Ludzka strona cyberbezpieczeństwa

Wyobraź sobie najgorszy scenariusz.

Całe centrum danych zostało wyłączone przez zaawansowany atak ransomware. Dział sprzedaży, dział obsługi klienta i dział finansów nie mogą działać. Jesteś doświadczonym liderem IT, odpowiedzialnym za przywracanie systemów, ale znalezienie rozwiązania okazało się trudne.

Zespół, już wcześniej działający w okrojonym składzie, od wielu tygodni pracuje bez dłuższych przerw i odpoczynku. Niektórzy specjaliści ***pracowali nawet przez 36 godzin*** bez przerwy. Obawiasz się, że zmęczenie może prowadzić do błędnych decyzji, co może zagrozić samemu procesowi odzyskiwania.

Pilnie potrzebujesz dodatkowych zasobów, które mogą natychmiast wkroczyć i pomóc w rozwiązaniu problemu, ale gdzie je znaleźć?

Ten scenariusz może brzmieć jak początek powieści, ale opiera się na rzeczywistych doświadczeniach klientów firmy Dell. Podkreśla on istotny problem w dzisiejszym środowisku cyberbezpieczeństwa: Element ludzki.

Najnowsze dane wskazują, że w branży brakuje prawie 5 milionów specjalistów ds. bezpieczeństwa. Chociaż potrzeby związane z zasobami są najbardziej odczuwalne podczas incydentu, rozwiązania zaczynają się znacznie wcześniej.

Zacznij od budowania i rozwijania puli talentów

Pierwszym krokiem do zapewnienia sobie odpowiednich zasobów jest utworzenie puli talentów.

Rekrutacja i staże na uczelni

Współpraca z lokalnymi uniwersytetami i szkołami technicznymi może odblokować stały strumień młodych talentów. Te osoby mogą zostać w przyszłości wysoko wykwalifikowanymi członkami zespołu.

Ciągłe szkolenia i rozwój

Podczas gdy czas i budżet są pod stałą presją, specjaliści ds. cyberbezpieczeństwa muszą nadążać za zmianami zarówno w zakresie narzędzi, jak i zagrożeń.

Skup się na retencji

Dobrzy praktycy są bardzo poszukiwani, zwłaszcza jeśli mają doświadczenie w postępowaniu po ataku. Jeśli nie zatrzymasz swoich najlepszych talentów, ktoś inny to zrobi.

Nawet silny zespół może nie wystarczyć, aby poradzić sobie ze stresem związanym z zarządzaniem atakiem, więc planuj z wyprzedzeniem, identyfikując dodatkowe wsparcie, zanim będzie potrzebne:

Ocena zasobów innych firm

Firmy konsultingowe zajmujące się cyberbezpieczeństwem i powiększaniem personelu mogą pomóc zespołowi zarówno w bieżących operacjach, jak i incydentach. Buduj relacje z tymi firmami, nawet jeśli ich teraz nie potrzebujesz, aby mieć dostęp do tych zasobów w razie potrzeby.

Firma Dell oferuje szereg usług, które mogą powiększyć istniejące zespoły, w tym wirtualne CISO (VCISO), reagowanie na incydenty i doradztwo w zakresie cyberbezpieczeństwa.

Wykorzystaj sztuczną inteligencję

Wykorzystaj nowe funkcje sztucznej inteligencji wbudowane w narzędzia cyberbezpieczeństwa, takie jak analiza dzienników, wykrywanie anomalii, selekcjonowanie alertów niskiego poziomu lub specjalistyczne szkolenia, aby pomóc w wypełnieniu luk w zasobach i zaspokojeniu potrzeb operacyjnych, co potencjalnie pozwala członkom zespołu skupić się na zadaniach wyższego rzędu.

Wyzwania związane z zasobami są największe podczas cyberataku

Jak pokazuje początkowy scenariusz, poważny cyberatak może sparaliżować organizację, uniemożliwiając działanie kluczowych systemów i operacji biznesowych. Każda minuta kosztuje firmę pieniądze, a zespół ds. cyberbezpieczeństwa będzie musiał szybko rozwiązać problem.

