Avisa

alert visualization assembly

# IDS Alert Visualization for Network Security Monitoring and Analysis

Hadi Shiravi, Ali Shiravi, Ali A. Ghorbani

Information Security Centre of Excellence

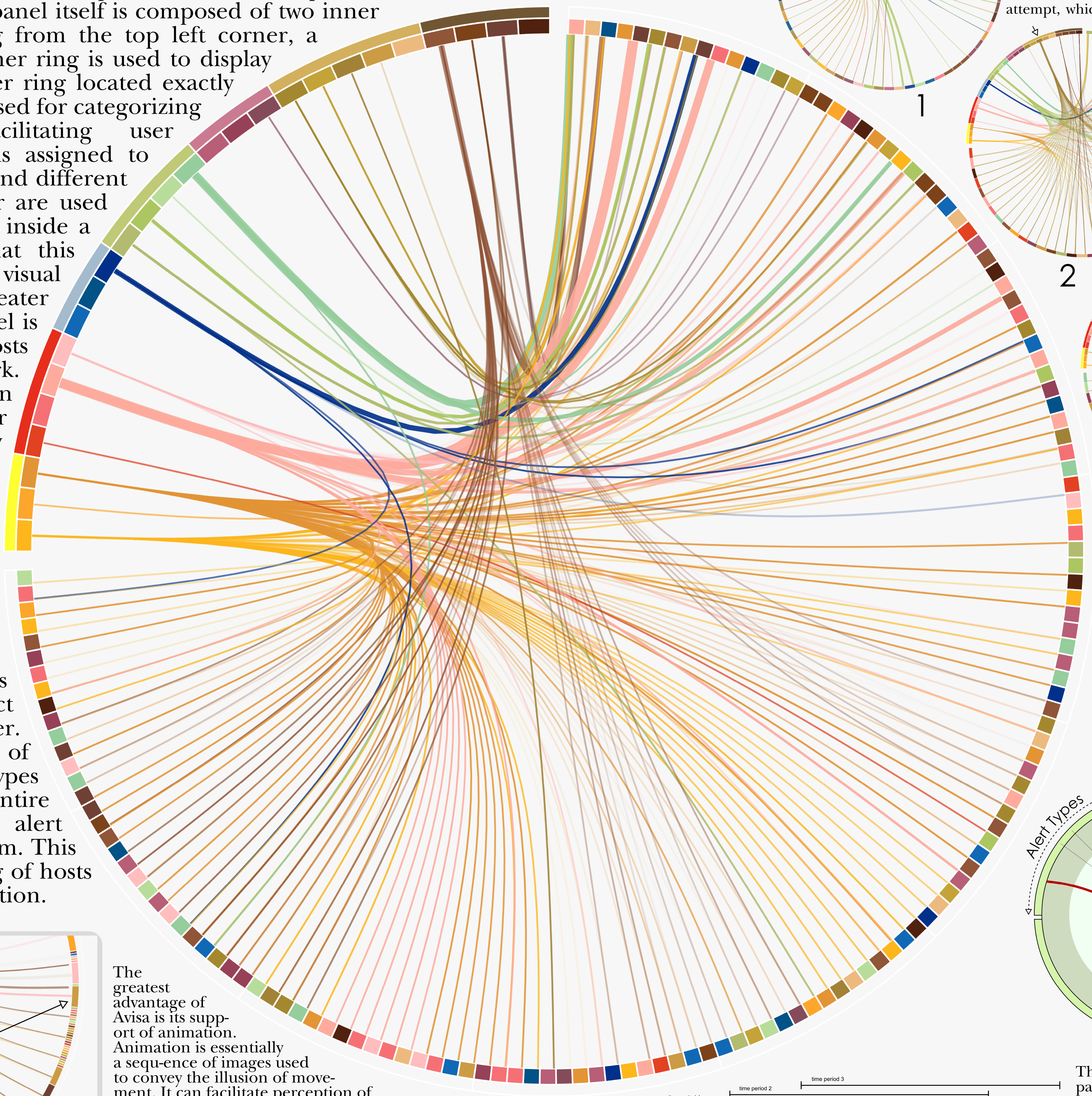
Faculty of Computer Science

www.iscx.ca

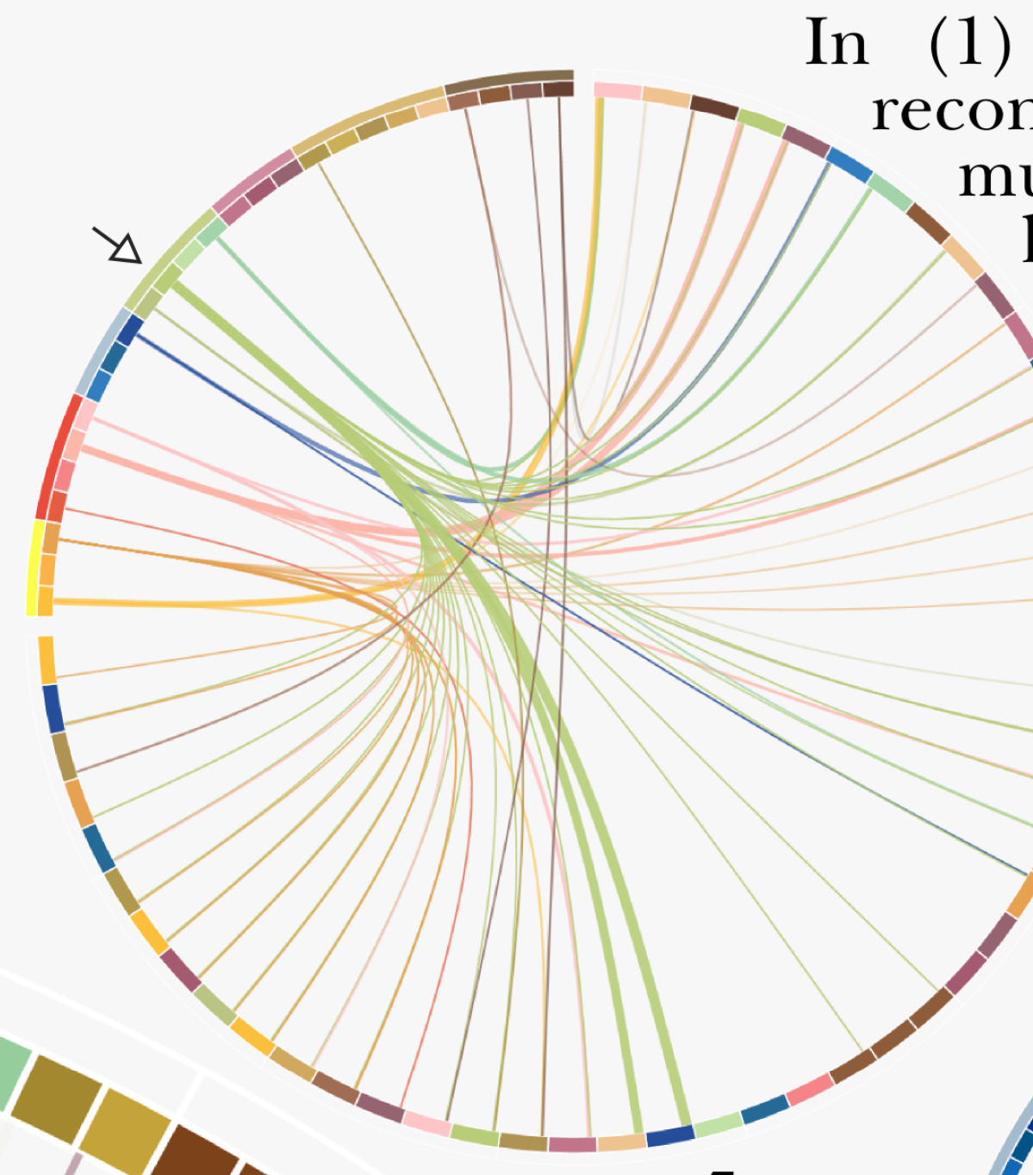
Avisa is a security visualization system that addresses the aforementioned problems. It is built upon an emerging information visualization paradigm, namely radial visualization. The paradigm is aesthetically pleasing, allows for data to be encoded on both the outer and interior parts of the ring and has a compact layout for an effortless user interaction [9].

