DRAGOS

The Real Risk to ICS Environments

Using Threat Intelligence to Improve Compliance and Risk Management

By Thomas Pope and Selena Larson

Executive Summary

The cyber threat to industrial control systems, including critical infrastructure, is greatly different than those theorized or targeted by compliance efforts, leaving ICS risk management struggling.

The cyber risk to industrial control systems (ICS) is significant and growing[1] and largely unmanaged against the real threats – including threats to life and the physical environment – facing ICS. There are a number of reasons for this: lack of data and visibility into threats, a dynamic threat landscape, and an increasing number of adversaries targeting this space.

We are experiencing an ever-changing landscape challenging our understanding of ICS threats and the threat behaviors, and defense against new threats is not fully addressed in compliance. Furthermore, compliance only leads to a bare minimum of security. Leveraging threat intelligence — knowledge about adversaries based on evidence collected and analyzed by ICS intelligence experts — is critical to securing ICS environments. As the numbers of adversaries and ICS attacks increase, companies need to re-evaluate how they treat risk to their ICS environments outside of natural events. This is especially true for those operating in critical infrastructure.

Applying ICS-specific threat intelligence to governance, risk, and compliance (GRC) can greatly reduce an organization's risk profile and help meet compliance mandates

Threat intelligence can provide context to detected threats or incidents and incorporate vertical-specific data into established security postures. For instance, knowing the behaviors of activity groups targeting transmission substations and grid operations can help electric utilities implement specific detection and mitigation strategies. Further, ICS threat intelligence can help organizations effectively prioritize compliance and governance tasks.

Companies struggle with consuming massive amounts of data and effectively applying intelligence to that data in order to make impactful decisions. This is especially true with the Governance, Risk and Compliance (GRC) disciplines. Applying ICS-specific intelligence to GRC can greatly reduce an organization's risk profile and help meet compliance mandates. Threat

---

[1] ICS Activity Groups and the Threat Landscape
https://dragos.com/resource/ics-activity-groups-and-the-threat-landscape/

intelligence can help organizations meet minimum compliance requirements, while going further to create a robust security strategy capable of adapting to evolving threats.

Table of Contents

ICS Threat Intelligence: Defined

ICS threat intelligence is having knowledge and an understanding of adversaries and their behaviors which enables defenders to have context and visibility around threats. Threat intelligence provides three critical elements: describing the threat, illustrating the impact, and recommending action.[2]

Threat intelligence is the product of evidence-based and hypothesis-led analysis from a number of data sources and identified behaviors. It can provide insight into: adversary tools, tactics, procedures; targets including geographic regions; motivation and intent; and operational behaviors and patterns.

Using real-life scenarios such as the CRASHOVERRIDE and TRISIS incidents, plus known trends and behavioral analytics[3] from tracked activity groups, allows defenders and policymakers to implement defenses that can stop real-world attacks.

ICS Threats Different Than Expected

Dragos learns about industrial cyber threats through customers that deploy our technology, the Dragos Platform, as well as our services engagements such as incident response and the work of our intelligence team. Over the last several years we have learned that the risk to ICS is significantly different than expected when compared to traditional enterprise security standards and ICS compliance frameworks.

The scope and consequences of ICS-specific targeting continue to expand; adversaries are targeting safety instrumented systems (SIS) with an apparent disregard for harm caused to physical processes or human workers, and more targets are experiencing the kinetic effects of cyber intrusions. Dragos has observed companies storing intellectual property in the OT network, not just on the corporate side. Businesses frequently do not properly account for this attack path due to a greater focus placed on preventing process disruption.

Adversaries are rarely using vulnerabilities in equipment and operating systems. They are taking advantage of misconfigurations, built-in legitimate functionality, and a lack of visibility in control environments.

When measuring risk to ICS, organizations must identify what is most critical to operations and identify the worst possible consequences if an adversary successfully disrupts them. Risk assessments should include a fundamental understanding of critical systems based on threat

---

[2] Industrial Control Threat Intelligence
https://dragos.com/blog/20171208-IndustrialControlThreatIntelligence.html
[3] Threat Analytics and Activity groups
https://dragos.com/blog/20180226ThreatAnalyticsAndActivityGroups.html

intelligence and behavioral analytics because ICS-specific adversaries are developing bespoke tools and strategies designed for individual processes. This is because what looks important to a neutral risk assessment may not be the same as an adversary.

