ACAMS® | Certificates

CRIME CIBERNÉTICO

Programa do curso

Público

O alvo principal é o analista de linha da frente, ensinando técnicas que beneficiam os funcionários novos e experientes, especialmente na medida em que aumentam as expectativas de mercado e reguladoras. Este curso pressupõe que o empregador já apresentou aqueles papéis, processos, sistemas e casos comuns exclusivos da organização e este curso não entrará em conflito com eles. Para trazer todos os estudantes para uma base compartilhada de terminologia, conceitos e processos, o curso começa com o vídeo "*Fundamentos*" e em seguida, desenvolve a partir daí.

O curso é escrito e apresentado por especialistas no assunto trabalhando ao redor do mundo. Traz exemplos de muitos países e é globalmente adequado. As lições e exemplos são relevantes para qualquer indústria. Um foco primário são as "instituições financeiras", incluindo bancos, cooperativas de crédito, gestores de ativos, seguros, MSB (empresas de serviços monetários), corretores e distribuidores de títulos, administradoras de cartões de crédito, sistemas de pagamento alternativos, etc.

Estrutura do curso

A ACAMS concede a você 4 semanas para completar **4 horas de curso**, incluindo uma avaliação final. Você será orientado usando um roteiro de aprendizado no sistema de gestão de aprendizagem (LMS) da ACAMS. Siga atentamente todas as instruções. Eventos ao viva em sala de aula virtual são pré-agendadas antes de você comprar o curso. Seu acesso expira 4 semanas a partir da data de início do curso.

	Tarefa	Formato	Download do LMS
Primeira semana	30 min – VIDEO *"Essentials"*	Vídeo: Ritmo próprio, disponível a qualquer hora	Consulta rápida em PDF
Segunda semana	90 min – SALA DE AULA VIRTUAL	Evento ao vivo: Ver o LMS para data/hora. Posteriormente uma gravação estará no LMS.	Slides PDF
Terceira semana	90 min – SALA DE AULA VIRTUAL	Live event: See LMS for date/time. Later a recording will be on the LMS.	Slides PDF
Quarta semana	15 mins– TAREFA DE CASA 15 min – AVALIAÇÃO ON-LINE	Ritmo próprio, disponível a qualquer hora Ritmo próprio, disponível a qualquer hora	Tarefa em PDF Certificado ACAMS em PDF

Para obter o certificado, você deve passar na avaliação nas 4 semanas. A avaliação possui 20 perguntas. A pontuação mínima para passar é 80%. São permitidas múltiplas tentativas. Quando você passar, seu Certificado ACAMS estará disponível no próprio roteiro de aprendizado. Clique aqui para fazer o download do PDF. A ACAMS adicionará automaticamente 4 Créditos CAMS ao seu perfil.

Requisitos técnicos :

O curso é compatível com a maioria dos sistemas operacionais e navegadores para tornar mais fácil a participação. O sistema de gestão de aprendizagem (LMS) da ACAMS está em https://lms.acams.org. Entre em contato com o departamento de TI de sua organização para obter assistência.

Fortaleça as defesas da sua organização para proteger dados e ativos financeiros.

Resultados comportamentais deste curso:

1. Descrever a enorme ameaça que os crimes cibernéticos constituem para sua organização e identificar os métodos mais comuns de ataque
2. Identificar os "pontos fracos" onde a sua organização é mais vulnerável aos invasores cibernéticos
3. Criar uma preparação e plano de resposta a um ataque cibernético eficazes para proteger sua organização, seus clientes e sua reputação de ser explorado
4. Coletar, analisar e relatar informações de inteligência para auxiliar as autoridades policiais na identificação e captura de criminosos cibernéticos

