Voorbereiding op de opleiding SOC Analyst van OptiSec

Welkom alvast. In dit pdfje vind je waar SOC Analyst-werk om draait, hoe je laptop klaar te zetten, en welke gratis bronnen je nu al kunt pakken om soepel te starten. Pak een koffie, lees rustig door, en kijk of dit jouw vak is.

OPTISEC CYBER SECURITY TRAININGEN

LEES EERST, DAN INSTALLEER JE

Het is half drie 's nachts. Ergens klikt iemand op een verkeerde link.

Een log slaat aan. Een dashboard pikt het op. En iemand, met een koffie in de hand, denkt: hé, dit klopt niet. Dat moment is waar SOC werk begint. Geen sensatie, geen toetsenbord-hakkerij, gewoon iemand die goed kijkt en de juiste vragen stelt.

Wat een SOC analist écht doet

Een SOC, een Security Operations Center, is het team dat de digitale alarmcentrale van een organisatie bemant. Als analist krijg je een melding binnen, vaak niets bijzonders, soms wel. Jouw werk is uitzoeken welke het is. Detectivewerk in feite. Logs lezen, tijdlijnen reconstrueren, hypotheses toetsen, conclusies opschrijven.

Waarom dit leuk is om te leren

Je hoeft geen briljante programmeur te zijn. Je hoeft niet alles uit je hoofd te kennen. Je moet vooral nieuwsgierig zijn, geduld hebben om door logs heen te spitten, en het leuk vinden om puzzels op te lossen waar geen oplossingsboekje bij zit. Dat kan iedereen leren, op zijn eigen tempo.

BIJ OPTISEC

De meeste mensen hier komen binnen zonder IT-achtergrond. Deze gids maakt de start een stuk soepeler.

Zo ziet jouw route naar SOC Analyst eruit

De volledige opleiding bestaat uit meerdere modules en certificeringen. Je hoeft je daar nu nog niet druk om te maken. Dit document gaat alleen over de voorbereiding. Maar het is goed om te weten waar je naartoe werkt.

JIJ BENT HIER	MODULE 1	MODULE 2	MODULE 3	MODULE 4	MODULE 5
Voorbereiding	**IT Fundamentals**	**CC**	**AZ-900**	**SC-900**	**CDSA**
Tools installeren, basis-IT begrijpen, beetje Linux ruiken	De volledige IT basis. Hardware, OS, netwerken, allemaal van scratch	Certified in Cybersecurity. Eerste echte security certificering	Azure Fundamentals. Cloud begrijpen, want daar leeft tegenwoordig alles	Security, Compliance & Identity Fundamentals. De security kant van Azure	Certified Defensive Security Analyst. Hét eindcerticaat, hands-on SOC werk

Veel mensen denken bij cybersecurity meteen aan hacken. Dat is de aanvallerskant, het 'red team'. Wij leiden je op aan de verdedigingskant, het 'blue team'. Dat betekent dat je leert herkennen wat een aanvaller doet, niet hoe je het zelf zou doen. Iets minder Hollywood, een stuk meer puzzel.

Drie stappen om jezelf voor te bereiden

De stappen lopen op in moeilijkheid. Stap 1 is voor iedereen. Stap 2 is heel handig om alvast te doen. Stap 3 is voor wie er klaar voor is. Hoe verder je komt, hoe soepeler je start zal zijn. Geen verplichte stof, geen druk om alles af te krijgen.

1

Kennismaken en installeren

VMware en Kali Linux op je laptop, een notitie-app, en een AI-account voor als je vastloopt. Hier maak je je werkbank klaar.

2

Gratis leer-materiaal

Online bronnen waar je in je eigen tempo de IT basis kunt opbouwen. TryHackMe, Linux Journey, Professor Messer en HTB Academy.

3

Concepten verkennen

Een lijstje begrippen die in de eerste lesweek voorbij komen. Zoek ze één keer op, dan heb je er al een beeld bij als wij ze behandelen.

HOE JE DIT HET BESTE AANPAKT

Lees eerst dit document helemaal door voordat je begint. Niet om alles te onthouden, maar om te zien wat je te wachten staat. Daarna pak je rustig stap 1. Een paar avonden van een uur is meer dan genoeg om er goed doorheen te komen.

