

# Foundstone Incident Response Retainer Service

## Incident preparation is key to managing impact

With so many published security incidents every year, it is clear that breaches still happen, regardless of how secure an environment is. Be prepared ahead of time with a partner that supports you on site in case of a large-scale incident. Or better yet, reduces the likelihood and potential impact of security incidents.

As a trusted advisor, Foundstone® Services seeks to shift organizations from a highly reactive to a proactive posture. We leverage an “Assess, Build, and Train” model to sharply reduce the likelihood of a catastrophic breach requiring external support, while ensuring availability of industry experts in case there is a crisis.

### Foundstone Incident Response (IR) Retainer Options

The Foundstone Services team offers three incident response (IR) retainer models:

#### Tier 0—Best-Effort Response

This tier provides agreed-to terms for incident response. With no upfront cost to you, a locked-in rate is established, giving your team direct access to our experts when they are needed the most. In the event of a breach, our consultants strive to respond as rapidly as possible, but availability is not guaranteed.

#### Tier 1—Hourly IR Services Plus Workshop

Our second tier offering requires an initial up-front investment of \$15,000 to conduct an IR Foundations Workshop, which includes a one-day onsite workshop with your staff to understand the environment, delivery of a custom IR Plan, and a set of initial playbooks (up to 10) based on the environment. The service level agreement (SLA) includes an initial remote response within two hours and 48 hours for onsite response when required, with a discounted emergency IR rate in the event of a security incident.

#### Tier 2—Workshop Plus Dedicated IR Hours

This tier provides the most value in terms of knowledge transfer, IR support, and ultimate flexibility with a focus on maturing program capability in the weakest areas first, as well as yielding a rapid escalation path for large-scale incidents. It includes the IR Foundations Workshop and a dedicated pool of hours (the number of hours is

### Foundstone IR Retainer Service Tiers

---

#### Tier 0

Best-Effort Response

- Consultant availability not guaranteed
- No dedicated pool of hours
- Hourly rate

#### Tier 1

Two-Hour Remote Response, 48-Hour Onsite Response

- One-day onsite IR Foundations Workshop
- No dedicated pool of hours
- Discounted hourly rate

#### Tier 2

One-Hour Remote Response, 24-Hour Onsite Response

- One-day onsite IR Foundations Workshop plus potential IR hours reuse
- Dedicated pool of hours
- Lowest hourly rate

## DATA SHEET

scoped based on the environment size and complexity). This model allows for access to any of the non-urgent Foundstone services, with the option to convert to emergency IR hours for crisis coverage at a rate of 1.5 hours to one. The SLA for this tier is a two-hour initial remote response, with a 48-hour onsite arrival, if required.

### Key Benefits

Staffed with the best and most experienced IR talent in the business, our consultants provide the expertise and tools to help you through a crisis. Through the Foundstone IR Retainer model, we provide remote capability throughout the incident lifecycle, with a guaranteed response time for both Tier 1 and Tier 2 retainers. We also help your ongoing success by providing both strategic and technical recommendations.

Engaging with Foundstone Services ensures the following:

- **Confidentiality:** Your trust in us is deeply valued. We have a proven track record with our clients and the intelligence community for silence on incidents unless disclosure is expressly permitted with all details mutually agreed upon by our clients.

- **Experience:** We possess decades of combined experience delivering industry best practices.
- **Education:** Knowledge transfer is integral to every Foundstone engagement.

### Learn More

Fill the gaps in your information security program with trusted advice from Foundstone Services—part of the McAfee® 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 our services or email us at [foundstone@mcafee.com](mailto:foundstone@mcafee.com). Get more information at [www.foundstone.com](http://www.foundstone.com).

## Deliverables

---

### IR Foundations Workshop

- Foundstone IR Plan
- Foundstone Forensic Logging Strategy Guidance and Recommendations
- Debrief (discussion on high-level theme and proactive measures)

### Incident Response Engagement Executive Summary

- Project Overview
- Scope Description
- Summary of Findings
- Strategic Recommendations

### Technical Report

- Methodology/Tools
- Findings/Impact Detail
- Steps to Reproduce
- Affected Systems
- Recommendations
- Addendums as needed



2821 Mission College Boulevard  
Santa Clara, CA 95054  
888 847 8766  
[www.mcafee.com](http://www.mcafee.com)

McAfee and the McAfee logo and Foundstone are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2017 McAfee, LLC. 3034\_0517  
MAY 2017