Curso de Especialización de Ciberseguridad en Entornos de Tecnología de la Información (CETI)

Puesta en Producción Segura

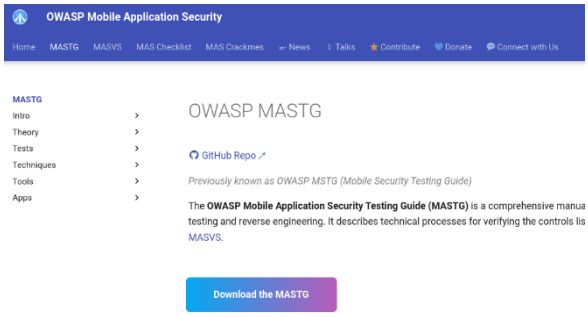
UD04. Defensas anti-ingeniería inversa y soluciones CASB.
Tarea Online.

JUAN ANTONIO GARCIA MUELAS

INDICE

1.- Descripción de la tarea.

Caso práctico



MASTG (Captura de pantalla)

Julián ha estado trabajando en un proyecto de una aplicación móvil junto con una solución CASB que quiere salir al mercado y ser revolucionaria.

Para comprobar que la aplicación es segura se ha seguido la última versión de la Guía de Pruebas de Seguridad de Aplicaciones Móviles (MASTG) desarrollada por OWASP.

Julián entiende que el Estándar de Verificación de Seguridad de Aplicaciones Móviles (MASVS) proporciona un marco claro y detallado que aborda los requisitos de seguridad esenciales para el desarrollo y la evaluación de aplicaciones móviles. Por otro lado, la Guía de Pruebas de Seguridad de Aplicaciones Móviles (MASTG) se alinea estrechamente con los requisitos establecidos por la MASVS, ofreciendo un conjunto adicional de directrices específicas para realizar pruebas de seguridad efectivas en aplicaciones móviles. La combinación de ambas herramientas, MASVS y MASTG, proporciona un enfoque integral para evaluar y mejorar la seguridad en aplicaciones móviles, permitiendo a los profesionales adaptar sus estrategias según el contexto específico.

Uno de los puntos que más se han trabajado durante el proyecto de la solución CASB es ser diferenciadores y poder corregir los problemas de adopción que han tenido las soluciones de MDM (Mobile Device Management). Saben que las soluciones para móviles tienen que ser capaces de lidiar con varios problemas como la privacidad, BYOD (*Bring Your Own Device*), etc.

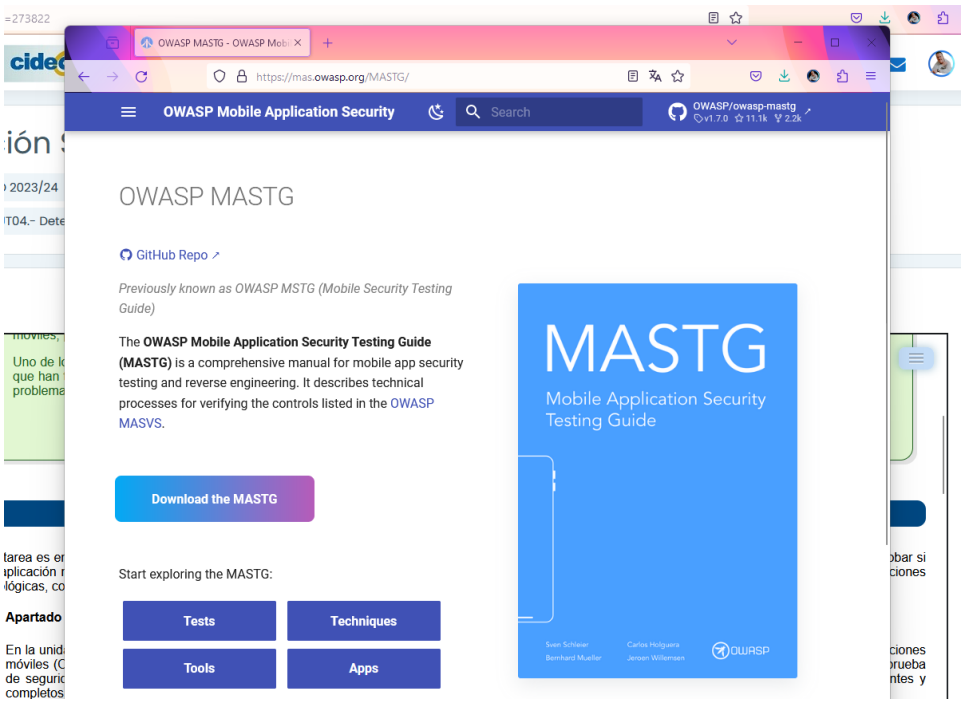
¿Qué te pedimos que hagas?

