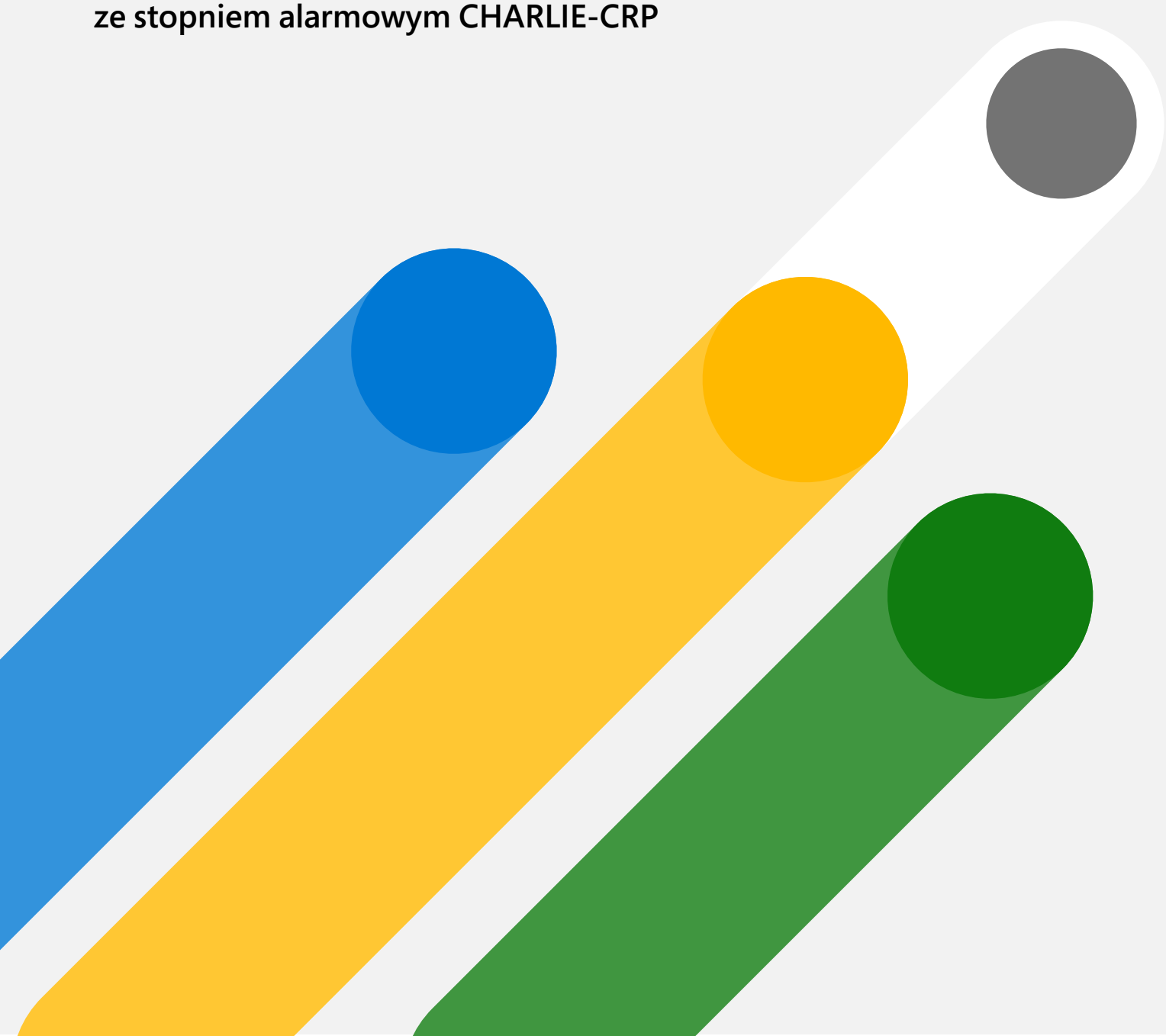
Microsoft Security

Ograniczanie ryzyka w obszarze cyberbezpieczeństwa

– zalecenia i rekomendacje w związku ze stopniem alarmowym CHARLIE-CRP



Dokument kierowany jest do osób odpowiedzialnych w organizacjach za zabezpieczanie środowisk cyfrowych, osób budujących strategię cyberbezpieczeństwa, jak również odpowiedzialnych za procedury bezpieczeństwa w organizacji.

Dokument odnosi się do zagadnień związanych z ograniczeniem ryzyk w obszarze cyberbezpieczeństwa i będzie najbardziej pomocny dla użytkowników Office 365, Microsoft 365 oraz Azure. Niniejszy dokument jest również skierowany do użytkowników lub osób planujących wdrożenie takich technologii.

Treść tego dokumentu ma wyłącznie charakter informacyjny. Ostateczna decyzja o wykorzystaniu opisanych w dokumencie technologii powinna wynikać z analizy stanu cyberbezpieczeństwa istniejącej infrastruktury, potrzeb oraz ryzyk związanych z eksploatacją systemów informatycznych.

Dokument przedstawia stan techniczny i możliwości poszczególnych usług w lutym 2022.

Zachęcamy do kontaktu i wspólnego przeprowadzenia analizy potrzeb i rozwiązań z wyspecjalizowanymi partnerami Microsoft lub do omówienia zagadnień z architektury cyberbezpieczeństwa z opiekunami państwa kontraktu suportowego Microsoft.

Spis Treści:

Wstęp

Usługi cyfrowe mają coraz większy wpływ na obywateli, struktury administracji i gospodarkę. Jesteśmy od nich uzależnieni w takim stopniu, że dysfunkcja pojedynczej usługi często powoduje skutki dalece wykraczające poza granice władającej nią organizacji i może doprowadzić do sytuacji kryzysowej.

Zmieniająca się sytuacja geopolityczna i rosnące zagrożenie działaniami hybrydowymi powodują konieczność implementacji do polskiego systemu prawnego nowoczesnych rozwiązań zapewniających bezpieczeństwo teleinformatyczne w obszarach takich, jak administracja publiczna, usługi kluczowe czy infrastruktura krytyczna. Jednym z dostępnych środków jest system stopni alarmowych CRP, który umożliwia stopniowe uruchamianie w organizacji rozwiązań pozwalających na wzmocnienie bezpieczeństwa systemów informatycznych.

Użytkownicy systemów informatycznych narażeni są na zaawansowane ataki wyspecjalizowanych grup hakerskich (zarówno motywowanych kryminalnie jak i politycznie), coraz częściej sponsorowanych przez rządy państw prowadzących ofensywne działania w cyberprzestrzeni. Zapewnienie bezpiecznego środowiska pracy wymaga wdrożenia określonych rozwiązań dotyczących między innymi:

- ochrony i zarządzania tożsamością pracowników, często w sfederalizowanym środowisku,
- ochrony urządzeń służbowych oraz prywatnych z których korzystają użytkownicy, w tym urządzeń typu PC, tabletów i smartfonów,
- wykrywania i blokowania ataków sieciowych i złośliwego oprogramowania dostarczanego najczęściej jako załączniki poczty elektronicznej oraz umieszczanego na stronach internetowych, na które przekierowywany jest nieświadomy zagrożenia użytkownik – największym wyzwaniem dla organizacji wciąż pozostaje ochrona przez zagrożeniami typu „zero-day", na które nie ma poprawek bezpieczeństwa,
- zapobiegania przypadkowemu lub świadomemu ujawnianiu informacji.

W niniejszym dokumencie przedstawione zostały scenariusze i obszary ataków przeprowadzane na organizacje i użytkowników oraz sposoby ograniczania tego typu ataków z wykorzystaniem rozwiązań zintegrowanych w Microsoft 365. Scenariusze te dotyczą zarówno urządzeń firmowych, z których korzysta użytkownik w domu, jak i urządzeń należących do użytkownika, które poza pracą wykorzystywane są do celów prywatnych (BYOD).

Wszystkie prezentowane poniżej rozwiązania wpisują się w zadania przeznaczone do realizacji przy wdrażaniu poszczególnych stopni alarmowych CRP – zgodnie z Rozporządzenie Prezesa Rady Ministrów z dnia 25 lipca 2016 r. *w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych*.

	ZADANIE	PROPONOWANE ROZWIĄZANIE MICROSOFT	STR.
Alfa-CRP	wprowadzić wzmożone monitorowanie stanu bezpieczeństwa systemów teleinformatycznych organów administracji publicznej lub systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej	Microsoft Defender for Endpoint	str. 27
		Microsoft Sentinel	str. 38
		Microsoft Defender for IoT/OT	str. 40
	monitorować i weryfikować, czy nie doszło do naruszenia bezpieczeństwa komunikacji elektronicznej	portal security.microsoft.com	str. 36
		Microsoft Defender for Office 365	str. 22
		Office 365 DLP, w tym dla Microsoft Teams	str. 33
		Azure Information Protection	str. 31
		Microsoft Sentinel	str. 38
	sprawdzać dostępność usług elektronicznych	Microsoft Defender for Endpoint	str. 27
		Exchange Online Protection	str. 20
		Microsoft Defender for Office 365	str. 22
	dokonywać, w razie potrzeby, zmian w dostępie do systemów	Microsoft Intune	str. 25
		Dostęp Warunkowy	str. 14
	sprawdzić aktualny stan bezpieczeństwa systemów i ocenić wpływ zagrożenia na bezpieczeństwo teleinformatyczne na podstawie bieżących informacji i prognoz wydarzeń;	Secure Score	str. 8
		Microsoft Defender for IoT/OT	str. 40
		Microsoft Defender for Endpoint – Threat & Vulnerability Management	str. 29
Bravo-CRP	zapewnić dostępność w trybie alarmowym personelu odpowiedzialnego za bezpieczeństwo systemów	Windows 365	str. 19
Charlie-CRP	wprowadzić całodobowe dyżury administratorów systemów kluczowych dla funkcjonowania organizacji oraz personelu uprawnionego do podejmowania decyzji w sprawach bezpieczeństwa systemów;	Microsoft Sentinel	str. 38
		portal security.microsoft.com	str. 36

Poniższa tabela zawiera zestawienie zagrożeń, podsumowanie omawianych scenariuszy wraz z zyskiem, jakie niosą dla bezpieczeństwa organizacji oraz określeniem stopnia skomplikowania wdrożenia:

TYP ZAGROŻENIA	MECHANIZMY ZABEZPIECZAJĄCE	WPŁYW NA BEZPIECZEŃSTWO	TRUDNOŚĆ WDROŻENIA
Kradzież tożsamości	Azure MFA	★★★	⚙⚙
	Identity Protection	★★★	⚙
	Privileged Identity Management	★★★	⚙⚙
	Dostęp Warunkowy	★★	⚙⚙
	Microsoft Defender for Identity	★★★	⚙⚙⚙
Złośliwy kod w poczcie elektronicznej	Exchange Online Protection	★★	⚙
	Microsoft Defender for Office 365	★★★	⚙
Brak monitoringu i zarządzania bezpieczeństwem urządzeń lokalnych i mobilnych	Microsoft Intune	★★★	⚙⚙
Ataki internetowe i wewnętrzne – w tym zaawansowane ataki APT	Microsoft Defender for Identity	★★★	⚙
Nieuprawnione ujawnienie informacji	Azure Information Protection	★★★	⚙⚙⚙
	Office 365 DLP	★★	⚙
Brak kontroli nad uruchamianymi aplikacjami chmurowymi	Microsoft Cloud App Security	★★★	⚙⚙
Brak monitoringu – ewidencji i dostępu do chronionych informacji	Portale M365	★★★	⚙
	O365 Advanced eDiscovery	★★★	⚙
Brak korelacji zdarzeń bezpieczeństwa z różnych systemów - rozproszone, pojedyncze widoki nie dające jednego, spójnego punktu raportowania	Azure Sentinel	★★★	⚙

2. Punkt wyjścia: ocena stanu cyberbezpieczeństwa

Budowę Referencyjnej Architektury Cyberbezpieczeństwa warto rozpocząć od wykorzystania dedykowanego narzędzia Microsoft Secure Score, dostępnego w ramach usługi Office 365. Narzędzie Secure Score pozwala na zidentyfikowanie obszarów podwyższonych ryzyk dla cyberbezpieczeństwa, z możliwością odniesień do międzynarodowych i niezależnych standardardów oceny bezpieczeństwa (np. NIST, CIS – Center for Internet Security i wiele innych).

