IDSPlanet: A Novel Radial Visualization of Intrusion Detection Alerts

Yang Shi
Central South University
shiyang1230@gmail.com

Yaoxue Zhang
Central South University
zyx@csu.edu.cn

Fangfang Zhou
Central South University
zff@csu.edu.cn

Ying Zhao
Central South University
zhaoying@csu.edu.cn

Guojun Wang
Central South University
csgjwang@csu.edu.cn

Ronghua Shi
Central South University
shirh@csu.edu.cn

Xing Liang
Arizona State University
xliang22@asu.edu

ABSTRACT

In this article, we present a novel radial visualization of IDS alerts, named IDSPlanet, which helps administrators identify false positives, analyze attack patterns, and understand evolving network conditions. Inspired by celestial bodies, IDSPlanet is composed of Chrono Rings, Alert Continents, and Interactive Core. These components correspond with temporal features of alert types, patterns of behavior in affected hosts, and correlations amongst alert types, attackers and targets. The visualization provides an informative picture for the status of the network. In addition, IDSPlanet offers different interactions and monitoring modes, which allow users to interact with high-interest individuals in detail as well as to explore overall pattern.

Keywords

Cyber security; IDS; Visualization.

1. INTRODUCTION

Intrusion Detection Systems (IDS) are commonly used today to assist network administrators in securing their enterprise's network. To better monitor network communication and computer system integrity, IDS are generally deployed along crucial nodes within the network system. When a pre-defined attack signature is matched, IDS produce an alert to indicate the detection of a potentially intrusive behavior. However, methods to detect attack signatures may be lacking in accuracy, precision, sensitivity. IDS may mislabel normal activities as malicious, causing false positives, or it may fail to identify malicious traffic, resulting in false negatives [6]. In addition, it is time-consuming and tedious to investigate the overwhelming number of textual alerts generated on daily basis.

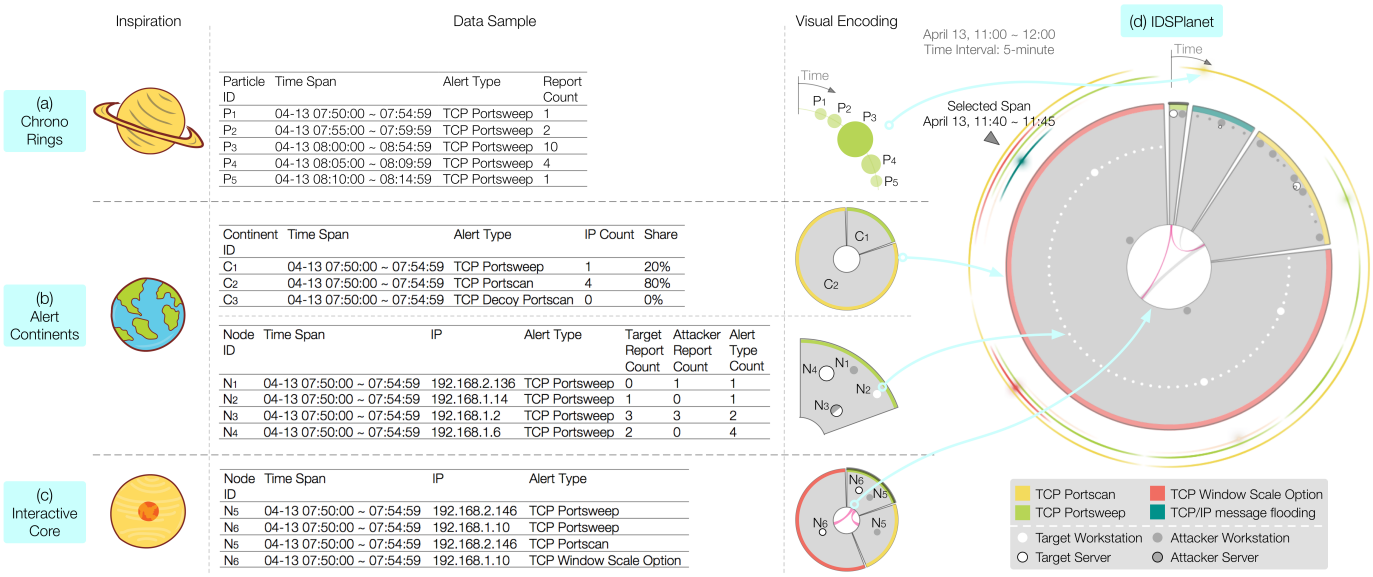
As an emerging inter-disciplinary field, visualization for network security leverages humans' perceptive and cognitive abilities to solve challenging security problems. Researchers have validated the significant contributions that can be made by visualization when used to analyze network security data and facilitate decision-making [10]. The visualization of IDS alert data, a form of network security data, has been the subject of inquiry for many domain researchers. Many visual tools [8] [1] [7] have been developed to process and visualize IDS logs. These efforts have helped reduce false positives, identify correlation among alerts, and enhance situational awareness.

