IMPLEMENTACJA MAPY ATAKÓW W MICROSOFT SENTINEL

Streszczenie

Artykuł prezentuje implementację systemu wizualizacji ataków w czasie rzeczywistym przy użyciu rozwiązań SIEM firmy Azure, ze szczególnym uwzględnieniem usług Microsoft Sentinel i Log Analytics. Nakreśla rosnące zagrożenia cybernetyczne, przed którymi stoją organizacje, oraz kluczową potrzebę szybkiego i skutecznego wykrywania i reagowania na zagrożenia. Oprogramowanie SIEM (Security Information and Event Management) jest podkreślane jako niezbędne do gromadzenia, analizowania i wizualizowania danych z różnych źródeł w celu identyfikacji potencjalnych zagrożeń dla infrastruktury IT. W artykule szczegółowo opisano system zbierania logów z nieudanych prób logowania na wirtualnej maszynie-wabiku, przetwarzanie tych logów za pomocą przestrzeni roboczej Log Analytics i wykorzystanie Microsoft Sentinel do wizualizacji ataków w czasie rzeczywistym. System ten wykorzystuje dane geolokalizacyjne z nieudanych prób logowania poprzez protokół Remote Desktop Protocol (RDP), aby wizualizować ataki na mapie, prezentując wykorzystanie zaawansowanych narzędzi analizy i wizualizacji danych w Azure do wzmacniania obrony cybernetycznej.

1. Wstęp

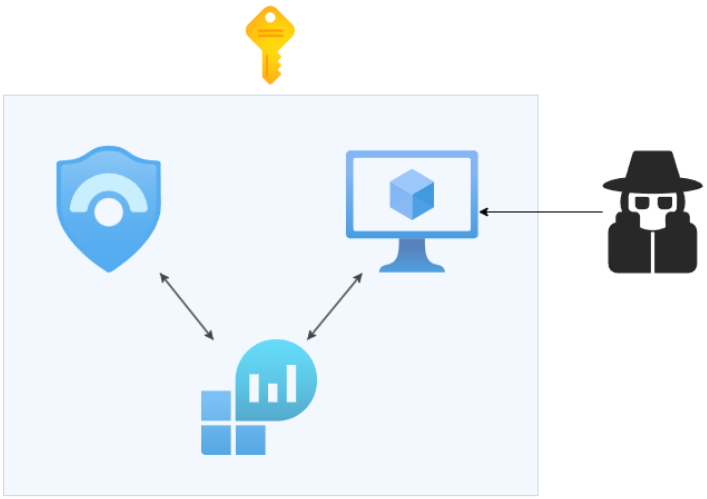
W dzisiejszych czasach, wciąż rozwijający się krajobraz cyberbezpieczeństwa wymusza na organizacjach wdrażanie coraz bardziej zaawansowanych narzędzi i strategii obronnych. Zagrożenia w sieci rosną w tempie niezwykle dynamicznym, a kluczową rolę odgrywa szybka i skuteczna reakcja na ataki oraz zdolność do identyfikacji potencjalnych zagrożeń w możliwie najkrótszym czasie. Naprzeciw tym wymaganiom wychodzą rozwiązania typu SIEM (ang. Security Information and Event Management). SIEM to rodzaj oprogramowania służącego do zarządzania informacjami i zdarzeniami związanych z bezpieczeństwem IT. Systemy te umożliwiają gromadzenie, analizę i wizualizację danych z różnych źródeł w celu identyfikacji potencjalnych zagrożeń dla infrastruktury informatycznej. Dzięki SIEM organizacje mogą monitorować swoje środowisko w czasie rzeczywistym, reagować na incydenty bezpieczeństwa oraz zapewniać pełną widoczność nad wydarzeniami w sieci.

Wraz z coraz częstszą migracją zasobów informatycznych do chmury, zabezpieczanie wirtualnej infrastruktury stało się bardzo istotnym elementem współczesnego cyberbezpieczeństwa. Dostawcy usług chmurowych udostępniają na swoich platformach dedykowane narzędzia do monitorowana środowiska i wykrywania cyberzagrożeń.

Przedstawiona w artykule wizualizacji ataków w czasie rzeczywistym bazuje na dostępnych na platformie Azure narzędziach takich jak Microsoft Sentinel czy Log Analytics.

