FireEye Threat Analytics Platform (TAP) Detect and Generic SIEM Platforms

Flexibility to Investigate Advanced Security Threats on Generic security Management Platforms

SOLUTION BRIEF

INTEGRATED SOLUTION HIGHLIGHTS

- Enables seamless FireEye integration with existing SIEM implementations.
- Leverages current incident response workflow and ticketing.
- Enhances ability to identify trends across multiple environments to develop business intelligence.
- Provides detection status for all alert levels.
- Gives insight into active and past alerts.
- Identifies trends and emerging patterns.
- Supports event detail and drill down.

OVERVIEW

Customers using FireEye Threat Analytics Platform (TAP) Detect can easily correlate and investigate threat events across multiple attack vectors using virtually any standard security information and event management (SIEM) platform. FireEye Threat Analytics Platform (TAP) Detect generates the alert. The alert is sent to the SIEM where the incident responder will utilize the SIEM to investigate the event.

THE CHALLENGE

Organizations are facing challenges after they set up Hadoop clusters and begin storing data in Hadoop. They need to find a way to garner value from the massive amounts of big data that pass through their organizations. But big data presents an inherent challenge because big data is variable, disparate, incomplete and often in motion. It's hard to get a grasp of big data in a way that delivers value.

Machine data is a critical subset of big data. It's valuable because it contains records of user behavior: purchasing habits, security violations, fraud attempts, social media posts and customer experiences.

Though Hadoop has made machine data easier to store, its value is elusive because few have the time or money to customize Hadoop and to develop assorted tools that deliver an effective analytical capability.

THE INTEGRATED SOLUTION

SIEM platforms provide a big data platform to collect, index, and harness machine-generated data coming from websites, applications, endpoints, servers, networks, and security products, such as FireEye.

The SIEM platform acts as an agent for log collection from remote machines. It collects logs from remote machines and puts it in a database for further processing and storage. It also forwards the log data to the FireEye Threat Analytics Platform (TAP) Detect for analysis and alert creation. FireEye Threat Analytics Platform (TAP) Detect provides the threat intelligence and analytics while utilizing the search and storage functionality of the SIEM.

Most SIEM platforms can scale to tens of thousands of remote systems, collecting terabytes of data with minimal impact on performance.

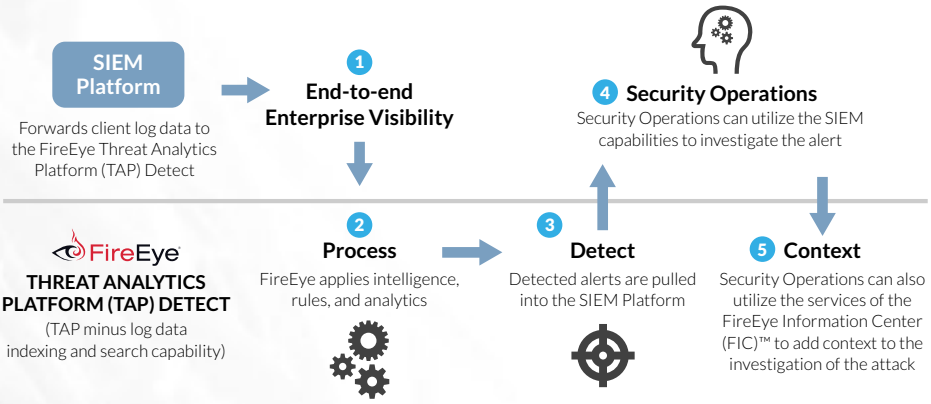
FIREEYE PRODUCT AND VERSION

FireEye Threat Analytics Platform (TAP) Detect

CSC PRODUCT AND VERSION

All Generic SIEM Platforms

FireEye Threat Analytics Platform (TAP) Detect and Generic SIEM Platforms



HOW THE JOINT SOLUTION WORKS TOGETHER

FireEye Threat Analytics Platform (TAP) Detect works together with generic SIEM platforms as follows:

- Client logs feed threat intelligence into the SIEM platform.
- From the SIEM platform, the appropriate logs (database, security, network, and endpoint) are sent into FireEye Threat Analytics Platform (TAP) Detect.
- FireEye Threat Analytics Platform (TAP) Detect applies rules and threat intelligence against those logs.
- The incident responder is notified of matches.
- The incident responder can utilize the SIEM platform to investigate the alert.
- Additionally, the incident responder can use FireEye Intelligence Center to get context on the alert.

Having the alerts fed back into the SIEM platform gives customers a single pane of glass for reporting and monitoring.

THE VALUE OF THIS PARTNERSHIP

The integration between FireEye Threat Analytics Platform (TAP) Detect and generic SIEM platforms allows clients to have the appropriate logs sent from their SIEM platform into FireEye Threat Analytics Platform (TAP) Detect. FireEye Threat Analytics Platform (TAP) Detect then applies rules and threat intelligence against those logs and generates alerts sent to the incident responder in Security Operations. In addition to using the SIEM platform for the investigation, the incident responder can also use the FireEye Intelligence Center (FIC) to determine the context of the attack.

This integration highlights the reporting and compliance strengths associated with generic SIEM platforms and the threat intelligence and analytics that are considered strengths of FireEye Threat Analytics Platform (TAP) Detect solution.

ABOUT FIREEYE

FireEye protects the most valuable assets in the world from today's cyber attackers. Our combination of technology, intelligence, and expertise — reinforced with an aggressive incident response team — helps eliminate the impact of breaches. FireEye has over 4,000 customers across 67 countries, including more than 650 of the Forbes Global 2000.

ABOUT SIEM

Security information and event management (SIEM) are approaches to security management that seek to provide a holistic view of an organization's information technology (IT) security. SIEM technology provides real-time analysis of security alerts generated by network hardware and applications.

For more information contact CSC@fireeye.com.

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | **www.fireeye.com**