UNIVERSITÉ Concordia UNIVERSITY

Proactive Non-Disruptive Cluster-level Mitigation in Container-based Environment

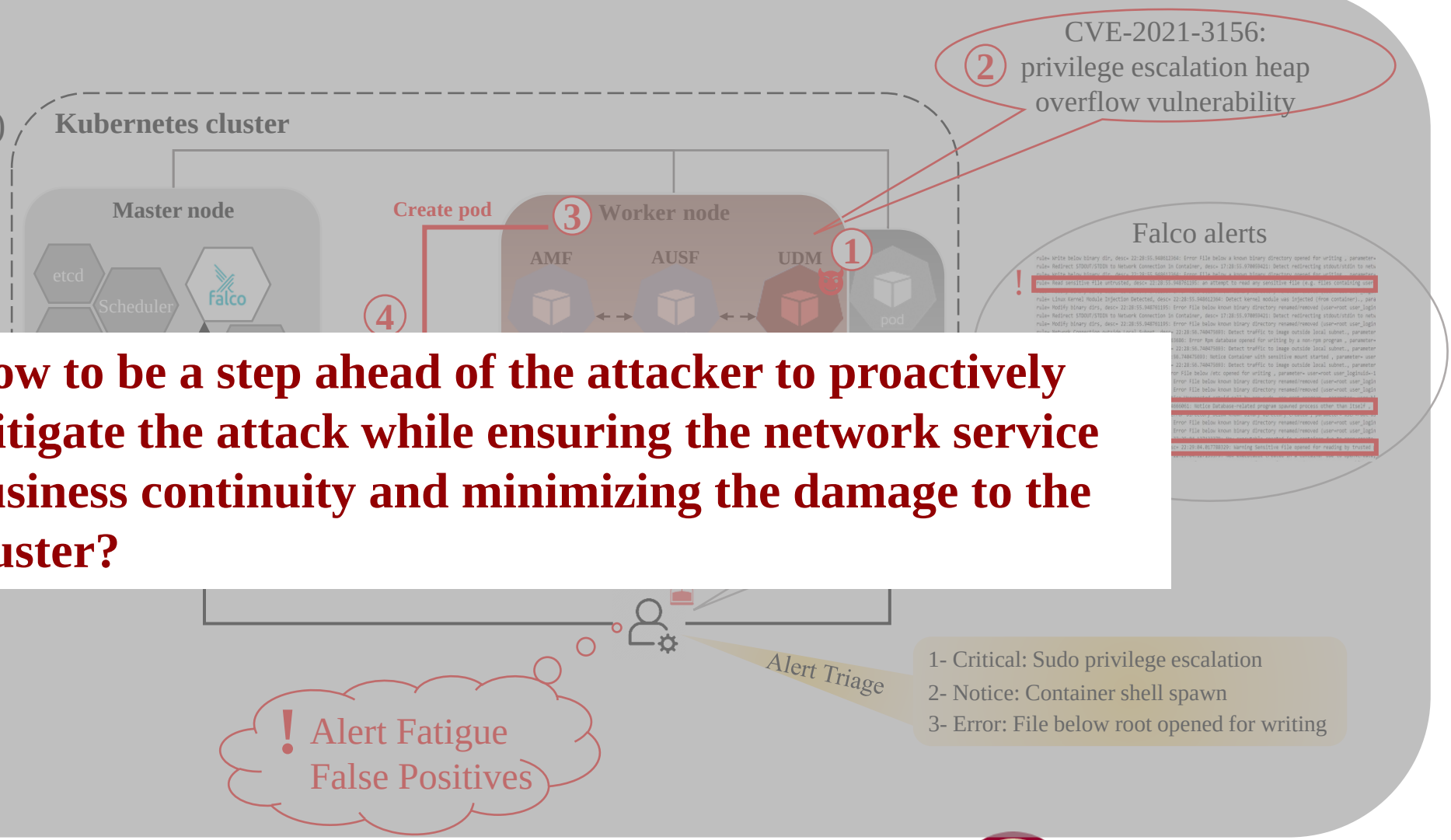
Sima Bagheri

Agenda

- Motivation
- Methodology with Running Example
- Preliminary Results
- Summary and Next Steps

