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, "hacktivist" 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

"Due to the increasing pressures from external and internal threats, organisations responsible for critical infrastructure need to have a consistent and iterative approach to identifying, assessing, and managing cybersecurity risk. This approach is necessary regardless of an organisations size, threat exposure, or cybersecurity sophistication today."

NIST Cyber
Security Framework

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

IDENTIFY | PROTECT | DETECT | RESPOND | RECOVER

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:

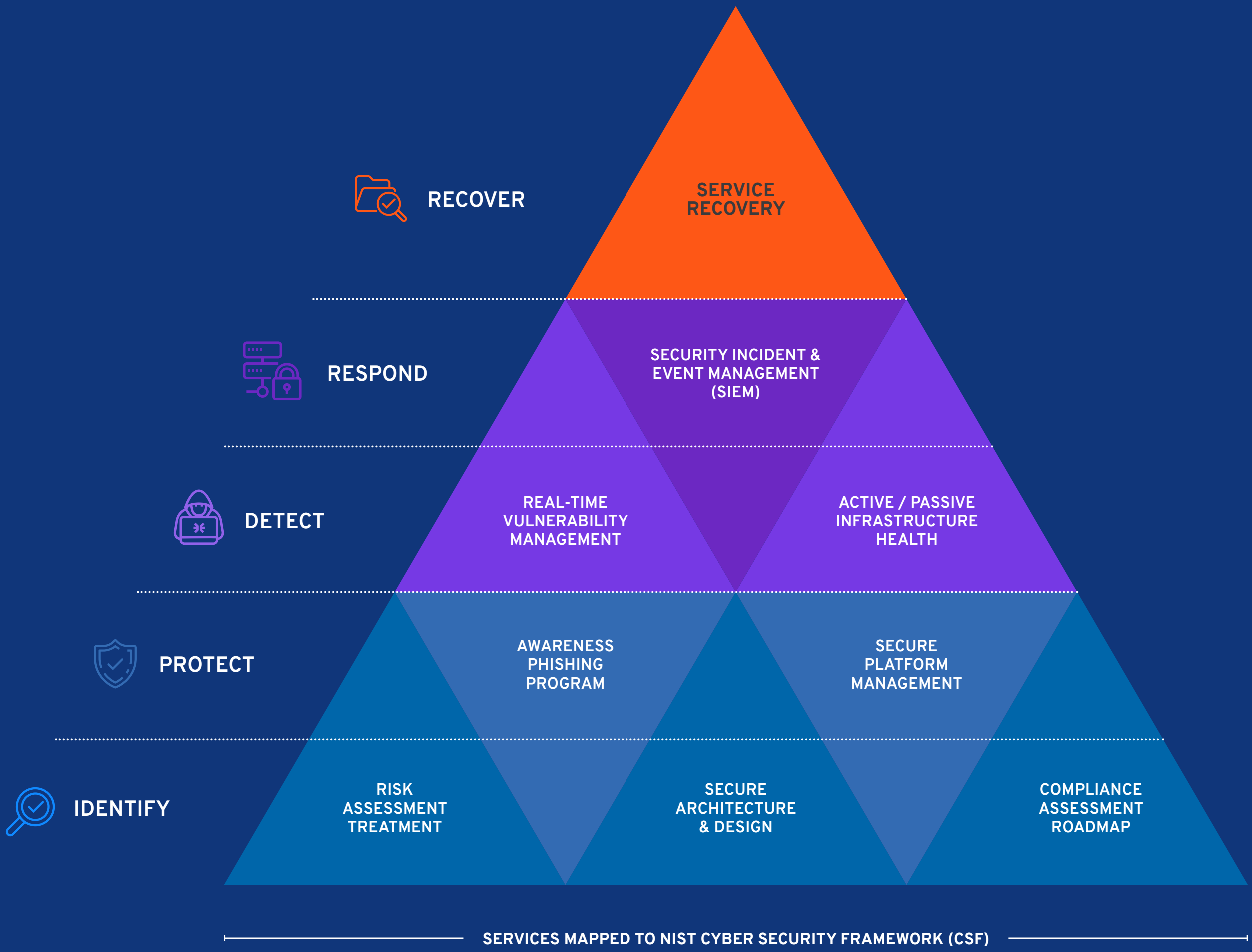
- ISO27001
- OG86
- CAF
- IEC 62443
- NIS-D

> *"As threats targeting critical infrastructure increase, choosing the right advisor and technology partner to secure your systems has never been more important. Our comprehensive portfolio of services & solutions are delivered by OT and industrial security experts with a demonstrable track record and over five decades of experience in the development and support of Industrial Control Systems (ICS) for customers in security-critical sectors."*

NIST Cyber
Security Framework

Our Services

Our comprehensive portfolio adds value to any stage of the OT security process - wherever you are in your journey - from risk assessments and training, to advanced real-time vulnerability management and service recovery. What's more, we can work with you whatever the size or scale, delivering standalone consultancy; embedded as part of a larger support contract.


RECOVER
SERVICE RECOVERY
RESPOND
SECURITY INCIDENT & EVENT MANAGEMENT (SIEM)
DETECT
REAL-TIME VULNERABILITY MANAGEMENT
ACTIVE / PASSIVE INFRASTRUCTURE HEALTH
PROTECT
AWARENESS PHISHING PROGRAM
SECURE PLATFORM MANAGEMENT
IDENTIFY
RISK ASSESSMENT TREATMENT
SECURE ARCHITECTURE & DESIGN
COMPLIANCE ASSESSMENT ROADMAP
SERVICES MAPPED TO NIST CYBER SECURITY FRAMEWORK (CSF)

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.

74%
of businesses don't have a current OT risk assessment

78%
Of companies don't have OT-specific security policies*

81%
Of businesses don't have an OT-specific security incident response plan*

*Source: Bloor Research, Oct 2018 - State of industrial and OT security report 2018

CAPULA

capula.com

Orion House,
Stone Business Park,
Staffordshire ST15 0LT
Tel: +44 (0)1785 827000

Get in touch:

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

Follow us on LinkedIn and Twitter