

Bridewell

# Bridewell

Cyber Security.  
Where it Matters.

## Managed Security Services Definition Document



 Cyber Consulting  Managed Security  Penetration Testing  Data Privacy

# Services Guide

Bridewell provides information assurance and cyber security advice under the specialist cloud services of the G-Cloud framework. Bridewell focuses on providing high quality information security and risk consulting services at competitive prices.

We provide, if required, industry-proven consultants with the highest levels of security clearance. We are able to quickly and efficiently provide solutions by simply focusing on the best qualified consultants to meet your needs.



# About Bridewell

Bridewell works together with our customers to support their digital transformation agenda by ensuring we improve cyber security, together.

Cyber security is critical for your business, and we work with you to embed it throughout your organisation to protect your people, processes and systems.

Creating a secure business empowers confident transformation, enabling you to open new markets and revenue streams while proving the ROI of your cyber investment.

With our team of award winning, industry leading experts, and cyber security, penetration testing, data privacy and managed security services, you can create competitive advantage and enable long-term business growth.

Established in 2013, Bridewell is a leading cyber security partner for organisations of critical national importance and is an Assured Service Partner working with the NCSC.

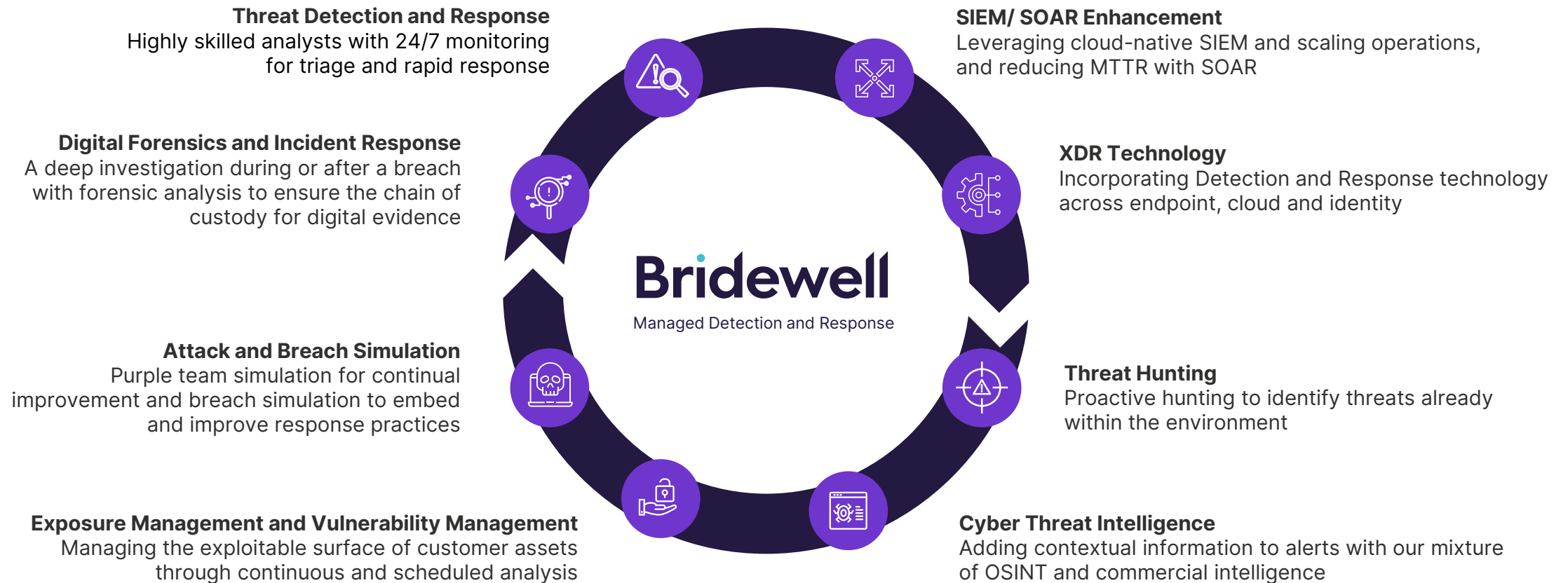
Bridewell is the UK's leading cyber security partner for organisations operating within Critical National Infrastructure (CNI), as well as companies in other highly regulated sectors who require the highest standard of cyber security.

Providing end-to-end cyber security services, including consulting, 24/7 managed security, data privacy and penetration testing, Bridewell work in continuous partnership with clients to implement robust security solutions which defend and protect against threats and attacks and allow organisations to operate safely and efficiently.

## Bridewell

# Managed Security Services

Our threat-informed approach to cyber security has helped our customers increase the effectiveness of their cyber defences, manage risk and prioritise budgets. To deliver this, Bridewell has a complete set of modern security operations services that include the following key components.



