Portfolio

RED- UND PURPLE-TEAMING BERATUNGSBUDGET

Unsere Red-Team-Spezialisierten prüfen für Sie relevante Angriffsvektoren praktisch oder in Tabletop-Übungen mit Ihnen gemeinsam.

Durch eine Kombination aus Tabletop-Übungen und –Analysen sowie ausgewählten praktischen Red-Teaming-Tests lässt sich die Effektivität Ihrer eingesetzten IT-Sicherheitslösungen zielgerichtet überprüfen. Die Verknüpfung dieser Vorgehensweisen erlaubt ein sehr wirtschaftliches Vorgehen und eine gezielte Untersuchung der Fragestellungen zur Angriffserkennung, die für Ihr Unternehmen wirklich relevant sind.

BERATUNGSKONTIGENT

Der Einsatz unserer Expertinnen und Experten über ein Beratungsbudget erlaubt Ihnen den flexiblen Abruf der gewünschten Tests und Projektinhalte bei maximaler Budget-Kontrolle und zielgerichtetem Ressourceneinsatz.

Die Prüfungen erlauben die detaillierte Betrachtung einzelner Aspekte aus der Angreifenden-Perspektive und sparen unnötigen Overhead ein.

Durch die offene Vorgehensweise bei der Planung der Szenarien können zusätzliche interne Informationen mit einbezogen werden, damit keine Szenarien untersucht werden, deren Ergebnis Sie oder Ihre Mitarbeitenden ohnehin schon kennen.

MINIMALER PROJEKTUMFANG:

Ab 8 Tage – Kick-Off, Vorbereitung Infrastruktur und Tooling, Durchführung von Prüfungen, regelmäßige Abstimmungen, Auswertung, Kurzbericht

Projektpreis: ab 14.000 EUR zzgl. MwSt.

Das Beratungskontingent ist besonders sinnvoll, wenn viele einzelne Angriffsvektoren an unterschiedlichsten Stellen von verschiedenen Angriffsketten geprüft werden sollen, da es hier die notwendige Flexibilität bietet. Gerne unterstützen wir Sie auch in vollumfänglichen Red-Teaming-Projekten. Wenden Sie sich zur Planung dieser gerne an unsere Ansprechperson.

BEISPIELHAFTE PROJEKTINHALTE

Gemeinsam mit Ihnen analysieren wir zu Beginn Ihre IT-Umgebungen dahingehend, welche Risiken erfahrungsgemäß besonders zutreffend sind und auf welchen Angriffsvektoren diese beruhen.

Das beauftragte Budget kann durch die Auftraggebenden dann flexibel für die Durchführung der folgenden Tätigkeiten abgerufen werden:

- **Durchführung theoretischer Analysen** von Systemen zur Angriffserkennung, deren Konfiguration und Kombination, der Absicherung von Systemen und der Identifikation möglicher Angriffsszenarien
- **Durchführung praktischer Red- und Purple-Teaming-Tests** in Assume-Compromise-Szenarien zur Verifikation einzelner Angriffsszenarien und deren Erkennung in der Praxis
- **Dokumentation der Ergebnisse** in einem Prüfbericht oder internen Systemen des Auftraggebenden

THOERETISCHE ANALYSE

Auf Basis gemeinsam durchgeführter Workshops sowie eventuellen zusätzlichen Untersuchungen, werden in der Theorie relevante Angriffspfade auf die IT-Systeme und –Umgebungen gemeinsam besprochen und analysiert.

HISOLUTIONS

HiSolutions AG
Schloßstraße 1
12163 Berlin

info@hisolutions.com
www.hisolutions.com

Fon +49 30 533 289-0
Fax +49 30 533 289-900

HISOLUTIONS

HiSolutions lässt relevante Praxiserfahrungen zu Angriffsarten, Umgehungsmöglichkeiten von Sicherheitsmaßnahmen und Erkenntnissen aus der IT-Forensik und unseren Threat-Intelligence-Quellen einfließen. Diese Informationen werden genutzt, um die vom Auftraggebenden bisher getroffenen Annahmen zur Bedrohungslage zu hinterfragen.

