Network Detection

The Network Detection service module automates the investigation of network traffic alerts and allows security teams to view those alerts in the context of other user activity. To enable this feature, the ActiveEye Intrusion Detection System (IDS) is deployed within Customer's network to perform real time signature and anomaly detection. The IDS analyzes traffic for signs of malicious activity in real time. In addition, the IDS performs packet level and flow level analysis, enabling network communications modeling. This information is used to identify anomalous behavior that is not captured by pre-defined traffic signatures, including activity over encrypted connections.