Radial visualization [3] is one of the most popular methods among various IDS visualization techniques [5] [2] [11]. Its compact layout is aesthetically pleasing while being easy to read, understand, and interact with. In particular, radial visualization is a powerful tool for presenting correlations among *Where*, *When*, and *What* attributes in the network security field. VisAlert [9] proposed a radial IDS alert visualization, which mapped the *Where* of host configuration, *When* of time period, and *What* of alert type onto a visualization as a circular map surrounded by bands representing time filled with color coded alert bars. However, problems of occlusion and visual clutter arose when lines were used to display *Where-What* connections. AlertWheel [4] reduced visual clutter by designating paths along concentric circles when associating hosts with alert types. Although the cobweb-like design resulted in a neat layout, the problem of easily identifying correlation within the *Where-What* domain remained unsolved.

In the early stage of research, we developed two IDS radial visualization tools, IDSRadar [12] and NetSecRadar [13]. These two tools improve temporal representation and host configuration based on the primary visualization layout of VisAlert. Bezier curve binding is used to help better identify correlations, when compared to line binding. However, it still results in visual clutter and occlusion in a certain degree. Besides, the fixed host configuration of conventional IDS radial visualization enables quick pinpointing but does not allow for dynamic aggregation of hosts who possess

VINCI '16, September 24-26, 2016, Dallas, TX, USA

DOI: http://dx.doi.org/10.1145/2968220.2968221



Particle ID	Time Span	Alert Type	Report Count
P1	04-13 07:50:00 ~ 07:54:59	TCP Portsweep	1
P2	04-13 07:55:00 ~ 07:59:59	TCP Portsweep	2
P3	04-13 08:00:00 ~ 08:54:59	TCP Portsweep	10
P4	04-13 08:05:00 ~ 08:09:59	TCP Portsweep	4
P5	04-13 08:10:00 ~ 08:14:59	TCP Portsweep	1

Continent ID	Time Span	Alert Type	IP Count	Share
C1	04-13 07:50:00 ~ 07:54:59	TCP Portsweep	1	20%
C2	04-13 07:50:00 ~ 07:54:59	TCP Portscan	4	80%
C3	04-13 07:50:00 ~ 07:54:59	TCP Decoy Portscan	0	0%

Node ID	Time Span	IP	Alert Type	Target Report Count	Attacker Report Count	Alert Type Count
N1	04-13 07:50:00 ~ 07:54:59	192.168.2.136	TCP Portsweep	0	1	1
N2	04-13 07:50:00 ~ 07:54:59	192.168.1.14	TCP Portsweep	1	0	1
N3	04-13 07:50:00 ~ 07:54:59	192.168.1.2	TCP Portsweep	3	3	2
N4	04-13 07:50:00 ~ 07:54:59	192.168.1.6	TCP Portsweep	2	0	4

Node ID	Time Span	IP	Alert Type
N5	04-13 07:50:00 ~ 07:54:59	192.168.2.146	TCP Portsweep
N6	04-13 07:50:00 ~ 07:54:59	192.168.1.10	TCP Portsweep
N5	04-13 07:50:00 ~ 07:54:59	192.168.2.146	TCP Portscan
N6	04-13 07:50:00 ~ 07:54:59	192.168.1.10	TCP Window Scale Option

Figure 1: (a) (b) (c) Design of each visual component of IDSPlanet, including illustration of its inspiration, data sample, and visual encoding. (d) A detailed view of IDSPlanet from 11:40 to 11:45 on April 13, 2011 (time interval: 5-minute).

similar features. And more specifically, the lack of details in individual illustration makes it harder to identify correlation between hosts, e.g., which role does a host take during attack, an attacker, a target, or both? who is the target when a host acts as an attacker? Therefore, given IDS radial visualization contains both advantages and disadvantages, the design must be carefully considered and balanced.