Esta tarea es eminentemente teórica donde el alumno deberá responder y desarrollar una serie de preguntas. El alumno debe saber manejar guías para comprobar si una aplicación móvil es segura o no, entender distintos conceptos como CASB, MDM, BYOD, etc y ser capaz de entender que capacidades aportan las soluciones tecnológicas, con qué problemas se encuentran en el mercado y qué capacidades adicionales podrían tener y qué las empresas valorarían.

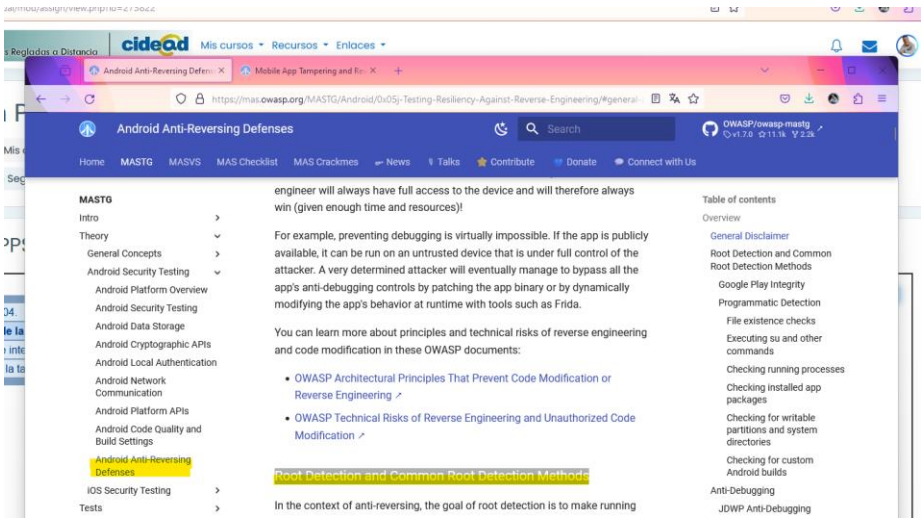
- ✓ **Apartado 1: MASTG (ver enlace)**

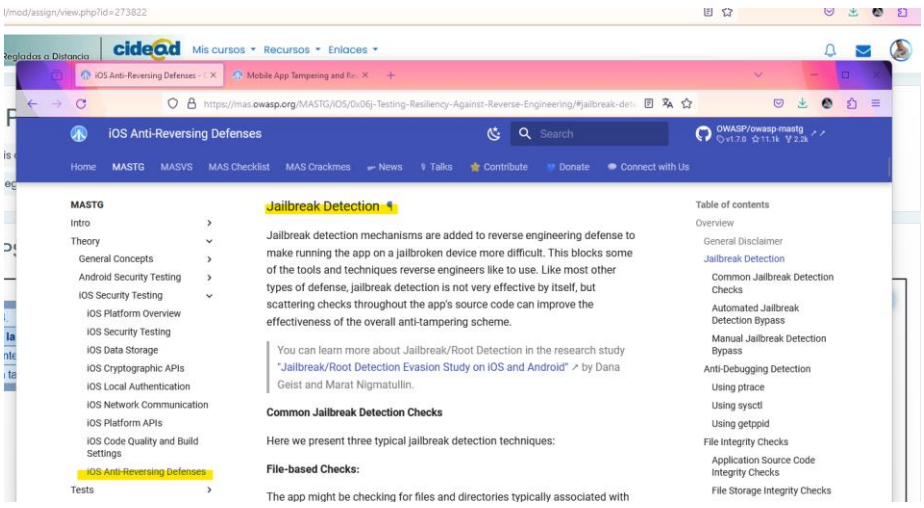
  En la unidad 2 ya vimos que OWASP ha desarrollado el proyecto Mobile Application Security (MAS) que proporciona un estándar de seguridad para