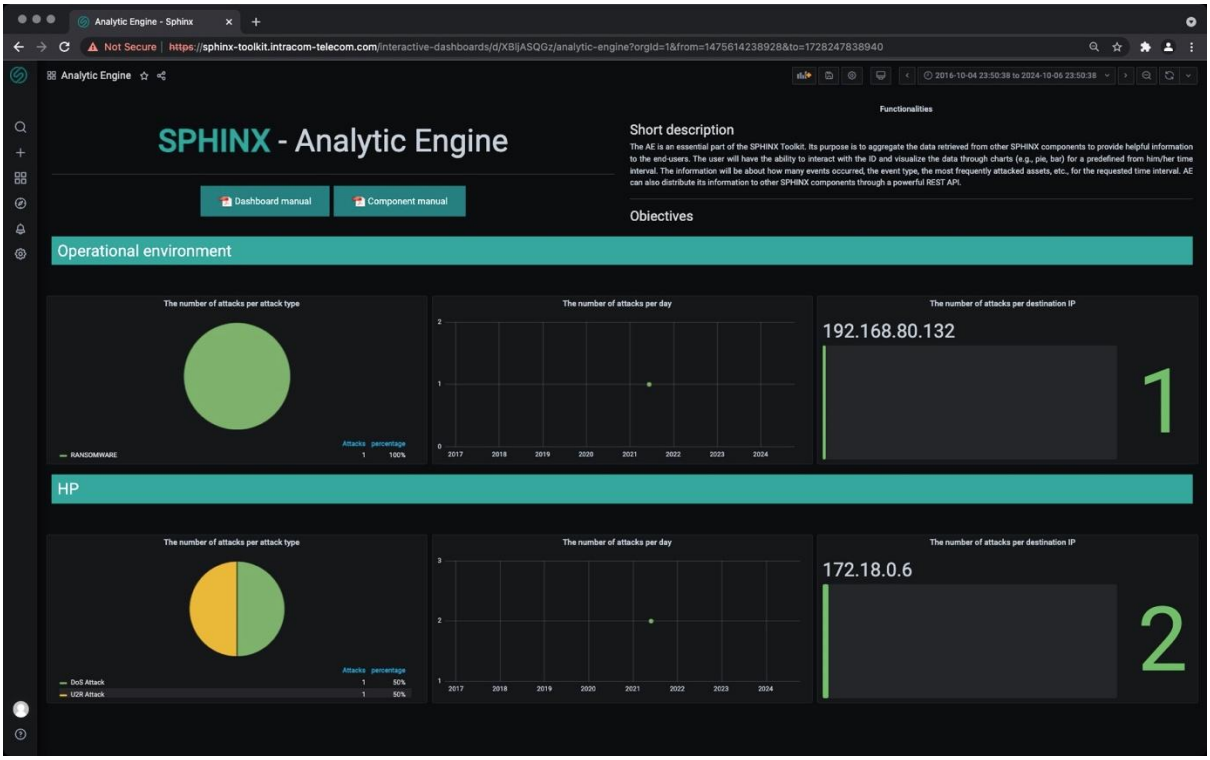
SPHINX AE



AE component uses HP, SIEM, DTM, and AD components to provide insight into the organization's cyber state. Line plots, pie charts, and bar charts support the user in identifying the day and time intervals that the system receives more alerts to increase users' awareness. The user can set a preferable time interval to visualize the historical data. The AE analytics are separated into the HP (i.e., the simulated environment) and the operational environment (i.e., the real one).

- **HP environment**: The HP component uses the AE's API to post reports containing details about the attacks identified (e.g., events type, attacker's IP) by the MLID component in the Honeypot environment. The identified attacks are stored to the AE's MongoDB database to be later aggregated and filtered for the time interval defined by the end-user, resulting in the final HP analytics.
- **Operational environment**: A Kafka consumer on the AE's side receives an alert for an attack published by the SIEM or the DTM to the respective Kafka topics in the actual operational environment. The received alerts are stored in the AE MongoDB database to be later aggregated and filtered for the time interval defined by the end-user, resulting in the final Operational Environment analytics.

For each of the environments, three different types of analytics are calculated.

1. The first type of analytics is the "**number of attacks per attack type**" which calculates the sum of all the reported attacks that share the same unique "attack type."

2. The second type of analytics is "**the number of attacks on a specific day**" within a predefined time interval. It is calculated based on the attack's identification timestamp.
3. The final type of analytics has to do with "**the number of attacks performed on every asset**". It calculates the sum of all the reported attacks that share the same destination IP.