Elastic SIEM Workshop

Lab 5 - Interacting with the SIEM app

Introduction

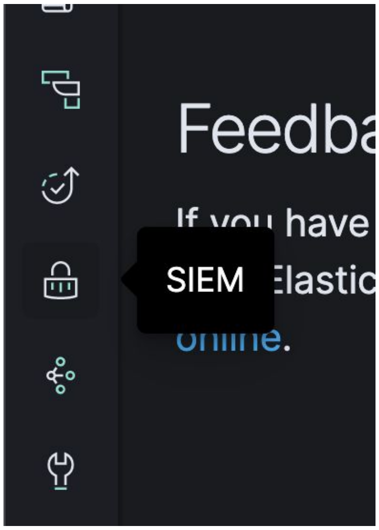
In this lab guide we will walk you through the SIEM ui and all its components.

Now that we have data flowing into our stack, we can walk through the different parts of the SIEM ui, which is made up of the following components:

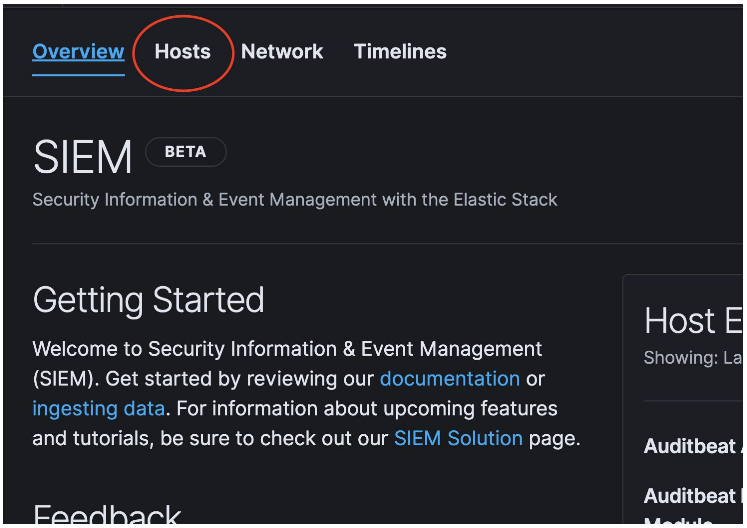
- Overview - This is a break down of events received by the SIEM app. It is split into the respective beats modules
- Hosts - This page shows information about all the reporting hosts. This includes some KPIs to get you started, an authentications table, an Uncommon Processes table, and an events table.
- Network - This view shows all related network activity, similar to the hosts view, it includes some KPIs to get started and some tables related to potential network anomalies such as top talkers and dns queries being made.

The Hosts View

Let’s start trying out the hosts view. If you haven’t already, click on the “SIEM” app in kibana.



Click on “Hosts” at the top of the screen:



SIEM BETA

Security Information & Event Management with the Elastic Stack

Getting Started

Welcome to Security Information & Event Management (SIEM). Get started by reviewing our documentation or ingesting data. For information about upcoming features and tutorials, be sure to check out our SIEM Solution page.

Feedback

Host E

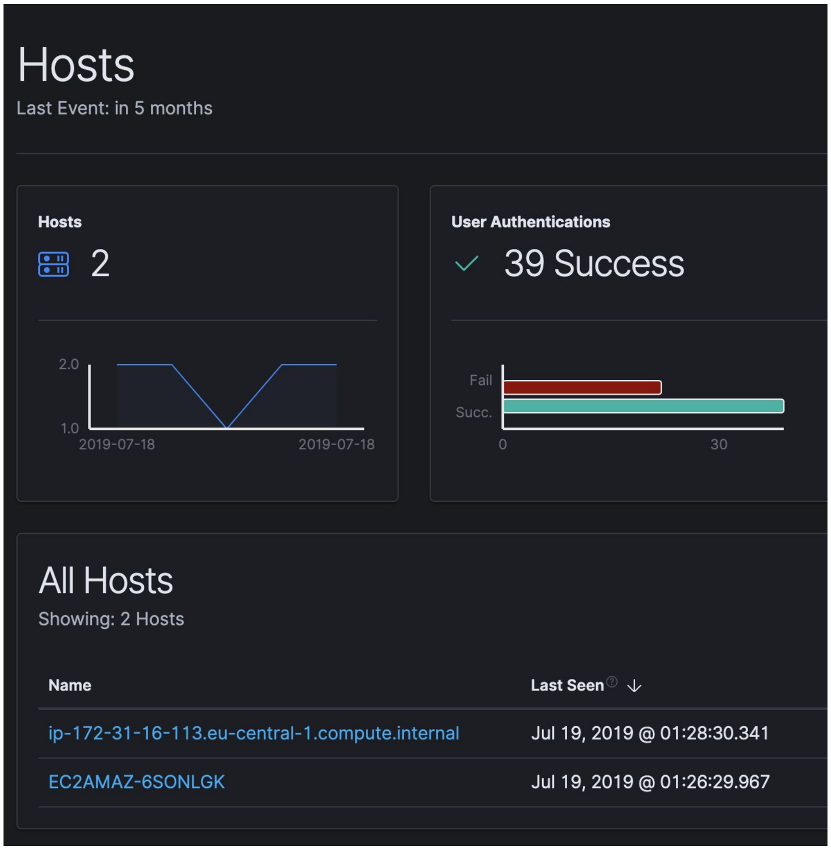
Showing: La

Auditbeat

Auditbeat

Module

You should now be able to see the populated hosts view with the two VM’s in your lab. The host names should be similar as seen below.



Hosts

Last Event: in 5 months

Hosts 2

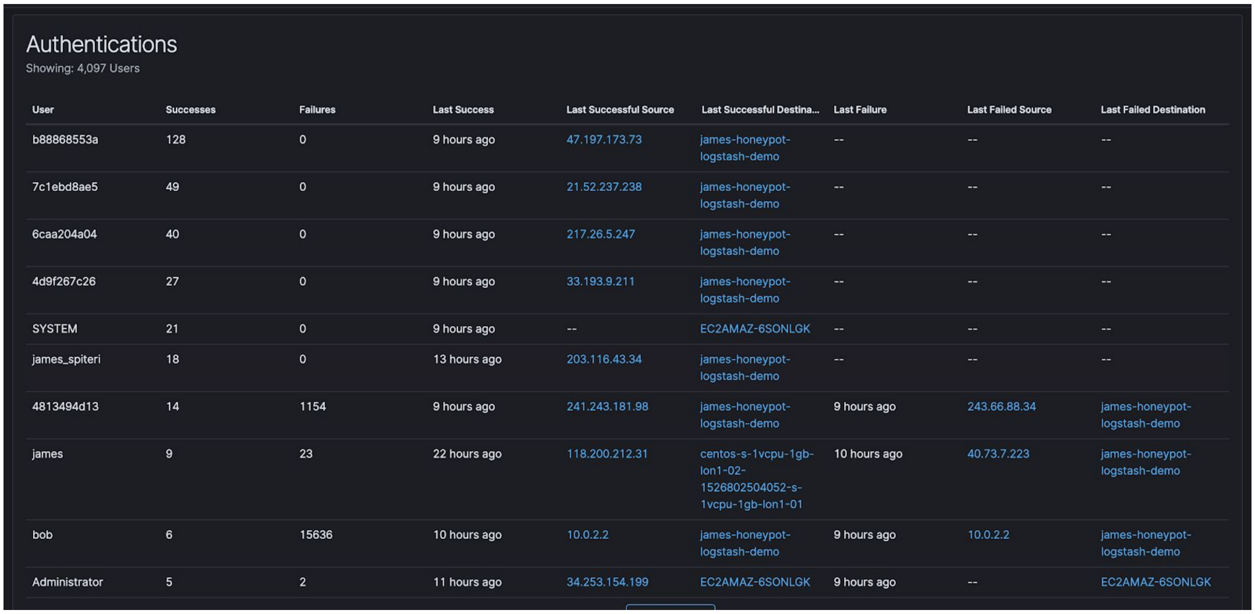
User Authentications ✓ 39 Success

All Hosts

Showing: 2 Hosts

Name	Last Seen ↓
ip-172-31-16-113.eu-central-1.compute.internal	Jul 19, 2019 @ 01:28:30.341
EC2AMAZ-6SONLGK	Jul 19, 2019 @ 01:26:29.967

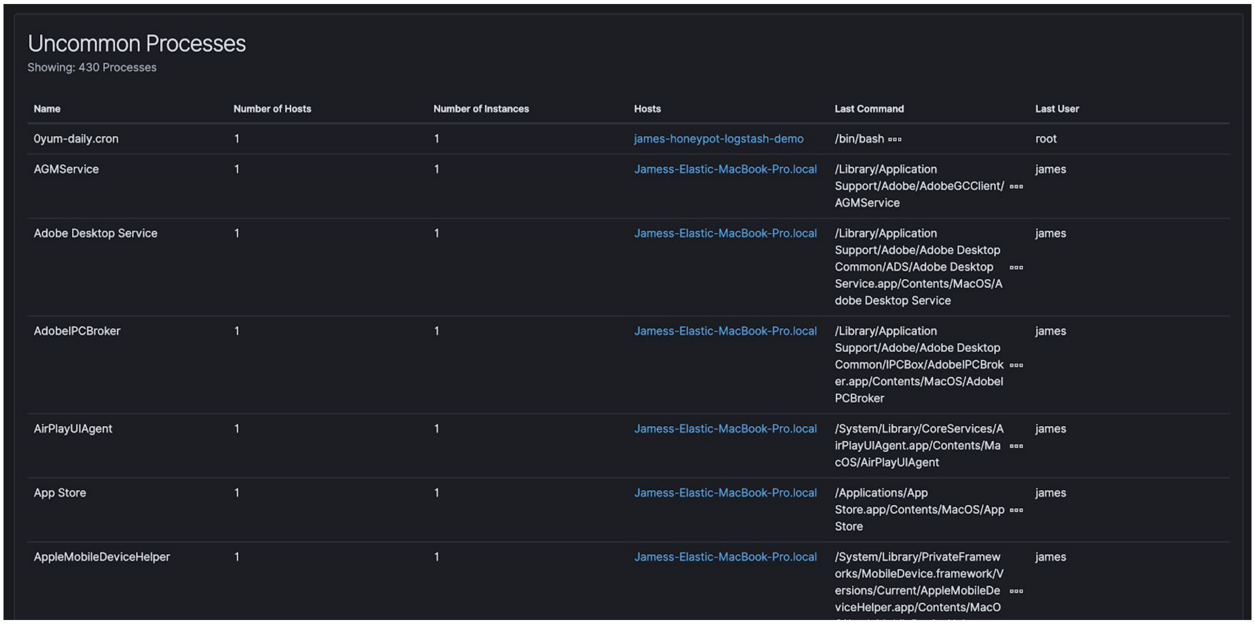
Further down, you will notice the authentication, uncommon process and events tables:



