DIGITAL DEFENCE

Retained Incident Response Service

Respond
Service

OVERVIEW

When an incident or cyber breach occurs, a rapid and effective incident response is critical to safeguarding your organization's systems and data. Any delay increases the losses from a security breach; unfortunately, these delays typically arise from a lack of resources. Incident response personnel must not only be available when needed, but they must possess the skills and tools to immediately respond to a variety of different possible attacks.

DigitalDefence's Retained Incident Response Service allows you to engage these skilled resources on a "as needed" basis. Members of the DigitalDefence Cyber Emergency Response Team, ddCERT, can deploy in a rapid manner to supplement or manage the end-to-end incident response process. Because the service is pre-planned, the financial costs can be planned in advance, and customers know that a rapid and effective response will be delivered under the contracted Service Level Agreement.

KEY BENEFITS

- Pre-planned incident response process minimizes the duration and impact of an incident; this significantly reduces impact to the business and the time required to respond and recover to normal operations
- Rapid and effective response immediately reduces operational costs; over the course of the incident, it reduces liability, regulatory fines, and business costs of downtime
- Pre-approved agreements enable long-term financial planning
- Guaranteed immediate remote response and on-site response times for prepaid tiers minimizes damage to organization's data resources

Improve corporate risk reduction with strategic security and privacy services.

Is the Retained Incident Response Service right for your company?

- Do you lack the specific resources, including personnel and skills, to effectively respond to a security breach?
- Do you want the comfort of having on-call specialists available at a pre-defined cost with availability covered under a service level agreement?

DigitalDefence's tiered service allows you to select the most cost effective response for your organization

- Access to remote and on-site teams of individual with skills in ethical hacking, technical and management approaches to incident response, and data forensics (required to support possible litigation)
- Access to complementary DigitalDefence services at a reduced rate

SERVICE DESCRIPTION

DigitalDefence's Retained Incident Response Service includes the following features:

- Single Point of Contact – DigitalDefence will assign your organization an Incident Response Manager who possesses both the technical knowledge and the management / business skills to support your organization
- Pre-Negotiated Agreements – All Terms of Engagement will be agreed to prior to an incident response; this minimizes costs and response time
- Pre-Paid Tiered Services – Depending on which service tier you select for your retained incident response service, you will have a pre-paid block of time available for incident response. Organizations can use this time to pay for incident response services, or redirect it to pay for any other DigitalDefence services at a discounted rate
- Response Readiness Assessment - Preparation for the incident response begins before the actual incident. Once the agreements have been signed and the required service level is defined, DigitalDefence will conduct an Incident Response Readiness Assessment of your monitoring and response abilities. DigitalDefence will then develop a response plan that identifies any gaps and a plan to address these
- Immediate Response - When an incident is reported, our experts will respond within minutes, delivering a remote assessment to provide direction on how best to contain and mitigate the breach and protect your data. This support is available 24 x7 for the duration of the response
- On-Site Response - The remote assessment will be followed by an on-site response, if required. A DigitalDefence response team, composed of a management lead as well as appropriate technical resources, will arrive within a defined space of time. The management specialist will communicate with key stakeholders to provide guidance during the response; they will also assist with communicating with media, law enforcement, and regulatory parties
- Appropriate Technical Specialists – DigitalDefence incident responders hold the most relevant industry qualifications. The incident manager may also engage additional support from our pool of pre-approved specialists if required. Examples of such specialists include lawyers, privacy law specialists, private investigators, translators, fraud examiners, grief counsellors, etc
- Rapid Mediation - DigitalDefence technical specialists will provide the skilled support to eradicate the threat and recover any impacted systems.

About DigitalDefence

DigitalDefence provides complete protection against data security breaches. We provide the advisory services that align security with your business strategy and practices. Our protection services secure your data by assessing vulnerabilities and validating security controls using audits and penetration testing, or "ethical hacking". And should you suffer a security or privacy breach, we provide the 24x7 response services and expertise to minimize financial and reputational loss.

- They will also perform a root cause assessment to ensure that the threat does not return due to incomplete eradication or lack of sufficient security controls. All actions will be performed assuming that litigation is a consideration; evidence will be retained in accordance with forensic principles to support such litigation
- Post-Incident Review and Follow-Up - Once the incident is deemed to have been closed, the incident manager will provide you with a post-incident report and assist in ensuring that the lessons learned are transmitted to the correct employees to prevent similar incidents in the future

Disclaimer

This document is for informational purposes only. DigitalDefence makes no warranties, express or implied, in this document.