Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Sie erreichen uns unter

Arrow ECS GmbH, Elsenheimerstraße 1, 80687 München

Email: training.ecs.de@arrow.com
Phone: +49 (0)89 930 99 168

SC-100T00: Microsoft Cybersecurity Architect

CODE:	LÄNGE:	PREIS:
MCS_SC-100T00	4 Tage	€2,290.00

Description

Erfahren Sie, wie Sie mit Microsoft Sentinel, Microsoft Defender for Cloud und Microsoft 365 Defender Bedrohungen untersuchen, auf sie reagieren und sie aufspüren können. In diesem Kurs lernen Sie, wie Sie Cyberbedrohungen mithilfe dieser Technologien abwehren können. Insbesondere konfigurieren und verwenden Sie Microsoft Sentinel und nutzen Kusto Query Language (KQL) zur Erkennung, Analyse und Berichterstellung. Der Kurs richtet sich an Personen, die im Bereich Security Operations tätig sind, und hilft Teilnehmern bei der Vorbereitung auf die Prüfung SC-200: Microsoft Security Operations Analyst.

Lernziel

Erworbene Qualifikationen

- Erläutern, wie Microsoft Defender für Endpunkt Risiken in Ihrer Umgebung eindämmen kann
- Administration einer Microsoft Defender für Endpunkt-Umgebung
- Konfigurieren von Regeln zur Verringerung der Angriffsfläche auf Windows-Geräten
- Ausführen von Aktionen auf einem Gerät mithilfe von Microsoft Defender für Endpunkt
- Untersuchen von Domänen und IP-Adressen in Microsoft Defender für Endpunkt
- Untersuchen von Benutzerkonten in Microsoft Defender für Endpunkt
- Konfigurieren von Warnungseinstellungen in Microsoft 365 Defender
- Ausführen einer Suche in Microsoft 365 Defender
- Verwalten von Incidents in Microsoft 365 Defender
- Erläutern, wie Microsoft Defender for Identity Risiken in Ihrer Umgebung eindämmen kann
- Untersuchen von DLP-Warnungen in Microsoft Defender für Cloud-Apps
- Erläutern der Arten von Aktionen, die Sie bei Insider-Risikomanagementfällen ausführen können
- Konfigurieren der automatischen Bereitstellung in Microsoft Defender für Cloud-Apps
- Beheben von Warnungen in Microsoft Defender für Cloud-Apps
- Erstellen von KQL-Anweisungen
- Filtern von Suchergebnissen basierend auf der Ereigniszeit, dem Schweregrad, der Domäne und anderen relevanten Daten mithilfe von KQL
- Extrahieren von Daten aus unstrukturierten Zeichenfolgenfeldern mit KQL
- Verwalten eines Microsoft Sentinel-Arbeitsbereichs
- Zugreifen auf die Watchlist in Microsoft Sentinel mithilfe von KQL

- Verwalten von Bedrohungsindikatoren in Microsoft Sentinel
- Erläutern der Unterschiede zwischen dem Common Event Format- und dem Syslog-Connector in Microsoft Sentinel
- Verbinden von Azure Windows-VMs mit Microsoft Sentinel
- Konfigurieren von Log Analytics-Agents zum Erfassen von Sysmon-Ereignissen
- Erstellen neuer Analyseregeln und Abfragen mithilfe des Assistenten für Analyseregeln
- Erstellen eines Playbooks, um die Reaktion auf Vorfälle zu automatisieren
- Verwenden von Abfragen für die Suche nach Bedrohungen
- Beobachten von Bedrohungen im Zeitverlauf mit Livestreams

Zielgruppe

Der Microsoft Security Operations Analyst arbeitet mit Projektbeteiligten im Unternehmen zusammen, um IT-Systeme des Unternehmens zu schützen. Ihr Ziel ist es, Risiken für das Unternehmen zu verringern, indem sie aktive Angriffe in der Umgebung schnell abwehren, Empfehlungen zur Verbesserung der Bedrohungsschutzmethoden aussprechen und Verstöße gegen die Unternehmensrichtlinien an die zuständigen Stellen weiterleiten. Zu den Zuständigkeiten gehören das Verwalten und Überwachen von sowie das Reagieren auf Bedrohungen durch den Einsatz einer Vielzahl von Sicherheitslösungen in ihrer Umgebung. Zu den Aufgaben dieser Rolle gehört in erster Linie das Untersuchen, Reagieren und Suchen nach Bedrohungen mithilfe von Microsoft Sentinel, Microsoft Defender for Cloud, Microsoft 365 Defender und Sicherheitsprodukten von Drittanbietern. Da der*die Security Operations Analyst die operative Ausgabe dieser Tools nutzt, ist er*sie auch ein*e wichtige*r Stakeholder*in beim Konfigurieren und Bereitstellen dieser Technologien.

