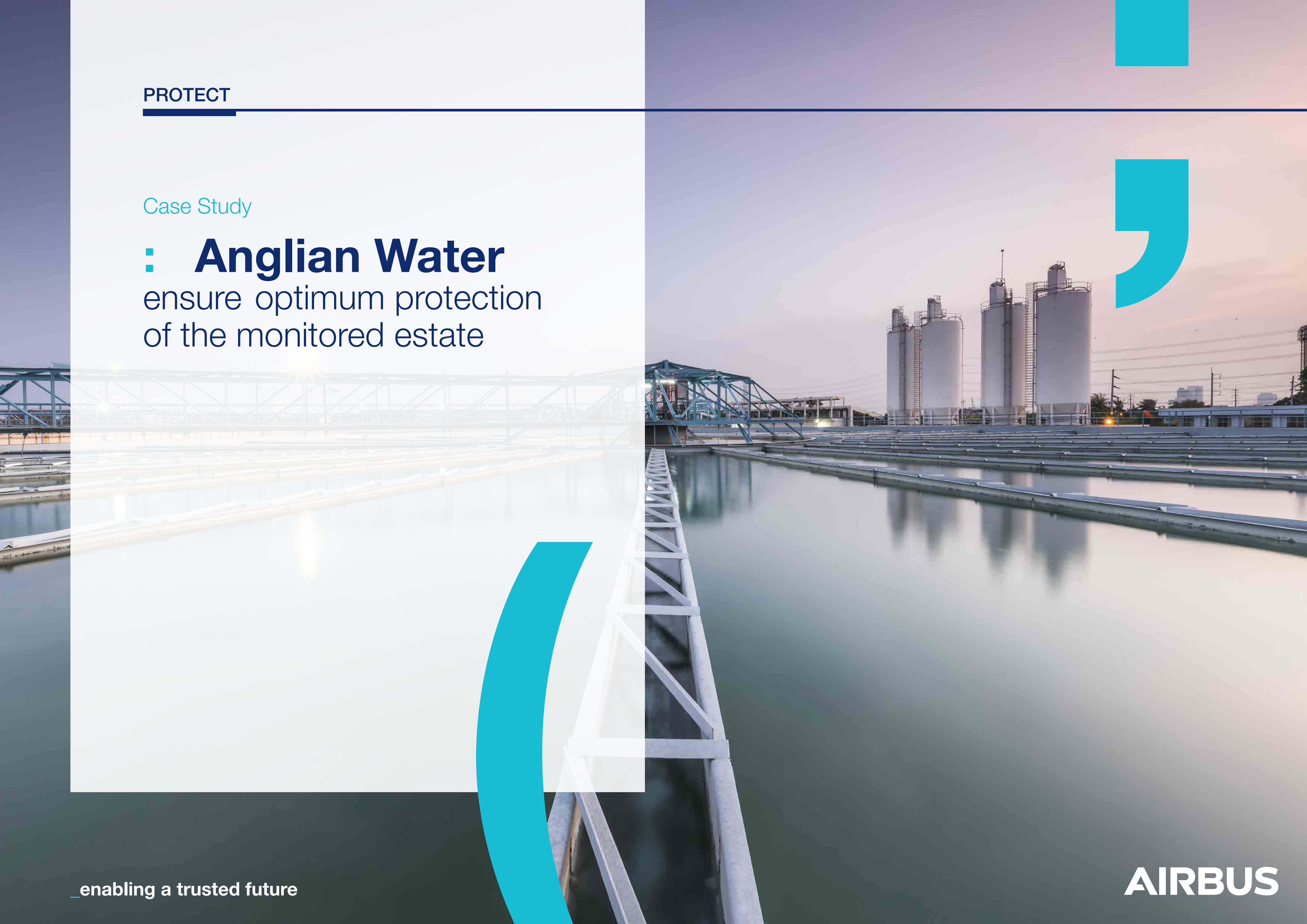
PROTECT



Case Study

: Anglian Water ensure optimum protection of the monitored estate

_enabling a trusted future

At a glance

Customer	Anglian Water Services (AWS)
Industry	Energy & Utilities
Key Challenges	• Provide holistic cybersecurity services within a Service Integration and Management (SIAM) model.
The solution	• Provide the best available technology and services, which achieve the best possible value for money.
Benefits	• A single framework contract, providing a single point of contact for all cyber topics.

