RAFAEL ADIOSDADO CABALLERO DIÉGUEZ

Analista de Ciberseguridad (Blue Team / SOC) · Perfil diferencial IT / OT industrial

Lucena, Córdoba (España) · +34 620 55 39 17 · adiosdado@adeodato.es · cabadier@gmail.com
adeodato.es · github.com/Adeodato-hub · LinkedIn

Disponibilidad inmediata · Certificado de discapacidad ≥ 33 %

PERFIL PROFESIONAL

Analista de ciberseguridad orientado a Blue Team y operaciones de SOC, con más de 20 años de experiencia real en entornos industriales (CNC, robótica KUKA, automatización y mantenimiento de maquinaria). Esa trayectoria aporta un perfil poco común: capacidad para desplegar y operar herramientas de seguridad IT y, al mismo tiempo, entender de primera mano los riesgos de los entornos de producción y de la tecnología operativa (OT) — maquinaria en red, sistemas de control y segmentación entre planta y administración.

Certificado Cisco CCST Cybersecurity. Experiencia práctica en despliegue de SIEM (Wazuh), IDS/NIDS (Suricata), creación de reglas de detección propias, orquestación SOAR (Shuffle), gestión de casos (DFIR-IRIS), automatización de respuesta a incidentes, análisis de logs, triaje asistido por IA con modelo local y mapeo de amenazas con MITRE ATT&CK y D3FEND, demostrada de extremo a extremo en una plataforma SOC propia y funcional (SOC Adeodato: ARGOS + AdeoSOC), documentada y publicada. Actualmente en **migración de esas detecciones propias a Microsoft Sentinel (KQL)**, con diseño de Data Collection Rules (Azure Monitor Agent), como puente al stack de mercado (objetivo SC-200).

Reorientación profesional a la ciberseguridad tras Incapacidad Permanente Total para la profesión industrial habitual, convirtiendo el conocimiento de los entornos productivos en una ventaja diferencial en seguridad IT/OT.

APORTACIÓN A LA EMPRESA: SOC ADEODATO

https://github.com/Adeodato-hub/SOC-Adeodato

No me presento solo con un CV: pongo a disposición de la empresa que me incorpore una plataforma SOC completa, ya construida y operativa, íntegramente sobre software open source y sin coste de licencias.

- Cobertura IT y OT en la misma plataforma, incluida la maquinaria en red que las soluciones genéricas ignoran.
- Arquitectura replicable y adaptable a un entorno corporativo real: detección, contención automática, gestión de casos y respuesta desde el móvil.
- Todo el núcleo opera en red privada (tailnet), sin exposición a Internet; en activos OT el aislamiento exige confirmación humana para no parar producción.
- Disponible para presentarla en demo técnica y para integrarla, ampliarla o transferir el conocimiento al equipo de sistemas/seguridad de la empresa.

COMPETENCIAS TÉCNICAS

- **Seguridad / Blue Team:** SIEM (Wazuh), IDS/NIDS (Suricata), detección de intrusiones, análisis de logs, telemetría con auditd y Sysmon, reglas de detección personalizadas, respuesta a incidentes, Active Response, SOAR (Shuffle), gestión de casos (DFIR-IRIS), triaje de alertas asistido por IA (RAG + LLM local), hardening de sistemas, MITRE ATT&CK y MITRE D3FEND, Cyber Kill Chain, ciclo PICERL. **Microsoft Sentinel, KQL, Azure Monitor Agent (AMA) y Data Collection Rules (DCR) — en formación (objetivo SC-200).**
- **Sistemas y redes:** Linux (Amazon Linux, Ubuntu/Lubuntu, Kali), Windows 11 / Windows Server, TCP/IP, segmentación de red, firewall, filtrado DNS, DNS-over-HTTPS (DoH), redes privadas con Tailscale, virtualización (VirtualBox, redes NAT), endurecimiento de routers y equipos de red.
- **Red Team / pentesting (nivel laboratorio):** Kali Linux, enumeración, fuerza bruta (Hydra), Metasploit, escalada de privilegios y explotación de CVE en entornos controlados. Aplicado a la validación de las propias defensas.
- **Scripting y automatización:** Python, Bash, automatización de alertas (Telegram, WhatsApp), backups cifrados y mantenimiento automatizado, integración de IA aplicada al triaje de alertas (Ollama / RAG).
- **Desarrollo y control de versiones:** Kotlin, Jetpack Compose, desarrollo de apps Android seguras, criptografía PBKDF2, Git y GitHub, gestión segura de secretos y credenciales (keystore, KeePassXC).
- **Desarrollo asistido por IA:** uso de asistentes y entornos agénticos (Claude, Claude Code) para scripting, desarrollo y despliegue de laboratorio, con revisión crítica del código generado y aplicación de buenas prácticas de seguridad.
- **Industrial / OT:** programación CNC e ISO, robótica KUKA, automatización, punzonado, plegado y corte por láser, AutoCAD 3D, impresión 3D, mantenimiento mecánico industrial.

