DELL Technologies

INTERAKTYWNE SCENARIUSZE CYBERBEZPIECZEŃSTWA — E-BOOK

Rzeczywiste scenariusze. Inteligentniejsze decyzje. Silniejsza obrona.

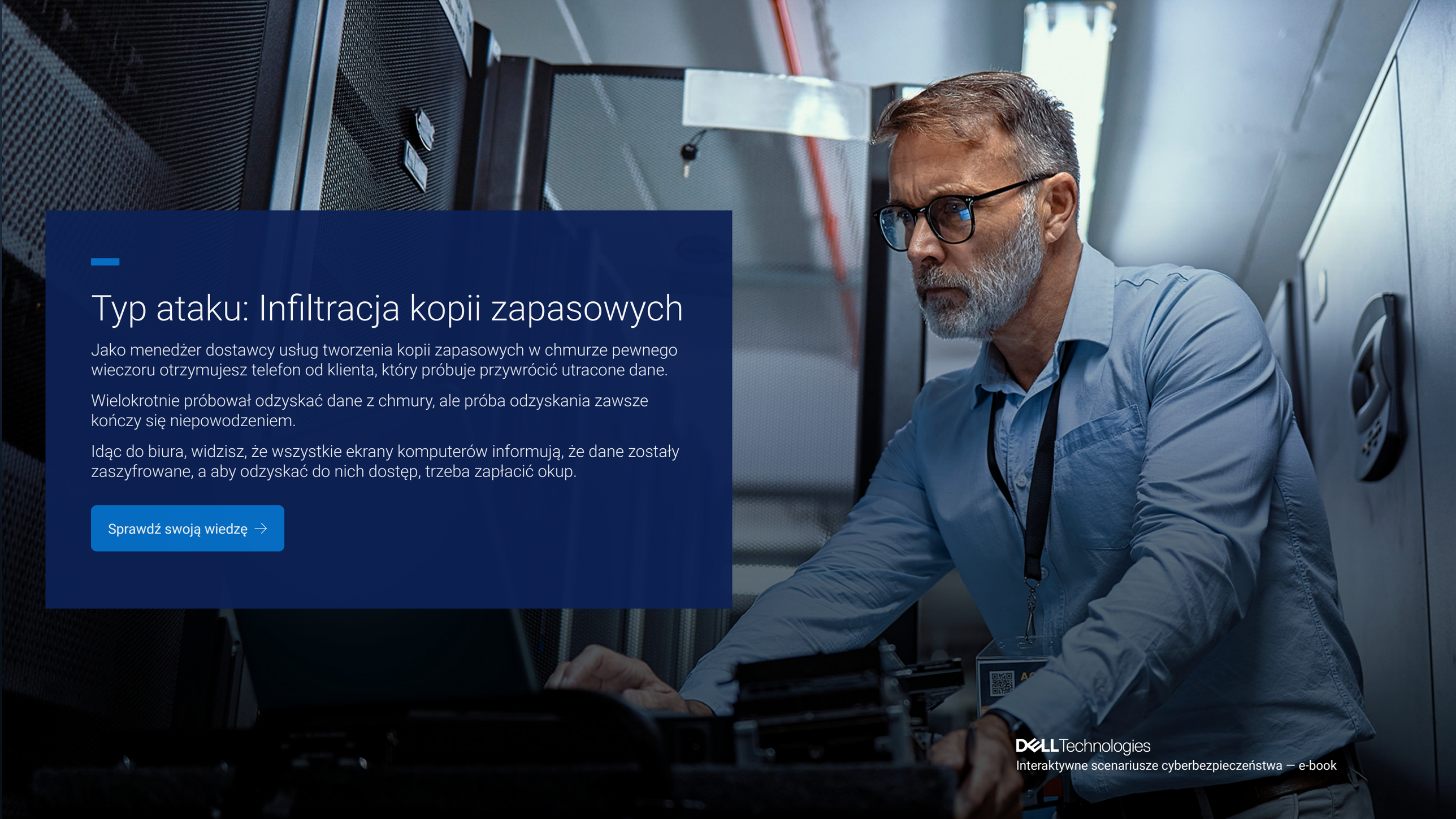
Zaangażowanie firmy Dell w bezpieczeństwo jest podstawą wszystkiego, co robimy. Poprzez udostępnienie informacji, najlepszych praktyk i innowacyjnych technologii ten e-book ma na celu zapewnienie narzędzi i wiedzy potrzebnych do wyprzedzania pojawiających się zagrożeń cybernetycznych.

Wybierz scenariusz ataku

Zagrożenia cyberbezpieczeństwa stale ewoluują, a organizacje muszą skutecznie reagować, aby chronić swoje dane. Aby jak najlepiej przygotować swoją organizację, weź udział w rzeczywistych ćwiczeniach symulacyjnych, które pomogą w opracowaniu skutecznych strategii cyberbezpieczeństwa i zwalczania cyberataków.

Zapoznaj się z szeroką gamą typów ataków i wyzwań branżowych w różnych sektorach, takich jak administracja państwowa, samorządowa i lokalna, usługi finansowe i opieka zdrowotna. Po drodze dowiesz się, w jaki sposób zintegrowane rozwiązania zabezpieczające firmy Dell — od notebooków i komputerów stacjonarnych po systemy klasy Enterprise — zapewniają ochronę przed tymi zagrożeniami.

- Infiltracja kopii zapasowych →
- Ransomware →
- Distributed Denial of Service (DDoS) →
- Sprzęt łańcucha dostaw →
- Złośliwe zagrożenie wewnętrzne →
- Oprogramowania łańcucha dostaw →
- Man-in-the-Middle (MITM) →
- Zero-Day →
- Szybkie wstrzyknięcie poleceń/kodu SQL →



Typ ataku: Infiltracja kopii zapasowych

Jako menedżer dostawcy usług tworzenia kopii zapasowych w chmurze pewnego wieczoru otrzymujesz telefon od klienta, który próbuje przywrócić utracone dane.

Wielokrotnie próbował odzyskać dane z chmury, ale próba odzyskania zawsze kończy się niepowodzeniem.

Idąc do biura, widzisz, że wszystkie ekrany komputerów informują, że dane zostały zaszyfrowane, a aby odzyskać do nich dostęp, trzeba zapłacić okup.

Sprawdź swoją wiedzę →

Typ ataku: Infiltracja kopii zapasowych

1: Zmniejszenie powierzchni ataku — 2 — 3 — 4

Nie masz pewności, które systemy tworzenia kopii zapasowych lub klienci zostali dotknięci problemem. Jaki powinien być Twój pierwszy krok?

- [ ] Powiadomienie władz
- [ ] Wyłączenie wszystkich systemów
- [ ] Próba powstrzymania i odizolowania zagrożenia
- [ ] Sprawdzenie, czy masz czystą kopię zapasową do przywrócenia

Zobacz prawidłową odpowiedź →

Typ ataku: Infiltracja kopii zapasowych

1: Zmniejszenie powierzchni ataku — 2 — 3 — 4

Nie masz pewności, które systemy tworzenia kopii zapasowych lub klienci zostali dotknięci problemem. Jaki powinien być Twój pierwszy krok?

- ✗ Powiadomienie władz
- ✗ Wyłączenie wszystkich systemów
- ✓ Próba powstrzymania i odizolowania zagrożenia
- ✗ Sprawdzenie, czy masz czystą kopię zapasową do przywrócenia

Natychmiastowe powstrzymywanie i izolowanie zagrożenia zapobiega dalszemu rozprzestrzenianiu się lub uszkodzeniu oraz pozwala na ocenę zakresu incydentu, potencjalnie minimalizując wpływ wszystkich rodzajów cyberataków, w tym związanych ze sztuczną inteligencją.

Następne pytanie →

Typ ataku: Infiltracja kopii zapasowych

1 — 2: Wykrywanie cyberzagrożeń i reagowanie na nie — 3 — 4

Twoim priorytetem jest szybkie udostępnianie danych klientów. Jak można go zrealizować?

- [ ] Zapłacić okup
- [ ] Zidentyfikuj szczep oprogramowania ransomware
- [ ] Powiadomienie władz
- [ ] Określ, jakie dane zostały naruszone

Zobacz prawidłową odpowiedź →

Typ ataku: Infiltracja kopii zapasowych

1 — 2: Wykrywanie cyberzagrożeń i reagowanie na nie — 3 — 4

Twoim priorytetem jest szybkie udostępnianie danych klientów. Jak można go zrealizować?

- ✗ Zapłacić okup
- ✗ Zidentyfikuj szczep oprogramowania ransomware
- ✗ Powiadomienie władz
- ✓ Określ, jakie dane zostały naruszone

Identyfikacja zagrożonych danych pomaga skupić wysiłki związane z odzyskiwaniem danych na przywracaniu najważniejszych informacji o kliencie, zapewniając szybszą dostępność danych i unikając niepotrzebnej pracy w systemach, których problem nie dotyczy.

Następne pytanie →

Typ ataku: Infiltracja kopii zapasowych

1 — 2 — 3: Odzyskiwanie danych po cyberataku — 4

Stwierdzasz, że masz kopię zapasową do odzyskania. Jaki powinien być pierwszy krok w procesie?

- [ ] Najpierw należy ustalić priorytety przywracania systemów o znaczeniu krytycznym
- [ ] Użycie analizy śledczej, aby potwierdzić, że atak jest w pełni powstrzymany
- [ ] Zmiana wszystkich haseł i wycofanie naruszonych dane uwierzytelniające
- [ ] Wdrożenie zasady „zero trust”

Zobacz prawidłową odpowiedź →

Typ ataku: Infiltracja kopii zapasowych

1 — 2 — 3: Odzyskiwanie danych po cyberataku — 4

Stwierdzasz, że masz kopię zapasową do odzyskania. Jaki powinien być pierwszy krok w procesie?

- ✗ Najpierw należy ustalić priorytety przywracania systemów o znaczeniu krytycznym
- ✓ Użycie analizy śledczej, aby potwierdzić, że atak jest w pełni powstrzymany
- ✗ Zmiana wszystkich haseł i wycofanie naruszonych dane uwierzytelniające
- ✗ Wdrożenie zasady „zero trust”

Przed przywróceniem systemów należy upewnić się, że atak jest w pełni powstrzymany, aby zapobiec przypadkowej ponownej infekcji oraz dalszym uszkodzeniom i uniknąć utrwalenia lub eskalacji zagrożeń w środowisku.

Następne pytanie →

Typ ataku: Infiltracja kopii zapasowych

1 2 3 4: Ogólne najlepsze praktyki

Jakie są potencjalne sposoby ograniczenia ryzyka wystąpienia tego problemu w przyszłości?

- [ ] Stosuj zasady „zero trust”
- [ ] Możliwości wykrywania zagrożeń na punktach końcowych i reagowania na nie (EDR)
- [ ] Implementacja niezmiennych i odizolowanych kopii zapasowych
- [ ] Wszystkie powyższe

Zobacz prawidłową odpowiedź →

Typ ataku: Infiltracja kopii zapasowych

1 2 3 4: Ogólne najlepsze praktyki

Jakie są potencjalne sposoby ograniczenia ryzyka wystąpienia tego problemu w przyszłości?

- [x] Stosuj zasady „zero trust”
- [x] Możliwości wykrywania zagrożeń na punktach końcowych i reagowania na nie (EDR)
- [x] Implementacja niezmiennych i odizolowanych kopii zapasowych
- [x] Wszystkie powyższe

Zastosowanie wielowarstwowej strategii obrony może zmniejszyć ryzyko, zminimalizować szkody i zwiększyć odporność organizacji, ponieważ żaden pojedynczy środek nie jest wystarczający samodzielnie.

Zobacz rozwiązania →

TYP ATAKU: INFILTRACJA KOPII ZAPASOWYCH

Przypomnienie

Infiltracja kopii zapasowych występuje, gdy cyberprzestępcy wykorzystują luki w zabezpieczeniach systemów kopii zapasowych w celu naruszenia, zniszczenia lub zaszyfrowania krytycznych danych odzyskiwania. Te wyrafinowane ataki mogą zbiegać się w czasie lub następować po innych incydentach, takich jak instalacja oprogramowania typu ransomware lub złośliwego oprogramowania, co zwiększa straty operacyjne i finansowe.

W firmie Dell wierzymy w umożliwienie organizacjom zachowania odporności w obliczu ewoluujących zagrożeń cybernetycznych. Dzięki naszym najnowocześniejszym rozwiązaniom, specjalistycznym usługom i zaufanym partnerstwom jesteśmy gotowi pomóc Ci chronić to, co najważniejsze.

Dowiedz się więcej o naszych rozwiązaniach i o tym, jak radzimy sobie z najtrudniejszymi wyzwaniami w zakresie cyberbezpieczeństwa.

Zapoznaj się z opracowaniem na temat infiltracji kopii zapasowych →

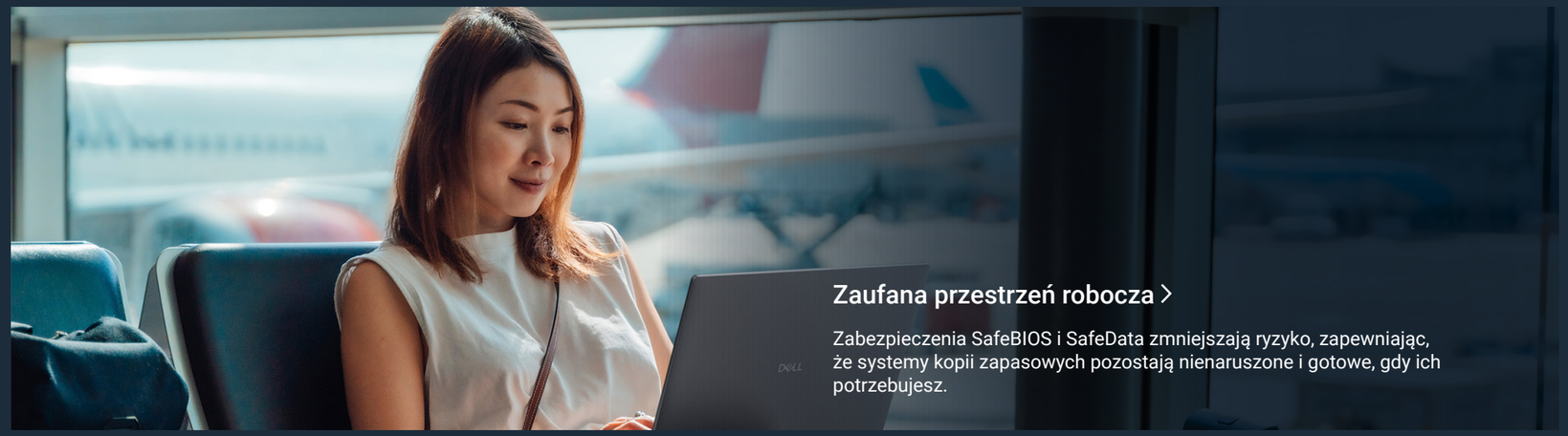
Wróć do scenariuszy

Oferta PowerProtect >

Nasze niezmienne, odizolowane i zaszyfrowane magazyny kopii zapasowych oparte na analizie sztucznej inteligencji CyberSense gwarantują szybkie wykrywanie ataków i odzyskiwanie danych, dzięki czemu odpowiednia odporność systemów jest zapewniona.

Serwery PowerEdge >

Dzięki bezpiecznemu rozruchowi, sprzętowemu źródłu zaufania i blokadzie systemu firma Dell zapewnia infrastrukturę, której można zaufać, jeśli chodzi o ochronę kopii zapasowych.

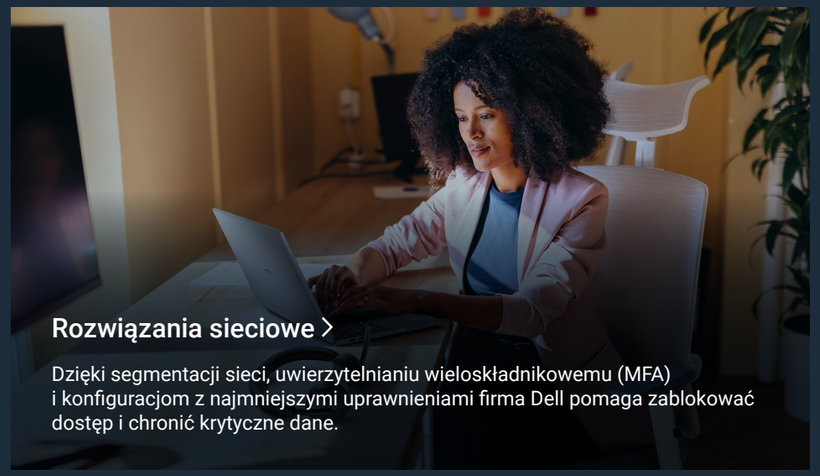


Zaufana przestrzeń robocza >

Zabezpieczenia SafeBIOS i SafeData zmniejszają ryzyko, zapewniając, że systemy kopii zapasowych pozostają nienaruszone i gotowe, gdy ich potrzebujesz.

