Detecting Kubernetes scanning activity

Scenario: Kubernetes is the most used container orchestration platform. It contains sensitive information and management privileges of production workloads, microservices, and applications. You need to defend your organization against Kubernetes cluster fingerprint scans and attacks by providing information on items such as source IP addresses, user agents, and cluster names when scans are detected. The Splunk Security Research team developed this use case to help you detect suspicious unauthenticated requests from the internet to a Kubernetes cluster.

Prerequisites

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

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

How to use Splunk software for this use case

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

- Amazon EKS Kubernetes cluster scan detection
- Amazon EKS Kubernetes pod scan detection
- Azure Kubernetes scan fingerprinting
- Azure Kubernetes pod scan fingerprinting
- GCP Kubernetes cluster scan detection

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 detecting Kubernetes scanning activity. The following are example metrics that can be useful to monitor when implementing this use case:
• Less unauthenticated traffic to sensitive URLs: The provided detections provide an understanding of the HTTP API traffic your cluster is seeing that is unauthenticated

• Identified presence of scanning tools: Tools such as Zgrep or Nmap are usually clear indicators of suspicious activity.

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:

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