Jak zabezpieczać swoje środowiska przy pracy zdalnej?

W obecnym czasie, kiedy zmuszeni jesteśmy do pracy zdalnej nie możemy zapominać o bezpieczeństwie. Wykorzystując narzędzia z platformy Microsoft Azure możemy uruchomić zbieranie oraz analizowanie logów pochodzących z różnych systemów również z komputerów domowych (Bring Your Own Device - BYOD). Poniżej zestawienie narzędzi, które mogą pomóc w poprawie bezpieczeństwa.

Azure Monitor

Azure Monitor składa się z kilku komponentów, główne komponenty to:

- Application Insights – zbieranie oraz analizowanie danych telemetrycznych z aplikacji
- Log Analytics – zbieranie oraz analizowanie logów jak również danych wydajnościowych z systemów operacyjnych Windows/Linux.

Rozwiązanie Azure Monitor nie wymaga tworzenia żadnej infrastruktury po stronie klienta, usługa działa w pełni w MS Azure. Po stronie klienta wymagane jest zainstalowanie agenta który będzie realizował wysyłkę logów. Azure Monitor Log Analytics posiada bardzo dużo wbudowanych gotowych paczek rozwiązań które po dodaniu zaczynają zbierać oraz analizować logi.

Wiećej informacji o produkcie można znaleźć na stronach:

https://docs.microsoft.com/en-us/azure/azure-monitor/

https://docs.microsoft.com/en-us/azure/azure-monitor/insights/solutions-inventory

https://docs.microsoft.com/en-us/azure/azure-monitor/app/app-insights-overview

https://azure.microsoft.com/en-us/pricing/details/monitor/

Azure Security Center

Usługa Azure Security Center to ujednolicony system zarządzania bezpieczeństwem infrastruktury. Ma on za zadanie zwiększenie poziomu bezpieczeństwa centrów danych i zapewnienie zaawansowanej ochrony przed zagrożeniami w przypadku rozwiązań hybrydowych w chmurze (zarówno na platformie Azure, jak i poza nią) oraz w środowisku lokalnym.

Jedną z możliwości Azure Security Center jest ochrona maszyny lokalnej przed zagrożeniami “Threat protection”. Warto przejrzeć listę alertów które Azure Security Center jest w stanie wykryć, lista alertów dostępna pod tym adresem https://docs.microsoft.com/en-us/azure/security-center/alerts-reference

Więcej informacji na temat Azure Security Center można znaleźć na stronach:

https://docs.microsoft.com/en-us/azure/security-center/security-center-intro

https://docs.microsoft.com/en-us/azure/security-center/threat-protection

https://docs.microsoft.com/en-us/azure/security-center/alerts-reference

https://azure.microsoft.com/en-us/pricing/details/security-center/

Azure Sentinel

Azure Sentinel jest w pełni chmurowym rozwiązaniem klasy SIEM oraz SOAR. Azure Sentinel dostarcza inteligentne rozwiązanie w zakresie zabezpieczeń i analizy zagrożeń w całym przedsiębiorstwie, zapewniając jedno rozwiązanie do wykrywania alertów, zagrożeń oraz aktywnego polowania i reagowania na zagrożenia.

- Zbieraj dane między różnymi użytkownikami, urządzeniami, aplikacjami i infrastrukturą, zarówno on-premises, Azure oraz multi cloud.
- Wykrywaj wcześniej niewykryte zagrożenia.
- Inwestyguj zagrożenia przy użyciu sztucznej inteligencji.
- Reaguj na zagrożenia szybko - dzięki wbudowanym systemom integracyjnym bazującym na architekturze event-driven.

Aby w pełni wykorzystać możliwości usługi Azure Sentinel warto odwiedzić Azure Sentinel Community: https://github.com/Azure/Azure-Sentinel

Więcej informacji na temat Azure Sentinel można znaleść na stronach:

https://docs.microsoft.com/en-gb/azure/sentinel/

https://docs.microsoft.com/en-gb/azure/sentinel/quickstart-get-visibility

https://azure.microsoft.com/en-us/pricing/details/azure-sentinel/

Azure DevOps

Azure DevOps dostarcza pełne wsparcie zespołów zarówno po stronie planowania pracy, jak i zarządzania kodem (aplikacji czy infrastruktury) oraz budowaniu i wdrażaniu rozwiązań w czasie rzeczywistym. Usługa ta działa w chmurze, ale również jest możliwość uruchomienia jej lokalnie, na własnym serwerze.

W ramach Azure DevOps można skorzystać m.in. z następujących usług:

- Azure Boards – jest to pakiet narzędzi do planowania i śledzenia pracy zespołów projektowych
- Azre Repos – repozytorium kodu zarówno aplikacji, jak i infradtruktury dla modelu IaaS
- Azure Pipelines – zapewnia pełne wsparcie dla procesów budowania i wdrażania rozwiązania w sposób ciągły i automatyczny (tzw. CI/CD)
- Azure Test Plans – wsparcie procesów testowania dostarczanego rozwiązania
- Azure Artifacts - umożliwia zespołom udostępnianie pakietów Maven, NPM i NuGet ze źródeł publicznych i prywatnych oraz integrację udostępnianych pakietów w Azure Pipelines

Azure DevOps dostarcza również w pełni konfigurowalne pulpity (dashboards), które umożliwiają śledzenie w czasie rzeczywistym postępu prac zarówno po stronie zepsołu, jak i procesów budowania i wdrażania rozwiązań. Dodatkowo mamy możliwość tworzenia dokumentacji projektowej czy procesowej przy wykorzystaniu Wiki oraz integracji Azure DevOps z innymi rozwiązaniami np. **MS Teams**.

Warto podkreślić, że wdrożenie Azure DevOps w organizacji może odbyć się szybko bez konieczności ponoszenia inwestycji. Pierwszych **5 użytkowników** w danej organizacji korzysta z usługi za darmo. Ponadto w każdym miesiącu mamy możliwość hostowania w chmurze jednego Azure Pipelines działającego aż **1800 minut** łącznie.

Więcej informacji można znaleźć na stronach:

https://dev.azure.com

https://azure.microsoft.com/en-us/pricing/details/devops/azure-devops-services/