Usługi związane z bezpieczeństwem i odpornością na zagrożenia >

Od bezpiecznego wdrożenia po proaktywne reagowanie na incydenty — nasi eksperci i partnerzy pomagają zwiększyć odporność na awarie i szybciej odzyskiwać dane.



Rozwiązania sieciowe >

Dzięki segmentacji sieci, uwierzytelnianiu wieloskładnikowemu (MFA) i konfiguracjom z najmniejszymi uprawnieniami firma Dell pomaga zablokować dostęp i chronić krytyczne dane.

Typ ataku: Rozproszona odmowa usługi (DDoS)

Jest wtorkowe popołudnie w agencji rządowej w dniu, w którym zapowiadana jest duża burza śnieżna.

Do zespołu IT w dziale transportu dociera zalew zgłoszeń od agentów, którzy nie mogą dostać się do żadnego ze swoich systemów, aby:

- Odnowić prawo jazdy
- Uzyskać pozwolenia drogowe
- Zapłacić podatki
- Sprawdzić warunki drogowe
- Uruchomić systemy reagowania kryzysowego, co opóźnia ekipom drogowym odśnieżanie/odladzanie dróg

wszystko ze względu na upłynięcie limitu czasu ich systemów.

Sprawdź swoją wiedzę →

Typ ataku: Rozproszona odmowa usługi (DDoS)

1: Zmniejszenie powierzchni ataku — 2 — 3 — 4

Co najpierw sprawdzić, aby dowiedzieć się, co się dzieje?

- [ ] Sprawdzić urządzenia sieciowe pod kątem nagłych, niewyjaśnionych skoków ruchu przychodzącego
- [ ] Sprawdzić urządzenia sieciowe pod kątem nietypowego ruchu z jednej lub ograniczonej liczby adresów IP
- [ ] Sprawdzić dzienniki zapory sieciowej lub narzędzi widoczności sieci pod kątem nadmiernej liczby nieudanych połączeń lub zdarzeń blokowania ruchu
- [ ] Wszystkie powyższe

Zobacz prawidłową odpowiedź →

Typ ataku: Rozproszona odmowa usługi (DDoS)

1: Zmniejszenie powierzchni ataku — 2 — 3 — 4

Co najpierw sprawdzić, aby dowiedzieć się, co się dzieje?

- [x] Sprawdzić urządzenia sieciowe pod kątem nagłych, niewyjaśnionych skoków ruchu przychodzącego
- [x] Sprawdzić urządzenia sieciowe pod kątem nietypowego ruchu z jednej lub ograniczonej liczby adresów IP
- [x] Sprawdzić dzienniki zapory sieciowej lub narzędzi widoczności sieci pod kątem nadmiernej liczby nieudanych połączeń lub zdarzeń blokowania ruchu
- [x] Wszystkie powyższe

Aby prawidłowo zdiagnozować powszechne awarie systemu, należy jednocześnie przejrzeć dzienniki aktywności urządzenia sieciowego i zapory sieciowej lub narzędzia widoczności, aby szybko wykryć nietypowe wzorce lub zdarzenia blokujące. Pozwala to na szybsze i dokładniejsze reagowanie na incydenty, ponieważ można wówczas odróżnić incydenty cybernetyczne od problemów z infrastrukturą.

Następne pytanie →

Typ ataku: Rozproszona odmowa usługi (DDoS)

1 — 2: Wykrywanie cyberzagrożeń i reagowanie na nie — 3 — 4

Podejrzewasz, że może to być atak DDoS. Jaki jest Twój pierwszy krok?

- [ ] Przekierowanie całego ruchu sieciowego za pośrednictwem usługi ograniczania DDoS
- [ ] Aktywowanie reguł zapory internetowej aplikacji (WAF) w celu odfiltrowania złośliwych wzorców
- [ ] Sprawdzenie, czy wzrost ruchu wynika z legalnych źródeł
- [ ] Wewnętrzne i zewnętrzne przekazanie aktualnych informacji

Zobacz prawidłową odpowiedź →

Typ ataku: Rozproszona odmowa usługi (DDoS)

1 — 2: Wykrywanie cyberzagrożeń i reagowanie na nie — 3 — 4

Podejrzewasz, że może to być atak DDoS. Jaki jest Twój pierwszy krok?

- ✗ Przekierowanie całego ruchu sieciowego za pośrednictwem usługi ograniczania DDoS
- ✗ Aktywowanie reguł zapory internetowej aplikacji (WAF) w celu odfiltrowania złośliwych wzorców
- ✓ Sprawdzenie, czy wzrost ruchu wynika z legalnych źródeł
- ✗ Wewnętrzne i zewnętrzne przekazanie aktualnych informacji

Przed aktywowaniem środków zaradczych DDoS należy sprawdzić zasadność wzrostu ruchu. Pozwala to uniknąć przypadkowego blokowania oryginalnych użytkowników, zapobiec zakłóceniom dla kluczowych interesariuszy i zapewnić, że wszelkie dalsze działania ochronne są odpowiednie i precyzyjnie ukierunkowane, minimalizując negatywny wpływ na operacje publiczne i ogólną ciągłość biznesową.

Następne pytanie →

Typ ataku: Rozproszona odmowa usługi (DDoS)

1 — 2 — 3: Odzyskiwanie danych po cyberataku — 4

Jakie kroki można podjąć, aby uniknąć ataku DDoS w przyszłości?

- [ ] Zablokowanie adresów IP, które naruszają bezpieczeństwo
- [ ] Przeprowadzanie regularnych testów penetracyjnych za pomocą symulacji DDoS
- [ ] Przeniesienie wszystkich aplikacji do chmury, ponieważ dostawcy chmury zwykle nie otrzymują ataków DDoS
- [ ] Wdrożenie zasady „zero trust”

Zobacz prawidłową odpowiedź →

Typ ataku: Rozproszona odmowa usługi (DDoS)

1 — 2 — 3: Odzyskiwanie danych po cyberataku — 4

Jakie kroki można podjąć, aby uniknąć ataku DDoS w przyszłości?

- ✗ Zablokowanie adresów IP, które naruszają bezpieczeństwo
- ✓ Przeprowadzanie regularnych testów penetracyjnych za pomocą symulacji DDoS
- ✗ Przeniesienie wszystkich aplikacji do chmury, ponieważ dostawcy chmury zwykle nie otrzymują ataków DDoS
- ✓ Wdrożenie zasady „zero trust”

Proaktywne testy penetracyjne przy użyciu symulacji DDoS określają i wzmacniają luki w zabezpieczeniach, podczas gdy mechanizmy zgodne z zasadami modelu „zero trust” koncentrują się na minimalizacji ryzyka poprzez wymuszanie nadania dostępu o najmniejszych uprawnieniach przez cały czas. Pomaga to zmniejszyć ryzyko zakłócenia podstawowych systemów, takich jak koordynacja reagowania awaryjnego lub sterowanie sygnałami drogowymi w czasie rzeczywistym, które muszą pozostać sprawne nawet podczas ataku.

Następne pytanie →

Typ ataku: Rozproszona odmowa usługi (DDoS)

1 2 3 4: Ogólne najlepsze praktyki

Kogo należy powiadomić w ramach ogólnego planu reagowania na incydenty i odzyskiwania danych (IRR)?

- [ ] Twój zespół prawny
- [ ] Twój dostawca cyberubezpieczeń
- [ ] CISA (Cybersecurity and Infrastructure Security Agency), FBI, MS-ISAC (Multi-State Information Sharing & Analysis Center)
- [ ] Wszystkie powyższe

Zobacz prawidłową odpowiedź →

Typ ataku: Rozproszona odmowa usługi (DDoS)

1 2 3 4: Ogólne najlepsze praktyki

Kogo należy powiadomić w ramach ogólnego planu reagowania na incydenty i odzyskiwania danych (IRR)?

- [x] Twój zespół prawny
- [x] Twój dostawca cyberubezpieczeń
- [x] CISA (Cybersecurity and Infrastructure Security Agency), FBI, MS-ISAC (Multi-State Information Sharing & Analysis Center)
- [x] Wszystkie powyższe

Podczas incydentu cybernetycznego na dużą skalę rozważ współpracę z agencjami prawnymi, ubezpieczeniowymi i rządowymi w zakresie zgodności z przepisami, roszczeń i egzekwowania prawa. Po sprawdzeniu, czy wszystkie wymogi regulacyjne są spełnione, Twoja organizacja może skutecznie odizolować incydent, rozwiązać go, a następnie odzyskać dane.

Zobacz rozwiązania →

TYP ATAKU: ROZPROSZONA ODMOWA USŁUGI (DDOS)

Przypomnienie

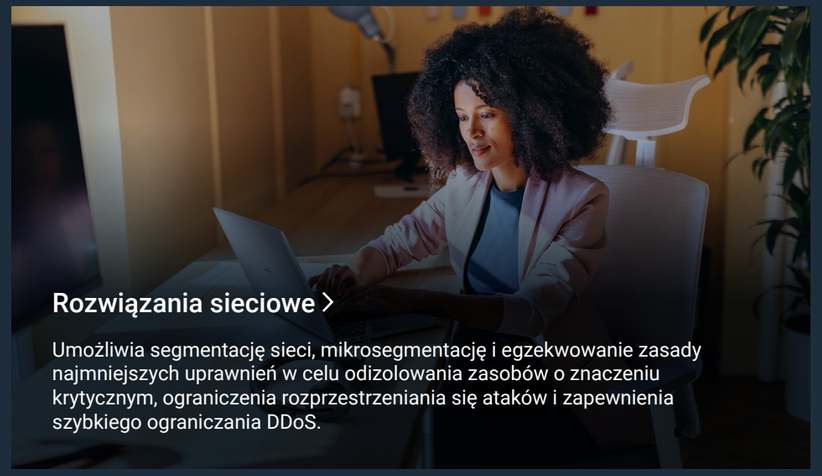
Atak DDoS ma na celu zakłócenie normalnego funkcjonowania sieci, usługi lub serwera poprzez przytłaczanie go ogromną ilością ruchu z wielu źródeł. Ataki te są wykonywane poprzez wykorzystanie botnetów, czyli sieci zainfekowanych urządzeń, które są zdalnie kontrolowane przez atakujących.

W firmie Dell pomagamy organizacjom zachować odporność na ataki DDoS, łącząc zaawansowane technologie wykrywania i minimalizacji zagrożeń ze specjalistycznymi usługami i podejściem zgodnym z modelem „zero trust", gwarantując szybką reakcję, minimalizację zakłóceń i wzmocnioną ochronę.

Dowiedz się więcej o zaawansowanych strategiach cyberodporności i o tym, w jaki sposób firma Dell może pomóc chronić Twoją organizację przed DDoS.

Zapoznaj się z opracowaniem na temat DDoS →

Wróć do scenariuszy



Rozwiązania sieciowe >

Umożliwia segmentację sieci, mikrosegmentację i egzekwowanie zasady najmniejszych uprawnień w celu odizolowania zasobów o znaczeniu krytycznym, ograniczenia rozprzestrzeniania się ataków i zapewnienia szybkiego ograniczania DDoS.

Serwery PowerEdge >

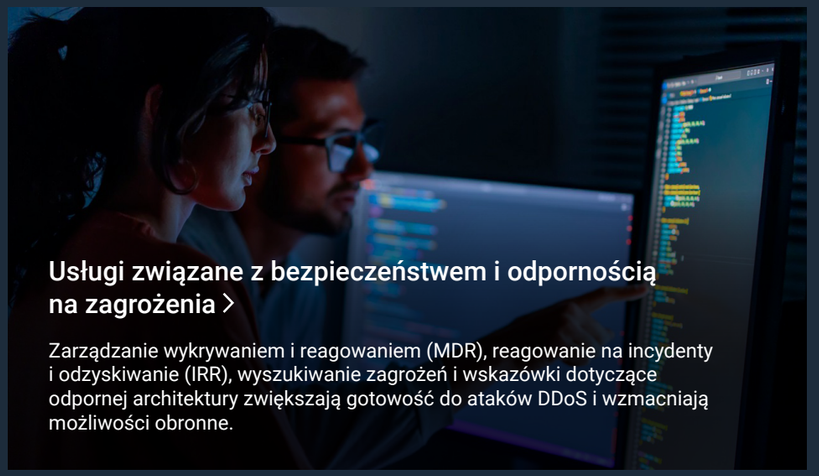
Dzięki sprzętowemu źródłu zaufania, rozwiązaniu Secure Boot, blokowaniu systemu i testom manipulacji w czasie rzeczywistym firma Dell zapewnia odporną, wydajną ochronę przed atakami DDoS i przyspieszone odzyskiwanie danych.

Zaufane urządzenia >

Zintegrowane funkcje SafeBIOS, SecureData oraz automatyczne wykrywanie i reagowanie zmniejszają powierzchnię ataku punktów końcowych nawet o 70%, zapobiegając dywersjom DDoS przemianę w wektory naruszeń.

Oferta PowerProtect >

Szyfrowane, niezmienne i odizolowane od sieci środowiska kopii zapasowych, obsługiwane przez analitykę zagrożeń opartą na AI, zapewniają szybkie, zweryfikowane przywracanie i utrzymują ciągłość działania podczas zakłóceń spowodowanych atakami DDoS.



Usługi związane z bezpieczeństwem i odpornością na zagrożenia >

Zarządzanie wykrywaniem i reagowaniem (MDR), reagowanie na incydenty i odzyskiwanie (IRR), wyszukiwanie zagrożeń i wskazówki dotyczące odpornej architektury zwiększają gotowość do ataków DDoS i wzmacniają możliwości obronne.

Typ ataku: Złośliwe zagrożenie wewnętrzne

Jest wtorek, 8:00 rano. Dzień roboczy dopiero się rozpoczyna dla pracowników w amerykańskiej firmie opieki zdrowotnej.

Pracowniczka wyższego szczebla, która pracuje z wysoce wrażliwymi danymi pacjentów, loguje się późnym wieczorem w biurze.

Zauważa zmiany w folderze, w którym pracowała poprzedniej nocy. Po konsultacji z zespołem kieruje zapytanie do działu IT.

Następnie po przeprowadzeniu dochodzenia odkrywają, że młodszy pracownik działu IT, który ma połączenia z syndykatem przestępczym, nakłonił pracownika wyższego szczebla do włożenia nośnika USB Rubber Ducky do urządzenia. W efekcie zamieniło to system podstawowych operacji wejścia-wyjścia (BIOS) w wersję podatną na ataki, co naraża cały system.

Sprawdź swoją wiedzę →

Typ ataku: Złośliwe zagrożenie wewnętrzne

1: Zmniejszenie powierzchni ataku — 2 — 3 — 4 — 5

Osoba, która wywołała atak wewnętrzny, zainicjowała ten atak przy użyciu dwóch metod śledzonych przez MITRE Adversarial Tactics, Technics i Common Knowledge, czyli strukturę MITRE ATT&CK. O jakie typy chodzi?

- [ ] Zaufana relacja + replikacja za pomocą nośników wymiennych
- [ ] Inżynieria społeczna + replikacja za pomocą nośników wymiennych
- [ ] Inżynieria społeczna + zewnętrzne usługi zdalne
- [ ] Zaufana relacja + dodatki sprzętowe

Zobacz prawidłową odpowiedź →

Typ ataku: Złośliwe zagrożenie wewnętrzne

1: Zmniejszenie powierzchni ataku — 2 — 3 — 4 — 5

Osoba, która wywołała atak wewnętrzny, zainicjowała ten atak przy użyciu dwóch metod śledzonych przez MITRE Adversarial Tactics, Technics i Common Knowledge, czyli strukturę MITRE ATT&CK. O jakie typy chodzi?

- ✗ Zaufana relacja + replikacja za pomocą nośników wymiennych
- ✓ Inżynieria społeczna + replikacja za pomocą nośników wymiennych
- ✗ Inżynieria społeczna + zewnętrzne usługi zdalne
- ✗ Zaufana relacja + dodatki sprzętowe

Stosując techniki MITER ATT&CK zarówno w zakresie manipulacji ludźmi, jak i replikacji za pośrednictwem przenośnej pamięci, osoba atakująca wykorzystała metody inżynierii społecznej, aby nakłonić starszego pracownika do podłączenia USB Rubber Ducky, co przekazało do urządzenia za pośrednictwem wymiennego nośnika uszkodzone dane.

Następne pytanie →

Typ ataku: Złośliwe zagrożenie wewnętrzne

1 — 2: Wykrywanie cyberzagrożeń i reagowanie na nie — 3 — 4 — 5

Dlaczego osoba atakująca musiała użyć obu metod?

- [ ] Przejść do sieci jako administrator globalny, aby obniżyć wersję systemu Basic Input/Output System (BIOS)
- [ ] Nakłonić administratora, aby umożliwił jej obniżenie wersji systemu BIOS
- [ ] Zmienić dostawcę systemu nazw domen (DNS) urządzenia, aby uzyskać poświadczenia potrzebne do jednorazowego dostępu do sieci
- [ ] Zainstalować złośliwe oprogramowanie na urządzeniu, aby uzyskać poświadczenia potrzebne do ciągłego dostępu do sieci

Zobacz prawidłową odpowiedź →

Typ ataku: Złośliwe zagrożenie wewnętrzne

1 — 2: Wykrywanie cyberzagrożeń i reagowanie na nie — 3 — 4 — 5

Dlaczego osoba atakująca musiała użyć obu metod?