Conteúdo do curso

1. Introdução
   a. Definição: A FinCEN define "Crimes Cibernéticos" como atividades ilegais (por exemplo, fraude, lavagem de dinheiro, roubo de identidade) efetuados ou facilitados por sistemas eletrônicos e dispositivos, tais como redes e computadores.
   b. Relação com PLD-CFT
      i. Como a notificação BSA ajuda as autoridades dos EUA a combater eventos e crimes cibernéticos
      ii. Requer um conjunto de habilidades técnicas adicional
      iii. Muitos estudantes serão vítimas
   c. Benefícios de combater o crime cibernético
      i. Para você, pessoalmente
      ii. Para a organização
      iii. Para as autoridades policiais
      iv. Para a sociedade
   d. Objetivos de aprendizagem: Após a conclusão desta atividade de aprendizagem, você será capaz de:
      i. Reconheça os caçadores: Descrever a enorme ameaça que os crimes cibernéticos constituem para sua organização e identificar os métodos mais comuns de ataque
      ii. Evitar ser a presa: Identificar os "pontos fracos" onde a sua organização é mais vulnerável aos invasores cibernéticos
      iii. Defender-se: Criar uma preparação e plano de resposta a um ataque cibernético eficazes para proteger sua organização, seus clientes e sua reputação de ser explorado

iv. Ser proativo x reativo: Coletar, analisar e relatar informações de inteligência para auxiliar as autoridades policiais na identificação e captura de criminosos cibernéticos

2. Reconheça os caçadores: Descrever a enorme ameaça que os crimes cibernéticos constituem para sua organização e identificar os métodos mais comuns de ataque
   a. Os crimes cibernéticos estão crescendo
   b. Cibercriminosos estão ficando melhores
   c. O alto custo do crime cibernético
      i. De um ponto de vista financeiro
      ii. Do ponto de vista de seu cliente
      iii. O cibercrime e extremamente danoso para a reputação de sua empresa
   d. As tipologias mais comuns
      i. Traditional AML types repackaged as cybercrime
         1. Ataques diretamente na instituição financeira ou dinheiro gerido pelo governo
            a. Acesso não autorizado a fundos, dados, linhas de crédito:
               i. Phishing (inclui Spear Phishing)
               ii. Falsificação
               iii. Malware
               iv. Engenharia social (como abusos contra idosos)
                  1. Inclui as mídias sociais, tais como mudanças de emprego anunciadas através do LinkedIn
               v. Hacking usando vulnerabilidades
            b. Ransomware
            c. DDoS
            d. Falsificação de fundos virtuais (por exemplo, cartões de crédito/débito/presente, transferências bancárias, etc.)
            e. Informações de transações falsificadas para disfarçar rotas ou histórias, a fim de permitir a lavagem de dinheiro, financiamento de terroristas, evasão de sanções
               i. Manipulação de dados
               ii. Abertura/acesso de conta virtual
               iii. Redirecionamento de dados ou fundos
               iv. Conversão de moedas
         2. Ataques contra os detentores de conta individuais
            a. Acesso não autorizado a fundos, dados ou linhas de crédito gerenciada pelo indivíduo e/ou instituição financeira (roubo de identidade)

i. Phishing
ii. Malware
iii. Engenharia social
iv. Hacking

b. Ransomware
c. Falsificação de fundos virtuais (cartões de
d. crédito/débito/presente, ACH ou "Automated Clearing House", etc.)

3. Exemplos
    a. Banco de Bangladesh, fevereiro de 2016
        i. i$ 81 milhões roubados
        ii. Até 1/2017, ainda sem resolução
    b. Tesco Bank, novembro de 2016
        i. Um dos maiores ataques cibernéticos já feitos em um banco do Reino Unido
        ii. Quase um terço das contas de depósito foram comprometidas
        iii. £ 2,5 milhões roubados
    c. Outro(s)

