HMTS
HM Training Solutions

INDEPENDENT • INNOVATIVE
INTERNATIONAL

LIVE-ONLINE-KURS

M 70

Ein neuer zweitägiger Kurs in deutscher Sprache

Google Cloud (GCP) Incident Response & Analysis

Lernen von den Profis – Ihre Trainer sind Ann-Marie Belz und Florian Bausch.

Kursbeschreibung

Die Cloud bietet Flexibilität – sowohl für den IT-Betrieb sondern auch für Angreifer. Wegen der Flexibilität wird immer mehr Infrastruktur von *on-premise* in die Cloud umgezogen. Angreifer finden daher immer mehr lohnenswerte Ziele vor, die nicht immer optimal geschützt sind. Doch egal, wie gut die Cloudumgebungen gehärtet werden, für IT-Sicherheitsteams steht früher oder später die Frage im Raum, wie Incident Response und IT-Forensik in den Cloud-Umgebungen sinnvoll und effizient durchgeführt werden können, um beispielsweise zu klären, ob ein Angriffs erfolgreich war, ob ein Zugriff und Exfiltration auf Daten erfolgt ist und wie darauf reagiert werden muss.

Der Kurs liefert das erforderliche Verständnis der Google Cloud Platform (GCP); darauf aufbauend werden mögliche Angriffe auf GCP-Projekte, deren Spuren, typische blinde Flecken, Analysemethoden, Werkzeuge und proaktive Maßnahmen aufgezeigt. Der Fokus liegt auf GCP, da diese public Cloud häufig eingesetzt wird, jedoch die hier behandelten Fragestellungen meist nicht betrachtet werden. Im Kurs betrachten wir, wie eine Fehlkonfiguration zur Privilege Escalation zum Project Owner ablaufen könnte. Auf dem Weg kompromittiert der Angreifer verschiedene Ressourcen eines GCP Projects, um auch längerfristig Zugang zur Infrastruktur zu behalten, falls diese Backdoors nicht erkannt und bereinigt werden. Wir gehen schrittweise durch die Angriffskette, führen einzelne Schritte selbst aus und analysieren die entstandenen Spuren. Auch die Analyse-Werkzeuge werden schrittweise aufgebaut, um nach und nach einen besseren Überblick über den gesamten Angriffsablauf zu erhalten und den Teilnehmern zu ermöglich künftig in ihrem eigenen Umfeld die erforderlichen Vorraussetzungen zu schaffen und Ansätze des Kurses zu übernehmen.

28. - 29. Januar 2026 - 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

Google Cloud (GCP) Incident Response & Analysis

M 70

Ein neuer zweitägiger Kurs in deutscher Sprache

Kursinhalte

Der Kursinhalt verteilt sich auf zwei Tage.

Tag 1:

- Einführung in GCP (Projekte, Organsationen etc.)
- Authentifizierung und IAM
  - Nutzer und Service Accounts
  - Rollenkonzept
- Einfache forensischer Analysen in GCP
  - Erstellen von Images von (laufenden) VMs
  - Auswerten vorhandener Logs

Tag 2:

- Aufbau einer forensischen Umgebung in GCP, z. B. mit
  - Packet Mirroring
  - Ressourcen
  - Werkzeugen
- Containment & Eviction
  - Maßnahmen, um einen Angriff zu unterbinden
  - Maßnahmen, um einen Angreifer „rauszuwerfen“
- Weitere / Proaktive Maßnahmen
  - Härtung
  - Überwachung

Warum Sie diesen Kurs besuchen sollten

- Der Kurs vermittelt grundlegende Mechanismen und Maßnahmen, um sicherheitsrelevante (forensische) Analysen und Incident Response in GCP durchzuführen.
- Das Verständnis im Bezug auf GCP hilft beim Verständnis ähnlicher Aufgaben in anderen public Clouds.
- Das Wissen über blinde Flecken und diverse Angriffsvektoren hilft bereits bei proaktiven Maßnahmen, nicht erst nach erfolgreichen Angriffen.