aplicaciones móviles (OWASP MASVS) y una guía de pruebas exhaustiva (OWASP MASTG) que cubre los procesos, técnicas y herramientas utilizados durante una prueba de seguridad de aplicaciones móviles, así como un conjunto exhaustivo de casos de prueba que permite a los probadores ofrecer resultados coherentes y completos.

  En este apartado se pide **revisar la guía MASTG,** centrándote en las **diferentes defensas contra la Ingeniería Inversa en Android** (Android Anti-Reversing Defenses) y **en IOS** (IOS Anti-Reversing Defenses)



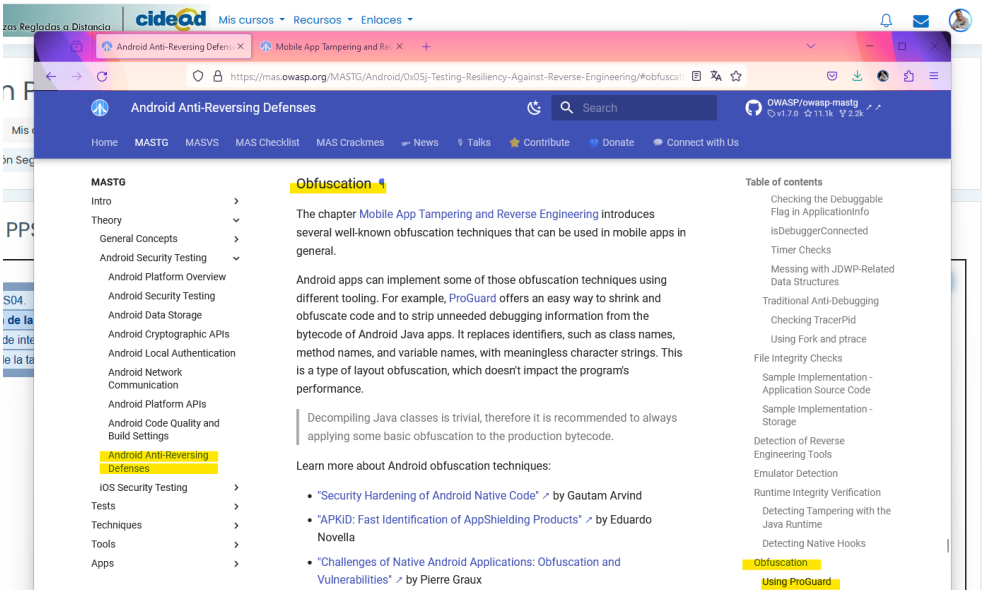
1. Una medida defensiva es **comprobar el "Rooteado" en Android y el "Jailbreak" en IOS**. Rellena la siguiente tabla utilizando la guía MASTG