Motivation

- Critical vulnerabilities in Kubernetes (e.g., CVE 2021-3156) can bring **the whole multi-tenant cluster** and **all customer containers** under the control of the attacker
- **Falco**, runtime security too can detect attack when it o
- **Not** all Falco alerts are rela to attack
- Great demand on alert triage and expert analysis

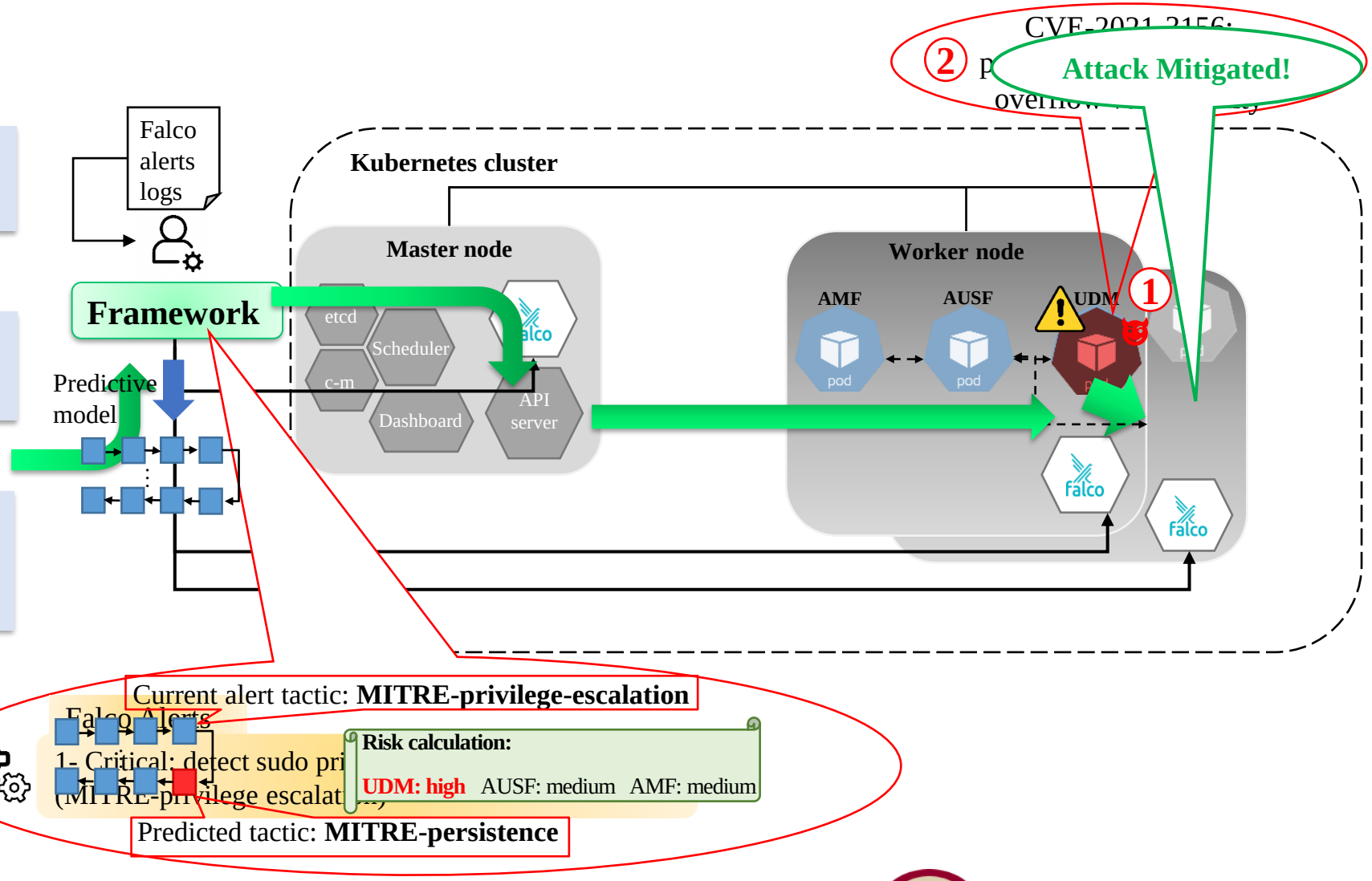


Methodology: Running Example

I - Learn Falco alerts sequence dependencies from alert logs via a predictive model

