INCIDENT RESPONSE DATA SHEET

UNRESTRICTED

1. OVERVIEW

1.1 INTRODUCTION

With data breaches, hacks and other cyber security incidents increasing in frequency and profile, the need for an organisation to have strong cyber incident response plans is vital. That's why Bulletproof introduced our incident response retainer packages. We take quick, effective action to help you minimise the impact of a cyber incident and take prudent steps to get your business back on track. Cyber incidents come from a variety of sources, so Bulletproof's experienced security analysts are always up-to-date with latest threat intelligence, meaning we can identify threat actors and compromise vectors, and swiftly apply full remediation.

1.2 KEY FEATURES

- Professional recovery from cyber incidents, such as ransomware, rogue employees and more
- Hackers never take a day off, so our crisis team are available round-the-clock
- Restore services with minimal disruption to your business operations
- Support post-incident, with recommendations and a detailed report
- Professional incident response in-line with CREST, NIST, and ISO 27035 standards

1.3 RETAINER SCHEME

Bulletproof Cyber Incident Response operates on a retainer model to give you the best possible response time. For a low set-up cost and fixed monthly fee, you gain total peace of mind that your organisation has the right practices in place to cope in case of an incident, with Bulletproof's experienced 24/7 crisis team only a phone call away. Plus with included incident response days, on-site support, and discounted rates on complex digital forensics, you're ideally placed to respond and recover effectively.

1.4 BENEFITS OF RETAINER SCHEME

Powerful benefits that deliver enhanced incident response.

Pre-approved Contract and Engagement Terms

Your first call to us starts the incident response process – meaning no need to find an available supplier, negotiate T&Cs, and scramble to authorise order forms in the middle of a crisis.

Infrastructure Foresight

Thanks to the on-boarding security audit, we'll already have a good working knowledge of your infrastructure. This means our first step can be to take action, rather than ask about your system configuration.

Pre-Defined Cost Structure

Hunting for someone to help you when you're being attacked could lead to you being taken advantage of, with some suppliers offering their help at an exaggerated premium. The retainer scheme means this is no longer a concern, as with the commercial framework already in-place, you know upfront what the cost implications are.

2. CYBER INCIDENT RESPONSE

2.1 SERVICE FEATURES

- Malware Analysis & Reverse Engineering
- Host Intrusion Analysis
- Network Packet Capture & Analysis
- Data Recovery
- Incident Testing
- First Responder Training
- Cyber Insurance Claims Coordination
- Digital Forensics
- Log Analysis
- Chain-of-Evidence Preservation

2.2 HOW DOES IT WORK?

2.2.1 THREE-STEP PROCESS

Bulletproof operates a three-step process, in-line with industry standards and best practices. These are:

PREPARE

- Business Impact Assessment
- Threat Assessment
- Define a CSIR Framework
- Readiness Audit

RESPOND

- See 2.2.2

SUPPORT

- Deep Analysis
- Trend Analysis
- Reporting
- Lessons Learnt

2.2.2 FOUR STAGES OF RESPONSE

Within the respond step are several processes that ensure an effective and efficient recovery:

1. **Analysis**

   Incident identification and investigation to understand the impact of suspected events

2. **Containment**

   Triage activities and invoking a containment strategy to contain the scope and magnitude

3. **Eradication**

   Clean-up of not only the affected components, but also the source

4. **Recovery**

   Return to a fully operational state, with a validation test to confirm normal operation

2.3 INVOCATION PROCEDURE

1. **Contact us 24/7**

   We have cyber security specialists on 24/7 watch, ready to take your call and start helping

2. **Telephone Triage**

   An incident response specialist will assess the situation and recommend a course of action

3. **Invoke IR Procedures**

   A pre-approved representative at your organisation authorises us to get involved

4. **Start Recovering**

   We'll assign an IR liaison who'll be your single point of contact during the incident

3. EXAMPLE PACKAGES

Each Bulletproof Cyber Incident Response package requires a number of on-boarding activities to ensure an organisation is prepared for a cyber incident. It starts with an initial security overview, where we'll establish your current security posture.

3.1 SET-UP AND ON-BOARDING

Typical Set-up Fee: £1,995-£4,995

- Initial security overview
- Infrastructure and business process audit
- Comprehensive risk assessments
- Create CSIR framework
- Readiness check

3.2 ESSENTIAL RESPONSE PACKAGE

Fixed Monthly Fee: £450

- 24/7 Telephone Triage
- Next business day on-site support SLA
- 1 day of on-site support included
- Discounted rate on additional on-site days, including Digital Forensics
- Yearly review of on-boarding activities is required to confirm CSIR Framework suitability

3.3 ENHANCED RESPONSE PACKAGE

Fixed Monthly Fee: £950

- 24/7 Telephone Triage
- 12-hour on-site support SLA
- 2 days of on-site support included
- Discounted rate on additional on-site days, including Digital Forensics
- Discounted yearly review of on-boarding activities to confirm CSIR Framework suitability

T: 01438 532 900 E: contact@bulletproof.co.uk W: www.bulletproof.co.uk