Narzędzie Secure Score nie wymaga instalacji dodatkowych narzędzi, weryfikuje obecny stan konfiguracji usług i dostarcza bazę wiedzy dla administratorów bezpieczeństwa w organizacji, wspomagając definiowanie niezbędnych działań podnoszących poziom cyberbezpieczeństwa. W efekcie analizy z wykorzystaniem Secure Score można uzyskać na przykład rekomendacje dotyczące:

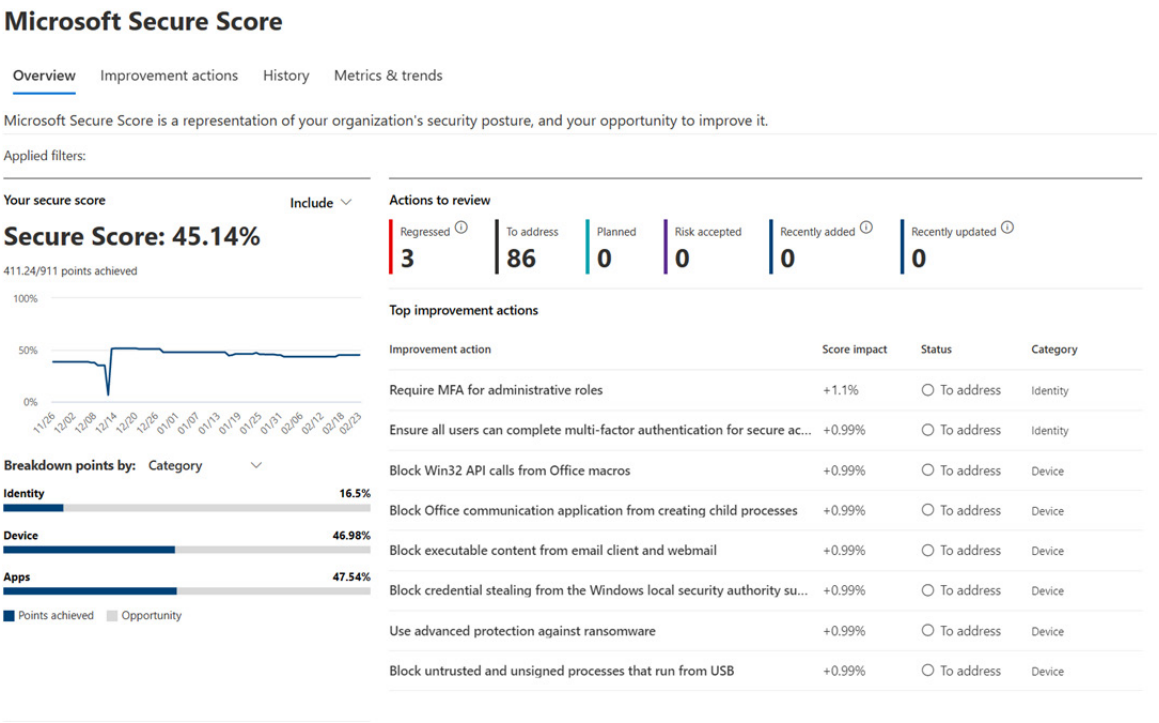
- oceny bezpieczeństwa tożsamości pracownika i wdrożenie dodatkowego składnika uwierzytelnienia poprzez wykorzystanie funkcji Azure Multi-factor authentication (SMS na komórkę, telefon od agenta MFA, czy aplikację generującą jednorazowe kody dostępowe), wyłączenia niebezpiecznych protokołów w organizacji,
- zbyt wysokich uprawnień w systemie w ramach grup administracyjnych, co może skutkować dostępem do danych wrażliwych innych użytkowników,
- wdrożenia zarządzania urządzeniami mobilnymi i kontrolowania przepływu danych pomiędzy aplikacjami na urządzeniach mobilnych, czyli przykładowe skopiowanie załącznika z poczty do nieuprawnionej aplikacji zewnętrznej,
- wdrożenia polityk informujących o próbie nieuprawnionego ujawnienia informacji/danych poza organizację
- innych zaleceń zdefiniowanych w standardach i benchmarkach bezpieczeństwa.

Zalecenia z narzędzia Secure Score obejmują różne obszary i są komplementarne, tj. nie muszą być wdrażane jednocześnie, chociaż ich wzajemne dopełnianie się umożliwia uzyskanie dodatkowych korzyści z synergii rozwiązań, a wzajemna integracja daje możliwość większej kontroli przy jednoczesnym zachowaniu elastycznych możliwości pracy przez użytkownika.

Każdy **typ cyber-zagrożenia** oraz odpowiadające mu **mechanizmy zabezpieczające** zostały sklasyfikowane pod kątem **wpływu na bezpieczeństwo** (za pomocą symbolu od 1 (najmniejsze) do 3 (największe)) oraz **trudności wdrożenia** (poziomu skomplikowania) (za pomocą symbolu od 1 (najmniejsza) do 3 (największa)).

Aby zweryfikować środowisko organizacji pod kątem aktualnej konfiguracji oraz dalszych zaleceń, administrator środowiska Office 365 uruchamia narzędzie Secure Score dostępne pod adresem https://security.microsoft.com/securescore – posiadanie uprawnień administracyjnych wymagane jest w celu weryfikacji zaleceń Secure Score.

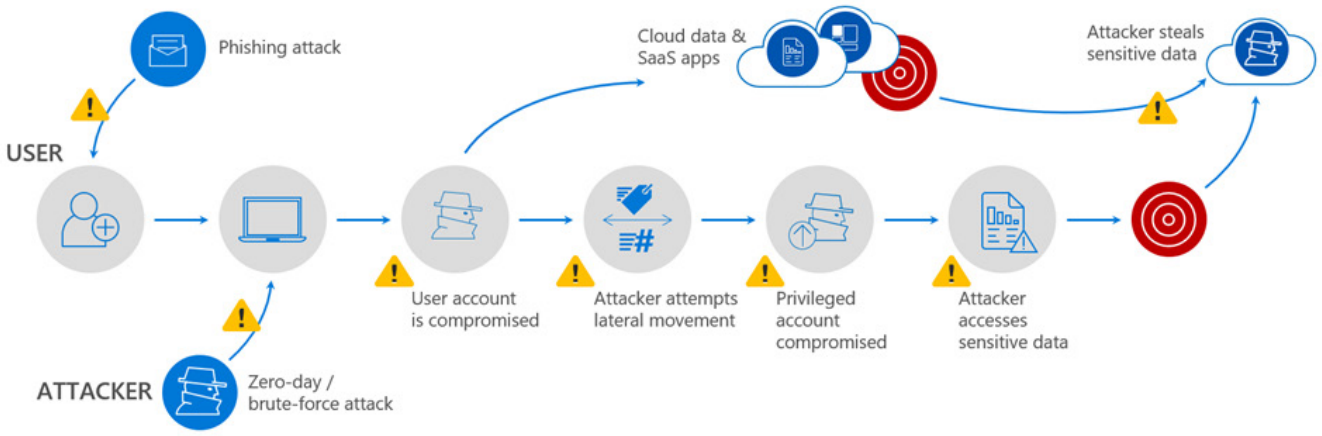
Na poniższym zrzucie ekranowym znajduje się przykład z raportu Secure Score. Otrzymany wynik wskazuje ponadto obszary, w których wykryto ryzyka oraz szczegółowe punkty, które nie zostały prawidłowo zaadresowane pod kątem spełnienia zaleceń bezpieczeństwa.



3. Ograniczenie wektorów ataku

Współcześnie atakujący wykorzystują coraz to nowsze techniki ataków na organizacje, gdzie łańcuch ataku (ang. *kill chain*) i jego fazy mogą gwarantować profesjonalnej grupie hakerów pozyskanie tożsamości pracownika instytucji poprzez wykorzystanie kierunkowych ataków typu phishing lub spear phishing (próba zachęcenia użytkownika do zalogowania na fałszywej stronie).

Po uzyskaniu dostępu do konta pracownika, który dał złapać się w pułapkę lub przechwyceniu dostępu do jego komputera firmowego lub personalnego, atakujący zaczynają wykonywać analizę, do czego pracownik ma dostęp, co ostatecznie prowadzi do wycieku danych wrażliwych lub zaatakowaniu kolejnych osób w organizacji.



W ramach pakietu Microsoft 365 dostępne są narzędzia, które są w stanie ograniczyć ryzyka związane z podatnościami bezpieczeństwa:

- **Obecnie 96% ataków na organizacje rozpoczyna się poprzez wysłanie fałszywej wiadomości zawierającej link lub dokument z niebezpiecznym oprogramowaniem**. Kampanie typu wykradanie poświadczenia pracownika i szyfrowanie stacji pracownika są obarczone bardzo dużym

ryzykiem. Złagodzenie skutków tego ataku poprzez wykorzystanie technologii Microsoft Defender for Office 365 oraz drugiego składnika uwierzytelnienia (MFA) pozwala minimalizować ten wektor ataku na organizacje

- **Ataki na niezabezpieczoną stację pracownika lub urządzenie mobilne lub hasło użytkownika** to również bardzo duże zagrożenie. Jeśli pracownik wykorzystuje stację, która została skompromitowana przez atakującego może w dalszym kroku pozyskać informację o hasłach logowania do systemów instytucji lub wykradać wrażliwe danych w sposób niekontrolowany przez dział bezpieczeństwa. Tego typu ataki są bardzo trudne do wykrycia. W celu ograniczenia tego typu ataków niezbędne są mechanizmy umożliwiające zarządzanie bezpieczeństwem stacji roboczej pracownika i/lub urządzeniami mobilnymi, na którym wykonuje powierzone mu zadania. Jeśli pojawią się zaawansowane metody ataku na konto pracownika to możliwe jest wykrycie anomalii związanych z logowaniem (m.in. logowanie poza godzinami pracy, logowanie do zasobów do których pracownik nigdy nie sięgał, itp.) za pomocą technologii Microsoft Defender for Identity.

- **Nieuprawnione ujawnienie informacji z organizacji** to kolejny z etapów, gdzie po uzyskaniu dostępu do konta pracownika lub przełamaniu zabezpieczeń systemu operacyjnego, atakujący może pozostawać niewykryty przez długi czas i wykradać wrażliwe informacje. W tym celu rekomendowane jest wykorzystanie całej palety narzędzi do wykrywania nieuprawnionego ujawnienia lub próby ujawnienia informacji, co zostało opisane w dalszych częściach tego dokumentu. Są to między innymi mechanizmy *Data Loss Prevention* (DLP) zapobiegające wyciekom danych, technologie szyfrowania informacji, czy etykietowania danych wrażliwych przykładową klasyfikacją „informacja kontrolowana", czy „tylko dla pracowników". Nawet w przypadku wycieku informacji wrażliwej, atakujący nie posiadający dostępu do danych logowania nie będzie w stanie odszyfrować zawartości przykładowego dokumentu lub informacji w systemie poczty elektronicznej i to niezależnie od miejsca przechowywania pliku zawierającego te informacje.

- **Obrona przed atakami ukierunkowanymi na urząd/organizację przez wyspecjalizowane grupy (APT – Advanced Persistent Threat).** Nowoczesne metody ataków wykorzystujące tak zwane podatności *zero-day*, w sytuacji, w której producent nie jest świadom ryzyka lub nie została jeszcze wydana poprawka bezpieczeństwa - to niestety bardzo duże i trudno wykrywalne zagrożenie. Często tego typu ataki pozwalają na uzyskanie dostępu do telefonu, tabletu, czy

komputera ofiary, a następnie długotrwałe przybywanie hakera w systemie, co prowadzi do pełnej inwigilacji oraz jest punktem wyjścia do ataków na strukturę zarządzania domeną sieciową. Tutaj warto zadbać o możliwość wykrywania nietypowych zachowań systemu operacyjnego, czy pracownika na jego komputerze lub urządzeniu mobilnym i odpowiednim monitorowaniu przez operacyjne centra bezpieczeństwa (SOC – *Security Operation Center*) tego typu zdarzeń. Pozwoli to opracować sposób reakcji na incydenty, w momencie, kiedy zagrożenie się pojawiło i trzeba je jak najszybciej wyeliminować z infrastruktury teleinformatycznej organizacji.

4. Zabezpieczenie konta pracownika i dostęp zdalny

Wraz ze wzrostem znaczenia dostępu mobilnego i pracy zdalnej, rośnie waga ochrony tożsamości pracownika. Nazwa użytkownika i hasło do wielu systemów organizacji staje się wtedy kluczowym parametrem, który należy chronić.

Kompromitacja tożsamości (przechwycenie tożsamości, kradzież haseł, podszywanie pod pracownika po przejęciu kontroli) powoduje utratę kontroli nad danymi i może skutkować wyciekiem danych z organizacji. Bardzo ważny jest również aspekt rozliczalności działań użytkowników (logowanie się do systemów) oraz dostęp do zasobów organizacji (emaile, dokumenty, bazy wiedzy).

W celu przeciwdziałania kompromitacji tożsamości, należy korzystać z narzędzi i rozwiązań zapewniających monitorowanie i kontrolę działań użytkownika.