Authentications

Showing: 4,097 Users

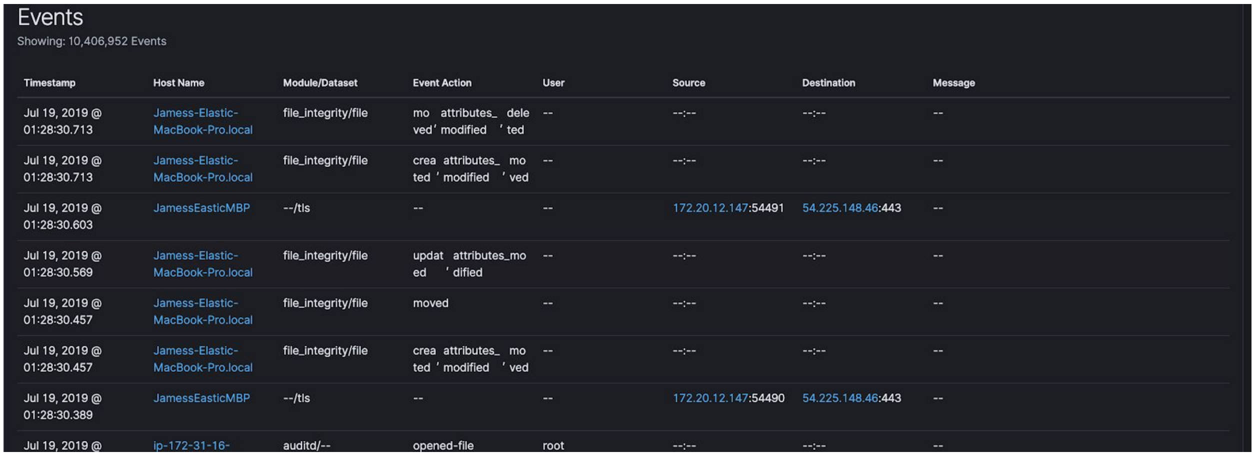
User	Successes	Failures	Last Success	Last Successful Source	Last Successful Destina...	Last Failure	Last Failed Source	Last Failed Destination
b88868553a	128	0	9 hours ago	47.197.173.73	james-honeypot-logstash-demo	--	--	--
7c1ebd8ae5	49	0	9 hours ago	21.52.237.238	james-honeypot-logstash-demo	--	--	--
6caa204a04	40	0	9 hours ago	217.26.5.247	james-honeypot-logstash-demo	--	--	--
4d9f267c26	27	0	9 hours ago	33.193.9.211	james-honeypot-logstash-demo	--	--	--
SYSTEM	21	0	9 hours ago	--	EC2AMAZ-6SONLGK	--	--	--
james_spiteri	18	0	13 hours ago	203.116.43.34	james-honeypot-logstash-demo	--	--	--
4813494d13	14	1154	9 hours ago	241.243.181.98	james-honeypot-logstash-demo	9 hours ago	243.66.88.34	james-honeypot-logstash-demo
james	9	23	22 hours ago	118.200.212.31	centos-s-1vcpu-1gb-lon1-02-1526802504052-s-1vcpu-1gb-lon1-01	10 hours ago	40.73.7.223	james-honeypot-logstash-demo
bob	6	15636	10 hours ago	10.0.2.2	james-honeypot-logstash-demo	9 hours ago	10.0.2.2	james-honeypot-logstash-demo
Administrator	5	2	11 hours ago	34.253.154.199	EC2AMAZ-6SONLGK	9 hours ago	--	EC2AMAZ-6SONLGK



Uncommon Processes

Showing: 430 Processes

Name	Number of Hosts	Number of Instances	Hosts	Last Command	Last User
0yum-daily.cron	1	1	james-honeypot-logstash-demo	/bin/bash	root
AGMService	1	1	Jamess-Elastic-MacBook-Pro.local	/Library/Application Support/Adobe/AdobeGCClient/AGMService	james
Adobe Desktop Service	1	1	Jamess-Elastic-MacBook-Pro.local	/Library/Application Support/Adobe/Adobe Desktop Common/ADS/Adobe Desktop Service.app/Contents/MacOS/Adobe Desktop Service	james
AdobeIPCBroker	1	1	Jamess-Elastic-MacBook-Pro.local	/Library/Application Support/Adobe/Adobe Desktop Common/IPCBox/AdobeIPCBroker.app/Contents/MacOS/AdobeIPCBroker	james
AirPlayUIAgent	1	1	Jamess-Elastic-MacBook-Pro.local	/System/Library/CoreServices/AirPlayUIAgent.app/Contents/MacOS/AirPlayUIAgent	james
App Store	1	1	Jamess-Elastic-MacBook-Pro.local	/Applications/App Store.app/Contents/MacOS/App Store	james
AppleMobileDeviceHelper	1	1	Jamess-Elastic-MacBook-Pro.local	/System/Library/PrivateFrameworks/MobileDevice.framework/Versions/Current/AppleMobileDeviceHelper.app/Contents/MacO	james

