DETECT: SECURITY OPERATIONS CENTRE

Security Information & Event Management

Carbon Neutral Organisation

Cyber Security Services

Security Services

- Predict
- Prevent
- **Detect**
- Respond
- Regulation & compliance

Overview

Remote Monitoring - 24 x 7 x 365

- Hypervisors
- Servers
- Storage
- Switches
- UPS

Remote Log Collection

- Appliances
- Applications
- Servers
- Services

Incident Response

- Threat information feeds
- Log data analysis
- Anomaly detection

Security of data is now the most important consideration for any organisation.

Our Cyber & Security Practice provides advice and services that **ensure** you are protected against the ever-changing threat landscape, helping you to predict, prevent, detect and respond to malicious attacks

Business Value

Our Threat Detect service combines managed SIEM (Security Information & Event Management) with our active response measures to keep your staff, applications and systems secure at all times.

Overview of Service

eacs Threat Detect provides a 24 x 7 x 365 incident response team to identify threats at any time of the day or night and notify the appropriate contacts.

This service combines the remote monitoring of IP enabled devices with remote log collection to gain insight into your environment. We then feed in multiple threat intelligence sources to help us identify common suspicious traffic and events and alert you to it.

After a baseline period allowing us to get to know your environment and usual traffic, we will then use our systems and engineers to identify the obvious and the more discrete suspicious activity that you should be aware of.

Although primarily security focussed, we look for any event which may cause disruption to your operations, including hardware or software failures.

Our Threat Detect team has extensive experience in monitoring and responding to incidents for large online websites, national and international brands during high volume time periods. This includes gambling sites during major sporting events, large airports during peak holiday seasons, online ticketing vendors during ticket releases and online retailers during peak shopping times.

Additional Services

eacs has a range of solutions and services that follow the proven industry model of Predict, Prevent, Detect and Respond. Discover vulnerabilities in your systems and remediate them, before they are exploited by someone else (predict). Significantly reduce the risk of damage from cyber attacks (prevent). Monitor applications, systems, and networks for intrusions and suspicious behaviour (detect). Recover systems and data; perform forensic analysis and bounce back stronger (respond).

In addition to IT security solutions and services, eacs can help your organisation to attain and maintain Cyber Essentials, ISO27001 and GDPR compliance.

Summary

The Threat Detect service is delivered from an established ISO27001 certified Security Operations Centre (SOC). A cutting edge, always on operation ensuring that your systems are supported by qualified, experienced staff, working to best-in-class processes and service levels.

eacs is the expert in the delivery of IT services to the mid market. It is an award winning and trusted provider of IT solutions and managed services to a wide range of UK organisations of all sizes. Founded in 1994, eacs supplies practical, innovative and cost-effective IT products, solutions and services to businesses. Solutions include infrastructure, end user computing and systems management. Our services range from ad-hoc consultancy, support and training through to fully managed or hosted IT systems. Partnerships with market leading manufacturers means eacs is positioned to provide organisations with the highest level of expertise and quality.

Some of our partners:

DELL Technologies Authorized Partner
Citrix Partner Gold Solution Advisor
DARKTRACE
paloalto NETWORKS
NEXTWAVE INNOVATOR
netwrix
thycotic
PC Partner Lenovo Silver
Data Center Partner Lenovo Gold
Partner First Gold
mimecast Premier Partner
mimecast Managed Service Provider
NetApp GOLD PARTNER PROFESSIONAL SERVICES SUPPORT SERVICES
Sophos Platinum Partner
Microsoft Partner Gold Cloud Platform Gold Cloud Productivity Gold Collaboration and Content
Bitdefender RESELLER SILVER

ISO accreditations:

- **ISO 9001** - Certified Quality Management System
- **ISO 14001** - Certified Environmental Management System
- **ISO 20000**—Service Management
- **ISO 22301** - Certified Business Continuity
- **ISO 27001** - Certified Information Security Management System
- **ISO 37001** - Certified Anti-bribery Management System
- **ISO 45001** - Certified Occupational Health & Safety System
- **Cyber Essentials & Cyber Essentials Plus**