



StackRox

# Mitigating Kubernetes Attacks

---

Wei Lien Dang – Co-founder and Chief Strategy Officer

Michelle McLean – VP of Marketing

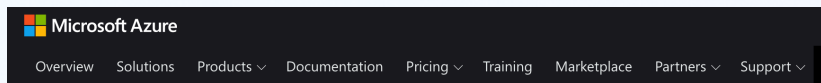
September 23, 2020

# Agenda

- Kubernetes and container attacks: real-world examples
- Kubernetes threats: what's different?
- Kubernetes attack matrix: overview
- Adversarial tactics and techniques: main themes
- Key takeaways and recommendations



# Kubernetes attacks in the wild



Blog / Security

## Detect large-scale cryptocurrency mining attack against Kubernetes clusters

Posted on April 8, 2020

[Yossi Weizman](#), Security Research Software Engineer, Azure Security Center



Azure Security Center | **WIRED** | BACKCHANNEL BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY | SIGN IN | SUBSCRIBE | SEARCH

At Ignite including [vulnerability](#)

## Hack Brief: Hackers Enlisted Tesla's Public Cloud to Mine Cryptocurrency

The recent rash of cryptojacking attacks has hit a Tesla database that contained potentially sensitive information.



MUST READ: [What we've lost in the push to agile software development, and how to get it back](#)

## Kubernetes' first major security hole discovered

There's now an invisible way to hack into the popular cloud container orchestration system Kubernetes.



June 10, 2020

## Misconfigured KubeFlow workloads are a security risk

START HACKING | LOG IN

hackerone

SOLUTIONS | PRODUCTS | WHY HACKERONE | COMPANY | RESOURCES | CONTACT US

**André Baptista (@xabc)** 1802 Reputation Rank 6.02 Signal 93rd Percentile 21.85 Impact 93rd Percentile

**#541878 SSRF in Exchange leads to ROOT access in all instances**

State: Resolved (Closed) Severity: Medium (5.9)

Disclosed: May 23, 2018 2:09pm -0700 Participants: 3

Reported To: [Shopify](#) Visibility: Disclosed (Full)

Asset: <https://exchange.marketplace.com/> (Domain)

Weakness: Server-Side Request Forgery (SSRF)

Bounty: \$25,000

Summary by Shopify: Shopify infrastructure is isolated into subsets of infrastructure. @xabc reported it was possible to gain root access to any container in one particular subset by exploiting a server side request forgery bug in the screenhotting functionality of Shopify Exchange. Within an hour of receiving the report, we disabled the vulnerable service, began auditing applications in all subsets and remediating across all our infrastructure. The vulnerable subset did not include Shopify core.



## Backdoored images downloaded 5 million times finally removed from Docker Hub

17 images posted by a single account over 10 months may have generated \$90,000.

DAN GOODIN - 6/13/2018, 8:10 PM

# StackRox research

- Honeypot setup
  - Large GKE clusters running hundreds of containerized apps exposed to the Internet for 5 months
  - Used popular images with known vulnerabilities and deployed with weak configurations
- Threats look similar to those that affect non-containerized applications
- Observed attacker actions
  - Injection attempts to download a file into /tmp/
  - Attempted downloads using wget
  - Intrusion attempts frequently occurring on well-known web ports
  - Attempted commands to gain additional targeting data or download binaries

# What's different about Kubernetes threats

- New attack surface
  - Kubernetes control plane
  - Cluster worker nodes
- Application components are highly distributed, dynamic, and ephemeral
- Increased operational complexity
- Broader impact due to orchestration and automation

# Kubernetes attack matrix: an overview

- Published by Microsoft Azure
- Part of ecosystem's continued focus on security
  - Kubernetes security audit
  - SIGs
  - NIST SP 800-190
  - CIS Kubernetes Benchmark
- Based on MITRE ATT&CK® framework



*The Kubernetes attack matrix extends the ATT&CK framework for the first time to Kubernetes to describe a total of 40 different techniques that fall under nine different tactics.*

