Expediting Issue Resolution

The continued advancement and reliance on technology has increased not only the probability but the severity of cyber attacks. While not all incidents are the same, there are over 2 million recorded attacks each year that impact organizations’ ability to function. This increased frequency and severity impacts everything from how an organization communicates to how it maintains confidential data. Businesses today need increased capabilities in monitoring, detecting, preventing and ultimately responding to such attacks in an efficient manner that lessens the impact.

Optiv’s strategic incident management program reduces the risk to an organization by implementing a systematic method for efficient detection, escalation and response to incidents. By enhancing internal coordination and communication, your business will reduce downtime, implement recovery efforts quickly and continuously improve incident response processes and procedures.

Optiv’s Incident Management Strategy

Optiv’s incident management program primarily follows the National Institute for Standards and Technology (NIST) incident response cycle and can customize your program based on your specific needs.

- **Preparation** is the process of gathering and compiling existing data, assets, security controls and defining response processes and procedures.

- **Detection and Analysis** involves collecting data from security tools and personnel, establishing baselines of normal behavior and correlating related events to look for deviations.

- **Containment, Eradication and Recovery** is the process of identifying the attack, adversary and affected resources, then minimizing damage by isolating affected systems, providing resolution and restoring operations to normal.

- **Post-Incident Activity** involves using findings to improve procedures, plans, processes and response policies.
Why Clients Choose Optiv

We understand the challenges within your organization’s incident management and strive to improve your security posture and mitigate risks. Optiv’s Incident Management Program will support your organization with:

- Reducing overall downtime
- Implementing recovery efforts quickly
- Reducing incident impact
- Continuous improvements to incident response processes and procedures

Process Overview

Optiv’s incident management assessments are designed with your security challenges in mind. We account for the current threat landscape and reduce enterprise risk by evaluating your incident response capabilities and creating an actionable plan to improve your ability to detect, contain, eradicate and recover. Our incident management framework contains multiple security controls that are derived from industry-accepted security standards such as NIST SP 800-61.

How We Do It

Optiv’s Incident Management Framework consists of five phases, each including a comprehensive list of objectives to identify, compensate for and remediate any incident.

1. **Escalation Process**: When an incident occurs, procedures should be in place to expedite awareness to key personnel.
2. **Status Updates**: Targeted times should be in place for all phases of an incident.
3. **Internal Coordination**: Manage and direct all communication between teams including legal, IT and other business entities.
4. **Communications**: Prioritized lists of who needs to be notified and what details to provide, both internally and externally.
5. **Resolution**: Comprehensive review of incidents and the identification of lessons learned should drive new policies, procedures and technologies to reduce the risk of a subsequent incident.

---

Secure greatness™

Optiv Security is the cyber advisory and solutions leader, delivering strategic and technical expertise to more than 7,000 companies across every major industry. We partner with organizations to advise, deploy and operate complete cybersecurity programs from strategy and managed security services to risk, integration and technology solutions. With clients at the center of our unmatched ecosystem of people, products, partners and programs, we accelerate business progress like no other company can. At Optiv, we manage cyber risk so you can secure your full potential.

©2022 Optiv Security Inc. All Rights Reserved. Optiv is a registered trademark of Optiv Inc.