

Perfil 2: Analista de Ciberseguridad

Responsabilidades Principales

Operación de Redes, Perímetro e Identidad (IAM)

- Administrar y optimizar la seguridad perimetral mediante Firewalls/UTM (Fortinet / FortiGate), segmentación de redes, políticas de tráfico y VPNs.
- Administrar y dar soporte operativo al Proveedor de Identidades (IdP) corporativo, integrando aplicaciones bajo protocolos SSO, OIDC y SAML.
- Aplicar y verificar el cumplimiento de las políticas de control de accesos corporativas.

Seguridad Operativa, Endpoints y Análisis de Vulnerabilidades

- Ejecutar escaneos periódicos de vulnerabilidades (OpenVAS) en la infraestructura y realizar búsquedas de inteligencia básica (OSINT).
- Administrar la consola centralizada de protección de endpoints , gestionando alertas, políticas de uso (AUP) y bloqueo de aplicaciones no autorizadas (PUA/PUP).
- Coordinar la respuesta a incidentes de seguridad y el análisis de causas raíz (RCA).

Integración DevSecOps (Soporte a Desarrollo)

- Configurar e integrar herramientas de escaneo de código (SAST/DAST) y análisis de dependencias dentro de los pipelines de CI/CD (GitLab CI, GitHub Actions).
- Ejecutar el escaneo de seguridad sobre imágenes de contenedores (Docker) antes de su paso a producción.
- Asistir a los desarrolladores en la interpretación y remediación de vulnerabilidades detectadas.

Aplicación de Políticas y Documentación

- Velar por la aplicación práctica de las políticas organizacionales de seguridad de la información.
- Documentar procedimientos operativos de seguridad, diagramas de red actualizados e informes técnicos de incidentes/vulnerabilidades.

Requisitos Excluyentes

- Formación/certificaciones con orientación en ciberseguridad
- Experiencia acreditable en puestos similares igual o mayor a 5 años

Stack Tecnológico, Competencias Técnicas y habilidades Obligatorias

- **Administración de Firewalls / UTM:** Experiencia práctica en configuración y operación diaria de equipos Fortinet / FortiGate (reglas, VPNs IPsec/SSL, políticas).
 - **Gestión de Identidades (IAM):** Experiencia operativa en integración de usuarios y aplicaciones con SSO, OIDC o SAML (ej. Keycloak, Active Directory).
 - **Protección de Endpoints:** Manejo de consolas de gestión de Antivirus/EDR corporativos y aplicación de políticas AUP/PUA.
 - **Integración DevSecOps y CI/CD:** Uso de Git y experiencia configurando etapas de escaneo automático de seguridad en pipelines de CI/CD (SonarQube, Trivy, OWASP ZAP o similares).
 - **Escaneo de Vulnerabilidades:** Manejo de herramientas de auditoría técnica como OpenVAS, Nessus o Nmap y técnicas de análisis OSINT.
 - **Hardenización de Redes y Sistemas:** Sólidos conocimientos en hardening de sistemas operativos (Linux/Windows), segmentación por VLANs y auditoría de eventos/logs.
-
- Orientación a la gestión de cambios.
 - Habilidades interpersonales y comunicación efectiva para interactuar con los equipos de desarrollo y soporte técnico.
 - Proactividad para el monitoreo constante y la resolución metódica de incidentes.

Competencias Deseables / Valoradas

- **Contenedores:** Conceptos básicos/intermedios de seguridad e inspección de imágenes en Docker y entornos orquestados (Kubernetes).
- **Sistemas Operativos y Hardening:** Conocimientos en administración y endurecimiento de Linux (Debian, Ubuntu Server) y Windows Server.
- **Scripting:** Automatización simple mediante Bash, Python o PowerShell.
- **Certificaciones Valoradas:** Fortinet, ISO 27001, NIST