Opleiding : Check Point R82, Netwerkbeveiliging, Niveau 1

Praktijkcursus - 4d - 28u00 - Ref. CPG
Prijs : 2580 € V.B.

NEW

In deze cursus maakt u kennis met de nieuwste versie van Check Point-producten: R82. Aan het einde van deze cursus bent u in staat om een uniform beveiligingsbeleid (Toegangscontrole en Dreigingspreventie) en een gedeeld beveiligingsbeleid (Geo Policy en HTTPS Inspection) te implementeren en te beheren.

Pedagogische doelstellingen

Aan het einde van de training is de deelnemer in staat om:

- Check Point R82 installeren en configureren
- Een beveiligingsbeleid implementeren en verkeer monitoren
- Externe sites implementeren en beveiligingsbeleid delen
- De visualisatie van logs en monitoring onder de knie krijgen
- Gebruikersauthenticatie beheren
- Een cluster met hoge beschikbaarheid implementeren

Doelgroep

Systeem-/netwerk-/beveiligingsbeheerders en -ingenieurs, technici.

Voorafgaande vereisten

Goede kennis van TCP/IP. Basiskennis van IT-beveiliging.

Opleidingsprogramma

DEELNEMERS

Systeem-/netwerk-/beveiligingsbeheerders en -ingenieurs, technici.

VOORAFGAANDE VEREISTEN

Goede kennis van TCP/IP.
Basiskennis van IT-beveiliging.

VAARDIGHEDEN VAN DE CURSUSLEIDER

De deskundigen die de cursus leiden zijn specialisten op het betreffende vakgebied. Zij werden geselecteerd door onze pedagogische teams zowel om hun vakkennis als hun pedagogische vaardigheden voor elke cursus die zij geven. Zij hebben minstens vijf tot tien jaar ervaring in hun vakgebied en oefenen of oefenden verantwoordelijke bedrijfsfuncties uit.

BEOORDELINGSMODALITEITEN

De cursusleider beoordeelt de pedagogische vooruitgang van de deelnemer gedurende de gehele cursus aan de hand van meerkeuzevragen, praktijksituaties, praktische opdrachten, ...
De deelnemer legt ook van tevoren en naderhand een test af ter bevestiging van de verworven kennis.

1 Gaia implementatie: installatie van [apparaten " Check Point

- Check Point-producten.
- Nieuwe functies in versies R81.xxx en R82.
- Introductie van het Gaïa-systeem.
- Elementen van drielagenarchitectuur.
- Modulaire software blade-architectuur.
- Check Point Infinity.
- Gedistribueerde en standalone architectuur.
- De beheerserver. Het SIC-protocol.

Praktisch werk

Installatie van Check Point R82.

2 Security Management Server, geïntegreerde beheertool Smart Console

- Communicatie via het SIC-protocol en objectbeheer.
- Aan de slag met SmartConsole R82.
- Beveiligingsbeleid. Beheer van regels.
- Uniform beleid.
- Pakketinspectie.
- Inline" Beleid (onder regels).
- Web SmartConsole.

Praktisch werk

SmartConsole installeren. Objecten aanmaken. Een beveiligingsbeleid aanmaken.

3 Adresomzetting (NAT)

- Regels voor adresvertaling voor IPv4 en IPv6.
- Statische NAT (One To One NAT) en dynamische NAT (.Many To One NAT)/PAT.
- Handmatige NAT.
- ARP en routing.

Praktisch werk

Implementatie van automatische statische NAT, verbergen en handmatige transactieregels.

4 Beheer op meerdere locaties

- Definitie van beleidspakketten.
- Beheer van beleidspakketten.
- Definitie en soorten lagen.
- Inspectie van pakketten in een geordende laag.
- Beleidslagen delen.
- Beheerderbeheer in SmartConsole.
- Communicatie met de externe gateway.

Praktisch werk

Een externe gateway installeren, een beveiligingsbeleid (Policy Pack) en basisregels voor de externe site maken. Aanmaken en delen van een geordende laag. Aanmaken van een nieuw rechtenprofiel met beperkte autorisaties.

PEDAGOGISCHE EN TECHNISCHE MIDDELEN

• De gebruikte pedagogische middelen en cursusmethoden zijn voornamelijk: audiovisuele hulpmiddelen, documentatie en cursusmateriaal, praktische oefeningen en correcties van de oefeningen voor praktijkstages, casestudies of reële voorbeelden voor de seminars.
• Na afloop van de stages of seminars verstrekt ORSYS de deelnemers een evaluatievragenlijst over de cursus die vervolgens door onze pedagogische teams wordt geanalyseerd.
• Na afloop van de cursus wordt een presentielijst per halve dag verstrekt, evenals een verklaring van de afronding van de cursus indien de stagiair alle sessies heeft bijgewoond.

