Descripción general del curso

Te damos la bienvenida a Fundamentos de la ciberseguridad, el primer curso del Certificado en Ciberseguridad de Google. ¡Acabas de comenzar una experiencia emocionante!

En este curso, aprenderás las principales responsabilidades y las habilidades básicas de quienes trabajan en el campo de la ciberseguridad. Explorarás los ocho dominios de seguridad del Certificado Profesional en Seguridad de Sistemas de Información (CISSP por sus siglas en inglés), distintos marcos y controles de seguridad, así como la tríada de confidencialidad, integridad y disponibilidad (CIA), uno de los modelos clave de seguridad. También verás algunas herramientas comunes utilizadas por las y los analistas de seguridad que ayudan a proteger tanto a las organizaciones como a las personas.

Flujo del curso

El programa del Certificado en Ciberseguridad de Google está compuesto de ocho cursos. Los fundamentos de la ciberseguridad es el primero.

Ocho íconos muestran los cursos secuencialmente de izquierda a derecha con el curso 1 resaltado.

Los fundamentos de la ciberseguridad

— (curso actual) Explora la profesión de especialista en ciberseguridad, incluidos los acontecimientos que llevaron al desarrollo de este campo y su importancia para la operación de las organizaciones. Aprende sobre las funciones y responsabilidades de nivel inicial de la especialización.

Ve a lo seguro: Gestiona los riesgos de seguridad

— Identifica cómo las y los profesionales de la ciberseguridad utilizan los marcos y controles para proteger las operaciones comerciales y explora las herramientas más comunes.

Conexión y protección: Redes y seguridad de redes

— Conoce las vulnerabilidades de las redes y cómo protegerlas.

Herramientas del oficio: Linux y SQL

— Explora los conocimientos informáticos básicos, incluyendo la comunicación con el sistema operativo Linux a través de la línea de comandos y la consulta de bases de datos con SQL.

Activos, amenazas y vulnerabilidades

— Conoce la importancia de los controles de seguridad y cómo se desarrolla la mentalidad de un agente de amenazas para poder prevenir, proteger y defender los activos de una organización frente a las diversas amenazas, riesgos y vulnerabilidades.

Haz sonar la alarma: Detección y respuesta

— Comprende el ciclo de vida de la respuesta a incidentes y práctica el uso de herramientas para detectar y responder a incidentes de ciberseguridad.

Automatiza las tareas de ciberseguridad con Python

— Explora el lenguaje de programación Python y escribe código para automatizar las tareas de ciberseguridad.

Ponlo en práctica: Prepárate para los trabajos de ciberseguridad

— Podría quedar: Aprende sobre clasificación de incidentes, la escala que adquieren y las formas de comunicación con las partes interesadas. Este curso cierra el programa con consejos sobre cómo relacionarse con la comunidad de la ciberseguridad y prepararse para la búsqueda de empleo.

Contenido del curso 1

Cada curso de este programa de certificados se divide en semanas. Puedes realizar los cursos a tu propio ritmo, pero la división en semanas está diseñada para ayudarte a terminar todo el Certificado en Ciberseguridad de Google en alrededor de seis meses.

Qué hay por delante? A continuación, presentamos una descripción general de las habilidades que adquirirás en cada semana de este curso.

Semana 1: Introducción al apasionante mundo de la ciberseguridad

Five icons show the course followed by the four modules sequentially from left to right with module 1 highlighted.

¡Comienza tu viaje hacia la ciberseguridad! En él explorarás el campo de la ciberseguridad y conocerás las responsabilidades de las y los profesionales de la ciberseguridad.

Semana 2: La evolución de la ciberseguridad

Explorarás cómo aparecieron y evolucionaron las amenazas de ciberseguridad paralelamente a la adopción de las computadoras. También comprenderás cómo los ciberataques pasados y presentes han influido en el desarrollo de este campo. Además, obtendrás una visión general de los ocho dominios de seguridad.

Semana 3: Protección frente a amenazas, riesgos y vulnerabilidades

Five icons show the course followed by the four modules sequentially from left to right with module 3 highlighted.

Estudiarás los marcos y controles de seguridad, que se utilizan para mitigar el riesgo empresarial. Cubrirás los principios de la tríada CID y varios marcos del Instituto Nacional de Estándares y Tecnología (NIST). Además, explorarás la ética de la seguridad.

Semana 4: Herramientas de ciberseguridad y lenguajes de programación

Descubrirás herramientas comunes utilizadas por las y los analistas de ciberseguridad para identificar y eliminar riesgos. Aprenderás sobre las herramientas de gestión de eventos e información de seguridad (SIEM), los analizadores de protocolos de red y lenguajes de programación como Python y SQL.

Qué puedes esperar

Cada curso ofrece muchos tipos de oportunidades de aprendizaje, que incluyen:

Videos dirigidos por especialistas de Google para que puedas aprender nuevos conceptos, empezar a usar las herramientas más relevantes, recibir apoyo profesional y escuchar historias personales inspiradoras.

Lecturas para que puedas incorporar nuevos conceptos, recibir consejos útiles y conocer casos prácticos con base en los temas discutidos en los videos.

F

oros de debate

sobre temas del curso para que puedas profundizar sobre ellos mientras chateas e intercambias ideas con otros/as estudiantes.

Autoevaluaciones y laboratorios para que puedas poner en práctica tus conocimientos y evaluar tu trabajo comparándolo con un ejemplo realizado.

Complementos interactivos para que puedas practicar tareas específicas y aplicar los conocimientos adquiridos en el curso.

Cuestionarios en video para que compruebes tu comprensión a medida que avanzas en cada video.

Cuestionarios de práctica para ayudarte a comprender el contenido presentado en cada video.

Cuestionarios con calificación para medir tu progreso, darte una retroalimentación valiosa y poder otorgarte tu certificado. De acuerdo con las pautas del programa, puedes realizar una prueba con calificación varias veces, hasta lograr una puntuación aprobatoria del 80% o más.

Consejos para tener éxito

Recomendamos tomar los cursos y recorrer los puntos de cada lección en el orden en que aparecen, ya que cada información y concepto nuevo se basa en los conocimientos anteriores.

Participa en todas las oportunidades de aprendizaje para obtener el mayor conocimiento y experiencia posibles.

Si algo es confuso, no dudes en volver a reproducir un video, revisar una lectura o repetir una actividad de autoevaluación.

Usa los

recursos adicionales

a los que se hace referencia en este curso. Están diseñados para consolidar tu aprendizaje. Cuando encuentres enlaces útiles en un curso, recuerda agregarlos a tus marcadores para que puedas consultar después la información y estudiarla o revisarla.

Comprende y sigue el

Código de conducta de Coursera

para garantizar que la comunidad de aprendizaje siga siendo un lugar acogedor, amigable y de apoyo para todas las personas.

1. Fundamentos de la ciberseguridad

En este curso:

Definirás el campo de seguridad

Reconocerás las habilidades y conocimientos básicos necesarios para convertirte en un analista de seguridad

Identificarás cómo los ataques a la seguridad afectan a las operaciones comerciales

Identificarás ocho dominios de seguridad

Definirás los marcos y controles de seguridad

Conjuntos de habilidades:

Comunicación eficaz

Colaboración con los demás

Identificación de amenazas, riesgos y puntos vulnerables

Resolución de problemas

2. Juega seguro: Gestiona los riesgos de seguridad

**En este curso:**

* Reconocerás y explicarás el enfoque de ocho dominios de seguridad
* Identificarás los pasos de la gestión de riesgos
* Describirás la tríada CID
* Identificarás los principios de seguridad
* Definirás y describirás el propósito de un manual de estrategias
* Explicarás cómo los analistas de seguridad de nivel inicial utilizan los paneles SIEM

**Conjuntos de habilidades:**

* Aplicación de la tríada CID a situaciones laborales
* Análisis de datos de registro

Identificación de las fases de un manual de estrategias de respuesta a incidentes

1. Conexión y protección: Redes y seguridad de las redes

En este curso:

Definirás tipos de redes

Explicarás cómo se envían y reciben datos a través de una red

Reconocerás los protocolos de red más comunes

Compararás y contrastarás las redes locales con la computación en la nube

Explicarás cómo proteger una red contra tácticas de intrusión

Conjuntos de habilidades:

Configuración de un firewall

Reconocimiento de los componentes de redes informáticas y de la computación en la nube

Análisis de amenazas

Implementación del reforzamiento de la seguridad

1. Conexión y protección: Redes y seguridad de las redes

**En este curso:**

* Definirás tipos de redes
* Explicarás cómo se envían y reciben datos a través de una red
* Reconocerás los protocolos de red más comunes
* Compararás y contrastarás las redes locales con la computación en la nube
* Explicarás cómo proteger una red contra tácticas de intrusión

**Conjuntos de habilidades:**

* Configuración de un firewall
* Reconocimiento de los componentes de redes informáticas y de la computación en la nube
* Análisis de amenazas
* Implementación del reforzamiento de la seguridad

1. Herramientas del oficio: Linux y SQL

**En este curso:**

* Describirás las principales funciones de un sistema operativo
* Explicarás la relación entre los sistemas operativos, las aplicaciones y el hardware
* Compararás una interfaz gráfica de usuario con una interfaz de línea de comandos
* Navegarás por el sistema de archivos utilizando comandos de Linux a través del shell Bash
* Usarás SQL para recuperar información de una base de datos

**Conjuntos de habilidades:**

* Interacción con una interfaz gráfica de usuario (GUI) y una interfaz de línea de comandos (CLI)
* Consultar una base de datos con SQL
* Filtrado de una palabra concreta con la línea de comandos de Linux
* Autenticación y autorización de usuarios con la línea de comandos de Linux

1. Activos, amenazas y vulnerabilidades

**En este curso:**

* Explicarás el papel de la seguridad en la mitigación del riesgo organizacional
* Describirás la estrategia de defensa en profundidad
* Explicarás cómo se utilizan las evaluaciones de vulnerabilidad para evaluar el riesgo potencial
* Desarrollarás una mentalidad de atacante para reconocer las amenazas
* Discutirás el papel que desempeñan el cifrado y el hashing en la protección de activos
* Identificarás formas de ingeniería social, malware y exploits basados en la web

**Conjuntos de habilidades:**

* Clasificación de activos
* Descifrado de un mensaje
* Búsqueda de aplicaciones vulnerables en la base de datos de CVE
* Análisis de superficies de ataque
* Aplicación del marco de modelado de amenazas PASTA

1. Haz sonar la alarma: Detección y respuesta

**En este curso:**

* Explicarás el ciclo de vida de un incidente
* Utilizarás herramientas de rastreo de paquetes para capturar y visualizar las comunicaciones de red
* Realizarás investigaciones de artefactos para analizar y verificar incidentes de seguridad
* Identificarás los pasos para contener, erradicar y recuperarse de un incidente
* Interpretarás la sintaxis básica y los componentes de las firmas y los registros en herramientas IDS y NIDS

**Conjuntos de habilidades:**

* Captura, visualización y análisis de un paquete
* Investigación de un archivo hash sospechoso
* Seguimiento de un manual de estrategias
* Examen de alertas, registros y reglas
* Realización de consultas con herramientas SIEM

1. Automatiza las tareas de ciberseguridad con Python

**En este curso:**

* Explicarás cómo se usa el lenguaje de programación Python en seguridad
* Escribirás un algoritmo sencillo
* Usarás expresiones regulares en Python para extraer información de un texto
* Utilizarás Python para automatizar tareas realizadas por profesionales de la seguridad
* Usarás Python para analizar un archivo

**Conjuntos de habilidades:**

* Trabajo con cadenas y sus valores de índice
* Aplicación de expresiones regulares (regex)
* Importación y análisis sintáctico de un archivo
* Depuración de un código

1. Ponlo en práctica: Prepárate para los trabajos de ciberseguridad

**En este curso:**

* Definirás las partes interesadas y describirás sus funciones en materia de seguridad
* Comunicarás información sensible con cuidado y confidencialidad
* Identificarás fuentes fiables dentro de la comunidad de seguridad
* Determinarás oportunidades para interactuar con la comunidad de seguridad
* Determinarás formas de establecer y avanzar en una carrera en el ámbito de la seguridad, interactuando con la comunidad de seguridad
* Buscarás, solicitarás y te prepararás para entrevistas de trabajo

**Conjuntos de habilidades:**

* Creación de un panel de control
* Creación o actualización de un currículum
* Uso del método STAR para las preguntas de la entrevista
* Redacción de un elevator pitch

Recursos y consejos útiles

Puedes elegir realizar uno o varios cursos de este programa. Sin embargo, para obtener tu certificado, deberás completar todos los cursos del programa. Aquí te contamos todo lo que se requiere para obtener un certificado y las mejores prácticas para que tengas una buena experiencia de aprendizaje en la plataforma.

Finalización del curso para obtener un certificado

Para enviar tareas con calificación y cumplir con todos los requisitos necesarios para recibir tu Certificado en Ciberseguridad de Google, deberás hacer lo siguiente:

Pagar la

tarifa del certificado

o solicitar y obtener la aprobación para una

ayuda financiera

de Coursera.

Aprobar todas las tareas con calificación, en los ocho cursos, con el nivel mínimo (o superior) de aprobación. Cada tarea con calificación en un curso es parte de una calificación acumulativa para ese mismo curso. La puntuación mínima requerida para aprobar los cursos es del 80 %.

Consejos para terminar el curso

Aquí hay una lista de las mejores prácticas que te ayudarán a completar los cursos en el programa de manera oportuna:

Planifica tu tiempo: si programas momentos de estudio regularmente, en forma semanal, y los respetas, el aprendizaje se hará parte de tu rutina. Utiliza un calendario o un cronograma y haz una lista de lo que planeas hacer cada día para dividir tu trabajo en objetivos realistas. Elige un lugar tranquilo para ver los videos, revisar las lecturas y realizar las actividades, así puedes concentrarte en el material.

Trabaja a tu propio ritmo: cada persona aprende de forma diferente, así que diseñamos este programa para que puedas avanzar a tu propio ritmo. Aunque tus plazos empiezan a correr cuando te inscribes, estos son solo una guía. Puedes avanzar por el programa a la velocidad que prefieras. No hay ninguna penalización por entregar las tareas después de la fecha límite; para obtener el certificado, simplemente tienes que terminar todo el trabajo. Si lo prefieres, puedes ampliar los plazos volviendo a Descripción general en el panel de navegación y haciendo clic en Cambiar sesión. Si no cumpliste con los plazos anteriores, haz clic en Restablecer mis plazos.

Aprovecha la curiosidad: si hay una idea que te entusiasma, ¡aprovéchala! Haz preguntas, busca más datos en línea, consulta los enlaces que te interesan y toma notas sobre tus descubrimientos. Cada pequeña cosa que hagas para nutrir tu aprendizaje a lo largo del proceso potenciará tus conocimientos, te abrirá más puertas en este campo de gran crecimiento y te ayudará a tener las calificaciones necesarias para buscar empleo.

Toma notas: las notas sirven para recordar información que crees que podría ser importante en el futuro, especialmente cuando te preparas para entrar en un nuevo ámbito laboral. Además, tomar notas es una forma eficaz de relacionar los temas entre sí y comprenderlos mejor.

Revisa los ejemplos: los ejemplos son tareas completadas que cumplen plenamente los criterios de las actividades. Utilízalos para validar tu trabajo o comprobar si has cometido errores. Aunque generalmente hay muchas maneras de completar una tarea, los ejemplos te ofrecen orientación e inspiración sobre cómo hacerlo.

Usa el chat (de manera responsable) con otras y otros estudiantes: quizás no seas la única persona que tiene preguntas o dudas. Ve al

foro de debate

para comunicarte con otras/otros estudiantes y pedir ayuda. También puedes visitar la

Comunidad global en línea

de Coursera. Consulta el

Código de honor

y el

Código de conducta de Coursera

para conocer otras cosas importantes que debes saber.

Actualiza tu perfil: considera

actualizar tu perfil

en Coursera con tu foto, tus objetivos profesionales y más. Cuando quienes estudian contigo te encuentren en los foros de debate, pueden hacer clic en tu nombre para ver tu perfil y conocerte más.

Documentos, hojas de cálculo, presentaciones y labs para las actividades del curso

Para completar ciertas actividades en el programa, deberás usar documentos digitales, hojas de cálculo, presentaciones y labs. Las y los profesionales de la seguridad utilizan estas herramientas de software para colaborar dentro de sus equipos y organizaciones. Si necesitas más información sobre el uso de una herramienta en particular, consulta estos recursos:

Microsoft Word: Ayuda y aprendizaje

: página de soporte técnico de Microsoft para Word

Documentos de Google

: página del Centro de Ayuda para Google Docs

Microsoft Excel: Ayuda y formación

: página de soporte técnico de Microsoft para Excel

Hojas de cálculo de Google

: página del Centro de Ayuda para las hojas de cálculo de Google

Microsoft PowerPoint: Ayuda y formación

: página de soporte técnico de Microsoft para PowerPoint

Cómo usar Presentaciones de Google

: página del Centro de Ayuda para Google Slides

Problemas comunes con labs

: ayuda para la resolución de problemas en las actividades de Qwiklabs

Glosarios del curso

En este curso, se abarcan muchos términos y conceptos, algunos de los cuales es posible que ya conozcas mientras que otros te resultarán nuevos. Para recordar el significado de un término o revisar los conceptos antes de las pruebas con calificación, consulta los siguientes glosarios:

Glosarios semanales: al final del contenido de cada semana, podrás revisar un glosario de los términos utilizados. Estos glosarios se basan en los términos de las semanas anteriores a ese curso y no se pueden descargar. Sin embargo, todos los términos y definiciones se incluyen en los glosarios del curso y del certificado, que sí te ofrecen esa posibilidad.

Glosarios del curso: al final de cada curso, podrás acceder y descargar un glosario que cubre todos los términos del mismo.

Glosario del certificado: este glosario incluye todos los términos del programa. Es un recurso útil al que puedes recurrir en cualquier momento ahora o en el futuro.

Puedes encontrar los glosarios del curso y del certificado a través de la sección de

Recursos

del curso, descargarlos y guardarlos en tu computadora.

También puedes acceder al glosario del Certificado en Ciberseguridad, haciendo clic en el siguiente enlace y seleccionando Use Template [Usar plantilla].

Glosario del Certificado en Ciberseguridad

O BIEN

puedes descargarlo directamente desde el archivo adjunto.

Comentarios del curso

Proporcionar comentarios sobre videos, lecturas y otros materiales es fácil. Abre el curso en tu navegador y busca los símbolos de pulgar hacia arriba y pulgar hacia abajo.

Haz clic en el pulgar hacia arriba en los materiales que te resulten útiles.

Haz clic en el pulgar hacia abajo en los materiales que no sean útiles para ti.

Si quieres marcar un problema específico, haz clic en el ícono de la bandera, selecciona una categoría y escribe tu explicación en el cuadro de texto. Estos comentarios van dirigidos a quienes desarrollan el curso y no son visibles para las/los estudiantes. Todos los comentarios ayudarán a mejorar los programas de certificación en el futuro.

Imagina que te estás preparando para una tormenta. Recibiste un aviso de emergencia y te preparas reuniendo las herramientas y materiales que necesitas para mantenerte a salvo. Aseguras las ventanas y las puertas, preparas un botiquín de primeros auxilios, herramientas, comida y agua. Lo tienes todo listo. Llega la tormenta y hay fuertes vientos y lluvias que usan su fuerza para tratar de entrar en tu hogar. Notas algunas entradas de agua y las arreglas rápidamente para minimizar riesgos o posibles daños. Hacer frente a un incidente de seguridad es parecido. Las organizaciones deben prepararse para la tormenta asegurándose de contar con herramientas para mitigar y responder a las amenazas externas. El objetivo es minimizar riesgos y posibles daños. Como analista de seguridad, trabajarás para proteger tu organización y a su personal de una serie de riesgos y amenazas externas. Y si un ataque logra entrar, tú y tu equipo deberán dar una solución. Para que entiendas mejor lo que significa, definiremos la ciberseguridad y hablaremos de los roles de profesionales de seguridad de las empresas. Comencemos con algunas definiciones: La ciberseguridad, o seguridad, es la práctica de garantizar la confidencialidad, la integridad y disponibilidad de la información protegiendo las redes, los dispositivos, a las personas y los datos del acceso no autorizado o la explotación delictiva. Por ejemplo, requerir contraseñas complejas para acceder a sitios y servicios mejora la confidencialidad y dificulta que un agente de amenaza los ponga en peligro. Un agente de amenaza es cualquier persona o grupo que representa un riesgo a la seguridad. Ya conoces la definición de ciberseguridad, veamos lo que hacen los equipos de seguridad en una organización. La cibereguridad protege contra amenazas externas e internas. Una amenaza externa es alguien de fuera de la organización intentando acceder a información privada, redes o dispositivos. Una amenaza interna procede del personal antiguo o actual, proveedores externos, o socios/as de confianza. Las internas suelen ser accidentales, como cuando una persona hace clic en un enlace comprometido en un correo. Otras veces, el agente interno participa intencionalmente en actividades como el acceso no autorizado a datos o abuso de los sistemas para uso personal. Los especialistas en ciberseguridad con experiencia ayudan a las organizaciones a mitigar o reducir el impacto de estas amenazas. Los equipos de seguridad también garantizan que una organización cumpla las normativas, leyes y directrices que requieran la implementación de estándares de seguridad específicos. Garantizar que las organizaciones cumplan la normativa puede evitar multas y auditorías, al tiempo que respetan su obligación ética de proteger a sus usuarios/as. Los equipos de seguridad mantienen y mejoran la productividad. Al crear un plan de continuidad del negocio, los equipos de seguridad permiten que cada cual haga su trabajo, incluso cuando ocurre una filtración de datos. Ser conscientes de la seguridad también puede reducir gastos vinculados a los riesgos, como la recuperación de datos o el tiempo de inactividad, y evitar posibles multas. La última ventaja de la que hablaremos es mantener la confianza en la marca. Si se comprometen los servicios o los datos de sus clientes, puede disminuir la confianza en la empresa, dañar la marca y el negocio. Si sus clientes pierden la confianza, implica menos ingresos para el negocio. Repasemos ahora algunos roles comunes basados en la seguridad. Después de completar esta certificación, estos son los posibles puestos que quizás desees buscar: Especialista o analista de seguridad, especialista o analista de ciberseguridad, analista del centro de operaciones de seguridad o SOC y analista de seguridad de la información. También conocerás las responsabilidades asociadas a algunos de estos puestos de trabajo, más adelante. Como te habrás dado cuenta, el campo de la seguridad incluye muchos temas y conceptos y cada actividad que completes en este programa es un paso más hacia un nuevo empleo. ¡Sigamos aprendiendo!

