CIBERDELITOS

Programa del curso

Audiencia

La audiencia principal es el analista de primera línea, se enseñan habilidades que benefician a los empleados nuevos y los que cuentan con experiencia, especialmente a medida que aumentan las expectativas de las entidades reguladoras y del mercado. Este curso supone que el empleador ya ha presentado los roles, procesos, sistemas y casos comunes exclusivos de la organización y el curso no entrará en conflicto con ellos. Para llevar a todos los alumnos a una base de referencia compartida de terminología, conceptos y procesos, el curso comienza con el video "*Aspectos básicos*" y se desarrolla a partir de allí.

El curso está escrito y presentado por expertos en la materia que trabajan en todo el mundo. Usa ejemplos de muchos países y es apropiado a nivel global. Las lecciones y los ejemplos son relevantes para cualquier industria. Un enfoque principal son las "instituciones financieras", que incluyen bancos, cooperativas de crédito, administradores de activos, seguros, MSB, corredores de valores, entidades emisoras de tarjetas de crédito, sistemas de pago alternativos, etc.

Estructura del curso

ACAMS le permite utilizar 4 semanas calendario para completar **4 horas de trabajo del curso**, incluida una evaluación final. Será guiado por medio de una ruta de aprendizaje en el sistema de gestión de aprendizaje (siglas en Ingles LMS) de ACAMS. Siga atentamente todas las instrucciones. Los eventos de aula virtual en vivo se programan previamente, antes de comprar el curso. Su acceso expirará tras 4 semanas de la fecha de inicio del curso.

	Asignación	Formato	Descargar del LMS
Semana uno	VIDEO de 30 minutos *"Aspectos básicos"*	Video: a su propio ritmo, disponible en cualquier momento.	PDF de referencia rápida
Semana dos	AULA VIRTUAL de 90 minutos	Evento en vivo: ver fecha/hora en el LMS. Luego, una grabación estará disponible en el LMS.	Diapositivas en PDF
Semana tres	AULA VIRTUAL de 90 minutos	Evento en vivo: ver fecha/hora en el LMS. Luego, una grabación estará disponible en el LMS.	Diapositivas en PDF
Semana cuatro	TAREA de 15 minutos EVALUACIÓN EN LÍNEA de 15 minutos	A su propio ritmo, disponible en cualquier momento. A su propio ritmo, disponible en cualquier momento.	Asignación en PDF Certificado de ACAMS en PDF

Para obtener el certificado, debe superar la evaluación dentro de las 4 semanas. La evaluación tiene 20 preguntas. La puntuación mínima para aprobar es del 80 %. Se permiten varios intentos. Cuando apruebe, su certificado de ACAMS estará disponible en la misma ruta de aprendizaje. Haga clic para descargar un PDF. ACAMS agregará automáticamente 4 créditos CAMS a su perfil.

Requisitos técnicos

El curso es compatible con la mayoría de los sistemas operativos y navegadores para que sea más fácil participar. El sistema de gestión de aprendizaje (LMS) de ACAMS es https://lms.acams.org. Póngase en contacto con el departamento de TI de su organización para obtener ayuda.

Refuerce las defensas de su organización para proteger los datos y los activos financieros..

Resultados conductuales de este curso:

1. Describir la tremenda amenaza que representa el ciberdelito para su organización e identificar los métodos de ataque más comunes.
2. Identificar los "puntos débiles" en los que su organización es más vulnerable a los ciberatacantes.
3. Crear un plan efectivo de preparación y respuesta para los ciberataques para evitar que se explote a la organización, los clientes y su reputación.
4. Recolectar, analizar e informar datos de inteligencia para ayudar a las fuerzas de seguridad en la identificación y captura de ciberdelincuentes.

