EC

Emiliano Agustín Cabañas Prieto

Practicante de Ciberseguridad

Datos de contacto

emi.cabanas13@gmail.com

Querétaro, México

ecapri.dev

linkedin.com/in/emiliano-cabañas-prieto

github.com/ecapri-dev

Estudios

- **Ingeniería en Tecnologías de la Información y Negocios Digitales**
  Universidad Anáhuac, Campus Querétaro
  Agosto 2023 – Presente · 7.º semestre

Habilidades

Análisis de malware — Intermedio

Pentesting y DAST — Intermedio

SIEM/XDR · Wazuh — Intermedio

Seguridad de endpoint — Intermedio

OSINT — Básico

Active Directory y PKI — Básico

NIST y LFPDPPP — Básico

Idiomas

Español — Nativo

Inglés — Intermedio-alto (B1 Cambridge)

Cursos

Hack The Box · SOPHOS · CyberGuard Day · Google Workspace

Resumen

Practicante de ciberseguridad en TGK México y estudiante de Ingeniería en Tecnologías de la Información y Negocios Digitales. Tengo experiencia en análisis de malware, pruebas de penetración a aplicaciones web (DAST), soluciones de seguridad de endpoint (EDR) y el despliegue de un SIEM/XDR con Wazuh. Busco un rol junior en seguridad ofensiva o en operaciones de seguridad (SOC / Blue Team).

Experiencia laboral

Practicante en Ciberseguridad — Antivirus y Pentesting (AV & PT), TGK México

Enero 2026 – Presente · Querétaro, México

- Desplegué y configuré un **SIEM/XDR con Wazuh** (nube y servidor en Ubuntu): enrolé agentes, integré Sysmon y File Integrity Monitoring (FIM) y creé un **decoder con reglas propias (parser)** para eventos de Deceptive Bytes vía Syslog.
- Realicé **evaluaciones de vulnerabilidades web (DAST)** con OWASP ZAP para dos dependencias gubernamentales, con reportes ejecutivo y técnico (clasificación CWE/WASC y remediación).
- Analicé más de **10 muestras de malware** en entornos aislados (sandbox), documentando su comportamiento.
- Evalué y comparé **soluciones de endpoint** (SOPHOS y Deceptive Bytes) frente a malware real en laboratorio.
- Monté un **laboratorio Windows con Active Directory (AD DC)** y una Autoridad Certificadora (AC / PKI); apliqué marcos como NIST y la LFPDPPP.
- Hice investigación de **OSINT** y exploración de la Dark Web con fines de inteligencia y seguridad.
- Practiqué seguridad ofensiva en **Hack The Box** y documenté el trabajo en reportes, un artículo de Pentesting y una guía de despliegue de Wazuh; presenté resultados al equipo y en eventos (CyberGuard Day, Google Enterprise).

Proyectos destacados

SIEM/XDR con Wazuh — despliegue end-to-end (nube y servidor Ubuntu) con decoder/parser para Deceptive Bytes vía Syslog.

Evaluación de vulnerabilidades web — DAST con OWASP ZAP y reportes ejecutivo/técnico (CWE/WASC).

Evaluación de soluciones EDR / Deception — comparativa de SOPHOS y Deceptive Bytes frente a malware real en laboratorio.

Análisis de malware en sandbox — 10+ muestras de MalwareBazaar documentadas en entorno controlado.