THREAT ANALYTICS PLATFORM: CLOUD COLLECTOR

EVENT GENERATOR THAT SECURELY CREATES AND STREAMS EVENT DATA TO THE FIREEYE THREAT ANALYTICS PLATFORM (TAP)

OVERVIEW

The FireEye® TAP Cloud Collector is a managed technology that securely generates meta-data in the form of network events and streams that data to the FireEye Threat Analytics Platform (TAP). In combination with TAP, the Collector provides a network security monitoring solution that applies threat intelligence to all network data and gives visibility across all locations without the operational complexity and costs associated with traditional solutions such as SIEMs.

A Simpler Way to Collect Event Data

The Cloud Collector speeds time-to-value for the Threat Analytics Platform by eliminating the complexity of deploying and managing log sources at each site. It comes preconfigured with the necessary parsers and software to securely stream network event data into TAP. Organizations only need to configure their TAP credentials.

Flexible Deployment Options

The Cloud Collector is deployed via SPAN or a network tap. It can be placed in various locations within a network, and provides differing value based on its positioning. The technology does not apply threat intelligence, analytics, or rules — all analysis is performed in the TAP cloud. This flexibility allows the Cloud Collector to be an affordable extension of your FireEye Threat Analytics Platform.

FireEye offers the Collector in software, for customers who wish to deploy it on their own hardware or virtual machine environments, or as a hardware solution.

Securely Stream Event and Log Data to TAP

The Cloud Collector watches network traffic passively and constructs events to describe the activity it sees. It can create logs for over 20 types of activities and artifacts including web browsing, file transfers, certificate exchanges, Windows file shares, and Remote Desktop sessions. All event data and logs are compressed and encrypted before being sent to TAP, thereby maximizing security while minimizing network bandwidth

HIGHLIGHTS

- Speeds TAP time-to-value by simplifying event & log aggregation
- Passively collects over 20 types of data from network data
- Eliminates need to configure log sources at each site
- Collects, compresses & encrypts data before sending to TAP
- Centrally managed as a part of the TAP ecosystem
- Deploys via SPAN or network tap
- Ideal for organizations with branch offices & remote sites

FireEye
SECURITY REIMAGINED

During a typical forensic investigation, most PCAPs are manually processed in order to extract a suspicious file or email. The File Analysis Framework feature allows specific file types to be pulled from the network stream to be analyzed automatically. This data can be optionally sent to cloud MVX for in depth behavioral analysis.

CC allows for capture of all observed network traffic for in depth analysis in FireEye products. PCAPs can be requested and retrieved through the Helix and TAP product interfaces.

Highly Scalable Architecture

The TAP + Cloud Collector deployment architecture is highly scalable and ensures high performance event collection, regardless of whether a handful or thousands of devices are deployed

Centrally Managed through TAP

All Cloud Collectors are centrally managed through the TAP cloud without the need for additional management consoles, staff, or training. Once connected, the TAP team manages the configuration and monitors health of the sensor remotely.

Ideal for Remote Offices

The cost-effective Cloud Collector is ideal for many use cases but one particularly powerful use case is branch offices or remote sites. The plug-and-play nature is ideal for locations without dedicated IT staff and can be rapidly installed in just a few minutes.

Together with TAP, the Cloud Collector delivers the industry's best threat intelligence and visibility to advanced threats targeting an organization's assets across all locations. All of this is accomplished without the operational complexity and costs associated with traditional solutions, such as SIEMs.

Event & Log Data Sources

The TAP Cloud Collector aggregates event data and logs from a broad range of protocols, software logs, SIEMs, and other 3rd party vendor devices. Some common event or log data sources are listed below:

SOURCE	WHAT IS COLLECTED	HOW LOGS ARE USED IN TAP
FireEye Logs	Alerts from FireEye Threat Prevention Platform devices	Analyzes FireEye alerts and correlates across all other events to reconstruct attacks
Security Device Logs	Event data from 3rd party security devices	Filters through the high volume of alerts to find the alerts that matter
Connection Logs	Connection information and duration between two hosts	Track movement of malicious hosts around the network
DNS Logs	All DNS requests	Identify malware or APT activity
Files Logs	Names/hashes of files	Useful for malware detection
SMTP Logs	All SMTP headers	Identify internal spam abuse or augment SMTP logs
HTTP Logs	Similar to proxy/webserver logs	See attacks on internal web servers or malware leaving an egress
SSL Certificate Logs	Certificate information such as CA	Identify known bad certificates
SMB Logs	Files and user access across Microsoft ports	Track files and authentications across the network boundaries
Remote Desktop Session Logs	Details on remote desktop sessions (keyboard language, source/dest)	Visibility into lateral movement
SIEM Logs	Event data from a local SIEM	Analyzed against threat intel to detect threats
ICS Logging	Logs all Modbus and DNP3 commands	ICS rule pack

In addition to the listed categories, the Cloud Collector can be configured to collect additional 3rd party security devices or customer log sources. Please contact FireEye for the full list of compatible events and log data.

