HMTS
HM Training Solutions

INDEPENDENT • INNOVATIVE
INTERNATIONAL

LIVE-ONLINE-KURS

M 64

Incident Analysis

Lernen von den Profis – Ihre Referenten sind Florian Bausch, Justus Hoffmann und Lucas Wenzel

Kursbeschreibung

Dieses Seminar behandelt Grundlagen (Tage 1 bis 3) und fortgeschrittene Themen (Tage 4 und 5) der Incident-Analyse als Teil des Incident-Response-Prozesses. Dabei wird neben der Darstellung des notwendigen technischen Hintergrundwissens auch großer Wert auf die Vermittlung unmittelbar anwendbarer praktischer Fertigkeiten gelegt. Dazu werden verschiedenste (insbesondere frei verfügbare) Software-Werkzeuge vorgestellt, deren Funktionsweise erläutert und anhand praktischer Hands-on-Beispiele die effektive Durchführung konkreter Incident-Analyse-Schritte eingeübt.

Im Grundlagenteil des Kurses (Tage 1 bis 3) erfolgt eine breitgefächerte Einführung in verschiedenste, in diesem Kontext relevante Themenbereiche, Techniken und Vorgehensweisen. Ein besonderer Fokus wird dabei auf die Untersuchung typischer, weitverbreiteter Incident-Szenarien wie die Ransomware-Kompromittierung einer Windows-Active-Directory-Umgebung gelegt.

Im Fortgeschrittenenteil des Kurses (Tage 4 und 5) werden tiefergehende Fertigkeiten der Analyse und Behandlung von IT-Sicherheitsvorfällen in Windows- und Linux-Umgebungen vermittelt. Diese beinhalten beispielsweise fortgeschrittene Techniken der Malware-Analyse wie den Einsatz eines Debuggers/Disassemblers/Decompilers und die Gewinnung von Incidators of Compromise (IoCs) aus Arbeitsspeicherdumps von physischen oder virtuellen Maschinen.

Der Kurs richtet sich vorwiegend an Praktiker aus den Bereichen IT-Sicherheit, Incident Response und Incident Analyse und wird wegen des hohen Praxisanteils durchgehend von drei Referenten durchgeführt.

Kurs Grundlagen Live-Online

25. - 27.11.2024 | 10. - 12.02.2025 | 31.03.-02.04.25 | 07. - 09.07.2025

Kurs Fortgeschritten Live-Online

28. - 29.11.2024 | 13. - 14.02.2025 | 03.-04.04.2025 | 10. - 11.07.2025

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

Kursteil „Grundlagen“ (Tage 1 bis 3)

Agenda

Tag 1

Begriffe und Grundlagen

- ❒ Attack Lifecycle
- ❒ Analysestrategien
- ❒ Timelines
- ❒ Indicators of Compromise (IoCs)

Analyse von Netzwerkverkehr

- ❒ Datenquellen und Datenformate
- ❒ Korrelation mehrerer Logquellen

Dateisystemanalyse

- ❒ Erstellung von Dateisystemimages
- ❒ File Carving
- ❒ Erstellen einer Timeline von Dateisystemaktivitäten
- ❒ Extrahieren von Dateien aus Disk Dumps
- ❒ Aufdecken und Wiederherstellen von gelöschten Dateien

Tag 2

Windows Analysis Basic

- ❒ Registry
- ❒ Windows Event Logs
- ❒ Malware Persistence Techniken
- ❒ Spuren ausgeführter Programme (Evidence of Execution)

Active Directory Basics

- ❒ Architektur
- ❒ Authentifizierung
- ❒ Angriffe und Angriffserkennung

Static Document Analysis

- ❒ PDF
  - Dateiformat und Analyse
  - Extrahieren von bösartigem Code
- ❒ MS-Office
  - Dateiformat und Analyse
  - Extrahieren von Macros und bösartigem Code

Tag 3

Analyse von PE-Dateien (EXE, DLL etc.)

- ❒ Dateiformat und statische Analysewerkzeuge
- ❒ Malwaretypische Windows API-Funktionen
- ❒ Erstellung und Nutzung von YARA-Regeln

DLL Injection

- ❒ Analyse und praktische Durchführung von DLL Injections
- ❒ Erkennung von DLL Injection und Process Hollowing

Automatisch-Dynamische Malwareanalyse mittels Sandbox-Lösungen

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.

Incident Analysis

M 64

Kursteil „Fortgeschritten“ (Tage 4 bis 5)

Agenda

Tag 4

Erweiterte Dateisystemanalyse

- Linux-Dateisysteme
- Analyse von ext-Dateisystemen
- Auswertung von Dateisystem-Journals

Linux Analysis Basics

- Angreifer-Persistenz auf Linux-Systemen
- Logs und andere Datenquellen für die Analyse

Decompiler

- Dekompilieren von Maschinencode und Bytecode
- Workflow und Strategien bei der Analyse
- Potenzielle Probleme und Tricks

Shellcode

- Grundlagen der Shellcodeanalyse

Tag 5

Dynamische Malwareanalyse

- Werkzeuge und Techniken für die dynamische Malwareanalyse
- Analyse mittels Sysinternals Tools, Debuggern und Sandboxen

Memory Analysis

- Betriebssystemdaten im RAM
- Malware Hiding/Injection Techniken
- Analyse ausgewählter Angriffstechniken

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.

