Security Awareness

FAKTY:

Człowiek nadal jest najsłabszym ogniwem systemu bezpieczeństwa.

- **Celem ataku jest człowiek**, a nie technologia.
- Najczęściej wykorzystywanym przez przestępców mechanizmem jest **socjotechnika.**
- **Brak świadomości pracowników** w obszarze zagrożeń bezpieczeństwa jest oceniany jako największa podatność firm na cyberataki.
- **79% incydentów zagrożenia bezpieczeństwa powodują aktualni pracownicy** ze względu na brak wiedzy w zakresie rozpoznawania zagrożeń i przeciwdziałania im.

ZAGROŻENIA:

- Wyciek poufnych informacji o klientach i umowach.
- Ujawnienie danych osobowych, haseł dostępowych do systemów.
- Straty środków finansowych w wyniku nieautoryzowanych transakcji.

ROZWIĄZANIE:

Program Security Awareness – najbardziej efektywny sposób na obniżenie ryzyka związanego z cyberzagrożeniami

Wdrożenie w przedsiębiorstwie usługi Security Awareness pozwala zredukować liczbę incydentów zagrożenia bezpieczeństwa nawet o ponad 50%. Inwestycja ta w połączeniu ze środkami technicznymi i procedurami pozwala na znaczące podniesienie poziomu bezpieczeństwa całej organizacji.

KORZYŚCI:

- Podwyższenie poziomu odporności firmy na cyberzagrożenia.
- Pomiar i kontrola ryzyka.
- Zaangażowanie pracowników i bezpieczeństwo firmy.
- Obniżenie kosztów obsługi incydentów bezpieczeństwa.
- Szybka i sprawna detekcja zagrożeń (proaktywność).

TRANSFER WIEDZY

- e-Learning (zindywidualizowane ścieżki szkoleniowe)
- Biuletyny bezpieczeństwa
- Ostrzeżenia
- Quizy

TESTY PRAKTYCZNE

- Phishing testowy (zindywidualizowane testy)
- Testy oparte na nośnikach wymiennych
- Badania Kultury Bezpieczeństwa

USŁUGI

- Analiza
- Wdrożenie
- Treści
- Realizacja programu
- Opieka merytoryczno-techniczna
- Raportowanie i wdrażanie działań korygujących

POMIAR | **ANALIZA RYZYKA** | **RAPORTOWANIE**

SIEM/SOC | **ANTYSPAM** | **ENDPOINT**

NARZĘDZIA:

Stosowane przez nas **narzędzia są unikalne i pozwalają na precyzyjny pomiar** poziomu Kultury Bezpieczeństwa organizacji, skupiając się na „miękkich" aspektach procesu, związanych z człowiekiem. Dzięki uzyskanym wynikom Kulturę Bezpieczeństwa możemy kształtować w pełni świadomie, co **pozwala osiągać najlepsze rezultaty i precyzyjnie mierzyć założone cele**.