Due to the variety of strategies and tools ICS adversaries deploy, including a greater use of "living off the land" techniques via commonly available tools in almost every environment, patching alone will not protect organizations from potential threats in ICS environments. Patching does not prevent abuse of protocols and inherent functionality of ICS software and equipment. Special care must be taken to understand the risks posed by leaving interfaces and accesses unsecured.

Here are seven lessons on how ICS threats manifest themselves in real events:

1. Rare Use of Zero-Days or Vulnerabilities

Current tracked activity groups seldomly use ICS zero-days (vulnerabilities unknown to anyone but the adversary) or known ICS vulnerabilities to achieve their objectives. However, some threats have leveraged known IT vulnerabilities, such as those patched by the Windows update MS17-010[4], to gain initial access to target environment and ultimately compromise operational networks. Adversaries used stolen and leaked exploits, known as the ETERNAL series, to exploit those vulnerabilities in the global WannaCry ransomware and NotPetya malware events, despite the flaws being patched months before. These events affected large numbers of ICS operations, most of which were not publicly reported. The exploits continue to work to this day.[5]

2. Limited ICS Edge Exploitation

Internet connectivity within ICS still poses significant risk, but Dragos finds ICS-targeting adversaries moving through IT environments more frequently. Malicious actors rely on content-based attacks like capturing credentials through phishing or watering hole techniques and "safe" tools like Windows SysInternals to compromise IT environments to pivot throughout operational networks and masquerade as legitimate users. However, this is not exclusive to the target IT network; adversaries could leverage connections to and relationships with vendors or system integrators as an ingress point, which Dragos has observed in recent cases.

3. Masquerading as Engineers

Attackers try to blend in with normal activities, making their pivoting activities more subversive and dangerous. In the ICS world, engineers are the gateway to operational equipment. Compliance would normally dictate restricting access as much as possible to only those who

---

[4] Microsoft Security Bulletin MS17-010 - Critical
https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010
[5] iPhone Chipmaker Blames WannaCry Variant for Plant Closures
https://www.bloomberg.com/news/articles/2018-08-06/iphone-chipmaker-blames-wannacry-variant-for-plant-closures

need it, but because engineers need that access, attackers may target them for credential theft and replay. To detect attacks, monitoring behavioral characteristics of engineer work habits would be more likely to catch an attacker.

4. Using Legitimate Protocols Illegitimately

The 2016 CRASHOVERRIDE[6] malware attack in Ukraine is an example of adversaries understanding their target's ICS environment to create specialized destructive malware. The activity group ELECTRUM developed an attack that directly affected switchgear inside a transmission substation to cause equipment failures. This was a highly effective and highly scalable way to target transmission-level substations without taking advantage of exploits or vulnerabilities. Because the attackers understood the protocols used in the target's ICS networks and how to send appropriate commands, they achieved their desired disruptive effect. In this event, the adversary resided in the environment for an extended period of time and briged the IT/OT gap via the historian database, which demonstrates the need to monitor communications in the ICS, and understand ICS protocols in monitoring.

5. Safety Systems Attacked

TRISIS[7] provides a real-world example of an attack on a SIS. An attack on a SIS is concerning, but a safety system should be at the most tightly-controlled levels of the network; however, this is not always the case, even if that is how the system was originally designed to operate. Attackers should need to compromise multiple defenses to have the opportunity to affect the SIS. However, the amount of damage that can be caused by compromising the safety facet of the SIS can be astronomical, including loss of life. While having asset identification and traditional anti-virus is useful, these mechanisms would not pick up abuse of engineering workstations or field devices. Asset owners and operators need to monitor OT communications and ICS protocols for deviation and abuse.

6. Long-Lead Times to Disruption

ICS adversaries rarely act immediately after compromising an environment. They are spending a long time within target networks before they attempt any action, conducting reconnaissance, learning the environment, giving defenders time to detect and respond to malicious activity. This is called “dwell time.”

---

[6] CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations
https://dragos.com/blog/crashoverride/CrashOverride-01.pdf
[7] TRISIS Malware
https://dragos.com/blog/trisis/TRISIS-01.pdf

The ICS Cyber Kill Chain[8] contains two stages and a number of opportunities for detection before the adversary executes an attack. Stage 1 includes planning, preparing, and the initial intrusion. In Stage 2, the attacker uses what they learn in Stage 1 to create an attack capability for the target operational environment and ultimately launch an attack.