Anglian Water is the largest water and water recycling company in England and Wales by geographic area. The organisation provides water, sewage and drainage services to almost seven million people in the East of England and Hartlepool.

Airbus Protect has held the IT Security Operations Centre Services contract with Anglian Water Services (AWS) since 2017. We are the designated Service Tower Provider (STP) for Security operating within a Service Integration and Management (SIAM) model.

We are responsible for the following services:

- Security Operations Centre and Managed Security Services
- Onsite Security Management – PKI Certificate Management, Security Compliance Reporting, Risk Assessment.
- Risk Management – IT and OT, Security Audit, Penetration Test findings management.
- Cyber Threat Intelligence – Threat assessment and continuous investigation of threat exposure.
- Security services and tools, including SIEM, IDPS, Darktrace, FireEye, Mimecast, SpamBin, Tripwire Vulnerability Management, Forensics and Incident Response.

As the Security STP, we operate with international teams from other Service Towers supporting the AWS environment and we are all charged with providing the best available technology and services which achieve the best possible value for money.

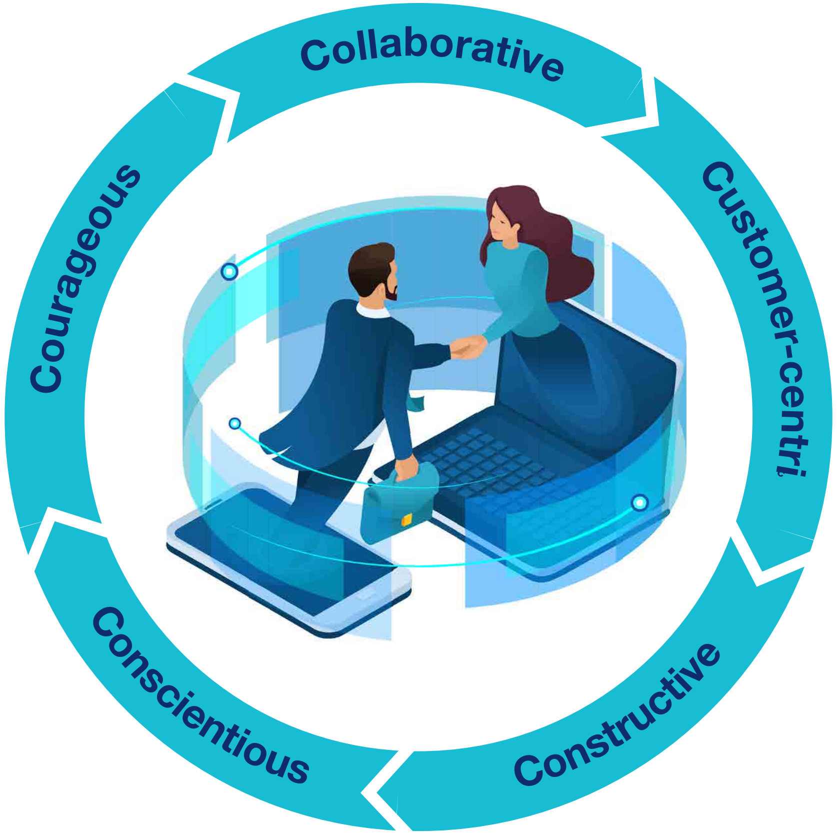
We have committed (along with the other STPs) to contribute to the delivery of high quality and continually improving services, as well as to the development of solutions and participation in the provision of new services (either as lead or in support of other STPs).

