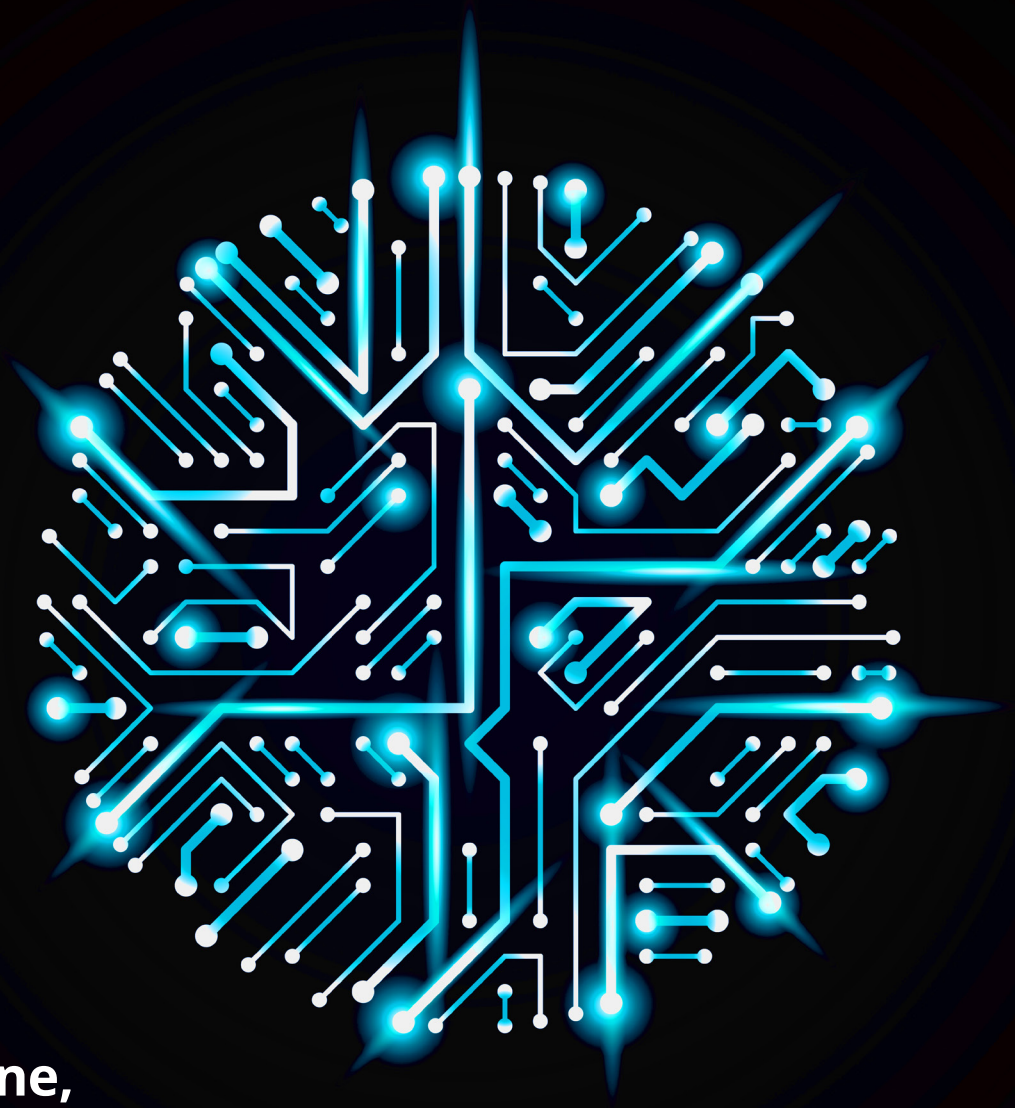
Deloitte.



Bezpieczeństwo fizyczne, zasoby ludzkie, a może cyberbezpieczeństwo? Czy znasz swoje słabe strony?

Operacje Ream Teaming

Red Teaming

Realistyczne podejście do testów bezpieczeństwa

Testy bezpieczeństwa polegające na przeprowadzeniu kontrolowanego ataku na podstawie realistycznych scenariuszy pozwalają organizacjom ocenić ich świadomość zagrożeń cyberbezpieczeństwa oraz stopień gotowości na prawdziwy atak.

Red teaming to znacznie więcej, niż testy podatności. Red teaming nie skupia się na wybranym aspekcie bezpieczeństwa, a sprawdza całą organizację z wykorzystaniem wyczerpującego podejścia opartego o realne scenariusze.

Red teaming napędza transformację organizacji w aspekcie cyberbezpieczeństwa, co w rezultacie pozwala zwiększyć dojrzałość procesów bezpieczeństwa.

