HACK2IMPROVE

Red vs Blue

ONE-DAY HACKING AND DEFENDING WORKSHOP

Sie möchten Ihr Knowhow im Bereich Netzwerk-Security schärfen und einen 360 °-Blick auf Angriffs-Szenarien einnehmen?
Dann laden wir Sie herzlich zu unserem 12.ten Hack2Improve-Workshop ein.

Es wurden keine Alarme entdeckt, aber es gibt Angreifer im Netzwerk.
In dieses Workshop schlüpfen Sie in die Rolle eines Sicherheitsanalysten und müssen Bedrohungen identifizieren, die im Netzwerk unentdeckt bleiben. Dazu nutzen Sie Mitre ATT&CK™, eine Wissensbasis über das Verhalten von Angreifern, die auf realen Beobachtungen beruht. ATT&CK™ ermöglicht es Analysten, nach Verhaltensmustern zu suchen und nicht nach Artefakten wie Hashes, IPs oder Domains.

Warum ist das wichtig?
Laut der „'The Pyramid of Pain" von David Bianco ist es für Angreifer zwar sehr einfach, diese Artefakte zu ändern, aber es ist viel schwieriger für sie, ihre Taktiken, Techniken und Verfahren (TTPs) zu ändern. Daher sind TTPs ein zuverlässigeres Mittel, um das Verhalten der Angreifer zu identifizieren.

Die Herausforderung im zweiten Teils des Workshop besteht aus mehreren Übungen, die sich an den technischen Zielen orientieren, die der Angreifer zu erreichen versucht (ATT&CK™-Taktiken), z. B. Erstzugriff, Persistenz, Privilegieneskalation, Befehl und Kontrolle. Sie werden aufgefordert, alle Techniken zu erkennen, die von einem Angreifer zur Erreichung dieser Ziele eingesetzt werden.

Der Workshop besteht aus zwei Phasen:

Phase 1

Angriff & Threat Hunt Walkthrough

- Sie führen verschiedene Techniken von Bedrohungsakteuren aus und wechseln dann in die Rolle eines Sicherheits-analysten, um nach den verwendeten Techniken zu suchen
- Dies dient dazu, sich mit den Techniken vertraut zu machen und zu erfahren, wie man sie mit Tools aus EDR, SIEM und Deception mittels Fortinet aufspüren kann

Phase 2

Herausforderung

- Sie jagen nach Bedrohungen, die bereits von einem fiktiven Bedrohungsakteur durchgeführt wurden, indem Sie die Tools und Jagdtechniken verwenden, die Sie im ersten Teil gelernt haben
- Da es sich um eine Herausforderung handelt, erhalten Sie nur minimale Anweisungen, aber es gibt Hinweise, wenn Sie diese benötigen

Interesse geweckt?

Dann schnellstens anmelden!

Anmeldeblatt kurz ausfüllen und im Sekretariat IN abgeben.