LOGICALIS
Architects of Change

Aberdeenshire COUNCIL

How Aberdeenshire Council achieved cost-effective cyber-resilience

AT A GLANCE

Customer: Aberdeenshire Council

Challenge: The Council needed to modernise its security operations in order to adhere to legislation, ease the burden on IT staff, and improve long-term strategic security planning. However, it also had a responsibility to keep costs to a minimum.

Solution: Logicalis implemented a Microsoft Sentinel Managed SOC, tailored to ensure the volume of data being analysed remained under an agreed cost cap while delivering a robust security posture.

Outcome: The Council now benefits from 24/7, real-time monitoring of threats, IT staff are freed up to work on more strategic work, and detailed reports help inform future security planning.

Background

Aberdeenshire Council is a Scottish public authority, serving a population of around 261,000 people. It provides IT services to 11,000 council employees and 30,000 school pupils who use a range of devices including laptops, desktop computers and mobile phones.

The Challenges

In 2022 the Council decided to implement a new 24/7 Managed Security Operations Centre (SOC) for its IT infrastructure. It wanted proactive monitoring, incident detection and response capabilities which would integrate with its other managed service security providers. It also required always-on, real-time reporting and a 'single pane of glass' view of threats and incidents.

There were three key factors driving the project:

- Firstly, the Council needed to comply with national legislative and regulatory obligations such as the Scottish Government's Cyber Resilience Framework Strategy, the Data Protection Act 2018, and the Public Services Network (PSN) Information Assurance Conditions.
- Next, it wanted to reduce the potential for human error and the drain on valuable IT teams' time associated with manually reviewing and triaging security alert logs.
- Finally, it was crucial to find a cost-effective way to improve visibility across all its security appliances, to more easily defend against immediate threats while also building a clearer picture for long-term planning.

"Logicalis has been pivotal in helping us achieve our ambition to harness the power of a Managed Security Operations Centre within a tight budget. The team went over and above to tailor their proposition to our infrastructure and requirements, providing advice, guidance and support to make the project a success."

Ray Wilson, *IT Service Delivery & Security Team Leader*

The Solution

As a public sector organisation, Aberdeenshire Council is naturally cost-sensitive. Therefore, it launched a tender process to select a partner which could balance quality, capability and price. Following a rigorous selection process, the Council appointed Logicalis.

To address the Council's requirements, the Logicalis proposal was based on Microsoft Sentinel – a comprehensive Security Information and Event Management (SIEM) solution that complemented the council's Microsoft ecosystem. Crucially, Logicalis's Managed Sentinel service is designed to integrate and orchestrate security across a digital ecosystem using a hyperscale cloud-native platform, providing automated insights – for instance; on unknown threats, potential false positives, and suspicious activities. These can be analysed and actioned in real-time, therefore increasing the speed of response.

Importantly, developing the most valuable and effective solution for Aberdeenshire Council was an iterative process. For example, the Council had multiple security appliances which the Logicalis team analysed to determine how alerts should prioritised and managed. As a result, they were able to streamline the data being fed into the Sentinel platform so that the ongoing analysis fees would remain under the cost cap set by the Council, all while maintaining a robust security posture.

With any complex IT programme, unexpected issues can occur during implementation. One such example was when the Council's third-party firewall providers were unsure how to integrate their service with the Sentinel platform – a crucial part of the Council's vision for a single, integrated operating model. To help, the Logicalis team went outside their original remit to step in and coordinate the external providers, successfully guiding everyone through the process.

The Outcome

The provision of a Managed Sentinel SOC has allowed Aberdeenshire Council to harness the power of Logicalis's 24/7 Security Operations Centre, AI, machine learning and analytics to transform its security operations and enhance its overall security posture, thereby protecting all stakeholders.

The Council has seen numerous benefits, including:

- The 24/7 monitoring and analysis of alerts makes threat detection more effective and shortens response times;
- The intelligent triage of alerts means resource isn't wasted and costs can be controlled
- The in-house IT team is freed up to work on more value-add tasks such as gap analysis, strategic planning and building out better cyber-resilience, adding further value to the Council and its constituents;
- The detailed reports generated via the platform give the Council a true picture of trends and patterns across its security estate, including vital information which it is building into its long-term strategic roadmap.

Today, Aberdeenshire Council leads the way as one of the first Scottish councils to introduce a Managed SOC – an important objective for all 32 local government bodies in Scotland.