01

STAP 1

Kennismaken en installeren

We beginnen met je werkbank klaarzetten. Een virtuele machine voor Kali Linux, een notitie-app, en een AI-account. Niets technisch om je nu zorgen over te maken, gewoon stap voor stap.

Installeer VMware Workstation Pro

Wat is een VM eigenlijk?

Een computer-in-een-computer, een sandbox waarin je veilig kunt klooien.

Een Virtual Machine is een complete nep-computer die binnen je echte computer draait. Eigen besturingssysteem, eigen bestanden, en als je hem stukmaakt gebeurt er niets met je echte laptop. Voor security werk ideaal.

Wat is VMware Workstation Pro?

Het programma waarin je die VM's draait, een huis voor je virtuele computers.

VMware Workstation Pro is sinds kort gratis voor persoonlijk gebruik. Het is beter dan VMware Player of VirtualBox qua performance. Je virtuele Kali Linux loopt er soepel mee.

Zo download je hem

1 Ga naar de Broadcom site en maak een account aan

VMware is overgenomen door Broadcom. Je downloadt VMware nu via hun portal. Een gratis account aanmaken is verplicht, kost een paar minuten.

2 Klik door naar My Downloads en daarna Free Downloads

Daar vind je VMware Workstation Pro. Klik die aan, en je komt op de downloadpagina met de releases.

3 Pak de versie 26H1

Dat is op dit moment de actuele stabiele versie. Oudere versies (zoals 25H2u1) gaan je telkens lastig vallen met update nag screens, dus pak meteen de juiste. Installeer hem zoals elk ander programma op Windows.

LOOP JE VAST?

Geen paniek. Het Broadcom portal is een doolhof, daar struikelt iedereen wel even. Plak je foutmelding in ChatGPT, Claude of Google en kom er zelf even uit. Uitzoeken en onderzoeken is óók onderdeel van de SOC mindset, dus dit is alvast goede oefening.

Installeer Kali Linux in VMware

Wat is Linux?

Een ander besturingssysteem dan Windows of macOS, vooral populair bij servers.

Linux is gratis, open-source, en heeft duizenden varianten. Vrijwel alle internet-servers draaien er op. Als SOC analist krijg je dagelijks met Linux te maken, en de terminal is een belangrijk gereedschap.

Waarom Kali specifiek?

Kali is een Linux variant met security tools al voorgeïnstalleerd.

Kali is bekend van hacker series en films, in feite een toolkit. Wij gebruiken hem niet om aan te vallen, maar om te begrijpen wat aanvallers doen. We gebruiken Kali ook in de opleiding zelf.

Installatie in vier stappen

1 Download de Kali VM image

Ga naar kali.org/get-kali en kies Virtual Machines. Pak de VMware variant. Ongeveer 3,5 GB. Pak uit op een vaste plek, bijvoorbeeld D:\VMs\Kali.

2 Voeg de VM toe aan VMware

Open VMware. Menu: File → Open. Navigeer naar de uitgepakte Kali map en kies het bestand met de extensie .vmx. De VM verschijnt in je library links.

3 Upgrade de hardware compatibility

Rechts-klik op de VM, ga naar Manage → Change Hardware Compatibility, en zet hem op Workstation 26H1. Hierdoor draait de VM op volle snelheid mee.

4 Verhoog het RAM (als je laptop dat aankan)

Open de VM settings en zet Memory van 2 GB naar 4 GB. Heeft je laptop minimaal 8 GB totaal, geen probleem. Daarna kun je de VM starten.

EERSTE LOGIN Gebruiker en wachtwoord zijn beide kali, dat is de standaard fabrieksinstelling van Kali. Veranderen hoeft niet, maar handig om te weten.

Kies een notitie-app en begin nu al

Tijdens de opleiding ga je veel zien, veel proberen, en veel vergeten. Dat is normaal. Iedereen, ook ervaren SOC analisten, werkt met cheat sheets en eigen notities. Begin daar nu al mee. Het hoeft niet mooi, het hoeft niet compleet, het moet voor jou werken.