La tecnología cambia rápidamente, al igual que las tácticas y técnicas que se usan en los ataques. Al tiempo que la infraestructura evoluciona, la ciberseguridad debe desarrollar continuamente sus habilidades para proteger y asegurar la información sensible. En este video, abordaremos algunas responsabilidades de un/a analista de seguridad principiante. Veamos, ¿qué hace un/a analista de seguridad? Un/a analista de seguridad se encarga de monitorear y proteger los sistemas y la información. Hablemos ahora de las tres responsabilidades principales que tiene. Empecemos por la protección de computadoras y sistemas de red. Para proteger las computadoras y los sistemas de red, un/a analista debe monitorear la red interna de una organización. Si detecta una amenaza, debe ser el primero en responder. Las y los analistas suelen participar en ejercicios para buscar puntos débiles en los sistemas de una organización. Por ejemplo, pueden contribuir en pruebas de penetración o hacking ético. El objetivo es penetrar o hackear la red interna de su propia organización para identificar vulnerabilidades y sugerir formas de reforzar la seguridad. Piénsalo así. Después de cerrar el auto, revisas las manijas de las puertas para asegurarte que nadie acceda a los objetos que guardas adentro. Las y los analistas de seguridad trabajan proactivamente para evitar que se produzcan amenazas. Una forma de hacerlo es colaborar con el departamento de TI, instalando software de prevención para identificar riesgos y vulnerabilidades. También pueden participar en el desarrollo de software y hardware, y trabajar con los equipos de desarrollo para respaldar la seguridad del producto implementando sistemas y procesos para proteger los datos. Por último, la realización periódica de auditorías de seguridad. Una auditoría de seguridad comprueba los registros, actividades y otros documentos de seguridad de una organización. Por ejemplo, un/a analista puede examinar problemas internamente, para garantizar que la información sensible, como las contraseñas, no esté disponible para todo el personal. Bien, hemos hablado de muchas cosas. Espero que te hayas hecho una idea de lo que hacen un/a analista de seguridad principiante. Las y los analistas de seguridad son una parte importante de cualquier organización. Sus tareas protegen a las pequeñas y grandes empresas, ONGs y agencias gubernamentales. También ayudan a mantener a salvo a la gente que trabaja para esas organizaciones.

Terminología común de ciberseguridad

Como aprendiste, la ciberseguridad (también conocida como seguridad cibernética) es la práctica de garantizar la confidencialidad, integridad y disponibilidad de la información mediante la protección de las redes, dispositivos y datos contra el acceso no autorizado. En esta lección, conocerás algunos términos clave utilizados en esta especialidad. Luego, encontrarás un recurso útil para mantenerte al día sobre los cambios en la terminología de ciberseguridad.

Términos y conceptos clave en ciberseguridad

Hay muchos términos y conceptos que son importantes para los/las profesionales de la ciberseguridad y conocerlos puede ayudarte a identificar mejor las amenazas que pueden perjudicar tanto a las organizaciones como a las personas. Un/a analista de seguridad o de ciberseguridad se centra en monitorear las redes en busca de infracciones. También ayuda a desarrollar estrategias para proteger una organización e investiga las tendencias de seguridad de las tecnologías de la información (TI) para mantenerse alerta y al día sobre posibles amenazas. Además, trabaja en la prevención de incidentes. Para realizar este tipo de tareas, necesitarás desarrollar tus conocimientos sobre los siguientes conceptos clave.

Cumplimiento normativo (compliance) es el proceso de adhesión a normas internas y reglamentos externos que permite a las organizaciones evitar multas, auditorías y fallos de seguridad.

Marcos de seguridad son las directrices que se utilizan para elaborar planes de seguridad que ayuden a mitigar los riesgos y las amenazas a los datos y la privacidad.

Controles de seguridad son medidas diseñadas para reducir riesgos de seguridad específicos. Se utilizan junto a los marcos de seguridad para establecer una postura de seguridad sólida.

Postura de seguridad es la capacidad de una organización para administrar su defensa de activos y datos críticos y reaccionar ante los cambios. Una fuerte postura de seguridad conduce a un menor riesgo para la organización.

Agente de amenazas, o atacante malicioso, es cualquier persona o grupo que representa un riesgo para la seguridad, que puede afectar a computadoras, aplicaciones, redes o datos.

Amenaza interna es un riesgo a la seguridad producido por una persona que pertenece o perteneció a una empresa o tiene una relación directa o de confianza con ella. Por ejemplo, si un/a empleado/a hace clic accidentalmente en un enlace de correo electrónico malicioso, o si el agente de amenazas interno realiza intencionadamente una actividad de riesgo, como acceder a los datos sin autorización.

Seguridad de la red es un conjunto de prácticas que buscan evitar accesos no autorizados a la infraestructura de red de una organización. Esto incluye datos, servicios, sistemas y dispositivos que se almacenan en la red de una organización.

Seguridad en la nube es el proceso de garantizar que los activos almacenados en la nube estén configurados o establecidos correctamente, y su acceso limitado a los/as usuarios/as autorizados/as. La nube es una red formada por un conjunto de servidores o computadoras que almacenan recursos y datos en ubicaciones físicas remotas conocidas como centros de datos a los que se puede acceder a través de Internet. La seguridad en la nube es un subcampo creciente de la ciberseguridad que se centra específicamente en la protección de este tipo de datos, aplicaciones e infraestructuras.

Programación es el proceso que permite crear un conjunto específico de instrucciones para que una computadora ejecute tareas Estas pueden incluir:

Automatización de tareas repetitivas (por ejemplo, buscar dominios maliciosos en una lista).

Revisión del tráfico web.

Alerta de actividades sospechosas.

Conclusiones clave

Comprender los términos y conceptos técnicos clave utilizados en el ámbito de la ciberseguridad te ayudará a prepararte para tu rol de analista de seguridad. Conocer estos términos te permitirá identificar amenazas, riesgos y vulnerabilidades comunes. Para explorar otros términos de ciberseguridad, visita el

glosario del Instituto Nacional de Estándares y Tecnología de Estados Unidos

, o busca glosarios de ciberseguridad fiables y de alta calidad de institutos de investigación o autoridades gubernamentales en internet. Los glosarios suelen estar disponibles en varios idiomas.

En cualquier trabajo, necesitas ciertas habilidades para tener éxito, y muchas de estas son transferibles de un puesto al siguiente. No importa en qué trabajas actualmente, es probable que ya poseas muchas de ellas. Tener una trayectoria diversa mejora tus habilidades básicas, es decir, tus perspectivas y tu experiencia personal son muy valiosas. En este video, hablaremos de las habilidades técnicas y transferibles que son muy útiles para un/a analista de seguridad. Las habilidades transferibles proceden de otras áreas y se pueden aplicar a otras profesiones, al igual que las habilidades técnicas, pero sin requerir conocimientos de herramientas, políticas y procedimientos específicos. Hablemos de las principales habilidades transferibles que tal vez ya tengas y te ayudarán como analista de seguridad. La comunicación es una habilidad transferible para un/a analista de seguridad. Con frecuencia tendrás que describir amenazas, riesgos o vulnerabilidades a personas que pueden no tener conocimientos técnicos. Por ejemplo, puedes tener que interpretar y comunicar directivas y procedimientos a otras personas. O deberás reportar tus hallazgos a tus supervisores/as, con el fin de adoptar las medidas apropiadas para proteger la organización. Otra habilidad transferible es la colaboración. Un/a analista de seguridad suele colaborar con ingenieros/as, investigadores/as forenses digitales y gerentes de programas. Por ejemplo, si estás trabajando para lanzar una nueva función de seguridad, es probable que tengas un/a gerente de proyecto, un/a ingeniero/a y un/a hacker ético en tu equipo. Un/a analista de seguridad también debe ser capaz de analizar escenarios complejos. Por ejemplo, puede necesitar hacer recomendaciones sobre cómo las distintas herramientas pueden mejorar la eficiencia y salvaguardar la red interna. La última habilidad transferible es la resolución de problemas. Detectar un problema de seguridad, diagnosticarlo y brindar soluciones es una habilidad necesaria para mantener seguras las operaciones. Entender los agentes de amenazas e identificar tendencias brinda información para manejar futuros ataques. Bien, ahora que cubrimos las principales habilidades transferibles, hablemos sobre las habilidades técnicas que debes desarrollar como analista de seguridad. Poseer conocimientos básicos en lenguajes de programación es importante, ya que puedes tener que programar para automatizar tareas e identificar mensajes de error. Al igual que al aprender un idioma, un lenguaje de programación puede parecer complicado al principio. Sin embargo, en este programa se supone que no tienes experiencia en programación, así que empezaremos desde cero y te brindaré varios ejercicios para que practiques con lenguajes como Python y SQL.

Reproduce el video desde :2:56 y sigue la transcripción2:56

Otra habilidad técnica importante es saber cómo usar herramientas de gestión de eventos e información de seguridad (SIEM). Un/a profesional de la seguridad usa las herramientas SIEM para identificar y analizar amenazas de seguridad, riesgos y vulnerabilidades. Por ejemplo, una herramienta SIEM puede avisarte que una persona desconocida accedió al sistema. En ese caso, puedes usar la informática forense para investigar el incidente. Hablemos ahora de la informática forense. Al igual que la investigación y la ciencia forense del sistema penal, la investigación forense digital trata de identificar, analizar y preservar las pruebas delictivas dentro de las redes, computadoras y dispositivos electrónicos. Ten en cuenta que es posible que ya poseas algunas de estas habilidades básicas. Y si no tienes las técnicas, no pasa nada. Este programa está diseñado para ayudarte a adquirir esas habilidades. Por ejemplo, en los siete años en los que trabajé en ciberseguridad, descubrí que debemos tener curiosidad intelectual y motivación para seguir aprendiendo y tener éxito. Personalmente, dedico tiempo de forma periódica para profundizar en Python y SQL, con el fin de satisfacer las demandas de los proyectos en los que trabajo. Podrás aprender Python y SQL más adelante. A lo largo del programa, adquirirás los conocimientos y habilidades necesarias para trabajar en ciberseguridad.

Habilidades transferibles y técnicas en ciberseguridad

Anteriormente, aprendiste que las y los analistas en ciberseguridad necesitan desarrollar ciertas habilidades básicas para tener éxito en el ejercicio de su profesión. Las habilidades transferibles son competencias de otras áreas de estudio o práctica que pueden aplicarse a diferentes carreras. Las habilidades técnicas también pueden aplicarse a varias profesiones; sin embargo, normalmente requieren el conocimiento de herramientas, procedimientos y políticas específicas. En esta lección profundizarás tanto en las habilidades transferibles como en las técnicas.

Habilidades transferibles

Probablemente hayas desarrollado habilidades transferibles a lo largo de tu vida; algunas de ellas te ayudarán a prosperar como profesional en ciberseguridad. Por ejemplo:

Comunicación: como analista de ciberseguridad, deberás comunicarte y colaborar con otras personas. Comprender las preguntas o inquietudes de los/las demás y comunicar la información con claridad a personas con conocimientos técnicos y no técnicos te ayudará a mitigar los problemas de seguridad rápidamente.

Resolución de problemas: una de tus principales tareas como analista de ciberseguridad será identificar y resolver problemas de forma proactiva. Puedes hacerlo reconociendo patrones de ataque y determinando la solución más eficaz para minimizar el riesgo. No tengas miedo de probar cosas nuevas y ten en cuenta que es difícil encontrar una solución perfecta a un problema, y es probable que te tengas que conformar con un punto intermedio.

Gestión del tiempo: tener sentido de la urgencia y priorizar adecuadamente las tareas es esencial en el campo de la ciberseguridad. Por lo tanto, una gestión eficaz del tiempo te ayudará a minimizar los posibles daños y riesgos para los activos y datos críticos. Además, será importante que sepas priorizar las tareas y enfocarte en el tema más urgente.

Mentalidad de crecimiento: la ciberseguridad es un sector en plena evolución, por lo que una habilidad transferible importante es la voluntad de aprender. La tecnología avanza rápido, ¡y eso es positivo! Esto no significa que tengas que aprender todo, pero sí que tendrás que seguir haciéndolo a lo largo de tu carrera. Afortunadamente, podrás aplicar gran parte de lo que aprendas en este programa a tu desarrollo profesional continuado.

Diversidad de perspectivas: la única manera de llegar lejos es trabajando conjuntamente con otras personas. El respeto mutuo y los diversos puntos de vista te permitirán encontrar mejores soluciones a los problemas de seguridad.

Habilidades técnicas

Hay muchos conocimientos técnicos que te ayudarán a tener éxito en el campo de la ciberseguridad. Aprenderás y practicarás estas habilidades a medida que avances en el programa de certificación. Estos son algunos conceptos y herramientas que tendrás que entender y utilizar:

Lenguajes de programación: comprender cómo usar los lenguajes de programación te permitirá automatizar tareas que de otro modo requerirían mucho tiempo, como por ejemplo, la búsqueda de datos para identificar posibles amenazas o la organización y el análisis de información para identificar patrones relacionados con problemas de seguridad.

Sistemas de detección de intrusiones (IDS): las y los analistas en ciberseguridad utilizan los IDS para monitorear la actividad del sistema y las alertas de posibles intrusiones. Es importante familiarizarse con ellos porque son una herramienta clave para proteger activos y datos. Por ejemplo, puedes usar un IDS para monitorear las redes en busca de signos de actividad maliciosa, como el acceso no autorizado a una red.

Conocimiento del panorama de amenazas: es vital estar al tanto de las tendencias actuales relacionadas con los agentes de amenazas, el malware o las metodologías. Este conocimiento permite a los equipos de ciberseguridad construir defensas más sólidas contra las tácticas y técnicas de los agentes de amenazas. Si te mantienes al día sobre las tendencias y patrones de ataque, serás capaz de reconocer cuando surgen nuevos tipos de amenazas, como, por ejemplo, una nueva variante de ransomware.

Respuesta a incidentes: las y los analistas en ciberseguridad deben poder seguir las políticas y procedimientos establecidos para responder adecuadamente a los incidentes. Por ejemplo, poder iniciar el proceso de respuesta a incidentes ante un posible ataque de malware lo que podría implicar tener que llevar a cabo una investigación para identificar el problema de raíz y establecer formas de remediarlo.

CompTIA Security+

Además de adquirir habilidades que te ayudarán a tener éxito como profesional de la ciberseguridad, el Certificado en Ciberseguridad de Google te ayuda a prepararte para el

examen CompTIA Security+

, la certificación líder en la industria. Obtendrás una doble credencial cuando completes ambos exámenes, que podrás compartir con posibles empresas empleadoras. Tras completar los ocho cursos del Certificado en Ciberseguridad de Google, obtendrás un descuento del 30% para el examen CompTIA Security+ y materiales de práctica adicionales.

Conclusiones clave

Comprender las ventajas de las habilidades técnicas y transferibles, puede ayudarte a preparar tu ingreso al mercado laboral de la ciberseguridad. A lo largo de este programa, tendrás múltiples oportunidades para desarrollar estas y otras habilidades clave en ciberseguridad. Como mencionamos, las y los profesionales de la seguridad protegen muchos activos físicos y digitales. Estas habilidades son buscadas por las organizaciones y entidades gubernamentales, porque deben gestionar riesgos. Hablemos de por qué es tan importante la ciberseguridad. Es esencial para garantizar la continuidad del negocio y el estatus ético de una organización. Hay implicaciones legales y morales para mantener la seguridad de una organización. Una filtración de datos, por ejemplo, afecta a toda la gente asociada a la organización. Esto se debe a que las pérdidas o fugas de datos pueden dañar la reputación de una organización, así como la vida y reputación de sus clientes. Con medidas de seguridad sólidas, las organizaciones aumentan la confianza de las personas, lo que permite que crezcan sus finanzas y su reputación. Como mencionamos, las organizaciones no son las únicas que sufren por una filtración de datos. Proteger los datos de usuarios/as, clientes y proveedores es una parte importante para prevenir incidentes que puedan exponer información de identificación personal. La información de identificación personal, o PII, es cualquier información de la que se pueda deducir la identidad de una persona. PII incluye el nombre, fecha de nacimiento, dirección física, número de teléfono, dirección de correo electrónico, protocolo de Internet, o dirección IP e información similar de una persona. La información de identificación personal sensible, o SPII, es un tipo específico de PII que se rige por pautas de manejo más estrictas y puede incluir números de seguridad social, datos médicos, financieros y biométricos, como el reconocimiento facial. El robo de datos SPII es potencialmente mucho más perjudicial para una persona que el robo de datos PII.

Los datos PII y SPII son activos clave que buscará un agente de amenazas si una organización sufre una filtración. Si la información de identificación personal se pone en riesgo, se filtra o se roba, la suplantación de la identidad es la principal preocupación. La suplantación de la identidad consiste en robar datos personales para cometer fraude haciéndose pasar por la víctima. Su objetivo principal es el beneficio económico. Vimos varias razones por las que la seguridad es importante. Las empresas necesitan analistas de seguridad como tú para cubrir la demanda actual y futura para proteger los datos, productos y personas, garantizando al mismo tiempo la confidencialidad, integridad y el acceso seguro a la información. Por esto, la Oficina de Estadísticas Laborales de EE. UU. espera que la demanda de profesionales de la seguridad aumente más del 30% para 2030.

Exploración: mantener la seguridad de las organizaciones

Pensamiento analítico

Los analistas de seguridad suelen utilizar el pensamiento analítico, que significa pensar detenida y minuciosamente. Los analistas utilizan esta habilidad cuando monitorean y protegen los sistemas informáticos y de red, responden a posibles amenazas, definen los privilegios del sistema y determinan formas de mitigar los riesgos.

Colaboración

Colaborar significa trabajar con las partes interesadas y otros miembros del equipo. Los analistas de seguridad a menudo utilizan esta habilidad cuando responden a una amenaza activa. Trabajarán con otras personas para bloquear el acceso no autorizado y garantizar el restablecimiento de los sistemas comprometidos.

Prevención de malware

Cuando se identifica una amenaza o vulnerabilidad específica, un analista puede instalar un software de prevención, que trabaja para prevenir proactivamente que se produzca una amenaza. Dado que el malware está diseñado para dañar dispositivos oredes, su prevención es esencial.

Comunicación

A medida que un analista previene y encuentra amenazas, riesgos o vulnerabilidades, documenta e informa de sus hallazgos. Un informe podría detallar los intentos de proteger los sistemas, comprobar los puntos débiles u ofrecer soluciones para mejorar el sistema. A la hora de comunicar los hallazgos, es importante tener habilidades sólidas de comunicación.

Comprensión de los lenguajes de programación

En ocasiones, los analistas pueden trabajar con equipos de desarrollo de software para analizar y respaldar la seguridad, instalar software y establecer los procesos adecuados. Cuando un analista participa en proyectos de desarrollo de software, puede resultarle útil comprender los lenguajes de programación.

Uso de herramientas SIEM

Cuando los analistas de seguridad necesitan revisar las vulnerabilidades, llevan a cabo una auditoría de seguridad periódica. Se trata de una revisión de los registros, actividades y documentos relacionados de una organización. Durante las auditorías, las herramientas de gestión de eventos e información de seguridad (SIEM) ayudan a los analistas a comprender mejor las amenazas, riesgos y vulnerabilidades de seguridad.

Ahora que ya sabes qué es la ciberseguridad y cómo las y los profesionales en este campo protegen a las personas y las organizaciones, es el momento de considerar tu propio rol en ciberseguridad. Imagina que es tu primer día como profesional y piensa en lo siguiente:

¿Qué problemas de ciberseguridad estás resolviendo?

Estoy resolviendo problemas relacionados con la protección de datos sensibles de mi organización, como evitar ataques de hackers, detener el malware y asegurar que nuestras redes sean seguras. También me enfoco en identificar y corregir vulnerabilidades en nuestros sistemas.

¿Cómo proteges a tu organización?

Protejo a mi organización implementando y manteniendo sistemas de seguridad robustos, como firewalls y antivirus. Realizo auditorías de seguridad regulares, entreno a los empleados en buenas prácticas de seguridad y monitorizo nuestras redes para detectar cualquier actividad sospechosa.

¿Cómo proteges a las personas?

Protejo a las personas asegurándome de que sus datos personales estén seguros y que sus comunicaciones sean privadas. También educo a los usuarios sobre cómo reconocer y evitar fraudes y phishing, y les doy herramientas y consejos para mantener sus propias cuentas seguras.

¿Qué es lo más emocionante de tu día?

Lo más emocionante de mi día es descubrir y neutralizar una amenaza potencial antes de que cause daño. También disfruto mucho cuando implemento una nueva medida de seguridad que sé que mejorará significativamente nuestra protección y ver cómo contribuye a mantener a todos a salvo.

Felicitaciones por completar la primera sección de este curso. Rapasemos rápidamente lo que vimos hasta ahora, antes de seguir. Definimos la ciberseguridad y presentamos las ventajas de implementar la seguridad en una organización. Luego hablamos sobre responsabilidades laborales, como gestión de amenazas e instalación de software preventivo. Presentamos algunas habilidades básicas importantes, como la colaboración y la informática forense. Terminamos hablando del valor de la seguridad y cómo respalda funciones empresariales cruciales. Espero que hayas comprendido mejor la ciberseguridad. Si crees que necesitas repasar antes de seguir, puedes retroceder y revisar cualquier contenido. Al aprender lo básico, estás sentando los cimientos de tu carrera en ciberseguridad. Próximamente, veremos algunos ataques que modelaron el sector de la seguridad. Estoy encantada de acompañarte en este recorrido.

Felicitaciones por completa

Términos y definiciones del curso 1, semana 1

Agente de amenaza: Persona o grupo de personas que representa una amenaza intencional para computadoras, aplicaciones o redes.

Amenaza: Cualquier circunstancia o evento que pueda afectar los activos de manera negativa.

Amenaza interna: Riesgo a la seguridad producido por una persona que pertenece o perteneció a una empresa o tiene una relación directa o de confianza con ella.

Ciberseguridad (o seguridad cibernética): Práctica de garantizar la confidencialidad, integridad y disponibilidad de la información mediante la protección de redes, dispositivos, personas y datos contra el acceso no autorizado o la explotación delictiva.

Habilidades técnicas: Competencias que requieren conocimiento de herramientas, procedimientos y políticas específicas.

Habilidades transferibles: Competencias de otras áreas que pueden aplicarse a diferentes carreras.

Información de identificación personal (PII por sus siglas en inglés): Cualquier información que pueda usarse para deducir la identidad de una persona.

Información de identificación personal sensible (SPII por sus siglas en inglés): Tipo específico de Información de identificación personal que se rige por pautas de manejo más estrictas.

