Major Incident Response Retainer Service Definition

Purpose

To provide guaranteed, on-demand access to expert incident response resources during critical cybersecurity events. This service ensures rapid containment, investigation, and recovery from major incidents such as ransomware attacks, data breaches, and advanced persistent threats, minimizing business disruption and financial impact.

Service Overview

The Major Incident Response Retainer offers:

- Pre-arranged contractual access to senior incident response specialists.
- Rapid mobilization of resources for containment and eradication.
- Forensic investigation and evidence preservation for legal and compliance needs.
- Advisory on remediation and recovery strategies.
- Post-incident reporting and lessons learned for future resilience.

Key Activities

- **Incident Triage & Containment** – Immediate actions to stop threat propagation.
- **Forensic Analysis** – Collect and analyse evidence to determine root cause.
- **Threat Eradication** – Remove malicious artifacts and restore system integrity.
- **Recovery Support** – Assist in restoring business operations securely.
- **Regulatory & Legal Support** – Provide documentation for compliance and litigation.
- **Post-Incident Review** – Deliver detailed reports and recommendations for improvement.
- **Proactive Readiness** – Conduct tabletop exercises and readiness assessments.

Value Delivered

- **Rapid Response** – Minimize downtime and operational impact during major incidents.
- **Expert Guidance** – Access to seasoned IR professionals with deep technical expertise.
- **Regulatory Compliance** – Ensure adherence to breach notification and reporting requirements.
- **Risk Reduction** – Contain threats quickly to prevent escalation.
- **Strategic Improvement** – Strengthen security posture through lessons learned.

Service Levels

- **Response Time:** Guaranteed engagement within agreed SLA (e.g., 1 hour for critical incidents).
- **Availability:** 24x7 access to incident response team.

- **Reporting:** Comprehensive incident report delivered within defined timeframe post-resolution.

Roles & Responsibilities

- **Incident Response Lead** – Coordinates response activities and client communication.
- **Forensic Analyst** – Performs evidence collection and analysis.
- **Threat Containment Specialist** – Executes containment and eradication measures.
- **Client Security Team** – Provides access and supports remediation efforts.

Dependencies

- Pre-established communication channels and escalation procedures.
- Access to relevant systems and logs for investigation.
- Integration with client's SOC and IT teams for coordinated response.