Referencia 2022_02

TRABAJO FIN DE GRADO

TÍTULO

Threath hunting activo investigando IOCs de fuentes externas de forma automatizada.

DESCRIPCIÓN

Durante los últimos años se están incrementando los delitos relacionados con la ciberseguridad. La mayoría de estos delitos son ataques no dirigidos que aprovechan vulnerabilidades en los sistemas informáticos (incluidos los equipos de comunicaciones).

Un SOC (Security Operations Center) monitoriza las alertas de los distintos sistemas de protección de seguridad que tienen implementados los clientes, además de investigar amenazas y realizar las operaciones oportunas para mantener las infraestructuras tecnológicas protegidas ante ataques informáticos.

El objetivo de este TFG es automatizar algunas de esas tareas. Para ello se plantea desarrollar una orquestación en la plataforma del SOC que realice un threath hunting activo basado en recoger IOCs de Talos Intelligence y otros sitios diariamente y lanzar una investigación automática en Cisco Secure-X Threat Response.

Desde la empresa Orbe Seguridad, se propone la realización de este Trabajo Fin de Grado.

PERFIL DEL CANDIDATO

- ✓ Grado Ingeniería Informática.
- ✓ Se valorarán certificaciones de Cisco.
- ✓ Conocimientos de Redes, Networking, IP, Routing y Switching, Wireless, Comunicaciones unificadas y equipamiento asociado. Principalmente Cisco.
- ✓ Formación en seguridad informática (Firewall, IPS, Antimalware, Certificados).
- ✓ Nivel fluido de inglés. Se aportarán certificaciones oficiales.
- ✓ Voluntad de aprendizaje y formación continua. Capacidad de adaptación a los continuos cambios tecnológicos (virtualización, big data, IoT, cloud computing, industria 4.0)
- ✓ Excelente trato con el cliente, buenas habilidades comunicativas.
- ✓ Carné de conducir y disponibilidad de vehículo.

CONDICIONES LABORALES

- ✓ La persona seleccionada se incorporará al Departamento de Ciberseguridad, y dependerá directamente del Director de este Departamento, compaginando el TFG con un contrato de prácticas en empresa inicialmente, para posteriormente cubrir un puesto indefinido en dicho Departamento.
- ✓ Condiciones económicas iniciales en prácticas, dependiendo de la valía, disponibilidad y experiencia del candidato.

Los interesados deberán enviar por correo electrónico (dsanchez@orbe.es) el CV, expediente y la carta de presentación.

ORBE SEGURIDAD
Ctro. Empresarial Miralbueno, SS2
Ctra. Madrid Km. 315,700
50012 ZARAGOZA
T. 976 300 000 • F. 976 336 300
www.orbeseguridad.es