Uwierzytelnienie wieloskładnikowe podczas logowania do krytycznych aplikacji - Azure Multi Factor Authentication ★★★ / ✪✪

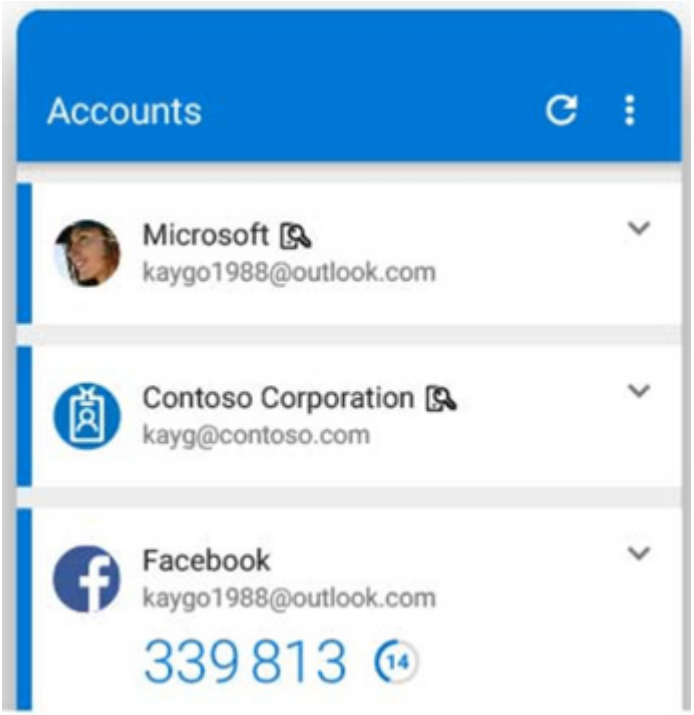
Najprostszym sposobem obrony konta logowania pracownika jest uruchomienie usługi dodatkowego składnika uwierzytelnienia (MFA – Multi-Factor Authentication). Działa to podobnie, jak w przypadku logowania do usług w banku, gdzie operacja logowania lub wykonania przelewu musi zostać potwierdzona na urządzeniu mobilnym należącym do właściciela konta. W ramach usługi Azure MFA uruchomiana jest

dodatkowa weryfikacja tożsamości podczas logowania wykorzystująca jedną z wymienionych metod:

- Wykorzystanie aplikacji Microsoft Authenticator, która generuje co 60 sekund nowy unikalny kod jednorazowego logowania.
- Użycie kluczy U2F
- Wysłanie wiadomości SMS z jednorazowym kodem dostępowym,
- Połączenie głosowe z wirtualnym asystentem logowania, który prosi o wprowadzenie unikalnego kodu PIN zdefiniowanego wcześniej przez pracownika,

Więcej na temat usługi Azure MFA można znaleźć w artykule bazy wiedzy: https://www.microsoft.com/en-us/security/business/identity/mfa

Na poniższym przykładzie zaprezentowano wykorzystanie aplikacji Microsoft Authenticator na urządzeniu mobilnym, gdzie zarówno dla kont firmowych oraz personalnych (Facebook) generowane są unikalne kody jednorazowe do logowania.



Włączenie usługi Azure MFA to jedna z najprostszych metod podniesienia bezpieczeństwa konta pracownika:

- **obniża możliwość kompromitacji kont użytkowników o 99,9%**, nawet jeśli poświadczenie zostanie skradzione to atakujący musi mieć dostęp do telefonu, żeby potwierdzić logowanie. Tutaj bardzo ważne jest również mitygowanie ryzyka związanego z przejęciem konta w atakach typu przechwycenie danych logowania za pomocą ataków phishingowych.
- **umożliwia wybór formy weryfikacji drugiego składnika** - nie tylko SMS lub aplikacja Microsoft Authenticator, ale też klucze FIDO2, tokeny sprzętowe i programowe.
- **zapewnia łatwą implementację bez konieczności posiadania własnej infrastruktury** – https://docs.microsoft.com/en-GB/azure/active-directory/authentication/howto-mfa-getstarted

Dostęp Warunkowy (Conditional Access) ★★ / ⚙⚙

Pracownicy najczęściej logują się z urządzeń firmowych do usług Office 365, czy aplikacji lokalnych. W momencie kiedy pojawia się wymaganie pracy zdalnej bardzo ważnym aspektem jest zadbanie o bezpieczeństwo logowania z zewnątrz. Z pomocą przychodzi tutaj usługa dostępu warunkowego pozwalająca na użycie „warunków" podczas próby logowania do konkretnej aplikacji. Rozważając najprostszy przykład logowania typowego użytkownika:

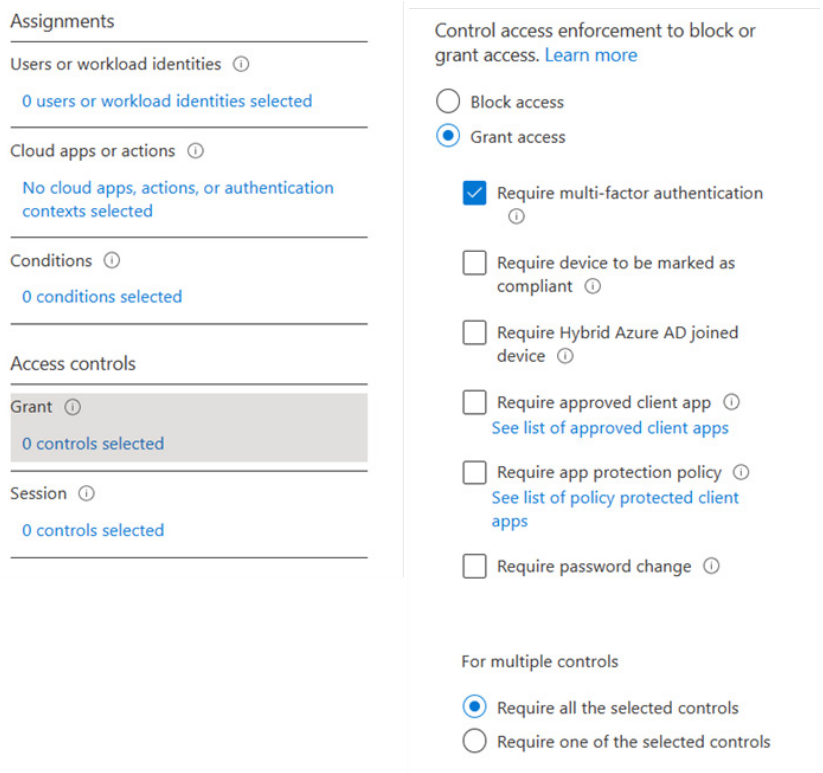
- Jeśli loguje się z siedziby instytucji to jest automatycznie zalogowany do usługi lub aplikacji.
- Jeśli logowanie następuje z domowego komputera, spoza sieci wewnętrznej to w tym wypadku pracownik powinien otrzymać prośbę o wprowadzenie kodu jednorazowego z usługi MFA.
- Jeśli logowanie następuje z domowego komputera lub personalnego urządzenia przenośnego to użytkownik powinien zaakceptować regulamin korzystania z usługi, na jego urządzeniu zostaną wymuszone polityki bezpieczeństwa i dopiero wtedy uzyska dostęp do aplikacji lub usługi.

Oznacza to, że dostęp warunkowy to lista dodatkowych działań, które mogą być wymuszone i sprawdzone podczas logowania do aplikacji, przykładowo:

- **weryfikacja próby ryzykownego logowania** przykładowo z sieci anonimowych (np. TOR), z sieci, które zostały zaatakowane lub przejęte przez hakerów czy podróż niemożliwa do przebycia (logowania z Polski, a po 5 minutach z Rosji, Chin itp.).
- **weryfikacja czy urządzenie jest zarządzane przez organizację i nie zostało zainfekowane.** W momencie, kiedy urządzenie jest prywatne mogą być na nim zastosowane odpowiednie polityki bezpieczeństwa i dopiero wtedy pracownik uzyska dostęp do systemu.
- **Logowanie tylko ze specyficznych lokalizacji**, przykładowo tylko sieci wewnętrzne.

Więcej informacji na temat warunków logowania w usłudze dostępu warunkowego (ang. Conditional Access) można znaleźć w artykule bazy wiedzy Microsoft: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

W poniższym przykładzie zaprezentowano politykę, gdzie dana grupa pracowników zostaje objęta regułą dostępu warunkowego, który wymusza dodatkowy składnik uwierzytelnienia przy logowaniu do konkretnej aplikacji.



Usługa dostępu warunkowego pozwala na zbudowanie strategii „nigdy nie ufaj, zawsze weryfikuj" (ang. Zero Trust), która znacznie podnosi bezpieczeństwo organizacji, po akceptacji poświadczenia logowania. W tym scenariuszu atakujący musi przejąć również dostęp do urządzenia mobilnego, które odpowiada za proces dwuskładnikowego uwierzytelnienia.

Podstawa przy wdrażaniu strategii „Zero Trust":
https://www.microsoft.com/en-us/security/business/identity/conditional-access

Więcej na temat modelu „Zero Trust":
Zabezpieczenia oparte na modelu Zero Trust (microsoft.com)

Wykrywanie nietypowych zachowań logowania pracownika ★★★ / ⚙

Jednym z kluczowych wymagań ochrony zasobów informacyjnych organizacji jest możliwość wykrycia zagrożeń jak nietypowa podróż, dostęp z anonimowych sieci (TOR), nietypowe logowanie, logowanie z adresu kojarzonego ze złośliwym oprogramowaniem czy phishingiem oraz wyciek danych logowania. Narzędziem realizującym w te funkcje w sposób zautomatyzowany jest **Identity Protection**.

Narzędzie to bazuje na analityce *Cyber Threat Inteligence* budowanej przez firmę Microsoft w ramach publicznej chmury obliczeniowej. Dane pochodzą z analizy 6,5 tryliona sygnałów dziennie wysyłanych przez urządzenia z systemem Windows, rozwiązania konsumenckie Microsoft, czy rozwiązania biznesowe. Jako przykład można tutaj podać nową mutację niebezpiecznego oprogramowania ransomware Bad Rabbit, która została wykryta na Ukrainie i zablokowana globalnie przez Microsoft w ciągu 15 minut.

Więcej informacji na temat funkcjonalności Identity Protection zawiera artykuł bazy wiedzy:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection

Ochrona tożsamości i uprawnień administratorów oraz użytkowników specjalnych za pomocą Privileged Identity Management (PIM) ★★★ / ⚙⚙

Wiele organizacji nie kontroluje pracy administratorów w działach IT, którzy mają wysokie uprawnienia w ramach dostarczanych i obsługiwanych aplikacji i systemów. Wysokie uprawnienia najczęściej umożliwiają dostęp do dowolnych danych i plików.

Usługa Privileged Identity Management (PIM) dostępna w ramach Azure Active Directory pozwala kontrolować wykorzystanie ról administracyjnych, analizę czy nie została wykonana operacja mająca na celu nieuprawnione ujawnienie informacji, czy też posiadanie zbyt wysokich uprawnień do wykonywania standardowych, codziennych czynności. Najlepszą praktyką jest przydzielanie uprawnień na zdefiniowany czas (*just-in-time access*) do wykonania specyficznej operacji administracyjnej, sam proces akceptacji nadania uprawnienia administracyjnego może wymagać akceptacji przełożonego w dziale IT lub dziale bezpieczeństwa.

Usługa PIM pozwalająca na zarządzanie, kontrolę i monitorowanie dostępu do ról uprzywilejowanych *Azure Active Directory* – https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

Ochrona przed kradzieżą tożsamości pracownika - usługa Microsoft Defender for Identity ★★★ / ⚙⚙⚙

Jeden z najczęstszych ataków hackerskich to kradzież tożsamości pracownika poprzez wykorzystanie skomplikowanych metod przejęcia poświadczeń w systemie operacyjnym lub próba wyłudzenia poświadczeń za pomocą fałszywej wiadomości e-mail.

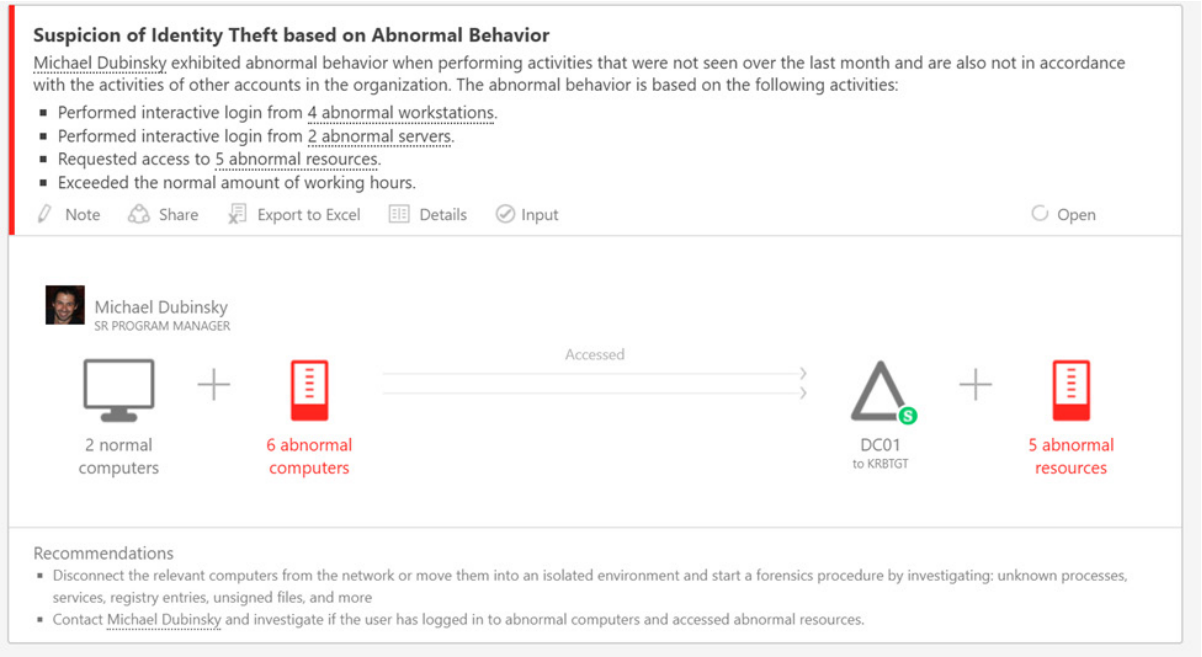
Usługa Microsoft Defender for Identity jest bardzo łatwym w implementacji rozwiązaniem umożliwiającym monitorowanie usług katalogowych w środowisku hybrydowym (obejmuje chmurę i usługi tożsamości zarządzane lokalnie), które za pomocą technologii uczenia maszynowego (ang. Machine Learning) buduje wzorzec codziennej pracy i zachowania pracownika organizacji. Oznacza to, że usługa zbiera dane o logowaniu do urządzeń i zasobów w organizacji, godziny pracy, z jakimi

komputerami i serwerami pracownik się komunikuje, po czym jest w stanie wykrywać różnego rodzaju odstępstwa od normy. Odstępstwem może być tutaj skomplikowana metoda ataku na tożsamość użytkownika i późniejsze sięganie do plików w kontekście tego konta, gdzie nigdy wcześniej nie zostało to zaobserwowane przez mechanizmy wykrywające i analizujące.