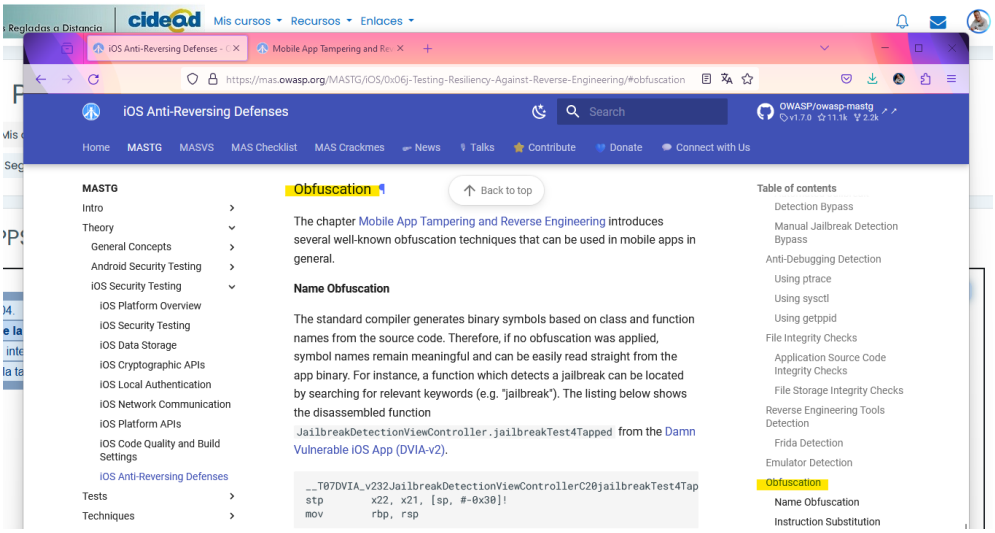




¿Qué son los dispositivos rooteados o con jailbreak?	Tanto en Android como en iOS, son dispositivos modificados mediante una vulnerabilidad para obtener acceso root.
Indica 1 medida para comprobar el rooteado	Incluir un NONCE con las solicitudes de verificación de integridad. Este valor aleatorio, generado por la aplicación o el servidor, ayuda al servidor de verificación a confirmar que las respuestas coinciden con las solicitudes originales sin manipulación de terceros
Indica 1 medida para comprobar el Jailbreak	Comprobar los Permisos de Archivo: La aplicación podría estar tratando de escribir a una ubicación que está fuera de la sandbox de la aplicación.

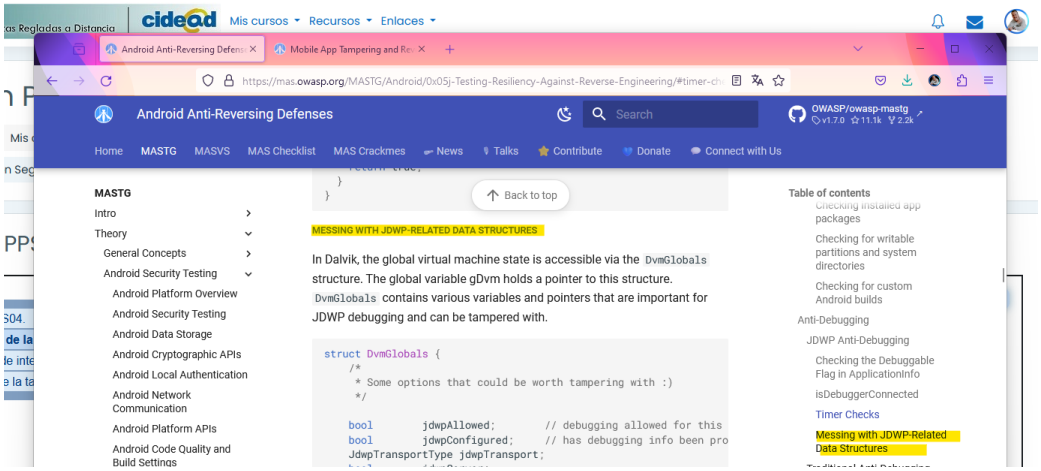
2. Otra medida defensiva es la **ofuscación**. Rellena la siguiente tabla utilizando la guía MASTG





