s/ashsec
Red Teaming Services

WHITEPAPER

RED TEAMING ASSESSMENTS

Whitepaper
Inhalt

01. Über slashsec

slashsec, gegründet 2021 in der pulsierenden Hauptstadt Österreichs, verbindet als unabhängiger Cyber-Security-Dienstleister Innovation mit einem klaren Fokus. Wir bringen jahrelange Expertise und praxisnahe Erfahrung zusammen, um professionelle Lösungen im Bereich der offensiven IT-Security anzubieten.

Innovation

slashsec beweist Innovationsführerschaft durch Forschung im Bereich Red Teaming. Wir richten unsere Red Teamings nach TIBER-AT aus.

Vertrauen

Internationale Kundschaft in kritischen Infrastrukturbereichen bestätigt unsere Expertise und Vertrauenswürdigkeit.

Praxiserfahrung

Unsere Red Teamer widmen einen Großteil ihrer Zeit der praktischen Arbeit an IT-Sicherheitsprojekten unserer Kunden. Zusammen verfügen wir über jahrzehntelange Expertise.

Expert:innen

An unseren Red Teaming Assessments wirken ausschließlich hochqualifizierte Expert:innen mit jahrelanger Erfahrung mit.

02. Über Red Teaming

In a nutshell

In der heutigen Zeit, in der die Bedrohung durch Cyber-Angriffe ständig zunimmt und Unternehmen hohe Investitionen in ihre Sicherheitssysteme tätigen, ist Red Teaming eine Schlüsselstrategie. Diese fortschrittliche Form der Bedrohungssimulation testet die robustesten Sicherheitsarchitekturen unter realistischen Angriffsbedingungen, ohne dass eine separate Testumgebung erforderlich ist. Angesichts der beträchtlichen Summen, die Unternehmen für den Schutz ihrer Netzwerke und Daten ausgeben, sind solche realistischen Angriffssimulationen ein entscheidendes Element, um die Wirksamkeit dieser Sicherheitsinvestitionen zu überprüfen.

Durch die Simulation komplexer und vielschichtiger Angriffsszenarien werden nicht nur Schwachstellen aufgedeckt, sondern auch die Reaktionsfähigkeit und organisatorische Resilienz gestärkt.

Besonderes Augenmerk wird auf die Überprüfung der Effektivität des Blue Teams gelegt, dessen Reaktionsprozesse, Analysefähigkeiten und Reaktionsgeschwindigkeit entscheidend zur Verbesserung der Cybersicherheitskultur beitragen. Ziel des Red Teaming ist es, den teilnehmenden Organisationen den größtmöglichen Nutzen zu bieten, indem die kontinuierliche Anpassung und Verbesserung ihrer Abwehrmechanismen gegen die immer raffinierteren Techniken der Angreifer gefördert wird, ohne deren Erfolg oder Misserfolg zu bewerten.
Organisationen, die einen beträchtlichen Teil ihres Sicherheitsbudgets in die Verbesserung ihrer Abwehrmaßnahmen investieren, werden daher ermutigt, auch in solche realistischen Tests zu investieren, um die Stärke und Wirksamkeit ihrer Sicherheitsarchitektur unter Beweis zu stellen.

Beantwortung folgender Fragen

01 | Wie zuverlässig sind die derzeitigen Sicherheitsmaßnahmen der Organisation zum Schutz wesentlicher und sensibler Daten?

02 | Sind die Alarm- und Überwachungssysteme der Organisation angemessen konfiguriert, um Sicherheitsvorfälle effektiv zu erkennen?

03 | Wie gut ist das Sicherheitsteam auf die Abwehr komplexer und strategischer Angriffe vorbereitet, die von fortgeschrittenen Angreifenden durchgeführt werden?

04 | Welche Gefahren entstehen, wenn Benutzer:innen oder ihre Geräte kompromittiert werden, und wie beeinflusst dies die Sicherheitslage der Infrastruktur?

05 | Kann das Sicherheitsteam effektiv aufklären und Angriffe rekonstruieren, oder gibt es Einschränkungen in der Sichtbarkeit?

