Insights into Building an Industrial Control System Security Operations Center

March 2017

As industrial control systems (ICS) become more interconnected with each other and homogenous, there needs to be sufficient compensating controls put into place to ensure the safety and reliability of the operations. One of most dedicated focuses towards security that can be implemented in a well-prepared ICS is a security operations center (SOC). A SOC is a combination of people, processes, and technology that proactively search for abnormalities in the environment to identify and respond to security incidents.

DRAGOS

Insights for Building an Industrial Control System Security Operations Center

As industrial control systems (ICS) become more interconnected with each other and homogenous, there needs to be sufficient compensating controls put into place to ensure the safety and reliability of the operations. One of most dedicated focuses towards security that can be implemented in a well-prepared ICS is a security operations center (SOC). A SOC is a combination of people, processes, and technology that proactively search for abnormalities in the environment to identify and respond to security incidents. Many enterprise information technology (IT) companies have achieved varying degrees of success with SOCs and are continually attempting to evolve the security landscape through best practices and new technologies. The purpose of this paper is not to repeat those efforts but instead extend that focus to ICS environments. Organizations with ICS such as those in the electric, water, oil, gas, nuclear, and manufacturing industries have typically not seen the same attention placed on the security of these systems as the enterprise. Many SOC best practices can apply to the ICS but tailoring is required.

Tailoring Required for ICS

Team Structure
There is not a "one size fits all" model. Each organization will have to tailor its ICS SOC to its organization. Some may choose to integrate ICS skill-sets within an existing centralized traditional SOC while others may choose one ICS SOC for each business unit and integrate these SOCs in a distributed matter. Traditional IT distributed models often have the centralized SOC serving as the subject matter experts. Centralizing expertise is an obvious choice when senior and skilled SOC staff are rare. However, a distributed ICS SOC is reversed where the local staff are more integrated with the systems and processes and are required for a strong specialization.

It is important to determine scope, roles, and responsibilities when choosing what SOC model is most appropriate. It's recommended that each of these are incorporated within the security policy framework of the enterprise or organization. This is particularly important for buy-in when working with multiple business units or stakeholders.

Decisions to Consider

Centralized vs. distributed model
How does the ICS SOC integrate or work with physical security, traditional IT SOCs, or external partners?

Finding differentiated services
The ICS SOC mission and value must increase reliability and safety in a way that others teams are not. How is the ICS SOC providing this value?

Visibility
The ICS SOC must have the innovative tools and techniques to create unique datasets within the enterprise. Deciding on the toolset will have long term ramifications.

Also, a roadmap of services provided to the business unit(s) must be considered. SOCs can range in functions including incident response, security monitoring and detection, threat hunting, threat intelligence, red teaming/penetration testing, end user escalation, and SOC-owned IT support. Many of these services have prerequisites. Figure **1** outlines the Sliding Scale of Cyber Security and reflects the concept that organizations will gain more benefit in investments by moving from left to right on the sliding scale. For instance, investing heavily in Active Defense services such as threat hunting will have limited returns until adequate Architecture and Passive Defense services are in place.

Figure 1: Sliding Scale of Cyber Security [3]

[1] The Dragos team has observed the leading choice among customers to be an OT specific SOC that works in conjunction with an IT specific SOC. Different considerations will drive organizations' choices but this appears to be a budding best practice.
[2] The Sliding Scale of Cyber Security denotes that most of the value towards security builds on the left hand side of the scale moving to the right. The operating assumption is that no organization should ever be able to invest in Offense as the return on investment is too minimal despite other legal and ethical issues involved with "hack back." Imagine the investment as a waterfall, Architecture should receive most of the attention, then well-tuned Passive Defenses and technologies, to Active Defense personnel, and capped with Intelligence. Intelligence as an example is a great addition to a well-functioning security program not a replacement for it.
3 https://www.sans.org/reading-room/whitepapers/analyst/sliding-scale-cyber-security-36240

People

SOCs rightfully place a large focus on the people. To be able to respond to human threats requires human defenders. Well trained analysts can be expensive but are often extremely effective at identifying real issues instead of escalating false positives. In security operations there are three levels of analysts that are commonly referred to: Tier 1 analysts who search logs and process, alerts, and other categorized events to identify and escalate abnormalities. Tier 2 analysts are the incident responders who triage the events, analyze the accompanying activity, and apply appropriate mitigations. Tier 3 analysts are there to act as subject matter experts when deeper analysis is required; especially against new threats. Tier 3 analysts should also utilize their time to act as threat hunters when possible. This focus moves them away from identifying and analyzing escalated events and instead dedicates a portion of their time to developing methods and analytics to search out threats missed by the other defenses put in place.

