Ejemplo de

informe sobre un incidente de ciberseguridad

Este **ejemplo** de informe refiere a un evento de seguridad diferente al escenario presentado en la actividad. Solo debe usarse para que te familiarices con el formato de informe esperado.

| **Parte 1: Proporciona un resumen del problema encontrado en el registro de tráfico DNS e ICMP** | |
| --- | --- |
| Los registros del analizador de protocolos de red indican que el puerto 443 es inaccesible cuando se intenta acceder al sitio web seguro de constatación de referencias de empleados/as. El puerto 443 se utiliza normalmente para el tráfico HTTPS. Esto puede indicar un problema con el servidor web o la configuración del cortafuegos (firewall). Es posible que esto indique un ataque malicioso al servidor web. | |
|

| **Parte 2: Explica tu análisis de los datos y proporciona una solución para implementar** |
| --- |
| El incidente se produjo a primera hora de la mañana, cuando el equipo de recursos humanos (RRHH) informó de que no podía acceder al portal web de constatación de referencias. El equipo de seguridad de red respondió y comenzó a realizar pruebas con la herramienta de análisis de protocolos de red tcpdump. Estas revelaron que no se puede acceder al puerto 443, que se utiliza para el tráfico HTTPS. Continuamos investigando el origen del problema para determinar cómo podemos restaurar el acceso al portal web seguro. Nuestros próximos pasos incluyen verificar la configuración del firewall para ver si el puerto 443 está bloqueado y contactar al administrador de sistema del servidor web para que compruebe si hay indicios de ataque. El equipo de recursos humanos cree que es posible que una determinada persona recién contratada quiera evitar que se lleve a cabo la constatación de referencias. El equipo de seguridad de red sospecha que esta persona podría haber lanzado un ataque para bloquear el sitio web de constatación de referencias. |