EAI Endorsed Transactions
on Industrial Networks and Intelligent Systems
Research Article EAI.EU

SIMURG: Strategic intelligent framework for real-time 3D visualization and high-altitude analysis of global cyber threats

Resul Das[1,2], Muhammed Onur Kaya[1]

[1]Firat University, Faculty of Technology, Department of Software Engineering, 23119 Elazig, Türkiye
[2]Edinburgh Napier University, School of Computing, Engineering & The Built Environment, Department of Cyber Security and System Engineering, Edinburgh, Scotland, United Kingdom

Abstract

The increasing volume and variety of cyber threats on a global scale make it difficult for security analysts to provide real-time situational awareness, pointing out the inadequacy of traditional two-dimensional (2D) visualization approaches. This study proposes SIMURG (Strategic Intelligent Monitoring and Unified Response Graph), a web-based and hardware-independent three-dimensional (3D) visualization system aimed at analyzing global cyber threats in real-time and intuitively. Named after the legendary bird of Turkic mythology to symbolize a sovereign, high-altitude perspective over the digital landscape, the system translates this metaphorical wisdom into a holistic monitoring framework. The system collects and processes cyber threat intelligence and OSINT-based data streams together with their timestamps, and visualizes source-target relationships, attack density, and geographic distributions on an interactive WebGL-based 3D globe. To support situational awareness, threat information is represented using multiple visual attributes, including color, height, and object size. Experimental evaluations indicate that SIMURG maintains an average rendering performance of 43.5 frames per second (FPS) while displaying 3,504 active nodes and up to 1,752 simultaneous attacks. When operating in batch analysis mode, supported by dedicated optimization algorithms, the refresh rate exceeds 144 FPS. In addition, analyses conducted on six months of historical data show that the system can reveal recurring temporal patterns in cyber threats and provide useful insights for operational decision-making.

Received on 19 April 2026; accepted on 19 May 2026; published on 07 July 2026

Keywords: Cyber Attack, Cyber Threat Visualization, WebGL Visualization, Cyber Threat Intelligence, Real-Time Visualization, Situational Awareness

doi:10.4108/eetinis.13.12740

1. Introduction

Today, cyberspace presents a wide and complex range of threats, from critical infrastructure to individual data. The proliferation of technologies such as the Internet of Things (IoT), cloud and edge computing (fog computing), 5G/6G communication infrastructures, and Software Defined Networking (SDN) has led to a significant increase in network traffic, both in volume and heterogeneity [1, 2]. This enables cybercriminals to develop various attack methods and devise sophisticated strategies that can circumvent traditional security systems. Attacks, particularly Distributed Denial of Service (DDoS) and Advanced Persistent Threats (APT) attacks, cause significant financial losses and reputational damage for organizations [3, 4].

Strategic Intelligent Monitoring and Unified Response Graph (SIMURG) is named after the legendary bird of Turkic and Eastern mythology, symbolizing a sovereign entity that observes the world from the highest peaks with profound wisdom and an all-encompassing gaze. The proposed system translates this ancient metaphorical perspective into the digital

*Corresponding author. E-mail: rdas@firat.edu.tr

realm by providing a high-altitude, holistic view of global cyber threats, enabling security analysts to discern intricate attack patterns and hidden anomalies with unprecedented clarity. In the era of big data, one of the most significant challenges faced by cybersecurity professionals is the ability to analyze extensive log data and network traffic in real-time [5]. Text-based log records and static reports are insufficient for monitoring the international scale and spread of attacks in real time. This is where the concept of Cyber Situational Awareness (CSA) becomes crucial. CSA is the process of detecting anomalies on the network, visualizing threats, and providing intelligence that allows decision-makers to act quickly [6]. In line with this need, this study, prepared for real-time monitoring and analysis of global cyber threats, introduces a three-dimensional visualization system called SIMURG. SIMURG combines Open Source Intelligence (OSINT) data, GeoIP location services, and high-quality Web Graphics Library (WebGL)-supported graphics to simulate cyber attacks on an interactive globe. In this study, the term "intelligent" does not refer to machine learning or autonomous AI agents; it denotes the platform's built-in analytical automation, including rule-based semantic classification, context-aware target mapping, dynamic risk scoring, and heuristic event prioritization for analyst decision support.

SIMURG is designed primarily for CTI-driven strategic cyber situational awareness rather than autonomous intrusion prevention. Its target users are SOC analysts, CTI researchers, and security decision-makers who monitor global OTX-derived threat trends, prioritize events, and communicate situational context. The platform supports operational monitoring (night mode) and academic/forensic reporting (day mode), but it does not replace SIEM/IDS validation pipelines; visualized arcs, severity labels, and recommended actions are decision-support outputs that require analyst confirmation.

1.1. Problem Statement

Today, as the number and complexity of cyber threats rapidly increase, Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM) systems generate vast amounts of data [7]. However, current techniques used in presenting this data create a bottleneck that challenges human perception. Many security tools still present data through line-based text records or static two-dimensional graphs, leading to the loss of important patterns in large datasets amidst the noise. These shortcomings in how data is represented, rather than in the data itself, bring about the following key operational challenges:

- Integrating and correlating thousands of log entries imposes a substantial cognitive load on human operators, often resulting in alarm fatigue among security analysts [8].
- The potential of visual elements such as color, height, and size is not fully utilized in current interfaces. Attack severity or intensity is typically represented through numerical indicators alone, neglecting perceptual dimensions such as three-dimensional spatial encoding and color depth, which could enable experts to rapidly and intuitively assess the scale of a threat.
- It is difficult to track the geographical and geopolitical connections between the source and target of an attack through standard two-dimensional maps or lists [9].
- Most current visualization tools suffer from performance loss or cause delays in the visualization process when processing live data streams [10].
- During intense DDoS attacks, the screen becomes overloaded with data points, rendering the visualization unreadable and making analysis impossible.

Beyond these technical challenges, the biggest shortcomings in academic resources are accessibility and comprehensibility [11, 12]. The highly technical terminology employed by existing tools hinders decision-makers' ability to accurately interpret the scale of cyber threats, while the widespread adoption of dark-mode interface designs adversely affects the readability of academic and written reports. In short, it is noteworthy that the literature lacks hybrid methods that both support high-quality real-time visualization and enhance reporting capabilities for users at all levels [13].

1.2. Main Contributions

This research offers innovative solutions to problems encountered in the field of cybersecurity visualization, such as big data fatigue, low state awareness, and performance bottlenecks. The main contributions of the SIMURG platform, developed to address the limitations mentioned in the Problem Statement section, are summarized below:

- To solve the latency problem experienced by existing online visualization tools in real-time data streams, a lightweight architecture has been created that combines group processing-oriented algorithms with a WebGL-based rendering infrastructure. The proposed method offers real-time visualization with fast response time and high frame rate without the need for an extra plugin.
- To overcome the limited perspective offered by two-dimensional maps, an integrated visual language has been developed that integrates attack

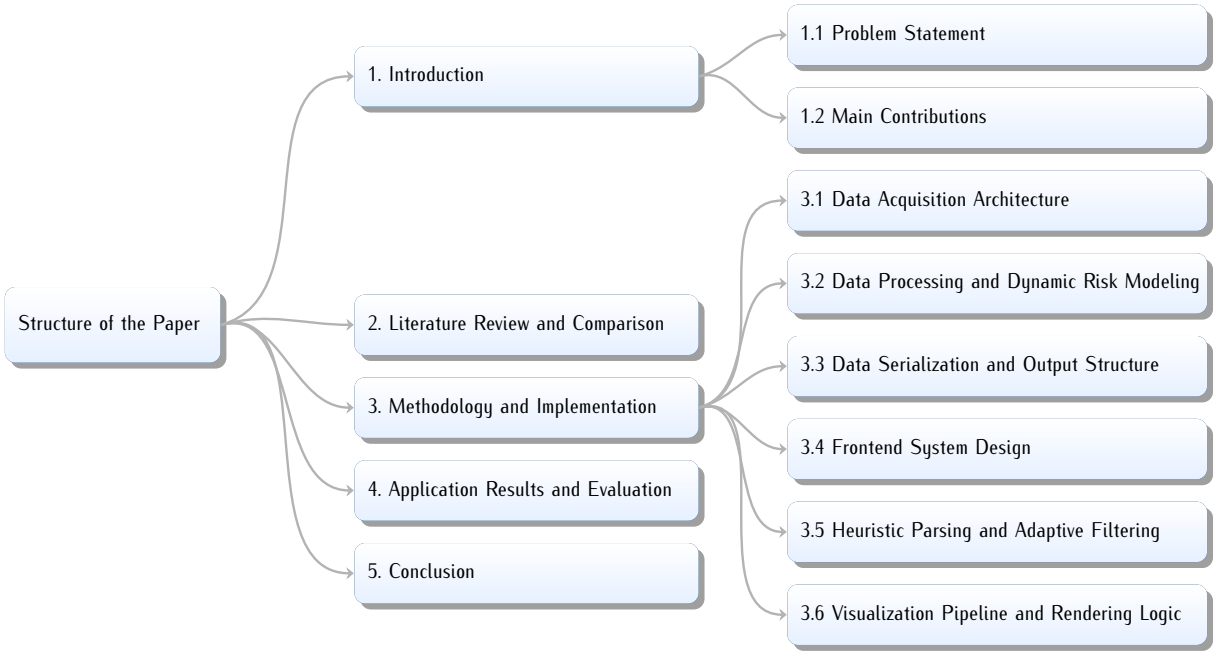

Figure 1. Organization of the paper

scope (V_{mag}) and strength with visual encodings based on height and background geometry. This method allows even stakeholders without technical knowledge to intuitively understand the magnitude and trends of cyber threats.

- The created Rule-Based Semantic Classifier automatically structures raw OTX text into a predefined visualization taxonomy and supports consistent attack-type grouping for situational-awareness display [14].
- To reduce alarm overload for Security Operations Centers (SOC) operators, this study goes beyond the dark-mode-oriented interfaces commonly adopted in the literature by proposing a dual-state semiotic mapping approach built on a dynamic Cascading Style Sheets (CSS) architecture, which offers a neon-contrast night mode for operational monitoring and a highly readable day mode for academic and forensic reporting.
- If real-time data streaming is unavailable due to Application Programming Interface (API) limitations, threat data from the AlienVault Open Threat Exchange (OTX) platform is analyzed using historical records [15]. Thus, the system can assess threat trends based on historical data.

This study provides a technical infrastructure for the real-time and intuitive visualization of high-volume cybersecurity data, as well as a holistic design proposal that considers the cognitive requirements of different user profiles (e.g., SOC operators, analysts, and decision-makers). The proposed contributions offer a more scalable and sustainable solution for identifying, interpreting, and reporting cyber threats compared to existing methods.

The rest of the article is structured as follows, as schematized in Figure 1. Section 2 presents the current literature in the field of cybersecurity visualization, relevant studies, and a comparative analysis of these studies. Section 3 details the data collection architecture, dynamic risk modeling processes, and WebGL-based visualization algorithms of the proposed SIMURG platform. Section 4 discusses the real-time performance tests of the developed system, its visual outputs under different attack scenarios, and its operational efficiency. Finally, Section 5 summarizes the results obtained from the study and offers suggestions for future studies.

