PROTECT

Case Study

: Nuclear Decommissioning Authority

Providing expertise to assist in a major cyber transformation programme

_enabling a trusted future

AIRBUS

At a glance

Customer	Nuclear Decommissioning Authority (NDA)
Industry	Energy & Utilities
Key Challenges	• Major transformation programme • Demanding regulatory compliances
The solution	• SOC • Consulting Services • Risk Assessments • CyberRange
Benefits	• Increased cyber resilience • Detailed understanding of position and vulnerabilities • A trusted partner with a collaborative, continuous improvement approach

The Nuclear Decommissioning Authority (NDA) is a nondepartmental UK public body dedicated to delivering safe, sustainable and publicly acceptable solutions to the challenge of nuclear clean-up and waste management.

Situation

The NDA has a requirement to support their Group CISO and seven Operating Companies with enterprise level cyber security via their Cyber Security Resilience Programme (CSRP). The CSRP is a major cyber transformation programme which will ultimately enhance and fully establish the NDA's own Cyber Security Centre of Excellence (CSCoE).

The mandate of the CSRP is to deliver, over a 5-year period, a consistent and harmonised view of cyber security risks and vulnerabilities across the NDA Group in accordance with the requirements of the Office for Nuclear Regulation (ONR), one of their regulatory bodies. To meet these requirements, the NDA contracted Airbus to assist with the Global Security Operating Centre (GSOC), Enterprise Risk Assessment, and Cyber Range projects.

Solution

GSOC Project

As part of standing up its CSCoE, the NDA sought to establish a best of breed centralised Protective Monitoring and Incident Monitoring/ Handling Service.

Functioning as a proof-of-concept capability, the project was initially tasked with establishing this service specifically for cloud services and uplifting processes to ensure consistency across the enterprise, such as Incident Response and Threat Intelligence.

The project will develop this proof-of-concept capability further by on-boarding additional services as these become available for the GSOC to connect to from each of the NDA Group Operating Companies' SOC's. This includes a specific focus on SOC for OT, which is an area where Airbus has deep knowledge and experience.

Airbus has provided a team of security cleared Levels 1-3 cyber security analysts, who are all subject matter experts in SOC Services ranging from incident monitoring/ handling, threat intelligence and vulnerability management.

>>> Approach: all support activities are currently undertaken remotely using NDA IT infrastructure from our secure SOC facility in Newport, with daily virtual stand-up meetings to discuss each day's agenda and targets.

Enterprise Risk Assessment Project

Airbus has provided a team of cyber security consultants, all of whom are security cleared, to assist with the Risk Assessment Project by undertaking Risk Assessments on IT and OT systems across the estate. Our consultants are all highly experienced in the practical application of risk management for CNI organisations, the Ministry of Defence, and Central Government. The NDA has developed its own Cyber Security System Risk Framework (CSSRF), derived from the NIST cyber security framework, as a method of cataloguing and categorising the myriad of systems across their enterprise. In addition to undertaking the risk assessment using the CSSRF, the Airbus delivery team was asked to enhance the framework, risk processes and to champion the use of this framework within the Operating Companies. Airbus has also supported the NDA's selection and adoption of a new Governance, Risk and Compliance (GRC) tooling solution to help bring greater consistency to risk management and reporting across their estate.

>>> **Approach:** Risk assessments are conducted against a prioritised annual Business Plan schedule as well as undertaking ad-hoc priority service requests from the NDA centre and Operating Companies.
Assessments are executed in three parts: review of evidence (including stakeholder workshops), formulation of Work Improvement Plans (WIPs) covering actions/timeframes and cost to mitigate the assessed control risks (again including stakeholder workshops), and a written final Report/ Security Case. Most workshops are held remotely, in part because of restrictions caused by COVID-19 but also to reduce the Carbon Footprint and cost. Where Risk Assessments are required within a tight deadline, these were conducted face-to-face whilst observing COVID-protocols at all times.

Cyber Range Project

The NDA required a Commercial-Off-The-Shelf (COTS) Cyber Range solution to establish a proof-of-concept capability providing additional functionality, capacity, flexibility, and supported by SMEs to:

- Demonstrate the benefits of physical and cloud-based COTS Cyber Ranges over bespoke versions
- Conduct off-line security assessments of both IT and OT case studies in order to prove the flexibility, utility and benefit of cyber range-based analysis
- Refine requirements for longer term cyber range services, in particular some of the non-functional requirements such as security, cyber range employment processes and links to wider CSRP services

>>> **Approach:** Airbus provided a team of SQEPs to configure and support our CyberRange (a self-contained mobile platform and a complementary SaaS-based system, both developed by Airbus). Following a successful PoC phase which established and demonstrated the required capability, our CyberRange was made available to the CSRP to conduct risk assessments against IT and OT system digital twins.
>>> **PoC phase:** we delivered a series of demonstrations on our cloud-hosted CyberRange to show the versatility of the system to a wide range of NDA stakeholders from their business, associated technical communities and CISOs. We were also asked to deliver a demonstration to a group of pan-nuclear sector organisations that included both the ONR and the Department for Business, Energy & Industrial Strategy (BEIS).

Our physical CyberRange platform was used to establish digital twins in both IT and OT systems using a combination of virtual images, physical devices and hybrid approaches. We also supported the NDA's CSCoE exercise by running an OT Ethical Hacking training exercise for NDA graduates and apprentices. A report was written for each PoC element along with an overall summary report and supporting cyber range strategy presentation to be used across the nuclear sector.

>>> **Risk Assessment Phase:** all work on the physical CyberRange was undertaken remotely (via secure connection to our physical CyberRange platform). External transfer mechanisms were used to upload virtual images for the digital twins, followed by design, build, and configuration activities. Work Package (WP) status update and alignment meetings were held weekly with all stakeholders; at the conclusion of each WP, a workshop was held to present our findings accompanied by a detailed technical report covering the lifecycle of each digital twin. This included use cases, scenarios, methodology for conducting the assessments together with screenshots of the CyberRange activities, technical findings, associated conclusions and recommendations.

We continue to support the NDA CSRP with resource, supporting material and capability for their participation in the annual national cyber security exercise and also for their new CSRP virtual Exhibition Room. Most recently, we are supporting a new development to enhance the NDA process for undertaking early supply chain security assurance.

Result

Our consistent, high quality delivery across all three projects, allied to our open and collaborative approach to all our engagements has been recognised by the NDA who now regard Airbus as a strategic partner.

Bringing together outstanding expertise in safety, cybersecurity and sustainability; Airbus Protect is a European leader in risk management.

Our cybersecurity offerings mentioned in this case study

SOC

We protect clients from both known and unknown cyber threats. Our comprehensive end-to-end Security Operations Centres (SOC) services are delivered 24/7 from secure premises in the UK, France, Germany and Spain.

Consulting Services

Protect your organisation by improving your corporate governance and security posture with our expert IT/OT consulting services.

CyberRange

CyberRange is our cybersecurity simulation and training platform used to build complex virtual and physical systems to replicate activities representative of your operations and conduct penetration tests. CyberRange simulates realistic scenarios, including real cyber-attacks, in isolated environments.

Contact Us
protect@airbus.com

Discover more case studies on our website

www.protect.airbus.com

AIRBUS

Airbus Protect, 31700 Blagnac, France

www.protect.airbus.com