In an ICS, it is important to identify personnel in the SOC that can spend time with the engineers and operations staff in the field. Likewise, it is important to have willing engineers and operators spend time in the SOC for appropriate training and temporary assignments. This can be a daunting task in organizations that constantly feel undermanned. However, one of the biggest problems in the ICS security community is the culture clash. When the security personnel and the operations personnel do not understand the value of each other, the pain points each has and the requirements for the overall business natural divides will occur that will lead to increased incident response time and self-inflicted issues that cause financial burden. For instance, tier 3 personnel should have an understanding of what they can provide field operators during outage/maintenance windows or change-freeze windows incurred due to weather events. An adversary cannot hope for a better security gap than a divide between teams responsible for infrastructure.

In addition to having the right people, the ICS SOC will need the appropriate team structure. An ICS SOC should consider incorporating support roles into the SOC. This includes IT support staff to maintain any ICS SOC owned equipment, such as network IDS and firewalls. Such support capacities allow dynamic support and flexible capabilities such as rapid signature deployment or other application needs.

Recommended Training Classes for ICS SOC Professionals

- SANS MGT517 – Managing Security Operations | Target Audience: Team Leads and Managers
- SANS ICS410 – ICS/SCADA Security Fundamentals | Target Audience: Tier 1 Professionals
- SANS ICS515 – ICS Active Defense and Incident Response | Target Audience: Tier 2-3 Professionals
- Dragos ICS Security Operations 5 Day Course | Target Audience: Tier 2-3 Professionals

Outsourcing and Managed Security Service Providers (MSSPs)

The ICS security community has significant challenges in identifying and retaining dedicated talent. Understanding IT security is important but is only part of the equation; security personnel also need to understand the ICS, its considerations, and how to safely respond to incidents. Identifying personnel ready to operate in the ICS can be challenging. Many enterprise IT companies rely on outsourced support for incident response for critical events or consistent monitoring support through MSSPs. Due to the skill gap in the ICS security community it is worthwhile to evaluate the need for an MSSP focused on ICS and the subject matter expertise they can bring to the SOC.

> *The Pitch:* Dragos, Inc. has assembled some of the world's top experts on security operations and incident response in ICS in the Dragos Threat Operations Center. Here, managed services such as compromise assessments, incident response, and threat hunting are available to ICS customers as standalone services or through the Dragos Platform.

Process

In all SOCs, there should be a high emphasis placed on establishing processes to guide the daily flow of security operations and collaboration. For example, how incidents are discovered should be clearly documented. This helps staff continually revisit codified procedures with an eye for continually improving and automating each series of steps. Escalating events for more analysis - and to whom these events are forwarded - are an important bridge between Tier 1 and Tier 2 analysts. Mature SOCs integrate such processes with business continuity programs supporting the organization to guard against downtime, given the common interruption consequences of cyber attacks, accidents, weather and other physical incidents. The business continuity requirements and the thresholds for informing senior management or gaining their approval for requested actions must all be documented. Additionally, models for the identification and classification of adversary activity such as the intrusion kill chain, the Diamond Model, and CSIRT OODA Loop help guide analysts and structure data in a way that knowledge can be extracted out of it to continually better the organization.

In an ICS, processes are even more important so that all parties' needs are met by the security team. Consider a scenario where the SOC is focused on an ICS control center leveraging supervisory control and data acquisition (SCADA servers across a gas pipeline. If an incident occurs at the control center there needs to be a clear threshold and process for informing the operations personnel in charge of the gas compressor stations. The pipeline is moving gas from an upstream location to a downstream location and thus an incident at the facility could also impact the upstream and downstream company which may or may not be the same company where the SOC is located. Likewise, interconnected vendor VPNs may act as a pivot point for adversaries into other networks and thus all parties must share information.

Furthermore, an ICS centric SOC must always balance the risk that vendors and contractors are coming in and out of the site with USBs or equipment that may inadvertently spread an infection to critical portions of the ICS. If not properly considered this may result in an extremely costly loss of operations and confidence in the security team. Likewise, if well intentioned security personnel inform operations of an issue that is not critical, can wait for a maintenance period, or was not analyzed properly to determine it was a false positive it will also erode trust. Indeed, ICS centric SOCs do not hinder maintenance windows but instead are aware and heighten their visibility to detect potential malicious activity while field personnel are unimpeded. Always include operations in as much of the process as possible especially for critical events. The time to do this is before the incident, not after one is declared

Pro Tip: ICS Security Models

Consider ICS security models to fully understand an ICS cyber attack as well as mechanisms to prevent the incident in the future, reduce its impact, and help detect it more quickly. For example, by combining the ICS Cyber Kill Chain, example shown in Figure 1, with the Sliding Scale of Cyber Security and the Bow Tie model a single incident can reveal 20-30 recommendations for better architecture, passive defenses, and active defenses in the organization. To really push ICS security forward complete that analysis for the top incidents each quarter. In the analyzed data trends will reveal themselves which will lead to the security team prioritizing the top 3-4 controls that need to be put into place to tailor the security against the threats that the organization faces.

