FIREEYE | MANDIANT

DEPLOYMENT & INTEGRATION SERVICES DATA SHEET

Security Orchestration, Automation and Response

BENEFITS

- **Efficient implementation** of highest priority use cases via playbook development by FireEye experts
- **Playbook prioritization** of the most costly manual processes
- **Integrations** with third-party products using standard and bespoke plugins
- **Operational readiness** facilitated by hands-on knowledge transfer to enable continued development of SOAR capabilities

Overview

FireEye Deployment and Integration Services for security orchestration, automation, and response (SOAR) use FireEye Security Orchestrator to automate your security processes, increase security operations efficiencies and reduce repetitive tasks, allowing your team to focus on higher level investigative and proactive security tasks. FireEye SOAR experts work with your team to implement a set of playbooks to handle your highest priority use cases. These professionals also show your team how to maintain existing playbooks, import and customize additional playbooks and create new playbooks. We offer three types of services to help you orchestrate and automate your security operations:

- SOAR Jumpstart Services
- Playbook Development
- FireEye Security Orchestrator Training

SOAR Jumpstart Services

Jumpstart Services for SOAR are designed to help you deploy FireEye Security Orchestrator and quickly automate aspects of your security operations. Each deployment starts with an Orchestration Planning Workshop to review your security monitoring, investigation and response processes and identify use cases that can be automated to increase your team's efficiency and effectiveness. FireEye experts help you evaluate proposed playbooks and prioritize them for implementation. They work with you to select up to four playbooks (depending on complexity) for development.

Using workshop data, FireEye experts develop and then review the process flow design for each playbook with your team, adjusting as appropriate based on your feedback. The experts then deploy Security Orchestrator and build out and test the newly developed playbooks for effectiveness and accuracy. During build out, FireEye experts show your system administrators how to manage and maintain Security Orchestrator; they also show your security analysts how to build, modify, operate and manage playbooks.

Jumpstart Services include:

- Use case review and playbook planning and prioritization
- Playbook process flow design and review
- Deployment and configuration of FireEye Security Orchestrator
- Playbook development, testing, and implementation
- Discussion of FireEye Security Orchestrator management
- Overview of playbook management and development process
- Introduction to FireEye customer resources such as the FireEye Customer Support Portal and Community and FireEye Market

Playbook Development

For customers that already have FireEye Security Orchestration deployed and want assistance to build out additional playbooks, FireEye provides SOAR development services customized based on playbooks to be developed and implemented. FireEye experts review the proposed use cases and determine the best implementation path. For each playbook to be developed, FireEye experts develop and then review the process flow design with your team, adjusting as appropriate based on your feedback. The experts then build out and test the playbooks for effectiveness and accuracy. The service also offers review sessions to help ensure that your team can manage and maintain Security Orchestrator and the new playbooks.

Security Orchestration Playbook Development Services include:

- Use case review and playbook planning and prioritization
- Playbook process flow design and review
- Playbook development, testing, and implementation

FireEye Security Orchestrator Training

FireEye offers an in-depth, hands-on security orchestration training course for customers that are new to FireEye Security Orchestrator or that want to build up their expertise. The two-day training course covers everything your team needs to know to manage and maintain FireEye Security Orchestrator and implemented playbooks as well as to create new playbooks. Most of the second day is spent on playbook development with a hands-on exercise that walks students through the process from start to finish. FireEye Security Orchestrator topics covered in the course include:

- Configuration and virtual appliance administration
- Plugins, packages, devices and adapters
- Tasks, tables and forms
- Architecture and data flows
- Command line interface and configuration files
- Logging
- Step-by-step playbook development
- Playbook and plugin troubleshooting
- Building custom scripts
- Array methods, JSON methods, control structures, and URI encoding

FireEye also offers hands-on plugin development training, which provides an additional two-days of training specific to Security Orchestrator plugin development. Students in this portion of the course should be able to program in Python and Java and will gain practical experience by writing a plugin during the course.

Table 1. Security Orchestration Services Comparison.

	Basic Jumpstart	Playbook Development	Training
Orchestration planning workshop with use case review	✓	✓	
Playbook* planning and prioritization	✓	✓	
Playbook process flow design and review	✓	✓	
Deployment and configuration of FireEye Security Orchestrator	✓		
Playbook development, testing, and implementation	Up to 4*	✓*	
Knowledge transfer session on FireEye Security Orchestrator management	✓		✓
Overview of playbook management and development	✓		✓
Hands-on playbook development training			✓

*Actual number of playbooks to be developed depends on complexity of requested playbooks. Playbooks to be included in scope will be mutually agreed upon.

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.