Facultad de Informática
Universidad Complutense de Madrid

ANUNCIO DE CONFERENCIA

1ª Conferencia: **Cyber Threat Intelligence - Contextualization and Applicability**

2ª Conferencia: **DevSecOps analysis using NLP and deep learning**

Bruce William Percílio Azevedo, Universidad de Brasilia, Brasil

Facultad de Informática

Sala de Grados – 19 de diciembre de 2025 - 19:00

Entrada libre hasta completar el aforo

Resumen 1ª Conferencia:

La presentación ofrece una visión integral y estructurada sobre Cyber Threat Intelligence, abordando su definición, relevancia estratégica y aplicación práctica en distintos contextos. Se explica cómo la inteligencia de amenazas permite a las organizaciones recopilar, analizar y difundir información sobre riesgos cibernéticos, fraudes y actividades maliciosas, apoyando la toma de decisiones informadas y la protección de activos críticos. Además, se detallan sus beneficios, fuentes de información (como dark web, feeds de inteligencia y salas de chat de hackers), el proceso completo de inteligencia (recolección, análisis, diseminación y acción), así como casos de uso en ciberseguridad, seguridad nacional, financiera y de infraestructuras. Finalmente, se analizan los principales desafíos, tendencias actuales —incluyendo el uso de inteligencia artificial— y se refuerza la importancia de adoptar programas de inteligencia de amenazas para fortalecer la resiliencia y la continuidad del negocio.

Resumen 2ª Conferencia:

La presentación expone una metodología aplicada para la categorización de malware en binarios PE32 mediante el uso de técnicas de Procesamiento del Lenguaje Natural (Word2vec) y Deep Learning, integrada dentro de un enfoque DevOps. Se describe el ciclo completo desde la planificación hasta el despliegue, destacando la construcción y normalización de un dataset de malware real, la extracción de funciones desde el encabezado PE y su transformación en vectores numéricos. A partir de estos datos, se entrena un modelo LSTM capaz de clasificar diferentes tipos de malware, alcanzando una precisión cercana al 91%, con validación práctica a través de una arquitectura automatizada basada en Docker, Python y APIs REST. Finalmente, se presentan los resultados obtenidos, las limitaciones del modelo y las líneas de trabajo futuro, como la ampliación del dataset y la evaluación de redes siamesas y otros modelos avanzados de aprendizaje profundo.

Sobre Bruce William:

Bruce William Percílio Azevedo es Ingeniero en Ciberseguridad, con más de doce años de experiencia profesional en grandes organizaciones y un sólido perfil académico e investigador. Es Licenciado en Ciencias de la Computación, Máster en Ingeniería de Telecomunicaciones, con especializaciones en Gestión de Seguridad y Estadística, y actualmente es Doctorando en Ingeniería Matemática, Estadística e Investigación Operativa en la Universidad Politécnica de Madrid. Ha desempeñado roles estratégicos en empresas como Itaú Unibanco, Grupo Boticário, Riachuelo, Cognyte y Avantsec, liderando el diseño, implementación y operación de arquitecturas avanzadas de seguridad (SIEM, SOAR, WAF, CNAPP, EDR/XDR, IAM, DLP, entre otras), con fuerte enfoque en cloud, DevSecOps y cumplimiento normativo internacional. En el ámbito académico actúa como investigador en la Universidad de Brasilia en inteligencia de amenazas y análisis de malware mediante inteligencia artificial y aprendizaje profundo, integrando investigación aplicada, innovación tecnológica y experiencia industrial.