Alfredo Nicolas Colombres

Buenos Aires, Argentina | +54 11 3039 5111

nicolas.colombres97@gmail.com

SKILLS

- Vulnerability Assessment
- Endpoint Security
- SIEM managementThreat Intelligence
- Log Analysis
- Incident Response
- Python Programming
- Nmap Scanning
- Security Awareness Training
- PowerShell Scripting

EDUCATION

- Fortinet NSE1 ~ Fortinet
- Database - SQL ~ EducacionIT

WORK HISTORY

Accenture - SOC Monitoring Analyst

Buenos Aires, Argentina (Remote) ~ 06/2024 - Current

- Daily monitoring alerts from Splunk, alert based on Workstation and Server
- Updating Splunk playbooks
- Knowdlege presentation for company user's, showing up Security incidents with real life case.
- Working with multiple teams for incident resolution.
- Maintained accurate documentation of all SOC activities

OmniAccess - SOC Analyst

Palma de Mallorca, Spain (Remote) ~ 03/2023 - 06/2024

- Reduced false alarms by fine-tuning intrusion detection system configurations based on historical analysis of incidents.
- Enhanced network security by monitoring systems for potential threats and vulnerabilities.
- Identified root causes of security breaches through thorough investigation and analysis of log data.
- Provided technical support during high-priority incidents, ensuring timely resolution with minimal impact on business operations
- Maintained accurate documentation of all SOC activities, facilitating knowledge sharing across the organization.
- Implemented automated tool for continuous monitoring of system logs, reducing manual efforts by the team.
- Investigated and resolved incidents of unauthorized access to sensitive information.

Telecom - Incident Response Team

Buenos Aires, Argentina ~ 01/2022 - 03/2023

- Improved incident response times by creating and maintaining detailed incident response procedures.
- Optimized incident response procedures for faster resolution and reduced downtime.
- Streamlined incident response processes for quicker threat detection and remediation.
- Provided critical incident response, maintaining composure under high-pressure situations.
- Improved incident response times by streamlining communication processes between departments.

LANGUAGES

Spanish: Native

English: B2