Voraussetzungen

Voraussetzungen

- Grundkenntnisse über Microsoft 365
- Grundlegendes Verständnis über Microsoft-Produkte zu Sicherheit, Compliance und Identität
- Fortgeschrittene Kenntnisse über Microsoft Windows
- Vertrautheit mit Azure-Diensten, insbesondere Azure SQL-Datenbank und Azure Storage
- Kenntnisse im Umgang mit virtuellen Azure-Computern und virtuellen Netzwerken
- Grundlegendes Verständnis der Konzepte zur Skripterstellung.

Inhalt

Modul 1: Abwehr von Bedrohungen mithilfe von Microsoft 365 Defender
Analysieren Sie Bedrohungsdaten domänenübergreifend, und beseitigen Sie Bedrohungen schnell mithilfe der integrierten Orchestrierung und Automatisierung in Microsoft 365 Defender. Erfahren Sie mehr über Bedrohungen der Cybersicherheit und wie die neuen Bedrohungsschutztools von Microsoft die Benutzer, Geräte und Daten in Ihrem Unternehmen schützen. Verwenden Sie die erweiterte Erkennung und Beseitigung von identitätsbasierten Bedrohungen, um Ihre Azure Active Directory-Identitäten und -Anwendungen vor Angriffen zu schützen.
Lektionen

- Einführung in den Bedrohungsschutz von Microsoft 365
- Abmildern von Incidents mithilfe von Microsoft 365 Defender
- Schützen Ihrer Identitäten mit Azure AD Identity Protection
- Minimieren von Risiken mit Microsoft Defender für Office 365

- Schützen Ihrer Umgebung mit Microsoft Defender for Identity
- Schützen Ihrer Cloud-Apps und -Dienste mit Microsoft Defender für Cloud-Apps
- Reagieren auf Warnungen zur Verhinderung von Datenverlust mithilfe von Microsoft 365
- Verwalten des Insiderrisikos in Microsoft 365

Lab: Abwehr von Bedrohungen mithilfe von Microsoft 365 Defender

- Erkunden von Microsoft 365 Defender

Nach Abschluss dieses Moduls werden die Teilnehmer in der Lage sein:

  - Erläutern, wie sich die Bedrohungslandschaft entwickelt
  - Verwalten von Incidents in Microsoft 365 Defender
  - Ausführen einer erweiterten Suche in Microsoft 365 Defender
  - Untersuchen von Warnungen in Microsoft 365 Defender
  - Beschreibung der Untersuchungs- und Beseitigungsfunktionen von Azure Active Directory Identity Protection
  - Erläutern, wie Sie mit Cloud Discovery einen Überblick über die Vorgänge in Ihrem Unternehmen erhalten

Modul 2: Abwehr von Bedrohungen mithilfe von Microsoft Defender für Endpunkt

Implementieren Sie die Microsoft Defender for Endpoint-Plattform, um erweiterte Bedrohungen zu erkennen, zu untersuchen und darauf zu reagieren. Erfahren Sie, wie Microsoft Defender für Endpunkt die Sicherheit Ihrer Organisation verbessern kann. Hier erfahren Sie, wie Sie die Microsoft Defender für Endpunkt-Umgebung bereitstellen, einschließlich des Onboardings von Geräten und der Sicherheitskonfiguration. Hier erfahren Sie, wie Incidents und Warnungen mithilfe von Microsoft Defender für Endpunkte untersucht werden. Sie können eine erweiterte Bedrohungssuche durchführen und sich an Experten für Bedrohungen wenden. Sie werden darüber hinaus lernen, wie Sie die Automatisierung in Microsoft Defender for Endpoint durch die Verwaltung von Umgebungseinstellungen konfigurieren können. Schließlich lernen Sie mithilfe des Bedrohungs- und Schwachstellenmanagements in Microsoft Defender for Endpoint die Schwachstellen Ihrer Umgebung kennen.

