**Respuestas de STAR**

| **Experiencias que demuestran mis habilidades** :   1. Ayudó al grupo Nice Touch Healthcare a fortalecer su postura de seguridad mediante la adhesión a las políticas y procedimientos estándar de la industria. 2. Mantuvo comunicaciones efectivas con varios equipos de la organización para garantizar la alineación general en las mejores prácticas de seguridad. 3. Completé el Certificado de Ciberseguridad de Google, lo que demuestra mi entusiasmo por aprender y desarrollar mis conocimientos y habilidades. | |
| --- | --- |
| **Pregunta 1:** Hábleme de alguna ocasión en la que haya tenido que trabajar con varios equipos internos en tareas de seguridad. ¿Cómo planificó y organizó los horarios adecuados para reunirse y los plazos mutuamente aceptables para todos estos equipos? ¿Cuál fue el resultado? | |
| **Situación** | Cuando era analista junior de ciberseguridad en Nice Touch Healthcare Group, la organización estaba experimentando un tremendo aumento en la cantidad de empleados que hacían clic en enlaces de correo electrónico de phishing. El equipo de seguridad determinó que varios líderes de departamento no estaban educando a sus empleados sobre la importancia de no hacer clic en todos los enlaces y archivos adjuntos que se encontraban en un correo electrónico. |
| **Tarea** | Fui parte de un equipo encargado de identificar qué departamentos hacían clic en la mayor cantidad de enlaces de phishing y comunicar esos hallazgos a los líderes de esos departamentos. |
| **Acción** | Entré en el calendario laboral de nuestra organización para encontrar horarios disponibles para reunirme con analistas de nivel superior para analizar los datos de phishing que habían recopilado. Analizamos el impacto de los datos y la necesidad de que yo los presentara en una presentación visual. Después de crear gráficos de barras para los datos de phishing, me comuniqué con los asistentes de los distintos líderes de departamento por correo electrónico para establecer la mejor fecha y hora para que mi equipo y esos líderes se unieran a una videollamada para analizar los datos. Elaboramos un plan para minimizar la cantidad de correos electrónicos de phishing en los que se hacía clic mediante el lanzamiento de una campaña de concienciación para los empleados y establecimos un cronograma para completar el plan antes de fin de año. |
| **Resultado** | La organización vio una disminución del 20% en la cantidad de enlaces de phishing en los que los empleados hicieron clic un mes después de que mi equipo y yo nos reunimos con todos los líderes del departamento. |
| **Pregunta 2:** Describa una experiencia en la que haya tenido que crear, desarrollar y/o mantener documentación relacionada con procesos y procedimientos de seguridad. ¿Cómo planificó, ejecutó y mantuvo estos documentos? | |
| **Situación** | Cuando comencé a trabajar en Nice Touch Healthcare Group, la organización estaba trabajando en el establecimiento de su programa de evaluación de terceros. El objetivo del programa era evaluar adecuadamente la seguridad de todas las empresas de terceros con las que trabajábamos para asegurarnos de que no tuvieran vulnerabilidades de seguridad importantes que pudieran afectar negativamente a nuestra organización. |
| **Tarea** | Después de trabajar en Nice Touch durante un año, me pusieron a cargo de administrar cualquier actualización o cambio en los procedimientos y políticas del programa de evaluación de terceros. |
| **Acción** | Me concedieron acceso a una unidad compartida que contenía las políticas y los procedimientos de evaluación de terceros. A partir de ahí, realicé una auditoría de las personas que tenían acceso a esa carpeta compartida. Descubrí que algunos empleados que ya no trabajaban para la empresa o que ya no trabajaban con el equipo de evaluación de terceros todavía tenían acceso a la carpeta compartida. Se lo comenté a mi supervisor directo y me dieron permiso para eliminar el acceso de esas personas a la carpeta compartida. A partir de ahí, organicé reuniones semanales con otros miembros del equipo de evaluación de terceros para analizar los nuevos cambios o ajustes que debían realizarse en las políticas y los procedimientos. También agregué o eliminé periódicamente el acceso de las personas a la carpeta compartida según fuera necesario. |
| **Resultado** | Los ejecutivos mencionaron el programa de evaluación de terceros en la reunión de revisión funcional de fin de año. Los ejecutivos comentaron que apreciaban lo mucho más ágil y colaborativo que se había vuelto el programa de terceros después de que comencé a mantener la documentación. |

**Preguntas de entrevistas de comportamiento habituales para analistas de ciberseguridad**

1. Describa una experiencia en la que haya asesorado y trabajado con unidades de negocio internas sobre cuestiones relacionadas con la seguridad. ¿De qué manera se reunió con los equipos, abordó preguntas, fomentó el cumplimiento normativo y ayudó a garantizar una productividad óptima?
2. Describe una experiencia en la que hayas implementado una solución de seguridad. ¿Cuál fue tu solución, cómo ayudaste con la implementación y cuáles fueron los resultados?
3. Describe una experiencia en la que hayas utilizado tus habilidades de ciberseguridad de manera eficaz. ¿Cómo analizaste las variables e identificaste anomalías para mejorar la seguridad y la productividad de tu empresa?
4. Cuénteme sobre alguna ocasión en la que una actualización en el campo de la seguridad de la información, la ciberseguridad o el cumplimiento normativo lo tomó por sorpresa. ¿En qué consistió esa actualización y cómo se enteró de ella? ¿Qué hace hoy para mantenerse al día con la información relevante?
5. Describa una experiencia en la que haya utilizado herramientas de seguridad técnica como parte de la resolución de problemas. ¿Cómo evaluó los problemas y llegó a la conclusión de que estas herramientas representaban la solución óptima? ¿Cuál fue el resultado?
6. Describa una experiencia en la que haya tenido que planificar, desarrollar, ejecutar y/o mantener documentación relacionada con procesos y procedimientos de seguridad. ¿Cómo planificó, ejecutó y mantuvo estos documentos?
7. Cuénteme sobre alguna ocasión en la que haya tenido que trabajar con varios equipos internos en tareas de seguridad. ¿Cómo planificó y organizó los momentos adecuados para reunirse y los plazos mutuamente aceptables para todos estos equipos? ¿Cuál fue el resultado?
8. Describa una experiencia en la que una fuga de seguridad u otro problema exigieron una respuesta, un análisis y una acción inmediatos. ¿Cómo organizó y ejecutó esto mientras priorizaba y se ocupaba de otras tareas que se vieron interrumpidas por este evento? ¿Cuál fue el resultado?
9. Cuénteme sobre alguna ocasión en la que tuvo que hablar con un alto directivo en su función de analista de ciberseguridad sobre problemas técnicos complejos y soluciones. ¿Cómo expresó información altamente técnica de una manera que pudiera ser entendida y respondida de manera efectiva?
10. Cuénteme sobre alguna ocasión, si es que alguna vez, en que haya experimentado reticencias por parte de algunos miembros de la alta dirección con respecto a un tema de seguridad o normativo. ¿Cómo consiguió que respaldaran sus opiniones, con quién habló y cuál fue el resultado?