In this article, we present IDSPlanet, an innovative radial visualization tool, which facilitates the analysis of network security and comprehension of IDS alert logs. First, IDSPlanet addresses the issues of visual occlusion and the functionality of pinpointing by replacing the line binding with container binding mechanism, in which hosts who reported the same alert types were collected. Second, IDSPlanet reinforces the capability to analyze correlation among alert types in both temporal and spatial dimensions. Third, in addition to the global monitoring perspective offered by many conventional radial visualization of IDS alerts, IDSPlanet also provides detailed view which enabled fine-grained observation of high-interest IPs. A case study was conducted to demonstrate the usability and effectiveness, as well as the both the advantages and disadvantages of our visualization.

2. VISUALIZATION DESIGN

2.1 Visualization

IDSPlanet is modeled as a celestial object with a composition similar to planets such as Earth and Saturn. The principal components includes an outermost Chrono Rings, which surround Alert Continents, and Interactive Core.

2.1.1 Chrono Rings

Inspired by the rings of Saturn, IDSPlanet possesses an orbital band which visualizes the temporal variations of alerts. Starting from the 12 O'clock position, each ring particle on the band represents an IDS alert incident. Alert incidents of the same type are gathered as a ring according to their time sequences in clockwise order and assign a unique color label. As a result, each ring represents time-varied frequency of a specific type of alert. The size and visibility of a ring particle is based on the frequency of alerts generated at a certain time interval. In other words, the visual intensity of a particle corresponds with its threat level derived from the IDS alert reports. For example, as shown in Figure 1-a, each particle represents a TCP Portsweep alert incident occurred in 5-minute, five particles are chronologically arranged as a TCP Portsweep ring and assigned a green label. A particle may expand, brighten, or even detonate if a sufficient spike in threat level is detected. These visual effects highlight the potentially malicious events and high-risk cases which users may be interested to investigate. Recognition of visual patterns along the Chrono Rings serve as a starting point for interpretation of IDS alerts. Once one or more time frames are selected, users could transition from the temporal perspective to in-depth analysis of alert incidents.

2.1.2 Alert Continents

The activity and behavior between hosts reported by different alerts is primarily visualized within IDSPlanet's Alert Continents. The Alert Continents' layer is analogous to the crust of a planet. The crust of Earth includes seven continents, with each possessing its own unique inhabitants. Drawing inspiration from the container-object relationship, IDSPlanet forms several continents according to current alert types, with each populated by IP nodes who had reported at least one incident of the continent's alert. The size of continents is based on its amount of IP nodes. Each Alert Continent along the crust receives a color label according to its alert type. The color is consistent with that of the corresponding Chrono Ring. For example, as shown in Figure 1-b-upper, the green TCP Portsweep continent and the yellow TCP Portscan continent form a planet. Based on their populations, the green continent occupies one fifth of

the circle while the yellow continent occupies four fifths of the circle.

In Alert Continent, the design focuses on host layout and visual encoding. IP nodes are placed according to the frequency of alerts, with distance between IP node and the core indicating the quantity. That is, IP nodes receives a large amount of attacks were considered more "burdened", causing it to sink toward the core. The size of an IP node shows the degree of variety among its alert types. As a result, nodes that experience a wide range of attacks are enlarged. For example, as shown in Figure 1-b-lower, N_3 who reports the highest total alerts is placed at nearest position from the core. N_4 who encounters the most alert types is represented as the biggest node. To differentiate between attacker and target of alerts, IP nodes are rendered with differing amounts of white and gray. The ratio between white and gray slices indicates the number of times a node acts as a target or source. For example, a node that's mostly white indicates an IP which has acted largely as a source of attacks (see N_1 in Figure 1-b-lower), while a node that's mostly gray represents a target of attacks (see N_2 in Figure 1-b-lower). And the server is addressed by adding black stroke (see N_3 and N_4 in Figure 1-b-lower). In summary, Alert Continents gives a spatial representation of numerous hosts report various alerts, where abnormal activity patterns of a subset of hosts could be found during visual analysis process. Combined with the individual behavior information through visual encoding of hosts, user could transition from the spatial perspective to fine-grained observation of several suspicious hosts.

