advanced
People. Partnership. Solutions.

Cyber Security Services
Managed Detection and Response Services

In today's connected world, securing your business is a necessity. Our Cyber Security Services are delivered in modules to improve your security and reduce risk for your organisation - while you focus on driving business success. We aim to be the fastest to find the threat and then fix the issue across Cloud, hosted and on-premise IT infrastructure.

Our Managed Detection and Response (MDR) Services, a specific package available within our Cyber Security portfolio, are designed to deliver everything you need to secure your IT system. We have partnered with award-winning cyber security specialists, Alert Logic, who support our offering with their powerful Professional and Enterprise platforms. For our Standard and Enhanced MDR Services, Alert Logic Professional provides visibility into your environments (Cloud, on-premises or hybrid), and helps you identify the remediation steps required to reduce exposures. You get an intrusion detection system that includes security monitoring and threat analysis from certified security experts to help you detect threats and eliminate vulnerabilities. Their Enterprise platform works with our Premium MDR offering, which offers additional solutions for our customers including Web Application Firewall (WAF) and Distributed Denial of Service (DDoS). These add-ons are most suitable for high-risk technology and web applications.

Benefits

- Tiered and extensive security protection delivered as a service
- Multi-Cloud platform detection, response and mitigation services
- Advanced leverage access to Global Information Assurance Certification qualified threat intelligence and security experts
- Improved ability to understand your state of compliance
- Reduce risk and eliminate vulnerabilities to improve your security posture
- Help protect your business by leveraging automated scanning and asset discovery
- Free up resources with informed advice and remediation steps from our highly qualified and experienced specialists
- Meet regulatory compliance mandates and deliver industry best practice, helping to secure your business
- PCI-DSS, GDPR, HIPAA, SOX, SOC2, ISO and NIST
- We are ISO27001 accredited. In addition, we also utilise a range of security frameworks to ensure best practice and transparency.

Service boundaries and customer obligations

Customers are responsible for:

- Custom and third party applications outside of the scope of Advanced Managed Services
- Change control and notification to the Advanced Service Desk prior to change of web applications and devices under security controls
- Providing Advanced staff with access to required people and systems in order to assess, design, deploy and manage the selected security solution
- Communicating any regulatory and compliance or other security requirements during any discovery, assessment and design engagements

Boundaries of service

- See below table of in-scope sites, platforms, applications and infrastructure

Why Advanced?

For over 15 years, our team of experts has successfully managed IT and information security for a vast range of organisations. We have actively sought accreditations to ensure that the services we deliver meet the most rigorous of standards. By partnering closely with you, we can develop and execute a strategy that will suit your needs, and create a secure and compliant environment for your employees and customers. Our leading technologies, successful collaborations and streamlined automation mean you can make the most of your IT infrastructure – and secure your future as a competitive organisation.

Service to platforms and technology compatibility:

Service	OS and devices	Cloud platforms	Applications	Containers
Standard and Ehanced	> Windows and Mac OS	> O365 (logging)	> Packaged apps > Middleware	> Docker > Kubernetes
Premium	> Windows 2003 and 2008 > Windows 2012 and 2012R2 > Linux > Windows 2016 > Network appliances (syslog) > Software-as-a-Service applications (subject to logging) > Firewalls and proxies (syslog)	> AWS and Outpost > Microsoft Azure and Azure Stack > Google Cloud > Hosted > On-premise	> App frameworks > Dev platforms > Databases > Middleware	> Elastic beanstalk > Elastic container service > CoreOS

Integrations with third-party malware and endpoint protection central logging access. Parsers for improved log search capabilities, including saved searching with notifications every 15 mins, may be subject to extra charges. Many parsers are available for industry-leading products.

Priority-based response times: P1: 15 mins, P2: 4 hours, P3: 24 hours	**Standard** **Threat Detection and Incident Managemnet 24x7**	**Enhanced** **Standard+** **Vulnerability Intelligence, Configuration Checks and Third Party Co-ordination**	**Premium** **Custom add-ons to the Enhanced services**
	Cyber Security Discovery Services+ Secure log collection, threat monitoring, intrusion detection and expert response	Standard Services+ Proactive vulnerability and exploit identification and remediation with third party co-ordination	Enhanced Services+ Advanced Cyber Defence, Security threat and anomalous behaviour detection
Services	Manage > Security log collection and management and 12 months minimum secure storage > Collection agent and appliance management > Specialist cyber security skill set Detect > Threat intelligence > Security analytics > Security event detection > Network traffic threat analysis > Anti-virus integration > Encrypted secure sockets layer interception capability > Intrusion detection > Cloud and on-premise Cloud logs (AWS security hub, CloudTrail, other PLatform-as-a-Service logs, Azure AD, Event Hub, activity logs) Azure and Amazon Web Services (AWS) user behaviour anonmaly > Office 365 and application log collection with search Respond > 24/7 incident security team response > Security team lead incident management Expert SOC analysts Threat triage Escalation and repsonse Organised containment and eradication End-to-end incident management and recovery > Event classification and response > Communication and co-ordination of service teams > Security remediation advice, may lead to chargeable consultancy	Manage > Standard Services+ additional log sources from external Cloud services Detect > Vulnerability intelligence scanning for enhanced detection > Cloud vulnerability detection with security configuration checks > Asset discovery and visibility > Compliance gap identification > Integration Domain Name System (DNS) monitoring (additional service tooling) Respond > Prerventative advice for security issues highlighted in reports > Malware analysis (if Malware Protection Service has been selected) > Configuration remediation > Third party supplier co-ordination for incident management > Supported digital forensic activities Report > Vulnerability intelligence report and PCI scanning reports provided to you on a monthly basis	Advanced Cyber Defence option (requires additional tooling) > Named security analyst > Integration with Data Loss Prevention > Dark web scanning (compromised credentials) > Proactive threat hunting > Security posture improvement and tuning, help with policy and best practice development > Integration with online security services (WAF & DDoS) Security Threat and Anomalous Behaviour Detection option (requires additional service tooling) > Artificial Intelligence-enabled systems for behaviour analysis > Latest generation security analytical service management > Brand protection and digital footprint monitoring and response Report > Monthly business reviews with extended content as a result of selection additional options

Services	Report > Monthly business reviews, threat index advice and remediation guidance		
Security Platform	> Estate and asset discovery > Vulnerability scanning > Compliance > Cloud configuration checks > Threat monitoring and visibility > Intrusion detection > Security analytics > Encrypted SSL interception capability > Advanced detection capabilities to spot and block malicious activity > Secure log collection and monitoring > Complex log search capabilities > Office 365 log collection and search > Anti-virus and Cloud vendor integrations		
Threat Intelligence	> Threat risk index > Advanced persistent threat research > Lost and stolen data searching > Expert intelligence informed by hacking group profiling > Intel-based escalation for incident response > Monitoring for bugs, vulnerabilities and exploits > Intelligence community participation User behaviour anomaly detection > Threat frequency, severity and status intelligence > Attack protection advantages > Comprehensive vulnerability library		> Dark web scanning, looking for compromised credentials

More information

w oneadvanced.com
t +44(0) 8451 605 555
e hello@oneadvanced.com

Ditton Park, Riding Court Road, Datchet, SL3 9LL