Een paar goede opties

AANBEVOLEN

Notion

Gratis, in de browser, makkelijk te delen. Werkt goed voor zowel tekst als screenshots. Voor de meeste mensen de eenvoudigste keuze.

VOOR WIE VAN STRUCTUUR HOUDT

Obsidian

Lokaal op je computer, markdown gebaseerd, krachtig met links tussen notities. Iets steiler om in te komen, maar voor SOC werk geweldig.

MICROSOFT MENSEN

OneNote

Komt vaak al met Office. Werkt prima, vooral als je toch al in het Microsoft ecosysteem leeft.

HACKER OUDE SCHOOL

Cherry Tree

Lokaal, hierarchisch, populair bij pentesters. Een tikje ouderwets uiterlijk maar doet zijn werk.

TIP Documenteer ook al wat je in deze voorbereiding leert. Dat geeft je meteen een idee welke notitie-app voor jou prettig werkt.

Maak een ChatGPT- of Claude-account aan

Een AI-assistent is geen vervanging voor leren, maar wel een goede sparringpartner. Loop je vast op een concept? Vraag hem het in eigen woorden uit te leggen. Begrijp je een log-regel niet? Plak hem erin en vraag wat het betekent. Het bespaart je veel tijd.

ChatGPT

De bekendste, gratis variant is meer dan voldoende voor wat je nu nodig hebt. chat.openai.com

Claude

Goede alternatief, vaak iets nauwkeuriger op technische uitleg. Ook gratis te gebruiken. claude.ai

Hoe je hem het beste gebruikt

- Vraag uitleg in eigen woorden, niet alleen een definitie. "Leg me uit wat een SIEM is alsof ik vijftien ben" werkt vaak beter dan "Wat is een SIEM".
- Plak logs of foutmeldingen er rechtstreeks in. Vraag wat ze betekenen. Niet alleen 'wat is het', ook 'waarom zou dit gebeuren' en 'is dit erg'.
- Gebruik hem niet voor antwoorden op opdrachten. Je leert er niets van. Wel om concepten op te helderen, dat is de bedoeling.
- Hij heeft het ook niet altijd bij het rechte eind. Twijfel je over een antwoord, dubbelcheck via een tweede bron.

02

STAP 2

Gratis leermateriaal

Bronnen waarmee je in je eigen tempo de basis kunt opbouwen. Allemaal gratis, allemaal beginner-vriendelijk. Pak één tegelijk, zonder druk om alles af te ronden.

TryHackMe, Pre Security Path

Als je tijd hebt voor één ding, doe dit dan. TryHackMe is een interactieve leeromgeving waar je in je browser oefent met netwerken, Linux, Windows en webfundamentals. Geen lange video's om door te ploegen, je doet het zelf, in stappen.

Pre Security Path

tryhackme.com/path/outline/presecurity

Vier modules: Cyber Security Introduction, Network Fundamentals, How the Web Works, en Linux Fundamentals. Samen ongeveer dertig uur, te doen in een paar avonden of weekenden. Perfect als je echt vanaf nul begint.

Waarom dit zo goed werkt

Je doet het zelf

Geen passief kijken. Elke oefening eindigt met een vraag die je beantwoordt door iets in een terminal te doen of een log te bekijken. Dat plakt veel beter dan een video.

Veilige sandbox

Alles draait in een browser-VM bij hen. Je kunt niets stukmaken, je hoeft niets te installeren. Klik op start, en je zit in een Linux terminal.

Helder opgebouwd

De cursus is genaaid in de juiste volgorde. Begin gewoon bovenaan, ga één voor één naar beneden. Geen keuzestress.

HOEVEEL TIJD ZOU IK ERIN STEKEN?

Als je hier een uur of dertig in stopt voor de opleiding begint, heb je een enorme voorsprong. Lukt dat niet, doe dan in elk geval de modules Network Fundamentals en Linux Fundamentals. Die twee zijn het belangrijkst.

Linux Journey en Professor Messer

Twee gratis bronnen die je naast TryHackMe kunt gebruiken. Beide leggen de IT basis op een andere manier uit, en herhaling helpt. Als één bron iets niet bij je laat landen, probeert een andere bron het vanuit een net andere hoek.