Im Rahmen der Workshops sowie nachgelagert dazu können, je nach Bedarf, folgende Tätigkeiten durchgeführt werden:

- Durchsicht von Dokumentation zur Untersuchung der Dokumente auf Schwachstellen in der Architektur und Lücken in getroffenen Schutzmaßnahmen
- Einsichtnahme in Systeme zur Prüfung der tatsächlichen Konfigurationseinstellungen auf Clients, Servern und Appliances soweit dies zur Identifikation oder Validierung von Angriffsvektoren dient
- Einsichtnahme in SIEM/SOC-Systeme zur Verifikation der getroffenen Einstellungen, angemessenen Definition von Use-Cases und zielführender Sammlung und Verknüpfung von Protokolldaten
- Unterstützung bei der Nachvollziehung von Angriffen, die im Rahmen der praktischen Verifikation von Angriffsszenarien durchgeführt wurden

PRAKTISCHE VERIFIKATION VON ANGRIFFSSZENARIEN

Sofern im Rahmen der theoretischen Analysen Angriffsszenarien identifiziert werden, für welche nicht klar ist, ob diese in der aktuellen Infrastruktur möglich sind oder diese erkannt werden würden, besteht die Option, dass HiSolutions entsprechende Angriffe praktisch simuliert.

Dazu können Methoden und Techniken angewendet werden, welche üblicherweise in Penetrationstests sowie Red- und Purple-Teaming-Projekten eingesetzt werden. Darunter technische Angriffe gegen IT-Systeme, Social-Engineering-Angriffe gegen Mitarbeitende und Nutzende sowie Angriffe gegen die physische Sicherheit von Standorten oder Bereichen.

Die Auswahl der praktischen Angriffe erfolgt, wo sinnvoll, nach dem „Assume Compromise" Ansatz, damit eine wirtschaftliche und zielgerichtete Durchführung im Rahmen des angestrebten Beratungsbudgets möglich ist.

RED- VS. PURPLE-TEAMING

Ziel unserer von Red- und Purple-Teaming-Projekte ist, dass die Abläufe und Vorkehrungen zur Erkennung und Abwehr von Sicherheitsvorfällen beim Auftraggebenden mit möglichst realen Vorfällen konfrontiert werden.

Dies geschieht dadurch, dass ausgewählte Angriffspfade, die sich aus den für das jeweilige Unternehmen ermittelten Schwachstellen und Risiken ergeben, im Rahmen realistischer Angriffssimulationen durch praktische Tests geprüft werden.

Beim Red-Teaming erfolgt dies so, dass eine Erkennung durch die Verteidigung möglichst lange vermieden wird.

Bei Purple-Teaming-Projekten erfolgt eine regelmäßige Abstimmung zwischen Red- und Blue-Team, um den Erkenntnisgewinn zu maximieren und stärker auf Besonderheiten und Wünsche des Auftraggebenden eingehen zu können.

DARUM HISOLUTIONS:

Unser Team von Fachleuten führt seit vielen Jahren technische Sicherheitstests und Incident-Response Forensik-Einsätze durch. Mit Unterstützung unserer internen Threat-Intelligence-Abteilung können die für Ihr Unternehmen kritischsten Angreifergruppen (ATPs) samt ihren eingesetzten Taktiken, Techniken und Prozeduren (TTPs) identifiziert werden. Diese Erkenntnisse werden durch unsere Sicherheitsexpertinnen und -experten realitätsnah abgebildet, sodass Ihre Verteidigungs- und Sicherheitsmaßnahmen gezielt mit realen Bedrohungsszenarien konfrontiert werden. Zur qualifizierten Durchführung von Penetrationstests beschäftigt HiSolutions u. a. mehrere BSI zertifizierte Penetrationstestende und zertifizierte Red-Team-Spezialisierte, sodass die Leistung immer von uns selbst erbracht wird (kein Nearshoring/Offshoring). Sprechen Sie uns gerne an, um gemeinsam das passende Projekt für Sie zu finden.

ANSPRECHPARTNER

Denis Werner
Senior Expert

info@hisolutions.com
Fon. +49 30 533 289-0