Seguridad de redes: Práctica de evitar accesos no autorizados a la infraestructura de red de una organización.

Te damos la bienvenida nuevamente. Cuando se trata de seguridad, hay mucho que aprender, y me encanta ser parte de este viaje. Este es un gran momento para aprender sobre seguridad. El haber aprendido acerca de los hackeos internacionales que afectan tanto a empresas privadas como a organizaciones gubernamentales me inspiró a trabajar en seguridad, porque me di cuenta de lo dinámico e importante que es esta área. Una razón por la que hay tantos puestos en el área de seguridad hoy en día tiene que ver con ataques que sucedieron en los años 80 y 90. Décadas después, las/los profesionales de seguridad continúan trabajando activamente para proteger las organizaciones y personas de variaciones de estos ataques informáticos. En esta sección del curso, analizaremos virus y software malicioso y presentaremos el concepto de ingeniería social. Luego, discutiremos acerca de cómo la era digital marcó el comienzo de una nueva era de agentes de amenaza. Conocer la evolución de cada ataque es clave para protegerse contra futuros ataques. Por último, daremos una visión general de ocho dominios de seguridad. A continuación, vamos a viajar en el tiempo, para explorar algunos de los virus, filtraciones de datos y ataques de software malicioso que ayudaron a dar forma a la industria tal como la conocemos hoy en día.

La industria de la seguridad está en constante evolución, pero muchos ataques actuales no son del todo nuevos. A menudo, las/los atacantes alteran o mejoran métodos anteriores. Comprender los ataques pasados puede orientarnos acerca de cómo manejar o investigar incidentes en tu trabajo como analista de seguridad. Primero, repasemos un par de términos clave que te ayudarán a entender los ataques que analizaremos. Un virus informático es un código malicioso escrito para interferir con operaciones informáticas y causar daños a los datos y el software. El virus se adhiere a programas o documentos en una computadora. Luego se propaga e infecta una o más computadoras en una red. Un gusano es un tipo de virus informático que puede duplicarse y propagarse por su cuenta, sin participación humana. Hoy en día, los virus son más conocidos como software malicioso, que es software diseñado para dañar dispositivos o redes. Hablaremos de dos ataques tempranos de software malicioso: el virus Brain y el gusano Morris. Fueron creados por desarrolladores de software malicioso para cumplir tareas específicas. Sin embargo, los desarrolladores subestimaron el impacto que su malware tendría y la cantidad de computadoras que este iba a infectar. Profundicemos un poco más en estos ataques y analicemos cómo ayudaron a dar forma a la ciberseguridad como la conocemos hoy en día. En 1986, los hermanos Alvi crearon el virus Brain, si bien la intención del virus era rastrear copias ilegales de software médico y evitar las licencias piratas, lo que el virus terminó haciendo fue inesperado. Una vez que una persona usaba una copia pirata del software, el virus infectaba esa computadora. Luego, cualquier disco que se insertara en la computadora también se infectaba. El virus se propagaba a una computadora nueva cada vez que alguien usaba uno de los discos infectados. Desapercibido, el virus se propagó por todo el mundo en un par de meses. Aunque la intención no era destruir datos o hardware, el virus ralentizó la productividad e impactó significativamente en las operaciones comerciales.

Reproduce el video desde :2:16 y sigue la transcripción2:16

El virus Brain alteró radicalmente la industria informática. Destacó la necesidad de un plan para mantener la seguridad y productividad.

Reproduce el video desde :2:26 y sigue la transcripción2:26

Como analista de seguridad, seguirás y mantendrás estrategias implementadas para asegurar que tu organización tenga un plan para mantener la seguridad de sus datos y personas. Otro ataque a computadoras influyente fue el gusano Morris. En 1988, Robert Morris desarrolló un programa para calcular el tamaño de Internet. El programa rastreó la web y se instaló en otras computadoras para calcular el número de equipos conectados a Internet. Parece sencillo, ¿verdad? Sin embargo, el programa no logró hacer un seguimiento de las computadoras que ya había puesto en riesgo, y seguía reinstalándose hasta que las computadoras se quedaron sin memoria y colapsaron. Cerca de 6000 computadoras se vieron afectadas, lo cual representaba el 10% de Internet en ese momento. Este ataque costó millones de dólares en daños debido a alteraciones en las empresas y a los esfuerzos necesarios para eliminar el gusano. Después del gusano Morris, se establecieron equipos de respuesta ante emergencias informáticas, conocidos como CERT®, para responder a incidentes de seguridad informática. Los CERT aún existen, pero su lugar en la industria de la seguridad se amplió, e incluye más responsabilidades. Más adelante en este programa, aprenderás más acerca de las funciones básicas de estos equipos de ciberseguridad, y podrás practicar con herramientas de detección y respuesta. Los primeros ataques jugaron un papel clave a la hora de dar forma a la industria de ciberseguridad actual. Y a continuación, analizaremos cómo los ataques evolucionaron en la era digital.

Con la expansión de una Internet confiable y de alta velocidad, el número de computadoras conectadas a ella aumentó muchísimo. Como el software malicioso puede propagarse por Internet, los agentes de amenaza ya no necesitaban de discos físicos para propagar virus. Para comprender mejor los ataques en la era digital, analizaremos dos ataques notables que dependieron de Internet: el ataque LoveLetter y la fuga de información de Equifax.

Reproduce el video desde ::29 y sigue la transcripción0:29

En el año 2000, Onel De Guzmán creó el malware LoveLetter para robar credenciales de inicio de sesión en Internet. Este ataque se extendió rápidamente y se aprovechó de personas que no habían aprendido a sospechar de los correos electrónicos no deseados. Los/las usuarios/as recibieron un correo con un "Te amo" en el asunto. Cada correo contenía un archivo adjunto titulado "Carta de amor para ti". Al abrir el archivo adjunto, el software malicioso escaneaba la libreta de direcciones de un/a usuario/a. Luego, se enviaba automáticamente a cada persona en la lista e instalaba un programa para recopilar información de usuario y contraseñas. Las personas pensaban que recibían un correo de un amigo, pero en realidad era software malicioso. LoveLetter terminó infectando a 45 millones de computadoras en todo el mundo, y se cree que causó daños por más de 10 mil millones de dólares.

Reproduce el video desde :1:22 y sigue la transcripción1:22

El ataque de LoveLetter es el primer ejemplo de ingeniería social. La ingeniería social es una manipulación técnica que explota el error humano para obtener información privada, acceso u objetos de valor. Luego de LoveLetter, los atacantes entendieron el poder de la ingeniería social. El número de ataques de ingeniería social aumenta con cada nueva aplicación de redes sociales que permite acceso público a los datos de personas. Hoy se prioriza muchísimo la conveniencia sobre la privacidad. El resultado de este cambio evolutivo es que estas herramientas pueden derivar en una vulnerabilidad mayor si no se usan apropiadamente. Como profesional de la seguridad, tu rol es identificar y gestionar un uso inapropiado de la tecnología que pueda poner a tu organización y todas las personas asociadas a ella en riesgo. Una forma de proteger a tu organización son las capacitaciones internas regulares. Como futuro analista de seguridad, puede que se te pida que las dirijas o que participes de ellas. Hoy en día, es común que se capacite a los/las empleados/as acerca de cómo identificar ataques de ingeniería social. Específicamente el phishing a través de correos que reciben. El phishing es el uso de comunicaciones digitales para engañar personas y provocar que revelen datos confidenciales o para propagar software malicioso. Ahora, hablemos de la fuga de información de Equifax. En 2017, atacantes se infiltraron con éxito en la agencia de informes de crédito Equifax. Esto dio lugar a una de las fugas de información más grandes de las que se tenga registro. Se robaron más de 143 millones de registros de clientes, y la fuga afectó a casi el 40% de todos/as los/las estadounidenses. Los registros contenían información personal identificable como números de seguridad social, fechas de nacimiento, licencias de conducir, domicilios y números de tarjetas de crédito. Desde el punto de vista de la seguridad, la fuga se produjo debido a múltiples fallas por parte de Equifax. No fue una única vulnerabilidad que los atacantes aprovecharon, sino varias. La empresa no tomó las medidas necesarias para reparar múltiples vulnerabilidades conocidas en los meses previos a la fuga. Al final, Equifax llegó a un acuerdo con el gobierno de los EE.UU. y pagó más de 575 millones de dólares para resolver reclamos de los clientes y cubrir las multas requeridas. Si bien hubo otras fugas de información antes y después de Equifax, el importante acuerdo con el gobierno de EE.UU. alertó a las empresas del impacto financiero de una fuga y de la necesidad de implementar medidas preventivas. Estos son solo un par incidentes conocidos que moldearon la industria de la seguridad. Saber de ellos te ayudará en tu carrera de ciberseguridad. Comprender los diferentes tipos de malware y los ataques de ingeniería social te permitirá comunicar acerca de los riesgos de seguridad en futuras entrevistas de trabajo. Como futuro profesional de seguridad, adaptarte y formarte constantemente acerca de las tácticas y técnicas de agentes de amenaza será parte de tu trabajo. Al observar tendencias, patrones y metodologías similares, tal vez puedas identificar una posible fuga y limitar daños futuros. Por último, comprender cómo la seguridad afecta la vida de las personas es un buen recordatorio de por qué el trabajo que harás es tan importante.

Ataques comunes y su eficacia

Anteriormente, aprendiste acerca de los ataques pasados y actuales que ayudaron a moldear el campo de la ciberseguridad. Estos incluyeron el ataque LoveLetter, también conocido como virus ILOVEYOU, y el gusano Morris. Uno de sus resultados fue el desarrollo de equipos de respuesta, que ahora se denominan más comúnmente equipos de respuesta ante incidentes de seguridad informática (CSIRT, por sus siglas en inglés). En esta lectura conocerás más detalles sobre los métodos de ataque más comunes. Si te familiarizas con los distintos métodos de ataque y las tácticas y técnicas cambiantes que utilizan los agentes de amenaza, podrás proteger mejor a las organizaciones y a las personas.

Phishing

Phishing es el uso de comunicaciones digitales en las que se suplanta la identidad de una persona o empresa con el objetivo de engañar a otras personas para que revelen datos confidenciales o implementen un software malicioso.

Algunos de los tipos más comunes de ataques de phishing actuales son:

Compromiso del correo electrónico empresarial (BEC): el agente de amenaza envía un mensaje de correo electrónico que parece provenir de una fuente conocida, para efectuar una solicitud aparentemente legítima de información o intentar que realice una acción, con el fin de obtener un beneficio financiero.

Phishing localizado (Spear phishing): un tipo de phishing focalizado en el que se envía un correo electrónico malicioso a un/a usuario/a o a un grupo de usuarios/as específicos/as, que parece provenir de una fuente confiable.

Ataque “caza de ballenas” (Whaling): un tipo de phishing localizado mediante el cual los agentes de amenaza buscan acceder a los datos confidenciales de ejecutivos/as de una empresa.

Vishing: un tipo de estafa por suplantación de identidad en la que se busca obtener información sensible a través de una llamada telefónica.

Smishing: ataque de phishing por SMS que implica el uso de mensajes de texto para engañar a los/las usuarios/as, con el fin de obtener información confidencial o hacerse pasar por una fuente conocida.

Software malicioso

El software malicioso es un software diseñado para dañar dispositivos o redes. El propósito principal de quienes realizan el ataque es obtener dinero o, en algunos casos, información que pueda utilizarse en contra de una persona, una organización o un territorio.

Algunos de los tipos más comunes de ataques de software malicioso actuales son:

Virus informático: un código malicioso creado para interferir con las operaciones de la computadora y dañar datos, software y hardware. El virus se instala en programas o documentos de una computadora y luego, se propaga e infecta una o más computadoras en una red.

Gusano: un software malicioso que puede duplicarse y propagarse por sí mismo en los sistemas.

Ransomware (secuestro de datos): un ataque malicioso en el que los agentes de amenaza cifran los datos de una organización y exigen un pago (rescate) para restablecer el acceso a ellos.

Spyware: un tipo de software malicioso que se usa para recabar y vender información sin consentimiento. El spyware se puede usar para acceder a dispositivos, lo cual permite a los agentes de amenaza recopilar datos personales, como correos electrónicos, mensajes de texto, grabaciones de voz e imagen y ubicaciones de índole privada.

Ingeniería social

La ingeniería social es una técnica de manipulación que aprovecha errores humanos para obtener información privada, acceso a sistemas o bienes de valor. A menudo, los errores humanos se deben al exceso de confianza en alguien. La misión de un agente de amenaza que actúa como ingeniero social es crear un entorno de confianza falso y mentir para aprovecharse del mayor número posible de gente.

Algunos de los tipos más comunes de ataques de ingeniería social actuales son:

Ataque de suplantación de identidad en redes sociales (Phishing en redes sociales): un tipo de ataque en el que el agente de amenaza contacta a la víctima en alguna red social, con el fin de robar información personal o tomar el control de la cuenta.

Ataque de “agujero de agua”: un agente de amenaza ataca un sitio web visitado con frecuencia por un grupo específico de usuarios/as.

Cebo USB: un agente de amenaza deja estratégicamente una unidad USB que contiene software malicioso para que un/a empleado/a la encuentre y la instale, con el fin de causar la infección involuntaria de una red.

Ingeniería social física: un agente de amenaza se hace pasar por una persona ligada a la empresa para obtener acceso no autorizado a una ubicación física.

Principios de la ingeniería social

La ingeniería social es asombrosamente eficaz porque las personas suelen ser confiadas y tienen muy arraigado el respeto a la autoridad. La cantidad de ataques de ingeniería social aumenta a medida que crece la cantidad de aplicaciones de redes sociales que permiten el acceso público a los datos de las personas. Aunque compartir datos personales (como tu ubicación o fotos) puede ser conveniente, también plantea un riesgo.

Los motivos por los cuales los ataques de ingeniería social son eficaces son:

Autoridad: los agentes de amenaza se hacen pasar por personas con autoridad porque los individuos suelen respetarlas.

Intimidación: los agentes de amenaza utilizan tácticas de hostigamiento, como asustar a las víctimas para que sigan sus órdenes.

Consenso/prueba social: como las personas a veces hacen cosas convencidas de que otras también las hacen, los agentes de amenaza utilizan esta confianza en los demás para dar una impresión de legitimidad. Por ejemplo, para obtener acceso a datos privados, un agente de amenaza puede decir a un/a empleado/a que otros miembros de la empresa ya le han otorgado el acceso en otras ocasiones.

Escasez: el agente de amenaza le da a entender a la persona que existe disponibilidad limitada de ciertos bienes o servicios, para convencerla de hacer algo.

Familiaridad: los agentes de amenaza establecen falsos lazos emocionales con los/las usuarios/as de quienes desean aprovecharse,para lograr su objetivo.

Confianza: los agentes de amenaza establecen una relación afectiva con los/las usuarios/as, que les permite aprovecharse de ellos con el paso del tiempo. Hacen uso de esta relación para ganarse la confianza de la víctima y acceder a su información personal.

Urgencia: un agente de amenaza persuade a las personas para que respondan con rapidez sin hacer preguntas.

Conclusiones clave

En esta lectura, aprendiste acerca de algunos ataques comunes y sus consecuencias, y sobre la ingeniería social y los motivos de su éxito. Si bien esta es solo una breve introducción a los tipos de ataques, durante el programa tendrás muchas oportunidades de profundizar aún más en la forma de identificar y defenderte de los ataques de ciberseguridad.

Software malicioso (malware)

Definición

Programa diseñado para dañar dispositivos o redes.

Virus

Programa malicioso que modifica otros programas informáticos insertando su propio código para dañar y/o destruir datos

Gusano

Software malicioso que se reproduce por sí mismo y se propaga a través de los sistemas y redes.

Secuestro de datos (Ransomware)

Definición

Ataque malicioso que consiste en cifrar los datos de una organización para exigir el pago de un rescate para restablecer el acceso a ellos

Spyware

Definición

Software malicioso que se usa para recabar y vender información sin el consentimiento de su propietario.

Phishing (suplantación de identidad)

Definición

Uso de comunicaciones digitales en las que se suplanta la identidad de una persona o empresa con el objetivo de engañar a otras personas para que revelen datos confidenciales o implementen un software malicioso

Phishing localizado (Spear phishing)

Definición

Ataque por correo electrónico malicioso dirigido a una persona o grupo de personas específico que parece provenir de una fuente confiable

Ataque de caza de ballenas (Whaling)

Definición

Tipo de ataque de suplantación de identidad dirigido específicamente a personas de alto rango de una organización

Compromiso de correo electrónico empresarial (BEC)

Definición

Tipo de ataque de suplantación de identidad, en el que un agente de amenaza se hace pasar por una persona conocida por la víctima e intenta que realice una acción, como enviar dinero u otorgar datos confidenciales de la compañía

Vishing

Definición

Tipo de estafa por suplantación de identidad en la que se busca obtener información sensible a través de una llamada telefónica

Ingeniería social

Definición

Técnica de manipulación que busca engañar a las personas con el fin de que revelen información o realicen determinadas acciones

Ataque de suplantación de identidad en redes sociales (Phishing en redes sociales)

Definición

Tipo de ataque en el que el agente de amenaza contacta a la víctima en alguna red social, con el fin de robar información personal o tomar el control de la cuenta

Ataque de “agujero de agua” (watering hole)

Definición

Tipo de ataque en el que un agente de amenaza compromete un sitio web visitado con frecuencia por un grupo específico de usuarios

Ingeniería social física

Definición

Ataque en el que un agente de amenaza se hace pasar por una persona ligada a la empresa para obtener acceso no autorizado a una ubicación física

Cebo USB (USB Baiting)

Definición

Ataque que consiste en incluir un software malicioso (malware) en una memoria USB para que una persona la encuentre e infecte involuntariamente una red, al utilizarla

Hola, mi nombre es Sean. Soy Gerente Técnico de Programas en Google Workspace. Tengo 30 años de experiencia en ciberseguridad, dentro del espacio de seguridad de seis industrias diferentes. Durante tu primera fuga de datos, lo más importante que debes hacer

Reproduce el video desde ::24 y sigue la transcripción0:24

es mantener la calma. Todos a tu alrededor enloquecerán. Si estás en el equipo de seguridad y estás gestionando el incidente, debes ser la persona más tranquila del lugar. Sé esa persona que tiene la pausa en la conversación. Alguien podría estar decir algo así como: "¿Sabes lo que está pasando?" "Claro que sí". Creo que la fuga de información más grande que tuve fue una llamada telefónica. Un ingeniero de otra financiera compró un servidor en eBay. Al encender ese servidor, resulta que no se había borrado. Tenía 20 millones de registros de tarjetas de crédito. Eso nos hizo dar cuenta de que no habíamos controlado cómo terceros, porque estábamos tercerizando centros de datos, limpiaban los servidores que ya no usábamos. Lo primero que hay que hacer es contener la fuga. Si todavía tienes hemorragias de datos, revisas tu progresión para detenerlas. Si eso significa apagar un servidor, un centro de datos, las comunicaciones o lo que sea que sirva para detener la pérdida de datos esa es tu prioridad número uno. Tu trabajo como gestor/a de incidentes, o como alguien que trabaja en una fuga, es detener dicha fuga y luego investigarla. Ejecutar la gestión de incidentes mediante un plan es lo más importante que una persona de nivel inicial debe tener en cuenta.

Así como evolucionan las tácticas de amenaza, también lo hacen los roles de las/los profesionales de ciberseguridad. Comprender bien los conceptos de seguridad básicos te ayudarán a crecer en esta área. Una forma de entender mejor estos conceptos básicos es organizarlos en categorías, llamadas dominios de seguridad. A partir de 2022, el CISSP definió ocho dominios para organizar el trabajo de las/los profesionales de ciberseguridad. Es importante entender que están relacionados, y que las fallas en un dominio pueden tener consecuencias negativas en toda una organización. También es importante entenderlos porque eso puede ayudarte a comprender mejor tus objetivos profesionales y tu rol dentro de una organización. A medida que aprendas más sobre los elementos de cada dominio, puede atraerte más el trabajo que involucra uno de ellos, que los demás. Este dominio puede convertirse en un camino para explorar aún más. El CISSP define ocho dominios en total, y analizaremos todos ellos entre este video y el siguiente. En este video, cubriremos los cuatro primeros: gestión de riesgos y seguridad, seguridad de los activos, arquitectura e ingeniería de seguridad, y seguridad de la comunicación y la red. Empecemos por el primer dominio: gestión de riesgos y seguridad. Este se centra en definir metas y objetivos de seguridad, mitigación de riesgos, cumplimiento, continuidad del negocio y la ley. Por ejemplo, las/los analistas de seguridad pueden tener que actualizar las políticas de una empresa relacionadas con la información de salud privada si se hace un cambio a una regulación de cumplimiento federal como la Ley de Transferencia y Responsabilidad de Seguros Médicos, o HIPAA. El segundo dominio es la seguridad de los activos. Este se centra en la seguridad de activos digitales y físicos. También se relaciona con el almacenamiento, mantenimiento, retención y destrucción de datos. Al trabajar con este dominio, las/los analistas de seguridad podrían tener la tarea de asegurarse de que los equipos viejos se eliminen y destruyan adecuadamente, incluido todo tipo de información confidencial. El tercer dominio es la ingeniería y arquitectura de seguridad. Este se centra en optimizar la seguridad de los datos al asegurarse de que las herramientas, sistemas y procesos efectivos estén en su lugar. Como analista de seguridad, quizá se te pida configurar un firewall. Un cortafuegos es un dispositivo que monitorea y filtra el tráfico que entra y sale de la red informática. Configurar un cortafuegos correctamente ayuda a prevenir ataques que podrían afectar la productividad. El cuarto dominio de seguridad es comunicación y seguridad de la red. Este se centra en la gestión y seguridad de las redes físicas y las comunicaciones inalámbricas. Como analista de seguridad, tal vez se te pida que analices el comportamiento de los/las usuarios/as dentro de tu organización. Imagina que descubres que los/las usuarios/as se conectan a puntos de acceso inalámbricos no seguros. Esto podría exponer a la organización y sus empleados/as a ataques. Para garantizar que las comunicaciones sean seguras, crearías una política de red para prevenir y mitigar la exposición. Mantener la seguridad de una organización es un esfuerzo de equipo, y tiene muchas partes móviles. Como analista de nivel inicial, seguirás desarrollando tus habilidades aprendiendo a mitigar los riesgos y así mantener seguras a personas y datos. No tienes que ser un/a experto/a en todos los dominios, pero tener un entendimiento básico de ellos te ayudará en tu trayectoria como profesional de la ciberseguridad. ¡Vas muy bien! Acabamos de presentar los cuatro primeros dominios de seguridad, y en el próximo video, analizaremos cuatro más. ¡Hasta pronto!

