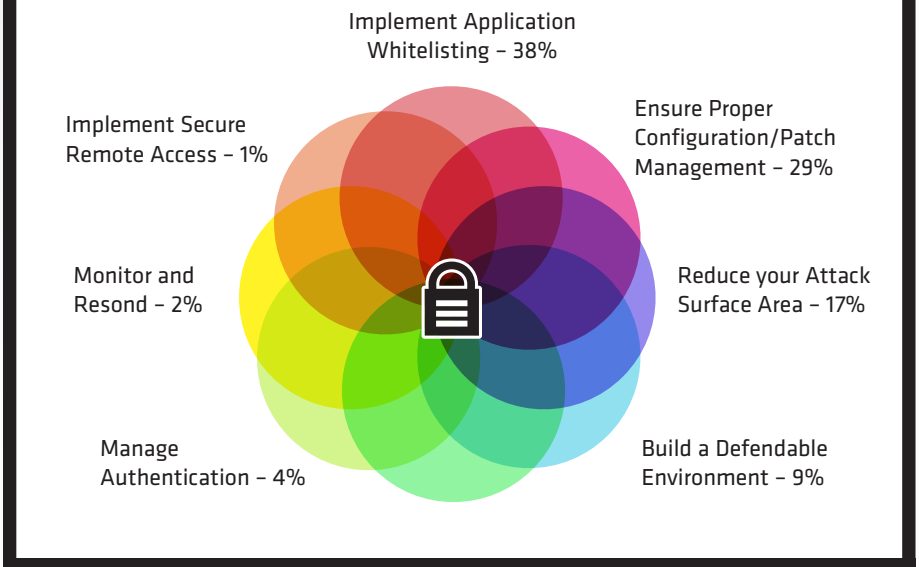

FIG. 2 *Seven Strategies to Defend ICSs. Percentage of ICS-CERT FY 2014 and FY 2015 Incidents Potentially Mitigated by Each Strategy.*

1. IMPLEMENT APPLICATION WHITELISTING

Traditional application whitelisting, which blocks execution of files, is often at the top of the list of most effective controls to deploy—so why is it used so infrequently? While blocking execution is obviously effective at stopping malicious code, it's also a huge risk in highly available, reliability focused environments. It's no surprise that people whose job includes keeping the lights on are wary of most automatic blocking technologies. Of course, highly dynamic environments present a different challenge in actually creating and managing the whitelist itself, let alone the endless complaints from users about lost productivity due to blocking.

The question of how you can take a manageable whitelisting approach, without the explicit blocking, is entirely valid. Tripwire's Whitelist Profiler App for Tripwire® Enterprise offers just this functionality. Rather than providing process-blocking capabilities, Tripwire manages and monitors whitelists of ports, services, users and applications.

With the Whitelist Profiler, Tripwire Enterprise users can manage a multi-domain whitelist of ports and services, applications and users in simple text files, or via integration with third-party products. Tripwire Enterprise will detect any changes in these objects on monitored systems and alert users to objects that aren't in the whitelist. Tripwire Enterprise doesn't block execution, but alerts and monitors, providing detailed data about what changed, even beyond the whitelist.

While *Seven Steps…* includes a recommendation for application whitelisting, the Whitelist Profiler App goes beyond just applications, to also monitor ports, installed software and users. This more comprehensive approach strengthens the solution by covering malicious activities in addition to just monitoring applications.

This implementation allows users to develop and monitor with a whitelist approach without the risks and drawbacks of a blocking technology.

2. ENSURE PROPER CONFIGURATION/PATCH MANAGEMENT

Seven Steps… focuses on unpatched systems being a target for attackers. While Tripwire doesn't directly offer a patch deployment product, Tripwire products are an integral part of assuring that patch management is effective. Tripwire's primary role with regard to patch management is validation.

Tripwire Enterprise gathers the list of installed patches from every host it monitors, which provides operators with independent validation of the patch deployment tool. In fact, the Dynamic Software Reconciliation App for Tripwire Enterprise (DSR) can automate the validation process by ensuring that approved updates are applied and don't include unapproved changes or files. DSR compares the actual changes on a target host to those specified in the update applied.

Tripwire IP360™ can be used to identify the risks that patch management leaves behind, either through incorrect scope, misconfiguration or failed installations. Tripwire IP360 focuses on finding vulnerabilities—not patches—and can help ensure that risks are identified and either accepted or addressed. The information produced by Tripwire IP360 helps customers prioritize their patching process to ensure that high risk vulnerabilities are detected and patched first.