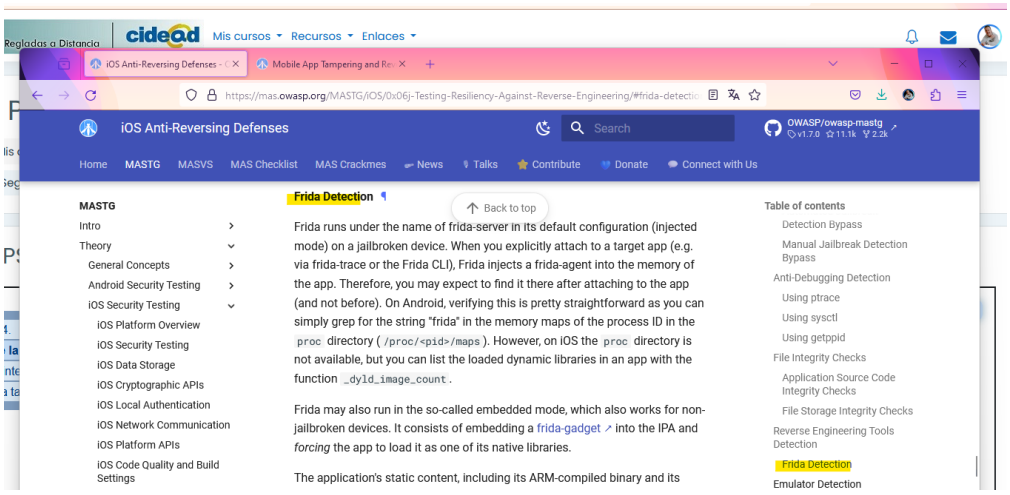
¿En qué consiste la ofuscación?	El compilador estándar genera símbolos binarios basados en nombres de clase y función del código fuente. Por lo tanto, si no se aplicó ofuscación, los nombres de símbolos siguen siendo significativos y se pueden leer fácilmente directamente desde el binario de la aplicación.
Indica para que se utiliza la herramienta **ProGuard** y cómo se utiliza	Los desarrolladores utilizan el archivo **`build.gradle`** para permitir la ofuscación. Crear excepciones para proteger algunas clases de la ofuscación (con **`-keepclassmembersy -keep class`**) es común. Por lo tanto, auditar el archivo de configuración de **ProGuard** para ver qué clases están exentas es importante. El método **`getDefaultProguardFile('proguard-android.txt')`** obtiene la configuración predeterminada de **ProGuard** de la carpeta **`<Android SDK>/tools/proguard/`**.
Indica para que se utiliza la herramienta **SwiftShield** y cómo se utiliza	**SwiftShield** se puede utilizar para realizar la ofuscación de nombre. Lee el código fuente del proyecto **Xcode** y reemplaza todos los nombres de las clases, métodos y campos con valores aleatorios antes de que se utilice el compilador.

3. Explorar aplicaciones utilizando un depurador es una técnica muy poderosa. No solo se puede rastrear variables que contienen datos confidenciales y modificar el flujo de control de la aplicación, sino también leer y modificar la memoria y los registros. Rellena la siguiente tabla utilizando la guía MASTG



Explica qué consiste la técnica antidepuración **JDWP en Android**	En Dalvik, el estado de la máquina virtual global es accesible a través de la estructura **`DvmGlobal`**. La variable global **`gDvm`** contiene un puntero a esta estructura. **`DvmGlobals`** contiene varias variables y punteros que son importantes para la depuración de **JDWP** y se pueden manipular. Puede manipular el comportamiento de la depuración tiempo de ejecución. Una manera de sobrescribir los punteros de método es sobrescribir la dirección de la función **`jdwpAdbState::ProcessIncoming`** con la dirección de **`JdwpAdbState::Shutdown`**. Esto hará que el depurador se desconecte inmediatamente.
Explica qué es **ptrace** y cómo se puede utilizar para evitar la depuración en **iOS.**	En Linux, **ptrace** es una llamada al sistema que se utiliza para observar y controlar la ejecución de un proceso y para examinar y cambiar la memoria y los registros de ese proceso. **ptrace** es la principal manera de implementar el rastreo de llamadas de sistema y depurar la depuración en código nativo. En iOS, la aplicación de la llamada al sistema de **ptrace** contiene una característica no estándar y muy útil: prevenir la depuración de los procesos. Esta característica se implementa como la petición **`PT_DENY_ATTACH`**, según se describe en el Manual oficial de llamadas del sistema BSD. En palabras simples, se asegura de que ningún otro depurador pueda adjuntar al proceso de llamada; si un depurador intenta adjuntar, el proceso terminará