Contenido del curso

1. Introducción
   a. Definición: FinCEN define el "ciberdelito" como actividades ilegales (por ejemplo, fraude, lavado de dinero, robo de identidad) realizadas o facilitadas por sistemas y dispositivos electrónicos, como redes y computadoras.
   b. Relación con ALD-CFT
      i. De qué modo los informes de BSA ayudan a las autoridades de los EE. UU. a combatir los cibereventos y el ciberdelito
      ii. Requiere un conjunto adicional de habilidades técnicas
      iii. Muchos estudiantes serán víctimas
   c. Beneficios de combatir el ciberdelito
      i. Para usted, personalmente
      ii. Para la organización
      iii. Para las fuerzas de seguridad
      iv. Para la sociedad
   d. Objetivos de aprendizaje: Una vez completada esta actividad de aprendizaje, podrá hacer lo siguiente:
      i. Conocer a los cazadores: Describir la tremenda amenaza que representa el ciberdelito para su organización e identificar los métodos de ataque más comunes.
      ii. Evitar convertirse en la presa: Identificar los "puntos débiles" en los que su organización es más vulnerable a los ciberatacantes.

iii. Defenderse: Crear un plan efectivo de preparación y respuesta para los ciberataques para evitar que se explote a la organización, los clientes y su reputación

iv. iv. Ser proactivo, no reactivo: Recolectar, analizar e informar datos de inteligencia para ayudar a las fuerzas de seguridad en la identificación y captura de ciberdelincuentes.

2. Conocer a los cazadores: Describir la tremenda amenaza que representa el ciberdelito para su organización e identificar los métodos de ataque más comunes.
   a. El ciberdelito está creciendo
   b. Los ciberdelincuentes están mejorando
   c. El alto costo del ciberdelito
      i. Desde el punto de vista financiero
      ii. Desde el punto de vista de su cliente
      iii. El ciberdelito es extremadamente perjudicial para la reputación de su empresa
   d. Las tipologías más comunes
      i. Tipos tradicionales de ALD disfrazadoscomo ciberdelito
         1. Ataques directos a la institución financiera o a dinero administrado por el gobierno
            a. Acceso no autorizado a fondos, datos, líneas de crédito:
               i. Phishing (incluye spear phishing)
               ii. Spoofing
               iii. Malware
               iv. Ingeniería social (como el abuso de personas mayores)
                  1. Incluye las redes sociales, como los cambios de trabajo anunciados a través de LinkedIn
               v. Hackear a través de vulnerabilidades
            b. Ransomware
            c. DDoS
            d. Fondos virtuales falsificados (por ejemplo, tarjetas de crédito/débito/regalo, transferencias bancarias, etc.)
            e. Información sobre transacciones falsificadas para ocultar rutas o historiales a fin de permitir el blanqueo de dinero, el financiamiento del terrorismo, la evasión de sanciones
               i. Manipulación de datos
               ii. Acceso/apertura de cuentas virtuales
               iii. Desviación de datos o fondos
               iv. Conversión de moneda

2. Ataques contra titulares de cuentas individuales
    a. Acceso no autorizado a fondos, datos o líneas de crédito administrados por el individuo o la institución financiera (robo de identidad)
        i. Phishing
        ii. Malware
        iii. Ingeniería social
        iv. Hacking
    b. Ransomware
    c. Fondos virtuales falsificados (tarjetas de crédito/débito/regalo, ACH, etc.)
3. Ejemplos
    a. Banco de Bangladesh, febrero de 2016
        i. USD 81 millones robados
        ii. Hasta el 1/2017, aún sin resolver
    b. Tesco Bank, noviembre de 2016
        i. Uno de los ciberataques más grandes contra un banco del Reino Unido
        ii. Casi un tercio de las cuentas de depósitos se vieron afectadas
        iii. GBP 2,5 millones robados
4. Otros

