TECH mahindra

CASE STUDY

Implementing State-of-the-Art Security Solutions for a UK Telecom Giant

Overview

Our client, one of the largest mobile network operators in the UK, delivers essential telecom and internet services to millions nationwide. Managing a complex IT ecosystem with 30,000 devices, 200+ use cases, and 35,000 events per second (EPS), the company faced multiple security challenges that required immediate attention and improvement.

Client Background and Challenge.

The client lacked a comprehensive, industry-leading security products portfolio that could integrate into a central system, thus failing to offer adequate protection and visibility against emerging threats.

- Perimeter protection & risk of missing the detection of suspicious events
- Lack of processes for managing the security landscape due to out-of-box solutions and legacy systems
- Lack of in-house skilled resources to properly analyse security events
- Average time to detect and respond to security events in days and weeks
- Limited automation and a more manual approach
- Limited visibility on emerging threats due to lack of integrated ecosystem
- High MTTA and MTTR, impacting operational efficiency

Our Approach and Solution

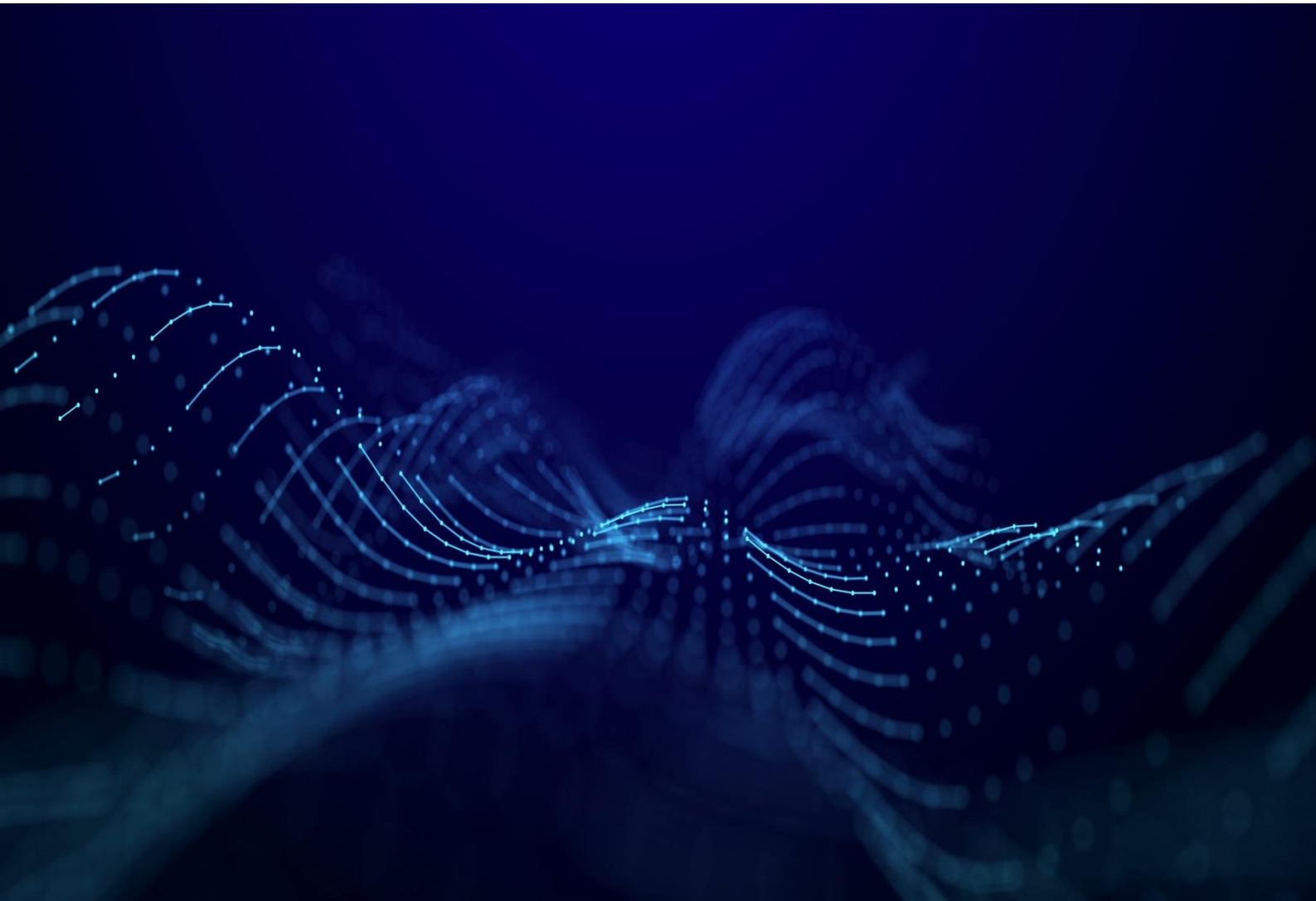
- Planned, designed, and built a dedicated SOC with a state-of-the-art security products portfolio to provide effective network, perimeter & endpoint security
- Set up 24x7x365 eye-on-the-glass monitoring to detect threats in real time and respond to mitigate business impact
- Integrated log sources (workstations, servers, network devices, applications) to expand the depth and breadth of security events detection
- Handled platform administration and fine-tuning and created custom use cases and rule development

Tools & Technology Used

- Microsoft Defender
- Azure AD (Identity & Access management solution)
- Dark Trace (AI-Powered Cyber defense Solution)
- Splunk (Enterprise Security)

Business and Community Impact

- 250+ SOC Rules implemented to automate threat scenarios and detect security threats across different platforms within the IT infrastructure
- Single pane glass view for all security events by onboarding all security tools and their logs into the SIEM
- Alignment to global MITRE ATTACK framework
- Proactive threat intelligence & threat advisories
- 45% and 25% improvement in MTTA and MTTR respectively
- 30% reduction in false positives and 20% auto closure of incidents
- 100% trained & certified resources
- 30% additional assets onboarded to the SOC platform
- 100% SLA met on platform availability



About Tech Mahindra

Tech Mahindra (NSE: TECHM) offers technology consulting and digital solutions to global enterprises across industries, enabling transformative scale at unparalleled speed. With 150,000+ professionals across 90+ countries helping 1100+ clients, Tech Mahindra provides a full spectrum of services including consulting, information technology, enterprise applications, business process services, engineering services, network services, customer experience & design, AI & analytics, and cloud & infrastructure services. It is the first Indian company in the world to have been awarded the Sustainable Markets Initiative's Terra Carta Seal, which recognises global companies that are actively leading the charge to create a climate and nature-positive future. Tech Mahindra is part of the Mahindra Group, founded in 1945, one of the largest and most admired multinational federation of companies. For more information on how TechM can partner with you to meet your Scale at Speed™ imperatives, please visit https://www.techmahindra.com/.

Note: This text was edited with the assistance of an AI tool. The original content, based on Tech Mahindra's intellectual property, was created by a human author. A human editor then reviewed the AI-edited version. Tech Mahindra Ltd. retains the copyright of this document.

TECH mahindra

www.techmahindra.com
top.marketing@techmahindra.com