2. Koncepcja systemu

Na zaimplementowany system składa się kilka komponentów wewnątrz jednej subskrypcji na platformie Azure. Na maszynie wirtualnej zbierane są logi o nieudanych próbach zalogowania, które następnie przyjmowane są przez Log Analytics Workspace i wykorzystywane przez Microsoft Sentinel do tworzenia i aktualizowania wizualizacji ataków w czasie rzeczywistym. System ten opiera się na poniższym schemacie.



Rys. 1. Schemat systemu

3. Maszyna wirtualna

Maszyna wirtualna (ang. Virtual Machine) to emulowane środowisko komputerowe działające jako niezależna instancja na fizycznym sprzęcie komputerowym. W ramach jednego fizycznego serwera lub komputera, maszyny wirtualne mogą być uruchamiane i działać jako oddzielne systemy operacyjne, z własnymi zasobami, jak procesor, pamięć RAM, dysk twardy itp.

Na potrzeby projektu uruchomiona została podstawowa maszyna wirtualna z systemem Windows 10. Została skonfigurowana w taki sposób, by przyjmowała cały zewnętrzny ruch sieciowy. Po jej uruchomieniu, za pomocą zdalnego pulpitu wyłączony został domyślny firewall systemu Windows. Dzięki temu maszyna wirtualna będzie widoczna w sieci, a więc łatwa do znalezienia i zaatakowania – maszyna odgrywa rolę honeypota (ang. wabika).

W środowisku PowerShell ISE został uruchomiony skrypt mający na celu wyklarowanie logów zawierających nieudane próby logowania za pośrednictwem protokołu RDP. Główną częścią skryptu jest nieskończona pętla, która co sekundę sprawdza zdarzenia w dzienniku zdarzeń systemu Windows. Jeśli znaleziony zostanie wpis dotyczący nieudanej próby logowania, skrypt pobiera niezbędne informacje, takie jak czas zdarzenia, nazwa hosta docelowego, nazwa użytkownika, adres IP źródłowy itp. Następnie na podstawie źródłowego adresu IP, za pomocą API ipgeolocation.io uzyskiwane są dane geolokalizacyjne - szerokość i długość geograficzna, państwo oraz region. Finalnie skrypt zapisuje wszystkie zebrane informacje do specjalnego pliku dziennika zdarzeń stworzonego na potrzeby projektu.

4. Log Analytics Workspace

Log Analytics Workspace to usługa dostępna w platformie Azure, która umożliwia zbieranie, analizowanie i wizualizowanie danych logów z różnych źródeł. Jest to centralne miejsce, w którym można gromadzić logi z aplikacji, systemów operacyjnych, urządzeń sieciowych i innych źródeł, aby uzyskać kompleksowy wgląd w działanie infrastruktury IT.

Aby przechwycić logi generowane na maszynie wirtualnej niezbędne było wykorzystanie właśnie tego narzędzia. Na podstawie tworzonego na maszynie specjalnego pliku dziennika zdarzeń został stworzony obszar roboczy usługi Log Analytics. By tworzyć zapytania dzienników na platformie Azure wykorzystywany jest język Kusto (KQL) - język zapytań stworzony specjalnie dla platformy Azure Data Explorer oraz Log Analytics Workspace, swoją składnią przypominający klasycznego SQL. Zostało w nim napisane specjalne query (ang. zapytanie) na potrzeby projektu, widoczne poniżej:

```
FAILED_RDP_WITH_GEO_CL
| extend Latitude = todouble(extract(@"latitude:(\d+\.\d+)", 1, RawData)),
         Longitude = todouble(extract(@"longitude:(\d+\.\d+)", 1, RawData)),
         DestinationHost = extract(@"destinationhost:(.*?),", 1, RawData),
         Username = extract(@"username:(.*?),", 1, RawData),
         SourceHost = extract(@"sourcehost:(.*?),", 1, RawData),
         State = extract(@"state:(.*?),", 1, RawData),
         Country = extract(@"country:(.*?),", 1, RawData),
         Label = extract(@"label:(.*?),", 1, RawData),
         Timestamp = todatetime(extract(@"timestamp:(.*?),", 1, RawData))
```

Rys. 2. Zapytanie w języku KQL

Po wykonaniu zapytania otrzymujemy wynik w postaci logów z przystępnie spreparowanymi polami danych: znacznik czasowy, szerokość i długość geograficzną, hosta docelowego, nazwę użytkownika, którą próbowano się zalogować, numer IP hosta źródłowego, oraz nazwa kraju. Dodatkowo, generowany jest znacznik 'Label' zawierający informację o kraju, z którego próbowano włamać się na maszynę, jak również adres IP, z którego próbowano tego dokonać.

