CERBEYRA
ACADEMY

La sicurezza parte dalla conoscenza

Knowledge that protects you

Proteggi il tuo futuro digitale con una formazione continua, progettata per creare un mondo più sicuro e consapevole

Restare un passo avanti alle minacce non è solo una necessità, è la chiave per affrontare con serenità le sfide del futuro digitale. La sicurezza informatica è una scelta strategica e imprescindibile per le organizzazioni che vogliono crescere e prosperare in un contesto digitale sempre più complesso e in rapida evoluzione.

Adottare solo strumenti tecnologici non basta, serve un cambio di mentalità che metta al centro la **cultura della prevenzione**. Una strategia vincente parte dalla **conoscenza** e dalla **consapevolezza**: solo un team formato può diventare la prima linea di difesa contro le minacce cibernetiche.

Con **Cerbeyra Academy**, la formazione si trasforma in un vero e proprio **asset strategico**. Ogni corso è progettato per potenziare le competenze del tuo team e offrire un approccio pratico e innovativo, basato su esercitazioni, simulazioni di scenari reali e le migliori pratiche internazionali. Questo approccio consente ai partecipanti di non limitarsi a comprendere i rischi, ma di sapere come anticiparli, gestirli e mitigare i loro effetti.

Perché investire nella formazione fa la differenza

Investire nella formazione significa fare della prevenzione una risorsa strategica: un team preparato rappresenta la prima linea di difesa contro le minacce digitali. La **consapevolezza** e le **competenze** acquisite consentono di individuare i rischi in anticipo e prevenirli in modo efficace.

Un team formato non solo riduce l'esposizione al rischio, ma assicura una gestione consapevole degli incidenti, minimizzando l'impatto sulle attività e garantendo la continuità operativa dell'azienda. Infine, un'organizzazione che investe nella sicurezza informatica rafforza la propria competitività, trasmettendo fiducia ai clienti e ai partner, consolidando la propria reputazione e distinguendosi per affidabilità e lungimiranza.

Perché scegliere **Cerbeyra Academy**?

Cerbeyra Academy offre una formazione continua, con corsi costantemente aggiornati per garantire conoscenze allineate alle normative più recenti e alle tecniche di difesa più efficaci. L'**approccio pratico** caratterizza ogni percorso: attraverso esercitazioni, simulazioni di attacchi e analisi di casi reali, i partecipanti acquisiscono competenze applicabili fin da subito al contesto lavorativo.

I partecipanti ricevono inoltre una **certificazione riconosciuta**, con attestati rilasciati dal **Centro Studi Cyber Defense** di Cerbeyra, un valore aggiunto che attesta il loro percorso formativo. La formazione offre flessibilità, combinando corsi online, accessibili ovunque grazie ai materiali digitali, e corsi in presenza per un'esperienza pratica e concreta.

Un altro punto di forza? La **personalizzazione**. Cerbeyra Academy offre percorsi modulari, progettati per rispondere alle esigenze specifiche di aziende di diverse dimensioni e settori, creando un'esperienza formativa su misura che si adatta alle necessità del team.

Scegliere Cerbeyra Academy significa investire nella **crescita professionale** delle persone, rafforzando la **resilienza** e garantendo la continuità operativa dell'intera organizzazione.

CERBEYRA
ACADEMY

Programma dei Corsi Formativi 2025

CERBEYRA

Cyber Security Fundamentals

Proteggi il tuo futuro digitale dalle basi

Il corso ***Cyber Security Fundamentals*** offre una panoramica completa sulle principali minacce informatiche e sugli strumenti per contrastarle. Scoprirai come prevenire attacchi comuni come phishing e malware e come creare una cultura della sicurezza che coinvolga tutta l'organizzazione.

COSA IMPARERAI

- Riconoscere le principali minacce informatiche e prevenirle con strategie efficaci.
- Applicare i principi fondamentali della sicurezza informatica, come il modello CIA (Confidenzialità, Integrità, Disponibilità).
- Difendere i sistemi aziendali dai malware attraverso un uso consapevole delle tecnologie.