W ramach usługi Microsoft Defender for Identity możliwe jest zapewnienie:

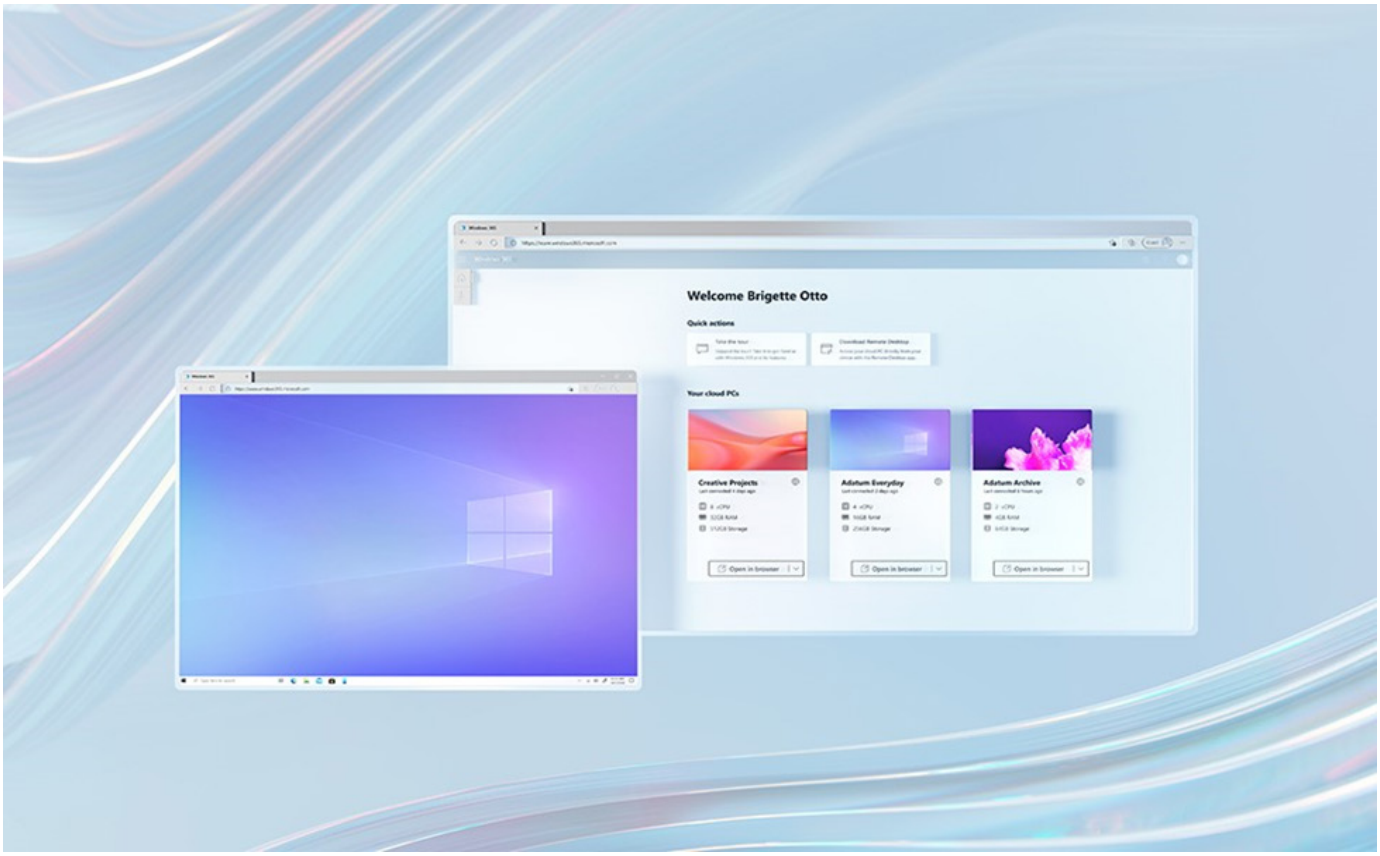
- ochrony lokalnej infrastruktury usługi katalogowej poprzez monitorowanie ruchu z i do kontrolerów domeny oraz kontrolowanie logów kontrolerów domeny. Ochrona dotyczy zarówno etapu rekonesansu m.in. enumeracja udziałów sieciowych, użytkowników, rekonesans usługi DNS, jak i samej fazy ataku (tutaj mowa o wielu atakach na tożsamość, m.in. *Pass-The-Hash*, *Pass-The-Ticket*, *Golden Ticket*, *Skeleton Key*).
- Uczenie się zachowania użytkowników (sposoby i czas logowania, używane zasoby) i wykrywanie anomalii pozwalające zatrzymać atak w przypadku użycia przez atakującego skradzionych uwierzytelnień pracowników.

Poniżej przedstawiony został przykład działania Microsoft Defender for Identity, gdzie atakujący przejął konto pracownika Michael Dubinsky, a następnie zaczął przeglądać zasoby sieciowe zaatakowanej organizacji oraz logował się kradzionym kontem do wielu komputerów w organizacji.



Bezpieczny dostęp zdalny

Windows 365 jest usługą typu Desktop-as-a-Service, która zapewnia bezpieczny dostęp do sieci firmowej z dowolnego urządzenia. Tego typu komputer w chmurze może służyć jako stacja przesiadkowa lub komputer dostępowy, aby w bezpieczny sposób korzystać z zasobów służbowych.



Komputery w chmurze mogą być łatwo konfigurowane, a także dostosowywane do potrzeb pracowników, aby bezpiecznie obsługiwać pracowników hybrydowych.

5. Ochrona przez dotychczas nierozpoznanym złośliwym oprogramowaniem oraz atakami phishingowymi

Według wielu branżowych statystyk, 96% cyberataków rozpoczyna się od systemów pocztowych. Złośliwy kod w ramach załączników (przykładowy PDF, czy Word) oraz odnośniki do witryn internetowych (zawierających złośliwy kod) są uruchamiane przez użytkowników w ciągu pierwszych pięciu minut trwania ataku. Większość ataków jest polimorficzna – kod używany jest zazwyczaj tylko jeden raz i nie jest możliwy do wykrycia przez typowe systemy antywirusowe bazujące na dynamicznych sygnaturach.

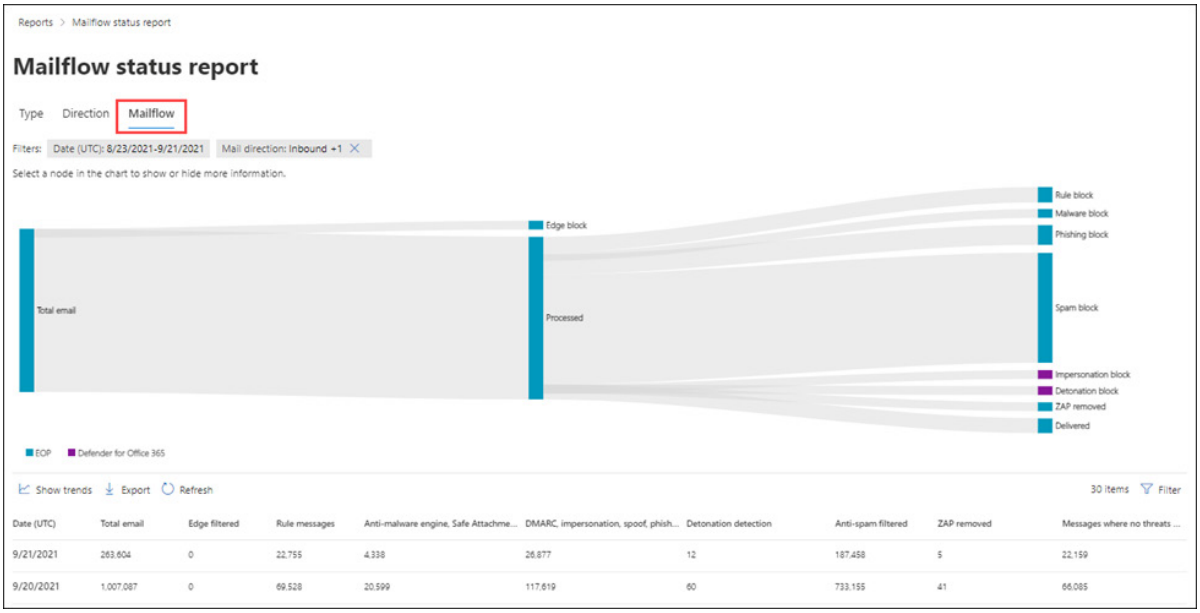
Oznacza to, że bez zastosowania mechanizmów analizujących każdy załącznik lub link w wiadomościach otrzymywanych przez urząd, możliwe jest zainfekowanie infrastruktury organizacji nowym rodzajem kodu złośliwego, które nie zostanie rozpoznane przez systemy antywirusowe na komputerze lub urządzeniu mobilnym. W celu ograniczenia tego ryzyka niezbędne jest wykorzystanie w systemie poczty elektronicznej zaawansowanych mechanizmów uczenia maszynowego, które w czasie rzeczywistym (on-click) analizują zawartość dokumentów i linków i są w tanie automatycznie zatrzymać dotychczas nierozpoznane nowe typy kodu, którego analiza może wskazywać na złośliwe cechy.

Ochrona systemu poczty elektronicznej w środowisku hybrydowym - Exchange Online Protection ★★ / ⚙

Usługa Exchange Online Protection (EOP) pozwala na zatrzymanie zagrożeń związanych ze złośliwym kodem, spamem, czy innymi niebezpiecznymi zachowaniami w poczcie e-mail. Usługa ta może być stosowana w środowisku hybrydowym – chroniąc lokalne systemy pocztowe usługi pocztowe publicznych chmurach obliczeniowych.

Usługa Exchange Online Protection:

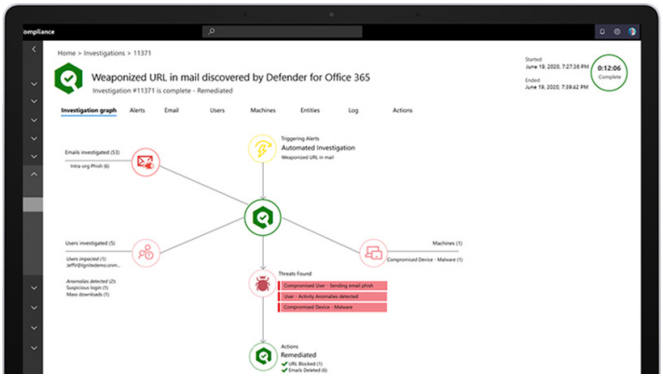
- chroni przed złośliwym kodem – trzy silniki antywirusowe
- chroni przed phishingiem – ponad 750 000 domen kwalifikowanych jako spam
- chroni przed spamem – obsługa 86 języków i 250 regionów
- możliwa do uruchomienia zarówno dla środowisk w chmurze jak i lokalnych. W momencie kiedy instytucja będzie chciała zabezpieczyć pocztę przechowywaną na lokalnych serwerach poczty, to wymagane jest przekierowanie rekordów MX w DNS na rozwiązanie Exchange Online Protection i zdefiniowanie odpowiednich łączników wysyłania i odbierania poczty pomiędzy lokalnymi serwerami a chmurą.
- dostępna bez potrzeby utrzymywania własnej infrastruktury.



Więcej informacji na temat Exchange Online Protection w artykule bazy wiedzy: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/exchange-online-protection-overview?view=o365-worldwide

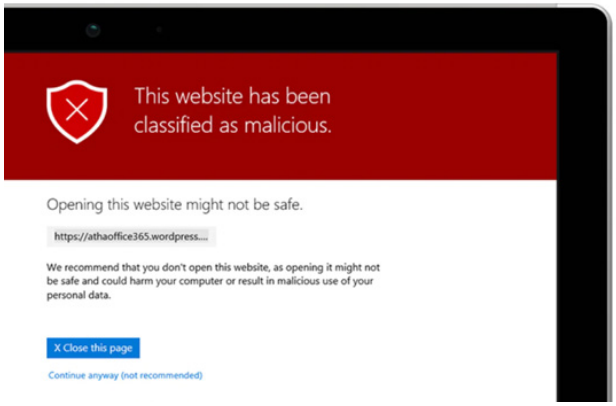
Detonacja niebezpiecznych linków i dokumentów w ramach Microsoft Defender for Office 365 ★★★ / ⚙

Dodatkowym komponentem usługi Exchange Online Protection jest warstwa detonacji niebezpiecznych załączników oraz linków realizowana w ramach modułu Defender for Office 365.

