ICT Berufsbildung
Formation professionnelle
Formazione professionale

Modulidentifikation

Modulnummer	**683**
Titel	Datenbestände analysieren und interpretieren

Kompetenz	Untersucht Rohdaten und Datenbestände auf kritische und sicherheitsrelevante Informationen, plausibilisiert die Ergebnisse und wertet die Untersuchung aussagekräftig und zielgruppengerecht aus.

Handlungsziele

1. Sammelt sicherheitsrelevante unstrukturierte, semistrukturierte und strukturierte Rohdaten aus den Systemen, Applikationen, Überwachungs- und Schutzlösungen einer Organisation.
2. Maskiert, pseudonymisiert oder anonymisiert sensitive Rohdaten bei Bedarf und unter Berücksichtigung des Datenschutzes.
3. Programmiert Skripts und Werkzeuge zur Auswertung, Bearbeitung und Darstellung von grossen Datenbeständen.
4. Führt Abfragen auf Datenbanken aus und bereitet die Abfrageergebnisse auf.
5. Untersucht Daten auf Anomalien, Indikatoren oder spezifischen Mustern von potenziellen Sicherheitsvorfällen.
6. Plausibilisiert die gewonnenen Daten, identifiziert und filtert False Positives und erhöht den Informationsgehalt der Ergebnisse mittels Anreicherung der Rohdaten mit lesbaren Zusatzinformationen.
7. Wertet die Untersuchung aus, bereitet die Ergebnisse in einem aussagekräftigen Abschlussbericht auf und präsentiert die Resultate den Entscheidungsträgern zielgruppengerecht.

Kompetenzfeld	Security/Risk Management
Objekt	Sicherheitsrelevante Rohdaten und Datenbestände aus Systemen, Applikationen, Überwachungs- und Schutzlösungen einer Organisation
Niveau	5
Voraussetzungen	Abläufe mit einer Scriptsprache automatisieren (122)
Anzahl Lektionen	40
Anerkennung	Eidg. Fachausweis

Modulversion	1.00

Copyright ICT-Berufsbildung Schweiz

info@ict-berufsbildung.ch
www.ict-berufsbildung.ch

Handlungsnotwendige Kenntnisse

Modulnummer	**683**
Titel	Datenbestände analysieren und interpretieren

Kompetenz	Untersucht Rohdaten und Datenbestände auf kritische und sicherheitsrelevante Informationen, plausibilisiert die Ergebnisse und wertet die Untersuchung aussagekräftig und zielgruppengerecht aus.

Handlungsnotwendige Kenntnisse

1.1 Kennt typische Beispiele von strukturierten, semi-strukturierten und unstrukturierten Daten und kann deren Unterschiede und die spezifischen Eigenschaften für die Datenanalyse erläutern.

1.2 Kennt typische Quellen für sicherheitsrelevante Daten in der ICT-Infrastruktur einer Organisation (z. B. SIEM, Log- und Protokolldateien von Geräten und Applikationen, E-Mail, Instant Messages, Datenbanken von Applikationen).

1.3 Kennt relevante textbasierte und binäre Datenformate für den Austausch und die Serialisierung von Daten (z. B. CSV, XML, JSON, BSON, YAML, HDF) und kann deren Merkmale, Unterschiede und Relevanz für die Datenanalysen erläutern.

1.4 Kennt unterschiedliche Standards und Formate von Log- und Protokolldateien (z. B. Syslog, Windows Ereignisprotokoll, Logdateien von Webservern).

1.5 Kennt geeignete Werkzeuge für das Log Management (z. B. Splunk, Papertrail, Loggly. GrayLog, Logstash) und kann deren Funktionalität erläutern (z. B. Sammlung, Indizierung, Auswertung und Visualisierung).

2.1 Kennt die Bedeutung der statischen und dynamischen Maskierung, Pseudonymisierung und Anonymisierung von Daten und kann deren Unterschiede und die Herausforderungen bei der Umsetzung erläutern.

2.2 Kennt unterschiedliche Methoden zur Maskierung, Pseudonymisierung und Anonymisierung von Daten (z. B. Löschung, Ersetzung, Verkürzung, Mischung, Varianzmethode, kryptografische Methoden) und kann deren Funktionsprinzip erläutern.

2.3 Kennt unterschiedliche Anonymisierungsverfahren (z. B. K-Anonymität, L-Diversity, Differential Privacy, Diffix) und kann deren Sicherheit bezüglich Deanonymisierung und den Einfluss auf die Qualität und Aussagekraft der Rohdaten erläutern.

