Quick Malware Analysis: PIKABOT INFECTION WITH COBALT STRIKE pcap from 2023-05-23

blog.securityonion.net/2023/09/quick-malware-analysis-pikabot.html

Thanks to Brad Duncan for sharing this pcap:
https://www.malware-traffic-analysis.net/2023/05/23/index.html

We did a quick analysis of this pcap on the NEW Security Onion 2.4. If you'd like to follow along, you can do the following:

- install Security Onion 2.4 in a VM:
  https://docs.securityonion.net/en/2.4/first-time-users.html
- import the pcap using so-import-pcap:
  https://docs.securityonion.net/en/2.4/so-import-pcap.html#so-import-pcap
- optionally enable the new DNS lookups feature:
  https://docs.securityonion.net/en/2.4/soc-customization.html?#reverse-dns-lookups

The screenshots at the bottom of this post show some of the interesting alerts, metadata logs, and session transcripts. Want more practice? Check out our other Quick Malware Analysis posts at:
https://blog.securityonion.net/search/label/quick%20malware%20analysis

About Security Onion

Security Onion is a versatile and scalable platform that can run on small virtual machines and can also scale up to the opposite end of the hardware spectrum to take advantage of extremely powerful server-class machines. Security Onion can also scale horizontally, growing from a standalone single-machine deployment to a full distributed deployment with tens or hundreds of machines as dictated by your enterprise visibility needs. To learn more about Security Onion, please see https://securityonion.net.

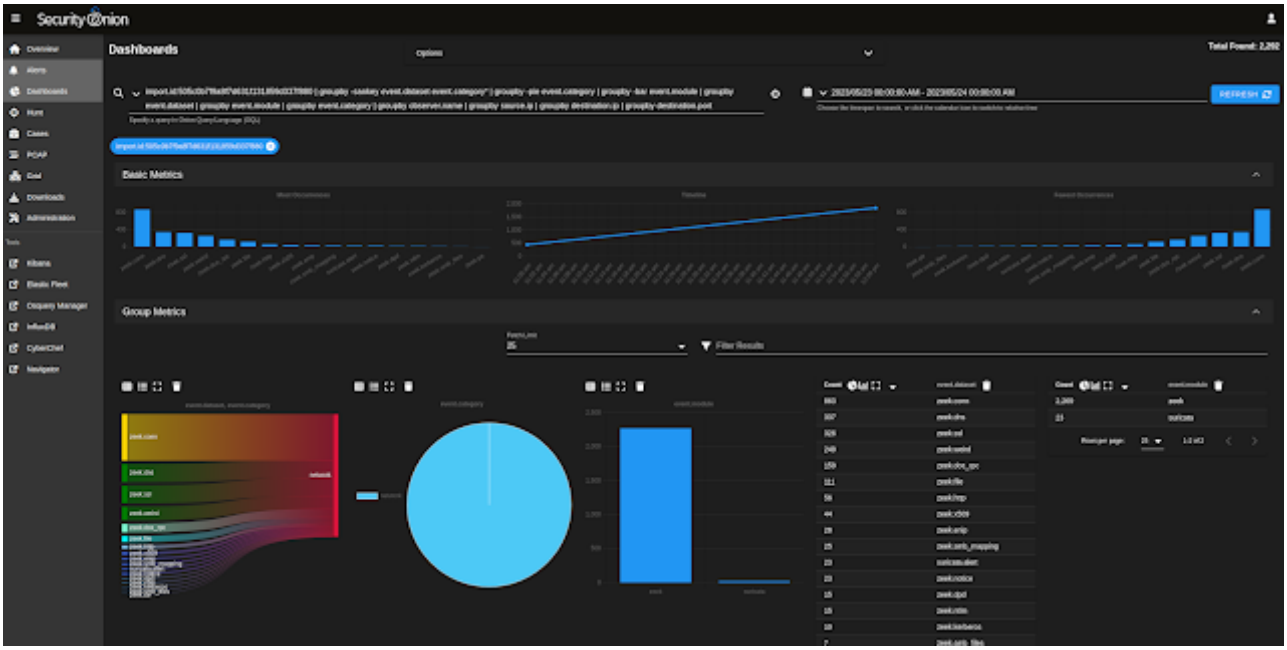
Our 10th Annual Security Onion Conference is coming up soon, so reserve your seat today! Last day to register is September 29. For more details, please see https://socaugusta2023.eventbrite.com/.