Avisa is composed of two main components. The radial panel and the interior arcs. The radial panel itself is composed of two inner and outer rings. Starting from the top left corner, a color band inside the inner ring is used to display IDS alert types. The outer ring located exactly above this color band is used for categorizing alert types and facilitating user interaction. One color is assigned to each alert type category and different shades of the same color are used for individual alert types inside a category. We believe that this color coding eases visual correlation. The greater portion of the radial panel is devoted to internal hosts residing inside a network. Hosts can be arranged in subnets or asset groups or even be manually arranged based on specific machines that an admin is interested in monitoring. The outer ring surrounding the individual hosts (subnet panel) depicts these arrangements.

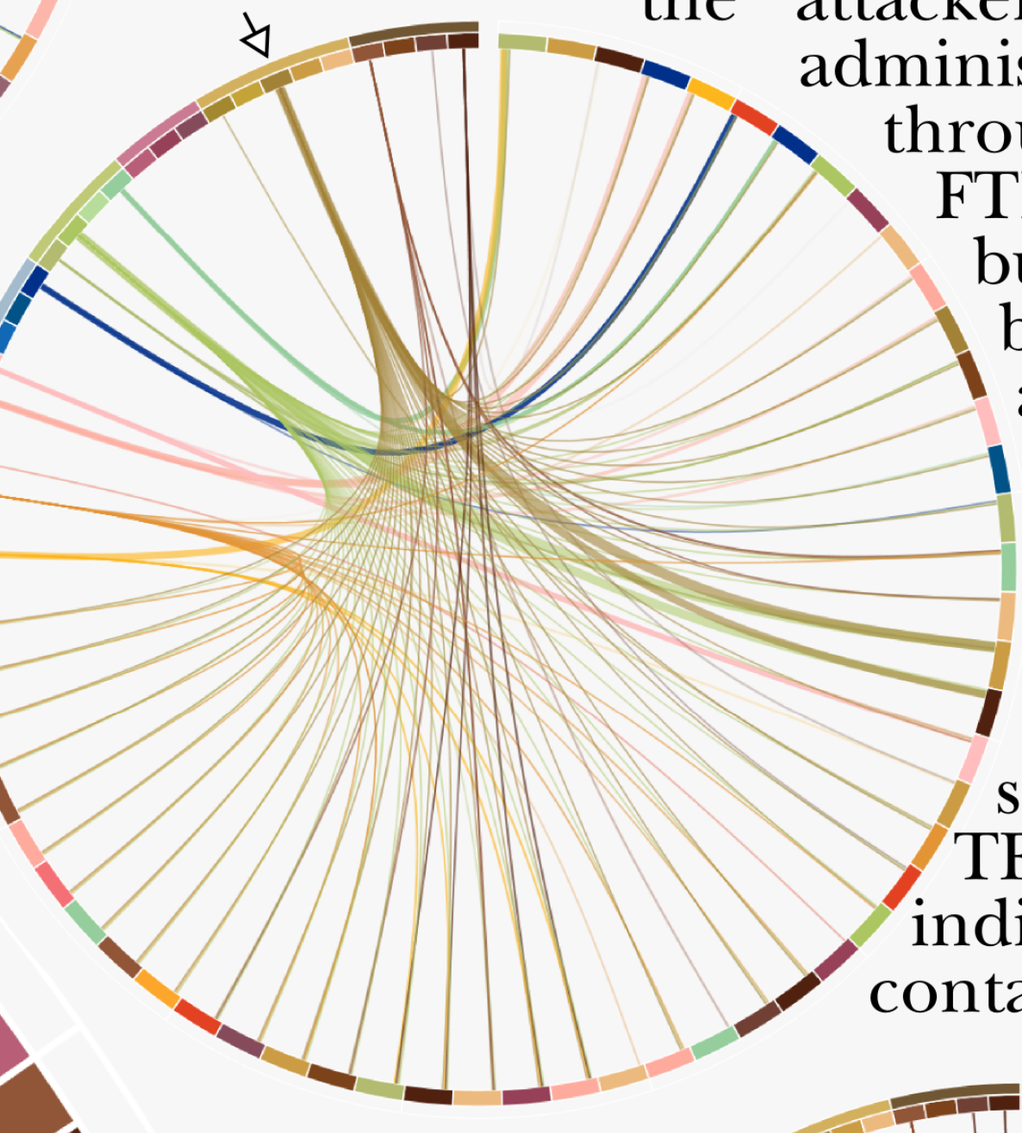
Avisa also supports filtering through direct interaction with the user. By simply clicking on any of the hosts, subnets, alert types or alert categories the entire portion of the host or alert panels are devoted to them. This feature allows for filtering of hosts and alerts in any combination.



