



Mitigating Kubernetes Attacks

Wei Lien Dang – Co-founder and Chief Strategy Officer

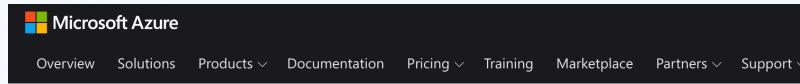
Michelle McLean – VP of Marketing

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



The Microsoft Azure homepage features a dark header with the Microsoft logo and "Microsoft Azure". Below the header are navigation links: Overview, Solutions, Products, Documentation, Pricing, Training, Marketplace, Partners, and Support. A "Blog / Security" link is visible in the top left.

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 Serverless from Infras and on-premises



BACKCHANNEL BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY

SIGN IN

SUBSCRIBE



LILY HAY NEWMAN SECURITY 02.28.2018 05:06 PM

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.



VIDEOS WINDOWS 10 5G IOT CLOUD AI SECURITY MORE NEWSLETTERS

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.



The Microsoft Security homepage features a header with the Microsoft logo and "Security". Below the header are navigation links: Solutions, Products, Operations, Partners, Resources, and Trust Center. A "All Microsoft" link is in the top right.

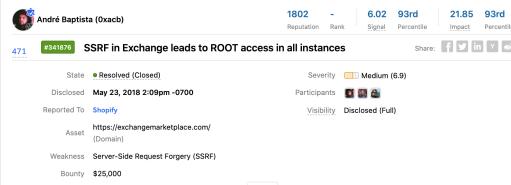
June 10, 2020

Misconfigured Kubeflow workloads are a security risk

hackerone

SOLUTIONS PRODUCTS WHY HACKERONE COMPANY RESOURCES

CONTACT US



André Baptista (Oxach) has a rank of 1802, Reputation of 6.02, and is 93rd percentile. The report ID is #341876. The report details an SSRF vulnerability in Exchange leading to root access in all instances. It was disclosed on May 23, 2018, at 2:09pm -0700. The severity is Medium (6.9). Participants include Oxach, and visibility is Disclosed (Full). The bounty is \$25,000.

SUMMARY BY SHOPIFY

Shopify infrastructure is isolated into subsets of infrastructure. Oxach 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 screenshotting 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.



BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STORE

BEWARE —

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	Process Injection	XSL Script Processing	Network Sniffing	Windows Remote Management	Video Capture	Scheduled Transfer	Web Service	Uncommonly Used Port	
Trusted Relationship	Trip	Extra Memory Injection	Two-Factor Authentication	System Time Discovery	Third Party Software	Screen Capture	Exfiltration Over Physical Medium	Standard Network Application	Standard Network Application	
Supply Chain Compromise	UAC Bypass	Bypass User Account Control	Interception Keys	System Service Discovery	Mal in the Browser	Mail in the Browser	Ephemeral Port Command and Control Channel	Standard Application Layer Protocol	Standard Application Layer Protocol	
Spreading via Service	Local Job Scheduling	Access Token Manipulation	Password Filter DLL	SSH Key Hijacking	System Network Configuration Discovery	Email Collection	Data Transfer Size Limits	Data Transfer Size Limits	Standard Application Layer Protocol	
Spearmarking Link	Launchch1	LMNR/NBT-NS Poisoning	System Network Configuration Discovery	Shared Webcam	Data Staged	Data Transfer Through Shared Webcam	Resilication Through Shared Webcam	Data from Removable Media	Removable Media Tools	
Spearmarking Attachment	XSL Script Processing	User Account Control Bypass	LMNR/NBT-NS Poisoning	Security Software Discovery	Remote System Discovery	Remote Desktop Protocol	Resilication Through Shared Webcam	Automated Collection	Port Knocking	
Replication Through Replication Manager	Windows Remote Management	Post Modification	Keychain	Query Registry	Remote File Copy	Remote File Copy	Automated Collection	Exfiltration Over Other Network Medium	Multihop Communication	
Exploit Public-Facing Application	User Account	Image File Execution Options Injection	DLL Search Order Hijacking	Input Prompt	Resilication Through Shared Webcam	Data from Local System	Clipboard Data	Clipboard Data	Multi-hop Proxy	
Hardware Additions	Trusted Developer Utilities	Web Shell	Trusted Developer Utilities	Input Capture	Remote System Discovery	Clipboard Data	Clipboard Data	Clipboard Data	Fallback Channels	
Drive-by Compromise	Spooler Service	Obtainpriv	Timestamping	Keyboard Hooking	Query Registry	Clipboard Data	Clipboard Data	Clipboard Data	Domain Fronting	
	Source	Service Registry Permissions Weakness	Template Injection	Forward Authentication	Pass the Hash	Clipboard Data	Clipboard Data	Clipboard Data	Data Encoding	
	Signed Script	Port Monitors	Space after Filename	Exploitation for Credential Access	Peripherals Device Discovery	Clipboard Data	Clipboard Data	Clipboard Data	Custom Cryptographic Protocol	
	Proxy Configuration	Parameter Pollution	Self-Signing	Check for Files	Logon Scripts	Clipboard Data	Clipboard Data	Clipboard Data	Custom Cryptographic Protocol	
	Service Execution	New Service	SIP and Trust	Credential Dumping	Network Service Scanning	Clipboard Data	Clipboard Data	Clipboard Data	Communication Through Removable Media	
	Scripting	Launch Daemon	Provider Hijacking	Brute Force	File and Directory Discovery	Clipboard Data	Clipboard Data	Clipboard Data	Removable Media	
	Rundll32	Hooking	Signed Binary	Bash History	Network Admin Shares	Clipboard Data	Clipboard Data	Clipboard Data	Multi-hop Protocol	
	Regedit	File System Weakness	Process Injection	Processor Monitoring	Application Deployment Software	Clipboard Data	Clipboard Data	Clipboard Data	Fallback Channels	
	Regsvr32/Regasm	Obtainpriv	Rootkit	Access Control Weakness	Port Knocking	Clipboard Data	Clipboard Data	Clipboard Data	Domain Fronting	
	PowerShell	Application Shimming	Rundll32	Secur3t! Memory	Application Discovery	Clipboard Data	Clipboard Data	Clipboard Data	Data Encoding	
	Mohist	Aspirin DLL	Rootkits	Credentials in Registry	System Network Connections Discovery	Clipboard Data	Clipboard Data	Clipboard Data	Custom Cryptographic Protocol	
	Java exploit	Applet DLL	Regedit	Redundant Access	System Information Discovery	Clipboard Data	Clipboard Data	Clipboard Data	Communication Through Removable Media	
	Graphical User Interface	Accessibility Features	Process Following	Process Hollowing	Account Discovery	Clipboard Data	Clipboard Data	Clipboard Data	Standard Cryptographic Protocol	
	Winlogon Helper DLL	Sudo Calling	Process Hollowing	Process Hollowing	Windows Admin Shares	Clipboard Data	Clipboard Data	Clipboard Data	Removable File Copy	
	Client Execution	UAC	Process Hollowing	Process Hollowing	Windows Firewall	Clipboard Data	Clipboard Data	Clipboard Data	Custom Command and Control Protocol	
	Execution via API	SID-History Infection	Port Knocking	Process Hollowing	Windows Firewall	Clipboard Data	Clipboard Data	Clipboard Data	Community Used Port	