CERTIFICACIONES

- Cisco Certified Support Technician (CCST) — Cybersecurity · Cisco / Certiport · jun. 2026 (válida 5 años) · ID de verificación: 4o53-XaBb (verify.certiport.com).
- Carrera Profesional de Analista Junior en Ciberseguridad · Cisco Networking Academy · jun. 2026.
- Carrera Profesional de Técnico en Redes (Network Technician) · Cisco Networking Academy · jun. 2026.
- Bootcamp en Ciberseguridad (400 h) — Red Team / Blue Team · 2026.

- Microsoft SC-200 (Security Operations Analyst) — **en preparación.**

PROYECTOS DESTACADOS

SOC Adeodato (ARGOS + AdeoSOC) — Plataforma vSOC IT/OT · github.com/Adeodato-hub/SOC-Adeodato
Integración de mis dos proyectos en una única plataforma de SOC gestionado (vSOC) para PYME e industria: detección en tiempo real, contención automática y respuesta orquestada, operable por una sola persona y sin exponer ningún servicio a Internet.

- Cadena completa de respuesta: Wazuh (SIEM/XDR) → Active Response (firewall-drop) → Shuffle (SOAR) → creación automática de caso en DFIR-IRIS con los datos reales del ataque (regla, nivel, agente, IP, técnica MITRE) → notificación a Telegram y a la app móvil.
- Cobertura OT real: inventario y monitorización de activos industriales, con alertas de exposición sin autenticación y aislamiento sujeto a confirmación humana para no detener producción.
- AdeoSOC (Kotlin): app Android de respuesta que permite al analista aislar un host, clasificar o cerrar un caso desde el teléfono, con análisis de severidad asistido por IA.
- Seguridad por diseño: todo el núcleo (Wazuh, Shuffle, IRIS) en tailnet privado con Tailscale, backups cifrados AES-256, sin secretos ni identificadores internos en el repositorio.
- Triaje con IA (ARGOS) integrado sobre los casos: enriquecimiento y priorización automática mediante modelo local servido con Ollama, sin enviar datos del incidente a servicios externos.
- Enriquecimiento con MITRE D3FEND: cada caso incorpora las contramedidas defensivas asociadas a la técnica ATT&CK detectada, de forma que el informe no solo dice qué pasó, sino qué hacer para que no vuelva a pasar.
- Mantenimiento automatizado (housekeeping, políticas de retención, anacron) y documentación del ciclo de vida completo del incidente (PICERL).

Migración a Microsoft Sentinel (KQL) — en ejecución
Traslado de las detecciones propias de ARGOS al stack de mercado (Microsoft Sentinel), como puente entre la plataforma on-premise y los SOC corporativos sobre Azure.

- Traducción y validación de reglas de Wazuh a KQL, contrastadas contra el histórico real de alertas del laboratorio (corrección de parseo y de correlación multi-evento).
- Diseño de Data Collection Rules (Azure Monitor Agent): recogida de Syslog/auditd en Linux y del canal Sysmon en Windows, con filtrado en origen para controlar volumen y coste.
- Runbook de despliegue extremo a extremo y control del perímetro económico (daily cap y alertas de presupuesto) antes de activar la ingesta. Objetivo de certificación: SC-200.

AdeoSOC — Cliente Android de respuesta del SOC · github.com/Adeodato-hub/AdeoSOC
App Android nativa (Kotlin + Jetpack Compose) que hace operable el SOC desde el bolsillo: vigilancia en segundo plano, notificaciones locales, triaje de alertas asistido por IA y respuesta activa de un toque, con convergencia IT/OT en un único panel.

- Respuesta activa en 1 toque: Bloquear IP (!firewall-drop) y Deshabilitar cuenta (!disable-account) vía la API nativa de Wazuh, con un usuario de mínimo privilegio (adeosoc_ar, rol acotado a active-response:command) y diálogo de confirmación; en activos OT, aviso reforzado antes de confirmar para no parar producción.
- Vigilancia en segundo plano (Foreground Service con reinicio tras reboot y exención de batería) y notificaciones locales para alertas Media/Alta/Crítica, sin duplicados.
- Enriquecimiento por IA no bloqueante desde el índice argos-ai-enrichment: narrativa en español (2-3 frases), gravedad y técnica MITRE generadas por el pipeline de ARGOS contra Ollama.
- Convergencia IT/OT en un único panel: filtro y etiqueta OT en Alertas, activos OT con detalle de exposición y telemetría, y tarjeta OT en vivo en Resumen.
- Seguridad: credenciales cifradas en el dispositivo (EncryptedSharedPreferences + Android Keystore AES-256), nunca hardcodeadas; APK de release firmada con hash verificado.

SOC Adeodato Dashboard — Monitor en tiempo real del vSOC ARGOS + AdeoSOC · github.com/Adeodato-hub/SOC-Adeodato-Dashboard
Panel de escritorio vitrina que unifica la vigilancia de seguridad de ARGOS (detección, correlación e inteligencia de amenazas) y AdeoSOC (contención automática y respuesta) en una sola vista operativa: alertas en vivo, severidad, casos con timeline PICERL, respuesta automática y técnicas MITRE ATT&CK.

- Sin exposición a Internet: escucha solo en loopback (127.0.0.1:8080), no abre ningún puerto a Internet ni a la red local; su única comunicación sale por red privada cifrada (Tailscale / WireGuard) hacia el propio ARGOS.
- KPIs en vivo, donut de severidad y feed de alertas filtrable por nivel (Todas / Críticas / Altas / Medias / Bajas), con recarga filtrada desde el backend.
- Casos de incidente con timeline PICERL y recomendaciones; respuesta automática ejecutada con su estado; técnicas MITRE ATT&CK correlacionadas, con las activas en casos abiertos resaltadas.
- Modo demo por botón (DEMO: ON/OFF) sin tocar la conexión real: ideal para presentaciones y vitrina.
- Python 3.9+ sin dependencias externas (solo librería estándar); credenciales fuera del repositorio (config.json ignorado por git); licencia MIT.

Proyecto ARGOS — Mini-SOC completo · github.com/Adeodato-hub/ARGOS

Diseño, despliegue y operación de un SOC funcional de extremo a extremo en laboratorio virtualizado, con SIEM, endpoints Linux y Windows monitorizados y máquina atacante. Documentación técnica de 50+ páginas.

- Wazuh como SIEM y Suricata como IDS/NIDS (ruleset ET Open), con trabajo de normalización y reducción de ruido de eventos — la parte realmente difícil de un despliegue IDS.
- Aproximadamente 30 reglas de detección propias mapeadas a MITRE ATT&CK: fuerza bruta SSH, abuso de sudo, creación de usuarios y accesos fuera de horario laboral.
- Cierre de un punto ciego de detección de persistencia (MITRE T1053.005, tareas programadas): diagnóstico de causa raíz —política de auditoría, no falta de reglas— y corrección mínima verificada extremo a extremo (Windows Security 4698 → Wazuh).
- Respuesta automatizada (Active Response): bloqueo por firewall y deshabilitación de cuentas comprometidas sin intervención humana, con alertado en tiempo real vía Telegram y WhatsApp.
- Pipeline de triaje con IA (Python): priorización de alertas mediante RAG (FAISS) y modelo local servido con Ollama.
- Gestión de incidentes reales del propio laboratorio, documentados con causa raíz y corrección — incluido un fallo silencioso del pipeline de ingesta en el que el agente reportaba estado correcto mientras dejaba de recibir logs.
- Análisis y mitigación de ataques DoS de Capa 7 (Slowloris / SlowHTTPTest): demostración en laboratorio, señales de detección y playbook de hardening, divulgado como material técnico.

AdeoShield — Aplicación Android de seguridad y control parental · github.com/Adeodato-hub/AdeoShield

Desarrollo íntegro y en solitario de una app Android nativa (Kotlin + Jetpack Compose) que filtra contenido mediante una VPN local que intercepta y resuelve el tráfico DNS por DNS-over-HTTPS, sin requerir root ni ADB.

- Arquitectura de servicios: VpnService para interceptación DNS, servicio de accesibilidad para proteger pantallas críticas de Ajustes y administrador de dispositivo contra la desinstalación.
- Autenticación del PIN parental mediante derivación de clave PBKDF2 (nunca en texto plano); APK de release firmado (keystore RSA 2048) y gestión segura de secretos fuera del control de versiones.
- Modelo de amenaza documentado, incluyendo las limitaciones estructurales de la plataforma Android.

EXPERIENCIA PROFESIONAL

Responsable de Turno — Sección de Chapa · Intarcon S.L. · 2011 – 2025

- Supervisión de la producción y de maquinaria de alta precisión (plegadoras, punzonadoras, corte por láser y robótica), asegurando los objetivos diarios de fabricación.
- Mantenimiento preventivo y correctivo de maquinaria CNC en red, reduciendo paradas de producción mediante revisión técnica continua de la programación ISO.
- Liderazgo de equipo de turno; enlace con oficina técnica y apoyo técnico directo en planta. Experiencia en la disciplina operativa de un entorno donde una parada tiene coste inmediato.

Operario Especialista CNC · Infrico S.L. / Torres Industrias Frigoríficas · 2003 – 2008

- Operación y programación de sistemas complejos: tren de distribución NIGHT TRAIN de Finn-Power y máquinas de corte por láser Finn-Power L6.
- Desarrollo de prototipos y piezas personalizadas mediante programación ISO de alta precisión.

Experiencia previa (1998 – 2000): carpintería industrial y soldadura MIG/MAG en estructuras metálicas.

FORMACIÓN

- Especialización en Nuevas Tecnologías: Inteligencia Artificial y Ciberseguridad (Red Team / Blue Team).
- Habilitación para la Docencia (en curso).
- Técnico Superior en Producción en Mecanizado, Conformado y Montaje Mecánico (Grado Superior).
- Técnico en Mecanizado (Grado Medio).

OTROS DATOS

- Idiomas: español (nativo); inglés técnico (lectura de documentación, rulesets y bibliografía de seguridad).
- Carnet de conducir y disponibilidad para desplazamiento.
- Portfolio técnico y documentación de proyectos disponibles en adeodato.es y github.com/Adeodato-hub.