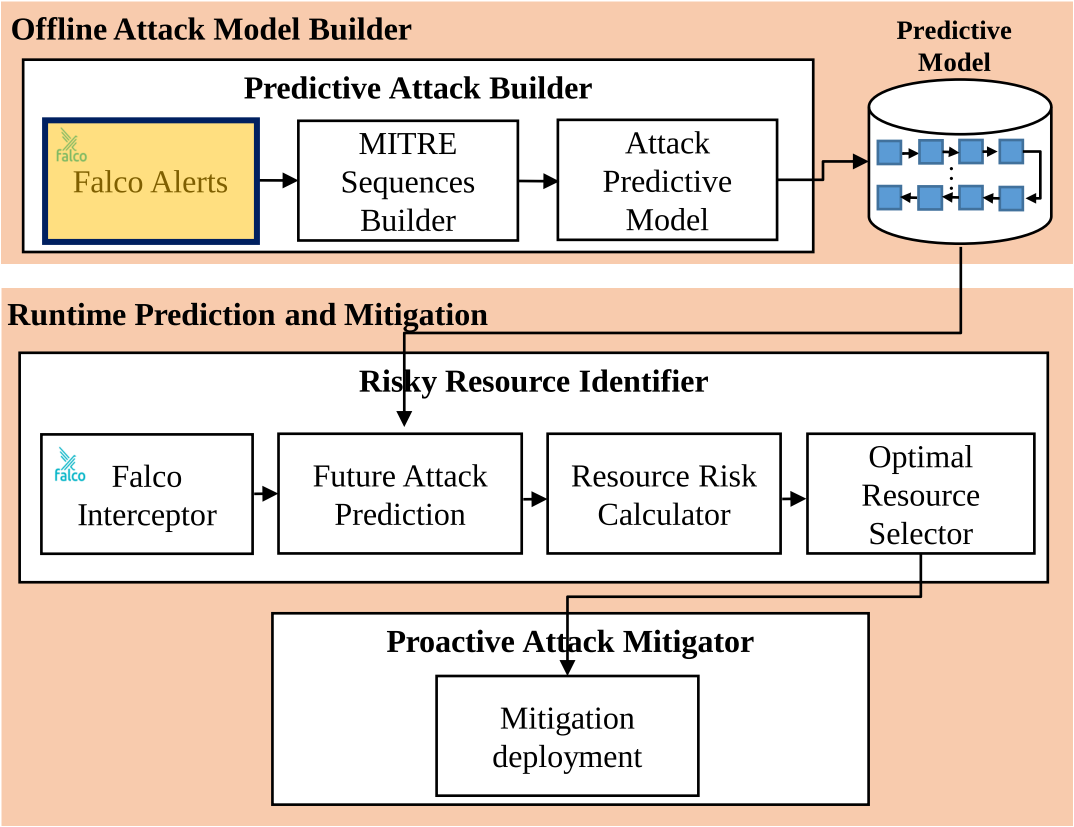
II- Predict the attacker next step in terms of MITRE tactic based on the current seen alert

III- Perform resource risk calculation and deploy non-disruptive mitigation (i.e., migration) to stop the attacker