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Impact
Using cloud credentials	Exec into container	Backdoor container	Privileged container	Clear container logs	List k8s secrets	Access the k8s API server	Access cloud resources	Data destruction
Compromised images in registry	bash/cmd inside container	Writable hostPath mount	Cluster-admin binding	Delete K8S events	Mount service principal	Access Kubelet API	Container service account	Resource hijacking
Kubeconfig file	New container	Kubernetes CronJob	hostPath mount	Pod/container name similarity	Access container service mount	Network mapping	Cluster internal networking	Denial of service
Application vulnerability	Application exploit (RCE)		Access cloud resources	Connect from Proxy server	Applications credentials in configuration files	Access k8s dashboard	Applications credentials in configuration files	
Exposed dashboard	SSH server running inside container					Instance Metadata API	Writable volume mounts on the host	
							Access k8s dashboard	
							Access tiller endpoint	



# MITRE ATT&CK® framework

- Knowledge base of adversarial tactics and techniques
- Use to categorize attack vectors and gauge their level of risk
- Based on real-world observations

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	CredentialAccess	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts		Scheduled Task		XSL Script Processing	Network Sniffing	Windows Remote Management	Video Capture	Physical Transfer	Web Service	
Trusted Relationship	Trap		Process Injection		Two-Factor Authentication Interception	System Time Discovery	Screen Capture	Exfiltration Over Physical Medium	Unconventional Used Port	
Supply Chain Compromise	LSASS Driver		Extra Window Memory Injection		System Service Discovery	Third-party Software	Input Capture	Main in the Browser	Standard Non-Application Layer Protocol	
Searchphishing via Service	Local Job Scheduling		Bypass User Account Control		Private Keys	System Owner/User Discovery	Task Shared Content	Email Collection	Standard Application Layer Protocol	
Searchphishing Link	Launchoff		Process Termination		Password Filter DLL	Size Hijacking	Size Hijacking	Size Hijacking	Standard Application Layer Protocol	
Searchphishing Attachment	XSL Script Processing		Valid Accounts		LMN/NTL-AS Poisoning	System Network	Shared Webcontent	Data Staged	Data Transfer Size Limits	
Replication Through Removable Media	Windows Remote Management		File Modification		Keychain	Configuration Discovery	Replication Through Removable Media	Data from Removable Media	Data Encrypted	Remote Access Tools
Exploit Public-Facing Application	Trusted Developer Utilities		Image File Execution Options Injection		Kernelwriting	Security Software Discovery	Replication Through Removable Media	Data from Network	Data Compressed	Port Knocking
Hardware Additions	User Execution		DLL Search Order Hijacking		Input Prompt	Remote System Discovery	Remote File Copy	Shared Drive	Automated Exfiltration	Multi-layer Encryption
Drive-by Compromise	Third-party Software		Web Shell		Input Capture	Query Registry	Remote Desktop Protocol	Data from Information Repositories	Exfiltration Over Other Network Medium	Multi-layer Encryption
	Startup Items		Web Service		Hooking	Process Discovery	Pass the Ticket	Automated Collection	Exfiltration Over Other Network Medium	Multi-layer Encryption
	Service		Service Registry Permissions Weakness		Forward Authentication	Permission Groups Discovery	Pass the Hash	Automated Collection	Exfiltration Over Other Network Medium	Multi-layer Encryption
	Port Monitor		Path Interception		Exploitation for Credential Access	Peripheral Device Discovery	Local Scripts	Audio Capture	Alternative Protocol	Fallback Channels
	Service Execution		New Service		Credential Dumping	Network Service Scanning	Remote Services	Clipboard Data	Domain Fronting	Domain Fronting
	Scritting		Launch Hijacking		Brute Force	File and Directory Discovery	Application Deployment Software	Windows Admin Shares	Custom Cryptographic Protocol	Custom Cryptographic Protocol
	RunDll32		Hooking		Signal Binary	Batch History	Remote Services	Distributed Component Object Model	Remote File Copy	Remote File Copy
	Regsvr32		File System Permissions Weakness		Account Manipulation	Security Memory	System Network Connections Discovery	System Information	Standard Cryptographic Protocol	Standard Cryptographic Protocol
	Regsvr32/Regasm		Dylib Hijacking		RunDll32	Account Manipulation	System Network Connections Discovery	System Information	Standard Cryptographic Protocol	Standard Cryptographic Protocol
	PowerShell		Application Shimmin		RunDll32	Credentials in Registry	System Network Connections Discovery	System Information	Standard Cryptographic Protocol	Standard Cryptographic Protocol
	Malware		AppCert DLLs		Regsvr32		System Information	System Information	Standard Cryptographic Protocol	Standard Cryptographic Protocol
	InstallUtil		AppCert DLLs		Regsvr32		System Information	System Information	Standard Cryptographic Protocol	Standard Cryptographic Protocol
	Graphical User Interface		Accessibility Features		Regsvr32		System Information	System Information	Standard Cryptographic Protocol	Standard Cryptographic Protocol
	Exploitation for Client Execution		Windows Management Instrumentation		Regsvr32		System Information	System Information	Standard Cryptographic Protocol	Standard Cryptographic Protocol
	Dynamic Data Exchange		Event Subscription		Regsvr32		System Information	System Information	Standard Cryptographic Protocol	Standard Cryptographic Protocol
	Control Panel Items		SIP and Trust Provider		Regsvr32		System Information	System Information	Standard Cryptographic Protocol	Standard Cryptographic Protocol
	Command-Line Interface		Security Support Provider		Regsvr32		System Information	System Information	Standard Cryptographic Protocol	Standard Cryptographic Protocol
	CHTSP		ScreenSaver		Regsvr32		System Information	System Information	Standard Cryptographic Protocol	Standard Cryptographic Protocol
	Registry Run		Key / Startup Folder		Regsvr32		System Information	System Information	Standard Cryptographic Protocol	Standard Cryptographic Protocol
	Windows Management Instrumentation		Re-spread Applications		Regsvr32		System Information	System Information	Standard Cryptographic Protocol	Standard Cryptographic Protocol
	Signal Binary		Port Knocking		Regsvr32		System Information	System Information	Standard Cryptographic Protocol	Standard Cryptographic Protocol
	Proxyc Execution		Offic Application Startup		Regsvr32		System Information	System Information	Standard Cryptographic Protocol	Standard Cryptographic Protocol
	Execution through Module Load		NTFS Helper DLL		Regsvr32		System Information	System Information	Standard Cryptographic Protocol	Standard Cryptographic Protocol
			Modify Existing Service		Regsvr32		System Information	System Information	Standard Cryptographic Protocol	Standard Cryptographic Protocol
			Logon Scripts		Regsvr32		System Information	System Information	Standard Cryptographic Protocol	Standard Cryptographic Protocol
			Logon: Run		Regsvr32		System Information	System Information	Standard Cryptographic Protocol	Standard Cryptographic Protocol
			LC_LOAD_DLLS Addition		Regsvr32		System Information	System Information	Standard Cryptographic Protocol	Standard Cryptographic Protocol
			Launch Agent		Regsvr32		System Information	System Information	Standard Cryptographic Protocol	Standard Cryptographic Protocol
			Kernel Modules and Extensions		Regsvr32		System Information	System Information	Standard Cryptographic Protocol	Standard Cryptographic Protocol
			Hidden Files and Directories		Regsvr32		System Information	System Information	Standard Cryptographic Protocol	Standard Cryptographic Protocol
			External Remote Services		Regsvr32		System Information	System Information	Standard Cryptographic Protocol	Standard Cryptographic Protocol
			Create Account		Regsvr32		System Information	System Information	Standard Cryptographic Protocol	Standard Cryptographic Protocol
			Component Object Model Hijacking		Regsvr32		System Information	System Information	Standard Cryptographic Protocol	Standard Cryptographic Protocol
			Change Default File Association		Regsvr32		System Information	System Information	Standard Cryptographic Protocol	Standard Cryptographic Protocol
			Bootkit		Regsvr32		System Information	System Information	Standard Cryptographic Protocol	Standard Cryptographic Protocol
			NTFS Jobs		Regsvr32		System Information	System Information	Standard Cryptographic Protocol	Standard Cryptographic Protocol
			Authentication Package		Regsvr32		System Information	System Information	Standard Cryptographic Protocol	Standard Cryptographic Protocol
			Account Manipulation		Regsvr32		System Information	System Information	Standard Cryptographic Protocol	Standard Cryptographic Protocol
			Backdoor and Shell		Regsvr32		System Information	System Information	Standard Cryptographic Protocol	Standard Cryptographic Protocol
			Time Providers		Regsvr32		System Information	System Information	Standard Cryptographic Protocol	Standard Cryptographic Protocol
			System Firmware		Regsvr32		System Information	System Information	Standard Cryptographic Protocol	Standard Cryptographic Protocol
			Shortcut Modification		Regsvr32		System Information	System Information	Standard Cryptographic Protocol	Standard Cryptographic Protocol
			Redundant Access		Regsvr32		System Information	System Information	Standard Cryptographic Protocol	Standard Cryptographic Protocol
			Hyperervisor		Regsvr32		System Information	System Information	Standard Cryptographic Protocol	Standard Cryptographic Protocol
			Component Firmware		Regsvr32		System Information	System Information	Standard Cryptographic Protocol	Standard Cryptographic Protocol
			Browser Extensions		Regsvr32		System Information	System Information	Standard Cryptographic Protocol	Standard Cryptographic Protocol

