Publicatiedatum : 03/04/2024

Opleiding : Uw gevirtualiseerde omgeving beveiligen

Synthese cursus - 2d - 14u00 - Ref. VMW
Prijs : 1720 € V.B.

4,2 / 5

In deze cursus krijgt u een technisch overzicht van oplossingen om de beveiliging van uw gevirtualiseerde omgevingen te garanderen: van de belangrijkste zwakke punten van gevirtualiseerde architecturen tot de optimale implementatie van beveiligingsoplossingen.

Pedagogische doelstellingen

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

- Beveiligingsbedreigingen in gevirtualiseerde omgevingen identificeren
- Typologieën van aanvallen begrijpen
- Het virtuele datacenter, VM's, servers en werkstations beveiligen
- De beschikbare hulpmiddelen en technieken beoordelen

Doelgroep

IT-managers, productie-/operatiemanagers en systeem- of netwerkbeheerders.

Voorafgaande vereisten

Basiskennis van technische architectuur (systemen en netwerken) en IT-beveiliging.

Opleidingsprogramma

1 Inleiding tot veiligheid

- Beveiliging: reactief, proactief, voorspellend.
- Interne en externe bedreigingen.
- Toepassingsgebieden (servers, werkstations, clients, applicaties).

DEELNEMERS

IT-managers, productie-/operatiemanagers en systeem- of netwerkbeheerders.

VOORAFGAANDE VEREISTEN

Basiskennis van technische architectuur (systemen en netwerken) en 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.

2 Virtualisatietechnieken

- Contextisolatie, hypervirtualisatie, paravirtualisatie.
- Input/Output (I/O) virtualisatie, klassiek en container.
- Unikernelsystemen, microspiegels.

3 Veiligheid in de industriële omgeving

- Het model van Reason.
- Organisaties en rampen.
- Back-ups, replicaties, DRP.
- Vertrouwde derde partij, man-in-the-middle aanval.

4 Beveiliging in een gevirtualiseerde omgeving

- Industriële voordelen, risico's.
- Luiers om op te letten.
- Het Zero Trust beveiligingsmodel: een nieuw paradigma?
- Microsegmentatie.
- Verdediging in de diepte.
- Beveiligingsdomeinen: netwerk, systeem, beheer, toepassingen.

5 Beveiliging met VMware

- De OSI-lagen.
- VLAN's, routing, virtuele switches, VSS, VDS, N1KV, VXLAN en logische switches.
- Certificering serviceprovider, AD, LDAP, Nis, VMware NSX Edge.
- Systeembeveiligingsprincipes: vertrouwde zones (DMZ), wachtwoordbeleid.
- Encryptie-algoritmen, publieke en private sleutels, zelfondertekende certificaten, vertrouwde autoriteit.

6 VMware applicatiebeveiliging

- Antivirus: VMsafe API, vShield Endpoint.
- Het in kaart brengen van toepassingen, stroombeheer.
- Isolatie: sandboxing toepassingen, containers.
- VMware Photon, ieVM.
- API-bescherming.

7 Voorspelling, preventie, detectie en herstel

- Overzicht van tools (Nessus, Nmap, Kali).
- Inbraakdetectie en testen.
- Logboeken, machinaal leren.
- Gedragsanalyse.
- Risico's en kriticiteit: vCenter Operations Manager (VMware).
- Risico's in kaart brengen.
- Toezicht en bewaking, alarmen.

8 Beveiliging beheer

- ACL, eenvoudige authenticatie, rollen en privileges.
- Social engineering.
- BYOD, schaduw-IT (rogue IT).
- Plan voor het harden van de virtuele infrastructuur.
- Beheer van updates en back-ups.

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.

Data en plaats

KLAS OP AFSTAND
2026 : 2 juni, 24 nov.

PARIS LA DÉFENSE
2026 : 2 juni, 24 nov.