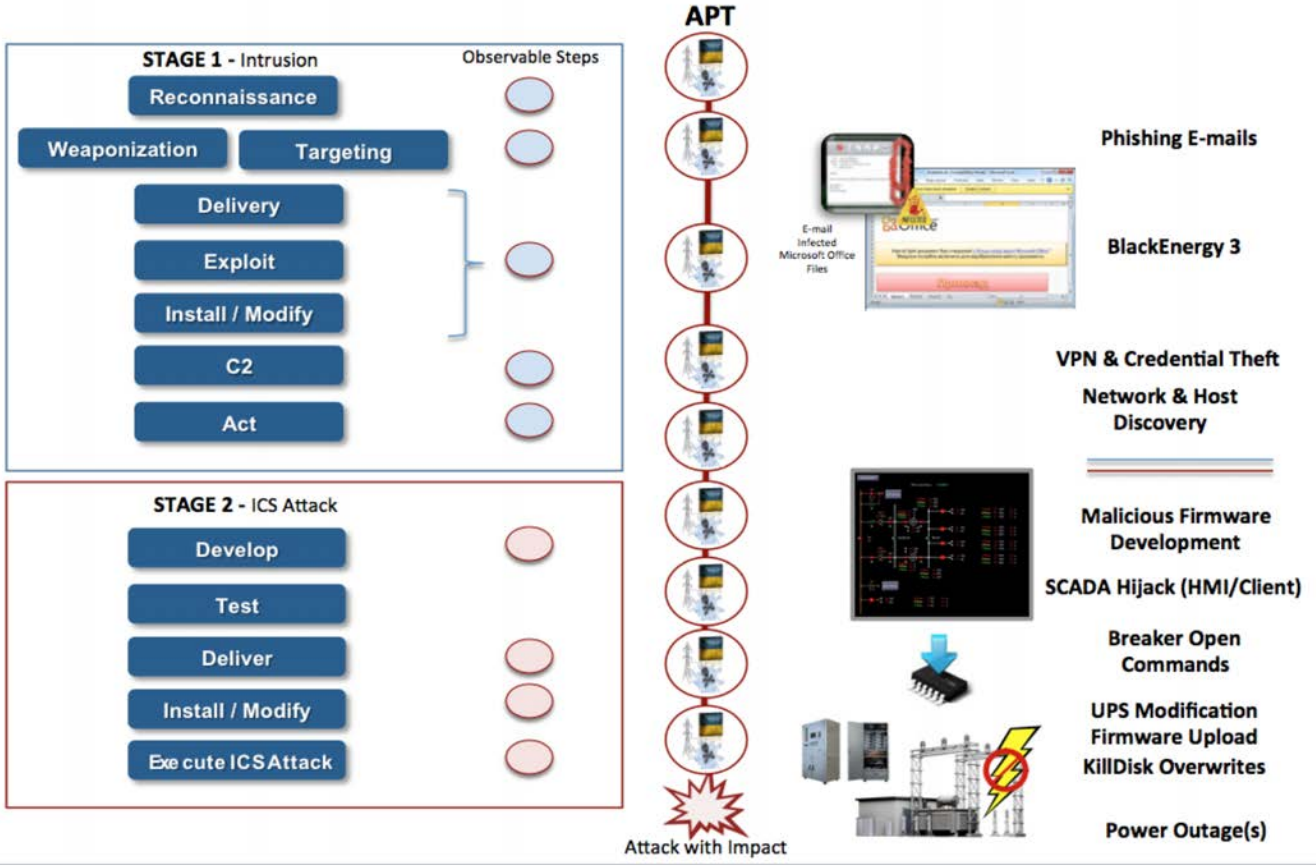

Figure 1: The Ukraine Power Grid Cyber Attack Mapped to the ICS Cyber Kill Chain [4]

Technology

It is a consistent struggle for enterprise IT SOCs to gain visibility across their enterprise. The number of unique internet protocol (IP) connected devices can reach the hundreds of thousands or millions very quickly depending on the size of the organization and its embrace of new technologies, user devices, and communication methods. This has led organizations to prioritize investments using a defense in depth model that includes endpoint security solutions, log aggregators, system information and event managers (SIEMs), and a variety of competing "next generation" technologies. Baselining the entire enterprise is improbable which forces a blacklist like culture on IT where they look for known issues more than abnormalities. While ICS data collection can be challenging it does not have the same problems.