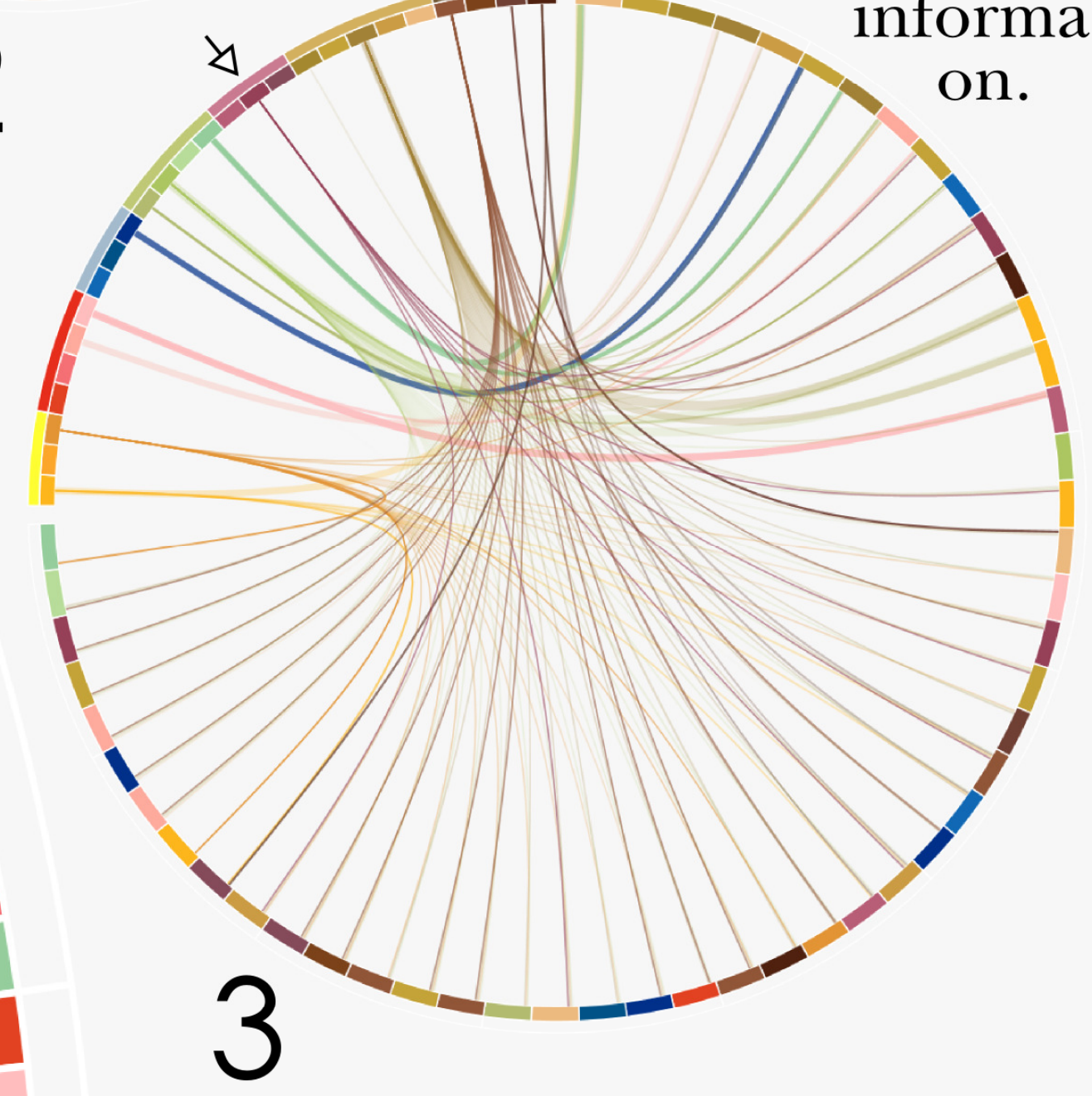
In (1) a large number of Nmap reconnaissance events have been triggered, targeting multiple hosts on the network. In (2) multiple failed login attempts are seen targeting the same range of IP addresses. Although these events are triggered at different time stamps, Avisa's time window facilitates visual correlation by displaying past and current events at the same time. The unusual number of attempts indicates that the intruder is attempting a brute force method of attack. The same procedure is seen in Figure (3) that after a brute force attempt, which is likely to have been unsuccessful, the attacker has tried to gain administrator privileges through exploit-ing several FTP severs vulnerable to buffer overflow. The bftpd chown overflow alert is generated on multiple servers indicating a possible intrusion. In Figure (4), the compromised FTP servers are receiving TFTP GET passwd alerts indicating a file transfer containing root level authentication information.



