DER LERNFAHRPLAN

Cybersecurity-Studienplan: 150 Mindmaps und 50 Praxisübungen

Vier Phasen, 20 Wochen und ein klarer Weg durch 150 Mindmaps und 50 Übungen

> Ein vollständiger, flexibel nutzbarer Studienplan für Einsteigerinnen und Einsteiger. Er führt von Computer- und Netzwerkgrundlagen über defensive und offensive Sicherheitskonzepte bis zu Cloud, Kryptographie und der Reaktion auf Sicherheitsvorfälle. Wochenzuordnungen, Meilensteine, sichere Praxisleitlinien und Selbstkontrollen unterstützen eine realistische Einschätzung des Lernstands.

01 Cover

02 Start hier: dein Lernrhythmus

03 Phase 1 · Grundlagen und Netzwerksicherheit

04 Selbstkontrolle · Phase 1

05 Phase 2 · Defensive und offensive Kernkonzepte

06 Selbstkontrolle · Phase 2

07 Phase 3 · Cloud, Kryptographie und Spezialisierung

08 Selbstkontrolle · Phase 3

09 Phase 4 · Fortgeschrittene Szenarien und Reaktion auf Sicherheitsvorfälle

10 Selbstkontrolle · Phase 4 und Abschluss

11 Zuordnungsmatrix · Überblick aller Einheiten

12 Lernprotokoll und Wochenabschluss

01

Cover

CYBERSECURITY-STUDIENPLAN
Ein strukturierter Lernpfad durch 150 Mindmaps und 50 Praxisübungen

Von den Grundlagen bis zur Reaktion auf Sicherheitsvorfälle
Vier Phasen · 20 Wochen · im eigenen Tempo

Wie solltest du eine Übung bearbeiten?

Die Aufgabe nennt ein eigenes Labor oder eine ausdrücklich autorisierte Umgebung.

Arbeite nur innerhalb dieses Umfangs und dokumentiere deine Beobachtungen.

Umfang oder Erlaubnis sind unklar.

Teste keine fremden Systeme. Kläre die Freigabe oder nutze eine lokale, isolierte Lernumgebung.

1. **Mindmap ansehen**

   Lies die Übersicht einmal vollständig und markiere unbekannte Begriffe.

2. **Thema erklären**

   Halte die Hauptidee in eigenen Worten fest und verbinde sie mit einem Beispiel.

3. **Übung durchführen**

   Bearbeite die zugeordnete Praxisübung in einer eigenen oder ausdrücklich autorisierten Lernumgebung.

4. **Wissen prüfen**

   Nutze die Checkliste und notiere, was du wiederholen möchtest.

- Für Einsteigerinnen und Einsteiger ohne Vorkenntnisse
- Gestaltung: dunkles Marineblau mit Cyan-Akzenten und klarer, gut lesbarer Typografie.

> **So nutzt du den Plan**
>
> Arbeite die Wochen der Reihe nach durch. Passe deine Lerntage an den Alltag an und nutze die Selbstkontrolle, bevor du zur nächsten Phase wechselst.

Startdatum

Mein wöchentliches Lernziel

02

Start hier: dein Lernrhythmus

Du brauchst keine Vorkenntnisse in Python oder Netzwerken. Beginne mit den ersten Wochen und lerne Begriffe schrittweise. Eine Mindmap gibt einen Überblick, ersetzt aber nicht das eigene Erklären und Üben. Plane pro Woche zwei bis vier Lerneinheiten: zum Lesen, Wiedergeben, Üben oder Wiederholen.

Zur Zuordnung dienen die fortlaufenden Nummern M001–M150 für Mindmaps und U01–U50 für Übungen. Die Nummern in den Wochenplänen bezeichnen diese Einheiten. Bearbeite sie in der angegebenen Reihenfolge. Falls das Material keine Nummern trägt, ordne es nach der Themenfolge zu und verwende die Matrix als Orientierung.

Was tun, wenn eine Übung nicht gelingt?

Ein Begriff oder eine Voraussetzung ist unklar.

Kehre zur passenden Mindmap zurück, notiere den Begriff und beginne die Übung anschließend erneut.

Die Aufgabe scheint außerhalb des erlaubten Labors zu liegen.

Stoppe sofort und teste keine fremden Systeme. Kläre den Umfang oder wähle eine sichere lokale Alternative.

