Falco

Descripción

Falco es un sistema de detección de intrusos para Kubernetes y contenedores. Monitorea el comportamiento en tiempo real basado en reglas.

Uso local

```
falco       # Inicia la monitorización
```

Reportes

- Logs, JSON, alertas.
- Puede enviar a Syslog, Slack, Webhooks, Prometheus.

Integración en CI/CD

- No escanea código, pero puede monitorear pods en tiempo real durante tests.

Integraciones

- Prometheus, Grafana, Slack, Microsoft Teams, Elasticsearch, Jira.
- VSCode: no aplicable.

UI

- No posee UI, se integra con dashboards como Grafana.

Licencia

- **Open source (Apache 2.0)**.
- Instalación sencilla en VMs o clústeres.

Facilidad de uso

- Avanzado. Requiere conocimientos de reglas y eventos del sistema.

Cumplimiento con estándares:

- **OWASP:** No aplica directamente, pero puede apoyar seguridad operacional en ambientes donde se despliegan apps OWASP.
- **NIST:** Compatible con NIST 800-53 en controles como SI-4 (detección de incidentes), AU-6 (auditoría y monitoreo).
- **ISO/IEC 27001:** Apoya el cumplimiento de controles como A.12.4 (registro de eventos) y A.16.1 (gestión de incidentes).
- **CIS Benchmarks:** Se utiliza para detectar desviaciones en tiempo real de configuraciones definidas por CIS.

Revisión #10
Creado 16 julio 2025 17:42:22
Actualizado 16 julio 2025 22:36:59