Finally, *Seven Steps* mentions, but doesn't fully address, the risk of misconfigured assets. There's no patch for default credentials or poorly configured access control. Tripwire Enterprise is specifically designed to monitor configurations against established policies. By creating policies that meet security requirements for ICSs and related systems, Tripwire can ensure that deployed configurations match a known baseline or standard.

Tripwire Enterprise will also monitor these systems for changes that might suspicious or take the devices out of compliance with the applied configuration policies.

3. REDUCE YOUR ATTACK SURFACE AREA

You can generally think of the attack surface as the opportunity space in which an attacker can operate. The larger the attack surface, the greater the opportunity for attackers. By reducing your attack surface you not only limit the attacker's opportunity space, but you also make investigating suspicious activity easier by reducing the amount of "noise" present.

The DHS and NCCIC define a few actions for reducing your attack surface. These include network segregation for ICS systems, reducing real-time connectivity to only defined business needs, employing unidirectional gateways where communication is required, and eliminating unnecessary ports and services. It's worth noting that these recommendations align very closely with the NERC CIP requirements for electric utilities in North America.

The Whitelist Profiler App for Tripwire Enterprise is designed specifically to allow customers to manage a known ports and services list, detect when new ports are opened on systems, and provide automated documented justification for known good services. Tripwire Enterprise will also alert when untrusted ports/processes appear. Eliminating unnecessary ports and services on the network has a very direct impact on the attack surface, but it's often done at initial deployment then forgotten; assets that aren't monitored against a baseline are subject to configuration drift. Attack surface can be monitored continuously with Tripwire Enterprise and the Whitelist Profiler App.

In the cases where Tripwire doesn't directly provide a control, such as network segregation, Tripwire Enterprise can validate that other controls are properly configured. After all, security controls are assets on the network, and they can be subject to configuration drift as well.

Beyond Tripwire Enterprise, Tripwire IP360 and the Tripwire Asset Discovery Appliance can be used to actively scan ICS environments to detect open ports and applications running on those ports. Tripwire IP360 and the Tripwire Asset Discovery Appliance both integrate directly with the Whitelist Profiler App. The scan data they produce can be used to supply the Whitelist Profiler with network port information.

Though DHS/NCCIC doesn't specifically recommend eliminating unnecessary devices as part of attack surface reduction, it's a valuable piece of the puzzle. A device that doesn't exist can't be attacked, and a device that's on the network always presents another target. Tripwire IP360 or the Tripwire Asset Discovery Appliance can be used to discover devices on the network.

4. BUILD A DEFENDABLE ENVIRONMENT

While there are many ways in which Tripwire products can help ensure an environment is defended, the defensibility of the environment is really determined by the systems and topology itself. These are solid recommendations from DHS/NCCIC and Tripwire can validate many of the configurations, but applying Tripwire products to an environment largely adds actual defense to a defendable environment.

Part of a defendable environment should be the ability to respond to realized threats quickly and confidently. With Tripwire Enterprise's change data about assets, operators can identify how systems changed during a breach. The information can be used to identify compromised hosts, to help revert hosts to a known good configuration and to provide out-of-band validation of baselines. Tripwire Log Center® is invaluable in breach identification and investigation; its correlation rules can be used to identify suspicious events that are bigger than a single log entry. Integration between Tripwire Log Center and Tripwire Enterprise adds efficiency to breach investigations.

5. MANAGE AUTHENTICATION

It's true that "[a]dversaries are increasingly focusing on gaining control of legitimate credentials." Using legitimate credentials not only makes access easier for an attacker, it also helps to mask much of their malicious activity. As with many attack tactics, there are already controls that can help—if deployed properly. Tripwire isn't an authentication company, but Tripwire products can be used in two specific ways to help with this requirement.

First, Tripwire Enterprise can validate authentication configurations to ensure that strong passwords or multi-factor authentication is being used. As noted above, security controls can be victims of configuration drift just like any other asset, and monitoring them for change against baselines will alert operators to unauthorized or insecure changes.

