Nazwa roli	Uprawnienia / dopuszczone operacje	Miejsce przypisania roli	Przeznaczenie roli
chm-netops-reader	Pozwala na przeglądanie w trybie Read Only: ▪ Grup zasobów w ramach przypisanych subskrypcji ▪ Dashboardów Azure dostępnych publicznie (tj. Dashoboard'y w trybie Shared) ▪ Konfiguracji usług sieciowych ▪ Danych monitoringu zebranych w usłudze Log Analytics, do wybranego zakresu tabel, interesującego z perspektywy osoby monitorującej sieć (logi z Network Watcher/Flow Logi, logi z Network Security Group, wybranego logi z Azure Firewall, Private DNZ Zone) ▪ Danych monitoringu zebranych w usłudze Network Watcher ▪ Danych monitoringu zebranych w usłudze Azure Monitor	▪ Rola jest dostępna na poziomie na poziome Root Management Group. ▪ Rola jest przypisana na poziome Root Management Group.	Rola przeznaczona dla zespołu sieciowego, odpowiedzialnego za architekturę sieci w środowisku chmury.
chm-netops-contributor	▪ Pozwala na modyfikację usług sieciowych w ramach wszystkich subskrypcji oraz MG ▪ W subskrypcji z siecią HUB pozwala na budowanie dedykowanych rozwiązań sieciowych (budowa i konfiguracja Network Appliance) ▪ Odpowiada za konfigurację usług Express Route, VPN do środowiska on-premises	▪ Rola jest dostępna na poziomie na poziome Root Management Group. ▪ Rola przypisana na poziomie Root Management Group. Rola może być ew. przypisywana na poziomie wybranych subskrypcji.	Rola przeznaczona dla zespołu sieciowego, odpowiedzialnego za architekturę sieci w środowisku chmury.
chm-secops-audytor	Pozwala na przeglądanie w trybie Read Only: ▪ Konfiguracji wszystkich usług uruchomionych w ramach subskrypcji ▪ Przypisanych uprawnień w ramach ról IAM ▪ Konfiguracji usług: o Azure Active Directory o Security Center o Azure Defender o Security Graph o Azure Policy ▪ Usługa nie pozwala na żadne operacje w ramach usług: o Azure KeyVault o Azure BluePrint o Azure Biling (dostęp do API zawierającego informacje precyzyjne o naliczonych kosztach usługi) o Cost Management	▪ Rola jest dostępna na poziomie na poziome Root Management Group. ▪ Rola jest przypisana na poziome Root Management Group.	▪ Rola przeznaczona dla zespołu wewnętrznego, odpowiedzialnego za audyt konfiguracji środowiska chmury. ▪ Rola nadawana per zgłoszenie na zadany okres do przeprowadzenia prac audytowych.
chm-secops-monitoring-contributor	Rola pozwala na: ▪ Zarządzanie usługą Azure Monitor (bez możliwości skasowania) ▪ Zgłaszanie i zarządzanie zgłoszeniami supportowymi w ramach środowiska Azure ▪ Zarządzanie usługą Log Analytics (bez możliwości skasowania usługi)	▪ Rola jest dostępna na poziomie na poziome Root Management Group. ▪ Rola jest przypisana na poziome Root Management Group.	Rola, przeznaczona dla osób, które będą odpowiadały za konfigurację usług monitoringu (dodanie konektorów, dodanie zapytań, ect) bez możliwości usunięcia czy utworzenia usługi. Rola w praktyce używana przez: ▪ zespół monitoringu

			▪ 2 linię zespołu SOC (pierwsza linia realizowana przez firmę zewnętrzną)
chm-secops-seceng	Rola pozwala na: ▪ Zarządzanie usługą Azure Monitor (bez możliwości skasowania) ▪ Zgłaszanie i zarządzanie zgłoszeniami supportowymi w ramach środowiska Azure ▪ Zarządzanie usługą Log Analytics (bez możliwości skasowania usługi) ▪ Zarządzanie alertami (tworzenie, zmiana, konfiguracja) na poziomie wskazanych usług	▪ Rola jest dostępna na poziomie na poziome Root Management Group. ▪ Rola jest przypisana na poziome Root Management Group.	Rola, przeznaczona dla osób, które będą odpowiadały za konfigurację monitoringu bezpieczeństwa środowiska Azure w wskazanych usługach.