This long dwell time in an industrial environment provides significant opportunity for defenders to detect and disrupt adversary options.

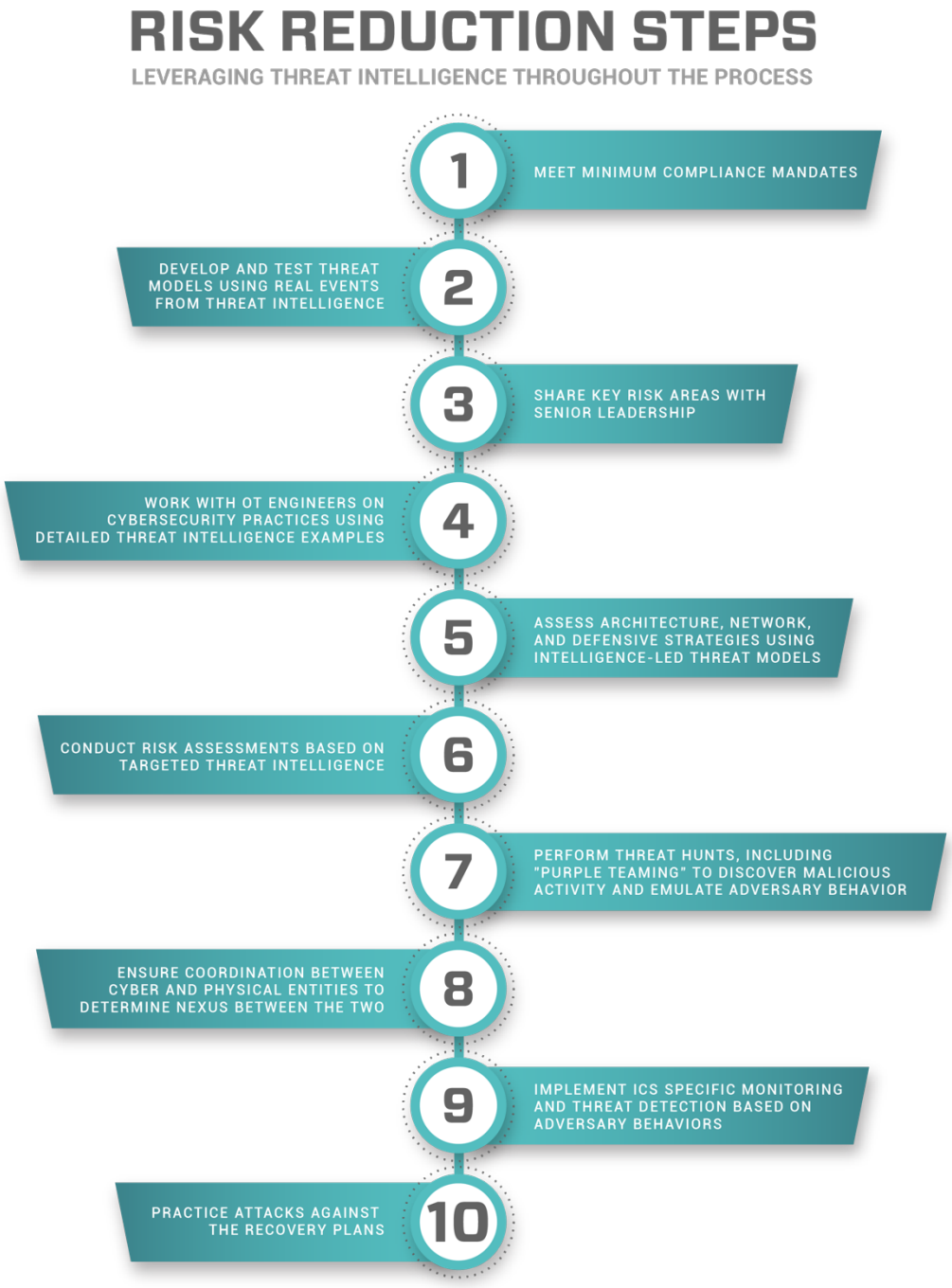
7. Attack Recovery Plans

The 2015 and 2016 Ukraine attacks both involved methods of attacking the expected recovery tools and processes. In 2015 attackers reconfigured the uninterruptible power supply (UPS) to disable emergency power functions, modified serial-to-ethernet gateways to prevent operators from remotely reaching substations, leveraged wiper malware to incapacitate workstations, and executed a denial of service attack on the phone systems at control centers to prevent customers from calling in outages.[9] Attackers in the 2016 event deployed a wiper module and denial of service capability leveraging a previously-disclosed vulnerability in Siemens SIPROTEC equipment and deleted the controller configuration files to prevent easy rebuilding. These behaviors demonstrate an effort not to just disrupt, but to cause the longest possible disruption.[10] The attack did not require these to be successful, but they contributed to its effectiveness.