Our Service Delivery team attends monthly Security Service Review meetings, attended by representatives from the AWS' internal cyber function and the other STPs to review the following areas:

- Service performance;
- Recent IT incidents;
- Trends in support calls;
- SOC service improvement opportunities;
- Metrics from other STPs which have an impact on the SOC service.

The Airbus Protect Onsite Security Manager is responsible for collating all metrics and ensuring the SIEM is tuned to minimise false positives. We constantly assess our own threat intelligence and create new use cases (in line with industry best practice) to ensure optimum protection of the monitored estate.

The AWS SIAM/SIF construct is underpinned by the need for Continual Service Improvement (CSI), anchored on core behaviours referred to as the "5 Cs":



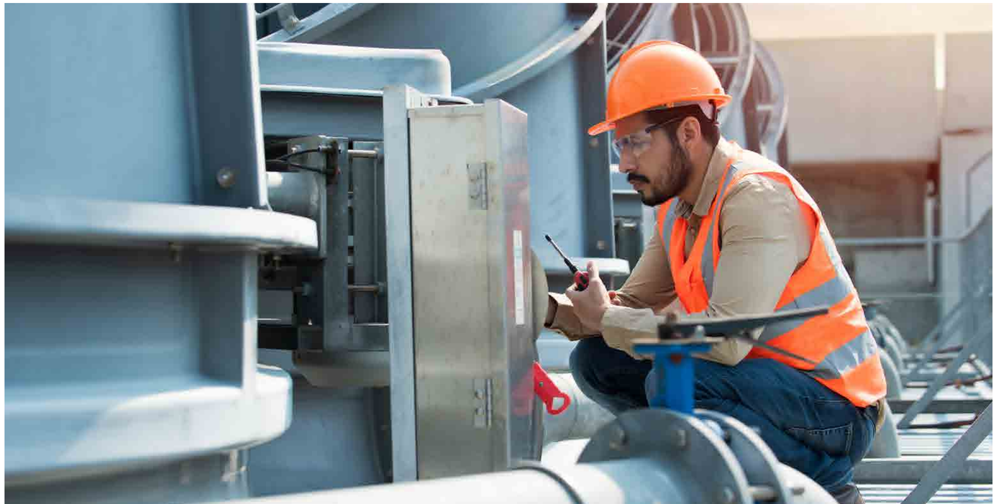
The "5Cs" and CSI examples

- **Csi Improvement & Knowledge sharing:** Improved relationship & collaboration with CSI team
- **SVR Communication:** Improved communications with Key stakeholders via regular scheduled calls
- **Latest INC:** Displayed good values focusing on cooperation and collaboration
- **MIM Training:** Raised with the IS Team to improve awareness
- **Service Management Team:** Established enhanced relationship built on trust and understanding. CSI raised based on capacity conversion

CSIs proposed by our team that are assessed for potential benefit and impact (internally) and, once accepted, submitted through the formal AWS CSI process and fed into the SIF review meetings.

Some additional CSI examples from 2021 are detailed below:

- Introduction of threat modelling to assist risk assessment and focus AWS investment
- Recommendation and implementation of the optional Darktrace Inoculation service for pre-emptive against new/novel threats detected elsewhere in the Darktrace community
- Introduction of an "Operations Call" to directly connect the AWS Security team and other STP contacts with the desk-level SOC Analysts enabling deeper, technical exchanges on a regular basis
- Creation of a dashboard to track telemetry statistics and provide early indicators and warnings
- Modification to availability and capacity reporting to capture trends and facilitate better planning



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

Governance, Risk & Compliance

Airbus Protect provides a range of services to help you understand your current threat landscape, anticipate risks before they materialise and stay up to date with current regulations. Our end goal is to increase your organisation's cyber resilience and guarantee you remain compliant in the face of even the most sophisticated threats. We'll assist you in setting up your cybersecurity governance strategy, and ensuring business continuity when a crisis happens.

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.

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