Linux Journey

linuxjourney.com

Een rustige, tekstuele cursus over Linux. Geen video, geen account nodig. Doe in elk geval alle modules onder Grasshopper. Daar zit de hele basis in: navigeren, bestanden lezen, gebruikersrechten, processen. Reken op een uurtje of zes voor het hele Grasshopper traject.

Professor Messer, CompTIA A+

professormesser.com

Gratis YouTube serie die de absolute IT basis behandelt. Hardware, besturingssystemen, troubleshooting. Engels gesproken, helder uitgelegd. Niet alles is even relevant voor SOC, maar voor wie nog nooit met IT te maken heeft gehad een hele goede start.

Professor Messer, CompTIA Network+

professormesser.com

Vervolg op A+, maar specifiek over netwerken. Voor SOC werk veel relevanter. TCP/IP, DNS, subnetting, routers en switches. Pak deze in elk geval als je weinig idee hebt hoe internet eigenlijk werkt onder de motorkap.

WELKE KIES IK?

Hou je van lezen en je eigen tempo? Linux Journey. Wil je liever iemand zien uitleggen op een whiteboard? Professor Messer. Mag allebei. Maar als je TryHackMe Pre Security al doet, heb je in feite het meeste hier al meegepakt.

HTB Academy, alleen de Tier 0 modules

Hack The Box Academy is het platform dat we tijdens de opleiding intensief gebruiken. Maak nu alvast een gratis account aan. Wat je daarmee gratis kunt doen zijn de Tier 0 modules. Daar hebben we een aantal voor je uitgezocht die mooi bij de start passen.

Een slimme selectie Tier 0 modules

Learning Process

3 uur · Tier 0

Hoe je het beste leert binnen HTB Academy. Klinkt soft, is het niet. Studeren leer je ook, en dit module bespaart je veel tijd later.

Introduction to Information Security

2 uur · Tier 0

De grondbegrippen van het vak. CIA triad, threat modeling, security principles. Korte module, doe hem zeker.

Network Foundations

4 uur · Tier 0

Hoe een netwerk werkt, vanaf de basis. Pakketjes, protocollen, routing. Onmisbaar voor SOC werk.

Linux Fundamentals

6 uur · Tier 0

Gaat sneller als je Linux Journey al hebt gedaan. Veel overlap, maar HTB Academy gaat een stap verder en is hands-on.

Windows Fundamentals

6 uur · Tier 0

De Windows kant van het verhaal. Belangrijk, want de meeste eindgebruikers waar je in een SOC naar kijkt zitten op Windows.

Web Requests

4 uur · Tier 0

Hoe browsers en servers met elkaar praten via HTTP. Veel SOC-detecties zitten op webverkeer, dus
Deze verdient zichzelf snel terug.

NAAST HTB NOG IETS

HTB is de hands-on helft. Je gaat tijdens de opleiding óók examens halen (CC, AZ-900, SC-900). Daar krijg je studiemateriaal en begeleiding voor zodra je officieel begint. Niets om je nu druk om te maken.

03

STAP 3

Concepten verkennen

Een lijstje begrippen die je in de eerste lesweken tegenkomt. Je hoeft ze niet uit je hoofd te leren. Zoek ze één keer op, lees twee minuten, en je hebt er al een beeld bij als wij er dieper op ingaan.

Wat is een SOC, en wat doet een analist?

SOC, Security Operations Center

De alarmcentrale van de digitale wereld.

Een team dat continu de IT systemen van een organisatie in de gaten houdt. Komt er een verdacht signaal binnen, een mislukte login, een raar bestand, een onbekend verbonden apparaat, dan kijkt het SOC of het iets is om je zorgen om te maken. Een groot SOC werkt 24/7 in shifts, een klein SOC werkt vaak alleen kantooruren met een wachtdienst.

De rollen in een SOC

TIER 1

Analyst

De eerste lijn. Bekijkt alle alerts die binnenkomen, beoordeelt of het echt of false positive is, en escaleert wat de moeite waard is naar Tier 2. Vaak waar je begint.

TIER 2

Senior Analyst

Pakt de echte incidenten op die Tier 1 doorgeeft. Doet diepere analyse, gaat de timeline reconstrueren, en bepaalt of het een echt incident is. Verzint daarnaast nieuwe detecties.

