Foundstone Forensic Investigation

Hunting down the source of your attack

Your security team has the discipline to ensure your Incident Response (IR) plan is current. Twice each year, you create security breach test scenarios to keep the team focused and sharp. You are confident you can handle nearly any situation. Then it happens. Information from a strictly confidential internal document shows up on a web blog. Your initial investigation reveals there were only six members of the senior leadership team that had access to the document. Now you must determine how the information in the document leaked out of your organization.

Benefits

The Foundstone® Services Forensic Investigation Team is ready to provide you with the special investigative skills needed to hunt down electronic data. Staffed with some of the best and most experienced forensic talent in the business, we respond immediately and help you through your crisis. Our consultants provide the investigative expertise and tools to answer your data breach questions.

Methodology

Foundstone Services' proven forensic methodology is compliant, consistent, focused, and confidential. We stay informed of the latest legal rulings, rules of evidence handling, and industry best practices. We use proven tools and test them often. Our forensic methodology is highly refined and constantly improving, providing you consistent results in every engagement. By keeping investigations focused and specific, we also save you time and money. And above all, we maintain strict confidentiality in our forensic engagements.

The Foundstone Services Forensic Investigation framework is based on this process:

1. Determination of investigation scope and authority
2. Creation of an investigative plan
3. Interviews with staff
4. Forensic acquisition of electronic data
5. Strict chain-of-custody management
6. Forensic analysis of acquired data
7. Forensic reporting and follow-up
8. Expert witness/testimony, if required

Deliverables

The Foundstone Forensic Investigation engagement includes:

- Dispatch of forensic investigation consultant(s) to your site or analysis of hard drive remotely at our Incident Response Lab
- Written document describing investigation scope, authority, and investigative plan
- Periodic written investigative updates describing initial findings
- Written chain-of-custody documentation for all devices within investigative scope
- Written final report containing all details of forensic engagement

Scope

A typical engagement ranges from one to four weeks, depending on the scope of the investigation. Investigations with a large number of devices may require more time. During the investigation, we collaborate closely with your security team, IT, human resources, and legal and compliance teams. A comprehensive report of our findings will be provided to you at the end of the engagement.

The Foundstone Difference

All Foundstone projects are managed using our proven Security Engagement Process (SEP) for project management. A pivotal aspect of this process is continual communication with your organization to ensure the success of your consulting engagements.

Learn More about Foundstone Services

Fill the gaps in your information security program with trusted advice from Foundstone Services—part of the McAfee® global professional services organization that provides security consulting, customized product deployments, and training and advisory services. Let our consultants help your organization assess current policies, create new programs that meet compliance goals, and cost effectively prepare for security emergencies. Speak with your technology advisor about integrating our services. You can get more information at **www.foundstone.com**.

Related Foundstone Services

We offer many related services and training classes, including:

- IR Program Development
- IR Policy and Procedure Definition and Review
- IR Plan Testing
- IR Gap Analysis
- On-Site IR Emergency Response Team
- IR Plan Execution
- Investigative Services
- Malware Analysis
- Chain-of-Custody Management
- Expert Testimony
- IR Partner Program
- Forensic and Incident Response Education (FIRE)
- Comprehensive Network and Infrastructure Security Assessment

McAfee™
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com