GENERAL ELECTRIC COMPANY & DRAGOS, INC

Enabling More Secure Industrial Control Systems

HIGHLIGHTS

- Enhanced threat detection and response to potential ICS threats, attack scenarios and impact through combined technology integration and industrial experience
- Insight into actual malicious tradecraft along with guidance on best practices for defense through shared ICS threat intelligence and analysis
- Holistic joint services to support and train ICS defenders around the world

THE CHALLENGE

Two main challenges facing industrial asset owners and operators today are:

- Limited visibility of industrial control systems (ICS) and the cyber threat landscape
- Lack of experienced ICS cybersecurity professionals to effectively detect and respond

The reduced visibility into ICS exists for a number of reasons: the overall intricacy of engineered systems, complex change requirements, lack of specifications/requirements for monitoring, and limited or legacy technology. While logging and monitoring have been prevalent practices on IT networks the limited information available for OT networks reduces operators' ability to fully understand their environment while detecting any threat behavior that may be present.

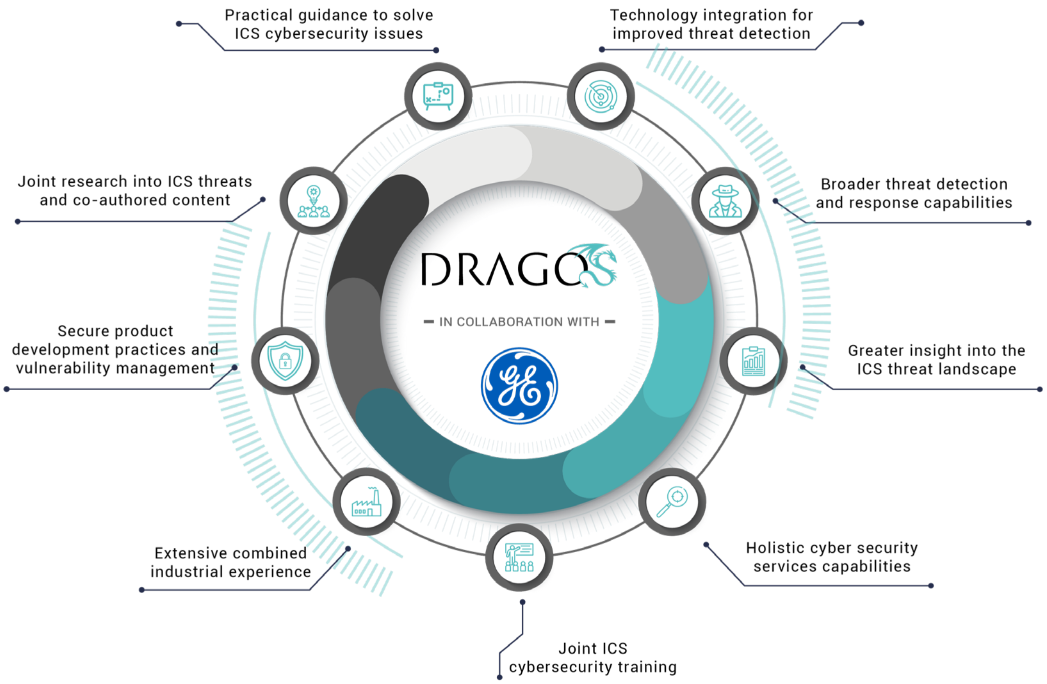
The general shortage of professionals that have both a good understanding of industrial systems and cyber security best practices working in this space has also been a contributing factor.

Furthermore, drivers such as IIoT and Industry 4.0 have led to increased digitization and interconnectivity in OT systems enabling benefits such as data analytics to improve OEE (Overall Equipment Effectiveness) and maintenance capabilities. This increased interconnectivity and digitization has also expanded the attack surface that can be leveraged by adversaries for malicious intent.

The risks and the consequences of ICS threats have never been greater. This was highlighted recently by the TRISIS malware targeting SIS (Safety Instrumented Systems), and the physical impact of any malicious behavior on ICS can be catastrophic.

SOLUTION OVERVIEW

The Dragos and GE collaboration empowers joint customers and the greater ICS community with more comprehensive ICS threat detection capabilities, through technology and experience. The collaboration is available to all GE business units globally. The collaboration enables more effective ICS defenses, with deep insight into the ICS threat landscape through:


Practical guidance to solve ICS cybersecurity issues
Technology integration for improved threat detection
Joint research into ICS threats and co-authored content
Broader threat detection and response capabilities
DRAGOS
IN COLLABORATION WITH
Secure product development practices and vulnerability management
Greater insight into the ICS threat landscape
Extensive combined industrial experience
Holistic cyber security services capabilities
Joint ICS cybersecurity training

TECHNOLOGICAL INTEGRATION:

With the Dragos' ICS threat detection and response platform's utilization of GE's extensive industrial operations information and experience, customers gain comprehensive insight into the ICS threat landscape and improved capabilities to detect and respond to industrial cybersecurity threats.

COLLABORATIVE ICS-SPECIFIC THREAT RESEARCH:

Joint research into the tactics, techniques & procedures (TTP's) of adversaries combined with ICS impact analysis improve detection and response. The results from Dragos' and GE's experienced industrial teams are shared via jointly-authored whitepapers, webinars and reports to ensure customers and the community have practical guidance to strengthen ICS defenses.

ENHANCED DETECTION AND RESPONSE CAPABILITIES:

Threat detection guidance shared through investigation playbooks provide step-by-step guidance throughout the response process to reduce mean time to recovery (MTTR). If supplemental support is needed during an escalated cyber incident, Dragos' & GE's incident response teams are available.

ICS THREAT INTELLIGENCE SHARING:

IT threat intelligence gathering and sharing has been a key function for security teams working in IT security. Dragos and GE's sharing and analysis of OT/ICS specific threat intelligence helps security teams gain insight into OT/ICS adversary trends and behaviors to enable improved defenses against malicious tradecraft.

AUGMENTED SERVICES OFFERINGS:

Customers can utilize GE's extensive industrial experience combined with Dragos' threat detection and incident response experience to access best in class support for their needs and requirements.

TRAINING & GUIDANCE:

Content and classes enable the next line of defenders to improve OT security capabilities in both detecting and responding to threats throughout the plant. Please refer to the initial whitepaper in the series "*Design and Build Productive and Secure Industrial Systems*".

FEATURES & BENEFITS

FEATURES	BENEFITS
TECHNOLOGY INTEGRATIONS	Protocol dissectors, device characterizations and threat behavior analytics improve overall visibility of GE systems while enabling improved detection of ICS threats.
THREAT RESEARCH	Experienced teams identify new attack vectors and attack scenarios on GE systems which are shared with the community through new detection tools, playbooks, and papers that provide specific guidance on how to respond.
ICS THREAT INTELLIGENCE SHARING	Collectively gathered intelligence enables experienced analysis of threats and tradecraft targeting GE technology thus enabling defenders to improve detection and defense capabilities.
AUGMENTED SERVICES	Combining GE's extensive network of support services with Dragos' specialist threat detection and incident response teams improves MTTR in the wake of a cyber event.
TRAINING	Knowledge sharing between the experienced GE and Dragos teams is made available via content, workshops and training classes that further improve customer awareness and ability to detect and respond to ICS threats.