Case Study

Accelerating the Implementation of a 24/7x365 Security Operations Centre (SOC)

CUSTOMER	INDUSTRY	KEY STATISTICS	SERVICES PROVIDED
Department for Transport	Central Government	24/7x365 MDR service under budget	Cyber Security as a Service

Background

The invasion of Ukraine by Russia in 2022 presented a severe threat from Foreign Intelligence Services for the UK Government. The DfTc, at the time, had a limited internal Security Operations Centre (SOC) that only operated during business hours, Monday through Friday, from 9am to 5pm. This SOC had limited resources and technology, minimal data feeds, and SIEM policies that were not fully enabled. This left the DfTc exposed to potential threats as their monitoring, detection, and response (MDR) capabilities were inadequate. In January 2022, the CDIO and Senior Members of the DfTc recognised the need for a 24/7x365 SOC to monitor the entire DfT estate by June 2022. However, the internal team informed the SLT that they would not be ready to initiate procurement until October 2022. The tmc3 team was employed to accelerate this programme in order to address this critical need.

STRATEGIC CYBER SECURITY PARTNERSHIP IN CENTRAL GOVERMENT

CUSTOMER

Department for Transport

INDUSTRY

Central Government

KEY STATISTICS

24/7x365 MDR service under budget

SERVICES PROVIDED

Cyber Security as a Service

SOLUTION

Our team swiftly mobilised to identify and assess the current tools, technology, data feeds, and resources in place at the DfTc. Through a series of workshops, we identified crucial MoSCoW requirements and captured the comprehensive procurement Statement of Work (SoW). Utilising the Crown Commercial Service's (CCS) Tech Services 3B Framework, we evaluated and scored potential suppliers in response to the SoW, taking into account technical capabilities and financial budgets, to determine the best fit for the DfTc's requirements. We collaborated with procurement to ensure an appropriate contract was fast tracked, enabling the SOC experts to be in place swiftly (May 2022). We meticulously crafted and published the Transition to Live Documentation to ensure a seamless integration of the service into live operations. By June 2022, the DfTc had a fully operational 24/7x365 MDR capability with their preferred, outsourced MDR provider.

RESULTS

We successfully expedited the programme by over 6 months, delivering a fully operational 24/7x365 MDR service under budget. Working in a true partnership with the DfTc, we ensured that all technology feeds were seamlessly managed by the SOC. This was perceived as a major achievement for DfTc and was reported back to Parliament. In addition, we fine-tuned policies and alerts to detect any previous compromise and to evidence compliance, we assessed the MDR service against the National Cyber Security Centre's Cyber Assurance Framework (NCSC CAF).

BENIFITS

The expedited programme provided assurance to the DfTc's board that threats from Foreign Intelligence Services were being effectively managed and also resulted in cost savings. The programme not only enabled the DfTc to evidence compliance with the NCSC CAF but also helped the DfTc to showcase their maturity and capabilities among their peers and other agencies (DVLA, DVSA, HS2, Highways England etc).