Secondly, Tripwire Log Center can be used to actively detect malicious activity even under legitimate credentials. Criminals don't compromise credentials to simply sit on them. They use them, and those patterns of use can be valuable indicators of a breach in progress. Tripwire Log Center correlation rules can be used to identify patterns of

misuse with user logins—including valid users. A popular attack tactic involves compromising a standard user login and then exploiting a vulnerability to add it to a privileged group. Tripwire Enterprise can detect changes in user privileges and group membership to identify attempts to escalate privileges with a legitimate account.

6. IMPLEMENT SECURE REMOTE ACCESS

The secure remote access requirements outlined by the DHS/NCCIC seem like common sense in text but can be challenging to actually implement, especially when being added to existing infrastructure. Change is hard and human beings develop habits.

Tripwire doesn't provide a secure remote access solution directly, but Tripwire Enterprise can validate the configuration of remote access products to ensure they match established policy. Through partnerships with industry-specific vendors, Tripwire is able to integrate with many industrial focused products for secure remote access. Tripwire Enterprise can also identify when new services are enabled that may provide alternate remote access services. Finally, Tripwire IP360 can scan an environment to identify remote access services as well.

While validating configurations and identifying services is important, abuse can still occur within an approved remote service. To address this possibility a monitoring solution is required. Tripwire Log Center can monitor remote access logs to identify anomalous or suspicious activity, such as authentication activity occurring outside a specified time window or with unusual accounts.

7. MONITOR AND RESPOND

The speed and efficiency of both initial investigation and response can directly affect the impact of a successful attack. When teams lack visibility into asset changes and events, they simply give the attacker more room to hide and more time to act.

While Tripwire isn't in the business of monitoring IP traffic, these recommendations from DHS/NCCIC do include specific functionality that Tripwire provides. During an investigation, it's invaluable to be able to quickly determine how a host has changed in a given time period. Tripwire Enterprise monitors assets for changes and can provide key data about what an attacker may have done while present on an asset.

Tripwire Log Center provides a centralized location for reviewing collected logs, which are important to tracing the path of an attacker. Tripwire Log Center can also monitor login activity for patterns of abuse that are tailored to your organization. Tripwire Enterprise also looks for changes, including those in user permissions, login capabilities and group membership.

Combining these capabilities, including "launch in context" integration between the products, gives customers the ability to efficiently and effectively investigate suspicious activity, determine if it's malicious, and take action to respond.

While not explicitly called for in the "Seven Steps," monitoring the external threat environment is an important part of an overall security program. The need to integrated threat information applies to ICS as much as it applies to corporate IT. Tripwire Enterprise can import threat feeds from major commercial vendors, and by using the open STIX/TAXII standards. Once imported, Tripwire Enterprise can search and monitor the environment for matching indicators.

CONCLUSION

Anyone who works in information security knows that there are no silver bullets. Defense requires a layered approach, with attention to the evolving threats. *Seven Steps to Effectively Defend Industrial Control Systems* provides a solid set of best practices that can materially improve the risk posture of ICS environments.

With a suite of flexible solutions and deep experience, Tripwire is uniquely positioned to help ICS-centric organizations implement the seven steps outlined by the DHS, NSA and NCCIC. Discovery and vulnerability scanning identify security issues before they're exploited. Tripwire's focus on baselining and change detection drives a proactive approach to security and compliance, while the ability to securely collect and centralize logs from Industrial Control Systems provides alerting about patterns of malicious activity and detailed information for response and forensics.

FOOTNOTES

1 https://en.wikipedia.org/wiki/Stuxnet

2 http://www.wired.com/2015/01/german-steel-mill-hack-destruction/

3 https://www.energyvoice.com/other-news/97940/cyber-attack-should-be-wake-up-call-for-energy-sector/

4 http://www.tripwire.com/company/news/press-release/tripwire-study-cyber-attackers-successfully-targeting-oil-and-gas-industry/

5 https://ics-cert.us-cert.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf

◆ Tripwire is a leading provider of endpoint detection and response, security, compliance and IT operation solutions for enterprises, service providers and government agencies. Tripwire solutions are based on high-fidelity asset visibility and deep endpoint intelligence combined with business context; together these solutions integrate and automate security and IT operations. Tripwire's portfolio of enterprise-class solutions includes configuration and policy management, file integrity monitoring, vulnerability management, log management, and reporting and analytics. Learn more at tripwire.com ◆

SECURITY NEWS, TRENDS AND INSIGHTS AT TRIPWIRE.COM/BLOG ◆ FOLLOW US @TRIPWIREINC ON TWITTER

WPDICS1a 201601