Asset owners and operators should create recovery plans based on crown jewel analysis and threat intelligence assessments of previous attacks which provide insight into modern activity group behaviors. This information can also be used in attack simulation.

---

[8] ICS Cyber Kill Chain
https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297
[9] Analysis of the Cyber Attack on the Ukrainian Power Grid
https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf
[10] Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE
https://dragos.com/resource/anatomy-of-an-attack-detecting-and-defeating-crashoverride/



Defenders use ICS threat intelligence to gain an understanding of adversary behaviors for use in threat detection, including grouping seemingly benign activities into an analytic that can flag potentially malicious behavior.

Understanding the threats to systems managing processes like electric energy and oil production is imperative to creating effective defenses. For customers in the ICS space, deference must be given to ICS-specific activity groups because they carry a specialized risk, similar to a bank being more worried about carders than a cell phone company.

***Note**: Dragos categorizes threats into activity groups. This distinction is necessary because, in the grand scheme of things, it does not matter at the tactical and operational level of security if "Russia is targeting me" as much as "these are the methods and tools actors are using to accomplish their mission" regardless of attribution.*

A current example of this is the activity group XENOTIME, the group behind TRISIS. The group initially targeted SISs in the Middle East, but later pivoted to include companies in North America and Europe. Additionally, XENOTIME recently expanded operations to include targeting ICS vendors and original equipment manufacturers (OEM) as well as electric utilities in North America and the Asia-Pacific region.[11] Knowing what activity groups affect specific verticals is essential and should be included in GRC processes as early as possible and can help drive risk assessments and compliance activities.

To conduct a risk assessment relating to XENOTIME, an organization would identify: the attack vertical and target environment weighed against potential damage. This activity is most concerning to oil and gas companies due to the observed victimology in the Middle East attack and the success of disrupting operations, thus those companies would consider the risk to be higher. However, SISs, OEMs, and ICS supply chain vendors are not unique to oil and gas, and the expanded targeting should concern verticals outside of this industry. Asset owners and operators should focus on relevant industry threats first, and then look at tangential threats to incorporate into risk assessments.

As threat activity expands to include new supply chain or industry targeting, those risk calculuses must change. Another example of changing risk calculuses is ELECTRUM, the group behind CRASHOVERRIDE. ELECTRUM was considered to be a lesser threat to the US because it used the ICS protocol IEC104, which is widely used throughout the European electric grid system. DNP3, which is a protocol used in the US was not part of the CRASHOVERRIDE malware framework. However the malware framework was modular with the adversary able to change quickly; support for DNP3 could be easily added to the CRASHOVERRIDE code, thus expanding its capabilities to target additional regions.

---

[11] XENOTIME Now Targeting Electric Sector
https://dragos.com/blog/industry-news/threat-proliferation-in-ics-cybersecurity-xenotime-now-targeting-electric-sector-in-addition-to-oil-and-gas/

The attack is an excellent case study in the adaptability of transmission attacks across regions and the lack of ability for defenders to be able to defend quickly.

Improving Compliance

Some regulators and lawmakers have codified language around cyber risks in order to lower the risk of catastrophic power loss (NERC CIP),[12] safely operate nuclear power (NRC 10 CFR 73.54),[13] and protect high value chemical facilities (CFATS)[14].

Operators can leverage ICS threat intelligence to meet and exceed compliance mandates by using in-depth reporting, behavioral analytics, and customized responses to improve defensive measures and help prevent a destructive cyber event.

NERC CIP

The electric industry instantiated NERC CIP[15] to protect against catastrophic loss to the power grid following a massive blackout on August 14, 2003 that caused 50 million people to lose power across parts of the US and Canada.[16] Dragos threat intelligence in our WorldView reporting, threat analytics in the Dragos Platform technology, and Dragos Services can satisfy some of the regulatory requirements in the current NERC CIP v6 standards.

