**LMS Questions for [DLBCSEEISC01\_D]**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Unit/**  **Question Number** | **Section** | **Question** | **Correct answer** | **Incorrect answer** | **Incorrect answer** | **Incorrect answer** |
| 1/1 | 1 | Wofür steht die Abkürzung CVE? | Common Vulnerabilities and Exposures | Common Vulnerabilities and Exploits | Common Vulnerabilities and Events | Certified Vulnerabilities and Events |
| 1/2 | 2 | Auf welcher Schicht werden Daten in Form von Nullen und Einsen verarbeitet? | Bitübertragungsschicht | Anwendungsschicht | Sitzungsschicht | Transportschicht |
| 1/3 | 3 | Welche der folgenden Aussagen trifft zu? | Statische Erkennungsverfahren können eingesetzt werden, wenn der zu analysierende Code nicht ausführbar ist. | Statische Erkennungs­verfahren spüren Schwachstellen durch Ausführung des Codes auf. | Statische Erkennungsverfahren sind extrem ressourcenintensiv. | Statische Erkennungs­verfahren sind komplex. |
| 1/4 | 4 | Wie lautet die korrekte Syntax des Nmap-Befehls zur Initiierung eines Schwachstellenscans? | nmap -Pn --script vuln <IP address> | nmap -Pn --script vuln <MAC address> | nmap -Pn --script vu <Port address> | nmap -Pn --script vu <MAC address> |
| 1/5 | 4 | Wie lautet der Name der grafischen Benutzeroberfläche für den Schwachstellenscanner Nmap? | Zenmap | Netmap | Nessmap | Zuimap |
| **Unit/**  **Question Number** | **Section** | **Question** | **Correct answer** | **Incorrect answer** | **Incorrect answer** | **Incorrect answer** |
| 2/1 | 1 | Welche der folgenden Aussagen über eine Sicherheitsreferenz­architektur (SRA) ist korrekt? | Eine SRA beleuchtet verschiedene Abstraktionsebenen und Funktionen. | Eine SRA ist keine Zusammenstellung logischer sicherheits­relevanter Repräsentationen bzw. Ansichten einer Systemarchitektur. | Risikomanagement­strategien finden in einer SRA keine Beachtung. | Eine SRA ist ein Standard mit Regeln zur Produktsicherheit. |
| 2/2 | 2 | Wie lautet die korrekte Formel zur Berechnung des Restrisikos? | Restrisiko = Inhärentes Risiko - Risikomindernder Effekt der Kontrollmaßnahmen | Restrisiko = Inhärentes Risiko \* Risikomindernder Effekt der Kontrollmaßnahmen | Restrisiko = Inhärentes Risiko + Risikomindernder Effekt der Kontrollmaßnahmen | Restrisiko = Inhärentes Risiko / Risikomindernder Effekt der Kontrollmaßnahmen |
| 2/3 | 3 | Welche der folgenden Antwortmöglichkeiten bezeichnet eine der Anforderungen an die Vertrauenswürdigkeit? | Konfigurations­management | Schutz der Benutzerdaten | Sicherheits­protokollierung | Kryptografische Unterstützung |
| 2/4 | 4 | Welcher Standard umfasst Vertrauenswürdigkeits­stufen (Evaluation Assurance Level, EAL)? | Common Criteria | Federal Information Processing Standards (FIPS) | Trusted Computer System Evaluation Criteria (TCSEC) | **Information Technology Security Evaluation Criteria** |
| 2/5 | 5 | Welche zwei Prozessschritte sollten Informationssysteme zur Prüfung ihrer Sicherheit durchlaufen? | Sicherheits­zertifizierung und Sicherheits­akkreditierung | Sicherheits­konfiguration und Sicherheits­garantie | Sicherheitsfreigabe und Sicherheitszuweisung | Sicherheits­bestätigung und Sicherheits­verknüpfung |
| **Unit/**  **Question Number** | **Section** | **Question** | **Correct answer** | **Incorrect answer** | **Incorrect answer** | **Incorrect answer** |
| 3/1 | 1 | Welche der folgenden Arten von Intrusion-Detection-Systemen zählt nicht zu den Kategorien eines auf Datenquellen basierenden Klassifizierungsschemas? | Verhaltensbasiertes IDS | Netzwerkbasiertes IDS | Hostbasiertes IDS | Hybrides IDS |
| 3/2 | 2 | Signaturbasierte Erkennungsmethoden ... | ... nutzen Regeln, um Hackerangriffe zu identifizieren. | ... sind zur Erkennung unbekannter Angriffe in der Lage. | ... erfassen Verhaltensdaten und erstellen daraus Profile. | ... eignen sich für ausgedehnte Netzwerke. |
| 3/3 | 2 | Welches der folgenden Tools ist kein Intrusion-Detection-System? | Wireshark | Zeek | Snort | Suricata |
| 3/4 | 3 | Das Akronym SIEM steht für ... | ... Security Information and Event Management. | ... Security Issues and Event Monitoring. | ... Security Identification and Event Monitoring. | ... Security Invigilation and Event Measuring. |
| 3/5 | 3 | Die aufbereiteten Daten zur Optimierung eines IDS durch maschinelles Lernen werden üblicherweise in Trainingsdaten und Testdaten aufgeteilt. In welchem Verhältnis geschieht dies? | 80:20 | 50:50 | 90:10 | 60:40 |
| **Unit/**  **Question Number** | **Section** | **Question** | **Correct answer** | **Incorrect answer** | **Incorrect answer** | **Incorrect answer** |
| 4/1 | 1 | Welches der folgenden Features einer ATP-Lösung überwacht und prüft die internen und externen Ressourcen auf Schwachstellen, die eine Gefahr für das Unternehmen bedeuten können? | Attack Surface Management | Dateianalyse | Rich Threat Intelligence | Kombinierte Erkennungs- und Abwehrfunktionen |
| 4/2 | 1 | Worin besteht der Hauptvorteil der statischen Analyse verdächtiger Dateien? | Schädliche Befehle, Strukturen usw. werden aufgedeckt, ohne dass eine Ausführung der Datei erforderlich ist. | Schädliche Befehle, Strukturen usw. werden durch Ausführung des Codes aufgedeckt. | Kosten und Zeitaufwand sind immer gleich hoch. | Das Verfahren schließt eine Sandbox-Analyse zur Aufdeckung getarnter Aktivitäten ein. |
| 4/3 | 2 | Welche der folgenden Aussagen ist falsch? | Die Urheber:innen eines Sybil-Angriffs manipulieren einen kompromittierten oder eingeschleusten Sensorknoten so, dass dieser die Rolle mehrerer Sensornetzwerke übernimmt. | Mithilfe von Sybil-Identitäten erhalten Angreifer:innen Zugriff auf einen großen Teil des Systems und erwecken den falschen Eindruck, dass bestimmte Netzwerk­segmente redundant gesichert sind. | Bei einem Replikationsangriff wird die ID eines legitimen Sensorknotens repliziert, sodass mit einem Mal mehrere Kopien desselben Knotens existieren. | Bei einem aktiven Angriff werden Pakete bei der Übertragung im drahtlosen Sensornetz modifiziert oder manipuliert. |
| 4/4 | 1 | Welche der folgenden Aussagen über ATP (Advanced Threat Protection) trifft zu? | Statische Analysen sind Teil einer ATP-Lösung. | ATP-Lösungen führen keine dynamischen Analysen durch. | Dateianalysen spielen im Bereich ATP keine Rolle. | ATP-Lösungen weisen eine hohe Fehlalarmquote auf. |