Die Schritte sind klar, aber das Ergebnis weicht ab.

Protokolliere Eingaben, Annahmen und Beobachtungen und vergleiche die Schritte nacheinander.

1. **Woche auswählen**

   Öffne die zugewiesenen Mindmaps und Übungen in Nummernfolge.

2. **Überblick gewinnen**

   Lies die Mindmap und notiere zentrale Begriffe sowie offene Fragen.

3. **Aktiv abrufen**

   Schließe die Übersicht und erkläre die Zusammenhänge aus dem Gedächtnis.

4. **Üben und festhalten**

   Bearbeite die Übung und halte Ergebnis und Lernfrage im Lernprotokoll fest.

- Plane pro Lerneinheit etwa 30–60 Minuten; passe die Dauer deinem Alltag an.
- Führe ein Glossar: Begriff, Erklärung in eigenen Worten und ein Beispiel.
- Bei Unsicherheit lies die Mindmap erneut, skizziere die Zusammenhänge und setze danach die Übung fort.
- Übungen zu Angriffstechniken ausschließlich in ausdrücklich autorisierten Lernumgebungen durchführen.

> **Einsteigerregel**
>
> Wenn ein Thema eine Voraussetzung hat, die dir noch fehlt, pausiere und wiederhole die frühere Mindmap. Das gehört zum Lernprozess.

Meine erste offene Frage

Ein Begriff, den ich heute erklären kann

03

Phase 1 · Grundlagen und Netzwerksicherheit

Wochen 1–5. Ziel: Computer, Betriebssysteme, grundlegende Netzwerkkommunikation und zentrale Sicherheitsbegriffe verstehen. Beginne mit M001. Python wird als Werkzeug eingeführt, nicht als Voraussetzung. Der Meilenstein: Du kannst den Ablauf einer einfachen Netzwerkverbindung verständlich beschreiben und die zugehörigen Übungen sicher bearbeiten.

Bist du bereit für Phase 2?

Du kannst die Kernbegriffe in eigenen Worten erklären und U01–U10 sicher bearbeiten.

Gehe weiter zu Phase 2.

Einzelne Konzepte sind noch unsicher.

Wiederhole die passenden Mindmaps und Übungen und notiere eine konkrete Frage pro Thema.

1. **Grundbegriffe aufbauen**

   M001–M016 und U01–U04: Rechner, Sicherheit und Netzwerkadressierung.

2. **Kommunikation verstehen**

   M017–M024 und U05–U06: Protokolle, Netzwerkgeräte und sichere Verbindungen.

3. **Systeme bedienen**

   M025–M032 und U07–U08: Betriebssysteme, Rechte, Protokolle und Lernumgebung.

4. **Python anwenden**

   M033–M040 und U09–U10: grundlegende Programmierbausteine und Eingabeprüfung.

- Woche 1 — M001–M008: Computer, Betriebssysteme, Dateien, Prozesse, Kommandozeile, IT-Sicherheitsgrundlagen, Vertraulichkeit–Integrität–Verfügbarkeit, Bedrohung und Risiko. U01–U02: Sicherheitsinventar eines eigenen Übungsgeräts; Bedrohungsübersicht für ein erfundenes Szenario.
- Woche 2 — M009–M016: Netzwerke, LAN/WAN, IP-Adressen, Subnetze als Konzept, MAC-Adressen, DNS, DHCP und Ports. U03–U04: Netzwerkbegriffe an einem eigenen oder simulierten Beispiel zuordnen; eine DNS-Auflösung nachvollziehen, ohne fremde Systeme zu scannen.
- Woche 3 — M017–M024: TCP und UDP, Verbindungsaufbau, HTTP/HTTPS, TLS-Grundidee, Router und Switches, Firewall, VPN und WLAN-Sicherheit. U05–U06: Verbindungsablauf skizzieren; die Konfiguration eines eigenen WLANs anhand einer Checkliste prüfen.
- Woche 4 — M025–M032: Linux- und Windows-Grundlagen, Benutzer und Rechte, Dateien und Berechtigungen, Protokolle, Updates, virtuelle Maschinen und sichere Lernumgebung. U07–U08: Verzeichnis- und Rechteübersicht in einer Testumgebung erstellen; ein isoliertes Labor planen.
- Woche 5 — M033–M040: Python-Einstieg, Variablen und Datentypen, Bedingungen, Schleifen, Funktionen, Module, Ein- und Ausgabe sowie sichere Skriptgewohnheiten. U09–U10: kleines Skript mit Eingabe und verständlicher Ausgabe schreiben; Eingaben prüfen und einen harmlosen Fehlerfall behandeln.