- ✗ Przejść do sieci jako administrator globalny, aby obniżyć wersję systemu Basic Input/Output System (BIOS)
- ✗ Nakłonić administratora, aby umożliwił jej obniżenie wersji systemu BIOS
- ✗ Zmienić dostawcę systemu nazw domen (DNS) urządzenia, aby uzyskać poświadczenia potrzebne do jednorazowego dostępu do sieci
- ✓ Zainstalować złośliwe oprogramowanie na urządzeniu, aby uzyskać poświadczenia potrzebne do ciągłego dostępu do sieci

Osoba atakująca musiała użyć obu metod — instalacji złośliwego oprogramowania za pośrednictwem narzędzia USB Rubber Ducky w celu naruszenia zabezpieczeń urządzenia i poświadczeń umożliwiających ciągły dostęp do sieci — w celu ustanowienia trwałej, nieautoryzowanej kontroli nad środowiskiem docelowym.

Następne pytanie →

Typ ataku: Złośliwe zagrożenie wewnętrzne

1 — 2 — 3: Wykrywanie cyberzagrożeń i reagowanie na nie — 4 — 5

Jaki jest jeden ze sposobów wykrywania nieregularnej aktywności sieci?

- [ ] Kontrola aplikacji
- [ ] Extended Detection and Response („XDR”)
- [ ] Oprogramowanie antywirusowe nowej generacji (NGAV)
- [ ] Geofencing punktów końcowych

Zobacz prawidłową odpowiedź →

Typ ataku: Złośliwe zagrożenie wewnętrzne

1 — 2 — 3: Wykrywanie cyberzagrożeń i reagowanie na nie — 4 — 5

Jaki jest jeden ze sposobów wykrywania nieregularnej aktywności sieci?

- ✗ Kontrola aplikacji
- ✓ Extended Detection and Response („XDR”)
- ✗ Oprogramowanie antywirusowe nowej generacji (NGAV)
- ✗ Geofencing punktów końcowych

Jeśli chodzi o zapewnienie szerokiej, skorelowanej widoczności w celu szybkiego wykrywania zagrożeń, XDR najlepiej wykrywa podejrzaną aktywność sieci, ponieważ stale monitoruje i analizuje aktywność w punktach końcowych, sieciach i środowiskach chmurowych.

Następne pytanie →

Typ ataku: Złośliwe zagrożenie wewnętrzne

1 2 3 4: Odzyskiwanie danych po cyberataku 5

Jakie wbudowane zabezpieczenia komputera mogą wykryć podejrzaną aktywność na wczesnym etapie łańcucha cyberataków?

- [ ] Zarządzanie informacjami o zabezpieczeniach i zdarzeniami (SIEM)
- [ ] Extended Detection and Response („XDR”)
- [ ] Wskaźniki dołączenia (IOA)
- [ ] Kontrola dostępu oparta na rolach (RBAC)

Zobacz prawidłową odpowiedź →

DELL Technologies

Interaktywne scenariusze cyberbezpieczeństwa — e-book

Typ ataku: Złośliwe zagrożenie wewnętrzne

1 — 2 — 3 — 4: Odzyskiwanie danych po cyberataku — 5

Jakie wbudowane zabezpieczenia komputera mogą wykryć podejrzaną aktywność na wczesnym etapie łańcucha cyberataków?

- ✗ Zarządzanie informacjami o zabezpieczeniach i zdarzeniami (SIEM)
- ✗ Extended Detection and Response („XDR”)
- ✓ Wskaźniki dołączenia (IOA)
- ✗ Kontrola dostępu oparta na rolach (RBAC)

IOA koncentruje się na wykrywaniu zachowań atakujących i podejrzanych wzorców aktywności w czasie rzeczywistym, umożliwiając zespołom bezpieczeństwa identyfikację zagrożeń wcześniej, niż pozwalają na to metody oparte na sygnaturach i interweniowanie przed wystąpieniem poważnych szkód.

Następne pytanie →

Typ ataku: Złośliwe zagrożenie wewnętrzne

1 2 3 4 5: Ogólne najlepsze praktyki

Jakie środki można podjąć, po zidentyfikowaniu metody początkowego dostępu, aby przywrócić sprawność i zapobiec podobnym przyszłym naruszeniom?

- [ ] Aktualizacja systemu BIOS do najnowszej wersji
- [ ] Wyłączenie opcji przywracania systemu BIOS
- [ ] Wyłączenie portów USB
- [ ] Wdrożenie szczegółowej kontroli w celu umożliwienia bezpiecznego korzystania z urządzeń USB i zapobiegania rozprzestrzenianiu się złośliwego oprogramowania
- [ ] Wszystkie powyższe

Zobacz prawidłową odpowiedź →

Typ ataku: Złośliwe zagrożenie wewnętrzne

1 2 3 4 5: Ogólne najlepsze praktyki

Jakie środki można podjąć, po zidentyfikowaniu metody początkowego dostępu, aby przywrócić sprawność i zapobiec podobnym przyszłym naruszeniom?

- [x] Aktualizacja systemu BIOS do najnowszej wersji
- [x] Wyłączenie opcji przywracania systemu BIOS
- [x] Wyłączenie portów USB
- [x] Wdrożenie szczegółowej kontroli w celu umożliwienia bezpiecznego korzystania z urządzeń USB i zapobiegania rozprzestrzenianiu się złośliwego oprogramowania
- [x] Wszystkie powyższe

Poprzez rozwiązanie różnych wektorów ataków w celu zapewnienia bezpieczeństwa sprzętu i blokowania obniżania poziomu zabezpieczeń można ograniczyć zagrożenia oparte na podłączeniu nośników USB, a rozprzestrzenianie się złośliwego oprogramowania jest wówczas zatrzymywane w wielu punktach, aby pomóc w tworzeniu kompleksowej, warstwowej ochrony, która przywraca uszkodzone systemy i chroni przed przyszłymi naruszeniami.

Zobacz rozwiązania →

TYP ATAKU: ZŁOŚLIWE ZAGROŻENIE WEWNĘTRZNE

Przypomnienie

Złośliwy atak wewnętrzny ma miejsce, gdy osoba w organizacji wykorzystuje swoje uprawnienia do naruszenia danych, zakłócenia działalności lub pozyskania poufnych informacji w celu osiągnięcia osobistych, finansowych lub konkurencyjnych celów. Osobą tą może być pracownik, wykonawca, partner lub ktokolwiek posiadający legalny dostęp do systemów i sieci firmy.

Firma Dell chroni się przed złośliwymi cyberatakami wewnętrznymi dzięki połączeniu zaawansowanych technologii i rygorystycznych protokołów bezpieczeństwa.

Dowiedz się więcej o zaawansowanych strategiach cyberodporności i o tym, w jaki sposób firma Dell może pomóc chronić Twoją organizację przed złośliwymi atakami wewnętrznymi.

Zapoznaj się z opracowaniem na temat złośliwych zagrożeń wewnętrznych →

Wróć do scenariuszy

Zaufane urządzenia i infrastruktura >

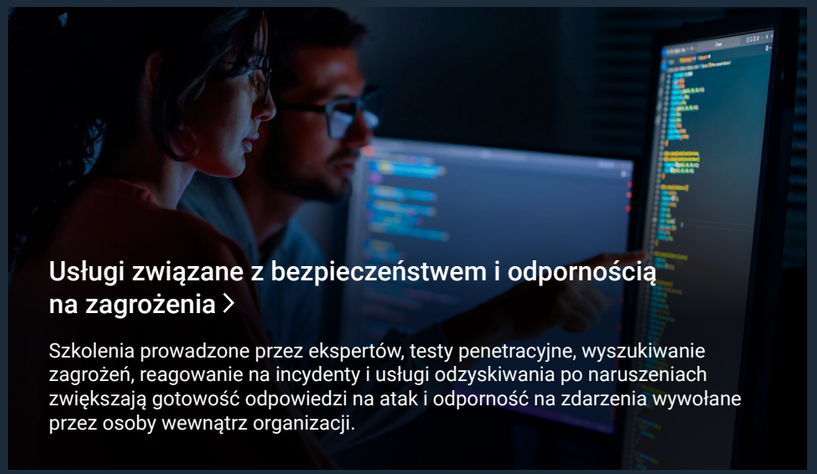
Wbudowane zabezpieczenia wymuszające dostęp o najmniejszych uprawnieniach, uwierzytelnianie wieloskładnikowe (MFA), kontrola dostępu oparta na rolach (RBAC), podwójne uwierzytelnianie i ochrona w modelu „zero trust" chronią punkty końcowe i infrastrukturę, zmniejszając ryzyko wystąpienia zagrożeń wewnętrznych.

Serwery PowerEdge >

Sprzętowe źródło zaufania, rozwiązanie Secure Boot, dynamiczne zarządzanie gniazdami USB i blokowanie systemu chronią przed manipulacjami i powstrzymują wewnętrzne ataki fizyczne lub oparte na oprogramowaniu wewnętrznym.

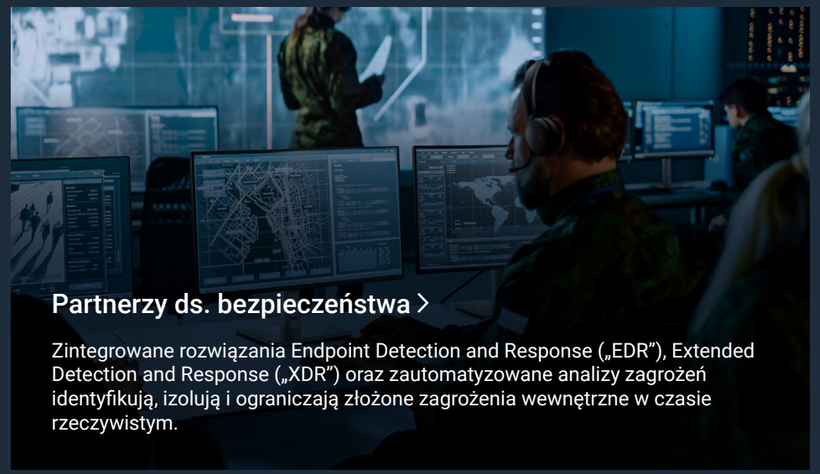
Oferta PowerProtect >

Niemodyfikowalne, izolowane kopie zapasowe zapewniają integralność danych, szybkie przywracanie i wczesne wykrywanie prób manipulacji danymi, umożliwiając odzyskiwanie danych po incydentach wewnętrznych.



Usługi związane z bezpieczeństwem i odpornością na zagrożenia >

Szkolenia prowadzone przez ekspertów, testy penetracyjne, wyszukiwanie zagrożeń, reagowanie na incydenty i usługi odzyskiwania po naruszeniach zwiększają gotowość odpowiedzi na atak i odporność na zdarzenia wywołane przez osoby wewnątrz organizacji.



Partnerzy ds. bezpieczeństwa >

Zintegrowane rozwiązania Endpoint Detection and Response („EDR"), Extended Detection and Response („XDR") oraz zautomatyzowane analizy zagrożeń identyfikują, izolują i ograniczają złożone zagrożenia wewnętrzne w czasie rzeczywistym.

Typ ataku: Man-in-the-Middle (MITM)

Nieświadomy klient łączy się z bezpłatną, niezabezpieczoną siecią Wi-Fi w kawiarni, aby sfinalizować ostatnie aktualizacje do wspólnego dokumentu zespołu.

Chwilę później dział IT jego firmy otrzymuje powiadomienia o nietypowych próbach logowania z konta pracownika, a także o nieautoryzowanym dostępie do danych z wielu lokalizacji na całym świecie.

Po przeprowadzeniu dochodzenia potwierdza, że osoba atakująca przechwyciła i manipulowała połączeniem bezprzewodowym, uzyskując dostęp do poufnych informacji.

Sprawdź swoją wiedzę →

Typ ataku: Man-in-the-Middle (MITM)

1: Zmniejszenie powierzchni ataku — 2 — 3 — 4

Gdzie jest pierwsze miejsce, które zespół IT powinien zbadać po wykryciu nietypowych prób logowania?

- [ ] Zapora internetowa, system wykrywania włamań, dzienniki systemu zapobiegania włamaniom (IPS) i rozszerzone wykrywanie i reagowanie (XDR)
- [ ] Notebook pracownika, którego dotyczy problem
- [ ] Ruch sieciowy w niezabezpieczonej sieci Wi-Fi w kawiarni
- [ ] Dzienniki uwierzytelniania z systemów firmy

Zobacz prawidłową odpowiedź →

DELL Technologies

Interaktywne scenariusze cyberbezpieczeństwa — e-book

Typ ataku: Man-in-the-Middle (MITM)

1: Zmniejszenie powierzchni ataku — 2 — 3 — 4

Gdzie jest pierwsze miejsce, które zespół IT powinien zbadać po wykryciu nietypowych prób logowania?

- ✓ Zapora internetowa, system wykrywania włamań, dzienniki systemu zapobiegania włamaniom (IPS) i rozszerzone wykrywanie i reagowanie (XDR)
- ✗ Notebook pracownika, którego dotyczy problem
- ✗ Ruch sieciowy w niezabezpieczonej sieci Wi-Fi w kawiarni
- ✓ Dzienniki uwierzytelniania z systemów firmy

Analizując te dzienniki zapory sieciowej oraz systemów IDS/IPS i uwierzytelniania, zespoły IT mogą monitorować próby nieautoryzowanego uzyskania dostępu, oceniać naruszone konta i lepiej zrozumieć zakres ataku.

Następne pytanie →

Typ ataku: Man-in-the-Middle (MITM)

1 — 2: Wykrywanie cyberzagrożeń i reagowanie na nie — 3 — 4

Jakie natychmiastowe działania powinien podjąć zespół IT po potwierdzeniu ataku MITM?

- [ ] Natychmiastowe odłączenie urządzenia pracownika, którego dotyczy problem, od sieci i jego wyizolowanie do analizy
- [ ] Zaktualizowanie reguł zapory sieciowej i konfiguracje sieci w celu zatrzymania dalszego nieautoryzowanego dostępu
- [ ] Zresetowanie haseł do wszystkich kont pracowników
- [ ] Wyłączenie systemów, których dotyczy problem, w ce;lu zapobieżenia eksfiltracji danych

Zobacz prawidłową odpowiedź →

Typ ataku: Man-in-the-Middle (MITM)

1 — 2: Wykrywanie cyberzagrożeń i reagowanie na nie — 3 — 4

Jakie natychmiastowe działania powinien podjąć zespół IT po potwierdzeniu ataku MITM?

- ✓ Natychmiastowe odłączenie urządzenia pracownika, którego dotyczy problem, od sieci i jego wyizolowanie do analizy
- ✓ Zaktualizowanie reguł zapory sieciowej i konfiguracje sieci w celu zatrzymania dalszego nieautoryzowanego dostępu
- ✗ Zresetowanie haseł do wszystkich kont pracowników
- ✗ Wyłączenie systemów, których dotyczy problem, w ce;lu zapobieżenia eksfiltracji danych

Natychmiastowe odłączenie i odizolowanie narażonego urządzenia zatrzymuje dostęp atakującego i zachowuje dowody śledcze, a jednocześnie aktualizuje zaporę i reguły sieciowe blokuje dalsze złośliwe połączenia i chroni szerszą sieć przed trwającymi atakami.

Następne pytanie →

Typ ataku: Man-in-the-Middle (MITM)

1 — 2 — 3: Odzyskiwanie danych po cyberataku — 4

Jakie środki zapobiegawcze mogły zmniejszyć podatność na atak MITM?

- [ ] Wymuszanie korzystania z wirtualnej sieci prywatnej (VPN) dla wszystkich pracowników
- [ ] Wdrożenie zasad bezpieczeństwa „zero trust”, takich jak uwierzytelnianie wieloskładnikowe (MFA)
- [ ] Unikanie korzystania z publicznych sieci Wi-Fi
- [ ] Szyfrowanie wrażliwych plików udostępnianych pocztą e-mail

Zobacz prawidłową odpowiedź →

DELL Technologies

Interaktywne scenariusze cyberbezpieczeństwa — e-book

Typ ataku: Man-in-the-Middle (MITM)

1 — 2 — 3: Odzyskiwanie danych po cyberataku — 4

Jakie środki zapobiegawcze mogły zmniejszyć podatność na atak MITM?

- ✓ Wymuszanie korzystania z wirtualnej sieci prywatnej (VPN) dla wszystkich pracowników
- ✓ Wdrożenie zasad bezpieczeństwa „zero trust”, takich jak uwierzytelnianie wieloskładnikowe (MFA)
- ✗ Unikanie korzystania z publicznych sieci Wi-Fi
- ✗ Szyfrowanie wrażliwych plików udostępnianych pocztą e-mail

Wymuszanie korzystania z VPN za pośrednictwem niezabezpieczonych sieci szyfruje ruch internetowy pracowników, aby zapobiec przechwyceniu, a jednocześnie wdraża zabezpieczenia modelu „zero trust”, podczas gdy uwierzytelnianie MFA zapewnia ciągłą weryfikację każdego żądania dostępu.

