

Integraal studieplan cyberbeveiliging

Een haalbaar traject in drie fasen voor de 150 mindmaps en bonussen

Doorloop de fundamenteën, bouw kennis op over verdediging en netwerken en verbind die met SOC, pentesting en cloud. Per fase vind je een volgorde, tijdsinschatting, zelfcontrole en koppelingen naar Bonus 2 en Bonus 4. Pas het tempo aan je voorkennis en beschikbare tijd aan; leerresultaten of certificering worden niet gegarandeerd.

01 Zo gebruik je dit studieplan

02 Fase 1 — Fundamenteën | weken 1–4

03 Fase 2 — Verdediging & Netwerken | weken 5–8

04 Fase 3 — SOC, Pentesting & Cloud | weken 9–12

05 Voortgang en terugblik

Zo gebruik je dit studieplan

Dit traject ordent alle 150 mindmaps in drie fasen. Het is bedoeld voor beginners die begrippen stap voor stap willen opbouwen en oefenen met defensieve, geautoriseerde scenario's. Reken op circa 12 weken bij ongeveer 5–7 uur per week; spreid een week gerust over meer tijd. Dit is een richtlijn, geen garantie op leerresultaat of certificering. Houd bij wat je bestudeerde, wat je kunt uitleggen en wat herhaling vraagt.



Wat laat je zelfcontrole aan het einde van een week zien?



Ik kan de belangrijkste begrippen uitleggen en een voorbeeld geven.

Ga door naar de volgende week en noteer een verband met eerdere stof.



Ik herken de termen, maar kan verband of voorbeeld niet uitleggen.

Herhaal de betreffende mindmaps en maak de casus opnieuw met eigen aantekeningen.



Ik weet niet zeker hoe ik veilig of bevoegd kan oefenen.

Beperk je tot de conceptuele uitleg; oefen praktisch pas in een lab of na toestemming.

1

Oriënteer

Lees het weekdoel en bekijk de bijbehorende mindmaps.

2

Bestudeer

Werk de onderwerpen in volgorde door en noteer kernbegrippen.

3

Oefen

Maak de gekoppelde casus uit Bonus 2 in een veilige, toegestane omgeving.

4

Controleer

Gebruik relevante punten uit Bonus 4 en leg zonder spiekbrieven uit wat je hebt geleerd.

5

Herhaal of vervolg

Herhaal onduidelijke onderdelen; ga verder wanneer je de zelfcontrole kunt beantwoorden.

- Lees de mindmaps in de aangegeven volgorde; noteer onbekende termen en verbind nieuwe onderwerpen met eerder geleerde begrippen.
- Reserveer per week ongeveer 3–4 uur voor mindmaps, 1–2 uur voor oefening en 30–60 minuten voor herhaling en zelfcontrole.
- Gebruik Bonus 2 voor de genoemde casussen en Bonus 4 voor toepasselijke beveiligingscontroles. Controleer alleen systemen en accounts waarvoor je verantwoordelijk bent.
- Ga verder wanneer je de kern in eigen woorden kunt uitleggen; herhaal of vertraag waar nodig.

Veilig oefenen

Voer technische tests alleen uit in een eigen oefenlab of met expliciete toestemming en afgesproken reikwijdte. Gebruik voor aanvallen uitsluitend veilige simulaties; richt geen scans of tests op systemen van derden.

Startdatum

Uren die ik deze week kan besteden

Mijn leerdoel voor dit traject

Fase 1 — Fundamenten | weken 1–4

Bouw eerst een begrippenkader op: wat moet worden beschermd, hoe risico's ontstaan, hoe netwerken en cryptografie werken en hoe veelvoorkomende dreigingen worden herkend. Deze volgorde helpt later verdedigingsmaatregelen te begrijpen. Besteed ongeveer 5–7 uur per week; verdeel nieuwe onderwerpen zo nodig over meer studiemomenten.

Kun je de basisbegrippen toepassen op een concreet, niet-operationeel scenario?

→ **Ja, ik kan risico, dreiging en de relevante beveiligingseigenschap uitleggen.**

Start fase 2 en verbind de begrippen met netwerk- en verdedigingsmaatregelen.

→ **Gedeeltelijk; ik verwar bijvoorbeeld hash, versleuteling of authenticatie.**

Herhaal mindmaps 003 en 013–017 en maak de relevante Bonus 2-oefeningen opnieuw.

→ **Nee, de onderliggende begrippen zijn nog onduidelijk.**

Neem extra studietijd voor de betreffende mindmaps; houd niet krampachtig vast aan de weekindeling.

1

Leg de basis vast

Vat per mindmap het centrale begrip en twee belangrijke verbanden samen.

2

Pas toe op een casus

Koppel de begrippen aan Bonus 2, oefening 1; bespreek welk deel van de CIA-triade geraakt kan zijn.

3

Herhaal gericht

Gebruik de zelfcontrole en bekijk relevante mindmaps opnieuw voordat je fase 2 start.

- Week 1 — Beveiligingsbasis en governance: mindmaps 001–008. Leer de CIA-triade, risico- en dreigingsmodellering, identiteiten, beleid, menselijke factoren en fysieke beveiliging.
- Week 2 — Netwerk- en cryptografiebasis: mindmaps 009–017. Volg OSI en TCP/IP, DNS, DHCP/ARP, symmetrische en asymmetrische cryptografie, hashes, handtekeningen en TLS.
- Week 3 — Dreigingen en applicatiebasis: mindmaps 018–030. Bestudeer malware, ransomware, beschikbaarheidsaanvallen, phishing, webkwetsbaarheden, wachtwoordaanvallen, patchbeheer en ATT&CK als ordeningskader.
- Week 4 — Consolidatie: herhaal mindmaps 001–030. Maak Bonus 2, oefening 1 (CIA-triade) en oefening 16 (symmetrische versus asymmetrische versleuteling). Gebruik Bonus 4 voor wachtwoorden en authenticatie, software-updates en phishingherkenning.

Zelfcontrole fase 1

Kun je vertrouwelijkheid, integriteit en beschikbaarheid onderscheiden en bij een eenvoudig scenario benoemen welke eigenschap wordt bedreigd? Kun je uitleggen waarom een hash niet hetzelfde is als versleuteling en welke aanwijzingen een phishingbericht verdacht maken? Herhaal de betreffende mindmaps als dit nog niet helder is.

Fase 1 — onderwerpen die ik zelfstandig kan uitleggen

Fase 1 — begrippen om te herhalen



Fase 2 — Verdediging & Netwerken | weken 5–8

Verbind netwerkkennis met beheersmaatregelen voor infrastructuur, identiteiten, endpoints en applicaties. Segmentatie, logging, toegangsbeheer, hardening en veilige ontwikkeling vullen elkaar aan. Reserveer wekelijks circa 5–7 uur, inclusief herhaling en casusoefening.



Welke vervolgstap past bij je begrip en bevoegdheid?



Ik kan risico's koppelen aan netwerk-, identiteits- of endpointmaatregelen.

Ga door naar fase 3 en benoem de onderliggende controles.



Ik kan een maatregel noemen, maar niet uitleggen wat die afdekt.

Herhaal de relevante mindmaps, vergelijk met een tweede maatregel en noteer beperkingen.



Ik heb geen toestemming voor praktische tests op de beoogde omgeving.

Test daar niet; kies een afgeschermd lab, simulatie of conceptuele casus.

1

Breng de omgeving conceptueel in kaart

Teken systemen, identiteiten en gegevensstromen op hoofdlijnen in een fictief scenario of bevoegde omgeving.

2

Koppel risico aan controle

Beschrijf het risico en hoe een controle, zoals segmentatie, MFA of logging, dit kan beperken of zichtbaar maken.

3

Controleer het begrip

Werk Bonus 2, oefening 5 en 22 uit; benoem welke toestemming nodig is voor uitvoering in de praktijk.

- Week 5 — Netwerkverdediging: mindmaps 031–042. Bestudeer segmentatie, firewalls, IDS/IPS, VPN, DMZ, WAF, wifi, NAC, DLP, e-mailbeveiliging en EDR/XDR.
- Week 6 — Identiteit en systemen: mindmaps 043–055. Volg IAM, toegangsmodellen, MFA, PAM, SSO, Zero Trust, Active Directory, Windows- en Linux-hardening en veilige SSH.
- Week 7 — Applicatiebeveiliging en testmethoden: mindmaps 056–065. Leer OWASP-risico's, SSRF, headers, SSDLC, softwareketens, ethisch testen, kwetsbaarheidsbeheer, scannen en webtesten op hoofdlijnen.
- Week 8 — Verdieping en consolidatie: mindmaps 087–094 en 100–101. Verbind draadloze risico's, API's, tokens, sleutelbeheer, dreigingsmodellering, tegenmaatregelen en codeanalyse met de stof uit weken 5–7. Dit is de eerste bestudering van deze mindmaps; herhaal ze in week 12.
- Oefen en controleer: maak Bonus 2, oefening 5 (firewall-regelanalyse) én oefening 22 (RBAC-ontwerp). Gebruik Bonus 4 voor software-updates, wifi en netwerk, en apparaatbeveiliging.

Praktijk binnen de reikwijdte

Scannen, testen en configureren zijn alleen passend op systemen waarvoor je toestemming hebt. Voor beginners volstaan een oefenlab, voorgeschreven simulatie of analyse van een voorbeeldconfiguratie; test geen openbare of andermans systemen.

Fase 2 — controlemaatregelen die ik kan toelichten

Fase 2 — veilige oefenomgeving of simulatie

🎯 Fase 3 — SOC, Pentesting & Cloud | weken 9–12

Rond het traject af met detectie, incidentrespons, cloudb beveiliging, forensische basisbegrippen en integratie. Pentestonderwerpen worden benaderd vanuit methodiek, toestemming, reikwijdte en verantwoorde rapportage; dit plan geeft geen opdracht om echte systemen aan te vallen. Reken op ongeveer 5–7 uur per week, met ruimte voor extra studietijd.

