David Fernández Domingo

Practica machine learning

Índice

1. Descripción del caso de uso

1.1 ¿Cuál es el problema?

En la empresa LabTech Solutions usan un sistema de clasificación para productos farmacéuticos, estos productos son detectados por una maquina y software que lee un código de etiquetado del producto y lo clasifica según su tipología. Por parte del departamento externo de ciberseguridad, se ha detectado en la máquina de clasificación que ha habido unos accesos a la maquina sin autorizar (intrusión remota), dicha maquina posee un software remoto para su configuración y ha habido una brecha de seguridad, es sabido por parte de los trabajadores que la conexión se puede realizar desde cualquier equipo que este en la misma subred y cuyas credenciales solo la conocen el personal autorizado.

Las dimensiones de esta problemática podrían afectar a toda la cadena de clasificación para estos productos pues podrían haber sido manipulados sin consentimiento de las partes autorizadas creando unos costes directos de millones de euros, en cuanto a evaluación de los riesgos que supone una brecha de tal magnitud y la implementación de un nuevo protocolo de seguridad, formación del personal y un nuevo sistema para el acceso a la máquina.

1.2 ¿Cómo se está afrontando ahora?

- Se está investigando la procedencia de la intrusión, se han encontrado conexiones externas que han conseguido acceder a la subred
- Se están actualizando servicios y aplicando parches en equipos y sistemas que se han detectado que hubo error en las actualizaciones automáticas
- Aislamiento de máquinas comprometidas
- Se han desconectado aquellas maquinas que se han visto comprometidas a dicha intrusión y se está realizando un análisis forense
- Se ha notificado a todo el personal que haga copia de seguridad de sus datos, así como cambio de sus contraseñas pues no se descarta que haya podido haber alguna fuga de datos

1.3 Acciones para solucionar el problema

Actualización de aquellos servicios que no estaban actualizados y han podido ser comprometidos

Mejora del equipamiento para la prevención (monitoreo, equipos IDS) y detección de intrusiones remotas, asi como la mitigación de posibles nuevos ataques, instalación de honeypots

Formacion de seguridad en la empresa sobre cómo actuar en casos de phishing, spam, redirecciones fraudulentas y capacitación del personal sobre los nuevos cambios a implementar para el acceso remoto de la maquina

1.4 KPIs – Indicadores de negocio

- **Tasa de Identificación Exitosa (TIE)**: Porcentaje de ataques correctamente identificados y clasificados por la herramienta en comparación con el total de ataques analizados.
- Fórmula: (Ataques Identificados Correctamente / Total de Ataques Analizados) * 100

- **Tiempo Promedio de Respuesta (TTR)**: Tiempo medio que tarda la herramienta en identificar y clasificar un ataque desde el momento de la detección inicial.
- Fórmula: Suma de tiempos de respuesta para cada ataque / Número total de ataques identificados

- **Tasa de Falsos Positivos**: Porcentaje de casos en los que la herramienta identifica incorrectamente un ataque (falso positivo) en comparación con el total de detecciones.
- Fórmula: (Falsos Positivos / Total de Detecciones) * 100

- **Cobertura Geográfica**: Áreas geográficas cubiertas por la herramienta en términos de identificación de patrones de ataques.

- **Porcentaje de Amenazas Prevenidas**: Porcentaje de amenazas identificadas por la herramienta antes de que causaran daño o comprometieran la seguridad.
- Fórmula: (Amenazas Prevenidas / Total de Amenazas Identificadas) * 100

- **Tendencias de Ciberdelincuencia Identificadas**: Identificación de nuevas tendencias o evoluciones en las tácticas de ciberdelincuentes a lo largo del tiempo.

- **Porcentaje de intentos de intrusión**

- Se ha visto que en aquellas máquinas que había servicios sin actualizar se ha incrementado el porcentaje de intentos sin ser detectados

- **Niveles de accesos a los datos y equipos**

- Se ha hecho una recopilación y análisis de información sobre privilegios de acceso a la maquina y acceso a aplicaciones y datos por parte de los empleados para resaltar cualquier problema de seguridad interna, así como cambios necesarios en los controles de acceso remoto de los usuarios.

- **Número de falsos positivos y negativos**

- Las alertas determinan que en un porcentaje del 3% fueron falsos positivos

1.5 ¿Cuáles son los mínimos que se esperan de este caso de uso?

