

# Bridewell

## 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, which 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

Member of  
Microsoft Intelligent  
Security Association



# 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

## 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.”

Head of Cyber Security Operations  
Manchester Airport Group



# About Bridewell

Trusted globally by highly-regulated and complex organisations to deliver tailored cyber security, managed security, penetration testing and data privacy services, providing protection against cyber attacks and driving continuous transformation.

Bridewell are a PCI DSS QSA company with NCSC, CREST, ASSURE, IASME Consortium, SOC2, Cyber Essentials Plus, ISO27001, and ISO9001 accreditations. It's award-winning team of experts, comprised of highly trained and certified consultants work closely to understand organisations key challenges and ambitions, creating flexible outcome-focussed solutions to strengthen cyber security posture, ensuring business continuity by keeping them protected and productive from the inside out.

In today's ever-changing digital economy, the importance placed upon critical infrastructure cannot be underestimated, with clients in sectors including transport and aviation, financial services, oil and gas, government and communications. Bridewell can be trusted to deliver solutions that keep critical services running and ultimately deliver real business impact. **Together.**

Call the Bridewell team on 03303 110 940  
or email [hello@bridewell.com](mailto:hello@bridewell.com)



+44 (0)3303 110 940  
[hello@bridewell.com](mailto:hello@bridewell.com)  
[bridewell.com](https://www.bridewell.com)

