CYBER RANGE

AUSTRIAN INSTITUTE OF TECHNOLOGY

GRUNDLAGEN DES CYBER SECURITY OPERATIONS CENTRE (SOC)

ZUSAMMENFASSUNG

Security Operations Centres (SOCs) sind zu einem grundlegenden Bestandteil der Cybersicherheit von Unternehmen geworden, da sie ein Bewusstsein für sicherheitskritische Situationen schaffen. Sie werden eingesetzt, um verschiedene sicherheitsrelevante Funktionen zu erfüllen, darunter technisches Schwachstellenmanagement, Bedrohungsanalyse und Unterstützung bei der Reaktion auf Cybersicherheitsvorfälle. Um dies zu erreichen, stützen sie sich auf die Fähigkeiten von Cybersicherheitsexpert:innen, die eine große Anzahl entsprechender Analyse-Werkzeuge zur Verfügung haben. SOCs können auf unterschiedliche Weise implementiert werden, wobei einige oder alle Funktionen an Dritte ausgelagert werden können, je nach Budget und Risikobereitschaft eines Unternehmens.

ZIELE

Ziel dieses Kurses ist es, die Teilnehmenden in die Grundlagen der Einrichtung und des Betriebs eines SOC für ihr Unternehmen einzuführen. Dieses Wissen ist von Vorteil, wenn beispielsweise Entscheidungsträger:innen von Unternehmen verstehen möchten, was der Zweck eines SOC ist, welche Konfiguration für Unternehmen sinnvoll ist und welche wichtigen Aktivitäten und Tools ein SOC durchführt und anwendet. Um dies zu erreichen, behandelt der Kurs mehrere Themen:

1. SOC Gründung, Ziele und Organisation
2. Tools, einschließlich Intrusion Detection Systeme, SIEM und SOAR-Lösungen
3. Informationen über Cyber-Bedrohungen
4. Technische Schwachstellenbewertung und -management
5. Reaktion auf Cyber-Sicherheitsvorfälle, einschließlich der Entwicklung von Playbooks
6. Digitale Forensik

Am dritten Kurstag findet eine Cyber Security Übung auf der AIT Cyber Range statt, in der die Teilnehmenden praktische Erfahrungen bei der Reaktion auf Sicherheitsvorfälle, der Kernaufgabe eines SOC, erwerben und vertiefen können.

ZIELGRUPPE

Der Kurs ist für verschiedene Interessengruppen relevant, die ein grundlegendes Verständnis von Cybersicherheit haben. Zum Beispiel profitieren sowohl Entscheidungsträger:innen, die ihre SOC-Fähigkeiten aufbauen oder verbessern wollen, von dem Kurs, wie auch technische Mitarbeiter:innen, die ihr Verständnis für programmbezogene Aspekte der Cybersicherheit vertiefen wollen. Der Kurs ist sowohl konzeptionell als auch technisch ausgerichtet und enthält nützliche Übungen, um die wichtigsten Konzepte zu festigen. Die Teilnehmenden werden durchgehend vom Ausbildungsteam unterstützt.

CYBER RANGE

AUSTRIAN INSTITUTE OF TECHNOLOGY

GLIEDERUNG DES KURSES

Tag 1: Cyber Situationsbewusstsein und Erkennung

Module

- Grundlagen des Security Operations Centre
- Eine Einführung in Sicherheitsüberwachung und Intrusion Detection Systeme
- SIEM und SOAR - Unverzichtbare SOC-Tools
- Cyber-Bedrohungsdaten nutzen

Übungen

- Festlegung der Anforderungen für ein SOC
- Integration eines IDS in eine SIEM-Lösung
- Analyse der Bedrohungsabdeckung mit MITRE ATT&CK

Tag 2: Reaktion auf Vorfälle, Bedrohungsanalyse und Schwachstellenmanagement

Module

- Reaktion auf Cyber-Sicherheitsvorfälle
- Eine Einführung in die digitale Forensik
- Einführung in das technische Schwachstellenmanagement

Übungen

- Playbooks für die Reaktion auf Vorfälle erstellen
- Auf der Jagd nach Indikatoren für Kompromisse (IoCs)
- Tools für das Asset- und Schwachstellenmanagement

Tag 3: Übung zur Reaktion auf Cyber-Sicherheitsvorfälle

Der dritte Tag des Kurses besteht aus einer abschließenden Übung zur Reaktion auf Cybersecurity-Vorfälle, die auf der AIT Cyber Range durchgeführt wird.

MARTIN LATZENHOFER
Senior Research Engineer
Center for Digital Safety & Security
AIT Austrian Institute of Technology
martin.latzenhofer@ait.ac.at
www.ait.ac.at

GREGOR LANGNER
Scientist
Center for Digital Safety & Security
AIT Austrian Institute of Technology
gregor.langner@ait.ac.at
www.ait.ac.at