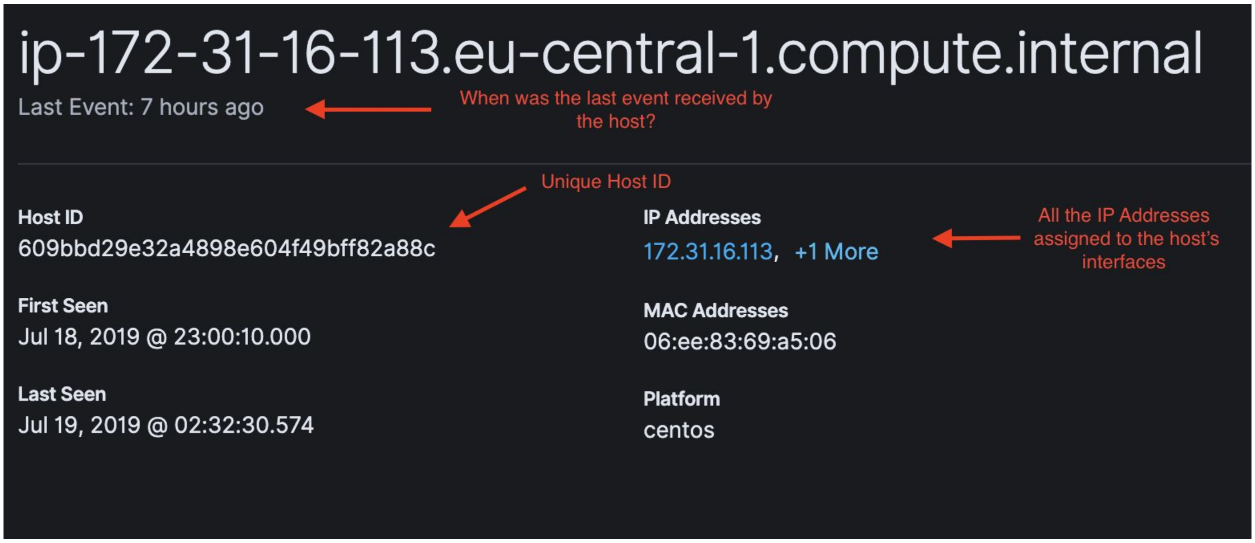


Events

Showing: 10,406,952 Events

Timestamp	Host Name	Module/Dataset	Event Action	User	Source	Destination	Message
Jul 19, 2019 @ 01:28:30.713	Jamess-Elastic-MacBook-Pro.local	file_integrity/file	moved attributes_modified deleted	--	--:--	--:--	--
Jul 19, 2019 @ 01:28:30.713	Jamess-Elastic-MacBook-Pro.local	file_integrity/file	created attributes_modified moved	--	--:--	--:--	--
Jul 19, 2019 @ 01:28:30.603	JamessEasticMBP	--/tls	--	--	172.20.12.147:54491	54.225.148.46:443	--
Jul 19, 2019 @ 01:28:30.569	Jamess-Elastic-MacBook-Pro.local	file_integrity/file	updated attributes_modified	--	--:--	--:--	--
Jul 19, 2019 @ 01:28:30.457	Jamess-Elastic-MacBook-Pro.local	file_integrity/file	moved	--	--:--	--:--	--
Jul 19, 2019 @ 01:28:30.457	Jamess-Elastic-MacBook-Pro.local	file_integrity/file	created attributes_modified moved	--	--:--	--:--	--
Jul 19, 2019 @ 01:28:30.389	JamessEasticMBP	--/tls	--	--	172.20.12.147:54490	54.225.148.46:443	--
Jul 19, 2019 @	ip-172-31-16-	auditd/--	opened-file	root	--:--	--:--	--

Let’s look at all the host info we get from our beats configuration. Click on any of the two hosts from the hosts table to drill down.



ip-172-31-16-113.eu-central-1.compute.internal

Last Event: 7 hours ago

When was the last event received by the host?

Unique Host ID

Host ID
609bbd29e32a4898e604f49bff82a88c

IP Addresses
172.31.16.113, +1 More

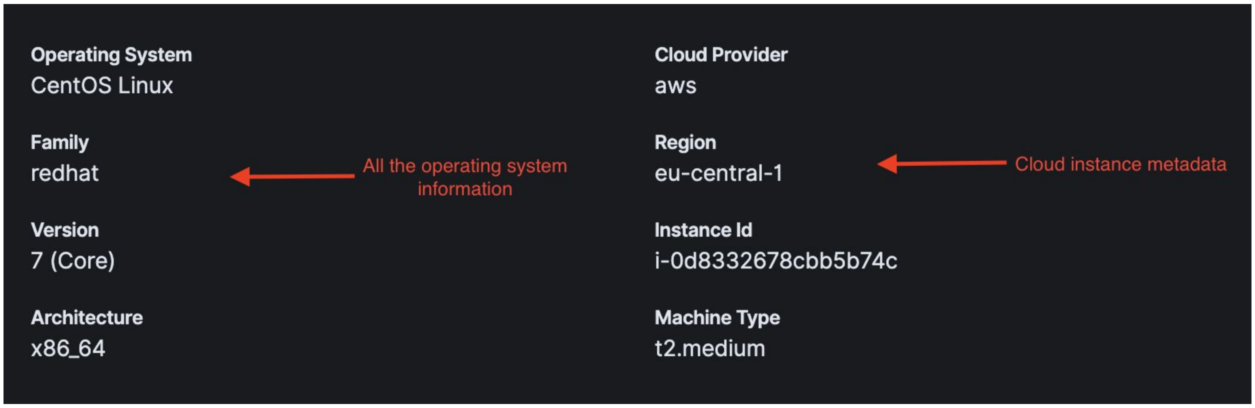
All the IP Addresses assigned to the host's interfaces

First Seen
Jul 18, 2019 @ 23:00:10.000

MAC Addresses
06:ee:83:69:a5:06

Last Seen
Jul 19, 2019 @ 02:32:30.574

Platform
centos



Operating System
CentOS Linux

Family
redhat

Version
7 (Core)

