VULNERABILITY SCANNING ESSENTIALS

PROACTIVE PREVENTION AGAINST CYBER EXPLOITATIONS

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 cyber security 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.

FORTRA

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. CSI's 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.

Hybrid Asset and Risk Discovery
Fortra's Alert Logic platform has been built to provide a common view on asset vulnerabilities and configurations on all environments. The dashboards show relevant information that allows targeted response and analysis of those things that affect security posture.

Endpoint Detection and Response
Endpoint protection prevents multiple attack techniques that try to compromise endpoints. Multi-vector attack monitoring and isolation recognises these techniques and stops them early before any damage is done. It uses signature-less machine learning to stay ahead of attackers and zero-day attacks, identifying malicious techniques and ransomware in real time and isolating the payload and remediation progress.

Essential Compliance Coverage
Our Vulnerability Scanning Essentials service provides complete compliance solutions that give clients peace of mind and deliver on best practices for PCI DSS compliance, GDPR, and other mandates. Cloud industry best practices can be reported in real-time through certified CIS Benchmarking for Azure and AWS.

GROW   SAVE   INNOVATE   PROTECT

CSI's Vulnerability Scanning Essentials Service

In order to protect an organisation, security teams must have visibility into deployed assets, misconfigurations, and vulnerabilities across the entire IT estate. Vulnerability Scanning Essentials provides 24/7 hybrid visibility and vulnerability scanning, audit-ready reporting, and endpoint detection and response.

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	Weekly
	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	✓

SUPPORT ELEMENTS	
Service Desk - core hours	✓
Service Desk - critical and high priority events	✓
Incident Management	✓
Security Operations Support	✓
Cadence calls *	Monthly
Service Reports	Monthly
Service Level Agreements	✓
Fortra's Alert Logic Portal	✓
Service Delivery Manager	Optional
* 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.	

Additional Cyber Resilience Services from CSI

• Managed Web Filtering
• Managed Endpoint Protection
• Managed Phishing Defence
• Endpoint Privilege Management
• Vulnerability Assessment
• Extended Detection and Response