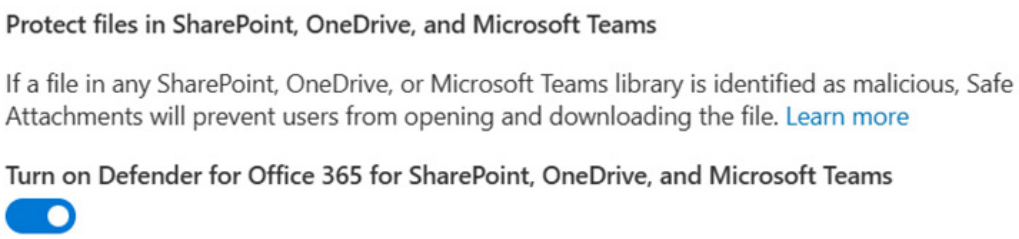


Oznacza to, że jeśli pracownik otrzyma zainfekowany plik lub link prowadzący do niebezpiecznego oprogramowania to taka próba ataku zostanie zatrzymana przy próbie otwarcia linku lub dokumentu.

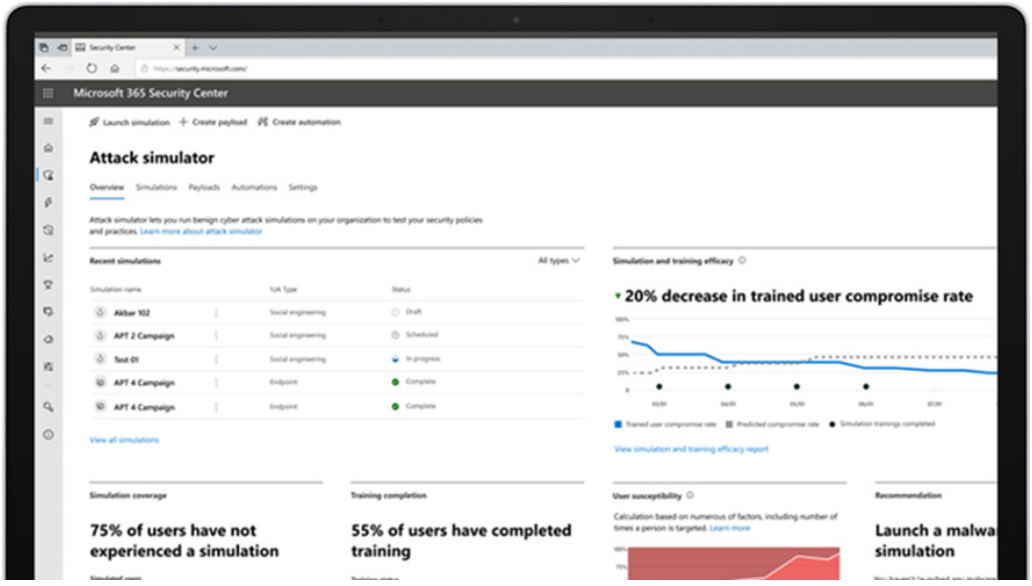
Poniżej przedstawiono przykład, gdzie pracownik otrzymał link w poczcie email prowadzący do wyłudzenia informacji lub instalacji niebezpiecznego oprogramowania. Link został zweryfikowany pod kątem reputacji bezpieczeństwa oraz został wykonany w komorze detonacyjnej, w której zweryfikowane zostało, co się stanie po otwarciu tej informacji na stacji typu PC/MAC/smartphone. Mechanizmy detonacji nie wprowadzają dodatkowych opóźnień związanych z dostarczeniem poczty, a standardowe skanowanie załącznika w komorze detonacyjnej pod kątem bezpieczeństwa trwa około 30 sekund.



Defender for Office 365 jest narzędziem umożliwiającym ochronę nie tylko poczty elektronicznej, ale całego systemu komunikacyjnego Microsoft w tym Microsoft Teams.

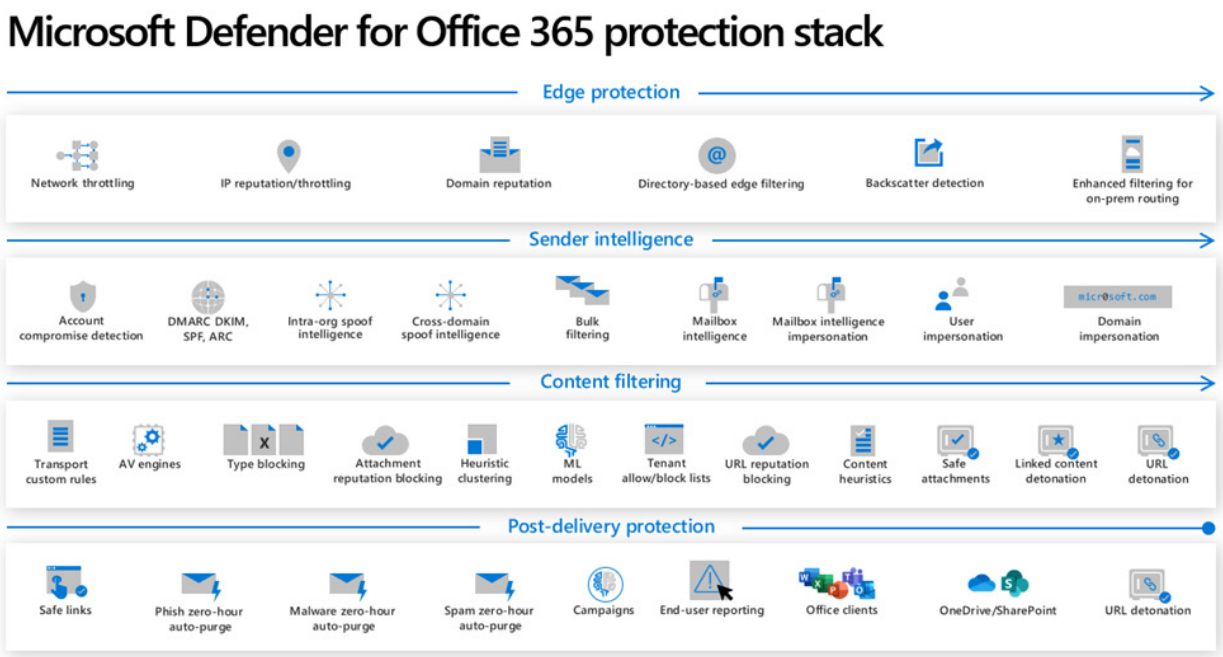


Defender for Office 365 pozwala także na wypracowanie świadomości użytkowników i wzmocnienie przekazów edukacyjnych poprzez przeprowadzanie okresowych symulacji ataków. Efektem takich ataków może być dedykowana kampania edukacyjna.



Funkcje Microsoft Defender for Office 365pozwalają między innymi na:

- ochronę przed nieznanymi zagrożeniami (także 0-day) oraz zdefiniowanie zaawansowanych polityk antyphishingowych dzięki wykorzystaniu globalnej bazy o zagrożeniach *Cyber Threat Intelligence* Microsoft.
- wykorzystanie mechanizmu *Safe Attachements* oraz *Safe Links* – weryfikacja załączników i linków wraz z detonacją w chmurze detonacyjnej
- automatyzację ochrony i reakcji na zagrożenia
- symulowanie ataków – pozwala na ćwiczenia organizacji pod kątem odporności na ataki przeprowadzane przez pocztę elektroniczną
- łatwe wdrożenie i utrzymanie usługi – automatycznie dostępne jako usługa, brak potrzeby utrzymywania własnej infrastruktury
- uruchomienie zarówno dla środowisk hybrydowych - w chmurze jak i lokalnych



6. Podniesienie poziomu bezpieczeństwa urządzeń służbowych i ochrona informacji służbowych w urządzeniach prywatnych

W sytuacji, gdy wielu pracowników pracuje z domu, z urządzeń służbowych lub prywatnych, istotną kwestią staje się zdalne zarządzanie urządzeniami i weryfikacja dostępu. Brak kontroli może powodować wiele naruszeń zasad bezpieczeństwa np.: nieuprawnione ujawnienie informacji, korzystanie z niezatwierdzonych aplikacji, uruchamianie złośliwego kodu.

Z tego powodu wiele organizacji stoi przed potrzebą wymiany klasycznych systemów zarządzania komputerami typu CMT (*Client Management Tools*) na zintegrowane systemy UEM (*Unified Endpoint Management*).

Zdalne zarządzanie urządzeniami typu PC, smartfon i tablety możliwe jest w ramach pakietu Microsoft 365 z wykorzystaniem rozwiązania Microsoft Endpoint Manager. Endpoint Manager pozwala również wdrożyć odpowiednie polityki bezpieczeństwa na urządzeniach końcowych, uruchomić polityki kontroli aplikacji, czy zweryfikować obecny stan bezpieczeństwa urządzenia.

Zarządzanie urządzeniami mobilnymi i komputerami za pomocą Microsoft Intune ★★★ / ⚙⚙

W ramach funkcji Endpoint Manager, dostępny jest system Microsoft Intune, czyli system klasy *Unified Endpoint Management,* dostarczający połączenie funkcjonalności MDM oraz EMM i CMT.

Pełny opis rozwiązania Intune dostępny jest na stronach Microsoft:
https://docs.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune

Microsoft Intune zapewnia realizację następujących funkcji zabezpieczających:

- zarządzanie urządzeniami (*Mobile Device Management*) jak i aplikacjami (*Mobile Application Management*). W ramach Mobile Application Management możliwe jest dostarczanie zaakceptowanych przez dział IT aplikacji na urządzenia, instalowanie aktualizacji, czy też kontrolowanie przepływu pomiędzy aplikacjami (aplikacja A nie może kopiować danych do aplikacji B), a także zarządzanie aplikacjami posiadającymi dostęp do informacji służbowych na prywatnych urządzeniach
- jednolity system do zarządzania systemami Windows 10 oraz urządzeniami na platformach mobilnych – iOS i Android
- Łatwe dołączanie (ang. *enrollment)* urządzeń mobilnych w organizacji. Możliwe jest tutaj dostarczenie procedury aktywacji urządzenia przez pracownika po zalogowaniu się na konto służbowe lub wymuszenie instalacji agenta Intune przy próbie dostępu do aplikacji firmowej (integracja z dostępem warunkowym).
- wsparcie dla wielu scenariuszy zarządzania (w tym *BYOD*), gdzie pracownik może korzystać z własnego urządzenia w bezpieczny sposób. Po zakończeniu stosunku pracy z lub zgubieniu urządzenia, usuwane są tylko dane firmowe z urządzenia końcowego.
- Windows Autopilot – szybka transformacja systemów Windows 10 zamiast klasycznego podejścia z instalacją obrazów systemów Windows. Oznacza to, że pracownik sam będzie mógł przeprowadzić instalację lub reinstalację systemu Windows, a następnie instalację aplikacji służbowych oraz konfigurację polityk bezpieczeństwa
- okresowa lub stała ocena zgodności urządzeń z polityką bezpieczeństwa organizacji oraz warunkami dostępu do poszczególnych kategorii zasobów służbowych (Dostęp Warunkowy) .

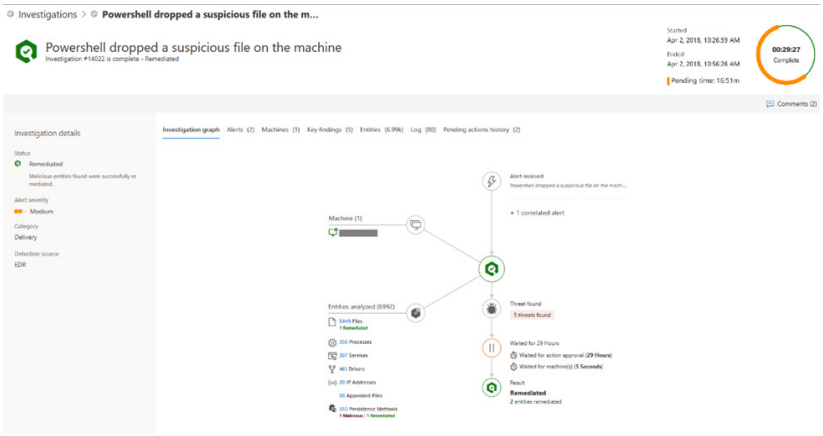
7. Ataki ukierunkowane na organizacje i zarządzanie podatnościami

Praca z różnych miejsc może powodować utratę kontroli organizacji nad środowiskiem sieciowym, do którego użytkownik podłącza swoje urządzenie. W rezultacie pracownik jest narażony na ataki hakerów, które mogą mieć na celu zaatakowanie systemu operacyjnego, ataki na podatne aplikacje i sterowniki oraz samego użytkownika (przechwycenie konta). Klasyczne systemy antywirusowe są niewystarczające ze względu na rosnącą liczę ataków typu file-*less* (przy użyciu makr i skryptów, wykorzystujące techniki wstrzykujące dane do pamięci oraz *exploity* systemu operacyjnego). Powoduje to, że na komputerze pracownika lub jego urządzeniu mobilnym powinna pojawić się dodatkowa ochrona oprócz systemu antywirusowego, która weryfikuje co dokładnie na tym urządzeniu jest uruchomione, jakie procesy i działania wykonał system operacyjny. Tego typu spojrzenie pozwoli wykryć bardzo zaawansowane ataki ukierunkowane na organizacje, które najczęściej wykorzystują grupy typu APT.