Architecture
x86_64

All the operating system information

Cloud Provider
aws

Region
eu-central-1

Instance Id
i-0d8332678cbb5b74c

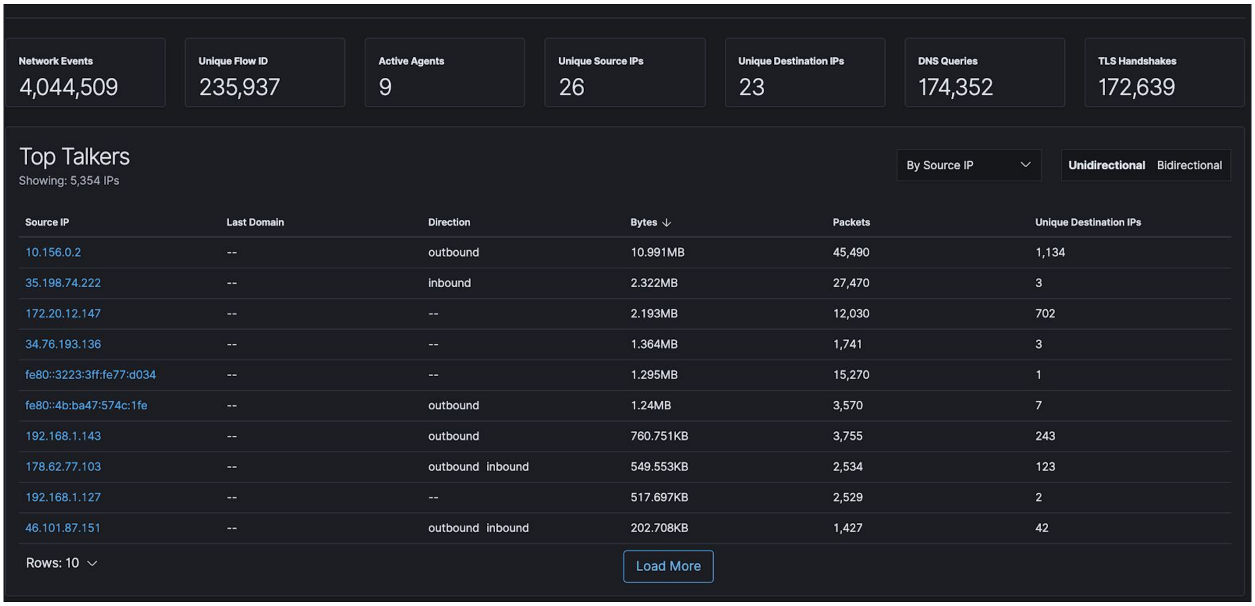
Machine Type
t2.medium

Cloud instance metadata

You will notice that the authentications and events table have switched context to this host.

The Network view

Let’s see the information we get in the network view. Switch from the hosts view to the network view.



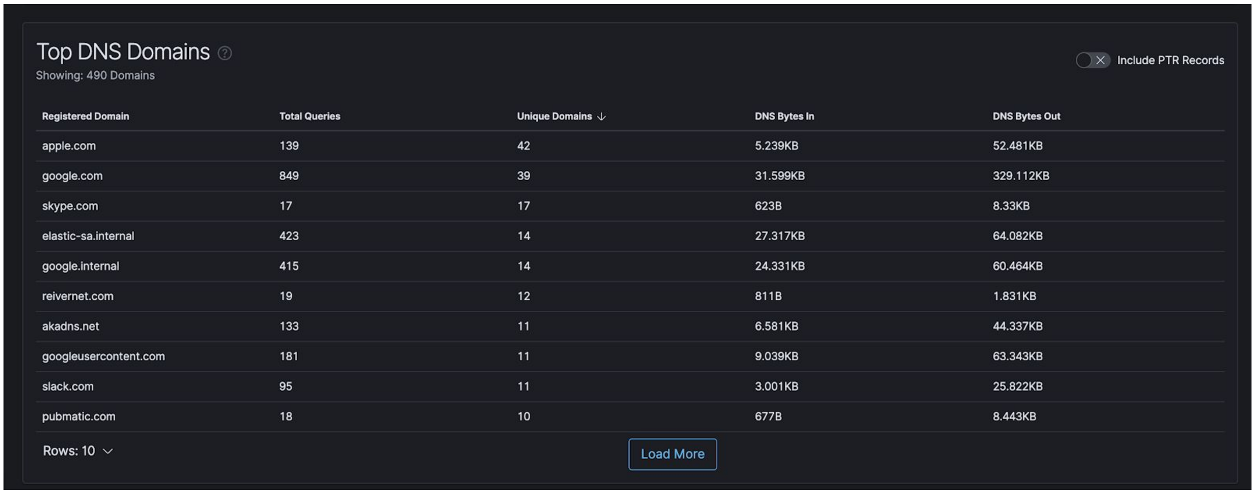
Network Events	Unique Flow ID	Active Agents	Unique Source IPs	Unique Destination IPs	DNS Queries	TLS Handshakes
4,044,509	235,937	9	26	23	174,352	172,639