Incremento de la detección de intrusiones en un 60% desde la implantación de un nuevo sistema

1.6 Validación: ¿Qué criterio se va a usar para decidir si la solución es aceptable?

Se hará uso de un modelo predictivo para el control de los tiempos de acceso y de las identidades de quienes pueden acceder según sus horarios

Se hará uso de un modelo de machine learning el cual aprenderá de todos aquellos accesos verificando y acceso biométrico del personal autorizado para tener un control

La mejora en la interpretación de los datos y el monitoreo

1.7 Experimentación: ¿Cómo vamos a corroborar el funcionamiento?

Conforme el modelo vaya aprendiendo sobre los accesos del personal autorizado, que asegure que la disponibilidad del trabajador coincide con que haya accedido al sistema y se haya validado. Se realizará un monitoreo y revisión semanal para comprobar si se cumple.

1.8 Productivización: ¿Qué salida debe tener la solución que se desarrolle?

Se capacitará al departamento de ciberseguridad que monitorea los equipos para la utilización del software que controla todos los datos de accesos biométricos y de validación del personal en los equipos

A su vez se hará una formación en prevención y respuesta a incidentes para toda la empresa

2. Equipo de trabajo

2.1 Identificación de personas colaboradoras

Colaborará el jefe de sistemas del departamento IT de la empresa LabTech Solutions para procurar la correcta funcionabilidad de dicho modelo y evitar falsos positivos, también tendrá acceso al software de monitorización y datos de acceso y validación del personal autorizado

Los implicados de la monitorización en el departamento externo de la empresa de ciberseguridad que da soporte a Labtech Solutions

3. Detalle del caso de uso

3.1 Detalle funcional

Conocimiento de negocio

Evaluar riesgos e identificar problemas: permite al auditor anticipar posibles riesgos y desafíos que puedan afectar los estados financieros o el proceso de auditoría.

Planear y desarrollar la auditoría de manera efectiva y eficiente: el auditor puede diseñar procedimientos de auditoría adecuados y enfocarse en áreas críticas.

Detección de intrusiones con SAS y Python

GitHub - dinismf/kdd_intrusion_detection: Network Intrusion classification using Neural Networks in Python and SAS Enterprise Miner

3.2 Identificación de orígenes de datos

- Datos biométricos para el acceso a los laboratorios por personal autorizado
- Datos de cuentas de usuarios

nombre	apellidos	perfil	dni	ultimo_ login

- Datos de los equipos, sistemas y subredes

ip	hostname	sistema	subred

- Datos sobre que maquinas se involucran en las medidas de seguridad
- Datos sobre los diferentes departamentos o equipos que forman la empresa
- Datos intentos de intrusión

Ip_posible_atacante	pais_origen	fecha	sistema	nivel_peligro

4. Desarrollo del caso de uso

4.1 Puntos intermedios o seguimiento

Con el software del control de accesos recolecta datos cuando un trabajador entra o marcha de un laboratorio

Con el datasheet y los modelos predictivos obtenemos cuando se puede puede producir un intento de intrusión y bloquearlo

Software Vectra AI se especializa en la detección y respuesta a amenazas cibernéticas, haciendo uso de machine learning para analizar el comportamiento de la red y detectar actividades sospechosas.

4.2 Aporte esperado por Big Data

- Sistemas de Detección de Intrusiones (IDS): Los IDS son aplicaciones que monitorean redes de computadoras o hosts en busca de actividad sospechosa o incumplimiento de reglas establecidas por las organizaciones.
- Hay dos enfoques principales para la detección de intrusiones:

- Basado en reglas y heurísticas: Detecta ataques conocidos, como intentos de fuerza bruta en aplicaciones web. Sin embargo, puede tener una alta tasa de falsos negativos para nuevos tipos de ataques.

- Basado en anomalías: Perfila el comportamiento normal del sistema o red y detecta comportamientos inusuales.

- Las aplicaciones de detección de anomalías en ciberseguridad incluyen:
- Detección de malware en redes que pueden ser el origen de ataques de denegación de servicio o ransomware.

- Detección de fraudes en transacciones financieras.

- Detección de ataques a aplicaciones web, como inyecciones SQL.

- El Big Data permite modelar previsiones futuras y detectar posibles ataques casi en tiempo real.

- Predicciones en tiempo real: Identificar ciberataques mientras ocurren.

- Control de acceso: Saber a qué clientes o usuarios se les proporciona acceso a información.

- Sistemas SIEM (Security Information and Event Management): Monitorear sistemas y correlacionar eventos de seguridad.

- Análisis en tiempo real: Los ataques ocurren con mayor frecuencia y rapidez, y surgen nuevas amenazas constantemente.

- Algoritmos de Aprendizaje Automático: Ayudan a detectar intrusiones tempranamente y tomar decisiones informadas.