Ochrona przed nieznanym atakiem za pomocą Microsoft Defender for Endpoint ★★★ / ⚙

Microsoft Defender for Endpoint jest rozwiązaniem chroniącym urządzenie końcowe pracownika typu PC/Mac/smartfon/tablet oraz systemy serwerowe Windows Server/Linux przed nieznanymi zagrożeniami lub bardzo skomplikowanymi atakami. Najważniejsze w tym rozwiązaniu jest to, że wdrożenie nie wymaga instalacji dodatkowego oprogramowania. W systemach Windows jest dostępny sensor wbudowany w system operacyjny, który należy odpowiednio poinformować, gdzie ma wysyłać logi dla operacyjnego centrum bezpieczeństwa obsługującego dany urząd.

Na poniższym przykładzie zaprezentowano mechanizm prowadzenia dochodzenia w ramach incydentu bezpieczeństwa „Skrypt Powershell spowodował pojawienie się niebezpiecznego pliku na komputerze", w ramach którego analityk ma dostęp do diagramu „Investigation graph". Pojawia się strona z instrukcjami, jak propagowało się zagrożenie w organizacji, które maszyny lub użytkownicy są objęci, jakie zagrożenia zostały znalezione (przykładowe infekcje plików), oraz jakie akcje naprawcze zostały wykonane.



Główne zalety wykorzystania mechanizmu ochrony stacji Microsoft Defender for Endpoint:

- monitorowanie wszelkich zdarzeń na urządzeniu w czasie niemal rzeczywistym i ich analiza w oparciu o modele uczenia maszynowego. Microsoft Security Graph pozwala na poinformowanie o nowych zagrożeniach, które pojawiły się w innych częściach globu.
- usługa jest wbudowana w Windows 10 oraz w Windows Server 2019, co skutkuje brakiem potrzeby instalacji oddzielnego oprogramowania.
- wbudowane mechanizmy odpowiedzi na zagrożenia umożliwiają szybkie przywrócenie (*remediation*) urządzenia do zdrowia po ataku, który nie został zatrzymany przez rozwiązania klasy *Endpoint Protection*.
- zbudowany w oparciu o technologie chmurowe Microsoft Defender for Endpoint może skalować się ponad milion końcówek dla pojedynczej organizacji
- *Threat Hunting* – Microsoft Defender for Endpoint umożliwia zespołom bezpieczeństwa wyszukiwania zagrożeń w obrębie danych przechowywanych przez sześć miesięcy
- raporty *Threat Analytics* umożliwiają organizacji szybkie zrozumienie nowych globalnych zagrożeń
- wbudowana ocena i nadawanie priorytetów podatnościom aplikacji wykrytym na podstawie systemu klasyfikacji podatności CVE organizacji MITRE.
- Dodatkowa ochrona oparta o blokowaniu dostępu do odpowiednich klasyfikacji witryn WWW

Zarządzanie podatnościami za pomocą Microsoft Defender for Endpoint ★★★ / ✪✪

Moduł Microsoft Defender for Endpoint o nazwie Threat & Vulnerability Management (TVM) pozwala na wykorzystanie pobranych z punktów końcowych informacji o zainstalowanym oprogramowaniu do określenia istniejących w nich podatności. W tym celu TVM korzysta z bazy CVE. Wynik stanowią rekomendacje dotyczące konieczności zainstalowania poprawek, nowszej wersji oprogramowania czy modyfikacji ustawień. TVM wspiera zarówno produkty Microsoft jak i firm trzecich.

Name	Vendor	Installed versio...	Weaknesses	Threats	Product Code (CPE)	Tags
Windows 10	Microsoft	10.0.19043.1288	142		microsoft:windows_10:10.0.1...	
Firefox	Mozilla	92.0.0.0	58		mozilla:firefox:92.0.0.0	
Office	Microsoft	16.0.14729.20260	5		microsoft:office:16.0.14729.2...	
Wireshark	Wireshark	3.4.8.0	18		wireshark:wireshark:3.4.8.0	
.net Framework	Microsoft	4.8.0.0	1		microsoft:.net_framework:4.8...	
Pdf Reader	Foxit	11.1.0.52543	2		foxit:pdf_reader:11.1.0.52543	
Npcap	Nmap	1.55.0.0	0		nmap:npcap:1.55.0.0	
Nmap	Nmap	7.92.0.0	0		nmap:nmap:7.92.0.0	
Edge Webview2 Runtime	Microsoft	98.0.1108.50	0		microsoft:edge_webview2_ru...	
Edge Chromium-based	Microsoft	98.0.1108.55	0		microsoft:edge_chromium-b...	
Chrome	Google	98.0.4758.102	0		google:chrome:98.0.4758.102	
Postman	Postman	9.14.0.0	0		postman:postman:9.14.0.0	
.net Framework	Microsoft	4.0.0.0	0		microsoft:.net_framework:4.0...	

W przypadku systemu operacyjnego TVM jest tak także w stanie zidentyfikować brak rekomendowanych konfiguracji czy włączonych funkcjonalności z zakresu bezpieczeństwa i zasugerować zmiany. Rekomendacje dotyczące podatności i konfiguracji biorą pod uwagę wiele czynników (nie tylko takich jak powaga podatności czy ilość urządzeń, której dotyczy, ale także to, czy na punkcie końcowym są np. dokumenty objęte wysoką klasyfikacją) i w odpowiedni sposób priorytetyzuje punkty końcowe, którymi należy się zająć w pierwszej kolejności.

Security recommendation	Weaknesses	Related component	Threats	Remediation type
Update Foxit Pdf Reader	2	Foxit Pdf Reader		Software update
Update Microsoft .net Framework	1	Microsoft .net Framework		Software update
Update Microsoft Office	5	Microsoft Office		Software update
Update Microsoft Windows 10 (OS and built-in applications)	142	Microsoft Windows 10		Software update
Update Mozilla Firefox to version 97.0.1.0	58	Mozilla Firefox		Software update
Update Wireshark	18	Wireshark		Software update
Enable Automatic Updates	1	Application (Microsoft Office)		Configuration change
Enable 'Hide Option to Enable or Disable Updates'	1	Application (Microsoft Office)		Configuration change
Disable 'Continue running background apps when Google Chrome is closed'	1	Application (Google Chrome)		Configuration change

TVM jest systemem opierającym się na kliencie, stąd w wykrywaniu podatności nie ma potrzeby wykorzystywania skanów sieciowych, które w przypadku braku dostępu do sieci organizacji mogą być niemożliwe do przeprowadzenia.

8. Ochrona informacji

Informacje powinny być chronione bez względu na to, czy znajdują się na firmowym serwerze plikowym, w usłudze chmurowej, czy na komputerze użytkownika w domu. Ochronę taką może zapewnić szyfrowanie oraz zarządzie prawami dostępu (*Right Management Services*). W przypadku dużej ilości przetwarzanych informacji niezwykle ważne jest zagwarantowanie automatyzacji procesu ochrony i włączanie jej w oparciu o słowa klucze lub wyrażenia regularne, co z jednej strony zapewni odpowiednią ochronę, a z drugiej ułatwi pracę użytkownikowi końcowemu, który nie będzie musiał za każdym razem sprawdzać, czy nadał informacji właściwą etykietę/klauzulę.

Aby wiedzieć, jak i jakie informacje chronić, najpierw należy je odpowiednio sklasyfikować. Etykiety klasyfikacyjne, opcjonalnie połączone z szyfrowaniem, w łatwy sposób pozwolą na rozpoznawanie typu informacji oraz zagwarantują jej odpowiednie przetwarzanie w systemach.

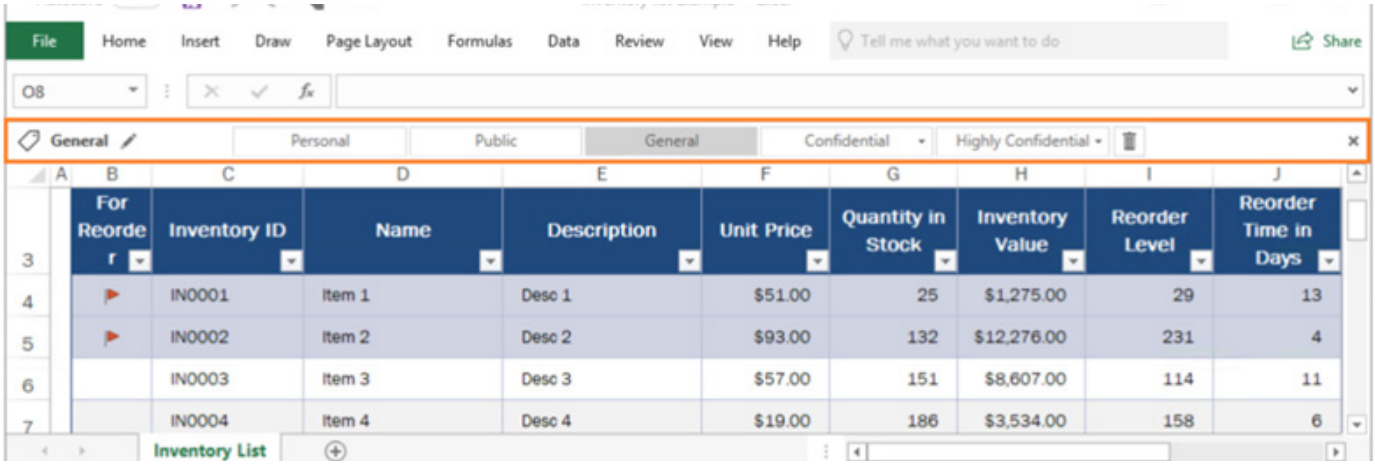
Etykietowanie informacji kontrolowanych/wrażliwych i szyfrowanie za pomocą Azure Information Protection ★★★ / ✪✪✪

Azure Information Protection jest systemem, który pozwala na wdrożenie klasyfikacji i ochrony plików i wiadomości e-mail. Klasyfikacja odbywa się na poziomie plików dokumentów oraz wiadomości e-mail. Osoba upoważniona do podpisania dokumentu dokonuje jego klasyfikacji, bądź korzysta z automatycznego systemu klasyfikacji.

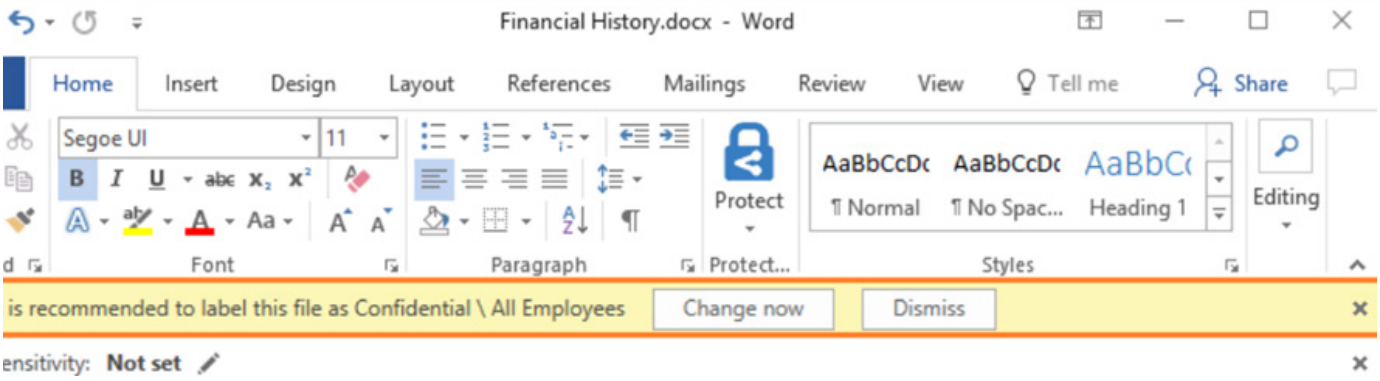
Dodatkowo etykiety, które są nakładane w czystym tekście w ramach metadanych informacji mogą umożliwiać integrację z rozwiązaniem szyfrującym bazującym na usługach Rights Management Services. Zakładając wykorzystanie przykładowej etykiety „Dokument wewnętrzny" na dokumencie PDF, czy MS Word można nałożyć stosowne uprawnienia w szablonie szyfrowania, przykładowo: tylko do wglądu dla danej grupy osób, zakaz drukowania, zakaz przesyłania dalej za pomocą email, zakaz robienia zrzutu ekranu z treścią dokumentu, zakaz kopiowania (Ctr-C/Ctr-V). Dokumenty po nadaniu odpowiedniej klasyfikacji mogą być opatrzone również znakiem wodnym.

W ramach systemu Azure Information Protection możliwe jest również nadanie uprawnienia do dokumentu na zdefiniowany czas i automatyczne odebranie uprawnienia po upływie tego terminu. Możliwy jest również wgląd, kto, z jakiej lokalizacji i kiedy dokument próbował otwierać.

