Ukryte aktywa, realne straty: jak zapomniana infrastruktura może napędzać incydenty?

Shadow IT, zapomniane subdomeny i stare IP: realny krajobraz ryzyka, którego nie widać w SIEM, EDR ani XDR

ATENDE

Wprowadzenie

Niniejszy raport został opracowany w oparciu o wieloletnią praktykę operacyjną w obszarze reagowania na incydenty bezpieczeństwa - zarówno w strukturach administracji publicznej, jak i w sektorze komercyjnym, gdzie wspierałem organizacje w procesach odzyskiwania ciągłości działania po atakach ransomware.

Analizie poddano kilkadziesiąt rzeczywistych przypadków naruszeń, obejmujących organizacje o różnej skali, profilu działalności oraz poziomie dojrzałości technologicznej. Pomimo istotnych różnic kontekstowych, w niemal każdym incydencie ujawniał się ten sam schemat: źródłem kompromitacji nie był zaawansowany exploit typu zero-day ani wyrafinowana technika ofensywna, lecz zaniedbany element powierzchni ataku.

Najczęściej były to:

- zapomniane subdomeny pozostawione bez nadzoru,
- historyczne adresy IP nadal dostępne z Internetu,
- prowizorycznie wdrożone narzędzia SaaS z tokenami dostępowymi, które nigdy nie zostały zrotowane,
- fragmenty infrastruktury, które formalnie przestały istnieć w dokumentacji - ale nadal funkcjonowały w przestrzeni publicznej.

W praktyce oznacza to, że skuteczność atakujących rzadko wynikała z „geniuszu technicznego", a znacznie częściej z konsekwentnego wykorzystywania luk w zarządzaniu zasobami i braku pełnej widoczności środowiska.
To właśnie te „osierocone" komponenty - niewidoczne dla zespołów IT, lecz doskonale indeksowane przez Internet - stanowiły punkt wejścia w zdecydowanej większości analizowanych przypadków.

Wyobraź sobie firmę jako nowoczesny biurowiec. Na wejściu masz ochronę, monitoring, kontrolę dostępu, rejestr gości. W cyberbezpieczeństwie tę rolę pełnią dziś SIEM, EDR i coraz częściej XDR: zbierają sygnały, korelują zdarzenia, wykrywają anomalie, pomagają reagować. Problem w tym, że wiele realnych włamań nie zaczyna się od głównego wejścia. Zaczyna się od drzwi technicznych, wejścia od zaplecza albo okna w piwnicy, o którym nikt już nie pamięta. I właśnie tam mieści się temat tego tekstu: Shadow IT, zapomniane subdomeny i stare adresy IP, czyli zewnętrzny krajobraz ekspozycji, którego nie widać w systemach detekcji, dopóki ktoś nie jest już w środku.

To nie jest opowieść o złych praktykach IT. To raczej opis naturalnego efektu ubocznego szybkości, w jakiej biznes buduje dziś rozwiązania. Wystarczy kampania marketingowa, partner handlowy, pilny projekt integracyjny albo proof-of-concept w chmurze, żeby powstały nowe publiczne zasoby. Część z nich zostaje potem na chwilę, a ta chwila zamienia się w lata. Internet natomiast ma pamięć: DNS, historia certyfikatów, cache, indeksy i automatyczne skanery sprawiają, że ślady dawnych wdrożeń nie znikają tak szybko, jak znikają z pamięci organizacji.

Ten tekst jest techniczny, ale świadomie ubrany w perspektywę biznesową. Bo z punktu widzenia zarządu problem nie brzmi: czy mamy dobre narzędzia? Problem brzmi: czy mamy publiczne zasoby i kanały przetwarzania danych, które istnieją poza formalną kontrolą i mogą stać się wejściem do incydentu? Shadow IT, zapomniane subdomeny i stare adresy IP czy konta są dokładnie takimi wejściami.

W praktyce warto od razu ustawić trzy pytania, które dobrze działają na poziomie zarządczym, bo wymuszają konkret:

1. Jaki procent publicznie dostępnych zasobów organizacji (domen, subdomen, adresów IP oraz usług) posiada formalnie przypisanego właściciela biznesowego oraz zdefiniowany baseline bezpieczeństwa?
2. Ile elementów naszej zewnętrznej powierzchni ataku pozostaje poza inwentarzem („unknown assets") — tj. zasobów widocznych z Internetu, które nie są objęte monitoringiem i nie generują telemetryki do SIEM/XDR ani innych systemów detekcji?
3. Jak szybko potrafimy zamknąć ekspozycję, gdy ją wykryjemy (MTTR ekspozycji), i kto podejmuje decyzję o wyłączeniu?

