SERVICE BRIEF

Threat Management: Incident Response Retainer Program
Enabling Response Readiness 24x7x365

Since 2002, experts at Optiv Security have been at the forefront of preventing and responding to large-scale attacks and intrusions of all types. Our experienced incident responders, investigators and malware reverse engineers possess the unique skills required to help you prepare 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 is well-positioned to ensure the successful development and testing of its 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.

Optiv's proven services ensure businesses are equipped to effectively respond to and/or investigate suspected incidents.

- 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.

- Post Mortem (IRP Improvement)
  Perform a post mortem 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 to 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.
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, cyber 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.