Xây dựng hệ thống giám sát bảo mật container với Falco - Thiết lập **Falco** để phát hiện hoạt động đáng ngờ trong Kubernetes. - Gửi cảnh báo đến Prometheus, Grafana, hoặc Slack qua AlerManager

Falco là gì?

Falco là một công cụ **giám sát bảo mật container** mã nguồn mở, giúp phát hiện **hành vi đáng ngờ** trong hệ thống Linux, Docker, Kubernetes. Nó phân tích các **syscalls (lời gọi hệ thống)** để phát hiện dấu hiệu tấn công.

Cách hoạt động của Falco

1. **Thu thập sự kiện từ kernel** thông qua driver eBPF hoặc kernel module.
2. **Áp dụng các quy tắc bảo mật** để kiểm tra xem có hành vi bất thường hay không.
3. **Gửi cảnh báo** đến hệ thống giám sát như Prometheus, Grafana hoặc gửi email, Slack.

Ví dụ về hành vi đáng ngờ mà Falco phát hiện

Container chạy với đặc quyền root.
Một tiến trình mới khởi động trong container (có thể là backdoor).
Một container thực thi lệnh `exec` để mở shell.
Thay đổi quyền truy cập file quan trọng `/etc/passwd`.
Kết nối mạng đáng ngờ từ container ra bên ngoài.

Cài đặt Falco trên Kubernetes

```
helm repo add falcosecurity https://falcosecurity.github.io/charts
helm repo update
helm install falco falcosecurity/falco
```

Sau khi cài đặt, Falco sẽ tự động giám sát hoạt động trong cluster.

Ví dụ về quy tắc Falco

Tạo một quy tắc phát hiện nếu container chạy lệnh `bash`:

```
- rule: Detect Bash Execution
  desc: Phát hiện khi một container chạy Bash
  condition: spawned_process and container and proc.name = "bash"
  output: "Container [%container.name] chạy Bash (PID: %proc.pid)"
  priority: WARNING
```

Gửi cảnh báo đến Prometheus, Slack

Falco có thể tích hợp với AlertManager để gửi cảnh báo. Ví dụ, để gửi alert đến Slack:

```
webhook_output:
  enabled: true
  url: "https://hooks.slack.com/services/XXX/YYY/ZZZ"
```

So sánh Falco với các công cụ khác

Công cụ	Chức năng
Falco	Giám sát container dựa trên syscall, phát hiện tấn công thời gian thực.
Sysdig	Phân tích hành vi hệ thống, hỗ trợ forensic.
Auditd	Giám sát hành vi Linux, không chuyên sâu cho container.

Lợi ích của Falco

Phát hiện tấn công container sớm trước khi hacker xâm nhập sâu hơn.
Nhẹ, hiệu suất cao, không làm chậm hệ thống.
Dễ tích hợp với các hệ thống giám sát hiện có (ELK, Prometheus, Grafana).