Promoting Full-Time Response Readiness

With ongoing security talent shortages, it can be difficult for organizations to get the coverage they need to stay vigilant against potential threats. Time is of the essence when responding to incidents, particularly for organizations who must quickly report them to regulatory bodies or their customers. That’s where Optiv’s Incident Response Retainer program can help. We offer a variety of retainer packages that can meet your organization’s unique circumstances. Whether you need quicker response times or a larger pool of hours, we’ve got you covered.

For over two decades, experts at Optiv Security have been at the forefront of preventing and responding to large-scale attacks and intrusions of all types. Our incident responders, investigators and malware reverse engineers take their decades of experience and unique skills and use them to prepare you for an incident, identify attacks, uncover indicators of compromise, provide guidance to reduce your attack surface and respond to incidents should they occur.

Optiv Solutions

Optiv’s place as a leader in the cybersecurity field allows us to successfully develop and test incident management capabilities through a formalized Incident Management Framework (IMF). Our IMF contains multiple security controls that are derived from industry-accepted security standards such as National Institute of Standards and Technology (NIST), System Administration, Networking and Security (SANS), International Organization for Standardization (ISO), Payment Card Industry (PCI) and more.

The dynamic range of Optiv’s proven services ensure clients are equipped to effectively respond to and/or investigate suspected incidents. Our IR retainers allow minimum engagements of two hours, so you can request sanity checks or detection verifications of emails, alerts, etc. without the overhead and larger minimum of non-retainer engagements. The vast majority of our enterprise incident management (EIM) group’s reactive incident response work can be done remotely, saving you time and travel costs. Retainer packages of over 100 hours allow you to repurpose unused hours when you renew your contract. Reused hours must be used within 90 days of renewal and must include EIM services, though they may be blended with other services from Optiv’s Threat Management practice.

Incident Management Program Development (IMPD) (Plan/Playbook)
Development of an Incident Management Program to help clients understand the strategic, tactical and functional response requirements/plan for a potential incident.

Postmortem (IRP Improvement)
Perform a postmortem review of a client’s technology, response efforts and outcomes to investigate if the appropriate actions were followed. Optiv then creates recommendations on process improvements.

Media Forensics and Malware Analysis
Review and analysis of binary applications and determine malware capabilities.

Containment and Isolation
Part of an overarching incident response engagement, Optiv will help a client regain control of their infrastructure, limit an attacker’s actions and minimize the impact to operations.

IRP Validation (Tabletop, Review, IRRA)
Testing and validation of a client’s incident management through workshops to assess a client’s maturity level or actual response efforts through a tabletop exercise.

Day 0/1 Response Team
Tactical response for Optiv retainer clients during an incident. Assistance with deploying technology to hunt for threats within a client environment.

Incident Management Coordination/Coordinator
Onsite assistance during an incident to lead the direction of response activities. This role acts as a liaison between client leadership and technical teams to move through the incident response process.
Why Clients Choose Optiv

Certified Professionals
Our 20+ full-time, dedicated incident responders use strong skill sets in both proactive and reactive methodologies and tool kits

Holistic Investigative Methodologies
Allow us to leverage numerous best-in-class technologies to discover, respond, contain and remediate intrusions and malware

Highly Secured Forensic Lab
Provides place for investigation and storage of evidence with strict controls established around how the data is received, used, stored and disposed of

Deep Understanding
Of threat actors allows us to better advise organizations on the best approach to quick detection and response

Pre-Negotiated Contractual Terms
And conditions in place to save time and provide peace of mind

Cybersecurity’s Best
As well as Optiv’s proprietary database of malware signatures and viruses

Proactive Services
That make your business more resilient in the face of an incident

Optiv’s Retainer Packages

INTRODUCTORY - BASE
- Includes 50 hours
- 2x hours multiplier on weekends/holidays
- Includes incident response onboarding
- Service Level Agreements (SLA) - Remote: 24 hour, on-site: 72 hour
- No reuse of hours

ESSENTIAL - VALUE
- Includes 100 hours
- 2x hours multiplier on weekends/holidays
- Includes incident response onboarding
- SLA - Remote: 4 hour, on-site: 48 hour
- Reuse of hours available at end of contract

BUSINESS - MOST POPULAR
- Includes 150 hours
- 2x hours multiplier on weekends/holidays
- Includes incident response onboarding
- SLA - Remote: 4 hour, on-site: 24 hour
- Reuse of hours available at end of contract

ENTERPRISE - CUSTOM
- Must include a block of hours
- Must include a SLA
- 2x hours multiplier on weekends/holidays
- No reuse of hours

Secure your security.™

Optiv is a security solutions integrator a one-stop trusted partner with a singular focus on cybersecurity. Our end-to-end cybersecurity capabilities span risk management and transformation, cyber digital transformation, threat management, security operations, identity and data management, and integration and innovation, helping organizations realize stronger, simpler and more cost-efficient cybersecurity programs that support business requirements and outcomes. At Optiv, we are leading a completely new approach to cybersecurity that enables clients to innovate their consumption models, integrate infrastructure and technology to maximize value, achieve measurable outcomes, and realize complete solutions and business alignment. For more information about Optiv, please visit us at www.optiv.com.

©2021 Optiv Security Inc. All Rights Reserved. Optiv is a registered trademark of Optiv Inc.