Jeżeli powyższe pytania nie mają dziś jednoznacznych odpowiedzi, należy traktować to jako istotny sygnał ostrzegawczy. Nie jest to kwestia niewydolności zespołów, lecz braku systemowych mechanizmów ciągłego odkrywania, klasyfikacji i porządkowania zasobów. W takiej sytuacji organizacja pozostaje permanentnie opóźniona względem własnej ekspozycji.

Systemy klasy SIEM, EDR czy XDR zaczynają dostarczać sygnałów dopiero w momencie aktywnej kompromitacji — czyli wtedy, gdy atakujący znajduje się już wewnątrz środowiska.

Niniejszy materiał koncentruje się na identyfikacji źródeł tej „ciemnej materii" infrastrukturalnej, sposobach jej praktycznego wykorzystywania przez atakujących oraz na metodach prowadzenia rozmowy o tym obszarze w kategoriach ryzyka i wartości biznesowej — zamiast ograniczać się wyłącznie do technicznej listy podatności.

Spis treści

1. Dlaczego SIEM, EDR i XDR nie widzą całego ryzyka.....6
    a. Źródła telemetryki vs powierzchnia ataku.....7
2. Shadow IT – nie „problem IT", tylko równoległa organizacja technologiczna.....9
3. Zapomniane subdomeny – widoczny DNS, niewidoczna odpowiedzialność.....11
4. Stare IP i technologiczny dług ekspozycji.....12
5. Jak atakujący łączą kropki: OSINT + automatyzacja + cierpliwość....13
6. Ryzyko finansowe bez straszenia: modelowanie scenariuszy.....14
7. Architektura kontroli: od widoczności do domknięcia.....15
    a. External Attack Surface Management w praktyce.....16
8. Podsumowanie.....16

Dlaczego SIEM, EDR i XDR nie widzą całego ryzyka?

SIEM, EDR i XDR są niezwykle ważne, ale mają wspólną cechę, o której rzadko mówi się głośno na poziomie zarządczym: ich widoczność jest funkcją wdrożenia. SIEM widzi to, co loguje się i co zostało zintegrowane. EDR widzi to, gdzie jest agent i gdzie endpoint jest zarządzalny. XDR próbuje poszerzyć perspektywę, ale nadal bazuje na sygnałach z podłączonych źródeł. Wszystko, co znajduje się poza tą siecią czujników, jest w najlepszym wypadku szumem z internetu, a w najgorszym – niewidzialnym korytarzem do środka.

W codziennej praktyce firm to oznacza, że:

- środowiska tymczasowe (dev/test/POC) bywają pomijane w EDR, bo to tylko na chwilę;
- zasoby vendorów podpięte pod domenę firmy nie wysyłają logów do SIEM, bo to nie nasza infrastruktura;
- stare IP w kolokacji lub dawnych projektach nie są wpięte w pipeline, bo nikt nie pamięta, że istnieją;
- Shadow IT SaaS nie trafia do żadnego centralnego widoku, bo zakup był lokalny, a logowanie i audyt zostają w konsoli dostawcy;
- DNS i certyfikaty mogą ujawniać hosty, o których nie wie nikt w SOC.

To rodzi ważną konsekwencję biznesową: zarząd może mieć poczucie rosnącej dojrzałości (więcej use-case'ów w SIEM, więcej pokrycia EDR, lepszy MTTD), a jednocześnie realne ryzyko może rosnąć, bo firma szybciej produkuje publiczną ekspozycję niż potrafi ją inwentaryzować i domykać. Z punktu widzenia atakującego to nie jest problem. To jest przewaga.

Jeszcze jedna rzecz, która bywa myląca: EDR/XDR świetnie radzą sobie z detekcją na endpointach, ale wiele współczesnych wektorów wejścia jest bezwęzłowych z perspektywy endpointu. Przejęta subdomena, błędnie skonfigurowany bucket, publiczny panel zarządzania, token API do integracji, dostęp do SaaS przez przejęte konto. Często nie ma złośliwego pliku na komputerze, więc EDR nie ma czego łapać. A SIEM nie ma logów, jeśli zasób nie jest wpięty. W efekcie organizacja może reagować dopiero wtedy, gdy atak wejdzie w warstwę tożsamości, poczty, aplikacji produkcyjnych lub sieci, czyli gdy koszty eskalują.

