La sicurezza dei sistemi, dei dati e delle reti

Il corso affronta il problema della sicurezza, analizzando tutti i componenti a rischio presenti in un'azienda che utilizza reti aperte basate su tecnologia TCP/IP, con particolare attenzione alle vulnerabilità dell'interconnessione con l'Internet pubblica. Una volta introdotte le problematiche di scenario, in relazione agli attacchi ai sistemi e alle possibili azioni e contromisure, vengono presentati approfondimenti specifici sulle tecniche più diffuse tra gli hacker per attaccare un sistema.L'attenzione viene poi focalizzata sulla crittografia, utilizzata come strumento per assicurare riservatezza e integrità ai dati e per prevenire rischi derivanti dall'accesso non autorizzato alle informazioni veicolate tramite servizi di larga diffusione, come, la posta elettronica e il WWW.Il corso prosegue analizzando le possibili soluzioni per realizzare una adeguata protezione perimetrale utilizzando i Firewall e per estendere i confini della propria rete privata con l'ausilio di tunnel cifrati tra più sedi e utenti remoti interconnessi tramite una rete dati pubblica.

Agenda (5 giorni)

La sicurezza informatica: lo scenario di riferimento, i concetti base.

Introduzione alla sicurezza aziendale: architettura, gestione e procedure:

standard di riferimento per la sicurezza: TCSEC, ITSEC, CC.
una classificazione dei possibili attacchi: esterni/interni
vulnerabilità intrinseche dell'architettura TCP/IP.

Tecniche per condurre un attacco:

attacchi di bassa complessità: packet sniffing, spoofing, session hijacking, man-in-the-middle
anatomia di un attacco e tools usati.

Strumenti per la sicurezza dei dati: crittografia, algoritmi simmetrici e asimmetrici, funzioni di hash:

algoritmi a chiave simmetrica (DES, AES) e a chiave asimmetrica (DH, RSA)
applicare la crittografia: firma digitale e certificati digitali.

Esempi applicatici: la sicurezza wi-fi (WEP e WPA).

Problematiche di sicurezza connesse ai principali servizi Internet_based:

soluzioni per una posta elettronica sicura: PGP e S/MIME
standard per transazioni commerciali e web: Secure Socket Layer (SSL)
la sicurezza dei sistemi e delle applicazioni client: es. Internet Explorer e Outlook.

Strumenti di verifica livelli di sicurezza implementati: scanner, IDS:

strumenti di logging e event correlation.

Le problematiche di sicurezza nell'accesso alle risorse ospitate in una rete aziendale TCP/IP:

la sicurezza nell'accesso, autenticazione tramite RADIUS server
la sicurezza nell'accesso tramite Internet pubblica: router, ACL e proxy server
realizzare una soluzione di sicurezza perimetrale: architetture Firewall, possibili implementazioni.

Estendere i confini della propria rete privata: Reti Private Virtuali (IPSEC).

Obiettivi

Al termine del corso i partecipanti sono in grado di:

avere una chiara comprensione delle problematiche della sicurezza informatica e delle più comuni tipologie di attacco
conoscere i principali standard del settore
padroneggiare gli strumenti più idonei per rivelare/contrastare attacchi informatici.

Destinatari e Prerequisiti

A chi è rivolto

Responsabili di sistemi informativi, centri elaborazione dati e di infrastrutture di rete, progettisti di sistemi di rete e tutti coloro che desiderano avere una visione d'insieme delle varie tematiche connesse alla sicurezza dei sistemi e delle reti.

Prerequisiti

Conoscenza di base dell'uso delle reti di computer e dei principali protocolli connessi al TCP/IP.

Iscrizione

Quota di Iscrizione: 2.240,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

È un corso GOLD

con due partecipazioni potrai concordare con noi la data. Guarda i vantaggi della formula GOLD.

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

Cyber Security: Minacce e Criteri di Protezione

Il cyberspace è oggi il termine più utilizzato per indicare le dimensioni digitali della società dall'avvento di Internet. Per chi opera a garanzia degli interessi nazionali di un Paese o di una Industria è necessario impostare una propria politica di cyber security che oltre alle tecnologie affronti aspetti sociali, legali ed economici. Le minacce coinvolgono diversi attori. Istituzioni, Industria privata, Cittadini sono vulnerabili e il Cyber Crime può operare acquisendo informazioni riservate e/o delicate da utilizzare per attaccare infrastrutture critiche di vitale importanza o beni tangibili di singoli. Il cyberspace, secondo l'approccio militare, ha la dimensione di un vero campo di battaglia e come tale ci si muove con tecniche di intelligence (Cyber War). Lo scenario internazionale ed italiano si analizza sia in termini legislativi che di processi organizzativi e tecnologici per il contrasto al crimine, unitamente al livello di consapevolezza da parte dei vari settori sia istituzionali che privati di essere obiettivi sensibili e rischiare di poter subire notevoli perdite in termini economici e tecnologici. Gli elementi in gioco sono le infrastrutture critiche, gli asset esposti ai rischi di attacchi cyber in varie tipologie, i danni causati e potenziali, i valori economici in gioco. La cyber security, infatti, non è solo un'esigenza ma anche un'opportunità in termini di capacità industriali e di ricerca.

Agenda (3 giorni)

Quadro di riferimento:

Cyber Security Standard
infrastrutture critiche nazionali ed estere identificate, team di difesa e loro differenze (CERT, CSIRT, ecc.)
report ed evidenze su tipologia, target e danni economici causati dagli attacchi informatici (cyber attacks)
situazione internazionale in USA, Unione Europea e in Italia anche dal punto di vista normativo
enti e operatori coinvolti nel governo del Cyber Space e nelle misure di protezione e nelle strategie nazionali
misure di protezione, di difesa, di resilience e "proattive" per la prevenzione ed il contrasto del Cyber Crime
indicatori del livello di consapevolezza, difesa, interdipendenza transnazionale e propensione agli investimenti in sicurezza
analisi delle tecniche di protezione tradizionali ed emergenti e delle minacce correlate (CyberCrime).

Obiettivi

Acquisire gli elementi principali sugli aspetti normativi, regolatori, sugli standard di riferimento.

Avere evidenze della situazione internazionale e nazionale in merito dimensione del fenomeno, alle minacce, agli attacchi di tipo Cyber ed ai criteri di protezione.

Analizzare le principali tecniche di attacco e di difesa in funzione del contesto.

Individuare le infrastrutture potenziali obiettivi, le strutture e i centri di prevenzione e di risposta ed il grado di esposizione al rischio degli asset tangibili e non.

Destinatari e Prerequisiti

A chi è rivolto

Responsabili IT, Security Manager, Forze dell'Ordine e quanti operano nella gestione dei dati informatici e telematici riservati e/o critici per l'erogazione dei servizi o del business.

Prerequisiti

Conoscenze di base di informatica e di telecomunicazioni.

Iscrizione

Quota di Iscrizione: 1.790,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza

80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

È un corso GOLD

con due partecipazioni potrai concordare con noi la data. Guarda i vantaggi della formula GOLD.

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

Obiettivi

Destinatari e Prerequisiti

Iscrizione

Date e Sedi

Il corso si pone come obiettivo quello di far comprendere le contromisure da adottare per garantire il livello desiderato di sicurezza del proprio sistema informativo. È destinato ai responsabili di sistemi informativi, centri elaborazione dati e di infrastrutture di rete; progettisti e amministratori di sistemi di rete; operatori che vogliano acquisire una visione d'insieme delle tematiche connesse alla sicurezza dei sistemi e delle reti.

Agenda (3 giorni)

Valutazione delle misure di sicurezza

Individuazione degli Asset Informatici; Risk Analysis; Vulnerability Assessment; Penetration Test; Comprendere le minacce che insistono sugli Asset; Requisiti di sicurezza base (riservatezza, integrità, disponibilità); Misure di sicurezza preventive e reattive; Gestione del rischio residuo; Incident Handling.

La sicurezza dei dati

Ciclo di vita dei dati (produzione, trattamento, conservazione); Proteggere i dati memorizzati; Soluzioni per assicurare la riservatezza e l'integrità dei dati trasmessi; Soluzioni per garantire l'autenticità della sorgente dei dati; Identità digitale; Firma digitale e non ripudio; Autorità di certificazione e certificati digitali; Utilizzo della crittografia nei principali servizi Internet (Web, Mail).

Progettazione di reti sicure

Suddividere la rete in contesti di sicurezza mutamente separati; Tassonomia soluzioni di accesso alla rete (wired, wireless, LAN, WAN, VPN); La sfida alla sicurezza rappresentata dagli accessi wireless e VPN; Controllo accessi alla rete: EAP e 802.1x; Realizzazione di uno schema AAA tramite RADIUS; Principi di hardening per gli apparati di rete (eliminazione servizi non necessari, protezione tabelle di instradamento e tabelle ARP, blocco protocolli non richiesti); Gestione e controllo degli apparati di rete; Creazione di una rete dedicata al Network Management.

Hardening dei sistemi

Individuazione delle componenti software necessarie per l'erogazione del servizio; Determinazione della versione del software attivo sul sistema; Mapping tra porte e servizi erogati; Rilevazione vulnerabilità e patch rilasciate dai vendor; Rimozione account di default; Riconfigurazione password amministrative; Eliminazione componenti software non necessarie; Blocco avvio automatico di servizi non indispensabili; Binding tra servizi ed interfacce di rete negli host multihomed; Attivazione funzionalità di logging; Analisi dei log; Conservazione sicura dei log; Installazione Antivirus, Personal Firewall, Host IDS; Integrazione tra controllo accessi alla rete e sicurezza delle postazioni di lavoro tramite Network Admission Control (NAC).

Difendere il perimetro della rete

Soluzioni di difesa perimetrale; Attivazione di un firewall; Ispezione dei pacchetti a livello applicativo; Blocco della posta indesiderata; Pubblicazione indiretta dei servizi tramite Reverse Proxy; Soluzioni per la rilevazione degli attacchi (IDS); Prevenire la compromissione degli Asset tramite IPS; Raccolta e centralizzazione dei log di sicurezza; Security Information & Event Management.

Obiettivi

Destinatari e Prerequisiti

A chi è rivolto

Tecnici che operano nell'ambito della protezione delle reti e dei sistemi di elaborazione, personale preposto alla pianificazione e/o progettazione di sistemi di sicurezza informatica.

Prerequisiti

Conoscenza di base dell'uso delle reti di computer e dei principali protocolli connessi al TCP/IP. È propedeutico il corso SEC302.

Iscrizione

Quota di Iscrizione: 1.790,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda

40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

Ethical Hacking e Penetration Test di Applicativi Web

Le applicazioni web rappresentano il vettore d'attacco più utilizzato da parte di criminali informatici. I motivi sono molteplici fra cui: enorme diffusionenotevole superficie d'attaccoscarsa attenzione in fase di progettazione agli aspetti di sicurezza.Tutto questo ha portato anche alcune grandi realtà come Sony, Yahoo, Apache, ecc. a scontrarsi con fenomeni quali: furto di dati riservati e di carte di creditodefacement di siti Webspionaggio industrialeutilizzo di siti web compromessi per diffondere Malware e creare Botnetaumento del "Ransom Malware".Soltanto conoscendo le principali tecniche di attacco e verificando in modo proattivo la sicurezza dei propri applicativi, si possono prevenire o ridurre gli attuali pericoli che provengono dal mondo del Cybercrime. Unire così la "Sicurezza Difensiva" alla "Sicurezza Proattiva" rappresenta ormai una necessità irrinunciabile. Saranno affrontate anche tematiche di "raccolta delle informazioni" ("Information Gathering") e tecniche e tools di cracking di password e hash. Sono previste, molte esercitazioni tratte da casi reali.

Agenda (3 giorni)

Associazioni, risorse e documentazione sulla sicurezza delle applicazioni web.

Metodologia ed analisi di tipo "Black-Box"/"White Box".

"Modus Operandi" e l'importanza del pensiero "out-of-the-box".

La distribuzione Linux BackTrack: concetti di base, architettura generale e panoramica dei principali tools installati.

Altre distribuzioni Linux utili al Security Assessment di applicativi web.

Information Gathering (tecniche e tools).

Detect Host Live, Port Scanning and Service Enumeration.

Information Gathering di applicazioni web.

Password/Hash Cracking.

Vulnerabilità delle applicazioni web, evasione di WAF e contromisure.

Laboratorio ("Capture The Flag!").

Indicazioni per la scrittura di un report finale di Penetration Test applicativo.

Obiettivi

Illustrare le principali e più diffuse vulnerabilità delle applicazioni web, nonché i più comuni errori nella scrittura di un applicativo web dal punto di vista della sicurezza.

Analizzare gli attuali attacchi client-side e server-side.

Destinatari e Prerequisiti

A chi è rivolto

Personale che si occupa della verifica della sicurezza di applicativi e sistemi, IT Security Engineer, sviluppatori di applicativi, responsabili della sicurezza IT.

Prerequisiti

Conoscenze di base dei concetti relativi al funzionamento di applicativi e sistemi e di rete. Conoscenze di base delle principali problematiche della IT security.

Iscrizione

Quota di Iscrizione: 2.060,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

Ethical Hacking e Penetration Test: dalla teoria alla pratica

La sicurezza informatica non può risolversi solo nella progettazione ed ingegnerizzazione di un'architettura di rete ed applicativa, basata sul principio meglio conosciuto come "Sicurezza Difensiva". Questo modo di procedere rappresenta una forte limitazione, producendo a volte danni economici e d'immagine, quali: furto di carte di credito furto di dati riservati violazione di sistemi web, scada, rete, ecc. spionaggio industriale, governativo o militare "Malware Banking" "Ransom Malware". che non hanno risparmiato grandi realtà come Sony, Yahoo,™ Soltanto conoscendo le principali tecniche di attacco e verificando in modo proattivo la sicurezza dei propri sistemi, si possono prevenire o ridurre gli attuali pericoli che provengono dal mondo del Cybercrime.Unire la "Sicurezza Difensiva" alla "Sicurezza Proattiva" rappresenta una necessità irrinunciabile.

Agenda (5 giorni)

Associazioni, risorse e documentazione utili ad un Penetration Tester.

Metodologia ed analisi di tipo "Black-Box"/"White Box".

"Modus Operandi" e l'importanza del pensiero "out-of-the-box".

La distribuzione Linux BackTrack: concetti di base, architettura generale e panoramica dei principali tools installati.

Altre distribuzioni Linux utili ad un Penetration Tester.

Information Gathering (tecniche e tools).

Detect Host Live, Port Scanning and Service Enumeration.

Information Gathering di applicazioni web.

Attacchi di reti di tipo M.I.T.M.

Buffer Overflow.

Vulnerabilità delle applicazioni web.

Password / Hash Cracking.

V.A., Exploitation e Post-Exploitation.

Cenni al funzionamento ed evasione di programmi Antivirus.

Indicazioni per la scrittura di un report finale di un Penetration Test.

Obiettivi

Alla fine del corso i partecipanti acquisiscono tecniche e metodologie utilizzate durante una attività di Penetration Test di applicativi, rete e sistemi e sono in grado di realizzare in autonomia i Penetration Test.

Destinatari e Prerequisiti

A chi è rivolto

Personale che si occupa della verifica della sicurezza di applicativi e sistemi, IT Security Engineer, responsabili della sicurezza IT.

Prerequisiti

Conoscenze di base dei concetti relativi al funzionamento di applicativi e sistemi e di rete. Conoscenze di base delle principali problematiche della IT security.

