BLUE Vortex

AMPEX

Do You Know What's On Your Network?

We don't always know about ALL the devices on our networks. We also don't know exactly who our connected devices talk to and how. The ever-increasing number of connected "things" (IoT) makes complete network situational awareness seemingly impossible, leaving us vulnerable to limitless attack vectors.

Ampex's BLUE Vortex offers a unique solution to this problem with a sophisticated visualization engine that displays your network nodes and communications pathways.

Features

- **Informs you of devices connected on your network**
- **Live, precise model of your network and communication pathways, graphically illustrated**
- **Live, network forensics**
- **Ingests PCAP files for offline forensics**
- **Small form factor**
- **Encrypted storage**
- **Removable solid state drive**
- **Creates baseline for BLUE Lightning**

How It Works

The BLUE Vortex device uses passive, full packet "capture" techniques to create a live model of your network. This includes showing all attached devices and who they talk to, enabling network forensics in real-time.

BLUE Vortex can create the same model and visual depiction using a network capture file (PCAP) for offline forensics.

Additionally, BLUE Vortex can establish the initial baseline model of network characteristics and behavior for complimentary, cyber protection devices such as Ampex's BLUE Lightning device. BLUE Lightning employs two advanced algorithms for behavior-based, network anomaly detection (non malware signature-based) and data validation (counters spoofing attacks).

How it's Used

Ampex's BLUE Vortex device is the perfect tool for security assessment teams that are responsible for evaluating network vulnerabilities. Additionally, it is a great tool for asset or inventory management and accountability.

03/19