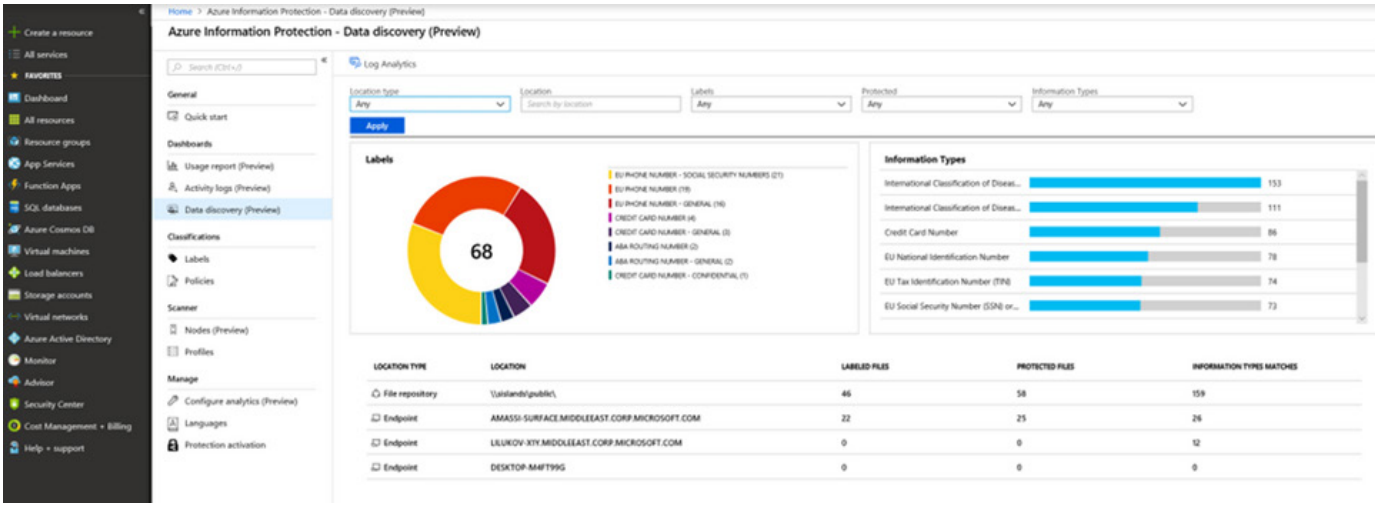
Na poniższym zrzucie ekranowym przedstawiono wykorzystanie belki klasyfikacji dokumentu w ramach arkusza kalkulacyjnego Excel – pracownik wybiera klasyfikację ręcznie:



Przykład poniżej dotyczy zastosowania klasyfikacji „Confidential” w dokumencie Word, gdzie tylko pracownicy danej organizacji mają uprawnienie do odszyfrowania zawartości dokumentu:



Kolejny przykład dotyczy systemu raportowania wykorzystania etykiet w organizacji służącego do inwentaryzacji liczby klasyfikowanych dokumentów i ich lokalizacji:



Możliwości platformy klasyfikacji i ochrony informacji Azure Information Protection:

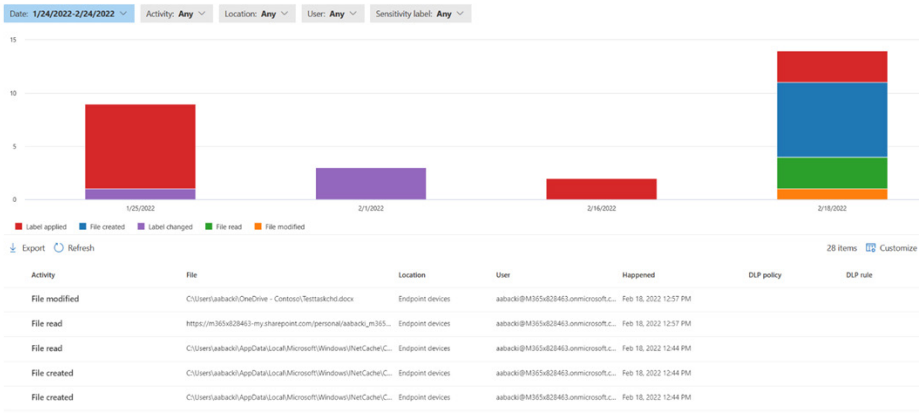
- klasyfikacja informacji oraz i ich ochrony lokalnie i w chmurze przy użyciu *Azure Right Management Services*
- kompatybilność z wieloma typami plików: Microsoft Office, Adobe PDF, pliki CAD, obrazy i wiele innych, również możliwość definiowania nowych formatów chronionych plików
- bezpieczne współdzielenie plików poza organizację także po ich zaszyfrowaniu – możliwość przyznawania dostępu zdalnie
- funkcja pełnej automatyzacji nadawania dokumentom etykiet na podstawie słów kluczowych i wyrażeń regularnych
- współdzielenie etykiet klasyfikujących z systemem Office 365 DLP (*Data Loss Prevention*)
- pełny monitoring wykorzystania etykiet oraz mechanizmów szyfrowania
- elastyczne prawa dostępowe do dokumentów (m.in. tylko do odczytu, zakaz przekazywania dalej, zakaz drukowania i inne)
- integracja z aplikacjami Office i Adobe
- dostępność skanera do automatycznej klasyfikacji dużej ilości plików bez potrzeby działania ze strony użytkownika (np. na serwerach plikowych).

System zapobiegania nieuprawnionemu ujawnianiu informacji - Office 365 Data Loss Prevention (DLP) ★★/ ⚙

To wbudowany w usługi Office 365 mechanizm ochrony plików, wiadomości i chatów dla Exchange Online, SharePoint Online, OneDrive for Business, Microsoft Teams oraz Microsoft Windows 10 (Endpoint DLP), obejmujący:

- wykrywanie informacji na podstawie słów kluczowych i wyrażeń regularnych w obrębie usług Microsoft Office bez potrzeby instalacji jakiejkolwiek infrastruktury – usługa jest wbudowana
- budowanie alertów w oparciu o zdarzenia systemu DLP

- pełny dostęp do raportów i monitoringu
- współdzielenie etykiet klasyfikujących z systemem Azure Information Protection
- wykrywanie wycieku informacji na stacjach klienckich przy próbie udostępniania chronionych danych na dysk USB, zasób sieciowy czy do aplikacji chmurowych



9. Wykrywanie i identyfikacja korzystania przez pracowników z nieautoryzowanych usług chmurowych

Pracownik pracujący z domu lub pracownik mobilny, ze względu na brak wykorzystywania proxy organizacji lub też z uwagi na fakt wykorzystywania własnego urządzenia, może mieć dostęp do aplikacji chmurowych stron trzecich nieuznawanych przez organizację za zaufane.

Pracownicy bardzo często instalują również narzędzia firm trzecich w których przetwarzają informacje firmowe, co niekiedy bywa bardzo trudne do wykrycia.

W przypadku wykorzystywania usankcjonowanych usług chmurowych urząd/organizacja chce i powinna mieć pewność, że dane znajdujące się tam nie zawierają kontrolowanych/chronionych

informacji, które nie powinny być ujawniane poza organizacją. Dodatkowo może zaistnieć potrzeba przeszukania wszystkich tych zasobów pod kątem istnienia na nich jakiejś informacji, np. w przypadku otrzymania wniosku podmiotu danych osobowych o ich usunięcie w ramach RODO.

Wykrywanie nieautoryzowanych usług (Shadow IT) oraz kontrola jakie informacje pracownik publikuje do chmury - Microsoft Defender for Cloud Apps ★★★ / ⚙⚙

Rozwiązanie klasy *Cloud Access Security Broker* jest brokerem zabezpieczeń dostępu w chmurze, który obsługuje różne tryby wdrażania, w tym zbieranie dzienników, łączniki interfejsu API i zwrotny serwer *proxy*. Zapewnia rozbudowaną widoczność, kontrolę nad przepływem danych oraz zaawansowaną analizę, aby identyfikować dane i zapobiegać atakom na nich w usługach chmurowych Microsoft i stron trzecich.

Głowne funkcje Microsoft for Cloud Apps to:

- identyfikacja wykorzystywanych przez użytkowników aplikacji typu PaaS i SaaS
- gotowe do wykorzystania przy podejmowaniu decyzji o zezwoleniu / zablokowaniu danej aplikacji chmurowej raporty dotyczące bezpieczeństwa dla ponad 16000 usług chmurowych wraz z opisem ich zgodności z wieloma standardami. Pozwala to nie tylko na wykrycie tzw. *Shadow IT*, ale także na jego proaktywne blokowanie
- polityki oferujące ochronę danych, *data governance*, monitoring, wykrywanie nietypowego zachowania użytkowników i więcej.
- pełny monitoring wykorzystania usług chmurowych przez użytkowników wraz z raportami dotyczącymi ilości przesyłanych w obie strony danych, adresów IP, nazw urządzeń i loginów oraz plików i więcej.
- alerty i automatyczne działania w przypadku wykrycia nieprawidłowego zachowania
- wymuszanie zgodności z politykami ochrony przed nieuprawnionym ujawnieniem informacji, także w oparciu o etykiety klasyfikacyjne
- integracja z Dostępem Warunkowym Azure AD

- Inspekcja sesji połączenia pozwalająca na wprowadzenie dodatkowych restrykcji (blokowanie np.: kopiowania lub drukowania ze wskazanych aplikacji)
- wsparcie dla szerokiego wachlarza urządzeń brzegowych (proxy/firewall), zarówno fizycznych jak i wirtualnych.

10. Monitorowanie i raportowanie poziomu bezpieczeństwa, nadużyć oraz obsługa incydentów

Wiele organizacji zmaga się z brakiem lub ograniczoną możliwością zintegrowanego zbierania i analizy danych dotyczących poziomu bezpieczeństwa, występowania nadużyć i obsługi incydentów. Skutkuje to niemożnością ujęcia tych informacji w raportach oraz brakiem alertów.

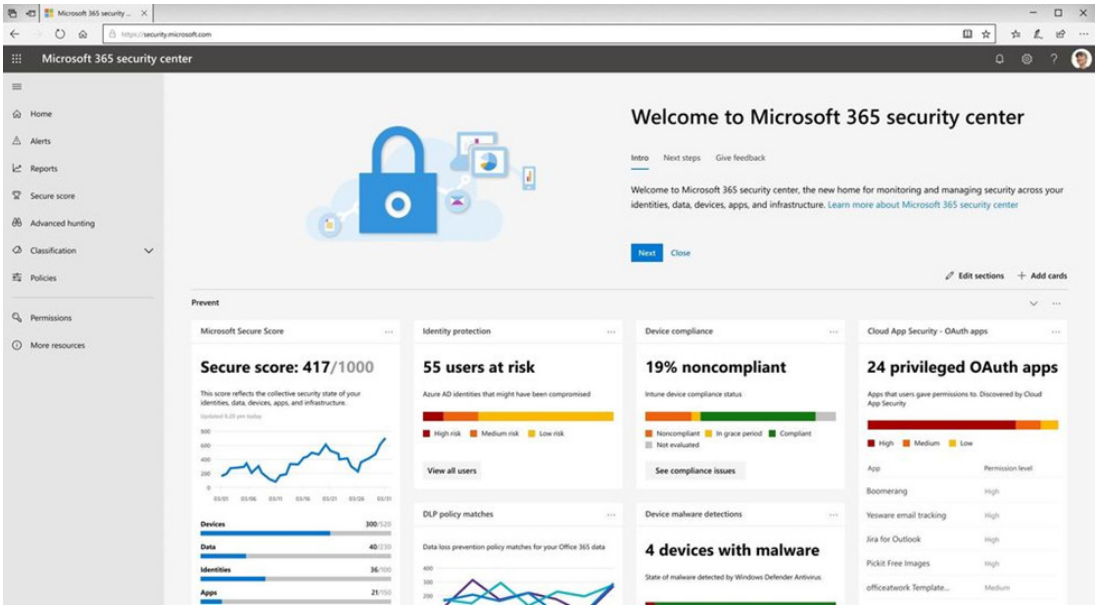
Takie funkcje zostały zintegrowane w pakiecie Microsoft 365. Bogate opcje raportowania i alertów dostarczają informacji niezbędnych dla kontrolowania i monitorowania użytkowników i ich urządzeń lokalnych, zdalnych i mobilnych.

Portale: Microsoft 365 Security oraz Microsoft 365 Compliance ★★★ / ⚙

Zunifikowany dostęp do wszystkich informacji dotyczących bezpieczeństwa i zgodności w ramach usługi Microsoft 365.

Narzędzia pozwalają na dostęp do:

- raportów i alarmów w ramach funkcjonalności usługi Microsoft 365
- łatwy dostęp do ustawień bezpieczeństwa i zgodności usługi Microsoft 365
- rozbudowany system *Role-Based Access Control*, który pozwala na nadawanie odpowiednich uprawnień we wszystkich rozwiązaniach wchodzących w skład pakietu Microsoft 365 – przykładowa prezentacja statystyk bezpieczeństwa poniżej:



Łatwe wykrywanie i wyszukiwanie danych w Office 365 Advanced eDiscovery ★★★ / ⚙

System wyszukiwania informacji w całym środowisku organizacji w oparciu o mechanizmy uczenia maszynowego. Advanced eDiscovery ułatwia znalezienie potrzebnych informacji przy użyciu takich funkcji jak wykrywanie niemal-duplikatów (*near-duplicate detection*) oraz analizę wątków wiadomości poczty elektronicznej.

