Monitoring Kubernetes sensitive role activities

Scenario: Kubernetes is the most used container orchestration platform. It contains sensitive roles that, if accessed by an attacker, can lead to cluster compromise. These roles can define permissions on namespaces or clusters, grant access to cluster-scoped resources and non-resource endpoints, and read secrets. You want to detect sensitive role usage within your Kubernetes clusters to verify that activity is legitimate. The Splunk Security Research team developed this use case to help you detect suspicious requests against Kubernetes sensitive role activities.

Prerequisites

To succeed in implementing this use case, you need the following dependencies, resources, and information.

- People: Threat hunter, system administrator, security tools engineer
- Technologies: Splunk Enterprise or Splunk Cloud Platform
- Data:
  - Common Information Model
  - Kubernetes for AWS, Azure, or GCP

How to use Splunk software for this use case

You can run many searches with Splunk software to monitor Kubernetes sensitive role activities. Depending on what information you have available, you might find it useful to identify some or all of the following:

- Kubernetes sensitive roles
- Most active Kubernetes service accounts
- Kubernetes role-based access control authorizations

Results

To maximize their benefit, the how-to articles linked in the previous section likely need to tie into existing processes at your organization or become new standard processes. These processes commonly impact success with this use case:

- Kubernetes best practices for securing your cluster

Measuring impact and benefit is critical to assessing the value of monitoring Kubernetes sensitive role activities. The following are example metrics that you can track when implementing this use case:

- Permission requests from unknown or unauthorized users
- Sensitive role activities performed by unknown or unauthorized users
• Top sources of IP addresses, users and user groups requesting or performing activities under sensitive roles

Additional resources

If you have questions about this use case, see the Security Research team’s support options on GitHub. In addition, these Splunk resources might help you understand and implement this use case:

• Conf Talk: Effective strategies for monitoring Docker and Kubernetes environments
• Conf Talk: Attacking and defending Kubernetes
• Blog: Challenges in monitoring Kubernetes environments
• Blog: Approaching Azure Kubernetes security
• Tech Talk: Monitor and troubleshoot Kubernetes-based deployments
• Tech Talk: Splunk Operator for Kubernetes: Effortlessly deploy, scale, and manage Splunk

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.