Te damos la bienvenida nuevamente. En el último video, te presentamos los cuatro primeros dominios de seguridad. En este video, te presentaremos los siguientes cuatro dominios de seguridad: gestión de accesos e identidad, evaluación de seguridad y pruebas, operaciones de seguridad y seguridad de desarrollo de software. Familiarizarte con estos dominios te permitirá navegar por el complejo mundo de la ciberseguridad. Los dominios describen y organizan cómo las/los profesionales de ciberseguridad trabajan en equipo. Dependiendo de la organización, los roles de analista pueden ubicarse en la intersección de múltiples dominios o enfocarse en un dominio en específico. Saber dónde encaja un rol en particular dentro del panorama de seguridad te ayudará en entrevistas laborales y a la hora de trabajar en un equipo de seguridad. Pasemos al quinto dominio: gestión de acceso e identidad. La gestión de acceso e identidad se enfoca en mantener seguros los datos al garantizar que se sigan políticas establecidas para controlar y administrar activos físicos, como espacios de oficina, y activos lógicos, como redes y aplicaciones. Validar las identidades de empleados/as y documentar roles de acceso es fundamental para resguardar la seguridad digital y física de la organización. Por ejemplo, como analista de seguridad, quizá se te asigne la configuración de la tarjeta de acceso a edificios de los/las empleados/as. El sexto dominio es la evaluación de seguridad y pruebas. Este dominio se centra en realizar pruebas de control de seguridad, recolectar y analizar datos y realizar auditorías de seguridad para monitorear riesgos, amenazas y vulnerabilidades. Las/los analistas de seguridad pueden realizar auditorías periódicas de permisos de usuario para asegurarse de que tengan el nivel de acceso correcto. Por ejemplo, el acceso a la información de la nómina suele limitarse a ciertos/as empleados/as, así que se les puede pedir a las/los analistas que auditen permisos regularmente para asegurarse de que ninguna persona no autorizada pueda ver los salarios de los/las empleados/as. El séptimo dominio es el de operaciones de seguridad. Este se dedica a realización de investigaciones y la implementación de medidas preventivas. Imagina que tú, como analista de seguridad, recibes una alerta de que un dispositivo desconocido se conectó a tu red interna. Deberás seguir las políticas y procedimientos de la organización para detener rápidamente la potencial amenaza. El octavo y último dominio es seguridad de desarrollo de software. Este se centra en el uso de prácticas seguras de codificación, que son una serie recomendaciones que se utilizan para crear aplicaciones y servicios seguros. Un/a analista de seguridad puede trabajar con equipos desarrolladores de software para garantizar que las prácticas de seguridad se incorporen en el ciclo de vida del desarrollo de software. Si, por ejemplo, uno de tus equipos asociados está creando una nueva aplicación móvil, se te puede pedir que brindes asesoramiento acerca de las políticas de contraseñas o que te asegures de que los datos de usuario se protegen y gestionan adecuadamente. Esto pone fin a nuestra introducción a los ocho dominios de seguridad del CISSP. Ponte el reto de comprender mejor cada uno de estos dominios y cómo afectan la seguridad general de una organización. Aunque quizá todavía tengas dudas en esta parte inicial del programa, analizaremos estos dominios en mayor detalle en el próximo curso. ¡Nos vemos allí!

Cómo determinar el tipo de ataque

Anteriormente, conociste cuáles son los ocho dominios de seguridad del profesional certificado en seguridad de sistemas de información (CISSP), que te permiten entender cómo organizar en categorías las responsabilidades de un analista de seguridad. Además, pueden ayudarte a comprender cómo gestionar el riesgo. En esta lectura, conocerás otros métodos de ataque. También podrás reconocer los tipos de riesgo que estos ataques presentan.

Tipos de ataques

Gráfica de los ocho iconos que representan los dominios de seguridad del CISSP.

Ataque de contraseña

Un ataque de contraseña tiene el propósito de acceder a dispositivos, sistemas, redes o datos protegidos por contraseña. Algunos tipos de ataques de contraseña que conocerás más adelante en el programa de certificación son:

Fuerza bruta

Tabla arcoíris o Rainbow

Los ataques de contraseña pertenecen al dominio de seguridad de las comunicaciones y las redes.

Ataque de ingeniería social

La ingeniería social es una técnica de manipulación que aprovecha errores humanos para obtener información privada, acceso a sistemas o bienes de valor. Algunos de los tipos de ataque de ingeniería social que seguirás conociendo en el transcurso del programa son:

Phishing (Suplantación de identidad)

Smishing

Vishing

Phishing localizado (Spear phishing)

Ataque de caza de ballena (Whaling)

Ataque en redes sociales (Phishing en redes sociales)

Compromiso del correo electrónico empresarial (BEC)

Ataque de “agujero de agua”

Cebo USB (Baiting)

Ingeniería social física

Los ataques de ingeniería social están relacionados con el dominio de seguridad y gestión de riesgos.

Ataque físico

Un ataque físico es un incidente de seguridad que afecta no solo a los entornos digitales, sino también a los físicos en los que se produce el incidente. Algunos tipos de ataques físicos son:

Cable USB malicioso

Unidad flash maliciosa

Clonación y skimming de tarjetas

Los ataques físicos pertenecen al dominio de seguridad de los activos.

Inteligencia artificial antagónica

La inteligencia artificial antagónica es una técnica que manipula

la tecnología de inteligencia artificial y el aprendizaje automático

para perpetrar ataques de manera más eficiente. Pertenece a los dominios de seguridad de comunicaciones y redes y al de gestión de identidad y acceso.

Ataque a la cadena de suministro

Un ataque a la cadena de suministro se dirige a los sistemas, las aplicaciones, el hardware y el software con el fin de identificar una vulnerabilidad en la que instalar software malicioso. Como cada artículo que se vende pasa por un proceso que involucra a terceros, esto significa que la vulneración de seguridad puede producirse en cualquier punto de la cadena de suministro. Estos ataques resultan costosos porque pueden afectar a varias organizaciones y a las personas que trabajan para ellas. Los ataques a la cadena de suministro pertenecen a los dominios de seguridad y gestión de riesgos, arquitectura e ingeniería de seguridad y operaciones de seguridad.

Ataque criptográfico

Un ataque criptográfico afecta a las formas seguras de comunicación protegidas por un sistema criptográfico. Algunos tipos de ataques criptográficos son:

Cumpleaños

Colisión

Degradación

Los ataques criptográficos pertenecen al dominio de seguridad de las comunicaciones y las redes.

Conclusiones clave

Los ocho dominios de seguridad del CISSP pueden ayudar a una organización y a su equipo de seguridad a reforzar sus defensas y prepararse para una filtración de datos. Las filtraciones de datos pueden ser simples o complejas y pertenecer a uno o más dominios. Considera que los métodos de ataque que hemos analizado son solo unos pocos de los muchos que existen. Durante el programa de certificación, aprenderemos sobre estos y otros tipos de ataques.

Conoce a los atacantes

Anteriormente, te presentamos el concepto de agente de amenaza. A modo de recordatorio, un agente de amenaza es cualquier persona o grupo que presenta un riesgo de seguridad. En este artículo, aprenderás acerca de los diferentes tipos de agentes de amenaza. Además, conocerás sus motivaciones, sus intenciones y su influencia en la industria de la ciberseguridad.

Tipos de agentes de amenaza

Amenazas avanzadas persistentes

Una amenaza persistente avanzada (APT) es un conjunto de procesos informáticos sigilosos orquestados por un tercero con la intención y la capacidad de atacar de forma avanzada y continuada en el tiempo, un objetivo determinado. Las APT suelen investigar a sus objetivos (p. ej., grandes corporaciones u organismos de gobierno) con antelación y pueden permanecer indetectables por un período prolongado. Sus intenciones y motivaciones pueden incluir:

Dañar infraestructura crítica, como la red eléctrica y recursos naturales

Acceder a propiedad intelectual, como secretos comerciales o patentes

Amenazas internas

Las amenazas internas abusan de su acceso autorizado para obtener datos que pueden perjudicar a una organización. Sus intenciones y motivaciones pueden incluir:

Sabotaje

Corrupción

Espionaje

Acceso no autorizado a datos o filtraciones de datos

Hacktivistas

Las/los hacktivistas son agentes de amenaza que actúan por motivaciones políticas. Abusan de la tecnología digital para alcanzar sus metas, las cuales pueden incluir:

Manifestaciones

Propaganda

Campañas de cambio social

Fama

Tipos de hackers

Seis hackers en computadoras.

Un/a hacker es cualquier persona o grupo que utiliza computadoras para acceder a datos sin autorización. Puede tratarse de una persona sin experiencia o profesional, experta en tecnología, que usa sus habilidades para diversos fines. Estas son las tres categorías principales de hackers:

Los/las hackers autorizados/as también se denominan hackers éticos. Respetan un código de ética y cumplen la ley para realizar evaluaciones de riesgos de una organización. Su motivación es proteger a las personas y a las organizaciones de los agentes de amenaza maliciosos.

Los/las hackers semiautorizados/as se consideran investigadores/as. Buscan vulnerabilidades, pero no aprovechan las que identifican.

Los/las hackers no autorizados/as también se denominan hackers no éticos. Son agentes de amenaza maliciosos/as que no cumplen ni respetan la ley. Su objetivo es recopilar y vender información confidencial para obtener un beneficio financiero.

Nota: existen varios tipos de hackers que pertenecen a una o más de estas tres categorías.

Los agentes de amenazas sin experiencia y poco hábiles tienen diversos objetivos, como por ejemplo:

Aprender y desarrollar sus habilidades de hackeo

Llevar a cabo una venganza

Aprovechar las vulnerabilidades de seguridad utilizando software malicioso, secuencias de comandos de programación y otras tácticas existentes

Otros tipos de hackers no tienen otra motivación que no sea realizar el trabajo para el que fueron contratados.

También existen hackers que se consideran a sí mismos/as como vigilantes, y su propósito principal es proteger al mundo de las/los hackers no éticos.

Conclusiones clave

Los/las agentes de amenaza y los/las hackers son hábiles en el campo técnico. Comprender sus motivaciones e intenciones te ayudará a prepararte mejor para proteger a tu organización y a las personas a las que esta sirve contra los ataques maliciosos ejecutados por algunos de estos grupos o personas.

Términos de glosario de la semana 2

Términos y definiciones del curso 1, semana 2

Ataque de contraseña: Intento de acceder a dispositivos, sistemas, redes o datos protegidos con una contraseña.

Ataque a la cadena de suministro: Ataque que se dirige a sistemas y aplicaciones de empresas desarrolladoras y proveedoras de hardware y/o software para localizar una vulnerabilidad en la que se pueda implementar malware.

Ataque criptográfico: Ataque que afecta las formas seguras de comunicación protegidas por un sistema criptográfico.

Ataque de “agujero de agua”: Tipo de ataque en el que un agente de amenaza compromete a un sitio web visitado con frecuencia por un grupo específico de usuarios/as.

Ataque de suplantación de identidad en redes sociales (Phishing en redes sociales): Tipo de ataque en el que el agente de amenaza contacta a la víctima en alguna red social, con el fin de robar información personal o tomar el control de la cuenta.

Ataque físico: Incidente de seguridad que afecta a los entornos digitales y físicos en donde se implementa.

Autenticación: Proceso para verificar la identidad de una persona.

Cebo USB (USB Baiting): Ataque que consiste en incluir un software malicioso (malware) en una memoria USB para obtener una ventaja financiera.

Compromiso de correo electrónico empresarial (BEC): Tipo de ataque de suplantación de identidad, en el que un agente de amenaza se hace pasar por una persona conocida por la víctima e intenta que realice una acción, como enviar dinero u otorgar datos confidenciales de la compañía.

Hacker: Cualquier persona o grupo de personas que utiliza computadoras para acceder a datos sin autorización.

Ingeniería social física: Ataque en que un agente de amenaza se hace pasar por una persona ligada a la empresa para obtener acceso no autorizado a una ubicación física.

Ingeniería social: Técnica de manipulación que busca engañar a las personas con el fin de que revelen información o realicen determinadas acciones.

Inteligencia artificial (IA) antagónica: Técnica que manipula la tecnología de inteligencia artificial y aprendizaje automático para ejecutar ataques más eficientes.

Software malicioso (malware): Programa diseñado para dañar dispositivos o redes.

Phishing (Suplantación de identidad): Uso de comunicaciones digitales para engañar a las personas de manera que revelen datos confidenciales o instalen software malicioso en sus equipos.

Phishing localizado (Spear phishing): Ataque por correo electrónico malicioso dirigido a una persona o grupo de personas específico que parece provenir de una fuente confiable.

Virus: (consultar Virus informático).

Virus informático: Código malicioso creado para interferir en el funcionamiento de las computadoras y dañar los datos y el software

Vishing: tipo de estafa por suplantación de identidad en la que se busca obtener información sensible a través de una llamada telefónica.

¡Hola, me alegro de verte de nuevo! Ya completaste la mitad del primer curso, estás progresando muy bien. Aquí hablaremos sobre cómo las organizaciones se protegen contra amenazas, riesgos y vulnerabilidades aprendiendo principios fundamentales como marcos, controles y ética. Entendamos con una analogía cómo esto se vincula con el análisis de ciberseguridad. Si quisieras plantar un jardín, investigas planificas, preparas y compras material, y también piensas en los posibles riesgos para tu jardín. Creas un plan para arrancar malezas, echar pesticidas, y regar con frecuencia para evitar problemas o incidentes. Pero, con el paso del tiempo, surgen problemas inesperados. El tiempo es impredecible, y hay plagas que intentan infiltrarse.

Reproduce el video desde ::54 y sigue la transcripción0:54

Implementas mejores formas de proteger tu jardín. Instalas una cámara de vigilancia, construyes una valla y cubres tus plantas para que el jardín esté sano y florezca. Tras entender las amenazas de tu jardín y cómo proteger tus plantas, creas mejores políticas y procedimientos para monitorear y proteger tu jardín. Así, la ciberseguridad se asemeja a un jardín. Es un sector en evolución que te desafía a mejorar continuamente las políticas y procedimientos que protegen a la organización y a sus usuarios/as. Para ello veremos los marcos y controles de seguridad, y por qué son importantes. Veremos los componentes principales con ejemplos de marcos y controles, como la tríada de confidencialidad, integridad y disponibilidad, denominada la tríada CID. Hablaremos sobre la ética de la seguridad y veremos inquietudes de ética en el campo de la ciberseguridad. La evolución de las prácticas de ciberseguridad parece abstracta, pero estas se usan a diario. Por ejemplo, uso claves de seguridad, que son un tipo de control de seguridad, como segunda autenticación para acceder a mis cuentas. Estas garantizan que solo yo acceda a mis cuentas, aunque alguien logre obtener mi contraseña. Al mejorar la confidencialidad, garantizan también la integridad de mis cuentas. Tener procesos y procedimientos para organizar la seguridad y tomar decisiones informadas es importante para todo el mundo. Me entusiasma comenzar, ¡espero que a ti también!

Imagina que trabajas como analista de seguridad y recibes alertas de actividad sospechosa en la red. Descubres que deberás implementar más medidas para evitar incidentes graves. Pero ¿por dónde empiezas? Como analista, primero debes identificar los activos y riesgos cruciales. Luego implementarás los marcos y controles necesarios. En este video, veremos cómo las/los profesionales de seguridad usan marcos para identificar y gestionar el riesgo. También veremos cómo usar controles de seguridad para gestionar o reducir riesgos. Los marcos de seguridad son pautas usadas en la creación de planes para mitigar riesgos y amenazas a los datos y la privacidad. Ofrecen un enfoque estructurado para implementar un ciclo de seguridad. El ciclo de seguridad lo conforman políticas y normas en evolución que definen cómo la organización gestiona los riesgos, sigue las políticas establecidas y cumple con normas o leyes.

Reproduce el video desde :1:5 y sigue la transcripción1:05

Hay varios marcos de seguridad que pueden usarse para manejar riesgos empresariales y cumplimiento normativo. Entre sus fines están proteger la información de identificación personal, abreviada como PII, proteger la información financiera, identificar debilidades de seguridad, manejar riesgos organizacionales y alinear los objetivos de seguridad con los de la empresa. Los marcos tienen cuatro componentes principales. Al conocerlos manejarás mejor los riesgos potenciales. El primer componente principal es identificar y documentar los objetivos de seguridad. Por ejemplo, una organización tiene el objetivo de alinearse con el Reglamento General de Protección de Datos de la UE, también conocido como RGPD. El RGPD es una ley de protección de datos creada para dar a los ciudadanos europeos más control sobre sus datos personales.

Reproduce el video desde :2:3 y sigue la transcripción2:03

Se puede pedir a un/a analista de ciberseguridad identificar y documentar áreas de incumplimiento con el RGPD. El segundo componente es crear pautas para alcanzar los objetivos de ciberseguridad. Por ejemplo, al implementar políticas para cumplir con el RGPD, puede que la organización deba crear nuevas políticas sobre cómo manejar solicitudes de datos de usuarios/as individuales. El tercer componente es implementar procesos de seguridad fuertes. En el caso del RGPD, un/a analista que trabaja para una empresa de redes sociales puede diseñar procedimientos para cumplir con las solicitudes de datos de sus usuarios/as. Un ejemplo de estas solicitudes es cuando una persona intenta actualizar o eliminar su información de perfil. El último componente de los marcos de seguridad es monitorear y comunicar los resultados. Por ejemplo, puedes monitorear la red interna de la organización y reportar a tu superior o responsable de cumplimiento un problema de seguridad potencial que afecta el RGPD.

Reproduce el video desde :3:15 y sigue la transcripción3:15

Tras presentar los cuatro componentes de los marcos de seguridad, analicémoslos juntos. Con los marcos, las y los analistas trabajan con otros miembros del equipo de seguridad para documentar, implementar y usar las políticas y los procedimientos. La/el analista de nivel inicial debe entender este proceso, pues impacta directamente en su trabajo y en cómo colabora con los demás.

Reproduce el video desde :3:40 y sigue la transcripción3:40

A continuación, veremos controles de seguridad. Los controles de seguridad son medidas que reducen ciertos riesgos de seguridad. Por ejemplo, puede haber una directiva de que los colaboradores deben hacer una capacitación de privacidad para evitar la filtración de datos. Como analista, puedes usar una herramienta de software para asignar de forma automática y ver quiénes realizan la capacitación. Los marcos y los controles son vitales para gestionar la seguridad de toda organización y garantizar que todas las personas colaboren para mantener un nivel de riesgo bajo. Al entender su propósito y cómo se usan, las/los analistas contribuyen al logro de los objetivos de seguridad y protegen a los/las usuarios/as. En los siguientes videos, veremos marcos y principios que las/los analistas deben conocer para minimizar el riesgo y proteger los datos y a los/las usuarios/as.

¡Hola de nuevo! Antes, hablamos sobre marcos y controles en general. Aquí aprenderás sobre marcos y controles específicos que las organizaciones usan voluntariamente para minimizar riesgos contra sus datos y proteger a sus usuarios/as. ¡Empecemos! La tríada CID es una guía fundamental que informa cómo las organizaciones evalúan el riesgo y crean sistemas y políticas de seguridad. CID es el acrónimo de confidencialidad, integridad y disponibilidad. La confidencialidad implica que solo las personas autorizadas pueden acceder a activos o datos específicos. Por ejemplo, deben implementarse controles de acceso estrictos que definan quién puede acceder a los datos y quién no a fin de proteger la información confidencial. La integridad implica que los datos son correctos, auténticos y confiables. Para la integridad, las/los profesionales usan protección de datos como el cifrado para impedir que se altere la información. La disponibilidad implica que quien tiene autorización tenga acceso a los datos. Por ejemplo, un director puede tener más acceso a ciertos datos que un gerente, pues el director suele supervisar a más colaboradores. Definamos un término que vimos al hablar de la tríada CID: activo. Un activo es un elemento percibido como valor para una organización. El valor lo determina el costo del activo en cuestión. Por ejemplo, una app que almacena datos confidenciales, como números de seguridad social o cuentas bancarias, es un activo valioso. Conlleva más riesgo, por lo que requiere controles más estrictos en comparación con un sitio que comparte noticias públicas. Como recordarás, antes vimos los marcos y controles en general. Ahora veremos un marco creado por el Instituto Nacional de Estándares y Tecnología de EE.UU., el Marco de Ciberseguridad, conocido como el CSF, del NIST. El CSF del NIST es un marco de adhesión voluntaria que consiste en estándares, pautas y prácticas recomendadas para manejar riesgos de ciberseguridad. Es importante conocer este marco, pues los equipos de seguridad lo usan como base para gestionar el riesgo a corto y largo plazo. Gestionar y minimizar riesgos, y proteger activos contra agentes de amenazas son objetivos clave del trabajo de seguridad. Es importante entender los motivos de un agente de amenazas e identificar los activos más valiosos de la organización.

Reproduce el video desde :2:43 y sigue la transcripción2:43

Entre las mayores amenazas están los empleados descontentos. Son los más peligrosos porque suelen tener acceso a información delicada y saben dónde hallarla. Para reducir este riesgo, las/los profesionales usan el principio de disponibilidad y pautas organizacionales basadas en marcos para que los/las empleados/as solo accedan a datos que necesitan para su trabajo. Hay agentes de amenazas en todo el mundo. Los equipos de seguridad diversos ayudan a las organizaciones a identificar las intenciones de los atacantes. Tener varias perspectivas ayuda a las organizaciones a entender y reducir el impacto de la actividad maliciosa. Con esto concluimos la introducción a la tríada CID y el marco de Ciberseguridad del NIST, que se usa para crear procesos y proteger a las organizaciones y a sus usuarios/as. Te pueden preguntar si conoces los marcos y principios de la seguridad. O te pueden pedir explicar cómo se usan para proteger activos organizacionales. En ambos casos, en este programa habrá varias oportunidades de aprender más al respecto y aplicar los conocimientos a situaciones reales. A continuación, veremos la ética de la seguridad. ¡Hasta pronto!

Controles, marcos y cumplimiento

Anteriormente, conociste los marcos de seguridad y cómo estos proporcionan un enfoque estructurado para implementar un ciclo de vida de seguridad. Como recordatorio, el ciclo de vida de seguridad consiste en un conjunto de políticas y estándares en constante evolución. En esta lectura, profundizarás en cómo se utilizan los marcos de seguridad, los controles y las regulaciones de cumplimiento, o leyes, de manera conjunta para gestionar la seguridad y garantizar que cada cual cumpla su parte para minimizar el riesgo.

