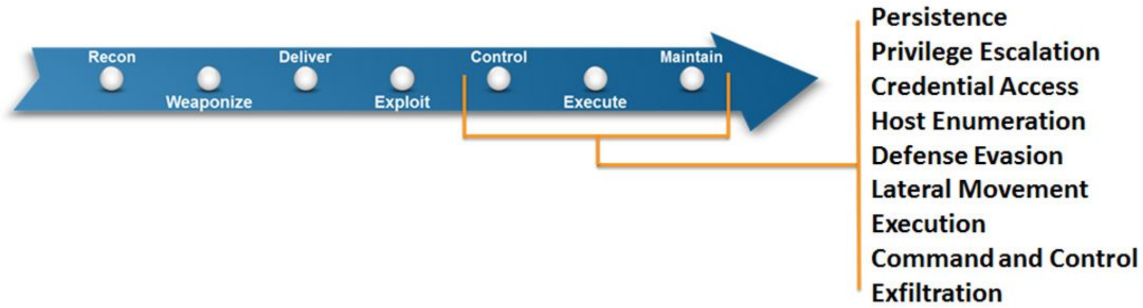
Windows Log Analysis using MITRE ATT&CK Frame

Rony Xavier(rx294)

MITRE’s Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) is a curated knowledge base and model for cyber adversary behavior, reflecting the various phases of an adversary’s lifecycle and the platforms they are known to target.
https://attack.mitre.org/wiki/Main_Page

The Cyber Analytics Repository (CAR) is a knowledge base of analytics developed by MITRE based on the Adversary Tactics, Techniques, and Common Knowledge (ATT&CK™)threat model.
https://car.mitre.org/wiki/Main_Page

Using ATT&CK™ threat model to analyze Windows Event Logs can expose the presence of Advanced Persistent Threat (APT) on enterprise system that might evade traditional Anti-virus systems.



Correlating possible adversary tactics detected through the analysis, to stages in the ATT&CK Frame will expose systems that are at a higher probability of infection.

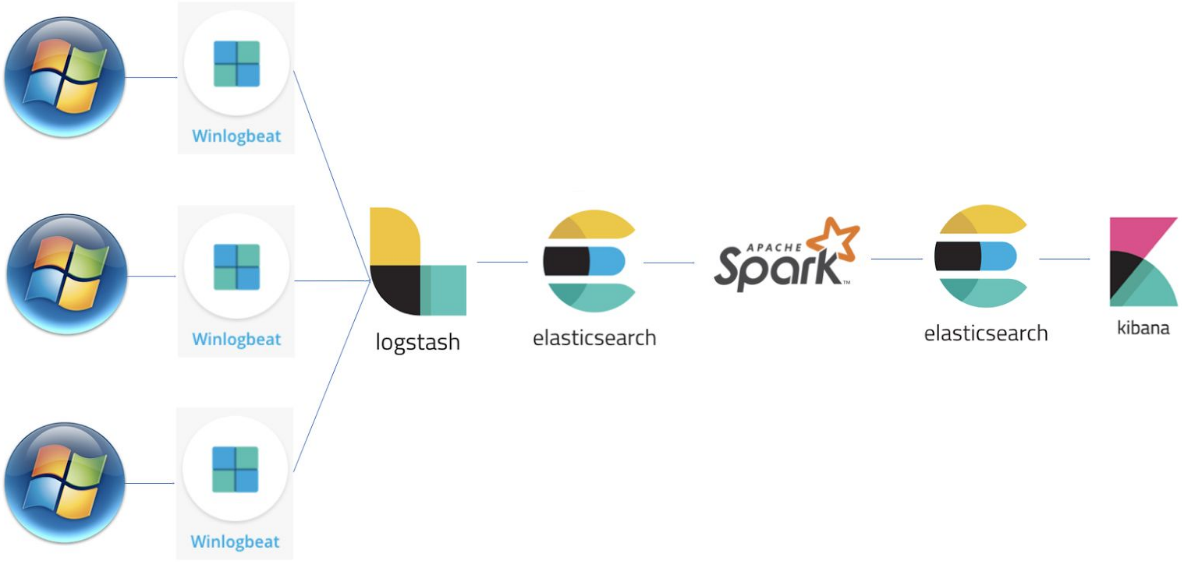
The CAR analytics repository provides pseudocode to analyze Windows event logs to track Adversary Tatic.

For example
CAR-2013-02-008: Simultaneous Logins on a Host :

```
users_list = search UserSession:Login
users_grouped = group users_list by hostname
users_grouped = from users_grouped select min(time) as earliest_time, max(time) as latest_time count(user) as user_count
multiple_logins = filter users_grouped where (latest_time - earliest_time <= 1 hour and user_count > 1)
output multiple_logins
```

Analytic: CAR-2013-02-008: Simultaneous Logins on a Host ----> Attack Technique : Valid Accounts ----> Tactics: Defense Evasion, Persistence, Privilege Escalation

The proposed system will be able to collect and analyze logs at an enterprise level from multiple windows system.



The Windows Event Logs will be collected from multiple systems using WinlogBeat and loaded to elastic cluster using Logstash. The logs in the Elasticsearch is analyzed using Apache Spark and the results of the analysis is stored to Elasticsearch and is visualized using Kibana.