INDUSTRIAL CYBERSECURITY SERVICES

web: http://www.controlshield.co.uk
email: info@controlshield.co.uk

CONTROLSHIELD
Cyber Risk Consultants

CONTROLSHIELD
Cyber Risk Consultants

INDUSTRIAL THREAT LANDSCAPE

IN 2023, A SURGE IN GLOBAL TENSION RESULTED IN AN INCREASE IN CYBER THREAT ACTIVITY AND DISRUPTIONS IN CRITICAL INFRASTRUCTURE WORLDWIDE.

ESCALATING CONFLICTS EMBOLDENED ADVERSARIES AND HACKTIVISTS TO DEVELOP NEW CAPABILITIES AND REUSE OLD TECHNIQUES. SIMULTANEOUSLY, RANSOMWARE ATTACKS AFFECTED MORE INDUSTRIAL ORGANISATIONS, WITH A NEARLY 50 PERCENT INCREASE IN REPORTED INCIDENTS.

ASSET OWNERS MUST TAKE NECESSARY PRECAUTIONS TO ADDRESS THESE THREATS OR FALL VICTIM TO THEM.

KEY FIGURES

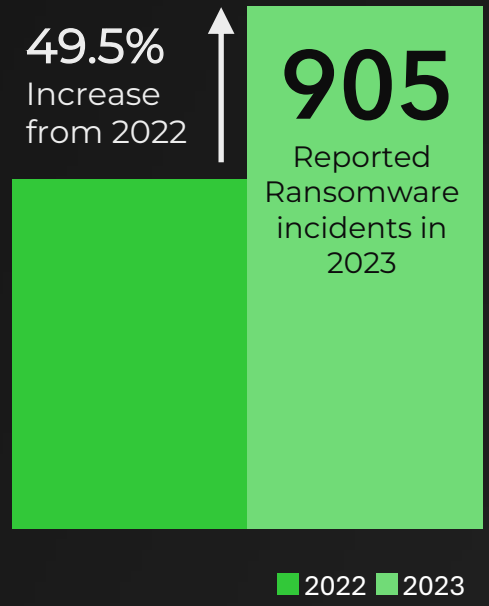
28%

Increase in ransomware groups targeting ICS/OT in 2023

In 2022, malicious objects were blocked on more than

40%

of Operational Technology computers (Kaspersky)



CONTROLSHIELD
Cyber Risk Consultants

NIS REGULATIONS AND THE CAF

NETWORK AND SYSTEMS REGULATIONS (2018)

NIS APPLIES TO ALL OPERATOR OF ESSENTIAL FUNCTIONS (OES) SITES IN EUROPE AND THE UK

THE DEPARTMENTS OF ENERGY, SECURITY AND NET ZERO (DESNZ) ARE THE UK COMPETENT AUTHORITY FOR NIS REGULATIONS COMPLIANCE

Department for Energy Security & Net Zero

NIS REGULATIONS ARE DESIGNED TO ENSURE THAT OES HAVE APPLIED ADEQUATE PROTECTIONS TO SAFEGUARD THE NATIONS CRITICAL SERVICES FROM THE RISKS OF CYBER ATTACKS

OES CATEGORIES

- ENERGY: ELECTRICITY, OIL AND GAS
- WATER: DRINKING WATER SUPPLY AND DISTRIBUTION
- TRANSPORT: AIR, RAIL, WATER AND ROAD
- TELECOMS: DIGITAL INFRASTRUCTURE PROVIDERS AND OPERATORS
- HEALTH: HEALTHCARE SETTINGS

CONTROLSHIELD
Cyber Risk Consultants

THE CAF

THE NCSC CYBER ASSESSMENT FRAMEWORK (CAF) PROVIDES A SYSTEMATIC AND COMPREHENSIVE APPROACH TO ASSESSING THE EXTENT TO WHICH CYBER RISKS TO ESSENTIAL FUNCTIONS ARE BEING MANAGED BY THE ORGANISATION RESPONSIBLE

THE CAF IS USED BY DESNZ TO ASSESS THE LEVEL OF MATURITY OF AN OES CYBERSECURITY PROGRAMME AND COMPLIANCE WITH NIS REGULATIONS

