RESUMEN DE LA TESIS DOCTORAL

DECISION SUPPORT ELEMENTS AND ENABLING TECHNIQUES TO ACHIEVE A CYBER DEFENCE SITUATIONAL AWARENESS CAPABILITY

La presente tesis doctoral realiza un análisis en detalle de los elementos de decisión necesarios para mejorar la comprensión de la situación en ciberdefensa con especial énfasis en la percepción y comprensión del analista de un centro de operaciones de ciberseguridad (SOC). Se proponen dos arquitecturas diferentes basadas en el análisis forense de flujos de datos (NF3). La primera arquitectura emplea técnicas de Ensemble Machine Learning mientras que la segunda es una variante de Machine Learning de mayor complejidad algorítmica (λ-NF3) que ofrece un marco de defensa de mayor robustez frente a ataques adversarios. Ambas propuestas buscan automatizar de forma efectiva la detección de malware y su posterior gestión de incidentes mostrando unos resultados satisfactorios en aproximar lo que se ha denominado un SOC de próxima generación y de computación cognitiva (NGC2SOC). La supervisión y monitorización de eventos para la protección de las redes informáticas de una organización debe ir acompañada de técnicas de visualización. En este caso, la tesis aborda la generación de representaciones tri-dimensionales basadas en métricas orientadas a la misión y procedimientos que usan un sistema experto basado en lógica difusa. Precisamente, el estado del arte muestra serias deficiencias a la hora de implementar soluciones de ciberdefensa que reflejen la relevancia de la misión, los recursos y cometidos de una organización para una decisión mejor informada. El trabajo de investigación proporciona finalmente dos áreas claves para mejorar la toma de decisiones en ciberdefensa: un marco sólido y completo de verificación y validación para evaluar parámetros de soluciones y la elaboración de un conjunto de datos sintéticos que referencian unívocamente las fases de un ciberataque con los estándares Cyber Kill Chain y MITRE ATT & CK.