The MITRE ATT&CK™  
Enterprise Framework  
attack.mitre.org

© 2019 The MITRE Corporation. All rights reserved. Approved for Public Release; Distribution Unlimited. Case Number 15-1288.





# Tactics and techniques of the attack matrix

- 9 tactics, 40 techniques
- Tactics: the “why” behind a particular technique
- Techniques: specific offensive actions - the “how” for a given objective
- Some techniques can be classified under multiple tactics
- A technique may warrant multiple, different mitigations

The Kubernetes attack matrix extends the ATT&CK framework for the first time to Kubernetes to describe a total of 40 different techniques that fall under nine different tactics.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Impact
Using cloud credentials	Exec into container	Backdoor container	Privileged container	Clear container logs	List k8s secrets	Access the k8s API server	Access cloud resources	Data destruction
Compromised images in registry	bashcmd inside container	Writable hostPath mount	Cluster-admin binding	Delete K8S events	Mount service principal	Access Kubelet API	Container service account	Resource hijacking
Kubeconfig file	New container	Kubernetes CronJob	hostPath mount	Podcontainer name similarity	Access container service mount	Network mapping	Cluster internal networking	Denial of service
Application vulnerability	Application exploit (RC3)		Access cloud resources	Connect from Proxy server	Applications credentials in configuration files	Access k8s dashboard	Applications credentials in configuration files	
Exposed dashboard	SSH server running inside container					Instance Metadata API	Writable volume mounts on the host	
							Access k8s dashboard	
							Access tiller endpoint	

## Examples: 1.4 Application vulnerability, 2.4. Application exploit

- Scan container images for vulnerabilities
- Use admission control to prevent containers with high-severity vulnerabilities from launching
- Configure Network Policies to limit external access to pods
- Restrict service account permissions using Kubernetes RBAC
- Do not allow pods to run as root
- Set up filesystem as read-only
- Minimize container access to underlying host

# Your best protection: apply native Kubernetes controls



*The Kubernetes attack matrix extends the ATT&CK framework for the first time to Kubernetes to describe a total of 40 different techniques that fall under nine different tactics.*

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Impact
Using cloud credentials	✓ Esc into container	✓ Backdoor container	✓ Privileged container	✓ Clear container logs	✓ List k8s secrets	✓ Access the k8s API server	✓ Access cloud resources	✓ Data destruction
Compromised images in registry	bash/cmd inside container	✓ Writable hostPath mount	✓ Cluster-admin binding	✓ Delete k8s mounts	✓ Mount service principal	✓ Access kubelet API	✓ Container service account	✓ Resource hijacking
✓ kubeconfig file	✓ New container	✓ Kubernetes CronJob	✓ hostPath mount	✓ Pod/container name similarity	✓ Access container service mount	✓ Network mapping	✓ Cluster internal networking	✓ Denial of service
✓ Application vulnerability	✓ Application exploit (RCE)		✓ Access cloud resources	✓ Connect from Proxy server	✓ Applications credentials in configuration files	✓ Access k8s dashboard	✓ Applications credentials in configuration files	
✓ Exploited dashboard	✓ SSH server running inside container					✓ Instance Metadata API	✓ Writable Instance mounts to the host	
							✓ Access k8s dashboard	
							Access tiller endpoint	



