FIREEYE | MANDIANT

DEPLOYMENT & INTEGRATION SERVICES DATA SHEET

Staff Augmentation

BENEFITS

- **FireEye product expertise** directly from FireEye experts for effective solution deployment and maintenance
- **Enhanced visibility** through integration of FireEye and third-party cloud and on-premise data sources to maximize visibility
- **Use case implementation** with guidance on data source selection, custom rule development and threat hunting enablement
- **Operational readiness** that enables rapid identification, triage and containment of security events

Overview

FireEye Deployment and Integration Services can help plan, deploy and manage all aspects of an organization's security program and architecture. These FireEye services offer both FireEye product expertise and in-depth knowledge of security systems for organizations of every size.

Staff Augmentation services provide expertise on both FireEye products and information security to fill gaps in your team on a temporary or semi-permanent basis. They can help deliver timely knowledge or skills, cover an open position during the hiring process or meet requirements of a long term position. Resources offered are backed by all the expertise and experience of both FireEye and Mandiant professionals.

The three most commonly filled roles are FireEye security engineers, FireEye SIEM/SOAR engineers, and FireEye security analysts. Services offered by these roles include:

- Deployment and implementation of FireEye solutions
- Ongoing management and maintenance of FireEye solutions
- On the job knowledge sharing with your team
- SIEM and SOAR development and implementation
- Best practices for alert analysis and investigation
- Analysis and threat hunting with FireEye solutions

FireEye Security Engineer
A FireEye Security Engineer staff augmentee can join you at any point along your FireEye journey. They can help you architect your FireEye solution, plan deployment and handle all aspects of the solution implementation. As your operations evolve, the engineer manages, maintains and updates the FireEye solution, reviews and implements applicable add-on modules from FireEye Market, and trains your security team on new capabilities, features and modules. The engineer also helps integrate the FireEye solution into your existing security stack and your security operations playbooks and procedures. In short, the FireEye Security Engineer provides the FireEye product expertise you need to maximize the value of your FireEye Security solution.

FireEye SIEM/SOAR Engineer
A FireEye SIEM/SOAR Engineer brings expertise in security event management, security orchestration and automation and security operations to your organization to help build and implement security use cases and playbooks in your SIEM and SOAR platforms. For organizations with a mature security operations program and well-defined use cases, the engineer can help configure the SIEM to apply relevant data sources to those use cases and build out rules and dashboards to provide the visibility the SOC needs. The engineer can also enhance your SOC capabilities through automation, implementing defined playbooks in Security Orchestrator.

For organizations that are still defining SOC use cases and building out playbooks, the engineer gains an understanding of current processes and identifies opportunities to mature SOC capabilities through use cases implemented in your SIEM. The engineer can also highlight opportunities to increase team efficiency through automation of repetitive processes, which helps teams focus on higher-value security tasks.

FireEye Security Analyst
A FireEye Security Analyst has in-depth knowledge of FireEye security products as well as alert analysis and security operations. The analyst offers your team the expertise required to manage and get the most from deployed FireEye solutions. In addition to daily analysis, the analyst also helps integrate FireEye solutions into security operations, train teams on FireEye products, review common use cases and recommend approaches for alert review and analysis, threat investigation and triage. The analyst can also help your team with threat hunting and sweeping the environment for specific threat indicators.

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

M-EXT-DS-US-EN-000354-01

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.