



## PROFESSIONAL SERVICES

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

## EDUCATION

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

## SOFTWARE

- FIRST RESPONSE
- WEB HISTORIAN



# INCIDENT RESPONSE PROGRAM DEVELOPMENT

As the sophistication and threat of computer security incidents increase, demands are being placed on organizations to have efficient incident response (“IR”) programs defined and in place. These programs should consist of formally documented guidelines and practices the organization will use in responding to incidents consistently and promptly, utilizing appropriate documentation and technical tools.

In the course of responding to hundreds of computer security incidents, Mandiant has developed an understanding of the tools, techniques and approaches that result in successful incident response. Leveraging this experience, Mandiant works with clients to build and implement IR programs customized to their unique needs.

Mandiant employs a structured process to:

- Assess the current state of an organization's incident response program
- Develop or enhance program processes and documentation
- Educate technical responders on specific technical response approaches
- Enable organizations to practice and refine their response techniques
- Communicate key program elements to specific groups that are either affected by the program or who have incident response responsibilities

Mandiant combines its technical expertise with its years of experience responding to major incidents in the private and public sectors to assist its clients with developing incident response programs that are both comprehensive and practical.

## Mandiant's IR Program Development process consists of four-steps:

### IR PROGRAM DEVELOPMENT AND ANALYSIS

Mandiant evaluates the state of the organization's current incident response capabilities and works with the organization to:

- Establish IR Program Goals
- Describe and document the IR process
- Define Response Team organization structure and roles
- Create forms, reports, checklists

### IR TRAINING

Once the IR program has been outlined and established, Mandiant provides training to the organization's first responders. Topic areas include:

- Collecting data from live systems
- Investigating issues in various operating system environments
- Collecting and analyzing network information
- Creating forensically sound images and performing forensic analysis on that data
- Creating live response tool kits

### DRY RUN EXERCISES

Incident response is improved by rehearsing and practicing the steps that are required prior to responding in a real situation. Mandiant works with clients to conduct dry run exercises. Activities include:

- Identifying one or more incidents to simulate
- Planning the incident set-up requirements and response activities in detail
- Performing incident set-up activities
- Executing the incident
- Monitoring and critiquing the exercise

### PROGRAM ROLL-OUT

For an IR program to be effective, appropriate constituencies within the organization must understand that the program exists and how it works. Mandiant helps organizations gain that understanding by:

- Working with clients to identify appropriate groups to brief
- Crafting the message to be communicated
- Helping communicate the IR program to the organization, from senior management to end-user