Następne pytanie →

Typ ataku: Man-in-the-Middle (MITM)

1 2 3 4: Ogólne najlepsze praktyki

Jakie długoterminowe strategie, po rozwiązaniu problemu naruszenia, powinna wdrożyć Twoja organizacja?

- [ ] Regularne audyty i poprawki systemów
- [ ] Zwiększenie segmentacji sieci w celu odizolowania wrażliwych danych i systemów
- [ ] Wdrożenie rozwiązań do wykrywania punktów końcowych i reagowania na nie (EDR) oraz zarządzanych rozwiązań do wykrywania i reagowania na nie (MDR)
- [ ] Wdrożenie solidnych i regularnych szkoleń dla pracowników
- [ ] Wszystkie powyższe

Zobacz prawidłową odpowiedź →

Typ ataku: Man-in-the-Middle (MITM)

1 2 3 4: Ogólne najlepsze praktyki

Jakie długoterminowe strategie, po rozwiązaniu problemu naruszenia, powinna wdrożyć Twoja organizacja?

- [x] Regularne audyty i poprawki systemów
- [x] Zwiększenie segmentacji sieci w celu odizolowania wrażliwych danych i systemów
- [x] Wdrożenie rozwiązań do wykrywania punktów końcowych i reagowania na nie (EDR) oraz zarządzanych rozwiązań do wykrywania i reagowania na nie (MDR)
- [x] Wdrożenie solidnych i regularnych szkoleń dla pracowników
- [x] Wszystkie powyższe

Aby chronić się przed różnymi zagrożeniami, te długoterminowe strategie łączą siły w celu utworzenia kompleksowego, odpornego stanu bezpieczeństwa, który blokuje atakujących przed wykorzystywaniem luk w zabezpieczeniach oraz zapewnia szybką i skuteczną reakcję na naruszenia sieci zabezpieczeń.

Zobacz rozwiązania →

TYP ATAKU: MAN-IN-THE-MIDDLE (MITM)

Przypomnienie

Atak typu MITM ma miejsce, gdy cyberprzestępca potajemnie przechwytuje komunikację między dwiema stronami, np. między pracownikiem a serwerem korporacyjnym lub klientem a witryną firmową. Cel atakującego może być różny, ale wynik jest taki sam: naruszenie zaufania i bezpieczeństwa.

W firmie Dell dostarczamy innowacyjne, skalowalne rozwiązania w zakresie zabezpieczeń, które umożliwiają organizacjom neutralizację zagrożeń MITM, ochronę zasobów i utrzymanie integralności biznesowej dzięki narzędziom i wiedzy eksperckiej potrzebnej do niezawodnego wykrywania zagrożeń, reagowania na nie i odzyskiwania danych.

Dowiedz się więcej o zaawansowanych strategiach cyberodporności i przekonaj się, w jaki sposób firma Dell może pomóc chronić Twoją organizację przed atakami MITM.

Przeczytaj krótki opis ataków MITM →

Wróć do scenariuszy

Zaufane urządzenia >

Dzięki uwierzytelnianiu na poziomie sprzętu, zabezpieczeniom oprogramowania wewnętrznego, takim jak SafeBIOS i SafeID, solidnemu szyfrowaniu i strukturze „zero trust", firma Dell zabezpiecza punkty końcowe i dane w ruchu.

Serwery PowerEdge >

Bezpieczny rozruch, źródło zaufania, dynamiczne zarządzanie portami USB i blokady systemu zapewniają integralność sprzętu i ochronę krytycznych obciążeń roboczych przed zagrożeniami sieciowymi.

Rozwiązania pamięci masowej >

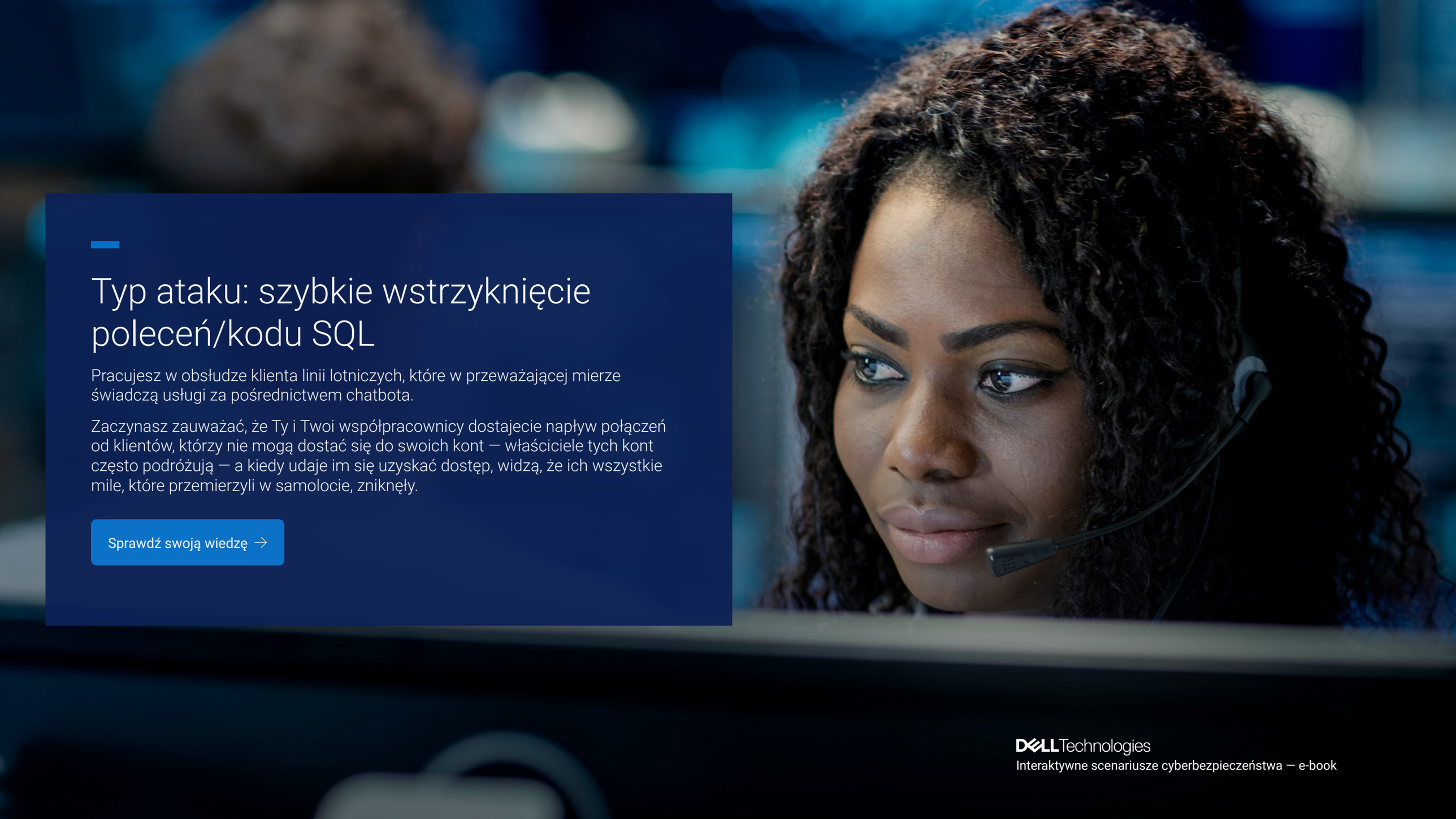
Szyfrowane dane w spoczynku i w trakcie transmisji, w połączeniu z izolowanymi migawkami i funkcjami szybkiego odzyskiwania, zapewniają, że pliki pozostają bezpieczne i mogą być szybko przywrócone po ataku MITM.

Oferta PowerProtect >

Niemodyfikowalne, izolowane kopie zapasowe i analiza CyberSense oparta na sztucznej inteligencji umożliwiają szybkie odzyskiwanie i przywracanie zaufanych danych w przypadku ataku MITM.

Usługi związane z bezpieczeństwem i odpornością na zagrożenia >

Eksperci i partnerzy firmy Dell zapewniają kompleksowe wsparcie w celu wzmocnienia zabezpieczeń — od oceny podatności i szkoleń użytkowników po testy penetracyjne i reagowanie na incydenty.



Typ ataku: szybkie wstrzyknięcie poleceń/kodu SQL

Pracujesz w obsłudze klienta linii lotniczych, które w przeważającej mierze świadczą usługi za pośrednictwem chatbota.

Zaczynasz zauważać, że Ty i Twoi współpracownicy dostajecie napływ połączeń od klientów, którzy nie mogą dostać się do swoich kont — właściciele tych kont często podróżują — a kiedy udaje im się uzyskać dostęp, widzą, że ich wszystkie mile, które przemierzyli w samolocie, zniknęły.

Sprawdź swoją wiedzę →

Typ ataku: szybkie wstrzyknięcie poleceń/kodu SQL

1: Zmniejszenie powierzchni ataku — 2 — 3 — 4

Po sprawdzeniu widać pewne błędy w dziennikach; *Błąd składni w instrukcji języka zapytań strukturalnych (SQL) lub Nieprawidłowa nazwa kolumny „admin”*. Jaki to rodzaj incydentu cybernetycznego?

- [ ] Skradzione poświadczenia
- [ ] Szybkie wstrzyknięcie poleceń lub kodu SQL:
- [ ] Atak typu Man-in-the-Middle (MITM)
- [ ] Wyłudzanie informacji

Zobacz prawidłową odpowiedź →

Typ ataku: szybkie wstrzyknięcie poleceń/kodu SQL

1: Zmniejszenie powierzchni ataku — 2 — 3 — 4

Po sprawdzeniu widać pewne błędy w dziennikach; *Błąd składni w instrukcji języka zapytań strukturalnych (SQL)* lub *Nieprawidłowa nazwa kolumny „admin”*. Jaki to rodzaj incydentu cybernetycznego?

- ✗ Skradzione poświadczenia
- ✓ Szybkie wstrzyknięcie poleceń lub kodu SQL:
- ✗ Atak typu Man-in-the-Middle (MITM)
- ✗ Wyłudzanie informacji

„Szybkie wstrzyknięcie poleceń lub kodu SQL” jest poprawną odpowiedzią, ponieważ błędy dziennika, takie jak „Syntax error in SQL statement” lub „Invalid coull name ‘admin’”, ujawniają fakt, że atakujący wykorzystali pola wejściowe chatbota, używając złośliwego kodu SQL, w celu uzyskania dostępu do danych konta klienta lub zmiany tych danych, które są jasnymi wskaźnikami technicznymi potencjalnego ataku

Następne pytanie →

Typ ataku: szybkie wstrzyknięcie poleceń/kodu SQL

1 — 2: Wykrywanie cyberzagrożeń i reagowanie na nie — 3 — 4

Zdajesz sobie sprawę, że masz do czynienia z szybkim wstrzyknięciem poleceń/kodu SQL za pośrednictwem chatbota obsługi klienta. Co należy zrobić?

- [ ] Przełączyć bota w tryb offline
- [ ] Zbadać dzienniki bazy danych pod kątem nieautoryzowanego dostępu oraz skradzionych, zmodyfikowanych lub usuniętych danych
- [ ] Zastosować się do wszystkich przepisów dotyczących ujawniania naruszeń danych
- [ ] Wszystkie powyższe

Zobacz prawidłową odpowiedź →

Typ ataku: szybkie wstrzyknięcie poleceń/kodu SQL

1 — 2: Wykrywanie cyberzagrożeń i reagowanie na nie — 3 — 4

Zdajesz sobie sprawę, że masz do czynienia z szybkim wstrzyknięciem poleceń/kodu SQL za pośrednictwem chatbota obsługi klienta. Co należy zrobić?

- [x] Przełączyć bota w tryb offline
- [x] Zbadać dzienniki bazy danych pod kątem nieautoryzowanego dostępu oraz skradzionych, zmodyfikowanych lub usuniętych danych
- [x] Zastosować się do wszystkich przepisów dotyczących ujawniania naruszeń danych
- [x] Wszystkie powyższe

Reagowanie na atak za pomocą szybkiego wstrzyknięcia poleceń/kodu SQL wymaga przełączenia chatbota w tryb offline, zbadania dzienników bazy danych pod kątem nieautoryzowanego dostępu i zapewnienia zgodności z przepisami dotyczącymi ujawniania informacji. Kroki te są niezbędne do powstrzymania wykorzystania danych, oceny szkód oraz spełnienia wymogów prawnych i etycznych.

Następne pytanie →

Typ ataku: szybkie wstrzyknięcie poleceń/kodu SQL

1 — 2 — 3: Odzyskiwanie danych po cyberataku — 4

Jakie możliwości należy wdrożyć, aby pomóc w zatrzymaniu szybkich wstrzyknięć poleceń/kodu SQL?

- [ ] Edukowanie zespołów programistów, aby używały przygotowanych instrukcji i sparametryzowanych zapytań jako praktyki kodowania
- [ ] Narzędzia Manage Detection and Response (MDR)
- [ ] Wdrożenie dostępu o najmniejszych uprawnieniach, takich jak uwierzytelnianie wieloskładnikowe (MFA), kontrola dostępu oparta na rolach (RBAC), zapora aplikacji sieciowych (WAF) itp.
- [ ] Segmentowanie backendowych baz danych/baz wiedzy

Zobacz prawidłową odpowiedź →

Typ ataku: szybkie wstrzyknięcie poleceń/kodu SQL

1 — 2 — 3: Odzyskiwanie danych po cyberataku — 4

Jakie możliwości należy wdrożyć, aby pomóc w zatrzymaniu szybkich wstrzyknięć poleceń/kodu SQL?

- ✓ Edukowanie zespołów programistów, aby używały przygotowanych instrukcji i sparametryzowanych zapytań jako praktyki kodowania
- ✗ Narzędzia Manage Detection and Response (MDR)
- ✓ Wdrożenie dostępu o najmniejszych uprawnieniach, takich jak uwierzytelnianie wieloskładnikowe (MFA), kontrola dostępu oparta na rolach (RBAC), zapora aplikacji sieciowych (WAF) itp.
- ✗ Segmentowanie backendowych baz danych/baz wiedzy

Szkolenie zespołów programistów z korzystania z przygotowanych instrukcji i zapytań o określonych parametrach blokuje ataki „wstrzykiwania poleceń/kodu SQL" u źródła, a jednocześnie wymusza kontrolę dostępu o najmniejszych uprawnieniach, takich jak MFA, RBAC i WAF, co ogranicza wpływ każdej próby wstrzyknięcia, uniemożliwiając atakującym eskalację uprawnień lub poprzecznemu przenoszeniu zagrożeń.

Następne pytanie →

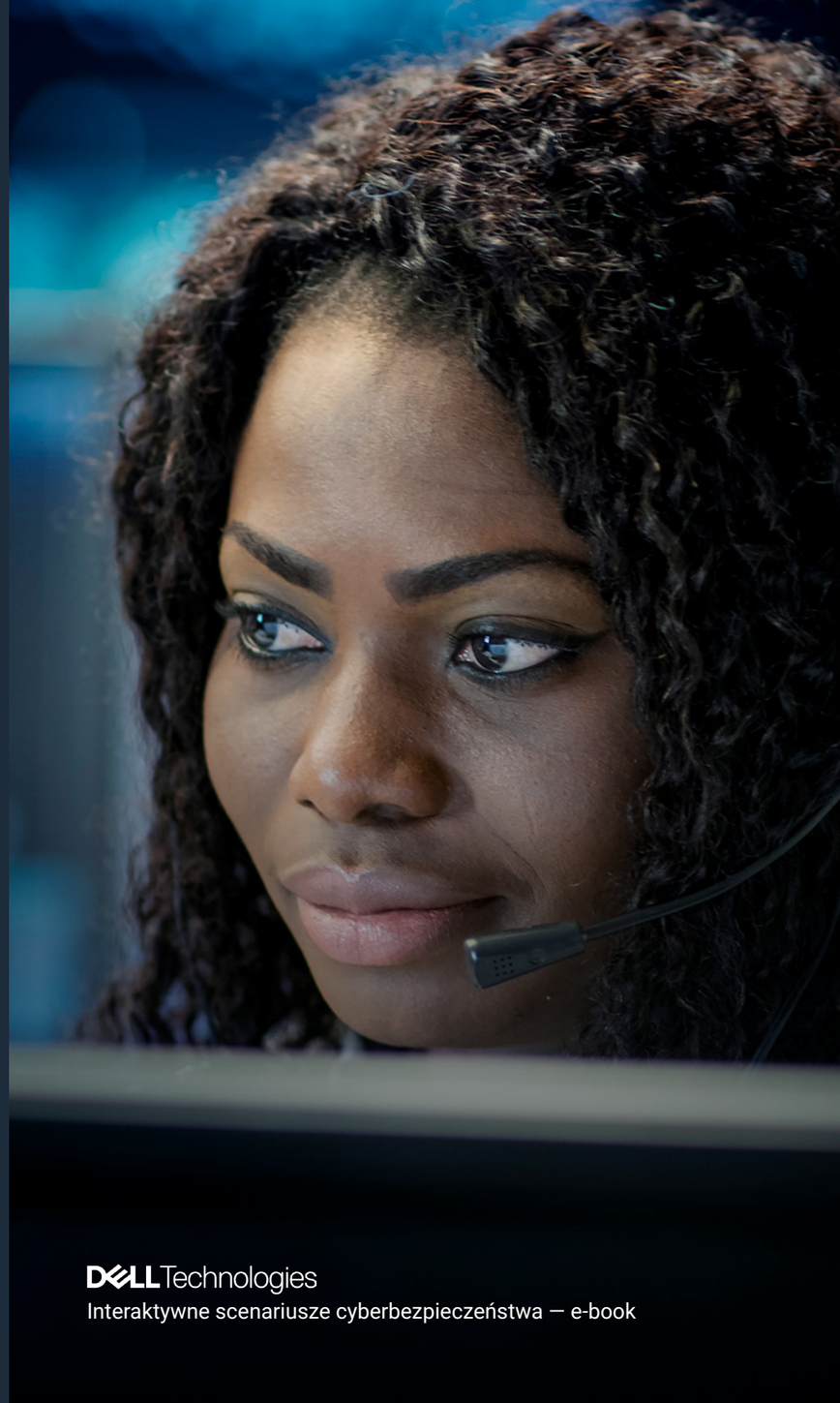
Typ ataku: szybkie wstrzyknięcie poleceń/kodu SQL

1 2 3 4: Ogólne najlepsze praktyki

Jakie kroki należy podjąć, aby odzyskać dane klientów linii lotniczych?

