RSAC | 2025 Conference

Many Voices.
One Community.

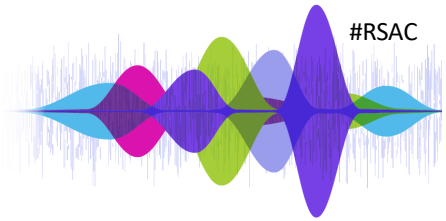
SESSION ID: LAB1-T09

Attacking and Defending Kubernetes: Privilege Escalation & Lateral Movement

Eric Johnson
Author & Instructor, SANS Institute
Principal Security Engineer, Puma Security
linkedin.com/in/eric-m-johnson/

Shaun McCullough
Author & Instructor, SANS Institute
Cloud Security Architect, GitHub
linkedin.com/in/cybergoof/

Disclaimer



Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

RSAC | 2025 Conference

Getting Started

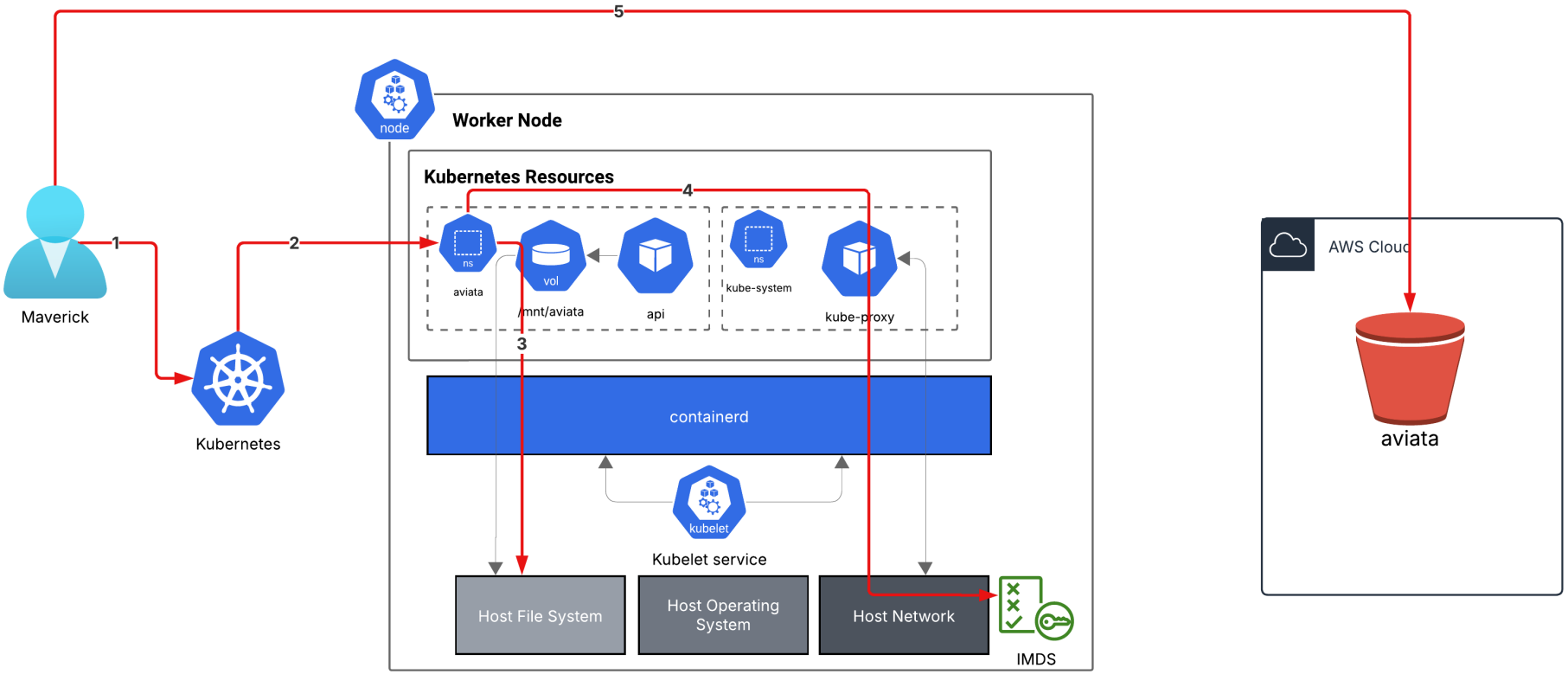
10 minutes

https://sec540.com/rsa25-lab1-t09

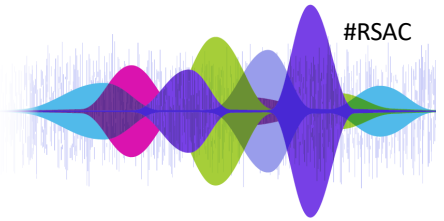
- Follow the Getting Started instructions to connect to the OpenVSCode server
- The facilitator will provide you with a link to access the SmartProxy configuration file

Many Voices.
One Community.

