Problem. Detect Advanced Persistent Threat (APT) activity in networks to proactively react to sabotage and virus expansion using anomaly detection and visualization.

Task. Gain insight in (false positive) alert collections by studying correlations between alerts, messages, and attributes.

Alerts. Compute probability scores on protocol fields to detect misusage.

Exploration Water Plant control system

Results. Detection of Man-In-The-Middle activity in water plant facility consisting of 5 hosts. Water tank overflow without notification to the monitoring system.

Analysis of 80,000 messages, 2000 alerts, and 170 attributes

Save & Select
Store message collections of interest for further investigation.

Rank & Inspect
Per-attribute histograms are used to (de)select (malicious) messages of interest based on attribute values.

Sort attributes to discover patterns and correlations in selections.

Traffic overview
Select alert burst in time.

Attributes
Select
Refine

Divide & Conquer
Alert assessment requires viewpoints:

1. Infiltration
2. Expansion
3. Sabotage

Context & Conversations
Compute probability scores on protocol fields to detect misusage.

Contextual search by dynamically choosing visualizations & data partitionings.

Detection of Man-In-The-Middle activity in water plant facility consisting of 5 hosts. Water tank overflow without notification to the monitoring system.

Select alert burst in time.

Inspect overlap in attributes

Discovery of IP address used by multiple hosts