PARTNER BRIEF

DRAGOS and THE CHERTOFF GROUP

Cybersecurity Risk Advisory Services and Technology for Industrial Organizations

HIGHLIGHTS

- **The Chertoff Group** provides strategic guidance on building effective, risk-based cybersecurity programs. **Dragos** provides expert services and technology to understand industrial risks and build effective technical controls.
- **Together we enable enterprise security risk management** across the converged enterprise (IT) and operational technology (OT) environment with expert advisory services and technology.
- **Our joint approach** applies proven methodology from The Chertoff Group to address unique industrial risks and leverages the industry leading Dragos Platform, ICS threat intelligence, and proactive & responsive cybersecurity services.

THE CHALLENGE

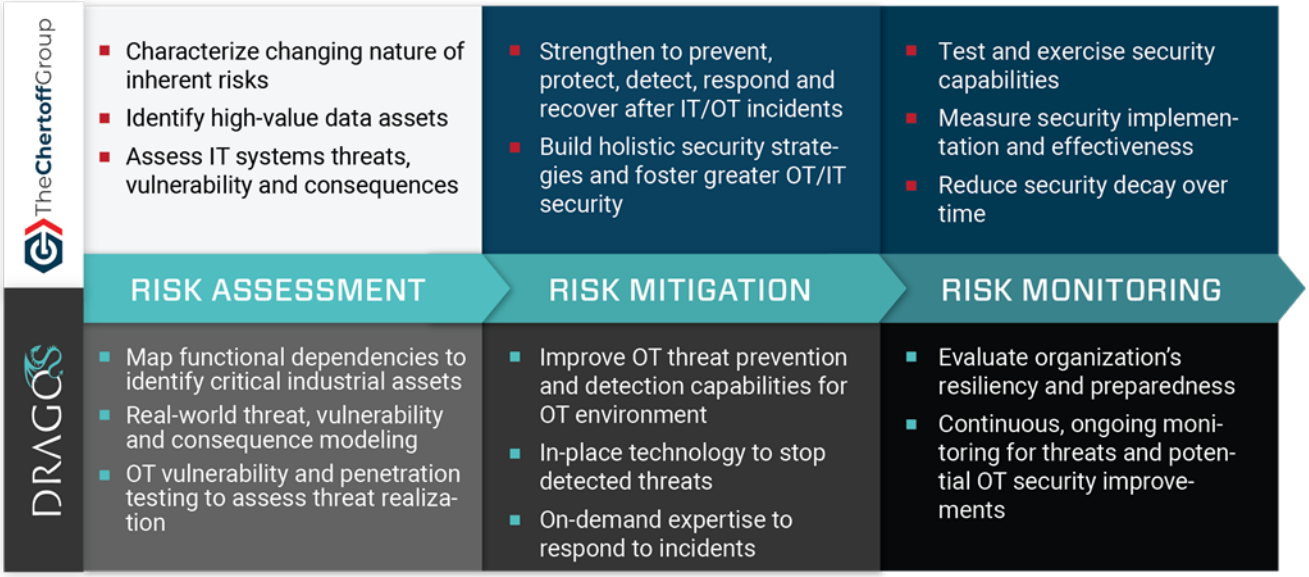
Many industrial organizations are rapidly embracing digital transformation by connecting their enterprise (IT) and operational technology (OT) networks – this convergence enables innovative new offerings; improves customer support; and enhances the safety, responsiveness and productivity of their operations, but it can also heighten security risk.

Why? Critical infrastructure organizations—including industrial organizations in the power (electric and oil & gas), manufacturing, and transportation sectors—are attractive 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.

Without proper security planning, convergence not only expands the attack surfaces within ICS environments, but can also result in physical consequences.

To manage this risk, industrial organizations must consider interdependencies between their IT and industrial control systems (ICS)/OT environments as part of a holistic enterprise security risk management strategy.

JOINT RISK MANAGEMENT APPROACH



DRAGOS-CHERTOFF GROUP CONVERGED APPROACH EXPERIENCE – EXAMPLE PROJECTS:

Threat Environment Analysis for Major Electric Utility

- Built client-specific threat model including likelihood and capability descriptions based on Dragos threat intelligence.
- Supplemented analysis with open-source and "Dark Web" analysis to determine potential adversaries.
- Used threat intelligence and threat modeling to prioritize defensive recommendations.

Operational Technology Threat Assessment for Mining Firm

- Evaluated operational security capabilities for a manufacturing facility, including but not limited to:
  - Assessing connection to OT systems from IT systems.
  - Vulnerability and penetration testing of onsite systems.
  - Development of threat scenarios and mitigation recommendations.

Cyber Risk Strategy for Transportation Sector Client

- Developed cybersecurity strategy covering safety-critical, mission-critical, and business-critical systems for a regional rail client.
- The strategy includes an initial risk register, needed capabilities, OT/IT success metrics and measures, and model contract language for vendors.