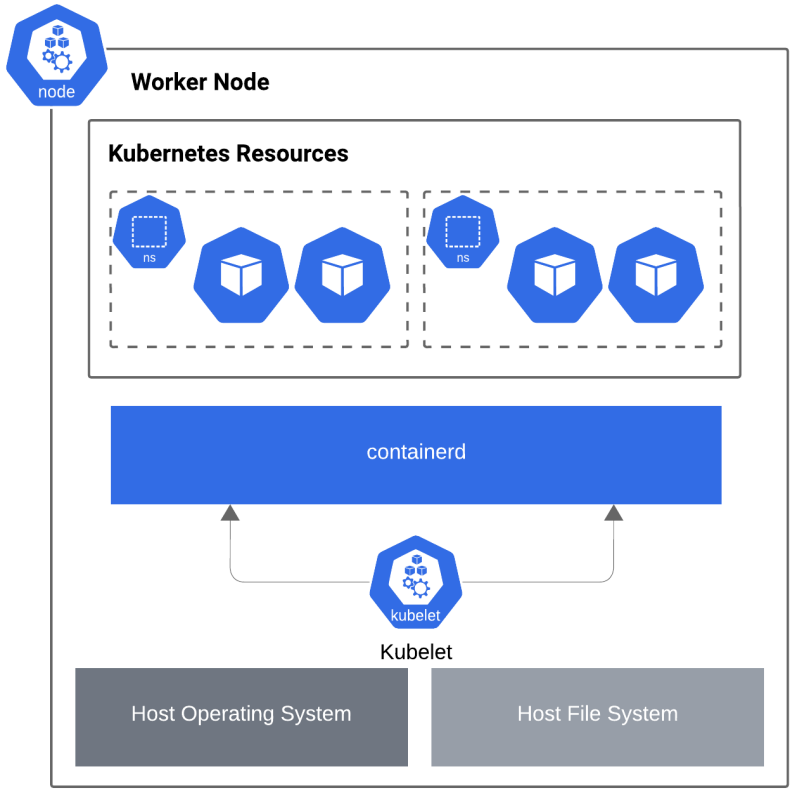
Learning Lab Goals



Kubernetes Node Components



- Kubernetes worker nodes run a host operating system (e.g., Google COS, Amazon Linux 2, Amazon Ubuntu, RHEL) and a container runtime
- Container runtimes, containerd, provide isolation for containers running on the worker node
- Kubernetes resources are managed by the kubelet running on the host through containerd
- Pods directly using the host's namespace or file system can bypass container security controls



RSAC | 2025 Conference

Host Path Mount Misconfiguration

- Identify the pod using a host path mount
- Find the Shadowhawk passphrase on the node's file system