chm-secops-policyadmin	Rola pozwala na przeglądanie w trybie Read-Only: ▪ konfiguracji usług bezpieczeństwa takich jak: Security Center, Azure Monitor, Azure Sentinel, Log Analytics ▪ Polityk i inicjatyw przypisanych na poziomie Management Group Rola pozwala na tworzenie nowych polityk (definicji) i inicjatyw. Rola nie pozwala na kasowanie i edycję polityk, które są przypisane oraz nie pozwala na przypisywanie nowych bądź zmianę przypisania aktualnych polityk.	▪ Rola jest dostępna na poziomie na poziome Root Management Group. ▪ Rola jest przypisana na poziome Root Management Group.	Rola przeznaczona dla osób w zespole bezpieczeństwa, odpowiedzialna za definicję oraz zmiany w zakresie definicji polityk (Azure Policy) oraz Inicjatyw (Azure Policy Initative). Rola nie pozwala na przypisywanie polityk do struktury subskrypcji oraz Management Group.
chm-secops-policyowner	Rola posiada wszystkie uprawnienia roli chm-secops-policyadmin (rola zdefiniowania wyżej) a dodatkowo pozwala na zarządzanie przypisywaniem polityk oraz inicjatwy. Technicznie, rola pozwala również na definiowanie Deny Assigments natomiast wymaga to użycia w środowisku Azure Blueprint.	▪ Rola jest dostępna na poziomie na poziome Root Management Group. ▪ Rola jest przypisana na poziome Root Management Group.	▪ Rola przeznaczona dla osób w zespole bezpieczeństwa, odpowiedzialna za przypisywanie polityk do struktury subskrypcji oraz Management Group.
chm-devops-projecttechnicalowner	Rola dedykowana zespołom developerskim, które w środowiskach nieprodukcyjnych będą odpowiedzialne za utworzenie środowiska infrastruktury pod projekt. Rola pozwala na tworzenie usług w określonych wersjach (tzw. SKU), dopuszczonych do użycia poza usługami takimi jak: ▪ Dowolne usługi sieciowe poza usługami: ▪ Load Balancer ▪ Azure Application Gateway ▪ Network Interface ▪ Oraz możliwością wykonania operacji join do sieci ▪ Usługi monitoringu poza usługą Application Insights dla potrzeb projektu ▪ Usługi bezpieczeństwa (Log Analytics, Sentinel, Defender, Security Center)	▪ Rola jest dostępna na poziomie na poziome Root Management Group. ▪ Rola jest przypisana na poziomie grup zarządzających (Management Group), które agregują subskrypcje dla środowisk nie produkcyjnych. ▪ Rola nie występuje w subskrypcjach TRANSIT, SHARED SERVICES	Rola przeznaczona dla osób per projekt, które odpowiadają za tworzenie środowiska.
chm-devops-vmoperator	▪ Rola odpowiedzialna za utrzymanie maszyn wirtualnych bez możliwość zmian konfiguracji komponentów sieci i bezpieczeństwa.	▪ Rola jest dostępna na poziomie na poziome Root Management Group. ▪ Rola jest przypisywana per	Rola przeznaczona do prac utrzymaniowych w ramach wybranego zestawu usług.

		projekt – na poziomie Resource Group ▪ Rola nie występuje w subskrypcjach TRANSIT, SHARED SERVICES	
chm-devops-dboperator	Rola odpowiedzialna za utrzymanie usług baz danych bez możliwość zmian konfiguracji komponentów sieci i bezpieczeństwa.	▪ Rola jest dostępna na poziomie na poziome Root Management Group. ▪ Rola jest przypisywana per projekt – na poziomie Resource Group ▪ Rola nie występuje w subskrypcjach TRANSIT, SHARED SERVICES	Rola przeznaczona do prac utrzymaniowych w ramach wybranego zestawu usług.