- [ ] Prześledzenie skradzionych danych
- [ ] Poproszenie klientów o odbudowę profili
- [ ] Odkupienie ich od cyberprzestępców
- [ ] Przywrócenie z najnowszej, niezagrożonej kopii zapasowej w celu przywrócenia utraconych danych dotyczących mil lojalnościowych za przeloty często podróżującym klientom, a następnie poinformowaniu ich o konieczności zmiany hasła i sprawdzenia kart kredytowych

Zobacz prawidłową odpowiedź →



DELL Technologies

Interaktywne scenariusze cyberbezpieczeństwa — e-book

Typ ataku: szybkie wstrzyknięcie poleceń/kodu SQL

1 — 2 — 3 — 4: Ogólne najlepsze praktyki

Jakie kroki należy podjąć, aby odzyskać dane klientów linii lotniczych?

- ✗ Prześledzenie skradzionych danych
- ✗ Poproszenie klientów o odbudowę profili
- ✗ Odkupienie ich od cyberprzestępców
- ✓ Przywrócenie z najnowszej, niezagrożonej kopii zapasowej w celu przywrócenia utraconych danych dotyczących mil lojalnościowych za przeloty często podróżującym klientom, a następnie poinformowaniu ich o konieczności zmiany hasła i sprawdzenia kart kredytowych

Odzyskanie utraconych danych z najnowszej nienaruszonej kopii zapasowej pomaga utrzymać integralność danych i skrócić przestoje. Szybkie informowanie klientów o konieczności zresetowania haseł i monitorowania aktywności kart kredytowych dodatkowo wpływa na poprawne przestrzeganie zgodności z przepisami po destrukcyjnym ataku „wstrzyknięcia".

Zobacz rozwiązania →

TYP ATAKU: SZYBKIE WSTRZYKNIĘCIE POLECEŃ/KODU SQL

Przypomnienie

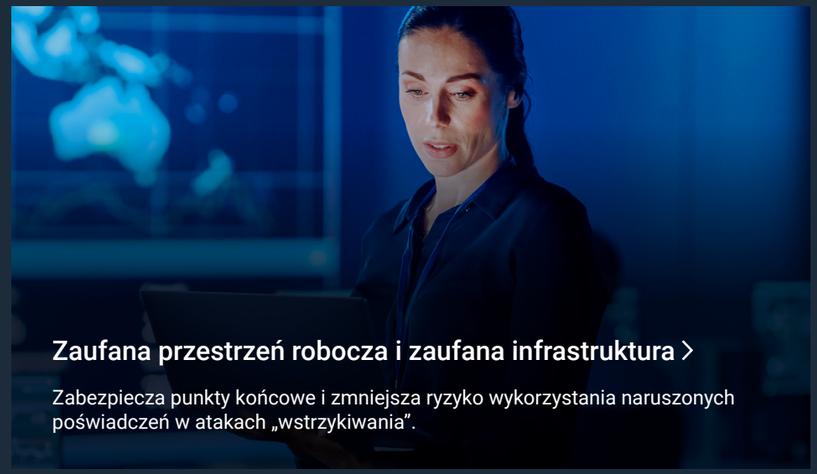
Ataki polegające na szybkim wstrzyknięciu poleceń/kodu SQL wielokrotnie okazywały się jednymi z najbardziej szkodliwych i wszechobecnych metod cyberataku używanych przez cyberprzestępców. Ataki te wykorzystują luki w zabezpieczeniach systemów zapytań użytkowników lub baz danych, umożliwiając złośliwym podmiotom manipulowanie serwerami, kradzież danych lub zakłócanie przepływów pracy.

Ochrona organizacji przed ewoluującymi zagrożeniami i atakami szybkich wstrzyknięć poleceń/kodu SQL jest elementem ciągłego zaangażowania firmy Dell w cyberbezpieczeństwo. Zapewniamy narzędzia i wiedzę ekspercką potrzebne do wykrywania, reagowania i odzyskiwania danych.

Odkryj zaawansowane strategie cyberodporności i przekonaj się, w jaki sposób firma Dell może pomóc Twojej organizacji w ochronie przed atakami polegającymi na szybkim wstrzyknięciu poleceń/kodu SQL.

Zapoznaj się z omówieniem na temat szybkiego wstrzyknięcia poleceń/kodu SQL →

Wróć do scenariuszy

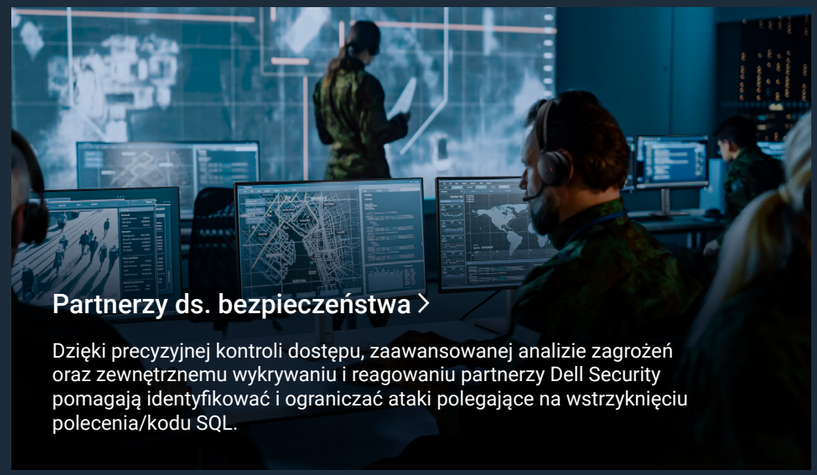


Zaufana przestrzeń robocza i zaufana infrastruktura >

Zabezpiecza punkty końcowe i zmniejsza ryzyko wykorzystania naruszonych poświadczeń w atakach „wstrzykiwania”.

Serwery PowerEdge >

Serwery Dell PowerEdge zapewniają odporną na manipulacje infrastrukturę, która uruchamia wyłącznie zaufany kod, ponieważ zapewniają sprzętowe źródło zaufania, rozwiązanie Secure Boot, zabezpieczenia na poziomie układów scalonych i weryfikację konfiguracji w czasie rzeczywistym.

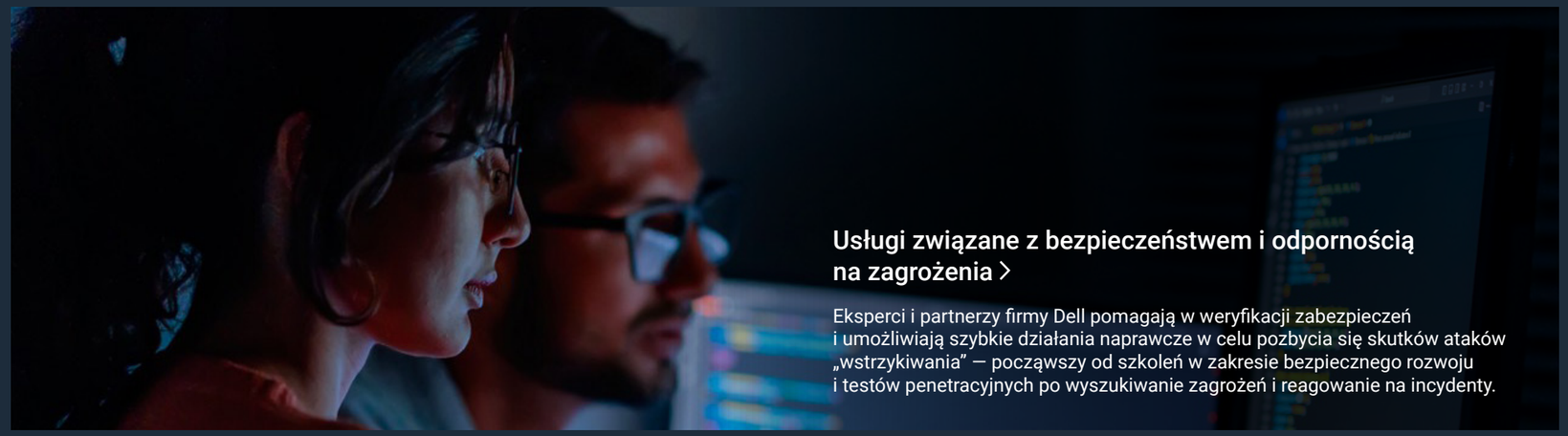


Partnerzy ds. bezpieczeństwa >

Dzięki precyzyjnej kontroli dostępu, zaawansowanej analizie zagrożeń oraz zewnętrznemu wykrywaniu i reagowaniu partnerzy Dell Security pomagają identyfikować i ograniczać ataki polegające na wstrzyknięciu polecenia/kodu SQL.

Oferta PowerProtect >

Niemodyfikowalne, odizolowane od sieci kopie zapasowe firmy Dell oraz zaawansowane analizy odzyskiwania danych zapewniają zaufane punkty przywracania, umożliwiając szybkie przywrócenie danych w przypadku ich uszkodzenia lub wycieku.



Usługi związane z bezpieczeństwem i odpornością na zagrożenia >

Eksperci i partnerzy firmy Dell pomagają w weryfikacji zabezpieczeń i umożliwiają szybkie działania naprawcze w celu pozbycia się skutków ataków „wstrzykiwania” — począwszy od szkoleń w zakresie bezpiecznego rozwoju i testów penetracyjnych po wyszukiwanie zagrożeń i reagowanie na incydenty.

Typ ataku: Ransomware

Jesteś specjalistą IT w regionalnym szpitalu znanym z połączonych systemów medycznych — w tym elektronicznej dokumentacji medycznej (EHR), inteligentnych pomp infuzji i obrazowania radiologicznego — wszystko powiązane ze scentralizowaną siecią.

W nocy kilka systemów zaczęło się jednocześnie zawieszać. Rano personel kliniczny zgłasza, że ich dostęp do dokumentacji pacjentów został zablokowany.

Na kilku terminalach pojawia się następujący list z żądaniem okupu:

„Twoje pliki są zaszyfrowane. Zapłać 20 Bitcoinów w ciągu 72 godzin albo dane pacjentów zostaną opublikowane”.

Sprawdź swoją wiedzę →

Typ ataku: Ransomware

1: Zmniejszenie powierzchni ataku — 2 — 3 — 4

Dział pomocy technicznej otrzymuje ponad 100 zgłoszeń o błędach szyfrowania plików i aplikacji. Dzienniki zabezpieczeń pokazują nietypową aktywność zmieniania nazw plików z konta domeny wewnętrznej. Jaki jest Twój pierwszy krok?

- [ ] Natychmiastowa zapłata okupu w celu przywrócenia usług o znaczeniu krytycznym
- [ ] Powiadomienie organów ścigania i radcy prawnego
- [ ] Rozpoczęcie ponownego tworzenia obrazów wszystkich punktów końcowych, których dotyczy problem
- [ ] Odłączenie zainfekowanych systemów od sieci

Zobacz prawidłową odpowiedź →

Typ ataku: Ransomware

1: Zmniejszenie powierzchni ataku — 2 — 3 — 4

Dział pomocy technicznej otrzymuje ponad 100 zgłoszeń o błędach szyfrowania plików i aplikacji. Dzienniki zabezpieczeń pokazują nietypową aktywność zmieniania nazw plików z konta domeny wewnętrznej. Jaki jest Twój pierwszy krok?

- ✗ Natychmiastowa zapłata okupu w celu przywrócenia usług o znaczeniu krytycznym
- ✗ Powiadomienie organów ścigania i radcy prawnego
- ✗ Rozpoczęcie ponownego tworzenia obrazów wszystkich punktów końcowych, których dotyczy problem
- ✓ Odłączenie zainfekowanych systemów od sieci

Natychmiastowe odłączenie i odizolowanie zainfekowanych systemów szpitalnych powstrzymuje rozprzestrzenianie się oprogramowania typu ransomware, chroni krytyczne urządzenia medyczne i wrażliwe dane pacjentów, zachowuje dowody na potrzeby późniejszego dochodzenia, a przede wszystkim kupuje niezbędny czas na skoordynowaną reakcję i odzyskanie danych.

Następne pytanie →

Typ ataku: Ransomware

1 — 2: Wykrywanie cyberzagrożeń i reagowanie na nie — 3 — 4

Zespół ds. reagowania na incydenty odkrył, że atak prawdopodobnie rozpoczął się od naruszonego konta, które zostało użyte do uzyskania dostępu do serwera bez uwierzytelniania wieloskładnikowego (MFA). Który z poniższych elementów przyczynił się najbardziej bezpośrednio do ataku?

- [ ] Przestarzałe definicje antywirusowe
- [ ] Ujawniona baza danych elektronicznej dokumentacji medycznej (EHR)
- [ ] Brak MFA w dostępie zdalnym
- [ ] Słabe filtrowanie poczty e-mail

Zobacz prawidłową odpowiedź →

Typ ataku: Ransomware

1 — 2: Wykrywanie cyberzagrożeń i reagowanie na nie — 3 — 4

Zespół ds. reagowania na incydenty odkrył, że atak prawdopodobnie rozpoczął się od naruszonego konta, które zostało użyte do uzyskania dostępu do serwera bez uwierzytelniania wieloskładnikowego (MFA). Który z poniższych elementów przyczynił się najbardziej bezpośrednio do ataku?

- ✗ Przestarzałe definicje antywirusowe
- ✗ Ujawniona baza danych elektronicznej dokumentacji medycznej (EHR)
- ✓ Brak MFA w dostępie zdalnym
- ✗ Słabe filtrowanie poczty e-mail

Brak MFA w dostępie zdalnym umożliwił naruszenie serwera, pozwalając atakującym na zalogowanie się za pomocą skradzionych lub zgadywanych poświadczeń bez dodatkowego kroku weryfikacji. W przypadku uwierzytelniania MFA nawet naruszone konta wymagałyby zastosowania drugiego czynnika, znacznie zmniejszając ryzyko nieautoryzowanego dostępu.

Następne pytanie →

Typ ataku: Ransomware

1 — 2 — 3: Odzyskiwanie danych po cyberataku — 4

Pracownicy medyczni polegają teraz na przepływach pracy w formie papierowej. Pacjentów zaplanowanych do operacji dzisiaj nie można zweryfikować w systemie. Jakie są najlepsze krótkoterminowe działania wspierające operacje szpitalne?

- [ ] Ponowne uruchamianie głównego serwera bazy danych w celu podjęcia próby całkowitego ponownego uruchomienia
- [ ] Włączenie wszystkich starych kopii zapasowych, nawet jeśli mają już sześć miesięcy
- [ ] Aktywowanie ręcznych procedur na wypadek przestoju w szpitalu i przekazanie sprawy zespołowi reagowania kryzysowego
- [ ] Powierzenie personelowi decyzji, jak postępować w poszczególnych przypadkach

Zobacz prawidłową odpowiedź →

Typ ataku: Ransomware

1 — 2 — 3: Odzyskiwanie danych po cyberataku — 4

Pracownicy medyczni polegają teraz na przepływach pracy w formie papierowej. Pacjentów zaplanowanych do operacji dzisiaj nie można zweryfikować w systemie. Jakie są najlepsze krótkoterminowe działania wspierające operacje szpitalne?

