Descripción del proyecto

Equipo:
Error 404

Track:
Converge

Propuesta

Por medio de herramientas y procedimientos implementables en **Grafana,** crear un sistema de detección de **anomalías internas**; tal que, minimice los defectos en la gestión de permisos por medio de interacción humana, gracias a la evaluación de rutinas y patrones para cada trabajador independientemente de su rol, por medio de **Machine learning.**

Recursos

Grafana:
Grafana es una plataforma interactiva y dinámica open source escrita en lenguaje Go que se utiliza principalmente para monitorizar infraestructuras y aplicaciones IT.

Grafana Machine Learning:
Grafana Machine Learning es una herramienta poderosa con una gama en expansión de capacidades de análisis de datos e inteligencia artificial generativa diseñada para facilitar e informar la toma de decisiones proactiva y la respuesta a incidentes.

Falco (enlazado a Grafana):
Falco es una herramienta de seguridad nativa de la nube diseñada para sistemas Linux. Emplea reglas personalizadas sobre eventos del kernel, enriquecidos con metadatos de contenedores y Kubernetes, para proporcionar alertas en tiempo real.

KubeBench (enlazado a Grafana):
Kube-bench es una aplicación escrita en Go que verifica si Kubernetes está implementado de forma segura ejecutando las pruebas documentadas en el CIS Kubernetes Benchmark.

Trivy (enlazado a Grafana):
Trivy es un escáner de seguridad completo. Es confiable, rápido, extremadamente fácil de usar y funciona donde sea que lo necesites. Trivy cuenta con diferentes escáneres que buscan diferentes problemas de seguridad, y diferentes objetivos donde puede encontrar esos problemas.

Acciones

Lanzamiento de alertas dependiendo del grado o nivel de “importancia”, esto directo a las personas encargadas de TI y administradores globales.

Usaremos IA, la cual “**aprenderá” las rutinas** o acciones que llevan a cabo los usuarios, donde se hará un monitoreo y se reportará de acciones que pueden estar fuera de su rutina aprendida por la IA, siendo así un **proyecto autosostenible.**

Existirá el bloqueo de acciones o en sí, un bloqueo general el cual solo podrá ser removido por las personas encargadas y capacitadas, verificando así si esta **acción es maliciosa** o no.

Fortalezas

Autosustentabilidad: Gracias al aprendizaje de las rutinas de los usuarios, los administradores sólo tendrán que encargarse de la validación manual, más no de la supervisión de el mismo proceso, dicho así, no habrán aperturas de canales ni permisos, fuera de los rangos normalmente establecidos.

Accesibilidad: Al ser una herramienta de evaluación en segundo plano, no representa una interacción directa con el humano, salvo los que posean roles administrativos.

Adaptabilidad: Esta solución tiene una implementación viable para casi cualquier entorno correspondiente.

Debilidades

Configuración: Es imprescindible la adecuada configuración de roles, permisos, dispositivos y credenciales de acceso, ya que de ello depende el correcto entendimiento de las rutinas.

Poca intervención humana: Su fortaleza se vuelve su debilidad, todavía depende de la intervención humana´para verificar los incidentes, de modo que dependiendo de la situación, se ve puede ver rebasado los incidentes.

Anomalías falsas: Al inicio se pueden detectar anomalías falsas debido al poco aprendizaje de la IA, por lo cual se complementa con el punto anterior.

Beneficios según los roles.

Trabajadores:

- Eficacia y rapidez en la petición de permisos especiales.
- Acceso inteligente a recursos de la empresa.

IT/Admins:

- Reducción de mantenimiento e intervención.
- Adaptabilidad de rutinas.
- Optimización de procesos recurrentes.

Directivos:

- Reducción de la intervención humana.
- Mejoras en la disponibilidad de personal.
- Ahorro de tiempos por automatización
- Reducción de brechas de seguridad en el acceso al sistema.