PROGRAMMA DEL CORSO

- **Introduzione alla Cyber Security**: Definizione, contesto attuale e importanza per le aziende.
- **Il modello CIA**: Analisi approfondita dei tre pilastri della sicurezza informatica e loro applicazione pratica.
- **Difesa contro il phishing**: Tecniche per riconoscere e gestire tentativi di frode.
- **Prevenzione dei malware**: Strategie per ridurre al minimo i rischi legati a virus, trojan e ransomware.
- **Best practice per la sicurezza delle reti**: Gestione delle credenziali, autenticazione a più fattori e monitoraggio delle attività.

Durata: 2 ore

Modalità: Online

CERBEYRA

Corso di Formazione sulla Direttiva NIS2

Rafforza la tua conformità alle normative europee

La ***Direttiva NIS2*** rappresenta un pilastro della sicurezza informatica europea. Questo corso è progettato per guidarti attraverso i requisiti chiave, aiutandoti a sviluppare strategie efficaci di protezione delle reti e dei sistemi aziendali e a gestire gli incidenti con prontezza.

COSA IMPARERAI

- Comprendere gli obiettivi della Direttiva NIS2 e le sue implicazioni operative.
- Applicare misure di sicurezza per la protezione di reti, sistemi e infrastrutture critiche.
- Implementare processi di gestione del rischio informatico.
- Prepararti a notificare e documentare gli incidenti secondo le tempistiche previste.
- Valutare la conformità della tua organizzazione attraverso audit interni ed esterni.

PROGRAMMA DEL CORSO

- **Introduzione alla Cyber Resilience:** Principi chiave, differenze con focus su resistenza, risposta e recupero.
- **Gestione del rischio:** Strategie per identificare e mitigare i rischi con framework come ISO 27001 e NIST.
- **Governance e resilienza operativa:** Best practice per integrare la sicurezza nei processi aziendali e sviluppare una governance solida.
- **Protezione delle infrastrutture critiche:** Misure proattive di difesa: firewall, crittografia, MFA e sistemi di rilevamento delle intrusioni.
- **Gestione degli incidenti:** Creazione di un piano di risposta efficace con simulazioni pratiche e gestione della crisi.
- **Casi studio e simulazioni**: Esercitazioni su scenari reali per consolidare competenze e migliorare la risposta.

Durata: 2 ore **Modalità**: Online

CERBEYRA

Corso di Formazione su DORA

Rendi la tua organizzazione resiliente ai rischi operativi digitali

Il corso ***DORA (Digital Operational Resilience Act)*** è pensato per chi opera nel settore finanziario e desidera acquisire le competenze necessarie per gestire la resilienza operativa e rispettare i requisiti della normativa. I partecipanti impareranno a implementare strategie di protezione e piani di continuità operativa efficaci.

COSA IMPARERAI

- Comprendere i requisiti chiave di DORA e la loro applicazione pratica.
- Implementare misure di resilienza digitale per garantire la continuità dei servizi.
- Sviluppare strategie per monitorare e gestire i rischi dei fornitori di servizi digitali.

PROGRAMMA DEL CORSO

- **Introduzione a DORA:** Obiettivi principali e ambiti di applicazione.
- **Gestione del rischio operativo digitale:** Tecniche di analisi dei rischi e mitigazione delle vulnerabilità.
- **Pianificazione per la continuità operativa:** Creazione di piani di recovery per garantire l'operatività anche in caso di attacco informatico.
- **Monitoraggio e test:** Come effettuare audit di sicurezza e simulazioni per verificare la resilienza.

Durata: 2 ore

Modalità: Online

CERBEYRA

Cyber Resilience per il Management

Una visione strategica per una sicurezza proattiva

Il corso ***Cyber Resilience***, progettato per il management aziendale, esplora le competenze necessarie per integrare la resilienza digitale nei processi aziendali. Dalla gestione dei rischi alla creazione di un piano di risposta agli incidenti, il corso copre tutti gli aspetti essenziali per una protezione completa.

COSA IMPARERAI

- Integrare la resilienza digitale nella strategia aziendale.
- Definire piani di business continuity per ridurre al minimo l'impatto di un attacco.
- Promuovere una cultura della sicurezza e sensibilizzare i dipendenti.