Incident Analysis

M 64

Während dieses Kurses lernen Sie unter anderem, wie man

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

Wer sollte diesen Kurs besuchen

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

Inhaltliche Voraussetzungen

Netzwerk- und (grundlegende) Programmier-Erfahrung sind von Vorteil. Da ein Großteil der Übungen auf der Kommandozeile unter Linux stattfindet, ist entsprechende Vorerfahrung hier hilfreich, aber nicht zwingend notwendig.

Technische/Organisatorische Voraussetzungen

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.

Incident Analysis

M 64

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.

Justus Hoffmann ist ursprünglich Dipl.-Ing. Elektrotechnik und Informationstechnik, im Laufe der Zeit hat er sich dem Themengebiet IT-Sicherheit zugewandt.
Seit 2021 arbeitet er bei der ERNW Research GmbH als Incident Analyst und Pentester.

Lucas Wenzel studierte IT-Sicherheit und Informationstechnik an der Ruhr-Universität Bochum und schrieb seine Abschlussarbeit über die Effizienz von Mitigationen zu Hardware Schwachstellen auf tiefgehender Betriebssystemebene. Seit 2024 arbeitet er bei der ERNW Research GmbH als Security Analyst und Incident Responder.

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

»Der Kurs war sehr spannend, extrem gut aufbereitet, sehr anschaulich und es wird nicht der letzte Kurs gewesen sein den ich wahrnehme.«

Darius Happe, IT-Security Manager, rku.it GmbH, Herne

»Ausgezeichneter Überblick über Thema, Techniken und Tools. Richtige Balance zwischen Überblick/Details und Theorie/Praktische Übungen.«

Markus Lauer, Beratung und Entwicklung, DIaLOGIKa — Gesellschaft für angewandte Informatik mbH, Saarbrücken

»Ein sehr spannender Kurs und Praxis nah aufgebaut. Die Referenten sind fachlich wie persönlich „eins a“ und kann den Kurs nur weiterempfehlen. Für mich hat sich das Seminar gelohnt und kann das Gelernte in den Alltag überführen – vielen Dank!«

Martin Zeindler, Leiter Operations Management, Emmi Schweiz AG

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

3-tägiger Kurs Grundlagen
2.950,– € + 19% MwSt.

2-tägiger Kurs Fortgeschritten
2.290,– € + 19% MwSt.

5-tägiger Kurs (Grundlagen und Fortgeschritten)
4.980,– € + 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 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

(M 64 Grundlagen)

- ❒ **3 Tage: 25. – 27. November 2024**
- ❒ **3 Tage: 10. – 12. Februar 2025**
- ❒ **3 Tage: 31. März – 02. April 2025**
- ❒ **3 Tage: 07. – 09. Juli 2025**

❒ Bitte reservieren Sie _____ Platz/Plätze für den Live-Online-Kurs M64 Grundlagen zum oben ausgewählten Termin **zum Einzelpreis von 2.950,– €** + 19% MwSt.

(M 64 Fortgeschritten)

- ❒ **2 Tage: 28. – 29. November 2024**
- ❒ **2 Tage: 13. – 14. Februar 2025**
- ❒ **3 Tage: 03. – 04. April 2025**
- ❒ **3 Tage: 10. – 11. Juli 2025**

❒ Bitte reservieren Sie _____ Platz/Plätze für den Live-Online-Kurs M64 Fortgeschritten zum oben ausgewählten Termin **zum Einzelpreis von 2.290,– €** + 19% MwSt.

(M 64 Grundlagen und Fortgeschritten)

- ❒ **5 Tage: 25. – 29. November 2024**
- ❒ **5 Tage: 10. – 14. Februar 2025**
- ❒ **5 Tage: 31. März – 04. April 2025**
- ❒ **5 Tage: 07. – 11. Juli 2025**

❒ Bitte reservieren Sie _____ Platz/Plätze für die beiden Live-Online Kurse M64 Grundlagen und Fortgeschritten zum oben ausgewählten Termin **zum Einzelpreis von 4.980,– €** + 19% MwSt.

Wir senden Ihnen die Kursdokumentation vor Kursbeginn und die Folien nach Kursende zu.

Hiermit melde ich folgende(n) Teilnehmer zum Live-Online-Kurs an:

Herr/Frau Vorname Nachname

_____

Funktion _____

Firma _____

Adresse _____

_____

_____

Postleitzahl _____ Ort _____

Land _____

Telefonnummer _____

Mobilfunknummer _____

E-Mail _____

Unterschrift _____

Zusätzliche Teilnehmer

Kurs Grundlagen

Herr/Frau Vorname Nachname

_____

Funktion _____

E-Mail _____

Herr/Frau Vorname Nachname

_____

Funktion _____

E-Mail _____

Herr/Frau Vorname Nachname

_____

Funktion _____

E-Mail _____

Kurs Fortgeschritten

Herr/Frau Vorname Nachname

_____

Funktion _____

E-Mail _____

Herr/Frau Vorname Nachname

_____

Funktion _____

E-Mail _____

Herr/Frau Vorname Nachname

_____

Funktion _____

E-Mail _____

Kurs Grundlagen und Fortgeschritten

Herr/Frau Vorname Nachname

_____

Funktion _____

E-Mail _____

Herr/Frau Vorname Nachname

_____

Funktion _____

E-Mail _____

Herr/Frau Vorname Nachname

_____

Funktion _____

E-Mail _____

Zahlung

BUCHUNGSREFERENZ M 64

❒ Bitte um Rechnungsstellung

Rechnungsadresse (falls nicht identisch mit obiger Anschrift).

_____

_____

_____

PO-Nummer _____