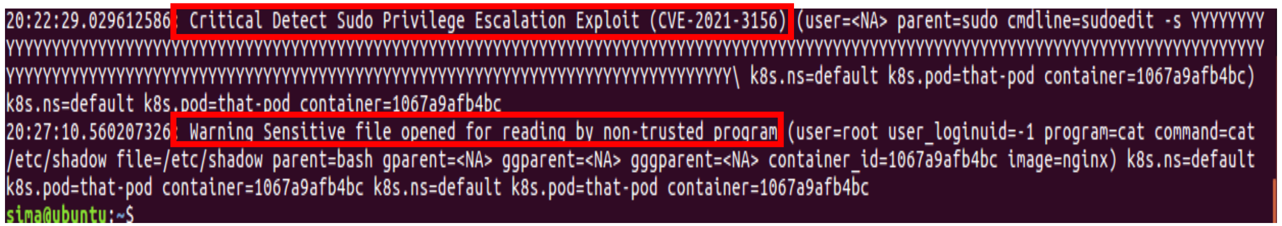


Preliminary Results

Framework Architecture



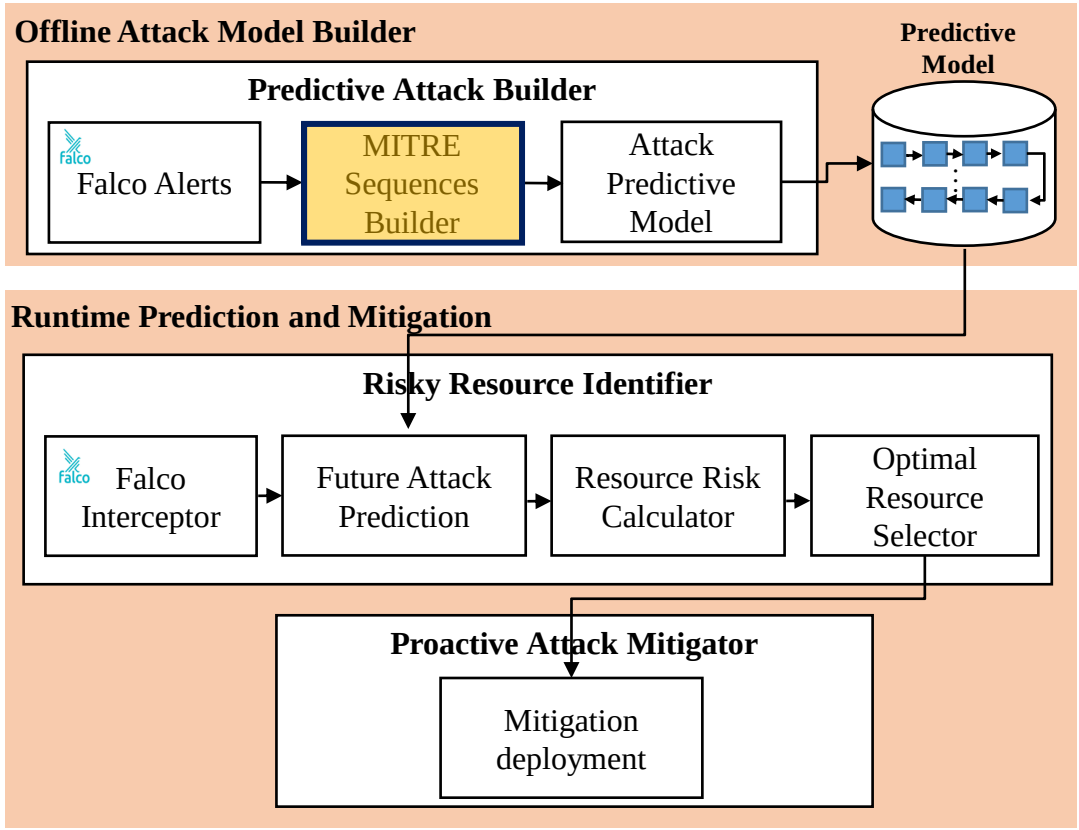
- Example of Falco alerts



- Dataset of Falco alerts collected from the simulation of attacks during the normal operation of cluster:
  - Strategic web compromise (SWC): CVE-2015-5122
  - APT3: CVE-2015-3113
  - APT29 (Cozy bear)
  - Etc…

