

MANAGED DETECTION AND RESPONSE SERVICE

THE KEY TO WINNING TODAY'S SECURITY BATTLES

Many cyber security professionals agree that improving threat detection is more difficult to achieve than it was just two years ago. Escalating volume and complexity of threats as well as a shortage of skilled security practitioners is leading to a shift from products to services.

The challenge of facing too many threats is increased by too many disparate tools and not enough people to effectively deal with them. Managed Detection and Response (MDR) services can bridge security gaps, providing access to advanced technology and skilled resources as and when needed to ensure that organisations can achieve their objectives. At CSI, we offer a partnership that gives you a perpetual edge over cyber security threats. Our advisory, professional and managed security services are brought together by a methodology that puts the reduction of risk at the heart of everything we do and ensures successful delivery of the security outcomes that underpin your business.



Moving Beyond Alerting with CSI and Alert Logic

A lot of managed cyber security services have their hands full simply with collecting alerts from the technology implemented to address cyber threats. MDR services do collate information from different systems, but they are also action-oriented to actively address the threats that they face in an efficient and effective manner.

CSI Managed Detection and Response Service

CSI's Managed Detection and Response Service helps organisations to secure their technology environments. CSI can augment real-time threat detection with threat hunting to mitigate any malicious actors that bypass existing prevention and detection capabilities.

CSI delivers MDR services in conjunction with leading security partner Alert Logic. Their award-winning security platform and cutting-edge threat intelligence enables us to identify and respond faster to attacks.

Our dedicated Security Operations Centre (SOC) experts will monitor your systems 24/7 and leverage a diverse range of data collection and analytics methods for rapid threat detection.

CSI SERVICE OPTIONS

- Essentials Service Level**

The Essentials service includes asset discovery, vulnerability management and next-generation endpoint threat protection & detection.

- Professional Service Level**

The Professional service includes all 'Essentials' services plus enhanced threat protection and detection, and PCI services.



GROW



SAVE



INNOVATE



PROTECT

CSI Managed Detection and Response Service

SERVICE LEVEL	ESSENTIALS	PROFESSIONAL
Asset Discovery		
Agent and cloud API-based asset discovery	✓	✓
Full documentation of CIDR-based network information within portal	✓	✓
Vulnerability Management		
Internal vulnerability scanning against all network assets	quarterly	monthly
External vulnerability scanning against Internet facing assets	quarterly	monthly
Identification of vulnerabilities caused by mis-configurations in public cloud environments	✓	✓
Cloud configuration checks / CIS benchmarks	✓	✓
Threat Detection and Prevention		
Next-generation endpoint threat protection and detection	optional	✓
Collection and review of logs from all customer dedicated compatible assets		✓
Network monitoring		✓
File integrity monitoring		✓
Web log analytics		✓
User behaviour monitoring		✓
PCI Services		
PCI approved log review		optional
PCI approved scanning vendor vulnerability scans		optional
PCI compliance management and assistance in dispute resolution		optional
Web Application Firewall		
Managed in-line web application firewall (priced per 5 unique application profiles)		Enterprise licensing
Threat Hunting		
Named threat hunting analyst		Enterprise licensing

SUPPORT LEVELS	ESSENTIALS	PROFESSIONAL
Service Desk - Core Hours	✓	✓
Service Desk - 24x7 (critical and high events)		✓
Incident Management	✓	✓
Security Operations Support	✓	✓
Report frequency	quarterly	monthly
Cadence reviews	quarterly	monthly
Service Level Agreements	✓	✓
Alert Logic portal	✓	✓
CSI Service Delivery Manager	optional	optional

CSI UK Head Office

CSI House
2940 Trident Court
Birmingham Business Park
Solihull Parkway
Birmingham B37 7YN

T +44 (0)800 1088 301

E info@csiltd.co.uk

W www.csiltd.co.uk