Iscrizione

Quota di Iscrizione: 3.490,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

Sicurezza di rete: firewall, IPS e VPN

Uno dei problemi più importanti nei sistemi informativi aziendali è la protezione del proprio sito da attacchi esterni provenienti da Internet. Le prime azioni di difesa sono affidate ai "Firewall", che controllando i punti di accesso minimizzano il rischio di accessi non autorizzati. Per integrare le funzionalità del Firewall e soprattutto per ridurre il rischio di attacchi provenienti dall'interno si può aggiungere il controllo eseguito dagli IDS/IPS, che esaminano il traffico alla ricerca di azioni illecite e/o di codice malevolo.Il corso si conclude con l'esame delle diverse soluzioni di reti private virtuali che, utilizzando una infrastruttura pubblica, permettono di interconnettere i siti su base geografica.Il corso offre una visione d'insieme delle tematiche connesse alla sicurezza dei sistemi e delle reti.

Agenda (4 giorni)

La sicurezza in Internet/Intranet: analisi dei principali requisiti di sicurezza e delle minacce delle reti TCP/IP.

Tecnologie di firewalling e meccanismi di funzionamento:

descrizione delle funzionalità di base di un firewall
progettazione della politica di sicurezza di un firewall
tipologie di firewall (Packet filter, Application proxy, stateful) e loro campi di impiego.

Funzionalità accessorie di un firewall:

Network Address Translation (NAT), Port Address Translation (PAT)
Virtual Private Network (VPN)
High availability, load balancing.

Selezione di prodotti di firewalling:

Rassegna dei principali prodotti di firewalling commerciali
Rassegna dei principali prodotti in libera distribuzione
Linee guida sulla selezione di un prodotto di firewalling.

Architetture implementative di firewalling:

modelli architetturali per la protezione di una Intranet da reti esterne interconnesse (Internet, altri Sistemi informativi)
modelli architetturali per la realizzazione di aree protette all'interno della Intranet
architetture per l'alta affidabilità/load balancing.

Intrusion prevention system:

IDS ed IPS
descrivere come i sensori possono limitare gli attacchi
conoscere i parametri di sistema essenziali
analizzare gli eventi e sintonizzare un sensore.

Reti private Virtuali (VPN):

protocollo IPSec, tunnel e transport mode, main e aggressive mode.

Obiettivi

Al termine del corso i partecipanti sono in grado di comprendere e saper utilizzare gli apparati di rete per garantire il livello di sicurezza richiesto.

Destinatari e Prerequisiti

A chi è rivolto

Tecnici che operano nell'ambito della protezione delle reti e dei sistemi di elaborazione, personale preposto alla pianificazione e/o progettazione di sistemi di sicurezza informatica.

Prerequisiti

Buona conoscenza della suite di protocolli TCP/IP.

Iscrizione

Quota di Iscrizione: 1.840,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

OpenVPN e CISCO VPN

Il corso affronta le tematiche della sicurezza di rete, in particolare, le diverse soluzioni di infrastrutture VPN (Virtual Private Networks) basate su sistemi Unix-like e/o interoperabili con apparati CISCO.

Agenda (4 giorni)

Panoramica sulle soluzioni VPN disponibili su Linux.

IPSEC: Principi e protocollo.

IPSEC: Installazione e configurazione su apparati CISCO in Alta Disponibilità.

IPSEC: Interoperabilità con sistemi e apparati terzi (es. Microsoft).

IPSEC: VPN Lan2Lan.

OPENVPN: Installazione e configurazione anche in Clustering/Virtualizzazione.

OPENVPN: Interoperabilità con Windows.

SSH: Tunnel e port forwarding.

Soluzioni di port knocking

Obiettivi

Al termine del corso i partecipanti sono in grado di saper installare e configurare una VPN basata su OpenVPN, saper installare e configurare una VPN su router CISCO, conoscere le potenzialità di tunneling e portforwarding di SSH, valutare soluzioni di port knocking.

Destinatari e Prerequisiti

A chi è rivolto

Responsabili di sistemi informativi, di centri elaborazione dati e di infrastrutture di rete; progettisti e amministratori di sistemi di rete; consulenti nel settore del Security management; sistemisti di rete; supervisori di sistemi di sicurezza.

Prerequisiti

Per trarre i massimi benefici da questo corso i partecipanti devono possedere le seguenti conoscenze di base: modello di riferimento OSI, stack di protocolli TCP/IP, principi di base sul routing, uso e configurazione di base di apparati Cisco, sicurezza delle reti e gestione sistemistica di sistemi Unix-like.

Iscrizione

Quota di Iscrizione: 2.190,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

Reti sicure in ambiente SonicWall: aspetti di base

Il corso garantire ai discenti di acquisire le conoscenze necessarie per poter mettere in esercizio e configurare firewall SonicWall. Ciò comporta la capacità di gestire le operazioni quotidiane dei dispositivi SonicWall a supporto di specifiche politiche aziendali. Questo corso, dopo la presentazione della famiglia di prodotti SonicWall, ha l'obiettivo di fornire una solida comprensione della configurazione e del monitoraggio quotidiano dei dispositivi SonicWall.Il corso fornisce le competenze necessarie per sostenere l'esame di certificazione SonicWall Network Security Basic Administration (NS-102-A).

Agenda (2 giorni)

Registrazione del prodotto.

System Backup & Restore.

WAN ISP Failover and Load Balancing.

Policy Based Routing.

VPN: Gateway-to-Gateway, Hub and Spoke, Mesh.

GVC with Local User DB.

SSL VPN & Global VPN Client with LDAP Authentication.

Content Filtering Service using Single Sign-On.

Security Services.

Troubleshooting.

Appendix: High Availability.

Obiettivi

Al termine del corso i partecipanti sono in grado di valutare e attivare i vari meccanismi di sicurezza messi a disposizione dagli apparati SonicWall.

Destinatari e Prerequisiti

A chi è rivolto

Responsabili di sistemi informativi, di centri elaborazione dati e di infrastrutture di rete; progettisti e amministratori di sistemi di rete; consulenti nel settore del Security management; sistemisti di rete; supervisori di sistemi di sicurezza. Candidati alla certificazione SonicWall Network Security Basic Administration (NS-102-A).

Prerequisiti

Per trarre i massimi benefici da questo corso i partecipanti devono possedere le seguenti conoscenze di base: modello di riferimento OSI, stack di protocolli TCP/IP, principi di base sul routing.

Iscrizione

Quota di Iscrizione: 1.190,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

È un corso GOLD

con due partecipazioni potrai concordare con noi la data. Guarda i vantaggi della formula GOLD.

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

Reti sicure in ambiente Cisco, difesa perimetrale con IOS Firewall

Il corso presenta le varie tipologie di attacco a cui può essere sottoposta una rete enterprise e le tecniche atte a mitigare tali attacchi attivando le funzionalità di sicurezza che sono presente nei sistemi operativi dei router e degli switch: controllo degli accessi, firewall ed IPS. Inoltre, essendo le reti enterprise geografiche sempre più spesso realizzate utilizzando backbone IP, il corso illustra come mettere in sicurezza le reti usando le reti private virtuali.Per ciascuna soluzione vengono valutati gli aspetti di sicurezza e le metodologie pratiche di messa in sicurezza degli apparati costituenti la rete, con particolare riferimento agli apparati Cisco. Il corso prevede, oltre alla descrizione teorica degli argomenti trattati, una rilevante attività di laboratorio 'hands on' su un ricco laboratorio, costituito da router e switch Cisco, nel quale sono riprodotte situazioni analoghe a quelle reali. Oltre alle operazioni di configurazione saranno effettuate esercitazioni che, partendo da reti già configurate, mirano ad aggiungere servizi/applicazioni ed a modificare le configurazioni dei dispositivi per conseguire miglioramenti nella sicurezza della rete.

Agenda (5 giorni)

Sicurezza a livello di data link:

tipi di attacchi
come mitigare gli attacchi
mettere in sicurezza il layer 2: PVLAN, controllo del DHCP e dell'ARP.

Gestione degli accessi alla rete: 802.1X.

Network Foundation Protection: mettere in sicurezza il piano dati, gestione e controllo.

Dispositivi di Sicurezza nei router Cisco:

Network address translation
Cisco IOS Firewall
implementazione e configurazione di Cisco IOS firewall in modo classico (interface-based)
implementazione e configurazione di Cisco IOS firewall basato sulle zone (zoned-based)
configurare l'Authentication Proxy
Cisco IOS IPS
implementazione e configurazione di Cisco IOS IPS.

Reti Private Virtuali:

il protocollo IPSec
implementazione di VPN IPSec con pre-shared keys e con PKI
implementazione di VPN IPSec facilmente scalabili
configurazione di Tunnel GRE su IPSec
configurazione di VPN su più siti, Dynamic Multipoint VPN
configurare VPN altamente affidabili
implementare l'accesso remoto
configurazione di VPN SSL
configurazione di Easy VPN.

Obiettivi

Destinatari e Prerequisiti

A chi è rivolto

Responsabili di sistemi informativi, di centri elaborazione dati e di infrastrutture di rete; progettisti e amministratori di sistemi di rete; consulenti nel settore del Security management; sistemisti di rete; supervisori di sistemi di sicurezza. Candidati alle certificazioni Cisco CCNP Security.

Prerequisiti

Per trarre i massimi benefici da questo corso i partecipanti devono possedere le seguenti conoscenze di base: modello di riferimento OSI, stack di protocolli TCP/IP, principi di base sul routing, uso e configurazione di base di apparati Cisco.

Iscrizione

Quota di Iscrizione: 2.400,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

PCI DSS v3.1 (Payment Card Industry Data Security Standard)

Agenda (2 giorni)

Introduzione alle problematiche di sicurezza delle transazione con carta di credito.

Introduzione agli standard PCI.

Analisi degli obiettivi di controllo del PCI DSS:

costruire e mantenere la rete sicura
proteggere i dati di titolari di carta
utilizzare programmi per la gestione delle vulnerabilità
implementazione di rigide misure di controllo dell'accesso
monitorare e eseguire test sulle reti regolarmente
definire una politica di sicurezza delle informazioni.

Obiettivi

Al termine del corso il partecipante acquisisce le conoscenze di tutti i requirements dello standard PCI DSS.

Destinatari e Prerequisiti

A chi è rivolto

Responsabili di sistemi informativi, centri elaborazione dati e di infrastrutture di rete; progettisti e amministratori di sistemi di rete; consulenti nel settore del Security management; sistemisti di rete; supervisori di sistemi di sicurezza.

Prerequisiti

Nessuno.

Iscrizione

Quota di Iscrizione: 1.280,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

È un corso GOLD

con due partecipazioni potrai concordare con noi la data. Guarda i vantaggi della formula GOLD.

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

Reti sicure in ambiente Cisco, difesa perimetrale e accesso remoto con ASA NG

Il corso affronta come le tematiche della sicurezza perimetrale e dell'accesso remoto possono essere risolte usando in rete apparati Cisco ASA Next Generation configurati opportunamente. In particolare è illustrato come configurare e implementare le policy che i nuovi apparati Cisco ASA Next Generation devono imporre nei punti perimetrali esterni ed interni. Gli argomenti su cui verteranno le lezioni sono principalmente le tecnologie utilizzate per rafforzare la sicurezza del perimetro di una rete: Network Address Translation, Intrusion Prevention System, policy e application inspect. Il corso affronta successivamente le soluzioni Virtual Private Network (VPN) che gli ASA mettono a disposizione: IPsec-VPN, SSL VPN, anyconnect, IPsec VTI, DMVPN, FlexVPN.

Agenda (5 giorni)

Principi di sicurezza perimetrale:

Zone di Sicurezza, Architetture modulari, SecureX, TrustSec.
Funzionalità di un Firewall:
Stateless Packet Filtering Application Layer Gateway (Proxy) Stateful Packet Filtering (SPF) Application Inspection and Control Filtering (AIC) Context-Aware Firewalls
Funzionalità complementari

Sviluppo di protezione dell'infrastrutture di Rete:

Sicurezza sul control plane Cisco IOS
Sicurezza sul Management plane Cisco ASA

NAT su Cisco IOS e ASA:

Configurare il NAT (Network Address Traslation) sugli ASA
Configurare network object, static NAT usando network object NAT, dynamic PAT usando netvork object NAT
Configurare twice NAT o manual NAT
Configurare dynamic NAT usando manual NAT
Configurare twice NAT usando manual NAT

Controlli delle minacce sul Cisco ASA:

Implementare policy base su Cisco ASA
Implementare policy avanzate su Cisco ASA
Implementare policy Reputation-based su Cisco ASA
Implementare policy Identity-based su Cisco ASA.

Cisco ASA Next-Generation Firewall (NGFW):

Cisco ASA NGFW
Architettura Cisco ASA NGFW
Implementare Policy Objects su ASA NGFW
Monitoring del Cisco ASA NGFW
Implementare access policies su Cisco ASA NGFW
Implementare identity policies su Cisco ASA NGFW
Implementare decryption policies su Cisco ASA NGFW.

Cisco Intrusion Prevention System:

Configurazione base del Cisco IPS
Tuning del Cisco IPS
Configurazioni personalizzate delle signaures IPS
Configurare le Anomaly Detection nel Cisco IPS
Configurare le Cisco IPS Reputation-Based.

Fondamenti di crittografia e Tecnologia VPN:

Il ruolo delle VPN nella sicurezza della rete
VPN e crittografia.

Implementare IPsec point-to-point su Cisco ASA:

Soluzioni Cisco Secure site-to-site
Implementare VPN IPsec point-to-point con Cisco IOS FlexVPN
Implementare VPN IPsec Hub-and-spoke con Cisco IOS FlexVPN.

Implementare clientless SSL VPNs:

Implementare Clientless SSL VPNs
Implementare Clientless SSL VPNs su Cisco ASA

Implementare applicazioni di accesso per clientless su Cisco ASA
Implementare Authentication and Authorization avanzata per clientless VPN SSL

Implementare Cisco AnyConnect VPN:

Implementare AnyConnect SSL VPN base su Cisco ASA
Implementare AnyConnect SSL VPN azanzato su Cisco ASA
Implementare Authentication e Authorization su Cisco AnyConnect VPN
Implementare Cisco VPN AnyConnect IPSec/IKEv2.

Obiettivi

Al termine del corso i partecipanti saranno in grado di:

identificare le caratteristiche dei modelli di Security Appliance in commercio
configurare il Firewall dalla command line interface e graficamente attraverso l'ASDM
realizzare VPN con implementazione della AAA
abilitare un accesso protetto di gestione da remoto dei Security Appliance.

Destinatari e Prerequisiti

A chi è rivolto

Responsabili di sistemi informativi di centri elaborazione dati e di infrastrutture di rete; progettisti e amministratori di sistemi di rete; sistemisti di rete; supervisori di sistemi di sicurezza.

Prerequisiti

Buona conoscenza dell'architettura TCP/IP e dell'Internetworking IP in ambiente Cisco.

Iscrizione

Quota di Iscrizione: 2.400,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

La sicurezza nei Sistemi operativi Windows: aspetti e strumenti di gestione

Il corso illustra gli aspetti di sicurezza di Windows sia lato server che lato desktop. Per Windows Server 2008/2012 si esamina, innanzitutto, la configurazione di Active Directory, proseguendo con l'utilizzo dei Group Policy, per terminare con l'analisi degli aspetti di sicurezza a livello di rete, software, file e cartelle. Per Windows 7/8, invece, si analizzano gli aspetti di sicurezza locale, di rete ed internet. Infine viene descritta la configurazione ottimale di Internet Explorer.

Agenda (5 giorni)

Sicurezza in Windows Server 2008/2012

Ruoli di Windows Server.

Active Directory Domain Services:

creazione di account di utenti e computer
creazione di gruppi e unità organizzative
amministrare l'accesso alle risorse
amministrare AD DS Trusts.

Creazione e configurazione di Group Policy.

Configurare utenti e computer utilizzando Group Policy.

Amministrare la sicurezza del server tramite WSUS e Audit policy.

Implementare IT Security Layers.

Implementare la sicurezza di file e cartelle.

Implementare la sicurezza di rete.

Implementare la sicurezza del software.

Sicurezza in Windows 7/8

Configurare i profili utente.

Windows Workgroups e Active Directory Domains.

Condivisione delle cartelle.

Utilizzare NTFS Encryption.

Connettere Windows 7/8 in rete.

Implementare la sicurezza locale, di rete ed internet.

Configurare Internet Explorer.

Obiettivi

Fornire le competenze per rendere sicuri i sistemi operativi Windows Server 2008/2012 e Windows 7/8.

Destinatari e Prerequisiti

A chi è rivolto

Responsabili di sistemi informativi, progettisti e amministratori di sistemi di rete; tecnici di supporto; supervisori di sistemi di sicurezza.

Prerequisiti

Conoscenze di networking di base e dei sistemi operativi Windows Server 2008/2012, Windows 7/8.

Iscrizione

Quota di Iscrizione: 2.240,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:

10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

Progettare e realizzare la sicurezza di Sistemi Operativi Microsoft Windows

Il rischio di vulnerabilità di sistemi Windows può essere notevolmente ridotto con una opportuna configurazione del sistema. Mentre alcuni accorgimenti dovrebbero essere presi in ogni situazione, la configurazione più adatta a mettere in sicurezza un sistema in ogni contesto di esercizio deve essere valutata di caso in caso. Per raggiungere questo livello di abilità, è necessario conoscere in dettaglio il progetto e l'implementazione della sicurezza di sistemi basati su piattaforme Windows Server e Client.

Agenda (5 giorni)

Funzionalità e strumenti di sicurezza base dei sistemi operativi Windows.

Richiami sul modello di sicurezza nei sistemi Windows:

gestione delle utenze, dell'autenticazione, dell'autorizzazione, Access Control List
sicurezza del file system, dei processi, del sottosistema I/O, del sistema di memory management.

Tecniche tradizionali di intrusione nel sistema:

cracking delle password ed impersonamento; Virus e minacce correlate; Memory leak e Buffer overflow.

Richiami sul modello di sicurezza distribuita nei sistemi Windows:

implementazione e configurazione del TCP/IP e del Netbios Windows
servizi di rete base del S.O. (RPC; Servizi di naming: NetBios e DNS; File Sharing, Distributed File Sharing e Print Sharing; Web Server: IIS; Remote Control di sistemi Windows)
gestione distribuita delle utenze (Domain Controller, Active Directory) e configurazioni avanzate del sistema di autenticazione e autorizzazione
rilevazione delle intrusioni tramite logging e auditing
l'event viewer di Windows
tecniche di rilevazione statistica delle intrusioni: strumenti di monitoraggio statistico e real time del sistema
software di intrusion detection
tecniche di rilevazione basate su regole: utilizzo di firewall locali.

Hardening e Policy Compliance: Windows Domain e Group Policy; Network Access Protection.

Protezione dei dati e delle comunicazioni:

utenti mobili e BIT Locker
cifrare le comunicazioni con i certificati
Remote Access in SSL VPN
Windows Direct Access.

Soluzioni e architetture di prodotti anti virus: trade-off nelle prestazioni di sistemi protetti da sistemi antivirus.

Dimostrazioni e esercitazioni.

Analisi della configurazione di prodotti: per la difesa/attacco di un sistema: Sniffer, Spoofer, Portscanner per l'hardening di un sistema operativo in libera distribuzione: software di firewalling per la cifratura e la firma di posta elettronica: configurazione ed uso di certificati digitali con Netscape, MS-Explorer, MS-Outlook.

Obiettivi

Al termine del corso i partecipanti hanno conoscenze in dettaglio e competenze per configurare e gestire la sicurezza dei sistemi operativi Windows, sia stand alone che nelle più complesse configurazioni in rete.

Destinatari e Prerequisiti

A chi è rivolto

Responsabili di S.I., CED e di infrastrutture di rete, Progettisti e amministratori di sistemi di rete, Consulenti junior di Security management, Sistemisti di rete, Supervisori di sistemi di sicurezza.

Prerequisiti

Buona conoscenza dei sistemi operativi Windows, delle reti di computer, della suite di protocolli TCP/IP e conoscenza di base sulla amministrazione di sistemi informativi complessi.

Iscrizione

Quota di Iscrizione: 2.240,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

La sicurezza nei Sistemi operativi UNIX/Linux

I rischi di vulnerabilità di sistemi Unix può essere notevolmente ridotto con una opportuna configurazione del sistema stesso. Mentre alcuni accorgimenti dovrebbero essere presi in ogni situazione, la configurazione più adatta a mettere in sicurezza un sistema in ogni contesto di esercizio deve essere valutata di caso in caso. Per raggiungere questo livello di abilità, è necessario conoscere in dettaglio il progetto e l'implementazione della sicurezza di sistemi basati su piattaforme Unix.

Agenda (4 giorni)

Funzionalità e strumenti di sicurezza base dei sistemi operativi Unix/Linux.

Richiami sul modello di sicurezza nei sistemi Unix/Linux:

gestione di: utenze, autenticazione, autorizzazione; Access Control List
sicurezza di: file system, processi, sottosistema I/O e sistema di memory management.

Tecniche di intrusione nel sistema:

cracking delle password ed impersonamento
memory leak
buffer overflow.

Richiami sul modello di sicurezza distribuita nei sistemi Unix/Linux.

Personalizzazioni del kernel per attuare le contromisure.

Implementazione e configurazione del TCP/IP.

Servizi di rete base del S.O.:

servizi di identificazione; SMTP; File Sharing; Web Server; esportazione del display
gestione distribuita delle utenze: NIS/NIS+. YP
gestione delle utenze delle applicazioni di rete: mail, web.

Rilevazione delle intrusioni tramite logging e auditing:

standard syslog
tecniche di rilevazione statistica delle intrusioni:strumenti di monitoraggio statistico e real time
software di intrusion detection
tecniche di rilevazione e filtraggio basate su regole (Linux):Ipchain/Iptables.

Esercitazioni:

analisi della configurazione di prodotti per la difesa/attacco di un sistema:Sniffer, Spoofer, Portscanner
analisi della configurazione di prodotti per l'hardening di un sistema operativo
strumenti per la verifica della tenuta di Firewall e strumenti IDS.

Analisi della configurazione di prodotti per la implementazione di SSL ed HTTPS:

configurazione di un client e di un server.

Obiettivi

Il corso è finalizzato ad acquisire le competenze per la configurazione e gestione della sicurezza dei S.O. Unix/Linux, sia stand alone sia nelle più complesse configurazioni in rete.

Destinatari e Prerequisiti

A chi è rivolto

Responsabili di sistemi informativi, progettisti e amministratori di sistemi di rete; tecnici di supporto; supervisori di sistemi di sicurezza.

Prerequisiti

Conoscenza di base di S.O., reti di computer, suite di protocolli TCP/IP e della amministrazione di sistemi informativi complessi.

Iscrizione

Quota di Iscrizione: 1.980,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

Application Security: criteri e aspetti operativi per lo sviluppo di applicazioni sicure

Lo sviluppo di applicativi sicuri è il passo principale per contrastare le minacce e le vulnerabilità che potrebbero essere insite nelle applicazioni web. Con la progressiva diffusione di architetture distribuite, aperte e flessibili, garantire la sicurezza e l'integrità dei sistemi informativi aziendali è divenuto un compito complesso; se da un lato le applicazioni web hanno portato evidenti benefici in termini di fruibilità per l'utente, dall'altro hanno sicuramente introdotto un nuovo elemento debole ai sistemi. Il requisito della sicurezza nelle applicazioni web che diventa, ad oggi, uno dei principali problemi che affligge questa tecnologia. L'Open Web Application Security Project (OWASP) è un'organizzazione mondiale no profit, che si pone come obiettivo il miglioramento continuo della sicurezza delle applicazioni software, evidenziando sfide e criticità, in modo da permettere a imprese e organizzazioni di prendere decisioni efficaci e adottare soluzioni concrete per contrastarne i rischi.

Agenda (3 giorni)

Scenari e mandatory principles in materia di sicurezza applicativa.

Criteri e metodologie da adottare per lo sviluppo di applicazioni sicure.

Normativa in materia di sviluppo di codice sicuro, introduzione all'OWASP e alle politiche correlate.

Principi fondamentali di testing.

Test di applicativi web, reporting, casi ed esempi.

Ambiti e Perimetri interessati:

ciclo di vita del software
ambienti di sviluppo, collaudo ed esercizio di applicazioni
analisi dei principali tool di mercato e open source
descrizione della documentazione necessaria e di come condurre le verifiche.

Obiettivi

Acquisire le competenze di base per la scrittura di applicazioni sicure.

Acquisire i criteri per condurre un progetto di Secure Code.

Acquisire le conoscenze in merito alle metodologie e ai principali tool per la scrittura e la verifica di codice sicuro da adottare anche ai fini di conformità richieste.

Individuare i requisiti richiesti per la scelta di piattaforme e tool idonei al proprio contesto aziendale.

Destinatari e Prerequisiti

A chi è rivolto

Responsabili IT, IT Administrator, Project Manager, Analisti, Programmatori e quanti operano negli ambienti di disegno e sviluppo software, di collaudo e di esercizio di applicazioni informatiche e di porting da ambienti legacy al web.

Prerequisiti

Conoscenze di base di informatica e fondamenti di sviluppo di applicazioni web.

Iscrizione

Quota di Iscrizione: 1.690,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

Autorità di certificazione, certificati digitali, carta nazionale dei servizi e posta elettronica certificata

Le tecnologie utilizzate per la sicurezza fondate sul principio delle chiavi asimmetriche sono state utilizzate in unione a precise normative europee e, di conseguenza, italiane allo scopo di realizzare degli strumenti finalizzati all'uso di servizi per i cittadini, partendo dalle categorie professionali e proseguendo con la cittadinanza "informaticamente evoluta", utilizzatrice abitudinaria di risorse internet. Questo scenario ha introdotto necessariamente delle problematiche di carattere normativo prima e di interoperabilità tecnologica poi. Infatti, sempre più frequentemente i "system manager" e più in generale gli addetti informatici specializzati nell'help desk sia a livello operativo, che a livello di responsabilità, hanno a che fare con questa situazione ibrida che rende gli strumenti informatici "legalmente validi", obbligandoli a confrontarsi con uno scenario molto diverso da quello presidiato esclusivamente per via tecnica.

Agenda (3 giorni)

Autorità di certificazione:

Requisiti di una Autorità di certificazione; Procedura di accreditamento; Procedure operative; Infrastrutture tecniche; Infrastrutture fisiche e continuità operativa; Circuito di emissione; Ciclo di vita dei certificati; Sistemi di pubblicazione dello stato dei certificati.

Firma digitale:

Direttiva europea sulle firme elettroniche; Quadro normativo italiano attuale; Diffusione della firma digitale; Standard di riferimento per le smart card; Come funzione la firma digitale; Struttura dei certificati; Componenti di un kit di firma digitale; Quadro normativo attuale; Formati della firma digitale: PKCS#7, PDF, XML; Firma digitale singola e firma digitale automatica; Procedure di verifica della firma digitale; Integrazione della firma digitale nei processi informatici tipici del "e-government"; Marcatura temporale.

Posta elettronica certificata (PEC):

Quadro normativo attuale; Cosa è e a cosa serve; Quadro normativo attuale; Funzionamento del servizio; Standard tecnologici; I gestori di PEC; Attivazione del servizio; Interoperabilità con servizi di posta "standard"; Ambiti di applicazione.

Carta Nazionale dei Servizi (CNS):

Quadro normativo attuale; Regolamento concernente la diffusione della CNS; Standard di riferimento per le smart card; Struttura dei certificati di autenticazione; Descrizione della tecnologia e costituzione di una CNS; Circuito di emissione; Utilizzo di una CNS: autenticazione, firma digitale, pagamenti; Interoperabilità; Applicazioni in ambito sanitario della CNS; Architetture di sicurezza.

Obiettivi

Offrire un'adeguata e aggiornata formazione orientata a comprendere le funzioni, le norme e relative implicazioni e i requisiti di sistema delle tecnologie informatiche asservite alla digitalizzazione della pubblica amministrazione.

Destinatari e Prerequisiti

A chi è rivolto

Responsabili di sistemi informativi, Responsabili di progetti IT, tecnici di supporto; supervisori di sistemi di sicurezza.

Prerequisiti

Conoscenza di base delle infrastrutture PKI, dell'uso delle reti di computer, dei principali protocolli connessi al TCP/IP. Conoscenza di base del significato del rispetto dei livelli di servizio e processi di comunicazione B2B, B2G e B2U.

Iscrizione

Quota di Iscrizione: 1.690,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza

80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

Rilevamento della sicurezza di un sistema informatico

Le pubbliche amministrazioni a seguito dell'introduzione del Codice per l'Amministrazione Digitale (CAD) nel 2006, e successive modificazioni, hanno avviato una profonda attività di ristrutturazione dei processi con particolare riguardo alla trasformazione in digitale dei processi cartacei. In questo processo, gli aspetti formativi sono fondamentali, come sottolineato dalla DigitPA. Il rischio è infatti l'inefficienza del Personale perché non formato alle nuove tecnologie di trattamento digitale delle informazioni. La logica dei bit è molto diversa da quella della carta; pertanto sono necessari percorsi formativi che portino ad un'innovazione non traumatica dei processi.

Agenda (3 giorni)

Schemi di riferimento della sicurezza nei processi.

Audit interno, Azioni correttive, Azioni preventive.

Controllo gestionale, Sicurezza del personale, Sicurezza fisica.

Manutenzione e sviluppo dei sistemi (SDLC)

Continuità operativa.

Rispetto di leggi vigenti, norme specifiche.

Classificazione degli attacchi, Tecniche e Strumenti.

Schemi metodologici per i test di sicurezza.

L'utilizzo di NESSUS.

Conduzione e predisposizione dei test, analisi dei risultati, presentazione dei risultati e attività di revisione.

Aree di operazione: fisica, logica ed organizzativa.

Aspetti generali di una certificazione, Schemi di certificazione.

Nozioni sulle certificazioni ISO 27001, ISO 27002.

Analisi dei rischi.

Piano gestione rischi.

Requisiti di un sistema di gestione della sicurezza

Limitazioni della responsabilità nella esecuzione delle operazioni.

Piano di rientro, Supporto all'applicazione del piano di rientro.

Esercitazione pratica sulla redazione di un piano di verifica di vulnerabilità.

Esame di risultati relativi a test già condotti.

Strumenti software open source.