2. Literature Review and Comparison

At the heart of enhancing the resilience of information systems lies the timely identification and effective prevention of cyber threats. As network traffic increases and becomes more complex, it becomes increasingly difficult for security professionals to analyze gross data [23, 24]. Therefore, data visualization methods play a crucial role in detecting anomalies by leveraging the pattern recognition ability of human perception. Recent

Table 1. Comparison of cyber threat visualization studies with SIMURG

Ref.	Technology	Objective	Method	Analysis and Findings
[16]	3D Mixed Reality	Enhancing communication and situational awareness of cyber teams.	Network topology was visualized using 3D mixed reality to support decision-making and readiness analysis.	The group using 3D mixed reality demonstrated higher shared cyber situational awareness and communication performance compared to the 2D group.
[17]	Virtual Reality	Providing situational awareness for SOC operators.	A virtual reality-based monitoring environment was evaluated in a pilot user study against non-VR conditions.	Virtual reality showed promising improvements in cyber situational awareness, especially for overall data perception; findings were reported with limitations due to modest sample size and pilot scope.
[18]	Dashboard-Based Security Visualization	Improving situational awareness for USB data exfiltration monitoring.	Three interoperable dashboards were developed via a co-design process with multiple stakeholders and assessed with usage and acceptance metrics.	The approach increased visibility into anomalous USB transfer behavior and supported practical investigation workflows; adoption indicators were evaluated using usability feedback and TAM-based measures.
[19]	CyCOP Framework	Designing real-time cyber situational awareness.	Response times of user interfaces, symbols, and visual objects were measured.	Interface and object symbol design, along with speed criteria, were proposed for rapid cyber situational awareness; real-time visualization performance was evaluated.
[20]	Web-Based Visual Analysis	Identifying abnormal network traffic patterns.	A coordinated multi-view web system used DWT feature extraction and uncertainty quantification on CIC-IDS2017 data.	Case studies identified abnormal attack patterns effectively; however, global CTI-based globe-scale threat mapping was not addressed.
[21]	3D Interactive Visualization	Improving the analyzability of intrusion detection system outputs.	Machine learning-based intrusion detection data were interactively visualized in 3D space.	3D visualization enabled faster and more intuitive understanding of attack patterns in high-dimensional intrusion detection data; however, a global and real-time cyber threat context was not provided.
[22]	Cyber Threat Intelligence Pipeline, 2D Visualization	End-to-end management of cyber threat intelligence data.	A methodological framework covering collection, preprocessing, analysis, and visualization of cyber threat intelligence data was proposed.	Visualization was shown to support analyst decision-making in cyber threat intelligence processes; however, the lack of real-time and global-scale 3D cyber threat visualization was emphasized.
SIMURG	**WebGL, CTI/OSINT**	**Real-time global cyber threat situational awareness.**	**CTI-based threat streams were interactively visualized on a web-based 3D globe with source–target relationships and temporal intensities.**	**By providing hardware-independent, real-time, and global-scale 3D cyber threat awareness, a visual analytics platform is presented that overcomes the limitations of existing 2D and static approaches.**

research reveals a shift, particularly from static 2D graphics to dynamic and interactive 3D spaces. [20, 25].

Shiravi et al., researching traditional visualization methods, meticulously examined the advantages and disadvantages of various visualization techniques and categorized network security visualizations into five main categories [26]. They also presented a detailed taxonomy by classifying visualization solutions based on use cases such as server/host monitoring, port activity, and attack patterns. Sharafaldin et al. further deepened this area by establishing evaluation criteria to compare proposed visualization systems and presenting a comparison of their performance and interaction features [23]. Ahmad et al. surveyed immersive cyber situational awareness systems and classified how VR, AR, and MR

techniques affect perception, comprehension, and projection; they emphasized interaction design and visual density as key factors [27]. Cobilean et al. reviewed visualization workflows for cyber-physical security with a smart grid case study and emphasized that data acquisition, processing, tool configuration, and interaction must be designed holistically; they reported that no single visualization method satisfies all operational requirements [28].

Web-based and interactive solution proposals are increasingly common in the literature. The system developed by Jeong et al., also summarized in Table 1, presents a coordinated multi-view web visualization system that integrates DWT-based feature extraction and uncertainty quantification to support continuous visual analysis of network traffic data [20]. Such methods are important for exploratory analysis of high-volume traffic data. Some studies explore the combination of visualization with multi-scale analyses and signal processing techniques; for example, multi-layered analysis based on Discrete Wavelet Transform has been used to better distinguish attack patterns [29]. In parallel, 3D and mixed-reality approaches provide analysts with enhanced spatial context for communicating cyber events. The experimental study by Ask et al. reported improved shared cyber situational awareness and communication outcomes in the 3D mixed-reality condition compared with a 2D setting [16]. Visualization and machine learning are also increasingly integrated in network security analytics. Studies such as Bendiab et al. and Zong et al. show how visual representations can support interpretation of model outputs and intrusion patterns in complex datasets [21, 30]. In cyber threat intelligence workflows, end-to-end frameworks further combine collection, preprocessing, analysis, and visualization stages to improve analyst decision support [22].

In summary, studies in the existing literature are either performance-oriented and lack visual aesthetics or are visually rich but lack real-time data processing capabilities. Table 1 is restricted to directly comparable, implemented, or experimentally evaluated visualization studies; surveys, reviews, foundational taxonomies, and related research articles addressing complementary or narrower problem settings are discussed in the narrative to provide a broader methodological context. Table 1 presents a comparison of these studies in terms of key features. In contrast, the SIMURG platform effectively fills this gap by offering both high-performance real-time data processing and intuitive and interactive visualization capabilities.

3. Methodology and Implementation

This section details the data processing architecture underlying the SIMURG platform, the structural characteristics of data sources, and the proposed dynamic risk calculation methods. SIMURG is defined as a strategic visualization framework that embodies the high-altitude, all-encompassing gaze of the legendary bird from Turkic mythology. The system functions by mapping real-time cyber attack vectors onto a dynamic 3D globe, utilizing distinct color gradients and multi-dimensional visual variables to represent source-target relationships and attack types across international borders. It also examines the end-to-end data processing process, from raw data collection to the WebGL-supported three-dimensional visualization interface, as well as the system's real-time decision-making support mechanisms. In this research, physics-based rendering algorithms and adaptive interface modes, developed to enhance analysts' situational awareness, are evaluated within the framework of the system's holistic structure.

3.1. Data Acquisition Architecture

For real-time cyber threat simulation, the diversity and reliability of data sources play a vital role [31, 32]. In this research, OTX, the world's largest crowdsourced threat intelligence network, was selected as the primary data source. The continuously updated and dynamic threat indicators provided by the platform ensure that the simulation environment remains sensitive to constantly changing attack methods.

The data collection system interacts with the OTX API endpoints thanks to a custom engine developed in Python. The dataset consists of two main structures in the OTX format, named "Pulse" and "Indicator" [33]:

1. *Pulse:* It is a metadata set that aggregates related threats (for example, the activity of a specific ransomware campaign or APT group) [34].

2. *Indicator of Compromise (IoC):* Technical evidence includes Internet Protocol (IP) addresses belonging to the attackers, hashes of malicious files, or domain names [35].

The system queries IPv4-based indicators with high reliability scores for the last 'x' days using the 'OTXv2' library. The structural characteristics of the raw dataset are presented in Table 2. For Experiment-I, x=30 days. Data were acquired via an on-demand OTXv2.getsince(since_timestamp) call, retaining records with type=IPv4 indicators and high reliability scores, and resolvable GeoLite2-City coordinates; records with missing coordinates or required metadata were discarded during preprocessing. The measured 30-day acquisition run retrieved 169 pulses and 9,175 IoCs; 8,980 non-IPv4 indicators were excluded. As no

duplicate records were identified in the Experiment-I pull, duplicate removal was not performed at the ETL stage; in Experiment-II, by contrast, repeated records were removed during preprocessing where present. A total of 358 valid IPv4 records (0.30 MB) were exported for evaluation.

Table 2. Attributes and data types of the OTX raw dataset

Data Field	Data Type	Description
`pulse_id`	String (UUID)	Unique identifier of the threat event
`indicator`	String (IPv4)	IP address of the attacker
`adversary`	String	Identified threat group (e.g., Lazarus, APT28)
`targeted_countries`	List<String>	Geopolitically targeted ISO country codes
`tags`	List<String>	Contextual tags (e.g., *log4j*, *ransomware*)
`created`	ISO 8601 Date	Timestamp of the initial report

While the dataset obtained via API provides a comprehensive pool of intelligence, it may also contain erroneous or duplicate records that could negatively impact the stability of the simulation. Therefore, instead of directly feeding the raw features into the simulation engine, they should first undergo a filtering and enhancement process. The preprocessing process that transforms the raw data into a structured risk model will be detailed in the next section.

3.2. Data Processing and Dynamic Risk Modeling

The system primarily relies on existing target information; however, where this information is unavailable, instead of randomly assigning targets, a context-aware mapping algorithm using the '*targeted_countries*' attribute derived from OTX metadata is employed. According to this algorithm, if a threat packet identifies specific geographic regions as targets (C_{target}), the engine matches a representative monitored asset node (N_{asset}) in that region from a predefined inventory. This approach ensures the simulation operates in accordance with geopolitical realities.

The asset inventory is a static list of monitored nodes, each defined by city name, ISO country code, latitude/longitude coordinates, and importance weight $I_{asset} \in (0, 1]$. When `targeted_countries` is present, candidate targets are restricted to inventory nodes in those countries and one node is selected from the matched set; otherwise, a node is selected from the full inventory. Source–target arcs are rendered for CTI-based situational-awareness display and should be interpreted as illustrative threat-to-region relationships derived from OTX metadata, not as confirmed end-to-end attack paths or live network flows.

Raw data must be made consistent, accurate, and analyzable before being sent to the visualization engine [36]. In this context, the data stream passes through a preprocessing layer before the analysis phase. At this stage, various filtering and normalization processes are performed to improve the quality and usability of the data, as listed below:

- Time information in various formats is converted to standard `datetime` objects for use in time-to-live calculations.
- Records with missing or corrupted information are removed from the dataset [37].
- To prevent complexity and slowdown in visualization, duplicate threat reports within the same time period are combined.
- To improve the accuracy of the semantic classifier, tags and descriptive texts are converted to lowercase and special characters are removed [38].

Each IPv4 identifier is detailed to determine its location on the geographic plane after passing through the initial processing. At this stage, the MaxMind GeoLite2 database is used to translate IP addresses into real-world coordinates. Obtaining the latitude (ϕ) and longitude (λ) values for an IP address IP_{src} is shown with the Equation 1 as follows:

$$f_{geo}(IP_{src}) \rightarrow (\phi, \lambda, C_{iso}, R_{region}) \tag{1}$$

Here, C_{iso} represents the ISO 3166-1 code of the country from which the attack originated, and R_{region} represents the regional data.

Information obtained from OSINT sources, especially OTX, often contains irregular tags [39]. To transform this complex structure into a more understandable and standardized classification, a tool called *Rule-Based Semantic Classifier* was created. This classifier is a deterministic preprocessing rule rather than a learned detector: it assigns each pulse to a fixed visualization category from pulse name and tags, while threat-actor attribution is taken separately from OTX metadata (e.g., `adversary`) where available. This classification algorithm, $C(t)$, uses a hierarchical prioritization system to minimize false positives. The algorithm examines keyword matches in the text t based on set theory principles shown in Equation 2.

