



PROFESSIONAL SERVICES

- INCIDENT RESPONSE
- COMPUTER FORENSICS
- APPLICATION SECURITY
- NETWORK SECURITY
- RESEARCH & DEVELOPMENT

EDUCATION

- INCIDENT RESPONSE
- MALWARE ANALYSIS
- ADVANCED MALWARE ANALYSIS
- NETWORK TRAFFIC ANALYSIS
- WEB APPLICATION SECURITY
- WIRELESS INVESTIGATIONS
- LINUX FOR SECURITY PROFESSIONALS

SOFTWARE

- FIRST RESPONSE
- WEB HISTORIAN
- RED CURTAIN

MANDIANT™

WHY AN INCIDENT RESPONSE HEALTH CHECK?

Data breaches and losing personally identifiable information create significant negative publicity and legal issues. MANDIANT's *Incident Response Health Check* provides you with the assurance that your organization's Incident Response team is equipped and prepared to meet your corporate objectives.

The Health Check provides our clients with a comprehensive assessment of their existing Incident Response capabilities, processes and tools; and it allows MANDIANT to develop specific, cost-effective recommendations for improvement. MANDIANT's Health Check examines key program areas to answer the following questions:

- Does your organization have the mechanisms in place to rapidly detect an incident?
- Does your staff clearly understand their roles and responsibilities during Incident Response?
- Do your response strategies support applicable regulatory and legal requirements?
- Do you have a clearly communicated method for rapidly responding to potential customer data breaches?
- Is your Incident Response staff organized effectively?
- Does your staff have the training they need to respond effectively and efficiently to potential incidents?
- Does your organization have the necessary hardware and software to respond across your enterprise?
- Does your management team understand the challenges and time pressures in today's Incident Response environment?
- Are your Legal, Human Resources and Public Relations personnel aware of the key issues in Incident Response?

WHY MANDIANT?

MANDIANT consultants have worked with banks, government organizations and Fortune 100 firms to manage their incidents from detection to resolution. We have helped these same organizations develop their Incident Response programs from the ground up. Our combination of hand-ons technical experience and the ability to manage international and large incidents from detection through resolution makes MANDIANT uniquely capable of helping improve your Incident Response program.

MANDIANT'S INCIDENT RESPONSE HEALTH CHECK



Step 1: Assess Your Incident Response Program

MANDIANT consultants will collect and review your Incident Response program documentation to get an overview of your current practices. We will also conduct detailed interviews of your staff to discover any undocumented processes that are important to your program. We then compare your information to industry best practices, and we identify changes you should consider adopting.

Step 2: Perform a Dry Run Exercise

Incident Response is improved by repetition. Therefore, we provide you with a set of exercise scenarios to choose from, customizing one to best match your requirements. Common scenarios include system compromise, internal leak of PII data, internal investigation of inappropriate use and threatening email. MANDIANT will conduct a simulated incident that allows your team to perform a response. During your team's response, MANDIANT assists and evaluates the effort from initial detection to resolution.

Step 3: Improve Your Incident Response Program

MANDIANT will provide you with a final report and presentation that blends our review of your procedures, your staff's insights from the interviews, and our observations during the exercise. We will focus on benchmarking your program against applicable legal or regulatory requirements and industry best practices, highlighting your program's strength as well as possible areas for improvement.

Optional: One-Day Training

MANDIANT believes staff education is one of the most critical components of your Incident Response program. Depending on your requirements, MANDIANT can conduct a one-day Incident Response Training to prepare your staff. The training is designed for all levels of your organization, including technical staff, legal counsel, public relations and human resources. We highlight core skills and emphasize each group's particular roles and responsibilities in the Incident Response process. Participants perform technical exercises that expose them to investigative approaches that should be used in a variety of computer security incidents.