Obiettivi

Al termine del corso i partecipanti hanno acquisito la conoscenza:

sui costituenti reali che sono coinvolti in un sistema informativo complesso, esaminato come risultante di una interazione tra gli elementi fisici, logici ed organizzativi di una organizzazione pubblica e/o privata
di base su metodologie di processo di sicurezza certificato e norme correlate.

Destinatari e Prerequisiti

A chi è rivolto

Manager IT, Responsabili della sicurezza informatica, responsabili di progettazione di sistemi di sicurezza.

Prerequisiti

Conoscenza di base delle reti di computer, dei principali protocolli di internet e delle norme base per il trattamento dei documenti elettronici.

Iscrizione

Quota di Iscrizione: 1.690,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

È un corso GOLD

con due partecipazioni potrai concordare con noi la data. Guarda i vantaggi della formula GOLD.

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

ICT Security: aspetti di base

Il personale interno di ogni organizzazione deve essere consapevole dei rischi legati all'attività che svolge quotidianamente utilizzando il computer aziendale. Solo così è possibile prevenire, almeno in parte, incidenti e minacce alla sicurezza informatica dell'azienda stessa.Il corso mira a far conoscere i rischi in ambito IT e offre una panoramica sulle attività di prevenzione e sugli strumenti (open e commerciali) da utilizzare per migliorare la sicurezza delle informazioni in azienda.

Agenda (3 giorni)

ICT security overview.

External attack.

Internal attack.

Analisi delle vulnerabilità tecniche.

Il social engineering.

Gestione degli accessi.

Policy e procedure.

Wireless security.

Gestione degli incidenti.

Sistemi di gestione per la sicurezza delle informazioni.

Certificati digitali, firma digitale e Posta elettronica certificata.

Aspetti legali.

Principi di crittografia.

Cenni di computer forensic.

Esercitazioni pratiche.

Obiettivi

Acquisire la conoscenza sui principali aspetti della sicurezza ICT e sulle attività aziendali in termini di prevenzione ed utilizzo dei sistemi in dotazione al personale.

Destinatari e Prerequisiti

A chi è rivolto

Manager di sistemi informativi, supervisori di sistemi di sicurezza e quanti debbano conoscere le buone pratiche sul tema.

Prerequisiti

Conoscenza dei principali strumenti ICT.

Iscrizione

Quota di Iscrizione: 1.640,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

È un corso GOLD

con due partecipazioni potrai concordare con noi la data. Guarda i vantaggi della formula GOLD.

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

Gestione degli incidenti in un sistema informativo (Incident Management)

I danni causati dalle intrusioni ai sistemi informativi sono direttamente proporzionali alla criticità delle informazioni contenute. Le attività di gestione dell'incidente, qualora si rilevi una violazione, attraverso un Team pronto ad intervenire in tempi brevissimi, sono finalizzate a: ricostruire l'evento e isolarne le cause comprendere il grado di compromissione delle risorse limitare l'entità dei danni subiti e neutralizzare la minaccia prevenire nuove violazioni raccogliere/predisporre le informazioni sull'incidente per eventuali indagini giudiziarie.

Agenda (3 giorni)

Eventi ed incidenti.

Realizzazione di policy operative, piani, procedure e liste di controllo per la risposta ad incidenti.

Struttura del Team di risposta agli incidenti.

Operazioni gestite dal Team.

Gestire un incidente.

Rilevamento ed analisi.

Contenimento, eliminazione e recupero.

Attività a seguito dell'incidente.

Gestire diverse tipologie di incidente

Normative di riferimento.

Evidenza informatica.

Mezzi di ricerca della prova.

Modalità di intervento.

Acquisizione dell'evidenza informatica.

Computer forensic.

Strumenti software open source per la implementazione della piattaforma di test.

Obiettivi

Acquisire la conoscenza sulle linee guida per la definizione di un piano per la gestione degli incidenti: definizione delle policy, costituzione del Team, predisposizione dei dispositivi hardware e software. Sono tenute in considerazione le norme vigenti e le modalità di ricerca ed analisi delle evidenze informatiche.

Destinatari e Prerequisiti

A chi è rivolto

Responsabili di sistemi informativi, progettisti e amministratori di sistemi di rete; tecnici di supporto; supervisori di sistemi di sicurezza.

Prerequisiti

Conoscenza delle reti di computer e dei principali protocolli di Internet. Conoscenza delle norme base per il trattamento dei documenti elettronici.

Iscrizione

Quota di Iscrizione: 1.690,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza

80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

È un corso GOLD

con due partecipazioni potrai concordare con noi la data. Guarda i vantaggi della formula GOLD.

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

La gestione della Continuità Operativa - Business Continuity Management

L'obiettivo primario della Gestione della Continuità Operativa è consentire all'azienda di proseguire le proprie attività anche in condizioni estreme, adottando opportune strategie di continuità, di ripristino e di gestione della crisi al fine di salvaguardare la propria immagine, gli interessi dei clienti e la propria capacità di creare valore.Da un semplice approccio tecnologico, dopo l'attentato dell'11 settembre, la Gestione della Continuità Operativa ha rivolto l'attenzione non solo agli aspetti di ripristino dei sistemi ma anche a quella che oggi è definita la social security. L'obiettivo primario del corso è fornire ai partecipanti tutte le informazioni, teoriche e pratiche, per comprendere e progettare un piano di continuità operativa in accordo con le strategie aziendali al fine di rendere l'azienda più resiliente a potenziali minacce e ripristinare l'operatività nei tempi stabiliti. Il corso inoltre tratta aspetti di contorno come i test dei piani e le strategia di comunicazione durante una crisi.

Agenda (3 giorni)

La Continuità Operativa: introduzione e obiettivi.

Best practice di settore.

Concetti di social security.

Piani di continuità operativa.

Emergency Response.

Piani di Disaster Recovery.

Scelta della Strategia di Recovery.

Legislazione in materia di continuità operativa (PA e privati).

La business Impact Analysis (BIA).

Legami tra continuità operativa e analisi dei rischi.

Legami tra continuità operativa e BIA.

Test dei piani di continuità operativa.

Crisis Communication.

Obiettivi

Al termine del corso i partecipanti hanno acquisito la conoscenza su:

contenuti di un piano di Business Continuity
modalità di scelta e realizzazione di un piano di Disaster Rcovery
best practice di settore (DRI, ISO, ISACA).

Destinatari e Prerequisiti

A chi è rivolto

Manager IT, Responsabili della sicurezza informatica, Responsabili di area, operatori IT.

Prerequisiti

Conoscenza di base della Information Technology e degli aspetti basilari relativi alla sicurezza delle informazioni.

Iscrizione

Quota di Iscrizione: 1.790,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

È un corso GOLD

con due partecipazioni potrai concordare con noi la data. Guarda i vantaggi della formula GOLD.

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

Analisi dei Rischi Informatici

Il corso si basa prevalentemente su esercitazioni pratiche, che permettono al discente di avere una conoscenza dell'argomento sul campo, attuando immediatamente, sotto la supervisione del docente, quanto appreso teoreticamente. Il corso si basa sulla metodologia MAGERIT e sul tool EAR-PILAR, ma fornisce anche le basi per operare con qualunque altra metodologia.

Agenda (3 giorni)

Elementi base del concetto di rischio.

Metodologie qualitative e metodologie quantitative.

Il processo di analisi dei rischi:

- ambito dell'analisi
- perimetro e data di riferimento
- metodo di lavoro
- personale coinvolto
- identificazione degli asset e loro valorizzazione.

Data asset.

Hardware asset.

Software asset.

Location Asset.

Human asset.

Case Study.

I modelli degli asset.

Valorizzazione degli asset.

Identificazione delle minacce.

Identificazione delle vulnerabilità.

Identificazione delle contromisure.

Case Study:

- calcolo del rischio assoluto
- calcolo del rischio residuo.

I controlli.

Il processo decisionale.

Le caratteristiche ideali di una metodologia per l'analisi dei rischi.

Obiettivi

Al termine del corso i partecipanti sono in grado di interpretare e mantenere un'Analisi dei Rischi.

Destinatari e Prerequisiti

A chi è rivolto

Responsabili della sicurezza informatica, responsabili di progettazione di sistemi di sicurezza, EDP auditor e analisti di sicurezza.

Prerequisiti

Buona conoscenza delle problematiche di sicurezza logica.

Iscrizione

Quota di Iscrizione: 1.640,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

È un corso GOLD

con due partecipazioni potrai concordare con noi la data. Guarda i vantaggi della formula GOLD.

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

La gestione della Sicurezza dell'Informazione (ISMS): dalla norma ISO/IEC 27001 all'Audit UNI EN ISO 19011

Le informazioni rappresentano beni intangibili che aggiungono valore all'interno di una organizzazione, pertanto è necessario proteggere i dati da minacce di ogni tipo, al fine di assicurarne l'integrità, la riservatezza e la disponibilità. Gli standard di sicurezza delle informazioni introducono una serie di attività che consentono di elevare il livello di sicurezza delle informazioni aziendali in modo sistematico e controllato attraverso la realizzazione di un sistema di gestione (certificabile da parte di Organismi di Certificazione abilitati). La Norma ISO/IEC 27001:2013 è lo standard internazionale di riferimento che fornisce i requisiti per implementare un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI o ISMS), efficace e efficiente nel tempo. Il primo ottobre 2013 è stata pubblicata la nuova versione della norma che condensa alcuni controlli ed assume una forma comune ad altri schemi per facilitarne l'integrazione. Il corso si basa sull'analisi di tutti gli aspetti teorici e pratici della norma e sulle tematiche di audit dei sistemi di gestione, corredate da diverse attività pratiche, che permetteranno al discente di avere una conoscenza dell'argomento sul campo, attuando immediatamente, sotto la supervisione del docente, quanto appreso teoricamente.

Agenda (3 giorni)

Introduzione alla gestione della sicurezza dell'informazione.

Finalità dello standard.

Approccio per processi.

Riferimenti normativi.

Termini e definizioni.

Sistema di gestione per la sicurezza delle informazioni:

- contesto dell'organizzazione
- campo di applicazione.

Leadership; Politica; Ruoli, Responsabilità, Autorità della Direzione.

Pianificazione; Valutazione e Trattamento dei rischi relativi alla sicurezza delle informazioni.

Obiettivi

Supporto; Gestione delle risorse; Competenza; Consapevolezza; Comunicazione.

Gestione della documentazione del SGSI.

Monitoraggio del SGSI.

Audit interni del SGSI.

Riesame del SGSI da parte della Direzione.

Miglioramento del SGSI:

- non conformità e azioni correttive
- miglioramento continuo.

Allegato A: Obiettivi di controllo e controlli.

Audit dello schema ISO 27001 secondo la norma UNI EN ISO 19011:2012</br>

Prerequisiti

- Redazione di un piano di audit e redazione di un programma di audit.
- Conduzione dell'audit sul campo.
- Redazione di un rapporto di audit.
- Il ciclo di audit interni.
- Le check-list.
- Case study ed esercitazioni pratiche.

Al termine del corso i partecipanti saranno in grado di valutare le attività necessarie per la realizzazione di un SGSI certificabile secondo la norma ISO/IEC 27001:2013 e delle tematiche in tema di audit dei sistemi di gestione. Inoltre, saranno in grado di ricevere un audit sia interno sia esterno.

Destinatari e Prerequisiti

A chi è rivolto

Responsabili della sicurezza informatica, responsabili di progettazione di sistemi di sicurezza, internal auditor, analisti di sicurezza, personale tecnico di sistemi informativi.

Non sono necessari prerequisiti particolari se non di tipo ICT generale e di alcune basi di sicurezza delle informazioni.

Iscrizione

Quota di Iscrizione: 1.690,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

È un corso GOLD

con due partecipazioni potrai concordare con noi la data. Guarda i vantaggi della formula GOLD.

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

Aggiornarsi alla norma ISO/IEC 27001:2013 e tematiche di Audit

Ad Aprile 2014 è stata pubblicata l'ultima versione della norma ISO/IEC 27001, in lingua italiana. Nella nuova versione sono state introdotte alcune modificazioni che ne migliorano l'implementazione e ne facilitano l'integrazione con altri schemi. Contestualmente è stata pubblicata la nuova ISO/IEC 27002 per poter fornire le linee guida necessarie ad aggiornare il proprio sistema di gestione. In questo corso è stato introdotto anche un breve modulo per lo svolgimento di audit del Sistema di Gestione per la Sicurezza delle Informazioni secondo la norma UNI EN ISO 19011:2012.

Agenda (2 giorni)

Nuova struttura della norma

Modifiche rispetto alla precedente versione.

Novità rispetto alla precedente versione.

La documentazione del SGSI.

Il nuovo Annex A.

I controlli e gli obiettivi di controllo.

Audit dello schema ISO 27001 secondo la norma UNI EN ISO 19011:2012.

Obiettivi

Al termine del corso i partecipanti avranno conoscenza delle novità e delle modifiche introdotte dal nuovo della norma ISO/IEC 27001:2014 e delle principali tematiche in tema di audit dei sistemi di gestione.

Destinatari e Prerequisiti

A chi è rivolto

Responsabili della sicurezza informatica, Responsabili di progettazione di sistemi di sicurezza, internal auditor, analisti di sicurezza, personale tecnico di sistemi informativi.

Prerequisiti

Conoscenza della norma ISO/IEC 27001:2005.

Iscrizione

Quota di Iscrizione: 1.280,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

È un corso GOLD

con due partecipazioni potrai concordare con noi la data. Guarda i vantaggi della formula GOLD.

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

Informatica Forense (Computer Forensics): aspetti pratici

Il corso affronta, con un approccio orientato alla sperimentazione, la scienza che studia l'individuazione, la conservazione, la protezione, l'estrazione, la documentazione e ogni altra forma di trattamento del dato informatico al fine di essere valutato in sede processuale.Al termine del corso si acquisiranno le competenze necessarie al "computer forensic expert" ovvero la figura professionale che presta la sua opera nell'ambito dei reati informatici o del computer crime con lo scopo di "preservare, identificare, studiare ed analizzare i contenuti memorizzati all'interno di qualsiasi supporto o dispositivo di memorizzazione". Le attività sono dirette non solo a tutte le categorie di computer, ma a qualsiasi attrezzatura elettronica con potenzialità di memorizzazione dei dati (ad esempio, cellulari, smartphone, sistemi di domotica, autoveicoli e tutto ciò che contiene dati memorizzati.

Agenda (3 giorni)

Individuazione:

Conservazione e Protezione:

il computer forensic expert deve garantire il massimo impegno per conservare l'integrità della prova informatica. Il dato originale non deve essere modificato e danneggiato e quindi si procede realizzandone una copia (bit-a-bit), su cui il computer forensic expert compie l'analisi. Dopo aver effettuato la copia è necessario verificarne la consistenza rispetto al dato originale: per questo motivo si firmano digitalmente il dato originale e la copia, che devono coincidere.
esercitazioni in laboratorio su: dd, ddrescue, md5sum, autopsy (calcolo hash e analisi di device).

Estrazione:

è il processo attraverso il quale il computer forensic expert, servendosi di diverse tecniche e della sua esperienza, trova la posizione del dato informatico ricercato e lo estrae. Verrà fatta una panoramica sui forensics tool Helix, CAINE ed Encase
esercitazioni in laboratorio su: recupero file cancellati, ricerche su file e settori allocati/non allocati, creazione ed interpretazione della timeline, analisi di pagefile.sys/hiberfile.sys/NTUSER.DAT, funzionamento di Emule, utilizzo dell'analizzatore di protocolli di rete Wireshark.