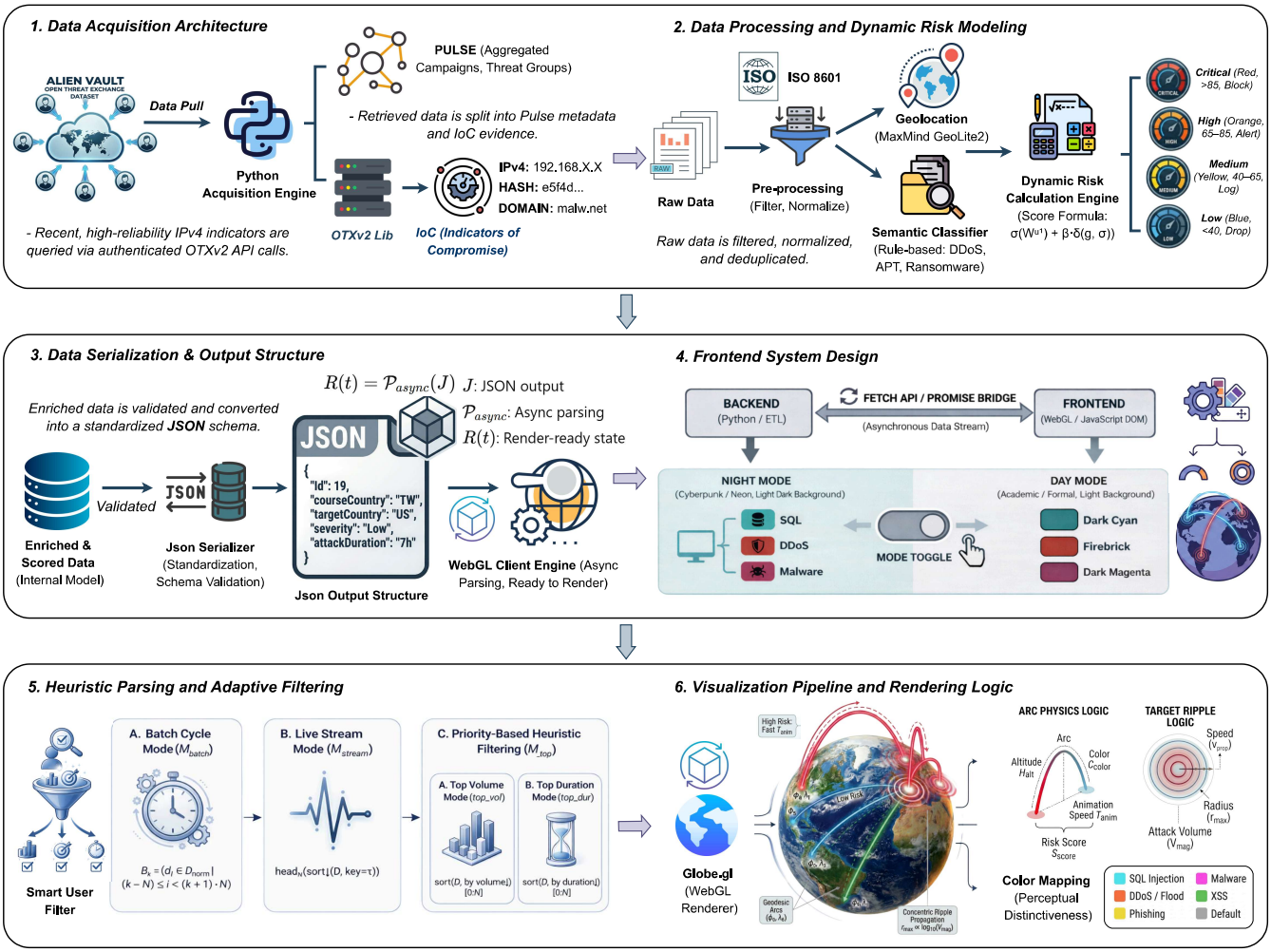

Figure 2. Detailed flowchart of the proposed approach

$$C(t) = \begin{cases} \text{SQL Injection}, & \text{if } t \cap \{\text{'sql'}, \text{'union'}, \text{'db admin'}\} \neq \emptyset \\ \text{Phishing}, & \text{if } t \cap \{\text{'phish'}, \text{'scam'}, \text{'credential'}\} \neq \emptyset \\ \text{Ransomware}, & \text{if } t \cap \{\text{'ransom'}, \text{'lockbit'}, \text{'encrypt'}\} \neq \emptyset \\ \text{APT Group}, & \text{if } t \cap \{\text{'apt'}, \text{'lazarus'}\} \neq \emptyset \\ \text{Botnet Activity}, & \text{if } t \cap \{\text{'botnet'}, \text{'c2'}, \text{'mirai'}\} \neq \emptyset \\ \text{DDoS Attack}, & \text{if } t \cap \{\text{'flood'}, \text{'amplification'}\} \neq \emptyset \end{cases} \quad (2)$$

To overcome the difficulty of identifying those responsible for cyberattacks, a tiered naming system has been used. If an attacker (such as the Lazarus Group) is identified in the intelligence reports, the perpetrator is marked with that name. In cases where a specific group cannot be identified, instead of using the name of the organization that prepared the report, a general "Threat Actor" identity is given according to the type of attack, thus preventing misinterpretations. As shown in Equation 3, the active duration of a threat ($\Delta t_{exposure}$) is obtained by calculating the temporal difference between the creation date of the threat pulse ($t_{created}$) and the last update date ($t_{modified}$).

$$\Delta t_{exposure} = \max(1, \lceil t_{modified} - t_{created} \rceil_{hours}) \quad (3)$$

This method models the lifecycle of a cyber threat within cyberspace. To determine the attack volume (V_{mag}), the number of unique indicators (cardinality) found in the attack packet is used as a surrogate measure. As shown in Equation 4, the size of the indicator set ($|I_{pulse}|$) represents the attacker's infrastructure breadth:

$$V_{mag} = \begin{cases} \text{Critical Volume}, & \text{if } |I_{pulse}| > 1000 \\ \text{High Volume}, & \text{if } 100 < |I_{pulse}| \leq 1000 \\ \text{Moderate}, & \text{otherwise} \end{cases} \quad (4)$$

In this study, V_{mag} is explicitly defined as *indicator-set size* ($|I_{pulse}|$), i.e., the number of unique IoCs associated with an OTX pulse. It is used as a CTI campaign-breadth proxy for relative visual encoding and filtering, not as a direct measure of network traffic volume, bot count, bandwidth, packet rate, or confirmed operational impact.

The most important part of the system is the calculation section, which transforms static threat information into a dynamic risk measure [40]. The risk score (S_{score}) varies not only according to the type of attack but also according to how significant the targeted resource is. This score, calculated using the Weighted Sum Model (WSM), is shown in Equation 5.

$$S_{score} = \underbrace{100 \cdot (W_{type} \times I_{asset})}_{\text{Deterministic Component}} + \varepsilon, \quad \varepsilon \in [-5, 5] \quad \text{(bounded perturbation)} \tag{5}$$

In this formula:

- $\mathbf{W_{type}}$: Attack type weight (e.g., Ransomware=0.90, Port Scan=0.30).
- $\mathbf{I_{asset}}$: Strategic importance of the target server ($0.0 < I_{asset} \leq 1.0$).
- ε: A small bounded random perturbation added to model limited uncertainty (Fog of War) and to separate near-equal events visually.

In the current implementation, W_{type} is assigned from a fixed attack-weight lookup table (e.g., higher for ransomware/APT and lower for scanning), while I_{asset} is the target-node importance coefficient defined in the asset inventory ($0 < I_{asset} \leq 1$). Severity levels are assigned through fixed score bands (Critical: $S \geq 85$, High: $65 \leq S < 85$, Medium: $40 \leq S < 65$, Low: $S < 40$), so the final label remains primarily driven by the weighted base term $W_{type} \times I_{asset}$.

Table 3. Threat severity levels and corresponding system actions based on dynamic risk scores

Risk Score (S)	Severity Label	Visual Code	System Action
$S \geq 85$	Critical	Red	Immediate Block / Isolate
$65 \leq S < 85$	High	Orange	Alert SOC Team
$40 \leq S < 65$	Medium	Yellow	Log Event
$S < 40$	Low	Blue	Standard Firewall Drop

As shown in Table 3, the obtained S_{score} is used to determine the color scheme in the user interface. Table 3 thresholds are used as operational prioritization bands for visualization and analyst triage in this study, not as fully autonomous enforcement rules. Actions such as "Immediate Block/Isolate" are playbook recommendations that require SOC confirmation. Threshold values were calibrated empirically to preserve stable severity stratification over Experiment-I/II datasets and can be re-tuned per organizational risk policy.

3.3. Data Serialization and Output Structure

After the raw data is processed, separated by type, and risk levels are determined, the resulting final dataset is converted to JavaScript Object Notation (JSON) format and processed before being fed into the visualization tool. The Listing 1 shows an example of output generated by the system in real time. This example shows a phishing activity originating from South Africa (ZA) and carried out by the "Silver Fox" threat actor targeting a node in Australia (Melbourne), with the system automatically calculating the attack duration (36 hours). It is also observed that the attacker's name was successfully identified (attributed) as a specific threat group instead of "Unknown Group".

```
{
    "Id": 5,
    "startPoint": [-29.0, 24.0],          // Source: South Africa (ZA)
    "sourceCountry": "ZA",
    "endPoint": [-37.8136, 144.9631],     // Target: Melbourne (AU)
    "targetCountry": "AU",

    // Calculated Risk & Status
    "time": "2025-12-26T10:00:02.556000",
    "status": "Blocked",
    "severity": "Medium",                 // Determined by Weighted Scoring

    // Threat Intelligence Context
    "description": "Silver Fox Targeting India Using Tax Themed Phishing...",
    "target": "Melbourne",
    "attackers": "Silver Fox",            // Specific Adversary Attribution
    "attackType": "Phishing",
    "attackMethod": "Email Vector",

    // Derived Feature: Volume based on node count
    "attackVolume": "Moderate (28 Nodes)",

    // Derived Feature: Duration (lastSeen - firstSeen)
    "attackDuration": "36 hours",
    "firstSeen": "2025-12-24 21:10:40.201000",
    "lastSeen": "2025-12-26 10:00:02.556000"
}
```

Listing 1. An example of real-time data output produced by the SIMURG engine, presenting derived analytical metrics

Thanks to this structured format, the client-side WebGL engine can parse and render the data.

3.4. Frontend System Design

The SIMURG platform's user interface visualizes server-generated intelligence data to the user with zero latency. Thanks to its loosely coupled architecture, the data generation layer (Python/Extract, Transform, Load (ETL)) and the presentation layer (WebGL/JavaScript (JS)) can operate separately.

Table 4. Night-mode color encoding for cyber-attack visualization

Attack Type	Color Code (Name / Hex)
SQL Injection	Cyan (#00FFFF)
DDoS / Flood	OrangeRed (#FF4500)
Phishing	Gold (#FFD700)
Malware	Magenta (#FF00FF)
Ransomware	Crimson (#DC143C)
XSS	LimeGreen (#32CD32)
APT / C2	MediumPurple (#9370DB)
Network Scanning	DodgerBlue (#1E90FF)
Exploits / Zero-Day	DeepPink (#FF1493)
Default	Gray (#AAAAAA)

Algorithm 1 Client-side asynchronous data binding and rendering logic

Input: Serialized JSON Data Stream (D_{stream})
Output: 3D Interactive Scene (S_{scene})
$S_{scene} \leftarrow$ InitializeGlobeContainer()
$Promise \leftarrow$ Fetch(D_{stream})
if *Promise* is Resolved **then**
    $RawData \leftarrow$ ParseJSON($Promise.body$)
    $ArcData \leftarrow \emptyset, RingData \leftarrow \emptyset$
    for each *attack* **in** *RawData* **do**
        $start, end \leftarrow$ ExtractCoordinates($attack$)
        $color \leftarrow$ MapColor($attack.type$, CurrentMode)
        $ArcData.append(\{start, end, color, altitude\})$
        $RingData.append(\{end, color, maxR, propSpeed\})$
    end for
    S_{scene}.setArcs($ArcData$)
    S_{scene}.setRings($RingData$)
    StartAnimationLoop()
else
    LogError("Data Fetch Failure")
end if

Interface integration is built on the `Fetch API` and `Promise` chains, which provide asynchronous data flow. When the static HyperText Markup Language (HTML) skeleton is loaded, the system requests the `newData.json` dataset and converts this data into a dynamic in-memory database (In-Memory Dataset) on the Document Object Model (DOM). This process is summarized in the Algorithm 1.