# 1.0 Managed Detection and Response (MDR)

**Bridewell's Managed Detection and Response (MDR) service delivers a leading 24/7, threat intelligence-led cyber defence service, delivered from the UK by a leading SC Cleared cyber security experts.**

By leveraging the latest in cloud-based SIEM and XDR technology, Bridewell provides a highly effective solution that addresses threats regardless of technology footprint. This is supported by Bridewell's continual growing security content library that integrates with and takes ownership of the incident response across on-premise equipment, OT, ICS, applications and DevOps.

## Features

- 24/7 UK-based, CREST-registered SOC with security cleared individuals.
- CREST and GIAC certified staff.
- Tiered service levels to provide optimal service requirements.
- Analysis and correlation of security information from cloud, on-premise and ICS systems.
- Inclusive of custom detection content development.
- Threat intelligence led security content development.
- Threat intelligence advisories.
- Threat hunting.
- Integrated threat intelligence feeds.
- Intrusion analysis.
- Intelligence integrated incident response.
- Blended human analysis and automated response.
- Supports a wide range of security technology.
- Clear depiction of coverage with MITRE ATT&CK.
- Cloud based SIEM technology, with UK data sovereignty.
- Proactive ownership of the incident response process.
- OT and ICS experience.
- Highly experienced in the delivery of a hybrid/ co-managed SOC to extend internal teams.
- SOC2 accredited service



# 1.0 Managed Detection and Response (MDR)

## Benefits

- Cost effective over traditional SOC and in-house services.
- Rapidly mature your detection and response capability.
- Doesn't limit incident response support to provider driven technology.
- Customised incident response plans and playbooks.
- Flexible and scalable service to meet all requirements.
- Able to rapidly deploy and transition to a leading Microsoft security stack comprising of Microsoft Sentinel and the full Microsoft Defender XDR product suite (if required).
- Cost, benefit management for cloud SIEM technologies.
- Continual integration of threat intelligence for the improvement of detection and response, along with risk management and the identification of preventative improvements to link into budget planning.
- Flexible contract terms.

## Pricing

Pricing of the MDR service is driven by the number of users and non-user allocated devices/ nodes.

Pricing is variable based upon the service tier and agreed scope.

Item	From (per month)
Users	£5.25
Servers	£3.04

Deployment costs vary based upon the technology and process integration requirements and are costed based upon the SFIA rate card, starting at £500 per day.

## 2.0 Managed SIEM and SOC

**Bridewells Security Operations Centre (SOC) aims to ensure our customers obtain the maximum value and performance from their investments in security technology through the integration of a highly experienced cyber defence team and established processes.**

Our managed SIEM and SOC services enable organisations to partner with Bridewell to build an effective SOC strategy that can also incorporate hybrid/ co-managed operating models.

### Features

- Analysis and correlation of security information from cloud, on-premise and ICS systems.
- Threat intelligence-led security content development.
- Integrated public and private threat intelligence feeds.
- 24/7 UK based, CREST-registered SOC with security cleared individuals.
- Supports a wide range of security technology. Clear depiction of coverage with MITRE ATT&CK.
- CREST and GIAC certified staff. OT and ICS experience.
- Highly experienced in the delivery of a hybrid/ co-managed SOC to extend internal teams.
- SOC2 accredited threat hunting
- Blended human analysis and automated response.



## 2.0 Managed SIEM and SOC

### Benefits

- Cost effective over traditional SOC and in-house services.
- Rapidly mature your cyber defence capability. Flexible and scalable service to meet all requirements.
- Able to rapidly deploy and transition to a leading Microsoft security stack comprising of Microsoft Sentinel and the full Microsoft Defender XDR product suite (if required).

### Pricing

Pricing of the managed SIEM and SOC is variable based upon the technology stack and agreed scope.

Item	From (per month)
Users	£5.25
Servers	£3.04

Deployment costs vary based upon the technology and process integration requirements and are costed based upon the SFIA rate card, starting at £500 per day.

## 3.0 Managed Cyber Threat Intelligence

Bridewell's Cyber Threat Intelligence (CTI) gathers information from our own threat research in addition to a range of open, private and trusted sources about current or potential attacks that are relevant to your organisation's sector and operations.

The information is analysed, refined, organised and prioritised by our cyber threat intelligence team so it can be used within your SOC, managed services and organisation to prioritise, minimise and mitigate cyber security risks.

### Features

- Threat landscape report generated and maintained.
- MITRE ATT&CK navigator report.
- Threat advisories.
- Analysis and correlation of data tracking malicious actors, campaigns, and breaches.
- Malicious infrastructure tracking provided by Bridewell's proprietary platform.
- Threat hunting.
- Provision of security content in sharable languages based upon TTP's observed within the threat landscape and MITRE ATT&CK reports.
- Monthly threat report.
- Request for intelligence.

