Fidelis® Cybersecurity

DATASHEET

# Incident Response Readiness Assessment

**Our experts evaluate, assess and validate your incident response plan and your ability to respond to critical security incidents.**

## Put Your Incident Response Plan to the Test

The tools and techniques of attackers are rapidly evolving. To keep pace with attackers, security teams need to continually assess, review, and revise their incident response programs. When a serious security incident occurs, it's critical for the security team to have a solid understanding of the response plan and escalation matrix so they can quickly take action and begin to respond, minimizing the potential loss of critical data and intellectual property.

Our experienced security professionals have been on the front lines responding to security incidents for over eighteen years. We've seen what's failed as well as what works, and apply this knowledge along with best practices to help you improve your ability to detect and respond to an incident — reducing the amount of time a threat actor is active in your environment and increasing your security posture against advanced threats.

## Overview

The Incident Response Readiness Assessment is an analysis of your organization's security event monitoring, threat intelligence and incident response capabilities.

To meet each organization's specific needs, we apply a variety of incident response best practices and guidelines — including those defined by the National Institute of Standards and Technology (NIST) and Carnegie Mellon University Computer Emergency Response Team (CSIRT) — as well as our team's vast real-world experience. This in-depth process provides a comprehensive picture of your readiness posture and a clear plan for strengthening it.

**Response Evaluation:** We perform a thorough review of your incident response plan including team roles and responsibilities, security policy and procedures, and security controls.

**Gap Analysis:** Our experts create a comparison of their findings to industry best practices and application of our own experience to identify gaps, opportunities for improving your readiness.

**Hands-On Testing:** We conduct exercises to evaluate how your team would respond during a security incident, test their awareness of the current incident response processes and determine their ability to effectively identify and respond to an incident.

## Our Experience

- Members of our security consulting team have over 18 years of incident response experience on average.
- We have responded to over 4,000 security cases in both the commercial and government sectors.
- Our security professionals were instrumental in building one of the first security operations centers.
- We have provided expert testimony in over 100 court proceedings.
- Our team successfully guided one of the largest forensic laboratories (DCFL) to achieve international digital forensic accreditation.
- We have a dedicated malware team focused on reverse engineering malicious files and researching the latest exploits.

### IDENTIFY

- Incident Artifact Handling
- Forensics
- Incident Management
- Team Composition

### ANALYZE

- Gap Analysis
- Best Practice Comparison
- Table Top Exercise

### REPORT

- Gaps in Plan
- Security Enhancement Recommendations
- Observations

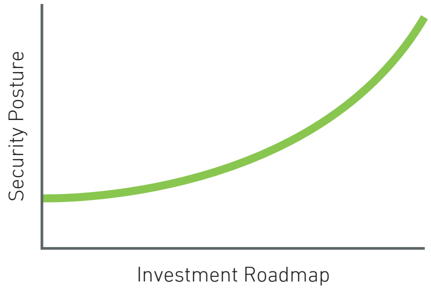
Evaluate, assess and validate your incident response plan and ability to respond.

## Our Approach

Our experience responding to critical security incidents gives us a front-row seat to the latest tools and tactics of advanced attackers. We perform our assessment based on this first-hand knowledge of evolving threats and adversaries to evaluate your preparedness.

We evaluate the current state of your incident response program to improve your ability to quickly identify and respond to advanced threat actors. We also identify areas that should be further developed.

By improving your readiness, your team will be able to quickly identify and respond to an incident.



*We evaluate your current incident response program and align our recommendations to your organization's business goals.*

## Methodology

The Incident Response Readiness Assessment is a three phase process that evaluates the current state of your incident response program to improve your team's ability to quickly identify and respond to advanced threats. The assessment also identifies areas in your security program that should be further developed to enhance your security defense posture.

**Evaluate:** During the first phase of the assessment we perform an in-depth review of your incident response plan, including team roles and responsibilities, security policy and procedures, and security controls.

**Analyze:** After performing a detailed review we compare findings to industry best practices and apply our first-hand experience responding to security incidents to identify gaps and opportunities to improve your readiness.

**Test:** We prepare practical exercises to evaluate how your team would respond during a security incident to determine their awareness to the current incident response process and their ability to effectively identify and respond to an incident.

.

## What You Get

At the end of the assessment we provide a detailed report that identifies areas for improvement in your process, procedures and technology. We also provide roadmaps and recommendations that align to your business objectives and will enhance your security program. The report also includes:

**Key Findings** in an executive summary and in the context of industry standards — providing you with a clear picture of your security posture and in a format that can be easily communicated to other stakeholders.

**Gap Analysis** identifying deficiencies in your organization's incident response capabilities that could hamper your ability to contain the impact of a security incident.

**Threat Mitigation Roadmap** that provides specific recommendations to enhance your incident response capabilities, includes short- and long- term goals and is tailored to your business — so you can proactively strengthen your defense.

## Contact Us Today to Learn More

**Fidelis Cybersecurity | 800.652.4020 | info@fidelissecurity.com**

Fidelis Cybersecurity is a leading provider of threat detection, hunting and response solutions. Fidelis combats the full spectrum of cyber-crime, data theft and espionage by providing full visibility across hybrid cloud / on-prem environments, automating threat and data theft detection, empowering threat hunting and optimizing incident response with context, speed and accuracy. Fidelis is trusted by Global 1000s and Governments as their last line of defense. Get in the hunt. For more information go to www.fidelissecurity.com.