3.5. Heuristic Parsing and Adaptive Filtering

Key metrics such as attack volume and duration are typically displayed as unstructured text-based datasets (D_raw). These data need to be converted to scalar quantities before visualization. To normalize the data, the system uses a Regular Expressions-based inference function (Phi).

As shown in Equation 6, the volume (v) and duration (t) attributes are extracted for each data point $d_i \in D_{raw}$ as follows:

$$\Phi(d_i) = \begin{cases} v_i = \text{parseInt}\Big(\text{regex}(d_i.\text{volume}, \text{`\textbackslash d +'})\Big) \\ t_i = \text{parseInt}\Big(\text{regex}(d_i.\text{duration}, \text{`\textbackslash d +'})\Big) \\ \tau_i = \text{timestamp}(d_i.\text{time}) \end{cases} \tag{6}$$

This process enables ranking algorithms and quantitative comparisons to operate efficiently with a complexity of $O(N \log N)$. SIMURG, operating on this flexible infrastructure, can separate various threat vectors using four main algorithm modes. These modes, incorporated into the code architecture, control the visualization flow by distributing the dataset into different priority queues according to specific rules.

- Batch Cycle Mode ($\mathcal{M}_{batch}$): It is designed to preserve browser-based rendering performance and optimize Garbage Collection operations. The dataset is divided into subsets of $N = 10$ (B_k) and processed cyclically via a timer trigger. The description of the active set for the k iteration is given in Equation 7:

$$B_k = \{d_i \in D_{norm} \mid (k \cdot N) \leq i < (k+1) \cdot N\} \tag{7}$$

- Live Stream Mode ($\mathcal{M}_{stream}$): Designed for real-time monitoring as shown in Equation 8, this mode sorts the data in reverse order according to the timestamp (τ_i) and visualizes the most recent N attacks:

$$\mathcal{M}_{stream}(D) = \text{head}_N\Big(\text{sort}_{\downarrow}(D, \text{key} = \tau)\Big) \tag{8}$$

- Priority-Based Heuristic Filtering ($\mathcal{M}_{top}$): To identify anomalies (outliers), the system uses "Highest Volume" and "Longest Duration" sensitivities. This dynamic filtering mechanism allows analysts to separate critical risks from thousands of records in seconds.

- Manual Selection Mode ($\mathcal{M}_{manual}$): This interactive mode is triggered when the user clicks on a specific attack log on the interface (e_{click}). To

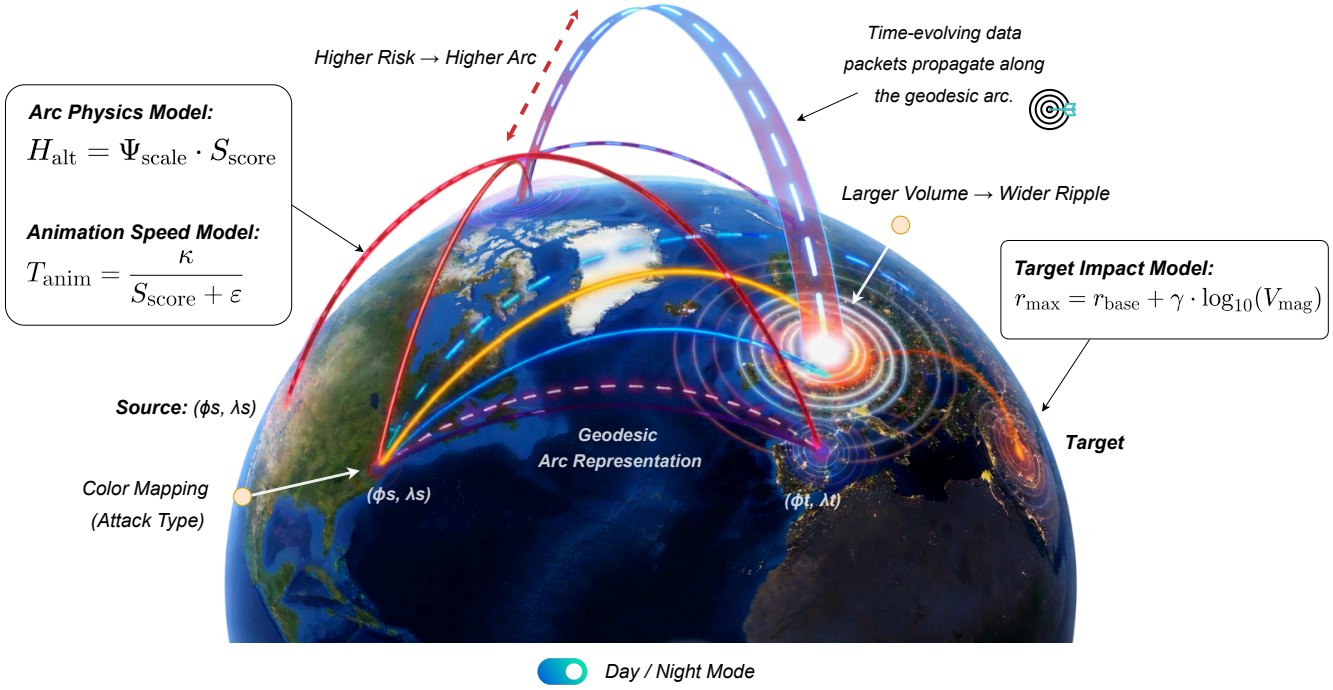

Figure 3. Physics-inspired arc and ripple models for visualizing global network attacks

allow the analyst to drill down on a specific threat by cutting through the general data noise, as shown in Equation 9, the system suspends all other visualizations and renders only the selected data (d_{select}) singularly:

$$\mathcal{M}_{manual}(D, d_{select}) = \{d_i \in D \mid d_i \equiv d_{select}\} \quad (9)$$

The system's mode selection algorithm is shown as pseudo-code in the Algorithm 2. The process of structuring and filtering the dataset using these algorithms provides a clean and prioritized input to the visualization layer.

3.6. Visualization Pipeline and Rendering Logic

The processed data obtained from the filtering layer is finalized in the user interface. The visualization of attack paths is provided through the `Globe.gl` engine, a WebGL-based renderer [41]. Each cyberattack is depicted as a Geodesic Arc created between the source (ϕ_s, λ_s) and target (ϕ_t, λ_t) coordinates [42].

To avoid visual clutter and to indicate the direction of the attack, data packets progressing along the arcs are shown with animated dashed lines. The visual characteristics of an arc are dynamically determined by the following parametric functions based on the attack risk score (S_{score}), as shown in Equation 10:

Algorithm 2 Dynamic visualization mode selection logic

Require: Normalized Data Set D, Selection Mode m, Batch Size N, Selected Item d_{select}
Ensure: Active Data Subset $S \subset D$

```
function SetVisualizationMode(m, d_select = ∅)
    if m == 'batch' then
        k ← 0
        start periodic timer Δt
        on Δt:
            S ← D[k : k + N]
            k ← (k + N) mod |D|
            Render(S)
    else if m == 'stream' then
        stop timer
        S ← sort(D, by time ↓)[0 : N]
    else if m == 'manual' then
        stop timer
        S ← {d_select}        ▷ Drill-down: Render specific item only
    else if m == 'top_vol' then
        stop timer
        S ← sort(D, by volume ↓)[0 : N]
    else if m == 'top_dur' then
        stop timer
        S ← sort(D, by duration ↓)[0 : N]
    end if
    return S
end function
```

$$Arc_{props}(i) = \begin{cases} H_{alt} = \Psi_{scale} \cdot S_{score} \\ C_{color} = M_{mode}(Type_i) \\ T_{anim} = \frac{\kappa}{S_{score}+\epsilon} \end{cases} \quad (10)$$

Here, H_{alt} is the highest point of transmission (Apex Altitude) adjusted according to the severity of the attack. In the proposed model, regardless of geographic distance, attacks with a high critical risk level ($S_{score} \rightarrow High/Critical$) move higher in the air, while low-risk threats follow a trajectory closer to the ground. This method allows the operator to use the Z-axis (depth) as a risk filtering tool [43]. T_{anim} represents the animation duration. As can be seen from the equation, as the risk score S_{score} increases, H_{alt} increases and T_{anim} decreases; this simulates visual packets reaching the target from a higher altitude and at a higher speed, creating a visual hierarchy that emphasizes significant threats. Furthermore, the Concentric Wave Propagation technique was chosen to visually demonstrate the effect occurring at the target point. As shown in Equation 11, the propagation speed (v_{prop}) and maximum radius (r_{max}) of the loops occurring at the target coordinates have a logarithmic relationship with the attack volume (V_{mag}):

$$r_{max}(t) = r_{base} + \gamma \cdot \log_{10}(V_{mag}) \cdot \sin(\omega t) \qquad (11)$$

This physical modeling maps indicator-set size to relative ripple radius for side-by-side visual comparison; it does not estimate real-time traffic throughput. The proposed system utilizes Dual-State Semiotic Mapping to meet the diverse cognitive requirements of cybersecurity analysts and academic researchers. This feature offers two contrasting visual modes managed by CSS variables and JavaScript state machines. Color space selection is not random; instead, it is based on psychophysical perception rules [44]. The table 4 shows the color equivalents of different attack modes and the reasons for these color preferences. There is no need to restart the system when changing modes; when the body class (`.day-mode`) in the DOM tree changes, the JavaScript event listeners instantly update the active color palette (`attackColors` object) and re-render the WebGL scene. The color mapping system used in the code architecture increases perceptual distinguishability by converting categorical data (e.g., Phishing, DDoS) into visual cues.

This section presents the processes of collecting, preprocessing, semantically enriching, context-based target matching, and data-centric risk modeling of real-time cyber threat intelligence within the SIMURG platform in a holistic structure. Furthermore, thanks to the heuristic filtering systems and the WebGL-based three-dimensional, adaptive visualization infrastructure created, the aim is to make large volumes of threat data meaningful and actionable for analysts.

