UNIVERSITÉ Concordia UNIVERSITY

IEEE ICC™ 2023

Warping the Defence Timeline: Non-disruptive Proactive Attack Mitigation for Kubernetes Clusters

Sima Bagheri, Hugo Kermabon-Bobinnec, Suryadipta Majumdar, Yosr Jarraya, Lingyu Wang, Makan Pourzandi

NSERC CRSNG

ERICSSON

29 May 2023

Agenda

- Context
- Motivation
- Methodology
- Implementation/Experiments
- Conclusion

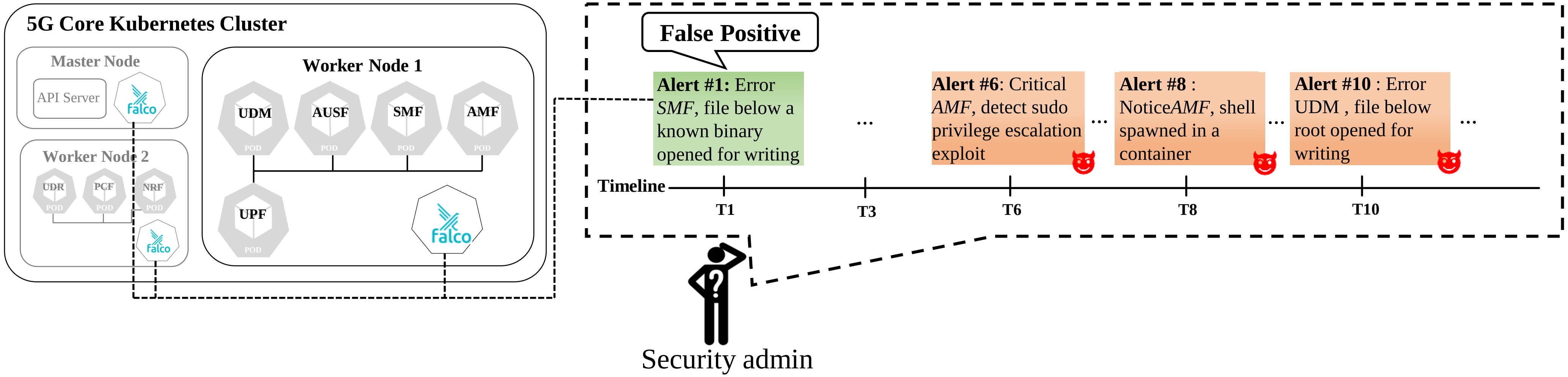
Context

- Critical vulnerabilities in Kubernetes (e.g., CVE-2021-3156) can bring **the whole multi-tenant cluster** and **all customer containers** under attack.

- **Falco**, Kubernetes runtime security tool, can detect attack when it occurs.

- **Not all** Falco alerts are related to attack (false positive).

- Huge demand on **alert triage** and **expert analysis**.



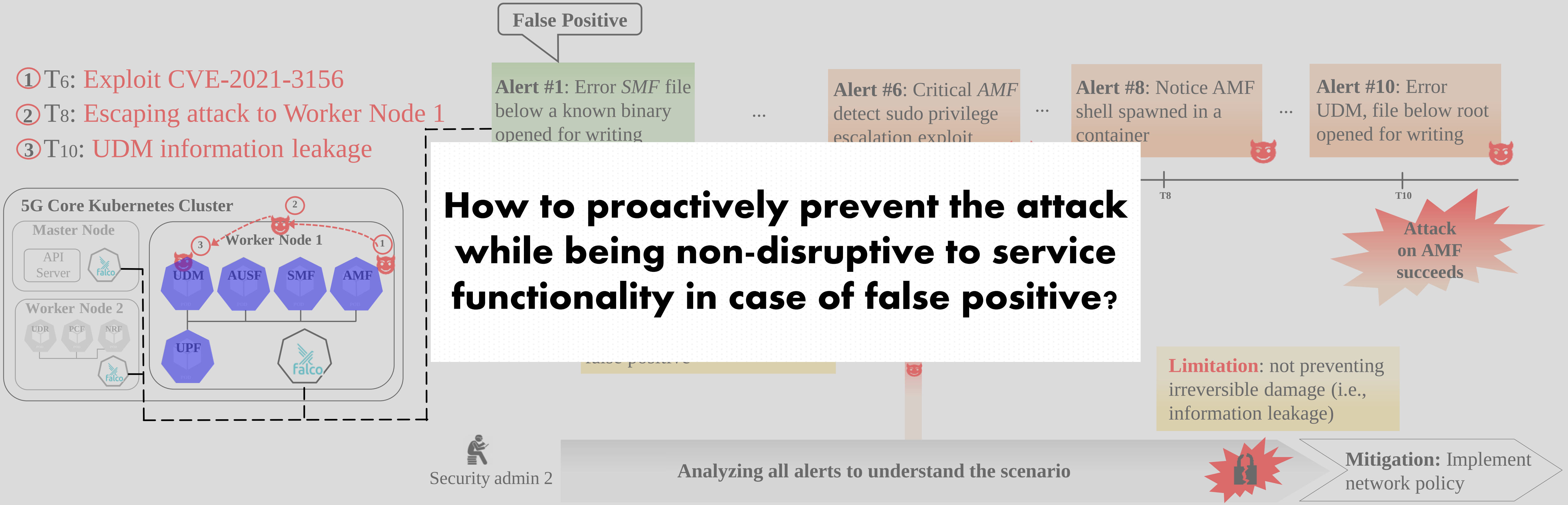
Alert #1: Error *SMF*, file below a known binary opened for writing

Alert #6: Critical *AMF*, detect sudo privilege escalation exploit

Alert #8 : Notice*AMF*, shell spawned in a container

Alert #10 : Error UDM , file below root opened for writing

Motivation



① T6: Exploit CVE-2021-3156
② T8: Escaping attack to Worker Node 1
③ T10: UDM information leakage
5G Core Kubernetes Cluster
Master Node
API Server
Falco
Worker Node 2
UDR
PCF
NRF
Worker Node 1
UDM
AUSF
SMF
AMF
UPF
False Positive
Alert #1: Error *SMF* file below a known binary opened for writing
…
Alert #6: Critical *AMF* detect sudo privilege escalation exploit
Alert #8: Notice AMF shell spawned in a container
Alert #10: Error UDM, file below root opened for writing
T8
T10
Attack on AMF succeeds
Limitation: not preventing irreversible damage (i.e., information leakage)
Security admin 2
Analyzing all alerts to understand the scenario
Mitigation: Implement network policy

How to proactively prevent the attack while being non-disruptive to service functionality in case of false positive?