chm-devops-aksoperator	Rola odpowiedzialna za utrzymanie usług AKS bez możliwość zmian konfiguracji komponentów sieci i bezpieczeństwa.	▪ Rola jest dostępna na poziomie na poziome Root Management Group. ▪ Rola jest przypisywana per projekt – na poziomie Resource Group ▪ Rola nie występuje w subskrypcjach TRANSIT, SHARED SERVICES	Rola przeznaczona do prac utrzymaniowych w ramach wybranego zestawu usług.
chm-finops-operator	Rola odpowiedzialna za rozliczanie kosztów w kontekście wszystkich subskrypcji, może zakładać i tworzyć budżety, może tworzyć alerty i akcje na budżetach, nie ma jednak dostępu do usług w trybie wyższym niż Read. Rola ta zostanie zbudowana w oparciu o rolę Cost Management Contributor (https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#cost-management-contributor)	▪ Rola jest dostępna na poziomie na poziome Tenant Root Group.	Rola przeznaczona do rozliczania kosztów środowiska.
chm-devops-imagecontributor	Rola będzie odpowiedzialna za tworzenie, utrzymywanie i rozwijanie obrazów dla maszyn wirtualnych. https://docs.microsoft.com/en-us/azure/virtual-machines/shared-image-galleries Uprawnienia dla tej roli będą oparte o rolę Contributor dla tylko do tych usług, które potrzebne są do budowy obrazu (VM, Sieć, SharedImage Gallery)	▪ Rola jest dostępna na poziomie na poziome Tenant Root Group.	Rola odpowiedzialna za zarządzanie obrazami.
chm-cirt-debugger	Rola pozwala na pracę z usługą Azure Log Analytics i wykonywanie zapytań do usługi w zakresie określonej listy tabel. List tabel, do której rola ma dostęp jest spójna z listą tabel dostępnych dla roli chm-cirt-line1.	▪ Rola jest dostępna na poziomie na poziome Tenant Root Group. ▪ Rola ma wybrane uprawnienia na tabelach w Log Analytics (do ustalenia, które logi mają być dostępne)	Rola przeznaczona do pracy z wybranymi logami środowiska zgromadzonymi w usłudze Log Analytics.

chm-cirt-line1	Rola operatora I zdarzeń incydentów z dostępem do wybranych logów, umożliwiających otwieranie obsługi, prowadzenia analiz. Rola ma dostęp do Azure Sentinel i Log Analytics, ale tylko na poziomie odczytu i analizy (do wybranych tabel). Rola posiada dostęp do Security Center w trybie Read. W ramach roli nie można tworzyć ani kasować zdarzeń oraz incydentów.	▪ Rola jest dostępna na poziomie na poziome Tenant Root Group. ▪ Rola ma wybrane uprawnienia na tabelach w Log Analytics (do ustalenia, które logi mają być dostępne)	Rola odpowiedzialna za pracę pierwszej linii wsparcia.
chm- cirt-line2	Rola operatora II zdarzeń incydentów z dostępem do wszystkich logów, umożliwiających otwieranie obsługi, prowadzenia analiz, zarządzania supresjami, zarządzania watchlist w Sentinel. Rola ma dostęp do usług Log Analytics, Security Center, Security Center. Rola nie może zarządzać regułami automatyzacyjnymi.	▪ Rola jest dostępna na poziomie na poziome Tenant Root Group.	Rola odpowiedzialna za pracę drugiej linii wsparcia.
chm-cirt-line3	Rola operatora III ma wszystkie uprawnienia roli operatora II + zarządzanie pozostałymi funkcjonalnościami Sentinel, rola pozwala również na dodawanie i budowanie operacji SOAR opartych o Logic Apps. Rola ma dostęp do usług Log Analytics, Security Center, Security Center, Azure Policy.	▪ Rola jest dostępna na poziomie na poziome Tenant Root Group.	Rola odpowiedzialna za pracę trzeciej linii wsparcia.
Subscription Owner / Account Owner	Role, które pozwalają na dodawanie subskrypcji / modyfikację kont Azure.	▪ Rola jest dostępna na poziomie Azure AD.	Rola odpowiedzialna za tworzenie subskrypcji i przypisywanie uprawnień.