PARTNER BRIEF

DRAGOS and ISA GLOBAL CYBERSECURITY ALLIANCE

Helping Defenders of Industrial Automation Against OT Threats

HIGHLIGHTS

- The **GCA** leverages a wide range of **OT cybersecurity** experience to help grow and strengthen the global community.
- As a **founding member, Dragos** shares the relevant and extensive domain expertise in detecting and responding to OT threats and behaviors.
- **Dragos** will help lead the advancement of cybersecurity awareness, education, readiness, and knowledge sharing with the broader OT defender community.

THE CHALLENGE

Owners and operators of industrial control systems (ICS) across various industries have a responsibility to ensure safe and reliable operations. Conversely sophisticated adversaries are actively targeting ICS using cyber-attacks as an effective means to not only steal intellectual property but to also impact and disrupt systems that could lead to physical damage and/or loss of life. This puts increased pressure on various ICS stakeholders such as leadership, engineering, security specialists, vendors etc. to ensure readiness with sufficient hardening, detection and response mechanisms to neutralize the threat and reduce overall business risk.

In addition, there is typically limited sharing of attack details across different organizations, vertical markets, geographies etc. This limits how many details defenders are able to obtain to learn more about potential adversaries and their actions from previous events. Details such as who and what has been targeted, where it was targeted and how it was targeted for example TTP's (Tactics, Techniques and Procedures) can provide valuable threat intelligence that defenders can learn from to improve readiness.

Finally, while standards and guidelines exist to help increase general awareness and guide defenders of ICS to apply industry recognized best practices, effective standards can still be somewhat challenging to navigate and to apply in unique environments with different levels of expertise and experience.

THE SOLUTION

The International Society of Automation (ISA) is a global, non-profit organization primarily responsible for developing industrial standards & providing training and certification. Many in the industrial cybersecurity realm recognize ISA for the industrial-focused cybersecurity standard ISA99 which later evolved into the ISA/IEC 62443 standards. In 2019 ISA created the Global Cybersecurity Alliance (GCA) to continue to advance education, readiness, and knowledge sharing in manufacturing and critical infrastructure. The Alliance brings together the expertise and experience across end-user companies, automation and control systems providers, IT infrastructure providers, service providers, system integrators, government and other cybersecurity stakeholder organizations together to proactively address growing threats.

Dragos joined the ISA GCA as a founding member to support the objectives of the alliance by providing our extensive experience and insight that will be shared with the greater community. The Dragos WorldView that intelligence team can contribute valuable insights based on real-world adversary activity to help prepare defenders and the Dragos professional services team can contribute knowledge, lessons learned, and best practices to help arm defenders with the skills to detect and respond to threats targeting OT environments.

Projects managed by the ISAGCA membership are organized into four working groups: Awareness & Outreach; Compliance & Prevention; Education & Training; and Advocacy & Adoption. These working groups include experts from member organizations that collectively work on the following projects:

- Easy-to-follow, a condensed guide to implementing the ISA/IEC 62443 series of standards.
- Roadmap for expanded cooperation with worldwide governments that are currently referencing the standards in their regulatory requirements or recommended practices.
- Multi-dimensional reference guide mapping system lifecycle phases and stakeholder roles to specific industrial cybersecurity knowledge, skills, and abilities needed for each phase.
- Database of speakers with expertise and experience in automation cybersecurity targets for a number of threat actor groups, who aim to surveil and potentially disrupt mission-critical systems, which can have tremendous financial, operational, and business impacts.

BENEFITS and IMPACT

BENEFITS	IMPACT
Expanded Community Contributions	Leveraging real-world ICS cybersecurity experience and intelligence to provide knowledge sharing, education, and improved standards in an open environment to help build a stronger ICS-focused cybersecurity community.
Improved ICS Cybersecurity Priorities	Support the adoption and implementation of a more complete set of ICS cybersecurity priorities from manufacturers, software providers, service companies, government agencies, and end-users.
Extended Visibility	Providing assistance with the development and effective communication to a large audience of timely and relevant educational material regarding the ICS threats and standards-based defensive strategies that ensure people, processes, and technology are better cyber protected.
Enriched Training Services	Developing certification and education programs for industry professionals with sensible approaches that work with world governments and regulatory bodies.

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