Our Solution

WARP the Defense Timeline: Non-disruptive Proactive Attack Mitigation for Kubernetes Clusters

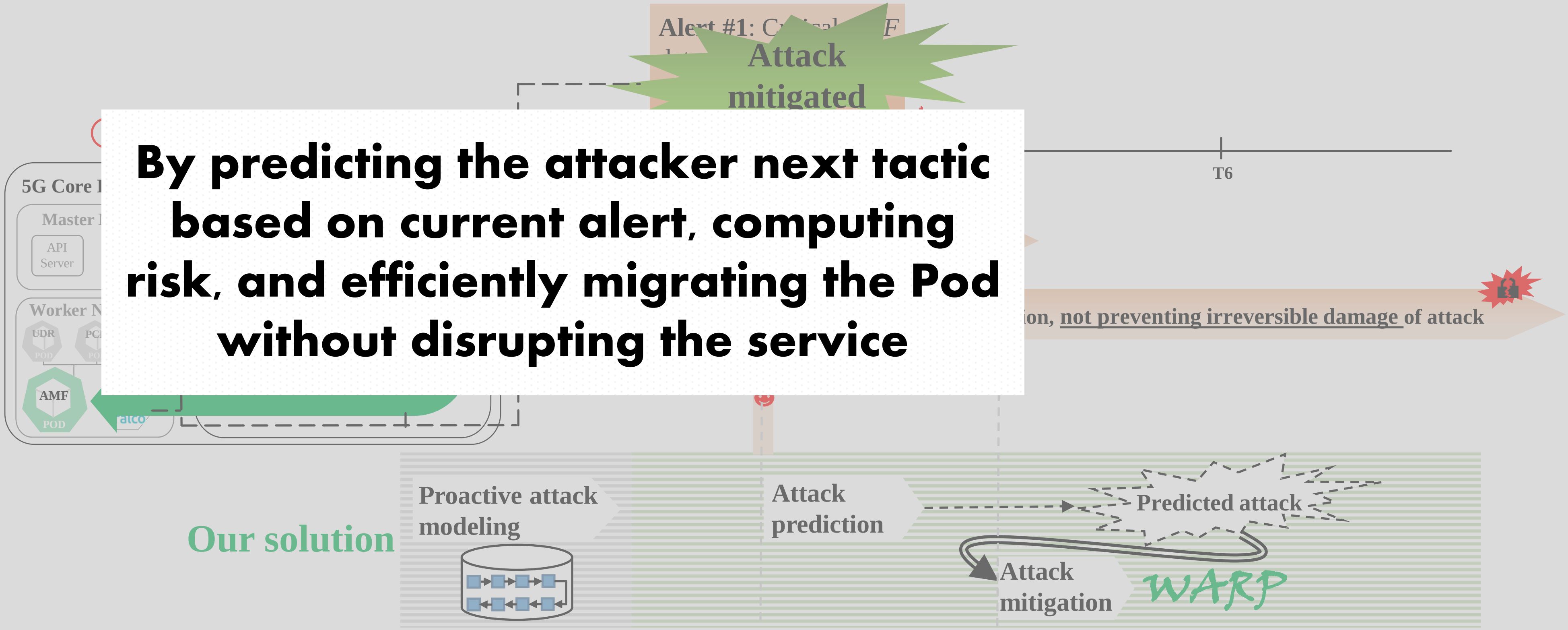
I- Proactive predictive model generation based on MITRE ATT&CK tactics

II- Attack prediction using risk score

III- Non-disruptive attack mitigation to *WARP* the defence

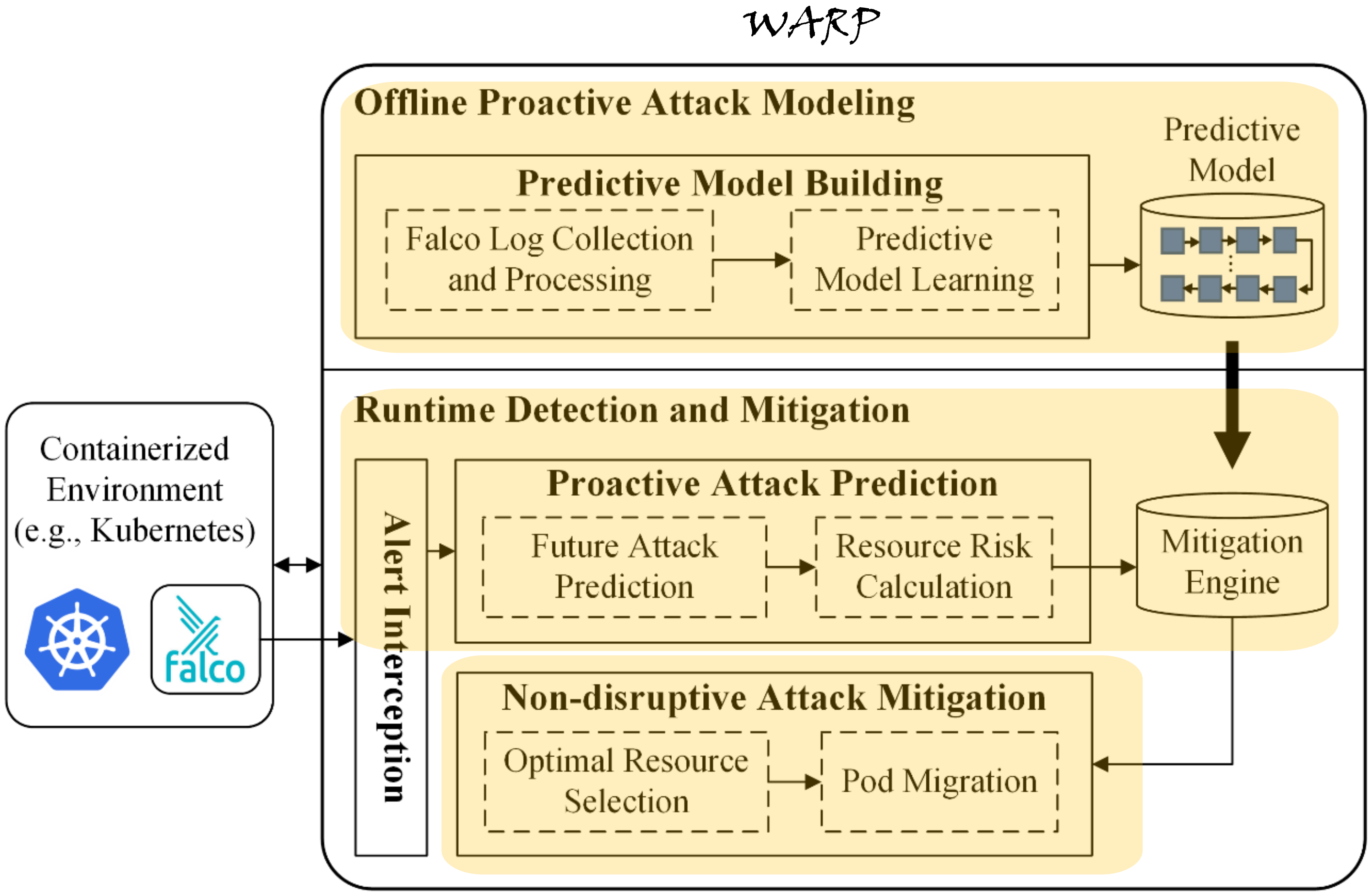
Benefits:

