

# BDO MANAGED SECURITY SERVICES

DETECT IN DEPTH



## Why Managed Security Services?

With the emerging cyber security threats and challenges organisations face today, a preventative controls framework is no longer a fully effective strategy for mitigating information security risks. As attacks and threat actors get sophisticated and ubiquitous, organisations are realising that proactive management and testing is needed and that a rapid detection and response capability is an integral part of their security strategy.

Do you know what assets you have? How do you identify rogue access points and devices on your network? How do you monitor your network and identify suspicious events? Are you including the latest threat intelligence to respond rapidly to the constantly-evolving cyber threats? Are you proactively testing your environment for the latest vulnerabilities and keeping up with changes to controls? BDO's Managed Security Services helps to answer these questions by building your capability.

### OUR SOLUTION

BDO's solution includes a fully managed detection and response (MDR) service to detect, analyse and respond to security incidents. Our fully Managed Security Services such as Vulnerability Management Services and cyber defence capabilities support this solution, where BDO can use its in-house technical subject matter expertise to fully manage security services on behalf of our clients.

### Through our Managed Security Services we are able to:

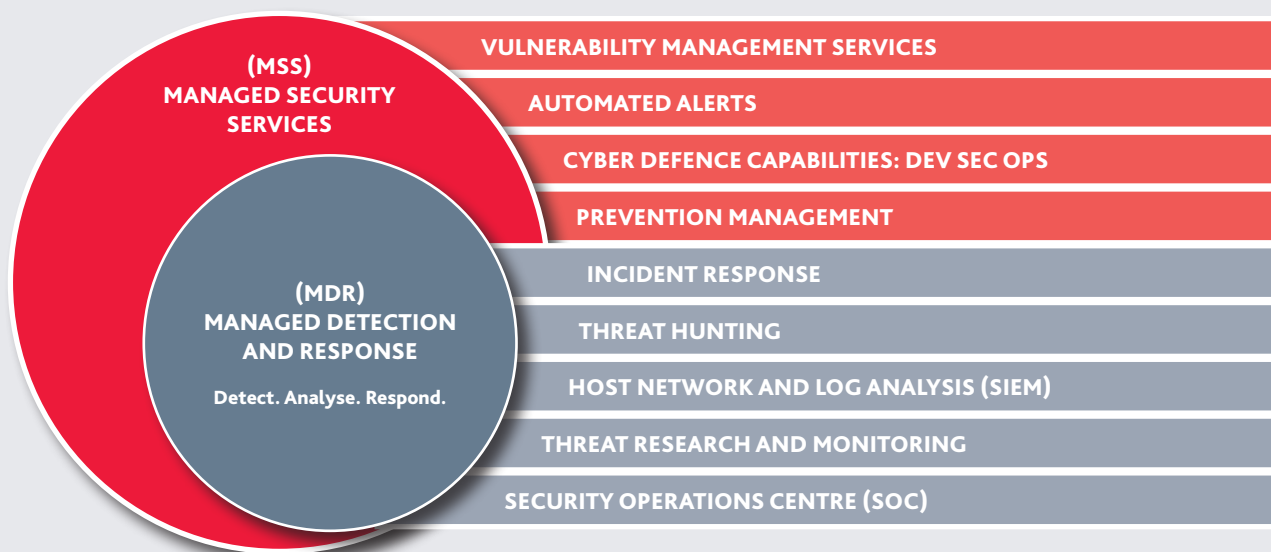
- Deliver a coordinated operational and technical approach to ensure security of you data and systems (24/7/365 service)
- Provide peace of mind that malicious activity and anomalous behaviour are detected, identified, classified and acted upon when and where appropriate.
- Facilitate an extension of your internal team, providing flexible scalability in building capability, capacity and personnel
- Deliver the cost benefits of operating at scale to an organisation of any size.

### Our Team

- BDO are a CREST and FIRST accredited team, providing worldwide coverage
- All team members performing penetration testing are industry certified (SSCP, CEH, CHFI, LPT).

### OUR METHODOLOGY

To establish a threat focused approach for security, organisations need to adopt a model defining the relationships between threats, assets and controls.



## BDO INCIDENT RESPONSE CAPABILITY

Our incident response capability provides an organized approach to addressing and managing the aftermath of a security breach or attack, handling the situation in a way that limits damage and reduces recovery time and costs.

BDO follows the kill chain methodology to respond to a Cyber Security Incident. When BDO responds to an incident we perform a complete kill chain analysis, including prior phases, to identify root causes and advise on the best course of action to mitigate future intrusion.

### Our service enables:

- A global Incident Response capability, including Red Teaming
- In-house advanced malware and reverse engineering team skills
- Full network packet capture, with threat detection including Demisto, Iron WASP, Palo Alto Traps
- A fully managed vulnerability scanning programme
- Analysts around the clock
- A team to respond to any queries and interpret results, removing false-positives.



## ADVISE, TRANSFORM, RUN

## BDO: A single source for Cyber resilience

**Advise:** We help our clients identify and understand their cyber risks.

**Transform:** We can help remediate identified issues and improve cyber resilience with the help of 'best in class' technology partners.

**Run:** Finally, where appropriate, we can provide a fully managed cyber security service so that our clients have peace of mind and assurance that their organisation is ready to face cyber threats.

For more information: BDO CYBER SECURITY TEAM | +44 (0)203 219 4582 | [cyber@bdo.co.uk](mailto:cyber@bdo.co.uk)