COFENSE PROTECT™

Zatrzymaj phishing w czasie rzeczywistym dzięki rozwiązaniu **COFENSE Protect**

Problem z phishingiem

Zagrożenia stale docierają do skrzynek odbiorczych użytkowników, ponieważ atakujący stają się coraz bardziej zaawansowani i szybko zmieniają taktykę. Istniejące zabezpieczenia poczty, które zatrzymują zidentyfikowane zagrożenia nie są już wystarczające. Cyberprzestępcy tworzą miliony złośliwych witryn i coraz częściej osadzają w nich adresy URL, prowadzące do wyłudzania poświadczeń, pokonując bezpieczne bramy poczty e-mail.

Cofense Protect wykrywa i zatrzymuje zaawansowane zagrożenia phishingowe przeoczone przez SEG, zanim pojawią się na listach odrzuconych *(Deny List)*.

Rozwiązanie

Cofense Protect to zaawansowane rozwiązanie do ochrony przed phishingiem, które chroni organizacje przed wyrafinowanymi atakami phishingowymi, takimi jak wyłudzanie danych uwierzytelniających i ataki na firmową pocztę e-mail (BEC).

Cofense Protect wizualnie analizuje i sprawdza treść wiadomości, w tym adresy URL, strony docelowe i załączniki, korzystając z technologii Computer Vision oraz sztucznej inteligencji, aby zatrzymać phishingowe wiadomości i strony internetowe w czasie rzeczywistym zanim zostaną dodane do listy odrzuconych.

Nasze kompletne rozwiązanie oparte jest na **Cofense Intelligence** i sieci 30 milionów ludzkich "czujników" zgłaszających phishing za pośrednictwem Cofense Phishing Defense Center. Zapobiega temu, co może ominąć SEG, m.in. wielopoziomowym atakom z przekierowaniem, phishingowi z zaszytymi załącznikami HTML, fałszywym prośbom o zalogowanie, atakom BEC oraz nowym i nieznanym adresom URL, które nie pojawiają się jeszcze na listach odrzuconych.

Computer Vision naśladuje sposób interakcji człowieka z pocztą e-mail

Nasza technologia Computer Vision koncentruje się na emulacji ludzkiego zachowania wykrywając ataki phishingowe tak, jakby zrobił by to człowiek. **Protect** "ogląda" przychodzące wiadomości i analizuje ich wizualny wygląd, aby wykryć próbę podszycia się. Protect przechwytuje tysiące obrazów każdego dnia z popularnych stron logowania i porównuje te obrazy w bezpiecznej "piaskownicy", aby upewnić się, czy e-maile nie są phishingiem. Technologia Cofense jest zasilana danymi od ponad 30 milionów użytkowników, którzy raportują ataki phishingowe z całego świata.

Poziom inteligencji stale rośnie

Natychmiastowe wykrywanie jest coraz lepsze, ponieważ **Protect** stale się uczy. Technologia Cofense jest zasilana bazą Cofense Intelligence, która rozpoznaje aktywne zagrożenia z całego świata. **Protect** korzysta bezpośrednio z danych dotyczących zgłaszanych przez ludzi ataków, które ominęły SEG. Dodatkowo, aktywnie monitoruje setki najlepszych marek w celu ochrony przed poszywaniem się oraz jest na bieżąco z nowymi "zestawami" phishingowymi dodając nowo odkryte złośliwe witryny do list odrzuconych z korzyścią dla wszystkich użytkowników.

40-sekudnowe wdrożenie zapewnia natychmiastową ochronę

Rozpocznij ochronę środowiska Microsoft O365 lub Google Workspace niemal natychmiast. Wdrożenie odbywa się za pomocą zaledwie kilku kliknięć na serwerze pocztowym bez przekierowań ani zmian rekordów MX. Wiadomość phishingowa jest usuwana ze skrzynki pocztowej użytkownika natychmiast po wykryciu, a złośliwe adresy URL są dezaktywowane.

Jak działa COFENSE Protect

Cofense Protect to natywna dla chmury, zaawansowana technologia wykrywania phishingu i analizy wiadomości e-mail. Została stworzona, aby powstrzymywać ataki, które omijają podstawowe mechanizmy wykrywania wbudowane w system Microsoft O365 i Google Workspace. Użytkownicy korzystają z mocy Computer Vision do wykrywania w czasie rzeczywistym wyrafinowanych ataków, które dziś wymykają się systemom SEG.