	Dynamic Data Exchange	Exploitation for Privilege Escalation	Obfuscated Files or Information	Port Knocking	Windows Firewall	Clipboard Data	Clipboard Data	Clipboard Data		
	Control Panel Items	SIP and Trust Provider	Network Share Configuration	Process Hollowing	Windows Firewall	Clipboard Data	Clipboard Data	Clipboard Data		
	Compiled DLL File	Adjusting	Modify Registry	Process Hollowing	Windows Firewall	Clipboard Data	Clipboard Data	Clipboard Data		
	Compiled EXE File	Security Configuration Provider	Massqueering	Process Hollowing	Windows Firewall	Clipboard Data	Clipboard Data	Clipboard Data		
	Common Language Interface	Screen savers	LCM Massqueering	Process Hollowing	Windows Firewall	Clipboard Data	Clipboard Data	Clipboard Data		
	CMSTF	Reopen Applications	Launch	Install-IT	Windows Firewall	Clipboard Data	Clipboard Data	Clipboard Data		
	Windows Management Instrumentation	Re-opened Applications	Install Root Certificate	Install-IT	Windows Firewall	Clipboard Data	Clipboard Data	Clipboard Data		
	Instrumentation	Rc common	Install Root Certificate	Indicator Removal/Deception	Windows Firewall	Clipboard Data	Clipboard Data	Clipboard Data		
	Signal Binary	Root Knocking	Component Firmware	Indicator Removal from Tools	Indicator Blocking	Clipboard Data	Clipboard Data	Clipboard Data		
	Proxy Execution	Office Application Startup	Indicator Removal/Deception	Hidden Files and Directories	Hidden Files and Directories	Clipboard Data	Clipboard Data	Clipboard Data		
	Execution through Module Load	Nethelp Helper DLL	Component Firmware	Hidden Files and Directories	Hidden Files and Directories	Clipboard Data	Clipboard Data	Clipboard Data		
		Modify Existing Service	Indicator Removal from Tools	Hidden Files and Directories	Hidden Files and Directories	Clipboard Data	Clipboard Data	Clipboard Data		
		Logon Scripts	Indicator Blocking	Hidden Files and Directories	Hidden Files and Directories	Clipboard Data	Clipboard Data	Clipboard Data		
		UAC	Hidden Window	Hidden Files and Directories	Hidden Files and Directories	Clipboard Data	Clipboard Data	Clipboard Data		
		LC LOAD DLLB Addition	Hidden Users	Hidden Files and Directories	Hidden Files and Directories	Clipboard Data	Clipboard Data	Clipboard Data		
		Launch Agent	Hidden Window	Hidden Files and Directories	Hidden Files and Directories	Clipboard Data	Clipboard Data	Clipboard Data		
		Kernel Modules and Extensions	Hidden Users	Hidden Files and Directories	Hidden Files and Directories	Clipboard Data	Clipboard Data	Clipboard Data		
		Hidden Files and Directories	Indicator Removal/Deception	File System Logical Offsets	File System Logical Offsets	Clipboard Data	Clipboard Data	Clipboard Data		
		External Remote Services	External Remote Services	File Permissions Modification	File Permissions Modification	Clipboard Data	Clipboard Data	Clipboard Data		
		Create Account	Create Account	File Deletion	File Deletion	Clipboard Data	Clipboard Data	Clipboard Data		
		Component Object Model Hijacking	Change Default File Association	Exploit for Defense Evasion	Exploit for Defense Evasion	Clipboard Data	Clipboard Data	Clipboard Data		
		Change Default File Association	Bootup	Disabling Security Tools	Disabling Security Tools	Clipboard Data	Clipboard Data	Clipboard Data		
		BITS jobs	BITS jobs	Deobfuscate Files or Information	Deobfuscate Files or Information	Clipboard Data	Clipboard Data	Clipboard Data		
		Authentication Package	Authenticode Signature	Control Panel Items	Control Panel Items	Clipboard Data	Clipboard Data	Clipboard Data		
		Administrator Privileges	Hash profile and hash	Component Object Model Hijacking	Component Object Model Hijacking	Clipboard Data	Clipboard Data	Clipboard Data		
		Time Providers	Compiled HTML File	Code Signing	Compiled HTML File	Clipboard Data	Clipboard Data	Clipboard Data		
		System Firmware	CMSTF	CMSTF	CMSTF	Clipboard Data	Clipboard Data	Clipboard Data		
		Shared Modules	Clear Control and History	BITS jobs	Clear Control and History	Clipboard Data	Clipboard Data	Clipboard Data		
		Redundant Access	Signed Script Proxy Execution	Signed Script Proxy Execution	Signed Script Proxy Execution	Clipboard Data	Clipboard Data	Clipboard Data		
		Hypervisor	Scripting	Scripting	Scripting	Clipboard Data	Clipboard Data	Clipboard Data		
		Component Firmware	NTFS Attributes	NTFS Attributes	NTFS Attributes	Clipboard Data	Clipboard Data	Clipboard Data		
		Browser Extensions	Motd	Indicator Removal on Host	Indicator Removal on Host	Clipboard Data	Clipboard Data	Clipboard Data		
			DLL Side-Loading	OCHashflow	OCHashflow	Clipboard Data	Clipboard Data	Clipboard Data		

