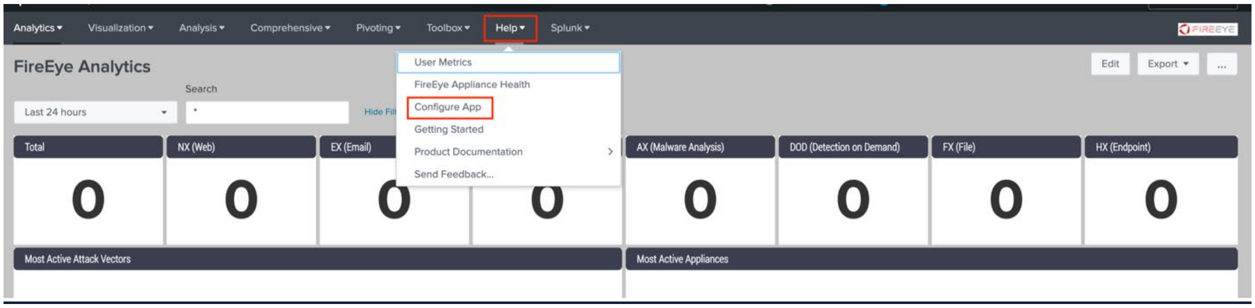
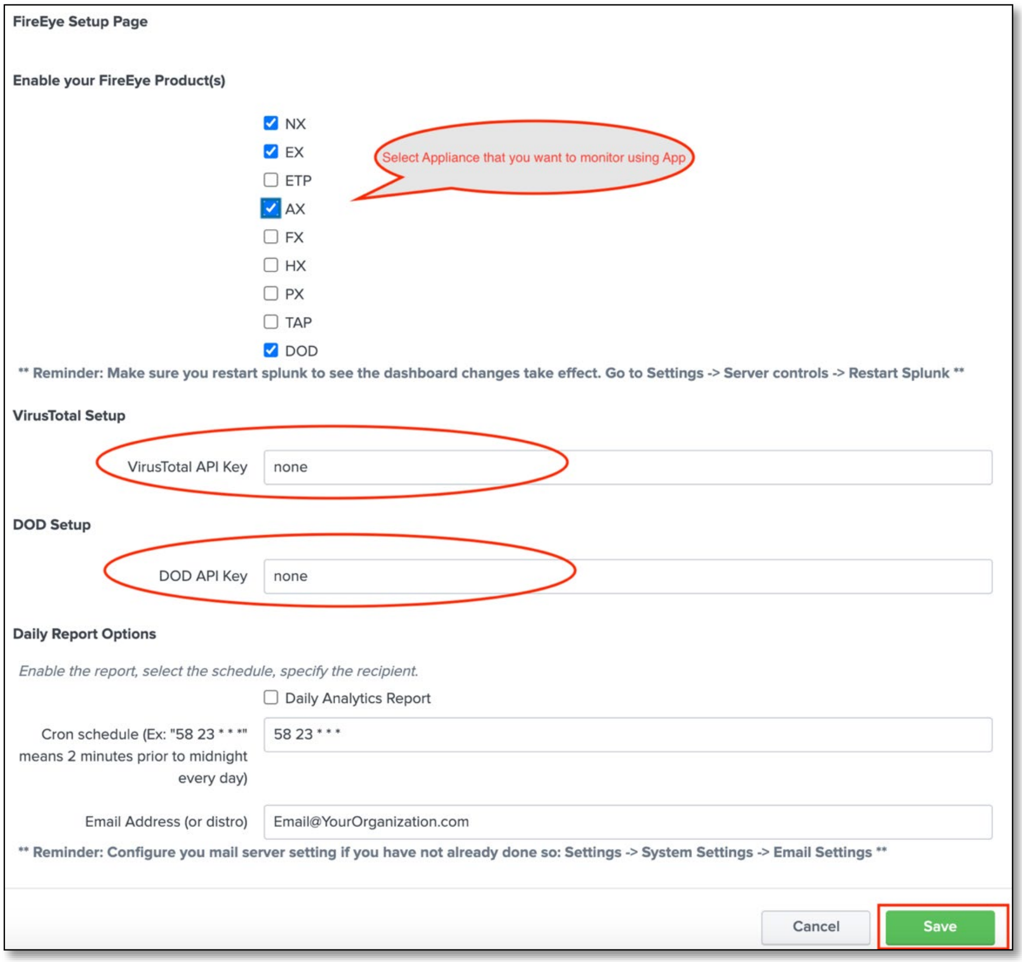
Configure Fireeye splunk app

Help → Configure App



Setup page –

Select All Appliances that you want to monitor.
Enter API key for DOD *(used for detailed dod report generation)*.
Enter API key for Virustotal *(used to get Virustotal analysis report for a particular Hash).*
Click Save.