Cómo se relacionan los controles, los marcos y el cumplimiento

La tríada de confidencialidad, integridad y disponibilidad (CID) es una guía que ayuda a las organizaciones a evaluar los riesgos y a establecer sistemas y políticas de seguridad.

Un triángulo que representa la tríada de confidencialidad, integridad y disponibilidad (CID)

La tríada de CID son los tres principios fundamentales utilizados por las/los profesionales de la ciberseguridad para establecer controles adecuados que mitiguen amenazas, riesgos y vulnerabilidades.

Como recordarás, los controles de seguridad son medidas diseñadas para reducir riesgos específicos de seguridad. Por lo tanto, se utilizan junto con marcos para asegurar que los objetivos y procesos de seguridad se implementen correctamente y que las organizaciones cumplan con los requisitos regulatorios.

En tanto, los marcos de seguridad son pautas utilizadas para elaborar planes que ayuden a mitigar riesgos y amenazas a los datos y la privacidad. Tienen cuatro componentes principales:

Identificación y documentación de objetivos de seguridad

Establecimiento de pautas para lograr los objetivos de seguridad

Implementación de procesos de seguridad sólidos

Supervisión y comunicación de resultados

Finalmente, el cumplimiento normativo, o compliance, es el proceso de adhesión a reglamentos internos y regulaciones externas.

Controles específicos, marcos y cumplimiento

El Instituto Nacional de Estándares y Tecnología (NIST) es una agencia con sede en los Estados Unidos que desarrolla varios marcos de cumplimiento voluntario que las organizaciones de todo el mundo pueden utilizar para ayudar a gestionar el riesgo. Cuanto más alineada al cumplimiento esté una organización, menor será el riesgo.

Entre los ejemplos de marcos que se presentaron anteriormente se encuentran el Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST) y el Marco de Gestión de Riesgos (RMF) del NIST.

Ten en cuenta que las especificaciones y pautas pueden variar según el tipo de organización para la que trabajes.

Además del

Marco de Ciberseguridad del NIST

y el

Marco de Gestión de Riesgos (RMF) del NIST

, existen varios otros controles, marcos y normas de cumplimiento con los que es importante que las/los profesionales de seguridad se familiaricen, para contribuir a mantener seguras a las organizaciones y a las personas a las que brindan servicio.

La Comisión Federal de Regulación de Energía - Corporación de Confiabilidad Eléctrica América del Norte (FERC-NERC)

La FERC-NERC es una regulación que se aplica a las organizaciones que trabajan con electricidad o que están involucradas con la red eléctrica de los Estados Unidos y América del Norte. Este tipo de organizaciones tienen la obligación de prepararse, mitigar y reportar cualquier incidente de seguridad potencial que pueda afectar negativamente a la red eléctrica. También están legalmente obligadas a cumplir con los Estándares de Confiabilidad de Protección de Infraestructura Crítica (CIP) definidos por la FERC.

Programa Federal de Gestión de Riesgos y Autorizaciones (FedRAMP®)

El FedRAMP es un programa del gobierno federal de los Estados Unidos que estandariza la evaluación, autorización, monitoreo y gestión de seguridad de los servicios en la nube y las ofertas de productos. Su objetivo es proporcionar consistencia en todo el sector gubernamental y proveedores de servicios en la nube de terceros.

Centro de Seguridad en Internet (CIS®)

El CIS es una organización sin fines de lucro que se enfoca en múltiples áreas. Proporciona un conjunto de controles que pueden utilizarse para proteger sistemas y redes contra ataques. Su objetivo es ayudar a las organizaciones a establecer un mejor plan de defensa. Además, el CIS proporciona controles aplicables que las/los profesionales de seguridad pueden seguir ante un eventual incidente de seguridad.

Reglamento General de Protección de Datos (RGPD)

El RGPD es una normativa general de datos de la Unión Europea (UE) que protege el procesamiento de los datos de sus residentes y su derecho a la privacidad dentro y fuera del territorio. Por ejemplo, si una organización no es transparente en relación con los datos que posee sobre un/a ciudadano/a de la UE o la razón por la que los tiene, esto constituye una infracción que puede resultar en una multa para la organización. Además, si se produce una filtración y los datos de una persona se ven comprometidos, este debe ser informado. La organización afectada tiene 72 horas para notificarla sobre esta situación.

Estándares de seguridad de datos del sector de las tarjetas de pago (PCI DSS)

PCI DSS es un estándar de seguridad internacional destinado a garantizar que las organizaciones que almacenan, aceptan, procesan y transmiten información de tarjetas de crédito lo hagan en un entorno seguro. El objetivo de esta norma es reducir el fraude con tarjetas de crédito.

Ley de Transferencia y Responsabilidad de los Seguros Médicos (HIPAA)

La HIPAA es una ley federal de los Estados Unidos establecida en 1996 para proteger la información médica de las personas. Esta ley prohíbe que la información de un/una paciente sea compartida sin su consentimiento. Se rige por tres reglas:

Privacidad

Seguridad

Notificación de filtraciones

Las organizaciones que almacenan datos de pacientes tienen la obligación legal de informarles en caso de que ocurra una violación de seguridad, ya que la exposición de la Información Médica Protegida (PHI) de las/ los pacientes puede conducir al robo de identidad y al fraude de seguros. La PHI se refiere a la información relacionada con la salud física o mental pasada, presente o futura de una persona, ya sea un plan de atención o pagos por la atención. Además de comprender la HIPAA como una ley, las/los profesionales de la seguridad también deben familiarizarse con la Alianza de Confianza de Información de Salud (HITRUST®), que es un marco de seguridad y un programa de garantía que ayuda a las instituciones a cumplir con la HIPAA.

Organización Internacional para la Normalización (ISO)

La ISO fue creada para establecer estándares internacionales relacionados con la tecnología, la fabricación y la gestión en todo el mundo. Ayuda a las organizaciones a mejorar sus procesos y procedimientos en cuanto a retención del personal, planificación, gestión de residuos y servicios.

Controles de Sistemas y Organizaciones (SOC tipo 1, SOC tipo 2)

Este estándar fue desarrollado por la junta de normas de auditoría del Instituto Americano de Contables Públicos Certificados® (AICPA). Los informes SOC1 y SOC2 se enfocan en las políticas de acceso de los/as usuarios/as de una organización en diferentes niveles, tales como:

Asociado/a

Supervisor/a

Gerente/a

Ejecutivo/a

Proveedor/a

Otros

Estos informes se utilizan para evaluar el cumplimiento financiero de una organización, así como los niveles de riesgo asociados. También abordan aspectos críticos como la confidencialidad, privacidad, integridad, disponibilidad, seguridad y la seguridad general de los datos. Es importante destacar que cualquier falla en el control de estos aspectos puede resultar en posibles fraudes.

Consejo profesional: Existen numerosas regulaciones que se revisan con frecuencia. Te recomendamos mantenerte al día con los cambios y explorar más marcos, controles y normas de cumplimiento. Dos sugerencias para investigar: la Ley Gramm-Leach-Bliley y la Ley Sarbanes-Oxley.

Orden Ejecutiva Presidencial de los Estados Unidos 14028

El 12 de mayo de 2021, el presidente de los Estados Unidos Joe Biden emitió una orden ejecutiva con el objetivo de mejorar la ciberseguridad de la nación y hacer frente al aumento de la actividad de quienes perpetran amenazas. Esta medida tiene como objetivo principal abordar y solucionar las vulnerabilidades presentes en las agencias federales y en terceros vinculados a la

infraestructura crítica

de los Estados Unidos. Para obtener más información, revisa la

Orden Ejecutiva para Mejorar la Ciberseguridad de la Nación

.

Conclusiones clave

En esta lectura, has conocido más acerca de los controles, los marcos y el cumplimiento regulatorio. También, has aprendido cómo estos elementos trabajan en conjunto para ayudar a las organizaciones a mantener un nivel de riesgo bajo.

Como analista de seguridad, es importante mantenerse al día con los marcos de referencia, controles y normativas de cumplimiento más habituales y estar al tanto de los cambios que se presentan en el panorama de la ciberseguridad. Esto permite ayudar a garantizar la seguridad tanto de las organizaciones como de las personas.

La ética en la ciberseguridad

Para la seguridad, las nuevas tecnologías traen nuevos desafíos. No siempre está claro cuál es la decisión correcta o incorrecta para cada nuevo incidente o riesgo. Por ejemplo, imagina que trabajas como analista de seguridad de nivel inicial y recibes una alerta de riesgo alto. La investigas y descubres que se transfirieron datos sin autorización.

Reproduce el video desde ::24 y sigue la transcripción0:24

Te esmeras para identificar quién hizo la transferencia y descubres que es un amigo del trabajo. ¿Qué haces? Éticamente, como profesional, debes ser imparcial y preservar la seguridad y confidencialidad. Aunque es normal proteger a un amigo, sin importar quién sea el usuario en cuestión, tienes la responsabilidad y obligación de seguir las políticas y protocolos que aprendiste en la capacitación. En muchos casos, los equipos de seguridad tienen más acceso a datos e información que otros colaboradores. Las/los profesionales deben respetar ese privilegio y actuar éticamente. La ética de la seguridad da pautas para tomar decisiones apropiadas como profesional. Otro ejemplo: si como analista tienes la capacidad para darte acceso a los datos de nómina y aumentarte el sueldo, ¿deberías hacerlo solo porque puedes? La respuesta es no. Nunca debes abusar del acceso que se te ha otorgado y confiado. Hablemos de los principios éticos que plantean dudas al estudiar soluciones para mitigar los riesgos. Estos son la confidencialidad, la protección de la privacidad y las leyes. Empecemos por el primero: confidencialidad.

Reproduce el video desde :1:46 y sigue la transcripción1:46

Antes vimos la confidencialidad como parte de la tríada CID. Ahora analicemos cómo aplicarla a la ética.

Reproduce el video desde :1:56 y sigue la transcripción1:56

Como profesional de ciberseguridad, verás información propietaria o información privada, como PII. Tu deber ético es mantener su confidencialidad y protegerla. Por ejemplo, puedes ayudar a un colega dándole acceso informático fuera de los canales debidamente documentados. Sin embargo, esta violación ética puede tener consecuencias graves, incluyendo sanciones, la pérdida de tu reputación profesional y repercusiones legales tanto para ti como para tu colega. El segundo principio a considerar es la protección de la privacidad. Esta implica preservar los datos personales contra un uso no autorizado. Por ejemplo, tu superior te envía un correo personal fuera del horario laboral para pedir el teléfono de un colega. Te explica que no puede acceder a los datos de empleados en ese momento, pero necesita hablar urgentemente con esa persona. Como analista de ciberseguridad, debes seguir las políticas y procedimientos. En este ejemplo, indican que los datos de empleados/as se guardan en una base de datos segura que nunca se debe ver ni compartir de otra forma. Por lo tanto, acceder y compartir datos personales no sería ético.

Reproduce el video desde :3:14 y sigue la transcripción3:14

En este tipo de situación, es difícil saber qué hacer. La mejor respuesta es seguir las políticas y procedimientos establecidos.

El tercer principio que veremos es la ley. Las leyes son reglas que reconoce una comunidad y que aplica una entidad gobernante. Por ejemplo, imagina un profesional de un hospital capacitado para manejar PII y SPII para cumplir con las normativas. Tiene archivos con datos confidenciales que nunca deben dejarse sin supervisión. Pero llega tarde a una reunión. En lugar de guardar los archivos en un área designada, los deja en su escritorio sin supervisión. Al regresar, los archivos no están. Esta persona infringió varias regulaciones de cumplimiento, y sus acciones no fueron ética ni legalemente correctas, ya que su negligencia causó la pérdida de datos privados de pacientes y del hospital. En el campo de la seguridad, recuerda que la tecnología evoluciona, y también las tácticas y técnicas de los atacantes. Debido a esto, las/los profesionales deben seguir pensando críticamente cómo responder a los ataques. Tener una ética sólida guía las decisiones para seguir los procesos y procedimientos correctos a fin de mitigar los riesgos en evolución.

Los conceptos éticos que guían las decisiones sobre la ciberseguridad

Previamente, se te presentó el concepto de ética de la ciberseguridad. La ética de la ciberseguridad refiere a una serie de pautas fundamentales para tomar decisiones apropiadas como profesional de la seguridad. Ser ético/a implica mantener la imparcialidad y preservar la seguridad y confidencialidad de los datos privados. Contar con un sólido sentido de ética te ayudará a tomar decisiones acertadas como profesional de la ciberseguridad, permitiéndote mitigar las amenazas planteadas por las tácticas y técnicas en constante evolución de ataques maliciosos. En esta lectura, ampliarás tus conocimientos sobre conceptos éticos adicionales que son esenciales para tomar decisiones adecuadas sobre cómo responder legal y éticamente a los ataques, protegiendo tanto a las organizaciones como a las personas involucradas.

Preocupaciones éticas y leyes relacionadas con los contraataques

Postura de los Estados Unidos sobre los contraataques

En los Estados Unidos, está prohibido realizar contraataques contra agentes de amenaza debido a leyes como la Ley de Abuso y Fraude Informático de 1986 y la Ley de Intercambio de Información de Seguridad Cibernética de 2015, entre otras. En lugar de contraatacar, solo se permite la defensa. La acción de contraatacar en los Estados Unidos se considera un acto de justicia por mano propia, reservado para las fuerzas del orden. Además, los contraataques pueden llevar a una escalada de la situación y causar aún más daño. Por último, si el agente amenazante es un/a hacktivista patrocinado/a por el estado, los contraataques pueden tener serias implicaciones internacionales. Un/a hacktivista es una persona que utiliza el hackeo (hacking) o piratería informática para lograr objetivos políticos, como promover cambios sociales o desobediencia civil.

Por estas razones, solo se permite que los/las empleados/as autorizados/as por el gobierno federal y el personal militar realicen contraataques en los Estados Unidos.

Postura internacional sobre los contraataques

La Corte Internacional de Justicia (CIJ), que actualiza regularmente sus políticas y regulaciones, establece que una persona o grupo puede contraatacar si:

El contraataque solo afectará a la parte que atacó primero.

El contraataque es una comunicación directa pidiendo al atacante inicial que se detenga.

El contraataque no escala la situación.

Los efectos del contraataque se pueden revertir.

Normalmente, las organizaciones no realizan contraataques porque los escenarios y parámetros mencionados anteriormente son difíciles de medir. Existe mucha incertidumbre en cuanto a lo que es y no es legal, y, a veces, es muy difícil controlar los resultados negativos. Las acciones de contraataque generalmente conducen a un resultado peor, especialmente si no se es un/a profesional experimentado/a en el campo.

Para obtener más información sobre escenarios específicos y preocupaciones éticas desde una perspectiva internacional, te recomendamos revisar las actualizaciones proporcionadas en el Tallinn Manual 2.0 On The International Law Applicable to Cyber Operations o accede al

Tallin Manual en línea

.

Metodologías y principios éticos

Dado que los contraataques generalmente son desaprobados o ilegales, en el ámbito de la ciberseguridad se han creado marcos y controles, como la tríada de confidencialidad, integridad y disponibilidad (CID) y otros discutidos anteriormente en el programa, para abordar cuestiones relacionadas con la confidencialidad, protección de la privacidad y cumplimiento de leyes. Con el fin de comprender mejor la relación entre estos aspectos y las obligaciones éticas de las/los profesionales de la ciberseguridad, es importante revisar los siguientes conceptos fundamentales sobre el uso de la ética para proteger a las organizaciones y a las personas.

La confidencialidad implica que solo los/as usuarios/as autorizados/as pueden acceder a activos o datos específicos. Desde el punto de vista ético, la confidencialidad requiere un alto nivel de respeto por la privacidad con el objetivo de proteger los activos y datos privados.

La protección de la privacidad implica preservar la información personal de un uso no autorizado. La información de identificación personal (PII) y la información de identificación personal sensible (SPII) son tipos de datos personales que pueden causar daño a las personas en caso de robo. Los datos de PII incluyen cualquier información que se puede utilizar para deducir la identidad de una persona, como su nombre y número de teléfono. Por otro lado, los datos de SPII son una categoría más restrictiva de PII y abarcan números de seguridad social y números de tarjetas de crédito. Para proteger adecuadamente los datos de PII y SPII, las/los profesionales de ciberseguridad tienen la responsabilidad ética de proteger la información privada, identificar vulnerabilidades de seguridad, gestionar los riesgos empresariales y alinear las medidas de seguridad con los objetivos del negocio.

Las leyes son normas reconocidas por una comunidad y aplicadas por una entidad gubernamental. Como profesional de la seguridad, tendrás la responsabilidad ética de proteger a tu organización, su infraestructura interna y a las personas allí involucradas. Para lograrlo debes:

Mantener la imparcialidad y llevar a cabo tu trabajo de manera honesta, responsable y con el máximo respeto por la ley.

Ser transparente y basar tus acciones en evidencias.

Garantizar un profundo compromiso con el trabajo que realizas, para que puedas abordar de manera adecuada y ética los problemas que surjan.

Mantenerte al día y buscar constantemente mejorar tus habilidades, de manera que puedas contribuir al avance y al mejoramiento del panorama de la ciberseguridad.

Un ejemplo relevante es la Ley de Transferecia y Responsabilidad de los Seguros Médicos (HIPAA), una ley federal de los Estados Unidos establecida para proteger la información de salud de las/los pacientes, también conocida como Protected Health Information (PHI) o información de salud protegida. Esta ley prohíbe compartir la información de las/los pacientes sin su consentimiento. Por lo tanto, como profesional de la ciberseguridad, es tu responsabilidad garantizar que la organización en la que trabajas cumpla con su obligación legal y ética de informar a las personas en caso de que se produzca una violación de seguridad que exponga sus datos médicos.

Conclusiones clave

Como futuro/a profesional de la seguridad, la ética desempeñará un papel importante en tu trabajo diario. Comprender la ética y las leyes te ayudará a tomar las decisiones correctas si te enfrentas a una amenaza de seguridad o a un incidente que resulte en una violación de datos.

Hola, soy Holly, arquitecta de Seguridad en la Nube, Google Cloud. Al comienzo de mi carrera, vendía medias a la vez que estudiaba. Trabajé en la banca, y más tarde en telecomunicaciones. Después trabajé para una firma proveedora de seguridad y aprendí de seguridad. En parte, pude cambiar el rumbo de mi carrera tecnológica inicial como administradora de base de datos para pasar a la ciberseguridad mediante certificados como este que haces. Me ayudaron a ganar credibilidad ante empleadores potenciales cuando aún no tenía experiencia en este sector. La ética es el núcleo de la ciberseguridad. Debes siempre actuar de forma ética para ser un/a profesional de ciberseguridad. Algunos ejemplos de comportamientos poco éticos suelen ser algo de pereza, tomar atajos sin pensar en las consecuencias de las acciones. Como cuando se comparten contraseñas de sistemas, se releva información privada, o se busca en sistemas información personal propia o bien de personas conocidas o celebridades. Me enfrenté a una situación muy difícil en mi carrera de tecnología en cuanto a la ética poco después de los atentados del 11S. El jefe del jefe de mi jefe se me acercó con muchas palabras clave relacionadas con el ataque en Nueva York y me pidió que consultara la base de datos que administraba, que tenía los mensajes de toda la empresa de telecomunicaciones sin nada por escrito ni una orden judicial. Fue una situación muy incómoda decirle a alguien con un puesto mucho más alto que no me sentía cómoda haciéndolo. Le sugerí que me diera la indicación por escrito. Al final encontró a otra persona que lo hizo. Al enfrentarse a una decisión difícil como esta, es bueno pensar en las consecuencias de la decisión. A ti, que estás haciendo este programa, te recomiendo, pues recompensa enormemente, ayudar a proteger a la empresa, a las personas o la organización contra la ciberdelincuencia. Estamos del lado bueno y protegemos a la industria y a las personas contra ataques cibernéticos y contra ciberdelincuentes. ¡Es gratificante!

Términos del glosario de la semana 3

Términos y definiciones del curso 1, semana 3

Activo: Elemento percibido como valioso para una organización.

Arquitectura de seguridad: Tipo de diseño de seguridad compuesto por múltiples herramientas y procesos, que se utiliza para proteger a una organización de los riesgos y amenazas externas.

Confidencialidad: Propiedad según la cual únicamente las personas autorizadas pueden acceder a activos o datos específicos.

Controles de seguridad: Pautas diseñadas para abordar y eliminar riesgos de seguridad específicos, como la alteración o la eliminación de información de perfiles, entre otros.

Disponibilidad: Principio según el cual los datos son accesibles para las personas autorizadas a utilizarlos.

Ética de la seguridad: Pautas para tomar decisiones apropiadas como profesional de la seguridad.

Gobernanza de seguridad: Prácticas que ayudan a apoyar, definir y dirigir los esfuerzos de seguridad de una organización.

Hacktivista: Persona que utiliza el hacking para lograr objetivos políticos.

Información médica protegida (PHI por sus siglas en inglés): Cualquier información relacionada con la salud, o la condición física o mental pasada, presente o futura de una persona.

Integridad: Cualidad que identifica a los datos como correctos, auténticos y confiables.

Ley de Transferencia y Responsabilidad de los Seguros Médicos (HIPAA): Ley federal de los Estados Unidos establecida para proteger la información de salud de los pacientes.

Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST por sus siglas en inglés): Marco de adhesión voluntaria creado en los Estados Unidos, que incluye estándares, pautas y prácticas recomendadas para gestionar los riesgos de ciberseguridad.

Marcos de seguridad: Pautas utilizadas para crear planes que ayuden a mitigar el riesgo y las amenazas a los datos y la privacidad.

Open Web Application Security Project (OWASP): Organización sin fines de lucro centrada en mejorar la seguridad de software.

Protección de la privacidad: Acto de proteger la información personal de usos no autorizados.

Tríada de confidencialidad, integridad y disponibilidad (CID): Guía que ayuda a las organizaciones a evaluar los riesgos y establecer sistemas y políticas de seguridad.

Herramientas habituales de ciberseguridad

Como ya se mencionó, la seguridad es como prepararse para una tormenta. Si identificas una fuga, el color o la forma del balde que usarás para atrapar el agua no importa. Lo importante es mitigar los riesgos y amenazas a tu hogar mediante el uso de las herramientas a tu disposición. Como analista de seguridad de nivel inicial, tendrás un montón de herramientas en tu kit que puedes usar para mitigar riesgos potenciales. En este video, analizaremos los propósitos principales y las funciones de algunas herramientas comúnmente usadas. Y más adelante, tendrás oportunidad de practicar su uso. Antes de seguir con las herramientas, analicemos brevemente los registros, que son las fuentes de datos que las herramientas que veremos deben organizar. Un registro es un historial de eventos que ocurren dentro de los sistemas de una organización. Algunos ejemplos incluyen registros de inicios de sesión de empleados/as en sus computadoras o accesos a servicios en la red. Los registros ayudan a las/los profesionales de la seguridad a identificar vulnerabilidades y potenciales fugas de información.