Threat Analysis and Risk Management for Global Airline

- Based on the Chertoff-Dragos team's understanding of threats to specific industries, created threat briefings for the airline's senior security leaders.
- Provided both strategic & worldview and operational & technical pictures of the threat environment the client was operating in and potential impacts to business objectives.

To fully address the enterprise security risk management needs, industrial organizations—from the board and C-suite to plant management and engineering—must be able to answer the following questions confidently:

- How would a motivated adversary attempt to disrupt our industrial operations?
- What are the industrial and operational assets critical to keeping our business functioning?
- What are the potential cyber threats to those critical operational assets?
- Are we capable of detecting and responding to those threats before they have an adverse impact on our business?

Successful enterprise security risk management in this rapidly evolving threat environment requires a multi-disciplinary approach across the entire organization, including enterprise risk management, physical security, IT and OT cybersecurity, process control, and engineering.

Through our joint offering, we help forward-thinking industrial organizations manage risk by providing deep industrial security and ICS-focused experience along with the equally deep enterprise security experience to build cybersecurity risk management capabilities across the entire organization.

THE SOLUTION

Your converged enterprise (IT) and production (OT) environment requires a comprehensive enterprise security risk management approach. The Chertoff Group and Dragos have teamed up to assist you in addressing the complete range of business-related security risks to achieve greater resiliency and advance the safety, responsiveness, and productivity of your operations.

- Address your industrial cyber defense needs comprehensively with enterprise risk management services from The Chertoff Group in conjunction with the unique and specialized ICS threat detection and response technology and services from Dragos.
- Leverage strategic guidance from The Chertoff Group on how to structure and build strategic, risk-based cybersecurity programs
- Gain an in-depth understanding of technical risks and build effective technical controls with technology and expert services provided by Dragos.
- Apply a threat-oriented and consequence-driven approach to prioritize and address real-world risks and better secure your ICS operations with appropriate technical, process, and human-centered countermeasures.

Dragos and The Chertoff Group are fluent in the key languages required in the industrial environment— from the board and management level to operators and plant managers—to successfully implement and manage cybersecurity best practices. The Chertoff Group is a premier global advisory firm, founded in 2009 by former Secretary of Homeland Security Michael Chertoff, that helps clients understand, manage and communicate about security risk. We apply our insights into technology, threat, and policy to help our clients improve their resiliency, build competitive advantage, and accelerate growth. Dragos was founded in 2016 by former members of the intelligence community who specialize in hunting and responding to national threats to industrial infrastructure and building the tools to combat them.

The Chertoff Group's enterprise risk management approach works in conjunction with the unique and specialized OT threat detection and response technology and services from Dragos to thoroughly address the client's industrial control system (ICS) cyber defense needs.

> "We are excited about the Chertoff – Dragos partnership that helps us ensure best-in-class safety and security in our systems through a converged OT/IT cyber risk management assessment."
>
> - Lori Willox, Chief Financial Officer of Texas Central Railway

THE JOINT APPROACH

Together, Dragos and The Chertoff Group bring a differentiated approach to your industrial cybersecurity. We begin by fully understanding your business objectives and then design an effective security program for your converged IT and OT environment to support and advance those objectives. We do this by:

Using Dragos industrial threat intelligence, and the risk assessment methodology developed by The Chertoff Group, the team works closely with your safety and security teams to:

1) Assess the criticality of OT and IT infrastructure to business operations.
2) Identify likely threat adversaries seeking to cause harm and build plausible cyber threat scenarios.
3) Understand the potential impact and consequences of an industrial attack.
4) Map threat scenarios to current-state defensive countermeasures and identify potential vulnerabilities and OT-IT connectivity.
5) Apply diagnostics to evaluate whether countermeasures are operating as intended.
6) Develop business case justifications for incremental investments in people, process and technology.

BENEFITS and IMPACT

BENEFITS	IMPACT
Improved Risk Management	Combines The Chertoff Group's proven cyber risk services with the industry-leading Dragos Platform, ICS threat intelligence, and proactive & responsive services – to improve enterprise security risk management and resilience of converged industrial IT and OT networks.
Comprehensive ICS Security	Provides industrial organizations with comprehensive ICS-focused services and technology to seamlessly address risk response and mitigation across the converged environment – to save time and resources while reducing the impact of threats.
Real-World, Proven Approach	Leverages a threat-oriented and consequence-driven approach to help industrial organizations prioritize and address real-world issues – to better secure ICS operations with appropriate technical, process, and strategic countermeasures.
Joint Services Agreement	Covers the spectrum of enterprise security risk management for industrial organizations under one services agreement – to engage proven expertise for proactive services across the entire converged environment.

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