

JOINT INCIDENT RESPONSE (IR) RETAINER FOR ENDPOINT AND INDUSTRIAL CONTROL SYSTEMS (ICS) ENVIRONMENTS

CROWDSTRIKE SERVICES HELPS ORGANIZATIONS PREPARE FOR AND RESPOND TO BOTH ICS AND ENDPOINT THREATS

The ICS threat landscape is still substantially uncharted, making timely and effective incident response all the more challenging. As the need for ICS incident response increases, CrowdStrike® provides services that help organizations respond to and protect against these damaging threats. Experience is the key factor in effectively responding to an ICS security breach, which is why CrowdStrike is partnered with Dragos, renowned ICS cybersecurity experts, to help organizations prepare for and respond to ICS threats 24x7.

The situation can be chaotic with an ICS breach because often the operational technology (OT) staff may have little experience with cybersecurity and the IT staff may have insufficient experience with ICS breaches. These factors can lead to protracted resolution times, which can have serious safety, financial and reputational consequences. CrowdStrike and Dragos bring the expertise required to prevent, assess and respond to endpoint and ICS threats and meet the needs of both IT and OT teams.

CrowdStrike offers retainer options that provide a “one-stop shop,” allowing an organization to quickly and effectively respond to and prevent threats targeting both endpoints and ICS.

CROWDSTRIKE SERVICES FOR ENDPOINT AND ICS PROVIDES THE FOLLOWING BENEFITS TO IT AND OT TEAMS:

Provides an elite team of cybersecurity experts on standby to deal with any suspected endpoint or ICS incidents

Ensures the services of experienced threat responders, as well as proven endpoint and ICS threat intelligence and advanced threat detection and response tools

Provides in-depth domain knowledge of ICS/OT

Delivers a wide range of incident response and proactive offerings focused on securing ICS

Offers flexible retainer options for protecting both endpoints and ICS assets

JOINT INCIDENT RESPONSE (IR) RETAINER FOR ENDPOINT AND INDUSTRIAL CONTROL SYSTEMS (ICS) ENVIRONMENTS

KEY CAPABILITIES

1. FLEXIBLE RETAINER OPTIONS

- CrowdStrike provides IR services that span both ICS and endpoints to ensure your organization is prepared to secure and protect its key IT and operational assets.
- You are ensured access to a 24/7 incident response hotline.
- During the period of the retainer, if your organization hasn't needed CrowdStrike IR services, the remaining value can be applied to a wide range of proactive services covering both ICS and endpoint assets.

2. ADVANCED THREAT DETECTION AND RESPONSE TOOLS

- The CrowdStrike Falcon® platform offers instant visibility, response and protection across the enterprise and prevents attacks on endpoints on or off the network.
- The Dragos Platform compiles and correlates ICS security events at a scale and speed that allows human experts to uncover even more insights.

3. DOMAIN KNOWLEDGE AND INTELLIGENCE

- CrowdStrike is acknowledged as a the leader in cloud-delivered endpoint protection solutions and IR and proactive services.
- Dragos has emerged as one of the industry's most trusted IR teams, applying expert human intelligence and threat behavior analytics to redefine industrial ICS cybersecurity.
- CrowdStrike and Dragos have the combined enterprise and industry intelligence capable of enhancing ICS cyber solutions and services, driving much needed operational context about cyber threats for more effective protection for ICS and endpoint devices.

ABOUT CROWDSTRIKE

CrowdStrike is the leader in cloud-delivered endpoint protection. The CrowdStrike Falcon® platform offers instant visibility and protection across the enterprise and prevents attacks on endpoints on or off the network. Falcon seamlessly unifies next-generation antivirus (AV) with best-in-class endpoint detection and response (EDR), backed by 24/7 managed hunting. There's much more to the story of how Falcon has redefined endpoint protection but there's only one thing to remember about CrowdStrike: We stop breaches.

Learn more at

www.crowdstrike.com

Email: services@crowdstrike.com

KEY DIFFERENTIATORS

Domain Knowledge:

Seasoned experts focus on preventing, assessing and responding to ICS/ SCADA cyber incidents to improve visibility into and protection against the broad range of threats that impact infrastructures with both networked endpoint and ICS devices. This includes Manufacturing, Logistics/ Distribution, Energy/Utility and other verticals.

Experience and Expertise:

The CrowdStrike Services team comprises "the best of the best" from the world of cybersecurity, incident response, forensics and operations. This elite team draws on decades of expertise and experience working for leading law-enforcement, government, private and consulting organizations.

Flexibility and Comprehensiveness:

CrowdStrike offers retainer options that give you the flexibility to engage both proactive and IR services as you need them. During the period of the retainer, if your organization has not needed CrowdStrike IR services, any remaining value can be used for an extensive range of proactive services.

IR Speed and Precision: This service provides advanced technology and tools that are easy to deploy and provide detection and visibility into ICS and endpoint assets and activity. They deliver threat behavior analytics, pinpoint malicious behavior and include threat intelligence for the context and tools you need to respond to attacks with speed and confidence.