Reproduce el video desde :1:6 y sigue la transcripción1:06

Las primeras herramientas que veremos son herramientas de información de seguridad y gestión de eventos, o herramientas SIEM. Una herramienta SIEM es una aplicación que recolecta y analiza datos de registro para monitorear actividades críticas en una organización. El acrónimo S-I-E-M puede pronunciarse "SIM" o "SIEM", pero usaremos "SIEM" a lo largo de este programa. Las herramientas SIEM recopilan información en tiempo real, o instantánea, y permite que las/los analistas de seguridad identifiquen fugas potenciales mientras ocurren. Imagina tener que leer páginas y páginas de registros para determinar si hay amenazas de seguridad. Según la cantidad de datos, puede tomar horas o días. Las SIEM reducen la cantidad de datos que un/a analista debe revisar al brindar alertas para tipos específicos de riesgos y amenazas. Ahora repasemos ejemplos de herramientas SIEM de uso común: Splunk y Chronicle. Splunk es una plataforma de análisis de datos, y Splunk Enterprise proporciona soluciones SIEM. Splunk Enterprise es una herramienta autoalojada que se usa para retener, analizar y buscar datos de registro de una organización. Otra herramienta SIEM es Chronicle, de Google. Chronicle es una SIEM nativa de la nube, que almacena datos de seguridad para búsqueda y análisis. El ser nativa de la nube significa que Chronicle permite una entrega rápida de nuevas características. Ambas herramientas SIEM, y las SIEM en general, recopilan datos de distintos lugares, luego los analizan y filtran para permitir a los equipos de seguridad prevenir y reaccionar rápidamente ante posibles amenazas a la seguridad. Como analista de seguridad, puede que te encuentres usando las SIEM para analizar eventos y patrones filtrados, realizar análisis de incidentes o buscar amenazas de forma proactiva. Según la configuración de las SIEM y el enfoque de riesgo de tu organización, las herramientas y la manera en que estas funcionan puede diferir. Pero en última instancia, todas se usan para mitigar el riesgo. Otras herramientas clave que usarás como analista de seguridad, y cuyo uso podrás practicar más adelante en el programa, son los manuales de estrategias, y analizadores de protocolo de red. Un manual de estrategias proporciona detalles acerca de cualquier acción operativa, como la forma de responder a un incidente. Estos manuales, que varían de acuerdo a la organización, orientan a las/los analistas sobre cómo manejar un incidente de seguridad antes, durante y después de que ocurrió.

Reproduce el video desde :3:41 y sigue la transcripción3:41

Pueden corresponder a revisiones de conformidad o seguridad, gestión del acceso y muchas otras tareas organizacionales que requieren un proceso documentado de inicio a fin. Otra herramienta que puedes usar como analista de seguridad es un analizador de protocolos de red, o Sniffer de paquetes. Un Sniffer de paquetes es una herramienta diseñada para capturar y analizar el tráfico de datos dentro de una red. Los analizadores de protocolos de red comunes incluyen TCPdump y Wireshark. Como analista de nivel inicial, no tienes que ser un/a experto/a en estas herramientas. A medida que avances en este programa y obtengas más práctica, entenderás más y más acerca de cómo usar estas herramientas para identificar, evaluar y mitigar los riesgos.

Herramientas para proteger las operaciones comerciales

Anteriormente, te presentamos distintas habilidades técnicas que las/los analistas de seguridad necesitan desarrollar, además de algunas herramientas que las/los analistas de nivel inicial pueden tener en su caja de herramientas. En esta lectura, profundizarás sobre cómo las habilidades y herramientas técnicas ayudan a mitigar los riesgos.

La caja de herramientas de un/a analista de nivel inicial

Cada organización puede proporcionar una caja de herramientas diferente, dependiendo de sus necesidades de seguridad. Como futuro analista, es importante que te familiarices con las herramientas estándar de la industria y que puedas demostrar tu capacidad para aprender a usar otras similares, en un lugar de trabajo diferente.

Una persona carga un estuche con diferentes herramientas en su interior

Herramientas de información de seguridad y gestión de eventos (SIEM)

Una herramienta SIEM es una aplicación que recopila y analiza datos de registro para monitorear actividades críticas en una organización. Un registro recopila eventos que ocurren dentro de los sistemas de una organización. Dependiendo de la cantidad de datos con los que estés trabajando, podría tomarte horas o días filtrar los datos del registro. Las herramientas SIEM proporcionan alertas para tipos específicos de amenazas, riesgos y vulnerabilidades, lo que reduce la cantidad de datos que un/a analista debe revisar.

Además, las herramientas SIEM ofrecen una serie de paneles con indicadores (dashboards) que organizan visualmente los datos en categorías, lo cual permite a los/las usuarios/as seleccionar aquellos que desean analizar. Las diferentes herramientas SIEM tienen distintos tipos de paneles de control, que muestran la información a la cual tienes acceso.

Las herramientas SIEM también cuentan con diferentes opciones de alojamiento: on-premise (local) y en la nube. Las organizaciones pueden elegir la opción de alojamiento que prefieran, en función de la experiencia de los miembros del equipo de seguridad. Por ejemplo, dado que una versión alojada en la nube suele ser más fácil de configurar, usar y mantener que una versión local, un equipo de seguridad con menos experiencia puede elegir esta opción.

Analizadores de protocolo de red (programas detectores de paquetes)

Un analizador de protocolo de red, también conocido como un programa detector de paquetes, es una herramienta diseñada para capturar y analizar el tráfico de datos en una red. Esto significa que la herramienta mantiene un registro de todos los datos que encuentra una computadora dentro de la red de una organización. Más adelante en el programa, tendrás la oportunidad de practicar el uso de algunas de las herramientas más comunes de un analizador de protocolos de red.

Manual de estrategias

Un manual de estrategias (o playbook) brinda detalles sobre cualquier acción operativa, como la forma de responder a un incidente de seguridad. En general, las organizaciones tienen varios manuales de estrategias, que documentan los procesos y procedimientos para que sus equipos los sigan. Los manuales de estrategias varían de una organización a otra, pero todos tienen un propósito similar: guiar a las/los analistas mediante una serie de pasos, para completar tareas específicas relacionadas con la seguridad.

Por ejemplo, considera que estás trabajando como analista de seguridad para una empresa de respuesta a incidentes y se te presenta un caso que involucra una clínica médica pequeña que fue víctima de una fuga de información. Tu trabajo es ayudar con la investigación forense y proporcionar evidencia a una compañía de seguros de ciberseguridad. De acuerdo a los hallazgos obtenidos, se determinará si la clínica recibirá o no el pago del seguro.

En este ejemplo, los manuales describirán las acciones específicas que debes tomar para llevar a cabo la investigación. También ayudan a que te asegures de que estás siguiendo los protocolos y procedimientos adecuados. Cuando trabajas en un caso forense, hay dos manuales que puedes seguir:

El primero que puedes consultar es el manual de la cadena de custodia. La cadena de custodia es el proceso de documentar la posesión y el control de la evidencia durante el ciclo de vida del incidente. Como analista de seguridad involucrado/a en un análisis forense, trabajarás con los datos que fueron vulnerados. Junto con el equipo forense, también deberás documentar quién, qué, dónde y por qué tienen la evidencia recopilada. Mientras estén en tu poder, las pruebas son tu responsabilidad, y deben rastrearse y mantenerse seguras. Cada vez que la evidencia se mueve, debe reportarse. Esto permite a todas las partes involucradas saber exactamente dónde está en todo momento.

El segundo manual de estrategias que tu equipo podría usar se llama manual de protección y preservación de la evidencia. La protección y preservación de la evidencia es el proceso de trabajar adecuadamente con evidencia digital frágil y volátil. Como analista de seguridad, es fundamental comprender qué es la evidencia digital frágil y volátil, y por qué existe un procedimiento. Al seguir este manual, consultarás el orden de volatilidad, que es una secuencia que describe el orden de los datos que deben conservarse, del primero al último. Prioriza los datos volátiles, que son datos que pueden perderse si el dispositivo en cuestión se apaga, independientemente de la razón. Durante una investigación, la gestión inadecuada de la evidencia digital puede comprometerla y alterarla. Cuando esta se maneja incorrectamente durante una investigación, ya no se puede usar. Por esta razón, la prioridad en cualquier investigación es preservar adecuadamente los datos. Para conservar los datos, puedes hacer copias y utilizarlas al llevar a cabo la investigación.

Conclusiones clave

En esta lectura, aprendiste sobre algunas herramientas que un/a analista de seguridad puede tener en su caja de herramientas, dependiendo de dónde trabajen. También exploraste dos tipos importantes de manuales de estrategias: la cadena de custodia y la protección y preservación de la evidencia. Estos son solo dos procedimientos que ocurren al comienzo de una investigación forense. Si te interesan las investigaciones forenses, te animamos a explorar más a fondo esta trayectoria profesional o práctica de seguridad. En el proceso, puedes aprender sobre las herramientas forenses que quieras agregar a tu caja de herramientas. Aunque en este programa de certificación no se cubrirán todos los componentes forenses que conforman una investigación, algunos conceptos se analizarán en cursos posteriores.

Recursos para obtener información adicional

El

Informe Threat Horizon

del Equipo de acción de Ciberseguridad de Google proporciona inteligencia estratégica para hacer frente a las amenazas a la empresa en la nube.

La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) tiene una lista de

servicios y herramientas gratuitas de ciberseguridad

. Consulta la lista para obtener más información sobre las herramientas de ciberseguridad de código abierto.

**Introducción a Linux, SQL y Python**

Como ya vimos anteriormente, las organizaciones usan una variedad de herramientas, como SIEM, manuales de estrategias y detectores de paquetes para gestionar, monitorear y analizar mejor las amenazas a la seguridad. Pero esas no son las únicas herramientas en el kit de un/a analista. También usan lenguajes de programación y sistemas operativos para lograr tareas esenciales. En este video, te presentaremos la programación SQL y Python, y el sistema operativo Linux. Tendrás la oportunidad de practicar y usarlas más adelante en el programa. Las organizaciones pueden usar la programación para crear instrucciones específicas que una computadora ejecute. La programación permite a las/los analistas completar tareas y procesos repetitivos con un alto grado de precisión y eficiencia. También ayuda a reducir el riesgo de error humano, y puede ahorrar horas o días en comparación con el trabajo manual. Ahora que sabes para qué se usan los lenguajes de programación, analicemos un sistema operativo específico y relacionado llamado Linux y dos lenguajes de programación: SQL y Python. Linux es un sistema operativo de código abierto o públicamente disponible. A diferencia de otros SO con los que puedas estar familiarizado/a, como MacOS o Windows, Linux depende de una línea de comandos como la interfaz de usuario principal. Linux en sí no es un lenguaje de programación, pero sí permite el uso de comandos de texto entre el usuario y el sistema operativo. Aprenderás más sobre Linux más adelante. Un uso común de Linux para las/los analistas de seguridad de nivel inicial es la examinación de registros para entender mejor lo que ocurre en un sistema. Por ejemplo, quizá uses comandos para revisar un registro de errores mientras investigas un tráfico de red inusualmente alto. A continuación, veamos el SQL. SQL significa lenguaje de consulta estructurado. SQL es un lenguaje de programación usado para crear, interactuar y solicitar información de una base de datos. Una base de datos es una colección organizada de información o datos. Puede haber millones de datos en estas bases. Entonces, un/a analista de seguridad de nivel inicial usaría SQL para filtrar los datos y recuperar información específica. El último lenguaje de programación que presentaremos es Python. Las/los profesionales de la seguridad pueden usar Python para realizar tareas repetitivas y desgastantes, y que requieren un alto nivel de detalle y precisión. Como futuro/a analista, es importante entender que el kit de herramientas de cada organización puede ser diferente según sus necesidades de seguridad. Lo importante es que te familiarices con algunas herramientas estándar, ya que es les mostrará a los/las empleadores/as que tienes la habilidad de aprender a usar sus herramientas para proteger la organización y sus clientes. ¡Muy buen trabajo! Más adelante, aprenderás más sobre Linux y lenguajes de programación. También practicarás mediante el uso de estas herramientas en escenarios relacionados con la seguridad.

**Usa herramientas para proteger las operaciones comerciales**

Anteriormente, te presentamos la programación, los sistemas operativos y las herramientas que usan comúnmente las/los profesionales de la ciberseguridad. En esta lectura, aprenderás más sobre la programación y los sistemas operativos, así como otras herramientas que las/los analistas de nivel inicial utilizan para ayudar a proteger a las organizaciones y las personas a las que sirven.

Herramientas y sus propósitos

Programación

La programación es un proceso que se puede usar para crear un conjunto específico de instrucciones para que una computadora ejecute tareas. Las/los analistas de seguridad utilizan lenguajes de programación, como Python, para ejecutar la automatización. La automatización es el uso de la tecnología para reducir el esfuerzo humano y manual en la realización de tareas comunes y repetitivas. También ayuda a reducir el riesgo de errores humanos.

Otro lenguaje de programación que utilizan las/los analistas se llama Structured Query Language (SQL). SQL se utiliza para crear, interactuar y solicitar información de una base de datos. Una base de datos es una colección organizada de información o datos. Puede haber millones de datos en una base. Un dato es una pieza específica de información.

Sistemas operativos

Un sistema operativo es la interfaz entre el hardware de la computadora y el usuario. Linux®, macOS® y Windows son sistemas operativos. Cada uno ofrece diferentes funcionalidades y experiencias de usuario.

Ya mencionamos a Linux como un sistema operativo de código abierto. El código abierto significa que el código está disponible para el público y permite a las personas hacer contribuciones para mejorar el software. Linux no es un lenguaje de programación; sin embargo, sí implica el uso de una línea de comandos dentro del sistema operativo. Un comando es una instrucción que indica a la computadora que haga algo. Una interfaz de línea de comandos es una interfaz de usuario basada en texto que utiliza comandos para interactuar con la computadora.

Vulnerabilidad de la web

Una vulnerabilidad de la web es un código o comportamiento malicioso que se utiliza para aprovechar las fallas de codificación en una aplicación web. Agentes de amenaza pueden explotar las aplicaciones web vulnerables, lo que permite el acceso no autorizado, el robo de datos y la implementación de software malicioso.

Para mantenerte al día sobre los riesgos más críticos para las aplicaciones web, revisa el

Open Web Application Security Project (OWASP) Top 10

.

Software antivirus

El software antivirus (o anti-malware) es un programa utilizado para prevenir, detectar, y eliminar malware y virus. Dependiendo del tipo de software antivirus, puede escanear la memoria de un dispositivo para encontrar patrones que indiquen la presencia de software malicioso.

Sistema de detección de intrusiones

Un sistema de detección de intrusiones (IDS) es una aplicación que monitorea la actividad del sistema y alerta sobre posibles intrusiones. El sistema escanea y analiza paquetes de red, que transportan pequeñas cantidades de datos a través de una red. La pequeña cantidad de datos hace que el proceso de detección sea más fácil para que un IDS identifique posibles amenazas a los datos confidenciales. Otras ocurrencias que un IDS es capaz de detectar pueden incluir el robo y el acceso no autorizado.

Cifrado

El cifrado es el proceso de convertir datos de un formato legible a un formato codificado. La codificación criptográfica significa convertir texto plano en texto cifrado seguro. El texto plano es información sin cifrar y el texto cifrado seguro es el resultado del cifrado. Una forma criptográfica de código se utiliza para comunicarse en secreto y evitar el acceso no autorizado y no aprobado a datos, programas o dispositivos.

Nota: la codificación y el cifrado sirven para diferentes propósitos. La codificación utiliza un algoritmo de conversión pública para permitir que los sistemas que utilizan diferentes representaciones de datos compartan información. El cifrado hace que los datos sean ilegibles y difíciles de decodificar para usuarios/as no autorizados/as; su objetivo principal es garantizar la confidencialidad de los datos privados.

Pruebas de penetración

Las pruebas de penetración, también llamadas pen testing, son testeos que simulan un ataque, con el objetivo de ayudar a identificar vulnerabilidades en sistemas, redes, sitios web, aplicaciones y procesos. Mediante este cálculo de riesgos exhaustivo se pueden evaluar e identificar amenazas externas e internas, así como debilidades.

Conclusiones clave

En esta lectura, aprendiste más sobre la programación y los sistemas operativos. También te presentamos distintas herramientas y procesos. Cada organización selecciona su propio conjunto de herramientas. Por lo tanto, cuantas más conozcas, mayor será el valor que podrás aportar a una organización. Las herramientas ayudan a las/los analistas de seguridad a completar sus tareas de manera más eficiente y efectiva.

**Crea una cartera de ciberseguridad**

A lo largo de este programa de certificación, tendrás múltiples oportunidades para desarrollar una cartera profesional de ciberseguridad para mostrar tus habilidades y conocimientos de seguridad.

En esta lectura, aprenderás qué es una cartera y por qué es importante desarrollar una cartera profesional de ciberseguridad. También aprenderás sobre las opciones para crear una cartera en línea o autoalojada que puedes compartir con posibles empleadores/as cuando empieces a buscar trabajo en temas de ciberseguridad.

¿Qué es una cartera profesional y por qué es necesaria?

Las/las profesionales de ciberseguridad utilizan carteras para demostrar su educación, habilidades y conocimientos en seguridad cuando solicitan puestos de trabajo. Así, pueden mostrar a los/las potenciales empleadores/as que les apasiona su trabajo y que pueden desempeñar el puesto que solicitan. Las carteras profesionales son más completas que un currículum, que por lo general es un resumen de una a dos páginas que brinda información sobre educación relevante, experiencia laboral y logros. En el último curso de este programa, tendrás la oportunidad de desarrollar un currículum y finalizar tu cartera.

Opciones para crear tu cartera

Hay muchas maneras de presentar una cartera, incluidas las opciones autoalojadas y en línea, como:

Carpeta de documentos

Google Drive o Dropbox™

Google Sites

Repositorios Git

Opción 1: Carpeta de documentos

Descripción: Una carpeta de documentos es una carpeta creada y guardada en el disco duro de tu computadora. Tú administras la carpeta, las subcarpetas, los documentos y las imágenes dentro de ella.

Las carpetas de documentos te permiten tener un acceso directo a tu documentación. El tener tus documentos profesionales, imágenes y otra información bien organizados puede ahorrarte mucho tiempo cuando vayas a solicitar un trabajo. Por ejemplo, es posible que quieras crear una carpeta principal titulada “Documentos profesionales”. Luego, dentro de tu carpeta principal, puedes crear subcarpetas con títulos como:

Currículum

Educación

Documentos de la cartera

Herramientas de ciberseguridad

Programación

Configuración: las carpetas de documentos se pueden crear de varias maneras, dependiendo del tipo de computadora que utilices. Si no tienes claro cómo crear una carpeta en tu dispositivo, puedes buscar en Internet videos o documentos instructivos, de acuerdo al tipo de computadora que usas.

Opción 2: Google Drive o Dropbox

Descripción: Google Drive y Dropbox ofrecen funcionalidades similares que te permiten almacenar tu documentación profesional en una plataforma en la nube. Ambas opciones también tienen funciones para compartir archivos, por lo que puedes compartir fácilmente los documentos de tu cartera con posibles empleadores/as. Cualquier adición o cambio que hagas en un documento de esa carpeta se verá reflejado automáticamente y así lo verá cualquier persona que tenga acceso a tu cartera.

Al igual que una carpeta de documentos, mantener bien organizada tu cartera basada en Google Drive o Dropbox será útil a medida que comiences o avances en tu trayectoria profesional.

Configuración: para saber cómo cargar y compartir archivos en estas aplicaciones, visita los sitios web de Google Drive y Dropbox.

Opción 3: Google Sites

Descripción: Google Sites y las opciones de alojamiento de sitios web similares tienen una variedad de funcionalidades fáciles de usar para ayudarte a presentar los elementos de tu cartera, que incluyen diseños personalizables, páginas web responsivas, capacidades de contenido incrustado y publicación web.

Las páginas web responsivas ajustan automáticamente su contenido para adaptarse a una variedad de dispositivos y tamaños de pantalla. Esto es útil porque los/las empleadores/as potenciales pueden revisar tu contenido utilizando cualquier dispositivo y tus medios se mostrarán como tú quieras. Cuando tengas todo listo, puedes publicar tu sitio web y recibir una URL única. Puedes agregar este enlace a tu currículum para que las personas a cargo de las contrataciones accedan fácilmente a tu trabajo.

Configuración: para saber cómo crear un sitio web en Google Sites, visita el sitio web de Google Sites.

Opción 4: Repositorio Git

Descripción: un repositorio Git es una carpeta dentro de un proyecto. En este caso, el proyecto es tu cartera, y puedes usar tu repositorio para almacenar los documentos, laboratorios y capturas de pantalla que completes durante cada curso del programa de certificado. Hay varios sitios de repositorios Git que puedes usar, entre ellos:

GitLab

Bitbucket™

GitHub

Cada repositorio Git te permite mostrar tus habilidades y conocimientos en un espacio personalizable. Para crear una cartera de proyectos en línea en cualquiera de los repositorios mencionados, debes usar una versión de Markdown.

Configuración: para obtener información sobre cómo crear una cuenta de GitHub y usar Markdown, sigue los pasos descritos en el documento

Comienza con GitHub

.

Cartera de proyectos

Como mencionamos anteriormente, tendrás múltiples oportunidades a lo largo del programa de certificación para desarrollar elementos para incluir en tu cartera. Estas oportunidades incluyen:

Redacción de una declaración profesional

Realización de una auditoría de seguridad

Análisis de la estructura y seguridad de la red

Uso de comandos de Linux para administrar permisos de archivos

Aplicación de filtros a consultas SQL

Identificación de vulnerabilidades para una pequeña empresa

Documentación de incidentes con el diario de un gestor de incidentes

Importación y análisis de un archivo de texto en un escenario relacionado con la seguridad

Creación o revisión de un currículum

Nota: no incluyas en tu carpeta documentos privados, protegidos por derechos de autor o de propiedad intelectual. Además, si utilizas uno de los sitios descritos en esta lectura, mantén tu sitio configurado en “privado” hasta que termines.

Conclusiones clave

Ahora que conoces algunas opciones para crear y alojar una cartera profesional, puedes tomarlas en cuenta a medida que desarrollas elementos para incorporar, a lo largo del programa de certificación. Cuanto más proactivo/a seas a la hora de crear una cartera, bien armada, mayores serán tus posibilidades de impresionar a un/a empleador/a potencial y obtener un trabajo en ciberseguridad.

