ENTERPRISE INCIDENT MANAGEMENT SOLUTIONS

Experts When You Need Them

OVERVIEW

Preparation and readiness are essential to minimizing damage when an incident happens. So is having the right partner. Our expert team of incident responders, analysts and engineers has the expertise needed to help you avoid trouble, identify vulnerabilities, eliminate malware and provide assistance in the event of a breach or compromise. Whether your issues stem from mishandling of data by a well-intentioned employee to a targeted assault launched by a skilled attacker, we have the knowledge and know-how to help you minimize the likelihood of an event and help you get back to business as usual should an event occur.

Enterprise Incident Management (EIM) Services:

Optiv helps our clients reduce the likelihood of an attack or incident, secure their environment against threats and recover from incidents while minimizing disruption. With some of the best minds in the industry, we're there when you need us.

Our services include:

- Cyber Defense Development
- Incident Response and Recovery
- Compromise Assessment
- Forensic Analysis

Analysts estimate 70 to 90 percent of **all enterprise systems are INFECTED.**

Unplanned downtime **costs large enterprises an estimated:**

$5,000 per MINUTE.

$300,000 per HOUR.

Can you afford **not to address your malware problem**?

1. Cyber Defense Development

Goal

Organizations that proactively prepare for incident response limit costs, confusion and lost time. Proper preparation and documentation can also help staff secure key evidence in the event of a compromise.

Overview

Planning and preparation can mean the difference between recovering well and not recovering at all when a breach or attack occurs. Our experts can help you limit vulnerabilities, develop an action and communication plan and monitor your environment for potential threats.

SERVICES

- Incident Response Planning
- Attack Simulation
- Managed Malware Monitoring

BENEFITS

- Discovery of Existing Vulnerabilities
- Documentation of Key Personnel and Escalation Steps
- Actionable Instructions for Securing Machines and Limiting Damage
- Expert Advice to Help Reduce Your Attack Surface
- Recommendations for Next Steps to Make Your Organization More Secure

2. Incident Response and Recovery

Goal

We help our clients discover and respond to cyber security incidents and events of all kinds.

Overview

Incidents and compromises can create major issues for your staff who may not possess the unique skills to assess and regain control after an attack. We help you respond and recover with advice, guidance and hands-on expertise. Our services include securing the scene, defining the scope of the compromise, collecting and analyzing data related to the event and issuing a report documenting findings.

SERVICES

- Incident Discovery
- Incident Rapid Response (IRR) Program

BENEFITS

- Uncover the Attackers' Actions
- Detail the Scope of the Compromise
- Identify Steps to Remove Active Binaries and Malware
- Limit Data Loss
- Secure Your Business

3. Compromise Assessment

Goal

We can provide an assessment of what occurred, the areas of compromise and details about the event. We can also remove malware from your environment and advise on next steps.

Overview

Our security and malware experts will examine your systems to determine if a compromise has occurred. With an understanding of regulations and data disclosure requirements, we can help you comply with the law and help limit your organization and reputational risk.

SERVICES

- Incident Discovery
- Malware Remediation

BENEFITS

- Examination of Your Systems for Indicators of Compromise
- Analysis Informed by a Vast Proprietary Knowledge Store of Malicious Code, Signatures and Attacks
- Inspection of your access points, vulnerabilities and data stores
- Knowledgeable experts at your side

4. Forensic Analysis

Things happen fast in a crisis. Preserving key evidence can sometimes get overlooked until it's too late. Capturing key forensic details is essential to discovering the extent and potential origins of an attack. We can help you understand the details of your event and preserve data for future legal or enforcement action. Our scientists and researchers can also reverse engineer malware found on your systems to discover hidden details about the attack and its potential origins.

SERVICES

- Malware Reverse Engineering
- Forensic Analysis and Data Capture

BENEFITS

- Understand the Target and Scope of the Event
- Limit Over-reporting a Data Loss or Disclosure
- Determine the Who, What, Where, When, Why and How Long of an Incident Whenever Possible

5. Bespoke Engagements

We provide custom services to existing and new clients seeking to address incidents and system vulnerabilities.

SERVICES

- Incident Response Advising
- Incident Response Consulting

OPTIV

1125 17th Street, Suite 1700
Denver, CO 80202

800.574.0896 | optiv.com