CASO 27 - Blindado de tráfico de red frente a tráfico anómalo

Consorcio: Ayesa Ibermatica; i3B

Tecnología: Ciberseguridad; Cuantica

Descripción general:

El presente caso de uso se enmarca en el ámbito de la ciberseguridad avanzada aplicada a Centros de Operaciones de Seguridad (Security Operations Center – SOC), orientados a la monitorización y análisis de tráfico y eventos de red procedentes de infraestructuras IT y OT conectadas.

La creciente digitalización de las organizaciones, junto con la adopción de servicios cloud, dispositivos IoT/IIoT, arquitecturas híbridas y sistemas distribuidos, ha incrementado significativamente la complejidad de las redes y la superficie de exposición frente a amenazas cibernéticas. Como consecuencia, los SOC deben gestionar volúmenes masivos de información generados por múltiples fuentes heterogéneas, incluyendo tráfico de red, eventos SIEM, logs de infraestructura, sistemas IDS/IPS y plataformas EDR/XDR.

En paralelo, el ecosistema de amenazas ha evolucionado hacia escenarios de mayor sofisticación técnica, caracterizados por ataques persistentes, automatización maliciosa, técnicas avanzadas de evasión y patrones de comportamiento cada vez más difíciles de detectar mediante mecanismos tradicionales basados exclusivamente en reglas estáticas o firmas conocidas.

En este contexto, la detección de anomalías sobre tráfico de red se ha convertido en una capacidad estratégica para identificar tanto amenazas externas como comportamientos anómalos internos, permitiendo mejorar la capacidad de respuesta y resiliencia de las infraestructuras digitales. Además de la detección temprana de ciberataques, el análisis avanzado del tráfico también permite identificar fallos operativos, configuraciones incorrectas o usos ineficientes de los recursos de red.

Programa: Red.es

Duración: 8 meses (01/05/2026 – 31/12/2026)

Presupuesto global proyecto: 80.000,00€

Presupuesto Grupo Ayesa: 80.000,00 €

Unión Europea
Fondo Europeo de Desarrollo Regional "Una manera de hacer Europa"
Plan de Recuperación, Transformación y Resiliencia

Financiado por la Unión Europea – Next Generation EU –

CASO 27 - Blindado de tráfico de red frente a tráfico anómalo

Consorcio: Ayesa Ibermatica; i3B

Tecnología: Ciberseguridad; Cuántica

Rol de Ayesa:

En este escenario, las tecnologías de Quantum Machine Learning (QML) representan una línea emergente de investigación orientada a explorar nuevas capacidades analíticas sobre datos de ciberseguridad.

El objetivo principal del proyecto es desarrollar un método avanzado de detección y análisis de anomalías sobre tráfico de red de redes IT/OT de empresas industriales mediante técnicas de Quantum Machine Learning, orientado a reforzar las capacidades operativas de un SOC frente a amenazas avanzadas y comportamientos sospechosos.

De forma específica, el caso de uso persigue:

- Detectar actividades anómalas e intrusiones sobre tráfico y eventos de red procedentes de entornos IT y OT.
- Mejorar la capacidad de identificación temprana de amenazas avanzadas y comportamientos no habituales.
- Reducir el volumen de falsos positivos generados por los sistemas tradicionales de monitorización.
- Evaluar la aplicabilidad de modelos QML sobre datasets de ciberseguridad altamente desbalanceados.