The Power of the Collective

ZAANGAŻOWANIE W DOSTARCZANIE ŚWIATOWEJ KLASY ZABEZPIECZEŃ

W sytuacji, gdy 90% naruszeń bezpieczeństwa jest spowodowanych udanymi atakami phishingowymi, organizacje szybko wskazują źródło problemu — swoich pracowników. Nie zgadzamy się z tym. Cofense wierzy że pracownicy powinni być istotnym elementem obrony przed atakami i zdobywać na bieżąco informacje, by pomagać w powstrzymaniu trwających ataków.

Phishing to najpopularniejsza metoda ataku

Phishing jest najczęstszą metodą naruszania zabezpieczeń w 90% przypadków cyberataków na całym świecie. Co więcej, wiele głośnych naruszeń jest następstwem pojedynczego udanego ataku. Ponieważ w większości przypadków wykrycie naruszenia zajmuje ponad 200 dni, firmy powinny skoncentrować się na działaniach prewencyjnych i neutralizowaniu tych wysoce skutecznych metod hackerów.

Rozwiązania antyphishingowe angażujące ludzi

Nawet przy rekordowych inwestycjach liczba naruszeń spowodowana atakami phishingowymi stale rośnie. Staje się oczywiste, że sama technologia nie stanowi rozwiązania problemu. Dlatego rozwiązania Cofense skupiają się na angażowaniu ludzi — ostatniej linii obrony po pokonaniu innych zabezpieczeń — w celu usprawnienia zapobiegania i reagowania na ataki. Cofense dostarcza platformę kompleksowej obrony przed phishingiem, która koncentruje się na dawaniu większych możliwości pracownikom i umożliwianiu zespołom ds. reagowania na wydarzenia szybkie analizowanie i reagowanie na wykryte ataki phishingowe.

NASZE ROZWIĄZANIA DLA FIRM

Rozpoznawanie

Gdy atak phishingowy pokona zabezpieczenia, pracownicy muszą być w stanie zidentyfikować tę próbę.

Zgłaszanie

Zaangażowanie pracowników w zgłaszanie aktualnych ataków może znacząco skrócić czas reakcji na bieżące zagrożenia i ataki.

Reagowanie

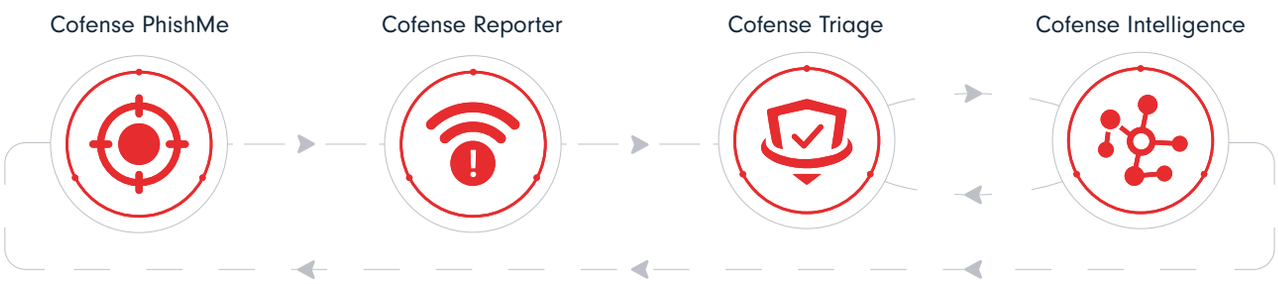
Cofense pomaga znacząco przyspieszyć proces identyfikowania, analizowania i reagowania na zagrożenia phishingowe.

Badanie

Cofense skupia się na zagrożeniach typu phishing i dostarcza sprawdzone przez ekspertów analizy ataków phishingowych i ransomware oraz powiązanego z nimi złośliwego oprogramowania.

Sposób działania

CONDITION EMPLOYEES
To RECOGNIZE AND REPORT Threats



SPEED INCIDENT RESPONSE
Collect, Analyze, and RESPOND to Verified Active Threats

Pracownicy w roli informatorów

Połączenie **Cofense PhishMe™** oraz **Cofense Reporter™** szkoli pracowników w sposobach obrony przed atakami typu phishing i pozwala im stać się częścią systemu zabezpieczeń poprzez możliwość zgłaszania potencjalnie szkodliwych ataków w czasie rzeczywistym.

Cofense PhishMe™ — ograniczanie podatności pracowników na phishing

Cofense PhishMe wykorzystuje sprawdzone metody szkolenia behawioralnego, aby lepiej przygotować pracowników do rozpoznawania szkodliwych ataków i zapobiegania im, przekształcając najbardziej podatny element w najważniejszy element obrony przed atakami.