TOEGANGSMODALITEITEN EN TERMIJNEN

De inschrijving dient 24 uur voor aanvang van de cursus plaatsgevonden te hebben.

TOEGANKELIJKHEID VOOR MINDERVALIDEN

Is voor u speciale toegankelijkheid vereist? Neem contact op met mevr. FOSSE, contactpersoon voor mindervaliden, via het adres psh-accueil@ORSYS.fr om uw verzoek en de haalbaarheid daarvan zo goed mogelijk te bestuderen.

5 Logboeken en bewaking

- Beleid voor logboekbeheer.
- Verbindingen bijhouden met logs en monitor (oude SmartView Tracker).
- De monitor.
- Logboekbeheer.
- SmartView Monitor, functies en alarmdrempels.
- Speciale logserver.

Praktisch werk

Monitoring : utilisation du Suspicious Activity Monitoring Protocol, visualisation du trafic, monitoring de l'état de la politique de sécurité. Troubleshooting : accéder au mode expert, aux commandes "tcpdump" et "fw ctl zdebug drop", visualiser et manipuler les utilitaires CPView et Top.

6 Ontcijfering-HTTPS

- Creëren van outbond en inbound regels.
- Beheer van certificaten.
- Server Name Indications (SNI).
- Geavanceerde tools beheren in de SmartConsole.
- Presentatie van de leermodus en prestatievoorspellingen.
- Inleiding tot Client Side Fail-modus.
- Weergave van de functie Bypass onder belasting.
- Ondersteunt HTTP/3 streams met QUIC (UDP) transportprotocol.

Praktisch werk

Implementatie van HTTPS-inspectie.

7 Toepassingsbeheer/URL-filtering

- De beperkingen van een traditionele firewall per IP en poort.
- Toepassingsherkenning.
- Toegangscontrole.
- De "AppWiki". URL filteren.
- De gebruikerscontrole.
- DNS filteren met het blad Geavanceerde DNS.
- Gebruikersgebaseerd beleid.
- Herstellen van gebruikersidentiteit, Identity Awareness authenticatiemethoden.

Praktisch werk

Filtrage web et applications : créer et partager la politique de Filtrage Web et Applications en tant que inline layer et ordered layer. Authentification : mise en place d'Identity Awareness, création de rôles et des accès.

8 IPSec site-to-site VPN en toegang op afstand

- VPN-architectuur.
- De basis van encryptie, inleiding tot IKE en IPSec.
- Certificeringsautoriteit (CA). Domein-gebaseerd VPN.
- Vereenvoudigde modus. VPN-gemeenschappen configureren.
- VPN-routering.
- Gebruik van het nieuwe Network Probe object om de status van VPN tunnels te controleren.
- SSL VPN en IPSec VPN.
- Blade Mobiele Toegang.
- Type mobiele toegang: Toegang op afstand.
- VPN voor eindpuntbeveiliging.
- NAT-Traversal, Visitor Mode, Hub Mode en Office Mode.

Praktisch werk
VPN-IPSec Inter-sites (gedeeld geheim). VPN-IPSec Intersites (certificaten). Het opzetten van een remote access VPN verbinding via de Check Point Mobile client, ook voor Active Directory gebruikers.

9 Beleid ter voorkoming van bedreigingen

- Het Threat Prevention-beleid en de bijbehorende softwarebladen.
- Regels beheren.
- Veiligheidsprofielen.
- Presentatie van AI-gebaseerde preventie-engines: ThreatCloud Graph, Kronos, Deep Brand Clustering.
- Introductie van autonome preventie van bedreigingen.
- Automatische Zero Phishing-configuratie.
- Feature "Adaptive Hold" voor Anti-Virus en Anti-Bot bladen.

Praktisch werk
Anti-Virus en Anti-Bot.

10 Clustering

- Firewall redundantie.
- ClusterXL in High Availability modus.
- ClusterXL in de modus voor het delen van lasten.
- ClusterXL in actief-actief modus.
- Problemen met VMAC en ARP.

Praktisch werk
Implementatie van ClusterXL in High Availability modus.

Data en plaats

KLAS OP AFSTAND
2026 : 2 juni, 15 sep., 24 nov.

PARIS LA DÉFENSE
2026 : 2 juni, 15 sep., 24 nov.