COMPUTER VISION i AI.

Cofense Protect wykorzystuje (zgłoszoną do opatentowania) technologię do wykrywania ataków typu phishing poprzez wizualną analizę i kontrolę wiadomości e-mail, adresów URL, stron docelowych i załączników. Niemal natychmiast są podejmowane działania, w razie prawdopodobnej złośliwej wiadomości. Ataki phishingowe są niezwłocznie usuwane ze skrzynki odbiorczej użytkownika. Protect dezaktywuje złośliwe łącza, dzięki czemu nie stanowią zagrożenia dla użytkowników, w odróżnieniu od innych rozwiązań, które tylko alarmują „podejrzany" baner, ale łącza pozostawiają nienaruszone.

ZINTEGRUJ TWOJE ŚRODOWISKO BEZPIECZEŃSTWA Z COFENSE PROTECT

Cofense oferuje niestandardową ochronę organizacjom poprzez konfigurowalne reguły kontroli zarządzania incydentami. Integracja API z narzędziami SOC i SIEM, zapewnia pełny wgląd w ochronę przed phishingiem.

ZARZĄDZAJ OCHRONĄ Z COFENSE PROTECT.

Automatyczne raporty COFENSE Protect zawierają pełne informacje dotyczące ataków na daną organizację.

- Uzyskaj wgląd w zagregowane dane, w tym liczbę przeskanowanych e-maili i plików oraz wykrytych ataków phishingowych
- Zobacz jakie rodzaje ataków phishingowych zostały wykryte i jakie cele ataków są wybierane najczęściej
- Zarządzaj i klasyfikuj e-maile do określonych kategorii
- Zbadaj szczegółowo każdy złośliwy email w bezpiecznym środowisku

Cofense Protect to jedyne, kompletne rozwiązanie antyphishingowe wykorzystujące możliwości *Computer Vision* do wykrywania nieznanych ataków w czasie rzeczywistym. Silnik AI Protect jest zasilany przez duże zbiory danych i nieustannie uczy się na podstawie tego, czego brakuje w SEG na całym świecie, zapewniając najwyższe bezpieczeństwo.

Dlaczego Protect?

Analiza wizualna: Nasze rozwiązanie „spogląda" na wiadomości e-mail i odpowiadające im strony internetowe, analizując ich rzeczywistą reprezentację wizualną w celu wykrycia oszustw.

Wykrywanie w czasie rzeczywistym: nowe i właśnie utworzone wiadomości e-mail oraz zestawy do phishingu są wykrywane i blokowane, zanim zostaną otwarte przez namierzonego odbiorcę.

Całkowita ochrona pracowników przed: witrynami phishingowymi, stronami "mediatorów", e-mailami od oszustów (BEC, CEO Fraud), ukrytym oprogramowaniem, ransomware'em, phishingiem w załącznikach.

Łatwe wdrożenie i konserwacja: szybkie wdrożenie po stronie serwera, bez proxy, przy minimalnym wsparciu i konserwacji.

Niestandardowe ochrona: konfigurowalne reguły kontroli zarządzania incydentami, w tym integracja z czołowymi dostawcami SOC i SIEM.

Zaawansowane raportowanie: szczegółowa analiza zeskanowanych oraz wykrytych fałszywych witryn, docelowego użytkownika, ź ła, lokalizacji i marki

Cofense® jest wiodącym dostawcą rozwiązań do wykrywania i reagowania na phishing. Zaprojektowana dla organizacji korporacyjnych platforma Cofense Phishing Detection and Response (PDR) wykorzystuje globalną sieć blisko 30 milionów osób aktywnie zgłaszających podejrzenia o wyłudzenie informacji, w połączeniu z zaawansowaną automatyzacją, aby szybciej zatrzymać ataki phishingowe i wyprzedzić włamania. Wdrażając pełny pakiet rozwiązań Cofense, organizacje mogą edukować pracowników, jak identyfikować i zgłaszać phishing, wykrywać phishing w ich środowisku i szybko reagować na zagrożenia. Dzięki bezproblemowej integracji z większością głównych TIP, SIEM i SOAR rozwiązania Cofense łatwo dopasowują się do istniejących ekosystemów bezpieczeństwa.

COFENSE

CONNECT DISTRIBUTION Sp. z o.o.
tel.: +48 22 400 1234 mob. +48 784 302 005
e-mail: m.danilowicz@connectdistribution.pl