PROGRAMMA DEL CORSO

- **Concetti chiave di Cyber Resilience:** Differenze tra cyber security e cyber resilience.
- **Risk management:** Analisi dei rischi informatici e strategie di mitigazione.
- **Risposta agli incidenti:** Implementazione di piani di intervento per contenere e risolvere gli attacchi.
- **Simulazioni di attacchi:** Esercitazioni per testare la prontezza del team e migliorare le misure di difesa.

Durata: 2 ore **Modalità**: Online

CERBEYRA

Corso di Cognitive Security

Anticipare le minacce, rafforzare la mente

Il corso ***Cognitive Security – Social Engineering & Phishing Simulation*** fornisce competenze avanzate per creare e gestire campagne di phishing mirate, sfruttando le tecniche di social engineering. I partecipanti impareranno a identificare e sfruttare le vulnerabilità psicologiche e cognitive degli utenti, testando la resilienza aziendale contro minacce reali tramite la piattaforma di Phishing Simulator di Cerbeyra.

COSA IMPARERAI

- Identificare e sfruttare le vulnerabilità psicologiche e cognitive degli utenti.
- Creare e gestire campagne di phishing mirate utilizzando tecniche avanzate di social engineering.
- Valutare l'efficacia della risposta aziendale attraverso simulazioni di attacco.
- Migliorare la resilienza dell'organizzazione contro minacce di social engineering.
- Sviluppare strategie per prevenire e contrastare attacchi di phishing e manipolazione psicologica.

PROGRAMMA DEL CORSO

- **Introduzione alla Cognitive Security:** Fondamenti e importanza della sicurezza cognitiva.
- **Tecniche di Social Engineering:** Come individuare e sfruttare le vulnerabilità cognitive degli utenti.
- **Phishing Simulation:** Creazione e gestione di campagne di phishing tramite la piattaforma di Cerbeyra.
- **Valutazione della resilienza:** Analisi della risposta organizzativa e miglioramento dei processi.
- **Strategie di prevenzione e difesa:** Best practice per aumentare la consapevolezza e rafforzare le difese aziendali.

Durata: 4 ore

Modalità: Online

CERBEYRA

Corso di Ethical Hacking Avanzato

Oltre i confini della sicurezza: attacco e difesa avanzati

Il corso ***Ethical Hacking Avanzato*** offre un approccio avanzato alle tecniche di vulnerability assessment e penetration testing, includendo attacchi fisici, cognitivi e su sistemi di intelligenza artificiale. I partecipanti impareranno a eseguire test di penetrazione su sistemi, reti e infrastrutture, sfruttando vulnerabilità fisiche e psicologiche per valutare e migliorare la sicurezza aziendale. Il corso include l'uso di strumenti open hardware per simulare scenari di attacco complessi e aumentare la resilienza organizzativa.

COSA IMPARERAI

- Eseguire vulnerability assessment e penetration test avanzati su sistemi, reti e infrastrutture fisiche.
- Sfruttare vulnerabilità fisiche e psicologiche per testare la resilienza aziendale.
- Utilizzare strumenti open hardware per simulare scenari di attacco complessi.
- Testare la sicurezza di sistemi di intelligenza artificiale e rispondere a minacce cognitive.
- Migliorare la strategia di difesa aziendale attraverso l'analisi degli scenari di attacco.

PROGRAMMA DEL CORSO

- **Introduzione all'Ethical Hacking Avanzato:** Evoluzione delle tecniche di attacco e difesa.
- **Vulnerability Assessment:** Identificazione e analisi delle vulnerabilità su sistemi, reti e applicazioni.
- **Penetration Testing:** Esecuzione di test avanzati per individuare e sfruttare vulnerabilità.
- **Attacchi fisici e cognitivi:** Sfruttare vulnerabilità umane e fisiche per testare la resilienza.
- **Open Hardware e simulazioni di attacco:** Utilizzo di dispositivi di hacking fisico per creare scenari reali.
- **Risposta e mitigazione:** Strategie per rafforzare la sicurezza dopo la valutazione dei rischi.

Durata: 2 giorni **Modalità**: In Presenza

CERBEYRA ACADEMY

Knowledge that protects you

Cerbeyra S.p.A. - Gruppo Vianova S.p.A
Via Libeccio 48/F - Z.I. Cotone
55049 Viareggio (LU)
P.IVA e CF 01766360463

www.cerbeyra.com | info@cerbeyra.com | 0584.43671