Results | Chart

TimeGenerated [UTC]	Latitude	Longitude	DestinationHost	Username	SourceHost	State	Country	Label
2/25/2024, 6:21:34.579 PM	37.55886	126.99989	honeypot-vm	ADMINISTRATOR	87.251.75.145	Seoul	South Korea	South Korea - 87.251.75.145

Rys. 3. Przykładowy log po wykonaniu zapytania

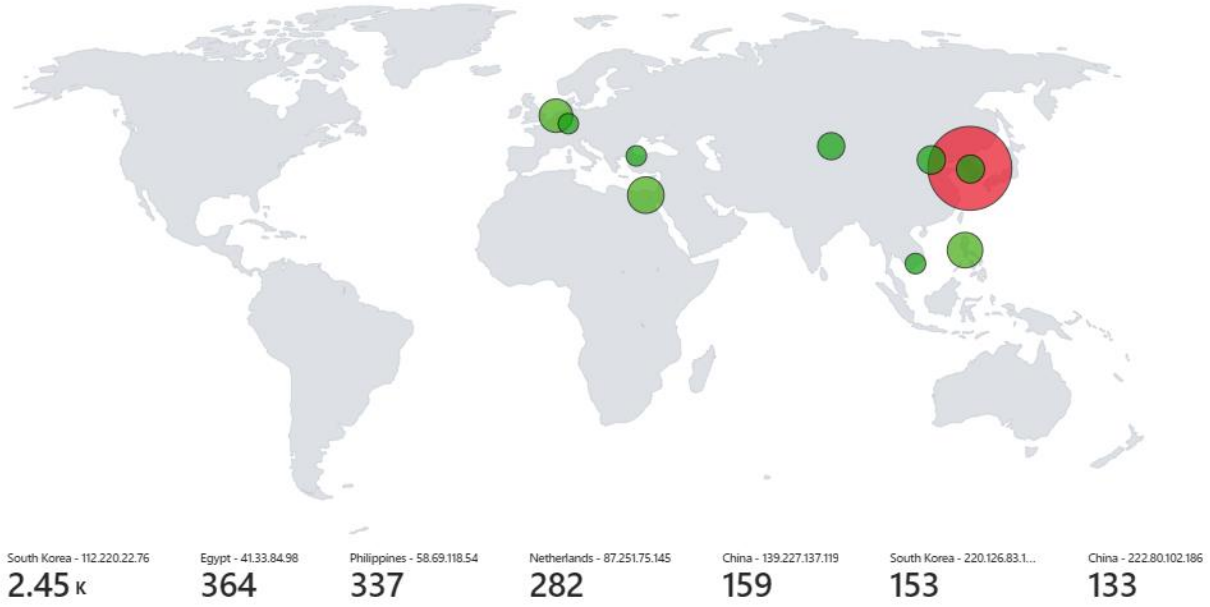
Przygotowane w ten sposób logi posłużą za wsad do systemu SIEM i umożliwią ich łatwą i przejrzystą wizualizację w postaci mapy.

5. Microsoft Sentinel

Microsoft Sentinel (dawniej Azure Sentinel) to platforma usługowa typu SIEM (Security Information and Event Management), rozwijana przez firmę Microsoft, która umożliwia monitorowanie, analizę i reakcję na zagrożenia w infrastrukturze IT. Dzięki zaawansowanym mechanizmom analizy danych, w tym sztucznej inteligencji i uczeniu maszynowemu, Sentinel pozwala szybko identyfikować nietypowe zachowania i wykrywać potencjalne zagrożenia dla bezpieczeństwa. Integruje się także z innymi produktami i usługami Microsoft, co umożliwia kompleksowe zarządzanie bezpieczeństwem w różnych środowiskach, w tym w chmurze i on-premises.

Usługa ta udostępnia użytkownikowi Skoroszyty Sentinel (ang. Sentinel Workbooks), czuli interaktywne i konfigurowalne narzędzia do wizualizacji danych, które umożliwiają użytkownikom tworzenie, analizowanie i udostępnianie szczegółowych informacji na podstawie danych zabezpieczeń zebranych przez usługę Microsoft Sentinel. Skoroszyty zapewniają przyjazny dla użytkownika interfejs do eksplorowania danych związanych z bezpieczeństwem za pomocą różnych wykresów, tabel i innych elementów wizualnych.

Na potrzeby niniejszego projektu został utworzony skoroszyt „Failed RDP Map", który wizualizuje pozyskane dane za pomocą mapy.



Rys. 4. Wizualizacja w postaci mapy ataków

Mapa jako jedna z dostępnych w usłudze opcji wizualizacji danych, prezentuje wszystkie kontynenty i może być w łatwy sposób skonfigurowana tak, by ukazywała informacje pożądane przez użytkownika. W tym przypadku, na podstawie parametrów „Latitude" oraz „ Longitude" wskazywane są miejsca na mapie, z których próbowano włamać się na maszynę-wabik. Widoczne okręgi są tym większe, im więcej żądań pochodzących z konkretnej lokalizacji zostało zaobserwowanych na maszynie. Został wykorzystany motyw kolorystyczny „Green to Red", który dodatkowo informuje o względnej liczbie żądań - gradient od zielonego do czerwonego wraz ze wzrostem liczby prób zalogowania. Mapa ta aktualizowana jest co minutę, by odczytywane z maszyny dzienniki zdarzeń były możliwie szybko analizowane i przetwarzane. W ten sposób uzyskano możliwość monitorowania maszyny w czasie rzeczywistym.

6. Podsumowanie

Dzięki narzędziom i usługą dostarczonym przez firmę Microsoft na platformie Azure, mamy możliwość budowania w wygodny i efektywny sposób złożonych systemów przetwarzania i wizualizacji danych. Implementacja mapy ataków w Azure Sentinel pokazuje, jak za pomocą dostępnych narzędzi można w prosty sposób zebrać, przetworzyć i zwizualizować dane dotyczące prób nieautoryzowanego dostępu do infrastruktury IT. Wykorzystanie maszyny wirtualnej w charakterze honeypota do zbierania logów, Log Analytics Workspace do ich analizy, a następnie Microsoft Sentinel do prezentacji danych na interaktywnej mapie, dowodzi elastyczności i mocy obliczeniowej, jaką oferuje chmura Azure. Projekt ten nie tylko zwiększa świadomość zagrożeń cybernetycznych, ale również demonstruje, jak można wykorzystać dostępne narzędzia do stworzenia kompleksowego systemu bezpieczeństwa IT. Realizacja takiego projektu na platformie Azure umożliwia szybką reakcję na zagrożenia oraz efektywne zarządzanie bezpieczeństwem danych i infrastruktury, co jest kluczowe w dzisiejszym, dynamicznie zmieniającym się świecie cyberbezpieczeństwa. Azure Sentinel, z jego zaawansowanymi funkcjami analitycznymi i możliwościami predykcyjnymi, staje się niezbędnym elementem w strategii obronnych, pozwalającym nie tylko na obronę przed aktualnymi, ale i przewidywanie przyszłych zagrożeń.

Literatura

1. Oficjalna dokumentacja firmy Microsoft https://learn.microsoft.com/en-us/azure/?product=popular

Abstract

The article presents an implementation of a real-time attack visualization system using Azure's SIEM solutions, specifically focusing on Microsoft Sentinel and Log Analytics. It outlines the escalating cyber threats organizations face and the crucial need for rapid and effective threat detection and response capabilities. SIEM (Security Information and Event Management) software is highlighted as essential for gathering, analyzing, and visualizing data from various sources to identify potential IT infrastructure threats. The paper details the setup within an Azure subscription, including the collection of logs from unsuccessful login attempts on a honeypot virtual machine, processing these logs through Log Analytics Workspace, and using Microsoft Sentinel for real-time attack visualization. This system leverages geolocation data from failed Remote Desktop Protocol (RDP) login attempts to visualize attacks on a map, showcasing the use of advanced data analysis and visualization tools in Azure to enhance cybersecurity defenses.