Najkrótsze podsumowanie dla zarządu brzmi tak: SIEM/EDR/XDR są narzędziami reakcji i detekcji w znanym środowisku. Nie są narzędziami kompletnej kontroli nad tym, co firma wystawia na Internet.

Źródła telemetryki vs powierzchnia ataku

Warto rozdzielić dwie listy, które w wielu organizacjach błędnie uważa się za tożsame.

Lista powierzchni ataku

Domeny i subdomeny, delegacje DNS, rekordy CNAME do dostawców, publiczne IP, otwarte porty, panele administracyjne, API, hosty ujawnione przez certyfikaty, zasoby w chmurze z publicznym dostępem, aplikacje SaaS, które dotykają danych firmowych, webhooki i tokeny integracyjne, a także wszelkie „resztki” po migracjach.

Lista źródeł telemetryki

Firewalle, proxy, AD/IdP, EDR, serwery krytyczne, aplikacje produkcyjne, chmura (częściowo), systemy IAM, czasem CASB. Ta lista jest wynikiem architektury oraz budżetu: integrujesz to, co najważniejsze i to, co umiesz zintegrować.

Różnica jest fundamentalna: telemetria jest od środka, powierzchnia ataku jest od zewnątrz. Atakujący działa od zewnątrz, a firma często buduje kontrolę od środka. Gdy te dwa światy się nie spotykają, powstaje luka.

W praktyce ta luka ma bardzo biznesowy wymiar: organizacja inwestuje w narzędzia i ludzi, ale część ryzyka pozostaje poza zasięgiem, więc zwrot z inwestycji w detekcję jest niższy, niż mógłby być. Dlaczego? Bo detekcja będzie „gasiła" incydenty, które dało się prewencyjnie zdusić usuwając jeden rekord DNS, wyłączając stare IP albo legalizując jedno narzędzie SaaS przez SSO i MFA.

Dla zarządu dobrym sposobem myślenia jest potraktowanie powierzchni ataku jako aktywa, które mają swój bilans ryzyka. Jeśli nie wiesz, ile ich masz, nie wiesz, ile ryzyka niesiesz. A jeśli nie wiesz, kto jest właścicielem, to nie wiesz, kto ma je minimalizować. To jest analogia do finansów: nie zarządzasz portfelem, którego nie widzisz.

Najbardziej podstępna część tej układanki jest psychologiczna. Dashboardy dają komfort. Jeśli liczba incydentów spada, a SLA reakcji rośnie, łatwo uwierzyć, że ryzyko maleje. Tymczasem możesz mieć po prostu spadek widoczności tam, gdzie problem się zaczyna.

Cicha luka powstaje najczęściej w miejscach, które nie mają naturalnego właściciela:

- subdomeny tworzone na potrzeby kampanii lub partnera,
- zasoby w chmurze tworzone w ramach POC,
- stare IP w dawnych projektach,
- automatyzacje no-code działające na kontach użytkowników,
- integracje oparte o tokeny, które nikt nie rotuje.

Atakujący lubi ciche luki, bo one mają trzy cechy:

1. Brak rutyny patchowania – bo nikt nie czuje odpowiedzialności.
2. Brak monitoringu – bo to nie jest krytyczne.
3. Wysoką wiarygodność – bo działa pod domeną lub marką firmy.

Z biznesowego punktu widzenia to jest ryzyko o strukturze długu. Zostawione rzeczy nie stoją w miejscu. One z czasem stają się coraz bardziej ryzykowne, bo:

- zmienia się krajobraz podatności,
- zmieniają się standardy uwierzytelnienia,
- ludzie odchodzą, dokumentacja ginie,
- vendorzy zmieniają mechanikę usług,
- a internetowe indeksy i archiwa utrwalają ślady.

Najgorsze w tym wszystkim jest to, że ten dług nie generuje odsetek w postaci kosztu operacyjnego na bieżąco. On generuje je w momencie incydentu, a wtedy koszt jest skokowy. I to jest moment, w którym zarząd zadaje pytanie: „jak to możliwe, że coś takiego w ogóle istniało?". Odpowiedź „bo nie było w SIEM/EDR/XDR" nie brzmi dobrze, bo zarząd nie kupuje narzędzi po to, żeby dowiedzieć się o problemie po fakcie.

