HMTS
HM Training Solutions

INDEPENDENT • INNOVATIVE
INTERNATIONAL

LIVE-ONLINE-KURS

M 64

Ein neuer dreitägiger Kurs in deutscher Sprache

Incident Analysis

Ihre Trainer sind Florian Bausch und Frank Block

Eine Teilnahme am Kurs ist von jedem PC/Laptop mit stabiler Internetverbindung aus möglich. Es wird keine zusätzliche Software benötigt. Wir empfehlen die Verwendung von Google Chrome - falls möglich, andernfalls sind Firefox und Edge auf Chrome Basis unterstützt. Wir empfehlen eine direkte Internetverbindung. Wenn der Zugriff über ein VPN erfolgt, kann es zu qualitativen Einschränkungen kommen, die nicht in unserem Einflußbereich liegen. Auch der Zugriff auf das Training erfolgt über den Browser. Übungen können also ebenfalls realisiert werden, ohne dass zusätzliche Software benötigt wird. Die Schulung wird selbstverständlich live aus dem ERNW-Studio übertragen. Das Kursmaterial, sowie mögliche Demos und natürlich die Trainer sind stets sichtbar und werden je nach Erfordernis gezeigt bzw. hervorgehoben. Das Schulungsmaterial stellen wir Ihnen zusätzlich im Vorfeld elektronisch zur Verfügung. Fragen werden direkt von den Trainern beantwortet. Mikrofon und/oder Kamera sind optional, Sie können die Fragen auch über einen Chat stellen.

Kursbeschreibung

Dieses Seminar behandelt die Incident Analyse, einen Teil des Incident Response Prozesses, und legt dabei den Fokus auf die Analyse und Behandlung von IT-Sicherheitsvorfällen wie APTs oder Ransomware-Kompromittierungen von Windows-Umgebungen. Es wird technisches Hintergrundwissen vermittelt, Software-Werkzeuge vorgestellt, deren Funktionsweise erläutert und anhand praktischer hands-on Übungen die effektive Durchführung einer Incident-Analyse vermittelt. Hierbei werden unterschiedliche, in diesem Kontext relevante, Themenbereiche mit großer technischer Tiefe behandelt. Der Kurs richtet sich daher vorwiegend an Praktiker aus den Bereichen IT-Sicherheit, Incident Response und Incident Analyse.

09. – 11. Mai 2023 – live online

24. – 26. Oktober 2023 – live online

Diese Veranstaltung wird als Weiterbildung bei Rezertifizierungsmaßnahmen von verschiedenen Instituten anerkannt.

HM Training Solutions, Falkenstraße 6 · D-63820 Elsenfeld
Telefon +49 (0) 6022 508 200,Fax +49 (0) 6022 508 9999
E-Mail: info@hm-ts.de – Internet: https://www.hm-ts.de

Incident Analysis

M 64

Ein dreitägiger Kurs in deutscher Sprache

Seminarplan - Inhalte

Erster Tag

Begriffliche Grundlagen
Analyse von Netzwerkverkehr

- ❒ Verbindungsorientiert
- ❒ Pattern basierend
- ❒ Manuell

Korrelation mehrere Logquellen zur genaueren Analyse eines bestimmten Events
Windows Analysis Basics

- ❒ Windows Architektur
- ❒ Analyse relevanter Event Logs
- ❒ Registry Analysis
- ❒ Malware Persistence Techniken

Zweiter Tag

File System Analyse am Beispiel von NTFS

- ❒ Aufdecken und wiederherstellen von gelöschten Dateien
- ❒ Erstellen einer Timeline von Dateisystemaktivitäten
- ❒ Extrahieren von Dateien aus Disk Dump

Malware Analyse – Part 1

- ❒ Tools und Techniken der statischen Analyse
- ❒ Analyse und praktische Durchführung von DLL Injections
- ❒ Analyse von schadhaften PDF- und Word-Dokumenten
- ❒ Dynamische Analyse von JavaScript

Dritter Tag

Malware Analyse – Part 2

- ❒ Shellcode Grundlagen
- ❒ Tools und Techniken der dynamischen Analyse
- ❒ Dynamische Analyse mittels Cuckoo

Memory Analyse mit Volatility

- ❒ Betriebssystem Daten im RAM
- ❒ Malware Hiding/Injection Techniken
- ❒ Analyse ausgewählter Angriffstechniken

Während dieses Kurses lernen Sie, wie man

- Indicators Of Compromise identifiziert,
- Festplatten und Hauptspeicherabbilder forensisch analysiert,
- Malware analysiert und ihr Verhalten nachvollzieht,
- Unterschiedliche Log-Daten auswertet und korreliert.

Wer sollte diesen Kurs besuchen

- Mitglieder eines CERT
- IT-Sicherheitsbeauftragte
- Interessierte an der Thematik

Voraussetzungen

Netzwerk- und Programmier-Erfahrung sind von Vorteil. Für die praktischen Übungen sollte VirtualBox bereits auf dem Laptop vorinstalliert sein und der Teilnehmer für eventuelle Konfigurationen über administrative Rechte auf dem Hostrechner verfügen.

Da der Großteil der Übungen auf der Kommandozeile unter Linux stattfindet, ist Vorerfahrung hier hilfreich, aber nicht notwendig.

Incident Analysis

M 64

Ein dreitägiger Kurs in deutscher Sprache

Profil der Referenten

Florian Bausch studierte Digitale Forensik und schrieb seine Master Thesis über die forensische Analyse von Ceph (Distributed Storage). Seit 2019 arbeitet er als Forensiker und Pentester bei der ERNW Research GmbH.

