

SERVICE AND CAPABILITIES

CYBER

INDUSTRIAL CYBER SECURITY

Enabling Industry to build and maintain cyber resilience
for the connected operational enterprise of tomorrow

CAPULA

THE CHALLENGES

As technology continues to evolve at an unprecedented pace many businesses are embracing these developments to help enhance their operations in order to deliver greater efficiency, optimise their assets and improve safety and sustainability. However, these enhancements are bringing with them a raft of security challenges.

New Layers of interconnectivity

Industrial enterprises are investing in technologies that accelerate change. This digital age is increasingly connecting systems to help enhance agility, resilience and give businesses the space to innovate. These digital environments blur the traditional boundaries that existed between information and operational technologies (IT/OT), and where this separation previously prevented cyber threats, these smarter systems are resulting in a higher degree of risk but equal opportunity.

Rise of threat actors

Cyber-attacks on critical and industrial infrastructure are on the rise, they include foreign states, criminals, “hactivist” groups and terrorists. According to the annual IBM X-Force® Threat Intelligence Index*, Operational technology (OT) attacks have surged 2,000% year-over-year.

Failure destroys brand reputation

The cyber threat and possible impact it can have on critical infrastructure and operations has placed an even greater board level focus on OT security. Failure to manage or mitigate such threats is well understood to have significant impact on reputation as well as shareholder value.

Increasing pressure

Industrial businesses are being pressured from multiple angles to take advantage of new technologies whilst maintaining cyber resilience. For companies managing these OT environments this is resulting in a number of concerns and challenges.



COMPLIANCE &
REGULATION



SHORTAGE
OF SKILLS



MANAGING LEGACY
EQUIPMENT



DISRUPTION
TO OPERATION



CONSTRAINED
RESOURCE



WE HELP BUSINESSES IMPROVE THEIR CYBER RESILIENCE THROUGH OUR INDUSTRY ALIGNED HOLISTIC APPROACH TO CYBER SECURITY.

OUR HOLISTIC APPROACH

There is no single product, technology, or methodology that can fully secure OT environments. A multi-faceted, holistic approach is required to address the varying (and increasing number of) threats. Following a security framework can help guide organisations into such a holistic approach.

Building on decades of experience supporting critical infrastructure, our services and solutions are closely aligned to the NIST framework, often seen as the gold standard for preventive security measures. This framework aligns to our recommended approach to optimise and maintain security practices in keeping businesses safe. However, no matter what regulation, compliance or industry standard you adhere to, our services can be aligned to in accordance. We commonly help businesses align to:

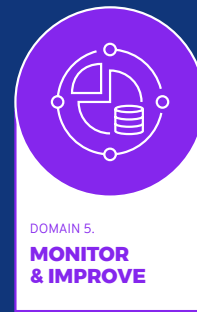
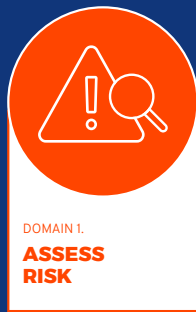
- CAF
- NIS/NIS2
- OG86
- IEC 62443

OUR CREDENTIALS



OUR PARTNERS





The Five Domains of Industrial Cyber Resilience, Bridging the gap between technology: a holistic approach

Our Securing OT environments demands more than reliance on a single product, technology, or methodology. The increasing complexity and volume of cyber threats require a multi-faceted, holistic approach to achieve effective resilience.

Adopting a recognised security framework provides organisations with a structured pathway to address risks comprehensively, spanning people, processes, and technology.

With decades of experience supporting critical infrastructure, our services and solutions are built on industry best practices, delivering compliance with key regulations such as NIS and alignment with standards like IEC 62443. We utilise a simple yet effective 5-step framework:

- **Assess Risk** – Identify vulnerabilities and evaluate potential impacts.
- **Develop Strategy** – Create a tailored roadmap for strengthening security.
- **Strengthen Defences** – Implement measures to protect critical assets.

- **Cultivate Awareness** – Build a culture of security through education and training.
- **Monitor and Improve** – Continuously refine and adapt to emerging threats.

This framework aligns with our recommended approach to optimise and sustain security practices, ensuring businesses remain safe. Regardless of the regulation, compliance requirement, or industry standard you follow, our services can be tailored to meet your specific needs.

End to end solutions

Our end to end security approach is built on 5 key pillars - with each stage ensuring businesses are either able to anticipate and prevent security risks, or respond to and recover from security events. Furthermore, this aids organisations to express their management of cybersecurity risk at a high level and identify clear risk management activities.

95%

Of organisations are unable to have 100% visibility into their OT systems

80%

Of organisations do not have basic visibility and segmentation in OT environments

73%

Of cases, both IT and OT systems were impacted by cybersecurity incidents

*Source: Dragos 2025 OT Cybersecurity Report: A Year in Review



DOMAIN 1.

ASSESS RISK

Understanding your organisation's risk landscape is the foundation of cyber resilience. By conducting comprehensive risk assessments and quantifying risks with proven methodologies, organisations can align security goals with business priorities, justify targeted investments, and reduce risks to acceptable levels.