Preliminary Results

Framework Architecture

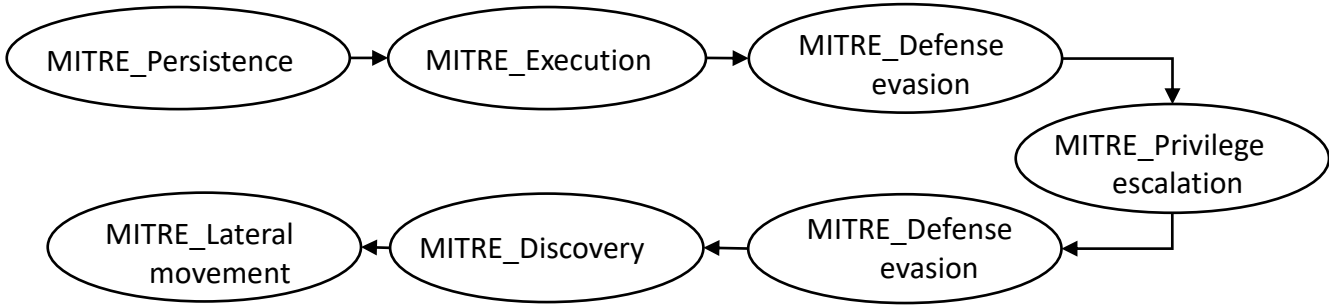


- Falco alerts collected in JSON format

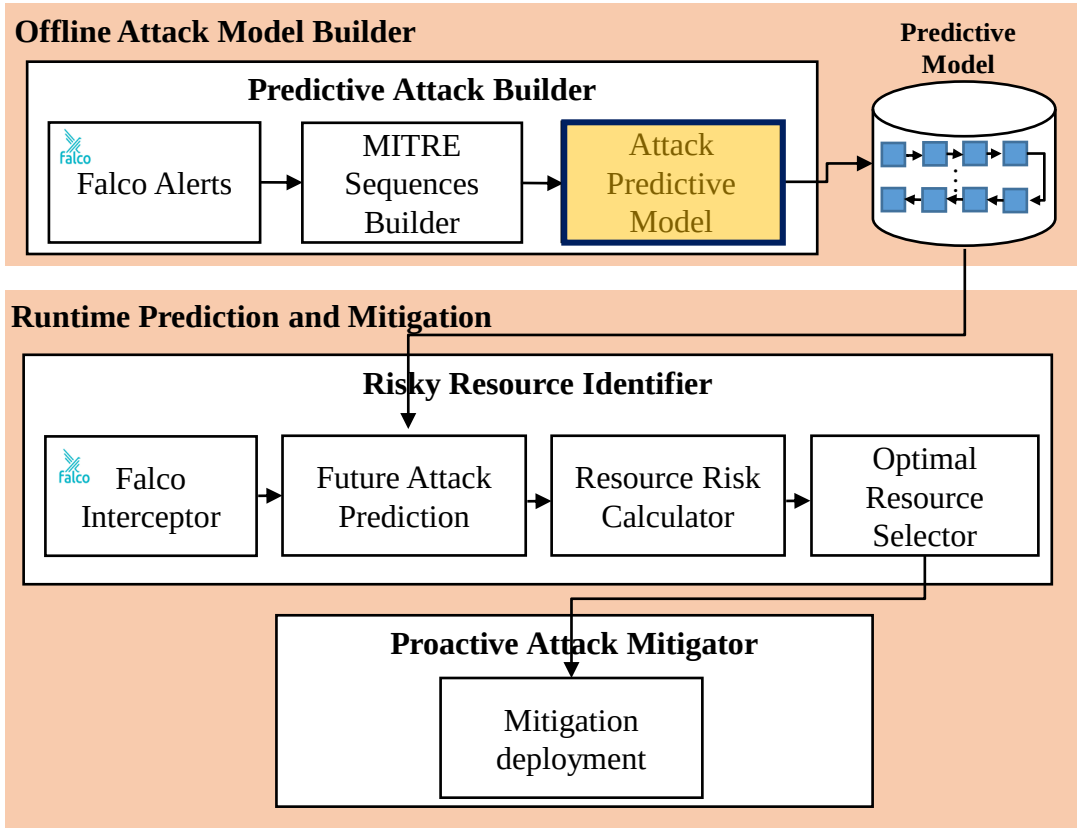

```
"output": "20:32:59.895623281: Notice A shell was spawned in a container with an attached terminal
"priority": "Notice",
"rule": "Terminal shell in container",
"source": "syscall",
"tags": [
  "container",
  "mitre_execution",
  "shell"
```