Términos del glosario de la semana 4

Términos y definiciones del curso 1, semana 4

Analizador de protocolo de red (rastreador de paquetes): Herramienta diseñada para capturar y analizar el tráfico de datos dentro de una red.

Base de datos: Colección organizada de información o datos estructurados.

Información de seguridad y gestión de eventos (SIEM): Solución de seguridad que recopila y analiza los datos de registro para monitorear actividades críticas en una organización.

Linux: Sistema operativo de código abierto.

Orden de volatilidad: Secuencia que establece el orden en que deben conservarse los datos, del primero al último, en relación al tiempo en que estarán disponibles.

Programación: Proceso que permite crear un conjunto específico de instrucciones para que una computadora ejecute tareas.

Protección y preservación de la evidencia: Proceso de trabajar adecuadamente con evidencia digital frágil y volátil.

Punto de dato: Elemento de información específico.

Registro: Inventario de eventos que tienen lugar dentro de los sistemas de una organización.

Sistema de detección de intrusiones (IDS): Aplicación que monitorea la actividad del sistema en busca de actividades intrusivas y toma medidas para detenerlas.

Software de antivirus: Programa utilizado para prevenir, detectar, y eliminar software malicioso y virus.

SQL (Structured Query Language): Lenguaje de programación utilizado para crear, interactuar y solicitar información de una base de datos.

¡Felicitaciones por completar el Curso 1 del Certificado de Carrera de Google en Ciberseguridad: Fundamentos de la ciberseguridad! En esta parte del programa, aprendiste sobre las posibles trayectorias profesionales y habilidades clave para los profesionales de ciberseguridad. También te presentamos los términos y conceptos fundamentales de la ciberseguridad que seguirás explorando a lo largo del programa de certificación.

El Certificado en Ciberseguridad de Google consta de ocho cursos.

Ocho íconos muestran los cursos secuencialmente de izquierda a derecha. El primer ícono es de un color diferente para indicar

Los fundamentos de la ciberseguridad — Explora la profesión de especialista en ciberseguridad, incluidos los acontecimientos que llevaron al desarrollo del campo de este campo y su importancia para la operación de las organizaciones. Aprende sobre las funciones y responsabilidades de nivel inicial de la especialización. (Este es el curso que acabas de completar. ¡Bien hecho!)

Ve a lo seguro: Gestiona los riesgos de seguridad — Identifica cómo las y los profesionales de la ciberseguridad utilizan los marcos y controles para proteger las operaciones comerciales y explora las herramientas más comunes.

Conexión y protección: Redes y seguridad de redes — Conoce las vulnerabilidades de las redes y cómo protegerlas.

Herramientas del oficio: Linux y SQL — Explora los conocimientos informáticos básicos, incluyendo la comunicación con el sistema operativo Linux a través de la línea de comandos y la consulta de bases de datos con SQL.

Activos, amenazas y vulnerabilidades — Conoce la importancia de los controles de seguridad y a conocer cómo se desarrolla la mentalidad de un agente de amenaza para poder prevenir, proteger y defender los activos de una organización frente a las diversas amenazas, riesgos y vulnerabilidades.

Haz sonar la alarma: Detección y respuesta — Comprende el ciclo de vida de la respuesta a incidentes y practica el uso de herramientas para detectar y responder a incidentes de ciberseguridad.

Automatiza las tareas de ciberseguridad con Python — Explora el lenguaje de programación Python y escribe código para automatizar las tareas de ciberseguridad.

Ponlo en práctica: Prepárate para los trabajos de ciberseguridad — Aprende sobre clasificación de incidentes, notificación a superiores y formas de comunicación con las partes interesadas. Este curso cierra el programa con consejos sobre cómo relacionarse con la comunidad de la ciberseguridad y prepararse para la búsqueda de empleo.

Ahora que completaste este curso, tienes todo listo para pasar al siguiente:

Ve a lo seguro: Gestiona los riesgos de seguridad

**Registros y herramientas SIEM**

Como analista de seguridad, una de tus responsabilidades podría incluir el análisis de datos de registro para mitigar y gestionar amenazas, riesgos y vulnerabilidades. Recuerda, un registro recopila eventos que ocurren dentro de los sistemas y redes de una organización. Las/los analistas de seguridad acceden a varios registros de diferentes fuentes. Tres fuentes de registro comunes incluyen: registros de firewall, registros de red y registros de servidor. Exploremos cada uno de estos con más detalle. Un registro de firewall documenta conexiones establecidas o intentadas para el tráfico entrante de Internet. También incluye solicitudes salientes a Internet desde dentro de la red.

Un registro de red es un registro de todos los dispositivos y computadoras que ingresan y salen de la red. También registra las conexiones entre dispositivos y servicios en la red. Por último, un registro de servidor es un registro de eventos relacionados con servicios, como sitios web, correos electrónicos o archivos compartidos. Incluye acciones como las solicitudes de inicio de sesión, contraseña y nombre de usuario. Mediante el monitoreo de registros como el que se muestra aquí, los equipos de seguridad pueden identificar vulnerabilidades y potenciales fugas de datos. Comprender los registros es importante porque las herramientas SIEM se basan en estos para monitorear sistemas y detectar amenazas a la seguridad. Una herramienta de gestión de eventos e información de seguridad, o SIEM, es una aplicación que recopila y analiza datos de registro para monitorear las actividades críticas en una organización. Proporciona visibilidad en tiempo real, monitoreo y análisis de eventos y alertas automáticas. También almacena todos los datos de registro en una ubicación centralizada. Dado que las herramientas SIEM indexan y minimizan el número de registros que un/a profesional de seguridad debe revisar y analizar manualmente, aumentan la eficiencia y ahorran tiempo. Pero las SIEM deben configurarse y personalizarse para satisfacer las necesidades particulares de cada organización. A medida que surgen amenazas y vulnerabilidades nuevas, las organizaciones deben personalizar continuamente sus herramientas SIEM para garantizar que se detecten las amenazas y abordarlas con rapidez. Más adelante en el programa, podrás practicar el uso de diferentes herramientas SIEM para identificar posibles incidentes de seguridad. Próximamente, exploraremos los paneles SIEM y cómo las/los profesionales de ciberseguridad los usan para monitorear amenazas, riesgos y vulnerabilidades.

**Paneles SIEM**

Hemos explorado cómo se usan las herramientas SIEM para recopilar y analizar datos de registro. Sin embargo, esta es una de las tantas formas en que las SIEM se usan en ciberseguridad. Las SIEM también se pueden usar para crear paneles. Es posible que hayas encontrado paneles en una aplicación en tu teléfono u otro dispositivo. Presentan información sobre tu cuenta o tu ubicación en un formato que es fácil de entender. Por ejemplo, las aplicaciones del clima muestran datos como temperatura, precipitaciones, velocidad del viento, y el pronóstico del tiempo mediante tablas, gráficos y otros elementos visuales. Este formato facilita identificar con rapidez patrones y tendencias del tiempo para que puedas prepararte y planificar tu día en consecuencia. Al igual que estas aplicaciones ayudan a las personas a tomar decisiones rápidas e informadas basadas en datos, los paneles SIEM brindan a las/los analistas de seguridad acceso rápido y fácil a la información de seguridad de su organización en forma de cuadros, gráficos o tablas. Por ejemplo, un/a analista de seguridad recibe una alerta sobre un intento de inicio de sesión sospechoso. El/la analista accede a su panel SIEM para recopilar información sobre esta alerta. Mediante el panel de control, el/la analista descubre que hubo 500 intentos de inicio de sesión para la cuenta de Ymara en un lapso de cinco minutos. También descubre que dichos intentos sucedieron en ubicaciones geográficas fuera de la ubicación usual de Ymara y fuera de su horario habitual de trabajo. Mediante un panel de control, el/la analista de seguridad pudo revisar rápidamente representaciones visuales de la cronología de dichos intentos, la ubicación, y el horario exacto de la actividad, y luego determinó que la actividad era sospechosa. Además de proporcionar un resumen exhaustivo de datos relacionados con la seguridad, los paneles SIEM también ofrecen a las partes interesadas diferentes métricas. Las métricas son atributos técnicos clave como el tiempo de respuesta, la disponibilidad y la tasa de errores, que se usan para evaluar el rendimiento de una aplicación de software. Los paneles SIEM se pueden personalizar para mostrar métricas específicas u otros datos relevantes para los distintos miembros de una organización. Por ejemplo, un/a analista de seguridad puede crear un panel de control que muestra métricas para el monitoreo diario de operaciones comerciales, como el volumen del tráfico de red entrante y saliente. Hemos examinado cómo los/las analistas de seguridad usan los paneles SIEM para ayudar a las organizaciones a mantener su postura de seguridad. ¡Bien hecho! A continuación, analizaremos algunas herramientas SIEM comunes utilizadas en la industria de la ciberseguridad. Nos vemos ahí.

El futuro de las herramientas SIEM

Anteriormente, aprendiste sobre las herramientas de gestión de eventos e información de seguridad (SIEM) y revisaste algunos ejemplos. En esta lectura, profundizarás en cómo se usan para proteger las operaciones de la organización. También conocerás cómo y por qué las herramientas SIEM están cambiando, para ayudar a proteger a las organizaciones y a las personas de la evolución de las tácticas y técnicas de los agentes de amenaza.

Soluciones SIEM actuales

Una herramienta SIEM es una aplicación que recopila y analiza datos de registro para monitorear actividades críticas, en una organización. Mediante el monitoreo y seguimiento en tiempo real de los registros de eventos de seguridad, se obtienen datos que se utilizan para realizar un análisis exhaustivo de cualquier amenaza, riesgo o vulnerabilidad de seguridad potencial identificada. Las herramientas SIEM tienen muchas opciones de panel de control y cada una de ellas ayuda a los miembros del equipo de ciberseguridad a gestionar y monitorear los datos de la organización. De todas maneras, estas herramientas requieren de la interacción humana para el análisis de eventos de seguridad.

El futuro de las herramientas SIEM

Como la ciberseguridad evoluciona y opera cada vez más en la nube, las herramientas SIEM continúan desarrollándose, para funcionar en entornos alojados y nativos de la nube. Las herramientas SIEM alojadas en la nube son operadas por proveedores que se encargan de mantener y administrar la infraestructura requerida. Se puede acceder a ellas fácilmente a través de Internet y representan una solución ideal para las organizaciones que prefieren no invertir en la creación y el mantenimiento de su propia infraestructura.

Al igual que las alojadas en la nube, las herramientas SIEM nativas de la nube son totalmente mantenidas y administradas por los proveedores, y se accede a ellas a través de Internet. Además, están diseñadas para aprovechar al máximo las capacidades de computación en la nube, como la disponibilidad, la flexibilidad y la adaptabilidad.

Las herramientas SIEM continuarán evolucionando, para adaptarse a la naturaleza cambiante de la tecnología y, también, a las nuevas tácticas y técnicas de los agentes de amenaza. Por ejemplo, piensa en el desarrollo actual de dispositivos interconectados con acceso a Internet, conocido como Internet de las cosas (IoT). Como cuantos más dispositivos interconectados haya, mayor será la superficie de ataque de ciberseguridad y la cantidad de datos que los agentes de amenaza pueden aprovechar, es esperable que aumente la diversidad de ataques y datos que requieren una atención especial.

Por otra parte, a medida que la tecnología de inteligencia artificial (IA) y aprendizaje automático (ML) progresen, las capacidades SIEM mejorarán, y podrán identificar mejor la terminología relacionada con la amenaza, así como la visualización del panel y la funcionalidad de almacenamiento de datos.

Además, la implementación de la automatización ayudará a incrementar la velocidad de respuesta de los equipos de seguridad frente a posibles incidentes, porque permite realizar numerosas acciones sin esperar una respuesta humana. Por ejemplo, Orquestación, Automatización y Respuesta de Seguridad (SOAR) es un conjunto de aplicaciones, herramientas y flujos de trabajo que utilizan la automatización para responder a incidentes de seguridad. Al utilizarlo, el manejo de incidentes comunes relacionados con la seguridad mediante el uso de herramientas SIEM se convierte en un proceso más simplificado y con menos intervención manual. Esto es importante ya que permite que las/los analistas de seguridad puedan abocarse a incidentes más complejos y poco comunes, que no se pueden automatizar con un SOAR.

Por otra parte, se espera que las plataformas referidas a la ciberseguridad se comuniquen e interactúen entre sí, aunque si bien ya existe la tecnología que permite la comunicación entre sistemas y dispositivos interconectados, aún está en fase de desarrollo.

Conclusiones clave

Las herramientas SIEM desempeñan un papel importante en el monitoreo de los datos de una organización. Como analista de seguridad de nivel inicial, puedes monitorear los paneles de SIEM como parte de tus tareas diarias. Investigar regularmente los nuevos desarrollos en tecnología SIEM te ayudará a crecer y adaptarte a los cambios en el campo de la ciberseguridad. La computación en la nube, la integración de aplicaciones SIEM y la automatización son solo algunos de los avances que las y los profesionales de seguridad pueden esperar en la futura evolución de las herramientas SIEM.

**Explora las herramientas comunes de SIEM**

¡Hola otra vez! Ya vimos cómo las herramientas SIEM ayudan a las/los analistas de seguridad a monitorear los sistemas y detectar amenazas a la seguridad. En este video, veremos algunas SIEM líderes en la industria que probablemente encuentres como analista de seguridad. Primero, vamos a analizar los distintos tipos de herramientas SIEM que las organizaciones pueden elegir según sus necesidades de seguridad. Las herramientas SIEM autoalojadas requieren que las organizaciones instalen, operen y mantengan la herramienta mediante su propia infraestructura física, como la capacidad del servidor. Quien gestiona y mantiene estas aplicaciones es el departamento de TI de la organización, no un proveedor de terceros.

Reproduce el video desde ::50 y sigue la transcripción0:50

Las herramientas SIEM autoalojadas son ideales cuando una organización debe mantener el control físico de datos confidenciales. Como alternativa, las herramientas SIEM alojadas en la nube son mantenidas y gestionadas por los proveedores de SIEM, lo cual las hace accesibles a través de Internet. Las SIEM alojadas en la nube son ideales para organizaciones que no quieren invertir en crear y mantener su propia infraestructura. O bien, una organización puede optar por utilizar una combinación de herramientas SIEM autoalojadas y alojadas en la nube, lo cual se conoce como una solución híbrida. Las organizaciones pueden elegir una solución SIEM híbrida para aprovechar las ventajas de la nube mientras mantienen el control físico sobre los datos confidenciales. Splunk Enterprise, Splunk Cloud, y Chronicle son herramientas SIEM comunes que utilizan muchas organizaciones para ayudar a proteger sus datos y sistemas. Comencemos con Splunk. Splunk es una plataforma de análisis de datos, y Splunk Enterprise ofrece soluciones SIEM. Splunk Enterprise es una herramienta autoalojada que se utiliza para retener, analizar y buscar los datos de registro de una organización para brindar información de seguridad y alertas en tiempo real. Splunk Cloud es una herramienta alojada en la nube que se utiliza para recopilar, buscar y monitorear datos de registro. Splunk Cloud es útil para organizaciones con entornos híbridos o solo en la nube, donde algunos o todos los servicios están en la nube. Por último, está Chronicle de Google. Chronicle es una herramienta nativa de la nube diseñada para retener, analizar y buscar datos. Chronicle ofrece monitoreo de registros y análisis y recolección de datos. Al igual que las alojadas en la nube, las herramientas nativas de la nube también son mantenidas y gestionadas por el proveedor. Pero estas están diseñadas específicamente para aprovechar al máximo las capacidades de la computación en la nube, como la disponibilidad, la flexibilidad y la adaptabilidad. Debido a que los actores de amenaza tienden a mejorar sus estrategias para comprometer la confidencialidad, integridad y disponibilidad de sus objetivos, es importante para las organizaciones usar varias herramientas de seguridad para defenderse de los ataques. Las herramientas SIEM que acabamos de ver son solo algunas de las herramientas disponibles para que los equipos de seguridad protejan a sus organizaciones. Más adelante en el programa, tendrás la emocionante oportunidad de practicar con Splunk Cloud y Chronicle.

Más información sobre herramientas de ciberseguridad

Anteriormente, conociste varias herramientas que usan los miembros del equipo de ciberseguridad para monitorear e identificar posibles amenazas, riesgos y vulnerabilidades de seguridad. En esta lectura, profundizarás en las herramientas de ciberseguridad más comunes, tanto de código abierto como propietarias, que puedes usar como profesional de la ciberseguridad.

Herramientas de código abierto

Las herramientas de código abierto suelen ser gratuitas y fáciles de usar. Su objetivo es proporcionar a los/las usuarios/as un software creado por las personas, de manera colaborativa, que puede resultar más seguro. Además, las herramientas de código abierto permiten una mayor personalización por parte de los/las usuarios/as, lo que da lugar a una variedad de nuevos servicios, creados a partir del mismo paquete de software de código abierto.

Los/las ingenieros/as de software crean proyectos de código abierto para mejorar el software y ponerlo a disposición de cualquier persona, siempre y cuando se respete la licencia especificada. El código fuente para proyectos de código abierto está fácilmente disponible para los/las usuarios/as, así como el material de capacitación que los acompaña. Esto permite a los/las usuarios/as modificar y mejorar los materiales del proyecto.

Herramientas propietarias

Las herramientas propietarias son propiedad de la persona o empresa que las desarrolla, y los/las usuarios/as generalmente pagan una tarifa por su uso y para su capacitación. Las/los dueños/as de las herramientas propietarias son los/las únicos/as que pueden acceder y modificar el código fuente. Esto significa que los/las usuarios/as tienen que esperar a que se realicen actualizaciones en el software y, posiblemente, pagar una tarifa por estas. El software propietario generalmente permite a los/las usuarios/as modificar un número limitado de características o funcionalidades para satisfacer las necesidades de una persona u organización. Algunos ejemplos de herramientas propietarias son las herramientas SIEM Chronicle y Splunk®.

Conceptos erróneos habituales

Existe la idea errónea de que las herramientas de código abierto son menos efectivas y no tan seguras de usar, en relación a las propietarias. Sin embargo, a lo largo de los años los/las desarrolladores/as han ido creando materiales de código abierto que se han convertido en estándares de la industria. Aunque es cierto que los agentes de amenaza han intentado manipular herramientas de código abierto, la realidad es que, justamente por ser de código abierto, es más difícil que las personas con intenciones maliciosas logren causar daño. La amplia exposición y el acceso inmediato al código fuente por parte de usuarios/as y profesionales bienintencionados/as e informados/as hace que sea menos probable que ocurran problemas, ya que pueden solucionarlos tan pronto como se identifican.

Ejemplos de herramientas de código abierto

En ciberseguridad, hay muchas herramientas que son de código abierto y comúnmente disponibles. Dos ejemplos son Linux y Suricata.

Linux

Linux es un sistema operativo de código abierto ampliamente utilizado, que te permite adaptarlo a tus necesidades a través de una interfaz de línea de comandos. Un sistema operativo es la interfaz entre el hardware de la computadora y el usuario, y se usa para comunicarse con el hardware de una computadora y gestionar las aplicaciones de software.

Existen distintas versiones de Linux para realizar tareas específicas. Más adelante en el programa de certificación, hablaremos a fondo de Linux y su interfaz de línea de comandos.

Suricata

Suricata es un software de análisis de redes de código abierto y detección de amenazas. Este tipo de software se utiliza para analizar el tráfico de red, identificar comportamientos sospechosos y generar registros de datos de red. Al detectar la actividad entre usuarios, computadoras o direcciones de Protocolo de Internet (IP), ayuda a descubrir posibles amenazas, riesgos o vulnerabilidades.

Suricata fue desarrollado por la Open Information Security Foundation (OISF), una organización que se dedica a mantener el uso del código abierto del proyecto Suricata, para así garantizar que sea gratuito y esté disponible públicamente. Suricata es muy usado en el sector público y privado, y se integra con muchas herramientas SIEM y otras de seguridad. También profundizaremos sobre Suricata más adelante en el programa.

Conclusiones clave

Las herramientas de código abierto son muy usadas en la profesión de la ciberseguridad. A lo largo del programa de certificación, tendrás múltiples oportunidades para aprender y explorar en detalle las herramientas, tanto de código abierto como propietarias.

Usa herramientas SIEM para proteger a las organizaciones

Anteriormente, leíste sobre las herramientas de gestión de eventos e información de seguridad (SIEM) y algunos paneles SIEM. También aprendiste sobre diferentes amenazas, riesgos y vulnerabilidades que una organización puede experimentar. En esta lectura, conocerás más acerca de los datos del panel de control de SIEM y cómo las y los profesionales de ciberseguridad los utilizan para identificar una amenaza, riesgo o vulnerabilidad potencial.

Splunk

Splunk ofrece diferentes opciones de herramientas SIEM: Splunk® Enterprise y Splunk® Cloud. Ambas te permiten revisar los datos de una organización en paneles (dashboards). Esto ayuda a las y los profesionales de seguridad a gestionar la infraestructura interna de una organización mediante la recopilación, búsqueda, monitoreo y análisis de datos de registro de múltiples fuentes, y a observar así la totalidad de las operaciones diarias de una organización.

Revisa los siguientes paneles de Splunk y sus propósitos:

Panel de postura de seguridad

El panel de postura de seguridad está diseñado para centros de operaciones de seguridad (SOC). Muestra los acontecimientos y tendencias destacados de una organización en cuanto a seguridad, durante las últimas 24 horas, y permite a las/los profesionales determinar si la infraestructura y las políticas de seguridad funcionan según lo diseñado. Las/los analistas de seguridad pueden usar este panel para monitorear e investigar amenazas potenciales en tiempo real, como una actividad de red sospechosa cuyo origen es una dirección IP específica.

Panel de resumen ejecutivo

El panel de resumen ejecutivo analiza y monitorea la salud general de la organización a lo largo del tiempo. Esto ayuda a los equipos de seguridad a mejorar las medidas que reducen el riesgo. Las/los analistas de seguridad podrían usar este panel para proporcionar información de alto nivel a las partes interesadas, como generar un resumen de incidentes y tendencias de seguridad durante un periodo de tiempo determinado.

Panel de revisión de incidentes

El panel de revisión de incidentes permite a las/los analistas identificar patrones sospechosos que pueden ocurrir en caso de un incidente. Además, destaca elementos de alto riesgo que necesitan una revisión inmediata por parte de un/a analista. Este panel puede ser muy útil porque proporciona una cronología visual de los eventos que condujeron a un incidente.

