



SecCore

Purple Team Exercises

Purple Teaming verbindet die Perspektiven von **Red Team** (Angreifer) und **Blue Team** (Verteidiger), um die Erkennung und Reaktion auf Cyberangriffe gezielt zu verbessern.

Die Übungen in enger Zusammenarbeit mit Ihrem Security Operations Center (SOC) simulieren realistische Angriffe entlang der Unified Kill Chain, wie **Initial Access** (erster Zugriff auf ein System), **Lateral Movement** (Ausbreitung im Netzwerk)

oder **Data Exfiltration** (Abfluss sensibler Daten). Diese Szenarien zeigen, wie gut Ihre Sicherheitsmaßnahmen Angriffe erkennen und stoppen.

Wir entwickeln **Indicators of Compromise (IoCs)**, optimieren **Erkennungsregeln für SIEM/EDR** und verbessern **Incident-Response-Playbooks** für schnellere Reaktionen. So entsteht ein praxisnaher Lernprozess, der Ihr Team befähigt, echte Bedrohungen schneller zu erkennen und wirksamer abzuwehren.

Tabletop Exercise

Was sind die Inhalte der Übung?

Gemeinsames, theoretisches Durchspielen vordefinierter Angriffsszenarien. Der Fokus liegt auf Planung, Rollen, Abläufen und Entscheidungswegen.

Wann ist die Übung sinnvoll?

Ideal zum Aufbau oder zur Überprüfung grundlegender SOC-Konzepte. Hilft, Verantwortlichkeiten und Prozesse klar zu definieren.

Dauer

Ab 2 Arbeitstagen

Detection Engineering

Ausarbeitung realistischer Angriffsszenarien (technische Durchführung durch uns). Gemeinsam werden bestehende Erkennungsregeln optimiert und neue Alarmierungsregeln entwickelt.

Für Unternehmen, die Detection-Regeln entwickeln oder verfeinern möchten. Insbesondere für SOCs im Aufbau oder mit Entwicklungsbedarf.

Ab 5 Arbeitstagen

Adversary Emulation

Simulation realer TTPs (Tactics, Techniques & Procedures) bekannter Angreifergruppen. Dabei wird die gesamte Alarmkette analysiert und Blind Spots werden identifiziert.

Für reife SOCs, die ihre Detection-Fähigkeiten unter realistischen Bedingungen testen und letzte Lücken schließen wollen.

Ab 9 Arbeitstagen

Sie wollen wissen, wie gut Ihre Systeme wirklich geschützt sind? Wir liefern die Antwort!

Kontaktieren Sie uns für Ihr unverbindliches Angebot: