IA Cibersecurity Lab

Valencia

15 Octubre 2024

DOSSIER DE FORMACIÓN

/Rooted

Día 15 de Octubre

Formaciones

ADEIT Fundación Universidad-Empresa de la Universidad de Valencia.

Día 16 de Octubre

Ponencias presentadas por speakers internacionales y expertos técnicos.

Ciudad de las Artes y las Ciencias Valencia

Presentación

- **Misión**: Queremos compartir conocimientos, atraer diferentes culturas, exponer el talento local y marcar la diferencia.
- **Visión**: Ser responsables haciendo algo diferente, compartiendo cultura y construyendo una red de conocimiento. Ser un evento honesto, confiable, beneficioso y establecer alianzas y colaboraciones con socios, clientes y competidores.
- **Nuestra cultura ganadora y nuestros valores en vivo:** Colaboración, diversidad, talento por todas partes, pasión, calidad y enfoque en los clientes (cada persona que asiste a nuestros eventos).

Profesor: Pablo González

Máster Universitario en Seguridad Informática por la Universidad Internacional de La Rioja. Ingeniero en Informática por la Universidad Rey Juan Carlos. Ingeniero Técnico en Informática de Sistemas en la Universidad Rey Juan Carlos. Premio al mejor expediente de su promoción en la Universidad Rey Juan Carlos y Premio Extraordinario Fin de Carrera en Ingeniería Técnica en Informática de Sistemas. MVP Microsoft Security desde 2017.

Trabaja en Telefónica como Responsable del Departamento de Ideas Locas del área CDO. Es docente y Director en el Máster de Seguridad de Tecnologías de la Información y de las Comunicaciones en la Universidad Europea de Madrid. Además, es docente en otros másteres de seguridad de la información. Trabajó en Informática64 durante 4 años en Formación, Consultoría y Auditoría.

Tiene diversas publicaciones en el ámbito de la Seguridad de la Información en la editorial 0xword

Pablo ha impartido formación en Rooted CON 2013-2019. También ha sido docente en los Labs de No cON Name 2013 y 2014 con Metasploit para Pentesters. Ha sido ponente en Rooted CON 2013, 2014, 2016, 2018 y 2019, No cON Name, Navaja Negra y otros congresos como Hackron, Sh3llCon, Cybercamp o Rooted Valencia, entre otros. Ponente en congresos internacionales como la Black Hat Europe Arsenal 2017, 2018 y 2019, BlackHat USA 2020, BlackHat Europe 2021 y 2022, 8dot8 en 2014,2018 y 2019, EkoParty 2018, LeHack 2019, Bsides Colombia en 2016 o el IEEE SBS Gold en 2012. Fundador de hackersClub Academy

Profesor: Fran Ramírez

Es Ingeniero/Grado en Informática de Sistemas, Técnico Superior en Electrónica Digital, Máster Universitario en Seguridad Informática y Máster Universitario en IA/Ciencia de Datos. Más de 15 años de experiencia como Administrador de
Sistemas realizando múltiples proyectos internacionales sobre todo en Inglaterra, EEUU y Canadá. Desde el año 2017, trabajo
como Investigador de Ciberseguridad en el equipo de Ideas Locas CDO, realizando proyectos relacionados con Ciberseguridad y Machine Learning. Ponente en eventos nacionales (RootedCon, Mobile World Congress, etc) y otros
internacionales (Black Hat Europe Arsenal en Londres, Hacktiviy en Hungría, LeHack en París, etc). Fundador de www.cyberhades.com (cybercaronte) sobre Seguridad Informática entre otros temas geek. Co-autor del libro "MicroHistorias: anécdotas y curiosidades de la Informática", "Machine Learning aplicado a la Ciberseguridad" y "Docker:SecDevOps" ambos de la editorial 0xWord

Objetivos

En este IA Cibersecurity Lab se presenta el panorama actual de amenazas cibernéticas y cómo la Inteligencia Artificial será un ayudante en la detección, pero también una amenaza y aliado de los atacantes. Es vital, hoy día, tener skills en Deep Learning, Machine Learning y conocer cómo es la base de la auditoría y pentesting de sistemas con IA.
Es fundamental que los profesionales de la ciberseguridad tengan una comprensión profunda de cómo la IA puede utilizarse por atacantes como por defensores en el día a día. Esto permite contrarrestar los TTPs utilizados por los adversarios.

El enfoque del taller es eminentemente práctico, pudiendo realizar pruebas de concepto sobre los conceptos estudiados. El taller comienza con una serie de fundamentos y conceptos de la IA aplicados a la Ciberseguridad. Se trabaja el concepto de Deep Learning y Machine Learning y se aplican casos prácticos basados en mejorar la detección de sistemas. Además, se hablará de la seguridad de los modelos, lo cual es sumamente importante hoy día, ya que cualquier empresa utiliza sistemas con IA.

Puedes consultar el índice detallado del curso y entrar en el mundo de la IA y la ciberseguridad.

A quién va dirigido

Profesionales del sector de la Seguridad de la Información
Estudiantes
Administradores de sistemas y redes
Desarrolladores que quieran mejorar su perfil
Cuerpos y Fuerzas de Seguridad
Docentes

Requisitos: Conocimientos

Conocimientos básicos en redes TCP/IP
Conocimientos básicos en desarrollo con Python
Conocimientos básicos en Deep Learning y Machine Learning (Deseable, pero opcional)

Requisitos: Técnicos

Equipos con memoria RAM de 16 GB
Portátil propio (no hace falta GPU)

Guía de Contenidos:

1. Fundamentos y herramientas de la IA aplicada a la Ciberseguridad
    1. Conceptos generales en IA y en Ciberseguridad
    2. Casos de uso de IA en Ciberseguridad
2. Escenarios de ciberseguridad
    1. Amenazas y casos actuales
    2. Escenarios ejemplificados de ciberseguridad orientado a entornos ofensivos y defensivos
3. Machine Learning y Ciberseguridad
    1. Concepto de Machine Learning
    2. Tipo de Aprendizaje, supervisado, no supervisado y reforzado.
    3. Detección de anomalías y protección contra amenazas
    4. Respuesta a incidentes
    5. Análisis práctico de Malware (Python)
    6. Análisis práctico de Logs (Python)
4. Deep Learning, conceptos y herramientas
    1. Redes Neuronales
    2. Deep Learning
    3. Herramientas de DeepLearning para IA (Tensorflow, Keras, etc)
    4. Detección práctica de amenazas en el correo usando DeepLearning (Python)

Guía de Contenidos II

5. Seguridad en los modelos de IA
    1. Auditoría de modelos de IA
    2. DeepFakes
    3. Cómo auditar modelos de IA
    4. Tipos de ataques a modelos
    5. FGSM Ataques
    6. OMLASP

FAQ

1. ¿Dónde se celebra la formación?
   - Las formaciones se celebran en en el edificio del ADEIT Fundación Universidad – Empresa de la Universidad de Valencia.
   - Plaza Virgen de la Paz, 3 46001 Valencia
   - ¿Qué diferencia hay entre BootCamp y RootedLab?
   - Diferenciamos los trainings por horas de formación. Un **RootedLab tiene 8 horas** de formación, mientras que un **BootCamp tiene unas 24h**.
2. ¿Qué horario tiene la formación?
   - La formación comienza a las 9:00h de la mañana, pero procura estar un poco antes para poder acreditarte y tener tu portátil preparado. El primer día recomendamos estar a las 8:30h.
   - Las formaciones suelen acabar entre las 18:00h y 19:00h.
3. ¿Cómo puedo registrarme?
   - Para el registro, ve directamente al Rooted Manager: https://reg.rootedcon.com. Ahí, una vez registrado podrás seleccionar la formación y pagar directamente. Una vez se imparta la formación podrás solicitar la factura siguiendo los pasos indicados.
4. ¿Puedo pagar con transferencia bancaria?
   - Si, desde el propio Rooted Manager podrás gestionar el pago mediante transferencia bancaria.
5. ¿El training incluye comida?
   - Los trainings **no incluyen comida**. Pero hay varias opciones en la zona, y el profesor os dará más información.

/Rooted

Contacto:
info@rootedcon.com