4. La presencia de herramientas, frameworks y aplicaciones comúnmente utilizadas por la ingeniería inversa puede indicar un intento de realizar ingeniería inversa en la aplicación. Algunas de estas herramientas sólo pueden ejecutarse en un dispositivo con jailbreak o rooteado, mientras que otras obligan a la aplicación a entrar en modo de depuración o dependen del inicio de un servicio en segundo plano en el teléfono móvil. Por lo tanto, **existen diferentes formas que una aplicación puede implementar para detectar un ataque de ingeniería inversa y reaccionar ante él**, por ejemplo, finalizándose ella misma. Utilizando la guía MASTG



Explica qué es y para que se utiliza la herramienta **Frida**	Es un framework muy utilizado en ingeniería inversa que permite inyectar código en procesos en ejecución para modifica su comportamiento. Detectarlo, puede ser de ayuda para ver si un dispositivo ha sido atacado o rooteado.
Explica cómo se puede detectar en iOS (Frida Detection)	Frida se ejecuta bajo el nombre de **`frida-server`** en su configuración predeterminada (modo inyectado) en un dispositivo rooteado. Cuando se adhiere explícitamente a una aplicación de destino (por ejemplo, a través de **`frida-trace`** o el Frida CLI), Frida inyecta un **`Frida-agent`** en la memoria de la aplicación. Por lo tanto, es posible que esperes encontrarlo allí después de adjuntar a la aplicación (y no antes).

✓ Apartado 2: CASB y MDM

Los servicios **CASB (Cloud Access Security Broker**) y las plataformas **MDM (Mobile Device Management)** desempeñan roles esenciales en la seguridad de la información en entornos empresariales modernos. La combinación de CASB y MDM proporciona un enfoque integral para abordar las amenazas modernas, asegurando tanto los datos en la nube como los dispositivos móviles, lo que es crucial para salvaguardar la integridad y confidencialidad de la información empresarial.

1. ¿Qué diferencias hay entre CASB y MDM (Mobile Device Management)?

Enfoque: Mientras CASB se centra en la **seguridad de los datos en la nube**, protegiendo aplicaciones SaaS, IaaS y PaaS, controlando el acceso a la información y previniendo fugas de datos, **MDM** lo hace centrándose en la **seguridad de los dispositivos móviles**, protegiéndolos contra malware, administrando aplicaciones, borrando datos de forma remota y controlando configuraciones de seguridad.

Arquitectura: **CASB** se puede implementar en la nube o en la red empresarial, y no requiere la instalación de software en los dispositivos móviles. En el caso de **MDM**, requiere que la instalación de un software en los dispositivos móviles, permitiendo a la empresa controlar el acceso a los recursos empresariales.

Alcance: **CASB** protege **toda la información en la nube**, independientemente del dispositivo que sea utilizado para acceder a ella y a sus recursos. **MDM** limita este alcance a la seguridad de los **dispositivos móviles** bajo su gestión, ya sean propiedad de la empresa o del usuario.

