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 Fortra

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 Fortra. Its award-winning Alert Logic MDR 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's MDR Services eliminates threats both pre-breach and post-breach:

- **PRE-BREACH**

Reduces the likelihood of attacks by addressing threats vulnerabilities and configuration issues

- **POST-BREACH**

Reduces the impact of a successful attack via rapid detection, notification and recommended response guidance.

GROW SAVE INNOVATE PROTECT

CSI Managed Detection and Response Service

SERVICE ELEMENTS	FEATURES	
Asset Discovery	Agent and cloud API based asset discovery	✓
	CIDR based network information within Fortra's Alert Logic portal	✓
Vulnerability Management	Internal vulnerability scanning against all network assets in scope of the service	Monthly
	External vulnerability scanning against Internet facing assets	Monthly
	Identification of vulnerabilities caused by misconfigurations in public/private cloud environments	✓
	Cloud configuration checks / CIS benchmarks	✓
	Remediation/mitigation of Critical/High Vulnerabilities (as per CSI Vulnerability Management policy) where in scope of service	✓
Threat Detection	Next-generation endpoint threat protection & detection #	Optional
	Central collection and review of logs from Client dedicated compatible assets (as scoped)	✓
	Custom Correlations ##	✓
	Network monitoring (Intrusion Detection System - IDS)	✓
	File integrity monitoring	✓
	Web log analytics	✓
	User behavior monitoring	✓
PCI Services	PCI approved log review	Optional
	PCI Approved Scanning Vendor (ASV) 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
# Endpoint threat protection & detection service subject to additional scoping if required as part of overall solution		
## Custom correlations limited to 20 correlations per 50 nodes/log sources		

SUPPORT ELEMENTS	
Service Desk - core hours	✓
Service Desk - critical and high priority events	✓
Incident Management (managed infrastructure)	✓
Incident Management (client managed infrastructure)	✓
Security Operations Support	✓
Cadence calls *	Monthly
Service Reports	Monthly
Service Level Agreements	✓
Fortra's Alert Logic Portal	✓
* A remote meeting with a SOC analyst to present findings and analysis of the previous month's activity. Cadence calls will typically include discussion of threat events, devices added, license count review and agent update rollouts.	

CSI Ltd Head Office

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

CONTACT
+44 (0) 800 1088301
info@csiltd.co.uk
www.csiltd.co.uk