🔗 Wat is de beste vervolgstap na de eindcontrole?

➔ **Ik kan kernconcepten uitleggen en preventie, detectie, respons en herstel verbinden.**

Gebruik de mindmaps als naslag en kies een volgend leerdoel voor verdere verdieping.

➔ **Ik begrijp de basis, maar cloud, forensica of SOC-processen blijven lastig.**

Herhaal de betreffende mindmaps en Bonus 2-casussen; plan extra tijd in plaats van door te gaan uit tijdsdruk.

➔ **Ik wil praktische pentestactiviteiten uitvoeren.**

Werk uitsluitend met expliciete toestemming, afgebakende reikwijdte en passende oefenomgeving; begin niet op systemen van derden.

1

Volg signalen

Beschrijf hoe logs, meldingen en context samen een verdedigende onderzoeksvraag kunnen vormen.

2

Bepaal respons en bewijs

Leg de eerste responsdoelen uit en waarom zorgvuldige vastlegging en beperkte toegang belangrijk zijn.

3

Pas cloudverantwoordelijkheid toe

Koppel een fictieve dienst aan gedeelde verantwoordelijkheden en benoem welke configuraties de klant beheert.

4

Verbind de fasen

Maak een synthese van risico, preventie, detectie, respons en herstel voor één fictief scenario.

- Week 9 — SOC en incidentrespons: mindmaps 066–073 en 095–098. Bestudeer SOC-rollen, SIEM, SOAR, responsfasen, bewijsketen, geheugen- en netwerkforensica, dreigingsinformatie en threat hunting.
- Week 10 — Cloud en weerbaarheid: mindmaps 074–086 en 099. Leer gedeelde verantwoordelijkheid, cloud-IAM, opslag, containers, Kubernetes, privacy, gegevensclassificatie, continuïteit, back-ups, IoT, OT, mobiele beveiliging en cloudforensica.
- Week 11 — Verdieping en architectuur: mindmaps 102–130. Groepeer onderwerpen rond playbooks, beveiligingsarchitectuur, web- en identiteitsrisico's, regelgeving, AI, cloud en softwareketens.
- Week 12 — Geavanceerde onderwerpen en synthese: mindmaps 131–150; herhaal daarnaast 087–094 en 100–101 uit week 8. Hiermee zijn de mindmaps 001–150 elk op een samenhangende plek ingedeeld: 001–030 in fase 1, 031–065 en 087–094 plus 100–101 in fase 2, en 066–086, 095–099 en 102–150 in fase 3. Maak Bonus 2, oefening 42 (incidentrespons en triage) en oefening 47 (gedeelde verantwoordelijkheid in de cloud). Gebruik Bonus 4 als eindcontrole van toepasselijke beveiligingspraktijken.
- Let op de omvang: mindmaps 102–150 bevatten veel specialistische thema's. Verdeel weken 11 en 12 gerust over extra weken; de weeknummers zijn een route, geen deadline.

Zelfcontrole fase 3

Kun je een melding benaderen als verdedigende triagevraag, aangeven welke gegevens zorgvuldig moeten worden bewaard en uitleggen wie verantwoordelijk is voor welke cloudlaag in een dienstmodel? Kun je een pentest onderscheiden van een kwetsbaarheidsscan en uitleggen waarom toestemming en afgesproken reikwijdte vooraf nodig zijn?

Fase 3 — onderwerpen die ik verder wil bestuderen

Mijn synthese: risico, controle, detectie en herstel

Datum van mijn terugblik

☒ Voortgang en terugblik

Gebruik deze registratie om je eigen voortgang te volgen. Een vinkje betekent dat je de stof hebt bestudeerd en zelf kunt toelichten; het is geen externe beoordeling. Pas volgorde en duur aan je voorkennis, beschikbare tijd en leerbehoefte aan. Bonus 2-casussen en Bonus 4-controles zijn oefenen en controlepunten, geen examens.

- ☐ Fase 1 bestudeerd en zelf gecontroleerd — datum: _____
- ☐ Fase 2 bestudeerd en zelf gecontroleerd — datum: _____
- ☐ Fase 3 bestudeerd en zelf gecontroleerd — datum: _____
- ☐ Bonus 2-casussen bij de gekozen fasen gemaakt — nummers: _____
- ☐ Relevante Bonus 4-controles doorgenomen — categorieën: _____
- ☐ Onderwerpen voor herhaling of verdere studie genoteerd.

Flexibele planning

Een leertraject hoeft niet in twaalf kalenderweken afgerond te zijn. Verleng weken wanneer nieuwe termen, oefencasussen of beschikbare studietijd daarom vragen; begrip en veilig oefenen zijn belangrijker dan tempo.

Wat kan ik nu beter uitleggen dan bij de start?

Mijn volgende concrete leerdoel