FireEye Setup Page

Enable your FireEye Product(s)

☑ NX
☑ EX
☐ ETP
☑ AX
☐ FX
☐ HX
☐ PX
☐ TAP
☑ DOD

**** Reminder: Make sure you restart splunk to see the dashboard changes take effect. Go to Settings -> Server controls -> Restart Splunk ****

VirusTotal Setup

VirusTotal API Key: none

DOD Setup

DOD API Key: none

Daily Report Options

Enable the report, select the schedule, specify the recipient.

☐ Daily Analytics Report

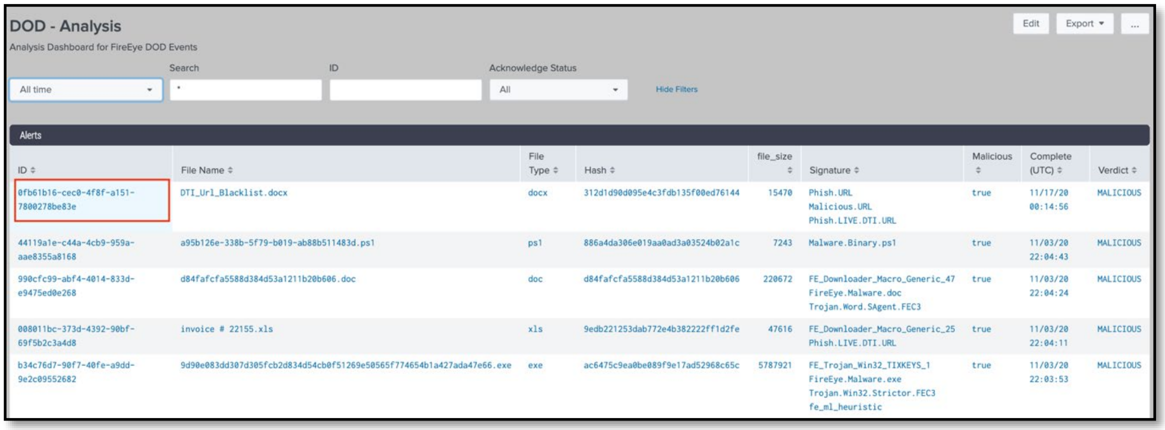
Cron schedule (Ex: "58 23 * * *" means 2 minutes prior to midnight every day): 58 23 * * *

Email Address (or distro): Email@YourOrganization.com

**** Reminder: Configure you mail server setting if you have not already done so: Settings -> System Settings -> Email Settings ****

Detailed Report DOD –

Click on report ID that you are interested in getting complete detail report for sample submission



DOD - Analysis

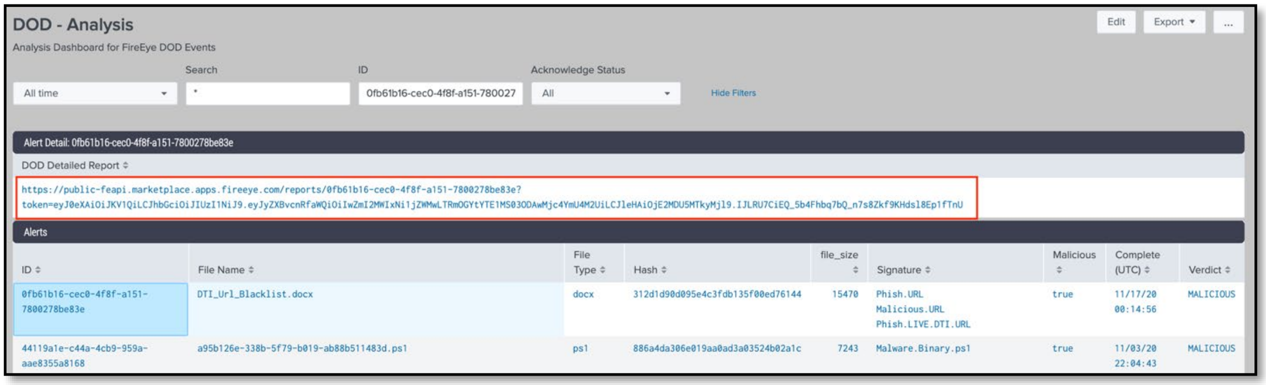
Analysis Dashboard for FireEye DOD Events

