**Informe Técnico**

**Evaluación y Mejora Continua de la Seguridad en una API RESTful – SecureConnect**

**1. Escenario**

La empresa **SecureConnect** expone públicamente una API RESTful para la autenticación y consulta de clientes. Durante una auditoría rutinaria se identificaron deficiencias en la gestión de logs, ausencia de métricas de seguridad, falta de pruebas de penetración periódicas y exposición de información sensible en respuestas de error. El objetivo del análisis fue **documentar las debilidades encontradas y proponer un plan de mejora integral** basado en monitoreo, métricas y pruebas continuas de seguridad.

**2. Debilidades y Medidas Correctivas**

| **Debilidad Identificada** | **Medida Correctiva / Control Propuesto** | **Justificación Técnica** |
| --- | --- | --- |
| Falta de logs de acceso y errores | Implementar **sistema centralizado de logging** (ELK, Wazuh, Splunk). | Permite correlacionar incidentes, detectar accesos maliciosos y cumplir con normativas de auditoría. |
| Ausencia de métricas de seguridad (KPI) | Definir KPIs como **tasa de errores 5XX** y **MTTR (Mean Time To Resolution)**. | Proporciona visibilidad continua del estado de seguridad y eficacia de las medidas aplicadas. |
| No realizar pentesting en la API | Programar **pruebas de penetración trimestrales** con OWASP ZAP o Burp Suite. | Detecta vulnerabilidades antes de que sean explotadas y valida la efectividad de los parches. |
| Respuestas de error con detalles internos | Configurar mensajes de error genéricos y habilitar **manejadores de excepciones seguras**. | Evita la filtración de información sensible (cabeceras internas, rutas, estructuras de BD). |

**3. Indicadores de Seguridad (KPI)**

1. **% de reducción mensual de errores 5XX**
   * **Propósito:** medir la efectividad de las mejoras aplicadas en la estabilidad de la API.
   * **Medición:** número de errores 5XX registrados en logs dividido por total de peticiones, comparado mes a mes.
2. **Tiempo promedio de resolución de alertas (MTTR)**
   * **Propósito:** evaluar la capacidad del equipo para responder ante incidentes de seguridad.
   * **Medición:** tiempo promedio desde la detección de una alerta hasta su cierre documentado.

**4. Implementación de Monitoreo Continuo**

Se recomienda un esquema híbrido con **herramientas open source**:

* **Logs y SIEM:** ELK Stack (Elasticsearch + Logstash + Kibana) o Wazuh para correlación de eventos.
* **Pruebas periódicas:** OWASP ZAP automatizado en pipeline CI/CD para detectar vulnerabilidades OWASP Top 10.
* **Métricas y visualización:** Prometheus + Grafana para recolectar y mostrar KPIs en paneles en tiempo real.
* **Alertas:** Integración con Slack/Teams o correo electrónico para notificaciones inmediatas al SOC.

**5. Conclusión**

El análisis de la API de SecureConnect reveló debilidades críticas de visibilidad y control que comprometen su seguridad. La implementación de **logging centralizado, definición de KPIs, pruebas de penetración periódicas y monitoreo continuo** permitirá mejorar la postura defensiva de la organización, alineándola con buenas prácticas de **OWASP API Security Top 10** y marcos de referencia como **NIST SP 800-53**.