Podstawowe funkcje bezpieczeństwa realizowane przez w Office 365 Advanced eDiscovery:

- mechanizmy predykcyjne uczenia maszynowego bazujące na oznaczonych przez użytkownika poprawnie odnalezionych dokumentach umożliwiają szybkie pozbycie się duplikatów oraz uporządkowanie informacji w logiczne wątki
- przeszukiwanie w obrębie skrzynek poczty Exchange Online, grup Office 365, Microsoft Teams, zawartości SharePoint Online oraz OneDrive for Business, a także rozmów Skype for Business.
- Wykorzystanie mechanizmów optycznego rozpoznawania znaków (OCR)

- zgodność z *Electronic Discovery Reference Model* (EDRM)
- możliwość eksportu odkrytych informacji
- rozwinięty system kontroli dostępu *Role-Based Access Control*.
- możliwość budowy bazy wiedzy w oparciu o odkryte w środowisku treści
- odkrywanie danych podlegających ochronie w ramach RODO
- wyszukiwanie miejsc w których znajdują się w organizacji dane chronione

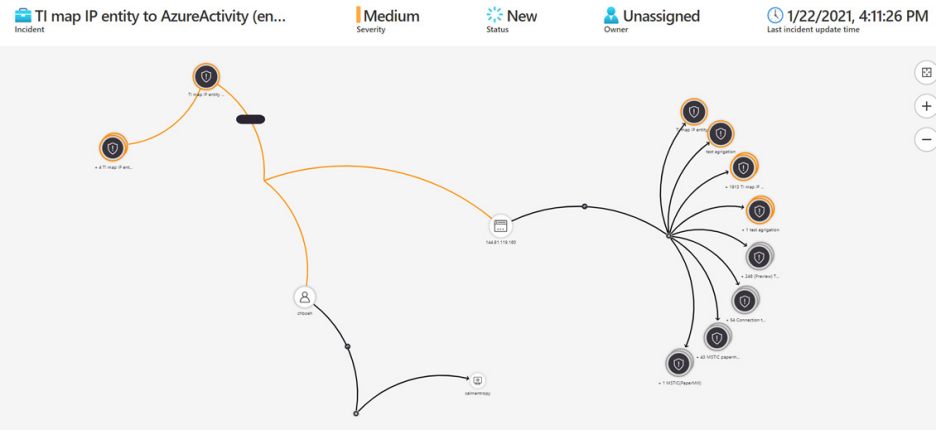
Gromadzenie, analiza i reakcja na incydenty w Microsoft Sentinel ★★★ / ⚙

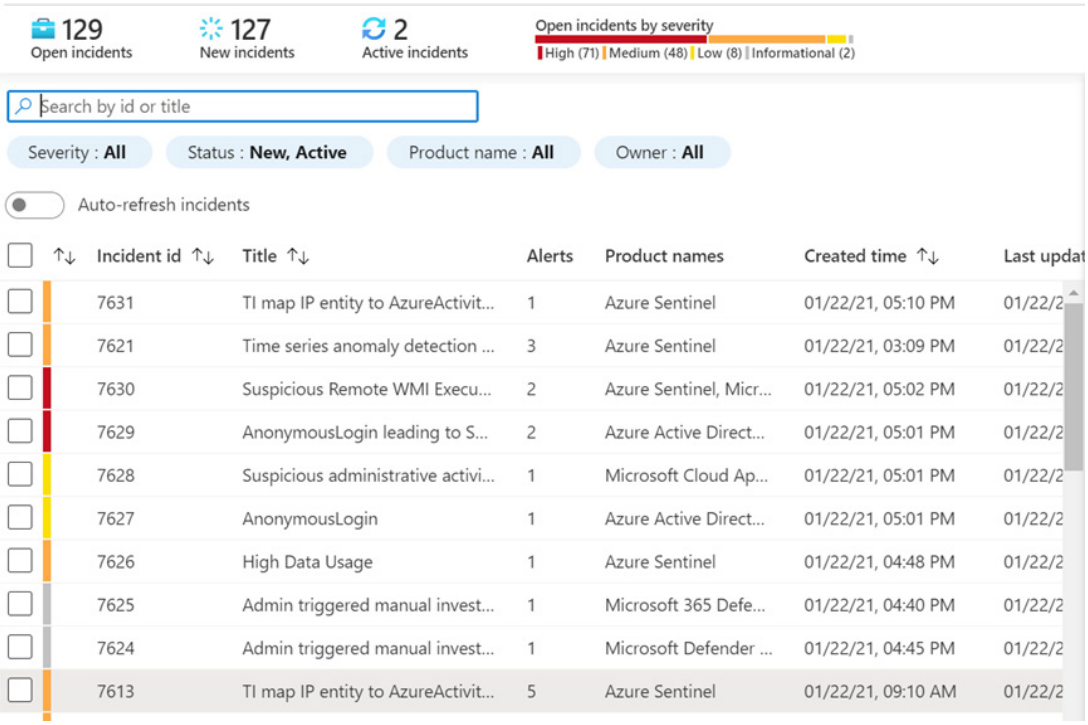
Microsoft Sentinel to rozwiązanie typu SIEM i SOAR zaprojektowane z myślą o zastosowaniu w środowiskach hybrydowych.

Microsoft Sentinel pełni funkcję zapewnienia pojedynczego widoku i spójnej analizy dla wszystkich systemów, usług, użytkowników oraz hostów w chmurze i lokalnych.

Podstawowe funkcje bezpieczeństwa realizowane przez Microsoft Sentinel

- przechowywanie i analiza zdarzeń wszystkich urządzeń, użytkowników, usług i serwerów. Zarówno w chmurze jak i on-premises
- wykorzystanie sztucznej inteligencji do łączenia zdarzeń w celu wykrycia złożonych ataków
- wykorzystanie analizy behawioralnej w celu zbudowania profili zachowań użytkowników, komputerów, adresów IP, aplikacji i dzięki temu umożliwienie wskazania odstępstw od normy
- minimalizowanie fałszywych alarmów
- automatyczne reagowanie na incydenty bezpieczeństwa
- ułatwienie analizy zagrożeń za pomocą automatycznego łączenia zdarzeń z różnych źródeł
- możliwość włączenia do analizy danych taktycznych z wielu źródeł


TI map IP entity to AzureActivity (en...
Incident
Medium
Severity
New
Status
Unassigned
Owner
1/22/2021, 4:11:26 PM
Last incident update time


129
Open incidents
127
New incidents
2
Active incidents
Open incidents by severity
High (71) Medium (48) Low (8) Informational (2)
Search by id or title
Severity : All
Status : New, Active
Product name : All
Owner : All
Auto-refresh incidents
Incident id
Title
Alerts
Product names
Created time
Last updat
7631 TI map IP entity to AzureActivit... 1 Azure Sentinel 01/22/21, 05:10 PM
7621 Time series anomaly detection ... 3 Azure Sentinel 01/22/21, 03:09 PM
7630 Suspicious Remote WMI Execu... 2 Azure Sentinel, Micr... 01/22/21, 05:02 PM
7629 AnonymousLogin leading to S... 2 Azure Active Direct... 01/22/21, 05:01 PM
7628 Suspicious administrative activi... 1 Microsoft Cloud Ap... 01/22/21, 05:01 PM
7627 AnonymousLogin 1 Azure Active Direct... 01/22/21, 05:01 PM
7626 High Data Usage 1 Azure Sentinel 01/22/21, 04:48 PM
7625 Admin triggered manual invest... 1 Microsoft 365 Defe... 01/22/21, 04:40 PM
7624 Admin triggered manual invest... 1 Microsoft Defender ... 01/22/21, 04:45 PM
7613 TI map IP entity to AzureActivit... 5 Azure Sentinel 01/22/21, 09:10 AM

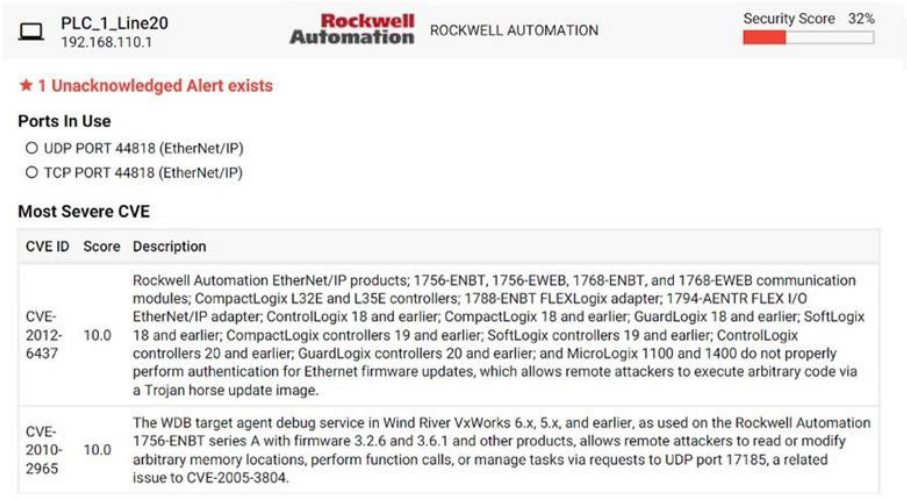
11. Ochrona sieci automatyki przemysłowej (Defender for IoT/OT)

Sieć automatyki przemysłowej to niezwykle wrażliwe środowisko wymagające ochrony i monitorowania pod kątem zagrożeń, ale i tam również możemy wykorzystać ochronę urządzeń stosując podejście oparte na ryzyku.

Co bardzo istotne usługa może funkcjonować w wyizolowanych sieciach bez dostępu do Internetu.

Najważniejsze funkcje związane z identyfikacją zagrożeń dla sieci OT:

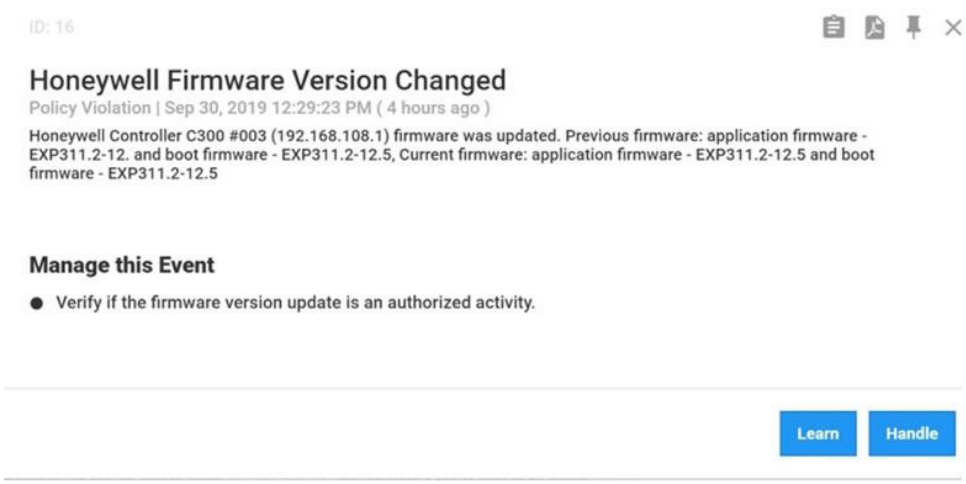
- Proaktywne usuwanie luk w zabezpieczeniach w środowisku IoT/OT na bazie pasywnego monitorowania sieci
- Identyfikacja zagrożeń, takie jak brakujące poprawki, otwarte porty, nieautoryzowane aplikacje i nieautoryzowane połączenia podsieci
- Wykrywanie zmian konfiguracji urządzeń, logiki kontrolera i oprogramowania układowego
- Ustalanie priorytetów poprawek na podstawie oceny ryzyka i automatycznego modelowania zagrożeń, które identyfikuje i wizualizuje najbardziej prawdopodobne ścieżki ataków.



Przykład identyfikacji zagrożeń dla modułu automatyki przemysłowej

W zakresie wykrywania i monitorowania zagrożeń specyficznych dla sieci IOT/OT możliwa jest realizacja przykładowych scenariuszy, które mogą być również korelowane ze środowiskiem IT poprzez wykorzystanie połączenia z usługą Sentinel:

- Monitorowanie pod kątem nietypowych lub nieautoryzowanych działań.
- Wzmocnienie zabezpieczenia usługi IoT/OT z wykorzystaniem taktyki Zero Trust- wykrywanie nieautoryzowanego dostępu zdalnego lub urządzeń z naruszonymi zabezpieczeniami.
- Szybka klasyfikacja alertów w czasie rzeczywistym, badanie ruchu historycznego i wyszukiwanie zagrożeń.
- Przechwytywanie nowoczesnych zagrożeń, takich jak złośliwe oprogramowanie typu luka w zabezpieczeniach 0-day
- Analiza przechwyconych pakietów (PCAP), w celu uzyskania bardziej szczegółowych informacji



Przykładowa identyfikacja nieautoryzowanej zmiany firmware