Documentazione:

l'intero lavoro del digital forenser deve essere costantemente documentato, a partire dall'inizio dell'investigazione fino al termine del processo. La documentazione prodotta comprende, oltre alla catena di custodia, un'analisi dei dati rinvenuti e del processo seguito. Un'accurata documentazione è di fondamentale importanza per minimizzare le obiezioni e spiegare come ripetere l'estrazione con un analogo processo sulla copia.

Obiettivi

Al termine del corso i partecipanti sono in grado di investigare (individuare, estrarre) mediante utilizzo di strumenti open source e documentare con precisione il processo seguito ed i risultati ottenuti.

Destinatari e Prerequisiti

A chi è rivolto

Tecnici informatici, Ingegneri informatici, CTP/CTU, membri delle Forze dell'Ordine e cultori della materia.

Prerequisiti

Per trarre i massimi benefici da questo corso i partecipanti devono possedere le seguenti conoscenze di base: sistema operativo linux, principi di base di networking.

Iscrizione

Quota di Iscrizione: 1.790,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:

10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

È un corso GOLD

con due partecipazioni potrai concordare con noi la data. Guarda i vantaggi della formula GOLD.

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

Digital Forensics

La criminalità per far perdere le tracce dei delitti commessi e degli autori coinvolti ricorre sempre più spesso a strumenti informatici. Per contrastare il fenomeno tra gli investigatori cresce la necessità di figure professionali specializzate nella Digital Forensics, la branca della Criminalistica che si occupa dell'identificazione, preservazione e analisi di quanto contenuto nei sistemi informatici o telematici e che evidenzia l'esistenza di fonti di prova digitali che resistano a contestazioni circa la solidità e la capacità probatoria in ambito civile o penale.La Digital Forensics è una scienza nuova che solo nel febbraio 2008 l'American Academy of Forensic Sciences (AAFS) ha inserito nel novero delle scienze riconosciute. Il corso consente di acquisire le competenze necessarie sia al Digital Evidence First Responder (DEFR) che al Digital Evidence Specialist (DES) per lo svolgimento delle attività di sopralluogo digitale e di analisi di reperti virtuali.

Agenda (3 giorni)

Introduzione:

introduzione alla Digital Forensics e al concetto di prova digitale
standard ISO di riferimento
legislazione in materia di criminalità informatica.

Il Sopralluogo Digitale:

attuazione della ISO27037:2012 sulla scena del crimine informatico, attraverso lo studio delle fasi di:
Identificazione (Identification): ricerca della fonte di prova digitale Acquisizione (Acquisition): rilievo tecnico volto a congelare la fonte di prova digitale Repertamento (Collection): attività volta ad assicurare la fonte di prova digitale Preservazione (Preservation): attività volta a garantire l'integrità e riservatezza della fonte di prova digitale Validazione (Validation): conferma che sono stati rispettati i requisiti per i fini d'indagine (principio di pertinenza). </dd> Verifica, Analisi ed Interpretazione dei dati: uso di software, preferibilmente Open Source, al fine di attuare le principali tecniche di verifica ed analisi di reperti virtuali, secondo procedure scientificamente derivate dirette a confermare, o confutare, una tesi accusatoria l'interpretazione è l'unica fase soggettiva dell'intero processo in cui l'investigatore fornisce valutazioni di merito alla pertinenza con il contesto d'indagine e l'uso dei dati per l'eventuale proseguimento delle indagini.
Documentazione e Presentazione: la documentazione è l'insieme di atti e documenti volti a storicizzare le attività svolte. Tale attività è prologo della presentazione, dove lo specialista dovrà aver cura di fornire una giustificazione dell'attinenza con l'indagine della traccia informatica rilevata, ossia fornire un legame logico-deduttivo comprensibile a persone che non hanno un'elevata competenza informatica, come ad esempio Giudice, Pubblico Ministero ed Avvocato. la professionalità sia del DEFR che del DES sarà quindi misurata anche nel saper realizzare: una solida Catena di Custodia (Chain of Custody), ossia l'insieme di documenti che accompagnano la vita del reperto dalla sua formazione alla sua restituzione all'avente diritto o distruzione un Verbale (art. 134 c.p.p. e seg.) di operazioni tecniche, in caso l'operatore appartenga alla PG Referto tecnico nel caso in cui l'operatore non appartenga alla PG (es. CTU, CTU, Perito). </dd> Cenni sulle Tecniche investigative in internet tecniche di OSINT (Open Source Intelligence) Sopralluogo Virtuale tracciamento.

Obiettivi

Al termine del corso i partecipanti sono in grado di investigare nel rispetto dei principi stabiliti sia dal Legislatore italiano (ex L.48/2008) che dai principali standard (ISO 27037 e segg.) e linee guida internazionali (NIST, ™).

Destinatari e Prerequisiti

A chi è rivolto

Tecnici informatici, Ingegneri informatici, CTP/CTU, membri delle Forze dell'Ordine e cultori della materia.

Prerequisiti

Per trarre i massimi benefici da questo corso i partecipanti devono possedere le seguenti conoscenze di base: sistema operativo linux, principi di base di networking.

Iscrizione

Quota di Iscrizione: 1.790,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di

partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

È un corso GOLD

con due partecipazioni potrai concordare con noi la data. Guarda i vantaggi della formula GOLD.

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

Analisi Forense dei Dispositivi Mobili (Mobile Forensics)

Nelle indagini relative alla commissione di reati, sempre più frequentemente, i dispositivi mobili e le tecnologie informatiche - tablet, smartphone, telefono cellulare, navigatore satellitare - forniscono utili indizi alla risoluzione del caso. La Mobile Forensics è il settore della Digital Forensics che si occupa di recuperare prove digitali, da dispositivi mobili, usando metodi che non compromettano il loro stato probatorio.Il corso affronta le problematiche inerenti le attività di analisi forense su dispositivi mobili, le procedure per la preservazione, acquisizione, analisi e reporting delle informazioni digitali, utilizzando strumenti open-source e tool proprietari. Al termine del corso si acquisiscono le competenze necessarie sia come Digital Evidence First Responder (DEFR) che Digital Evidence Specialist (DES) per poter svolgere analisi approfondite sui sistemi operativi dei più diffusi dispositivi mobili fra cui Android, iOS, Windows Mobile, Windows Phone, Blackberry, Symbian etc.

Agenda (3 giorni)

Introduzione:

introduzione alla Mobile forensics
panoramica e caratteristiche sui sistemi operativi più diffusi fra cui Android, iOS, Windows Phone, Windows Mobile, Blackberry, Symbian
modelli procedurali sulla scienza del crimine.

L'acquisizione:

l'acquisizione Fisica
l'acquisizione Logica
esercitazioni in laboratorio con strumenti proprietari (XRY, UFED etc.) e tool open-source;
confronto dei risultati.

Acquisizioni Avanzate:

l'acquisizione tramite il JTAG
il Chip-Off: L'acquisizione tramite lettura del chip di memoria da dispositivi danneggiati.

L'analisi dei File Systems:

il File System FAT/FAT32/EXT/YAFFS2/iOS File System
file di sistema e Log.

L'analisi dei Database:

i database di sistema
text messages (SMS/MMS), Contacts, Call logs, E-mail / Instant Messenger/Chat etc.

Analisi delle Apps:

i database interni delle App
i database SQLite.

L'analisi della geolocalizzazione.

Obiettivi

Al termine del corso i partecipanti sono in grado di investigare nel rispetto dei principi stabiliti sia dal Legislatore italiano (ex L.48/2008) che dai principali standard (ISO 27037 e segg.) e linee guida internazionali (NIST, ™).

Destinatari e Prerequisiti

A chi è rivolto

Tecnici informatici, Ingegneri informatici, CTP/CTU, membri delle Forze dell'Ordine e cultori della materia.

Prerequisiti

Per trarre i massimi benefici da questo corso i partecipanti devono possedere le seguenti conoscenze di base: sistema operativo linux, principi di base di networking.

Iscrizione

Quota di Iscrizione: 1.690,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

È un corso GOLD

con due partecipazioni potrai concordare con noi la data. Guarda i vantaggi della formula GOLD.

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

La Business Impact Analysis (BIA)

Nel più ampio contesto della continuità operativa ed applicazione delle strategie di continuità o di recovery si inserisce con fondamentale importanza l'analisi degli impatti sul business. La Business Impact Analysis valuta le perdite (qualitative e quantitative) per il business di un'organizzazione a seguito di una prolungata interruzione dei propri servizi. Rappresenta quindi l'input principale alla gestione della continuità operativa aziendale per la definizione di una strategia che ottimizzi i costi e minimizzi le perdite. Il corso è strutturato in modo da applicare praticamente quanto appreso dalla teoria, attraverso delle esercitazioni su scenari reali; tale approccio consente ai partecipanti di apprendere i concetti principali associati alla BIA e di saperli riportare un ambito pratico.

Agenda (3 giorni)

Introduzione alla BIA: il contesto.

Business Continuity Management.

Risk Management.

Le vulnerabilità e la loro gestione.

Recovery Time Objective.

Recovery Point Objective.

Minumim Business Continuity Objective.

Maximum Tolerable Downtime.

La conduzione di una BIA:

- la scelta del perimetro
- le interviste
- la raccolta dei dati
- l'analisi dei dati
- la reportistica finale.

La definizione delle strategie di continuità.

Esercitazioni e case study.

Obiettivi

Al termine del corso i partecipanti avranno una conoscenza teorico pratica delle tematiche associate alla Business Impact Analysis ed alla sua realizzazione.

Destinatari e Prerequisiti

A chi è rivolto

Responsabili della sicurezza informatica, responsabili di progettazione di sistemi di sicurezza, internal auditor, analisti di sicurezza, personale tecnico di sistemi informativi.

Prerequisiti

Non sono necessari prerequisiti particolari se non di tipo ICT generale.

Iscrizione

Quota di Iscrizione: 1.690,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda

40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

È un corso GOLD

con due partecipazioni potrai concordare con noi la data. Guarda i vantaggi della formula GOLD.

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

I sistemi di monitoraggio e controllo in rete

Il corso illustra l'evoluzione di sistemi dall'analogico al mondo IP nel modello 3P (dati, voce immagine, sistemi di controllo). In particolare sono affrontate le problematiche relative alla sicurezza di tali sistemi nel passaggio dall'operatività stand-alone alla modalità integrata su rete, mettendo in evidenza: vantaggi, svantaggi, punti deboli e punti di forza.Sono analizzate le evoluzioni verso IP dei sistemi di telefonia (VoIP), di videosorveglianza (IP-Surveillance), di monitoraggio (antincendio, gestione emergenze, gestione ascensori, monitoraggio processi industriali), di controllo processi (SCADA) e di sicurezza (controllo accessi fisico, antintrusione fisica).

Agenda (3 giorni)

Il modello 3Play.

La sicurezza informatica.

La sicurezza fisica.

I sistemi di monitoraggio e controllo in ambito industriale.

I sistemi di monitoraggio e controllo in ambito territoriale.

La convergenza su IP.

I vantaggi delle soluzioni IP.

La messa in sicurezza logica di sistemi integrati.

Affidabilità e continuità di servizio in ambiente mission critical.

Obiettivi

Formare nuove competenze trasversali che consentano un approccio integrato su IP e sulle tematiche relative alla messa in sicurezza e al monitoraggio di ambienti complessi.

Destinatari e Prerequisiti

A chi è rivolto

Responsabili di sistemi informativi, progettisti e amministratori di sistemi di rete; tecnici di supporto; supervisori di sistemi di sicurezza.

Prerequisiti

Reti IP. LAN, MAN, Wired e Wireless. Conoscenze di base sulla sicurezza informatica in ambito perimetrale.

Iscrizione

Quota di Iscrizione: 1.690,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

Il corso illustra l'evoluzione di sistemi di videosorveglianza dal mondo analogico al mondo IP. In particolare sono affrontate le problematiche relative alla sicurezza di tali sistemi nel passaggio dalla operatività stand-alone alla modalità integrata su rete, mettendo in evidenza: vantaggi, svantaggi, punti deboli e punti di forza.

Agenda (2 giorni)

I sistemi analogici di videosorveglianza.

La evoluzione in ambiente IP.

Architetture dei sistemi di IP Surveillance.

La sicurezza informatica dei sistemi di IP Surveillance.

Affidabilità e continuità di servizio in ambiente mission critical.

La normativa in vigore sulla Privacy.

Obiettivi

Destinatari e Prerequisiti

A chi è rivolto

Responsabili di sistemi informativi, progettisti e amministratori di sistemi di rete; tecnici di supporto; supervisori di sistemi di sicurezza.

Prerequisiti

Reti IP. LAN, MAN, Wired e Wireless. Conoscenze di base sulla sicurezza informatica in ambito perimetrale.

Iscrizione

Quota di Iscrizione: 1.090,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

Il Sistema di Gestione dei Servizi IT (SGSIT): introduzione alla norma ISO/IEC 20000-1:2011

La norma ISO/IEC 20000-1:2011 è il primo standard internazionale dedicato alla gestione dei servizi IT (IT Service Management) che prevede la certificazione del sistema di gestione. Essa infatti stabilisce i requisiti per la realizzazione di un sistema di gestione dei servizi in ambito IT (SGSIT), che un'organizzazione deve rispettare per raggiungere un elevato livello nella fornitura dei propri servizi. Il corso è basato sull'analisi della norma da un livello di astrazione tale da comprenderne tutti gli aspetti più specifici ed averne una conoscenza di base.

Agenda (1 giorno)

Introduzione alla gestione dei servizi IT.

Sistema di gestione dei servizi IT:

- Incident Management
- Problem Management
- Configuration Management
- Change Management
- Release Management
- Service Level Management
- Budgeting and Accounting for IT Services
- Capacity Management
- Service Continuity and Availability Management
- Service Reporting
- Information Security Reporting
- Business Relationship Management
- Supplier Management

Il processo di certificazione di un Sistema di Gestione dei Servizi IT.

Obiettivi

Al termine del corso i partecipanti avranno conoscenza degli aspetti salienti della norma, della gestione dei servizi IT e del processo di certificazione del SGSIT.

Destinatari e Prerequisiti

A chi è rivolto

Manager, responsabili dei servizi, responsabili di progettazione di servizi, analisti, personale tecnico di sistemi informativi.

Prerequisiti

Non sono necessari prerequisiti particolari.

Iscrizione

Quota di Iscrizione: 640,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

È un corso GOLD

con due partecipazioni potrai concordare con noi la data. Guarda i vantaggi della formula GOLD.

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

Il Sistema di Gestione dei Servizi IT (SGSIT): dalla norma ISO/IEC 20000-1:2011 agli audit interni (UNI EN ISO 19011)

La norma ISO/IEC 20000-1:2011 è il primo standard internazionale dedicato alla gestione dei servizi IT (IT Service Management) che prevede la certificazione del sistema di gestione. Essa infatti stabilisce i requisiti per la realizzazione di un sistema di gestione dei servizi in ambito IT (SGSIT), che un'organizzazione deve rispettare per raggiungere un elevato livello nella fornitura dei propri servizi. Il corso si basa sull'analisi e l'applicazione di tutti gli aspetti teorici e pratici della norma e sulle tematiche di audit interni del SGSIT; le esercitazioni su specifici requisiti della norma e sullo svolgimento di audit interni su scenari reali di un SGSIT, ne facilitano l'apprendimento, facilitando anche l'apprendimento delle modalità di implementazione di un SGSIT nella propria Organizzazione. Inoltre verranno affrontati gli argomenti inerenti la certificazione del SGSIT, gli Organismi di Certificazione e gli audit di parte terza. Queste informazioni consentiranno al discente di comprendere gli aspetti specifici della certificazione.