	Search	ID	Acknowledge Status
All time ▾	*		All ▾

Alerts

ID ⇕	File Name ⇕	File Type ⇕	Hash ⇕	file_size ⇕	Signature ⇕	Malicious ⇕	Complete (UTC) ⇕	Verdict ⇕
0fb61b16-cec0-4f8f-a151-7800278be83e	DTI_Url_Blacklist.docx	docx	312d1d90d095e4c3fdb135f00ed76144	15470	Phish.URL Malicious.URL Phish.LIVE.DTI.URL	true	11/17/20 00:14:56	MALICIOUS
44119a1e-c44a-4cb9-959a-aae8355a8168	a95b126e-338b-5f79-b019-ab88b511483d.ps1	ps1	886a4da306e019aa0ad3a03524b02a1c	7243	Malware.Binary.ps1	true	11/03/20 22:04:43	MALICIOUS
990cfc99-abf4-4014-833d-e9475ed0e268	d84fafcfa5588d384d53a1211b20b606.doc	doc	d84fafcfa5588d384d53a1211b20b606	220672	FE_Downloader_Macro_Generic_47 FireEye.Malware.doc Trojan.Word.SAgent.FEC3	true	11/03/20 22:04:24	MALICIOUS
008011bc-373d-4392-90bf-69f5b2c3a4d8	invoice # 22155.xls	xls	9edb221253dab772e4b382222ff1d2fe	47616	FE_Downloader_Macro_Generic_25 Phish.LIVE.DTI.URL	true	11/03/20 22:04:11	MALICIOUS
b34c76d7-90f7-40fe-a9dd-9e2c09552682	9d90e083dd307d305fcb2d834d54cb0f51269e50565f774654b1a427ada47e66.exe	exe	ac6475c9ea0be089f9e17ad52968c65c	5787921	FE_Trojan_Win32_TIXKEYS_1 FireEye.Malware.exe Trojan.Win32.Strictor.FEC3 fe_ml_heuristic	true	11/03/20 22:03:53	MALICIOUS

URL for detail report would be generated (DOD API Key used for report link generation)



DOD - Analysis

Analysis Dashboard for FireEye DOD Events

	Search	ID	Acknowledge Status
All time ▾	*	0fb61b16-cec0-4f8f-a151-780027	All ▾

Alert Detail: 0fb61b16-cec0-4f8f-a151-7800278be83e

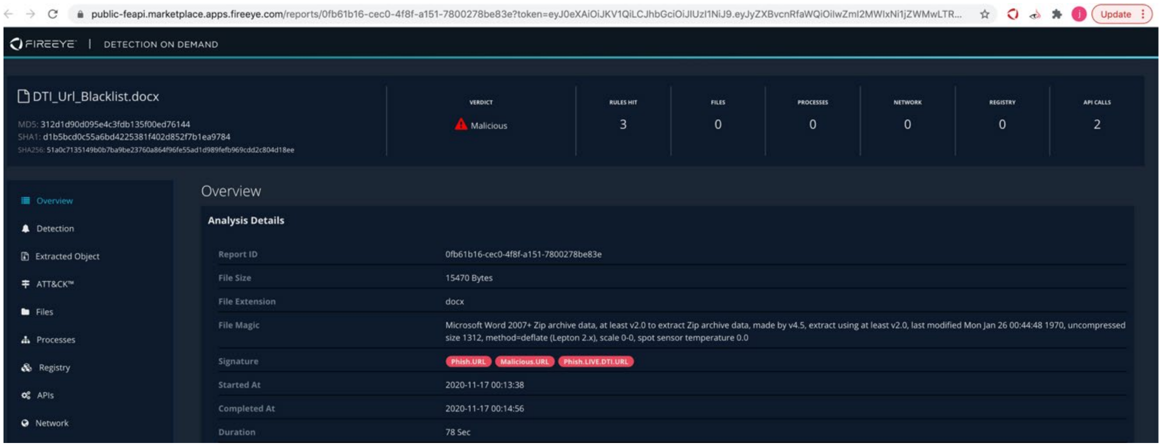
DOD Detailed Report ⇕

```
https://public-feapi.marketplace.apps.fireeye.com/reports/0fb61b16-cec0-4f8f-a151-7800278be83e?
token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJyZXBvcnRfaWQiOiIwZmI2MWIxNi1jZWMwLTRmOGYtYTE1MS03ODAwMjc4YmU4M2UiLCJleHAiOjE2MDU5MTkyMjl9.IJLRU7CiEQ_5b4Fhbq7bQ_n7s8Zkf9KHdsl8Ep1fTnU
```