> **Meilenstein Phase 1**
>
> Erkläre ohne Vorlage den Unterschied zwischen IP-Adresse und Port, den Zweck von DNS sowie den Unterschied zwischen TCP und UDP. Beschreibe auch, warum Updates und begrenzte Rechte wichtig sind.

Mein Beispiel für Vertraulichkeit, Integrität und Verfügbarkeit

Was ich über einen Netzwerkverbindungsablauf erklären kann

04

Selbstkontrolle · Phase 1

Kreuze einen Punkt erst an, wenn du ihn ohne bloßes Ablesen erklären oder zeigen kannst. Ein leeres Kästchen hilft dir, gezielt zu wiederholen.

Wie gehst du mit deiner Selbstkontrolle weiter?

Die Kernpunkte sind verständlich und praktisch nachvollziehbar.

Beginne die nächste Phase und nutze die Checkliste später erneut.

Mehrere Grundlagen sind noch unsicher.

Wiederhole die entsprechenden Wochen, bevor du neue Themen hinzunimmst.

1. **Punkte prüfen**

   Gehe die Aussagen durch und erkläre jede angekreuzte Fähigkeit mit einem Beispiel.

2. **Lücken auswählen**

   Ordne leere Kästchen den passenden Mindmaps oder Übungen zu.

3. **Wiederholen**

   Bearbeite die ausgewählten Inhalte erneut und prüfe dein Verständnis ohne Vorlage.

- [ ] Ich erkläre Vertraulichkeit, Integrität und Verfügbarkeit mit je einem passenden Beispiel.
- [ ] Ich unterscheide IP-Adresse, MAC-Adresse und Port auf grundlegender Ebene.
- [ ] Ich beschreibe, wozu DNS und DHCP dienen.
- [ ] Ich erkläre den grundlegenden Unterschied zwischen TCP und UDP.
- [ ] Ich erkläre, wozu Protokolle, Updates und Benutzerrechte beitragen.
- [ ] Ich kann in Python eine einfache Bedingung, Schleife und Funktion schreiben.
- [ ] Ich habe U01–U10 nur in einer eigenen oder ausdrücklich autorisierten Umgebung bearbeitet.
- [ ] Ich habe offene Fragen im Lernprotokoll festgehalten und geklärt oder für später markiert.

> **Entscheidung statt Punktzahl**
>
> Es gibt keine Mindestpunktzahl. Wenn Grundlagen fehlen, wiederhole die betreffenden Wochen. Wenn die Begriffe sitzen, gehe weiter und greife bei Bedarf zurück.

Themen, die ich wiederhole

Mein nächster konkreter Schritt

05

Phase 2 · Defensive und offensive Kernkonzepte

Wochen 6–10. Ziel: Schutzmaßnahmen, Schwachstellen und Angriffsabläufe verantwortungsvoll einordnen. Offensive Konzepte dienen hier dem Erkennen und Absichern. Praktische Tests beschränken sich auf bereitgestellte Trainingsziele oder Systeme mit ausdrücklicher Erlaubnis.

Ist eine praktische Testaufgabe für dich freigegeben?

Die Aufgabe nennt ein Trainingsziel oder einen ausdrücklich genehmigten Umfang.

Arbeite innerhalb der Freigabe und dokumentiere Vorgehen und Beobachtungen.

Ziel oder Erlaubnis sind nicht eindeutig.

Führe keinen Test aus; nutze Theorie, Simulation oder ein eigenes isoliertes Labor.

1. **Schutzmodell ansehen**

   M041–M048 und U11–U12: Risiken, Identität und menschliche Angriffspunkte.

2. **Anwendungen verstehen**

   M049–M056 und U13–U14: Webmechanismen und sichere Eingabeverarbeitung.

3. **Erkennen und absichern**

   M057–M064 und U15–U16: Konfiguration, Überwachung und Protokolle.

4. **Kryptographie einordnen**

   M065–M072 und U17–U18: Funktionen, Grenzen und Schlüsselverwaltung.

5. **Testen verantworten**

   M073–M080 und U19–U20: Umfang, Befund, Bericht und Behebung.