- Collect the MITRE tactic associated with each Falco alert
- Generate sequences of MITRE tactics

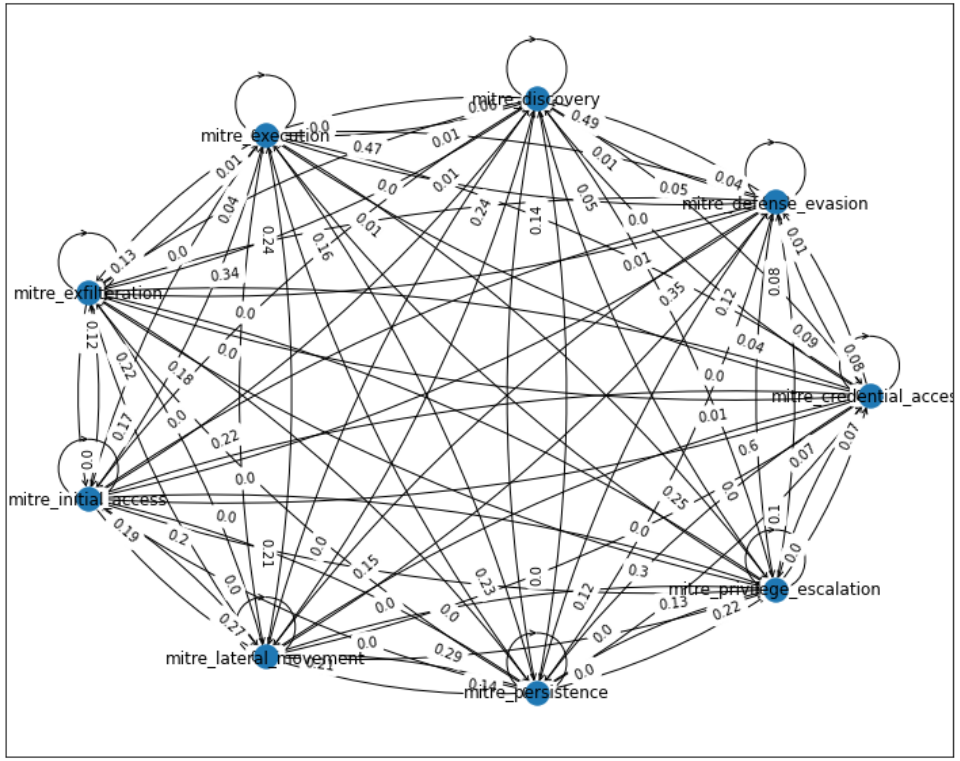
Example of MITRE tactic sequence for APT 29