- ✗ Ponowne uruchamianie głównego serwera bazy danych w celu podjęcia próby całkowitego ponownego uruchomienia
- ✗ Włączenie wszystkich starych kopii zapasowych, nawet jeśli mają już sześć miesięcy
- ✓ Aktywowanie ręcznych procedur na wypadek przestoju w szpitalu i przekazanie sprawy zespołowi reagowania kryzysowego
- ✗ Powierzenie personelowi decyzji, jak postępować w poszczególnych przypadkach

Aktywacja ręcznych procedur na wypadek przestoju i eskalacja do zespołu reagowania kryzysowego zapewnia natychmiastową ciągłość krytycznych klinicznych przepływów pracy, chroni bezpieczeństwo pacjentów oraz ustanawia standard procesu weryfikacji i dokumentowania pomocy. Takie podejście minimalizuje błędy, pozwala skutecznie zarządzać ryzykiem i zasobami oraz wspiera specjalistów w bezpiecznym przywracaniu systemów cyfrowych.

Następne pytanie →

Typ ataku: Ransomware

1 2 3 4: Ogólne najlepsze praktyki

Lokalne media podchwyciły tę historię. Kierownictwo zastanawia się, czy powinno wydać publiczne oświadczenie, a prawnicy pytają o obowiązki wynikające z ustawy o przenośności i odpowiedzialności ubezpieczeń zdrowotnych (HIPAA). Jaki jest najodpowiedniejszy następny krok?

- [ ] Publiczne zanegowanie doniesień o incydencie, dopóki nie będą dostępne dokładniejsze informacje
- [ ] Wydanie komunikatu prasowego obwiniającego zewnętrznego dostawcę IT
- [ ] Powiadamianie organów regulacyjnych i rozpoczęcie wewnętrznych procedur powiadamiania o naruszeniu
- [ ] Natychmiastowe zapłacenie okupu i unikanie uwagi opnii publicznej

Zobacz prawidłową odpowiedź →

Typ ataku: Ransomware

1 — 2 — 3 — 4: Ogólne najlepsze praktyki

Lokalne media podchwyciły tę historię. Kierownictwo zastanawia się, czy powinno wydać publiczne oświadczenie, a prawnicy pytają o obowiązki wynikające z ustawy o przenośności i odpowiedzialności ubezpieczeń zdrowotnych (HIPAA). Jaki jest najodpowiedniejszy następny krok?

- ✗ Publiczne zanegowanie doniesień o incydencie, dopóki nie będą dostępne dokładniejsze informacje
- ✗ Wydanie komunikatu prasowego obwiniającego zewnętrznego dostawcę IT
- ✓ Powiadamianie organów regulacyjnych i rozpoczęcie wewnętrznych procedur powiadamiania o naruszeniu
- ✗ Natychmiastowe zapłacenie okupu i unikanie uwagi opnii publicznej

Niezwłoczne zgłaszanie naruszeń chronionych informacji zdrowotnych organom i osobom, których dotyczy problem — zgodnie z wymogami HIPAA i przepisów prawa stanowego — zapewnia zgodność z przepisami, ochronę prawną i przejrzystość zastosowanych najlepszych praktyk w celu zapobiegania szkodom prawnym i reputacji, spełniania koniecznych obowiązków informacyjnych oraz ustanowienia właściwej komunikacji z pacjentami, personelem i interesariuszami.

Zobacz rozwiązania →

TYP ATAKU: RANSOMWARE

Przypomnienie

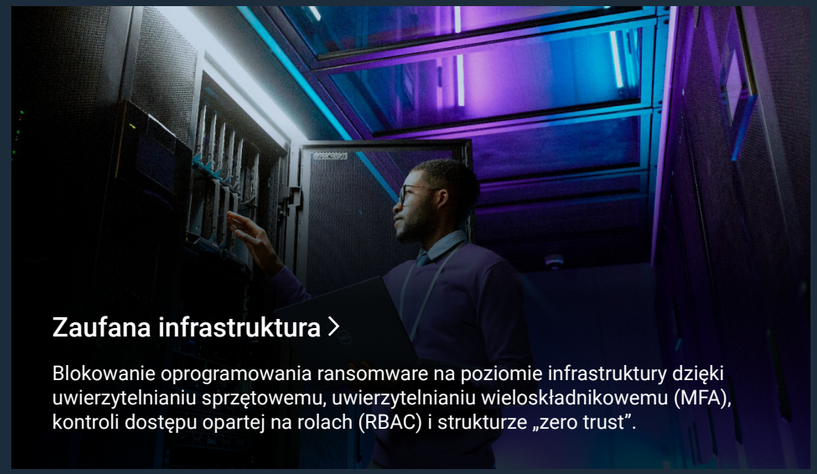
Ransomware to rodzaj złośliwego oprogramowania, które blokuje dostęp do systemu komputerowego lub danych do momentu zapłacenia okupu. Jest to jeden z najbardziej destrukcyjnych typów cyberataków. Pięćdziesiąt procent organizacji na całym świecie zostało dotkniętych oprogramowaniem ransomware co najmniej raz w ciągu ostatniego roku, a średni czas przestoju po ataku ransomware wynosi trzy tygodnie, co prowadzi do poważnych zakłóceń operacyjnych.

W firmie Dell nadajemy priorytet ochronie Twojej organizacji za pomocą struktur w modelu „zero trust”, ochrony punktów końcowych i segmentacji sieci, aby blokować dostęp oprogramowania ransomware i ograniczać jego rozprzestrzenianie się. Dzięki specjalistycznemu planowaniu reagowania na incydenty pomagamy zachować odporność i szybko odzyskiwać sprawność po atakach.

Dowiedz się więcej o zaawansowanych strategiach cyberodporności i przekonaj się, w jaki sposób firma Dell może pomóc chronić Twoją organizację przed atakami typu ransomware.

Zapoznaj się z krótkim opisem ataków ransomware →

Wróć do scenariuszy

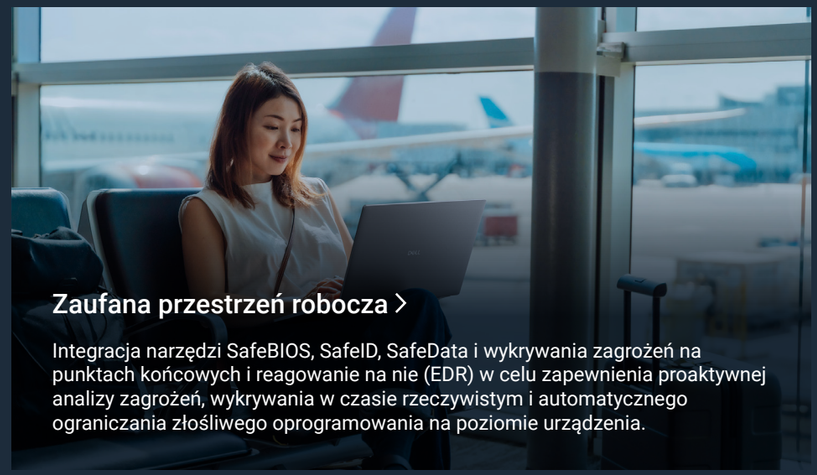


Zaufana infrastruktura >

Blokowanie oprogramowania ransomware na poziomie infrastruktury dzięki uwierzytelnianiu sprzętowemu, uwierzytelnianiu wieloskładnikowemu (MFA), kontroli dostępu opartej na rolach (RBAC) i strukturze „zero trust”.

Serwery sieciowe i PowerEdge >

Ogranicz rozprzestrzenianie się oprogramowania ransomware. Obejmuje to segmentację sieci, bezpieczny rozruch, krzemowe źródło zaufania, dynamiczne zarządzanie portami USB i blokadę systemu.



Zaufana przestrzeń robocza >

Integracja narzędzi SafeBIOS, SafeID, SafeData i wykrywania zagrożeń na punktach końcowych i reagowanie na nie (EDR) w celu zapewnienia proaktywnej analizy zagrożeń, wykrywania w czasie rzeczywistym i automatycznego ograniczania złośliwego oprogramowania na poziomie urządzenia.

Oferta PowerProtect >

Ochrona danych o znaczeniu krytycznym dzięki niemodyfikowalnym, odizolowanym kopiom zapasowym, inteligentnej analizie Cyber Recovery i funkcjom szybkiego przywracania w celu zapobieżenia wymuszeniom i zapewnienia odporności na ataki.

Usługi związane z bezpieczeństwem i odpornością na zagrożenia >

Współpracuj z ekspertami, na przykład z CrowdStrike, aby pomóc w ocenach, zarządzaniu lukami w zabezpieczeniach, szkoleniach w zakresie świadomości bezpieczeństwa, testach penetracyjnych i reagowaniu na incydenty.

Typ ataku: Sprzęt łańcucha dostaw

Twoja firma wprowadza 500 nowych notebooków w swoich biurach na całym świecie. Aby przyspieszyć ten proces, zlecasz przygotowanie obrazów i sprzętu zewnętrznemu dostawcy logistycznemu IT. Wysyła on wstępnie skonfigurowane maszyny bezpośrednio do pracowników.

W ciągu kilku dni otrzymujesz kilka połączeń z pola o treści:

- Żądania uwierzytelniania wieloskładnikowego (MFA) są omijane i nie działają prawidłowo.
- Zespół ds. zabezpieczeń odnotował szereg nieautoryzowanych logowań administratora w godzinach nocnych.
- Widzą również ruch wirtualnej sieci prywatnej (VPN) od użytkowników, którzy rzekomo są w trybie offline.

Sprawdź swoją wiedzę →

Typ ataku: Sprzęt łańcucha dostaw

1: Zmniejszenie powierzchni ataku 2 3 4

Pracownik zgłasza otrzymywanie powiadomień push związanych z uwierzytelnianiem wieloskładnikowym (MFA), choć nie próbował się zalogować. Pulpit zabezpieczeń organizacji pokazuje, że logowanie pochodzi z urządzenia z firmową plakietką identyfikacyjną. Jaki jest najbardziej logiczny pierwszy krok dla zespołu centrum operacji bezpieczeństwa (SOC)?

- [ ] Wyłączenie konta użytkownika i zdalne wyczyszczenie notebooka
- [ ] Porównanie adresu IP logowania i odcisku palca urządzenia z innymi znanymi użytkownikami, których dotyczy problem
- [ ] Eskalowanie do działu HR przy założeniu, że to użytkownik ponosi winę
- [ ] Wysłanie alertu do całej firmy, aby wszyscy natychmiast zmienili hasła

Zobacz prawidłową odpowiedź →

Typ ataku: Sprzęt łańcucha dostaw

1: Zmniejszenie powierzchni ataku — 2 — 3 — 4

Pracownik zgłasza otrzymywanie powiadomień push związanych z uwierzytelnianiem wieloskładnikowym (MFA), choć nie próbował się zalogować. Pulpit zabezpieczeń organizacji pokazuje, że logowanie pochodzi z urządzenia z firmową plakietką identyfikacyjną. Jaki jest najbardziej logiczny pierwszy krok dla zespołu centrum operacji bezpieczeństwa (SOC)?

- ✗ Wyłączenie konta użytkownika i zdalne wyczyszczenie notebooka
- ✓ Porównanie adresu IP logowania i odcisku palca urządzenia z innymi znanymi użytkownikami, których dotyczy problem
- ✗ Eskalowanie do działu HR przy założeniu, że to użytkownik ponosi winę
- ✗ Wysłanie alertu do całej firmy, aby wszyscy natychmiast zmienili hasła

Gdy zespół SOC ustali, czy podejrzana aktywność jest elementem szerszego ataku lub odizolowanego ataku w celu umożliwienia szybkiego rozpoznawania wzorców, ukierunkowana reakcja na incydenty i ograniczenie dalszego ryzyka jest logicznym pierwszym krokiem podczas identyfikacji ataku danego sprzętu w łańcuchu dostaw.

Następne pytanie →

Typ ataku: Sprzęt łańcucha dostaw

1 — 2: Wykrywanie cyberzagrożeń i reagowanie na nie — 3 — 4

Twoja grupa reagowania na incydenty stwierdza, że wiele zainfekowanych notebooków ma wersje oprogramowania układowego SSD, które nie pasują do oficjalnych notatek wydawcy. Wykrywanie zagrożeń na punktach końcowych i reagowania na nie (EDR) nie pokazuje żadnych złośliwych procesów. Co to najprawdopodobniej oznacza?

- [ ] Błąd konfiguracji dostawcy usług IT
- [ ] Nowy typ oprogramowania ransomware, który usuwa się samodzielnie
- [ ] Naruszenie bezpieczeństwa w łańcuchu dostaw na poziomie oprogramowania wewnętrznego
- [ ] Normalne zachowanie podczas obrazowania

Zobacz prawidłową odpowiedź →

Typ ataku: Sprzęt łańcucha dostaw

1 — 2: Wykrywanie cyberzagrożeń i reagowanie na nie — 3 — 4

Twoja grupa reagowania na incydenty stwierdza, że wiele zainfekowanych notebooków ma wersje oprogramowania układowego SSD, które nie pasują do oficjalnych notatek wydawcy. Wykrywanie zagrożeń na punktach końcowych i reagowania na nie (EDR) nie pokazuje żadnych złośliwych procesów. Co to najprawdopodobniej oznacza?

- ✗ Błąd konfiguracji dostawcy usług IT
- ✗ Nowy typ oprogramowania ransomware, który usuwa się samodzielnie
- ✓ Naruszenie bezpieczeństwa w łańcuchu dostaw na poziomie oprogramowania wewnętrznego
- ✗ Normalne zachowanie podczas obrazowania

Nieautoryzowane oprogramowanie wewnętrzne dysków SSD w wielu notebookach, niewykryte przez EDR i niezgodne z oficjalną wersją, wskazuje na celowe ingerencje w sprzęt lub oprogramowanie wewnętrzne — znak rozpoznawczy naruszenia łańcucha dostaw na poziomie oprogramowania wewnętrznego.

Następne pytanie →

Typ ataku: Sprzęt łańcucha dostaw

1 — 2 — 3: Odzyskiwanie danych po cyberataku — 4

Zidentyfikowano 100 podejrzanych urządzeń z nieautoryzowanym oprogramowaniem SSD. Musisz zdecydować, co dalej, nie dając się wykryć napastnikowi, który może mieć zdalny dostęp. Jaki będzie najlepszy następny krok?

- [ ] Wyłączenie wszystkich urządzeń i ich przesłanie do działu śledczego
- [ ] Usunięcie zrzutów pamięci na żywo i badanie, gdy systemy zostaną uruchomione
- [ ] Powiadomienie dostawcy zewnętrznego o naruszeniu zabezpieczeń
- [ ] Wyczyszczenie wszystkich urządzeń i ponowne wydanie nowych notebooków wszystkim użytkownikom na całym świecie

Zobacz prawidłową odpowiedź →

Typ ataku: Sprzęt łańcucha dostaw

1 — 2 — 3: Odzyskiwanie danych po cyberataku — 4

Zidentyfikowano 100 podejrzanych urządzeń z nieautoryzowanym oprogramowaniem SSD. Musisz zdecydować, co dalej, nie dając się wykryć napastnikowi, który może mieć zdalny dostęp. Jaki będzie najlepszy następny krok?

- ✗ Wyłączenie wszystkich urządzeń i ich przesłanie do działu śledczego
- ✓ Usunięcie zrzutów pamięci na żywo i badanie, gdy systemy zostaną uruchomione
- ✗ Powiadomienie dostawcy zewnętrznego o naruszeniu zabezpieczeń
- ✗ Wyczyszczenie wszystkich urządzeń i ponowne wydanie nowych notebooków wszystkim użytkownikom na całym świecie

Zrzuty pamięci na żywo mają kluczowe znaczenie dla zachowania niestabilnych dowodów, takich jak aktywne złośliwe oprogramowanie i rootkity, ponieważ umożliwiają ukierunkowane reagowanie na incydenty poprzez wykrywanie ukrytych zagrożeń i punktów dostępu przed ich utratą lub zwróceniem uwagi atakujących.

Następne pytanie →

Typ ataku: Sprzęt łańcucha dostaw

1 2 3 4: Ogólne najlepsze praktyki

Główny specjalista ds. bezpieczeństwa informacji prosi o podsumowanie tego, w jaki sposób ten atak przeniknął Twoje środowisko. Musisz przedstawić zwięzłe wyjaśnienie zespołowi zarządzającemu. Jak wyjaśnić atak?

- [ ] Wirus został przypadkowo pobrany z linku phishingowego
- [ ] Mieliśmy do czynienia z nieprawidłową konfiguracją sieci, która umożliwiła dostęp zewnętrzny
- [ ] Złośliwe oprogramowanie zostało wprowadzone przez zainfekowanego dostawcę sprzętu podczas konfiguracji notebooka.
- [ ] Jeden z naszych programistów wprowadził niezabezpieczony kod do produkcji

Zobacz prawidłową odpowiedź →

Typ ataku: Sprzęt łańcucha dostaw

1 2 3 4: Ogólne najlepsze praktyki

Główny specjalista ds. bezpieczeństwa informacji prosi o podsumowanie tego, w jaki sposób ten atak przeniknął Twoje środowisko. Musisz przedstawić zwięzłe wyjaśnienie zespołowi zarządzającemu. Jak wyjaśnić atak?