- Woche 6 — M041–M048: Angriffsflächen, Schwachstellen und Bedrohungsmodelle, Authentifizierung, Autorisierung, Mehr-Faktor-Authentifizierung, Passwortspeicherung, Phishing-Erkennung und Social Engineering. U11–U12: Bedrohungsmodell einer fiktiven Anwendung; Beispielnachrichten auf Phishing-Warnzeichen untersuchen.
- Woche 7 — M049–M056: Malware-Kategorien, sichere Analysegrundsätze, Web-Grundlagen, Sitzungen und Cookies, Eingabevalidierung, Injection und Cross-Site Scripting als Schwachstellenklassen, sichere Webentwicklung. U13–U14: Validierungsregeln für ein fiktives Formular; eine absichtlich verwundbare lokale Lernanwendung nach bereitgestellter Anleitung untersuchen.
- Woche 8 — M057–M064: Schwachstellenmanagement, sichere Konfiguration, Endpunktschutz, Netzwerksegmentierung, IDS/IPS-Grundidee, Protokollierung, Alarmierung und SIEM-Grundlagen. U15–U16: Schutzmaßnahmen für ein fiktives kleines Netz entwerfen; Beispieldaten in Protokollen nach einem vorgegebenen Muster untersuchen.
- Woche 9 — M065–M072: Kryptographie, Hashfunktionen, symmetrische und asymmetrische Verschlüsselung, digitale Signaturen, Zertifikate, Schlüsselverwaltung, sichere Kommunikation sowie Sicherung und Wiederherstellung. U17–U18: Hash, Verschlüsselung und Signatur anhand eines Falls unterscheiden; Wiederherstellungsplan für erfundene Daten erstellen.
- Woche 10 — M073–M080: Ablauf eines Penetrationstests, Umfang und Erlaubnis, passive Informationssammlung, sichere Testplanung, Schwachstellenbewertung, Nachweisführung, Berichterstattung, Behebung und erneute Prüfung. U19–U20: erlaubten Umfang für ein fiktives Labor festlegen; Beispielbefund mit Auswirkung, Nachweis und Abhilfe formulieren.

> **Sicherheitsgrenze**
>
> Eine Lernübung ist keine Erlaubnis, Systeme Dritter zu testen. Ohne Freigabe beschränkst du dich auf Theorie, Simulation oder ein eigenes isoliertes Labor.

Beispiel für eine Schwachstelle und passende Abhilfe

Was in einem klaren Testumfang stehen muss

06

Selbstkontrolle · Phase 2

Nutze die Punkte als Kompetenznachweis: Erkläre, skizziere oder zeige ein Ergebnis aus deiner autorisierten Lernumgebung.

Was zeigt deine Selbstkontrolle?

Du kannst die Kernideen erklären und deine Übungsergebnisse einordnen.

Beginne Phase 3.

Umfang, Abhilfe oder Grundbegriffe bleiben unklar.

Wiederhole die passenden Einheiten und kläre zuerst den sicheren Übungsumfang.

1. **Fähigkeiten prüfen**

   Erkläre jede angekreuzte Aussage mit einem Beispiel oder Ergebnis.

2. **Lernlücken festhalten**

   Notiere die Mindmap oder Übung, die du zur Wiederholung brauchst.

3. **Nächsten Schritt wählen**

   Gehe weiter, wenn die Kernideen verständlich sind; andernfalls wiederhole gezielt.

- [ ] Ich unterscheide Authentifizierung und Autorisierung.
- [ ] Ich skizziere ein einfaches Bedrohungsmodell mit schützenswertem Gut, Bedrohung und Maßnahme.
- [ ] Ich erkenne Warnsignale in einer Phishing-Nachricht, ohne enthaltene Links zu öffnen.
- [ ] Ich erkläre, warum Eingabevalidierung und sichere Sitzungsverwaltung wichtig sind.
- [ ] Ich unterscheide Hashfunktion, Verschlüsselung und digitale Signatur konzeptionell.
- [ ] Ich beschreibe, wie Protokolle und Alarme bei der Erkennung helfen und warum Kontext wichtig ist.
- [ ] Ich benenne Umfang, Erlaubnis und Grenzen einer Sicherheitsübung.
- [ ] Ich habe U11–U20 in einer freigegebenen Lernumgebung bearbeitet oder ihre Lernziele theoretisch nachvollzogen.