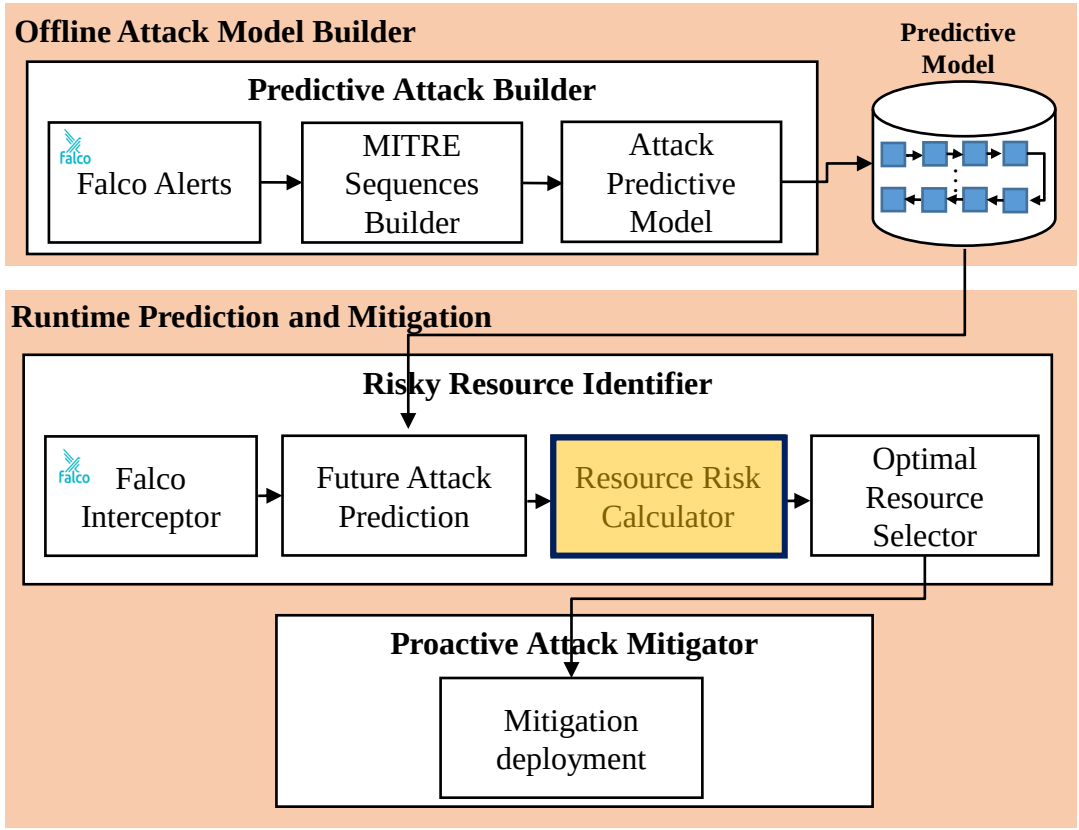
Framework Architecture



- Build the predictive model out of the sequence of tactics



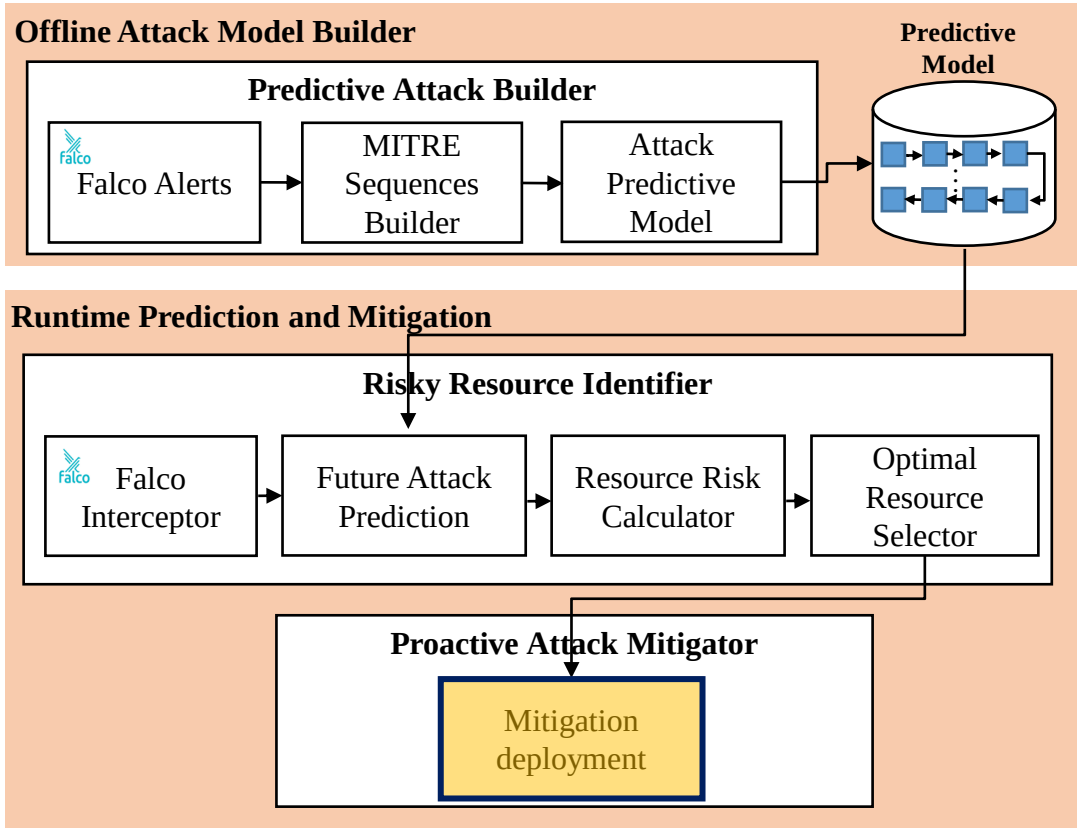
Framework Architecture



- **Risk score**: (∑ alert priority × tactic_severity) × (∑ predicted_tactic_prob × tactic_severity) × downtime_sensitivity × context_severity

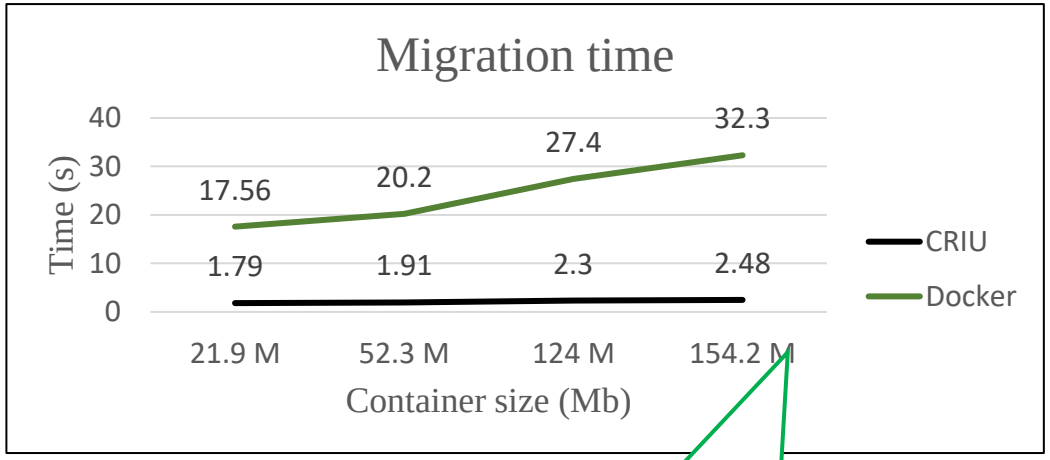
alert priority	Assigned priority (e.g., critical, warning) inside the Falco alert
tactic severity	Average severity score for the alert tactics
predicted tactic probability	The probability of predicted tactic via predictive model
downtime sensitivity	The degree of downtime sensitivity for the container migration
context severity	Severity score for suspicious parameters inside the Falco alerts (e.g., used command, user)

Framework Architecture



Migration of containers performance experiment:

- CRIU: Checkpoint/Restore In Userspace
- Docker: loading the latest safe image of the container



Migration using CRIU achieves better time performance

Summary and Next Steps

- Summary
  - Built a predictive model based on MITRE tactics and use it to predict the attacker next move
  - Developed a resources risk optimization score
  - Experimented with migration as potential mitigation for the highly risky resource using CRIU
  - By predicting and optimizing we can reduce the risks without disrupting business continuity through migration
- Next steps
  - Experiment and validate the risk score
  - Experiments on attack damage, migration time, effectiveness, and overhead
  - Evaluation using real attack data

Thank you!