Standard	The Dragos Benefit
CIP-007-6 R2: Security Patch Mgmt, 2.1 A patch management process for tracking, evaluating and installing patches must be in place.	The Dragos Platform can be built into the patch management process as an authoritative source. In addition, each WorldView vulnerability report describes in-depth whether a patch actually mitigates an issue, whether there are appropriate workarounds, and often provides more comprehensive advice than the initial reports.

[12] NERC CIP
https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
[13] NRC 10 CFR 73.54
https://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html
[14] Chemical Facility Anti-Terrorism Standards (CFATS)
https://www.dhs.gov/chemical-facility-anti-terrorism-standards
[15] NERC CIP
https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
[16] History of NERC
https://www.nerc.com/news/Documents/History of NERC_January2018.pdf

CIP-007-6 R2: Security Patch Mgmt, 2.2 & 2.3 For applicable patches, an evaluation must be performed to either apply a patch or file/update a mitigation plan.	Applying a patch may not fix an issue or may cause an unsafe device state. Dragos WorldView vulnerability reports provide patching guidance and solutions applicable to ICS environments, and what actions are least likely to adversely affect BES cyber assets.
CIP-007-6 R3: Malicious Code Prevention 3.1 & 3.2 The standards outline methods for detection and remediation of malicious code that may be found on the applicable systems.	The Dragos Platform uses threat analytics to detect signatures and patterns to match malicious behavior. The WorldView offering supplies indicators of compromise (IOCs) and rules to detect known-bad malware and attack patterns that could be happening inside of an ICS network. The indicators exist in the Dragos Platform as well. The Dragos Platform also provides playbooks to help defenders identify and address malicious activities on a system.
CIP-007-6 R4: Security Event Monitoring 4.1 & 4.2 Logs at the BES Cyber System or Cyber Asset levels must be collected for security incidents, including login attempts and malicious code, and alert upon them.	The Dragos Platform can collect these log types and alert upon pre-built analytics as well as ones customized for or by the asset owner.

Standard	The Dragos Benefit
CIP-008-5 R1: Incident Reporting and Response Planning, 1.1 One or more processes to identify, classify, and respond to Cyber Security Incidents.	Inside the Platform are Playbooks which work in conjunction with alerts to guide analysts throughout the triage process.
CIP-008-5 R1: Incident Reporting and Response Planning, 1.4 Incident handling procedures for Cyber Security Incidents.	Dragos can help identify weaknesses or gaps from a tabletop exercise and actual intrusion events.
CIP-008-5 R2: Incident Reporting and Response Planning, 2.1 Test each Cyber Security Incident response plan(s) at least once every 15 calendar months.	Dragos conducts tabletop exercises that can help fulfill the requirement.

CIP-008-5 R3: Incident Reporting and Response Planning, 3.1.1 Document lessons learned from recovery plan.	Dragos can document recommendations for incidents and recovery plans following the completion of a tabletop exercise.

Standard	The Dragos Solution
CIP-009-6 R1: Recovery Plans for BES Cyber Systems, 1.1 Conditions for activation of recovery plan(s).	Scenarios can be tested as part of tabletop exercises where real world incidents are played out for activation of recovery plans.
CIP-009-6 R1: Recovery Plans for BES Cyber Systems, 1.3 One or more processes for the backup and storage of information required to recover BES Cyber System functionality.	Processes can be tested as part of tabletop exercises for recovery of BES Cyber Systems.
CIP-009-6 R1: Recovery Plans for BES Cyber Systems, 1.5 One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.	Processes can be tested as part of tabletop exercises for data preservation.
CIP-009-6 R2: Recovery Plans for BES Cyber Systems, 2.1 Test each recovery plan at least once every 15 calendar months.	Dragos conducts tabletop exercises that can be used to fulfill the requirement.
CIP-009-6 R3: Recovery Plans for BES Cyber Systems, 3.1 3.1.1: Document lessons learned from recovery plan. 3.1.2: Update recovery plan. 3.1.3: Notify people of role changes.	Dragos conducts tabletop exercises that could be used to fulfill the requirement. Dragos can document lessons learned and recommendations for recovery plans and role changes.

Standard	The Dragos Solution
CIP-010-2 R3: Vulnerability Assessments 3.1 & 3.2 At least once every 15 calendar months, conduct a paper or active vulnerability assessment.	Dragos Services team conducts architecture reviews and vulnerability assessments, including on-site visits. The assessments can be used to partially or wholly satisfy the requirement.
CIP-010-2 R3: Vulnerability Assessments 3.4 Document the results of the assessments including action plans for remediation/mitigation of vulnerabilities discovered during activities.	Dragos WorldView industrial intelligence can inform asset owners of possible mitigations to issues. If Dragos personnel find any vulnerabilities during an exercise, we provide mitigations as part of our write-up.

