DEPLOYMENT AND INTEGRATION SERVICES

Threat Analytics Platform

OVERVIEW

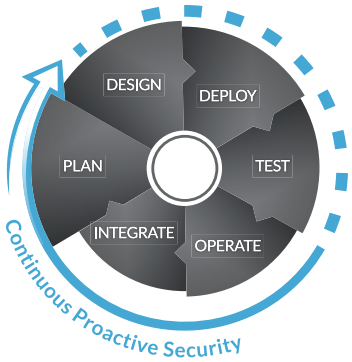
Deployment and Integration Services for the FireEye Threat Analytics Platform (TAP) combine TAP deployment and knowledge transfer with world-class threat intelligence and security consulting, allowing organizations to detect and respond to cyber security incidents faster. Several levels of engagement are available:

- The **basic jumpstart** is for organizations with minimal data sources that want to accelerate implementation and integration with their existing security operations.
- The **advanced jumpstart** is for organizations with larger or more complex networks as well as a larger set of data sources with deeper analytics requirements.
- The **FireEye as a Service TAP basic jumpstart** is for organizations with FireEye as a Service subscriptions that want to quickly augment their security monitoring posture with TAP visibility.
- The **TAP optimization service** is for organizations that want to maximize the effectiveness of their existing TAP deployments. FireEye professionals validate existing TAP deployments against current detection methodologies, identify data source gaps, and fine-tune rules, lists and other TAP content. They also review the security use cases to ensure that the TAP deployment meets the organization's needs.

HIGHLIGHTS

- **Efficient Deployment:** Accurate, best-practice configuration deployed by FireEye experts
- **Leading Threat Intelligence:** Cutting-edge FireEye threat intelligence applied to event sources
- **Maximum TAP Value:** Guidance on data source selection, custom rule development and threat hunting enablement
- **Efficient Analysis:** Effective and meaningful search of billions of records
- **Periodic Check-ups:** Configuration validations and health checks

DEPLOYMENT AND INTEGRATION



FireEye

Table 1. Deployment and Integration Services for TAP.

	TAP Basic JumpStart	TAP Advanced JumpStart	FireEye as a Service TAP Basic Jumpstart	TAP Optimization
Number of hours	64	120	80	40
Customer type	New or existing	New or existing	New or existing	Existing only
Onsite visits	1 visit, 32 hours	2 visits, 32 hours	1 visit, 32 hours	Remote only
Deployment of Communication Broker or Cloud Collector	1-3	4-10	1-3	
Data source on-boarding	3-5	6-10	5-7	1-2
Conduct TAP workshop	5 staff	10 staff	As needed	As needed
Configure rules, lists, custom intelligence	Yes	Yes	As needed	As needed
Create custom rules	1–5	1–15	As needed	As needed
Configure and tune dashboards	Yes	Yes	As needed	Yes
Conduct hunting enablement		Yes		
Document/verify use case		Document		Verification
Perform configuration validation		Yes		Yes
Conduct rule efficiency analysis		Yes		Yes

TAP Basic Jumpstart

The basic TAP jumpstart is designed to help new or existing TAP deployments swiftly integrate TAP with existing security operations. It includes a data source workshop where FireEye professionals review your current architecture and data sources and recommend the steps necessary to ingest data specific to a customized use case while maximizing the value of TAP. FireEye helps deploy and configure up to three Communication Brokers or Cloud Collectors, and will integrate up to five event sources into TAP. FireEye experts review data source and event information for parsing accuracy, validate field mappings and perform gap analysis.

FireEye configures TAP lists and rule data specific to your organization (for example, high-value assets, domains and network spaces) so you can use the TAP interface to gain situational awareness of your environment. FireEye also configures up to five custom rules specific to your environment to allow the creation of TAP custom dashboards.

During this jumpstart, FireEye consultants will ensure that your staff can:

- Understand basic TAP architecture and user interface basics
- Use search effectively to find threats
- Use custom rules, indicators and dashboards
- View and respond to TAP alerts with contextual intelligence from the FireEye Intelligence Center (FIC).

TAP Advanced Jumpstart

The TAP advanced jumpstart includes the basic TAP jumpstart and adds enhanced integration for larger environments. It provides advanced hunting and optimizations to ensure the effectiveness and longevity of your TAP and Cloud Collector deployment. FireEye professionals help facilitate and conduct hunting exercises in TAP to find threats, anomalies, visibility gaps and misconfigurations. They also recommend improvements.

Periodic TAP optimization sessions help you maintain your TAP implementation and operations by reviewing and updating:

- Custom use cases
- Custom lists and dashboards
- Data and log source gaps
- Rules optimization
- Use of new features

FireEye as a Service TAP Basic Jumpstart

This jumpstart enables FireEye as a Service for TAP monitoring. It helps implement TAP, integrate existing data sources, tune and parse events, and deploy FireEye as a Service monitoring and response capabilities, using the advanced cloud threat analytics offered in TAP.

To provide you with situational awareness of your environment, FireEye professionals configure contextual data by identifying high-value assets and network spaces. FireEye consultants also examine current data sources and identify possible visibility gaps to ensure that FireEye security operations centers can monitor your entire landscape. FireEye also conducts periodic TAP optimization sessions to identify data and log source gaps and to close gaps in event parsing and detection. During these sessions, FireEye professionals review custom rules and other TAP metadata to ensure optimal monitoring and detection.

TAP Optimization

With the addition of new features and code enhancements, the TAP Optimization service ensures that your TAP instance can maintain its effectiveness as your environment grows and changes. Designed for existing TAP customers, this remote engagement identifies and verifies data source gaps, unparsed or mis-parsed events, excessive alert volumes, custom list content, dashboard efficiency, rule posture, account usage and use case alignment. The service also identifies new rules and additional data sources you need to ensure the continued success of your TAP implementation.

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