Do you want to deploy the new Security Onion 2.4 to your enterprise but need training? Our first 4-day public training class on Security Onion 2.4 will be in beautiful Augusta GA as part of Augusta Cyber Week! The class is at a very special price AND you get a free ticket to BOTH Security Onion Conference AND BSidesAugusta! For more information, please see https://blog.securityonion.net/2023/07/registration-now-open-for-augusta-cyber.html.

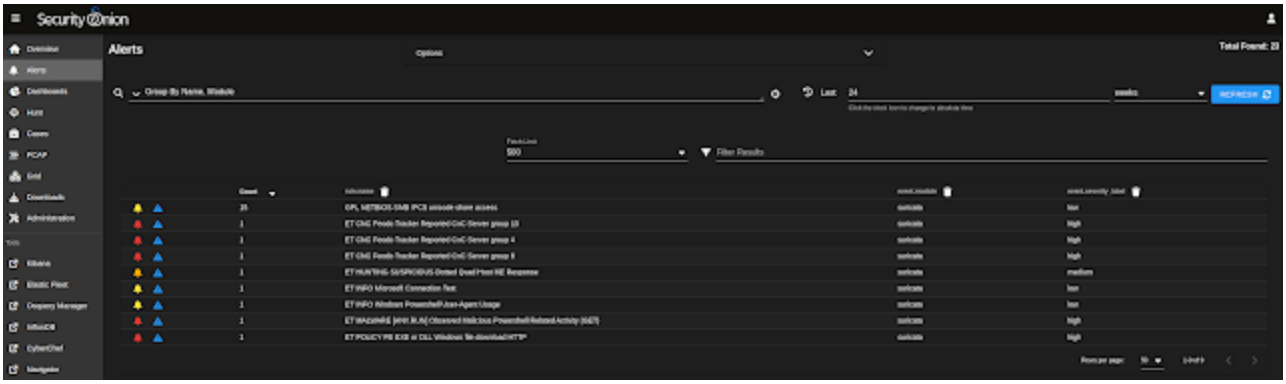
Do you want to deploy Security Onion to your enterprise and want the best enterprise hardware? We know Security Onion's hardware needs, and our appliances are the perfect match for the platform. Leave the hardware research, testing, and support to us, so you can focus on what's important for your organization. Not only will you have confidence that your Security Onion deployment is running on the best-suited hardware, you will also be supporting future development and maintenance of the Security Onion project! For more information, please see https://securityonionsolutions.com/hardware.

Screenshots

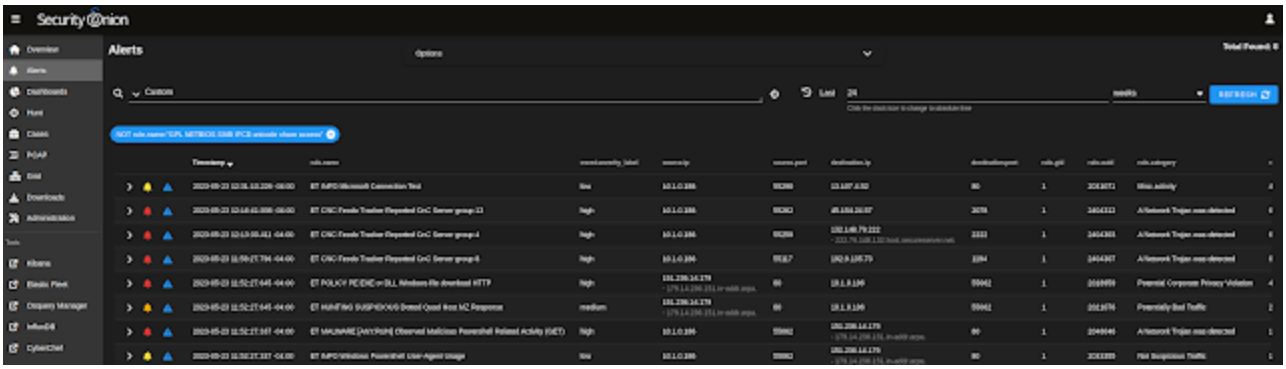
First, we start with the overview of all alerts and logs:



Next, we focus on the alerts:

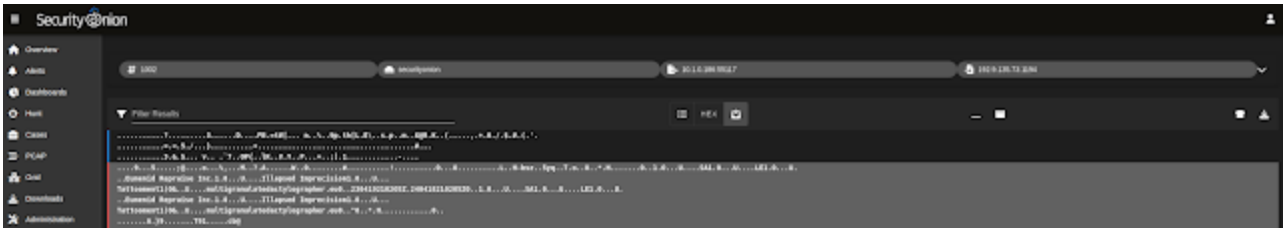


We can switch to ungrouped mode to see more detail:

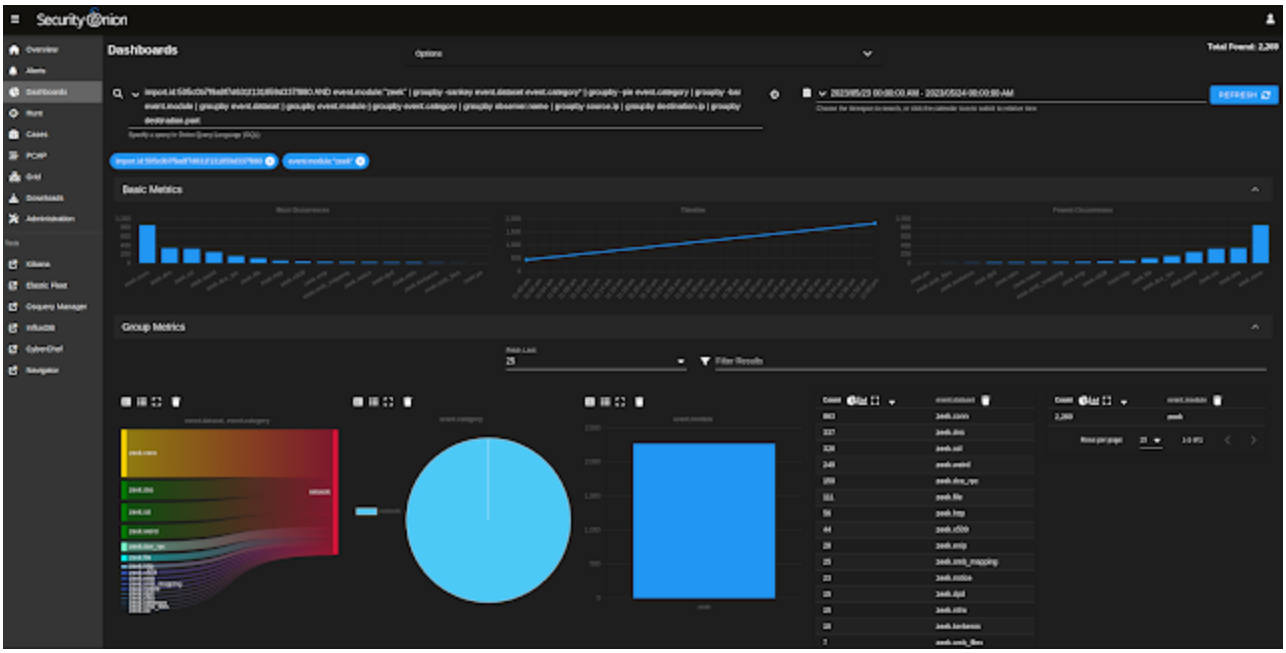


Notice that the last 4 alerts are for the same TCP stream, so let's pivot to pcap. Notice the user agent string, the bare IP host header, and the executable file that is downloaded:

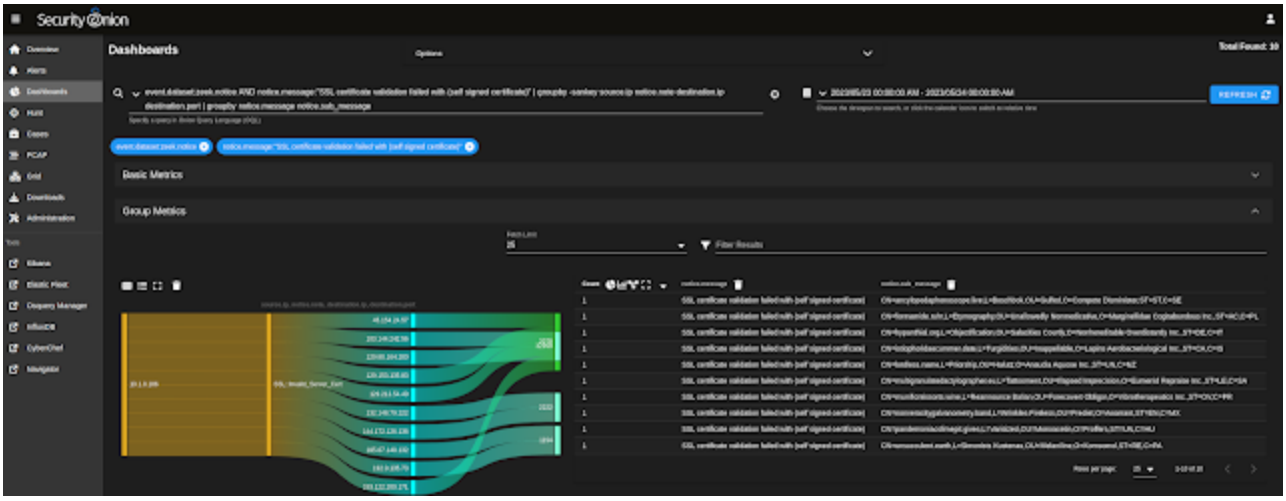
Back at the alerts, let's take a look at the pcap for the 3 "ET CNC Feodo Tracker Reported CnC Server" alerts:



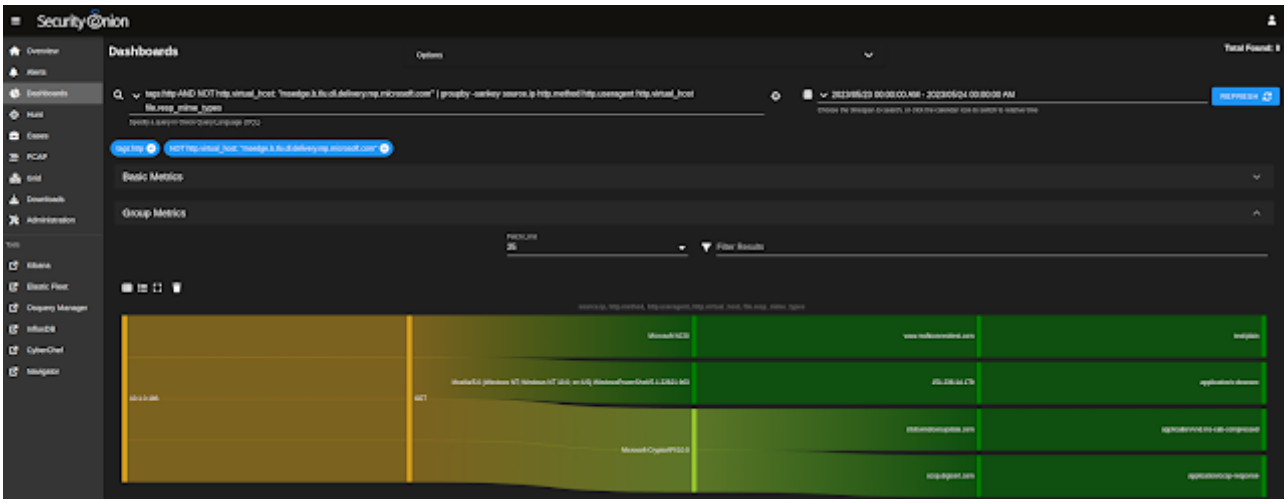
After reviewing alerts, let's look at all of the protocol metadata:



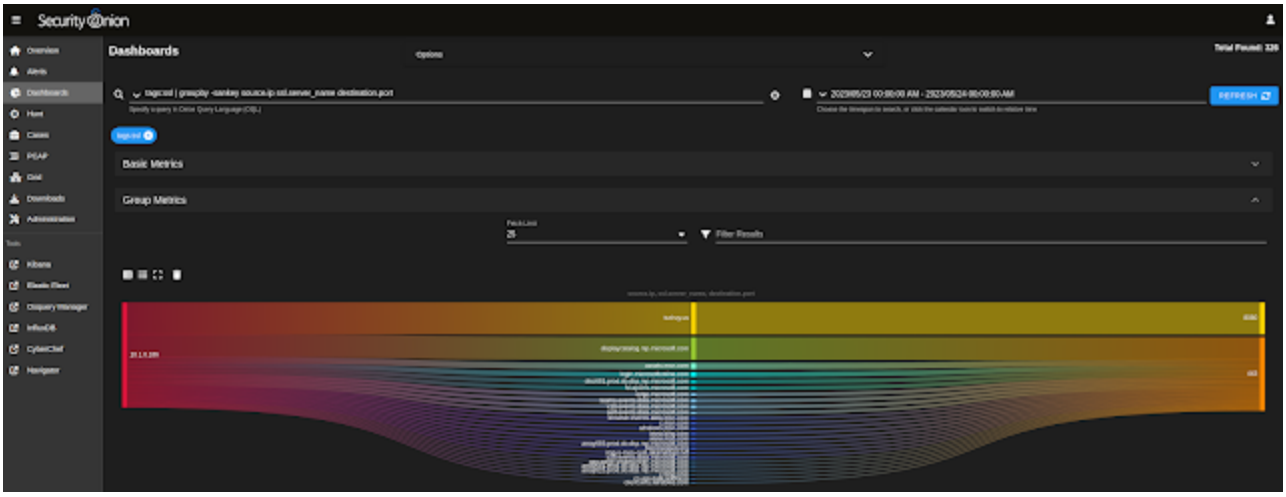
Next, let's look at the Zeek Notices:



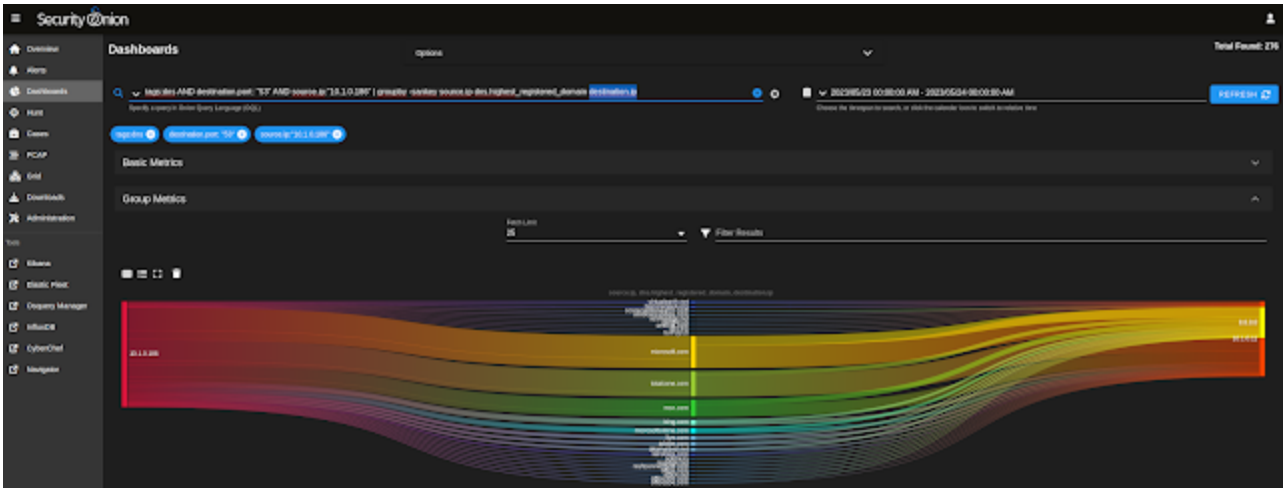
We'll next review HTTP transactions:



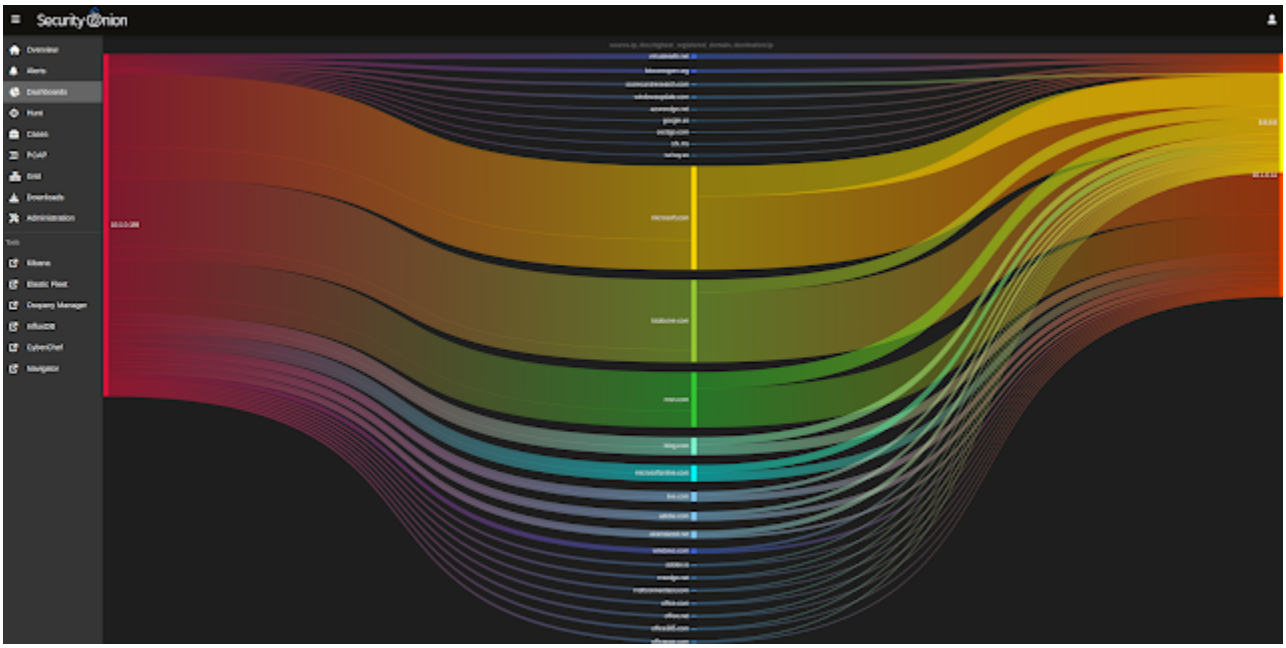
Next, here are the SSL/TLS connections:



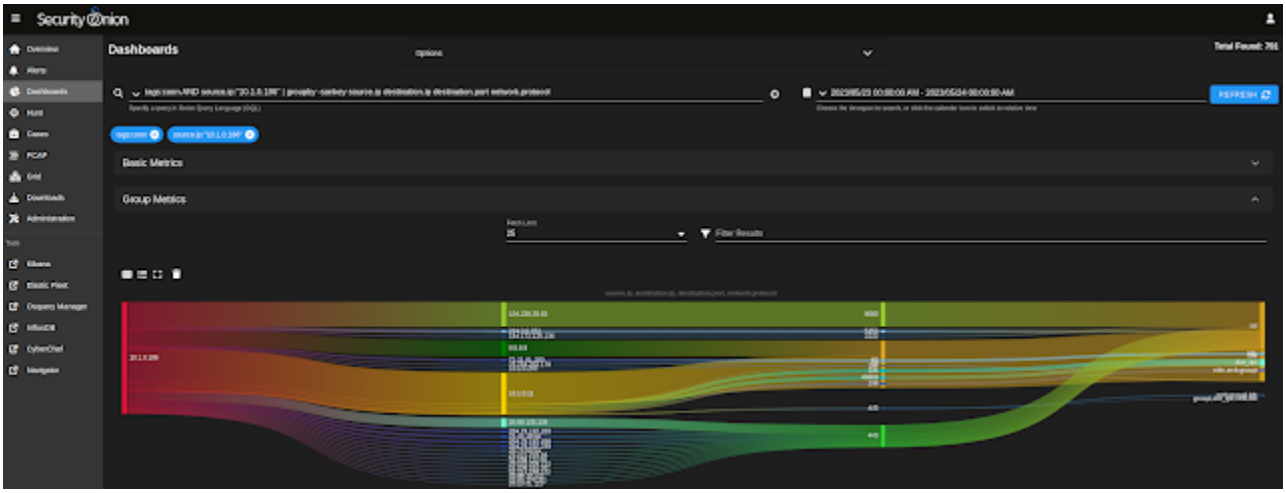
We'll next review the DNS lookups:



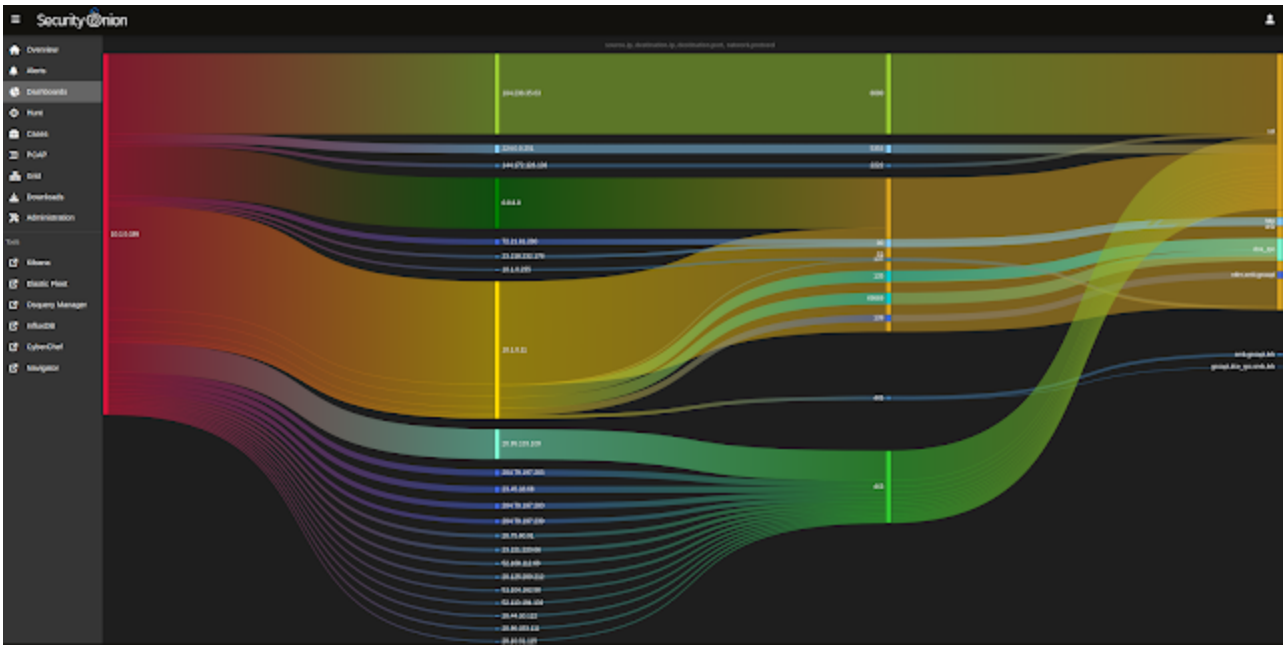
That sankey diagram is a little crowded, so let's maximize it:



Finally, let's look at all connections:



and in maximized format:


Security Onion
Overview
Alerts
Dashboards
Hunt
Cases
PCAP
Grid
Downloads
Administration
Tools
Kibana
Elastic Fleet
Osquery Manager
InfluxDB
CyberChef
Navigator