Umfang des Engagements

Menschen

Mitarbeiter:innen und Partnerfirmen

Technologie

Extern und intern erreichbare Netzwerkinfrastrurkuren und Applikationen

Physische Assets

Büros, Rechenzentren, Lagerstätten, etc.

03. Die Zielgruppe

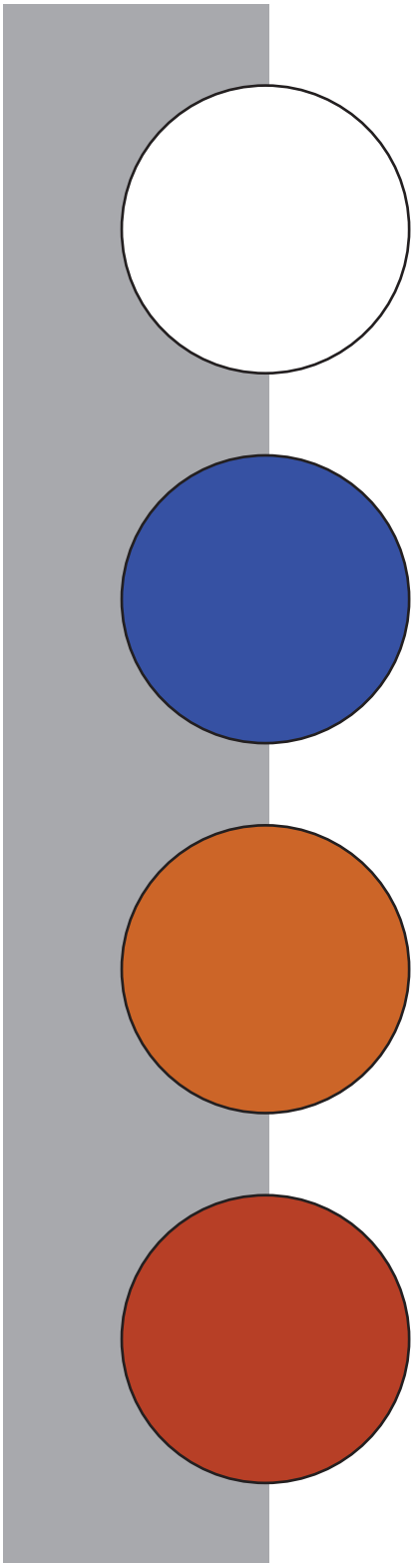
Für wen sind Red Teaming Assessments geeignet?

Red Team Assessments sind darauf ausgerichtet, die Cyber-Resilienz von Organisationen in einem breiten Spektrum von Branchen zu stärken. Das Hauptziel besteht darin, die Fähigkeit dieser Organisationen zu verbessern, mit potenziellen Risiken umzugehen und ihre Widerstandsfähigkeit gegenüber verschiedenen Bedrohungen zu erhöhen. Dies trägt dazu bei, die Sicherheit und Robustheit von Organisationen unabhängig von ihrer spezifischen Rolle in der Gesellschaft oder Wirtschaft zu gewährleisten.
Die Definition der Zielgruppe ist bewusst weit gefasst, damit eine individuelle Beurteilung der Eignung der Red Team Assessments möglich ist.
Um von einem Red Team Assessment effektiv profitieren zu können, ist ein gewisser Sicherheitsreifegrad erforderlich. Der wahre Wert solcher Assessments kommt erst dann voll zum Tragen, wenn die grundlegenden Sicherheitslücken und -defizite behoben sind. Dies ermöglicht es, sich auf die Erkennung und Abwehr von spezifischeren und anspruchsvolleren Angriffsarten zu konzentrieren.

Im Einklang mit den allgemeinen bewährten Verfahren im Bereich der Cyber-Sicherheit werden folgende Stellen adressiert:

- Große Organisationen mit erheblicher infrastruktureller oder wirtschaftlicher Bedeutung.
- Unternehmen, die kritische Dienstleistungen erbringen, wie Energieversorgung, Gesundheitswesen und Finanzindustrie.
- Betreibende von Informations- und Kommunikationstechnologien, die Dienste für kritische Funktionen anbieten.