TIER 3

Threat Hunter

Werkt niet vanuit alerts maar vanuit hypotheses. Zoekt proactief naar aanvallers die door alle detecties heen zijn geslipt. Vergt veel ervaring en domeinkennis.

WAT DOET EEN ANALYST OP EEN DAG?

Alerts triagen, logs lezen, IPs en hashes opzoeken in threat intelligence, mailtjes bekijken die door medewerkers gemeld zijn als verdacht, rapportages maken van wat is gedaan, en handover doen aan de volgende shift. Geen Hollywood scenes. Wel detective werk, en veel ervan.

Basis netwerk begrippen

Een SOC analist kijkt voortdurend naar netwerkverkeer. Welke computer heeft contact met welke server, op welke poort, met welk protocol. Hieronder de begrippen die je heel vaak gaat tegenkomen.

IP adres

Het huisnummer van een apparaat op een netwerk.

Elk apparaat heeft een uniek IP adres, zoals 192.168.1.10. Daarmee weet de rest van het netwerk waar pakketjes naartoe moeten.

Poort

De voordeur, achterdeur en zijdeur van dat huis.

Een apparaat kan tegelijk allerlei diensten draaien. Een poort is het deurnummer waarop een specifieke dienst luistert. Poort 80 is voor HTTP, 443 voor HTTPS, 22 voor SSH.

DNS

Het telefoonboek van het internet.

Mensen onthouden google.com, computers werken met IP adressen. DNS vertaalt het ene naar het andere. Vreemde DNS-aanvragen verraden vaak malware.

TCP versus UDP

Aangetekende post versus een schreeuw door de straat.

TCP is netjes en betrouwbaar, bevestigt of pakketjes zijn aangekomen. UDP is snel en luidruchtig. Websites en logins gebruiken TCP, streaming vaak UDP.

HTTP en HTTPS

Het protocol waarmee websites praten met je browser.

HTTPS is de versleutelde versie. Vrijwel alles is tegenwoordig HTTPS. Voor een SOC analist zit veel actie hier, omdat aanvallers via webverkeer komen en gaan.

Firewall

De portier bij de ingang van het netwerk.

Controleert al het verkeer dat binnenkomt en uitgaat, op basis van regels. Wat niet mag, wordt geweigerd. Firewall logs zijn een belangrijke bron voor SOC werk.

Logs en SIEM

Vraag een SOC analist wat hij of zij de hele dag doet, en het antwoord is bijna altijd: naar logs kijken. Het zoeken, lezen, en interpreteren van logs is het hart van het werk. Hieronder de twee belangrijkste begrippen.

Log

Het papieren spoor van alles wat een systeem doet.

Elke server, elke applicatie, elk apparaat schrijft op wat er gebeurt. Wie logt in, wat doet die, om hoe laat, vanaf waar. Een Windows server produceert duizenden logregels per dag, zonder dat er iets bijzonders gebeurt. Tussen die regels zit af en toe het bewijs van een aanval.

SIEM, Security Information and Event Management

De centrale bibliotheek waar alle logs binnenkomen, plus een hele goede zoekmachine.

Een SIEM verzamelt logs van overal in de organisatie en bewaart ze op één plek. Daar kun je doorheen zoeken, correlaties leggen tussen verschillende bronnen, en alerts laten genereren als bepaalde patronen voorbij komen. Bekende SIEMs zijn Splunk, Elastic en Microsoft Sentinel. Bij OptiSec werken we met Splunk en Sentinel.

Waarom dit zo centraal staat

- Zonder logs ben je blind. Een aanvaller kan dagen of weken in een netwerk zitten. De sporen die hij achterlaat in logs verraden hem.
- Met alleen logs ben je verloren. Miljoenen regels per dag handmatig doorlopen werkt niet. Een SIEM met goede zoekqueries maakt het werkbaar.
- Daarom oefen je dit veel. Veel van de opleiding gaat over zoekqueries schrijven en logs lezen. Lijkt saai, in de praktijk is het puzzelen en best verslavend.

Wat probeert een aanvaller eigenlijk?

