VISUALIZATION OF CYBERSECURITY PROCESSES THROUGH GRAPHICAL USER INTERFACE DESIGN

Saburova Shohista Shavkat qizi
Master's Student, Faculty of Television Technologies, Computer Graphics and Design, TUIT
Saburova Sarvara Shavkat qizi
Student of the Faculty of Computer Engineering, TUIT
Omonova Parvina Sayfiddin kizi
Trainee Lecturer, Department of Television and Media Technologies, TUIT

Abstract: *This paper examines the application of graphic design principles in building interfaces for cybersecurity management systems. The key visualization components are analyzed: dashboards, interactive network activity graphs, and color-coded alert schemes. The study demonstrates that a well-designed GUI reduces the cognitive load on security operators, shortens incident response time, and minimizes the probability of human error.*

Keywords: *cybersecurity, graphical user interface, GUI, threat visualization, dashboard, UX design, security monitoring.*

The growing volume of cyberattacks and the increasing complexity of network infrastructures place heightened demands on security management tools. Security Operations Center (SOC) analysts process thousands of security events daily, and their effectiveness directly depends on the quality of the interface through which this information is presented.

Traditional systems based on text logs and command-line interfaces have a significant drawback: human perception processes visual information far more efficiently than unstructured text. This paper analyzes GUI design principles oriented toward cybersecurity tasks, with an emphasis on visualization as a primary tool for improving management effectiveness.

Effective dashboards are built on several interconnected design principles. Information hierarchy ensures that critical threats are visually emphasized and positioned at the top of the screen, while secondary data occupies the periphery. Minimalism reduces cognitive load by eliminating unnecessary interface elements that slow decision-making. Consistency, achieved through a unified color system (red for critical threats, yellow for warnings, green for normal status), allows operators to assess system state at a glance, without reading text labels.

Graphical representation of network traffic is one of the most informative elements of a cybersecurity interface. Interactive node-link graphs allow operators to visually identify anomalous patterns, such as a sudden spike in connections to a single node characteristic of DDoS attacks, or unusual outbound connections indicative of potential data exfiltration. Heatmaps complement this by displaying the geographic distribution of threats and the temporal dynamics of attacks, while animated timelines enable analysts to replay the sequence of events during an incident, significantly simplifying the investigation process.

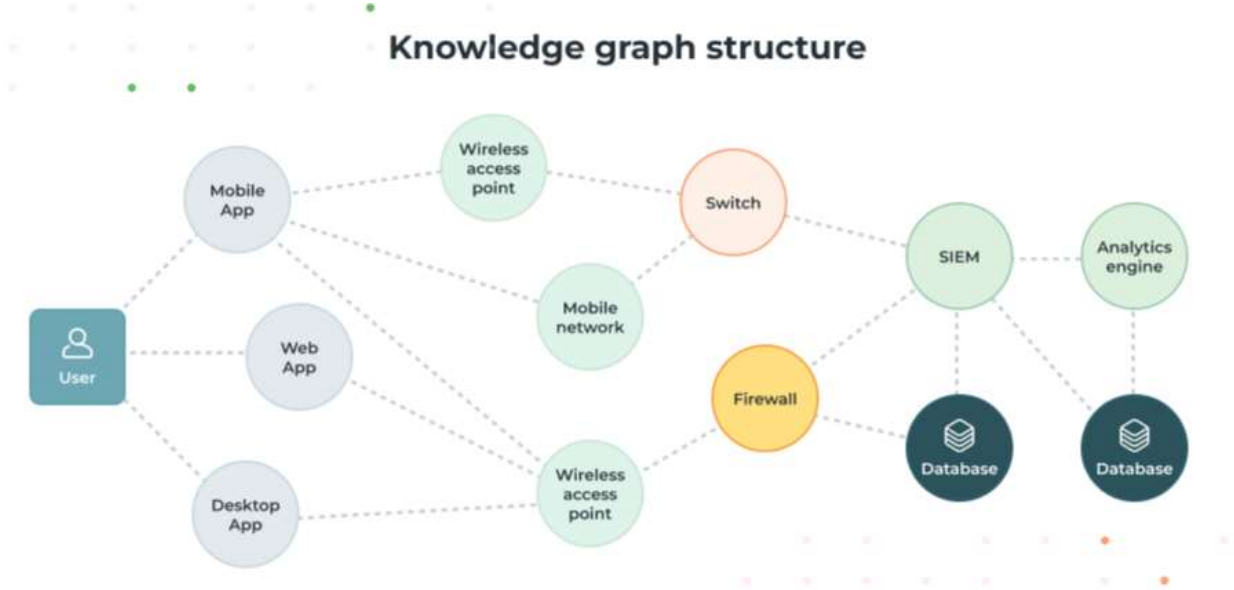

Fig. 1. Example of a node-link graph for network infrastructure visualization

In security interfaces, color serves a functional rather than decorative purpose. UX research indicates that semantically grounded color coding reduces threat identification time by 30–40% compared to monochrome interfaces. Accessibility must also be considered, as approximately 8% of men have some form of color vision deficiency, which requires that color signals be supplemented with shape or texture cues.

Typography also affects perceptual efficiency: monospaced fonts such as JetBrains Mono are optimal for displaying IP addresses and event codes, while readable proportional typefaces are preferable for analytical text blocks.

Table 1. Comparative analysis of visualization methods in cybersecurity GUI

Visualization Method	Advantages	Limitations
Dashboard (KPI Panel)	Instant system status overview; high configurability	Risk of information overload with large numbers of metrics
Network Graph	Clear visualization of topology and anomalous patterns	Becomes unreadable at high node density
Heatmap	Effective display of temporal and	Requires interpretation not

Visualization Method	Advantages	Limitations
	geographic threat dynamics	immediately intuitive for new users
Color-Coded Alerts	Instant prioritization without reading text	Accessibility issues for users with color vision deficiency

CONCLUSION

The analysis demonstrates that the quality of the graphical interface is a defining factor in the effectiveness of cybersecurity management systems. A well-designed GUI, built on the principles of information hierarchy, functional color coding, and interactive visualization of network data, can substantially reduce threat detection time and decrease the cognitive burden on security operators.

A promising direction for future research is the development of adaptive interfaces capable of automatically restructuring the visual layout in response to the current threat level and the specific profile of each operator.

REFERENCES:

1. Chung M.-H., Yang Y., Wang L. et al. Enhancing cybersecurity situation awareness through visualization: A USB data exfiltration case study // Heliyon. — 2023.
2. Shiravi H., Shiravi A., Ghorbani A.A. A Survey of Visualization Systems for Network Security // IEEE Transactions on Visualization and Computer Graphics. — 2012.
3. Few S. Information Dashboard Design: Displaying Data for At-a-Glance Monitoring. — 2nd ed. — Burlingame: Analytics Press, 2013.
4. Ware C. Information Visualization: Perception for Design. — 4th ed. — Cambridge: Morgan Kaufmann, 2021.