- No service disruption
- Prevention of irreversible damage

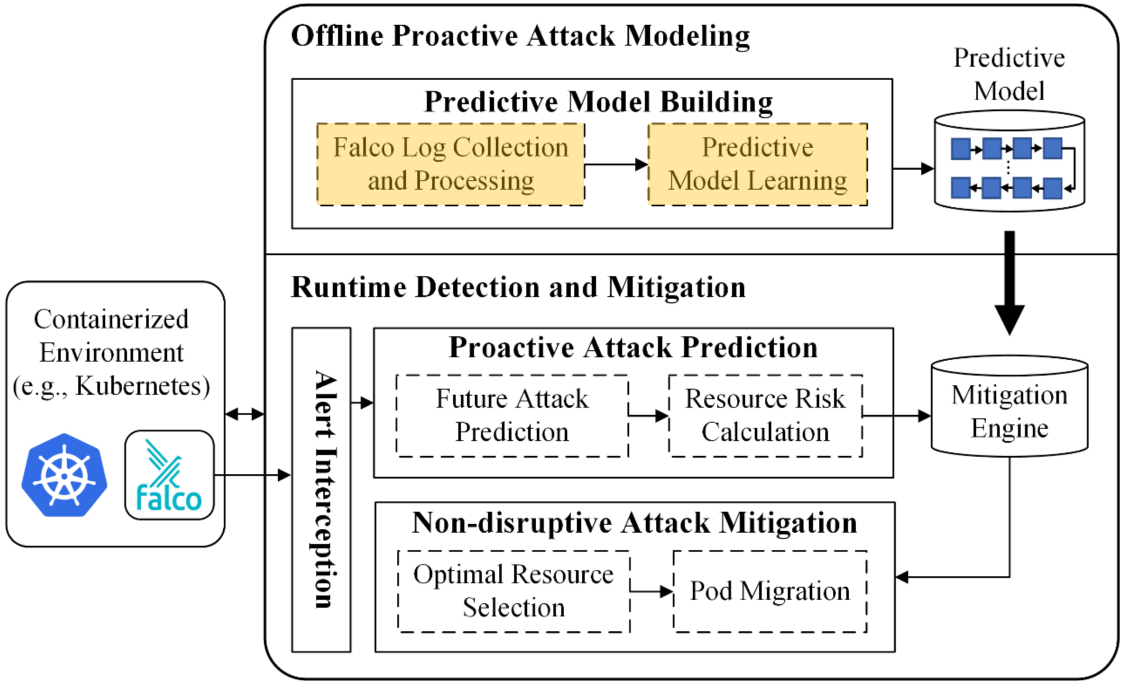


By predicting the attacker next tactic based on current alert, computing risk, and efficiently migrating the Pod without disrupting the service

Methodology Overview


WARP
Offline Proactive Attack Modeling
Predictive Model Building
Falco Log Collection and Processing
Predictive Model Learning
Predictive Model
Runtime Detection and Mitigation
Alert Interception
Proactive Attack Prediction
Future Attack Prediction
Resource Risk Calculation
Mitigation Engine
Non-disruptive Attack Mitigation
Optimal Resource Selection
Pod Migration
Containerized Environment (e.g., Kubernetes)
falco

