Romina Castro Rodriguez

Guayaquil, Ecuador | +593 998915276 | rominaarlleycastro@gmail.com | Github | Portafolio

Ingeniera en Tecnologías de la Información con más de 7 meses de experiencia en Ciberseguridad, desempeñando funciones como Analista SOC en entornos financieros de alta criticidad. Experiencia comprobada en monitoreo, análisis y respuesta a incidentes, simulación de adversarios, manejo de SIEMs como Adlumin y Wazuh, despliegue de honeypots, integración de firewalls y soluciones DLP. Certificada en Adlumin y StellarCyber. Con sólida base en estándares como ISO 27001, NIST, MITRE ATT&CK y PCI DSS. Capaz de generar informes técnicos, CTEM y casos de uso, con visión analítica y foco en mejora continua.

EXPERIENCIA LABORAL

ORION Cybersecurity — Guayaquil
Cybersecurity Engineer — Abril 2025 – Actual

- Monitoreo de eventos de seguridad y generación de alertas desde Adlumin SIEM en más de 100 activos (Windows y Linux).
- Simulación de técnicas TTPs basadas en MITRE ATT&CK mediante PowerShell y Atomic Red Team para validación de visibilidad y generación de alertas.
- Uso de GoPhish para campañas de ingeniería social personalizadas, incluyendo landing pages HTML.
- Despliegue y configuración de honeypots FTP y SMB para detección temprana de lateral movement interno.
- Integración de dispositivos de red (FortiGate, Sophos), soluciones DLP y servidores (Windows y Linux) al SIEM.
- Generación de informes técnicos, análisis de incidentes, ajuste de reglas y uso de inteligencia de amenazas.
- Desarrollo de reportes CTEM mensuales con hallazgos técnicos, vulnerabilidades, recomendaciones y mapeo MITRE.
- Uso de herramientas como Flare y VirusTotal para validación de reputación de IoCs, dominios y hashes

BANECUADOR B.P. — Guayaquil
Pasante de Seguridad de la Información — Oct 2023 – Dic 2023

- Soporte técnico (100+ casos), priorizando eficiencia y tiempos de respuesta entre 3-6 min.
- Asignación de permisos en AD, mejorando la distribución de carga en el equipo.
- Apoyo en informes del Comité de Seguridad (métricas y recomendaciones).
- Verificación del Esquema de Seguridad de la Información y apoyo en proyectos de mejora.

EDUCACIÓN

UNIVERSIDAD ESTATAL DE MILAGRO — Milagro, Ecuador
Ingeniera en Tecnologías de la Información — Graduada Nov 2024

CERTIFICACIONES

- Lead Auditor ISO 27001:2022 (CertiProf) — 2024 – 2027
- ISO 27001 Certified Lead Implementer (CertiProf) — 2024 – 2027
- Programa de Analista Junior de Cibserseguridad (Google y Cisco, en curso) — 2025
- Adlumin Certified Engineer — 2025
- StellarCyber Open XDR Certified — 2025

HABILIDADES TÉCNICAS

Herramientas y tecnologías: Adlumin, Gophish, PowerShell, Atomic Red Team, WinRM / Evil-WinRM, FortiGate CLI, VMware, Wazuh, Sophos Central, Safetica, PrivX, Nessus, MySQL, Firebase, WordPress.
Frameworks y estándares: MITRE ATT&CK, ISO 27001, PCI DSS, NIST

COMPETENCIAS TÉCNICAS

- Correlación de eventos y ajustes de reglas SIEM
- Simulación de TTPs MITRE (Discovery, Lateral Movement, Exfiltration)
- Automatización de comandos con PowerShell.
- Implementación y respuesta ante incidentes de DLP (Forcepoint, Safetica)
- Integración de sistemas de seguridad con APIs (Sophos, Adlumin), despliegue y monitoreo de honeypots y agentes EDR.
- Gestión de plataformas híbridas Linux-Windows en entornos virtualizados (VMware, cloud)
- Generación de informes técnicos, CTEM, y respuesta a auditorías de cumplimiento
- Análisis estático inicial de ejecutables .exe mediante revisión de cabeceras PE y uso de herramientas como PEStudio

IDIOMAS: Español: Nativo | Inglés Intermedio técnico – Lectura y redacción en entornos profesionales de ciberseguridad.