

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

Sima Bagheri







- Motivation
- Methodology with Running Example

Agenda

- Preliminary Results
- Summary and Next Steps



Critical vulnerabilities in Kubernetes (e.g., CVE 2021-3156) / can bring **the whole multitenant 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 related to attack
- Great demand on alert triage and expert analysis



How to be a step ahead of the attacker to proactively mitigate the attack while ensuring the network service business continuity and minimizing the damage to the cluster?

Motivation



Concordia

Methodology: Running Example

CVE_2021_2156. **Attack Mitigated!** overno Falco I - Learn Falco alerts sequence dependencies **Kubernetes cluster** alerts from alert logs via a predictive model logs Master node Worker node ò AMF AUSF UDM Framework etcd II- Predict the attacker next step in terms of MITRE tactic based on the current seen alert Predictive model falco III- Perform resource risk calculation and falco deploy non-disruptive mitigation (i.e., migration) to stop the attacker Current alert tactic: MITRE-privilege-escalation **Risk calculation:** 1- Critical: defect sudo pri MITRE-privilege escalat Predicted tactic: MITRE-persistence

Framework Architecture

UNIVERSITÉ

Concordia

UNIVERSITY



• Example of Falco alerts

20:27:10.560207326 Warning Sensitive file opened for reading by non-trusted program (user=root user_loginuid=-1 program=cat command=cat /etc/shadow file=/etc/shadow parent=bash gparent=<NA> gggparent=<NA> container_id=1067a9afb4bc image=nginx) k8s.ns=default k8s.pod=that-pod container=1067a9afb4bc k8s.ns=default k8s.pod=that-pod container=1067a9afb4bc sima@ubuntu:~S

- 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...

Framework Architecture

UNIVERSITÉ

Concordia

UNIVERSITY



• 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



Concordia UNIVERSITÉ UNIVERSITY

Preliminary Results

Framework Architecture



• Build the predictive model out of the sequence of tactics



Framework Architecture

UNIVERSITÉ

Concordia

UNIVERSITY



 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)

8

Framework Architecture

UNIVERSITÉ

Concordia

UNIVERSITY



Migration of containers performance experiment:

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





- 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