Agenda (3 giorni)

Introduzione alla gestione dei servizi IT.

Finalità dello standard.

Approccio per processi.

Riferimenti normativi.

Termini e definizioni.

Sistema di gestione dei servizi IT:

- Incident Management
- Problem Management
- Configuration Management
- Change Management
- Release Management
- Service Level Management
- Budgeting and Accounting for IT Services
- Capacity Management
- Service Continuity and Availability Management
- Service Reporting
- Information Security Reporting
- Business Relationship Management
- Supplier Management

Audit dello schema ISO 20000-1 secondo la norma UNI EN ISO 19011:2012.

Redazione di un piano di audit e di un programma di audit.

Conduzione dell'audit sul campo.

Redazione di un rapporto di audit.

Il ciclo di audit interni.

Le check-list.

Case study ed esercitazioni pratiche.

Il processo di certificazione di un Sistema di Gestione dei Servizi IT.

Cenni agli audit di parte terza.

Obiettivi

Al termine del corso i partecipanti saranno in grado di valutare le attività necessarie per la realizzazione di un SGSIT certificabile secondo la norma ISO/IEC 20000-1:2011 e delle tematiche in tema di audit dei sistemi di gestione. Inoltre, saranno in grado di ricevere un audit sia interno sia esterno.

Destinatari e Prerequisiti

A chi è rivolto

Responsabili dei servizi, responsabili di progettazione di servizi, internal auditor, analisti, personale tecnico di sistemi informativi.

Prerequisiti

Non sono necessari prerequisiti particolari se non di tipo ICT generale e di alcune basi di gestione dei servizi IT (es. ITIL).

Iscrizione

Quota di Iscrizione: 1.690,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

È un corso GOLD

con due partecipazioni potrai concordare con noi la data. Guarda i vantaggi della formula GOLD.

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

Il Sistema di Gestione per la Sicurezza delle Informazioni (SGSI): introduzione alla norma ISO/IEC 27001:2013

La norma ISO/IEC 27001:2013 è lo standard internazionale che fornisce i requisiti per implementare un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI), avente il fine di garantire l'integrità, la riservatezza e la disponibilità delle informazioni di un'Organizzazione.Il corso è basato sull'analisi della norma da un livello di astrazione tale da comprenderne tutti gli aspetti più specifici e di avere una conoscenza di base sia della norma, sia del processo di certificazione del SGSI.

Agenda (1 giorno)

Introduzione alla gestione della sicurezza dell'informazione.

Il Sistema di gestione per la sicurezza delle informazioni:

contesto dell'organizzazione
campo di applicazione
Leadership; Politica; Ruoli, Responsabilità, Autorità della Direzione
Pianificazione; Valutazione e Trattamento dei rischi relativi alla sicurezza delle informazioni
Obiettivi per la sicurezza delle informazioni
Supporto; Gestione delle risorse; Competenza; Consapevolezza; Comunicazione
Gestione della documentazione del SGSI
Monitoraggio del SGSI
Audit interni del SGSI
Riesame del SGSI da parte della Direzione
Miglioramento del SGSI
Allegato A: Obiettivi di controllo e controlli

Il processo di certificazione di un Sistema di Gestione per la Sicurezza delle Informazioni.

Obiettivi

Al termine del corso i partecipanti avranno conoscenza degli aspetti salienti correlati ad un SGSI, alla protezione delle informazioni ed al processo di certificazione del SGSI.

Destinatari e Prerequisiti

A chi è rivolto

Manager, responsabili della sicurezza informatica, responsabili di progettazione di sistemi di sicurezza, analisti, personale tecnico di sistemi informativi.

Prerequisiti

Non sono necessari prerequisiti.

Iscrizione

Quota di Iscrizione: 640,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

È un corso GOLD

con due partecipazioni potrai concordare con noi la data. Guarda i vantaggi della formula GOLD.

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

ISO/IEC 27001 Foundation (APMG)

La norma ISO/IEC 27001:2013 è lo standard internazionale che fornisce i requisiti per implementare un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI), avente il fine di garantire l'integrità, la riservatezza e la disponibilità delle informazioni di un'Organizzazione.Il corso è strutturato per l'apprendimento di tutti contenuti ed i requisiti legati alla norma ISO/IEC 27001:2013 ed all'implementazione di un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI). Lo schema di qualifica del personale sviluppato da APMG e l'utilizzo di docenti accreditati secondo tale schema è garanzia dell'apprendimento da parte dei partecipanti.

Agenda (3 giorni)

Lo schema certificativo APMG

Le modalità d'esame

Introduzione alla gestione della sicurezza delle informazioni

Finalità dello standard

Il Sistema di gestione per la sicurezza delle informazioni:

- contesto dell'organizzazione
- campo di applicazione
- leadership; politica; ruoli, responsabilità, autorità della direzione
- Pianificazione; Valutazione e Trattamento dei rischi relativi alla sicurezza delle informazioni
- Obiettivi per la sicurezza delle informazioni
- Supporto; Gestione delle risorse; Competenza; Consapevolezza; Comunicazione
- Gestione della documentazione del SGSI
- Monitoraggio del SGSI
- Audit interni del SGSI
- Riesame del SGSI da parte della Direzione
- Miglioramento del SGSI
- Allegato A: Obiettivi di controllo e controlli

Case study.

Il processo di certificazione di un Sistema di Gestione per la Sicurezza delle Informazioni.

Cenni agli audit di parte terza.

Obiettivi

Al superamento dell'esame di certificazione i partecipanti avranno conoscenza di:

- l'ambito e le finalità di ISO/IEC 27001
- la terminologia e le definizioni
- i requisiti per ottenere la certificazione del SGSI
- i processi e gli obiettivi di sicurezza
- il campo di applicazione e l'eligibilità di un SGSI;
- l'utilizzo dei controlli per mitigare i rischi
- gli audit interni e di terza parte
- i vantaggi della certificazione.

Destinatari e Prerequisiti

A chi è rivolto

Responsabili della sicurezza informatica, responsabili di progettazione di sistemi di sicurezza, internal auditor, analisti di sicurezza, personale tecnico di sistemi informativi.

Prerequisiti

Non sono necessari prerequisiti particolari se non di tipo ICT generale.

Iscrizione

Quota di Iscrizione: 1.690,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di

partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

È un corso GOLD

con due partecipazioni potrai concordare con noi la data. Guarda i vantaggi della formula GOLD.

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

La Cloud Security

La nuova evoluzione dei sistemi informativi porta allo spostamento dei servizi verso centri di erogazione esterni alle organizzazioni. Lavorare in Cloud vuol dire attivare dei servizi applicativi e preoccuparsi solo del loro utilizzo e non della loro gestione sistemistica in termini di Infrastruttura HW/SW o Data Protection. Questo nuovo scenario si innesta ad integrazione del sistema informativo classico basato sul modello server-farm based. Ci si pone come obiettivo la formazione di nuove competenze in grado di progettare, implementare e gestire un sistema di sicurezza informatica in ambiente ibrido, ovvero con parte dei servizi gestiti a livello tradizionale e l'altra parte secondo il paradigma del Cloud Computing. Si rivedono, in quest'ottica, i concetti di sicurezza Classica(logica e perimetrale) e di protezione dei dati.

Agenda (2 giorni)

Il Cloud Computing:

cenni di virtualizzazione
architettura ed attori del cloud computing
i servizi di delivery
Infrastructure as a Service Platform as a Service Software as a Service
i modelli di delivery
privato, pubblico ibrido
la multi-tenancy
i principali Brand.

Sicurezza delle Informazioni nel Cloud:

parere del Garante privacy sull'uso del Cloud
sicurezza del Cloud Provider
data protection
Data Lost Prevention
gli impatti dell'ubicazione del dato nei rapporti transnazionali
PCI-DSS e Cloud Computing
sicurezza fisica e logica
firewalling autenticazione forte crittografia Business Continuity e Disaster Recovery. </dd>

Obiettivi

Formare nuove competenze per progettare, implementare e gestire un sistema di sicurezza informatica in ambiente Cloud Computing.

Destinatari e Prerequisiti

A chi è rivolto

Responsabili di sistemi informativi, progettisti e amministratori di sistemi di rete; tecnici di supporto; supervisori di sistemi di sicurezza.

Prerequisiti

DataCenter HW, Sistemi Operativi Enterprise, Storage, Reti (IP, LAN, MAN, Wired e Wireless).
Conoscenze di base sulla sicurezza informatica sia logica che perimetrale.

Iscrizione

Quota di Iscrizione: 1.280,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308

corsi@ssgrr.com

Date e Sedi

Date da Definire

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

Realizzare reti sicure con CheckPoint

corrisponde a Check Point Certified Security Administrator

Il corso affronta i concetti di base per configurare Check Point Security Gateway e Management Software Blades. Gli argomenti su cui verteranno le lezioni sono principalmente le Security Policy e la gestione ed il monitoraggio di una rete sicura. Inoltre, verrà analizzato come configurare il Security Gateway per realizzare una rete privata virtuale per utenti interni, esterni e remoti. Il corso fornisce le competenze necessarie per sostenere l'esame di certificazione "Check Point Certified Security Administrator (CCSA-R77)".

Agenda (3 giorni)

Overview sulla tecnologia CheckPoint:

il Firewall CheckPoint
meccanismo di controllo del traffico
architettura del Security Gateway Inspection
Security Policy Management
SmartConsole
Security Management Server.

Piattaforme CheckPoint:

UTM-1 Edge Appliance
IP Appliance
IP Network Voyager
IPSO
SecurePlatform.

Security Policy:

Security Policy Base
Managing Object
Rule Based
Gestione Policy e Revision Control
NAT.

Monitoraggio del Traffico e delle Connessioni:

SmartView Tracker
SmartView Monitor
Monitoring Sospicius Activity Rules
Gateway Status.

Smart Update:

SmartUpdate e Gestione Licenze
architettura SmartUpdate.

User Management e Authentication:

Users e Groups
Security Gateway Authentication
User Authentication
Session Authentication
Client Authentication
LDAP User Management con SamrtDirectory.

Identity Awareness:

abilitare l'Identity Awareness
definizioni di Access Rule.

CheckPoint VPN:

configurare le VPN
topologie VPN
Access Control e VPN Communities
integrazione di VPN in una Rule Base
Remote Access VPN.

Obiettivi

Al termine del corso i partecipanti sono in grado di valutare e attivare i vari meccanismi di sicurezza messi a disposizione dai sistemi Check Point.

Destinatari e Prerequisiti

A chi è rivolto

Responsabili di sistemi informativi, di centri elaborazione dati e di infrastrutture di rete; progettisti e amministratori di sistemi di rete; consulenti nel settore del Security management; sistemisti di rete; supervisori di sistemi di sicurezza. Candidati alla certificazioni Check Point Certified Security Administrator.

Prerequisiti

Per trarre i massimi benefici da questo corso i partecipanti devono possedere le seguenti conoscenze di base: modello di riferimento OSI, stack di protocolli TCP/IP, principi di base sul routing.

Iscrizione

Quota di Iscrizione: 1.880,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

È un corso GOLD

con due partecipazioni potrai concordare con noi la data. Guarda i vantaggi della formula GOLD.

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

Realizzare reti sicure con CheckPoint: aspetti avanzati

corrisponde a Check Point Certified Security Expert

Il corso affronta i concetti avanzati su Check Point Security Gateway e Management Software Blades. In particolare il corso fornisce una preparazione pratica per ottenere competenze avanzate necessarie per gestire e risolvere i problemi su Check Point R77 Software Blades, tra cui firewall avanzati, gestione avanzate degli utenti e clustering, IPsec e VPN avanzata e accesso remoto. Inoltre, i discenti, andranno ad eseguire il debug sui processi dei firewall e ad ottimizzare le prestazioni della VPN. Il corso fornisce le competenze necessarie per sostenere l'esame di certificazione "Check Point Certified Security Expert (CCSE-R77)".

Agenda (3 giorni)

Upgrading Avanzato:

Back up and Restore Security Gateways
Workflow
Upgrade Cluster
Inter-VDOM link.

Firewall Avanzato:

Infrastruttura Firewall-1
Secure Gateway
Kernel Tables
NAT
FW Monitor.

Clustering e Acceleration:

ClusterXL: Load Balancing
Gestione HA
SecureXL: Secure Acceleration
CoreXL: Multicore Acceleration
Forwarding Domain.

User Management Avanzato:

User Management
Identity Awareness.

IPSec VPN avanzato e Accesso Remoto:

VPN Azanzate
VPN per Accesso Remoto
Multiple Entry Point VPN
Tunnel Management
VPN Debug.

Auditing e Reporting:

Processi di Auditing e Reporting
SmartEvent
SmartReporter
Virtual Clustering.

Obiettivi

Al termine del corso i partecipanti sono in grado di valutare e attivare i vari meccanismi di sicurezza avanzati messi a disposizione dai sistemi CheckPoint.

Destinatari e Prerequisiti

A chi è rivolto

Responsabili di sistemi informativi, di centri elaborazione dati e di infrastrutture di rete; progettisti e amministratori di sistemi di rete; consulenti nel settore del Security management; sistemisti di rete; supervisori di sistemi di sicurezza. Candidati alla certificazione CheckPoint Certified Security Expert.

Prerequisiti

Per trarre i massimi benefici da questo corso i partecipanti devono possedere le seguenti conoscenze di base: modello di riferimento OSI, stack di protocolli TCP/IP, principi di base sul routing, uso e configurazione di base di sistemi CheckPoint.

Iscrizione

Quota di Iscrizione: 1.930,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

È un corso GOLD

con due partecipazioni potrai concordare con noi la data. Guarda i vantaggi della formula GOLD.

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

Reti sicure in ambiente Fortinet: aspetti di base

corrisponde a Fortinet Certified Network Security Associate

Agenda (2 giorni)

User Management Avanzato:

- User Management
- Identity Awareness.

IPSec VPN avanzato e Accesso Remoto: Overview and System Setup:

- La soluzione Fortinet
- Basi di Firewalling
- FortiGate
- Device Adminsitrator.

Servizi FortiGuard:

- FortiGuard Distribution Network
- FortiGuard Antivirus Service
- FortiGuard Intrusion Protection System Service
- FortiGuard Web Filtering Service
- FortiGuard AntiSpam Service.

Logging and Alerts:

- Log Storage Location
- Logging Levels
- Log types
- Configure Logging.

Basic VPN:

- Fortigate VPN
- SSL VPN
- PPTP VPN
- IPSec VPN.

Authentication:

- Metodi di autenticazione
- Utenti e Gruppi di Utenti
- PKI Authentication
- Radius Authentication
- LDAP Authentication
- TACACS+
- Microsoft ActiveDirectory Authentication.

Antivirus:

- Antivirus Elements
- File Filter
- Virus Scan
- Grayware
- Quarantena.

Spam Filtering:

- Metodi di Spam Filtering
- FortiGuard Antispam
- Banned Word
- Black\White List

Web Filtering:

- Web Content Block
- Web content Exemption
- URL Filter
- FortiGuard Web Filter.

Obiettivi

Al termine del corso i partecipanti sono in grado di valutare e attivare i vari meccanismi di sicurezza messi a disposizione dagli apparati Fortinet.

