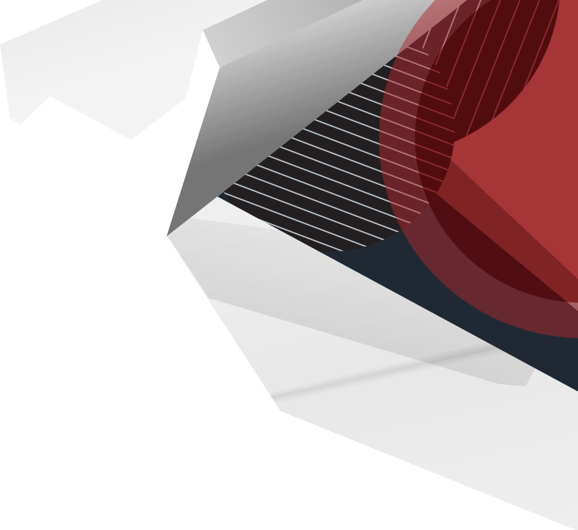

DEPLOYMENT & INTEGRATION SERVICES DATA SHEET

Analysis Best Practices

BENEFITS

- **Alert prioritization** and response for rapid threat identification and triage
- **Malware identification** through the use of both internal and open source intelligence
- **Malware analysis** using FireEye OS change reports and other artifacts
- **Endpoint investigation** using available tools to create an activity timeline associated with alerts and potential compromise
- **Customized indicators of compromise** created and tuned for use cases in your environment with FireEye-provided tools and scripts

Overview

FireEye Deployment and Integration Services can help provide teams with valuable skills and knowledge to ensure successful implementation and ongoing use of FireEye technologies.

Analysis Best Practices is a 2-5 day hands-on workshop that gives participants the expertise and step-by-step guides they need for malware detection, analysis and response using FireEye security products. During an Analysis Best Practices workshop, your team will learn how to:

- Use FireEye technologies more effectively across the enterprise
- Integrate FireEye product alerts into your response processes
- Develop a deep forensic understanding of FireEye alerts
- Implement best practices for investigating alerts

FireEye collaborates with you to develop an agenda from available topics based on your team's needs and relevant FireEye technologies. Whenever possible, the workshop uses alerts and data from your FireEye systems to provide real world examples and build capabilities within your systems. The workshop complements **FireEye Course Catalog** offerings that provide product training in a classroom environment with access to a training lab for student practice.

Analysis Best Practices Workshop Topics

The Analysis Best Practices workshop is customized to address the FireEye technologies used by your organization. The workshop can include content on roles and responsibilities, existing response processes and response workflow best practices, and the use of FireEye technology in your response processes. The required quantity of Analysis Best Practices SKUs depends on topics selected. Currently available topics include:

General Topics

- Threat landscape and FireEye ecosystem overview
- Mandiant Attack Lifecycle and MITRE ATT&CK framework
- FireEye Market
- Working with FireEye Support

Network Security (NX series)

- MVX technology for Network Security
- Alert types and analysis
  - Web infections, malware objects, and malware callbacks
  - Detailed review of attack scenarios and resulting alerts
- OS Change Report
  - FireEye OS Change Report deep dive, including API calls and mutexes
  - Hands-on exercise with real malware examples
  - Extracting indicators of compromise (IOCs) from FireEye alerts
- SmartVision capabilities
  - Client-side and east/west detection
  - Server-side and web shell detection
  - JA3 fingerprinting
- Evidence Collector and metadata streaming for network traffic analysis
- Alert review on your Network Security systems, applying learned methodologies
- Investigating and reporting a possible false positive
- Validation of network alerts using Redline (and Endpoint Security, if applicable)

Email Security (EX series and ETP)

- MVX technology for Email Security
- Secure Email Gateway and antivirus/anti-spam (AV/AS) (ETP only)
  - Reputation block lists
  - Smart DNS
  - PenPal analysis
  - Impersonation detection and business email compromise (BEC)
- Email Advanced Threat Detection
  - FireEye Advanced URL Defense Engine (FAUDE), URL rewriting and retroactive detection/clawback
  - Controlled Live Mode
  - Skyfeed
  - Dynamic URL analysis
  - YARA rules
- Phishing detection
  - FAUDE
  - PhishVision
  - Kraken

Endpoint Security (HX series)

- Endpoint Security agent operations and communication
- Agent troubleshooting and performance tuning
- Endpoint detection engines, alert types and analysis
  - Real-time intelligence-based detection
  - Exploit Guard
  - Malware Protection
  - Malware Guard
  - Innovation architecture and endpoint modules (such as Process Tracker and Enricher, Logon Tracker, Process Guard, UAC Protect and Event Streamer)
- Agent policies and best practices
- User roles and permissions
- Containment processes
- Enterprise Search with example use cases, including the use of IOCs from OS Change Reports (if applicable)
- Data Acquisitions (basic and advanced) with example use cases
- HXTool and HX API, including bulk acquisitions and data stacking use cases
- Hands-on Endpoint Investigation workshop using Triage Viewer and Redline
- Hands-on custom IOC workshop using IOC Editor (testing, validating, tuning IOCs)

Network Forensics (PX and IA series)

- Architecture and operation
- Management and administration
- Integrations with threat intelligence and other FireEye products
- Troubleshooting network traffic visibility
- Visibility in the attack lifecycle
- Alerts and custom rules
- Search and Builder overview and session analysis
- Distributed search using the investigation analysis appliance
- Lists, dashboards and alert aggregation
- Protocol, metadata and application identification
- Use of event based capture (EBC) policies and alerts in a threat hunting process
- Management of logs and system health

Helix

- Architecture and operation
- Data source selection and best practices
- Helix fundamentals
  - Features and capabilities
  - Events, alerts, and cases
  - Data parsing, including creating custom parsing rules
  - Management and administration
  - Integrations (FireEye ecosystem and cloud integrations)
- Alerting and investigation
  - Alert details
  - Entity-based alert correlation
  - Investigative workflow
- Case management
- Search and MQL
- Rules and lists
- Custom dashboards and reporting
- Hands-on threat hunting
- Use of the Helix API to integrate alerts into third-party tools

To learn more about FireEye, visit: **www.FireEye.com**

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

About FireEye, Inc.

At FireEye, our mission is to relentlessly protect organizations with innovative technology, intelligence and expertise gained on the frontlines of cyber attacks. Learn how at www.FireEye.com.

About Mandiant Solutions

Mandiant Solutions brings together the world's leading threat intelligence and frontline expertise with continuous security validation to arm organizations with the tools needed to increase security effectiveness and reduce business risk.