Machine learning Supported Cibersecurity

Investigación y aplicación de las tecnologías más novedosas de analítica de grandes volúmenes de datos en tiempo real, de aprendizaje automático y las técnicas de analítica visual, combinadas con profundos conocimientos de seguridad, para su aplicación en la detección de amenazas e incidentes.

Situación actual

La ciberseguridad es una de las tecnologías capacitadoras clave para el desarrollo de la transformación digital que está dando ahora a nivel mundial en todos los negocios, y como tal, se trata de una tecnología transversal con aplicación en cualquier negocio conectado.
Según el Informe Anual de Seguridad de Cisco de 20161:

- Solo el 45% de las empresas confían en sus sistemas de seguridad.
- Más del 85% de las empresas analizadas por estaban infectadas de alguna forma.
- El número de organizaciones que consideran actualizada su infraestructura de seguridad ha caído del 64% al 59%,
- El 92% de los dispositivos de Internet analizados (IoT) albergaban vulnerabilidades.
- El número de pymes que usan soluciones de seguridad ha caído del 59% al 48%.
- Sólo el 24% de los ataques que recibe una compañía son detectados a tiempo.
- El tiempo medio de detección desde que se descubre un archivo anómalo hasta que se detecta la amenaza es de entre 100 y 200 días.
- La vía de acceso principal de los ciberdelincuentes son los empleados. Ya sea a través de un mal uso de su correo o su navegador, la falta de conciencia y desconocimiento los convierte en una continua fuente de riesgos.
- El 92% del 'malware' conocido utiliza DNS como soporte clave, aprovechándose de la escasa atención que le prestan los equipos de seguridad y la falta de comunicación entre los departamentos de la empresa.

De este escenario se desprenden los siguientes necesidades y retos a los que se tratará de dar respuesta en el siguiente proyecto:

- ✓ Es necesario disponer de soluciones de bajo coste que "socialicen" el acceso a una solución de seguridad.
- ✓ Las soluciones deben actualizarse dinámicamente a medida que se detectan nuevas amenazas.
- ✓ Las soluciones tienen que minimizar el tiempo de exposición a ataques a los que está expuesta una organización, mediante la generación de alertas tempranas.
- ✓ Las soluciones deben ser accesibles para cualquier perfil, sin una gran especialización, dada la dificultad de encontrar profesionales formados.
- ✓ La infraestructura conectada de las empresas es cada vez más extensa y compleja, dando lugar a un incremento del riesgo, ya que la seguridad depende siempre eslabón más débil de la cadena. Por tanto, deben buscarse soluciones específicas a cada medio, a cada problema y a cada sector, pero a poder ser de un modo integrado y siguiendo los principios de la estrategia de defensa en profundidad, sin que cada una de ellas suponga una nueva herramienta.

Ventana de exposición a incidentes de ciberseguridad

Objetivos

- **Generación de una base de datos colaborativa y compartida de Indicadores de Compromiso (IOC), con IOCs verticales para cada sector, cuyo fin es paliar los efectos de las principales amenazas en la red (conocidas e incluso desconocidas hasta la fecha), mediante la aplicación de tecnologías de machine learning que permitan identificar nuevos comportamientos anómalos desconocidos hasta la fecha, así como su sencilla interpretación por personal no experto mediante técnicas de visual analytics.**

- **Cambiar la tendencia en cuanto a las técnicas de detección de amenazas, pasar de técnicas y procedimientos reactivos (se daba un ataque, se analizaban logs, y se identificaba la vulnerabilidad empleada por el atacante) a unos más proactivos, a través de la identificación de patrones de comportamiento habituales, de modo que cuando un comportamiento difiera del habitual resulte sospechoso, se pueda facilitar la detección incluso en los casos de ataques zero-day o desconocidos.**

ACTUACIÓN COFINANCIADA POR EL GOBIERNO VASCO Y LA UNION EUROPEA A TRAVÉS DEL FONDO EUROPEO DE DESARROLLO REGIONAL 2014-2020 (FEDER)

Europar Batasuna Unión Europea
Fondo Europeo de Desarrollo Regional (FEDER) "Una manera de hacer Europa"
Eskualde Garapenerako Europar Funtsa (EGEF) "Europa egiteko modu bat"
EUSKO JAURLARITZA GOBIERNO VASCO

Nº Exp: ZE-2017/00030