PROTECT

Case Study

Security Operations Centre for UK Ministry of Defence

_enabling a trusted future

AIRBUS

At a glance

Customer	UK Ministry of Defence (MOD)
Industry	Critical National Infrastructure
Key Challenges	• Airbus Protect is responsible for handling all security incidents relating to the client's estate.
The solution	• An Airbus service framework underpinned by ITIL framework.
Benefits	• Working in the heart of the GOSC permits short-term and long-term continuous enhancements to the service.

The UK Ministry of Defence (MoD) is the British government department responsible for implementing UK defence policy, and is the headquarters of the British Armed Forces.

Airbus Protect has been providing Security Operations Centre (SOC) services to the UK MoD from within the client's Global Operations Security Coordination Centre (GOSCC) for over sixteen years.

Services

The Airbus Protect SOC monitors the client estate using IPS and SIEM tools providing an indepth view of network traffic in real time. Analysts quickly identify events of interest and analyse them either escalating them for further analysis, determining them to be false positives or using their knowledge of the supported systems to find mitigating factors. In each as where a data breach is confirmed or has yet to be ruled out, the appropriate playbook is followed and key stakeholders engaged appropriately and within SLA. The Airbus Protect SOC also includes the protective monitoring of the Crown IL5 Cloud datacentres supporting the Crown's New Style of IT where we provide MDR activity along with the full management of the SIEM and associated Cloud and physical log sources.

Within the GOSCC, the Airbus Protect SOC operates on a 24x7x365 basis alongside the MoD's own Cyber department and Computer Emergency Response Team (CERT).

Airbus Protect's responsibilities, over and above traditional SOC services, include day-today coordination of all cyber related security incidents between the CERT and the federation of third-party Managed Service Providers operating in the SIAM model.

Uniquely, the Airbus Protect SOC is both a Tower Provider and additionally provides Cyber Technical Assistance to the Operations Security Manager (OSM) as well as the OSM Cyber Security Team.

The Airbus Protect SOC is responsible for handling all security incidents relating to the client's estate; analysts perform initial triage and analysis of incidents (or vulnerabilities) and report their findings to the client, where client action and/or awareness is required.

The analyst will manage each security incident to its resolution providing regular feedback to the client as the incident progresses. If an analyst is unable to resolve an incident directly and further remedial action is required to restore service and\or prevent future incidents the analysts will task the appropriate support team (Airbus Protect or other service providers) to take that action, again aligned to playbooks and the client's incident response plan.

The Airbus Protect SOC maintains close co-operative relationships with other service providers, within the client's business and external managed service providers. Our processes for escalation and information exchange are mature and well documented ensuring a smooth operational environment when they are required.

Reporting

The Airbus Protect SOC SLA's are based on service availability and process response times. The KPI's have been carefully chosen to drive the right behaviour of all key stakeholders. The metrics are reported via a range of outputs including real-time client facing dashboards, formal reports presented at key stakeholder security working groups & service delivery management meetings.

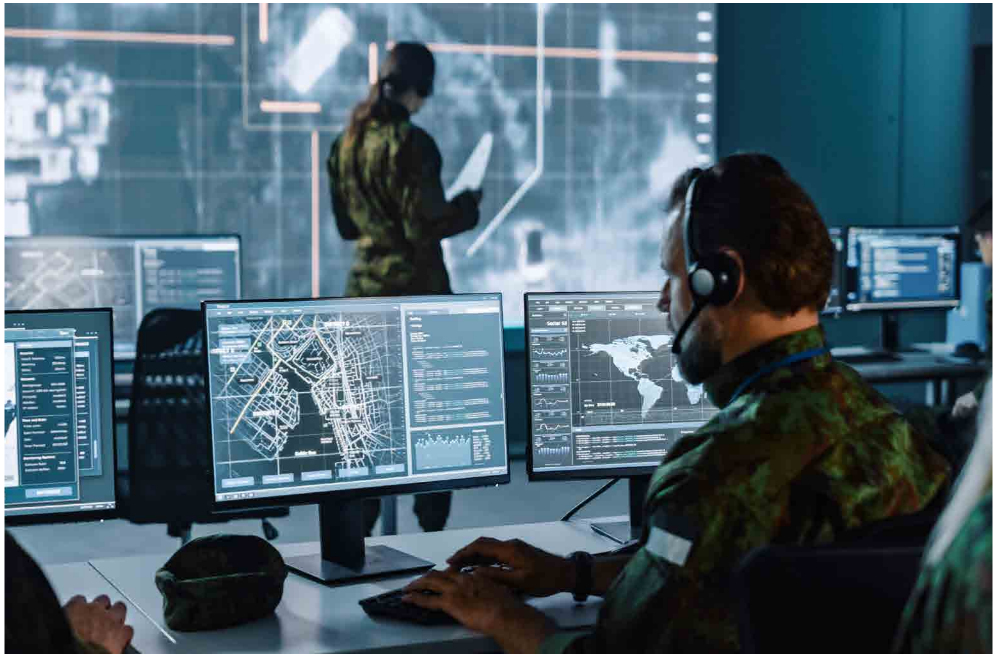
As part of the post-incident reporting process, root cause analysis may require the incident to be passed to Problem Management.

The Airbus Protect service framework is underpinned by ITIL framework that has Continuous Service Improvement (CSI) underpinning the lifecycle. As such, CSI and Change & Deployment Management play a key part in our approach to service enhancements no matter if the need is short or long term.

All incidents on resolution and considered for Lessons Identified (LIs) and contribute to the CSI lifecycle.

Short Term Enhancements - working in the heart of the GOSCC frequently presents high pressure, short notice changes or service enhancement requests in support of ongoing live operations. The 'One Team' approach or 'Whole Force' is something Airbus are very proud to share with the client and other MSPs.

Long Term Enhancements – enhancements to our services are continually worked on in partnership with the client from autonomous Intrusion Prevention to an ongoing provision of SOC services and reporting capability for multiple Managed Private Cloud solutions.



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.

Vulnerability Assessments

Reveal your organisations true cyber maturity by uncovering hidden vulnerabilities and understanding potential system exploits.

Is your organisation looking for a new SOC partner?

Get in touch to discover how we can support you

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