Alerts

ID ⇕	File Name ⇕	File Type ⇕	Hash ⇕	file_size ⇕	Signature ⇕	Malicious ⇕	Complete (UTC) ⇕	Verdict ⇕
0fb61b16-cec0-4f8f-a151-7800278be83e	DTI_Url_Blacklist.docx	docx	312d1d90d095e4c3fdb135f00ed76144	15470	Phish.URL Malicious.URL Phish.LIVE.DTI.URL	true	11/17/20 00:14:56	MALICIOUS
44119a1e-c44a-4cb9-959a-aae8355a8168	a95b126e-338b-5f79-b019-ab88b511483d.ps1	ps1	886a4da306e019aa0ad3a03524b02a1c	7243	Malware.Binary.ps1	true	11/03/20 22:04:43	MALICIOUS

On clicking url generated detail report opens on new tab-



public-feapi.marketplace.apps.fireeye.com/reports/0fb61b16-cec0-4f8f-a151-7800278be83e?token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJyZXBvcnRfaWQiOiIwZmI2MWIxNi1jZWMwLTR...

DTI_Url_Blacklist.docx

MD5: 312d1d90d095e4c3fdb135f00ed76144
SHA1: d1b5bcd0c55a6bd4225381f402d852f7b1ea9784
SHA256: 51a0c7135149b0b7ba9be23760a864f96fe55ad1d989fefb969cdd2c804d18ee

VERDICT	RULES HIT	FILES	PROCESSES	NETWORK	REGISTRY	API CALLS
Malicious	3	0	0	0	0	2

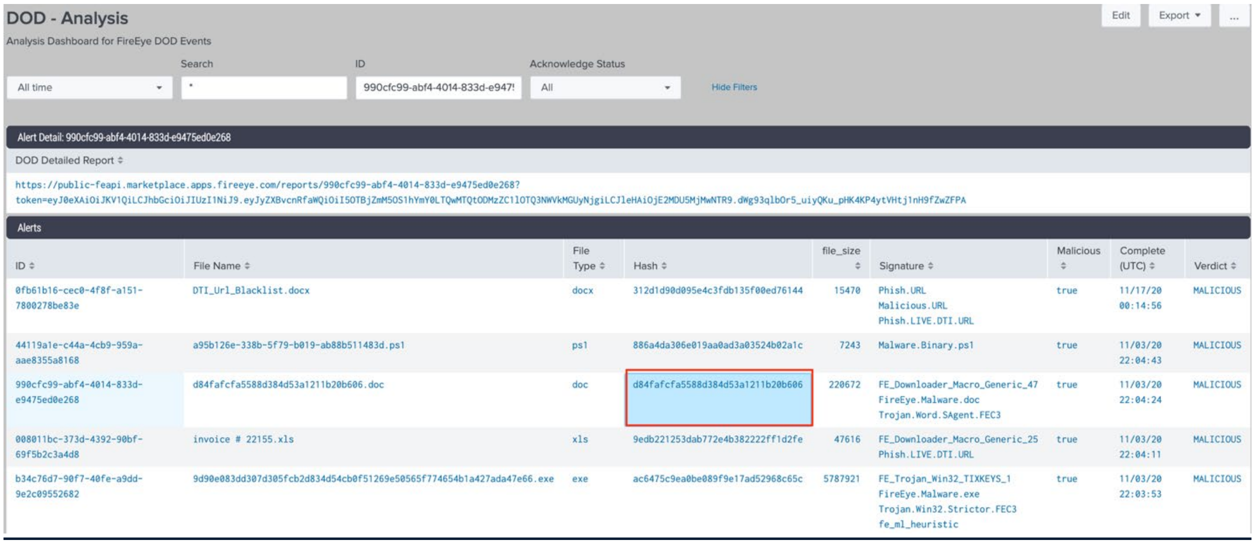
Overview

Analysis Details

Report ID	0fb61b16-cec0-4f8f-a151-7800278be83e
File Size	15470 Bytes
File Extension	docx
File Magic	Microsoft Word 2007+ Zip archive data, at least v2.0 to extract Zip archive data, made by v4.5, extract using at least v2.0, last modified Mon Jan 26 00:44:48 1970, uncompressed size 1312, method=deflate (Lepton 2.x), scale 0-0, spot sensor temperature 0.0
Signature	Phish.URL Malicious.URL Phish.LIVE.DTI.URL
Started At	2020-11-17 00:13:38
Completed At	2020-11-17 00:14:56
Duration	78 Sec

Virustotal Analysis for Hash-

Click on Hash that you are interested in getting complete Virustotal detail-



DOD - Analysis

Analysis Dashboard for FireEye DOD Events

	Search	ID	Acknowledge Status	
All time ▾	*	990cfc99-abf4-4014-833d-e947!	All ▾	Hide Filters