Frank Block ist Security Researcher bei der ERNW Research GmbH mit mehr als 10 Jahren Erfahrung, und ein externer Doktorand an der Universität Erlangen-Nürnberg (Abteilung Informatik), mit einem Fokus auf Speicher-Forensik. Seine Hauptarbeitsgebiete sind Incident Analysen und Penetrationstests. Darüber hinaus forscht er in verschiedenen Bereichen wobei die Ergebnisse typischerweise auf Konferenzen wie der DFRWS USA, Black Hat USA/EU und Troopers präsentiert werden.

Teilnehmerstimmen zum Kurs

»Ein absolut gut strukturiertes und informatives Seminar. Die Referenten sind super kompetent, freundlich und erklären toll. Das Seminar hat mir viel Spaß gemacht. Danke sehr dafür!«

Hochschulrechenzentrum der Universität Bonn, Vitaly Konchakov

*»Der Kurs bietet einen guten Überblick, welche Quellen es für eine Incident Analyse gibt, gibt Anregungen zu einer professionellen Dokumentation, geht aber auch technisch in die Tiefe und bietet einen guten Einstieg in statische und dynamische Malware Analyse. Ebenfalls erhält man einen guten Einblick in Memory Forensik. Die Referenten wissen, wovon sie sprechen und können ihr Wissen gut an die Teilnehmer*innen transportieren. Technisches Vorwissen bei den Teilnehmer*innen ist zwar nicht notwendig, aber von Vorteil.«*

Magdalena Kurek, Security Engineer, Twinformatics, Wien

»Hervorragender Kurs. Gute Steigerung in der Lernkurve. Dozenten haben sehr frei gesprochen. Daran hat gut man gemerkt, dass sie wissen wovon sie reden.«

Tom Reisenberg, Sachgebietsleiter SOC und Analyst,
Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH

»Ein spannendes Seminar – vielen Dank!«

Dipl. Wirt.-Inf. Michael Raith, Informationssicherheitsbeauftragter / CISO; Stabsabteilung Recht, Compliance, Revision;
Medizinische Einrichtungen des Bezirks Oberpfalz, Regensburg

HM TRAINING SOLUTIONS ON-SITE SERVICE

Alle HM Training Solutions Seminare stehen auch firmenintern zur Verfügung. Sie können auf den Bedarf Ihrer Organisation zuge schnitten werden. Weitere Details erhalten Sie unter der Telefonnummer +49 (0) 6022 508 200.

DETAILS ZUM ANMELDEFORMULAR

Vier Wege zur Anmeldung

Per Post: Bitte dieses Anmeldeformular ausfüllen und an HM Training Solutions senden.
Per E-Mail: **Info@hm-ts.de**
Per Webseite: **https://www.hm-ts.de**

Gebühren

2.690 € + 19% MwSt..

Bestätigungsbrief

Ihre Anmeldung bestätigen wir per Mail oder Brief.
Er enthält Details über die Veranstaltung. Der Kurspreis enthält die Seminardokumentation, Zugriff auf die Online-Plattform sowie die Ausstellung eines Zertifikats.

Änderungen

HM Training Solutions behält sich das Recht vor, bei Eintreten nicht vorhersehbarer Umstände das Seminar räumlich und/oder zeitlich zu verlegen, einen anderen Referenten ersatzweise einzusetzen oder die Veranstaltung zu stornieren. Weitergehende Ansprüche bestehen nicht.

Stornierung seitens des Teilnehmers

Bitte reichen Sie Stornierungen schriftlich per Post oder Email (info@hm-ts.de), ein. Bestätigte Anmeldungen können bis zu sechs Wochen vor Seminarbeginn kostenfrei storniert werden, danach berechnen wir die gesamte Seminargebühr. Eine Übertragung an einen Ersatzteilnehmer ist jederzeit möglich.

Firmeninterne Seminare

Alle Trainings von HM Solutions können auch firmenintern und zugeschnitten auf den Bedarf der jeweiligen Organisation durchgeführt werden. Weitere Informationen erhalten Sie unter der Telefon-Nr. +49 (0) 6022 508 200.

Die Teilnehmerzahl ist begrenzt. Wir berücksichtigen Ihre Anmeldung in der Reihenfolge des Eingangs.

ANMELDEFORMULAR

Incident Analysis

- ❒ **09. – 11. Mai 2023 – live online**
- ❒ **24. – 26. Oktober 2023 – live online**

❒ Bitte reservieren Sie _____ Platz/Plätze
zum Einzelpreis von 2.690 €+ 19% MwSt..

Wir senden Ihnen die Kursdokumentation als pdfs vor Kursbeginn zu!

Herr/Frau Vorname Nachname

_____

Funktion _____

Firma _____

Adresse _____

_____

_____

Postleitzahl _____ Ort _____

Land _____

Telefonnummer _____

Mobilfunknummer _____

E-Mail _____

Unterschrift _____

BUCHUNGSREFERENZ M64

Zahlung

❒ Bitte um Rechnungsstellung

Rechnungsadresse (falls nicht identisch mit obiger Anschrift).

_____

_____

_____

PO-Nummer _____

Zusätzliche Teilnehmer

1. Herr/Frau Vorname Nachname

_____

Funktion _____

E-Mail _____

2. Herr/Frau Vorname Nachname

_____

Funktion _____

E-Mail _____

3. Herr/Frau Vorname Nachname

_____

Funktion _____

E-Mail _____