Examine Suricata logs

Now let's examine some logs generated by Suricata.
In Suricata, alerts and events are output in a format known as EVE JSON.
EVE stands for Extensible Event Format and JSON stands for JavaScript Object Notation.
As you previously learned, JSON uses key-value pairs, which simplifies both searching and extracting text from log files.
Suricata generates two types of log data: alert logs and network telemetry logs.
Alert logs contain information that's relevant to security investigations.
Usually this is the output of signatures which have triggered an alert.
For example, a signature that detects suspicious traffic across the network generates an alert log that captures details of that traffic.
While network telemetry logs contain information about network traffic flows, network telemetry is not always security relevant, it's simply recording what's happening on a network, such as a connection being made to a specific port.
Both of these log types provide information to build a story during an investigation.
Let's examine an example of both log types.
Here's an example of an event log.
We can tell that this event is an alert because the event type field says alert.
There's also details about the activity that was logged including IP addresses and the protocol.
There are also details about the signature itself, such as the message and id.
From the signature's message, it appears that this alert relates to the detection of malware.
Next up, we have an example of a network telemetry log, which shows us the details of an http request to a website.
The event type field tells us it's an http log.
There's details about the request.
Under hostname, there's the website that was accessed.
The user agent is the name of software that connects you to the website.
In this case, it's the web browser Mozilla 5.0.
And the content type, which is the data the http request returned.
Here it's specified as HTML text.
That sums it up on the different types of log outputs.
In the upcoming activity, you'll be applying what we just explored by getting hands-on with Suricata.
Have fun!

Revision #1
Created 2023-11-02 13:00:34 UTC by naruzkurai
Updated 2023-11-02 13:00:51 UTC by naruzkurai