94%
naszych ćwiczeń red teaming zakończyła się skutecznym włamaniem

70%
naszych klientów nie posiada wystarczających zasobów potrzebnych do wykrywania i zapobiegania atakom na systemy i krytyczne zasoby

1 dzień
tyle czasu średnio potrzebujemy na zdobycie dostępu do sieci wewnętrznej klienta po zakończonej fazie rekonesansu

6 dni
tyle średnio potrzebujemy na osiągnięcie zadanego celu po fazie rekonesansu

Trzy podstawowe elementy

Bezpieczeństwo fizyczne
budynki, biura, sejfy oraz cała fizyczna infrastruktura informatyczna

Zasoby ludzkie
Pracownicy, klienci, kontrahenci, współpracownicy

Cyberbezpieczeństwo
Internet, Intranety korporacyjne i wszystkie inne sieci komputerowe

Zasady Red Teamingu

Wierzymy w:

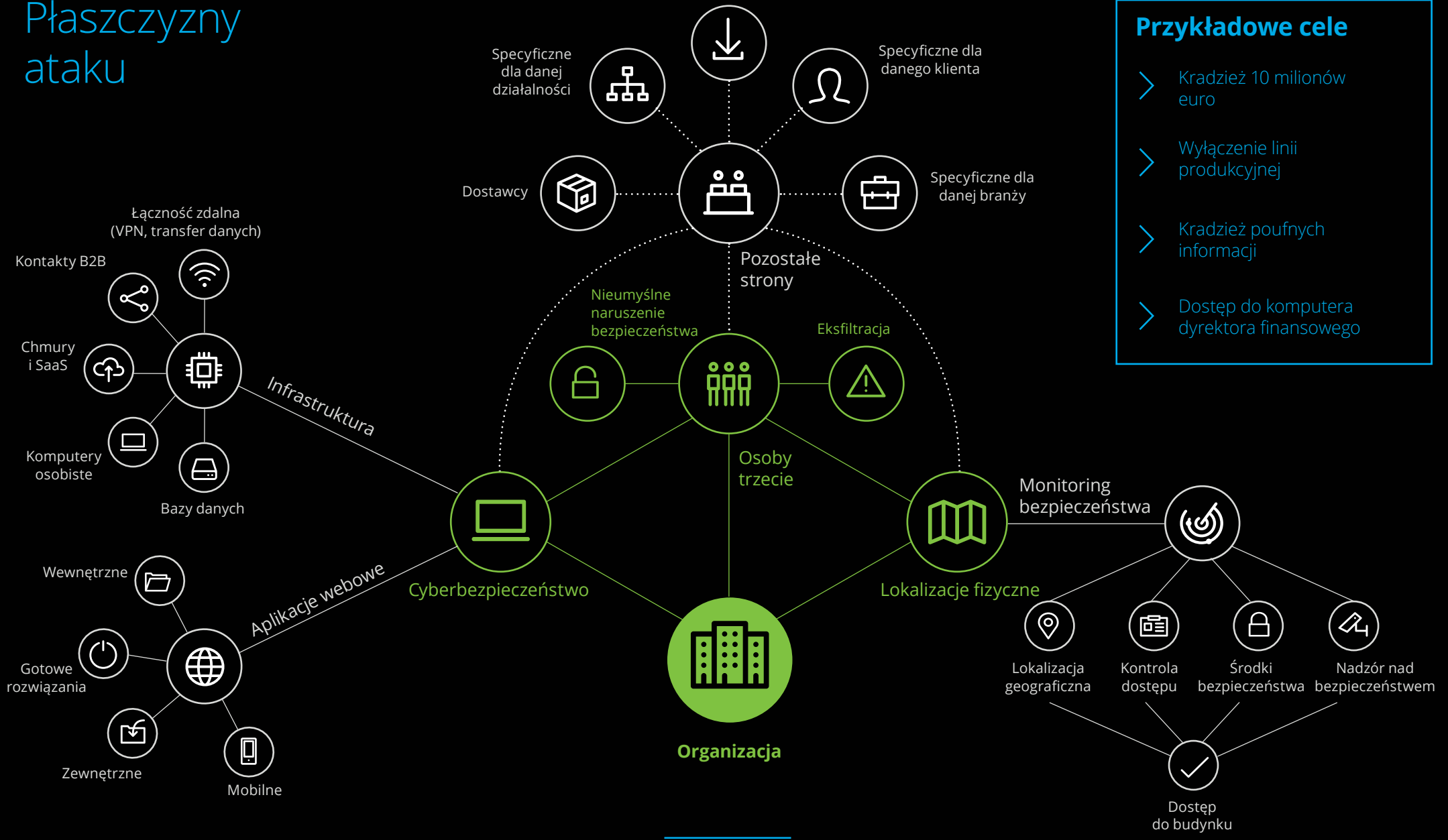
... odpowiednie połączenie biznesu i technologii. Red teaming wymaga zrozumienia i połączenia aspektów biznesowych oraz strony technicznej w celu dostarczenia miarodajnych wyników.

... zaangażowanie strony defensywnej - blue team. Współpraca obu stron, połączenie wiedzy eksperckiej z zakresu ofensywy jak i obrony przed atakami pozwala na osiągnięcie lepszych rezultatów.

... znaczenie zrozumienia i dokładnego odwzorowania strony atakującej. Sposób działania i zamiary atakującego, wynikające z charakterystyki biznesowej i profilu ryzyka przedsiębiorstwa, tworzą scenariusze testów red team.

... staranne dobranie i realizację scenariuszy ataku, które wynikają z faktycznych zagrożeń. Nie wierzymy w losowe ataki i ich przypadkowe cele. Dogłębne zrozumienie działalności naszych klientów połączone z odpowiednim zarządzaniem ryzykiem oraz faktycznym kontekstem zagrożeń daje najlepsze rezultaty.

Płaszczyzny ataku



Przykładowe cele

- Kradzież 10 milionów euro
- Wyłączenie linii produkcyjnej
- Kradzież poufnych informacji
- Dostęp do komputera dyrektora finansowego

Ocena **świadomości** i **gotowości** na cyberzagrożenia poprzez kontrolowany atak według przygotowanego scenariusza **dopasowanego** do Twojej organizacji.