Wer sollte diesen Kurs besuchen

- MitarbeiterInnen von CERTs/SOCs/…, die Analysen in (Google) Cloud-Projekten durchführen werden
- IT-Security Spezialisten für die Incidents in einer GCP Umgebung relevant werden könnten
- IT-ForensikerInnen, die einen Einblick in die Cloud gewinnen möchten
- CISOss, IT Krisenmanager, Incident Manager

Grundlagen, die für den Kurs vorteilhaft sind

- Grundlegendes Wissen im Bereich IT-Forensik
- Grundlegendes Wissen im Bereich Pentests/ Readteaming
- Erfahrung im Umgang mit Kommandozeilen (vor allem Bash auf Linux)
- Grundlegendes Wissen im Bereich public Cloud (z. B. Azure, AWS, GCP)
- Wissen über IP-Netzwerke
- Diese Grundlagen sind für eine Teilnahme nicht zwingend erforderlich, fördern aber den Lernerfolg während des Kurses.

Teilnahmevoraussetzungen

- Der Kurs wird über ein Microsoft-Teams-Meeting durchgeführt.
- Es wird eine Laborumgebung bereitgestellt, die über SSH und den Browser genutzt werden kann.

Eine Teilnahme am Kurs ist von jedem PC/Laptop mit stabiler Internetverbindung aus möglich. Es wird keine zusätzliche Software benötigt. Wir empfehlen die Nutzung eines aktuellen Browsers und 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 durchgeführt 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.

HM TRAINING SOLUTIONS ON-SITE SERVICE

Alle HM Training Solutions Seminare stehen auch firmenintern zur Verfügung. Sie können auf den Bedarf Ihrer Organisation zugeschnitten werden. Der Kurs kann auf Wunsch firmenintern in englischer Sprache gegen Aufpreis durchgeführt werden. Weitere Details erhalten Sie unter der Telefonnummer +49 (0) 6022 508 200.

Google Cloud (GCP)
Incident Response & Analysis

M 70

Ein neuer zweitägiger Kurs in deutscher Sprache

Profil der Seminarleiter

Ihre Trainerin, Ann-Marie Belz arbeitet als IT Security Consultant bei der ERNW Research GmbH. Sie absolvierte ihr Bachelor- und Masterstudium im Bereich Medizinische Informatik, wodurch sie interdisziplinäre Einblicke in IT, Medizin und Sicherheitstechnologien gewann. In ihrer Abschlussarbeit legte sie den Fokus auf die automatische Erkennung von Kompromittierungen in Festplatten-Images und sammelte dadurch Erfahrungen in den Bereichen Incident Analyse und digitale Forensik.

Ihr Trainer, Florian Bausch studierte Digital Forensics und schrieb seine Masterthesis über forensische Analyse von verteiltem Ceph-Speicher. Seit 2019 arbeitet er bei ERNW Research GmbH als Pentester und Incident Analyst.

© 2025 HM Training Solutions. Ohne unsere ausdrückliche Genehmigung darf keine Vervielfältigung dieser Broschüre erfolgen.

Google Cloud (GCP) Incident Response & Analysis

M 70

Ein neuer zweitägiger Kurs in deutscher Sprache

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

Kurs **2.290,– €** + 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.

© 2025 HM Training Solutions. Ohne unsere ausdrückliche Genehmigung darf keine Vervielfältigung dieser Broschüre erfolgen.

Google Cloud (GCP)
Incident Response & Analysis

M 70

Ein neuer zweitägiger Kurs in deutscher Sprache

ANMELDEFORMULAR

Google Cloud (GCP)
Incident Response & Analysis

❒ **2 Tage: 28. - 29.01.2026 - LIVE ONLINE**

❒ Bitte reservieren Sie _____ Platz/Plätze für den LIVE ONLINE-Kurs M 70 Google Cloud (GCP) zum oben ausgewählten live online-Termin **zum Einzelpreis von 2.290,– €** + 19% MwSt.

Herr/Frau Vorname Nachname

_____

Funktion _____

Firma _____

Adresse _____

_____

_____

Postleitzahl _____ Ort _____

Land _____

Telefonnummer _____

Mobilfunknummer _____

E-Mail _____

Unterschrift _____

Zusätzliche Teilnehmer

Herr/Frau Vorname Nachname

_____

Funktion _____

E-Mail _____

Herr/Frau Vorname Nachname

_____

Funktion _____

E-Mail _____

Herr/Frau Vorname Nachname

_____

Funktion _____

E-Mail _____

Zahlung

BUCHUNGSREFERENZ HM 70

❒ Bitte um Rechnungsstellung

Rechnungsadresse (falls nicht identisch mit obiger Anschrift).

_____

_____

_____

PO-Nummer _____

© 2025 HM Training Solutions. Ohne unsere ausdrückliche Genehmigung darf keine Vervielfältigung dieser Broschüre erfolgen.