Data Collection in ICS

In an ICS one of the most significant challenges for security is data collection. Technologies on the market have historically not focused on ICS. When they do the ICS aspect is often an add-on module to an IT solution. This is not always bad but has led to a lack of technologies suitable for the ICS. Endpoint security solutions cannot be deployed on

[4] Credit: The SANS Ukraine Power Grid Cyber Attack Defense Use Case http://ics.sans.org/duc5

embedded devices such as programmable logic controllers (PLCs) in an acceptable manner and to do so on the Windows supervisory environment can lead to voided warranties. In addition, antivirus can often do more harm than good as it alerts on heuristics it believes to be malicious that are commonplace for the ICS application. Unmanaged infrastructure, legacy equipment, proprietary technologies and IP protocols that contain vital information about the ICS require technology to be tailored for the ICS and an emphasis placed on gathering as much data as possible in an environment where there are less logs and events to collect.

Gathering data after a suspected incident is increasingly difficult in ICS environments. Coordination of what tools and technologies can be safely introduced into the environment and who has the authority to collect and analyze the data are common issues. Additionally, be careful to determine what tools can operate safely in different ICS zones. In a standard ISA99 reference architecture deploying systems that can scan or interact with systems may be appropriate in Level 4 but would be potentially dangerous or disruptive in Level 1. Technologies that operate passively are important but the technology should also have different approaches for analysis of data across different zones based on the requirements, normal activity, and data available.

There are also historically less devices to collect logs and events from in the ICS compared to IT. For these reasons, prior to standing up a SOC, make a concerted effort to prepare the environment. Managed switches to gather network data, identifying if equipment such as PLCs have data such as syslog that can be centrally collected, syncing up the IT and ICS side of the firewalls to forward logs, gaining approval for a lightweight passive collector on Windows and Linux environments to collect host events, and integration with physical security systems such as CCTV camera networks for alerts at unmanned physical sites are all vital to visibility in the ICS.

Common Data Sources in ICS Environments and Relative Ease to Gather	
Netflows (IPFIX, Sflow, AppFlow, etc.)	Easy (requires managed network infrastructure)
Network traffic (pcap)	Easy (requires managed switches)
Process controller logs (syslog)	Moderate (requires functionality on controllers)
Process/Data Historian	Moderate (requires API access and integration)
Host based logs (Windows and Linux supervisory systems)	Hard (usually requires vendor approval)
ICS Software Events and Alarms	Hard (requires API access/integration or centralized collection and integration and specialized analysis)
Specialized Equipment logs (e.g. digital relay logs, CCTV, physical security systems, etc.)	Hard (requires functionality on device and special integrations as well as specialized analysis)

The Pitch: Dragos, Inc. developed the Dragos Platform as a secure technology for passively collecting information out of the ICS (from all the data sources mentioned above) into a central repository with ICS specific user interfaces and prioritization of events. The platform focuses on asset identification, threat detection, and workflow automation to ensure that even small teams can operate like a full SOC while automating daily tasks.

One benefit of the ICS is that once the data is collected an organization can then apply a whitelist styled approach of baselining the environment. PLCs have fairly static communication patterns and protocols. It would be more than abnormal for a PLC to attempt to reach out to new IP addresses. There should be no users browsing to Facebook, Twitter, LinkedIn, and other social media websites. Emails and their attachments should also not be in the ICS. Simply put, ICS environments are more static and often much smaller than an IT environment. Through a dedicated approach to learning the ICS and what normal looks like the SOC personnel can baseline it and respond to abnormalities with a much higher confidence of identifying issues over false positives. Additionally, in an ICS, systems updates are often restricted to scheduled maintenance periods, any many changes common on hosts in an Enterprise networks (changing files, processes, and registries) should be very uncommon in an ICS and can be a key indicator of compromise.