HARDWARE SPECIFICATIONS	
CLOUD COLLECTOR 100	
Performance	Up to 100 Mbps, [#] EPS
Network Interface Ports	5x 10/100/1000 BASTE T-Ports
Management Ports	1x 10/100/1000 BASTE T-Ports
IPMI Port	Included
PS/2 Keyboard & Mouse, DB15 VGA Ports	Included
USB Ports	2x type A USB Ports
Serial Port	115, 200 bps, No Parity, 8 Bits, 1 Stop bit
Drive Capacity	Dual 2TB HDD, Internal fixed
Enclosure	1RU, Fits 19 inch Rack
Chassis Dimension	16.8" x 14" x 1.7" (427 x 356 x 43mm)
AC Power Supply	Internal 200W, 100-240 VAC 3-1.5A, 50-60Hz IEC60320-C14
Appliance Weight lb. (kg)	11 lb. (5 kg)
Regulatory Compliance	RoHS, REACH, WEEE

HARDWARE SPECIFICATIONS	
CLOUD COLLECTOR 25	
Performance	25Mbps
Network Interface Ports	5x 10/100/1000BASE-T Ports
Management Ports	1x 10/100/1000BASE-T Ports
IPMI Port	Not included
PS/2 Keyboard & Mouse, DB15 VGA Ports	Not included
USB Ports	2x type A USB Ports
Serial Port	rj45 serial console (cable included)
Drive Capacity	Single 500 GB HDD, internal, fixed
Enclosure	11.02 x 6.9 x 1.73 inches
Chassis Dimension	11.02" x 6.9" x 1.73" (280 x 176 x 44mm)
AC Power Supply	Non-redundant, non-FRU, internal 60W, 100-240 VAC 1.5A, 50-60Hz
Appliance Weight lb. (kg)	3.1 lbs (1.4 kg)
Regulatory Compliance	RoHS, REACH, WEEE, Conflict Minerals

HARDWARE SPECIFICATIONS

CLOUD COLLECTOR 250

Performance	250Mbps
Network Interface Ports	5x 10/100/1000BASE-T Ports
Management Ports	1x 10/100/1000BASE-T Ports
IPMI Port	Not included
PS/2 Keyboard & Mouse, DB15 VGA Ports	Not included
USB Ports	2x type A USB Ports
Serial Port	rj45 serial console (cable included)
Drive Capacity	Single 3.5 " 1TB SATA drive, internal fixed
Enclosure	1 RU, Fits 19-inch rack
Chassis Dimension	17" x 19.7" x 1.7" (430 x 500 x 44mm)
AC Power Supply	Non-redundant, non-FRU, internal 250W, 100-240 VAC (+/-10%) 3.5 A, 47-63Hz
Appliance Weight lb. (kg)	16.2 lbs (7.3kg)
Regulatory Compliance	RoHS, REACH, WEEE Conflict minerals

HARDWARE SPECIFICATIONS

CLOUD COLLECTOR 2000

Performance	2Gbps
Network Interface Ports	8x 10/100/1000BASE-T Ports, 2x 10 Gbps, SFP +
Management Ports	2x 10/100/1000BASE-T Ports
IPMI Port	Included
PS/2 Keyboard & Mouse, DB15 VGA Ports	DB15 VFA, PS/2 Keyboard and mouse not included
USB Ports	4x type A USB Ports
Serial Port	DB9
Drive Capacity	48TB
Enclosure	2 RU, Fits 19-inch rack
Chassis Dimension	17.2" x 25.5" x 3.5" (43.7 x 64.8 x 8.9cm)
AC Power Supply	Redundant (1 + 1) 1280W, 100-240 VAC 8-6 A, 50/60 Hz Auto-ranging
Appliance Weight lb. (kg)	52 lbs (23.6 kg)
Regulatory Compliance	USA - UL listed Canada - CUL listed EN 60950/IEC 60950 CB Report CCC Certification

For more information on FireEye, visit:

www.FireEye.com

About FireEye, Inc.

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

www.FireEye.com

FireEye