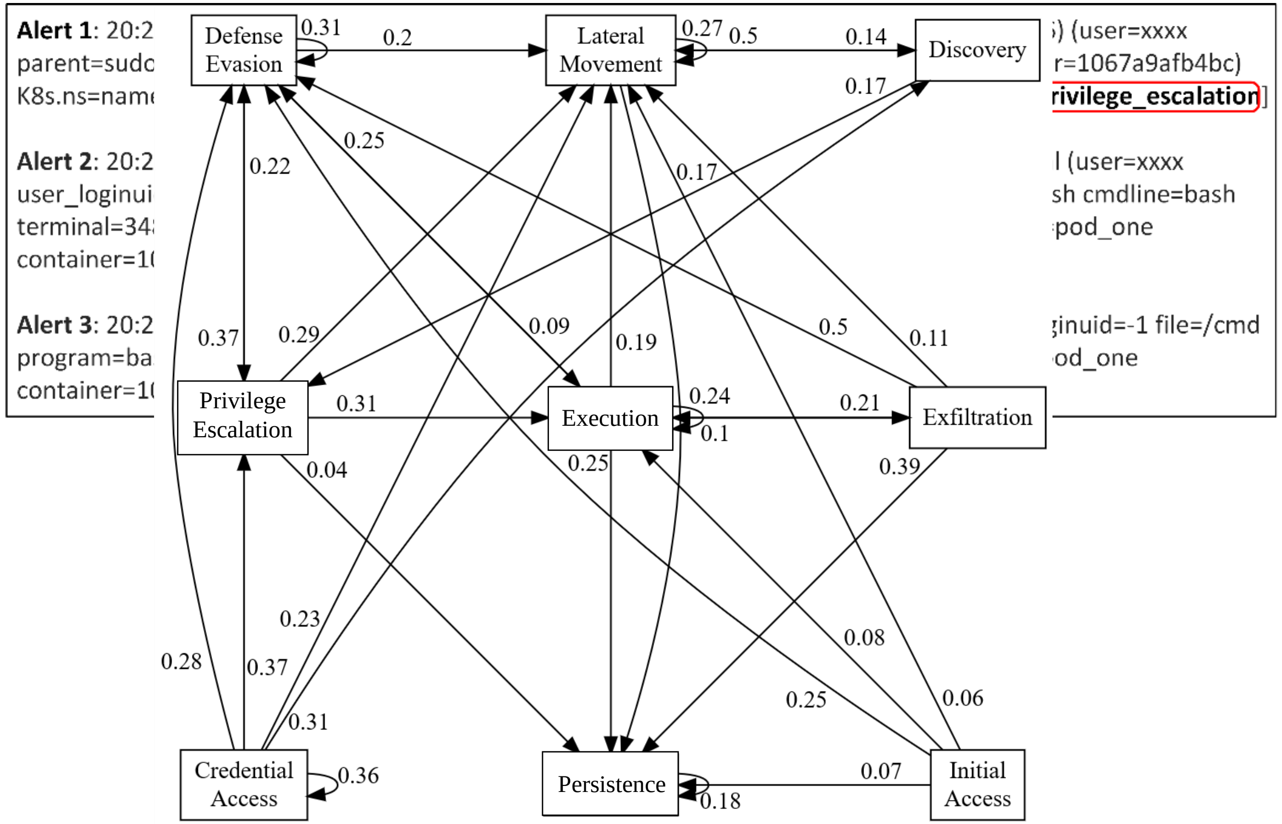
Methodology



Offline Proactive Attack Modeling
Predictive Model Building
Falco Log Collection and Processing
Predictive Model Learning
Predictive Model
Runtime Detection and Mitigation
Containerized Environment (e.g., Kubernetes)
falco
Alert Interception
Proactive Attack Prediction
Future Attack Prediction
Resource Risk Calculation
Mitigation Engine
Non-disruptive Attack Mitigation
Optimal Resource Selection
Pod Migration

WARP

- Falco Log Collection and Processing
- Predictive Model Learning (i.e., Bayesian network)

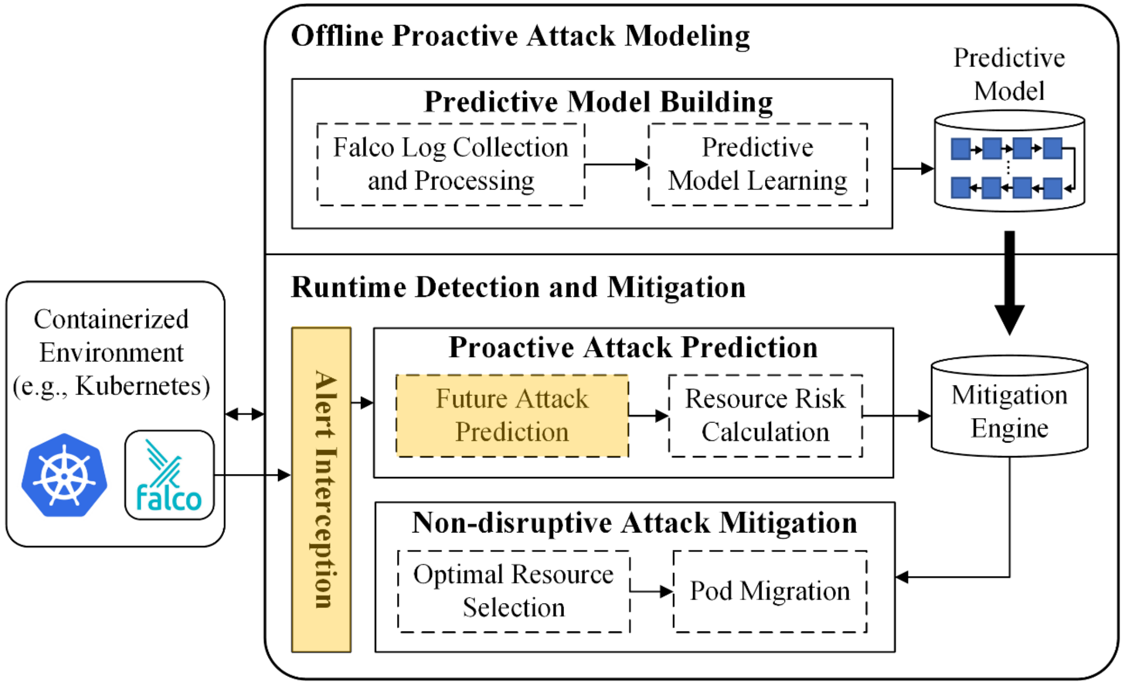


```
Alert 1: 20:2          ;) (user=xxxx
parent=sudo            r=1067a9afb4bc)
K8s.ns=name            rivilege_escalation]

Alert 2: 20:2          l (user=xxxx
user_loginui           sh cmdline=bash
terminal=34:           pod_one
container=10

Alert 3: 20:2          ginuid=-1 file=/cmd
program=ba             od_one
container=10
```

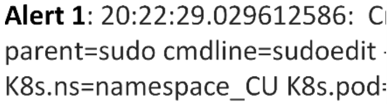
Methodology


Offline Proactive Attack Modeling
Predictive Model Building
Falco Log Collection and Processing
Predictive Model Learning
Predictive Model
Runtime Detection and Mitigation
Containerized Environment (e.g., Kubernetes)
falco
Alert Interception
Proactive Attack Prediction
Future Attack Prediction
Resource Risk Calculation
Mitigation Engine
Non-disruptive Attack Mitigation
Optimal Resource Selection
Pod Migration