## 3.0 Managed Cyber Threat Intelligence

### Benefits

- Enhanced ability to identify, assess, and mitigate cyber threats.
- Access to global threat intelligence and insights from Bridewell CTI.
- Strengthened cyber security posture through timely notification, expert analysis, and tailored threat intelligence.
- Reduced risk of security breaches.
- Improved understanding and response to emerging threats.

### Pricing

Item	From (per annum)
Managed CTI	£70,000

## 4.0 Incident Response Retainer

**Bridewell has a true, UK based 24/7 incident response function. An incident response retainer with Bridewell enables customers to have rapid, SLA backed access to Bridewell's SC-cleared incident response team whenever they are needed.**

The service will integrate and enhance your existing Incident Response processes and capabilities.

### Features

- NCSC Cyber Incident Response Level 2.
- NCSC assured Cyber Incident Exercising.
- CREST registered SOC.
- CSIRT Team comprising of responders, analysts, intelligence, incident management, testers and DevSecOps specialists.
- Investigations underpinned by intelligence bases analysis methodologies.
- Technical analysis including forensics, cloud, network and malware analysis.
- 24/7 SOC phonenumber.
- Service Level Agreement for response times.
- CREST and GIAC certified staff.
- Incident tabletop Exercises
- OT and ICS experience. Readiness assessment

## 4.0 Incident Response Retainer

### Benefits

- Immediate enrichment of your incident response capabilities.
- Cost-effective and scalable.
- Service Level Agreement for response times.
- Reliable and experienced incident responders and analysts.
- Integration of threat intelligence into the intrusion analysis and investigation.
- Multi-discipline CSIRT team with cloud and application security experience.
- Never lose out. Repurpose unused time.

### Pricing

Pricing scales on the number of retained hours within the agreement.

Hours	Price (per annum)
40	£18,000.00
80	£27,000.00
100	£36,000.00
Additional 8 Hours	£1,800.00

## 5.0 Emergency Incident Response (CSIRT)

**Bridewell have a true, UK based 24/7 incident response function that are multi-disciplined and SC Cleared.**

**The Bridewell team have extensive experience of incident response in cloud, application and on-premise breaches, providing support to companies when emergencies arise.**

The Bridewell CSIRT team will enrich active incident investigations with expert advice, management, analysis and investigation to restore operations quickly and effectively and minimising long-term risk.

### Features

- NCSC Cyber Incident Response Level 2.
- CREST-registered SOC.
- CSIRT Team comprising of responders, analysts, intelligence, incident management, testers and DevSecOps specialists.
- 24/7 SOC phonenumber.
- CREST and GIAC certified staff.
- OT and ICS experience.

### Benefits

- Reliable and experienced incident responders and analysts.
- Multi-discipline CSIRT team with cloud and application security experience.
- Integration of threat intelligence into the intrusion analysis and investigation.
- Never lose out. Repurpose unused time.

### Pricing

- Pricing for Emergency Incident Response is fixed at £2,200 per 8 hours/ day consumed.



## 6.0 Incident Response tabletop Assessment

The frequency and breadth of cyber security threats continues to grow as adversaries are finding increasing success in exploiting complex business environments. Bridewell's incident response tabletop assessment is designed to leverage threat intelligence and intrusion analysis to test your incident response readiness in a safe environment.

Throughout the engagement, Bridewell will share all data, scenarios, playbooks and learnings to ensure the assessment provides a valuable rehearsal that improves coordination during an active incident response situation.

With "Lessons Learnt" being a key stage in the IR process, your team will develop alongside Bridewell and prioritise activities that would improve the overall resilience of your organisation by improving your ability to respond to incidents effectively.

### Features

- Assured NCSC Cyber Incident Exercising provider.
- Scenarios that mimic real world intrusions.
- CREST and GIAC Consultants
- Collaborative table-tops that are designed to improve incident response readiness.

### Benefits

- Test your Incident Response effectiveness ahead of time in a safe environment.
- Leverage the experience and intelligence from a leading cyber defence team.
- Identify areas for improvement across people, technology and process.

### Pricing

- Please see SFIA Rate Card.

## 7.0 Purple Team Engagement (Simulated Attack and Response)

The assurance of your cyber defence capabilities is important to develop maturity and manage the risk of active cyber threats. By leveraging threat intelligence and adversary information, Bridewell offers a Purple Team Engagement led by a combination of our incident response, SOC, threat intelligence, and offensive security teams.

Working closely with your existing teams and providers, our methodology allows for a transparent and collaborative approach to testing and a supportive environment for the identification and testing of improvements.

### Features

- Adversarial-led purple team engagement.
- Collaborates with existing teams and providers to measure effectiveness and highlight areas for improvement.
- OSCP, CREST, and GIAC-certified consultants.

