HMTS
HM Training Solutions

INDEPENDENT • INNOVATIVE
INTERNATIONAL

ONLINE WORKSHOP

M 64

Ein neuer dreitägiger Workshop in deutscher Sprache

Incident Analysis

Ihre Trainer sind Andreas Dewald und Frank Block

Eine Teilnahme am Workshop ist von jedem PC/Laptop/Tablet mit stabiler Internetverbindung aus möglich. Es wird keine zusätzliche Software benötigt, ein aktueller Browser genügt (aktueller Microsoft Edge, Google Chrome oder Firefox). Auch der Zugriff auf das Trainings-Lab 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 Workshopmaterial, 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 ist ein praktischer Incident Response Workshop, der sich auf die Analyse und Behandlung von IT-Sicherheitsvorfällen wie APTs oder Emotet-Kompromittierungen von Windows-Umgebungen konzentriert.
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.

23. – 25. Juni 2020

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 Workshop 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 Workshop in deutscher Sprache

Profil der Referenten

Andreas Dewald ist IT-Security Researcher und Geschäftsführer der ERNW Research GmbH. Außerdem ist er assoziierter Post-Doc an der Friedrich-Alexander Universität Erlangen-Nürnberg (FAU), wo er von 2012 bis Januar 2016 als Forscher und Dozent tätig war. Er beschäftigt sich in Forschung und Profession mit allen Bereichen der IT-Sicherheit, mit einem besonderen Schwerpunkt auf die Forensische Informatik und Incident Response.

Von 2013 bis 2016 leitete er an der FAU die Forschungsgruppe „Applied Forensic Computing“, nachdem er seine Promotion im Dezember 2012 unter der Betreuung von Prof. Dr.-Ing. Felix Freiling mit der Dissertation „Formalisierung digitaler Spuren und ihre Einbettung in die Forensische Informatik“ als Doktor der Ingenieurwissenschaften (Dr.-Ing.) abgeschlossen hatte.

Bis Oktober 2013 betreute er von Seiten der FAU den ersten deutschen Master-Studiengang in digitaler Forensik, der in einem Kooperationsprojekt an der Hochschule Albstadt-Sigmaringen angeboten wird.

Von August 2009 bis April 2012 war Andreas Dewald wissenschaftlicher Mitarbeiter am Lehrstuhl für praktische Informatik 1 für IT-Sicherheit der Universität Mannheim.

Zuvor hatte er an der Universität Mannheim Informatik mit Schwerpunkt IT-Sicherheit studiert. Für seine Diplomarbeit „Detection and Prevention of Malicious Websites“ erhielt er 2010 den Wissenschaftspreis der Gesellschaft für Datenschutz und Datensicherheit.

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.

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

Drei Wege zur Anmeldung

Per Post: Bitte dieses Anmeldeformular ausfüllen und an HM Training Solutions senden.
Per Fax: Bitte dieses Formular an folgende Faxnummer senden: +49 (0) 6022 508 9999.
Per E-Mail: **Info@hm-ts.de**

Gebühren

€ 2.200 € +19% Mehrwertsteuer

Bestätigungsbrief

Ihre Anmeldung bestätigen wir per Mail oder Brief.
Er enthält Details über die Veranstaltung.

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 Fax, Fax-Nr. +49 (0) 6022 508 9999, ein. Bestätigte Anmeldungen können bis zu sechs Wochen vor Seminarbeginn kostenfrei storniert werden, danach berechnen wir die gesamte Seminar - gebühr. 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

❒ **23. - 25. Juni 2020**

❒ Bitte reservieren Sie _____ Platz/Plätze
zum Einzelpreis von 2.200 € +19% Mwst.

Wir senden Ihnen die Kursdokumentation als pdfs vor Kursbeginn zu!

Herr/Frau Vorname Nachname

_____

Funktion _____

Firma _____

Adresse _____

_____

_____

Postleitzahl _____

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 _____

2. Herr/Frau Vorname Nachname

_____

Funktion _____

3. Herr/Frau Vorname Nachname

_____

Funktion _____