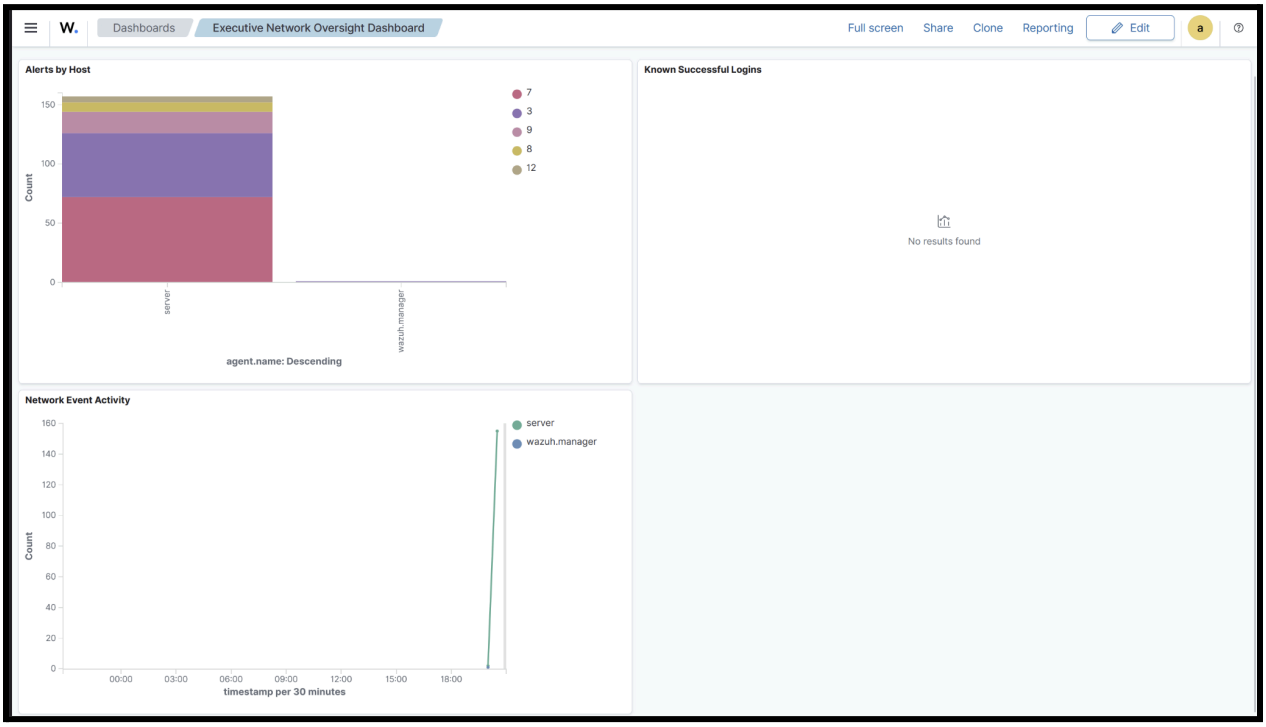
Executive Summary

Dashboard Name: Executive Network Oversight Dashboard

This dashboard provides high-level visibility into the security posture of the business environment. It collects data across all managed hosts to display network activity trends, verify user access accountability, and highlight systems experiencing elevated alert volumes.



Analyst Guide: Using the Network Oversight Dashboard

1. How to Reach the Dashboard

To access the surveillance dashboard:

1. Log into the Wazuh web interface.
2. Navigate to the sidebar menu **(the three lines on the top left)**.
3. Select **Dashboard** under the "OpenSearch Dashboards" section.
4. Select **Executive Network Oversight Dashboard** from the list.

2. Dashboard Sections & Interpretation

A. Network Activity (Packets/Events)

- **What it shows:** A timeline view of network-related security events (firewall logs, web traffic, and connection attempts) aggregated by host.

- **Why it matters:** This provides a baseline of "normal" traffic volume. Sudden spikes in this graph often indicate a network scan, a Denial of Service (DoS) attempt, or a data exfiltration event (large amounts of data being sent).

B. Known Successful Logins

- **What it shows:** A tabular breakdown of every user account that has successfully authenticated to a system, grouped by the Hostname and Username.
- **Why it matters:** Accountability. It allows analysts to verify that only authorized personnel are accessing critical servers.

C. Alerts per Host

- **What it shows:** A bar chart comparing the total volume of security alerts generated by each specific computer/server in the network.
- **Why it matters:** It helps identifying "Noisy" hosts. If one single server is generating 80% of the alerts, it is likely compromised, misconfigured, or under active attack.

3. Tips for Suspicious Activity Detection

When monitoring this dashboard, analysts should look for the following indicators of compromise (IOCs):

- **After-Hours Activity:**
    - Look for: Spikes in the **Network Activity** graph during non-business hours (e.g., 2:00 AM on a Saturday). Unless there is a scheduled backup, this is often an indicator of an attacker moving laterally when no one is watching.
- **The "Brute Force" Success:**
    - Look for: A high bar in the **Alerts per Host** section (indicating many failed attempts/alerts) followed immediately by an entry in the **Known Successful Logins** table for that same host. This suggests an attacker tried many passwords and finally guessed the correct one.

Visualization 1: Known Logins

Goal: "Include a section that details known logins onto various systems."

1. In that "New Visualization" window you are staring at, click **Data Table** (top row, 4th icon).

2. It will likely ask you to "Choose a source". Click **wazuh-alerts-*** (or whatever index pattern appears).
3. **Configure the Table:**
    - **Metrics:** Leave it as "Count".
    - **Buckets:**
        - Click **Add** -> **Split rows**.
        - Select **Terms**.
        - Field: agent.name.
        - Click **Add** -> **Split rows** (again).
        - Select **Terms**.
        - Field: data.srcuser OR user.name (Try user.name first; if empty, try data.srcuser or data.dstuser).
4. **Add the Filter:**
    - In the top search bar, type: rule.groups: "authentication_success"
    - Press Enter.
5. Click **Save and return** (or "Save" in top right).
    - Title: Known Successful Logins.

Visualization 2: Alerts per Host

Goal: "Visualize alerts on a per-host basis."

1. Now you are back at your dashboard. Click **+ Create new** (or "Add") to open that menu again.
2. Click **Vertical Bar** (bottom row, last icon).
3. Select source: **wazuh-alerts-***.
4. **Configure the Chart:**
    - **Buckets (X-axis):**
        - Click **Add** -> **X-axis**.
        - Aggregation: **Terms**.
        - Field: agent.name.
    - (Optional) **Split Series:**
        - Click **Add** -> **Split series**.
        - Aggregation: **Terms**.
        - Field: rule.level.
5. Click **Save and return**.
    - Title: Alerts per Host.

Visualization 3: Network Packets

Goal: "Visibility into network packets... aggregate and per-host."

1. Click **+ Create new** (or "Add") again.

2. Click **Area** (top row, 1st icon) or **Line** (middle row, 2nd icon).
3. Select source: **wazuh-alerts-***.
4. **Configure the Chart:**
    - **Buckets (X-axis):**
        - Aggregation: **Date Histogram**.
        - Field: timestamp.
    - **Split Series:**
        - Click **Add** -> **Split series**.
        - Aggregation: **Terms**.
        - Field: agent.name.
5. **Add the Filter:**
    - In the search bar, type: rule.groups: "firewall" OR rule.groups: "web" (Note: If this shows no data, just remove the filter to see all events as a proxy for activity).
6. Click **Save and return**.
    - Title: Network Activity.