| 4/5 | 3 | Indikatoren sind ... | ... technische Artefakte, die Unternehmen auf eine akute Bedrohung hinweisen. | ... Benachrichti­gungen, die von Product Security Incident Response Teams (PSIRTs) und anderen Gremien versendet werden. | ... ein gängiges Mittel für den schnellen Austausch von Bedrohungsdaten zwischen Unternehmen. | ... für Menschen lesbare Benachrichtigungen über Schwachstellen, Bedrohungen, Exploits usw. |
| **Unit/**  **Question Number** | **Section** | **Question** | **Correct answer** | **Incorrect answer** | **Incorrect answer** | **Incorrect answer** |
| 5/1 | 1 | Welches der aufgeführten Merkmale zählt nicht zu den Features eines Operational Data Store? | Verarbeitung kleinerer Datenmengen | Umfassende Berichts­funktionen | Fehlertoleranz | Geringerer Platzbedarf |
| 5/2 | 1 | Das Funktionsprinzip eines ODS ähnelt einem ETL-Prozess, wenn wir einmal davon absehen, dass ... | ... die extrahierten Daten im Fall eines ETL-Prozesses zusätzlich transformiert und an die Zieldatenbank übermittelt werden. | ... die extrahierten Daten im Fall eines ETL-Prozesses direkt an die Zieldatenbank übermittelt werden. | ... die extrahierten Daten in einem ODS zusätzlich transformiert und an den Empfänger übermittelt werden. | ... die extrahierten Daten durch ein ODS-System langsamer aufbereitet werden als durch eine ETL-Lösung. |
| 5/3 | 3 | Eine NBA-Lösung stellt verschiedene wertvolle Features für Netzwerk­administrator:innen bereit. Welcher Bereich ist davon ausgenommen? | Netzwerk­management | Erkennung von Anomalien im Netzwerk | Diagnose und Behebung von Netzwerkstörungen | Netzwerk­überwachung |
| 5/4 | 6 | Welche der folgenden Phasen ist kein Bestandteil des NIST-Frameworks für Incident Response? | Lessons Learned (Erkenntnis­gewinnung) | Preparation (Vorbereitung) | Containment (Eindämmung) | Eradication (Beseitigung) |
| 5/5 | 6 | Eines der gängigstem IR-Frameworks wurde durch das SANS Institute entwickelt. Wofür steht das Akronym SANS? | SysAdmin, Audit, Network, and Security | SysAdmin, Accredit, Netmask, and Security | SysAdmin, Accredit, Network, and Services | SysAdmin, Audit, Network, and Services |
| **Unit/**  **Question Number** | **Section** | **Question** | **Correct answer** | **Incorrect answer** | **Incorrect answer** | **Incorrect answer** |
| 6/1 | 1 | Auf welcher Stufe der Umsetzung eines Sicherheitsprogramms ist die Erstellung einer geeigneten Datenbasis mit großen Schwierigkeiten verbunden, da kaum Daten verfügbar sind? | Stufe 1 | Stufe 2 | Stufe 3 | Stufe 4 |
| 6/2 | 1 | Welche Art von Metrik ist auf Stufe 3 der Umsetzung eines Sicherheitsprogramms relevant? | Kennzahlen rund um die Implementierung | Zweckgebundene Kennzahlen | Zielorientierte Kennzahlen | Ergebnisbezogene Kennzahlen |
| 6/3 | 1 | Welche der folgenden Personen zählt zu den sekundären Stakeholder:innen? | Generalinspektor:in | Chief Information Officer | Systemsicherheits-beauftragte:r | Programmleiter:in |
| 6/4 | 2 | Penetrationstests lassen sich anhand der verwendeten Toolkits und der Zugriffsrechte der Tester:innen in drei Kategorien einteilen. Welcher der folgenden Begriffe bezeichnet keine dieser Kategorien? | Greenbox-Tests | Whitebox-Tests | Greybox-Tests | Blackbox-Tests |
| 6/5 | 2 | Welche der folgenden Antwortmöglichkeiten bezeichnet keine Produktfamilie des Tools Beyond Security? | beSTATIC | beSECURE | beSOURCE | beSTORM |