Mitigating real-time cyber risk with a cohesive IT/OT SOC

Operational Technology

OT underpins much of our critical national infrastructure (CNI) across water, energy, transportation and logistics, aerospace and defence, food and beverage, chemicals and pharmaceutical sectors. You will also find elements of OT supporting all modern enterprises, from IoT within data centres to physical security systems, CCTV, HVAC, elevators and escalators within office spaces.

Generally, OT suffers from multiple cyber security issues, including a high prevalence of legacy systems (with average lifecycles measured in decades), often insecure-by-design systems that prioritise availability with limited resources, many of which have significant potential consequences if they were to fail – with many industrial organisations facing both significant financial losses and potential safety implications.

Threat

The threat to our CNI continues to rise, with the number of cyber incidents and their impact increasing year-on-year. Industrial organisations continue to be a high-value target for attackers due to the relative ease of disruption, leading to interest from nation-state-aligned groups and those using ransomware to demand higher ransoms. The manufacturing sector continues to top lists of those experiencing the most attacks, paying the highest cyber insurance premiums, claiming the most on their policies, and experiencing the highest recovery costs.

Why Now?

Industry 4.0 has seen the digital transformation of our industries, enabling real-time decision-making and higher levels of productivity, flexibility, and agility. Unfortunately, this came at the cost of eroding the only level of cyber protection these systems often had – airgaps. The convergence of IT and OT environments has significantly increased the threat to our industrial environments without introducing risk mitigations. This has led to the increase in cyber incidents and cyber insurance costs we are now experiencing, increasing levels of government regulation to tackle the issue. These factors drive board-level engagement with cyber security, with many industrial organisations now acknowledging operational cyber risk as one of their top priorities across their entire business.

The Only 100% UK Owned & Operated IT & OT Security Provider

At Sapphire, we're more than just a cyber security company – we are your trusted partner and an extension of your team. We understand the immense pressures your security teams and leaders face. We're committed to ensuring you have a trusted advisor by your side, offering guidance and expertise to support you where it's most needed. Over twenty-five years of delivering tailored security solutions to organisations across the UK.

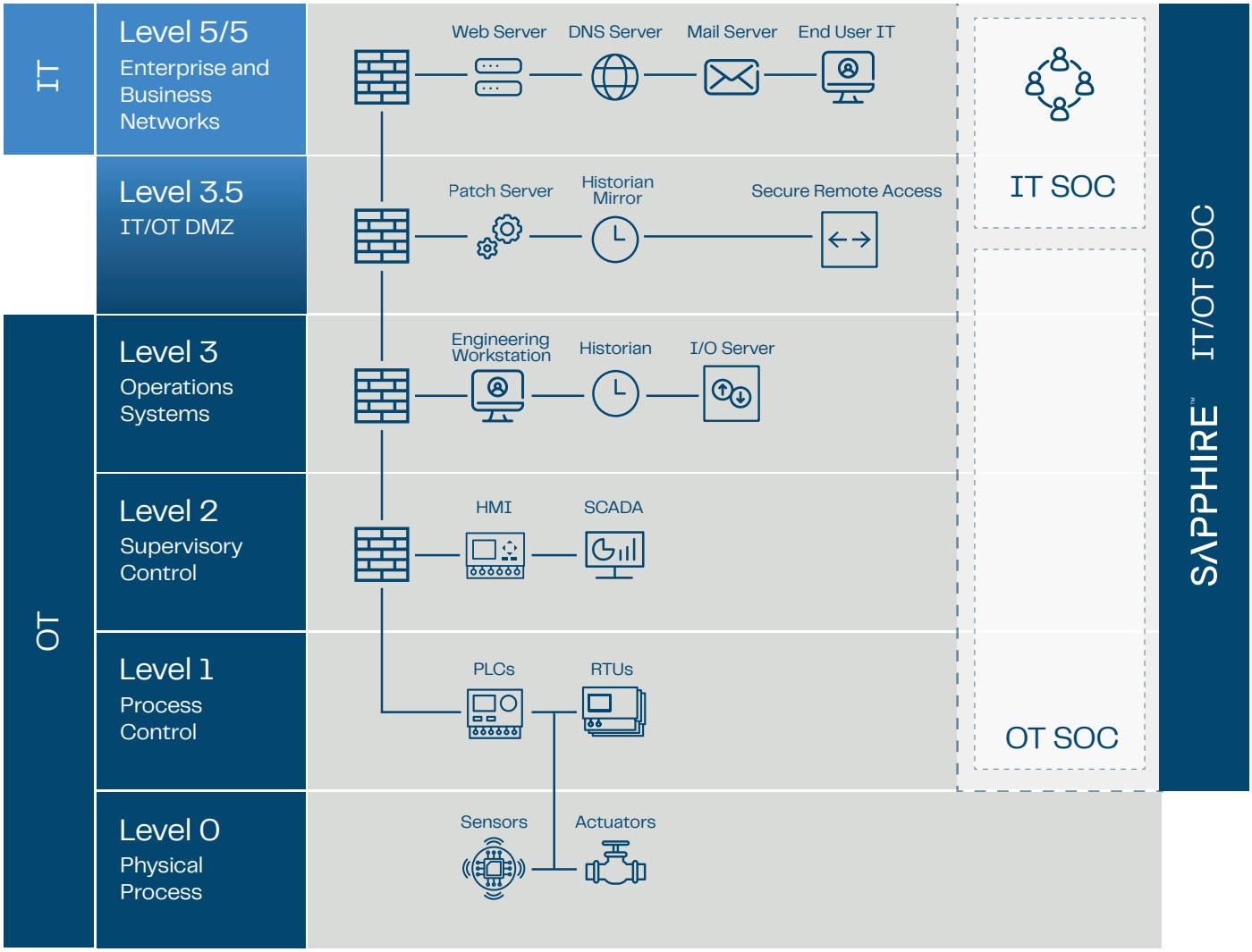
To find out more or to speak to an expert contact us today

CONTACT US TO FIND OUT MORE

Or call: 0845 58 27001

IT/OT SOC

As your IT and OT environments converge ever closer and the lines between them blur, you need to ensure your SOC can provide adequate cover across your entire IT/OT estate. Sapphire utilises OT-specific cyber solutions to gain in-depth visibility, working around the specialist requirements and constraints standard in operational networks, ensuring a single-pane-of-glass view of your entire environment. We operate with our own proprietary suite of OT cyber solutions and an expertly selected portfolio of partner technology solutions to underpin our IT/OT SOC, ensuring each client's uniquely designed cyber architecture provides a measurable return on investment and cyber risk mitigation. Our SOC analysts are trained in OT cyber incident management to identify and triage incidents in real-time, mindful of the differing priorities of confidentiality, integrity and availability across the IT/OT divide. With OT-utilising organisations experiencing numerous OT cyber incidents a year, Sapphire's IT/OT SOC will significantly reduce the potential impact and recovery time on your critical infrastructure.



To find out more or to speak to an expert contact us today

CONTACT US TO FIND OUT MORE

Or call: 0845 58 27001

Sapphire OT Services – NIST Framework Alignment

Identify

- Visibility of OT assets with Dot™
- Management of OT vulnerabilities with Dot™
- Alignment to regulations and standards with Profile™
- Automated OT risk management with Radiflow CIARA

Protect

- Next generation OT firewalls from Check Point for network separation & micro-segmentation
- Secure Remote Access by Cyolo
- Third Party Risk Management by Sapphire

Detect

- Anomaly/Intrusion Detection from Radiflow / Microsoft Defender for IoT / Tenable.OT
- Threat Detection by Check Point
- Endpoint Detection by Microsoft XDR
- OT Threat Intelligence by Sapphire

Respond

- Managed Converged IT/OT SOC by Sapphire
- OT Incident Response by Sapphire

Consultancy, deployment and support by

SAPPHIRE™

Microsoft Radiflow CHECK POINT Cyolo dot™ profile™

To find out more or to speak to an expert contact us today

CONTACT US TO FIND OUT MORE

Or call: 0845 58 27001