Lektionen

- Schützen vor Bedrohungen mit Microsoft Defender für Endpunkt
- Bereitstellen der Microsoft Defender für Endpunkt-Umgebung
- Implementieren von Windows-Sicherheitsverbesserungen mit Microsoft Defender für Endpunkt
- Durchführen von Geräteuntersuchungen in Microsoft Defender für Endpunkt
- Ausführen von Aktionen auf einem Gerät mithilfe von Microsoft Defender für Endpunkt
- Untersuchen von Beweisen und Entitäten mithilfe von Microsoft Defender für Endpunkt
- Konfigurieren und Verwalten der Automatisierung mit Microsoft Defender für Endpunkt
- Konfigurieren von Warnungen und Erkennungen in Microsoft Defender für Endpunkt
- Verwenden des Sicherheitsrisikomanagements in Microsoft Defender für Endpunkt

Lab: Bereitstellen von Microsoft Defender für Endpunkt

- Initialisieren von Microsoft Defender für Endpunkt
- Onboarding eines Geräts
- Konfigurieren von Rollen
- Konfigurieren von Gerätegruppen

Lab: Entschärfen von Angriffen mit Microsoft Defender für Endpunkt

- Simulierte Angriffe

Nach Abschluss dieses Moduls werden die Teilnehmer in der Lage sein:

  - Bestimmen der Möglichkeiten von Microsoft Defender für Endpunkt
  - Konfigurieren von Microsoft Defender für Endpunkt-Umgebungseinstellungen
  - Konfigurieren von Regeln zur Verringerung der Angriffsfläche auf Windows-Geräten
  - Beschreiben forensischer Geräteinformationen, die von Microsoft Defender für Endpunkt gesammelt werden
  - Durchführen der Sammlung forensischer Daten mithilfe von Microsoft Defender für Endpunkt
  - Untersuchen von Benutzerkonten in Microsoft Defender für Endpunkt
  - Verwalten von Automatisierungseinstellungen in Microsoft Defender für Endpunkt
  - Verwalten von Indikatoren in Microsoft Defender für Endpunkt
  - Beschreiben des Bedrohungs- und Sicherheitsrisikomanagements in Microsoft Defender für Endpunkt

Modul 3: Abwehr von Bedrohungen mithilfe von Microsoft Defender für Cloud
Verwenden von Microsoft Defender für Cloud, für Azure, Hybrid Cloud und lokalem Workloadschutz und lokaler Sicherheit. Erfahren Sie mehr über den Zweck von Microsoft Defender für Cloud und seine Aktivierung. Sie erfahren außerdem mehr über die von Microsoft Defender für Cloud für die einzelnen Cloudworkloads bereitgestellten Schutz- und Erkennungsfunktionen. Hier erfahren Sie, wie Sie Ihrer Hybridumgebung Funktionen von Microsoft Defender für Cloud hinzufügen.
Lektionen

- Planen von Workloadschutz in der Cloud mit Microsoft Defender für Cloud
- Verbinden von Azure-Ressourcen mit Microsoft Defender für Cloud
- Verbinden Azure-fremder Ressourcen mit Microsoft Defender für Cloud
- Verwalten Ihres Cloud Security Posture Management-Ansatzes
- Workloadschutz in der Cloud mit Microsoft Defender für Cloud
- Beheben von Sicherheitswarnungen mit Microsoft Defender für Cloud

Lab: Abwehr von Bedrohungen mithilfe von Microsoft Defender für Cloud

- Aktivieren von Microsoft Defender für Cloud
- Entschärfung von Angriffen mit Microsoft Defender für Cloud
-

Nach Abschluss dieses Moduls werden die Teilnehmer in der Lage sein:

  - Beschreiben von Funktionen von Microsoft Defender für Cloud
  - Erläutern, welche Workloads durch Microsoft Defender für Cloud geschützt werden
  - Erläutern der Funktionsweise von Microsoft Defender für Cloud-Schutzfunktionen
  - Konfigurieren der automatischen Bereitstellung in Microsoft Defender für Cloud
  - Beschreiben der manuellen Bereitstellung in Microsoft Defender für Cloud
  - Verbinden Azure-fremder Computer mit Microsoft Defender für Cloud
  - Beschreiben von Warnungen in Microsoft Defender für Cloud
  - Beheben von Warnungen in Microsoft Defender für Cloud

- Automatisieren der Reaktionen in Microsoft Defender für Cloud

Modul 4: Erstellen von Abfragen für Microsoft Sentinel mithilfe von Kusto Query Language (KQL)
Schreiben Sie die KQL-Anweisungen (Kusto Query Language) zum Abfragen von Protokolldaten, um Erkennungen, Analysen und Berichte in Microsoft Sentinel auszuführen. Dieses Modul konzentriert sich auf die am häufigsten verwendeten Operatoren. In den KQL-Beispielanweisungen werden sicherheitsbezogene Tabellenabfragen vorgestellt. KQL ist die Abfragesprache, die der Untersuchung von Daten zum Erstellen von Analysen und Arbeitsmappen sowie der Ausführung von Huntingvorgängen in Microsoft Sentinel dient. Im Folgenden finden Sie Informationen darüber, wie Sie mithilfe der grundlegenden KQL-Anweisungsstruktur komplexe Anweisungen erstellen. Hier erfahren Sie, wie Sie Daten in einer KQL-Anweisung zusammenfassen und visualisieren. Dies ist die Grundlage zum Erstellen von Erkennungen in Microsoft Sentinel. Erfahren Sie, wie Sie mithilfe der Kusto-Abfragesprache (Kusto Query Language, KQL) aus Protokollquellen erfasste Zeichenfolgendaten bearbeiten.
Lektionen

- Erstellen von KQL-Anweisungen für Microsoft Sentinel
- Analysieren von Abfrageergebnissen mithilfe von KQL
- Erstellen von Anweisungen mit mehreren Tabellen mithilfe von KQL
- Arbeiten mit Daten in Microsoft Sentinel mithilfe der Kusto-Abfragesprache

Lab: Erstellen von Abfragen für Microsoft Sentinel mithilfe von Kusto Query Language (KQL)

- Erstellen von Abfragen für Microsoft Sentinel mithilfe von Kusto Query Language (KQL)

Nach Abschluss dieses Moduls werden die Teilnehmer in der Lage sein:

- Erstellen von KQL-Anweisungen
- Durchsuchen von Protokolldateien nach Sicherheitsereignissen mithilfe von KQL
- Filtern von Suchergebnissen basierend auf der Ereigniszeit, dem Schweregrad, der Domäne und anderen relevanten Daten mithilfe von KQL
- Zusammenfassen von Daten mithilfe von KQL-Anweisungen
- Rendern von Visualisierungen mithilfe von KQL-Anweisungen
- Extrahieren von Daten aus unstrukturierten Zeichenfolgenfeldern mit KQL
- Extrahieren von Daten aus strukturierten Datenfeldern mit KQL
- Erstellen von Funktionen mit KQL

Modul 5: Konfigurieren Ihrer Microsoft Sentinel-Umgebung
Erste Schritte mit Microsoft Sentinel durch ordnungsgemäßes Konfigurieren des Microsoft Sentinel-Arbeitsbereichs. Das Einrichten und Konfigurieren herkömmlicher SIEM-Systeme (Security Information & Event Management) erfordert in der Regel viel Zeit. Außerdem sind diese Systeme nicht unbedingt für Cloudworkloads konzipiert. Microsoft Sentinel ermöglicht es Ihnen, sich anhand Ihrer Cloud- und lokalen Daten schnell wertvolle sicherheitsrelevante Erkenntnisse zu verschaffen. Dieses Modul unterstützt Sie beim Einstieg. Im Folgenden finden Sie Informationen darüber, wie Sie mit der Architektur von Microsoft Sentinel-Arbeitsbereichen Ihr System so konfigurieren, dass die Anforderungen an die Sicherheitsanforderungen Ihrer Organisation erfüllt werden. Als Security Operations Analyst müssen Sie die Tabellen, Felder und Daten verstehen, die in Ihrem Arbeitsbereich erfasst werden. Hier erfahren Sie, wie Sie die am häufigsten genutzten Datentabellen in Microsoft Sentinel abfragen.
Lektionen

