Security Operations Centre (SOC) & Security Information Event Management (SIEM)

(Protective Monitoring)

Overview

SIEM tools are an important part of the data security ecosystem: they aggregate data from multiple systems, monitor and analyse the network in order to identify abnormal behaviour or potential cyberattacks. SIEM tools provide a central place to collect events and alerts and provide a unique overview – but can be expensive, resource intensive, and customers report that it is often difficult to resolve problems with SIEM data.

Capita's Managed Security Services (MSS) capability provides industry-leading cyber security design, implementation, monitoring, management, threat intelligence and incident response expertise.

Our dedicated Security Operations Centres (SOCs) (also sometimes referred to as protective monitoring) are staffed with vetted and vendor-certified cyber professionals. They are locally based, managed within the UK, and are centres of excellence for our MSS capability.

The key aims of a SOC are:

- Provides comprehensive cyber expertise to protect organisations, staff, and citizens
- Manage solutions which protect your organisation's data from internal/external threats
- Secures applications and data access in the cloud and on-premise
- Delivers confidence and risk assurance for service users and staff
- Reduces risk of attack outages, through cyber health-checks and remediation

Capita

Our approach

- Capita start by understanding your customer's unique business needs, capturing requirements from business and technology stakeholders
- Define and document the IT assets to be brought within the scope of the service
- Agree priorities and produce designs and plans accordingly
- Where appropriate, we deploy and analyse information using discovery and migration tools to further update designs and plans
- Our programme and project managers ensure the transition, migration and implementation of the services following industry standard Prince2 methodologies
- Where requested, Capita can provide appropriately security cleared staff

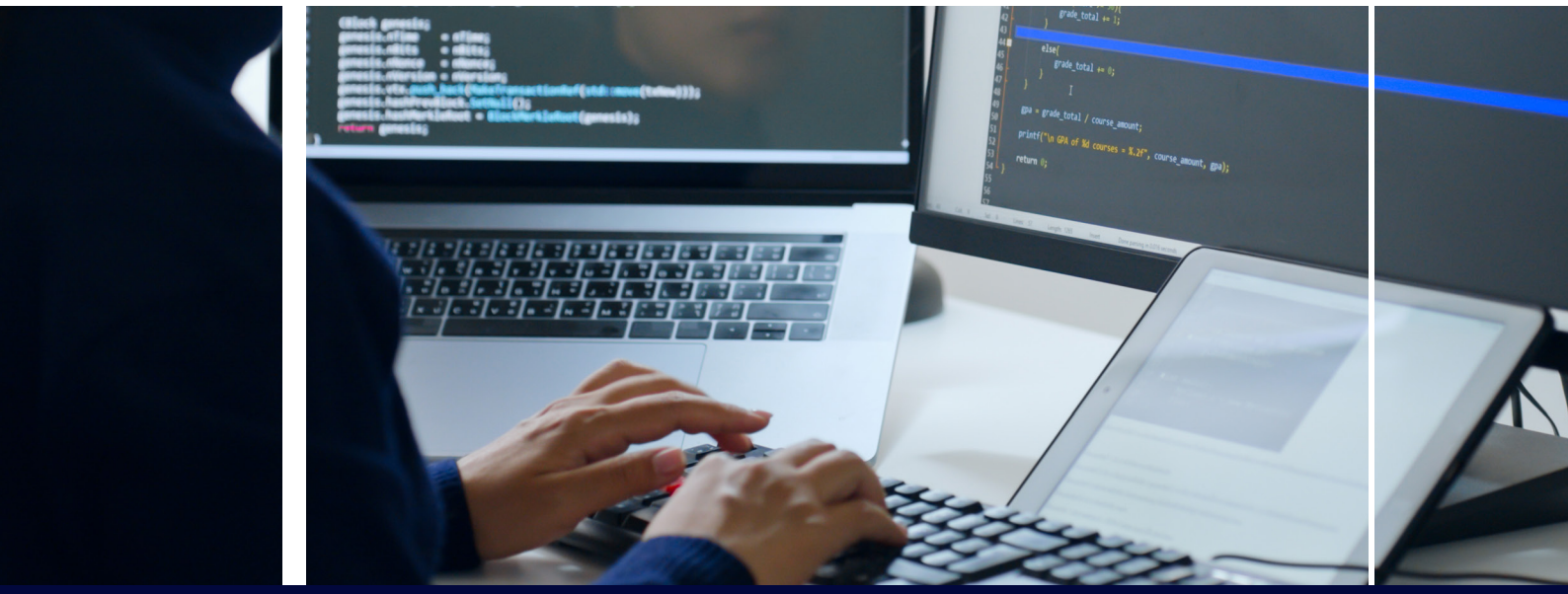
Implementation and Response

The SOC will be responsible for:

- Liaising with your business contacts in order to resolve Incidents
- Notifying your business of Capita identified Incidents
- For Incidents relating to the performance of a service, investigating and coordinating activities to affect a resolution
- Updating your business on the status of outstanding Incidents
- Maintaining an Incident Log of outstanding Incidents

Markets / Industries

- All



For more information please contact:

Jim Fox CISM, MBCS, MSyI
James.fox2@capita.com