Date: Friday, October 12th
Speakers: Adam Pumphrey, Director of Professional Services, Bricata

Network Data Enrichment for Analysis and Hunting

Analysts continually accrue knowledge as they work, reviewing network communications, investigating alerts and making decisions about suspicious traffic and potential threats. They learn about the hosts in the environment and their function, and they gain experience that allows them to make quicker, better-informed decisions. This combination of tradecraft and environmental acumen is invaluable to the analyst but is not easily passed around. How can we share this institutional knowledge and context to accelerate investigations and threat hunting?

We can use Bro to enrich network traffic data with contextual information, using terms that describe host, network and communication attributes - and, by doing so, begin to share some of that tribal knowledge gained from familiarity with a network environment. Simple labels like "known", "authorized", or any number of descriptive terms allow analysts to quickly and easily filter large volumes of network transactions, focusing their attention on those that are "unknown". Analysts can describe communications in such a way that anything deviating from a normal pattern can be considered notable and worthy of further investigation. This enrichment also provides a foundation for creating accurately labeled training data for use in pattern recognition AI.

This talk will describe the need for, and utility of, network data enrichment using Bro. It will share some custom frameworks and Bro Script developed for this purpose and will discuss how these tools can be applied to enhance threat hunting.