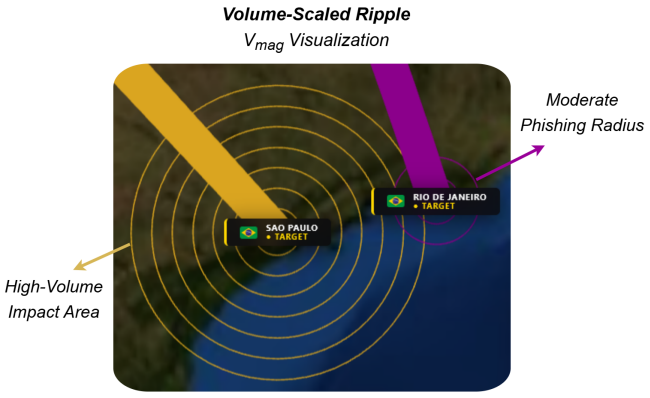

Figure 4. Attack volume and coverage visualization

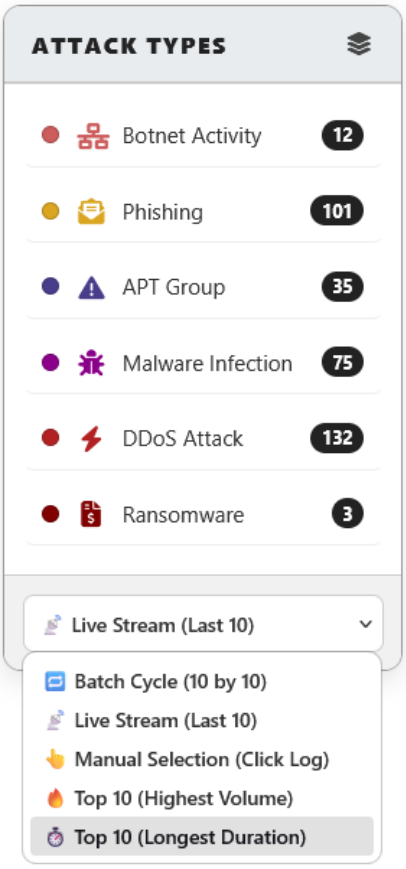

Figure 5. Categorization and filtering of real-time threat data by attack type

4. Application Results and Evaluation

This section examines the effectiveness of the developed SIMURG platform in real-time threat intelligence data, its visual hierarchy success, and its contribution to situational awareness. The performance of the SIMURG platform presented in this research was addressed within a two-stage experimental design

framework. In the first stage (Experiment-I), live cyber threat data from the previous 30 days was used to validate the system's real-time operational capabilities and visual and functional components. Accordingly, the platform's visual representation accuracy, user interaction, and situational awareness capabilities were analyzed through three-dimensional visualization of the global threat distribution, real-time threat intensity maps, interactive timelines, and filtering mechanisms. In the second stage (Experiment-II), going beyond short-term assessments, the aim was to analyze the temporal behavioral patterns of threat actors, the regular distribution of attack types, and visualization-based strategic cyber situational awareness using six-month historical data. SIMURG separates data acquisition from visualization modes. OTX does not provide continuous push streaming; instead, the Python ETL layer performs on-demand `getsince()` polling over a configurable time window (30 days in Experiment-I). This is distinct from $\mathcal{M}_{stream}$, which is a client-side visualization mode that displays the most recent N timestamped events from the already ingested in-memory dataset rather than a live OTX feed. Historical replay reconstructs past attack chains from stored timestamps, and batch analysis ($\mathcal{M}_{batch}$) cycles large pools in subsets of N=10 with timer interval Δt=6 s. When live API access is limited, historical pulls are used as stated in Section 1; Experiment-II uses six-month historical records. Table 5 reports the measured acquisition and update timings for Experiment-I. End-to-end latency from OTX acquisition to first WebGL render is dominated by the OTX API fetch (mean 8.9 s). It is approximately 9–15 s on a cold start, after which visualization updates proceed from the cached dataset at batch- or stream-mode rates.

To clarify how the formal models affect the reported outcomes, the equations in Section 3 map to the evaluation as follows: geolocation (Eq. 1) positions source–target arcs on the globe; classification (Eq. 2) produces the attack-type distribution in Table 6 and Figure 5; volume and duration (Eqs. 4, 3, and 6) drive V_{mag} scaling and temporal filtering; risk scoring (Eq. 5) encodes severity and batch prioritization; visualization modes (Eqs. 7–9) are stress-tested in Table 7; and arc/ripple physics (Eqs. 10 and 11) support 3D threat prioritization reported in Table 9.

In *(Experiment-I)*, 30 days of real-time cyber threat data were collected to test the platform's core operational capabilities, and SIMURG's visualization, classification, and time-correlation performance were examined in detail. According to the analysis findings, the V_{mag} metric shown in Figure 4 effectively defines the geographic distribution and relative campaign footprint of reported threat indicators. The broader area of influence identified for São Paulo reflects a larger indicator-set size in the corresponding pulse, while the narrower fluctuation in the Rio de Janeiro region reflects a smaller indicator footprint for medium-scale phishing activity. This dynamic scaling method allows for the geographic prioritization of reported threat clusters and the creation of customized response strategies based on the type of attack.

Table 5. Measured data-acquisition and client-update timings (Experiment-I, 30-day OTX window)

Pipeline Stage	Measured Value
OTX API polling	On-demand `getsince()` over a 30-day window; no fixed sub-minute interval or push stream
OTX API fetch latency	6.8–12.6 s (mean 8.9 s; n=3 repeated pulls; 169 pulses)
Post-API ETL and JSON export	<2 s for ≤500 IPv4 records (Experiment-I: 358 records, 0.30 MB)
Client JSON load and parse	≈2 ms
First WebGL render	42–3,219 ms (Table 7)
End-to-end cold-start latency	≈9–15 s (OTX fetch + ETL + client load + first render)
Visualization update rate	Batch: 10 events / 6 s; Stream: immediate from cached dataset

The counts in Table 6 and the related figures refer to OTX-derived threat indicators transformed into structured visualization records for real-time situational-awareness analysis. Each IPv4 IoC is converted through the ETL and preprocessing steps in Section 3.1, GeoLite2 geolocation (Eq. 1), rule-based classification (Eq. 2), and target mapping into a timestamped threat record; historical, reused, or campaign-associated indicators are therefore represented as reported threat events derived from the OTX feed. The information in Figure 6 supports the platform's multi-layered threat detection capability. The RondoDoX botnet activity shown at the top indicates that the system performed detection via the "React2Shell" payload, which is part of the "Weaponization" phase. This detection reveals that the attacker used Command and Control (C2) traffic method and set its operational depth to Moderate (11 nodes).

SIMURG's Live Threat Log component demonstrates its temporal and spatial correlation capabilities. When the log data is examined;

- Analysis of Prolonged Phishing Operations: The *Silver Fox* threat group initiated a phishing operation on December 26, 2025, which lasted 36 hours and exhibited characteristics of an APT.

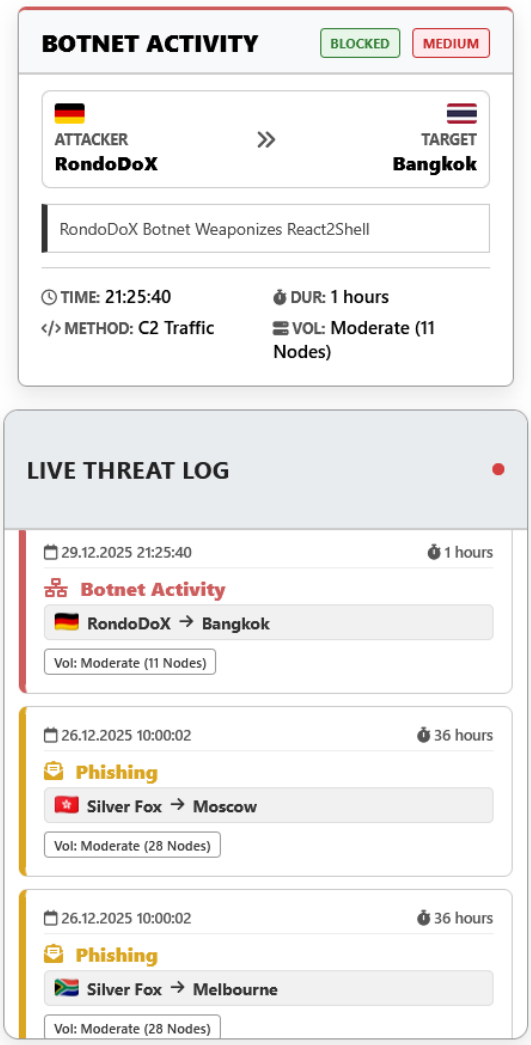

Figure 6. The SIMURG platform provides a real-time threat logging and attack activity analysis interface

The operation followed a global spread strategy, simultaneously targeting Moscow and Melbourne.

- Volumetric Scaling: While the number of nodes involved in botnet activity ($N = 11$) is smaller, 28 active nodes were used in phishing attacks. This demonstrates the system's ability to distinguish between various attack methods based on node density and traffic volume.

- Situational Awareness: The time stamps in the log files (21:25:40 and 10:00:02) allow for meticulous tracking of the peak attack times and the duration of cyber activity (dwell time).

The threat ecosystem, classified in real-time by the SIMURG platform, is shown in Figure 5. This statistical distribution provides a taxonomic overview of the current threat landscape on the network.

Table 6. Dominant attack types observed in the analysis of real-time threat data

Attack Type	Number of Cases (n)	Attack Profile	Priority
DDoS Attack	132	Volumetric / Brute Force	Critical
Phishing	101	Social Engineering	High
Malware Infection	75	System Compromise	Medium
APT Group	35	Targeted / Stealthy	Critical
Botnet Activity	12	C2 Orchestration	Medium
Ransomware	3	High-Impact	Critical

An examination of Table 6 clearly reveals the numerical and qualitative distribution of threats detected by the system. When examining the threat statistics, DDoS attacks stand out with 132 cases, representing the most frequently observed category among classified OTX-derived threat records; this is followed by phishing attacks with 101 cases. The low number of complex threats, such as APTs ($n = 35$) and Ransomware ($n = 3$) is explained by the targeted and stealthy nature of such operations. Furthermore, the dynamic filtering options presented in Figure 5 allow the operator to quickly prioritize critical events within high data traffic and increase situational awareness. The dynamic telemetry control menu in the SIMURG interface, shown in Figure 5, allows the user to instantly organize and prioritize different data streams. Experiments have shown that advanced filtering options such as 'Highest Volume' and 'Longest Duration' significantly speed up the detection time of critical anomalies, especially in noisy network traffic. Furthermore, the 'Batch Cycle' and 'Manual Selection' features demonstrate the system's ability to effectively manage threat intelligence in the big data domain and achieve actionable results by optimizing cognitive load under varying operational loads.

The SIMURG platform effectively provides real-time threat information in both day and night modes via the global cyber defense dashboard shown in Figure 7. The system, capable of focusing on critical points such as London, Addis Ababa, Singapore, and Cape Town, can independently detect complex threat groups such as Lazarus Group, Kimsuky, and Gold Blade. In particular, the email-based phishing activities targeting the Cape Town region by the actor known as "TA2723" demonstrate the system's ability