Dostępny w formie platformy szkoleniowej opartej na SaaS Cofense PhishMe symuluje scenariusze ataków phishingowych odtwarzające różnorodne rzeczywiste techniki, jak np.:

- **Ataki typu spear phishing**
- **Ataki wykorzystujące inżynierię społeczną**
- **Złośliwe oprogramowanie i załączniki**
- **Ataki typu „drive-by”**
- **Zaawansowane ataki phishingowe podczas rozmowy**

Narzędzie Cofesne PhishMe jest łatwe w obsłudze i dostarcza dokładne informacje, oceny i możliwości zgłaszania. Rozwiązanie zapewnia stale rozwijaną bibliotekę gotowych i edytowalnych scenariuszy w 19 językach oraz szablony HTML 5, filmy i moduły gier.

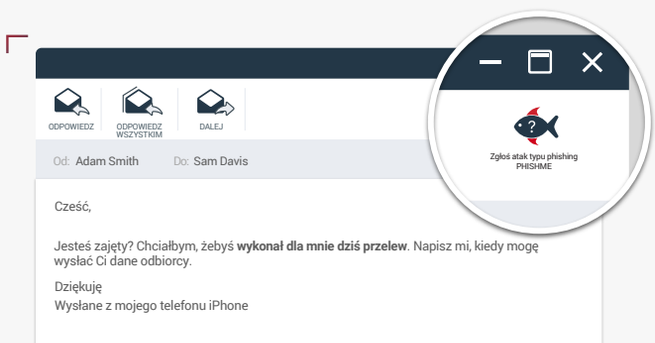
Poruszane jest wiele zagadnień dotyczących bezpieczeństwa, między innymi:

- **Phishing**
- **Świadomość znaczenia bezpieczeństwa**
- **Ryzyko i zgodność**
- **Różne formy mediów społecznościowych**

Narzędzie Cofense Cofense jest łatwe w obsłudze i dostarcza dokładne informacje, oceny i możliwości zgłaszania.

Cofense Reporter™ — łatwy sposób zgłaszania ataków dla pracowników

Cofense Reporter to łatwy w użyciu dodatek do klienta poczty, który umożliwia użytkownikom zgłaszanie podejrzanych wiadomości jednym kliknięciem. Zgłoszenia od użytkowników i zawierające pełne nagłówki i treść podejrzanych wiadomości są przesyłane do zespołów ds. bezpieczeństwa w celu umożliwienia dalszej analizy i podjęcia odpowiednich działań. Dodatek Cofense Reporter jest częścią standardowej licencji Cofense Simulator, aby usprawnić proces gromadzenia informacji na temat ataków. Współpracuje z większością klientów poczty, jak np. Outlook, Office 365, Gmail i IBM Notes.



Cofense Reporter to łatwy w instalacji i użyciu dodatek dla komputerów PC lub MAC wyposażonych w paski narzędzi Outlook, o365, Gmail lub Lotus Notes.

Cofense CBFree™ — DARMOWE CBT

Cofense zdaje sobie sprawę z tego, jak szkolenia komputerowe (CBT) pomagają spełnić wymagania dot. zgodności z przepisami. Dlatego opracowany został zestaw darmowych materiałów kompatybilnych ze SCORM dostępny dla każdej organizacji. Nasza biblioteka szkoleń z zakresu świadomości znaczenia bezpieczeństwa obejmuje 15 modułów opracowanych zgodnie z najnowszymi technikami e-learning, które gwarantują zaangażowanie uczestnika. Ukończenie jednego modułu zajmuje 5 minut, po czym możliwe jest przeprowadzenie opcjonalnej, 5-minutowej sesji pytań i odpowiedzi. CBFree działa z lub bez LMS, dzięki czemu może być łatwo dodane do każdego programu szkoleń online. Dodatkowo szkolenia Cofense dostępne są w 6 najpopularniejszych językach, a kolejne wersje językowe są aktualnie przygotowywane. Cofense oferuje również 3 moduły dotyczące zgodności w języku angielskim.

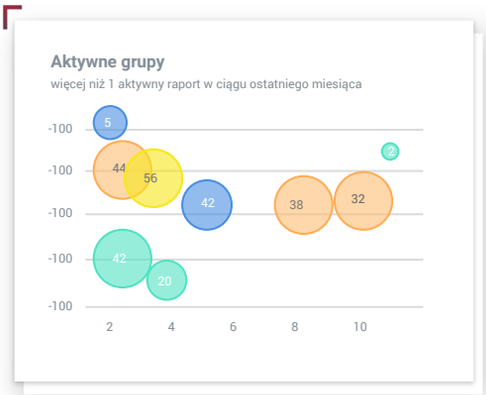
Szybkie reagowanie na wydarzenia

Cofense Triage™ i **Cofense Intelligence™** gwarantują usprawnienie identyfikowania i reagowania na ataki typu phishing. Gdy wszyscy pracownicy zgłaszają szkodliwe wiadomości, zespoły ds. bezpieczeństwa operacji i reagowania na zdarzenia muszą gromadzić, szeregować i analizować informacje, aby móc odpowiednio reagować na zgłaszane zagrożenia.

