Managed SOC/MDR

Proposition Overview

Managing advanced threats in a new digital era

Many NHS IT and security leaders will have heard of EDR solutions, which collect and analyse data about events and behaviours on endpoints to act as an early warning against sophisticated attacks. But increasingly, organisations need to go beyond the endpoint, and collect and correlate data from across networks, and hybrid cloud environments where remote working users and highly regulated data reside. This is where Managed Detection and Response (MDR) comes in.

At a glance

- ✓ We'll provide 24/7 threat detection and response across remote, endpoint, network, cloud and OT environments delivered by our Managed SOC service..
- ✓ We'll help to protect your organisation from data breaches, reduce attacker dwell time, and negate the impact of any malicious activity on your operations.
- ✓ We'll consume all of your security telemetry, with no limit on volume, and use the latest advancements in security analytics technology, combined with a highly skilled and experienced team to analyse your data, identify what's bad, and take action to stop it.

Problem solved

The NHS is a unique institution with some specific challenges that set it apart from most others. These include well-publicised resource and funding constraints, and a complex organisational structure which, it has been argued, leads to overlapping competencies, and slow incident response. In addition, most trusts do not have a dedicated Chief Security Officer (CSO) or similar. Adopting an MDR or Manged SOC service provides outsourced security expertise where in-house skills may be lacking, and it resolves the major financial and management headache of finding and retaining skilled SOC analysts, and kitting out a SOC with the requisite tech.

Benefits

An extension of your security team, freeing up in-house resource to be more strategic.

Rapid response to mitigate threats before they have had a chance to impact your organisation.

Swift detection and containment provides an extra layer of defence, because prevention can't catch everything.

BLOCK

block.co.uk