Zapewnienie, że Twoje zespoły są możliwie najbardziej na bieżąco, będzie miało bezpośredni wpływ na reakcję na incydenty i związany z tym stres dla zespołu.

Pamiętaj, że szkolenia muszą obejmować nie tylko specjalistów ds. bezpieczeństwa, ale także wszystkich pracowników, ponieważ są oni pierwszą linią obrony.

Ta historia podkreśla główne wyzwanie: Cyberprzestępcy są ostatecznie ludźmi. Mają ograniczenia, a po ich przekroczeniu nawet najsilniejsi profesjonaliści mogą ponieść porażkę. Zmęczenie psychiczne, stres i wypalenie są obecnie kluczowymi czynnikami wpływającymi na cyberbezpieczeństwo.

Copyright © 2025 Dell Inc. lub jednostki zależne Dell Inc. Wszelkie prawa zastrzeżone.

Chociaż nie ma jednego rozwiązania tego problemu, następujące strategie mogą być bardzo skuteczne:

Tworzenie mocnego zespołu i strategii pozyskiwania pracowników
Najbardziej podstawowym rozwiązaniem tego problemu jest niedopuszczenie do sytuacji kryzysowej — należy zbudować silny zespół z odpowiednimi zabezpieczeniami kadrowymi.

Planowanie ludzkiej strony ataku
Plany reagowania na incydenty mają kluczowe znaczenie i MUSZĄ obejmować plany zarządzania personelem, planowania i obsługi przestojów pracowników.

Wykorzystaj zasoby innych firm
Zewnętrzni konsultanci ds. cyberbezpieczeństwa mogą pomóc w rozwoju zespołu. Na przykład służby reagowania na incydenty firmy Dell mogą w ciągu kilku godzin zaangażować zespół ekspertów, który jest gotowy do natychmiastowej oceny, opanowania i rozpoczęcia działań naprawczych. Pomogliśmy wielu klientom przetrwać ataki cybernetyczne.

Sztuczna inteligencja może pomóc, ale nie jest cudownym rozwiązaniem wszystkich problemów

Sztuczna inteligencja ma ogromny potencjał w zakresie poprawy narzędzi i programów cyberbezpieczeństwa. Jego możliwości będą ostatecznie obejmować zakres od analizy predykcyjnej przez opracowanie dostosowanych programów szkoleniowych po proaktywne reagowanie na zagrożenia, zanim się rozprzestrzenią.

Co ważniejsze, sztuczna inteligencja może zapewnić obrońcom system wsparcia w czasie rzeczywistym podczas incydentu. Modele uczenia maszynowego wytrenowane na podstawie historycznych danych ataków mogą zalecać działania oparte na podobnych zdarzeniach z przeszłości.

Ponieważ przetwarzanie języka naturalnego staje się narzędziem cyberbezpieczeństwa, analitycy będą mogli bezpośrednio łączyć się ze swoimi systemami, identyfikować zagrożenia i wdrażać rozwiązania.

Sztuczna inteligencja może również monitorować wzorce zachowań, aby sygnalizować, gdy ludzki analityk popełnia powtarzające się błędy — być może z powodu wyczerpania — i podpowiadać zmianę lub inną perspektywę.

Chociaż narzędzia cyberbezpieczeństwa szybko integrują bardziej zaawansowane narzędzia sztucznej inteligencji, wiele z najbardziej zaawansowanych funkcji jest nadal w fazie rozwoju. Pamiętaj, że na razie AI nie może zastąpić umiejętności doświadczonego praktyka, ***zwłaszcza tego, który doświadczył już ataku***.

Zalecenia dotyczące korzystania ze sztucznej inteligencji:

Dowiedz się, w jaki sposób narzędzia mogą pomóc w operacjach bezpieczeństwa
Przeprowadź szczegółową analizę narzędzi sztucznej inteligencji i wdrażaj je tam, gdzie mogą być najbardziej skuteczne. Potencjalne łatwe korzyści obejmują zaawansowane wykrywanie zagrożeń, automatyzację powtarzalnych zadań i korzystanie ze sztucznej inteligencji w zarządzaniu tożsamością.

