ANDY BANCES CUENCA

Security Automation Engineer | Infrastructure Security | DevSecOps
Lomas de Zamora, Buenos Aires, Argentina
andybc262@hotmail.com
+541162665686
https://www.linkedin.com/in/andybances/
andybc262@hotmail.com | 1162665686 | Lomas de Zamora. Buenos Aires. Argentina

Perfil Profesional

Ingeniero de Sistemas con +5 años de experiencia en administración de infraestructura híbrida (Linux/Windows) y automatización de controles de seguridad. Especializado en hardening de sistemas, seguridad en Active Directory, protección perimetral con Fortinet y MikroTik, e integración de APIs para automatización de respuestas ante incidentes.
Experiencia en implementación de honeypots, monitoreo avanzado (Grafana, Kibana, Graylog), y desarrollo de automatizaciones con Ansible y PowerShell orientadas a reducir tiempos de respuesta y mejorar la postura de seguridad organizacional.
Perfil técnico con enfoque en eficiencia operativa, automatización de seguridad y mejora continua.

Experiencia Profesional

Netqual SRL – Argentina
SysAdmin SSr | Agosto 2024 – Actualidad

Administración de Infraestructura
- Gestión integral de servidores Linux y Windows en entornos virtualizados y físicos.
- Implementación de hardening en sistemas operativos y servicios críticos.
- Administración avanzada de Active Directory (GPOs, permisos, políticas de seguridad, control de accesos).

Automatización y DevSecOps
- Desarrollo de automatizaciones con Ansible y PowerShell para tareas operativas y de seguridad.
- Integración de APIs para procesamiento automático de alertas de seguridad.
- Automatización de generación de reglas dinámicas en firewalls MikroTik y Fortinet a partir de eventos detectados por ESET.

Seguridad y Monitoreo
- Implementación y administración de Wazuh para detección de intrusiones, monitoreo de integridad de archivos (FIM), análisis de logs y correlación de eventos de seguridad.
- Implementación y monitoreo de honeypots T-Pot para detección temprana de amenazas.
- Análisis de eventos y comportamiento de atacantes mediante Kibana y Graylog.
- Evaluación continua del estado de scripts de automatización mediante Grafana conectado a API de Semaphore.
- Supervisión de infraestructura con NetXMS, identificando riesgos operativos (disco, disponibilidad, dispositivos).

Redes y Seguridad Perimetral
- Configuración y administración de dispositivos MikroTik y Fortinet (VPN, NAT, VLANs, segmentación, control de tráfico).
- Configuración de switches Cisco y Aruba (VLAN, STP, trunking, QoS).

Plataformas Cloud Empresariales
- Administración de entornos Microsoft 365 y Google Workspace.
- Aplicación de políticas de seguridad y gestión de identidades.

Xpertia Consulting SAC - Perú
Analista de Seguridad de la Información | Junio 2020 – Actualidad

- Definición de estrategias de ciberseguridad para clientes corporativos.
- Implementación y fortalecimiento de políticas de seguridad en entornos Windows y Linux.
- Gestión de Active Directory, LDAP, Postfix y Exchange.
- Análisis de amenazas a través de consolas antivirus empresariales.
- Generación de reportes avanzados consultando bases de datos (MySQL, SQL Server, PostgreSQL, SQLite).
- Capacitación técnica en soluciones de ciberseguridad.
- Soporte N1, N2 y N3.
- software y soluciones de ciberseguridad.
- Soporte N1, N2, N3.

Experiencia Inicial – Perú

Feral Electronics SAC
Server Administrator Junior | Diciembre 2019 – Marzo 2020

- Administración de Debian, PostgreSQL, redes y soporte infraestructura

Cataliz Talent Lab SAC
Practicante de soporte técnico | Noviembre 2018 – Julio 2019

- Soporte usuarios, proxy Zentyal, inventario y configuración de equipos.

Gases y Tecnología SRL
Practicante de Soporte Técnico | Enero 2017 – Enero 2018

- Mantenimiento hardware/software, hosting, correo y soporte interno

Competencias Técnicas

Seguridad y Detección de Amenazas:

- Wazuh (SIEM, HIDS, File Integrity Monitoring, detección de vulnerabilidades)
- T-Pot (Honeypots de baja y alta interacción)
- Fortinet (NS1-NS3)
- MikroTik (Firewalling, segmentación, VPN)
- Hardening Windows/Linux
- Seguridad en Active Directory
- Análisis de eventos y correlación de logs
- Pentesting en entornos controlados (NMAP,Metasploit,Kali Linux)

Automatización:

- Ansible
- Terraform
- Powershell
- Bash
- Integración de APIs REST
- YAML

Infraestructura:

- Linux (Ubuntu,Centos,RedHat)
- Windows Server
- VMWare, Proxmox, Openshift
- Docker
- Apache / Nginx
- DNS, DHCP, SSH, Samba

Monitoreo y Observabilidad:

- Grafana
- Kibana
- Wazuh
- Graylog
- NetXMS
- T-Pot

Bases de Datos

- MySQL
- PostgreSQL
- SQL Server
- SQlite

Educación

Ingeniería de Sistemas
Universidad Nacional Federico Villarreal | 2014 – 2019, Lima, Perú

Multiplatform Network Administrator

CIBERTEC | 2019, Lima, Perú

Certificaciones

- Google Workspace Deployment Services
  Diciembre (2024)
- Ethical Hacking – Educación IT (2025)
- Certiprof | Ciber Security Foundation (CyBOK v1.0)
- Fortinet | NS1, NS2, NS3.

Idiomas

- Inglés: B2 (Intermedio Alto)