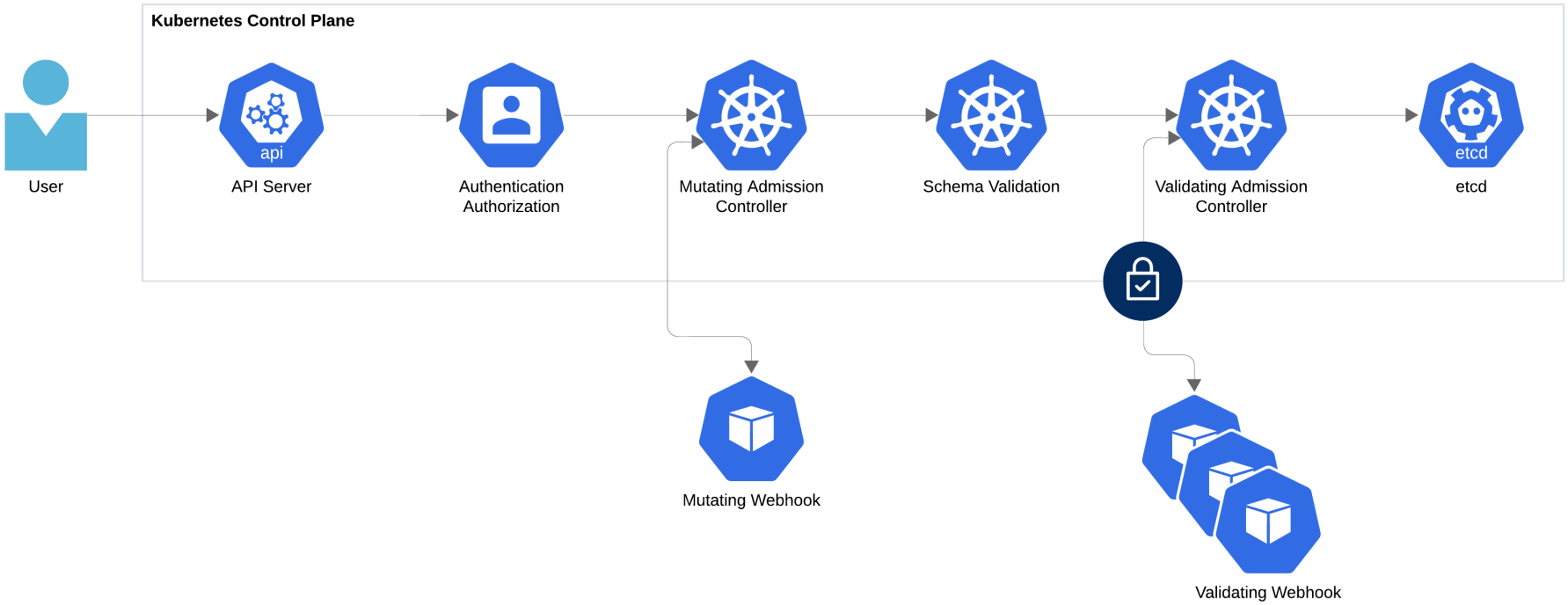
15 minutes

https://sec540.com/rsa25-lab1-t09

Many Voices.
One Community.

Kubernetes Admission Controllers

Deploy a validating admission controller that blocks the overly scoped host path mount configuration:



RSAC | 2025 Conference

OPA Gatekeeper Constraints

30 minutes

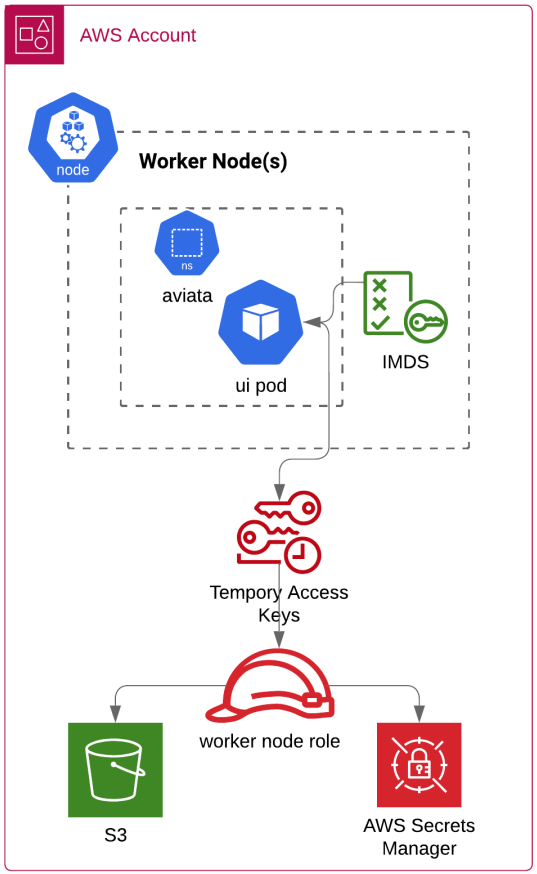
https://sec540.com/rsa25-lab1-t09

- Install the gatekeeper library constraint templates
- Create a constraint that prevents the host path mount configuration

Many Voices.
One Community.

