Tagesveranstaltung

Machine Learning in Cyber Security

Entdecken Sie die Möglichkeiten und den Nutzen von Machine Learning in der Cyber Security: Schützen Sie Systeme effektiver, erkennen Sie Bedrohungen smarter und erweitern Sie Ihr Fachwissen. In diesem Seminar lernen Sie in einem Grundlagen- und einem Anwendungsteil mit konkretem Use Case, wie Machine Learning effektiv zur Verbesserung der Cyber Security eingesetzt werden kann.

Berner
Fachhochschule

Portrait

In dieser eintägigen Lehrveranstaltung lernen Sie, wie Machine Learning (ML) effektiv zur Verbesserung der Cybersecurity eingesetzt werden kann.

Der erste Teil besteht aus einer Einführung in die Grundlagen des maschinellen Lernens. Aktuelle Anwendungsbereiche wie Anomalieerkennung, Malware-Klassifikation und Phishing-Prävention werden vorgestellt und es wird Kenntnis der notwendigen technischen Hilfsmittel vermittelt.

Der zweite Teil umfasst eine vertiefte praktische Übung zur selbstständigen Anwendung von Machine Learning in einem vorbereiteten Cybersecurity-Anwendungsfall gemäss NIST Framework (Identify, Protect, Detect, Respond, Recover). Abschliessend werden die Ergebnisse gemeinsam besprochen, Fragen beantwortet und das Erlernte gefestigt.

Theorie und Übungen werden ineinander verwoben, so dass Sie optimal für die praktische Anwendung profitieren können.

Zielpublikum

Die Veranstaltung richtet sich an Fachpersonen im Bereich Cybersecurity mit Interesse an Machine Learning. Fachleute aus Data & AI mit Vorkenntnissen in Machine Learning und Interesse an Cybersecurity sind ebenfalls willkommen.

Ausbildungsziele

- Wissen & Verstehen
  - Kenntnis verschiedener ML-Methoden und deren Anwendungsfälle
  - Verständnis der Funktionsweise & Anwendbarkeit einer spezifischen ML-Methode
  - Kenntnis von Tools & technischen Hilfsmitteln zum Einsatz von ML
- Anwenden von Wissen & Verstehen
  - selbstständiges Anwenden der vermittelten ML-Methode auf eine konkrete Aufgabenstellung
  - freie Zuhilfenahme der vorgestellten Tools & technischen Hilfsmittel
- Urteilen:
  - Beurteilung der Anwendbarkeit von ML-Techniken auf verschiedene Problemstellungen
  - Beurteilung der Ergebnisse von ML im Use Case

Voraussetzungen

- Verständnis für Cybersecurity, NIST Framework (Identify, Protect, Detect, Respond, Recover)
- Vorgängige Berührungspunkte mit Shell, Python, Betriebssysteme

Steckbrief

Tagung	Machine Learning & Cyber Security
Dauer	1 Tag
Datum	Dienstag, 17. Juni 2025, 9.00–16:30 Uhr
Kosten	CHF 190
Anzahl ECTS	keine
Unterrichtssprache	Deutsch, Unterlagen teilweise in Englisch
Durchführungsort	Switzerland Innovation Park, Aarbergstrasse 46, 2503 Biel

Kursinhalt

- Motivation & Übersicht der Machine-Learning-Methoden
- Vertiefung einer Machine-Learning-Methode spezifisch für den praktischen Anwendungsfall
- praktische Anwendung von ML auf einen Use Case
- Analyse der Ergebnisse, Lessons Learned

Organisation

Dozent
Benedict Simlinger
BFH/eraneos
E-Mail: benedict.simlinger@bfh.ch

Leitung BFH
Prof. Dr. Arno Schmidhauser
Tel: +41 31 848 32 75
E-Mail: arno.schmidhauser@bfh.ch

Berner Fachhochschule
Technik und Informatik
Weiterbildung
Aarbergstrasse 46 (Switzerland Innovation Park Biel/Bienne)
2503 Biel/Bienne

Telefon +41 31 848 31 11
E-Mail: weiterbildung.ti@bfh.ch
Web: bfh.ch/ti/weiterbildung

Berner
Fachhochschule