The MITRE ATT&CK™
Enterprise Framework

attack.mitre.org

MITRE

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	Background container	Privileged container	Clear container logs	List k8s secrets	Access the k8s API server	Access cloud services	Data destruction
Compromised images in registry	bash/cmd inside container	Writable hostPath mount	Cluster-admin binding	Delete k8s events	Mount service principal	Access Kublet 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 (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

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	Exec into container	Backdoor container	Pivoted container	Clear container logs	List k8s secrets	Access the k8s master server	Access cloud sources	Data exfiltration
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	Leave container	Kubernetes cronjob	hostPath mount	Port/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 host mounts on 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	Exec into container	Backdoor container	Privileged container	Clear container logs	List k8s secrets	Access the k8s 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 platform interface, specifically the RBAC section. The top navigation bar shows system statistics: 2 CLUSTERS, 3 NODES, 158 VIOLATIONS, 63 DEPLOYMENTS, 40 IMAGES, and 22 SECRETS. On the right, there are search, CLI, and AK buttons.

The left sidebar contains a navigation menu with the following items:

- DASHBOARD
- NETWORK GRAPH
- VIOLATIONS
- COMPLIANCE
- VULNERABILITY MANAGEMENT
- CONFIGURATION MANAGEMENT
- RISK
- PLATFORM CONFIGURATION
- API REFERENCE
- HELP CENTER

The bottom of the sidebar indicates the version: v3.0.45.0.

The main content area is titled "ROLES Entity List" and shows 189 ROLES. A specific role, "CLUSTER-ADMIN Role", is selected and detailed below:

Role Summary

- METADATA**:
 - Role Type: ClusterRole
 - Created: 06/04/2020 | 8:10:10PM
 - 0 LABELS
 - 0 ANNOTATIONS
- CLUSTER**: Shows a cluster icon labeled "production" with the number 3.
- USERS & GROUPS**: Shows the number 3.
- SERVICE ACCOUNTS**: Shows the number 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)
 - Verbs: * (All verbs) → Resources and Non-resource URLs: * (All resources)

