Proyectos coordinados de investigación para mejorar las técnicas de detección de anomalías en la seguridad informática

Rodney Busquim e Silva y Andrea Rahandini

La detección de anomalías en el funcionamiento de los sistemas informáticos que controlan funciones críticas de seguridad tecnológica y de seguridad física requiere amplios conocimientos especializados, y las medidas necesarias deben probarse, analizarse y ajustarse para que sean eficaces.

"La detección de anomalías desempeña un papel importante en la evaluación temprana de posibles amenazas contra los sistemas computarizados de instalaciones nucleares y radiológicas —afirma Scott Purvis, Jefe de la Sección de Gestión de la Información de la División de Seguridad Física Nuclear del OIEA—. Las técnicas de detección de anomalías suelen utilizan aplicaciones de la inteligencia artificial, como el aprendizaje automático, métodos basados en la estadística o los conocimientos y demás tecnologías". Estas tecnologías se utilizan para detectar desviaciones de las comunicaciones de red previstas o mediciones de procesos que pueden ser el primer indicio de que un intruso saltó las defensas de un sistema informático, y pueden detectar ciberataques en tiempo real.

Además, son importantes porque un agente con fines dolosos altamente capacitado puede introducir programas maliciosos que pongan en riesgo las funciones de seguridad tecnológica o de seguridad física de un sistema digital a la vez que falsifica los datos de sensores y los indicadores que se envían a un operador. Esto significa que el operador puede no saber que se está produciendo una actividad dolosa y, en un principio, reaccionará teniendo en consideración lo que se muestra en la sala de control, por lo que posiblemente tomaría una medida incorrecta. Solo mediante la detección automatizada de las más mínimas anomalías en un ciberataque de este tipo podría informarse correctamente a un operador.

Para abordar esta importante esfera de trabajo y otros desafíos relacionados con la seguridad informática, el OIEA puso en marcha un proyecto coordinado de investigación (PCI) específico en 2016.

La investigación y el desarrollo por medio de los PCI son una parte fundamental de las actividades del OIEA en materia de seguridad informática para la seguridad física nuclear. Estos proyectos producen un conjunto de investigaciones y conclusiones prácticas que complementan las iniciativas en curso del OIEA para fortalecer las capacidades de los países en materia de prevención, detección, respuesta y recuperación tras incidentes de seguridad informática que puedan afectar directa o indirectamente la seguridad nuclear tecnológica y física de instalaciones nucleares y radiológicas.

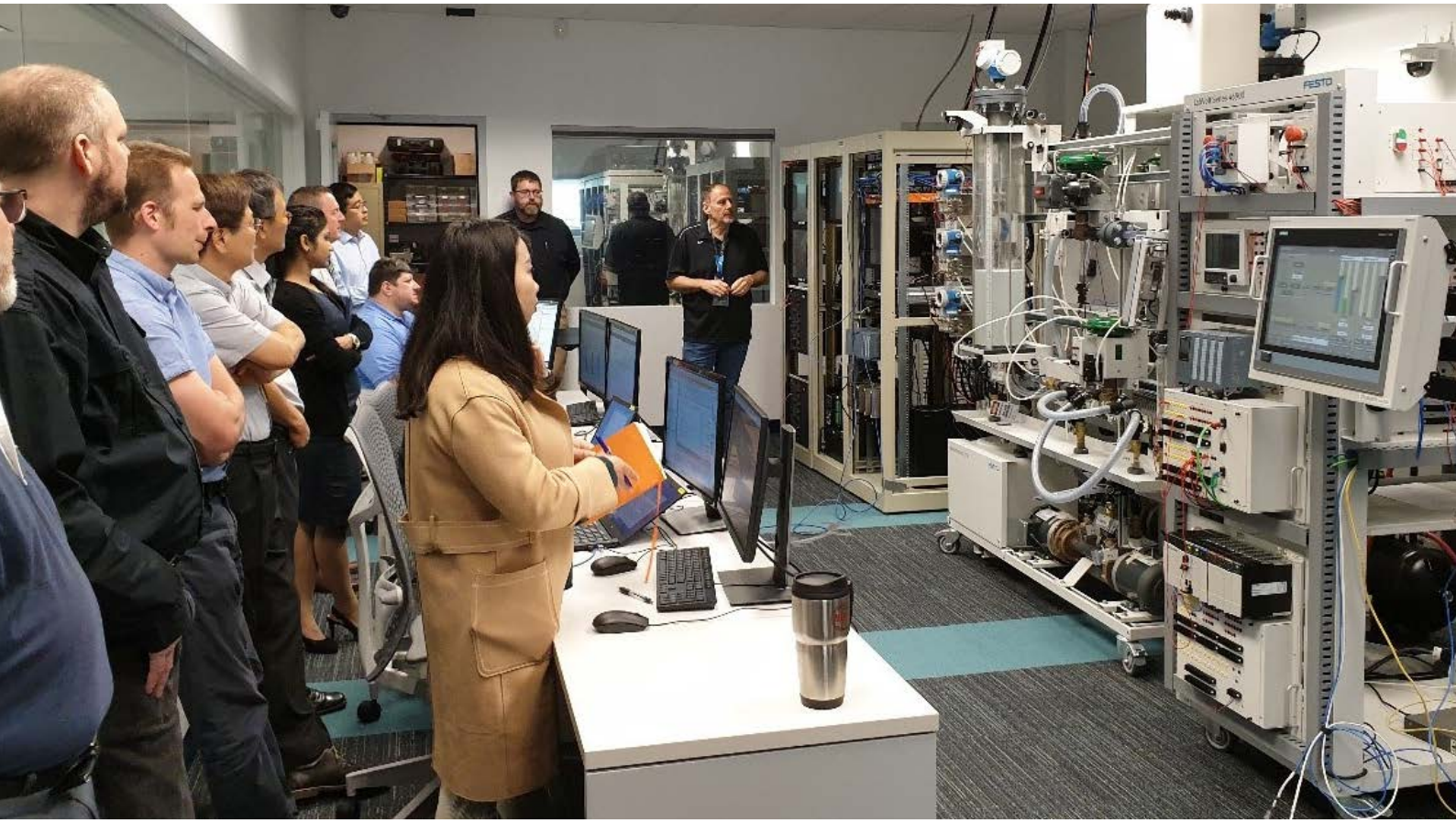
"Los adversarios son cada vez más sofisticados, y sus capacidades cibernéticas suponen desafíos cada vez mayores a la hora de desarrollar herramientas de detección de anomalías —dice el Sr. Purvis—. Para desarrollar técnicas de detección de anomalías es necesario acceder a datos de red y procesos de planta realistas y físicamente coherentes a fin de entrenar y probar los modelos de detección".