Alert Detail: 990cfc99-abf4-4014-833d-e9475ed0e268

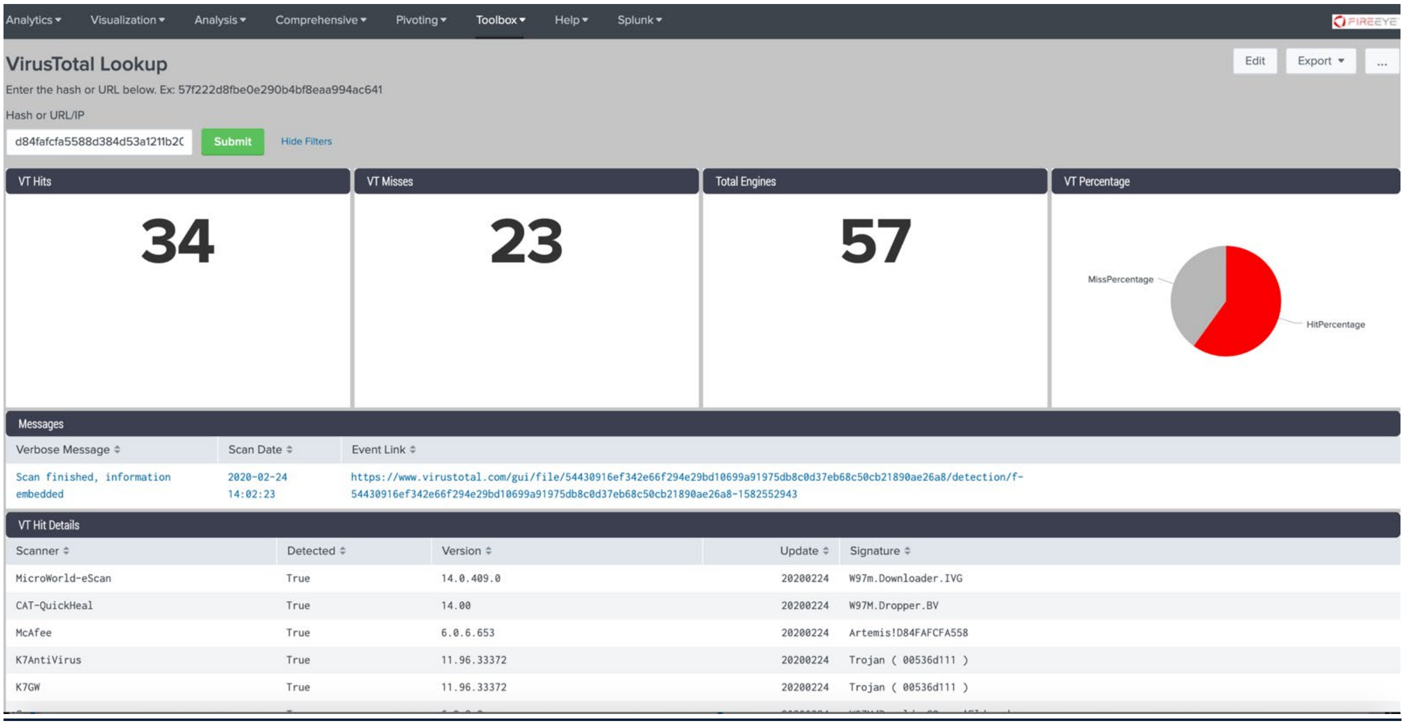
DOD Detailed Report ⇕

```
https://public-feapi.marketplace.apps.fireeye.com/reports/990cfc99-abf4-4014-833d-e9475ed0e268?
token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJyZXBvcnRfaWQiOiI5OTBjZmM5OS1hYmY0LTQwMTQtODMzZC1lOTQ3NWVkMGUyNjgiLCJleHAiOjE2MDU5MjMwNTR9.dWg93qlbOr5_uiyQKu_pHK4KP4ytVHtj1nH9fZwZFPA
```