Shadow IT – nie „problem IT", tylko równoległa organizacja technologiczna

Shadow IT to nie jest już „ktoś sobie zainstalował aplikację". To jest równoległy ekosystem technologiczny, który powstaje wtedy, gdy biznes potrzebuje szybkości, a oficjalne ścieżki są wolne lub zbyt kosztowne w czasie. I tu warto powiedzieć coś wprost: Shadow IT często powstaje, bo jest racjonalne z perspektywy celów biznesowych.

Jeśli dział sprzedaży potrzebuje narzędzia do automatyzacji leadów, marketing potrzebuje landing page'a na przyszły tydzień, a produkt potrzebuje środowiska demo dla partnera, ludzie wybiorą drogę, która dowiezie wynik. I to jest dokładnie to, co organizacje premiują.

Problemem nie jest więc fakt istnienia Shadow IT, tylko to, że Shadow IT:

- nie ma kontroli dostępu na poziomie organizacji (SSO/MFA),
- nie ma przeglądów bezpieczeństwa i zgodności,
- nie ma monitoringu i właściciela,
- i nie ma cyklu życia: kiedy powstaje, kiedy znika, kto sprząta.

Biznesowo Shadow IT uderza w trzy obszary: bezpieczeństwo danych, zgodność i ciągłość działania. A to oznacza, że to jest temat dla zarządu, nie tylko dla IT. Dlaczego? Bo często to zarząd decyduje o tym, czy firma ma działać szybko i lokalnie, czy centralnie i procesowo. Prawda jest taka, że firma musi robić i jedno, i drugie. Kluczem jest stworzenie ułatwień, które pozwalają na szybkość bez zostawiania otwartych drzwi.

Technicznie najgroźniejsze w Shadow IT jest to, że tworzy ono nowe ścieżki przepływu danych: webhooki, integracje z CRM, dostęp do poczty, dostęp do plików, tokeny do API. I to właśnie te ścieżki bywają niewidoczne dla SIEM/EDR/XDR, bo dzieją się w SaaS lub w usługach zewnętrznych, z logami schowanymi w konsolach dostawców, bez centralnej korelacji. Dlatego należy zbudować model, w którym Shadow IT wychodzi na światło: szybka ścieżka rejestracji, minimalny przegląd ryzyka i proste warunki brzegowe (SSO/MFA, klasyfikacja danych, właściciel, data przeglądu).

Biznesowa wartość takiego podejścia jest konkretna. Utrzymujesz szybkość działania zespołów, zmniejszasz ryzyko incydentu i koszt reakcji, zwiększasz kontrolę zgodności (np. umowy powierzenia, lokalizacja danych), ograniczasz podwójne koszty narzędzi (płacenie za to samo dwa razy) i poprawiasz ciągłość działania (bo narzędzia przestają zależeć od kont prywatnych).

Zapomniane subdomeny – widoczny DNS, niewidoczna odpowiedzialność

DNS jest publiczny. To oznacza, że Twoje subdomeny są jak drogowskazy. Nawet jeśli dana usługa przestała istnieć, rekord DNS może nadal mówić światu: „tu kiedyś coś było". A czasem mówi więcej: „tu było środowisko testowe", „tu był panel admin", „tu jest portal partnera".

Zapomniane subdomeny to klasyczny przykład ryzyka, które nie mieści się naturalnie w SIEM/EDR/XDR. Bo z perspektywy organizacji to bywa tylko rekord. Nie ma logów, nie ma endpointu, nie ma agenta. Ale z perspektywy atakującego to jest powierzchnia, którą można przejąć, podszyć się pod markę, wykonać phishing albo przeprowadzić atak łańcuchowy.

Biznesowo to ryzyko reputacji: jeśli ktoś zobaczy phishing pod twojafirma.pl, nie ma znaczenia, czy to stary rekord. To jest Twoja marka. W dodatku subdomeny bywają na białych listach, a użytkownicy mają odruch zaufania. To obniża barierę skutecznego oszustwa.

Osierocona subdomena powstaje najczęściej wtedy, gdy proces tworzenia jest łatwy, a proces usuwania nie istnieje. Subdomenę tworzy się, bo projekt, bo kampania, bo vendor. Usuwanie wymaga decyzji: czy na pewno nikt tego nie używa? A skoro nikt nie jest właścicielem, decyzja nie zapada.