Top Talkers

Showing: 5,354 IPs

Source IP	Last Domain	Direction	Bytes ↓	Packets	Unique Destination IPs
10.156.0.2	--	outbound	10.991MB	45,490	1,134
35.198.74.222	--	inbound	2.322MB	27,470	3
172.20.12.147	--	--	2.193MB	12,030	702
34.76.193.136	--	--	1.364MB	1,741	3
fe80::3223:3ff:fe77:d034	--	--	1.295MB	15,270	1
fe80::4b:ba47:574c:1fe	--	outbound	1.24MB	3,570	7
192.168.1.143	--	outbound	760.751KB	3,755	243
178.62.77.103	--	outbound inbound	549.553KB	2,534	123
192.168.1.127	--	--	517.697KB	2,529	2
46.101.87.151	--	outbound inbound	202.708KB	1,427	42

You can see that we are again presented with KPIs, this time related to network activity. We also have a table highlighting the “top talkers” (the IP addresses with the highest number of packets and bytes). Additionally, there is a list of the top domains being queries by DNS:

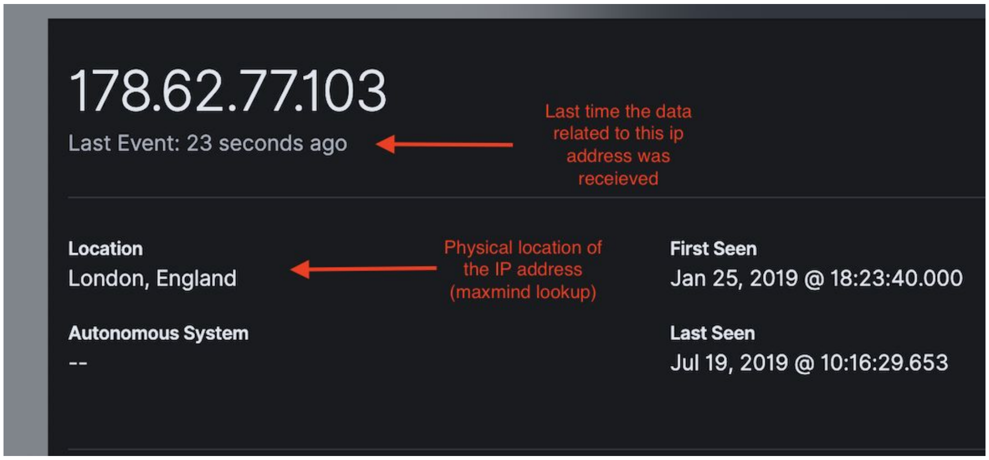


Top DNS Domains

Showing: 490 Domains

Registered Domain	Total Queries	Unique Domains ↓	DNS Bytes In	DNS Bytes Out
apple.com	139	42	5.239KB	52.481KB
google.com	849	39	31.599KB	329.112KB
skype.com	17	17	623B	8.33KB
elastic-sa.internal	423	14	27.317KB	64.082KB
google.internal	415	14	24.331KB	60.464KB
reivernet.com	19	12	811B	1.831KB
akadns.net	133	11	6.581KB	44.337KB
googleusercontent.com	181	11	9.039KB	63.343KB
slack.com	95	11	3.001KB	25.822KB
pubmatic.com	18	10	677B	8.443KB

We can pick any IP address from the list of top talkers (or anywhere within the SIEM app) to drill down and get more information related to it. Go ahead and click on any IP address you like:



178.62.77.103

Last Event: 23 seconds ago

Last time the data related to this ip address was receieved

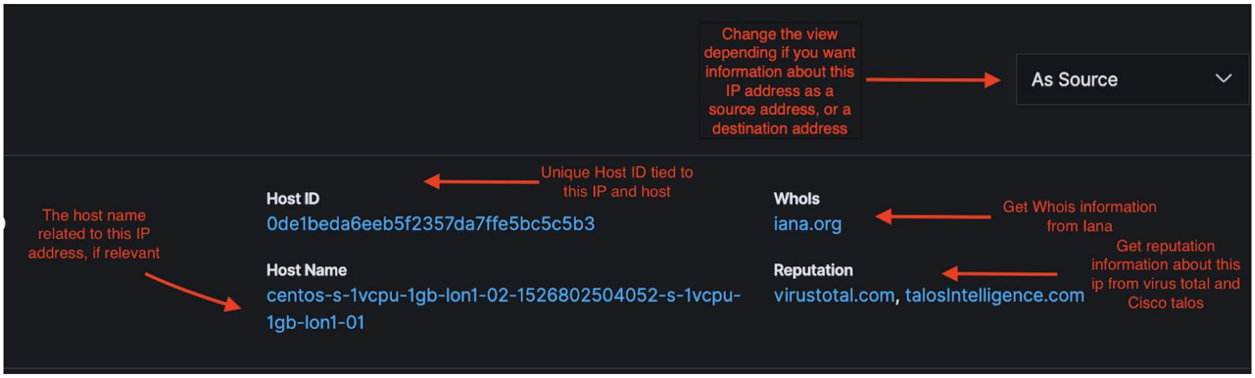
Location
London, England

Physical location of the IP address (maxmind lookup)

First Seen
Jan 25, 2019 @ 18:23:40.000

Autonomous System
--

Last Seen
Jul 19, 2019 @ 10:16:29.653



Change the view depending if you want information about this IP address as a source address, or a destination address

