EXTENDED DETECTION & RESPONSE SERVICE (XDR)

A UNIFIED CYBER SECURITY SOLUTION

Extended Detection and Response (XDR) identifies and addresses cyber threats across an organisation's entire digital environment, including its network, cloud storage, applications, and endpoints.

Cloud and mobile technologies provide significant opportunities for digital transformation, but they also dramatically expand the cyber-attack surface, leaving coverage gaps which can be exploited. When cyber-attackers can target endpoints, users, networks, cloud, and applications, effective cyber security must move past endpoint protection, no matter how effective. Just as much effort should be invested in mitigating the effects of breaches when they do occur.

Threat Prevention

CSI's first priority is to make every effort to prevent malware attacks. Sophisticated AI models are leveraged to recognise and prevent the execution of malware and zero-day attacks. However, if a breach occurs, this approach can't determine why it happened.

Context Analysis and Root Cause Analysis

Not all cyber-attacks are via malware; social engineering phishing, exploiting known vulnerabilities in widely-used applications or employees side-stepping security policies. Only a consolidated enterprise-wide view can identify seemingly innocent activities that are only revealed as malicious in the context of other security events.

Technology Optimisation

Security technology is only as good as it's configuration and management – and configurations drift out of 'best state' over time as an IT environment changes. Maximum security and return on investment are ensured by best-practice deployment, configuration and tuning. The end goal must be technology in a consistent state of prevention for the lifetime of the solution.

SOC Expertise: 24x7x365 Proactive Threat Hunting

Proactive threat hunting is most effective when driven by human analysts working together with self-monitoring endpoints and a unified correlation platform to detect and trace attacks. Advanced orchestration, playbooks, triage, and filtering methods can be custom tailored for each client.

Extended Detection and Response (XDR) Service

Services are provided by CSI's security operations centre (SOC) team supported by Blackberry's CylanceGUARD security experts.

NOTE: this service has a minimum of 100 devices.

BlackBerry Cybersecurity

SERVICE ELEMENT	MANAGED XDR
Service Management	
Service Desk - 24x7 for P1 incidents	✓
Incident Management	✓
Monthly cadence calls	✓
Service Delivery Manager	optional
Threat Prevention (EPP)	
Notifications ingested into CSI SOC via API integration	✓
CSI SOC triage all threats and complete remediation where applicable	✓
Custom policies can be set up where appropriate	✓
Exclusions (file or directory) required during and after onboarding phase	✓
Control use of USB mass storage devices	✓
Stop unauthorised scripts from running	✓
Restrict new applications from being added to user devices	✓
Prevent malicious use of memory	✓
Context Analysis and Root Cause Analysis (EDR)	
Monitor endpoints for malicious and suspicious activity via Context Analysis Engine	✓
Alert and event data stored in the cloud for offline analysis	✓
Root cause analysis of cyber incidents	✓
Automated containment and remediation response	✓
Customised response playbooks	✓
Collect, aggregate and present endpoint data via IQ searches	✓
Rapid restore of compromised systems to pre-threat state	✓
Technology Optimisation	
Deployment of Blackberry Cylance technology	✓
Initial configuration in passive mode	✓
Review of alerts and recommendations to clear false positives	✓
Active configuration of agreed policies	✓
Annual review of policies as environment changes	✓
24x7x365 SOC Expertise	
Management of policy settings to facilitate response readiness	✓
Managed detection and response – from alert to closure	✓
Proactive Threat Hunting	✓
Ongoing collection of artefacts from client environment to identify unidentified threats	✓
Communicate with client for all newly identified threats	✓
Access to CylanceGUARD XDR unified platform	✓

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