> **Meilenstein Phase 2**
>
> Du kannst einen einfachen Sicherheitsbefund verständlich formulieren: Was wurde beobachtet, welches Risiko entsteht, welche Abhilfe ist angemessen und wie lässt sie sich erneut prüfen?

Ein Befund, den ich verständlich formulieren kann

Ein Konzept, das ich noch übe

07

Phase 3 · Cloud, Kryptographie und Spezialisierung

Wochen 11–15. Ziel: Sicherheitsprinzipien auf Cloud-Umgebungen und ausgewählte Spezialgebiete übertragen. Konzentriere dich auf Zusammenhänge und Grenzen statt auf Produktnamen. Für Cloud-Übungen verwendest du ein eigenes Konto innerhalb des erlaubten Umfangs oder bereitgestellte Simulationen.

Wie führst du eine Cloud-Übung sicher durch?

Du hast ein eigenes Konto und der erlaubte Umfang ist klar.

Arbeite nur innerhalb dieses Umfangs und dokumentiere die verwendeten Einstellungen.

Die Aufgabe bietet eine Simulation oder ein bereitgestelltes Szenario.

Nutze die Simulation und halte Annahmen sowie Ergebnisse fest.

Konto, Umfang oder Freigabe sind unklar.

Verändere keine Cloud-Ressourcen; bearbeite das Szenario theoretisch oder kläre den Umfang.

1. **Cloud-Grundlagen**

   M081–M088 und U21–U22: Zuständigkeiten, Identitäten und sichere Konfiguration.

2. **Bereitstellung absichern**

   M089–M096 und U23–U24: Container, Automatisierung und Lieferkette.

3. **Kryptographie vertiefen**

   M097–M104 und U25–U26: Zertifikate, Daten und Schlüssel.

4. **Software schützen**

   M105–M112 und U27–U28: Entwicklung, Abhängigkeiten und APIs.

5. **Spezialisierung erkunden**

   M113–M120 und U29–U30: vernetzte Geräte, Risiken und Governance.

- Woche 11 — M081–M088: Cloud-Grundmodelle, geteilte Verantwortung, Identitäts- und Zugriffsverwaltung, Rollen und Richtlinien, Cloud-Netzwerke, Speicherfreigaben, Schlüssel und Geheimnisse sowie Cloud-Protokollierung. U21–U22: Verantwortlichkeiten in einem fiktiven Cloud-Szenario zuordnen; Rollen mit den minimal erforderlichen Rechten entwerfen.
- Woche 12 — M089–M096: Container, Images und Registries, Containerisolation, Orchestrierung als Konzept, Konfigurationsmanagement, Infrastruktur als Code, sichere Bereitstellung und Lieferkettenrisiken. U23–U24: Risiken eines fiktiven Container-Deployments markieren; Prüfpunkte für eine sichere Bereitstellung erstellen.
- Woche 13 — M097–M104: Public-Key-Infrastruktur, Zertifikatsprüfung, Transportverschlüsselung, Schlüsselrotation, Geheimnisverwaltung, Datenschutzgrundlagen, Datenklassifizierung, sichere Löschung und Aufbewahrung. U25–U26: einen vereinfachten Zertifikatsprüfpfad erklären; Daten nach Schutzbedarf klassifizieren und passende Behandlung ableiten.
- Woche 14 — M105–M112: sichere Softwareentwicklung, Codeprüfung, Abhängigkeiten, Tests, CI/CD-Sicherheit, API-Sicherheit, mobile Sicherheit und sichere Architektur. U27–U28: Prüfliste für eine Codeänderung erstellen; Sicherheitsanforderungen für eine fiktive API formulieren.
- Woche 15 — M113–M120: IoT-Sicherheit, drahtlose Netze, OT-Grundlagen, Datenschutztechnik, Bedrohungsanalyse, Risikobewertung, Sicherheitsrichtlinien, Governance und Compliance als Konzepte. U29–U30: Angriffsfläche eines fiktiven vernetzten Geräts beschreiben; Risiken priorisieren und begründen.

> **Cloud-Merksatz**
>
> Verantwortlichkeiten hängen vom Dienstmodell und der konkreten Konfiguration ab. Prüfe für jedes Szenario, wer Identitäten, Daten, Anwendungen und zugrunde liegende Infrastruktur verwaltet.

