**SIEM Dashboards in Cybersecurity**

SIEM (Security Information and Event Management) tools provide an essential platform for monitoring, analyzing, and responding to security threats. Among their key features are **dashboards**, which present security-related data in a visual, accessible format to help analysts make informed decisions quickly.

**1. What Are Dashboards?**

Dashboards present complex data visually, such as through **charts**, **graphs**, and **tables**. Similar to dashboards in apps like weather or fitness trackers, SIEM dashboards summarize critical information in an easily digestible way.

For example:

* A weather app might display metrics like temperature, wind speed, or precipitation trends to help users plan their day.
* SIEM dashboards allow security analysts to monitor metrics like login attempts, network traffic, or system availability.

**2. How Do Security Analysts Use SIEM Dashboards?**

Security analysts leverage SIEM dashboards to quickly identify and respond to potential threats.

**Example Use Case: Investigating Suspicious Login Attempts**

1. **Alert Notification:**  
   An analyst receives an alert about a suspicious login attempt.
2. **Dashboard Investigation:**  
   Using the SIEM dashboard, the analyst examines relevant data, such as:
   * **Timeline of Login Attempts:** 500 login attempts over 5 minutes.
   * **Geographic Locations:** Attempts originate from outside the user’s typical locations.
   * **Activity Timing:** Logins occurred outside normal working hours.
3. **Decision-Making:**  
   Based on this information, the analyst determines that the login activity is suspicious and takes appropriate action, such as locking the account or escalating the incident.

**3. Metrics Displayed on SIEM Dashboards**

Dashboards are versatile and can be customized to display a wide range of **metrics**. These metrics can support both security operations and broader organizational goals.

**Key Metrics Examples:**

* **Login and Authentication Activity:**  
  Monitor failed or unusual login attempts.
* **Network Traffic Volumes:**  
  Track incoming and outgoing traffic to detect anomalies.
* **Response Times and Availability:**  
  Assess system performance and downtime.
* **Failure Rates:**  
  Highlight vulnerabilities or weak points in the system.

**4. Customization of Dashboards**

Dashboards can be tailored to meet the needs of different stakeholders within an organization.

**Examples of Custom Dashboards:**

* **For Security Analysts:**  
  Focus on metrics such as:
  + Volume of failed login attempts.
  + Number of detected vulnerabilities.
  + Incoming and outgoing network traffic.
* **For IT Managers or Executives:**  
  Include higher-level metrics like:
  + System uptime and performance.
  + Incident response times.
  + Compliance-related metrics.

**5. Benefits of SIEM Dashboards**

* **Real-Time Monitoring:**  
  Dashboards provide a comprehensive, up-to-date summary of security activities.
* **Enhanced Decision-Making:**  
  Visual representations of data help analysts identify patterns, trends, and anomalies faster.
* **Efficiency:**  
  Simplifies complex data sets, reducing the need for manual analysis.
* **Collaboration:**  
  Metrics and visual summaries are easily shared across teams, helping align efforts.

**6. Moving Forward**

SIEM dashboards play a crucial role in maintaining an organization’s security posture. By combining real-time alerts, visual analytics, and customizable views, they empower security professionals to act swiftly and effectively.

Next, we’ll explore **some common SIEM tools** used across the cybersecurity industry. Stay tuned!