Alerts

ID ⇕	File Name ⇕	File Type ⇕	Hash ⇕	file_size ⇕	Signature ⇕	Malicious ⇕	Complete (UTC) ⇕	Verdict ⇕
0fb61b16-cec0-4f8f-a151-7800278be83e	DTI_Url_Blacklist.docx	docx	312d1d90d095e4c3fdb135f00ed76144	15470	Phish.URL Malicious.URL Phish.LIVE.DTI.URL	true	11/17/20 00:14:56	MALICIOUS
44119a1e-c44a-4cb9-959a-aae8355a8168	a95b126e-338b-5f79-b019-ab88b511483d.ps1	ps1	886a4da306e019aa0ad3a03524b02a1c	7243	Malware.Binary.ps1	true	11/03/20 22:04:43	MALICIOUS
990cfc99-abf4-4014-833d-e9475ed0e268	d84fafcfa5588d384d53a1211b20b606.doc	doc	d84fafcfa5588d384d53a1211b20b606	220672	FE_Downloader_Macro_Generic_47 FireEye.Malware.doc Trojan.Word.SAgent.FEC3	true	11/03/20 22:04:24	MALICIOUS
008011bc-373d-4392-90bf-69f5b2c3a4d8	invoice # 22155.xls	xls	9edb221253dab772e4b382222ff1d2fe	47616	FE_Downloader_Macro_Generic_25 Phish.LIVE.DTI.URL	true	11/03/20 22:04:11	MALICIOUS
b34c76d7-90f7-40fe-a9dd-9e2c09552682	9d90e083dd307d305fcb2d834d54cb0f51269e50565f774654b1a427ada47e66.exe	exe	ac6475c9ea0be089f9e17ad52968c65c	5787921	FE_Trojan_Win32_TIXKEYS_1 FireEye.Malware.exe Trojan.Win32.Strictor.FEC3 fe_ml_heuristic	true	11/03/20 22:03:53	MALICIOUS

On clicking Hash, Virustotal analysis report opens on new tab-



VirusTotal Lookup

Enter the hash or URL below. Ex: 57f222d8fbe0e290b4bf8eaa994ac641

Hash or URL/IP

d84fafcfa5588d384d53a1211b2(

VT Hits	VT Misses	Total Engines	VT Percentage
34	23	57	

Messages

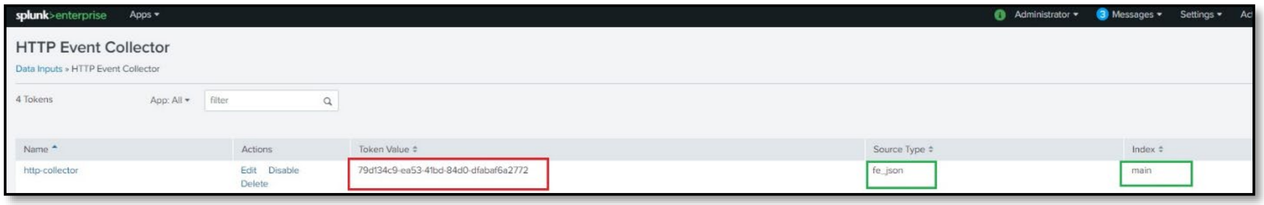
Verbose Message ⇕	Scan Date ⇕	Event Link ⇕
Scan finished, information embedded	2020-02-24 14:02:23	https://www.virustotal.com/gui/file/54430916ef342e66f294e29bd10699a91975db8c0d37eb68c50cb21890ae26a8/detection/f-54430916ef342e66f294e29bd10699a91975db8c0d37eb68c50cb21890ae26a8-1582552943

VT Hit Details

Scanner ⇕	Detected ⇕	Version ⇕	Update ⇕	Signature ⇕
MicroWorld-eScan	True	14.0.409.0	20200224	W97m.Downloader.IVG
CAT-QuickHeal	True	14.00	20200224	W97M.Dropper.BV
McAfee	True	6.0.6.653	20200224	Artemis!D84FAFCFA558
K7AntiVirus	True	11.96.33372	20200224	Trojan (00536d111)
K7GW	True	11.96.33372	20200224	Trojan (00536d111)