Using Dragos as an authoritative source for required detection and mitigation plans should help satisfy several evidential burdens. Please reach out to intel@dragos.com for further information.

NRC

The Nuclear Regulatory Commission (NRC) regulates civilian use of nuclear materials to protect public health and safety of US citizens. The NRC developed standards for the "Protection of Digital Computer and Communication Systems and Networks" in section 73.54 of NRC regulations 10 CFR. While the document could be used as a licensee's basis for their cybersecurity posture, most of the industry has opted for the Nuclear Energy Institute's "Cyber Security Plan for Nuclear Power Reactors," more commonly known as NEI 08-09,[17] as the standard to be judged against protecting cyber systems at nuclear facilities.

Dragos WorldView intelligence and the Dragos Platform and Dragos Services can be used to assist the licensee in their NEI 08-09 compliance activities. This starts in Section 4 which covers "Establishing, Implementing, and Maintaining the cybersecurity program."

[17] NEI 08-09
https://www.nrc.gov/docs/ML1011/ML101180437.pdf

Standard	The Dragos Solution
3.1.5: Tabletop Reviews and Validation Testing The standard pertains examination of cybersecurity practices regarding the implementation and execution of tabletop reviews and validation testing.	Dragos can run a tabletop exercise to review architecture, defensive strategies, and perform walkdowns.
3.1.6: Mitigation of Vulnerabilities and Application of Cybersecurity Controls This standard helps ensure defense-in-depth strategies are established.	Dragos WorldView and our intelligence analysts can provide alternative control/countermeasures to cybersecurity controls and not impact the licensee's safety.
4.6 (Appendix E7): Attack Mitigation and Incident Response These standards ensure the Safety, Security, and Emergency Preparedness functions of digital assets are not adversely impacted due to cyberattacks.	Dragos assists with Incident Response policy, training, testing, Incident Handling, and can be mobilized to assist the licensee during an incident.
4.8 (Appendix E9): Cybersecurity Training and Awareness This establishes the training requirements for licensee personnel and contractors to perform their assigned duties in implementing security requirements.	Dragos provides specialized cybersecurity training for the OT environment, including incident response.
4.9.1: Threat and Vulnerability Mgmt The standard pertains to the evaluation of threats and vulnerabilities to electronic controls systems and what programs are used to respond to notifications of threat and vulnerabilities from credible sources.	Dragos can be positioned as a “credible licensee-designated external organization" to assist licensees in determining severity and mitigations for emerging threats and vulnerabilities. Dragos reviews ICS-CERT notifications weekly and provides revised severity ratings with remediation recommendations that assist the licensee with establishing risk mitigation plans.
Appendix D, Technical Cybersecurity Controls 1.18: Insecure and Rogue Connections This technical cybersecurity control performs verification during deployment of CDAs, when	The Dragos Platform can identify external connections via baselining and zoning. These can be used to audit rogue connections.

changes or modifications occur to CDAs, and every 31 days for accessible areas, that CDAs are free of insecure (e.g. rogue) connections such as vendor connections and modems.	
Appendix D, Technical Cybersecurity Controls 1.20: Proprietary Protocol Visibility: This technical cybersecurity control ensures alternative controls/countermeasures are implemented to mitigate risk associated with the use of proprietary protocols that create a lack of visibility.	The Dragos Platform dissects multiple proprietary protocols that have been gained through partnerships with vendors. Additional protocols can be added dependent upon licensee requirements.
Appendix D, Technical Cybersecurity Controls 5.1: Removal of Unnecessary Services and Programs This security control documents why applications and networking ports are required for normal and emergency situations.	Vendors may specify more access than required to operate their software and hardware on a regular basis which can leave vulnerable services and ports open. Dragos can provide the licensee hardening guidelines for their process control networks, down to the Safety Instrumented Systems (SIS).
Appendix D, Technical Cybersecurity Controls 5.2: Host Intrusion Detection System This Technical cyber security control establishes, implements, and documents requirements to Host Intrusion Detection System (HIDS).	The Platform can ingest HIDS logs and will not adversely impact licensee's safety, security or emergency preparedness.
Appendix E, Management and Operational Controls 3.4: Monitoring Tools and Techniques This security control applies to monitoring and detecting events and attacks on CDAs, detecting and blocking unauthorized connections, and identifying unauthorized use of CDAs.	The Dragos Platform is able to passively monitor networks and host data for attacks with threat analytics. In this, the licensee will have visibility and monitoring of their networks giving the licensee the ability to respond to any alerts.
Appendix E, Management and Operational Controls 3.5: Security Alerts and Advisories Receiving security alerts, bulletins, advisories, and directives from credible licensee-designated external organizations on an ongoing basis, such	Dragos WorldView Intelligence can be designated by the licensee as a trusted third-party security vendor. In this capacity the licensee can generate new security directives and mitigations based on real world events.

