Javier Artiga Garijo

CYBERSECURITY ANALYST

CONTACTO

javier@artiga.es

Zaragoza, España

MIS ENLACES

jartigag

javier-artiga-garijo

jartigag.blog

mnf.red/jartigag

Idiomas

Español — NATIVO/BILINGÜE

Inglés — FLUIDO

Presentación

Soy un ingeniero de telecomunicaciones (máster en big data) en su sexto año de vida laboral, muy interesado en la ciberseguridad, el análisis de datos, el desarrollo de software con buenas prácticas, en colaborar con gente motivada por trabajar en un objetivo común y en general en seguir progresando en mi carrera profesional en el mundo tecnológico, que considero que ofrece infinidad de oportunidades de crecer en muchos sentidos.

Entre septiembre de 2021 y enero de 2024 estuve en más de una decena de proyectos relacionados con la ciberseguridad para clientes del sector público español, principalmente. Mi tarea fundamental era el threat hunting, empleando múltiples soluciones del mercado (como EDRs, SIEMs, etc.) integradas con mis propias herramientas. Contribuí de manera decisiva en la iniciativa RNS del CCN-CERT. También trabajé en varios CSIRTs y he apoyado en respuesta a incidentes, consultoría de infraestructuras seguras, auditoría de redes y desarrollo de productos internos.

Antes trabajé en una spin-off de monitorización de redes desde enero de 2019 hasta septiembre de 2021, dentro de un proyecto internacional cuyo enfoque principal fue construir un SIEM por completo, con el stack ELK y herramientas que desarrollamos en equipo. Lo hice junto a un grupo fantástico del que aprendí un montón y al que pude aportar en igual medida.

Creo que es más fácil conocerme leyendo un poco los artículos que escribo en: jartigag.blog.

EXPERIENCIA/CARRERA

esPublico Sistemas

Cybersecurity Analyst

feb 2024 — HOY

Centro de Servicios Avanzados (CSA)

Cybersecurity Analyst

sept 2021 — ene 2024 (2 años y 5 meses)

- Análisis proactivo de amenazas de ciberseguridad (Threat Hunting).
- Coordinación con otros equipos y CSIRTs, incluyendo la iniciativa RNS de CCN-CERT.
- Gestión de equipos de trabajo y seguimiento con clientes.
- Adaptación de múltiples servicios de ciberseguridad a diversos tipos de clientes públicos (ministerios, comunidades autónomas, diputaciones, ayuntamientos) y del sector privado.
- Automatizaciones, integraciones con APIs.
- Amplia experiencia con varias herramientas de CCN-CERT.
- Respuesta temprana ante incidentes.
- Auditoría de redes y seguridad.
- Consultoría para el diseño de infraestructuras seguras.

EDRs (CrowdStrike, Cytomic) | Threat Intelligence (MISP) | SIEM & Log Management (Splunk, Graylog, IBM QRadar)

TECNOLOGÍAS Y HERRAMIENTAS

Python / Windows / Linux / Git / Bash / Centos / RedHat / Pytest

Naudit HPCN

Observability Analyst

ene 2019 — sept 2021 (2 años y 9 meses)

- Implementación propia de diversas soluciones para clientes finales, enfocadas principalmente en ciberseguridad. Por ejemplo:
    - SIEM con logs de distintos firewalls, servidores Windows y muchas otras fuentes.
    - API de alertas por email sobre queries a Elasticsearch o PostgreSQL.
    - Informes de monitorización periódicos.
- Seguimiento continuo con clientes internacionales, ayudando en la definición de sus necesidades y personalización de sus despliegues.
- Diseño de dashboards para monitorizar datos de red, sistemas y negocio.
- Análisis de tráfico en grandes redes (investigación de incidencias, optimización).
- Desarrollo de procesados en tiempo real sobre altos volúmenes de logs.
- Administración de sistemas Linux. Scripting, automatización, mantenimiento.