> Najlepszym rozwiązaniem jest posiadanie partnera świadczącego usługi reagowania na incydenty, naprawy i odzyskiwania danych w ramach stałej współpracy”.
>
> ***Jason Rosselot***
> *Wiceprezes, dyrektor ds. cyberbezpieczeństwa i bezpieczeństwa jednostki biznesowej, Dell Technologies*

Planowanie przyszłości sztucznej inteligencji
Dowiedz się, kiedy pojawią się nowe możliwości, w jaki sposób przyniosą one korzyści Twojemu zespołowi, i opracuj plan ich wdrożenia.

Włączenie sztucznej inteligencji do planowania zasobów ludzkich
Ponieważ automatyzacja zmniejsza liczbę zadań ręcznych, skład zespołu ds. bezpieczeństwa może wymagać ewolucji. Możesz potrzebować zasobów wyższego szczebla, aby analizować informacje dotyczące bezpieczeństwa i podejmować na ich podstawie działania zamiast jedynie je gromadzić. Odpowiednio dostosuj strategie rekrutacji i rozwoju.

Sztuczna inteligencja stanie się istotną częścią operacji cyberbezpieczeństwa, jeśli już nią nie jest. Należy jednak pamiętać, że nic nie zastąpi wykwalifikowanego i doświadczonego praktyka. Celem powinno być wykorzystanie sztucznej inteligencji do automatyzacji operacji i zwiększenia efektywności zasobów ludzkich, a ostatecznie uniknięcie ataków i zminimalizowanie ich konsekwencji w razie wystąpienia.

Zaawansowana dojrzałość w zakresie cyberbezpieczeństwa: Krok po kroku

Tak jak w każdej dziedzinie cyberbezpieczeństwa, rozwiązywanie problemu ludzkiego jest procesem, a nie celem. Stopniowy wysiłek, a nawet drobne kroki w kierunku postępu mają znaczenie i z czasem przynoszą wymierne rezultaty. Trzeba pamiętać, że nawet najlepsze technologie i narzędzia bezpieczeństwa są ostatecznie tak dobre jak ludzie nimi zarządzający.

Copyright © 2025 Dell Inc. lub jednostki zależne Dell Inc. Wszelkie prawa zastrzeżone.

DELL Technologies

Produkty i rozwiązania firmy Dell, które mogą pomóc

Polecane rozwiązanie firmy Dell	Opis
Służby reagowania na incydenty	Zespół certyfikowanych w branży ekspertów ds. cyberbezpieczeństwa stoi w gotowości do szybkiej reakcji w przypadku cyberataku. Współpracujemy ramię w ramię, aby wyeliminować zagrożenia do czasu wznowienia normalnego działania.
Usługi doradztwa w zakresie cyberbezpieczeństwa	Specjalistyczne wskazówki, które mogą pomóc w identyfikacji i rozwiązaniu luk w strategii bezpieczeństwa, ochronie zasobów i danych oraz zapewnieniu ciągłej czujności i zarządzania.
vCISO	Wirtualny dyrektor ds. bezpieczeństwa informacji i ekspert ds. cyberbezpieczeństwa, który może pomóc w identyfikacji ryzyka i zarządzaniu nim, a także kierować strategicznym podejmowaniem decyzji.
Zarządzanie wykrywaniem i reagowaniem	Ogranicza nakłady ręcznej pracy i usprawnia codzienne operacje związane z bezpieczeństwem, zapewniając monitorowanie, wykrywanie zagrożeń, badanie i szybką reakcję na punktach końcowych, w sieci i w chmurze. Klienci wybierają preferowaną platformę XDR (Secureworks® Taegis™ XDR, CrowdStrike Falcon® XDR lub Microsoft Defender XDR) i otrzymują specjalistyczne wskazówki, kwartalne raporty i do 40 godzin reakcji na incydenty rocznie.

Więcej informacji o tym, jak radzić sobie z największymi wyzwaniami związanymi z cyberbezpieczeństwem, znajdziesz na stronie **dell.com/cybersecuritymonth**

Copyright © 2025 Dell Inc. lub jednostki zależne Dell Inc. Wszelkie prawa zastrzeżone.