as third party security alert notification services and vendor security alert lists.	

CFATS

According to the Department of Homeland Security (DHS) the Chemical Facility Anti-Terrorism Standards (CFATS) program "identifies and regulates high-risk chemical facilities to ensure they have security measures in place to reduce the risks associated with regulated chemicals." If DHS determines facilities to be high-risk, they are required to meet risk-based performance standards (RBPS)[18]. Additionally, the Chemical Security Assessment Tool (CSAT) provided by the DHS notes facilities are required to describe the body of technologies, processes, and practices designed to protect critical cyber systems from attack, damage, or unauthorized access.

Dragos can specifically assist with RBPS-8 Cyber and provide intelligence, Dragos Services and/or our Platform as an input for several available applicable metrics. The Dragos Platform also fulfills requirements provided by the CSAT documentation,[19] incuding "cybersecurity controls, monitoring, response and reporting." The Platform is able to passively monitor networks and host data for attacks with threat analytics and provide triage information via Playbooks.

Standard	The Dragos Solution
Metric 8.5.2: Network Monitoring (Q3.40.330 Network Monitoring & Q3.40.340 Network Monitoring Log) Networks are monitored in near real-time for unauthorized access or malicious code, with immediate alerts, cybersecurity event logging, daily log reviews, and timely alert response.	The Dragos Platform can identify ICS-specific attacks in control systems and malformed protocol sessions. The platform provides alerts and playbooks for defenders to handle incidents based on identified attacks. The Platform can ingest multiple log types to meet these requirements.
Metric 8.5.3: Incident Response The facility has a defined 24/7/365 computer incident response capability for cyber incidents.	Dragos is able to help support and exercise IR plans through retainer and tabletop exercise.

[18] RBPS Cyber Fact Sheet
https://www.dhs.gov/sites/default/files/publications/rbps-8-fact-sheet-508_0.pdf
[19] CSAT Documentaion
https://www.dhs.gov/sites/default/files/publications/csat-sva-ssp-instructions-508.pdf

Metric 8.5.5: Safety Instrumented Systems (Q3.40.350 Network Monitoring SIS) Facilities have configured Safety Instrumented Systems (SIS) so there is no insecure remote access and cannot be compromised through direct connections to the systems that manage the process the SIS is monitoring.	Dragos has done extensive research into SISs to provide defensive strategies. The Dragos Platform contains baked-in analytics for Triconex SIS activity and analytics on other types of SISs.
Metric 8.8.2: Cyber Asset Identification The facility has identified hardware, software, information, and services and has disabled all unnecessary elements where technically feasible. The facility also has identified and evaluated potential vulnerabilities and implemented appropriate compensating security controls.	This metric can be tackled via multiple avenues. The Platform can meet asset identification requirements, and WorldView intelligence can provide mitigations for potential vulnerabilities.
Metric 11.3: Drills and Exercise The facility plans and conducts security drills and exercises, which are documented and reviewed for lessons learned, on a periodic basis.	Dragos can provide tabletop exercises and penetration tests. Tabletops are required every two to three years and functional exercises every year for Tier 1 and Tier 2 organizations.

Conclusion

GRC needs to be applied at the corporate level, but due to the unique nature of ICS environments and increasing sophistication of threat actors specifically targeting these systems, ICS operators and security teams should be included in the decision-making process at the highest level. Relying on compliance or standard IT practices is not enough.

Companies are required to meet compliance standards and effectively articulate decision-making around security response plans. Buying and implementing piecemeal tools is a not an effective panacea. Comprehensive applications of GRC in ICS environments require a holistic approach using ICS-specific intelligence that can guide actions around real-world scenarios.