KnowBe4

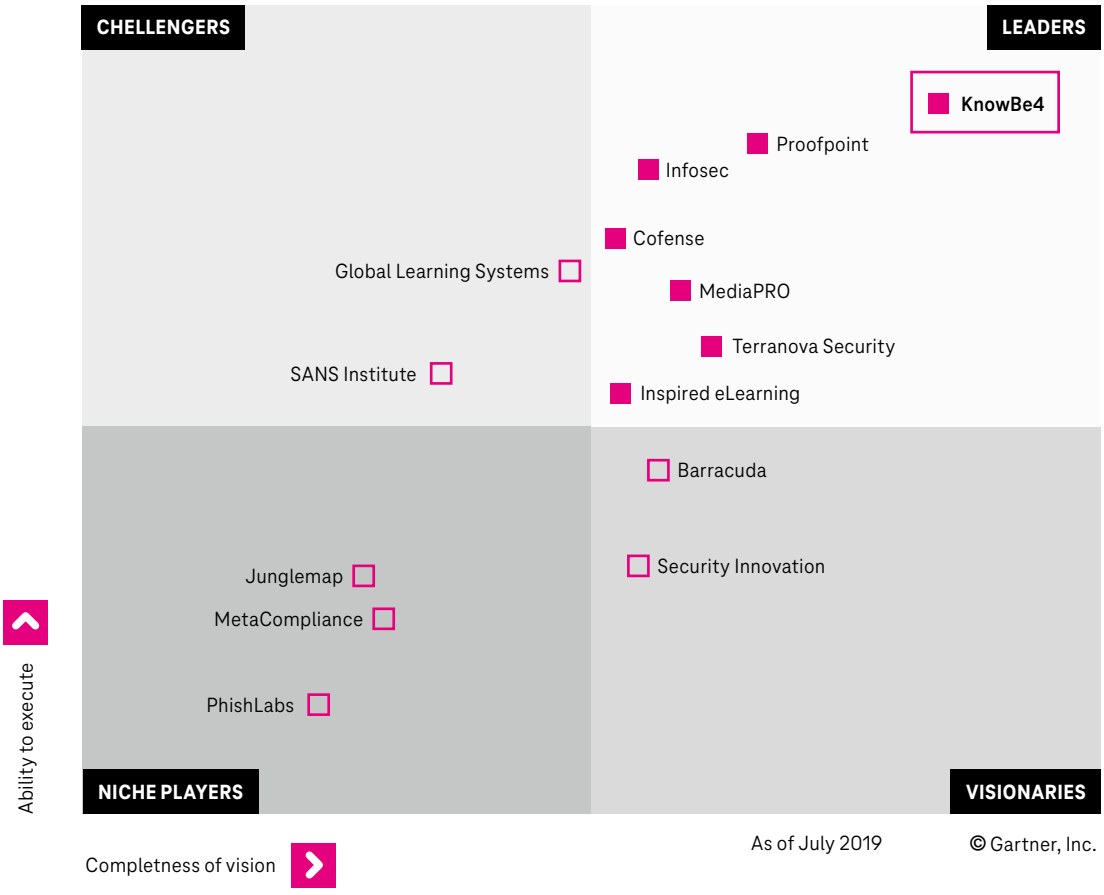
Security Awareness Training Platform

ZALETY:

- Kompletna platforma, zawierająca wszystkie niezbędne narzędzia (często unikalne), aby wdrożyć skutecznie Program Budowania Kultury Bezpieczeństwa w organizacji.
- Nie wymaga wdrożenia, a jedynie sparametryzowania.
- Platforma zrealizowana na bazie usług chmurowych wykorzystuje usługi Amazon Web Services (AWS), zapewniające właściwą skalowalność, dostępność, nadmiarowość i bezpieczeństwo. Nie trzeba inwestować we własne zasoby ani w ich utrzymanie.
- Narzędzia KnowBe4 wzbogacone o nasze usługi przygotowania, implementacji oraz zarządzania programem gwarantują szybkie i skuteczne wdrożenie takiego programu w każdym przedsiębiorstwie, niezależnie od jego skali.
- Światowy lider w dostawie narzędzi do realizacji Programów Budowy Świadomości Bezpieczeństwa (Security Awareness Program).
- Dla klientów zlokalizowanych na obszarze Unii Europejskiej wydzielona jest dodatkowa infrastruktura, zlokalizowana fizycznie w Irlandii, odseparowana od serwerów zlokalizowanych w USA.
- Zapewnia to zgodność z GDPR i gwarancję, że dane osobowe obywateli EU nie opuszczą jej i nie będą przetwarzane poza jej granicami.
- Posiada bogatą bibliotekę szkoleń i materiałów do transferu wiedzy oraz szeroki pakiet funkcjonalny.
- Platforma zawiera wielojęzyczny interfejs dla użytkowników, w tym dostępna jest oczywiście w języku polskim.

BEZPIECZEŃSTWO:

FedRAMP	**FedRAMP Li-SaaS authorized** Platforma KnowBe4 posiada Certyfikat Federalnego programu zarządzania ryzykiem i autoryzacją (FedRAMP), obejmujący cały rząd USA. FedRAMP określa wymagania w zakresie bezpieczeństwa, których dostawcy usług przetwarzania w chmurze muszą przestrzegać, aby rząd mógł korzystać z ich usług.
SOC 3	**SOC 2 & SOC 3** Wszystkie produkty KnowBe4 posiadają certyfikat SSAE18 SOC2 Type 2. **Oceny KnowBe4 SOC2 obejmują wszystkie kryteria usług zaufania, takie jak: bezpieczeństwo, dostępność, integralność przetwarzania, poufność i prywatność.**



Magic Quadrant for Security Awareness Computer-Based Traning 2019.

Numer materiału: 1721853.