Panel de análisis de riesgos

El panel de análisis de riesgos ayuda a las/los analistas a identificar el riesgo para cada objeto de riesgo (por ejemplo, un usuario específico, una computadora o una dirección IP). Muestra cambios en la actividad o el comportamiento en relación con el riesgo, como un/a usuario/a que inicia sesión fuera de las horas de trabajo normales o un tráfico de red inusualmente alto desde una computadora específica. Un/a analista de seguridad podría usar este panel para analizar el impacto potencial de las vulnerabilidades en activos críticos, lo cual ayuda a priorizar sus esfuerzos de mitigación de riesgos.

Chronicle

Chronicle es una herramienta SIEM nativa de la nube de Google que retiene, analiza y busca datos de registro para identificar posibles amenazas, riesgos y vulnerabilidades de seguridad. Chronicle te permite recopilar y analizar datos de registro de acuerdo con:

un activo específico

un nombre de dominio

un usuario

una dirección IP

Chronicle proporciona múltiples paneles que ayudan a las/los analistas a monitorear los registros de una organización, crear filtros y alertas y rastrear nombres de dominio sospechosos.

Revisa los siguientes paneles de Chronicle y sus propósitos:

Panel de información empresarial (Enterprise Insights)

El panel de información empresarial muestra las alertas recientes. Identifica nombres de dominio sospechosos en los registros, conocidos como indicadores de compromiso (IOC), y cada resultado se etiqueta con una puntuación de confianza para indicar la probabilidad de una amenaza. También proporciona un nivel de gravedad, que indica la importancia de cada amenaza para la organización. Un/a analista de seguridad podría usar este panel para monitorear los intentos de inicio de sesión o acceso a datos relacionados con un activo crítico, como una aplicación o sistema, desde ubicaciones o dispositivos inusuales.

Panel de transferencia y estado de los datos

El panel de transferencia y estado de los datos muestra el número de registros de eventos, fuentes de registro y tasas de éxito de los datos que se procesan en Chronicle. Un/a analista de seguridad podría usar este panel para asegurarse de que los orígenes de los registros estén configurados correctamente y que se reciban sin errores. Esto garantiza que el equipo de seguridad tenga acceso a los datos que se necesitan, al abordar los problemas relacionados con el registro.

El panel de coincidencias de IOC

El panel de coincidencias de IOC indica las principales amenazas, riesgos y vulnerabilidades para la organización. Las y los profesionales de seguridad utilizan este panel para observar los nombres de dominio, las direcciones IP y los IOC de los dispositivos a lo largo del tiempo, con el fin de identificar tendencias. Esta información les permite hacer foco en las principales amenazas. Por ejemplo, las/los analistas de seguridad pueden usar este panel para buscar actividad adicional asociada con una alerta, como un inicio de sesión de usuario sospechoso desde una ubicación geográfica inusual.

Panel principal

El panel principal muestra un resumen de alto nivel de la información relacionada con la ingestión de datos, las alertas y la actividad de eventos de la organización, a lo largo del tiempo. Las y los profesionales de seguridad pueden usar este panel para acceder a una cronología de eventos de seguridad, como un pico en intentos de inicio de sesión fallidos, para identificar tendencias de amenazas en fuentes de registro, dispositivos, direcciones IP y ubicaciones físicas.

Panel de detección de reglas

El panel de detección de reglas proporciona estadísticas de incidentes con el mayor índice de ocurrencias, severidades y detecciones a lo largo del tiempo. Las/los analistas de seguridad pueden usar este panel para acceder a una lista de todas las alertas activadas por una regla de detección específica, como una regla diseñada para alertar cada vez que un/a usuario/a abre un archivo adjunto malicioso conocido, desde un correo electrónico. Las/los analistas luego usan esas estadísticas para ayudar a gestionar incidentes recurrentes y establecer tácticas de mitigación, que permitan reducir el nivel de riesgo de una organización.

Panel de descripción general del acceso de usuarios

El panel de descripción general del acceso de usuarios proporciona información acerca del comportamiento de acceso de usuarios/as en toda la organización. Las/los analistas de seguridad pueden usar este panel para acceder a una lista de todos los eventos de inicio de sesión de usuarios para identificar las actividades inusuales, como el inicio de sesión de un mismo usuario desde varias ubicaciones al mismo tiempo. Esta información se usa para ayudar a mitigar las amenazas, los riesgos y las vulnerabilidades de las cuentas de usuario y las aplicaciones de la organización.

Conclusiones clave

Las herramientas SIEM proporcionan paneles (dashboards) que ayudan a las/los profesionales de seguridad a organizar y enfocar sus esfuerzos de seguridad. Esto es importante porque permite a las/los analistas reducir el riesgo al identificar, analizar y remediar los elementos prioritarios, de manera oportuna. Más adelante en el programa, tendrás la oportunidad de practicar el uso de varias funciones y comandos de la herramienta SIEM para consultas de búsqueda.

Conclusión

Revisemos rápidamente lo que abarcamos en esta sección del curso. Comenzamos hablando de la importancia de los registros y la ciberseguridad. Exploramos diferentes tipos de registro: registros del servidor, red y firewall. Luego exploramos los paneles de control SIEM y la manera en que utilizan representaciones visuales para brindar a los equipos de seguridad información clara y rápida sobre la postura de seguridad de una organización. Por último, presentamos herramientas SIEM comunes utilizadas en la industria de la ciberseguridad, como Splunk y Chronicle. Más adelante, exploraremos aún más herramientas de seguridad, y tendrás la oportunidad de practicar su uso. A continuación, analizaremos los manuales de estrategia y cómo ayudan a las/los profesionales de seguridad a responder adecuadamente para identificar amenazas, riesgos y vulnerabilidades. Nos vemos ahí.

Términos y definiciones del curso 2, semana 3

Chronicle: Herramienta nativa de la nube diseñada para conservar, analizar y buscar datos.

Información de seguridad y gestión de eventos (SIEM): Aplicación que recopila y analiza datos de registro para monitorear actividades críticas en una organización.

Manual de estrategias: Guía que proporciona detalles sobre cualquier acción operativa.

Métricas: Atributos técnicos clave, como el tiempo de respuesta, la disponibilidad y la tasa de fallos, que se utilizan para evaluar el rendimiento de una aplicación de software.

Orquestación, automatización y respuesta de seguridad (SOAR): Conjunto de aplicaciones, herramientas y flujos de trabajo que utilizan la automatización para responder a incidentes de seguridad.

Registro: Inventario de eventos que tienen lugar dentro de los sistemas de una organización.

Respuesta a incidentes: Intento rápido de una organización de identificar un ataque, contener los daños y corregir los efectos de una infracción de seguridad.

Sistema Operativo (SO): Interfaz entre la computadora y el/la usuario/a.

Splunk Cloud: Herramienta alojada en la nube que se utiliza para recopilar, buscar y monitorear datos de registro.

Splunk Enterprise: Herramienta utilizada para retener, analizar y buscar datos de registro de una organización y proporcionar información de seguridad y alertas en tiempo real.

**Fases de un manual de estrategias para responder a incidentes**

Anteriormente, vimos cómo las herramientas SIEM se utilizan para proteger activos y datos críticos de una organización. En este video, presentaremos otra herramienta importante para mantener la seguridad de la organización, conocida como manual de estrategias. Un manual de estrategias es una guía que brinda detalles sobre cualquier acción operativa. También aclaran qué herramientas deben usarse para responder a un incidente de seguridad. En el campo de la seguridad, los manuales de estrategias son fundamentales. La urgencia, la eficiencia y la precisión son necesarias para identificar y mitigar rápidamente una amenaza de seguridad y así reducir el riesgo potencial. Los manuales de estrategias garantizan que la gente siga una lista coherente de acciones de forma prescrita, independientemente de quién esté trabajando en el caso. Se utilizan diferentes tipos de manuales de estrategias. Estos incluyen manuales de respuesta a incidentes, alertas de seguridad y propósitos específicos de equipos y de productos. Aquí nos centraremos en un manual utilizado comúnmente en la ciberseguridad: el Manual de respuesta a incidentes. La respuesta a incidentes es el intento rápido de una organización para identificar un ataque, contener el daño y corregir los efectos de una fuga de información. Un manual de respuesta a incidentes es una guía con seis fases que se usa para ayudar a mitigar y gestionar incidentes de seguridad de principio a fin.

Reproduce el video desde :1:37 y sigue la transcripción1:37

Analicemos cada fase.

Reproduce el video desde :1:40 y sigue la transcripción1:40

La primera fase es la preparación. Las organizaciones deben prepararse para mitigar la probabilidad, el riesgo y el impacto de un incidente de seguridad, documentando procedimientos, creando planes para el personal y formando a los/las usuarios/as. La preparación sienta las bases para una respuesta a incidentes exitosa. Por ejemplo, las organizaciones pueden crear planes y procedimientos de respuesta a incidentes que delinean los roles y responsabilidades de cada miembro del equipo de seguridad. La segunda fase es detección y análisis. El objetivo de esta fase es detectar y analizar eventos mediante procesos y tecnología definidos. El uso de las herramientas y estrategias adecuadas durante esta fase ayuda a los/las analistas de seguridad a determinar si se produjo una fuga y analizar su posible magnitud.

Reproduce el video desde :2:39 y sigue la transcripción2:39

La tercera fase es la contención. El objetivo de la contención es prevenir un mayor daño y reducir el impacto inmediato de un incidente de seguridad. Durante esta fase, los/las profesionales de la seguridad actúan para contener un incidente y minimizar el daño. La contención es una prioridad alta para las organizaciones porque ayuda a prevenir riesgos permanentes para datos y activos críticos. La cuarta fase en un manual de respuesta a incidentes es la erradicación y recuperación. Esta fase implica la eliminación completa de los artefactos de un incidente, de manera que una organización pueda volver a operar con normalidad. Durante esta fase, los/las profesionales de seguridad eliminan los artefactos del incidente al suprimir códigos maliciosos y mitigar vulnerabilidades. Una vez que ejecutaron la debida diligencia, pueden comenzar a restaurar el entorno afectado a un estado seguro. Esto también se conoce como la restauración de TI.

Reproduce el video desde :3:43 y sigue la transcripción3:43

La quinta fase es la actividad posterior al incidente. En esta fase, se documenta el incidente, se informa a los/las directivos/as de la organización y se aplican las lecciones aprendidas para garantizar que la organización esté mejor preparada para manejar futuros incidentes. Dependiendo de la gravedad del incidente, las organizaciones pueden realizar un análisis de incidentes a gran escala para determinar el origen del incidente, e implementar varias actualizaciones o mejoras para mejorar su postura general de seguridad. La sexta y última fase en un manual de respuesta a incidentes es la coordinación. La coordinación implica informar incidentes y compartir información durante todo el proceso de respuesta a incidentes en base a los estándares de la organización. La coordinación es importante por muchas razones. Asegura que las organizaciones satisfagan los requisitos de cumplimiento y permite una respuesta y resolución coordinadas. Hay muchas maneras de alertar sobre un incidente a los/las profesionales de la seguridad. Acabas de aprender sobre las herramientas SIEM, y cómo recolectan y analizan datos. Estos datos se utilizan para detectar amenazas y generar alertas que pueden informar al equipo de seguridad de un posible incidente. Luego, cuando un/a analista de seguridad recibe una alerta SIEM, puede usar el manual de estrategias apropiado para guiar el proceso de respuesta. Los manuales y herramientas SIEM trabajan juntos para brindar una forma de respuesta estructurada y eficaz a posibles incidentes de seguridad. A lo largo del programa, tendrás la oportunidad de seguir profundizando en la comprensión de estos conceptos importantes.

Más sobre los manuales de estrategias

Anteriormente, aprendiste que los manuales de estrategias son herramientas que utilizan las y los profesionales de la ciberseguridad para identificar problemas de seguridad y responder a ellos. En esta lectura, aprenderás más sobre estos manuales y su propósito en el campo de la ciberseguridad.

Descripción general del manual de estrategias

Un manual de estrategias es una guía que brinda detalles sobre cualquier acción operativa. Básicamente, proporciona una lista predefinida y actualizada de pasos para responder a un incidente.

Una analista usando un manual de estrategias.

Los manuales van acompañados de una estrategia, que describe las expectativas de los miembros del equipo, a quienes se les asigna una tarea. Algunos también enumeran a las personas responsables. Las expectativas descritas van acompañadas de un plan, que indica cómo se debe completar la tarea específica descrita en el manual.

Los manuales de estrategias deben tratarse como documentos vivos, o sea, los miembros del equipo de seguridad los actualizan con frecuencia, para abordar los cambios de la industria y las nuevas amenazas. Generalmente, se administran de forma colaborativa, porque los miembros del equipo de seguridad tienen diferentes niveles de experiencia.

Los manuales de estrategias se modifican, particularmente, en los siguientes casos:

Cuando se identifica una falla, como un descuido en las políticas y procedimientos descritos o en el manual en sí.

Cuando hay un cambio en los estándares de la industria, por ejemplo, en las leyes o en el cumplimiento normativo.

Cuando el panorama de la ciberseguridad cambia debido a la evolución de las tácticas y técnicas de los agentes de amenaza.

Tipos de manuales de estrategias

Los manuales de estrategias a veces cubren vulnerabilidades e incidentes específicos. Estos podrían incluir ransomware (secuestro de datos), vishing, compromiso de correo electrónico empresarial (BEC) y otras ofensivas que ya mencionamos. Los manuales de respuesta a incidentes y vulnerabilidades son muy comunes, pero no son los únicos tipos de manuales que desarrollan las organizaciones.

Cada organización tiene un conjunto diferente de herramientas, metodologías, protocolos y procedimientos a los que adhieren, y diferentes personas están involucradas en cada paso del proceso de respuesta, dependiendo del país en el que se encuentren. Por ejemplo, los requisitos de notificación de incidentes de las leyes y regulaciones impuestas por el gobierno, junto con los estándares de cumplimiento, afectan al contenido de los manuales de estrategias. Estos requisitos están sujetos a cambios según el lugar donde se originó el incidente y el tipo de datos afectados.

Manuales de respuesta a incidentes y vulnerabilidades

Los manuales de respuesta a incidentes y vulnerabilidades son muy utilizados por las y los profesionales de ciberseguridad de nivel inicial. Se desarrollan en función de los objetivos descritos en el plan de continuidad empresarial de una organización, que es un camino establecido que permite a una empresa recuperarse y continuar operando con normalidad, a pesar de una interrupción como, por ejemplo, una fuga de información.

Estos dos tipos de manuales contienen listas predefinidas y actualizadas de pasos para responder a un incidente. Seguir estos pasos es necesario para garantizar que tú, como profesional de la seguridad, te adhieras a los estándares y protocolos legales y organizativos. Estos manuales también ayudan a minimizar los errores y garantizar que las acciones importantes se lleven a cabo en un plazo determinado.

Cuando un incidente, amenaza o vulnerabilidad ocurre o se identifica, el nivel de riesgo para la organización depende del daño potencial a sus activos. Una fórmula básica para determinar el nivel de riesgo es que el riesgo es igual a la probabilidad de una amenaza. Por esta razón, actuar rápido es fundamental. Si se lleva a cabo alguna tarea forense, también es importante seguir los pasos descritos en los manuales de estrategias, porque un mal manejo puede comprometer fácilmente estos datos y hacerlos inutilizables.

Los pasos comunes incluidos en los manuales de respuesta a incidentes y vulnerabilidades incluyen:

Preparación

Detección

Análisis

Contención

Erradicación

Recuperación ante un incidente

Los pasos adicionales incluyen la realización de actividades posteriores al incidente y una coordinación de esfuerzos, a lo largo de las etapas de investigación y respuesta a incidentes y vulnerabilidades.

Conclusiones clave

Es fundamental perfeccionar los procesos y procedimientos descritos en un manual de estrategias. Con cada incidente documentado, los equipos de ciberseguridad deben considerar lo que se aprendió de él y qué mejoras se deben implementar para lidiar con ellos de manera más eficaz en el futuro. De esta manera, los manuales de estrategias crean estructura y garantizan el cumplimiento de la ley.

Recursos para obtener información adicional

Los manuales de respuesta a incidentes y vulnerabilidades son solo dos ejemplos de los muchos manuales de estrategias que utiliza una organización. Si planeas trabajar como profesional de ciberseguridad fuera de los Estados Unidos, podrías explorar otros recursos como:

Reino Unido, National Cyber Security Center (NCSC) — manejo de incidentes

Gobierno de Australia — Plan de respuesta a incidentes cibernéticos

Gobierno de Canadá — Manual de prácticas sobre Ransomware

Gobierno de Escocia — Plantillas de manuales de estrategia

**Uso de un manual de respuesta a amenazas, riesgos o vulnerabilidades**

¡Hola de nuevo! En este video, vamos a repasar las herramientas SIEM y la manera en que se usan junto con los manuales de estrategias para reducir amenazas, riesgos y vulnerabilidades en la organización. Un manual de respuesta a incidentes es una guía que ayuda a los/las profesionales de la seguridad a mitigar los problemas con mayor urgencia pero manteniendo la precisión. Los manuales de estrategia crean estructura, garantizan el cumplimiento, y esbozan los procesos para la comunicación y la documentación. Las organizaciones pueden usar distintos tipos de manuales de respuesta a incidentes en función de la situación. Por ejemplo, una organización puede tener manuales de estrategias específicos para abordar diferentes tipos de ataques, como ransomware, software malicioso, denegación del servicio distribuida y más. Para empezar, analicemos cómo un/a analista de seguridad podría usar un manual para abordar una alerta SIEM, como un posible ataque de software malicioso.

Reproduce el video desde :1:4 y sigue la transcripción1:04

En esta situación, un manual de estrategias es fundamental para guiar a un/a analista a través de las acciones necesarias para abordar correctamente la alerta. La primera acción en el manual es evaluar la alerta. Esto significa determinar si es realmente válida al identificar por qué la alerta fue generada por la SIEM. Esto puede lograrse si se analizan los datos de registro y las métricas relacionadas. Luego, el manual de estrategias describe las acciones y herramientas a utilizar para contener el malware y reducir el daño aún más. Por ejemplo, este manual le enseña al analista a aislar o desconectar el sistema de red infectado para evitar que el software malicioso se propague en otras partes de la red. Después de contener el incidente, el tercer paso del manual de estrategias describe las formas de eliminar todo rastro del incidente y restaurar los sistemas afectados para que vuelvan a operar con normalidad. Por ejemplo, el manual de estrategias puede indicarle al analista que restaure el sistema operativo afectado, y luego hacer eso mismo con los datos afectados mediante una copia de seguridad limpia, creada antes del brote de malware. Por último, una vez resuelto el incidente, el cuarto paso del manual le indica al analista que realice varias actividades posteriores al incidente y tareas de coordinación con el equipo de seguridad. Algunas acciones incluyen crear un informe final para comunicar el incidente de seguridad a las partes interesadas, o informar del incidente a las autoridades competentes, como la Oficina Federal de Investigaciones de los EE.UU. u otras agencias que investigan delitos cibernéticos. Este es solo un ejemplo de cómo puedes seguir los pasos en un manual de estrategias, ya que las organizaciones desarrollan sus propios procedimientos para abordar incidentes de seguridad. Lo más importante es comprender que los manuales de estrategias proporcionan un proceso consistente que deben seguir las/los profesionales de la seguridad. Recuerda que los manuales de estrategias son documentos activos. Es decir: el equipo de seguridad hará cambios, actualizaciones y mejoras frecuentes para abordar nuevas amenazas y vulnerabilidades. Además, las organizaciones aprenden de incidentes de seguridad pasados para mejorar su postura de seguridad, perfeccionar las políticas y los procedimientos y reducir la probabilidad y el impacto de futuros incidentes. Luego, actualizan sus manuales en consecuencia. Como analista de seguridad de nivel inicial, quizá se te solicite usar estos manuales con frecuencia, en especial al monitorear las redes y responder a los incidentes. Comprender por qué los manuales de estrategias son importantes y cómo pueden ayudarte a lograr tus objetivos laborales asegurará tu éxito dentro de este campo.

Manuales de estrategias, herramientas SIEM y herramientas SOAR

Anteriormente, aprendiste que los equipos de seguridad suelen encontrar amenazas, riesgos, vulnerabilidades e incidentes y que utilizan los manuales de estrategias para abordar los problemas relacionados con la seguridad. En esta lectura, aprenderás más sobre los manuales de estrategias, incluida la forma en que se utilizan en la gestión de eventos e información de seguridad (SIEM) y en la orquestación, automatización y respuesta de seguridad (SOAR).

Manuales de estrategias y herramientas SIEM

Los manuales de estrategias son muy utilizados por los equipos de ciberseguridad ya que garantizan que, en caso de un incidente, se siga una lista consistente de acciones de una manera prescrita, independientemente de quién esté trabajando en el caso. Los manuales pueden ser muy detallados e incluir diagramas de flujo y tablas, para aclarar qué acciones tomar y en qué orden. También se utilizan para los procedimientos de recuperación, en caso de un ataque de ransomware (secuestro de datos). Los diferentes tipos de incidentes de seguridad tienen sus propios manuales de estrategias que detallan quién debe tomar qué acción y cuándo debe hacerlo.

Los manuales de estrategias suelen usarse junto con las herramientas SIEM. Si, por ejemplo, una herramienta SIEM señala el comportamiento inusual de un usuario, un manual de estrategias proporciona a las/los analistas instrucciones sobre cómo abordar el problema.

Manuales de estrategias y herramientas SOAR

Los manuales de estrategias también se utilizan con herramientas SOAR. Las herramientas SOAR son similares a las SIEM, ya que también se usan para el monitoreo de amenazas. SOAR es un programa informático utilizado para automatizar tareas repetitivas generadas por herramientas como las SIEM o la detección y respuesta administrada (MDR). Por ejemplo, si un/a usuario/a intentara iniciar sesión en su computadora demasiadas veces con la contraseña incorrecta, un SOAR bloquearía automáticamente su cuenta para detener una posible intrusión. Luego, las/los analistas consultarían el manual de estrategias para tomar medidas que permitan resolver el problema.

Conclusiones clave

Los manuales de estrategias, también llamados runbooks, indican acciones detalladas a ser implementadas por los equipos de seguridad, si se produce un incidente. Saber exactamente quién debe llevar a cabo cada acción y cuándo hacerlo puede ayudar a reducir el impacto de un incidente y el riesgo de daños a los activos críticos de una organización.

Términos y definiciones del curso 2, semana 4

Manual de estrategias: Guía que proporciona detalles sobre cualquier acción operativa.

Software antivirus: Programa utilizado para prevenir, detectar y eliminar software malicioso y virus.