Active Enterprise Defense.

Active Enterprise Defense.

Seminar | Zurzeit keine Termine | Teilnahmebescheinigung

Virtual Classroom | 16 Unterrichtseinheiten

Seminarnummer: 31491

Stand: 12.07.2025. Alle aktuellen Informationen finden Sie unter https://akademie.tuv.com/s/31491

Im Active Enterprise Defense Kurs mit über 15 Laboren und Fallstudien lernen Sie, wie Sie 0 Day- und 1-Day-Schwachstellen abwehren und Sicherheitsvorfälle erfolgreich eindämmen und aufklären. Vertiefen Sie Ihr Wissen in Bedrohungsmodellierung, sicherer Architektur, Windows-Event-Analyse, Täuschung, Sandboxing und Egress-Filterung in Windows-, Linux- und Cloud-Umgebungen wie M365 und AWS. Darüber hinaus bieten wir umfassende Einblicke zu privilegiertem Zugriff, Application Whitelisting, Forensik und DFIR (Digital Forensics and Incident Response). Sichern Sie Ihr Unternehmen nicht nur vor Ransomware, sondern auch vor fortschrittlichen APTs. Der Kurs gliedert sich in zwei Teile: Zunächst liegt der Fokus auf Prävention, anschließend vertiefen wir die Themen Analyse und Incident Response (DFIR).

Nutzen

Mit einem Reverse-Graph-Walk-Ansatz lernen Sie, wie Sie Ihre wichtigsten Ressourcen schützen, indem Sie potenzielle Sicherheitslücken identifizieren und die Strategien von Angreifern antizipieren.

Durch die Kombination aus Labor Fallstudien, theoretischen Inhalten und gemeinsamen Diskussionen streben wir danach, innovative Denkansätze für die Entwicklung nachhaltiger Verteidigungsstrategien zu fördern. Rüsten Sie Ihr Unternehmen mit dem Wissen aus, um 0-Day- und 1-Day Angriffe abzuwehren und die Anforderungen der GDPR- und NIS2 Verordnungen zu erfüllen.

Zielgruppe

Dieser Kurs ist für IT-Fachkräfte konzipiert, die ihre Fähigkeiten im Härten von Systemen gegen 0-/1 Day-Schwachstellen und der aktiven Verteidigung vertiefen möchten. Dazu zählen Administratoren, abgehende SOC-Operator und Sicherheitsbeauftragte.

Voraussetzungen

Verständnis von Grundlagen der Cybersicherheit: Die Teilnahme an am Kurs "**Cybersecurity Foundation für IT-Professionals**" wird empfohlen.

Grundlegende Kenntnisse in Programmier- und Skriptsprachen empfohlen: PowerShell, Python, Bash oder Javascript, Erfahrung auf der Windows- oder Linux-Kommandozeile.

Gute Kenntnisse im Betrieb und Management von IT-Seystemen.

Sie verstehen bereits einige gut dokumentierte Standardangriffe und Verteidigungstechniken wie LAPS, BitLocker, Protected Users, Channel Binding, Pass-the-Hash (PTH), Skeleton Key, IPsec und MaQ.

Inhalte des Seminars

Lernen Sie, potenzielle Bedrohungen und Schwachstellen durch umfassende Modellierung zu identifizieren und proaktive Maßnahmen zu ergreifen. Nutzen Sie leistungsfähige Härtungstechnologien moderner Systeme wie **Linux LSMs, Egress-Filtering, Port-Täuschung und das Enterprise Access Model**, um Ihre Systeme zu schützen.

Der Kurs konzentriert sich darauf, Sicherheitslücken gezielt zu schließen, indem Systeme tiefgehend verstanden und angepasste Schutzmaßnahmen implementiert werden. Mit einem **Reverse-Graph-Walk**-Ansatz lernen Sie, wie Sie Ihre wichtigsten Ressourcen schützen, indem Sie potenzielle Sicherheitslücken identifizieren und die Strategien von Angreifern antizipieren. Dabei spielt die Minimierung der **Trusted Computing Base (TCB)** eine entscheidende Rolle. Erkennen und vermeiden Sie gängige Cybersicherheits-Anti-Patterns, die Ihre Bemühungen untergraben könnten.

Während des Kurses implementieren und optimieren wir **Regelwerke und Abfragen für Applocker, osquery, Bloodhound und AppArmor**. Zudem setzen wir Überwachungsmaßnahmen um, die mittels minimaler, schnell umsetzbarer Alarmierung ohne große Logging- und SIEM-Infrastruktur funktionieren. Diese Maßnahmen umfassen die Erkennung und Alarmierung von **RDP- und SSH Angriffen** sowie die Vorbereitung auf Angriffe auf Webanwendungen.

Mit diesem Kurs wollen wir uns von der Fülle an offensiven Kursen, Herstellertrainings und Cyberranges abheben, indem wir die n**ächste Generation kreativer, interdisziplinärer Fachkräfte heranbilden** und fortgeschrittene, realistische Angriffe verhindern.

Im **DFIR-Teil** lernen Sie die Grundlagen der **Event-Analyse** von Windows Logs und den Umgang mit Log-Management und SIEM-Systemen anhand von **Elastic Search** und Zimmerman-Tools.

Einführung

- Compliance und Zertifizierungen
- Commodity-Verteidigungen
- Agilität und Ausgaben
- Produkte und Technologien

Grundkonzepte

- Grundprinzipien
- Bedrohungsmodellierung
- Denken in Graphen wie die Angreifer
- Architektur-Best-Practices
- Anti-Patterns
- Aktive Verteidigung
- Täuschung

Fallstudien

- Praktische Fallstudien
- Architektur Fallstudien

Terminübersicht und Buchung

Buchen Sie Ihren Wunschtermin jetzt direkt online unter https://akademie.tuv.com/s/31491 und profitieren Sie von diesen Vorteilen:

- Schneller Buchungsvorgang
- Persönliches Kundenkonto
- Gleichzeitige Buchung für mehrere Teilnehmer:innen

Alternativ können Sie das Bestellformular verwenden, um via Fax oder E-Mail zu bestellen.