Data Input to Splunk

Settings → Data Inputs → HTTP Event Collector



HTTP Event Collector

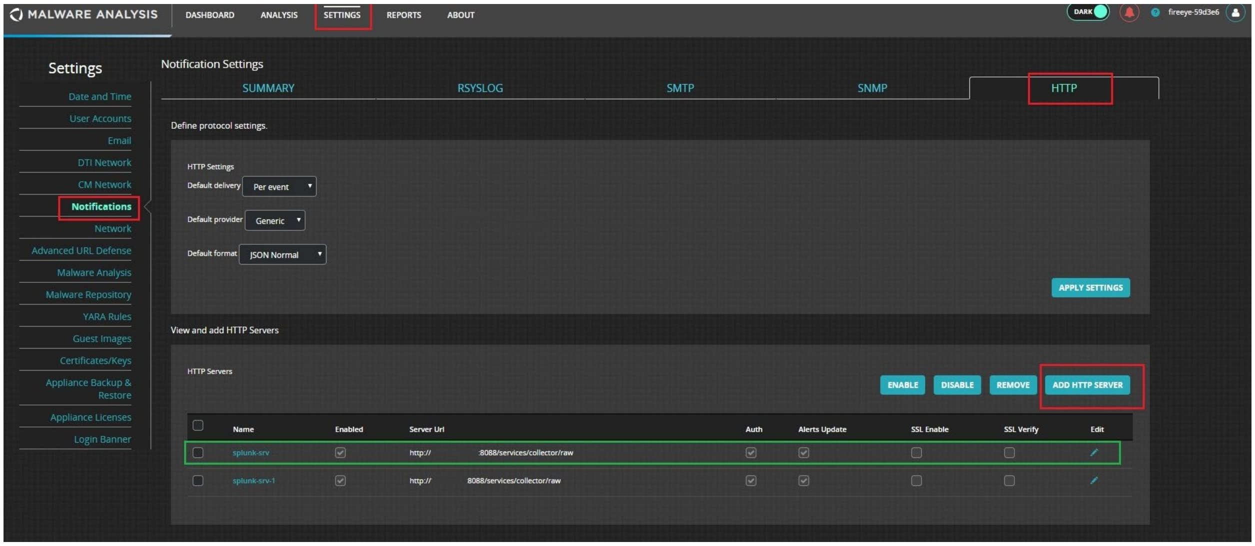
Data Inputs » HTTP Event Collector

4 Tokens   App: All ▾   filter

Name ▲	Actions	Token Value ⇕	Source Type ⇕	Index ⇕
http-collector	Edit Disable Delete	79d134c9-ea53-41bd-84d0-dfabaf6a2772	fe_json	main

Configuring Fireeye Appliances to forward Alerts to splunk server □

1. Go To “Settings” on top of page
2. Select “Notifications”
3. Select “HTTP”
4. Click “ADD HTTP SERVER”



Notification Settings

Define protocol settings.