Destinatari e Prerequisiti

A chi è rivolto

Responsabili di sistemi informativi, di centri elaborazione dati e di infrastrutture di rete; progettisti e amministratori di sistemi di rete; consulenti nel settore del Security management; sistemisti di rete; supervisori di sistemi di sicurezza. Candidati alla certificazione Fortinet FCNSA.

Prerequisiti

Per trarre i massimi benefici da questo corso i partecipanti devono possedere le seguenti conoscenze di base: modello di riferimento OSI, stack di protocolli TCP/IP, principi di base sul routing.

Iscrizione

Quota di Iscrizione: 1.190,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

È un corso GOLD

con due partecipazioni potrai concordare con noi la data. Guarda i vantaggi della formula GOLD.

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

Reti sicure in ambiente Fortinet: aspetti avanzati

corrisponde a Fortinet Certified Network Security Professional

Agenda (3 giorni)

Virtual Networking:

- Virtual Local Area Network
- Virtual Domain
- Inter-VDOM link.

Diagnostic:

- comandi di Diagnostica
- Self Help Options.

Modalità Trasparent:

- modalità Operative
- Vlan sul Fortigate in modalità Trasparent
- Broadcasting Domain
- Forwarding Domain
- Spanning Tree Protocol
- Link Aggregation.

Firewall Policy:

- firewall Policy
- firewall Addresses
- firewall Schedules
- firewall Services
- firewall Action
- firewall Policy Options
- Virtual IP
- Load Balacing.

Routing:

- Policies di routing, rotte statiche e NAT
- Dynamic Routes
- Multicat Routing.

Ottimizzazione del Traffico:

- tecniche Fortigate per l'ottimizzazione delle WAN
- Web cache
- supporto WCCPv2
- Quality of Service.

Gestione delle minacce:

- tecniche di Scansione dei contetnuti
- componenti architetturali della gestione delle minacce
- Antivirus
- Intrusion Prevention System
- Web Filtering
- Spam Filtering
- Data Leak Prevention
- Application Control
- Network Access Control Quarantine
- SSL Content Ispection.

Advanced Authentication:

- Identity-Based Polies
- User Groups
- Authentication Settings
- LDAP Authentication
- Certificate Authentication
- Directory Services Authentication.

Virtual Private Networks:

SSL VPN
IPSec VPN
Internet Key Exchange
Internet Browsing.

High Availability:

High Availability cluster
Protocolli di Clustering FortiGate
modalità di High Availability
Failover
Virtual Clustering.

Obiettivi

Al termine del corso i partecipanti sono in grado di valutare e attivare i vari meccanismi di sicurezza avanzati messi a disposizione dagli apparati Fortinet.

Destinatari e Prerequisiti

A chi è rivolto

Responsabili di sistemi informativi, di centri elaborazione dati e di infrastrutture di rete; progettisti e amministratori di sistemi di rete; consulenti nel settore del Security management; sistemisti di rete; supervisori di sistemi di sicurezza. Candidati alla certificazione Fortinet FCNSP.

Prerequisiti

Per trarre i massimi benefici da questo corso i partecipanti devono possedere le seguenti conoscenze di base: modello di riferimento OSI, stack di protocolli TCP/IP, principi di base sul routing; uso e configurazione di base di apparati Fortinet. acquisibile tramite il corso Fortinet base.

Iscrizione

Quota di Iscrizione: 1.690,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

È un corso GOLD

con due partecipazioni potrai concordare con noi la data. Guarda i vantaggi della formula GOLD.

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

Access Control: la gestione sicura degli utenti e relativi dispositivi di accesso in contesti critici

Le organizzazioni ICT hanno la necessità di ottenere livelli di sicurezza sempre più elevati in modo da garantire allo stesso tempo il business e il rispetto delle normative nazionali e internazionali relative alla protezione delle informazioni. Questi vincoli però si scontrano con le nuove tendenze del mondo ICT che vedono una forte diffusione dei servizi che non sono più relegati a uno stretto gruppo di tecnici. Inoltre negli ultimi anni con il successo dei dispositivi mobili e dell'outsourcing è sparito il tradizionale concetto di perimetro aziendale che determinava il confine logico tra l'azienda e il mondo esterno. Le tecnologie di Access Control permettono l'accesso controllato degli utenti da qualunque piattaforma (PC,notebook, smart phone, tablet) ai servizi ICT dell'azienda in modo sicuro e controllato, in maniera differenziata e profilata. Il corso mira a far acquisire le conoscenze generali della tematica, presentando una comparativa tra le principali soluzioni sul mercato, per poi approfondire le conoscenze tecniche necessarie per il design, configurazione e troubleshooting della soluzione Cisco Identity Service Engine. Gli argomenti illustrati saranno affiancati da attività di laboratorio durante le quali i partecipanti avranno modo di mettere in pratica quanto appreso.

Agenda (3 giorni)

Introduzione.

Mobility e BYOD.

Soluzioni NAC.

Architetture ed integrazioni.

Approfondimento tecnico: soluzione Cisco.

ISE 1.3: design e dimensionamento dell'infrastruttura.

Profiling e Classificazione.

Guest Access Management.

Client Provisioning e Posture Assessment.

Mobility Management.

VPN support.

Anyconnect agent.

Context sharing.

Gestione e Troubleshooting.

Online Demo.

Obiettivi

Fornire competenze, metodologie e criteri per la gestione dei controlli di accesso attraverso la tecnologia leader di mercato Cisco.

Destinatari e Prerequisiti

A chi è rivolto

Responsabili di sistemi informativi, progettisti e amministratori di sistemi di rete; tecnici di supporto; supervisori di sistemi di sicurezza.

Prerequisiti

Conoscenza di base dei Sistemi Informativi, TCP/IP, Sistema operativo Windows.

Iscrizione

Quota di Iscrizione: 1.690,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

Reti sicure in ambiente Juniper: aspetti base

equivalente a Junos Security (JSEC) e Junos Unified Threat Management (JUTM)

Il corso è pensato per i professionisti nell'ambito networking con conoscenze intermedie del software Juniper Network Junos per la serie di dispositivi SRX. Sono analizzate tematiche relative alla configurazione, alle operazioni e alle implementazioni di soluzioni per un ambiente di rete basato su SRX Service Gateway. Gli argomenti chiave, descritti in dettaglio nel programma, includono tecnologie di sicurezza come policy, intrusion detection e prevention, NAT, High Availability cluster, web filtering, antivirus, antispam e filtraggio dei contenuti.Il corso comprende i temi di "Junos Security (JSEC)" e "Junos Unified Threat Management (JUTM)" e fornisce le competenze necessarie per sostenere l'esame Juniper JN0-332, per la certificazione Juniper Networks Certified Specialist Security (JNCIS-SEC).

Agenda (4 giorni)

Panoramica Junos Security:

- Junos security architecture
- principali componenti hardware degli SRX Service Gateway
- Forwarding packet-based vs. session-based.

Zone:

- tipi di zone
- passi di configurazione delle zone
- ordini di configurazione
- monitoraggio e troubleshooting.

Policy di sicurezza:

- tipi, componenti e ordinamento di policy
- ispezione del traffico diretto al dispositivo e del traffico in transito
- Scheduling
- Rematching
- Application Level Gateway
- Address books
- applicazioni
- passi di configurazione delle policy
- configurazione applicazioni custom

Firewall User Authentication:

- tipi di autenticazioni utente
- supporto server di autenticazione
- Client groups.

Screen:

- opzioni di screen
- passi di configurazione degli screen

NAT:

- tipi di NAT/PAT
- linee guida alla configurazione
- passi di configurazione del NAT

VPN IPSec:

- caratteristiche e componenti delle secure VPN
- opzioni di implementazione di Junos OS per IPSec
- passi di configurazione delle VPN IPSec

High Availability (HA) Clustering:

- caratteristiche e componenti della HA
- modalità di cluster
- stato di sincronizzazione
- preparazione del cluster
- passi di configurazione del cluster

Unified Threat Management (UTM):

- Policy di flusso

supporto alla piattaforma
Licensing.

Filtro Antispam:

soluzioni antispam
Whitelist vs. blacklist
ordine delle operazioni
analisi del traffico
passi di configurazione usando la CLI

Protezione Antivirus:

metodi di scanning

Web Filtering:

caratteristiche e soluzioni di filtering

Obiettivi

Destinatari e Prerequisiti

A chi è rivolto

Amministratori di rete, responsabili della sicurezza di rete, consulenti di sicurezza, responsabili dell'implementazione di reti sicure di piccole/medie dimensioni.
Candidati al conseguimento della certificazione Juniper JN0-332.

Prerequisiti

Conoscenze di base su stack di protocolli TCP/IP, principi di base di sicurezza sulle reti, principi di base su switching e routing in ambiente Juniper e uso e configurazione di base di apparati Juniper

Iscrizione

Quota di Iscrizione: 2.190,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Quota di Iscrizione comprensiva del Voucher: 2.390,00 € (+ IVA)

Con l'acquisto del voucher è possibile sostenere l'esame di certificazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

È un corso GOLD

con due partecipazioni potrai concordare con noi la data. Guarda i vantaggi della formula GOLD.

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

Reti sicure in ambiente Juniper: aspetti avanzati

equivalente a Advanced Junos Security (AJSEC) e Junos Intrusion Prevention System Functionality (JIPS)

Il corso è pensato per i professionisti nell'ambito networking con conoscenze avanzate del software Juniper Network Junos per la serie di dispositivi SRX. Verranno coperti argomenti avanzati relativi alla configurazione, al monitoraggio e alle implementazioni di soluzioni Junos OS per la sicurezza. Gli argomenti chiave sono descritti di seguito nel dettaglio ed includono tecnologie di sicurezza come IPSec, virtualizzazione, AppSecure, NAT avanzato, sicurezza layer 2 e IPS.Il corso comprende i temi di "Advanced Junos Security (AJSEC)" e "Junos Intrusion Prevention System Functionality (JIPS)" e fornisce le competenze necessarie per sostenere l'esame Juniper JNO-633, per la certificazione Juniper Networks Certified Professional Security (JNCIP-SEC).

Agenda (5 giorni)

Servizi di sicurezza application-aware:

- elaborazione del traffico AppSecure
- AppID
- AppTrack
- AppFW
- AppDoS
- AppQoS.

Virtualizzazione:

- istanze di routing
- Gruppi RIB
- Routing tra istanze diverse
- Logical systems (LSYS)
- comunicazione Intra-LSYS e Inter-LSYS
- Filter-based forwarding (FBF).

NAT avanzato:

- elaborazione del traffico NAT
- NAT sulla destinazione
- NAT sulla sorgente
- NAT persistente
- NAT statico
- doppio NAT
- NAT trasversale
- DNS doctoring
- NAT IPv6 (Carrier-grade NAT) - NAT64, NAT46, NAT444, DS-Lite
- Routing
- NAT e FBF
- NAT e policy di sicurezza.

VPN IPSec avanzate:

- elaborazione del traffico IPSec
- VPN site-to-site
- VPN hub-and-spoke
- VPN di gruppo
- VPN dinamiche
- Routing su VPN
- VPN e NAT
- Public key infrastructure (PKI) per VPN IPSec
- VPN e dynamic gateways.

Intrusion Prevention:

- processo di ispezione pacchetti IPS
- IPS role-based
- rilevamento degli attacchi signature-based
- riconoscimento scansioni e impronte digitali
- Flooding, attacchi e spoofing
- opzioni di deployment degli IPS e considerazioni

impostazioni di rete
database di attacchi
Signature personalizzate
prevenzione dello scan.

Transparent Mode:

High Availability
traduzione VLAN
Sicurezza layer 2
IRB
Bridge groups
Elaborazione del traffico Spanning tree.

Troubleshooting:

analisi di flusso
SNMP
Show commands
Logging e syslog
Tracing, incluso flow traceoptions
Policy di flusso
cattura di pacchetti.

Obiettivi

Destinatari e Prerequisiti

A chi è rivolto

Amministratori di rete, responsabili della sicurezza di rete, consulenti di sicurezza, responsabili dell'implementazione di reti sicure di medie/grandi dimensioni.
Candidati al conseguimento della certificazione Juniper JN0-633.

Prerequisiti

Conoscenze di sicurezza sulle reti, sull'uso degli apparati della serie SRX, sull'uso e la configurazione di apparati di rete Juniper.

Iscrizione

Quota di Iscrizione: 3.100,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Quota di Iscrizione comprensiva del Voucher: 3.400,00 € (+ IVA)

Con l'acquisto del voucher è possibile sostenere l'esame di certificazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

È un corso GOLD

con due partecipazioni potrai concordare con noi la data. Guarda i vantaggi della formula GOLD.

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308

CCNA Security

corrisponde a Implementing Cisco IOS Network Security (IINS)

Il corso CCNA Security fornisce le competenze necessarie per amministrare in sicurezza una rete IP di medie dimensioni sia in ambito LAN che WAN. L'obiettivo del corso è quello di preparare i partecipanti a diventare delle figure professionali in grado di sviluppare una infrastruttura sicura di rete, di valutare le vulnerabilità della propria rete e di mettere in campo le opportune misure per contrastare le possibili minacce. Il corso fornisce le competenze necessarie per sostenere l'esame di certificazione Cisco 210-260 IINS v3.0.

Agenda (5 giorni)

Le componenti tecniche del "Sistema-Sicurezza":

disponibilità, integrità (autenticità, non-ripudio), riservatezza
sicurezza logica: servizi di sicurezza, tipologia degli attacchi, anatomia di un attacco
certificare la sicurezza (ISO 27000 e ISO 15408).

Esaminare le tipologie di attacco e minimizzare la probabilità di successo dell'attacco:

mitigare gli attacchi di accesso abusivo
attacchi basati sulle password
sfruttamento della fiducia (trust exploitation)
redirezione delle porte
mitigare gli attacchi di Buffer Overflow
IP Spoofing
attacchi DoS e DDoS
virus, worm, e trojan horse
attacchi a livello applicativo
protocolli di gestione
attacchi di raccolta delle informazioni (reconnaissance)
packet sniffer; port scan e ping sweep; query alla Internet pubblica.

Rendere sicuro l'accesso amministrativo degli apparati di rete:

configurare la password
creazione di un account utente
configurare Role-Based CLI access
configurare il supporto avanzato per Virtual Login.

Sicurezza nei router Cisco:

come mettere in sicurezza il piano dei dati, di controllo e di management
descrivere Cisco Security Manager
descrivere le implicazioni che IPv6 introduce nel campo della sicurezza.

Configurare AAA sui Router Cisco usando il database locale:

descrivere le funzioni e l'importanza di AAA
conoscere come i servizi di AAA (Authentication, Authorization, Accounting) sono supportati in Cisco IOS software
conoscere come rendere sicuro l'accesso ai dispositivi di rete e alle reti
configurare AAA con un database locale.

Configurare AAA con l'ausilio di Cisco Secure ACS:

comprendere i benefici di un AAA centralizzato
conoscere le caratteristiche di Cisco Secure Acces Control Server (ACS)
conoscere le caratteristiche dei protocolli RADIUS e TACACS+
installare e configurare il server ACS
configurare i protocolli RADIUS e TACACS+
verificare l'operatività di AAA (troubleshooting).

Liste di accesso:

access control lists (ACL)
standard IP ACL e Extended IP ACL
gestione avanzata delle ACL
configurare e verificare le ACL.

