Continuum Advantage RSYNC ingest of existing PCAP and PCAP-NG files

- Ingesting pcap and pcap-ng files from remote systems via rsync command retaining the original timestamps.
- This is in addition to capturing data off a separate live network span port interface at the same time.

Terminology

- Your Rsync Source – provides the pcap files to be rsync'd.
- Rsync Source Root Directory – rsync recursively copies from this directory from the Source system to the Destination system.
- Rsync User – username used for access to the source system. Must be a valid Linux user on the source system. All the files/directories under Rsync Source Directory must be removable by this user. This is identified as user_id_source in rsync_master.conf and rsync_slave.conf files described below.

Setup

- For RSYNC feature, there must be a Source system that has pcap data (PCAP and PAP-NG file formats) and a Continuum Advantage software subscription installed on a a separate customer computer or server that pulls these pcaps from the Source server, ingests these files, indexes and makes them available for search, events and alerts with the original timestamps (same capabilities as live wire network traffic).
- A Cat5 or Cat 5 cable is connected directly or indirectly (routable path via a switch) from the rsync capture interface on the computer or server the Continuum Advantage software is installed on to the computer/server running Linux with a local or attached file system that the existing PCAP files reside on
- Once the config file is setup, Run the following command on the Master or Source system where these existing PCAP and PCAP-NG files exist. This file is provide with the subscription service.

```
> cd /usr/local/nc/bin/
>
>
> ./nc_rsync_setup rsync_master.conf
```

```
 > ssh -i /usr/local/ncCrypto/rsync_source chris@5.5.5.8
Last login: Wed Nov 28 03:58:07 2018 from 5.5.5.7
[chris@localhost ~]$ ifconfig | grep 5.5.5.8
        inet 5.5.5.8  netmask 255.255.255.0  broadcast 5.5.5.255
[chris@localhost ~]$
```