Najprostszy sposób na przełamanie tego mechanizmu to uczynienie braku właściciela problemem samym w sobie. Jeśli rekord nie ma właściciela, trafia do puli do wygaszenia. Właściciel ma się zgłosić i uzasadnić. Jeśli się nie zgłosi, rekord znika. Wtedy decyzja ma właściciela, a nie jest niczyja.

Stare IP i technologiczny dług ekspozycji

Stare IP jest często synonimem starego świata. Serwery, które zostały po migracji, zasoby, o których pamięta tylko jeden administrator, hosty wystawione publicznie, bo kiedyś tak trzeba było. Ale w praktyce stare IP to też chmura, czyli publiczne adresy przypięte do zasobów, które dawno powinny zniknąć, lub zakresy utrzymywane „bo mogą się przydać".

Technicznie to kategoria bardzo ryzykowna, bo stare IP często nie ma monitorowania, nie ma patchowania i hardeningu, za to ma stare protokoły oraz porty i bywa drogą do sieci wewnętrznej przez np. dawne tunele.

Biznesowo to ryzyko o wysokiej asymetrii, czyli tanio zostawić, bardzo drogo naprawiać. Incydent zaczęty na starym IP bywa trudny do obsłużenia, bo pierwsze godziny idą na odpowiedź: „co to jest i kto to ma?". A w kryzysie czas jest walutą.

Najprostsza biznesowa zasada, która działa, jeśli to publiczne IP i nie ma właściciela, to jest to ryzyko krytyczne. Nie dlatego, że na pewno jest dziura. Tylko dlatego, że nikt nie gwarantuje, że jej nie ma.

Jak atakujący łączą kropki: OSINT + automatyzacja + cierpliwość

Atakujący rzadko zaczyna od szturmu na najlepiej bronioną bramę. Zaczyna od rozpoznania. I robi to tanio: DNS, enumeracja subdomen, analiza certyfikatów, fingerprinting usług, skanowanie portów. To jest automatyzowalne i masowe.

To ważne, bo pokazuje, że firma nie konkuruje z pojedynczym „hakerem". Firma konkuruje z przemysłową rutyną skanowania Internetu. Nawet jeśli nikt nie celuje w Ciebie osobiście, Twoje zasoby są skanowane jak każdy inny cel w Internecie. Skanują wyszukiwarki takie jak Shodan.io, ale również boty tworzone przez cyberprzestępców. A zapomniane subdomeny i stare IP są właśnie tym, co skanery lubią najbardziej: słabe, stare, niepilnowane.

Z punktu widzenia SIEM/EDR/XDR wiele z tych działań jest niewidocznych. Skanowanie z zewnątrz może wyglądać jak zwykły ruch. Przejęcie subdomeny odbywa się po stronie dostawcy. Kompromitacja tokena API nie wymaga endpointu. A jednak wszystkie te kroki składają się na łańcuch, który finalnie kończy się w środku organizacji.

Biznesowo warto to opisać jako mechanizm kosztowy: im wcześniej przerwiesz łańcuch, tym taniej. Usunięcie dangling DNS to koszt godzin. Gaszenie incydentu phishingowego na przejętej subdomenie to koszt dni i reputacji. Reakcja na kompromitację kont i danych to koszt tygodni i realnych pieniędzy.

Jeśli chcesz przerwać łańcuch wcześniej, musisz patrzeć na to, co widać z zewnątrz i mieć proces domykania.

Ryzyko finansowe bez straszenia: modelowanie scenariuszy

Shadow IT, zapomniane subdomeny i stare IP to kategorie ryzyka, które mają bardzo wyraźny związek z reputacją, ciągłością działania i zgodnością. Zarząd rozumie te trzy słowa, bo to są wymiary ryzyka, które wprost dotykają wyników finansowych i wartości firmy.

W praktyce wystarczy pokazać, że ryzyko w tym obszarze ma charakter długu ekspozycji i że dług może rosnąć, jeśli firma nie ma procesu, który go spłaca. Warto też podkreślić, że spłacanie długu ekspozycji poprawia efektywność inwestycji w SIEM/EDR/XDR. Mniej ekspozycji oznacza mniej incydentów, mniej fałszywych alarmów, mniej kosztów reakcji i mniej kryzysów wymagających udziału zarządu. To jest korzyść, którą łatwo przełożyć na czas i pieniądze.