Dashboards (Grafana, Kibana) | Desarrollo (Python) | Bases de datos (Elasticsearch, PostgreSQL) | Sysadmin (Linux)

TECNOLOGÍAS Y HERRAMIENTAS

Python / PostgreSQL / Elasticsearch / Linux / Git / Grafana / Logstash / Kibana / AWK

ElevenPaths

Contributor

jun 2018 — sept 2018 (4 meses)

Desarrollo de un proyecto (dentro del "Reto Ciberseguridad y Big Data") para detectar dominios typosquatting, que luego presenté como mi TFG.

TECNOLOGÍAS Y HERRAMIENTAS

Python / Elasticsearch / Linux

Banda Municipal de Música de Soria

Clarinetista

sept 2006 — sept 2012 (6 años y 1 mes)

EDUCACIÓN/GRADOS

Grados

UNIR - La Universidad en Internet

Master

sept 2019 — jun 2020 (10 meses)

Máster Universitario en Análisis y Visualización de Datos Masivos

- Inteligencia Artificial, Machine Learning
- Estadística
- MongoDB
- Hadoop, Spark
- R, Python
- BI, Tableau, D3js, principios de visualización de datos

TECNOLOGÍAS Y HERRAMIENTAS

R / MongoDB / D3 / Spark / Hadoop / Tableau

Universidad Pública de Navarra

Engineering

sept 2015 — jun 2019 (3 años y 10 meses)

Ingeniería de Telecomunicaciones, mención en telemática

TECNOLOGÍAS Y HERRAMIENTAS

PHP / JAVA / JavaScript / Matlab / Cisco

Certificados

Entrenamiento práctico de DFIR y análisis forense (20 h)

Emitido por: Securízame

jul 2023 — HOY (8 meses)

Pack Análisis Forense y DFIR Windows y Linux - Online++ (28 h)

Emitido por: Securízame

jun 2023 — HOY (9 meses)

Curso de desarrollo de software basado en agile y XP (160 h)

Emitido por: Biko
dic 2021 — **HOY** (2 años y 3 meses)

B2 First

Emitido por: Cambridge Assessment English
may 2011 — **HOY** (12 años y 10 meses)

CCFH (Hunter)

Emitido por: CrowdStrike
ago 2022 — **ago 2025** (3 años y 1 mes)

CCFR (Responder)

Emitido por: CrowdStrike
ago 2022 — **ago 2025** (3 años y 1 mes)

Cytomic Technical Certification

Emitido por: WatchGuard Technologies
nov 2022 — **nov 2024** (2 años y 1 mes)

Proyectos

jartigag.blog

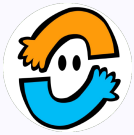
Blog personal y técnico.
https://jartigag.blog
ene 2019 — **HOY** (6 años)

Scavenger Security

CTF Player.
https://scavengersecurity.com/tags/jartigag
sep 2021 — **may 2022** (9 meses)

Caracterización de hosts por clustering en red empresarial

Clasificación de hosts según su actividad de red y detección de comportamientos sospechosos, usando clustering sobre logs de varios firewalls.
https://github.com/jartigag/tfm-clustering
may 2020 — **oct 2020** (6 meses)



TheyLendMe

App que facilita el préstamo de objetos entre individuos y grupos.
Aparición en prensa digital y en papel.

https://theylendme.github.io

oct 2018 — dic 2018 (3 meses)

Monitorización de dominios typosquatting

Sistema ELK para monitorizar dominios typosquatting con peticiones DNS, Whois y HTTP.

https://javier.artiga.es/paper-tfg-javier_artiga_garijo.pdf

jun 2018 — sep 2018 (4 meses)

PERO, ESPERA...
HAY INCLUSO MÁS EN MI PERFIL.

Esto es una versión corta de mi perfil, pero hay disponible una más larga en la que puedes ver datos más interesantes y relevantes.

Haz click aquí o escanea el código QR