As Source

Unique Host ID tied to this IP and host

The host name related to this IP address, if relevant

Host ID
0de1beda6eeb5f2357da7ffe5bc5c5b3

Host Name
centos-s-1vcpu-1gb-lon1-02-1526802504052-s-1vcpu-1gb-lon1-01

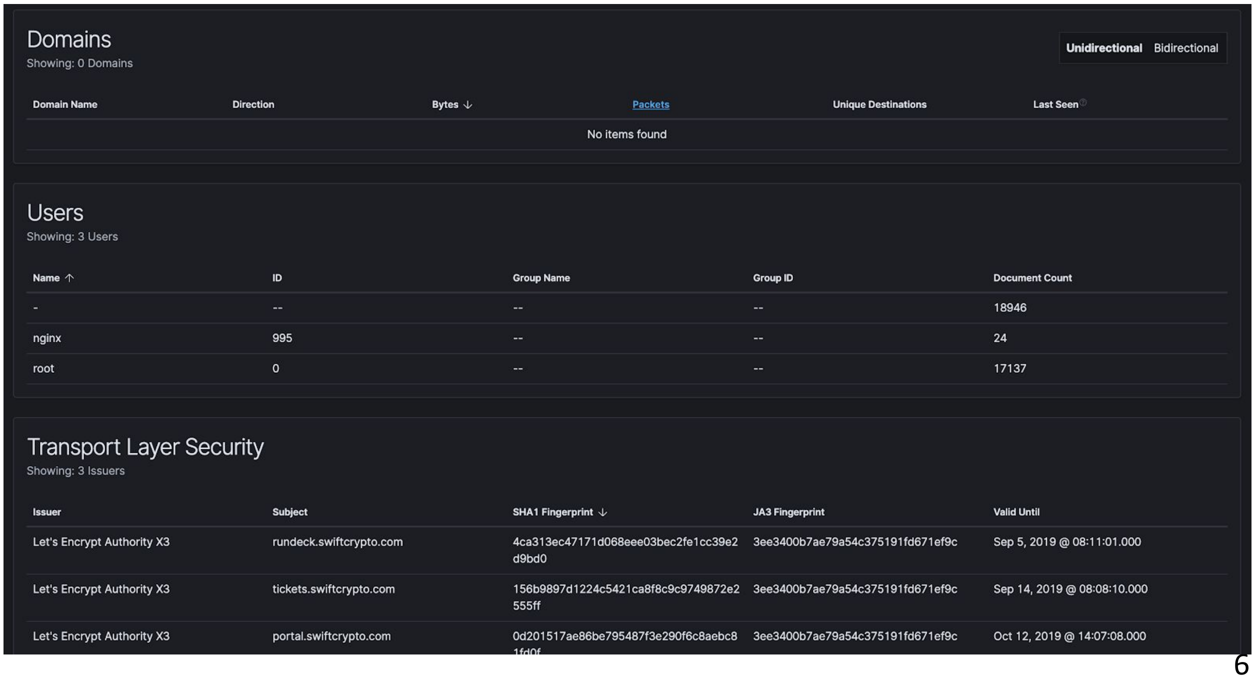
WhoIs
iana.org

Get Whois information from Iana

Reputation
virustotal.com, talosIntelligence.com

Get reputation information about this ip from virus total and Cisco talos

You will also notice some new tables when you drill down into an IP address:



Domains

Showing: 0 Domains

Unidirectional Bidirectional

Domain Name	Direction	Bytes ↓	Packets	Unique Destinations	Last Seen
No items found					

Users

Showing: 3 Users

Name ↑	ID	Group Name	Group ID	Document Count
-	--	--	--	18946
nginx	995	--	--	24
root	0	--	--	17137

Transport Layer Security

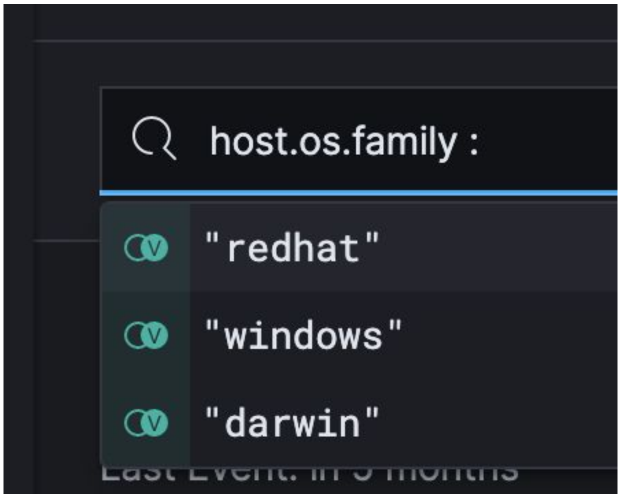
Showing: 3 Issuers

Issuer	Subject	SHA1 Fingerprint ↓	JA3 Fingerprint	Valid Until
Let's Encrypt Authority X3	rundeck.swiftcrypto.com	4ca313ec47171d068eee03bec2fe1cc39e2d9bd0	3ee3400b7ae79a54c375191fd671ef9c	Sep 5, 2019 @ 08:11:01.000
Let's Encrypt Authority X3	tickets.swiftcrypto.com	156b9897d1224c5421ca8f8c9c9749872e2555ff	3ee3400b7ae79a54c375191fd671ef9c	Sep 14, 2019 @ 08:08:10.000
Let's Encrypt Authority X3	portal.swiftcrypto.com	0d201517ae86be795487f3e290f6c8aebc81fd0f	3ee3400b7ae79a54c375191fd671ef9c	Oct 12, 2019 @ 14:07:08.000

These tables show:

- Any domains related to the IP address
- Users running processes making request to/from this IP address
- Encrypted TLS connections being made to/from this IP address

Feel free to play around in both the hosts view and the network view. You might have noticed that we have a filter bar and a time picker at the top of every page. Feel free to also experiment with any filtering. Autocomplete will help you build a query.