- Einführung in Microsoft Sentinel
- Erstellen und Verwalten von Microsoft Sentinel-Arbeitsbereichen
- Abfragen von Protokollen in Microsoft Sentinel
- Verwenden von Watchlists in Microsoft Sentinel
- Verwenden der Threat Intelligence in Microsoft Sentinel

Lab: Konfigurieren Ihrer Microsoft Sentinel-Umgebung

- Konfigurieren Ihrer Microsoft Sentinel-Umgebung

Nach Abschluss dieses Moduls werden die Teilnehmer in der Lage sein:

  - Identifizieren der verschiedenen Komponenten und Funktionen von Microsoft Sentinel
  - Identifizieren von Anwendungsfällen für Microsoft Sentinel
  - Beschreiben der Architektur von Microsoft Sentinel-Arbeitsbereichen
  - Installieren eines Microsoft Sentinel-Arbeitsbereichs
  - Verwalten eines Microsoft Sentinel-Arbeitsbereichs
  - Erstellen einer Watchlist in Microsoft Sentinel
  - Zugreifen auf die Watchlist in Microsoft Sentinel mithilfe von KQL
  - Verwalten von Bedrohungsindikatoren in Microsoft Sentinel
  - Verwenden von KQL für den Zugriff auf Bedrohungsindikatoren in Microsoft Sentinel

Modul 6: Verbinden von Protokollen mit Microsoft Sentinel

Verknüpfen Sie Daten auf Cloudniveau mit Microsoft Sentinel – benutzerübergreifend, anwendungs- und infrastrukturübergreifend sowie lokal als auch in mehreren Clouds. Zum Verbinden von Protokolldaten werden in erster Linie die von Microsoft Sentinel bereitgestellten Datenconnectors verwendet. Dieses Modul liefert einen Überblick über die verfügbaren Datenconnectors. Sie lernen die Konfigurationsoptionen und Daten kennen, die von Microsoft Sentinel-Connectors für Microsoft 365 Defender bereitgestellt werden.

Lektionen

- Verbinden von Daten mit Microsoft Sentinel mithilfe von Datenconnectors
- Herstellen einer Verbindung von Microsoft-Diensten mit Microsoft Sentinel
- Verbinden von Microsoft 365 Defender mit Microsoft Sentinel
- Verbinden von Windows-Hosts mit Microsoft Sentinel
- Verbinden von Common Event Format-Protokollen mit Microsoft Sentinel
- Verbinden von Syslog-Datenquellen mit Microsoft Sentinel
- Verbinden von Bedrohungsindikatoren mit Microsoft Sentinel

Lab: Verbinden von Protokollen mit Microsoft Sentinel

- Verbinden von Daten mit Microsoft Sentinel mithilfe von Datenconnectors
- Verbinden von Windows-Geräten mit Microsoft Sentinel über Datenconnectors
- Verbinden von Linux-Hosts mit Microsoft Sentinel über Datenconnectors
- Verbinden von Threat Intelligence mit Microsoft Sentinel über Datenconnectors

Nach Abschluss dieses Moduls werden die Teilnehmer in der Lage sein:

  - Erläutern der Verwendung von Datenconnectors in Microsoft Sentinel
  - Erläutern der Unterschiede zwischen dem Common Event Format- und dem Syslog-Connector in Microsoft Sentinel
  - Herstellen einer Verbindung für Microsoft-Dienstconnectors
  - Hintergrundkenntnisse zur automatischen Erstellung von Incidents in Microsoft Sentinel durch Connectors

- Aktivieren des Microsoft 365 Defender-Connectors in Microsoft Sentinel
- Verbinden von Azure Windows-VMs mit Microsoft Sentinel
- Verbinden von Azure Windows-Hosts mit Microsoft Sentinel
- Konfigurieren von Log Analytics-Agents zum Erfassen von Sysmon-Ereignissen
- Erläutern der Bereitstellungsoptionen des Common Event Format-Connectors in Microsoft Sentinel
- Konfigurieren des TAXII-Connectors in Microsoft Sentinel
- Anzeigen von Bedrohungsindikatoren in Microsoft Sentinel