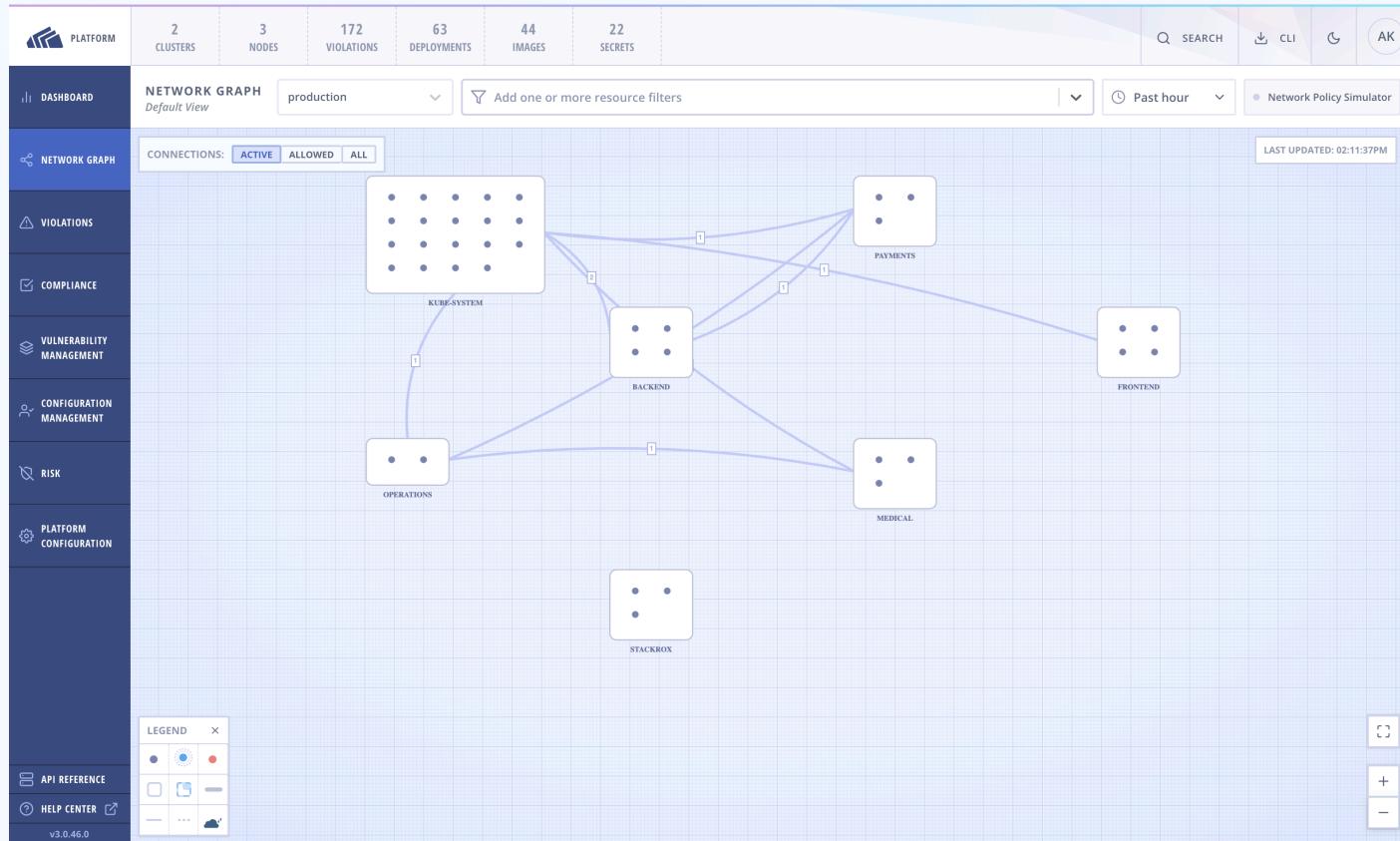
Step 2: Configure Network Policies

- 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 tapping	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 endpoint	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	Exec into container	Backdoor container	Privileged container	Clear container logs	List k8s secrets	Access the k8s API server	Access cloud sources	Data destruction
Compromised images in registry	bash/cmd inside container	Writable hostPath mount	Cluster-admin binding	Delete k8s secrets	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		

Detect insecure pod configurations

The screenshot displays the StackRox platform interface, specifically the Policies section. The left sidebar shows various navigation options: Platform, Dashboard, Network Graph, Violations, Compliance, Vulnerability Management, Configuration Management, Risk, Platform Configuration (selected), API Reference, and Help Center. The main dashboard shows summary statistics: 2 Clusters, 3 Nodes, 171 Violations, 63 Deployments, 40 Images, and 22 Secrets. The Policies section lists 64 policies, including:

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

The right side of the screen shows the "WRITABLE HOSTPATH MOUNT" configuration details, including policy criteria for host mount writability (Writable or Read-only) and volume source (Volume Source: /var/lib/docker). A sidebar on the right provides a list of policy fields to drag and drop, such as Image Registry, Image Remote, Image Tag, Image Contents, Container Configuration, Deployment Metadata, Storage, Networking, Process Activity, and 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