- ✗ Wirus został przypadkowo pobrany z linku phishingowego
- ✗ Mieliśmy do czynienia z nieprawidłową konfiguracją sieci, która umożliwiła dostęp zewnętrzny
- ✓ Złośliwe oprogramowanie zostało wprowadzone przez zainfekowanego dostawcę sprzętu podczas konfiguracji notebooka.
- ✗ Jeden z naszych programistów wprowadził niezabezpieczony kod do produkcji

Niezgodne wersje oprogramowania wewnętrznego i brak aktywnego złośliwego oprogramowania potwierdzają, że był to atak na poziomie oprogramowania wewnętrznego pochodzący od dostawcy, a nie błąd użytkownika czy nieprawidłowa konfiguracja.

Zobacz rozwiązania →

TYP ATAKU: SPRZĘT ŁAŃCUCHA DOSTAW

Przypomnienie

W ostatnich latach liczba ataków w łańcuchach dostaw znacznie wzrosła. Manipulując urządzeniami fizycznymi podczas produkcji, wysyłki lub wdrażania lub znajdując słabe punkty u dostawców oprogramowania, atakujący uzyskują środki do wprowadzania złośliwych komponentów lub kodu, uszkodzenia systemów lub pozyskania wrażliwych danych. Ofiarami mogą być zarówno małe firmy, jak i globalne przedsiębiorstwa, skutkiem czego doznają poważnych strat finansowych, obniżenia poziomu zaufania klientów i konsekwencji prawnych.

Firma Dell minimalizuje ataki na łańcuch dostaw sprzętu, integrując rygorystyczne oceny ryzyka dostawców i wdrażając zasady modelu „zero trust” wraz z ciągłą weryfikacją urządzeń i niezależnymi kontrolami integralności. Wzmacniamy integralność sprzętu w całym cyklu jego eksploatacji.

Dowiedz się więcej o zaawansowanych strategiach cyberodporności, aby zorientować się, w jaki sposób firma Dell może pomóc chronić Twoją organizację przed atakami na sprzęt w łańcuchu dostaw.

Zapoznaj się z krótkim opisem ataków sprzętowych w łańcuchu dostaw →

Wróć do scenariuszy

Gwarancja łańcucha dostaw >

Dzięki zaawansowanym metodom sprawdzania pochodzenia, logistyce odpornej na manipulacje i przejrzystemu pozyskiwaniu łańcuch dostaw firma Dell gwarantuje rygorystyczną weryfikację sprzętu, oprogramowania wewnętrznego i dostawców przed dostarczeniem ich do danej organizacji.

Secure Component Verification (SCV) >

Kryptograficzna weryfikacja komponentów komputera w fabryce i podczas instalacji zapewnia autentyczność, wykrywa ukryte zmiany i ogranicza ryzyko ingerencji w łańcuch dostaw.

Zaufana przestrzeń robocza i zaufana infrastruktura >

Uwierzytelnianie sprzętowe i ciągłe kontrole integralności oprogramowania wewnętrznego chronią punkty końcowe, ostrzegając o nieautoryzowanych zmianach lub złośliwych implantach, zanim staną się one zagrożeniami.

Śledzenie zasobów i pakiet ProSupport Suite z SupportAssist >

Kompleksowe śledzenie zasobów, monitorowanie pochodzenia urządzeń w czasie rzeczywistym i proaktywna weryfikacja integralności zapewniają szybkie wykrywanie anomalii i bezpieczeństwo całej floty.

Partnerzy w zakresie bezpieczeństwa: Wykrywanie i reagowanie oparte na sztucznej inteligencji >

Narzędzia zabezpieczające oparte na sztucznej inteligencji umożliwiają ciągłe monitorowanie, badania śledcze i automatyczne ograniczanie manipulacji zachowaniem urządzenia lub jego niecodziennemu działaniu, gwarantując szybkie podjęcie działania przeciwko zagrożeniom w łańcuchu dostaw.

Typ ataku: Oprogramowanie łańcucha dostaw

Twoja firma zapewnia oprogramowanie analityczne oparte na chmurze używane przez szpitale. Twoje usługi zaplecza zależą od powszechnie używanej biblioteki rejestrowania typu open source obsługiwanej przez zaufanego programisty zewnętrznego na GitHub.

Bez wiedzy Twojego zespołu deweloperskiego atakujący naruszyli konto GitHub i dodali złośliwą aktualizację, która zawiera ukryty kod zaprojektowany w celu:

- Eksfiltracji zmiennych środowiskowych, w tym kluczy interfejsu programowania aplikacji (API) i tajnych tokenów internetowych notacji obiektów JavaScript (JWT)
- Utworzenia powłoki odwrotnej, gdy określone adresy IP składają żądania
- Pozostania w stanie uśpienia, chyba że uruchomiono go zdalnie

Sprawdź swoją wiedzę →

Typ ataku: Oprogramowanie łańcucha dostaw

1: Zmniejszenie powierzchni ataku — 2 — 3 — 4

Interfejs API nagle zaczyna zwracać błędy 500 do kluczowych klientów. Monitorowanie chmury oznacza wykrywanie połączeń wychodzących z usług kontenerowych do nieznanej wcześniej domeny. Jaka jest Twoja pierwsza odpowiedź?

- [ ] Wyłączenie całego wychodzącego ruchu sieciowego z kontenerów
- [ ] Ponowne uruchomienie usług, których dotyczy problem, w celu usunięcia wszelkich problemów z pamięcią
- [ ] Sprawdzenie ostatnich zatwierdzeń kodu w repozytorium GitHub
- [ ] Kontakt z dostawcą hostingu domeny

Zobacz prawidłową odpowiedź →

Typ ataku: Oprogramowanie łańcucha dostaw

1: Zmniejszenie powierzchni ataku — 2 — 3 — 4

Interfejs API nagle zaczyna zwracać błędy 500 do kluczowych klientów. Monitorowanie chmury oznacza wykrywanie połączeń wychodzących z usług kontenerowych do nieznanej wcześniej domeny. Jaka jest Twoja pierwsza odpowiedź?

- ✓ Wyłączenie całego wychodzącego ruchu sieciowego z kontenerów
- ✗ Ponowne uruchomienie usług, których dotyczy problem, w celu usunięcia wszelkich problemów z pamięcią
- ✗ Sprawdzenie ostatnich zatwierdzeń kodu w repozytorium GitHub
- ✗ Kontakt z dostawcą hostingu domeny

Wyłączenie całego wychodzącego ruchu sieciowego z kontenerów natychmiast blokuje atakującym możliwość pozyskiwania wrażliwych danych lub ustanowienia zdalnego dostępu za pośrednictwem naruszonej biblioteki rejestrowania, izolując w ten sposób środowisko w czasie rzeczywistym i zapewniając tak istotny czas na zbadanie przypadku, zabezpieczenie kluczy i tajnych danych interfejsu API oraz zapobiegnięcie aktywacji uśpionych mechanizmów ataku.

Następne pytanie →

Typ ataku: Oprogramowanie łańcucha dostaw

1 — 2: Wykrywanie cyberzagrożeń i reagowanie na nie — 3 — 4

Twój kierownik techniczny potwierdza, że aplikacja automatycznie pobrała kod z GitHub trzy dni przed wystąpieniem problemów. Ta wersja nie jest jeszcze oznaczona jako złośliwa w żadnych publicznych bazach danych. Jakie są najbardziej odpowiedzialne natychmiastowe działania?

- [ ] Kontakt z opiekunem biblioteki bezpośrednio w GitHub
- [ ] Usunięcie wszystkich lokalnych zależności projektu i ich odbudowanie
- [ ] Przed podjęciem dalszych działań najlepiej poczekać na typowe luki w zabezpieczeniach i zagrożenia (CVE)
- [ ] Powrót do ostatniej znanej bezpiecznej wersji kodu

Zobacz prawidłową odpowiedź →

Typ ataku: Oprogramowanie łańcucha dostaw

1 — 2: Wykrywanie cyberzagrożeń i reagowanie na nie — 3 — 4

Twój kierownik techniczny potwierdza, że aplikacja automatycznie pobrała kod z GitHub trzy dni przed wystąpieniem problemów. Ta wersja nie jest jeszcze oznaczona jako złośliwa w żadnych publicznych bazach danych. Jakie są najbardziej odpowiedzialne natychmiastowe działania?

- ✗ Kontakt z opiekunem biblioteki bezpośrednio w GitHub
- ✗ Usunięcie wszystkich lokalnych zależności projektu i ich odbudowanie
- ✗ Przed podjęciem dalszych działań najlepiej poczekać na typowe luki w zabezpieczeniach i zagrożenia (CVE)
- ✓ Powrót do ostatniej znanej bezpiecznej wersji kodu

Powrót do ostatniej znanej wersji bezpiecznego kodu powoduje natychmiastowe usunięcie naruszonej aktualizacji, eliminuje przyczółki atakującego i przywraca integralność operacyjną w celu aktywnego ograniczania ryzyka i ochrony wrażliwych danych.

Następne pytanie →

Typ ataku: Oprogramowanie łańcucha dostaw

1 — 2 — 3: Odzyskiwanie danych po cyberataku — 4

Analiza potwierdza, że biblioteka przechwytywała klucze API i poświadczenia chmurowe. Zidentyfikowano wiele kontenerów zbudowanych z naruszoną wersją. Który krok jest najbardziej krytyczny w strategii ograniczania zagrożenia?

- [ ] Anulowanie i zaktualizowanie wszystkich poświadczeń we wszystkich środowiskach, których dotyczy problem
- [ ] Ponowne utworzenie obrazów kontenerów przy użyciu zaktualizowanego obrazu systemu operacyjnego
- [ ] Wyczyszczenie notebooków zespołu programistów
- [ ] Przesłanie powiadomienia o usunięciu do repozytorium GitHub

Zobacz prawidłową odpowiedź →

Typ ataku: Oprogramowanie łańcucha dostaw

1 — 2 — 3: Odzyskiwanie danych po cyberataku — 4

Analiza potwierdza, że biblioteka przechwytywała klucze API i poświadczenia chmurowe. Zidentyfikowano wiele kontenerów zbudowanych z naruszoną wersją. Który krok jest najbardziej krytyczny w strategii ograniczania zagrożenia?

- ✓ Anulowanie i zaktualizowanie wszystkich poświadczeń we wszystkich środowiskach, których dotyczy problem
- ✗ Ponowne utworzenie obrazów kontenerów przy użyciu zaktualizowanego obrazu systemu operacyjnego
- ✗ Wyczyszczenie notebooków zespołu programistów
- ✗ Przesłanie powiadomienia o usunięciu do repozytorium GitHub

Cofnięcie poświadczeń i ich zrotowanie to pierwszy krytyczny krok po naruszeniu zabezpieczeń chmury, który blokuje atakującym dostęp do usług, powstrzymuje kradzież danych i zabezpiecza systemy niezależnie od zakresu naruszenia.

Następne pytanie →

Typ ataku: Oprogramowanie łańcucha dostaw

1 2 3 4: Ogólne najlepsze praktyki

Otrzymujesz prośbę o wyjaśnienie, co się stało z dyrektorem ds. technologicznych i zespołami/prawnym ds. zgodności z przepisami. Jakie jest najdokładniejsze i najprostsze wyjaśnienie? Jak podsumować incydent?

- [ ] Nasze wewnętrzne narzędzia do ciągłej integracji i ciągłego wdrażania/dostarczania (CI/CD) zawiodły, umożliwiając wdrożenie złego kodu.
- [ ] Zależność oprogramowania innej firmy została naruszona, a nasza automatyzacja wprowadziła je do produkcji
- [ ] Programista zawarł nieprzetestowany kod w wersji przyspieszonej
- [ ] Atakujący brutalnie włamał się na nasze repozytorium GitHub

Zobacz prawidłową odpowiedź →

Typ ataku: Oprogramowanie łańcucha dostaw

1 — 2 — 3 — 4: Ogólne najlepsze praktyki

Otrzymujesz prośbę o wyjaśnienie, co się stało z dyrektorem ds. technologicznych i zespołami/prawnym ds. zgodności z przepisami. Jakie jest najdokładniejsze i najprostsze wyjaśnienie? Jak podsumować incydent?

- ✗ Nasze wewnętrzne narzędzia do ciągłej integracji i ciągłego wdrażania/dostarczania (CI/CD) zawiodły, umożliwiając wdrożenie złego kodu.
- ✓ Zależność oprogramowania innej firmy została naruszona, a nasza automatyzacja wprowadziła je do produkcji
- ✗ Programista zawarł nieprzetestowany kod w wersji przyspieszonej
- ✗ Atakujący brutalnie włamał się na nasze repozytorium GitHub

Pierwotną przyczyną był atak wymierzony w łańcuch dostaw: atakujący naruszyli zależność oprogramowania innej firmy, a zautomatyzowany proces kompilacji wprowadził złośliwą aktualizację bezpośrednio do systemu produkcji, wpływając na integralność aplikacji i wrażliwe środowiska — tym samym taki atak podkreśla ryzyko wystąpienia złośliwych aktualizacji w zaufanych zewnętrznych programach zależnych.

Zobacz rozwiązania →

TYP ATAKU: OPROGRAMOWANIE ŁAŃCUCHA DOSTAW

Przypomnienie

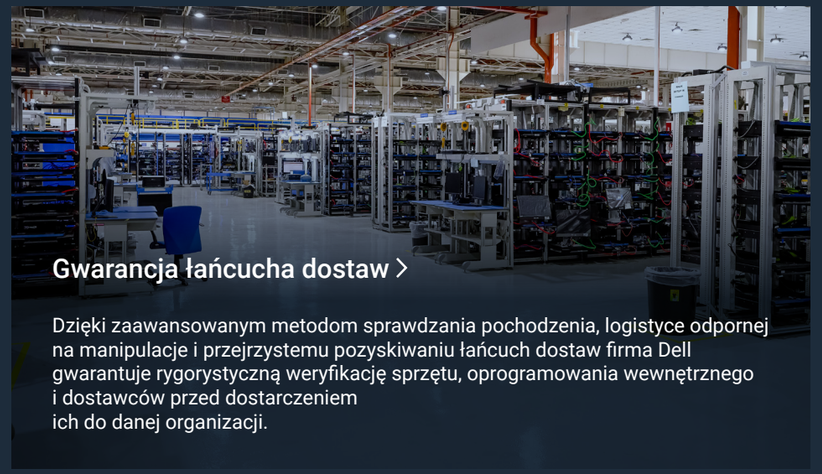
Ataki cybernetyczne na oprogramowanie łańcucha dostaw wykorzystują luki w aktualizacjach oprogramowania, integracjach z zewnętrznymi dostawcami i środowiskach programistycznych do wbudowania złośliwego kodu, który rozprzestrzenia się w sieciach. Ataki takie mogą powodować wszechobecne naruszenia danych oraz zakłócenia operacyjne i narazić na szwank całe ekosystemy, wpływając na firmy każdej wielkości.

Firma Dell dba o cyberodporność, kładąc nacisk na przejrzystość, bezpieczny rozwój i ciągłe monitorowanie przy jednoczesnym utrzymaniu solidnego planu reagowania na incydenty w celu zapewnienia szybkiego odzyskiwania danych i komunikacji z interesariuszami.

Dowiedz się więcej o zaawansowanych strategiach cyberodporności i przekonaj się, w jaki sposób firma Dell może pomóc chronić Twoją organizację przed atakami na oprogramowanie łańcucha dostaw.

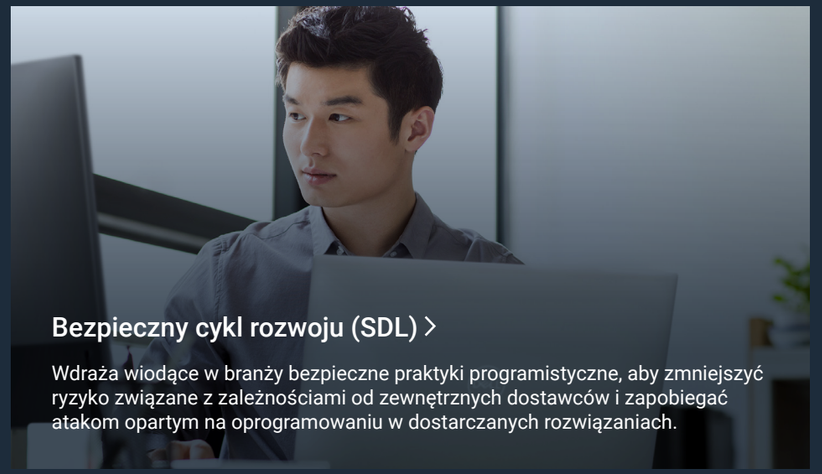
Zapoznaj się z krótkim opisem ataków na oprogramowanie łańcucha dostaw →

Wróć do scenariuszy



Gwarancja łańcucha dostaw >

Dzięki zaawansowanym metodom sprawdzania pochodzenia, logistyce odpornej na manipulacje i przejrzystemu pozyskiwaniu łańcuch dostaw firma Dell gwarantuje rygorystyczną weryfikację sprzętu, oprogramowania wewnętrznego i dostawców przed dostarczeniem ich do danej organizacji.