Gestione sicura degli apparati e monitoraggio:

gestione In-Band e Out-Band

linee guida generali sul Management e Reporting in sicurezza
usare i log per monitorare la sicurezza della rete; modelli e livelli di sicurezza di SNMP
Secure Shell (SSH).

Attacchi a livello 2:

proteggere le funzionalità di inoltro degli switch: MAC flooding, MAC spoofing
port security
prevenire il VLAN hopping: switch spoofing, doppio tag
prevenire le manipolazioni dello STP: BPDU guard, root guard, BPDU filtering
proteggere il DHCP
Private VLAN
monitoraggio su reti switched (SPAN: Switched Port Analyzer).

Tecnologie di firewalling:

soluzioni per la difesa del perimetro della rete aziendale
funzionalità di un firewall: packet filtering, proxy, statefull inspection
funzionalità complementari
architetture firewall: screened host, screened network o subnet (DMZ)
tipi di NAT usati nei firewall
configurare Network Address Translation (NAT) e Port Address Translation (PAT)
configurare Cisco IOS Zone-Based Policy Firewall usando CCP (Cisco Configuration Professional)
case studies su Zone-based firewall
apparati Cisco di firewalling: Adaptive Security Appliance (ASA).

Cisco IPS:

descrivere le funzioni di Cisco Intrusion Prevention System (IPS)
tecnologie IPS: Profile-based, Signature-based, Protocol-based
mitigazione delle minacce su un sistema distribuito utilizzando IPS
configurare Cisco IOS IPS usando CCP (Cisco Configuration Professional).

IPSec e VPN:

strumenti per la sicurezza dei dati, crittografia pratica
crittografia simmetrica o a chiave segreta crittografia asimmetrica o a chiave pubblica funzioni di hashing (MD5, SHA-1) ed HMAC
certificati Digitali e PKI
reti private virtuali (RPV o VPN): tipi e tecnologie
componenti e funzionalità di IPSec: AH, ESP e IKE
configurare IPSec site-to-site con chiavi precondivise
verificare l'operatività delle VPN
realizzare VPN con Secure Sockets Layer (SSL).

Simulazione dell'esame e test di preparazione.

Obiettivi

Fornire le conoscenze e competenze necessarie per l'installazione, la gestione ed il troubleshooting dei dispositivi di rete garantendo il mantenimento dell'integrità, della disponibilità e della riservatezza delle informazioni gestite dalla rete.

Destinatari e Prerequisiti

A chi è rivolto

Tecnici (end-user, Internet Service Provider e rivenditori di apparati) responsabili della progettazione, dell'integrazione e della configurazione di reti IP che vogliono minimizzare l'impatto che malfunzionamenti, provocati o accidentali, possono causare sulla propria rete IP.

Prerequisiti

Sono richieste nozioni sull'internetworking simili a quelle fornite nel corso CCNA: conoscenze sui concetti e i termini legati al mondo del networking e dell' IP, conoscenza del mondo LANs, WANs, e IP switching/ routing, capacità di configurare un router e uno switch con la CLI.

Iscrizione

Quota di Iscrizione: 2.300,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Quota di Iscrizione comprensiva del Voucher: 2.528,00 € (+ IVA)

Con l'acquisto del voucher è possibile sostenere l'esame di certificazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

È un corso GOLD

con due partecipazioni potrai concordare con noi la data. Guarda i vantaggi della formula GOLD.

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

Reti sicure in ambiente Cisco, difesa perimetrale con IOS e ASA

corrisponde a Implementing Cisco Edge Network Security Solutions (SENSS)

Agenda (5 giorni)

Principi di progettazione di Sicurezza:

zone di Sicurezza
architetture modulari
architettura SecureX
soluzione TrustSec.

Sviluppo di protezione dell'infrastrutture di Rete:

sicurezza sul control plane Cisco IOS
sicurezza sul Management plane Cisco IOS
sicurezza sul Management plane Cisco ASA
sicurezza a livello 2
sicurezza a livello 3.

NAT su Cisco IOS e ASA:

il NAT (Network Address Traslation)
implementare il NAT su Cisco ASA
implementare il NAT su Cisco IOS.

Controlli delle minacce sul Cisco ASA:

introduzione sul controllo di minacce sul Firewall Cisco
implementare policy base su Cisco ASA
implementare policy avanzate su Cisco ASA
implementare policy Reputation-based su Cisco ASA
implementare policy Identity-based su Cisco ASA.

Controlli delle minacce su Cisco IOS:

implementare policy base su Cisco IOS
implementare policy avanzate su Cisco IOS.

Obiettivi

L'obiettivo del corso è quello di fornire agli studenti le conoscenze fondamentali e le capacità per attuare e gestire la sicurezza delle reti tramite Firewall ASA, router e switch Cisco.

Destinatari e Prerequisiti

A chi è rivolto

Responsabili di sistemi informativi, di centri elaborazione dati e di infrastrutture di rete; progettisti e amministratori di sistemi di rete; consulenti nel settore del Security management; sistemisti di rete; supervisori di sistemi di sicurezza. Candidati alle certificazioni Cisco CCNP Security.

Prerequisiti

Per trarre i massimi benefici da questo corso i partecipanti devono possedere le seguenti conoscenze di base: modello di riferimento OSI, stack di protocolli TCP/IP, principi di base sul routing, uso e configurazione di base di apparati Cisco.

Iscrizione

Quota di Iscrizione: 2.700,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Quota di Iscrizione comprensiva del Voucher: 2.928,00 € (+ IVA)

Con l'acquisto del voucher è possibile sostenere l'esame di certificazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

Reti sicure in ambiente Cisco, difesa perimetrale avanzata con ASA

corrisponde a Implementing Cisco Threat Control Solutions (SITCS)

Il corso affronta le tematiche della sicurezza di rete, in particolare, l'architettura avanzata del firewall e la configurazione dei Cisco ASA next-generation firewall, utilizzando policy di accesso e di identità. Gli argomenti su cui verteranno le lezioni sono principalmente gli Intrusion Prevention System (IPS) e i componenti firewall context-aware, così come soluzioni di sicurezza Web (Cloud) e Email Security. È parte del percorso formativo per conseguire la certificazione CCNP Security, comprende i temi di "Implementing Cisco Threat Control Solutions (SITCS)" e fornisce le competenze necessarie per sostenere l'esame di certificazione 300-207 SITCS.

Agenda (5 giorni)

Cisco ASA Next-Generation Firewall (NGFW):

Cisco ASA NGFW
architettura Cisco ASA NGFW
Implementare Policy Objects su ASA NGFW
monitoring del Cisco ASA NGFW
implementare access policies su Cisco ASA NGFW
implementare identity policies su Cisco ASA NGFW
implementare decryption policies su Cisco ASA NGFW.

Cisco Web Security Appliance:

soluzioni Cisco Web Security appliance
integrazioni con Cisco Web Security appliance
implementare controlli di Authentication e identities sul Cisco Web Security appliance
implementare controlli anty-malware su Cisco Web Security appliance
implementare Cisco Web Security appliance Decryption
implementare Cisco Web Security appliance Data Security controls.

Cisco Cloud Web Security:

Soluzioni Cisco Cloud Web Security
Configurare Cisco Cloud Web Security
Web Filtering Policy su Cisco ScanCenter.

Cisco Email Security:

Soluzioni Cisco Email Security
Implementare componenti base del Cisco Email Security Appliance
implementare policies di Incoming e Outcoming del Cisco Email Security Appliance.

Cisco Intrusion Prevention System:

soluzioni Cisco IPS
integrazione del sensore Cisco IPS nella rete
configurazione base del Cisco IPS
tuning del Cisco IPS
configurazioni personalizzate delle signaures IPS
configurare le Anomaly Detection nel Cisco IPS
configurare le Cisco IPS Reputation-Based.

Obiettivi

Al termine del corso, gli studenti saranno in grado di ridurre il rischio per le proprie infrastrutture IT e le applicazioni che utilizzano funzionalità di appliance di sicurezza con Cisco Firewall Next Generation e fornire supporto operativo per Intrusion Prevention Systems, Web e Email Security.

Destinatari e Prerequisiti

A chi è rivolto

Responsabili di sistemi informativi, di centri elaborazione dati e di infrastrutture di rete; progettisti e amministratori di sistemi di rete; consulenti nel settore del Security management; sistemisti di rete; supervisori di sistemi di sicurezza. Candidati alle certificazioni Cisco CCNP Security.

Prerequisiti

Per trarre i massimi benefici da questo corso i partecipanti devono possedere le seguenti conoscenze di base: modello di riferimento OSI, stack di protocolli TCP/IP, principi di base sul routing, uso e configurazione di base di apparati Cisco.

Iscrizione

Quota di Iscrizione: 2.700,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Quota di Iscrizione comprensiva del Voucher: 2.928,00 € (+ IVA)

Con l'acquisto del voucher è possibile sostenere l'esame di certificazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

Reti sicure in ambiente Cisco, identificazione ed accessi sicuri

corrisponde a Implementing Cisco Secure Access Solutions (SISAS)

Il corso affronta l'implementazione dell'architettura di Secure Access Solution, utilizzando 802.1X e Cisco TrustSec. Nel dettaglio viene approfondita la conoscenza della soluzione architetturale Cisco Identity Services Engine (ISE) e i loro componenti come soluzioni complessive di mitigazione delle minacce di rete e di controllo degli endpoint. Il corso comprende anche i concetti fondamentali per integrare dispositivi esterni (BYOD) con il profiling servizi di ISE. È parte del percorso formativo per conseguire la certificazione CCNP Security, comprende i temi di "Implementing Cisco Secure Access Solutions (SISAS)" e fornisce le competenze necessarie per sostenere l'esame di certificazione 300-208 SISAS.

Agenda (5 giorni)

Mitigazione delle minacce tramite servizi Identificativi:

Servizi identificativi
802.1x e EAP
il sistema d'identificazione.

Cisco ISE:

Cisco ISE
Cisco ISE PKI
Cisco ISE Authentication
Cisco ISE External Authentication.

Controlli di accesso avanzati:

autenticazione Certified-based
autorizzazione
Cisco TrustSec and MACsec.

Autenticazione web e Guest Access:

implementare WebAuth
implementare Servizi Guest
implementare policy avanzate su Cisco ASA
implementare policy Reputation-based su Cisco ASA
implementare policy Identity-based su Cisco ASA.

Miglioramenti dei Controlli d'accesso degli Endpoint:

Implementare le caratteristiche dei servizi
Implementare i profili dei servizi
implementare BYOD.

Troubleshooting dei controlli d'accesso.

Obiettivi

Al termine del corso i partecipanti sono in grado di valutare e attivare i vari meccanismi di sicurezza degli accessi tramite firewall ASA o IOS dei router e degli switch.

Destinatari e Prerequisiti

A chi è rivolto

Responsabili di sistemi informativi, di centri elaborazione dati e di infrastrutture di rete; progettisti e amministratori di sistemi di rete; consulenti nel settore del Security management; sistemisti di rete; supervisori di sistemi di sicurezza. Candidati alle certificazioni Cisco CCNP Security.

Prerequisiti

Per trarre i massimi benefici da questo corso i partecipanti devono possedere le seguenti conoscenze di base: modello di riferimento OSI, stack di protocolli TCP/IP, principi di base sul routing, uso e configurazione di base di apparati Cisco.

Iscrizione

Quota di Iscrizione: 2.700,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di partecipazione.

Quota di Iscrizione comprensiva del Voucher: 2.928,00 € (+ IVA)

Con l'acquisto del voucher è possibile sostenere l'esame di certificazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

Reti sicure in ambiente Cisco, connessioni remote e VPN

corrisponde a Implementing Cisco Secure Mobility Solutions (SIMOS)

Il corso affronta le tematiche della sicurezza di rete, in particolare, come configurare e implementare le soluzioni Virtual Private Network (VPN) che Cisco ha a disposizione sul firewall Cisco ASA e sulle piattaforme software Cisco IOS. Gli argomenti su cui verteranno le lezioni forniranno le conoscenze necessarie per attuare correttamente le comunicazioni a distanza ad alta sicurezza attraverso la tecnologia VPN, come ad esempio l'accesso remoto SSL VPN e site-to-site VPN (DMVPN, FlexVPN). È parte del percorso formativo per conseguire la certificazione CCNP Security, comprende i temi di "Implementing Cisco Secure Mobility Solutions (SIMOS)" e fornisce le competenze necessarie per sostenere l'esame di certificazione 300-209 SIMOS.

Agenda (5 giorni)

Fondamenti di crittografia e Tecnologia VPN:

il ruolo delle VPN nella sicurezza della rete
VPN e crittografia.

Implementare IPsec point-to-point su Cisco ASA:

Soluzioni Cisco Secure site-to-site
implementare VPN IPsec point-to-point con Cisco IOS FlexVPN
implementare VPN IPsec Hub-and-spoke con Cisco IOS FlexVPN.

Implementare clientless SSL VPNs:

implementare Clientless SSL VPNs
implementare Clientless SSL VPNs su Cisco ASA
implementare applicazioni di accesso per clientless su Cisco ASA
implementare Authentication and Authorization avanzata per clientless VPN SSL
implementare policy Identity-based su Cisco ASA.

Implementare Cisco AnyConnect VPN:

implementare AnyConnect SSL VPN base su Cisco ASA
implementare AnyConnect SSL VPN azanzato su Cisco ASA
implementare Authentication e Authorization su Cisco AnyConnect VPN
implementare Cisco VPN AnyConnect IPSec/IKEv2.

Implementare sicurezza sugli Endpoint e Access Policy dinamiche:

implementare Host Scan
implementare DAP per VPN SSL.

Obiettivi

Al termine del corso i partecipanti avranno le conoscenze necessarie per attuare correttamente le connessioni remote ad alta sicurezza attraverso la tecnologia VPN.

Destinatari e Prerequisiti

A chi è rivolto

Responsabili di sistemi informativi, di centri elaborazione dati e di infrastrutture di rete; progettisti e amministratori di sistemi di rete; consulenti nel settore del Security management; sistemisti di rete; supervisori di sistemi di sicurezza. Candidati alle certificazioni Cisco CCNP Security.

Prerequisiti

Per trarre i massimi benefici da questo corso i partecipanti devono possedere le seguenti conoscenze di base: modello di riferimento OSI, stack di protocolli TCP/IP, principi di base sul routing, uso e configurazione di base di apparati Cisco.

Iscrizione

Quota di Iscrizione: 2.700,00 € (+ IVA)

La quota comprende la didattica, la documentazione, il pranzo e i coffee break. Al termine del corso sarà rilasciato l'attestato di

partecipazione.

Quota di Iscrizione comprensiva del Voucher: 2.928,00 € (+ IVA)

Con l'acquisto del voucher è possibile sostenere l'esame di certificazione.

Partecipazioni Multiple

Per le partecipazioni multiple che provengono da una stessa Azienda, è adottata la seguente politica di sconto:
10% sulla seconda
40% sulla terza
80% dalla quarta in poi.

Informazioni

Segreteria Corsi - Reiss Romoli s.r.l. - tel 0862 452401 - fax 0862 028308
corsi@ssgrr.com

Date e Sedi

Date da Definire

Formazione in House

Il corso può essere svolto presso la sede del Cliente e personalizzato nei contenuti.

Segreteria Corsi - Reiss Romoli s.r.l. - tel +39 0862 452401 - fax +39 0862 028308
email: corsi@ssgrr.com

Reiss Romoli 2022