Bridewell

Microsoft Intelligent Security Association

Microsoft Security

Microsoft Verified Managed XDR Solution

Microsoft Solutions Partner Security Specialist Cloud Security Threat Protection

Incident / Breach Response and Forensics

We offer a comprehensive rapid incident response service to provide expert advice and expertise to your business when it needs it the most. Our services can help your business prepare for, respond to, and resolve incidents. Common threats our incident response services help to address include:

- Business email compromise
- Credential or data breaches
- Advanced persistent threats (APT)
- Financially motivated crime
- Malware, Trojans and backdoor attacks
- Web application attacks
- Insider threats

Service Description

Microsoft Defender for Endpoint can be deployed within hours of an initial breach, with GIAC certified analysts in our CREST accredited Global SOC on hand 24/7 to begin analysing network traffic and information from thousands of endpoints. We will investigate initial client-provided leads to start building a threat profile, that will identify attacker activity while scanning the wider network.

We will monitor real time attacker activity, whilst searching for forensic activity of past actions and to establish dwell time and previous actions. In-depth analysis will be conducted to determine the initial attack vector and extent of the compromise.

Analysis can include:

- Live response analysis, directly on the endpoint
- Forensic analysis
- Network and traffic analysis
- Log analysis
- Dark web monitoring
- Malware analysis

Bridewell will work with your technical team to develop a custom containment and remediation strategy, based on the actions of the attacker and taking into consideration your organisation's requirements to eliminate the attacker's access, remove malware and improve the overall security posture of the environment.

What's Included

- XDR Technology
- Highly skilled incident response professionals
- Intelligence led incident response leveraging the Bridewell CTI team

Solution Outcomes

- Rapid and effective response to reduce the impact of a cyber incident
- Customisable service agreement to suit your organisation's requirements
- Rapid access to a wide range of cyber security, forensics, incident response and business advisory experts
- Highly customised remediation action plan that balances the business and security needs of your organisation
- Bridewell's technology allows the team to respond to and resolve complex incidents faster and more effectively, resulting in fewer affected hours incurred and lower costs.

Bridewell

Microsoft Intelligent Security Association

Microsoft Security

Microsoft Verified Managed XDR Solution

Microsoft Solutions Partner Security Specialist Cloud Security Threat Protection

What Our Customers Are Saying

"Bridewell have been exceptional. We have quickly moved from an operation that is fighting noise with the incumbent, to having actionable incidents and increased visibility."

MAG

About Bridewell

Bridewell is the trusted cyber security partner for organisations operating within Critical National Infrastructure (CNI), as well as companies who want the highest standard of cyber security. Our team are highly accredited by major industry bodies and have extensive experience of delivering cyber consulting and managed security services across highly regulated sectors. As a long-standing Microsoft partner, our team are experts in maximising the effectiveness of Microsoft Security technology to deliver robust and effective solutions.

We have a deep understanding of the challenges faced by CNI organisations and how to resolve them. We work in continuous partnership with our clients to implement the right security solutions to defend and protect them against threats and attacks, allowing them to continue operating safely and securely.

Get in Touch

+44 (0)3303 110 940

hello@bridewell.com

bridewell.com

Assured Service Provider – In association with National Cyber Security Centre – Cyber Incident Exercising; Consultancy: Risk Management; Consultancy: Audit & Review; CHECK Penetration Testing; Cyber Incident Response (Level 2); Consultancy: Security Architecture; Cyber Resilience Audit

UK Civil Aviation Authority ASSURE

AICPA SOC 2

CREST VA PEN TEST SOC CSIR

CfA ISO 27001 UKAS

CfA ISO 9001 UKAS

Crown Commercial Service Supplier

PCI Security Standards Council

IRAP 27701:2019

CYBER ESSENTIALS