Pod Permission Inheritance

- Cloud managed nodes need permissions to manage network resources (interfaces, load balancers, IP addresses, etc.)
- Service accounts are attached to cloud virtual machines to grant these permissions to the Kubelet and other *kube-system* pods running on the node
- Workloads (Web, API) inherit these permissions by default through the node's instance metadata service (IMDS)



RSAC | 2025 Conference

Pod Permission Inheritance

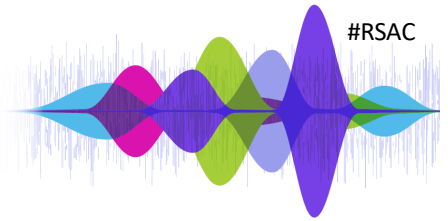
15 minutes

https://sec540.com/rsa25-lab1-t09

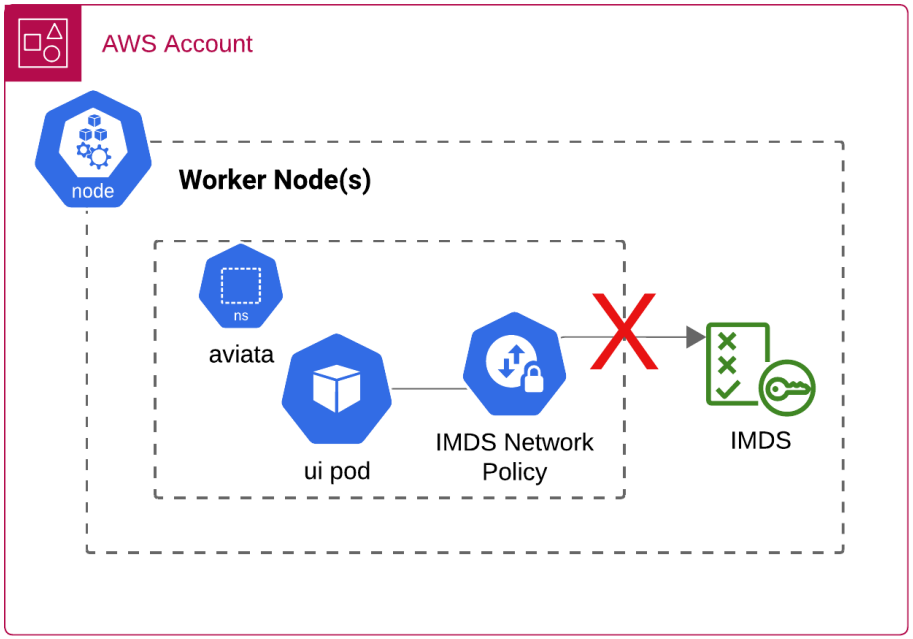
- Obtain temporary credentials from the node's instance metadata service
- Use the node's temporary credentials to exfiltrate the Shadowhawk startup code from S3

Many Voices.
One Community.

Calico Network Policy Enforcement



- Calico network policy extends Kubernetes policy with several advanced features:
  - Rule priority, deny rules, identity-based match options
  - Multiple types of endpoints including pods, VMs, and host interfaces.
- Write a Calico network policy that denies access to the node's IMDS



RSAC | 2025 Conference

Calico Network Policy Enforcement

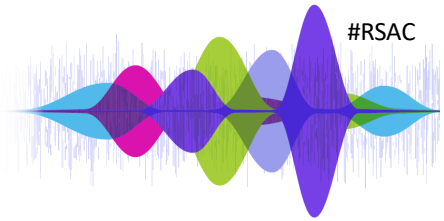
30 minutes

https://sec540.com/rsa25-lab1-t09

- Write a Calico network policy that denies access to the node's instance metadata service
- Verify that the pods can no longer access the IMDS

Many Voices.
One Community.

Apply What You Have Learned Today



- Next week you should:
  - Search clusters for overly scoped host path volume mounts
  - Audit pod access to the IMDS for privilege escalation issues
- Within three months, you should:
  - Deploy admission controllers blocking dangerous misconfigurations
- Within six months, you should:
  - Deploy network policy restricting east/west and egress pod traffic

RSAC | 2025 Conference

Many Voices.
One Community.

SESSION ID: LAB1-T09

Thank you for attending!

Eric Johnson
Author & Instructor, SANS Institute
Principal Security Engineer, Puma Security
linkedin.com/in/eric-m-johnson/

Shaun McCullough
Author & Instructor, SANS Institute
Cloud Security Architect, GitHub
linkedin.com/in/cybergoof/