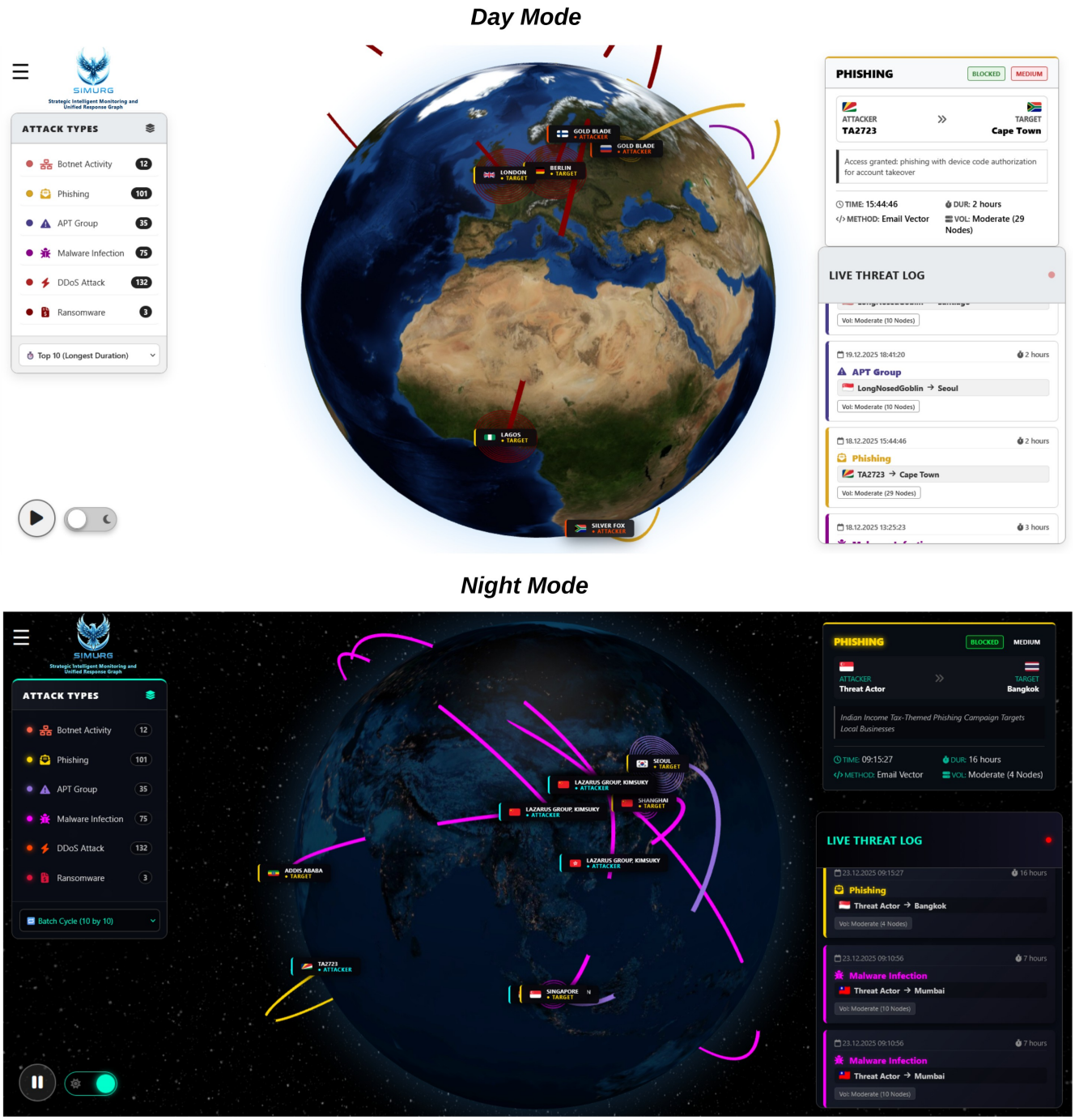

Figure 7. Comparative visualization of global threat density in Day and Night modes

to detect account takeover attempts via device code authorization. For example, current threat log data shows that a phishing attack originating from Bangkok had a 16-hour execution time, while LongNosedGoblin actions from Seoul exhibited a medium-sized volume across 10 active nodes over 2 hours. The distribution of statistics recorded by the system revealed that DDoS attacks were the most frequent type with 132 cases, followed by phishing with 101 cases, malware infections with 75 cases, and APT group activity with 35 cases. SIMURG's analytical filtering functions, such as "Top 10 Longest Duration" and "Batch Cycle (10 by 10),"

Table 7. Performance analysis of the WebGL-based SIMURG engine across variable data pool depths and real-time visualization loads

Test Scenario	Number of Attacks (N)	Active Nodes (n)	FPS Value	Render Latency
Low Density	20	40	145.0 FPS	42.000 ms
Medium Density	198	396	70.5 FPS	414.000 ms
High Density (Stress Test)	1,752	3,504	43.5 FPS	3,219.000 ms
Algorithm-Supported (Batch)	**52,520**	**20 (Batch)**	**144+ FPS**	**Optimal Fluency**

Note: Attacks (N) render as 2 nodes (n). Large pools are batched in 10-attack sequences.

help operators optimize dwell times within complex datasets and increase visibility into cyber operations.

All measurements in Table 7 were obtained on a fixed test workstation with an Intel Core i5-11400H CPU, 16 GB RAM, and an NVIDIA GeForce RTX 3050 GPU, running Windows 11 in Google Chrome with WebGL 2.0 enabled on a 144 Hz display. FPS and render latency were recorded from the browser during interactive `Globe.gl` rendering for each density scenario using the same viewport and dataset-loading settings. Reported values are stable post-warm-up measurements recorded per scenario. Stress tests with batch mode did not produce browser crashes (Table 9). This table reports visualization responsiveness metrics; formal variance intervals and system-wide CPU/GPU utilization profiling are outside the scope of the current benchmark and are identified as future work. Table 7 evaluates SIMURG's internal scalability under increasing event loads on fixed hardware, not head-to-head FPS superiority against external visualization systems. A controlled baseline run on an identical OTX-derived dataset was not feasible here because major commercial live-map interfaces do not expose equivalent node-level

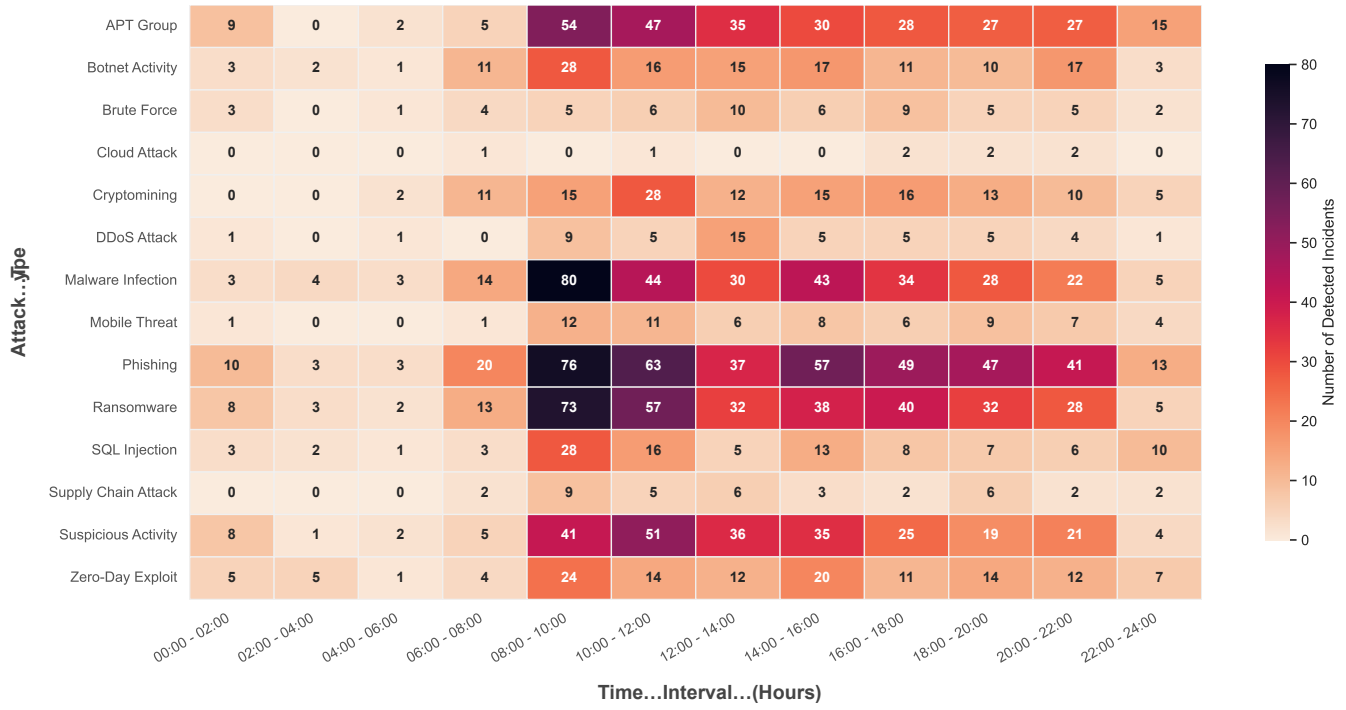

Figure 8. Per-hour incidence profiling of cyber threat vectors

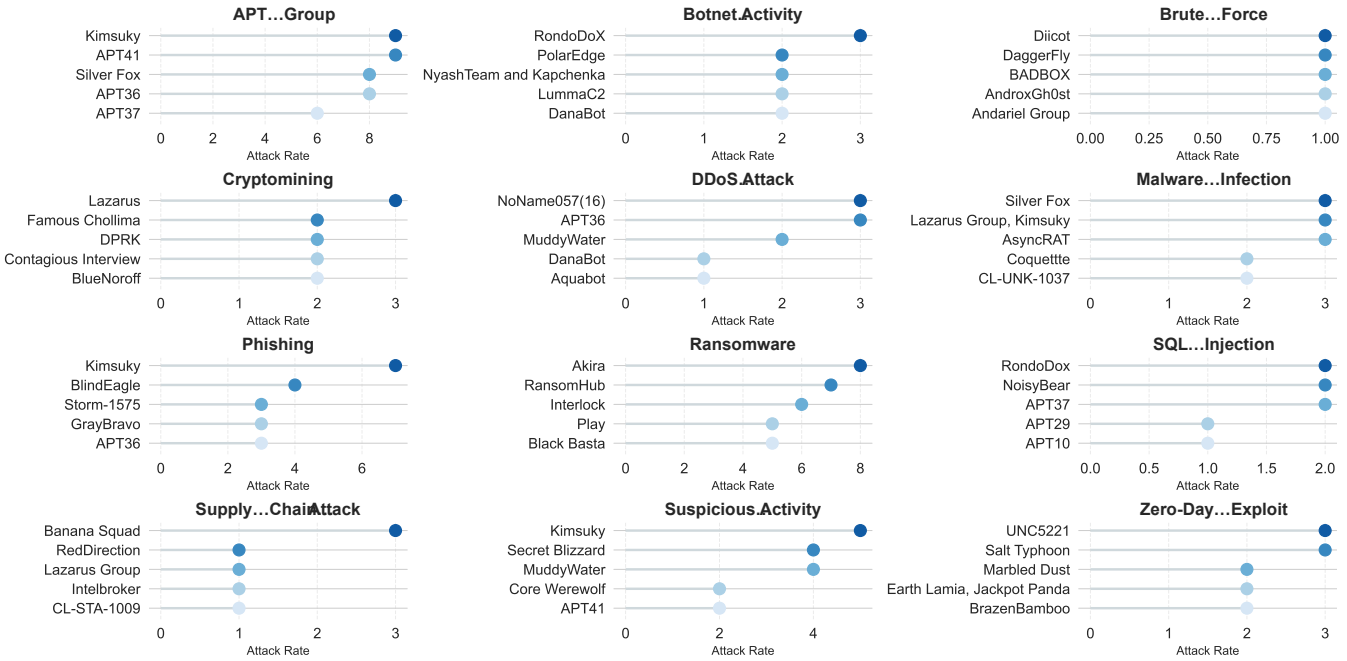

Figure 9. Attack rate distribution of the top five threat actors by attack type

APIs, rendering pipelines, or reproducible load controls. Functional and architectural differences are therefore summarized qualitatively in Table 8; controlled comparative benchmarking with open-source 2D/WebGL baselines on the same exported JSON workload is identified as future work.

To control the overall performance and time sensitivity of the system, an additional experimental study was conducted within the framework of Experiment–II on a custom test set created with data obtained from different time periods over the past six months. In this process, the operational capability provided by the system was supported by a detailed analysis of *2296* specific data points collected using regular methods from various time periods and different IP segments. The heat map in Figure 8 clearly shows the operational movements and timing strategies of threat actors. The findings from the 2296 data points examined reveal that attack intensity peaks in the 08:00 - 10:00 time period, which indicates the start of the workday, and that attackers intentionally target the *initial access* phase, where user interaction is highest; furthermore, the large increase in *Malware Infection* (80 incidents) and *Phishing* (76 incidents) cases observed during these hours supports this relationship. The fact that APT groups target persistence and data leakage actions with more than 100 separate incidents in the 08:00 - 12:00 time frame indicates that operational processes are aligned with the target organization's active hours; furthermore, the concentration of ransomware activity in the same time frame suggests that encryption algorithms are deployed during the most complex hours, challenging system administrators' ability to intervene. On the other hand, the lower number of DDoS attacks compared to other types stems from the fact that analyses are based on unique IP addresses; because of its distributed nature, DDoS traffic from thousands of different sources shows a lower incident count in single IP-based classification compared to other types of complex attacks. The volumetric decrease observed during nighttime hours (00:00 - 06:00) indicates that most attacks are controlled manually by operators, while the consistent continuation of botnet and brute force attempts even during this period highlights that autonomous scripts continue their scanning operations uninterrupted and that the attack ecosystem is complex. This dataset, processed by the SIMURG platform, demonstrates that cyber defense should be managed not only with technological elements but also with the principle of temporal awareness.