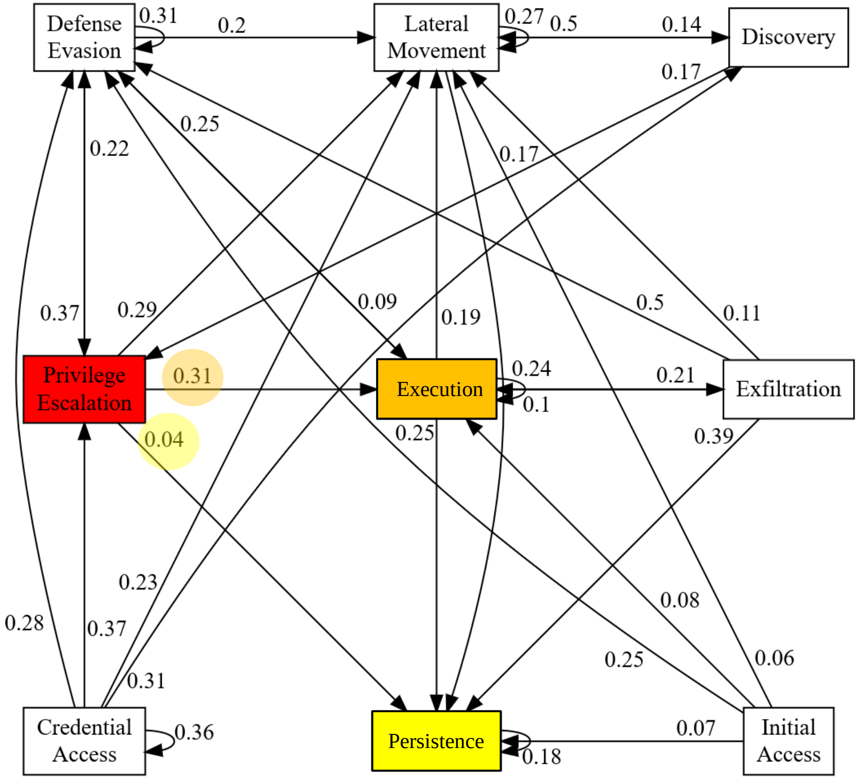
WARP

Attack scenario:

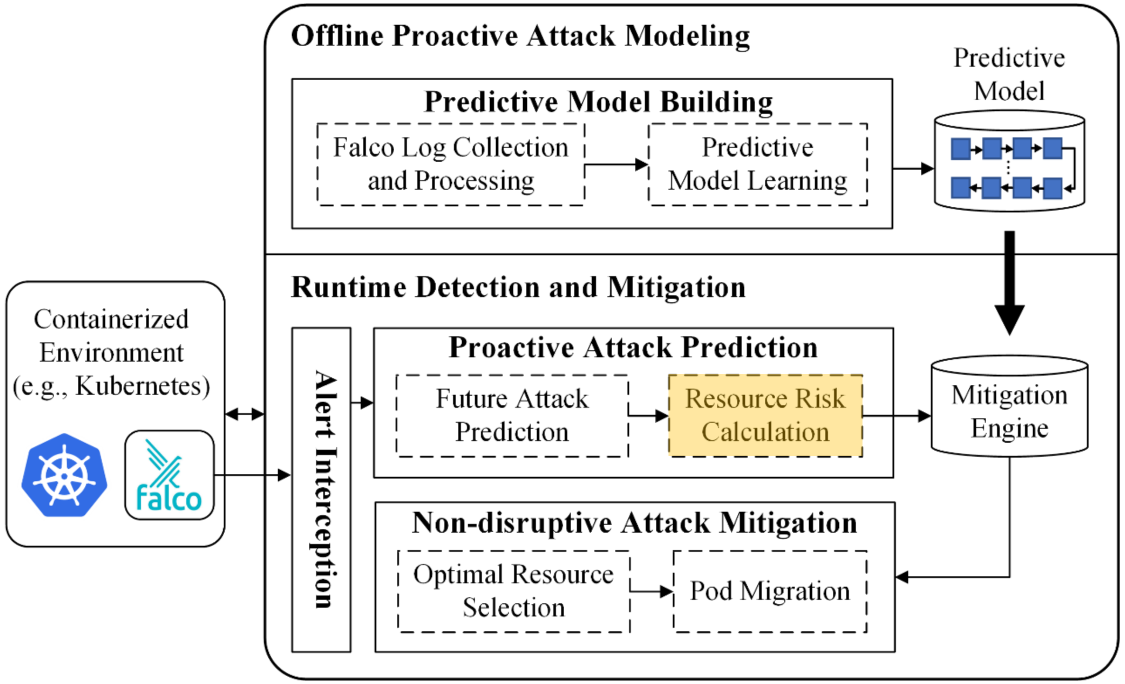
① Exploit CVE-2021-3156



Alert 1: 20:22:29.029612586: C
parent=sudo cmdline=sudoedit
K8s.ns=namespace_CU K8s.pod=
(x
fb4bc)
calation]



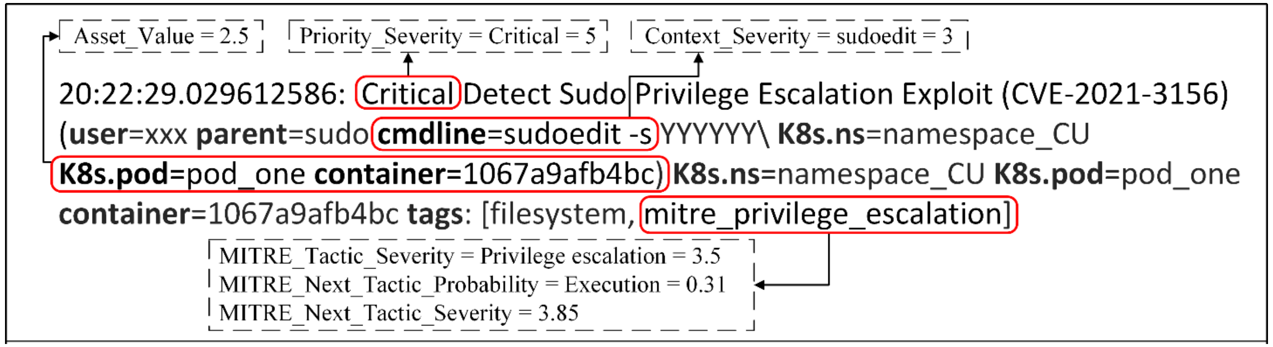
Methodology


Offline Proactive Attack Modeling
Predictive Model Building
Falco Log Collection and Processing
Predictive Model Learning
Predictive Model
Runtime Detection and Mitigation
Alert Interception
Proactive Attack Prediction
Future Attack Prediction
Resource Risk Calculation
Mitigation Engine
Non-disruptive Attack Mitigation
Optimal Resource Selection
Pod Migration
Containerized Environment (e.g., Kubernetes)
falco

WARP

- Resource Risk Calculation (i.e., Pod risk score)

$$\textbf{Risk} = (\sum \text{Priority\_Severity} \times \text{MITRE\_Tactic\_Severity} \times \text{Context\_Severity}) \times \max(\text{Next\_}\textit{Tactic\_Probability} \times 2\max(\sum \textit{MITRE\_Next\_Tactic}\text{\_Severity})) \times \text{Asset\_Value}$$



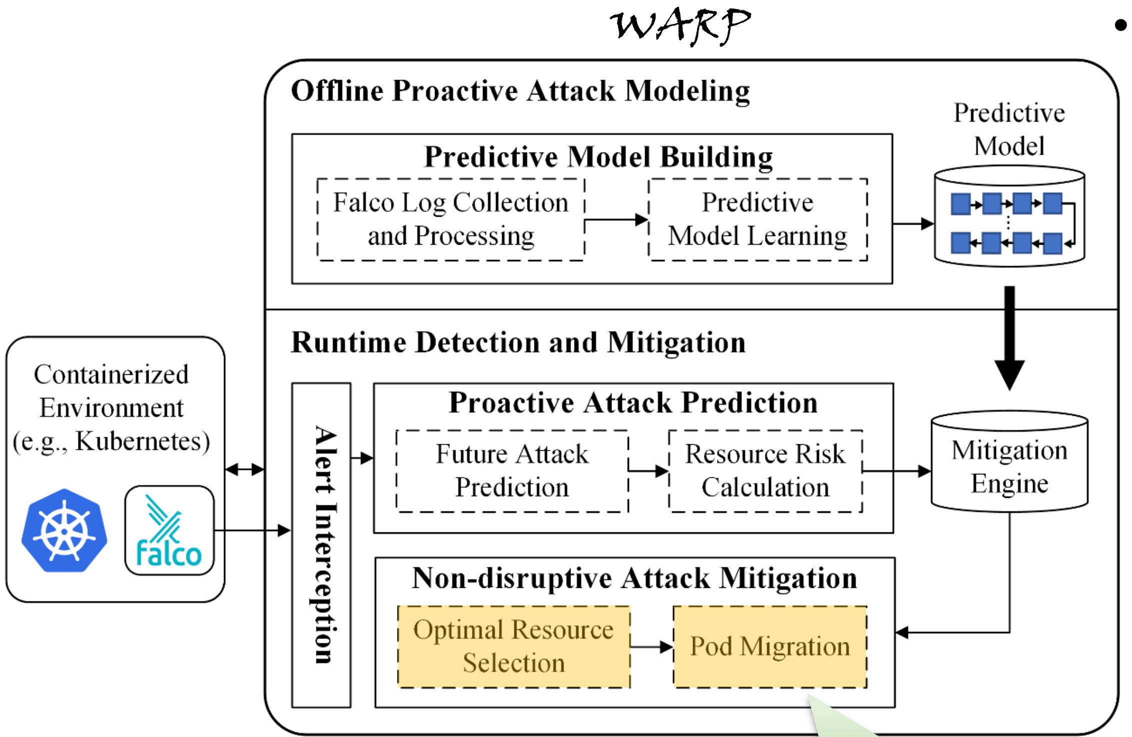
Asset_Value = 2.5 Priority_Severity = Critical = 5 Context_Severity = sudoedit = 3

```
20:22:29.029612586: Critical Detect Sudo Privilege Escalation Exploit (CVE-2021-3156)
(user=xxx parent=sudo cmdline=sudoedit -s YYYYYY\ K8s.ns=namespace_CU
K8s.pod=pod_one container=1067a9afb4bc) K8s.ns=namespace_CU K8s.pod=pod_one
container=1067a9afb4bc tags: [filesystem, mitre_privilege_escalation]
```

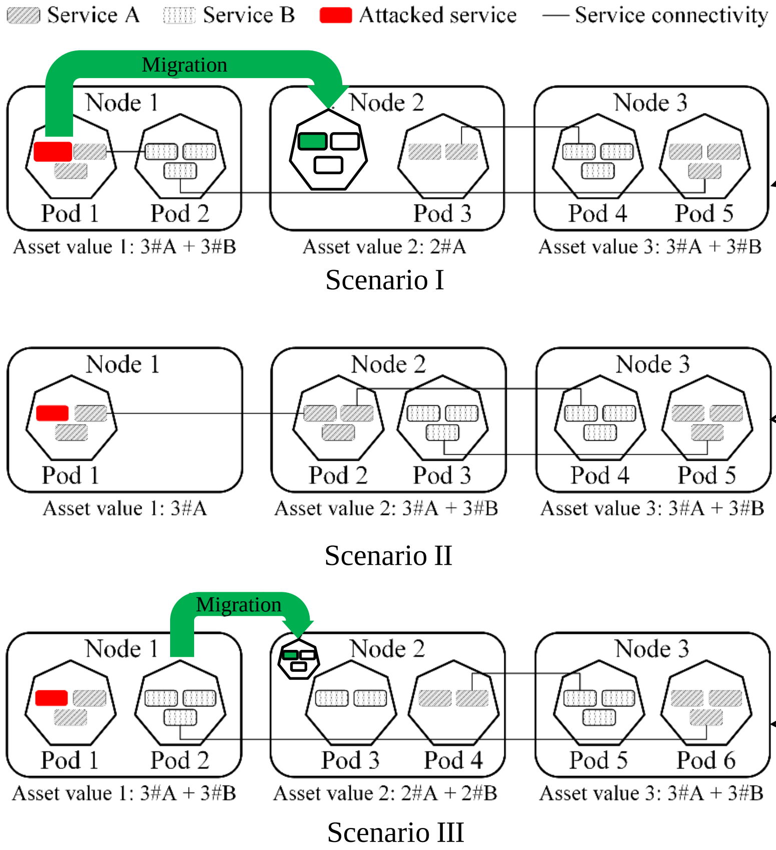
MITRE_Tactic_Severity = Privilege escalation = 3.5
MITRE_Next_Tactic_Probability = Execution = 0.31
MITRE_Next_Tactic_Severity = 3.85

Methodology

- Migrating the riskiest resource (Pod) is not always an optimal choice
- Optimal Resource Selection for Migration


WARP
Offline Proactive Attack Modeling
Predictive Model Building
Falco Log Collection and Processing
Predictive Model Learning
Predictive Model
Runtime Detection and Mitigation
Containerized Environment (e.g., Kubernetes)
falco
Alert Interception
Proactive Attack Prediction
Future Attack Prediction
Resource Risk Calculation
Mitigation Engine
Non-disruptive Attack Mitigation
Optimal Resource Selection
Pod Migration

CRIU for migrating Pod to the optimal resource



Regroup the Pods during migration by the service they serve to avoid introducing additional communication overhead

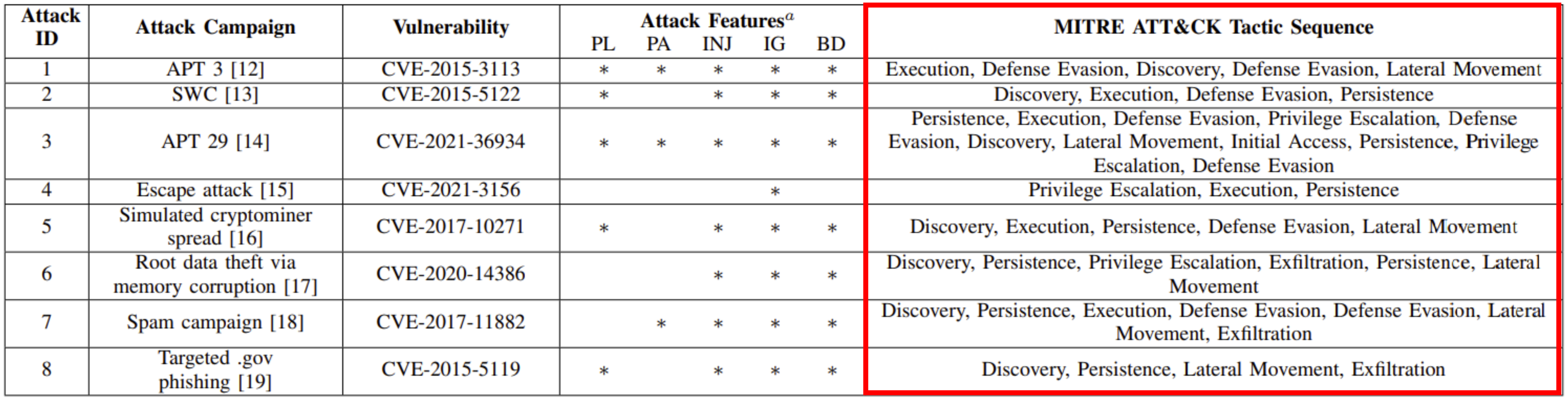
Isolate the Pod under attack (i.e., minimize its co-located Pods and their combined asset value)

Minimize the migration of resources with higher asset values. To reduce the negative impact of any migration delay on more important resources

Implementation/Experiments (1/3)

Building Dataset of Falco Alerts:

- Eight APT attacks simulated with CALDERA
- Balanced the dataset with oversampling attack alerts and undersampling normal alerts
- 231K alerts (including 2,314 attack alerts and 228,686 normal alerts)
- Sequence of MITRE ATT&CK tactics observed out of Falco alerts for each attack are used for predictive model



Attack ID	Attack Campaign	Vulnerability	Attack Features[a]					MITRE ATT&CK Tactic Sequence
			PL	PA	INJ	IG	BD	
1	APT 3 [12]	CVE-2015-3113	*	*	*	*	*	Execution, Defense Evasion, Discovery, Defense Evasion, Lateral Movement
2	SWC [13]	CVE-2015-5122	*		*	*	*	Discovery, Execution, Defense Evasion, Persistence
3	APT 29 [14]	CVE-2021-36934	*	*	*	*	*	Persistence, Execution, Defense Evasion, Privilege Escalation, Defense Evasion, Discovery, Lateral Movement, Initial Access, Persistence, Privilege Escalation, Defense Evasion
4	Escape attack [15]	CVE-2021-3156				*		Privilege Escalation, Execution, Persistence
5	Simulated cryptominer spread [16]	CVE-2017-10271	*		*	*	*	Discovery, Execution, Persistence, Defense Evasion, Lateral Movement
6	Root data theft via memory corruption [17]	CVE-2020-14386			*	*	*	Discovery, Persistence, Privilege Escalation, Exfiltration, Persistence, Lateral Movement
7	Spam campaign [18]	CVE-2017-11882		*	*	*	*	Discovery, Persistence, Execution, Defense Evasion, Defense Evasion, Lateral Movement, Exfiltration
8	Targeted .gov phishing [19]	CVE-2015-5119	*		*	*	*	Discovery, Persistence, Lateral Movement, Exfiltration

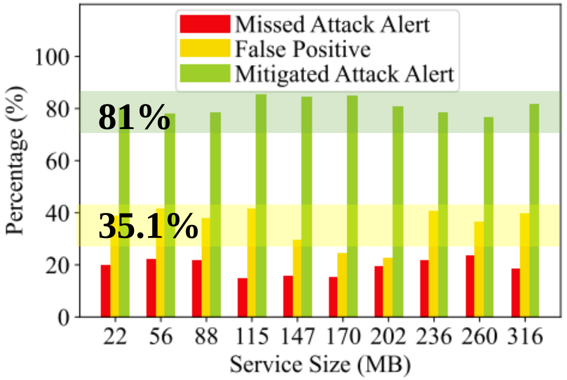
TABLE I: Overview of simulated APT attacks and exploits for WARP dataset.

[a] PL: Phishing email link. PA: Phishing email attachment. INJ: Injection. IG: Information gathering. BD: Backdoor.