HTTP Settings

Default delivery: Per event

Default provider: Generic

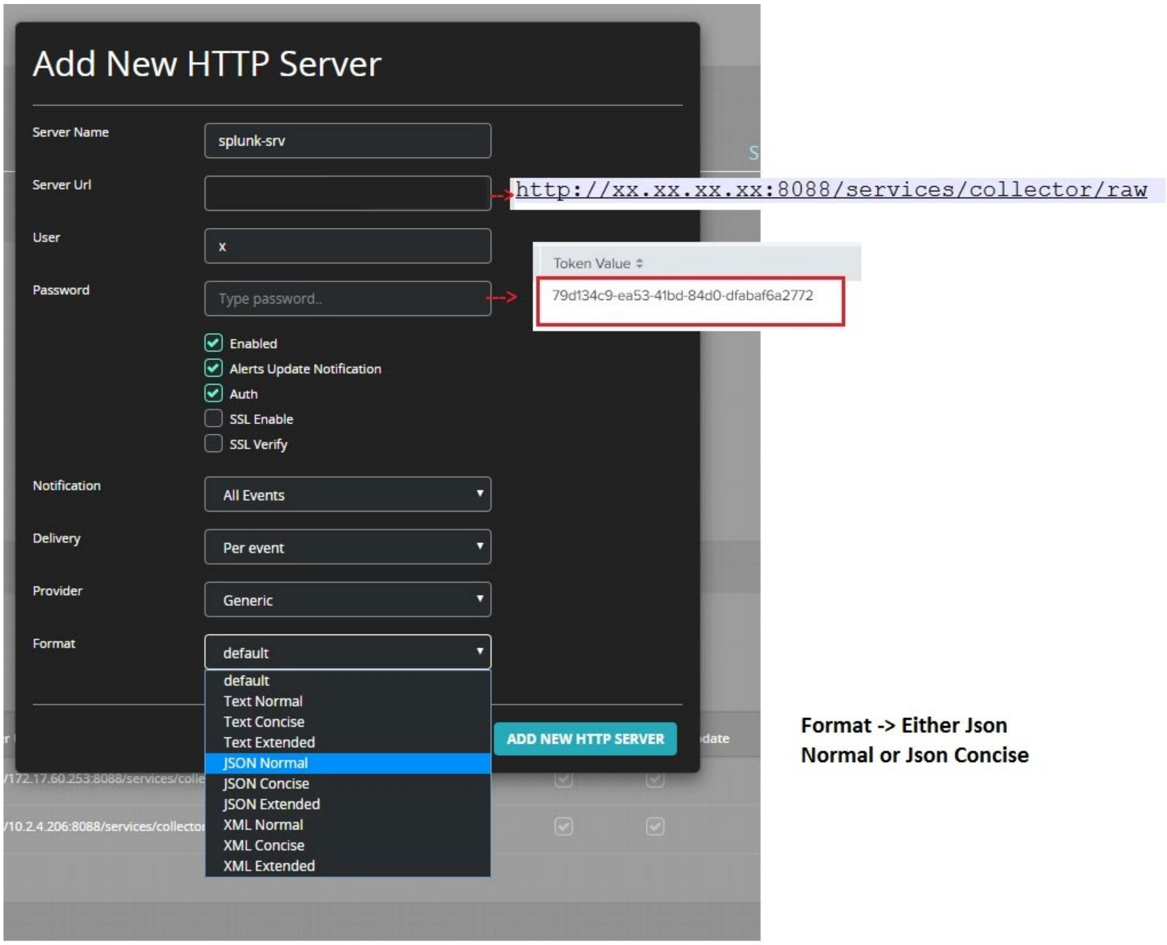
Default format: JSON Normal

View and add HTTP Servers

HTTP Servers

□	Name	Enabled	Server Url	Auth	Alerts Update	SSL Enable	SSL Verify	Edit
□	splunk-srv	☑	http:// :8088/services/collector/raw	☑	☑	□	□	✎
□	splunk-srv-1	☑	http:// 8088/services/collector/raw	☑	☑	□	□	✎

1. Enter a name for server under – “Server Name”
2. Server Url → http://<splunk_server_ip>:8088/services/collector/raw
3. User → “x”
4. Password → Token Value from HTTP Event Collector on Splunk server.
5. Select “Enabled”, “Alerts Update Notification”, ”Auth”
6. Notifications → “All Events”
7. Delivery → “Per Event”
8. Provider → “Generic”
9. Format → “Json Normal” or “Json Concise”



Add New HTTP Server

Server Name: splunk-srv

Server Url: http://xx.xx.xx.xx:8088/services/collector/raw

User: x

Password: Type password..

Token Value: 79d134c9-ea53-41bd-84d0-dfabaf6a2772

☑ Enabled
☑ Alerts Update Notification
☑ Auth
☐ SSL Enable
☐ SSL Verify

Notification: All Events

Delivery: Per event

Provider: Generic

Format: default

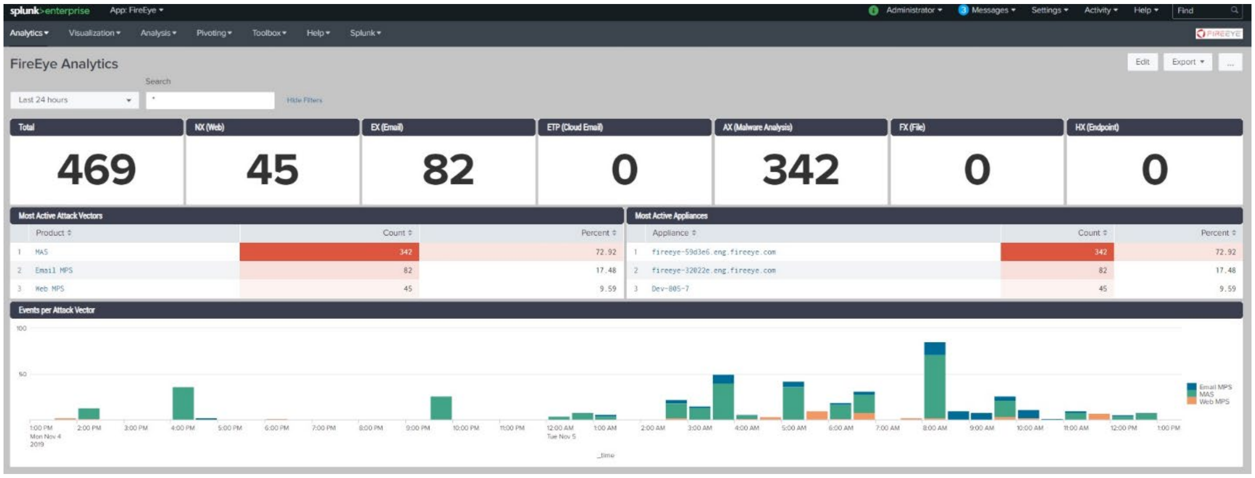
/172.17.60.253:8088/services/colle

/10.2.4.206:8088/services/collector

Format -> Either Json Normal or Json Concise

<u>Landing Page on Fireeye App –</u>

Sample of how landing page of Fireeye app for splunk looks like.



FireEye Analytics

Last 24 hours

Search: *

Total	NX (Web)	EX (Email)	ETP (Cloud Email)	AX (Malware Analysis)	FX (File)	HX (Endpoint)
469	45	82	0	342	0	0

Most Active Attack Vectors

	Product	Count	Percent
1	MAS	342	72.92
2	Email MPS	82	17.48
3	Web MPS	45	9.59

Most Active Appliances

	Appliance	Count	Percent
1	fireeye-59d3e6.eng.fireeye.com	342	72.92
2	fireeye-32022e.eng.fireeye.com	82	17.48
3	Dev-805-7	45	9.59

Events per Attack Vector