El escenario de ciberataques para crear capacidad

El PCI de 2016, titulado "Mejora del análisis de incidentes de seguridad informática en instalaciones nucleares", arrojó resultados importantes, por ejemplo, permitió seguir investigando herramientas y técnicas específicas que antes no se podían investigar sin el riesgo de exponer información sensible procedente de instalaciones nucleares y radiológicas.

El grupo del PCI, integrado por investigadores de 13 países y 17 organizaciones, creó una instalación ficticia, denominada Central Nuclear Asherah, y la Universidad de São Paulo creó un simulador (ANS) a partir de dicha instalación. Desarrollaron en conjunto escenarios realistas de ciberataque dentro de una instalación nuclear. Estos escenarios de ciberataque han permitido explorar y evaluar la eficacia de las medidas de seguridad informática y también las posibles consecuencias operativas de que un recurso digital se vea comprometido. Asimismo, el grupo trabajó en la obtención y el análisis de datos y en la elaboración y la puesta a prueba de técnicas para detectar ciberataques.

"Hemos desarrollado y utilizado el simulador ANS para generar un repositorio de datos a efectos de entrenar nuestros modelos de aprendizaje automático y evaluar su eficacia. El PCI del OIEA reunió a asociados internacionales para llevar a cabo investigaciones y creó nuevos conocimientos en este ámbito —expresa Ricardo Marques, profesor de la Escuela Politécnica de la Universidad de São Paulo (Brasil)—. La cooperación entre los participantes del PCI fue esencial para validar la labor realizada".



La Universidad de São Paulo desarrolló un simulador basado en una instalación ficticia denominada Central Nuclear Asherah.
(Fotografía: OIEA)

Los resultados prácticos del PCI también se han utilizado para la enseñanza y la capacitación continuas de un gran número de estudiantes de posgrado e investigadores de diversas disciplinas. Esto ha contribuido aún más a la investigación y los esfuerzos realizados con el objetivo de mejorar constantemente la seguridad informática en instalaciones nucleares y radiológicas.

"Parte de mi investigación como estudiante de doctorado se ha llevado a cabo utilizando el ANS y su interfaz persona-máquina, una interfaz que permite al usuario observar el simulador y comunicarse con él y que fue desarrollada en el marco del PCI del OIEA —cuenta Si Wen, estudiante de doctorado de la Universidad de Tsinghua (China)—. Llevé a cabo una investigación sobre técnicas de detección de anomalías, y el ANS fue clave para generar los datos necesarios para entrenar y evaluar un algoritmo de detección creado para centrales nucleares. Sin la colaboración entre todos los institutos participantes y las herramientas desarrolladas por el grupo del PCI, sería imposible llevar adelante mi investigación doctoral sobre la seguridad informática de los sistemas digitales de las centrales nucleares", agrega.

Los resultados prácticos del PCI —el ANS, las herramientas y las orientaciones— están a disposición de los institutos de investigación interesados de todo el mundo. Pueden conseguirse presentando al OIEA, a través de la autoridad nacional competente, un formulario de solicitud, que se encuentra disponible en el Portal de Información sobre Seguridad Física Nuclear (NUSEC) del OIEA.

Más recientemente, en 2023, el OIEA puso en marcha un nuevo PCI sobre la mejora de la seguridad informática para los sistemas de detección de radiaciones a fin de investigar metodologías y técnicas que mejoren la seguridad informática de los equipos de detección de radiación. Los proyectos de investigación previstos en el marco del nuevo PCI, con 12 organizaciones participantes (entre ellas, laboratorios nacionales, universidades e institutos nacionales de investigación) de 11 países, abordarán el uso de tecnologías digitales emergentes, como la computación en la nube, y seguirán estudiando y desarrollando técnicas innovadoras de detección de anomalías.