Cloud-Aufgabe und zugehörige Verantwortung

Ein Risiko aus einer Spezialisierung und seine Begründung

08

Selbstkontrolle · Phase 3

Prüfe, ob du Prinzipien auf neue Beispiele übertragen kannst. Nenne jeweils eine Begründung, nicht nur ein Schlagwort.

Kannst du ein neues Szenario nachvollziehbar beurteilen?

Du kannst Schutzbedarf, Zuständigkeiten und eine Maßnahme begründen.

Gehe weiter zu Phase 4.

Du kannst die Schlagwörter nennen, aber nicht begründen.

Wiederhole die passenden Mindmaps und Fallübungen.

1. **Übertragung prüfen**

   Erkläre ein Prinzip anhand eines anderen Beispiels als in der Mindmap.

2. **Begründung ergänzen**

   Notiere, weshalb die gewählte Schutzmaßnahme zum Risiko passt.

3. **Lücke schließen**

   Wiederhole die passende Einheit, wenn du eine Annahme nicht begründen kannst.

- [ ] Ich erkläre geteilte Verantwortung an einem Cloud-Beispiel.
- [ ] Ich skizziere eine Rolle mit minimal erforderlichen Rechten für eine klar umrissene Aufgabe.
- [ ] Ich benenne Sicherheitsrisiken bei Containern oder automatisierten Bereitstellungen.
- [ ] Ich erkläre den Zweck von Zertifikaten und warum Schlüssel geschützt und verwaltet werden müssen.
- [ ] Ich leite für eine fiktive API mindestens zwei konkrete Sicherheitsanforderungen ab.
- [ ] Ich priorisiere ein Risiko und begründe meine Einschätzung nachvollziehbar.
- [ ] Ich habe U21–U30 bearbeitet und Cloud-Übungen auf Simulationen oder ausdrücklich erlaubte Ressourcen beschränkt.

> **Meilenstein Phase 3**
>
> Du kannst für ein einfaches Cloud- oder Softwarebeispiel den Schutzbedarf, zuständige Sicherheitsaufgaben und eine praktikable Schutzmaßnahme erläutern.

Ein Prinzip, das ich auf ein neues Szenario übertragen kann

Meine nächste Lernfrage

09

Phase 4 · Fortgeschrittene Szenarien und Reaktion auf Sicherheitsvorfälle

Wochen 16–20. Ziel: Sicherheitsereignisse strukturiert einordnen, Reaktionen planen und Wissen übergreifend anwenden. Die Fallübungen dienen der Analyse und Dokumentation; sie erfordern keine Interaktion mit realen Angreifern oder fremden Systemen.

Wie gehst du mit einem Szenario um, das unvollständige Informationen enthält?

Eine Beobachtung ist direkt im Szenario angegeben.

Dokumentiere sie als Beobachtung und verknüpfe sie mit der möglichen Auswirkung.

Eine Erklärung ist plausibel, aber nicht belegt.

Kennzeichne sie als Annahme und notiere, welche Information sie prüfen könnte.

Ein vorgesehener Schritt würde ein fremdes System betreffen.

Führe ihn nicht aus; bleibe bei der Analyse des bereitgestellten Szenarios.

1. **Signale einordnen**

   M121–M128 und U31–U32: Alarme prüfen, priorisieren und eskalieren.

2. **Reaktion planen**

   M129–M136 und U33–U34: Phasen, Zuständigkeiten und Kommunikation verbinden.

3. **Szenarien bewerten**

   M137–M144 und U35–U36: Auswirkungen, Resilienz und Wiederherstellung betrachten.

4. **Wissen integrieren**

   M145–M150 und U37–U50: Dokumentation, Referenzmodelle und Abschlussübungen.

