OT Cybersecurity Consulting Services

OT Emergency Incident Response Retainer

Ensure Your Cyber Resilience in Industrial Production Networks.

Not if. When.

Breaches can, do, and will happen. There is ample evidence of this. Whether it is a targeted attack against an OT network directly, or whether it is something that is initiated through the IT network that then spreads, incident scenarios involving the OT domain are of paramount concern.

No matter the investment in preventative measures, no organization can consider itself impervious to a breach.

But you only need one phone number: **+45 31 35 95 69**.

A trusted Partner is a must have.

When there is an emergency triggered by a breach, you need to know whom to call, you need to know what will happen next, and you need to trust that you are in the expert hands of a trusted and experienced partner that will guide you through the process of addressing the chaos and returning to order through a thorough technical investigation to identify the root causes, and a robust resolution.

Further, hackers do not operate on a '9 to 5' schedule. On the contrary, most targeted attacks occur outside normal office hours to minimize detection. Because of that, you need to have a partner that is truly available 24x7x365.

Genuine depth of OT and IT experience.

Finding great talent in IT Emergency Incident Response is already a significant challenge. OT Emergency Incident Response is an even scarcer resource. Companies that can deliver both capability sets in an integrated manner are few and far between. CSIS, through its partnership with ICS Range, stands out from the crowd.

Phone: +45 88 13 60 30 www.csis.com

You have an OT cyber emergency? We respond.

Emergency Incident Response case types covered by our Retainer, though not limited to, will typically include one or more of the following:

- **Man-in-the-Middle (MitM) Attacks:**
  Interception of communication between devices, enabling unauthorized access or manipulation.
- **Insider Threats:**
  Malicious actions or negligence by individuals with authorized access to the OT environment.
- **Behavior-based Anomalies:**
  Industrial network protocols are predictable in pre-defined flow patterns and any deviations could potentially indicate an incident.
- **Supply Chain Attacks:**
  Compromising the security of components or software before they are integrated into the OT system.
- **Zero-Day Exploits:**
  Leveraging vulnerabilities that are unknown to the vendor or have not yet been patched.
- **Data Integrity Attacks:**
  Manipulating or corrupting data within the OT system, leading to incorrect or unsafe operations.

The services covered by our Retainer:

- Non-intrusive (passive) remote analysis of the industrial network to establish its current state and identify possible indications of compromise.
- Guidance on the case processes, acting as a case-handler.
- Guidance on case containment to avoid further compromise.
- Investigation to provide answers as to what, when, and how the incident occurred.
- Documentation of findings in a report, uploaded to the CSIS Threat Intelligence Portal.
- Provision of recommendations on what should happen next based directly on the investigation.

The service package that is aligned to your needs.

The OT Emergency Incident Response package includes the following services:

Emergency Incident Response Retainer Package	
Support Hotline	24/7/365
Incident response start-up*	<4 hours
Discount on Incident Response hours	15%
Threat Intelligence Portal Access	Free of charge
Incident start-up fee	Free of charge
Quarterly Threat Landscape Webinars	Free of charge
Onboarding 2-Day Workshop	Upon Onboarding

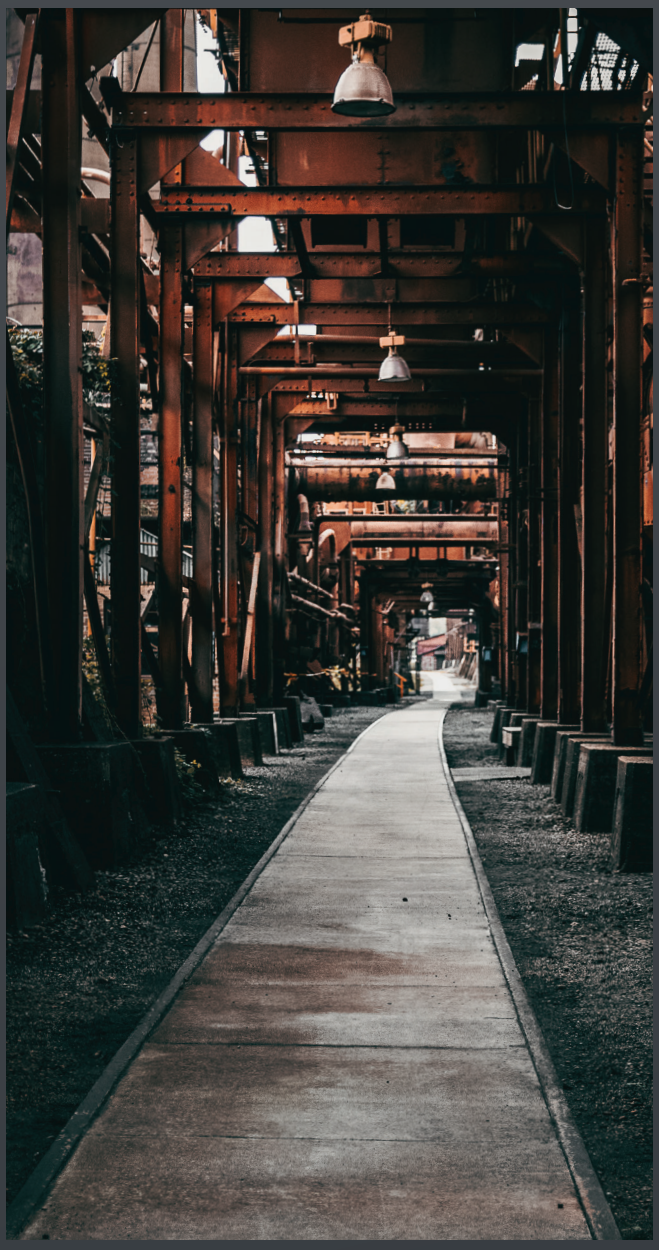
*From PCAP data having been successful uploaded in our Threat Intelligence Portal (TIP).

Threat Intelligence Portal

Our Threat Intelligence Portal (TIP) is the platform through which we handle your Emergency Incident Response Retainer, including services such as webinars and past emergency incident response cases. It provides a central repository and audit trail of all communication and information exchange.

Threat Landscape Webinars

Delve into anonymized insights derived from real-world incidents, providing valuable glimpses into emerging threats and trends. Stay ahead of the curve with our expert breakdown of the OT threat landscape, equipping you with the knowledge needed to fortify your defenses and navigate the evolving cybersecurity terrain. Don't miss out on this opportunity to enhance your understanding and proactive response in the realm of operational technology security.



OT Onboarding Workshop

In this onboarding workshop, we meticulously assess your existing emergency incident response plans, reviewing, and enhancing them to meet the distinctive challenges of the OT landscape. They contribute valuable insights, ensuring your plans seamlessly align with best practices.

Furthermore, other relevant information is covered off during the workshop, including:

- Network drawings, applicable IP ranges and equipment vendors.
- Network devices and any associated security systems.
- Leadership and department contacts, and internal escalation procedures.
- Potential special requirements on PPE (Personal Protective Equipment).
- Any other unique elements pertinent to your OT environment.

As a final step, you will be guided through the technical process of capturing network traffic and extracting essential PCAP files—an imperative initial phase for launching an emergency incident response investigation.

This workshop lays the groundwork for a robust and customized approach to fortifying your OT landscape, ensuring resilience and security in the face of evolving threats.

CSIS is your partner for OT cybersecurity services.

20+ years of cybersecurity experience.

Roster of blue-chip customers covering IT and OT domains.

Tried and tested methodologies.

Cyber intelligence backbone.

Strategic partnership with ICS Range (https://icsrange.com).

Phone: +45 88 13 60 30 www.csis.com