STIX Bundle Description

APT-29-CB

The IP address 103.216.221.19 is the IOC from TII we performed our first search on. Once we search on this IP address, we see an internal IP address of 10.120.209.202 that interacted with this IOC. Once we add these IP addresses to our case, we can continue to do a search on our internal IP address.

APT-29-Guradium

The IP address 10.120.209.202 is the machine of KHenderson. this is the IP address that needed to be searched. We find through DE that her machine made a couple queries to a critical asset within the organization. The queries found are to show the power of DE looking through several systems and alert the analyst of some possible data disclosure.

QRadar.json

This STIX bundle is more to fill CP4S with more demo data to show the power of DE the information that comes back. Once we performed the DE search on 10.120.209.202, we can see all the logs that were ingested by QRadar and can help our analyst understand where else an investigation needs to happen.