THE CAF IS APPLICABLE TO ALL STAGES OF THE OT SYSTEM LIFECYCLE

PILLARS OF THE CAF

MANAGING CYBERSECURITY RISK

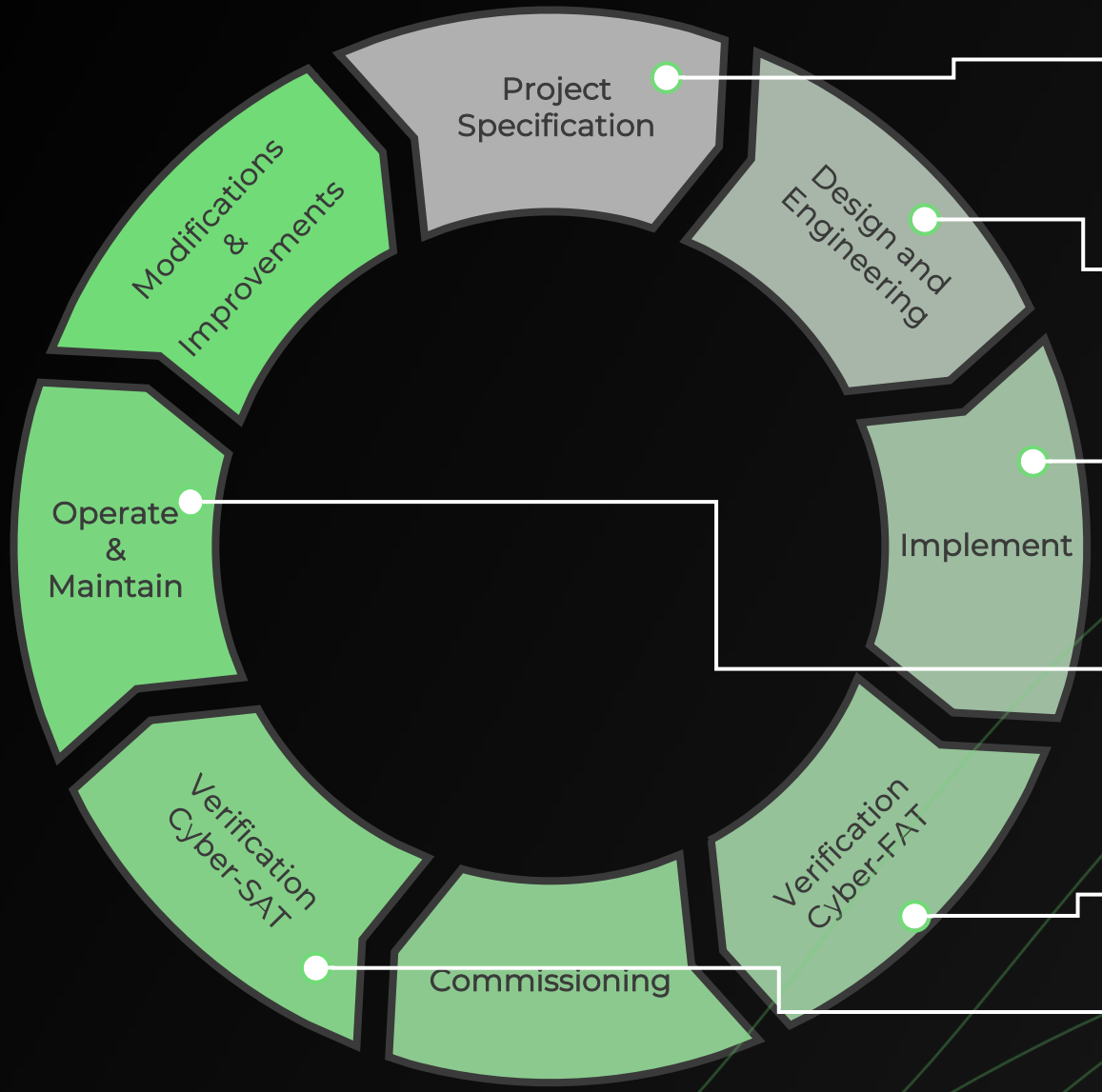
PROTECTING AGAINST CYBER ATTACKS

DETECTING CYBERSECURITY EVENTS

MINIMISING THE IMPACT OF INCIDENTS

CONTROLSHIELD
Cyber Risk Consultants

CONTROLSHIELD LIFECYCLE SERVICES



- PROJECT CYBERSECURITY MANAGEMENT PLAN
- CYBER RISK ASSESSMENT PLANNING AND EXECUTION
- FEED STUDY / DETAILED DESIGN INPUT

- CYBERSECURITY REQUIREMENT SPECIFICATIONS
- COUNTERMEASURE DESIGN
- CYBERSECURITY ASSESSMENT
- ZONE AND CONDUIT DIAGRAMS

- DEVICE HARDENING

- REGULATORY ASSISTANCE (CAF / OG-86)
- ASSET INVENTORY MANAGEMENT
- PATCH AND VULNERABILITY MANAGEMENT
- CYBERSECURITY MANAGEMENT SYSTEM
- EMERGENCY/INCIDENT RESPONSE PLANS
- AUDITS
- VULNERABILITY ASSESSMENTS

- CYBER-FAT REQUIREMENTS AND WITNESSING

- CYBER-SAT REQUIREMENTS AND WITNESSING

CONTROLSHIELD
Cyber Risk Consultants

FEATURED WORK

AT CONTROLSHIELD, WE TAKE PRIDE IN OUR TEAM OF EXPERTS WHO POSSESS A DIVERSE RANGE OF SKILLS AND KNOWLEDGE.

OUR TEAM MEMBERS HAVE CONSISTENTLY DELIVERED EXCEPTIONAL SERVICES TO OUR CLIENTS, LEVERAGING THEIR EXPERTISE TO PROVIDE INNOVATIVE SOLUTIONS

PROJECT SUPPORT

During an ICSS and CSS upgrade, ControlShield supported the client by producing a Project Cybersecurity Management Plan, conducting Risk Assessments for the upgraded system, developing Cybersecurity Requirements Specifications to ensure that the detailed design for the new systems would provide sufficient levels of protection against attack. Cybersecurity Assessments and Cyber-FAT were also performed.

CYBERSECURITY MANAGEMENT

Working for a clients with no existing Industrial Cybersecurity management systems in place. Our team developed and produced a range of policies and procedures using the IEC62443 framework. These documents were built with OG-86 and the CAF in mind for NIS assets whilst complementing existing Enterprise Cyber Security policies.

DESNZ CAF ASSESSMENTS

In 2023 the Department for Energy Security and Net Zero (DESNZ) requested that all Operators of Essential Services (OES) carry out a comprehensive review of Cybersecurity measures against the CAF basic profile. We worked with the company to compile several CAF reports in a short timescale. These reports were commended by DESNZ assessors as being some of the best received from a UK OES.