Workshop - aus der Praxis für die Praxis!

Erkennen von Cyberangriffen mit **Microsoft Advanced Threat Analytics (ATA)**

Planung, Bereitstellung, Konfiguration & Verwaltung

Die Häufigkeit von Cyberangriffen gegen Computernetzwerke nimmt seit Jahren ständig zu. Oft zielen die Angreifer dabei auf die „Achillesferse" der weltweit eingesetzten Windows-Betriebssysteme auf Client- und Servercomputern ab, die man im Verfahren der „einmaligen Anmeldung" (engl. Single-Sign-On, SSO) herausgefunden hat. Diese Schwachstelle ermöglicht es im schlimmsten Fall, die Kennwörter von Benutzern nach der Anmeldung einfach im Klartext aus dem betroffenen Computersystem herauszulesen - oder sich mittels „Pass-the-Hash-" oder „Pass-the-Ticket-Attacke" oft völlig unbemerkt im Namen des betreffenden Benutzers auf Ressourcen im Computernetzwerk zu verbinden. Microsoft Advanced Thread Analytics (ATA) bietet die notwendigen Funktionen für die Früherkennung solcher und ähnlicher Cyberattacken in modernen Computernetzwerken, und ermöglicht somit den notwendigen Schutz der darin verarbeiteten und gespeicherten Daten.

Dauer

2 Tage (Vollzeit)

Lernziele

Im Verlauf dieses 2-tägigen Workshops wird das notwendige Wissen für die erfolgreiche Planung, Bereitstellung, Konfiguration und Verwaltung von Microsoft Advanced Threat Analytics (ATA) als „Intrusion Detection System (IDS)" vermittelt. Anhand praktischer Übungen wird auch die (Früh-)Erkennung möglicher Cyberattacken durch den Einsatz entsprechender Angriffstools simuliert, so dass die Teilnehmer das Produkt im Anschluss an den Workshop auch zielgerecht einsetzen - und somit den Schutz für die in den Computernetzwerken eingesetzten Computersysteme und Daten entsprechend erhöhen können.

Zielgruppe

Der Praxisworkshop ist entworfen worden für:

Administratoren und Netzwerkplaner, System- und Netzwerkverwalter, IT- und Systemverantwortliche sowie IT-Sicherheitsbeauftragte

Voraussetzungen

Die Teilnehmer für diesen Kurs sollten die folgenden Voraussetzungen erfüllen:

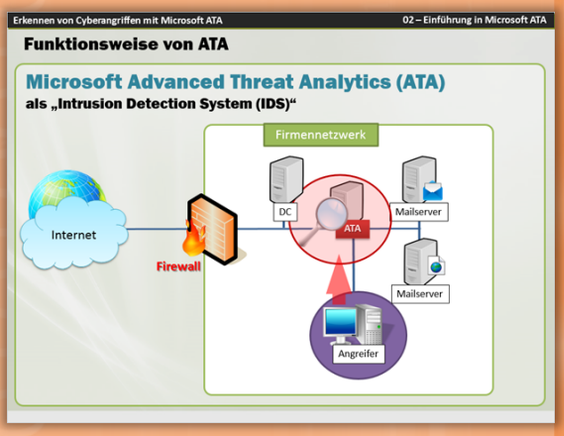
Kenntnisse und Fähigkeiten in der Konfiguration und Verwaltung von Windows-Betriebssystemen, Kenntnisse in der Konfiguration von Verzeichnisdiensten, grundlegende Kenntnisse zu LANs / lokalen Netzwerken sowie grundlegende Fähigkeiten im Umgang mit TCP/IP.

Workshop - aus der Praxis für die Praxis!

Erkennen von Cyberangriffen mit **Microsoft Advanced Threat Analytics (ATA)**

Planung, Bereitstellung, Konfiguration & Verwaltung

Unterrichtsmodule / Kursinhalte:



01 - Einführung und Grundlagen

Aktuelle Entwicklung, potentielle Bedrohungen

02 - Einführung in Microsoft Advanced Threat Analytics (ATA)

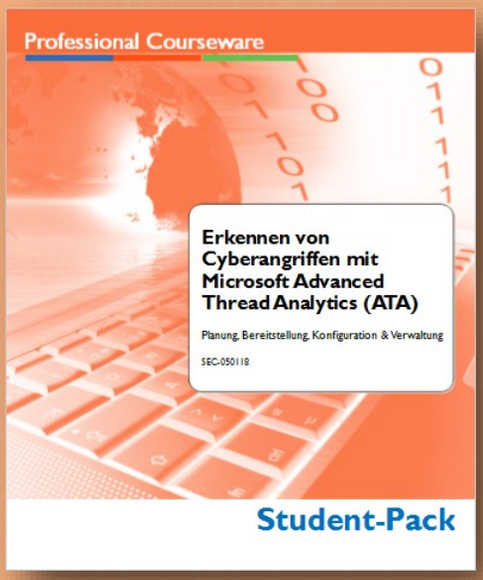
Funktionsweise und Architektur von ATA, SIEM-Unterstützung, Komponenten, Planen der ATA-Kapazität, ATA-Rollengruppen, Lizenzierung

03 - Bereitstellung von ATA

Bereitstellungsoptionen, Voraussetzungen für die einzelnen ATA-Komponenten, Netzwerkanforderungen, vorbereitende Schritte, Bereitstellungsschritte, Sammlung von Telemetriedaten, Konfiguration der Windows-Ereignisweiterleitung, VPN-Integration von ATA, Konfiguration verschiedener Einstellungen in ATA, Anpassung der Überwachung von Aktivitäten

04 - Angriffserkennung mittels ATA in der Praxis

Arbeiten mit verdächtigen Aktivitäten, Angriffserkennung mittels ATA anhand verschiedener Sicherheitstools, Anzeige von Aktivitäten in der ATA-Konsole, Anpassung der Ansichten, Bearbeiten verdächtiger Aktivitäten



05 - Berichtsgenerierung und -bereitstellung

Berichte manuell erstellen und Downloaden, Festlegen geplanter Berichte

06 - Wartung und Problembehandlung rund um ATA

Bearbeiten der ATA-Center-Konfiguration, Ersetzen des SSL-Zertifikats für das ATA-Center, Problembehandlung rund um ATA, Sichern und Wiederherstellen der ATA-Datenbank, Verschieben, der ATA-Datenbank, Notfallwiederherstellung der ATA-Center-Konfiguration

Nähere Informationen zum Workshop erhalten Sie bei: