Microsoft Advanced Threat Analytics (ATA) - Planung, Bereitstellung, Konfiguration & Verwaltung

Überblick

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 Threat 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

Preis:
1.350,00 € (1.606,50 € inkl. MwSt.)

Kursinhalt

Einführung und Grundlagen

- Aktuelle Entwicklung, potentielle Bedrohung

Einführung in Microsoft Advanced Threat Analytics

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

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

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

Berichtsgenerierung und -bereitstellung

- Berichte manuell erstellen und Downloaden
- Festlegen geplanter Berichte

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

Voraussetzungen

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

Zielgruppe

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