Monitoreo y logging

Parte 1

Ud. está trabajando en una plataforma web que recibe ataques SQLi, IDOR y XSS frecuentemente. Además, durante las noches son atacados mediante payloads que logran que la memoria RAM del servidor se ocupe en su totalidad, haciendo que la plataforma web se caiga.

1. ¿Qué logs definiría a nivel de aplicación? ¿Qué datos registraría por cada log?
2. ¿En qué aspecto de hardware realizaría monitoreo para poder reaccionar ante caídas de la plataforma web?
3. ¿Qué alertas definiría para enterarse lo antes posible ante un ataque?
4. Si el tamaño de los archivos de logs crecen mucho, ¿qué haría?
5. ¿Considera que una herramienta como Grafana serviría en este caso o prefiere ir por una alternativa más simple? Justifique.

Parte 2

1. Dado el archivo de logs subido a la UV, determinar si hubo intentos de ataques SQLi.
2. ¿Cómo haría para detectar en tiempo real un ataque SQLi?

Parte 3

Considerando el sistema de Ciudadano Digital de Córdoba (CiDi) y las siguientes 2 APIs.

API 1: Solicitar trámite.
API 2: Eliminar trámite.

1. Definir los riesgos de seguridad asociados a cada API (a nivel técnico). Por ejemplo, “Un ciberdelincuente elimina un trámite de otro ciudadano”.
2. Por cada riesgo, definir un nivel de probabilidad de ocurrencia y de impacto.
3. ¿Considera que una gestión de logs correcta podría resolver o minimizar el impacto o la probabilidad de ocurrencia de algún riesgo?