Retainer service

OT Cyber Incident Response

Protecting people, productivity and profits

Evolving cyber threats require unified Incident Response

Threats are moving deeper into OT environments, targeting lower-level systems where visibility is limited and response capabilities are rare. 70% of vulnerabilities are reportedly found below Purdue Level 3.5, in the core of industrial operations.

Few providers can respond to attacks across both IT and OT domains. That's why NCC Group and Dragos have joined forces - combining leading IT & OT cyber expertise and threat intelligence to deliver end-to-end incident response. When systems go down, the impact is immediate: lost revenue, downtime, reputational damage, and in industrial sectors, real-world safety risks.

A specialist OT & Cyber Incident Response Team (CIRT) is critical to contain threats fast and restore Industrial operations. Building this capability in-house can be costly and complex. Our integrated solution with Dragos gives you the resilience you need, without the overhead.

#1
Industrial organisations experience the highest volume of incidents (2023 & H1 of 2024)

$2M
average cost of breaches caused by phishing

73%
of OT devices are estimated to be "unmanaged"

Working with NCC Group

To effectively respond and mitigate the impact of cyber incidents in both industrial and corporate IT environments, organisations must prioritise cross-functional planning and preparedness activities that address the unique challenges of OT systems and their integration with enterprise IT resources.

Having instant access to incident response expertise is now becoming a vital cost of doing business. Through our partnership with Dragos, we can offer Operational Technology Incident Response support in addition to our Bronze, Silver and Gold Retainer packages.

This includes onsite support within 48 hours in UK, EU, North America and APAC alongside an additional 40 hours of pre-paid budget for Incident Response which can be used specifically for OT support.

Key benefits

- Full onboarding
- 40 hours of OT support from Dragos
- Global Incident Response staff on standby 24/7 to support remote or onsite
- Choose one OT Incident Readiness service in addition to your IT options:
  - OT Tabletop Exercise
  - OT Incident Response planning workshop

Proud to be partnered with DRAGOS

Key retainer steps for enhanced breach security

01

Detailed onboarding will ensure that we have all of the key information that we need to ensure that we can respond as quickly and efficiently as possible in the event of a breach.

02

Rapid response is the core component of an Cyber Incident Response Retainer. Our emergency hotline is staffed 24/7, 365 days a year, giving you direct access to our incident responders.

03

Throughout the duration of the Retainer, you will have the option to access First Responder Training and other Proactive IR Readiness services to ensure that your organisation is as prepared as possible for a breach.

04

If a breach occurs, we will provide either remote or onsite support across both IT and OT environments as required, with the support of Dragos, addressing the issue and returning your organisation to usual operations as quickly as possible.

Our IT and OT experts will swiftly support clients with data collection and analysis, containment and eradication of the threat, recovery and post-Incident activities, including root cause analysis.

05

We will provide a detailed report of our findings and a check-in during the days following any Incident

Start your OT cyber security journey here

- Access expert IT, OT Architects & Service resources; IT & OT expert industrial architects, technical testers, analysts, threat hunters, & responders to help you defend your facilities.
- Leverage both NCC Group and Dragos threat intelligence gathered globally with a mission to improve industry skills, communications, & resources to strengthen critical infrastructure of every countys.
- Technology enabled by Dragos for the most effective OT Security Platforms for visibility into OT assets, vulnerabilities, traffic, and threats to reduce risk.

Contact one of our experts to discuss a Cyber Incident Response retainer for IT & OT in more detail.
If you require emergency assistance please contact the Incident Response Hotline which can be found on our website homepage

+44 (0) 331 630 0690

Get in touch

ncc group