UnderDefense

DATA SHEET

Incident Response Retainer

Reduce incident response time and minimize the impact of a security incident

BENEFITS

• World-renowned experts on your side

• Access to ’s industryleading technology stack

• Pre-negotiated terms and conditions that reduce response time when it matters most

• Rapid response SLAs that mitigate the overall impact of a breach

• Access to the Incident Response Preparedness Service

• Guaranteed response times in the event of a suspected incident

• Flexibility to repurpose unused hours on a variety of technical and strategic services

Why UnderDefense
UnderDefense has been at the forefront of cyber security and cyber threat intelligence since 2004. Our incident responders have been on the frontlines of the most complex breaches worldwide. We have a deep understanding of both existing and emerging threat actors, as well as their rapidly changing tools, tactics and procedures (TTPs).

Overview
The UnderDefense Incident Response Retainer (IRR) allows you to establish terms and conditions for incident response services before a cyber security incident is suspected. With an IRR in place, you have a trusted partner on standby. This proactive approach can significantly reduce the response time, thereby reducing the impact of a breach.

The IRR gives you the flexibility to structure the retainer your organization needs.

• **No-cost retainer:** Establishes terms and conditions between your organization and for incident response services. The contract defines hourly rates for related services and technology fees. There is no financial commitment or annual cost. Charges are only incurred on a time and materials basis upon declaration of an incident.

• **Prepaid hours:** Purchase a pre-paid block of incident response hours at a discounted hourly rate, with the flexibility to repurpose unused hours. The pre-paid hours can be used on a variety of technical and strategic consulting services.[1]

In addition to pre-established terms and conditions, add an SLA and gain peace of mind from guaranteed response times. The standard SLA is a maximum of four hours, with an enhanced two-hour SLA to further reduce incident impact.

1 Hours must be repurposed within the contract term

Table 1. Benefits of prepaid hours.

Initial response	Service-level agreement	Incident Response Preparedness Service
• Triage security issue • Provide initial assessment based on UnderDefense intelligence and experience • Live response analysis of the systems to identify malicious activity	• Access to a 24/7 incident response hotline • Initial contact (via email or phone) within four hours: The first contact is with a incident responder who can immediately help with triaging the incident • Enhanced two-hour SLA available • Case is accepted once and client deem that incident response services are needed	• Triage security issue • Provide initial assessment based on UnderDefense intelligence and experience • Live response analysis of the systems to identify malicious activity

Table 2. Available consulting services for repurposing prepaid hours include:

Technical Services	Strategic Services	Education Services
• Compromise Assessment • Red Team Assessments • Penetration Testing	• Response Readiness Assessment • Strategic Program Assessment • Incident Response Tabletop Exercise • Cyber Defense Center Development	• Incident Response and Forensics • Malware Analysis • Cyber Security and Intelligence

For more information on consulting services, visit: https://underdefense.com/incident-response-retainer/

UnderDefense
suite 420, 111 John St New York, NY 10038, USA
Tel: +1 929 999 5101
email: help@underdefense.com

About UnderDefense

UnderDefense is entirely focused on cybersecurity by planning, building, running security programs for our customers through the right combination of people, processes and solutions.
Our services include security monitoring, remote IT security officer service, threat and vulnerability management, advanced threat prevention and response, incident detection and management, security awareness trainings, and penetration testing.