- Woche 16 — M121–M128: Sicherheitsüberwachung, Ereignis und Vorfall, Alarmtriage, Ereigniskorrelation, Fehlalarme, Priorisierung, Grundsätze der Beweissicherung und Kommunikationswege. U31–U32: Beispielalarme nach Dringlichkeit sortieren und begründen; einen knappen Eskalationsvermerk verfassen.
- Woche 17 — M129–M136: Lebenszyklus der Reaktion auf Vorfälle, Vorbereitung, Identifizierung, Eindämmung, Beseitigung, Wiederherstellung, Nachbereitung und Notfallkommunikation. U33–U34: Reaktionsplan für ein fiktiv kompromittiertes Konto skizzieren; Maßnahmen und Zuständigkeiten zeitlich ordnen.
- Woche 18 — M137–M144: Ransomware-Szenarien, möglicher Datenabfluss, DDoS-Grundidee und Reaktion, Insider-Risiken, Lieferketten- und Cloud-Vorfälle, Krisenmanagement, Wiederanlauf und Resilienz. U35–U36: vorgegebenes Szenario mit Risiko- und Maßnahmenmatrix analysieren; Wiederherstellungsprioritäten für einen fiktiven Dienst festlegen.
- Woche 19 — M145–M150: forensische Grundprinzipien, Beweiskette als Konzept, Bedrohungsinformationen, MITRE ATT&CK als Referenzmodell, Zusammenarbeit von Red und Blue Team sowie Sicherheitsmetriken. U37–U38: Szenariobeobachtungen strukturiert dokumentieren; eine defensive Erkennungsmaßnahme einem beschriebenen Angriffsschritt zuordnen.
- Woche 20 — Wiederholung M001–M150 und U39–U50: zwölf Integrationsübungen zu Grundlagen, Netzwerken, Python, Abwehr, Web, Kryptographie, Cloud, Softwareentwicklung und Reaktion auf Sicherheitsvorfälle. Bearbeite sie in den vorgesehenen Lern- oder Simulationsumgebungen und kehre bei Bedarf zu passenden Mindmaps zurück.

> **Meilenstein Phase 4**
>
> Du kannst ein vorgegebenes Vorfallszenario anhand von Beobachtungen, Auswirkungen, Eindämmung, Wiederherstellung und Nachbereitung strukturieren und Annahmen als solche kennzeichnen.

Erste drei Schritte in meinem fiktiven Vorfallsplan

Welche Annahme im Szenario müsste ich zuerst prüfen?

10

Selbstkontrolle · Phase 4 und Abschluss

Diese Abschlusskontrolle prüft, ob du Zusammenhänge erklären und nächste Lernschritte bestimmen kannst. Sie ist keine externe Zertifizierung oder Prüfung.

Was ist dein nächster sinnvoller Schritt?

Du möchtest Grundlagen festigen.

Wähle eine markierte Mindmap und erkläre sie anschließend ohne Vorlage.

Du möchtest Praxis vertiefen.

Wähle eine passende Übung und prüfe zuerst, ob der Umfang ausdrücklich erlaubt ist.

Du möchtest ein Gebiet spezialisieren.

Lege ein konkretes Lernziel fest und bestimme die dazu passenden Mindmaps und Übungen.

1. **Lernstand einschätzen**

   Prüfe jede Aussage anhand eines Beispiels, einer Erklärung oder eines dokumentierten Ergebnisses.

2. **Wiederholungsbedarf notieren**

   Markiere Themen und Einheiten, die du erneut bearbeiten möchtest.

3. **Nächstes Ziel wählen**

   Plane für die kommenden Wochen eine konkrete Vertiefung oder Wiederholung.

- [ ] Ich unterscheide ein Sicherheitsereignis von einem bestätigten Vorfall im jeweiligen Kontext.
- [ ] Ich dokumentiere eine Alarmtriage mit Beobachtung, möglicher Auswirkung und nächstem Schritt.
- [ ] Ich ordne Eindämmung, Beseitigung, Wiederherstellung und Nachbereitung sinnvoll in einen Reaktionsablauf ein.
- [ ] Ich benenne, warum Kommunikation, Zuständigkeiten und nachvollziehbare Dokumentation wichtig sind.
- [ ] Ich unterscheide in einem Szenario Beobachtungen von Vermutungen.
- [ ] Ich habe M001–M150 systematisch bearbeitet und Themen zur Wiederholung markiert.
- [ ] Ich habe U01–U50 bearbeitet oder bei unklarem Umfang eine sichere theoretische Alternative genutzt.
- [ ] Ich habe einen persönlichen Plan für die nächsten vier Wochen erstellt: Vertiefung, Wiederholung oder ein neues Grundlagenprojekt.

> **Abschluss heißt Weiterlernen**
>
> Cybersecurity entwickelt sich fortlaufend. Nutze deinen Lernstand, um ein Themengebiet zu vertiefen, nicht als Behauptung vollständiger Fachbeherrschung.

