INCIDENT RESPONSE RETAINER

OVERVIEW

Dragos and Rockwell Automation have partnered to offer a joint Incident Response Retainer (IRR) to help industrial organizations prepare for, respond to, and recover from cyber incidents. Our team of experienced incident responders can create a tailored strategy that allows you to quickly mitigate incidents and get back to business.

DRAGOS AND ROCKWELL AUTOMATION

Industrial Strength Incident Response

There's no question we live in the "Not if, But When" era of cybersecurity incidents. We're more connected than ever, and as organizations continue to look for operational efficiencies, there is more interconnectivity between enterprise and industrial networks than ever before.

Protecting industrial infrastructure is imperative. It's also true that building and maturing an effective OT cybersecurity program requires long-term investments in resources and expertise that many organizations just don't have the budget or experience to build.

And while there's no replacement for having a dedicated OT cybersecurity team, having access to a world-class team of ICS cybersecurity experts and field service engineers provides you with critical support so that you can quickly investigate, respond to, and recover from incidents as rapidly as possible.

INTELLIGENCE-DRIVEN

Dragos expertise backed by intelligence gathered on adversary tactics, techniques, and procedures (TTPs)

REDUCE MEAN TIME TO RECOVER

A tailored IR strategy allows you to quickly mitigate incidents and get back to business

ICS KNOWLEDGE TRANSFER

Learn directly from our team's expertise, best practices, and first-hand experience responding to critical incidents globally

HOW IT WORKS

Dragos Incident Response Service plans are based on prepaid retainer hours with specific response time service level agreements. Maximize the value of an IRR by burning down retainer hours on any service. Formally assess and understand your organizational maturity, or explore adversary TTPs and the specific ways that they might target your organization.

DRAGOS INCIDENT RESPONSE RETAINER

24/7 HOTLINE	✓
CONTACT ESTABLISHED WITHIN	8H
ENROUTE WITHIN	48H
READINESS ASSESSMENT	✓
PROACTIVE PREP & PLANNING	✓
POST ENGAGEMENT REPORTS	✓

FLEXIBLE RETAINER HOURS

Burn down prepaid retainer hours on any Dragos Service. Architecture Reviews are a great way to develop a preliminary understanding of the existing network and security posture of your OT environment, in relation to your protection, detection, and response capabilities.

ARCHITECTURE REVIEWS

EVALUATE YOUR EXISTING CYBERSECURITY PROGRAM

OBJECTIVES	COMPROMISE ASSESSMENT	ARCHITECTURE REVIEW	OT PROGRAM ASSESSMENT
PROGRAM REVIEW			✓
COLLECTION MANAGEMENT FRAMEWORK			✓
CROWN JEWEL ANALYSIS			✓
TOPOLOGY REVIEW		✓	✓
STANDARDS & REGULATIONS REVIEW		✓	✓
INDICATORS OF COMPROMISE SWEEP	✓	✓	✓
THREAT DISCOVERY	✓	✓	✓
ASSET INVENTORY	✓	✓	✓
ASSET VULNERABILITY ASSESSMENT	✓	✓	✓

PROGRAM REVIEW

Review of policies, procedures, and organizational structure around network security. Corporate and site plans also may be evaluated for consistency and completeness

COLLECTION MANAGEMENT FRAMEWORK

Document and institutionalizes data sources, outlining the what, where, how, and how long

CROWN JEWEL ANALYSIS

Identify primary assets and network locations where process disruption is most impactful to the organization, and analyze consequences

TOPOLOGY REVIEW

Evaluate industrial network segments to identify cybersecurity weaknesses and get recommendations to strengthen architecture and systems

COMPROMISE ASSESSMENT

Utilize the Dragos Platform to analyze asset maps, IOCs, threat behaviors, asset and protocol vulnerabilities, insecure credentials and more

To learn more about our Incident Response Retainer and other Professional Services, please contact sales@dragos.com or visit dragos.com/services

Copyright © 2022 Dragos, Inc.
All Rights Reserved

Last updated May, 2022