04. Die Beiteiligten



Das White Team (WT)

Das WT fungiert als Drehscheibe innerhalb der Organisation und besteht aus ausgewählten Expert:innen, typischerweise aus der IT-Sicherheitsabteilung, ggf. ergänzt durch ein Vorstandsmitglied. Das WT fungiert als einzige Schnittstelle zwischen allen beteiligten Parteien und ist für das Testen in allen Phasen verantwortlich — von der Testkonzeption über das operative Testen bis hin zur Identifizierung von Verbesserungsmaßnahmen.

Das Blue Team (BT)

Das BT ist intern verantwortlich für den Schutz der Systeme und Daten der Organisation vor Cyber-Angriffen und für die Abwehr von Angriffen des Red Teams. Das BT umfasst im Prinzip alle Mitarbeiter:innen der Organisation, die nicht Teil des WT sind, und spielt eine zentrale Rolle bei der Analyse nach dem Test.

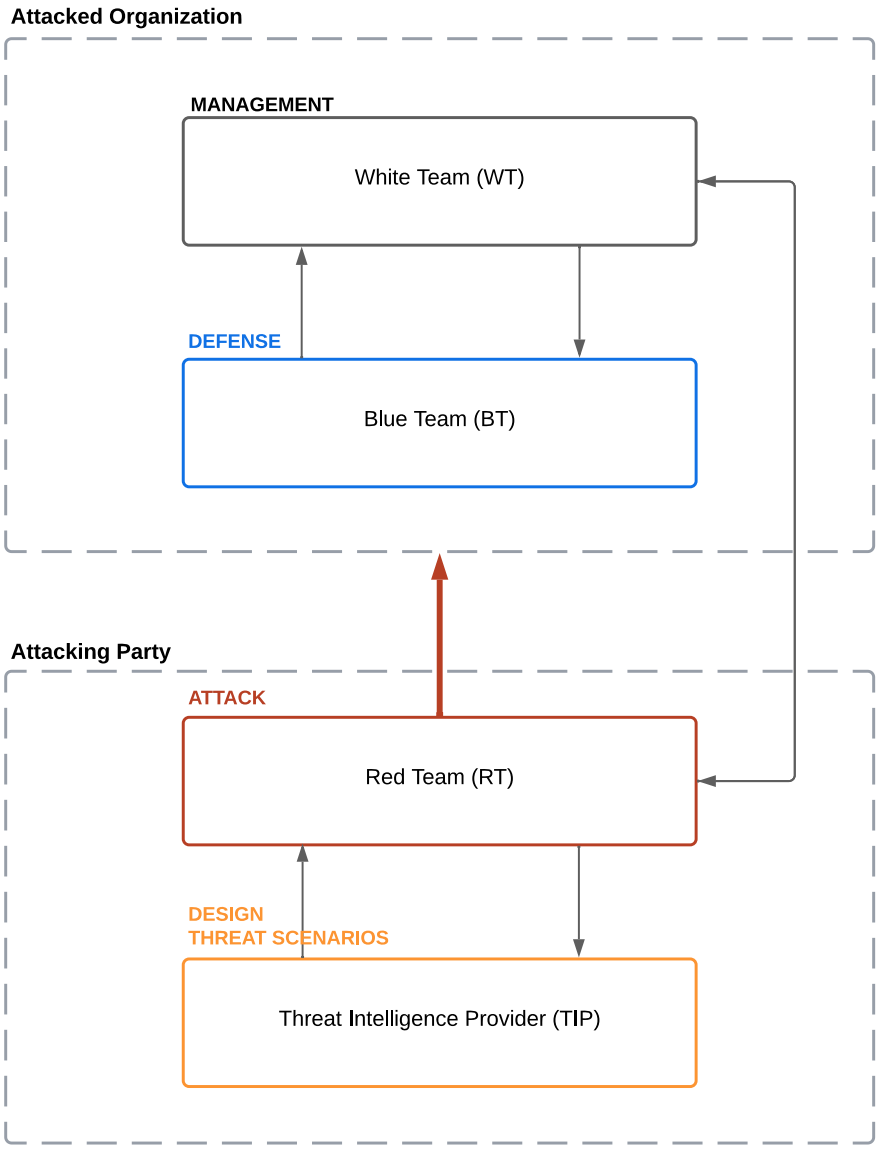
Der Threat Intelligence Provider (TIP)

Der TIP ist ein unabhängiger Anbieter, der die Ermittlungsbemühungen realer Bedrohungsgruppen nachahmt und für die Bereitstellung präziser, handlungsorientierter und zielgerichteter Bedrohungsinformationen verantwortlich ist. Der TIP arbeitet eng mit dem Red Team zusammen, um sicherzustellen, dass die Angriffsstrategie auf die spezifischen Schwachstellen der Organisation zugeschnitten ist.

Das Red Team (RT)

Das RT imitiert eine fortgeschrittene, zielgerichtete Bedrohung, die versucht, Zugang zu den Systemen und Daten der Organisation zu erlangen. Das Fachwissen und die Zuverlässigkeit des RT sind von entscheidender Bedeutung, da die Tests auf Live-Produktionssystemen durchgeführt werden und keinen realen Schaden verursachen dürfen.

05. Das Zusammenspiel



Der **Threat Intelligence Provider (TIP)** ist für die anfängliche Aufklärungsarbeit verantwortlich. Auf Basis der gewonnenen Informationen werden Angriffsvektoren identifiziert, ausgearbeitet und dem Red Team (RT) zur Verfügung gestellt. RT und TIP stehen in ständigem Austausch und arbeiten während der gesamten Dauer eines Red Team Assessments stets eng zusammen.

Das **White Team (WT)** steht in ständigem Austausch mit dem Red Team, was beispielsweise durch zweiwöchentliche Calls realisiert wird. Dabei informiert das RT das WT je nach Wunsch der Auftraggebenden über aktuelle Aktivitäten und berichtet über den Fortschritt des Assessments. Das WT wiederum erläutert beispielsweise Erkenntnisse aus erkannten Angriffen.

Das **Blue Team (BT)** arbeitet während eines Red Teaming Assessments normal weiter, wehrt Angriffe aktiv ab und wird nicht über die geplanten Aktivitäten des RT informiert. In den meisten Fällen findet der Austausch zwischen BT und WT in der Weise statt, dass eine zentrale Person des BT Teil des WT ist und Einblick in die Ereignisse und Aktionen des BT hat.

06. Typischer Ablauf eines Red Teamings

Vorbereitungen

Vertragliche Grundlagen werden geschaffen, Verantwortlichkeiten geklärt (z. B. wie setzt sich das WT zusammen), Do's and Dont's definiert (z. B. Physical Social Engineering im Scope?), sichere Kommunikationskanäle geschaffen, ...

Planung und Scoping

Ansätze aus der vorhergehenden Phase werden detailliert ausgearbeitet, RT-Ziele definiert, Maßnahmen zur Eskalationsvermeidung erarbeitet und definiert.

Threat Intelligence

Der TIP beginnt mit der Aufklärungsphase, in der ein umfassendes Bild der Schwächen der Organisation in Form eines Bedrohungsberichts dem Red Team zur weiteren Angriffsvorbereitung zur Verfügung gestellt wird.

4 - 6 Wochen

Red Teaming

Das RT führt gezielte Angriffe auf das Unternehmen durch und versucht, die zuvor definierten "Red Flags" zu erreichen. Es findet ein ständiger Austausch zwischen RT und WT statt.

12 - 14 Wochen

Evaluieren der Ergebnisse

Der Bericht des RT wird vom BT bewertet. Anschließend werden alle Stakeholder (BT, RT und TIP) vom WT in einem Workshop zusammengebracht.

4 - 6 Wochen

Planung Gegenmaßnahmen

Basierend auf den Erkenntnissen der Ergebnisevaluierungsphase werden gemeinsam mit dem BT detaillierte Gegenmaßnahmen erarbeitet.

