



Clique

Safeguarding Cyber Systems with Visualization

CHALLENGE

Enabling network defense against attacks that aim to steal information, disrupt service, or destroy resources requires the collection and analysis of staggering amounts of data. The ability to detect and respond to threats quickly is a paramount concern that spans government, utilities, financial and private sectors. These organizations share a common burden of threat identification contained within potentially billions of network transactions each day. To better equip analysts, data intensive visual analytic tools are needed to address the unique challenges within cyber security.

SOLUTION

Researchers at the Pacific Northwest National Laboratory (PNNL) have developed an innovative visual analytic capability with two powerful views that can take advantage of data intensive architectures to enable analysts and provide visibility and command of their data in ways that were not previously possible. Together, the two views support an investigative workflow.

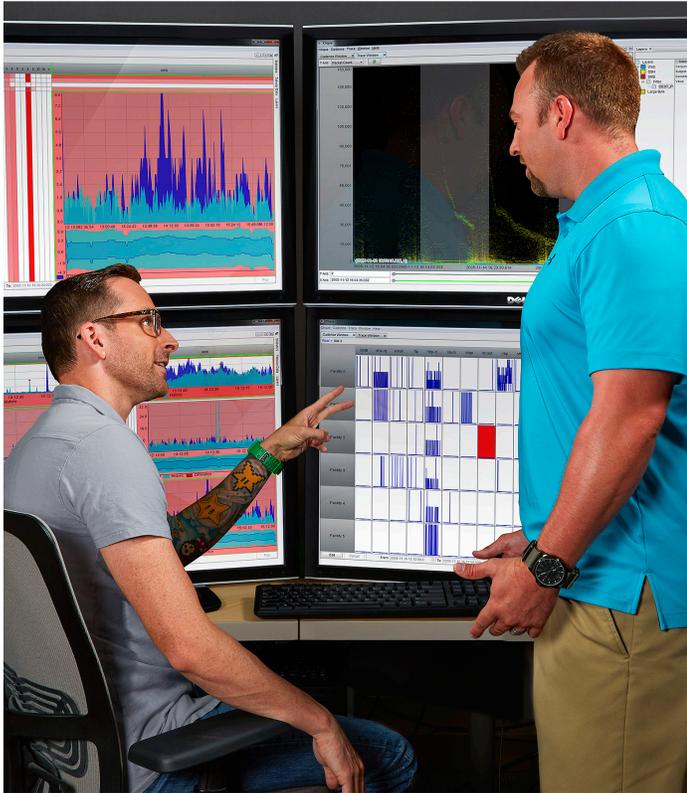
The Cadence view within Clique displays high-level overviews of network traffic using a behavioral model-based anomaly detection technique. This technique builds models for learning and classifying expected behavior of individual hosts on a network and compares these modeled behaviors to current data. The result is a deviation score that provides indicators of “non-normal” network activity.

The effectiveness of Cadence is enhanced by a graphical user interface that highlights anomalous activity using color saturation and progressive disclosure, empowering users with the ability to identify deviations from expected activity. Users can navigate through their data temporally, viewing



time periods as short as a few minutes or as long as many hours. Cadence models help analysts to see departures from normal behavior at any time scale. The user interface enables drill down capability so that analysts can view detailed displays of network activity to determine the machines, buildings, sites, or other sources of traffic behaving anomalously.

The Trace view within Clique provides analysts with a flexible and scalable two-dimensional scatterplot. This enables identification of patterns that exist in large volumes of network data. This visualization approach was specifically requested by defenders on the front lines to display raw network traffic using multiple attribute-based views and supports millions of communications events in a single view. Trace enables users to use human cognition to identify patterns contained within large volumes of data, a task that is tremendously difficult using other analytic techniques. This enables analysts to view typical communication patterns contained in their data and provides a mechanism to highlight patterns of interest.



Trace empowers analysts with the ability to interact and explore their data at scale. The view provides a mechanism for analysts to color code the data in meaningful ways to highlight features of interest.

Once a feature is identified, analysts can view summary statistics about a selection or display the underlying data in a common tabular view where they can export for reporting and use in other tools.

IMPACT

Clique delivers operational impact by eliminating several common analyst workflow actions and delivers a capability to support investigation as well as provide key indicators of off-normal network activity. Network defenders now have a mechanism to move seamlessly from high-level views of behaviors in Cadence down to detailed representations in Trace. The result is significantly improved situational awareness of network activity, which provides more efficient investigation to support prevention, response, and mitigation of harmful attacks.

ABOUT PNNL

Interdisciplinary teams at PNNL address many of America's most pressing issues in energy, the environment, and national security through advances in basic and applied science. Founded in 1965, PNNL employs 4,400 staff and has an annual budget of nearly \$1 billion. It is managed by Battelle for the U.S. Department of Energy's Office of Science.

For more information, contact:

Daniel Best

Senior Cyber Researcher
National Security Directorate
daniel.best@pnnl.gov
(509) 372-6728

Dave Thurman

Director, Computing Programs
National Security Directorate
dave@pnnl.gov
(206) 528-3221

Visit us online at analytics.pnnl.gov


Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by **Battelle** Since 1965

U.S. DEPARTMENT OF
ENERGY