Critical Path Exploration Dashboard for Alert-driven Attack Graphs

Azqa Nadeem[1] Sònia Leal Díaz[2] Sicco Verwer[1]

[1]Delft University of Technology [2]La Salle Ramon Llull University

Background

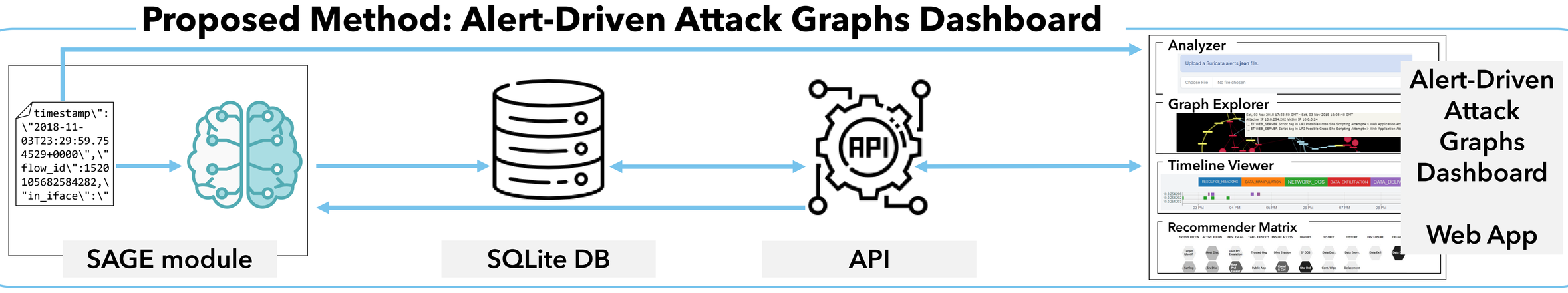
Excessive number of alerts generates alert fatigue, making it difficult to identify attacker strategies.

SAGE extracts per-victim, per-objective Attack Graphs (AG)s by compressing intrusion alerts.

SAGE mitigates alert fatigue, but…

- lacks filtering and interactive capabilities.
- does not identify global patterns.
- it is time-consuming to analyze all AGs.

