DEPLOYMENT & INTEGRATION

THREAT ANALYTICS PLATFORM SERVICES

OVERVIEW

FireEye Threat Analytics platform (TAP) deployment provides essential expertise to help security teams maximize their investment in the FireEye TAP product. These services combine TAP deployment and knowledge transfer services with world class threat intelligence and security consulting to enable faster detection and response to cyber incidents across organizations of any size. Available in multiple variations of engagement, customers can choose the right level of services to meet their needs

TAP Basic JumpStart

The Basic JumpStart service is designed for customers with minimal data sources looking to quickly accelerate their Threat Analytics Platform implementation and integration with their existing security operations.

TAP Advanced JumpStart

The Advanced JumpStart service is designed for customers with larger or more complex networks that need to implement and integrate the Threat Analytics Platform typically consisting of a larger set of data sources and deeper requirements for analysis.

FaaS Basic TAP Jumpstart

The FaaS Basic TAP JumpStart service is designed for customers with FaaS subscriptions that want to quickly enable, augment, and increase their security monitoring posture with the addition of TAP visibility.

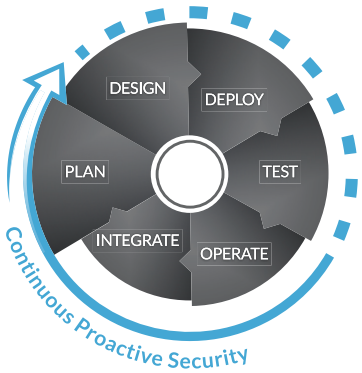
TAP Optimization

The TAP Optimization service is designed for customers with existing deployments who want to maximize their effectiveness of TAP. FireEye professionals validate existing TAP deployments versus current detection methodologies, identify data source gaps, and tune rules, lists, and other TAP content. They also review the security use cases to ensure TAP is meeting the needs of the organization.

HIGHLIGHTS

- **Efficient Deployment** – Accurate and best practice configuration deployed by FireEye experts
- **Threat Intel** – Apply bleeding edge FireEye Threat Intel to a myriad of event sources
- **Maximize TAP Value** – FireEye experts guide you through data source selection, custom rule development, and hunting enablement
- **Increase Enterprise Visibility** – Mine data you never could with legacy SIEM
- **Efficient Analysis** – Learn how to effectively and meaningfully search billions of records in seconds
- **Periodic Check-ups** – Configuration validations and health checks protect a TAP investment

DEPLOYMENT & INTEGRATION



FireEye
SECURITY REIMAGINED

	TAP BASIC JUMPSTART	TAP ADVANCED JUMPSTART	FAAS 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	1x32 hours	2x32 hours	1x32 hours	Remote
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 Intel	Yes	Yes	As needed	As needed
Create Custom Rules	Up to 5	Up to 15	As needed	As needed
Configure and Tune Dashboards	Yes	Yes	As needed	Yes
Conduct Hunting Enablement		Yes		
Document/Verify Use Case		Document		Verify
Perform Configuration Validation		Yes		Yes
Conduct Rule Efficiency Analysis		Yes		Yes

TAP Basic JumpStart Service Overview

FireEye services leverage world class consulting expertise to deliver cloud analytics solutions implementation, integration of existing data sources, event tuning and parsing, enablement, and customization. The Basic TAP Jumpstart Service is geared for new or existing TAP deployments to swiftly integrate and optimize in-place security operations into the Threat Analytics Platform.

The Basic TAP Jumpstart Service includes a Data Source Workshop, where FireEye professionals review the current architecture and data sources, and recommend necessary steps to ingest data specific to a customized use case while maximizing the value of TAP. FireEye professionals will assist in deploying and configuring up to three Communication Brokers or Cloud Collectors, and will integrate up to five event sources into TAP. Our professionals will review data source and event information for parsing accuracy, validate field mappings, and perform the necessary gap analysis.

FireEye will configure TAP lists and rule data specific to the customer enterprise (e.g., high value assets, domains, and network spaces) to provide environment situational awareness through the TAP interface. This service is designed to enable and create TAP custom dashboards and rules by configuring up to five custom rules specific to the environment.

During the project, TAP operators will learn the basics of User Interface navigation and use in daily operations, search best practices and syntax, event and alert analysis and handling, and intelligence context in FireEye Intelligence Center (FIC). FireEye consultants ensure TAP operators can:

- Understand TAP architecture and user interface basics
- Use search effectively to find evil
- Leverage custom rules, indicators and dashboards
- View and respond to TAP alerts

TAP Advanced JumpStart Service Overview

The TAP Advanced Jumpstart augments the Basic TAP JumpStart with enhanced integration for larger environments along with advanced hunting and optimizations to ensure the effectiveness and longevity of the TAP and Cloud Collector deployment. FireEye professionals will help facilitate and conduct Hunting exercises in TAP to find evil, anomalies, visibility gaps, and misconfigurations, as well as prepare findings for recommended improvements. In addition, periodic TAP optimization sessions are included to help sustain the 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

FaaS Basic TAP JumpStart Service Overview

The Faas TAP Basic Jumpstart is an ideal solution for implementation, integration of existing data sources, event tuning and parsing, and onboarding with FireEye as a Service (FaaS) monitoring and response capabilities, leveraging the advanced cloud threat analytics offered in TAP. The primary goal of this service is to enable the FaaS service for TAP monitoring. FireEye professionals will configure contextual data by identifying high value assets and network spaces to provide environment situational awareness. FireEye consultants will also examine current data sources and identify possible visibility gaps to ensure a complete landscape is monitored by our world-class Security Operations Centers. In addition, FireEye will conduct periodic TAP optimization sessions in order to identify data and log source gaps, as well as assist in closing gaps in event parsing and detection. During these sessions, FireEye professionals also review any custom rules and other custom TAP metadata to ensure optimal monitoring and detection posture in TAP.

TAP Optimization Service Overview

As environments grow and change, FireEye ensures TAP instances are able to maintain their efficacy through the TAP Optimization service. Designed for existing TAP customers, this entirely remote engagement identifies and verifies data source gaps, unparsed or mis-parsed events, excessive alert volumes, custom list content, dashboard efficiency, rule posture account audit, and use case alignment. The service identifies new rules and additional data sources required for continued success of the TAP implementation. Our team also enables the customer to make maximum use of the platform, including new TAP features and code enhancements.

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

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

www.FireEye.com