Cyber Threat Intelligence

Many SOCs rely heavily on cyber threat intelligence as an additional source of data to understand adversaries, their motives and capabilities, and how to identify them. In the ICS security community there is a significant lack of insight into the ICS threat landscape as traditional security vendors have not had the data sources, incident response data, and expertise required generate ICS threat intelligence. More IT threats are also making their way into the ICS and threat intelligence on IT threats can add value to what is uncovered but needs tailoring for the ICS. Drive the SOC to analyze the threats in the ICS to generate as much of their own ICS specific threat intelligence as possible. Utilize professional technologies to collect and store this analyzed information and enrich it with traditional IT data sources where appropriate. Ensure integration between what the IT SOC is seeing and what the OT SOC is seeing. Leverage strategic, operational, and tactical level threat intelligence where available but do not be so over-focused on indicators of compromise (IOCs) as not to realize the benefit of ICS environments to use behavioral analytics. Behavioral analytics can be more effective than baselining or anomaly detection by not only identifying the malicious activity but also pinpointing what the behavior was trying to accomplish in the ICS. This means it can closely be integrated with response plans.

Types of Threat Intelligence and Value to the ICS SOC	
Tactical Level Intelligence	Look for IOCs of new threats to scope the environment and notifications on ICS specific vulnerabilities that actually introduce risk to the ICS.
Operational Level Intelligence	Identify adversary tradecraft and what vulnerabilities adversaries are leveraging. New behavioral analytics and workflows to counter them should be included or correlated with the intel.
Strategic Level Intelligence	Understand what is going on across the ICS industry vs. your industry. Look for higher order analysis on events in the world and appropriate business responses that can incorporate cross-business unit prioritizations, investments, and preparation.

The Pitch: The Dragos Intelligence team creates ICS specific threat intelligence available to the industry. The first output is WorldView which is situational awareness level reports and strategic insights. The second output of the team is the creation of new behavioral analytics and indicators of compromise (IOCs) that get pushed to the Dragos Platform to ensure readiness against new emerging threats with appropriate responses.

Conclusion: Measuring Success

An innovative ICS SOC can follow many of the best practices of IT SOCs but requires tailoring across people, processes, and technology to ensure success. Organizations should look to measure success across a variety of areas including the time it takes for defenders to identify adversaries, respond to the incidents, and apply security measures to mitigate issues in the future. However, ICS organizations should also look to incorporate visibility into their metrics. Visibility into the ICS networks and activity taking place in them is abysmal across most companies in the ICS community. It is important to not only be able to identify adversary activity but also be able to respond in a timely manner to misconfigured devices, contractors and employees performing inappropriate actions in the ICS, and to gain an understanding of the networked assets and their topology.

Pro Tip: Performance Metrics

Develop performance metrics based on defender activity instead of adversary activity. Adversary activity should be fully tracked and understood including the number of incidents that occur and how they were successful. However, the SOC's performance evaluation should not be driven by adversaries alone. In a well defended ICS there may be a lack of adversary metrics but each incident averted is a significant cost savings for a company. Focus instead on defender based metrics such as their visibility into the environment based on the different network segments they can successfully monitor. Also consider how long it takes the SOC to work through established processes such as the time from the identification of the event to the full triaging of it across the ICS. Finally, although it may seem counterintuitive consider the availability of the systems for required work as a performance metric. Uptime cannot be valued so highly that it discourages proper security but good security should contribute to the reliability of operations.

Another good measure of success in an ICS SOC is the integration and trust that gets built between the security and ICS operations teams. This should not be a metric with a numerically assigned value but instead should be a focal point of management to encourage coordination between the various teams. An innovative ICS SOC is focused on the ICS but can just as easily share information valuable to the IT SOC as they can to engineers and operators at the organization. It is their responsibility to share the information in a method that helps each perform their job more efficiently instead of being stuck in a loop of reporting out metrics that they understand but do not add value to others.

In conclusion, an ICS SOC that operates in a defensible network environment and is properly tailored for the organization's requirements can significantly contribute to the security and availability of the operations systems. It is up to each organization to determine if a SOC is the best use of their resources and if so what type of SOC is most useful to them. It is important to consistently understand that value in appropriately measuring the security operations and its interconnected components of people, process, and technology. While each organization will differ in their requirements the consistent theme of people, process, and technology as well as how each need to be adapted properly for ICS acts as a good approach for organizations looking to build an ICS SOC.

Dragos, Inc. exists to safeguard civilization. Our approach is to bring together some of the world's most respected ICS security experts and create an ecosystem for the industrial community to leverage. The Dragos Ecosystem is compromised of the Dragos Platform, Dragos Threat Operations Center, and Intelligence and Analytics team. We ensure that our customers have access to the right technology, right information, and right people who have lived their problems – not just admired them.

For more information, contact us at info@dragos.com or visit our website at www.dragos.com

DRAGOS