

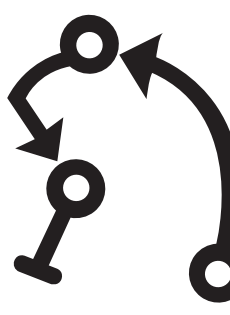
TOP 5 DATA SOURCES IN SECURITY VISUALIZATION SYSTEMS

 Packet Traces

Total Systems: 16

 Intrusion Alerts

Total Systems: 7

 BGP

Total Systems: 7

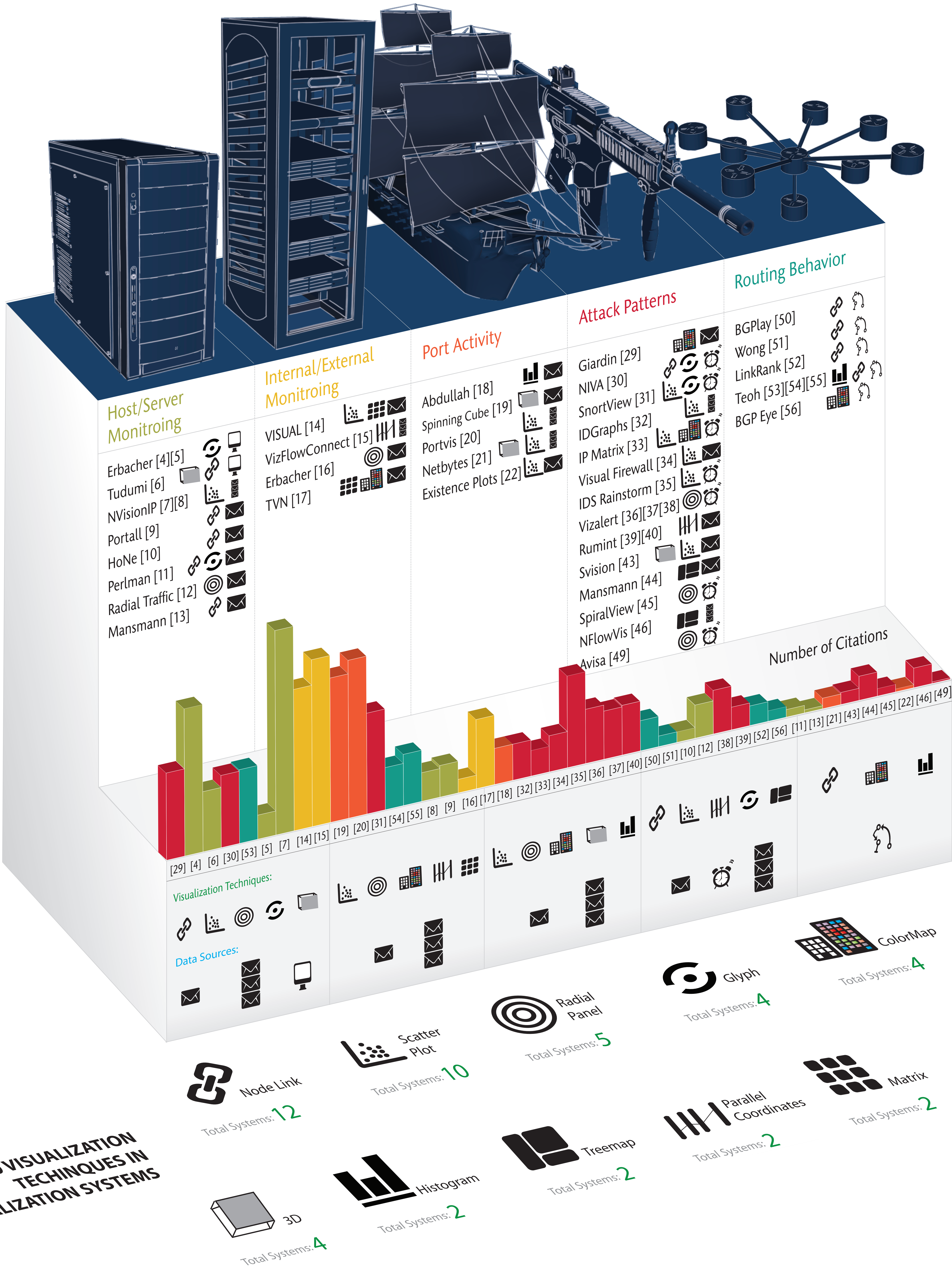
 Netflow

Total Systems: 6

 Server Logs

Total Systems: 2

It expresses the idea that common visualization techniques have been designed for use cases that are not supportive of security-related data, demanding novel techniques fine tuned for the purpose of thorough analysis. This infographic is the result of a comprehensive study of modern visualization systems for network security and portrays a novel taxonomy in the form of five use-case classes. The visualization systems, the incorporated visualization techniques, the utilized data sources, and the number of references for each paper are illustrated bellow.



Host/Server Monitoring:

In this class of visualization, the main display is devoted to the representation of hosts and servers. The intend is to display the current state of a network by visualizing the number of users, system load, status, and unusual or unexpected host or server activities.

Internal/External Monitoring:

Visualizations of this class are concerned with the interaction of internal hosts with respect to external IPs. Similar to the abovementioned class, this class of visualization also incorporates a display of internal hosts, but in relation to communicating external IPs.

Port Activity:

Designers of this class of visualization argue that various malicious programs like viruses, trojans and worms manifest themselves through unusual and irregular port activity. Visualizations of this class can aid in the detection of malicious software running inside a network. Scaling techniques must be incorporated in the design of visualizations of this class, due to the amount of traffic as well as the large range of possible port numbers and IP addresses.

Attack Patterns:

Visualizations of this class aid an administrator in not only the detection of attacks but also the display of multistep attacks. Different types of attacks show different behaviors and accordingly different visual patterns appear. Many types of attacks are carried out in multiple phases, generally starting with reconnaissance, followed by scanning, acquiring access, maintaining access, and finally clearing tracks and installing back doors for future access. Visualizations of this class should aid in displaying these phases.

Routing Behavior:

Understanding the evolution of Border Gateway Protocol (BGP) routing patterns over time is the main goal of this visualization class. The distributed nature of BGP and the lack of verification of the validity of the announcements causes Internet routing to be susceptible to attacks. The ability to detect and correct disruptions in Internet traffic caused by router misconfigurations or malicious attacks is considered in this class.