Proposed Method: Alert-Driven Attack Graphs Dashboard

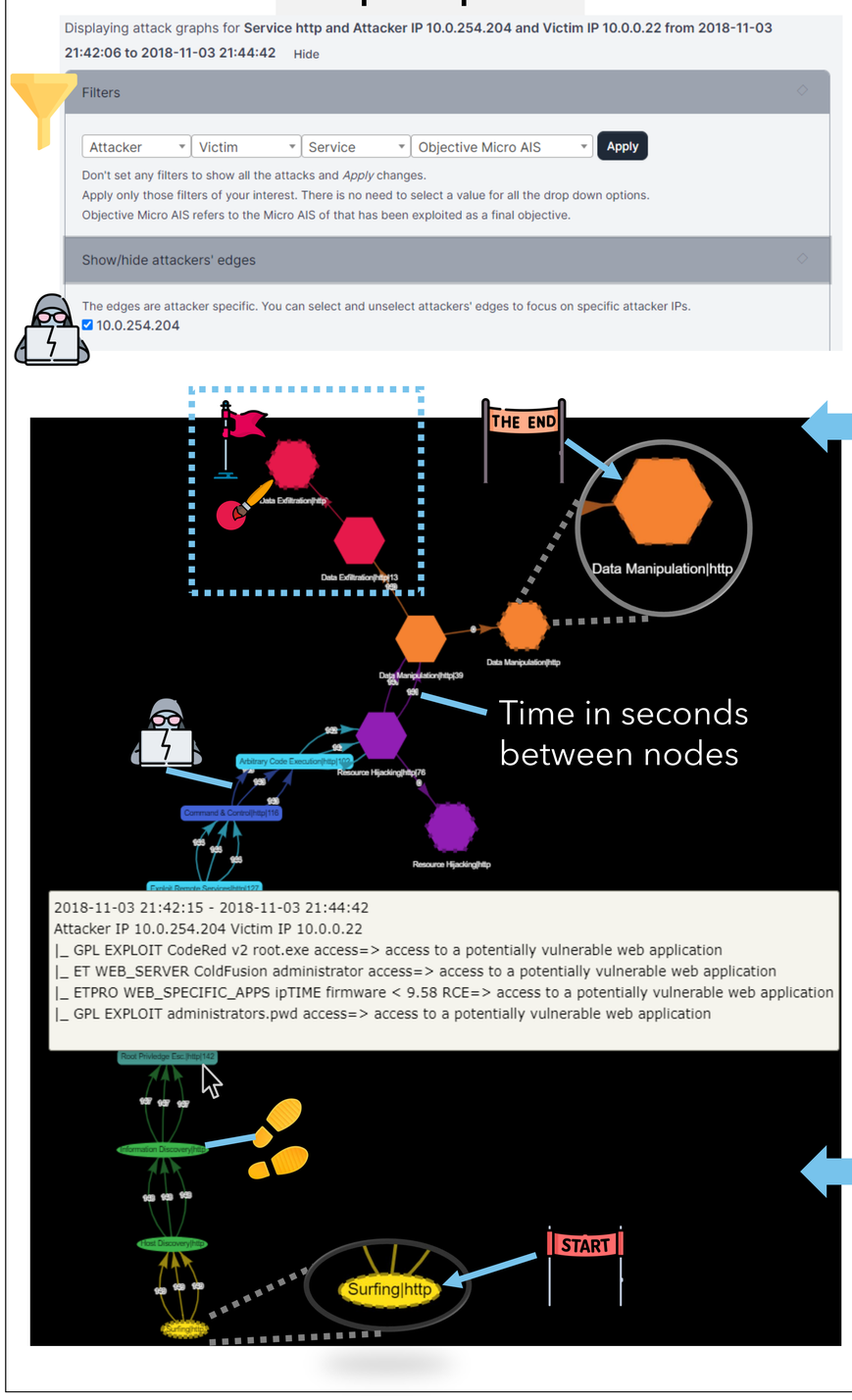


Key Results

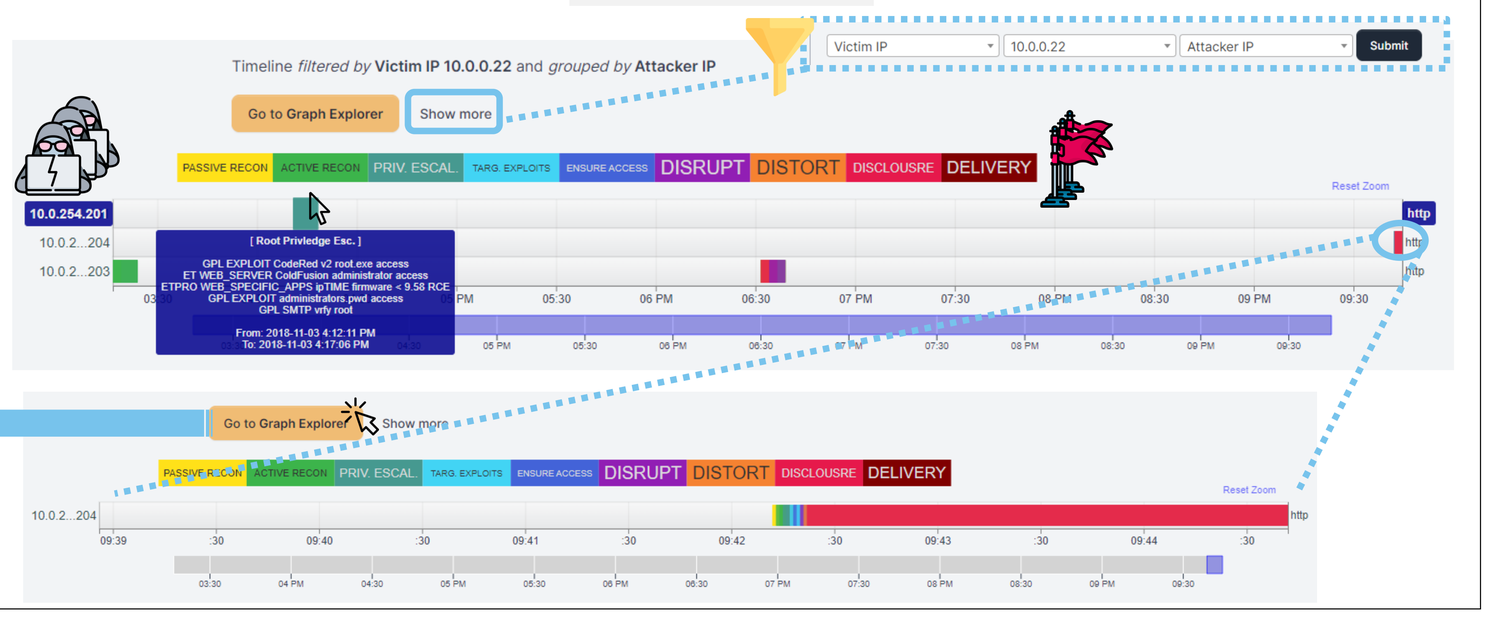
Filter · Attacker · Macro AIS* (tactic) · Micro AIS* (technique) · Node color · Attack starts · Attack ends

* Action-Intent State (AIS) from the Action-Intent Framework, which is based on MITRE ATT&CK®.