Bezpieczny cykl rozwoju (SDL) >

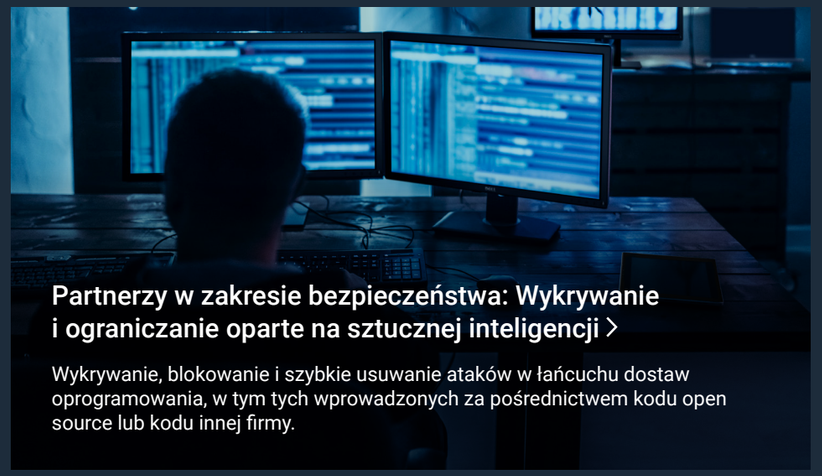
Wdraża wiodące w branży bezpieczne praktyki programistyczne, aby zmniejszyć ryzyko związane z zależnościami od zewnętrznych dostawców i zapobiegać atakom opartym na oprogramowaniu w dostarczanych rozwiązaniach.

Zaufana przestrzeń robocza i zaufana infrastruktura >

Zabezpieczenia SafeBIOS, SafeID i SafeDataDelivers zapewniają uwierzytelnianie sprzętowe, które gwarantuje, że urządzenia końcowe uruchamiają tylko zaufane oprogramowanie i umożliwiają szybkie wykrywanie nieautoryzowanych lub złośliwych modyfikacji oprogramowania.

Śledzenie zasobów i pakiet ProSupport Suite z SupportAssist >

Monitorowanie urządzeń i oprogramowania w czasie rzeczywistym pozwala na szybkie wykrywanie i reagowanie na anomalie wprowadzone w łańcuchu dostaw.



Partnerzy w zakresie bezpieczeństwa: Wykrywanie i ograniczanie oparte na sztucznej inteligencji >

Wykrywanie, blokowanie i szybkie usuwanie ataków w łańcuchu dostaw oprogramowania, w tym tych wprowadzonych za pośrednictwem kodu open source lub kodu innej firmy.

Typ ataku: Zero-day

Jesteś analitykiem ds. bezpieczeństwa monitorującym dzienniki uwierzytelniania firmy. Ostatnio użytkownicy zgłosili nieautoryzowany dostęp do swoich kont, chociaż nie udostępnili swoich poświadczeń.

Po sprawdzeniu dzienników można znaleźć następujące działanie:

```
[INFO] 2025-04-02 14:05:12 – Logowanie użytkownika – Identyfikator użytkownika: 1023 – IP: 192.168.1.15 – Wydano token JWT
[INFO] 2025-04-02 14:07:35 - User Login - UserID: 1023 - IP: 5.62.60.12 - JWT Token Reused
[INFO] 2025-04-02 14:08:00 – Logowanie użytkownika – Identyfikator użytkownika: 1023 – IP: 203.0.113.45 – Ponownie użyty token JWT
```

Jednocześnie analityk zabezpieczeń identyfikuje lukę w interfejsie programowania aplikacji (API):

- Tokeny internetowe notacji obiektów JavaScript (JWT) nigdy nie wygasają.
- Tokeny są przechowywane w lokalnej pamięci masowej zamiast plików cookie HTTPonly.
- Nie jest wymuszane uwierzytelnianie wieloskładnikowe (MFA).

Sprawdź swoją wiedzę →

Typ ataku: Zero-day

1: Zmniejszenie powierzchni ataku — 2 — 3 — 4

Przyjmij rolę członka zespołu ds. bezpieczeństwa — podejrzewasz atak typu „Zero-Day”, ponieważ nie pojawiły się żadne sygnały ostrzegawcze. Jak można to potwierdzić?

- [ ] Wyloguj wszystkich użytkowników ze swoich systemów
- [ ] Zidentyfikuj kluczowe anomalne zachowania uwierzytelniania w dziennikach
- [ ] Zadzwoń do znajomych w innych firmach, aby sprawdzić, czy mają ten sam problem
- [ ] Spróbuj skorelować z inną nieprawidłową aktywnością zabezpieczeń

Zobacz prawidłową odpowiedź →

Typ ataku: Zero-day

1: Zmniejszenie powierzchni ataku — 2 — 3 — 4

W roli członka zespołu ds. bezpieczeństwa — podejrzewasz atak typu „Zero-Day”, ponieważ nie pojawiły się żadne sygnały ostrzegawcze. Jak można to potwierdzić?

- ✗ Wyloguj wszystkich użytkowników ze swoich systemów
- ✓ Zidentyfikuj kluczowe anomalne zachowania uwierzytelniania w dziennikach
- ✗ Zadzwoń do znajomych w innych firmach, aby sprawdzić, czy mają ten sam problem
- ✓ Spróbuj skorelować z inną nieprawidłową aktywnością zabezpieczeń

Zidentyfikowanie anomalnych zachowań uwierzytelniania, takich jak nietypowe czasy logowania, ponowne wykorzystanie poświadczeń lub dostęp z nietypowych urządzeń, oraz skorelowanie ich z innymi nietypowymi działaniami bezpieczeństwa, takimi jak anomalie dostępu do danych lub eskalacja uprawnień, potwierdza skoordynowany atak typu zero-day.

Następne pytanie →

Typ ataku: Zero-day

1 — 2: Wykrywanie cyberzagrożeń i reagowanie na nie — 3 — 4

Ponieważ luka w zabezpieczeniach jest nieznana, zespoły ds. bezpieczeństwa muszą ograniczyć szkody podczas badania. Jak należy to zrobić?

- [ ] Unieważnienie wszystkich sesji uwierzytelniania w całym systemie
- [ ] Skoncentrowanie wszystkich zasobów na punkcie wejścia ataku
- [ ] Wymuszanie tylko logowania za p[omocą uwierzytelniania wieloskładnikowego (MFA)
- [ ] Poleganie na bieżących regułach zapór statycznych lub zapory aplikacji internetowych (WAF)

Zobacz prawidłową odpowiedź →

Typ ataku: Zero-day

1 — 2: Wykrywanie cyberzagrożeń i reagowanie na nie — 3 — 4

Ponieważ luka w zabezpieczeniach jest nieznana, zespoły ds. bezpieczeństwa muszą ograniczyć szkody podczas badania. Jak należy to zrobić?

- ✓ Unieważnienie wszystkich sesji uwierzytelniania w całym systemie
- ✗ Skoncentrowanie wszystkich zasobów na punkcie wejścia ataku
- ✓ Wymuszanie tylko logowania za p[omocą uwierzytelniania wieloskładnikowego (MFA)
- ✗ Poleganie na bieżących regułach zapór statycznych lub zapory aplikacji internetowych (WAF)

Wspólne działania wzmacniają bezpieczeństwo i minimalizują ryzyko, jednocześnie odcinając dostęp atakującym, aby zespoły ds. bezpieczeństwa mogły badać i rozwiązywać podstawowe luki w zabezpieczeniach.

Następne pytanie →

Typ ataku: Zero-day

1 — 2 — 3: Odzyskiwanie danych po cyberataku — 4

Komputery firmy Dell są wyposażone w technologie takie jak Secure Boot, moduły Trusted Platform Modules (TPM), ochronę haseł na poziomie podstawowego systemu wejścia/wyjścia (BIOS) i SafeBIOS. Jak mogą one pomóc w ataku Zero-Day?

- [ ] Chroni przed atakami zrzutu poświadczeń, które wykradają tokeny interfejsu programowania aplikacji (API)
- [ ] Uniemożliwia atakującemu z dostępem fizycznym obejście zabezpieczeń systemu operacyjnego w celu zainstalowania złośliwego oprogramowania, które kradnie tokeny uwierzytelniania
- [ ] Zapewnia, że atakujący nie mogą manipulować ustawieniami systemu BIOS w celu osłabienia bezpieczeństwa systemu operacyjnego, co może prowadzić do przejęcia sesji interfejsu API
- [ ] Wszystkie powyższe

Zobacz prawidłową odpowiedź →

Typ ataku: Zero-day

1 — 2 — 3: Odzyskiwanie danych po cyberataku — 4

Komputery firmy Dell są wyposażone w technologie takie jak Secure Boot, moduły Trusted Platform Modules (TPM), ochronę haseł na poziomie podstawowego systemu wejścia/wyjścia (BIOS) i SafeBIOS. Jak mogą one pomóc w ataku Zero-Day?

- [x] Chroni przed atakami zrzutu poświadczeń, które wykradają tokeny interfejsu programowania aplikacji (API)
- [x] Uniemożliwia atakującemu z dostępem fizycznym obejście zabezpieczeń systemu operacyjnego w celu zainstalowania złośliwego oprogramowania, które kradnie tokeny uwierzytelniania
- [x] Zapewnia, że atakujący nie mogą manipulować ustawieniami systemu BIOS w celu osłabienia bezpieczeństwa systemu operacyjnego, co może prowadzić do przejęcia sesji interfejsu API
- [x] Wszystkie powyższe

To wielowarstwowe podejście zapewnia kompleksową ochronę przed atakami typu zero-day ukierunkowanymi na system BIOS, oprogramowanie wewnętrzne, poświadczenia i konfiguracje systemu. Zapobiegając manipulacjom, nieautoryzowanemu dostępowi i kradzieży poświadczeń, technologie te pozostają skuteczne nawet w przypadku wykrycia nowych luk w zabezpieczeniach przez atakujących.

Następne pytanie →

Typ ataku: Zero-day

1 2 3 4: Ogólne najlepsze praktyki

Jaki jest najlepszy sposób na zapobieganie atakom Zero-Day?

- [ ] Nieużywanie oprogramowania open source
- [ ] Wykorzystanie zasad modelu „zero trust”
- [ ] Utrzymanie aktualności wszystkich poprawek systemów operacyjnych (OS), oprogramowania wewnętrznego, interfejsów programowania aplikacji (API), bibliotek i kontenerów
- [ ] Umieszczenie elektronicznej bramy wokół firmy w celu zapobieżenia zagrożeniom

Zobacz prawidłową odpowiedź →

Typ ataku: Zero-day

1 — 2 — 3 — 4: Ogólne najlepsze praktyki

Jaki jest najlepszy sposób na zapobieganie atakom Zero-Day?

- ✗ Nieużywanie oprogramowania open source
- ✓ Wykorzystanie zasad modelu „zero trust”
- ✗ Utrzymanie aktualności wszystkich poprawek systemów operacyjnych (OS), oprogramowania wewnętrznego, interfejsów programowania aplikacji (API), bibliotek i kontenerów
- ✗ Umieszczenie elektronicznej bramy wokół firmy w celu zapobieżenia zagrożeniom

Jeśli istnieją nieznane luki w zabezpieczeniach lub systemy bez poprawek, zasady modelu „zero trust” zapobiegają atakom typu „Zero-Day”, usuwając domyślne zaufanie użytkowników i urządzeń, wymuszając ciągłe uwierzytelnianie, ograniczając dostęp tylko do niezbędnych informacji i ograniczając ruch atakujących w celu znacznego zmniejszenia ryzyka organizacyjnego wynikającego z niewykrytych zagrożeń.

Zobacz rozwiązania →

TYP ATAKU: ZERO-DAY

Przypomnienie

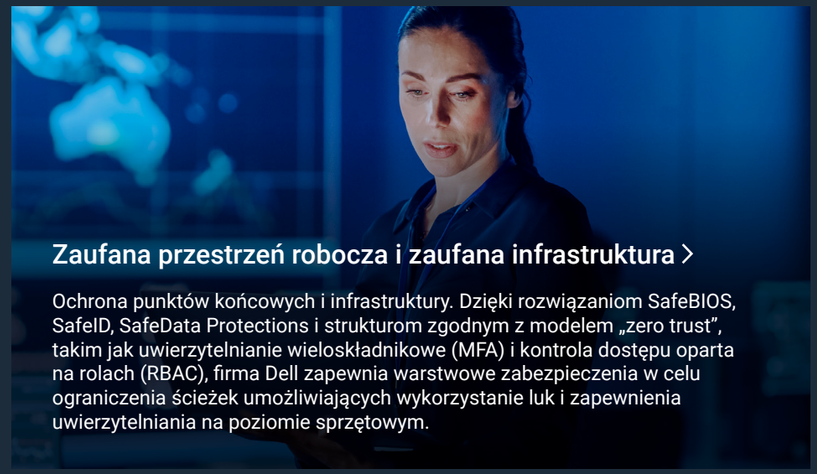
Atak typu „Zero-Day” polega na wykorzystaniu nieujawnionej luki w zabezpieczeniach oprogramowania lub sprzętu przed udostępnieniem poprawki lub rozwiązania. Atakujący wykorzystują lukę w zabezpieczeniach, często powodując poważne zakłócenia, zanim luka zostanie wykryta i naprawiona.

Firma Dell przeciwdziała atakom typu „Zero-Day” poprzez kontrole wg modelu „zero trust”, segmentację sieci, szybką izolacji i edukację użytkowników, co jeszcze bardziej wzmacnia ochronę przed nowymi zagrożeniami.

Dowiedz się więcej o zaawansowanych strategiach cyberodporności i przekonaj się, w jaki sposób firma Dell może pomóc chronić Twoją organizację przed atakami Zero-Day.

Zapoznaj się z krótkim opisem ataków typu zero-day →

Wróć do scenariuszy



Zaufana przestrzeń robocza i zaufana infrastruktura >

Ochrona punktów końcowych i infrastruktury. Dzięki rozwiązaniom SafeBIOS, SafeID, SafeData Protections i strukturom zgodnym z modelem „zero trust”, takim jak uwierzytelnianie wieloskładnikowe (MFA) i kontrola dostępu oparta na rolach (RBAC), firma Dell zapewnia warstwowe zabezpieczenia w celu ograniczenia ścieżek umożliwiających wykorzystanie luk i zapewnienia uwierzytelniania na poziomie sprzętowym.

Serwery PowerEdge >

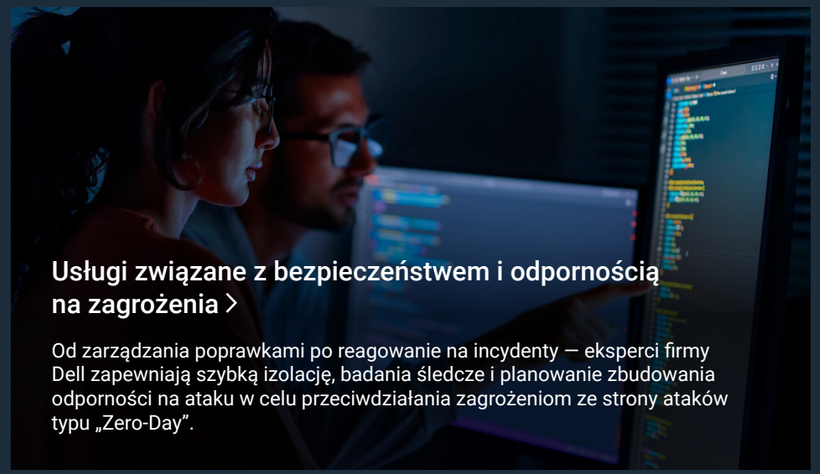
Rozwiązanie Secure Booth, mechanizm Silicon Root of Trust i segmentacja sieci SmartFabric ograniczają ruch boczny, gwarantując, że w infrastrukturze działa tylko zaufany kod.

Partnerzy ds. bezpieczeństwa >

Zaawansowana analiza zagrożeń, zarządzanie wykrywaniem i reagowaniem (MDR), rozszerzone wykrywanie i reagowanie (XDR) oraz precyzyjne mechanizmy kontroli dostępu pomagają wykrywać, tropić i powstrzymywać ataki Zero-Day, zanim się rozprzestrzenią.

Oferta PowerProtect >

Niezmienne kopie zapasowe, odizolowane magazyny Cyber Recovery i oparte na sztucznej inteligencji analizy CyberSense zapewniają szybkie przywracanie i odporność na ataki po naruszeniach typu „Zero-Day”.



Usługi związane z bezpieczeństwem i odpornością na zagrożenia >

Od zarządzania poprawkami po reagowanie na incydenty — eksperci firmy Dell zapewniają szybką izolację, badania śledcze i planowanie zbudowania odporności na ataku w celu przeciwdziałania zagrożeniom ze strony ataków typu „Zero-Day”.


DELL Technologies