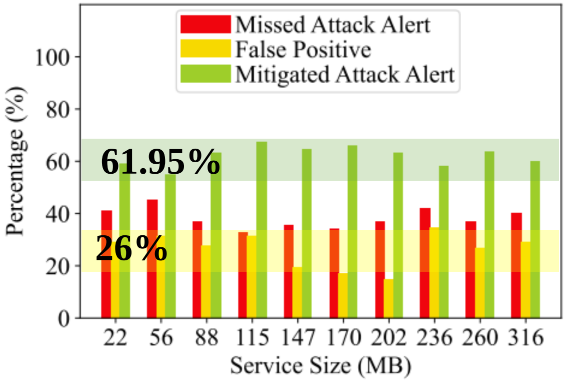
Implementation/Experiments (2/3)

- For migration, we need to set a threshold for the calculated risk
  if **Risk > threshold** then: **Migrate based on optimization objectives**
- Threshold adjusted based on security admin requirements (security sensitive ← **TRADE-OFF** → delay sensitive)

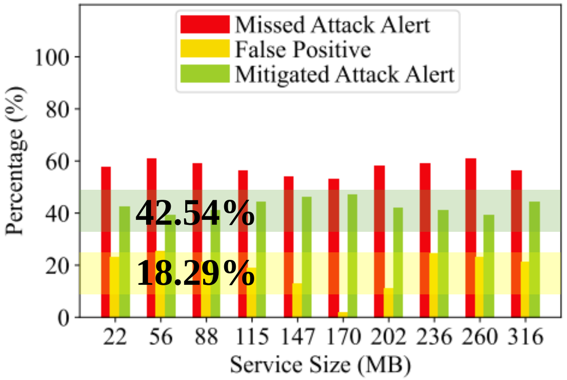
- WARP Effectiveness:
  - Mitigated attack alert (true positive)
  - Missed attack alert (false negative)
  - Mitigated non-attack alert (false positive)



Threshold 30% (security sensitive)



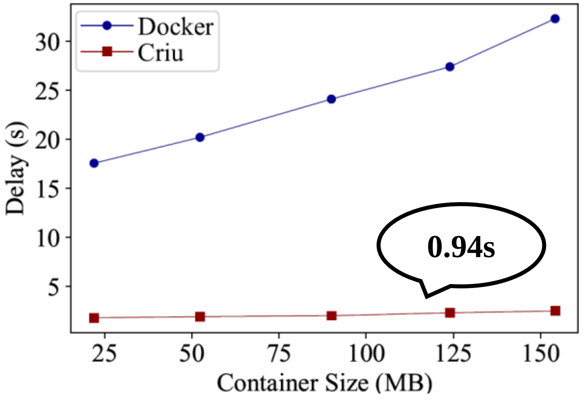
Threshold 50%



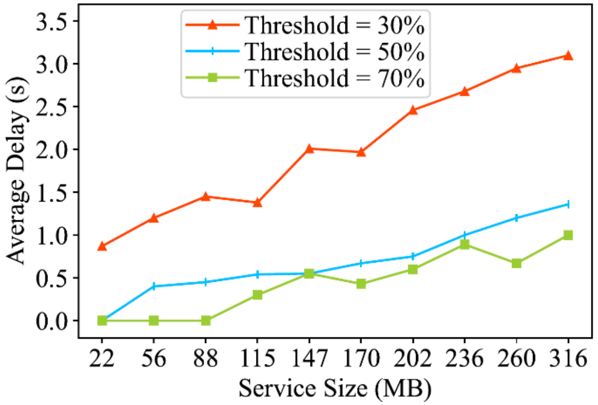
Threshold 70% (delay sensitive)

Implementation/Experiments (3/3)

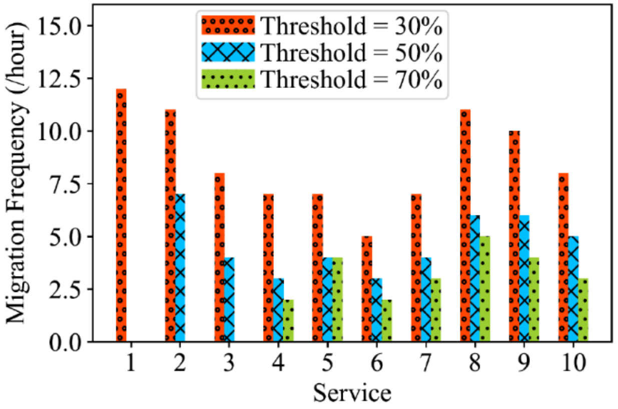
CRIU outperforming Docker for live migration of containers



Pod migration delay depends on the size of the inside containers

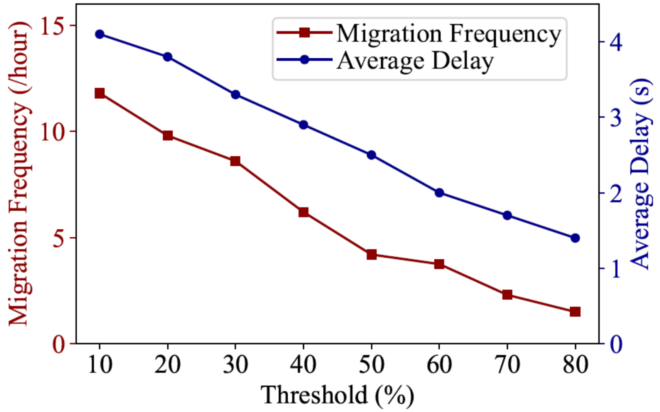


Migration delay for ten different sized services



Delay frequency for ten services

Helps security admin to select an appropriate threshold based on his cluster delay tolerance



Migration delay and frequency for different thresholds

The impact of our solution on services is negligible and non-disruptive

Conclusion

- Summary
  - Proposed an attack mitigation solution that reduces the risk through proactive migration without disrupting the service continuity
  - Built a predictive model based on MITRE ATT&CK tactics to predict the attacker next move
  - Developed a resources risk formula
  - Experimented with migration as potential mitigation for the highly risky resource
- Next steps
  - Developing risk predictive model
  - Adding other attack mitigation methods (e.g., network segmentation)

Thank you!