Visualization Examples for Cyber Security
Sample Visualization

OCEANS - Online Collaborative Explorative Analysis on Network Security:

Visualization and interactive analysis can help network administrators and security analysts analyze the network flow and log data. The complexity of such an analysis requires a combination of knowledge and experience from more domain experts to solve difficult problems faster and with higher reliability. The online visual analysis system called OCEANS was developed to address this topic by allowing close collaboration among security analysts to create deeper insights in detecting network events. Loading the heterogeneous data source (netflow, IPS log and host status log), OCEANS provides a multi-level visualization showing temporal overview, IP connections and detailed connections. Participants can submit their findings through the visual interface and refer to others’ existing findings. Users can gain inspiration from each other and collaborate on finding subtle events and targeting multi-phase attacks. Our case study confirms that OCEANS is intuitive to use and can improve efficiency. The crowd collaboration helps the users comprehend the situation and reduce false alarms.
Event correlation and subtle events detection. Pre-scanning (subtle) before the DDoS attack. (E3) Server (E2) DDoS attack with many comments on it. (E1) crash (subtle) after the DDoS attack
Sample Visualization

Botnet analysis. (a) Overview timeline. (b,c)-E1, firstly detected events, which turned out to be a botnet DDoS attack. (d)-E2, secondly detected events. By applying filters, user found the suspicious outbounce SSH connections. (e,f )-E3, botnet infection as subtle event. (g) Summarized attack pattern.
Sample Visualization

User evaluation: Feedback based on questionnaire
Sample Visualization

NStreamAware: Real-Time Visual Analytics for Data Streams to Enhance Situational Awareness

Integrated Perspectives

• Real-Time Data Stream Monitoring
• Real-Time Sliding Slices (NVisAware)
• Visual Feature Selection
• Summarized Sliding Slices
• Event Timeline & Insights
• Search & Exploration
Sample Visualization

Real-Time Data Stream Monitoring
Sample Visualization

Real-Time Sliding Slice

- Interactive Widgets
  - Treemaps
  - Counters
  - Node-link diagrams
- Interactions
  - Star/Annotate slice
  - Remove slice
  - Retrieve data
- Color Encoding
  - Background for similarity
  - Importance of alerts

12 Visualization Examples for Cyber Security
Sample Visualization
Sample Visualization

Example: Using Visual Analytics for Interactive Summarization
Sample Visualization

Multiple Queries with Conditional Attributes (QCATs) for Anomaly Detection and Visualization
Sample Visualization

SEEM: A Scalable Visualization for Comparing Multiple Large Sets of Attributes for Malware Analysis
Sample Visualization

Designing STAR: A Cyber Dashboard Prototype

A central challenge for a strong cyber defense is the appropriate communication of cyber information. There are many key stakeholders that make decisions and convey information up to different levels of authority, and this information may not always be in sync. Additionally, cyber analysts know and often utilize technical jargon to pass along information, and these analysts can spend significant time and effort to building their own visualizations manually, such as network summaries, patterns, and recent attacks. To aid communication, a working prototype of a cyber dashboard was developed which visualizes a simplified view of a network, particularly the key external players which are extracted from both IDS alerts and reports from a traffic analyst. This prototype is one step towards enabling analysts to simplify and encode information into a visualization that can help tell the story of a cyber attack or a network’s current defense status.
Sample Visualization

This paper presents a cyber visualization, or the STAR dashboard, an interactive web prototype with linked views that enable the use of simple stories by conveying both IDS alert data on top of analyst-created reports, connected through the use of external entities, both countries and cities, in the main treemap view.
Sample Visualization

Last updated on

Daily summary

Detailed hourly heatmap of alerts

Alerts per day

Priorities of Alerts

Priority level of alerts

Categories of Alerts

Categorization of alerts

Treemap view by country; hexagons are cities and states, sized by number of alerts; reports are shown as red circles

Report summary: dates, location, & incident details

Department of Computer Science and Engineering
Sample Visualization

CORGI: Combination, Organization and Reconstruction through Graphical Interactions
Sample Visualization

Visual Filter: Graphical Exploration of Network Security Log Files
Sample Visualization

A Tool for Rapid Visual Interrogation & Triage of Alerts

This paper presents a tool to assist in the rapid browsing and interrogation of network alert data from monitoring systems like Snort. The tool are designed for time-sensitive applications where further analysis is offloaded after initial identification; thus, rapid exploration and at-a-glance summaries are paramount. Towards these ends, our primary tool uses simple visualization and interaction for identifying what alerts need processing.
Sample Visualization

Alert Triage

- Sort by:
  - Age
  - Src IP
  - Dst IP
  - Src Type
  - Dst Type
  - Priority

- Order:
  - Ascending
  - Descending
  - Toggle View

The Alert Triage System. Events information is summarized in the center, with specific alert data and the event histogram to the right, navigation to the left.
Sample Visualization

Marking:
Compromised and malicious IPs can be marked in red for triage and later processing.
Sample Visualization
Sample Visualization
Sample Visualization
Sample Visualization