Om als verdediger goed te zijn, moet je begrijpen hoe aanvallers werken. Niet om het na te doen, maar om hun bewegingen in je logs te herkennen.

Phishing

Nep-mail of nep-website die eruitziet als echt, om je inloggegevens of een klik op iets gevaarlijks te ontfutselen. De nummer één manier waarop aanvallers binnenkomen.

Malware

Verzamelnaam voor kwaadaardige software. Daaronder vallen virussen, trojans, ransomware, info stealers en remote access tools. Ze willen iets op je systeem doen wat jij niet wilt.

Ransomware

Specifieke vorm van malware die je bestanden versleutelt en losgeld eist. Wereldwijd de grootste plaag. Een goed SOC kan dit vroeg signaleren, voordat versleuteling begint.

Brute force

Wachtwoorden raden door duizenden combinaties te proberen. Te detecteren aan veel mislukte loginpogingen in korte tijd. Effectief tegen zwakke wachtwoorden.

De kill chain, sterk vereenvoudigd

1 INITIAL ACCESS

Aanvaller komt binnen. Vaak via phishing, een gestolen wachtwoord of een kwetsbare server.

2 PRIVILEGE ESCALATION

Eenmaal binnen probeert hij hogere rechten te krijgen. Van gewone gebruiker naar admin.

3 LATERAL MOVEMENT

Met die rechten beweegt hij door het netwerk, op zoek naar waardevolle systemen.

4 IMPACT

De daad. Data stelen, versleutelen of saboteren. Dit is het moment dat het lawaai begint.

Het hele werk van een SOC is aanvallers vroeg spotten in deze keten. Hoe eerder, hoe minder schade. Stoppen bij stap 1 is veel goedkoper dan opruimen na stap 4.

Windows en Linux, je ziet ze allebei

De meeste eindgebruikers in een organisatie zitten op Windows. De meeste servers, vooral op het internet, draaien Linux. Als SOC analist krijg je beide werelden voor je kiezen. Niet meteen, maar wel uiteindelijk.

Windows in een SOC

Het besturingssysteem op de werkplekken en op een groot deel van de bedrijfsservers.

Wat je vooral ziet zijn Event Logs, Active Directory logins, Sysmon events, en logs van de Endpoint Detection tools (Defender, CrowdStrike). De volgende leuke uitdaging is dat Windows niet één type log heeft, maar tientallen, elk met hun eigen kuren.

Linux in een SOC

Het besturingssysteem op de meeste server-infrastructuur, vooral richting internet toe.

Wat je hier vooral ziet zijn de syslogs, auth logs, web server logs (Apache, Nginx) en applicatie logs. De terminal is je gereedschap. Daarom is het zo handig om voor de opleiding al een beetje vertrouwd te raken met Linux commando's.

JE HOEFT GEEN EXPERT TE ZIJN IN BEIDE

Veel SOC analisten hebben een voorkeur of een specialisatie. Iemand die uit Windows administration komt zal Linux logs langzamer doorgronden, en omgekeerd. Dat is prima. Wat we vragen is dat je in beide werelden de basis kan, en weet waar je extra hulp kan vinden als het verder gaat dan dat.

Klaar voor de start?
Dat is mooier dan je denkt.

Heb je deze gids doorgenomen en stap 1 gedaan, dan zit je al ruim boven het gemiddelde van wie op dag één binnenkomt. Wij beginnen sowieso bij het begin, dit document maakt jouw begin alleen wat soepeler.

Wat je mag verwachten van ons

Het tempo is stevig en de stof is geregeld pittig, daar zijn we eerlijk over. Daar zetten we persoonlijke begeleiding in kleine groepen tegenover. Vragen mogen altijd, hoe klein ook.

Wat wij van jou verwachten

Nieuwsgierigheid, doorzettingsvermogen op momenten dat iets niet werkt, en bereidheid om vragen te stellen. Verder niets. Geen voorkennis, geen vakdiploma's, geen IT-achtergrond.

VRAGEN OVER DEZE GIDS?

ChatGPT, Claude of een nette Google search lossen 90% op. Uitzoeken hoort sowieso bij SOC werk, zie het als de eerste oefening. Welkom alvast.