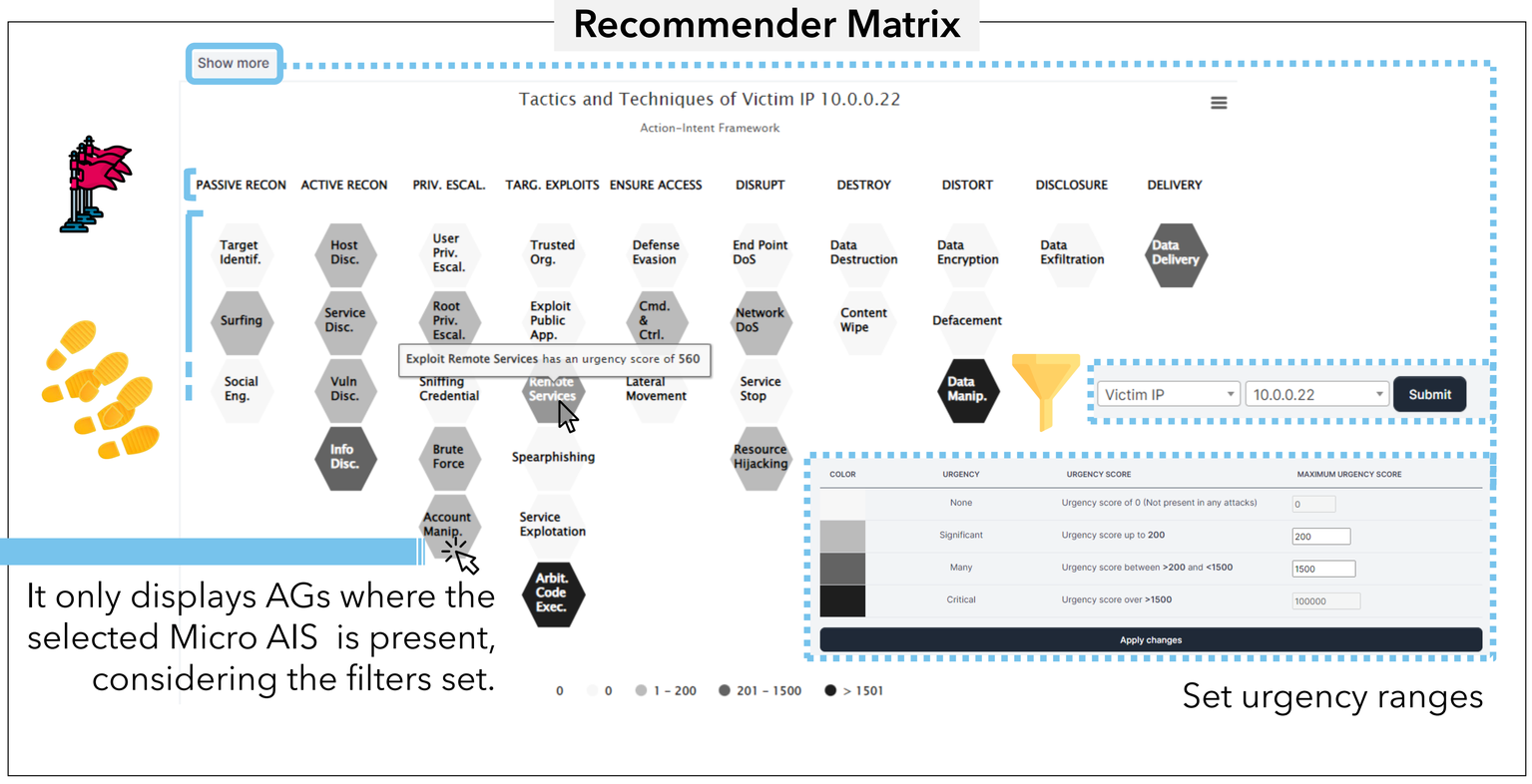
Graph Explorer



Timeline Viewer



Recommender Matrix



It only displays AGs where the selected Micro AIS is present, considering the filters set.

Set urgency ranges

Takeaways

- Interactive and filtering capabilities enable focusing on areas of interest, such as attacks that occurred after work hours or pinpointing data exfiltration paths.
- Visualizing all AGs facilitates understanding how attacks progressed over time, as well as provides detailed insight into attacker strategies and the related alerts triggered at each attack stage.
- The effort of assessing attacks is reduced by consolidating all AGs into one location. Prioritization is used to accurately detect the most urgent strategies used by attackers that should be addressed first.

Future Work

- In-depth evaluation with security practitioners
- Enhance the dashboard's User Experience
- Utilize graph DB