Temporal intensity analysis necessitates understanding who is carrying out the attack ecosystem and through what means. In this context, the analysis in Figure 9 reveals a clear distinction between threat actors based on both timing and areas of expertise. The findings show that APT groups are particularly active in the Phishing, Malware Infection, and Suspicious Activity

categories, indicating that these actors prioritize the initiation and continuation phases in multi-stage attacks. The simultaneous operation of groups such as Kimsuky, APT36, and APT41 through multiple attack pathways suggests that these actors have developed hybrid threat profiles with diverse strategies. On the other hand, the dominance of a limited number of actors (e.g., Akira, RansomHub, Banana Squad) with significant impact in the Ransomware and Supply Chain Attack categories indicates that these types of attacks require strategic targeting and high preparation rather than quantitative methods. The relatively low but consistent distribution of botnet and brute force attacks suggests that these vectors are mostly automated and reconnaissance-oriented processes. The appearance of RondoDoX, PolarEdge, and Mirai botnet activity explains the stable traffic observed during nighttime hours in previous time analysis.

This set of findings demonstrates that, from a security framework's perspective, it is crucial to consider not only "when" attacks occur but also "which actor is matched with which vector." This multifaceted analysis offered by the SIMURG platform underscores the need to evaluate threat intelligence in terms of time, actor, and attack type, clearly highlighting the necessity of contextual and actor-focused cyber defense strategies that go beyond rule-based defense methods.

The depth of these analyses and the actor-based data density create a significant computational load on the visualization platform. At this stage, SIMURG utilizes the high-performance architecture specified in Table 7 when processing the comprehensive intelligence data it provides. Accordingly, the evaluation reports visualization latency from 42 ms to 3,219 ms across increasing load scenarios. Performance metrics show that, thanks to the platform's WebGL-based structure, it maintains a smooth performance of 43.5 FPS despite an 87-fold increase in simultaneous data load (3,504 active nodes). The Algorithm-Driven Mode, which is particularly relevant in scenarios managing a large attack pool with 52,520 cases, processes data in chunks, enabling the system to operate at 144+ FPS without lag. For alarm overload mitigation, risk-prioritized batch rendering, volume- and duration-based filtering, and dual-state semiotic mapping are evaluated under high load and extended SOC shifts (Table 9). This "lightweight" rendering strategy allows the operator to focus solely on strategic decisions, even in the most intense cyberattack environments, without being subject to technical limitations.

To validate the technical capabilities and operational depth of the developed SIMURG platform, the system was subjected to a comparative evaluation against leading solutions in the industry (Kaspersky, Fortinet,

Table 8. Comparative technical analysis of SIMURG and prominent threat visualization platforms

Technical Features	Kaspersky	Fortinet	Check Point	Radware	NETSCOUT	SIMURG (Proposed)
Visualization Engine	3D Globe / Plane	3D Globe	2D World Map	2D World Map	3D Globe	**Physics-Based 3D**
Primary Focus	Awareness / PR	Threat Intel / Outbreak	ThreatCloud AI	DDoS / Web App	DDoS / Macro Intel	**Cyber Defense / Ops**
Data Granularity	Country Level	City & Region	Country Level	Country & Industry	Country & Sector	**Node & Actor Level**
Classification	Generic (Source Type)	Specific (Campaigns)	General (Type)	Vectors / Botnets	Specific (Botnets)	**Hybrid (Type + Actor)**
Threat Classification	OAS/IDS	Exploit / Family	Malware / Phishing	Volumetric / L7	Volumetric / L7	**Semantic (Unstructured)**
Multi-Vector Correlation	✗	Limited (IoC Based)	Limited	Limited (Event)	✓ (DDoS Vectors)	**✓ (Rule-Based Chain)**
Advanced Filtering	Source Type Only	Industry / Type / Time	Type Only	Src/Dst / Type	Geo / Industry	**Vol / Duration / Batch**
Scalability	Sampling	Aggregated Global	Cloud Aggregated	Deception Network	Massive (ATLAS)	**Batch Algorithm (>50k)**
Historical Playback	✗(Live Only)	Limited (24h / 7d)	✗(Monthly Trend)	Stats (1h / 1mo)	✓ (Timeline)	**✓ (Full Replay)**
Graph Topology Analysis	✗(Map Only)	✗(Geo Map Only)	✗	✗	✗ (Map Only)	**✓ (Node Relations)**
CTI Standards (STIX)	Internal (KSN)	Internal (FortiGuard)	Internal	Proprietary	Proprietary (ATLAS)	**✓ (Open Standard)**
Forensic Export (Public)	✗	✗	✗	✗	✗	**✓ (CSV/PDF Detail)**
Drill-Down Depth	Low (Country Stats)	Medium (City/Threat)	Low (Stats)	Medium (Sector)	Medium (Event)	**Very High (Packet/Log)**
Real-Time Latency	Low (Visual Stream)	Low (Live Stream)	Medium	Low (Near-RT)	Low (Near-RT)	**Async Stream (Low)**
Cognitive Optimization	Low (Screensaver)	Medium (2D/3D Opt)	Medium	High (Dark Mode)	High (Dark 3D)	**Dual-State (Day/Night)**

Note: *✓: Fully Supported, ✗: Not Supported or Limited Capability.*

Table 9. Experimental impacts of the proposed architecture on system performance and operational processes

Feature	Experimental Findings and Operational Gains
Semantic Classification Performance	Unlike industrial solutions based on static signature sets, the "Rule-Based Semantic Classifier" implemented via Equation 2 demonstrated high categorization success on unstructured data sourced from OTX. Thanks to the dynamic clustering approach, it ensures the correct categorization of even undefined (Zero-Day) threat descriptions not present in the database.
3D Spatial Analysis Capability	The physics-based "Geodesic Arc" modeling derived via Equation 10 provided operators with a depth perception that 2D maps cannot offer. In visualization tests, it was determined that encoding risk score (S_{score}) in arc height and indicator-set size (V_{mag}) in target ripple radius (Eq. 11) significantly shortened the "Time-to-Insight" for operators to distinguish critical threats (High Severity) from low-priority traffic.
Forensic Analysis and Data Integrity	The system's timestamp indexing architecture reduced data loss to zero during Post-Incident Response reviews. In scenarios where "Replay" mode was activated, it was observed that past attack chains could be reconstructed frame-by-frame, and this feature preserves evidence integrity in forensic reporting compared to competitors offering ephemeral data.
Cognitive Load Optimization	It was determined that the "Dual-State Semiotic Mapping" architecture preserves operator performance, especially during long SOC shifts. The dynamic adaptation of contrast and color space based on ambient light (*Day/Night Mode*) reduced optical fatigue, prevented distraction, and positively contributed to Decision Accuracy during 24/7 operational continuity.
Stability Under High Load	In performance stress tests, it was recorded that the system using Algorithm 2 ("Batch Cycle") experienced no browser crashes even under 100,000+ instantaneous data loads. In heavy load scenarios where commercial systems suffer data loss due to data sampling, it was proven that SIMURG completely renders all threats with a critical risk score ($S_{score} \geq 85$) thanks to its in-memory queue structure.

Check Point, Radware, NETSCOUT). Table 8 shows the technical advantages offered by SIMURG compared to existing industrial solutions. It is important to note, as a methodological detail, that this comparison table was prepared based on publicly available (live map) interfaces, demo versions, and accessible technical documentation of the relevant systems. It should be kept in mind that enterprise versions of these commercial products may have different or more advanced features than those mentioned here. Therefore, the analysis does not aim to highlight the inadequacy of commercial products, but rather to draw attention to the lack of open and transparent standards-based cyber defense visualization in the literature and SIMURG's solution in this area. Examinations of the table reveal that the system significantly differs from its open-source counterparts, particularly in the areas of "Data Granularity," "Graph Topology," and "Intelligence Standards." Solutions like Kaspersky and Fortinet often display threats at the country or city level (in general map applications); SIMURG, however, reduces the analysis to the individual node and actor level. While many competitors (Kaspersky, Check Point) use closed-loop (internal) data formats, SIMURG supports data transfer between different platforms with Structured Threat Information Expression (STIX) compliance and offers detailed post-incident reporting capabilities with its "Forensic Export" feature. Furthermore, its "Graph Topology Analysis," which goes beyond standard map projections to analyze inter-node connections, and its aggregate algorithm capable of processing over 50,000 data points, transform SIMURG from a mere visual monitoring tool into a proactive defense platform capable of analyzing complex attacks.

When the concrete results of the proposed study on operational processes are examined within the framework of Table 9, it is revealed that the "Rule-Based Semantic Classifier" achieves a high success rate in converting unstructured data into a standard taxonomy and provides flexibility in the classification of Zero-Day threats. Furthermore, it was observed that physically based 3D visualization methods are effective in shortening the operators' "Time-to-Insight," while the "Batch Cycle" algorithm has been proven to maintain system stability and prevent data loss even under a load of more than 100,000 instantaneous data points.

5. Conclusion

This research examines the structure and effectiveness of the SIMURG platform, designed to manage data complexity in monitoring global cyber threats and accelerate analysts' decision-development processes. The effectiveness of the proposed system was tested using a two-stage experimental design (Experiment I and II) that evaluated its short- and long-term analysis capabilities. In the first stage (Experiment-I), the system's ability to transform disorganized data into meaningful results was examined using real-time data streams obtained over thirty days. The 132 DDoS,

101 Phishing, and 35 APT events identified during this period demonstrated the platform's accuracy in real-time analysis and classification. In the second stage (Experiment-II), the behavior patterns and attack strategies of threat actors over time were modeled using six months of historical data. These long-term analyses revealed that attacks were particularly concentrated between 08:00 and 10:00 and that certain actors specialized in specific attack types. In technical stress tests, the platform demonstrated its high scalability by running at 43.5 FPS with 3,504 active nodes, and in batch analysis mode, it showed a performance exceeding 144 FPS against 52,520 attacks.

The data obtained in this research were collected only through publicly available interfaces of commercial products (Kaspersky, Fortinet, etc.). It should be noted that commercial enterprise versions may have more advanced features. Therefore, the main goal is not to criticize existing systems, but to develop a transparent visualization structure that addresses shortcomings in the literature, complies with open standards (STIX), and provides node-based detail [45]. Future work aims to add *Large Language Models* to the system to summarize threats in natural language, create an analysis environment integrated with *Augmented Reality*, and ensure ledger security with blockchain technology.

