

# WHAT IS VSOC AS A SERVICE?



The MYREDFORT VSOC

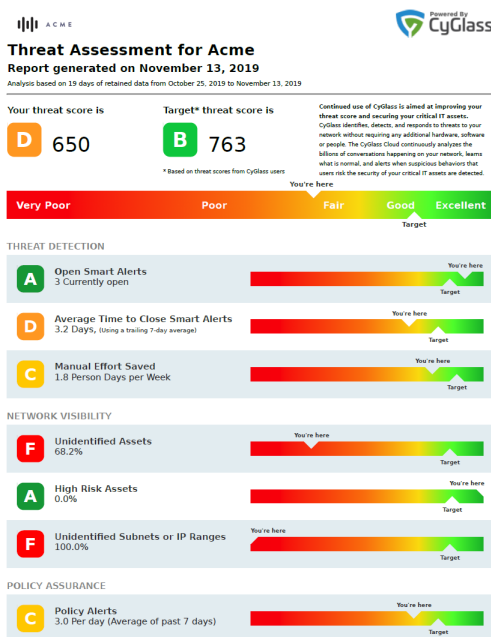
Service Powered by CyGlass, a Nominet company



## The MYREDFORT VSOC

VSOC simply and effectively identifies, detects, and responds to threats to your network without requiring any additional hardware, software, or people.

The VSOC uses the cloud to continuously analyse billions of conversations happening on a company's network, learns what is normal, and responds when suspicious behaviours that risk the security of your critical IT assets or your organisation's reputation are detected.



The VSOC provides a unique perspective on the security threats on a network. It delivers actionable intelligence in the form of a Network CyberScore. The Network CyberScore can be calculated for any node, subnet, zone or partner on your network. The Network CyberScore provides visibility into the security events affecting your network, and clear actions on how to address them.

The VSOC addresses data privacy as it doesn't require any personally identifiable information (PII) to detect threats.

## Fraudsters don't Come Through the Front Door

Through phishing, social engineering, or malware that exploits vulnerable systems, attackers can routinely get past traditional controls like firewalls and anti-virus. Once inside, attackers count on being invisible, undetectable in the everyday network traffic flows. They move freely on your network, scanning and probing machines, looking to gain an advantage, marching towards their goal - extortion via ransomware, stealing of sensitive information, or possibly even destroying critical systems.

## The MYREDFORT VSOC

### What are the Technical Advantages of a VSOC?

Knowing what's inside a network is the biggest advantage against attackers. The longer an attacker goes undetected, the more devastating the attack. Defenders have this advantage if they know what's "normal" in their network, whereas attackers will not.

A VSOC maximises visibility within the network and

- **Identifies:** This service identifies the assets, asset groups, and subnets on a network. It builds baselines of normal network behaviours for those assets
- **Detects:** This service detects policy violations, anomalies, and threats to the network.
- **Responds:** Alerts are generated and a VSOC analyst is able to make a determination if the alert is valid. The VSOC analyst can then initiate a response to stop the fraudster in their tracks.
- **Learns:** The system learns from the result of the incident in order to produce more accurate results going forward. The network data is archived so that historical traffic can be analysed to understand the impact of newly discovered vulnerabilities or attacks.

### How will a VSOC help my business?

**Visibility:** Companies of all sizes are looking for an easy to deploy, comprehensive, and cost-effective solution that provides visibility across the network through a security/risk lens.

**Compliance:** VSOC is focuses on Identify, Detect and Respond functions, based on the NIST CSF (Cyber Security Framework). Reports are generated that can use to prove monitoring of the network is taking place, thus proving compliance with the relevant audit and regulatory rules.

### The MYREDFORT VSOC

**Extra Resource:** Businesses can't hire enough cyber analysts to investigate alerts coming from their existing systems. VSOC provides tools that alert existing cyber teams to respond straight away.

**Reduced Costs:** Ultimately, VSOC leads to reduced cost of ownership due to the absence of an appliance and the corresponding complexities in appliance deployment and maintenance.

#### Key Benefits

- **Deploys in Minutes:** Traffic from your on-premise or cloud network can be securely connected in no time. Our Network Native approach works without the added cost and complexity reconfiguring your network of adding hardware or software appliances.
- **Discovers Your Network Assets:** The service quickly builds an understanding of the assets, gateways, and subnets that make up your network. It integrates with a wide range of Configuration Management Database (CMDB) systems to ensure asset inventories are up-to-date and immediately flags any unidentified assets or networks.
- **Learns Network Behaviours:** With its continuous learning capabilities, it builds and maintains a baseline of over 35 different aspects of the traffic patterns on a network. The core technology was funded and validated by US Intelligence agencies and Department of Defense (DoD), so it's built to work in real-world environments.
- **Alerts on Policy Violations:** It provides an important check on protective controls, such as firewalls and anti-virus software, to ensure that they are configured and running properly and have not been tampered. It also ensures compliance with relevant parts of ISO-27001, CSF by proving that your network traffic has been conforming to those requirements.

## WHAT IS A VSOC?

---

### The MYREDFORT VSOC

- **Detects Threats Behind Your Firewall:** The VSOC is like having a team of experts analysing network traffic, detecting anomalies and policy violations. It then triages the alerts, notifying you of anything serious occurs.
- **Measures Your Progress:** A Network CyberScore is calculated that can be used to measure network risk over time, and see how that risk compares to your goals. Weekly executive reports highlight trouble spots on the network that require additional attention. These reports can be used to communicate to the board of directors, partners, or regulators how much safer your network is.

## SPEAK TO OUR TEAM TO EXPLORE HOW WE CAN SUPPORT YOUR ORGANISATION

---

T: +44 (0) 1483 310 239

E: [sam.redwood@myredfort.com](mailto:sam.redwood@myredfort.com)

W: [www.myredfort.com](http://www.myredfort.com)