Modul 7: Erstellen von Erkennungen und Durchführen von Untersuchungen mithilfe von Microsoft Sentinel
Erkennen von zuvor unentdeckten Bedrohungen und schnelles Beheben von Bedrohungen mit integrierter Orchestrierung und Automatisierung in Microsoft Sentinel. Sie erfahren, wie Sie mit Microsoft Sentinel-Playbooks auf Sicherheitsbedrohungen reagieren. Sie sehen sich das Incidentmanagement in Microsoft Sentinel an, erhalten Informationen zu Ereignissen und Entitäten in Microsoft Sentinel und lernen Möglichkeiten kennen, Incidents aufzulösen. Sie erfahren auch mehr über das Abfragen, Visualisieren und Überwachen von Daten in Microsoft Sentinel.
Lektionen

- Bedrohungserkennung mit Microsoft Sentinel-Analysen
- Automatisierung in Microsoft Sentinel
- Reaktion auf Bedrohungen mit Microsoft Sentinel-Playbooks
- Verwaltung von Sicherheitsvorfällen in Microsoft Sentinel
- Identifizieren von Bedrohungen mit der Entitätsverhaltensanalyse in Microsoft Sentinel
- Datennormalisierung in Microsoft Sentinel
- Abfragen, Visualisieren und Überwachen von Daten in Microsoft Sentinel
- Verwalten von Inhalten in Microsoft Sentinel

Lab: Erstellen von Erkennungen und Durchführen von Untersuchungen mithilfe von Microsoft Sentinel

- Ändern einer Microsoft-Sicherheitsregel
- Erstellen eines Playbooks
- Erstellen einer geplanten Abfrage
- Verstehen der Erkennungsmodellierung
- Durchführen von Angriffen
- Erstellen von Erkennungen
- Untersuchen von Incidents
- Erstellen von Arbeitsmappen

Nach Abschluss dieses Moduls werden die Teilnehmer in der Lage sein:

- Erläutern der Bedeutung von Microsoft Sentinel Analytics
- Erstellen von Regeln anhand von Vorlagen
- Verwalten von Regeln mit Änderungen
- Erläutern der SOAR-Funktionen von Microsoft Sentinel.
- Erstellen eines Playbooks, um die Reaktion auf Bedrohungen zu automatisieren

- Untersuchen und Verwalten der Incidentauflösung
- Erläutern von User and Entity Behavior Analytics in Microsoft Sentinel
- Erkunden von Entitäten in Microsoft Sentinel
- Visualisieren von Sicherheitsdaten mithilfe von Microsoft Sentinel-Arbeitsmappen

Modul 8: Ausführen von Bedrohungssuche in Microsoft Sentinel
In diesem Modul erfahren Sie, wie Sie mithilfe von Microsoft Sentinel-Abfragen proaktiv Bedrohungsverhaltensweisen identifizieren können. Außerdem lernen Sie, Lesezeichen und Livestreams zum Suchen von Bedrohungen zu verwenden. Außerdem erfahren Sie, wie Sie Notebooks in Microsoft Sentinel für die erweiterte Bedrohungssuche verwenden.
Lektionen

- Erläutern der Bedrohungssuchkonzepte in Microsoft Sentinel
- Bedrohungssuche mit Microsoft Sentinel
- Verwenden von Suchaufträgen in Microsoft Sentinel
- Suchen von Bedrohungen mithilfe von Notebooks in Microsoft Sentinel

Lab: Ausführen von Bedrohungssuche in Microsoft Sentinel

- Ausführen von Bedrohungssuche in Microsoft Sentinel
- Bedrohungssuche mithilfe von Notebooks mit Microsoft Sentinel

Nach Abschluss dieses Moduls werden die Teilnehmer in der Lage sein:

- Beschreiben der Bedrohungssuchkonzepte für die Verwendung mit Microsoft Sentinel
- Definieren einer Bedrohungssuchhypothese für die Verwendung mit Microsoft Sentinel
- Verwenden von Abfragen für die Suche nach Bedrohungen
- Beobachten von Bedrohungen im Zeitverlauf mit Livestreams
- Erkunden von API-Bibliotheken für die erweiterte Bedrohungssuche in Microsoft Sentinel
- Erstellen und Verwenden von Notebooks in Microsoft Sentinel

Kurstermine

Auf Anfrage. Bitte kontaktieren Sie uns

Zusätzliche Information

Diese Schulung ist auch als Vor-Ort-Schulung verfügbar. Bitte kontaktieren Sie uns, um mehr zu erfahren.