Cofense Triage™ - Reagowanie na phishing

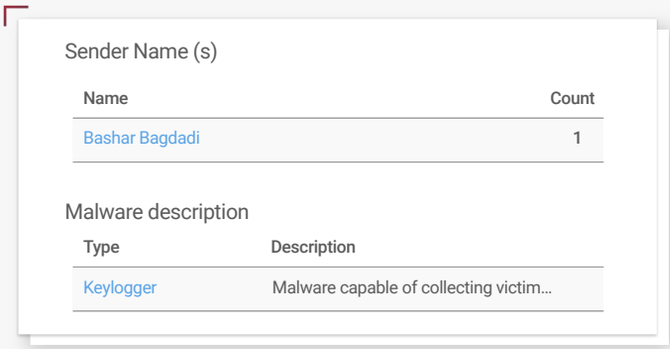
Cofense Triage to pierwsza dedykowana phishingowi platforma reagowania na zdarzenia, która umożliwia zespołom ds. bezpieczeństwa operacji oraz reagowania na zdarzenia automatyczną identyfikację i szeregowanie informacji oraz reagowanie na zagrożenia związane z atakami typu phishing prowadzonymi w formie wiadomości e-mail.

Cofense Triage daje członkom zespołu ds. reagowania na wydarzenia możliwość podglądu i analizowania ataków z użyciem wiadomości e-mail w czasie rzeczywistym. Cofense Triage umożliwia gromadzenie i szeregowanie zagrożeń zgłaszanych przez pracowników przez Cofense Reporter lub inne narzędzia. Platforma Triage jest dostępna jako rozwiązanie lokalne lub jako wirtualna platforma w chmurze, która



Cofense Triage dostarcza podgląd w czasie rzeczywistym i szybką weryfikację bieżących ataków.

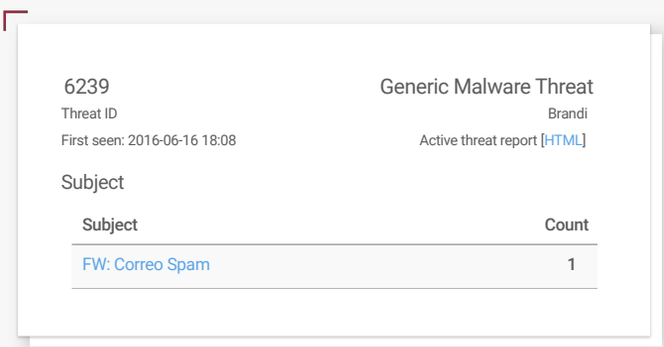
bezproblemowo łączy się z istniejącym narzędziem SIEM oraz systemami do analizy złośliwego oprogramowania i domen, jak również rozwiązaniami gromadzącymi informacje o zagrożeniach w różnych środowiskach infrastruktury.


Sender Name (s)

Name	Count
Bashar Bagdadi	1

Malware description

Type	Description
Keylogger	Malware capable of collecting victim...


6239
Threat ID
First seen: 2016-06-16 18:08

Generic Malware Threat
Brandi
Active threat report [HTML]

Subject

Subject	Count
FW: Correo Spam	1

Cofense Intelligence dostępne jest poprzez restful API i umożliwia dostęp do MRTI w formatach STIX, JSON i CEF.

Cofense Intelligence™ - informacje na temat zagrożeń

Cofense Intelligence to rozwiązanie dostępne jako samodzielny produkt lub część zestawu Cofense, które gwarantuje wysoką dokładność i weryfikowane przez ludzi informacje, pozwalające zespołom ds. bezpieczeństwa identyfikować, blokować i badać bieżące i rozwijające się zagrożenia. Dane na temat zagrożeń dostarczane są w różnych formach, aby umożliwić efektywne przygotowania i reakcje na ataki:

- **Raporty zawierające łatwe do odczytania informacje na temat zagrożeń dostarczają dokładną analizę największych zagrożeń.**
- **Informacje na temat zagrożeń odczytywalne maszynowo (MRTI) przesyłane bezpośrednio do urządzeń zabezpieczających i baz danych.**
- **Aplikacje SaaS pozwalające na badanie ataków typu phishing i malware.**
- **Porady ekspertów z naszego globalnego zespołu ds. bezpieczeństwa w kwestii wdrażania najlepszych praktyk, poprawy obrony przed phishingiem i ograniczaniu zagrożeń.**