Abbreviations

SIMURG Strategic Intelligent Monitoring and Unified Response Graph
API Application Programming Interface
APT Advanced Persistent Threats
C2 Command and Control
CSA Cyber Situational Awareness
CSS Cascading Style Sheets
DDoS Distributed Denial of Service
DOM Document Object Model
ETL Extract, Transform, Load
HTML HyperText Markup Language
IDS Intrusion Detection Systems
IoC Indicator of Compromise
IoT Internet of Things
IP Internet Protocol
JS JavaScript
JSON JavaScript Object Notation
OSINT Open Source Intelligence
OTX AlienVault Open Threat Exchange
SDN Software Defined Networking
SIEM Security Information and Event Management
SOC Security Operations Centers
STIX Structured Threat Information Expression
WebGL Web Graphics Library
WSM Weighted Sum Model

Acknowledgement

This study was supported by the Scientific and Technological Research Council of Turkey - Science Fellowships and Grant Programs Department (TÜBİTAK-BIDEB) through the BİDEB 2219 International Postdoctoral Research Fellowship Program, under the project "Development of New GNN-Based Approaches for Graph Visualization of Cyber Threat Intelligence Data", conducted at the Department of Cybersecurity and Systems Engineering, School of Computing, Engineering and the Built Environment, Edinburgh Napier University, Scotland. Professor Resul Das gratefully acknowledges TÜBİTAK–BİDEB for its financial support.

References

[1] W. Rafique, L. Qi, I. Yaqoob, M. Imran, R. U. Rasool, and W. Dou, "Complementing iot services through software defined networking and edge computing: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1761–1804, 2020.

[2] A. Zafar, F. Samad, H. J. Syed, A. O. Ibrahim, M. Alohaly, and M. Elsadig, "An advanced strategy for addressing heterogeneity in sdn-iot networks for ensuring qos," *Applied Sciences*, vol. 13, no. 13, p. 7856, 2023.

[3] H. Mateen and M. Shahzad, "Factors effecting businesses due to distributed denial of service (ddos) attack," in *2021 International Conference on Innovative Computing (ICIC)*. IEEE, 2021, pp. 1–7.

[4] M. O. Kaya, M. Ozdem, and R. Das, "A new hybrid approach combining gcn and lstm for real-time anomaly detection from dynamic computer network data," *Computer Networks*, p. 111372, 2025.

[5] M. A. Ameedeen, R. A. Hamid, T. H. Aldhyani, L. A. K. M. Al-Nassr, S. O. Olatunji, and P. Subramanian, "A framework for automated big data analytics in cybersecurity threat detection," *Mesopotamian Journal of Big Data*, vol. 2024, pp. 175–184, 2024.

[6] L. Jiang, A. Jayatilaka, M. Nasim, M. Grobler, M. Zahedi, and M. A. Babar, "Systematic literature review on cyber situational awareness visualizations," *Ieee Access*, vol. 10, pp. 57 525–57 554, 2022.

[7] A. R. Muhammad, P. Sukarno, and A. A. Wardana, "Integrated security information and event management (siem) with intrusion detection system (ids) for live analysis based on machine learning," *Procedia Computer Science*, vol. 217, pp. 1406–1415, 2023.

[8] S. Tariq, M. Baruwal Chhetri, S. Nepal, and C. Paris, "Alert fatigue in security operations centres: Research challenges and opportunities," *ACM Computing Surveys*, vol. 57, no. 9, pp. 1–38, 2025.

[9] D. G. Havlick and T. H. D. Dao, "Revealing vertical geopolitics: Quantifying the volume of militarised restricted airspaces in the usa using gis," *Transactions of the Institute of British Geographers*, vol. 48, no. 4, pp. 797–810, 2023.
[10] H. M. Shakeel, S. Iram, H. Al-Aqrabi, T. Alsboui, and R. Hill, "A comprehensive state-of-the-art survey on data visualization tools: Research developments, challenges and future domain specific visualization framework," *IEEE Access*, vol. 10, pp. 96 581–96 601, 2022.
[11] N. Moustafa, N. Koroniotis, M. Keshk, A. Y. Zomaya, and Z. Tari, "Explainable intrusion detection for cyber defences in the internet of things: Opportunities and solutions," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 3, pp. 1775–1807, 2023.
[12] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions," *Electronics*, vol. 12, no. 6, p. 1333, 2023.
[13] E. H. Korkut and E. Surer, "Visualization in virtual reality: a systematic review," *Virtual Reality*, vol. 27, no. 2, pp. 1447–1480, 2023.
[14] S. Chakraborty, S. K. Pandey, S. Maity, and L. Dey, "Detection and classification of novel attacks and anomaly in iot network using rule based deep learning model," *SN Computer Science*, vol. 5, no. 8, p. 1056, 2024.
[15] H. Sonwani, M. Divya, A. Dhawan, A. Mantri, H. Kumar *et al.*, "A comprehensive study on threat intelligence platform," in *2022 International Conference on Communication, Computing and Internet of Things (IC3IoT)*. IEEE, 2022, pp. 1–5.
[16] T. F. Ask, K. Kullman, S. Sütterlin, B. J. Knox, D. Engel, and R. G. Lugo, "A 3d mixed reality visualization of network topology and activity results in better dyadic cyber team communication and cyber situational awareness," *Frontiers in big Data*, vol. 6, p. 1042783, 2023.
[17] B. Munsinger, N. Beebe, and T. Richardson, "Virtual reality for improving cyber situational awareness in security operations centers," *Computers & Security*, vol. 132, p. 103368, 2023.
[18] M.-H. M. Chung, Y. A. Yang, L. Wang, G. Cento, K. Jerath, P. Taank, A. Raman, J. H. Chan, and M. H. Chignell, "Enhancing cybersecurity situation awareness through visualization: A usb data exfiltration case study," *Heliyon*, vol. 9, no. 1, 2023.
[19] K. Kim, J. Youn, S. Yoon, J. Kang, K. Kim, and D. Shin, "Study on cyber common operational picture framework for cyber situational awareness," *Applied Sciences*, vol. 13, no. 4, p. 2331, 2023.
[20] D. H. Jeong, J.-H. Cho, F. Chen, L. Kaplan, A. Jøsang, and S.-Y. Ji, "Interactive web-based visual analysis on network traffic data," *Information*, vol. 14, no. 1, p. 16, 2022.
[21] W. Zong, Y.-W. Chow, and W. Susilo, "Interactive three-dimensional visualization of network intrusion detection data for machine learning," *Future Generation Computer Systems*, vol. 102, pp. 292–306, 2020.
[22] L. J. Borges Amaro, B. W. Percilio Azevedo, F. L. Lopes de Mendonca, W. F. Giozza, R. d. O. Albuquerque, and L. J. Garcia Villalba, "Methodological framework to collect, process, analyze and visualize cyber threat intelligence data," *Applied Sciences*, vol. 12, no. 3, p. 1205, 2022.
[23] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "An evaluation framework for network security visualizations," *Computers & Security*, vol. 84, pp. 70–92, 2019.
[24] Y. Feng, J. Li, J. Mirkovic, C. Wu, C. Wang, H. Ren, J. Xu, and Y. Liu, "Unmasking the internet: A survey of fine-grained network traffic analysis," *IEEE Communications Surveys & Tutorials*, 2025.
[25] D. Clark and B. P. Turnbull, "Interactive 3d visualization of network traffic in time for forensic analysis." in *VISIGRAPP (3: IVAPP)*, 2020, pp. 177–184.
[26] H. Shiravi, A. Shiravi, and A. A. Ghorbani, "A survey of visualization systems for network security," *IEEE Transactions on visualization and computer graphics*, vol. 18, no. 8, pp. 1313–1329, 2011.
[27] H. Ahmad, F. Ullah, and R. Jafri, "A survey on immersive cyber situational awareness systems," *Journal of Cybersecurity and Privacy*, vol. 5, no. 2, p. 33, 2025.
[28] V. Cobilean, H. S. Mavikumbure, B. J. Mcbride, B. Vaagensmith, V. K. Singh, R. Li, C. Rieger, and M. Manic, "A review of visualization methods for cyber-physical security: Smart grid case study," *IEEE Access*, vol. 11, pp. 59 788–59 803, 2023.
[29] D. H. Jeong, B.-K. Jeong, and S.-Y. Ji, "Multi-resolution analysis with visualization to determine network attack patterns," *Applied Sciences*, vol. 13, no. 6, p. 3792, 2023.
[30] G. Bendiab, S. Shiaeles, A. Alruban, and N. Kolokotronis, "Iot malware network traffic classification using visual representation and deep learning," in *2020 6th IEEE Conference on Network Softwarization (NetSoft)*. IEEE, 2020, pp. 444–449.
[31] M. Aminu, A. Akinsanya, D. A. Dako, and O. Oyedokun, "Enhancing cyber threat detection through real-time threat intelligence and adaptive defense mechanisms," *International Journal of Computer Applications Technology and Research*, vol. 13, no. 8, pp. 11–27, 2024.
[32] K. D. O. Ofoegbu, O. S. Osundare, C. S. Ike, O. G. Fakeyede, and A. B. Ige, "Real-time cybersecurity threat detection using machine learning and big data analytics: A comprehensive approach," *Computer Science & IT Research Journal*, vol. 4, no. 3, 2024.
[33] M. Rashed, I. T.-D. Viso, and A. I. González-Tablas, "A comparison of cyber intelligence platforms in the context of iot devices and smart homes," *Electronics*, vol. 14, no. 22, p. 4503, 2025.
[34] M. O. Kaya, H. A. Dagdogen, M. Ozdem, and R. Das, "An effective new penetration test approach to detect web attacks on web applications," *Expert Systems with Applications*, p. 129623, 2025.
[35] S. Fujii, N. Kawaguchi, T. Shigemoto, and T. Yamauchi, "Extracting and analyzing cybersecurity named entity and its relationship with noncontextual iocs from unstructured text of cti sources," *Journal of Information Processing*, vol. 31, pp. 578–590, 2023.
[36] N. Yau, *Visualize this: the FlowingData guide to design, visualization, and statistics*. John Wiley & Sons, 2024.
[37] O. T. Taofeek, M. Alawida, A. Alabdulatif, A. E. Omolara, and O. I. Abiodun, "A cognitive deception model for generating fake documents to curb data exfiltration in networks during cyber-attacks," *IEEE Access*, vol. 10, pp.

41 457–41 476, 2022.

[38] M. Alshehri, A. Abugabah, A. Algarni, and S. Almotairi, "Character-level word encoding deep learning model for combating cyber threats in phishing url detection," *Computers and Electrical Engineering*, vol. 100, p. 107868, 2022.

[39] A. Tundis, S. Ruppert, and M. Mühlhäuser, "A feature-driven method for automating the assessment of osint cyber threat sources," *Computers & Security*, vol. 113, p. 102576, 2022.

[40] R. Das and M. Soylu, "A key review on graph data science: The power of graphs in scientific studies," *Chemometrics and Intelligent Laboratory Systems*, vol. 240, p. 104896, 2023.

[41] G. Yu, C. Liu, T. Fang, J. Jia, E. Lin, Y. He, S. Fu, L. Wang, L. Wei, and Q. Huang, "A survey of real-time rendering on web3d application," *Virtual Reality & Intelligent Hardware*, vol. 5, no. 5, pp. 379–394, 2023.

[42] T. N. Alrumaih and M. J. Alenazi, "Cgaad: Centrality- and graph-aware deep-learning model for detecting cyberattacks targeting industrial control systems in critical infrastructure," *IEEE Internet of Things Journal*, vol. 11, no. 13, pp. 24 162–24 182, 2024.

[43] C. Wang, J. Caja, E. Gómez, and P. Maresca, "Procedure for calibrating the z-axis of a confocal microscope: Application for the evaluation of structured surfaces," *Sensors*, vol. 19, no. 3, p. 527, 2019.

[44] B. Duinkharjav, K. Chen, A. Tyagi, J. He, Y. Zhu, and Q. Sun, "Color-perception-guided display power reduction for virtual reality," *ACM Transactions on Graphics (TOG)*, vol. 41, no. 6, pp. 1–16, 2022.

[45] M. O. Kaya and R. Das, "Scalable object-relational modeling for synthesizing multi-format visual analytics of stix-based cyber threat intelligence data," *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems*, vol. 13, no. 2, Jun. 2026.