2.1.3 Interactive Core

Similar to a planetary core, IDSPlanet's Interactive Core is situated as the central component of the visualization. It provides two functionalities. First, it displays correlation among hosts with various alert types. Correlation arcs linking the continents are used to indicate similarity between Alert Continents. The width of the arc depictes the percentage of identical IPs between two different alert types. For example, as shown in Figure 1-d, the IPs, 192.168.2.146 and 192.168.1.10, each reports two types of alerts. When the green TCP Portsweep Alert Continent is selected, pink correlation curves show that 50% of its IPs are identical to that in yellow TCP Portscan continent, and the other 50% is identical to that in the red TCP Window Scale Option continent. The curves travers across planet core along the shortest paths with minimal overlapping. The design is based on the consideration that a minimalist representation allows for simpler and more direct recognition of correlations between different alert types.

Second, Interactive Core allows fine-grained monitoring of suspicious servers and hosts as well as other crucial nodes. When users encounter multiple suspicious IPs, the core is used as a detailed view and acts as a monitoring station. For example, when an IP is placed in Interactive Core at selected time span, IDSPlanet switches to individual analysis mode of this IP node. Two types of attack are found relevant to this IP, IP 192.168.2.143 acts as a source of TCP Portsweep attack targeted IP 192.168.1.4 while IP 192.168.1.6 is the target of TCP Portscan attack initiated by IP 192.168.1.4. The transmission flows are depicted as flow arcs; pink input flow arc and grey output flow arc. Interactive Core allows in-depth observation and analysis of important individuals, offering users with the options to review alert incidents from multiple perspectives.

2.2 Interaction

IDSPlanet provides rich interactions, among which we address several customized interactions in details. These interactions enable users to obtain comprehension of threat detection and anomaly awareness.

Time Refinement. We offer time control with multiple resolutions. In our case study, we use 60-minute intervals for coarse-grained analysis and 5-minute intervals for fine-grained analysis as complements to each other. When the IDS log data is first loaded, users may tend to observe the overall trend over the entire time series. 60-minute granularity supports general observation. When a more detailed look into specific time point is required, 5-minute granularity allows for detailed analysis. Time refinement not only extends the utility of the Chrono Rings, but also better represents the differing temporal fluctuation on different time scales.

Alert Type Sorting. Since the order of alert types on the Chrono Rings and Alert Continents have a significant impact on pattern recognition, we provide options to sort them according to specific measures, i.e., incident time, IP quantity, and Pearson product-moment correlation coefficient (PPMCC). For example, when set to incident time option, the first incident reports took its position on the top of the IDSPlanet, at 12 O'clock. Other two types are explained in the following case studies. Sorting enables users to find different features such as trends, similarities, and periodicities in the IDS alerts.

IP Identification. When utilizing the container binding mechanism, a single IP reports multiple alert types necessitated multiple placements on different Alert Continents. Considering this dynamic representation of host configuration, IP Identification is used to quickly pinpoint and isolate a specific IP address. Users can hover their mouse over an IP, causing other instances of it in other continents to be highlighted. In addition, if users hover the mouse over an Alert Continent, correlation arcs showing the percentage of mutual IPs between these and other types would be highlighted. IP Identification enables the comparison of the actions of an IP taking part in various alerts, thus giving further insight into its role and behavior.

3. CASE STUDY

In the following, we demonstrates the usability and effectiveness of IDSPlanet through a user case study. The data consistes of the Snort IDS logs provided by the IEEE VAST Challenge in 2011 [12].

We visualize the IDS logs from a corporate network of a major shipping company from April 13, 2011 to April 15, 2011, including 8 alert types and about 20,000 alert records. Figure 2-a shows a global view of IDSPlanet. The alert types are sorted according to IP quantity. The alert type with the least incidences is represented by the innermost Chrono Ring, followed by successive outer rings of increasing quantity. In Alert Continents, the smallest continent is placed in the 12 O'clock position, with progressively ascending continent sizes in clockwise order.