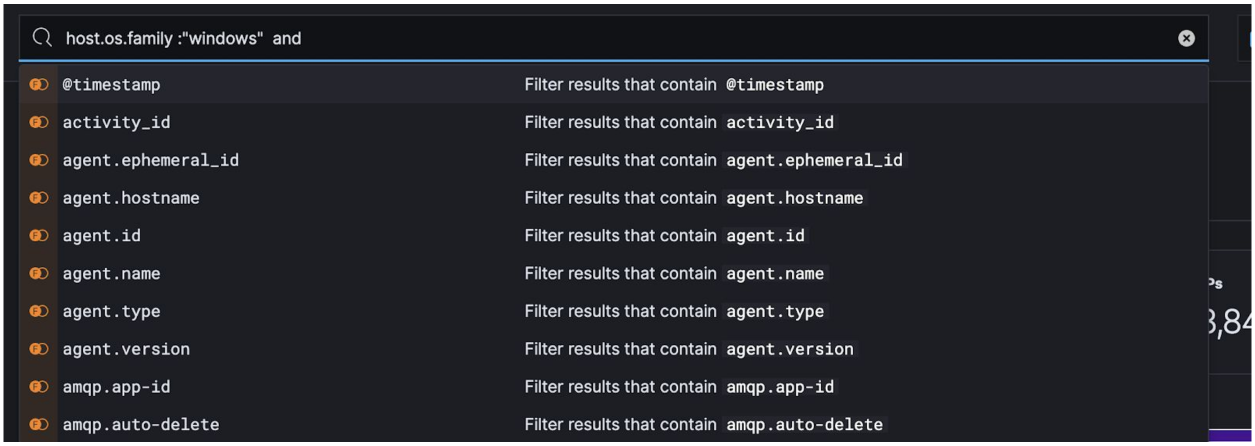


host.os.family :

"redhat"

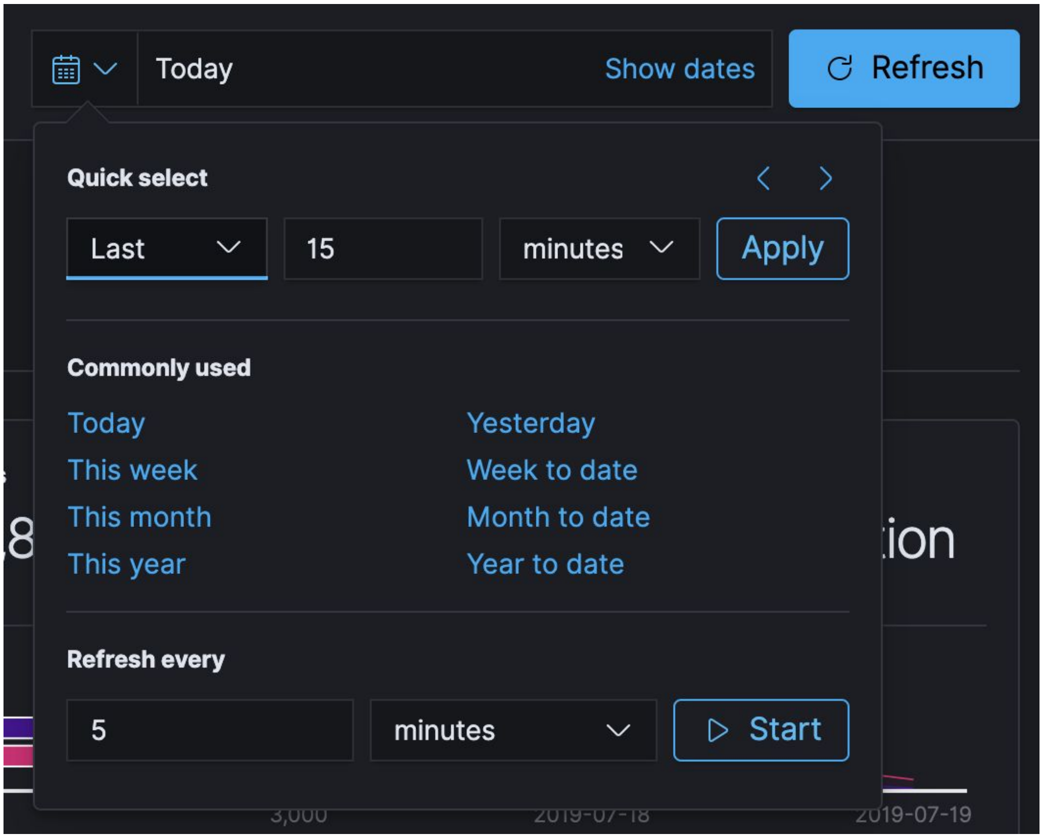
"windows"

"darwin"



host.os.family :"windows" and

@timestamp	Filter results that contain @timestamp
activity_id	Filter results that contain activity_id
agent.ephemeral_id	Filter results that contain agent.ephemeral_id
agent.hostname	Filter results that contain agent.hostname
agent.id	Filter results that contain agent.id
agent.name	Filter results that contain agent.name
agent.type	Filter results that contain agent.type
agent.version	Filter results that contain agent.version
amqp.app-id	Filter results that contain amqp.app-id
amqp.auto-delete	Filter results that contain amqp.auto-delete



Today

Show dates

Refresh

Quick select

Last | 15 | minutes

Apply

Commonly used

Today
Yesterday
This week
Week to date
This month
Month to date
This year
Year to date

Refresh every

5 | minutes

Start