Meine drei stärksten Themen

Themen für die nächste Wiederholungsrunde

Mein Lernziel für die kommenden vier Wochen

11

Zuordnungsmatrix · Überblick aller Einheiten

Die Matrix zeigt die vollständige Erstzuordnung der Mindmaps und Übungen. M001–M150 und U01–U50 werden jeweils einmal als erste Bearbeitung eingeplant. Woche 20 ergänzt eine Wiederholung aller Mindmaps; sie ersetzt nicht deren vorherige Erstbearbeitung. Die zwölf Abschlussübungen U39–U50 sind in Woche 20 integriert.

Wie nutzt du die Nummernzuordnung?

Die Einheiten sind im Material nummeriert.

Bearbeite die angegebenen Nummernbereiche der Reihe nach.

Die Nummern fehlen, die Themen sind aber erkennbar.

Ordne anhand der Themenfolge zu und halte deine Zuordnung im Lernprotokoll fest.

Thema oder Zuordnung ist nicht eindeutig.

Notiere die offene Zuordnung und arbeite zunächst mit einer eindeutig passenden Einheit weiter.

1. **Erstbearbeitung**

   Bearbeite M001–M150 und U01–U38 in den Wochen 1–19 gemäß der Phasenzuordnung.

2. **Integrationswoche**

   Sichte in Woche 20 die Mindmaps erneut und bearbeite U39–U50.

3. **Wiederholungsbedarf erfassen**

   Markiere Einheiten, bei denen du die Zusammenhänge noch nicht sicher erklären kannst.

- Phase 1 · Wochen 1–5: M001–M040; U01–U10.
- Phase 2 · Wochen 6–10: M041–M080; U11–U20.
- Phase 3 · Wochen 11–15: M081–M120; U21–U30.
- Phase 4 · Wochen 16–19: M121–M150; U31–U38.
- Woche 20 · Integration: erneute Sichtung M001–M150; Übungen U39–U50.
- Wochen 1–18 umfassen je acht Mindmaps und zwei Übungen. Woche 19 umfasst sechs Mindmaps und zwei Übungen. Woche 20 dient der Integration und Wiederholung.
- Kontrollrechnung: 18 × 8 + 6 = 150 Mindmaps; 19 × 2 = 38 Übungen in den Wochen 1–19; Woche 20 ergänzt zwölf Übungen, insgesamt 50.

> **Nummernzuordnung**
>
> Die Wochenreihenfolge bildet den Lernpfad; Themenbeschreibungen geben Orientierung. Falls Überschriften im Material abweichen, ordne nach der passenden Themenfolge und fortlaufenden Materialnummer.

Meine aktuelle Woche und die zugehörigen Einheiten

Einheiten, die ich zur Wiederholung markiert habe

12

Lernprotokoll und Wochenabschluss

Nutze pro Woche eine kurze Notiz, damit Fortschritte und offene Fragen sichtbar bleiben. Halte konkrete Beispiele fest: eine erklärte Verbindung in einer Mindmap, ein Übungsergebnis oder einen Begriff zum Nachschlagen. Greife offene Punkte zu Beginn der nächsten Lerneinheit wieder auf.

Was zeigt dein Wochenabschluss?

Du kannst die zentrale Erkenntnis verständlich wiedergeben.

Markiere die Woche als abgeschlossen und fahre im Lernpfad fort.

Eine offene Frage bleibt bestehen.

Notiere die passende Einheit und plane eine gezielte Wiederholung.

1. **Erledigte Einheiten markieren**

   Trage die bearbeiteten Nummern ein.

2. **Ergebnis notieren**

   Halte eine konkrete Beobachtung oder Erklärung fest.

3. **Lücke benennen**

   Formuliere eine offene Frage statt nur „unklar“ zu notieren.

4. **Wiederholung planen**

   Lege fest, wann und womit du die Lücke erneut bearbeitest.

- Datum und Woche eintragen.
- Mindmaps und Übungen der Woche abhaken.
- Eine Erkenntnis in eigenen Worten formulieren.
- Eine offene Frage und den nächsten Schritt festhalten.

Praktische Wiederholung

Wenn du ein Thema nach einigen Tagen nicht mehr erklären kannst, lies die Mindmap erneut und fasse sie anschließend ohne Vorlage zusammen.

Woche und Datum

Bearbeitete Mindmaps und Übungen

Eine Erkenntnis in eigenen Worten

Offene Frage und nächster Schritt