e. Advertencias

f. Sanciones

3. Evitar convertirse en la presa: Identificar los "puntos débiles" en los que su organización es más vulnerable a los ciberatacantes.
    a. Esta es la manera más probable que utilizarán los atacantes para entrar
        i. Los hackers son sofisticados, pero la mayoría obtiene acceso al engañar a un empleado crédulo
        ii. Artículo de Wall Street Journal, "Cyber Soft Spots: Hackers Exploit Staffers at Banks" (Puntos débiles cibernéticos: los hackers se aprovechan de los empleados de los bancos)
    b. Cómo se engaña a los empleados
        i. Memorias USB
        ii. A través de enlaces en correos electrónicos
            1. Phishing, Spear phishing
        iii. Archivos adjuntos

iv. Malware
    1. Disfrazados de juegos gratis o pornografía
    2. Malware de 2007, 2010, 2011, 2012, 2013 todavía en uso
v. Estafas de SWIFT
vi. Hackers
    1. Codiciadas credenciales de cuenta
    2. A menudo se encuentran en archivos desprotegidos, como las hojas de cálculo
    3. Las redes sociales brindan a los hackers inteligencia valiosa
        a. Nuevo trabajo o ascenso
        b. Los viajes de negocios: los mensajes automáticos por ausencia alertan a los hackers cuando la computadora no está monitoreada
    4. Los hackers venden datos
        a. Números de seguridad social, números de teléfono, direcciones, números de tarjetas de crédito
vii. Mulas de dinero
    1. Cuentas embudo
    2. Muchos usuarios, pero solo una identidad subyacente
viii. Ejemplos
    1. EE. UU.
    2. Reino Unido o global
ix. Evalúe su organización y dónde se encuentran las debilidades

4. Defenderse: Crear un plan efectivo de preparación y respuesta para los ciberataques para evitar que se explote a la organización, los clientes y su reputación.
    a. Simulaciones prácticas
    b. Trabaje conjuntamente con el equipo de sistemas
    c. Cree un plan
        i. Políticas aprobadas por el Consejo Directivo de la empresa
        ii. Informes
        iii. Haga cosas antes de tiempo para prepararse
        iv. Priorice según el impacto en la reputación y los niveles de pérdida de su organización
    d. Debe practicar su plan
        i. El equipo de respuesta instantánea debe establecer relaciones con las fuerzas de seguridad de antemano. (¡No elija a su equipo el día del juego!).
        ii. Ejemplo del banco de Bangladesh

e. Prácticas recomendadas
    i. Autenticación de dos factores
    ii. Gestión de parches
    iii. Identifique y proteja los activos más valiosos de su organización

5. Ser proactivo, no reactivo: Recolectar, analizar e informar datos de inteligencia para ayudar a las fuerzas de seguridad en la identificación y captura de ciberdelincuentes.
    a. Requisitos de presentación de ROS relacionados
        i. Incluya la información ciberrelacionada, relevante y disponible
            1. Direcciones IP con marcas de tiempo
            2. Información de billetera virtual
            3. Identificadores de dispositivo
            4. Metodologías utilizadas
            5. Etc.
    b. Involucre al equipo de seguridad de red de su organización
        i. Debe colaborar con las unidades internas de ciberseguridad
            1. La información provista por las unidades de ciberseguridad podría revelar patrones adicionales de comportamiento sospechoso e identificar sospechosos desconocidos previamente por las unidades de BSA/ALD
            2. Del mismo modo, el personal de ciberseguridad puede usar la información provista por BSA/ALD para protegerse contra los cibereventos y los delitos ciberrelacionados
    c. Comparta información con otras instituciones financieras para protegerse de, e informar sobre loo siguiente:
        i. Lavado de dinero
        ii. Financiación del terrorismo
        iii. Ciberdelitos
        iv. Según la sección 314(b), las instituciones financieras participantes pueden intercambiar información, incluida la ciberrelacionada, con respecto a:
            1. Individuos
            2. Entidades
            3. Organizaciones
            4. Países

v. Colaboración de la industria
    1. Alianza nacional de capacitación cibernética forense (NCFTA)
        a. Asociación público-privada
    2. Otros

d. Tendencias futuras en ciberseguridad
    i. Cómo mantenerse varios pasos por delante
    ii. Proactivo en comparación con Reactivo