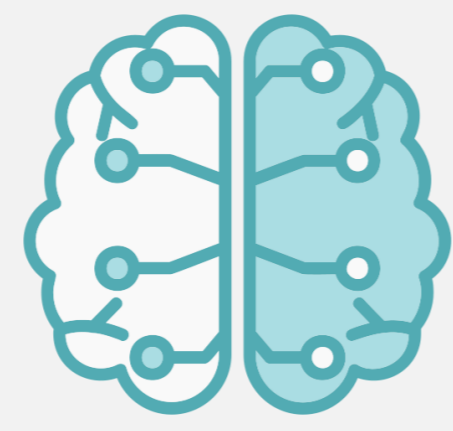


Critical Path Exploration Dashboard for Alert-driven Attack Graphs

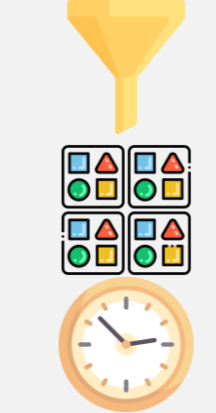
Background

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



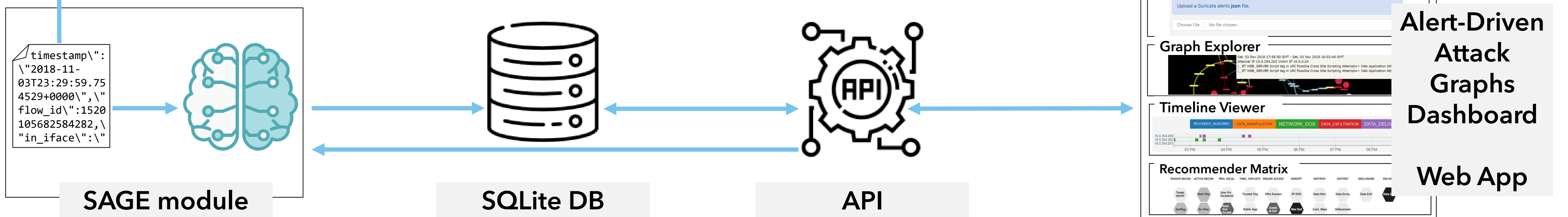
SAGE extracts per-victim, per-objective Attack Graphs (AG)s by compressing intrusion alerts.

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

Displaying attack graphs for Service http and Attacker IP 10.0.254.204 and Victim IP 10.0.0.22 from 2018-11-03 21:42:06 to 2018-11-03 21:44:42

Filters: Attacker, Victim, Service, Objective, Micro AIS

Time in seconds between nodes

Timeline Viewer

Timeline filtered by Victim IP 10.0.0.22 and grouped by Attacker IP

Recommender Matrix

Tactics and Techniques of Victim IP 10.0.0.22

PASSIVE RECON	ACTIVE RECON	PRIV. ESCAL.	TARG. EXPLOITS	ENSURE ACCESS	DISRUPT	DESTROY	DISTORT	DISCLOSURE	DELIVERY
Target Identif.	Host Disc.	User Priv. Escal.	Trusted Org.	Defense Evasion	End Point DoS	Data Destruction	Data Encryption	Data Exfiltration	Data Delivery
Surfing	Service Disc.	Root Priv. Escal.	Exploit Public App.	Cmd. & Ctrl.	Network DoS	Content Wipe	Defacement		
Social Eng.	Vuln Disc.	Sniffing Credential	Remote Services	Lateral Movement	Service Stop				
	Info Disc.	Brute Force	Spearphishing	Resource Hijacking					
	Account Manip.		Service Exploitation						
			Arbit. Code Exec.						

Exploit Remote Services has an urgency score of 560

Set urgency ranges

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

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