We focus on analyzing visual patterns from the three largest Alert Continents, which contains the most of IPs. The Chrono Rings show that the yellow TCP Portscan

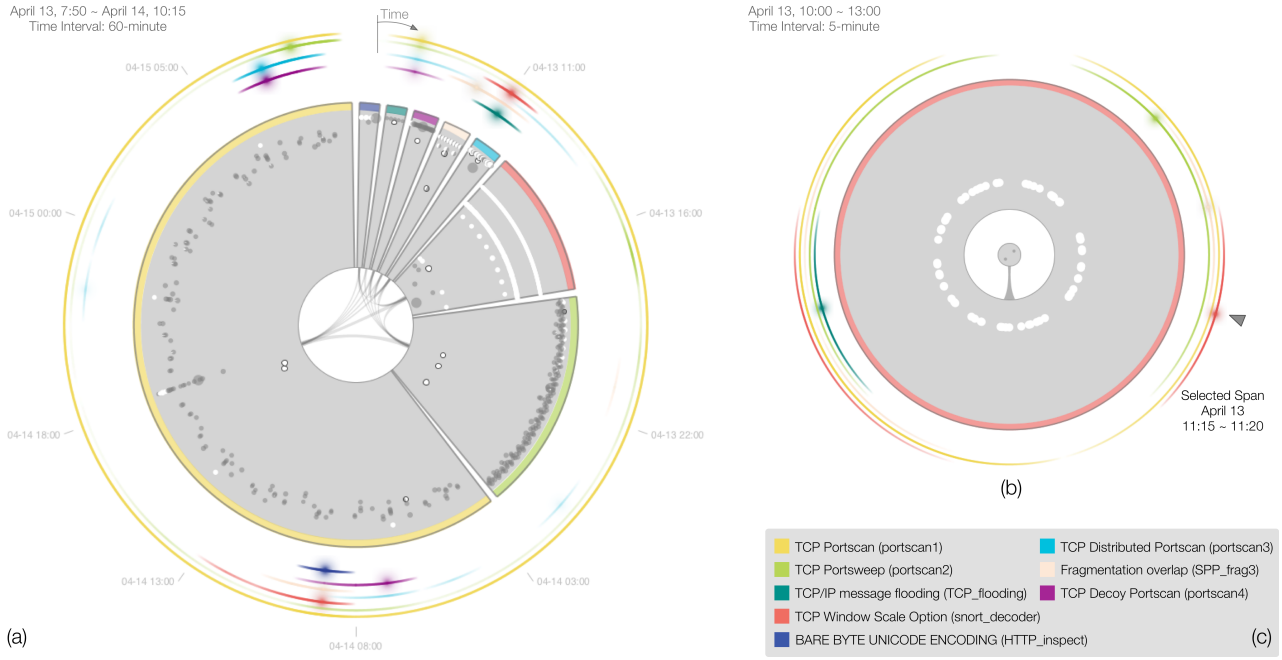


Figure 2: (a) A global view from April 13, 2011 7:50 to April 15, 2011 10:15 (time interval: 60-minute). (b) A detailed view of IP 192.168.2.171 and IP 192.168.2.173 from 11:15 to 11:20 on April 13 (time interval: 5-minute). (c) A legend of color encoding of alert types, including its names and abbreviations.

(Alert types are henceforth referred to with their colors and abbreviation, as shown in Figure 2-c) and green portscan2 persist for long durations over regular periods. The red snort_decoder occurs only in two time periods, accompanied with two detonations along the ring. This indicates a sudden increase of alert reports, which requires additional investigation. Using this temporal pattern, we decide to focus on the red snort_decoder alerts in the following exploration of the spatial features.

For the Alert Continents, we pay attention to the distribution of hosts. We find that the alert types of yellow portscan1 and green portscan2 possess many similarities. For example, they both feature a larger number of attackers, depicted as gray nodes, than targets, depicted as white nodes. In terms of the roles in attacks, several server IPs, display as white nodes with black strokes, appear near the core, indicating that they are the main targets of a distributed attack from a large number of sources. In the red Alert Continent, a pattern emerges where all the white nodes, which are targets of an attack, have been separated into four layers. IP nodes in the same layer keep the same distance to the center, suggesting that they receive an identical amount of attacks. The attacker IPs are those few gray nodes placed near the center. This highly structured attack pattern in a large amount of nodes implies a planned attack and called for further monitoring.

We transition to the fine-grain view and observed the alerts from 11:15 to 11:20 on April 13, when the initial burst of activity occurs. We find that a huge amount of workstations is attacked by five hosts which share similar behavior patterns. We then place two of the low-variety attackers, IP 192.168.2.171 and IP 192.168.2.173, into the Interactive Core to investigate their individual behaviors. As shown in Figure 2-b, we find that these two IPs are responsible for only red snort_decoder attacks. And the pattern of their targets which are all placed equidistantly from the core implied they attacked each target using identical strategies. From this observation, we draw the conclusion that the two IPs investigated may have been malicious because it attacks each of its many targets a fixed number of times.

In summary, yellow portscan1 and green portscan2 have a higher chance of containing false positives according to its patterns of continuous randomized alerts and concentrated list of targets. Due to inappropriate configuration of attack signatures, IDS may have marked normal communication between workstations and servers as threats or risks. On the other hand, red snort_decoder shows symptoms of a malicious targeted attack (e.g., worm) based on the observation of its sudden onset, high structured alert pattern, and regular attack distribution.

4. CONCLUSION

The article presents a novel radial visualization, IDSPlanet, which supports network administrators in obtaining insights into large logs of alerts generated by IDS. First, it optimizes the advantages of radial visualization in being aesthetically concise, highly interactive, and accurately portrayed correlation between *What, When, Where* attributes during network security analysis. Next, IDSPlanet replaces line binding with container binding, which not only minimizes visual clutter but also improved identification of relations in the *Where-What* domain. Lastly, IDSPlanet combines dynamic host layout and strategic monitor design in radial visualization, providing richer interactions, visual patterns and analysis perspectives.

Acknowledgment

This work is supported by the National Natural Science Foundation of China under Grant No. 61402540, 61272024.

5. REFERENCES

[1] K. Abdullah, C. Lee, G. Conti, J. A. Copeland, and J. Stasko. Ids rainstorm: Visualizing ids alarms. 2005.

[2] E. Bertini, P. Hertzog, and D. Lalanne. Spiralview: towards security policies assessment through visual correlation of network resources with evolution of alarms. In *Visual Analytics Science and Technology, 2007. VAST 2007. IEEE Symposium on*, pages 139–146. IEEE, 2007.

[3] G. M. Draper, Y. Livnat, and R. F. Riesenfeld. A survey of radial methods for information visualization. *Visualization and Computer Graphics, IEEE Transactions on*, 15(5):759–776, 2009.

[4] M. Dumas, J.-M. Robert, and M. J. McGuffin. Alertwheel: radial bipartite graph visualization applied to intrusion detection system alerts. *Network, IEEE*, 26(6):12–18, 2012.

[5] R. F. Erbacher, K. Christensen, and A. Sundberg. Designing visualization capabilities for ids challenges. In *Visualization for Computer Security, 2005.(VizSEC 05). IEEE Workshop on*, pages 121–127. IEEE, 2005.

[6] C.-Y. Ho, Y.-D. Lin, Y.-C. Lai, I.-W. Chen, F.-Y. Wang, and W.-H. Tai. False positives and negatives from real traffic with intrusion detection/prevention systems. *International Journal of Future Computer and Communication*, 1(2):87, 2012.

[7] D. Keim, F. Mansmann, J. Schneidewind, T. Schreck, et al. Monitoring network traffic with radial traffic analyzer. In *Visual Analytics Science And Technology, 2006 IEEE Symposium On*, pages 123–128. IEEE, 2006.

[8] H. Koike and K. Ohno. Snortview: visualization system of snort logs. In *Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security*, pages 143–147. ACM, 2004.

[9] Y. Livnat, J. Agutter, S. Moon, R. F. Erbacher, and S. Foresti. A visualization paradigm for network intrusion detection. In *Information Assurance Workshop, 2005. IAW'05. Proceedings from the Sixth Annual IEEE SMC*, pages 92–99. IEEE, 2005.

[10] H. Shiravi, A. Shiravi, A. Ghorbani, et al. A survey of visualization systems for network security. *Visualization and Computer Graphics, IEEE Transactions on*, 18(8):1313–1329, 2012.

[11] H. Shiravi, A. Shiravi, and A. A. Ghorbani. Ids alert visualization and monitoring through heuristic host selection. In *Information and Communications Security*, pages 445–458. Springer, 2010.

[12] Y. Zhao, F. Zhou, X. Fan, X. Liang, and Y. Liu. Idsradar: a real-time visualization framework for ids alerts. *Science China Information Sciences*, 56(8):1–12, 2013.

[13] F. Zhou, R. Shi, Y. Zhao, Y. Huang, and X. Liang. Netsecradar: A visualization system for network security situational awareness. In *Cyberspace Safety and Security*, pages 403–416. Springer, 2013.