07. Unser Fazit

Vor dem Hintergrund der zunehmenden globalen Digitalisierung und der damit einhergehenden wachsenden Bedrohung durch Cyber-Angriffe wird die Bedeutung umfassender Sicherheitsstrategien immer deutlicher. Red Teaming, eine fortgeschrittene Form der Bedrohungssimulation, hat sich als unverzichtbares Werkzeug erwiesen, um die Wirksamkeit bestehender Sicherheitsmaßnahmen unter realistischen und anspruchsvollen Bedingungen zu testen. Diese Methode ergänzt traditionelle und etablierte Sicherheitsansätze wie Schwachstellenanalysen und Penetrationtests, indem sie ein ganzheitliches Bild der organisatorischen Resilienz gegenüber Cyber-Bedrohungen zeichnet.

Die Implementierung von Red Teaming Assessments bietet Organisationen nicht nur die Möglichkeit, Schwachstellen in ihrer Sicherheitsarchitektur aufzudecken, sondern fördert auch eine kontinuierliche Verbesserung der Reaktionsfähigkeit und proaktiver Sicherheitsstrategien. Angesichts der zunehmenden Komplexität und Raffinesse von Cyber-Angriffen ist es für Organisationen unerlässlich, ihre Sicherheitsmaßnahmen regelmäßig auf den Prüfstand zu stellen. Red Teaming ist dabei ein entscheidendes Puzzleteil, das die Lücken traditioneller Sicherheitsaudits schließt und eine realistische Bewertung der Verteidigungsfähigkeiten ermöglicht.

Die bevorstehende Einführung regulatorischer Rahmenbedingungen wie DORA (Digital Operational Resilience Act) im Finanzsektor unterstreicht die Notwendigkeit fortschrittliche Sicherheitsbewertungen wie Red Teaming in die Sicherheitsstrategie von Organisationen zu integrieren. Diese Regelungen zielen darauf ab, die Cyber-Resilienz von Organisationen zu stärken und machen Red Teaming Assessments zu einem obligatorischen Bestandteil von Sicherheitsaudits. Vor diesem Hintergrund ist es umso wichtiger, dass sich Organisationen frühzeitig auf diese Anforderungen vorbereiten und ihre Red Teaming Maßnahmen an internationalen Standards ausrichten.

Die Anpassung unserer Red Team Assessments an den europäischen Standard TIBER ist ein prägnantes Beispiel dafür, wie wir bei slashsec nicht nur bestrebt sind, unseren geschätzten Kund:innen Dienstleistungen auf höchstem Niveau zu bieten, sondern auch intensiv darauf zu achten, dass diese Dienstleistungen zukunftssicher und vollständig konform mit den neuesten, sich ständig weiterentwickelnden regulatorischen Anforderungen sind. Dies spiegelt unser tiefgreifendes und dauerhaftes Engagement wider, die Cyber-Resilienz unserer Kund:innen nachhaltig und effektiv zu stärken, indem wir Bewertungen anbieten, die den strengsten internationalen Standards entsprechen.

Zusammenfassend lässt sich sagen, dass Red Teaming eine zentrale Rolle in der modernen Cyber-Sicherheitslandschaft spielt. Es ermöglicht Organisationen nicht nur, ihre Sicherheitsarchitektur unter realistischen Bedingungen zu testen, sondern bereitet sie auch auf die Einhaltung zukünftiger regulatorischer Anforderungen vor. Die Entwicklung hin zu einer umfassenden Sicherheitsbewertung, die Red Teaming einschließt, ist daher unvermeidlich und unerlässlich, um die langfristige Sicherheit und Widerstandsfähigkeit von Organisationen zu gewährleisten und zu stärken.

s/ashsec
Red Teaming Services

KONTAKT

Dipl.-Ing. David Wind, BSc
Geschäftsführer
slashsec Red Teaming GmbH
Kärtner Ring 5-7, A-1010

E dwind@slashsec.at
M +43 681/10 37 69 94