Modelowanie scenariuszy dobrze działa, bo zarząd myśli scenariuszami. Najrozsądniej jest wziąć kilka typowych zdarzeń i opisać je w kategoriach skutku. Przejęta subdomena użyta do phishingu to scenariusz reputacyjny, w którym koszty nie wynikają tylko z pracy IT, ale też z komunikacji, obsługi klienta i utraty zaufania.

Wejście przez stare IP i konieczność izolacji systemów to scenariusz operacyjny, w którym kosztem jest przestój, opóźnienia i roboczogodziny wielu zespołów. Shadow IT przetwarzające dane bez standardowych uzgodnień to scenariusz, w którym koszty przenoszą się na prawników, audyty i relacje z klientami.

Warto w tych scenariuszach uwzględnić jeszcze jeden element, który często jest pomijany: koszt chaosu. W kryzysie firma płaci nie tylko za techniczne działania, ale też za to, że wiele osób o wysokich stawkach przerywa swoją pracę i wchodzi w tryb zarządzania kryzysowego. Jeśli ekspozycja jest zapomniana, chaos jest większy, bo najpierw trzeba zrozumieć, co w ogóle zostało zaatakowane. Jeśli ekspozycja jest zarządzana i ma właścicieli, chaos jest mniejszy, a to oznacza realne oszczędności.

Architektura kontroli: od widoczności do domknięcia

Najważniejsze jest zrozumienie, że odkrycie ekspozycji bez procesu domykania jest tylko wiedzą o problemie, a nie redukcją problemu. Dlatego architektura kontroli powinna działać jak pętla: odkrywasz, klasyfikujesz, przypisujesz właściciela, domykasz i weryfikujesz. To brzmi jak oczywistość, ale w wielu organizacjach brakuje właśnie tych środkowych kroków.

Z technicznego punktu widzenia zarządzanie zewnętrzną powierzchnią ataku często przybiera formę EASM, ale nie trzeba zaczynać od wielkiego programu. Ważniejsze jest, żeby rutyna obejmowała DNS, publiczne IP i integracje. To są trzy obszary, w których najczęściej kryją się „zapomniane drzwi", a jednocześnie w których często wystarczy relatywnie prosta praca higieniczna, żeby znacząco obniżyć ryzyko.

External Attack Surface Management w praktyce

EASM w praktyce jest skuteczny wtedy, gdy firma traktuje go jako proces operacyjny, a nie jako jednorazowy audyt. Jednorazowy audyt jest jak sprzątanie mieszkania tylko wtedy, gdy przychodzą goście. Po tygodniu znów jest bałagan. W środowisku cyfrowym bałagan wraca szybciej, bo zasoby powstają codziennie.

Dojrzałe podejście polega na tym, że organizacja stale obserwuje, co Internet widzi pod jej marką, i ma mechanizm, który z tego robi konkretne działania. Gdy pojawia się nowa subdomena, ktoś ją przypisuje. Gdy rekord wskazuje w próżnię, ktoś go wygasza. Gdy pojawia się nowe publiczne IP bez właściciela, ktoś je identyfikuje i albo włącza do standardu, albo wyłącza. To nie jest polowanie na błędy. To jest utrzymanie.

Podsumowanie

SIEM, EDR i XDR są fundamentem nowoczesnej detekcji i reakcji, ale nie są pełną mapą ryzyka. One widzą to, co zostało podłączone do czujników. Tymczasem Shadow IT, zapomniane subdomeny i stare IP żyją często, poza tym obszarem, a mimo to są widoczne i atakowane z Internetu. To właśnie tam zaczyna się wiele incydentów, w miejscach bez właściciela, bez cyklu życia, bez monitoringu, ale z pieczęcią Twojej marki.

Z perspektywy zarządu to jest temat zarządzania ryzykiem operacyjnym i reputacyjnym. Największą wartość daje podejście, które łączy odkrywanie powierzchni ataku z procesem domykania i rutyną sprzątania.

Wtedy bezpieczeństwo przestaje być tylko reakcją na alerty i staje się realnym ograniczaniem wejść, które w ogóle mogą doprowadzić do incydentu.

Jeśli firma ma działać szybko, to musi mieć szybkie mechanizmy bezpieczeństwa. Nie po to, żeby spowalniać biznes, tylko po to, żeby biznes nie płacił za „zapomniane drzwi" w najmniej odpowiednim momencie.

Karol Kij

Ekspert ds. cyberbezpieczeństwa w Atende S.A.