### Benefits

- Improve resilience to active cyber threats.
- Gain assurance of your defensive capabilities.
- Increase leadership confidence in cyber security initiatives.
- Integration of red and blue team specialists with existing teams.

### Pricing

- Please see SFIA Rate Card.

## 8.0 Managed Digital Risk Protection

Unwanted exposure leads to digital risks. Traditional perimeter-based approaches to security no longer work for today's organisations who are increasingly cloud-based, reliant on expanding third-party ecosystems, and use digital channels to engage with customers. It's only a matter of time until your organisation's digital exposure is unearthed by a customer, competitor, researcher, attacker or manager. Organisations need threat intelligence to manage their digital exposure and minimise their digital risk.

Bridewell leverages the platform capabilities of Digital Shadows to deliver a managed digital risk protection service that integrates our Cyber Threat Intelligence and response capabilities to help manage and reduce the risk from your organisation's external exposure.

### Features

- **Brand Protection.** Impersonating domains, mobile apps, and social media profiles.
- **Data Leakage Detection.** Detection of exposed company data, including employee credentials.
- **Dark Web Monitoring.** Identification of threats across criminal forums and dark web markets.
- **Attack Surface Monitoring.** Weaknesses in internet-facing infrastructure.
- **Technical Leakage Detection.** Technical leakage from developers and contractors.

# 8.0 Managed Digital Risk Protection

## Benefits

- Access to a Cyber Threat Intelligence and incident response team that can support remediation of identified threats
- Reduce the external threats to your organisation and supply chain.

## Pricing

Item	From (per annum)
Managed Digital Risk Protection	£60,000

Deployment has a fixed cost of £5,000.00.

## 9.0 Vulnerability Management Service

**Gain a thorough, comprehensive understanding of your organisation's overall security posture, with detailed predictions of where an attack is most likely to take place.**

Our CREST-accredited vulnerability assessment services proactively identify, classify and address cyber risks.

Bridewell's vulnerability management service identifies areas vulnerable to attack and supports organisation's in taking measures to shore up these gaps by improving their cyber security posture.

The service is driven by insights from leading vulnerability assessment technologies and threat intelligence, integrating these into a singular data set and risk model that guides the entire vulnerability management lifecycle.

### Features

- Fully managed.
- Assessment enriched by threat intelligence and customer context.
- Vulnerabilities prioritised and relevant actions and remediations detailed.
- Managed and tracked vulnerability remediation, mitigation, and risk process.
- Integration of multiple tools and technologies.
- Risk-based scoring system.

# 9.0 Vulnerability Management Service

## Benefits

- Bridewell provides vulnerability management as a service (VMaaS), taking full ownership of relevant responsibilities.
- Prioritised risk remediations along with the acceptance and continual re-evaluation of risks.
- Ensure that risks are tracked and reduced across the environment.
- Provides a rich informed view across assets.
- Reduce the burden on your security team.
- Improved business processes.

## Pricing

Pricing is based upon vulnerability analyst effort required to deliver against the scope of service.

Please see SFIA Rate Card.



# SFIA Rate Card

	Strategy & architecture	Business change	Solution development & implementation	Service management	Procurement & management support	Client interface
1. Follow	£500	£500	£500	£500	£500	£500
2. Assist	£501 - £725	£501 - £725	£501 - £725	£501 - £725	£501 - £725	£501 - £725
3. Apply	£726 - £845	£726 - £845	£726 - £845	£726 - £845	£726 - £845	£726 - £845
4. Enable	£846 - £975	£846 - £975	£846 - £975	£846 - £975	£846 - £975	£846 - £975
5. Ensure / Advise	£976 - £1100	£976 - £1100	£976 - £1100	£976 - £1100	£976 - £1100	£976 - £1100
6. Initiate / Influence	£1101 - £1300	£1101 - £1300	£1101 - £1300	£1101 - £1300	£1101 - £1300	£1101 - £1300
7. Set Strategy / Inspire	£1301 - £1600	£1301 - £1600	£1301 - £1600	£1301 - £1600	£1301 - £1600	£1301 - £1600

## Standards for Consultancy Day Rate Cards

**Consultant's Working Day** – 8 hours exclusive of travel and lunch.

**Working Week** – Monday to Friday excluding national holidays. **Office Hours** – 09:00 - 17:00 Monday to Friday

**Travel and Subsistence** – Payable at department's standard T&S rates

**Mileage** – As above

**Professional Indemnity Insurance** – Included in day rate

**VAT** – The above costs are exclusive of VAT and any other applicable taxes or duties

# Our Certifications, Accreditations, and Awards

Bridewell is the UK's most certified cyber security provider by the National Cyber Security Centre (NCSC). Below are all of our certifications, accreditations and awards.