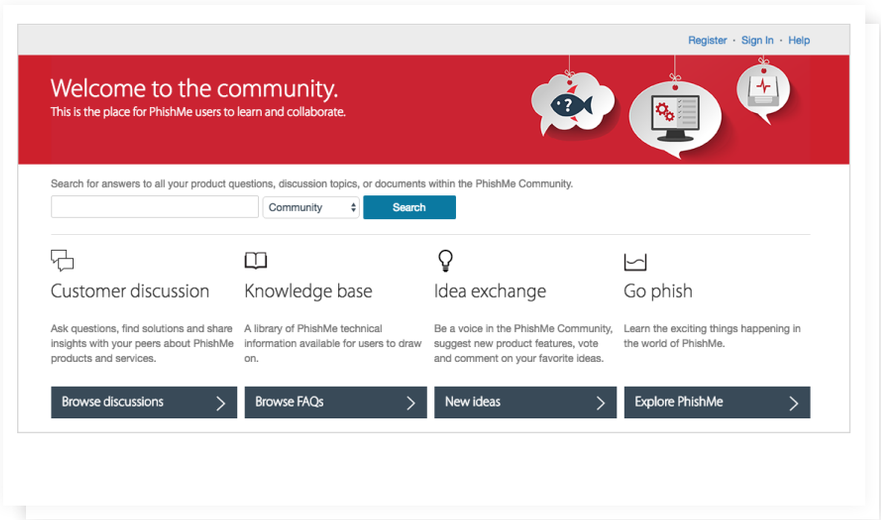
Rozwiązanie Cofense Intelligence jest wykorzystywane przez firmy z listy Fortune 100 i chwalone za niezawodne, wysokiej jakości źródło informacji na temat ataków phishingowych.

Usługi Cofense zapewniają sukces klientom

W przypadku ograniczonych zasobów dostępne są dedykowane profesjonalne usługi dla częściowych lub pełnych systemów Cofense, które obejmują dedykowanego eksperta ds. bezpieczeństwa przypisanego do każdego klienta w celu wspomagania tworzenia, wdrażania i analizowania programów zabezpieczających przed phishingiem. Programy dostosowane są do wymagań organizacji i zróżnicowanych środowisk kulturowych.

Wsparcie i społeczność Cofesnse

Każda licencja Cofense obejmuje dostęp do światowej klasy platformy zapewniającej wsparcie i umożliwiającej komunikację z klientami.



Wsparcie Cofense

Nasz dział wsparcia dostarcza informacje na temat wdrażania rozwiązań Cofense, w tym:

- **Porównywanie scenariuszy z najlepszymi praktykami stosowanymi w branży**
- **Efektywne wykorzystywanie rozwiązań Cofense**
- **Zapewnianie wsparcia w kwestii nowych funkcji i scenariuszy**
- **Tworzenie programów zabezpieczających dostosowanych do indywidualnych potrzeb każdej firmy**

Społeczność Cofense

Społeczność Cofense jest łatwo dostępną internetową bazą wiedzy, gdzie użytkownicy mogą dzielić się informacjami, odkrywać i rozwijać rozwiązania oraz kontaktować się z ekspertami w celu usprawniania ich programów Cofense. Społeczność Cofense jest miejscem dla użytkowników rozwiązań i produktów Cofense, w którym znajdują się wszystkie informacje i narzędzia potrzebne do usprawniania i rozszerzania programów zabezpieczających przed phishingiem.

Cofense jest wiodącym dostawcą rozwiązań obrony przed phishingiem dla organizacji obawiających się najpopularniejszego obecnie rodzaju ataku — spear phishing. Opierająca się na informacjach platforma Cofense zamienia pracowników w aktywną linię obrony umożliwiając im identyfikowanie, zgłaszanie i zapobieganie atakom typu spear phishing i „drive-by" oraz wykorzystującym złośliwe oprogramowanie. Nasze otwarte podejście umożliwia łatwą integrację Cofense z systemami zabezpieczeń, co zapewnia widoczne usprawnienie procesu decyzyjnego organizacji w kwestii bezpieczeństwa. Klienci Cofense należą do przemysłów obronnego, produkcyjnego i energetycznego, branży usług finansowych oraz opieki zdrowotnej. Poza tym, naszymi klientami jest 1000 globalnych organizacji, które zrozumiały, że zmiana zachowań użytkowników pozwoli poprawić bezpieczeństwo i reakcje na wydarzenia oraz zmniejszyć ryzyko narażenia.

Więcej informacji:

Strona: cofense.com/contact Tel.: 703 652 0717

Adres: 1602 Village Market Blvd, SE #200 Leesburg, VA 20175