# Step 1: Configure Kubernetes RBAC

- Limit who has the cluster-admin role in your organization
- Adopt a least-privilege model for service accounts and their role bindings
- Avoid complexity in role aggregation or overlap in role definitions

*The Kubernetes attack matrix extends the ATT&CK framework for the first time to Kubernetes to describe a total of 40 different techniques that fall under nine different tactics.*

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Impact
Using cloud credentials	✓ Esc into container	✓ Backdoor container	✓ Privileged container	Clear container logs	✓ List k8s secrets	✓ Access the k8s API server	Access cloud resources	✓ Data destruction
Compromised images in registry	bash/cmd inside container	Writable hostPath mount	✓ Cluster-admin binding	Delete K8S events	Mount service principal	Access Kubelet API	✓ Container service account	✓ Resource hijacking
Kubeconfig file	✓ New container	✓ Kubernetes CronJob	hostPath mount	✓ Pod/container name similarity	✓ Access container service mount	Network mapping	Cluster internal networking	Denial of service
✓ Application vulnerability	✓ Application exploit (RCE)		Access cloud resources	Connect from Proxy server	Applications credentials in configuration files	✓ Access k8s dashboard	Applications credentials in configuration files	
✓ Exposed dashboard	SSH server running inside container					Instance Metadata API	Writable volume mounts on the host	
							✓ Access k8s dashboard	
							Access tiller endpoint	

# Ensure you monitor your RBAC settings

The screenshot displays the StackRox user interface, specifically the 'ROLES' section. The top navigation bar shows various system metrics: 2 CLUSTERS, 3 NODES, 158 VIOLATIONS, 63 DEPLOYMENTS, 40 IMAGES, and 22 SECRETS. A search bar and user profile 'AK' are also present.

The left sidebar contains a list of navigation items: DASHBOARD, NETWORK GRAPH, VIOLATIONS, COMPLIANCE, VULNERABILITY MANAGEMENT, CONFIGURATION MANAGEMENT, RISK, PLATFORM CONFIGURATION, API REFERENCE, and HELP CENTER.

The main content area is titled 'ROLES Entity List' and shows a list of roles. The 'cluster-admin' role is selected, and its details are displayed in a modal window. The modal is divided into two sections: 'Role Summary' and 'Role Permissions And Rules'.

**Role Summary:**

- METADATA:** Role Type: ClusterRole, Created: 06/04/2020 | 8:10:10PM, 0 LABELS, 0 ANNOTATIONS.
- CLUSTER:** production
- USERS & GROUPS:** 3
- SERVICE ACCOUNTS:** 1

**Role Permissions And Rules:**

- 1 PERMISSIONS ACROSS THIS CLUSTER:** \* (All verbs), \* (All resources)
- 2 RULES:** Verbs: \* (All verbs), Resources and Non-resource URLs: \* (All resources)



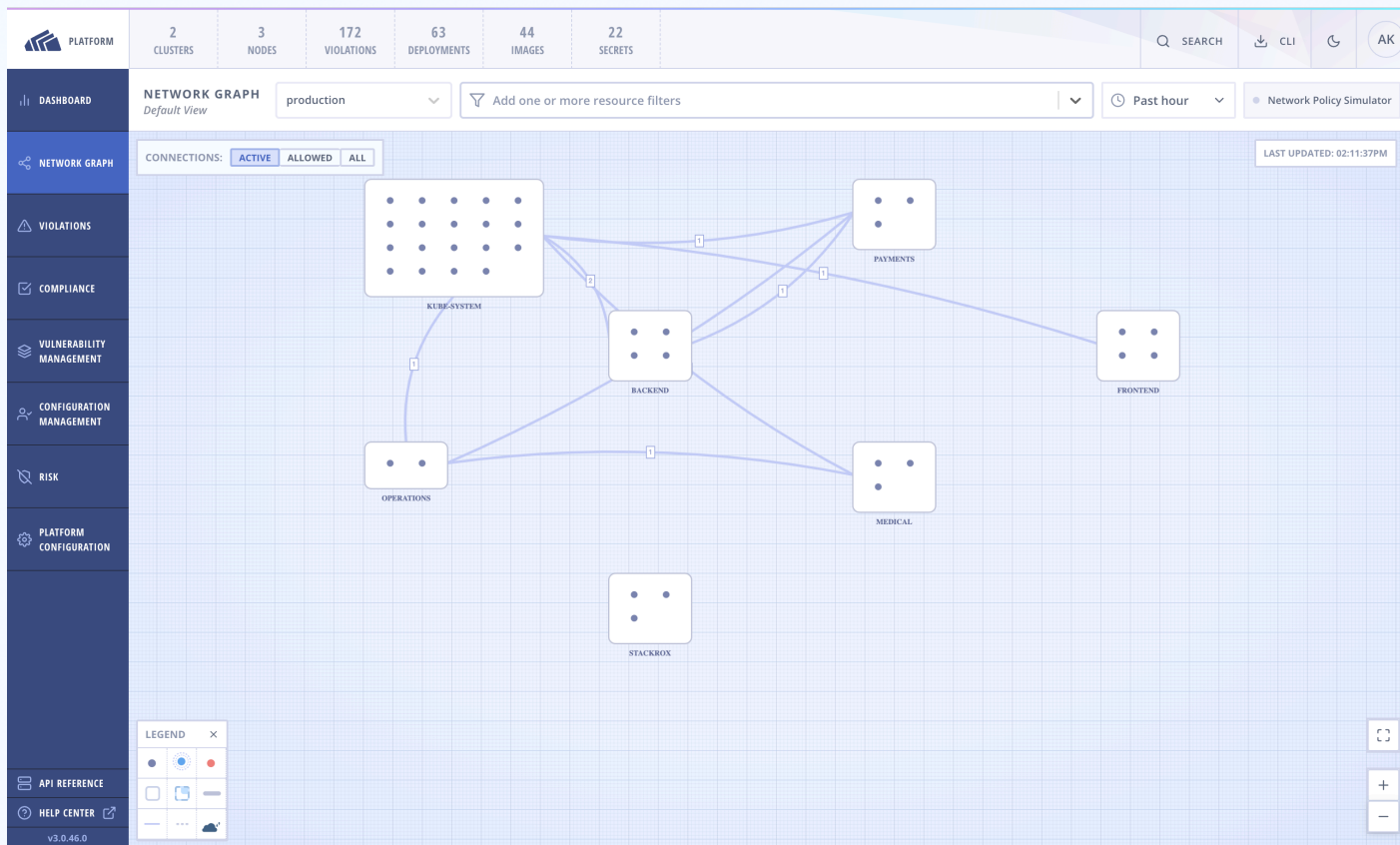
# Step 2: Configure Network Policies

- Use a CNI that implements the NetworkPolicy API and create policies that restrict pod traffic
- Start by applying a default-deny-all network policy
- Explicitly allow necessary Internet access and pod-to-pod communication

The Kubernetes attack matrix extends the ATT&CK framework for the first time to Kubernetes to describe a total of 40 different techniques that fall under nine different tactics.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Impact
Using cloud credentials	Exec into container	Backdoor container	Privileged container ✓	Clear container logs	List k8s secrets	Access the k8s API server	Access cloud resources	Data destruction
Compromised images in registry	bash/cmd inside container	Writable hostPath mount	Cluster-admin binding	Delete K8S events	Mount service principal	Access kubelet API ✓	Container service account	Resource hijacking
Kubeconfig file	New container	Kubernetes CronJob	hostPath mount	Pod/container name similarity	Access container service mount	Network mapping ✓	Cluster internal networking ✓	Denial of service ✓
Application vulnerability ✓	Application exploit (RCE)		Access cloud resources ✓	Connect from Proxy server	Applications credentials in configuration files	Access k8s dashboard ✓	Applications credentials in configuration files	
Exposed dashboard ✓	SSH server running inside container ✓					Instance Metadata API ✓	Writable volume mounts on the host	
							Access k8s dashboard ✓	
							Access tiller endpoint	

# Look for ways to automate Network Policy management



# Step 3: Harden pod configurations

- Configure security contexts for pods and/or containers
- Enforce policies on pod specifications
- Authorize policies by granting access to the pod's service account

*The Kubernetes attack matrix extends the ATT&CK framework for the first time to Kubernetes to describe a total of 40 different techniques that fall under nine different tactics.*

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Impact
Using cloud credentials	✓ Esc into container	Backdoor container	✓ Privileged container	✓ Clear container logs	List k8s secrets	Access the k8s API server	✓ Access cloud resources	Data destruction
Compromised images in registry	bash/cmd inside container	✓ Writable Path mount	Cluster-admin binding	✓ Delete k8s mounts	✓ Mount service principal	Access Kubelet API	Container service account	Resource hijacking
Kubeconfig file	New container	Kubernetes CronJob	✓ hostPath mount	Pod/container name similarity	Access container service mount	Network mapping	Cluster internal networking	Denial of service
✓ Application vulnerability	✓ Application exploit (RCE)		✓ Access cloud resources	Connect from Proxy server	Applications credentials in configuration files	Access k8s dashboard	Applications credentials in configuration files	
Exposed dashboard	✓ SSH server running inside container					Instance Metadata API	✓ Writable cloud mounts to the host	
							Access k8s dashboard	
							Access tiller endpoint	

# Detect insecure pod configurations

2 CLUSTERS

3 NODES

171 VIOLATIONS

63 DEPLOYMENTS

40 IMAGES

22 SECRETS

SEARCH

CLI

ad

DASHBOARD

NETWORK GRAPH

VIOLATIONS

COMPLIANCE

VULNERABILITY MANAGEMENT

CONFIGURATION MANAGEMENT

RISK

PLATFORM CONFIGURATION

API REFERENCE

HELP CENTER

v3.0.45.0

POLICIES

Default View

Add one or more resource filters

64 POLICIES

REASSESS ALL

IMPORT POLICY

NEW POLICY

Page 1 of 2

<input type="checkbox"/>	Name ↑	Description	Lifecycle	Severity
<input type="checkbox"/>	30-Day Scan Age	Alert on deployments with images that haven't been scanned in 30 days	Deploy	Medium
<input type="checkbox"/>	90-Day Image Age	Alert on deployments with images that haven't been updated in 90 days	Build, Deploy	Low
<input type="checkbox"/>	ADD Command used instead of COPY	Alert on deployments using a ADD command	Build, Deploy	Low
<input type="checkbox"/>	Alpine Linux Package Manager (apk) in Image	Alert on deployments with the Alpine Linux package manager (apk) present	Build, Deploy	Low
<input type="checkbox"/>	Alpine Linux Package Manager Execution	Alert when the Alpine Linux package manager (apk) is executed at runtime	Runtime	Low
<input type="checkbox"/>	Apache Struts: CVE-2017-5638	Alert on deployments with images containing Apache Struts vulnerability CVE-2017-5638	Build, Deploy	Critical
<input type="checkbox"/>	CAP_SYS_ADMIN capability added	Alert on deployments with containers escalating with CAP_SYS_ADMIN	Deploy	Medium
<input type="checkbox"/>	Compiler Tool Execution	Alert when binaries used to compile software are executed at runtime	Runtime	Low
<input type="checkbox"/>	Container using read-write root	Alert on deployments with containers with read-write root	Deploy	Medium

WRITABLE HOSTPATH MOUNT

PREVIOUS NEXT

Policy Criteria

Construct policy rules by chaining criteria together with boolean logic.

Policy Section 1

HOST MOUNT WRITABILITY:

WRITABLE READ-ONLY

AND

VOLUME SOURCE:

NOT

Volume Source

/var/lib/docker

AND

DROP A POLICY FIELD INSIDE

OR

Add a new condition

Drag out a policy field

Image Registry

Image Registry

Image Remote

Image Tag

Image Contents

Container Configuration

Deployment Metadata

Storage

Networking

Process Activity

Kubernetes Access



# Key takeaways and recommendations

- Use the Kubernetes attack matrix as your basis for systematically and comprehensively securing your containerized applications
- Applying a few native Kubernetes security features will mitigate most attacks:
  - Kubernetes RBAC
  - Kubernetes Network Policies
  - Restricted pod configurations
- You still need runtime monitoring!



## Q&A