Funcionalidades: **CASB:** Ofrece funcionalidades como **visibilidad y control** sobre el uso de aplicaciones en la nube, **monitorización** de la actividad en la nube para **detectar amenazas,** Prevención de **pérdida de datos** en la nube o **Integración** con otras soluciones de seguridad en la nube**. MDM,** por su parte ofrece funcionalidades como la **administración de aplicaciones** en dispositivos móviles, el **borrado remoto** de datos en caso de robo o pérdida del dispositivo o el control de **configuraciones de seguridad** del dispositivo.

2. **¿Con qué problemas se han encontrado las soluciones de MDM?**

Las **soluciones MDM** han encontrado algunos **problemas** como:

- ✓ **Falta de visibilidad en las aplicaciones en la nube:** No pueden controlar las aplicaciones SaaS que se ejecutan en los dispositivos móviles.
- ✓ **Dificultad para administrar dispositivos BYOD:** Son más efectivas para dispositivos propiedad de la empresa, pero se dificulta su implementación y administración en dispositivos BYOD.
- ✓ **Problemas de privacidad:** Pueden ser vistas como herramientas invasivas por los empleados, ya que recopilan información sobre sus dispositivos y su actividad.
- ✓ **Falta de integración con las soluciones de seguridad en la nube:** No siempre se integran bien con las soluciones de seguridad en la nube, creando brechas en la seguridad.

✓ Apartado 3: Diseño y capacidades de CASB

1. **¿Qué ventajas y desventajas en un entorno de CASB aporta tener un agente instalado en los terminales?**

Ventajas de tener un agente CASB instalado en los terminales:

- ✓ **Mayor visibilidad y control:** Permite un control más granular sobre las aplicaciones en la nube y los datos a los que se accede desde los terminales. Brinda información en tiempo real sobre la actividad en la nube, lo que facilita la detección de amenazas y la respuesta a incidentes. Permite aplicar políticas de seguridad más específicas y personalizadas a cada terminal.
- ✓ **Mejor protección contra malware y otras amenazas:** Puede detectar y bloquear malware y otras amenazas en tiempo real, antes de verse afectado el terminal. Puede realizar análisis de comportamiento para identificar posibles actividades sospechosas y prevenir ataques. También puede ayudar a proteger los datos confidenciales contra el robo o la fuga.

- ✓ **Mayor cumplimiento de las normas de seguridad:** Puede ayudar a las empresas a cumplir con las normas de seguridad acerca del control específico sobre los datos en la nube. Puede facilitar la auditoría y el seguimiento de la actividad en la nube.

Desventajas de tener un agente CASB instalado en los terminales:

- ✓ **Impacto en el rendimiento:** El agente puede consumir recursos del sistema, lo que puede llegar a afectar al rendimiento del terminal, pudiendo ser especialmente significativo en dispositivos móviles con recursos limitados.
- ✓ **Problemas de compatibilidad:** El agente puede no ser compatible con todos los tipos de dispositivos o sistemas operativos, lo que puede dificultar la implementación y la gestión del agente en un entorno heterogéneo.
- ✓ **Preocupaciones de privacidad:** La instalación de un agente puede ser vista como una invasión a la privacidad de los usuarios. Es importante tener una política clara sobre la recopilación y el uso de datos por parte del agente.

2. **¿Qué problema supone cuando un usuario se va de la empresa en un entorno de BYOD (Bring Your Own Device)?¿Qué mecanismos podríamos tener en nuestro entorno de CASB ideal para cuando un usuario abandone la compañía y siga siendo compatible con BYOD?**

Presenta un problema de seguridad respecto a los datos corporativos almacenados como:

- ✓ **Acceso no autorizado a datos confidenciales:** El usuario que deja la empresa puede seguir teniendo acceso a información confidencial de la empresa, como datos de clientes, información financiera o secretos comerciales.
- ✓ **Fuga de datos:** El usuario puede copiar o transferir datos confidenciales a dispositivos no autorizados o a terceros.
- ✓ **Pérdida de control sobre los dispositivos:** La empresa pierde el control sobre los dispositivos que ya no están bajo su posesión, lo que dificulta la eliminación de datos confidenciales o la aplicación de medidas de seguridad.

