

## **1. Peak Traffic Hours -> The Dark Hour Rises (Traffic peaks)**

This report shows which hours of the day receive the highest volume of requests to our site. By identifying the most active timeframes, we can ensure resource availability, optimize system performance, and plan support coverage accordingly. It also helps detect usage anomalies if activity spikes occur outside of typical peak windows.

---

## **2. Request Trend with Moving Average -> The Phantom Drop — Request Disturbances**

We analyze hourly request trends with a rolling average to smooth out fluctuations and detect subtle anomalies. The moving average highlights unexpected spikes or dips in activity that raw data might not reveal. This helps us react proactively to performance degradation or traffic surges.

---

## **3. Session Duration Distribution -> Session Shadows — How Long They Linger**

Users are grouped by how long they spend on the site, giving insight into engagement behavior. Short sessions might signal bots or casual bounces, while long ones suggest deeper exploration. This helps optimize design and content for different user types.

---

## **4. Top Visitors by Frequency -> The Council of Frequent Disturbers**

This lists IP addresses with the highest request counts. Frequent visitors can be loyal users, monitoring systems, or suspicious sources. Mapping their origin helps determine intent and regional interest or threats.

---

## **5. Top Users by Unique Pages Visited -> Lords of Navigation — Page-Walkers Revealed**

Ranks IPs based on the number of unique pages they've accessed. High counts may reflect deep curiosity or automated content scraping. It provides a view into who's exploring versus who might be harvesting data.

---

## **6. User Journey Flow -> The Path of the User — Descent into the Dark**

Shows how users move through the site by visualizing URI paths per session. Helps understand navigation flow and spot high-drop-off or high-conversion points. Critical for UX improvement and tracking suspicious behavior trails.

---

## **7. Web Scraper/Bot Detection -> The Hidden Apprentice — Silent Threats Tracked**

Detects users generating many requests in very short timeframes. Bots often access resources faster than humans, and this helps flag them. It's essential for protecting content and server integrity from scraping.

---

## **8. Repeated POST Requests -> The Clones Are Posting Again**

POST requests in bulk can indicate login brute-force attacks or spamming attempts. This report helps track such IPs before they cause damage. It's key for protecting forms, logins, and APIs from abuse.

---

## **9. Multiple 403 Forbidden Errors -> Access Denied... Just as I Have Foreseen**

This identifies IPs triggering 403 errors repeatedly, suggesting attempts to access restricted content. It could mean misconfigured crawlers or attack probes. Spotting these helps block persistent unauthorized access attempts.

---

## **10. Security Monitoring of Sensitive URIs -> Surveillance Grid — All Is Observed**

Tracks access to admin or login pages — common targets for hackers. Monitoring these pages helps detect early reconnaissance. It's one of the first lines of defense for access-based threats.

---

## **11. DDoS Detection -> DDoS Awakens — A Disturbance in the Force**

Highlights IPs flooding the server with unusually high traffic volumes. These patterns indicate potential DDoS attacks. Early detection enables rapid response to prevent service downtime.

---

## 12. Server Error Detection (500+ Errors) -> Revenge of the Server — Chaos in the Logs

Monitors spikes in 500+ server errors using statistical thresholds. This allows us to detect backend instability before users complain. It's vital for diagnosing outages and preventing cascading failures.

- ❑ calculates the **average number of 500+ errors per hour** across the entire dataset.
- ❑ Measures how much the hourly error counts **vary from the average**.
- ❑ A low std\_dev = stable system, A high std\_dev = erratic error behavior

You only see time periods when the error count **significantly exceeds** what's statistically expected

---

## 13. OS Statistics -> Droids in Disguise — OS Signature Breakdown

Breaks down the operating systems used by visitors. It helps us understand whether we're serving mostly mobile, desktop, or suspicious automation systems. Ideal for optimizing UI compatibility and spotting abnormal OS usage.

---

## 14. Geographic Access Map -> Mapping the Empire — Reach Across the Systems

Displays global distribution of user access across countries. Helps identify where users or threats are coming from and if any regional patterns emerge. This view is essential for compliance, localization, and identifying attack hotspots.