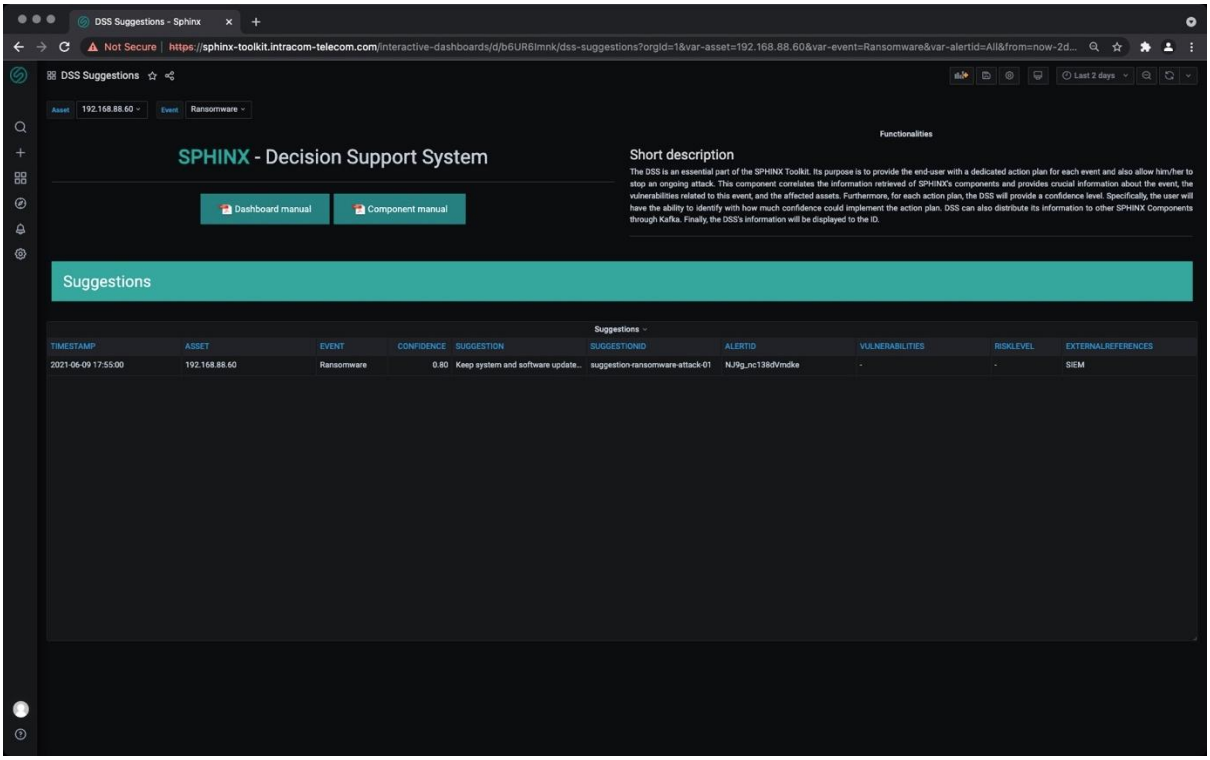
SPHINX DSS



The aim of the SPHINX DSS dashboard is to raise the awareness level of health care organizations and assist them in the decision-making process when dealing with cybersecurity threats. The DSS receives the alerts from several SPHINX components, correlates them with the other components' alerts, and recommends courses of action based on the correlated information.

Whenever the proactive part of the DSS predicts an attack, the following information is displayed:

- **TIMESTAMP**: The timestamp field is the time that the attack was predicted e.g., "2021-03-04 17:55:00.092000".
- **ASSETS**: The correlated assets field provides the assets' IPs that may correlate to the affected asset.
- **EVENT**: The event field is the name of the predicted event (i.e., Probe, DoS).
- **CONFIDENCE**: A confidence level is calculated as a measure of trustworthiness for the report. In this phase the level is a numeric value (i.e., 0-1) given primary directly by the model, presenting how likely the prediction is correct.
- **SUGGESTIONS**: A set of courses of action is proposed by the DSS to stop the ongoing attack (i.e., block the attacker's IP or Port).
- **VULNERABILITIES**: The reported vulnerabilities for the specific asset from the SPHINX Vulnerability Assessment as a Service (VAaaS) report are filtered using Information

Retrieval (IR) techniques, with the ongoing threat's related vulnerabilities from cve.mitre.org. Only the vulnerabilities related with the ongoing threat are reported.

- **RISK LEVEL**: The risk level for the specific asset/threat pair is retrieved from the SPHINX Real-time Cyber Risk Assessment (RCRA) component.
- **EXTERNAL REFERENCES**: A set of external references is retrieved by the Knowledge Base Registry related to the identified threat (i.e., CWE /CAPEC).