Pueden implementarse **mecanismos** como:

- ✓ **Borrado remoto de datos corporativos:** Permite eliminar de forma segura todos los datos corporativos del dispositivo del usuario, incluso si el dispositivo no está conectado a la red de la empresa. Es importante que el borrado remoto sea selectivo, para que solo se eliminen los datos corporativos y no los datos personales del usuario.
- ✓ **Revocación de permisos de acceso a aplicaciones y recursos**: Permite cancelar el acceso del usuario a las aplicaciones y recursos corporativos, como correo electrónico, archivos compartidos y plataformas de colaboración, ayudando a prevenir que el usuario siga teniendo acceso a información confidencial tras su salida de la empresa.
- ✓ **Cifrado de datos:** Permite proteger los datos corporativos en el dispositivo del usuario, incluso si este es robado o perdido, ya que el cifrado nos asegura que solo los usuarios autorizados puedan acceder a los datos.

- ✓ **Monitorización de la actividad del dispositivo:** Permite monitorizar la actividad del dispositivo del usuario en busca de comportamientos sospechosos, como intentos de acceso a datos confidenciales o transferencias de archivos no autorizadas. Esto ayuda a detectar y prevenir posibles fugas de datos.
- ✓ **Integración con herramientas de gestión de dispositivos móviles (MDM**): Permite unificar la gestión de dispositivos BYOD y la seguridad de los datos corporativos. Como ya se ha apuntado anteriormente, las herramientas MDM pueden ayudar a implementar políticas de seguridad, como el borrado remoto de datos y la restricción de aplicaciones.

3. ¿Qué capacidades adicionales podríamos añadir a nuestra solución de CASB?

- ✓ **Protección contra amenazas avanzadas:** Detección y prevención de intrusiones en la nube (Cloud IPS), protegiendo contra ataques a las aplicaciones y datos en la nube. Análisis de malware en la nube que detecta y bloquea malware en la nube, incluyendo ransomware y cryptojacking, o Sandbox de aplicaciones en la nube, permitiendo probar aplicaciones en un entorno seguro antes de implementarlas en producción.
- ✓ **Prevención de fuga de datos (DLP):** Clasificación de datos en la nube, control de acceso basado en roles (RBAC), que restrinja el acceso a datos sensibles en la nube a usuarios autorizados, o el cifrado de datos en la nube.
- ✓ **Gestión de la postura de seguridad en la nube (CSPM):** Evaluación de riesgos en la nube y remediación de riesgos en la nube, ayudando a implementar medidas para remediar riesgos de seguridad en la nube, o el cumplimiento normativo en la nube, que ayude a las empresas a cumplir con las normas de seguridad y privacidad en la nube.
- ✓ **Análisis de comportamiento de usuarios y entidades (UEBA):** Detección de anomalías en la nube, identificando comportamientos anómalos en la nube que pueden indicar un ataque o una fuga de datos. Investigación de incidentes en la nube.
- ✓ **Integración con otras herramientas de seguridad:** Con un sistema de gestión de información y eventos de seguridad (SIEM) o con una plataforma de orquestación, automatización y respuesta a incidentes (SOAR).
- ✓ **Soporte para múltiples proveedores de nube:** soporte para diferentes tipos de servicios (SaaS, IaaS y PaaS), o de datos en la nube (AWS, Azure y Google Cloud Platform).
- ✓ **Informes y análisis de seguridad en la nube.**

Webgrafía

https://mas.owasp.org/MASTG/

https://ciberseguridad.com/herramientas/agente-seguridad-acceso-nube-casb/

https://www.netskope.com/es/security-defined/what-is-casb

https://www.oracle.com/es/database/security/que-es-casb.html

https://www.ibm.com/es-es/topics/mobile-device-management

https://www.ibm.com/es-es/topics/byod

https://computerhoy.com/noticias/moviles/que-es-byod-ventajas-e-inconvenientes-7250