e. Sinais de alerta
f. Sanções

3. Evitar ser a presa: Identificar os "pontos fracos" onde a sua organização é mais vulnerável aos invasores cibernéticos
    a. Assim é como os invasores provavelmente vão entrar
        i. Os hackers são sofisticados embora a maioria entre enganando um funcionário ingênuo
        ii. Artigo do Wall Street Journal, "Pontos fracos cibernéticos: hackers exploram funcionários de bancos"
    b. Como os funcionários são enganados
        i. Pen drives
        ii. Através de links em e-mails
            1. Phishing, Spear phishing
        iii. Anexos
        iv. Malware
            1. Disfarçados como jogos grátis ou pornografia
            2. Malwares de 2007, 2010, 2011, 2012, 2013 ainda em uso

v. Golpes na SWIFT (Society for Worldwide Interbank Financial Telecommunications - Sociedade de Telecomunicações Financeiras Interbancárias Mundiais)
vi. Hackers
    1. Credenciais de conta cobiçadas
    2. Muitas vezes em arquivos desprotegidos como planilhas
    3. As mídias sociais dão aos hackers informações valiosas
        a. Novo emprego ou promoção
        b. Viagem a negócios - mensagens de "fora do escritório" alertam os hackers quando seu computador não é monitorado
    4. Hackers vendem dados
        a. Números da previdência social, números de telefone, endereços, números de cartão de crédito
vii. Mulas de dinheiro
    1. Contas funil
    2. Muitos usuários, mas uma identidade oculta
viii. Exemplos
    1. EUA
    2. Reino Unido ou global
ix. Avalia sua organização e onde estão as fraquezas

4. Defender-se: Criar uma preparação e plano de resposta a um ataque cibernético eficazes para proteger sua organização, seus clientes e sua reputação de ser explorado
    a. Simulações de mesa
    b. Trabalha em conjunto com as equipes de sistemas
    c. Cria um plano
        i. Políticas aprovadas pelo conselho de administração
        ii. Notificação
        iii. Fazer as coisas com antecedência para se preparar
        iv. Priorizar com base no impacto na reputação de sua organização e níveis de perda
    d. Precisa praticar seu plano
        i. A equipe de resposta instantânea deve estabelecer relações com as autoridades policiais com antecedência. (Não escolha sua equipe no dia do jogo!)
        ii. Exemplo do banco de Bangladesh
    e. Práticas recomendadas
        i. Autenticação de dois fatores
        ii. Gerenciamento de correções
        iii. Identificar e proteger os ativos mais valiosos de suas organizações

5. Ser proativo x reativo: Coletar, analisar e relatar informações de inteligência para auxiliar as autoridades policiais na identificação e captura de criminosos cibernéticos
    a. Requisitos de registro do SAR relacionados
        i. Incluir informações cibernéticas relevantes e disponíveis
            1. Endereços IP com carimbos de data/hora
            2. Informações de carteira virtual
            3. Identificadores de dispositivos
            4. Metodologias usadas
            5. Etc.
    b. Envolvendo a equipe de segurança de rede de sua organização
        i. Precisa colaborar com unidades de segurança cibernética internas
            1. Informações fornecidas pelas unidades de segurança cibernética revelariam padrões adicionais de comportamento suspeito e identificariam suspeitos não conhecidos previamente pelas unidades de BSA/PLD
            2. Da mesma forma, o pessoal de segurança cibernética pode usar informações fornecidas pela BSA/PLD para se proteger contra eventos/crimes cibernéticos
    c. Compartilhar informações entre outras instituições financeiras para proteção e notificação de:
        i. Lavagem de dinheiro
        ii. Financiamento de terroristas
        iii. Crime cibernético
        iv. Sob a Seção 314 (b), as IFs participantes podem trocar informações, incluindo informações cibernéticas, com relação a:
            1. Indivíduos
            2. Entidades
            3. Organizações
            4. Países
        v. Colaboração no setor
            1. National Cyber Forensic Training Alliance (NCFTA)
                a. Parceria público-privada
            2. Outros
    d. Futuras tendências em segurança cibernética
        i. Como ficar vários passos à frente
        ii. Proativo x Reativo