High-Level Risk Assessment (HLRA) for OT & ICS

Low-Level Risk Assessment (LLRA) for OT & ICS

Industrial Cyber Risk Quantification (ICRQ)

Industrial Cyber Risk Assessment (ICRA)

Vulnerability Assessment & Penetration Testing (VAPT)

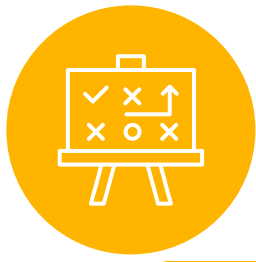
OT Site Assessment (OTSA)

Structured Threat and Risk Identification for Key Environments (STRIKE)

Cyber Resilience Testing (CRT) for Industrial Control Systems (FAT/SAT)

Physical Security Risk Assessment (OT-PSRA)

Cyber Security Gap Assessment (CSGA)



DOMAIN 2.

DEVELOP STRATEGY

Resilience begins with strategic design. Using frameworks like PERA to structure OT assets into secure zones and creating a cybersecurity roadmap ensures security is built into your systems, minimising breach impact and enabling quick recovery.

OT Cyber Strategy Discovery Day (CSDD)

Operational Technology Cyber Capability Assessment (OT-CCA)

OT Cybersecurity Target Operating Model (CTOM)

Capability Maturity Assessment (CMA)

OT Cybersecurity Roadmap Development (OCRD)

OT Security Architecture Design (OTSAD)

Secure OT Remote Access Strategy (SOTRAS)





DOMAIN 3.

STRENGTHEN DEFENCES

Proactive measures strengthen your ability to safeguard systems and respond to threats. Implementing OT-specific tools, testing incident response plan, and establishing dedicated response teams reduces downtime and mitigates attack impact.

SELECT – Technology Selection and Evaluation

OT Technology Selection Assessment Services (OT-TSAS)

PROTECT – Hardening OT Systems & Preventing Attacks

OT Zero Trust Secure Remote Access (OT-ZTA)

Industrial Network Segmentation & Firewalling (OT-Seg)

OT Endpoint Protection & Hardening (OT-EPH)

DETECT – Threat Monitoring & Anomaly Detection Solutions

OT Threat Detection & Visibility (OTTDV)

OT Security Logging & SIEM Integration (OT-SIEM)

REACT – Incident Response & Resilience Solutions

Industrial Incident Response Planning (ICS-IRP)

Industrial Control Security Response Team (ICSIRT) Establishment

Industrial Cyber Resilience Testing (OT-CRT)



DOMAIN 4.

CULTIVATE AWARENESS

People play a critical role in securing OT environments. Regular training, behavioural assessments, and fostering IT-OT collaboration transform staff from potential risks into your first line of defence, creating a culture of cybersecurity awareness.

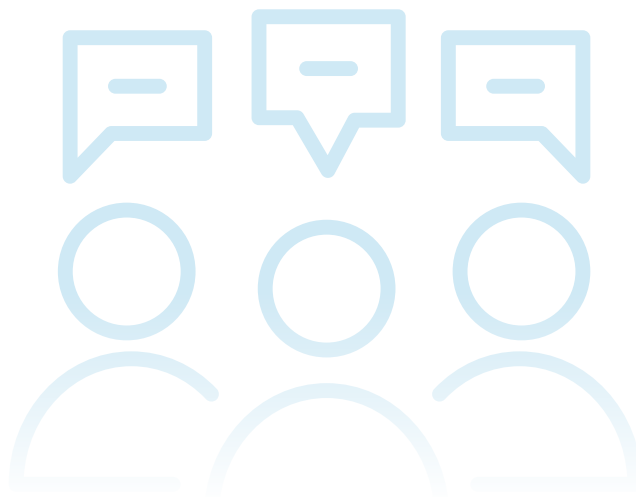
OT Cyber Risk & Security Management Workshop (OT-CRSM)

Advanced OT Cybersecurity Training for Cyber Engineers (OT-CET)

OPSWAT OT Cyber Academy Training (OT-OAT)

OT Cybersecurity Awareness as a Service (OT-CAAS)

OT Cybersecurity Leadership Coaching (OT-CLC)





DOMAIN 5.

MONITOR & IMPROVE

Cyber resilience requires ongoing vigilance and adaptability. Implementing a Cybersecurity Management System, real-time monitoring and regular updates to address emerging threats ensures continuous improvement and keeps organisations ahead of adversaries.

Cybersecurity Management System (CSMS) Development (OT-CSMSD)

Regulatory Submission & Compliance Readiness (OT-RSCR)

Managed Detection & Response (MDR) Deployment and Operation (OT-MDRD)

Cybersecurity Management System as a Service (CSMSaaS) (OT-CSMSaaS)

Managed Risk Services (OT-MRS)

Managed Compliance Services (OT-MCS)



CAPULA

capula.com

Orion House, Unit 10 Walton
Industrial Estate,
Beacon Road,
Stone,
ST15 0LT

Get in touch:

Tel: +44 (0)1785 827000
Email: contactus@capula.com

Follow us on LinkedIn