2.4 Kennt die gesetzlichen Vorgaben des Datenschutzes an die Pseudonymisierung und Anonymisierung von personenbezogenen

Copyright ICT-Berufsbildung Schweiz

info@ict-berufsbildung.ch
www.ict-berufsbildung.ch

Daten und kann die Gewährleistung der Rechtmässigkeit, Verhältnismässigkeit, Zweckbindung und Transparenz mit typischen Anwendungsbeispielen erläutern.

2.5 Kennt geeignete Werkzeuge zur Maskierung, Pseudonymisierung und Anonymisierung von Datenbeständen (z. B. Amnesia, Anonimatron, ARX).

3.1 Kennt reguläre Ausdrücke (regular expressions) und kann deren Relevanz für Datenanalysen erklären.

3.2 Kennt relevante Konzepte und Kommandos (z. B. Ein- und Ausgaben, Filter, Pipes, Redirection) von Kommandozeileninterpretern der Betriebssysteme Windows (cmd, PowerShell) und Unix/Linux (z. B. bash, ksh, zsh) und kann deren Möglichkeiten und Grenzen im Kontext der Datenanalyse erläutern.

3.3 Kennt die Syntax der Programmiersprache Python, relevante Bibliotheken (z. B. NumPy, SciPy, Pandas, Matplotlib) und gängige Werkzeuge (z. B. IPython, Jupyter Notebooks) für die Analyse und Darstellung von Daten.

3.4 Kennt alternative Programmiersprachen zu Python (z. B. R, Scala, Julia, MATLAB) und kann deren Relevanz im Kontext der Datenanalyse erläutern.

4.1 Kennt das Konzept von relationalen Datenbanken und SQL, kann typische Anwendungsbeispiele und Technologien nennen (z. B. MySQL, SQL Server, PostgreSQL) und kann deren Vor- und Nachteile bei der Verwaltung von grossen Datenmengen erläutern.

4.2 Kennt gängige Technologien von nicht-relationalen NoSQL-Datenbanken (z. B. Cassandra, BigTable, MongoDB, CouchDB, Riak) und kann deren Datenmodell (spaltenorientiert, dokumentorientiert, graphbasiert, Key-Value), die Möglichkeiten der Datenabfrage (z. B. UnQL, objektspezifische Methoden) und die Vor- und Nachteile bei der Verwaltung von grossen Datenmengen erläutern.

5.1 Kennt relevante Konzepte und Techniken für die Analyse von grossen Datenbeständen (z. B. Mustererkennung, A/B-Testing, Zeitreihenanalyse, statistische Korrelation und Regression, Maschine Learning).

5.2 Kennt typische Indikatoren einer Kompromittierung (Indicators of Compormise IoC, z. B. Hashwerte, Signaturen, Domainnamen, IP-Adressen, URL, E-Mail-Adresse, X-Mailer, HTTP User Agent).

5.3 Kennt typische sicherheitsrelevante Anomalien (z. B. Abweichungen bei der Bandbreite, Protokollen oder Ports).

6.1 Kennt die Bedeutung von False Positives für die Auswertung von Datenbeständen und kann typische Beispiele erläutern.

Copyright ICT-Berufsbildung Schweiz

info@ict-berufsbildung.ch
www.ict-berufsbildung.ch

6.2 Kennt typische Quellen für Zusatzinformationen zur Datenanreicherung (z. B. DHCP, AD, Inventar, Konfigurationsdatenbank).

6.3 Kennt relevante Befehle (Kommandos) zur Gewinnung von Zusatzinformationen (z. B. nslookup, whois, trace / tracert) und kann deren Informationsgehalt erläutern.

7.1 Kennt geeignete Methoden und Techniken zur Verdichtung und Darstellung von Informationen (z. B. Datenreduktion, Kennzahlenbildung, Häufigkeitstabellen und Histogramme, Aggregation mittels Kreuz- oder Pivot-Tabelle, Korrelationsdiagramm, Zeitreihen- und Trendanalyse).

7.2 Kennt die wesentlichen Inhalte eines Abschlussberichts einer Untersuchung (z. B. Summary, Kontext, Untersuchungsgegenstand, Methoden, Ergebnisse, Erkenntnisse, Handlungsoptionen, Empfehlung mit Begründung) und kann deren Beitrag für die Entscheidungsfindung erläutern.

7.3 Kennt die Inhalte und Gliederung einer guten Präsentation und kann den Einfluss der eigenen Auftrittskompetenz und relevanter Haltungen auf die Überzeugungsarbeit erläutern.

Kompetenzfeld	Security/Risk Management
Objekt	Sicherheitsrelevante Rohdaten und Datenbestände aus Systemen, Applikationen, Überwachungs- und Schutzlösungen einer Organisation
Niveau	5
Voraussetzungen	Abläufe mit einer Scriptsprache automatisieren (122)
Anzahl Lektionen	40
Anerkennung	Eidg. Fachausweis

Modulversion	1.00