**6/10/2024 Los ocho dominios de Seguridad CISSP – modulo2 – Google**

Tener un conocimiento sólido de los conceptos básicos de Seguridad respaldará su crecimiento en este campo. Una forma de entender mejor estos conceptos básicos es organizarlos en categorías, denominadas dominios de Seguridad.

A partir de 2022, el CISSP ha definido ocho dominios para organizar el trabajo de los profesionales de la Seguridad. Es importante entender que estos dominios están relacionados y que las brechas en un dominio pueden tener consecuencias negativas para toda la organización.

El CISSP define ocho dominios en total: seguridad y gestión de riesgos, seguridad de los recursos, arquitectura e ingeniería de seguridad y seguridad de la red y las comunicaciones. administración de identidades y accesos, evaluación y pruebas de seguridad, operaciones de seguridad y seguridad de desarrollo de software.

1. **La seguridad y la gestión de riesgos:** La administración de seguridad y riesgos, se centra en definir las metas y objetivos de seguridad, la mitigación de riesgos, el cumplimiento, la continuidad del negocio y la ley.

Por ejemplo, es posible que los analistas de seguridad deban actualizar las políticas de la empresa relacionadas con la información médica privada si se realiza un cambio en una regulación de cumplimiento federal, como la Ley de Transferencia y Responsabilidad de los Seguros Médicos, también conocida como HIPAA.

1. **La Seguridad de los recursos:** Este dominio se centra en proteger los activos digitales y físicos. También está relacionado con el almacenamiento, el mantenimiento, la retención y la destrucción de datos. Al trabajar con este dominio, es posible que los analistas de Seguridad tengan la tarea de asegurarse de que el equipo antiguo se deseche y destruya adecuadamente, incluido cualquier tipo de información confidencial.
2. **La arquitectura e ingeniería de Seguridad:** Este dominio se centra en optimizar la Seguridad de los datos garantizando la existencia de herramientas , sistemas y procesos eficaces. Como analista de seguridad, es posible que se le asigne la tarea de configurar un firewall. La configuración correcta de un firewall ayuda a prevenir los ataques que podrían afectar a la productividad.
3. **La seguridad de la red y la comunicación:** Este dominio se centra en administrar y proteger las redes físicas y las comunicaciones inalámbricas. Como analista de Seguridad, es posible que se le pida que analice el comportamiento de los usuarios dentro de su organización.
4. **La gestión de identidades y acceso:** La gestión de identidad y acceso se centra en mantener los datos seguros, garantizando que los usuarios sigan las políticas establecidas para controlar y administrar los activos físicos, como los espacios de oficina, y los activos lógicos, como las redes y las aplicaciones. La validación de las identidades de los empleados y la documentación de las funciones de acceso son esenciales para mantener la Seguridad física y digital de la organización.

Por ejemplo, como analista de Seguridad, es posible que se te asigne la tarea de configurar el acceso de los empleados a los edificios con tarjeta de acceso.

1. **La evaluación y las pruebas de Seguridad:** Este dominio se centra en la realización de pruebas de control de seguridad, la recopilación y el análisis de datos y la realización de auditorías de seguridad para supervisar los riesgos, las amenazas y las vulnerabilidades. Los analistas de seguridad pueden realizar auditorías periódicas de los permisos de los usuarios para asegurarse de que los usuarios tengan el nivel de acceso correcto. Por ejemplo, el acceso a la información de nómina suele estar limitado a ciertos empleados, por lo que es posible que se pida a los analistas que auditen periódicamente los permisos para garantizar que ninguna persona no autorizada pueda ver los salarios de los empleados.
2. **Las operaciones de Seguridad:** Este dominio se centra en la realización de investigaciones y la implementación de medidas preventivas. Imagine que usted, como analista de Seguridad, recibe una alerta de que un dispositivo desconocido se ha conectado a su red interna. Deberá seguir las políticas y los procedimientos de la organización para detener rápidamente la posible amenaza.
3. **La Seguridad del desarrollo de software:** Este dominio se centra en el uso de prácticas de programación seguras, que son un conjunto de directrices recomendadas que se utilizan para crear aplicaciones y servicios seguros. Un analista de seguridad puede trabajar con los equipos de desarrollo de software para garantizar que las prácticas de seguridad se incorporen al ciclo de vida del desarrollo de software. Si, por ejemplo, uno de sus equipos asociados está creando una nueva aplicación para dispositivos móviles: aplicación para dispositivos móviles, es posible que se le pida que informe sobre las políticas de contraseñas o que se asegure de que los datos de los usuarios estén protegidos y gestionados correctamente.

**Retro alimentación**

En primer lugar, hemos hablado de los virus, incluidos el virus Brain y el gusano Morris, y hemos analizado cómo estas primeras formas de software malicioso dieron forma a la industria de la Seguridad. También hemos hablado de cómo muchos ataques actuales son variantes de estos primeros ejemplos. Comprender los ataques anteriores es fundamental para los profesionales de la seguridad que trabajan para proteger a las organizaciones y a las personas de posibles variantes futuras. También hemos hablado de la ingeniería social y de los motivos de los agentes de amenaza al conocer el ataque LoveLetter y la filtración de datos de Equifax. Estos incidentes mostraron los amplios Impactos y Costos asociados de las violaciones de seguridad más recientes en la era digital. Por último, presentamos los ocho dominios de seguridad de CISSP y cómo pueden utilizarse para categorizar diferentes áreas de enfoque dentro de la profesión de la seguridad. ¡Espero que se sienta seguro de sus conocimientos básicos sobre seguridad! Aprender la historia de la seguridad puede permitirle comprender mejor la industria actual. Los ocho dominios de seguridad del CISSP proporcionan una forma de organizar el trabajo de los profesionales de la seguridad.