DEPLOYMENT AND INTEGRATION SERVICES

Analysis Best Practices

OVERVIEW

FireEye Analysis Best Practices is a three-day, hands-on workshop focused on knowledge transfer and procedural documentation for malware detection, analysis and response. During this workshop, your organization will:

- Learn how to leverage FireEye technologies more effectively across the enterprise
- Integrate FireEye product alerts into your response processes
- Develop a deep forensic understanding of FireEye alerts

At the end of the workshop you receive a customized Analysis Best Practice Response Procedures document that contains guidance on the interpretation of FireEye alerts and outlines appropriate actions for investigating and containing malware in your environment.

Analysis Best Practices Workshop Agenda

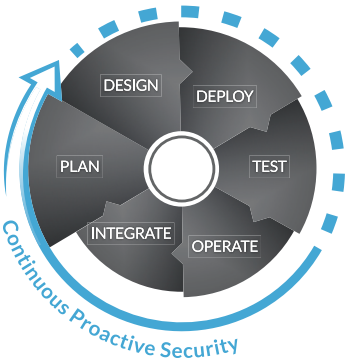
Day 1 starts with a four-hour collaborative session during which FireEye professionals work with your response team to:

- Review your organization's response roles and responsibilities
- Review existing response processes
- Discuss how your organization uses FireEye technologies in your response processes
- Perform a detailed review of attack scenarios and resulting alerts
- Review a standard FireEye OS Change Report
- Conduct a hands-on exercise with real malware examples
- Extract indicators of compromise (IOCs) from FireEye alerts
- Review your alerts, applying learned methodologies
- Examine alert information in FireEye interfaces

HIGHLIGHTS

- **Alert Prioritization and Response:** Understand the severity of alerts and learn processes to quickly identify and triage them
- **Malware Identification:** Learn to use both internal and open source intelligence to quickly identify malware and key malware traits
- **Malware Analysis:** Learn to analyze key details in FireEye OS change reports, such as Registry and Mutex data
- **Adaptive Response:** Learn procedures and prevention measures that correlate with other internal technologies to prevent future threats

DEPLOYMENT AND INTEGRATION



FireEye

Day 1 continues with an introduction to the FireEye Best Practices Process and Procedures document. Together, we discuss your specific scenarios and whiteboard the workflow for FireEye alerts.

Day 2 begins with another four-hour workshop where we:

- Discuss in detail the OS Change Report structure, including API calls, Mutexes and more
- Conduct a hands-on exercise with advanced malware
- If applicable, discuss processes to create IOCs in IOC Editor based on FireEye OS Change Report details and to leverage IOCs for endpoint threat prevention, detection and forensics
- Review the implementation and use of YARA rules in FireEye technologies
- Review the process for investigating and reporting possible false positive issues
- Use FireEye metrics with Python scripts (FireEye-csvTdata) to prioritize alerts or hosts for remediation

Day 2 continues with a tabletop scenario exercise that follows the process document using your alerts or the alerts reviewed during the hands-on exercise. Day 2 ends with an open discussion on any additional FireEye alerts or scenarios.

Day 3 is a remote session in which FireEye presents a customized Analysis Best-Practice Response Procedures document that contains:

- Detailed event scenarios and categories
- Guidance for specific alert and infection types identified by FireEye devices
- Event procedure workflow
- FireEye product alert event procedures, including correlating alerts with your other security technologies

FireEye concludes the workshop with a one-hour web conference to review the details of the procedural guide and make any updates or edits.

For more information on FireEye, visit:
www.FireEye.com

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035 tel: 408.321.6300 / 877 FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

FireEye® is the leader in intelligence-led security-as-a-service. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks. FireEye has over 5,000 customers across 67 countries, including more than 940 of the Forbes Global 2000.

FireEye