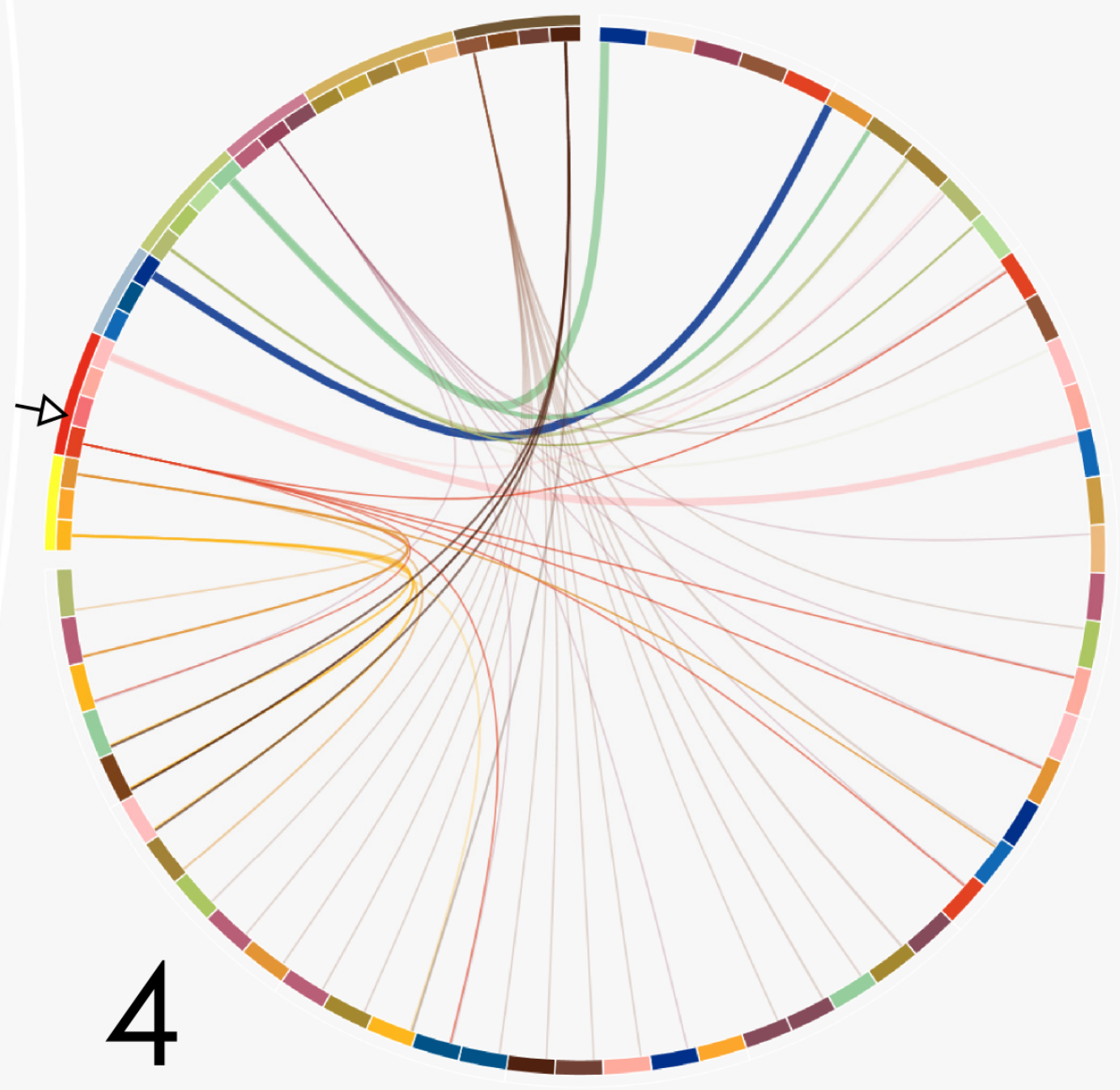
1



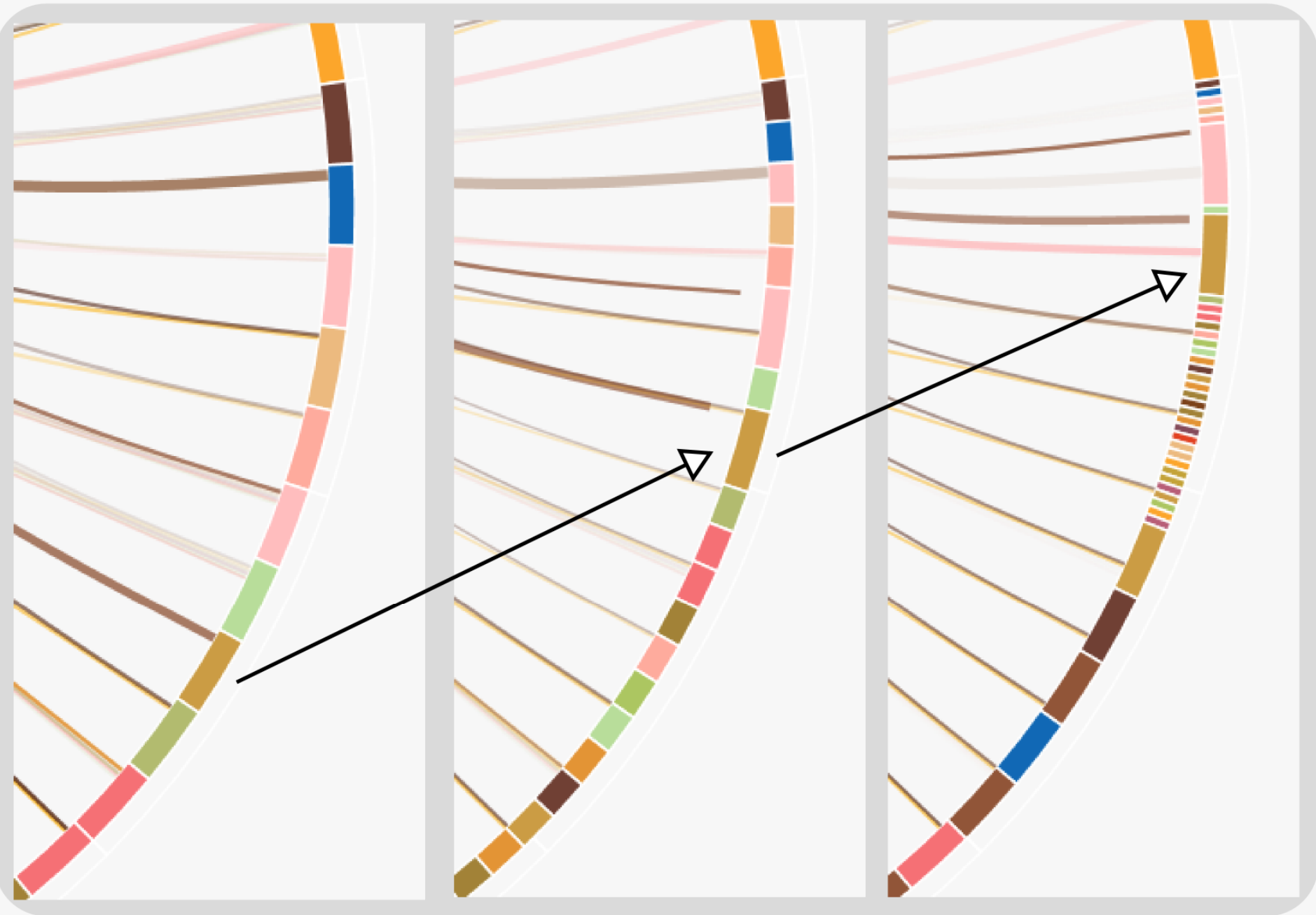
2



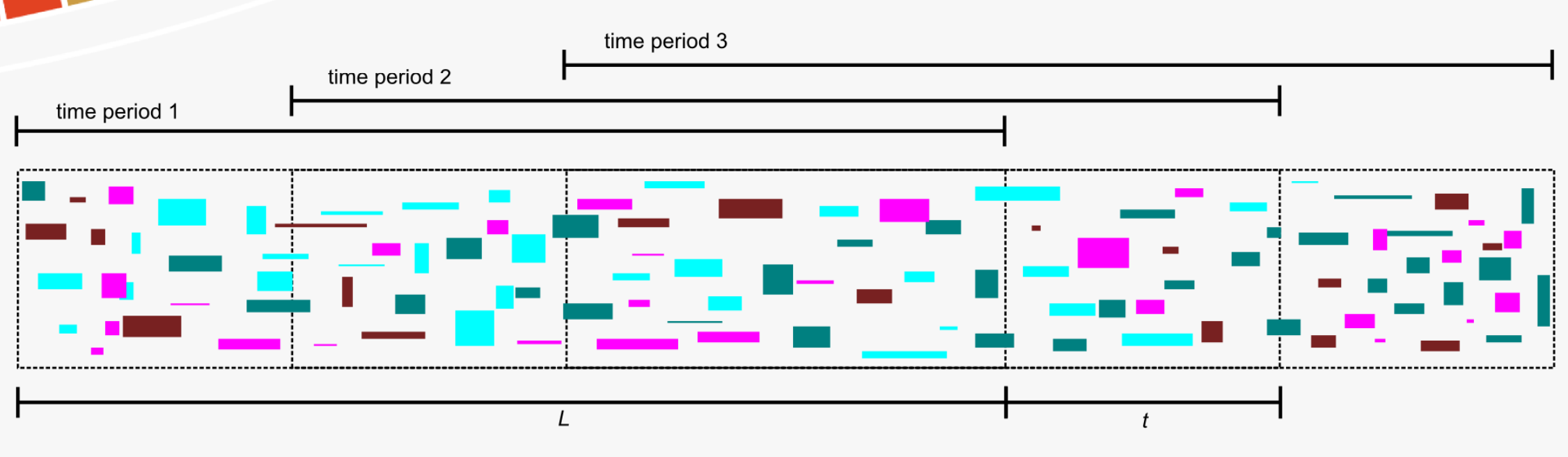
3



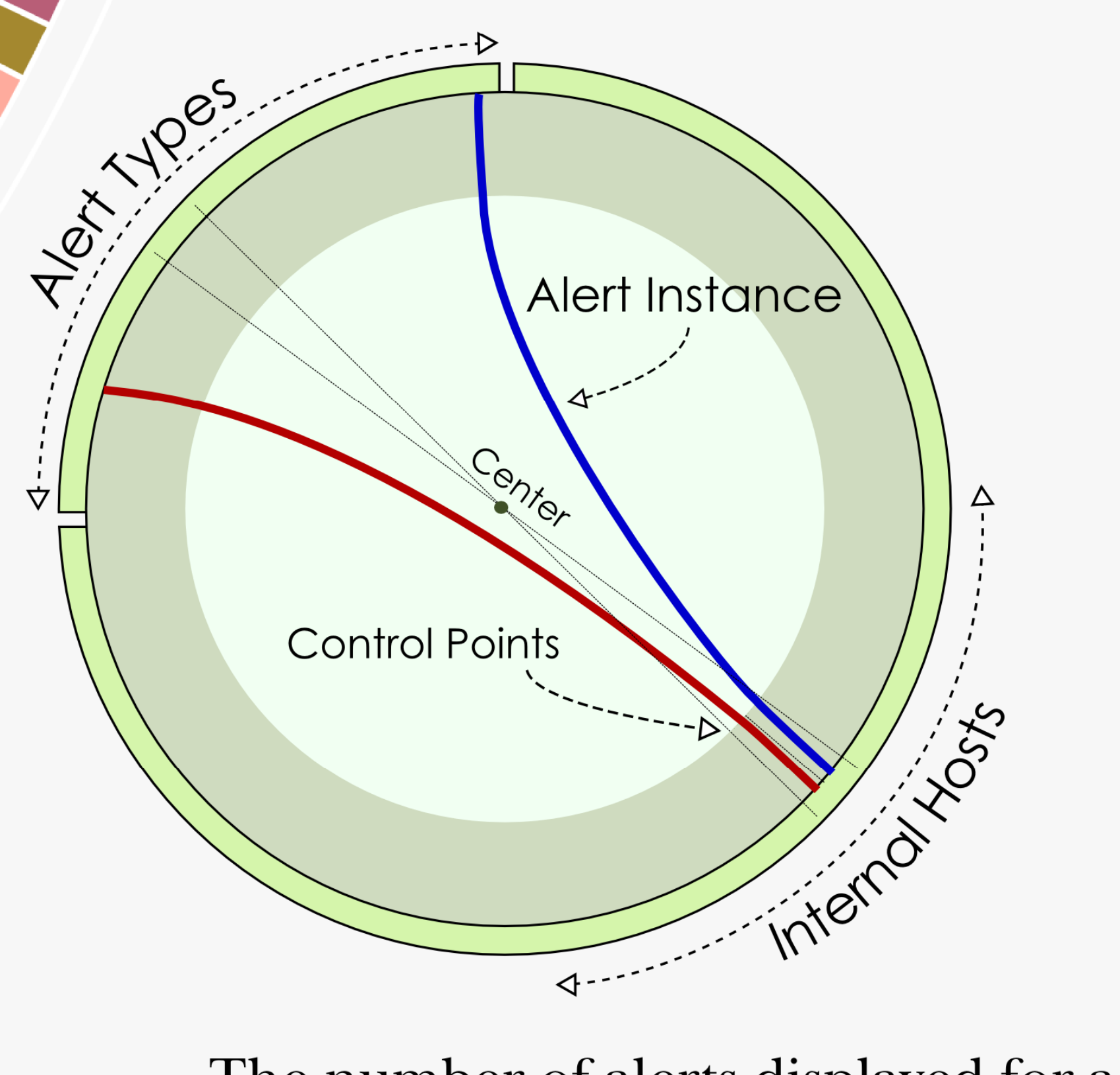
4



The greatest advantage of Avisa is its support of animation. Animation is essentially a sequence of images used to convey the illusion of movement. It can facilitate perception of change over time. In our case, animation is used not only to display transitions of one view to another, but to assist in enlightening system transitions from one state to another. In Avisa we support two methods of playback. Real-time playback and delayed playback.



The number of alerts displayed for a particular host on the host panel is constrained by a time window whose length is specified by the user. The time window is moved every user specified period of time. In this figure on left, L specifies the windows length and t specifies the update period.


Alert Types
Alert Instance
Center
Control Points
Internal Hosts