Geheimenbeheer ServiceNow

De zakelijke uitdaging

Organisaties zijn tegenwoordig afhankelijk van cloudtoepassingen om hun kritieke bedrijfsprocessen te beheren, nieuwe services aan hun eindgebruikers te leveren en hun concurrenten een stap voor te blijven. Cloudoplossingen bieden aanzienlijke voordelen, maar ze brengen ook uitdagingen met zich mee op het gebied van compliance en governance, waaronder de complexiteit van het beheer van digitale referenties (ook wel geheimen genoemd) in een groot aantal toepassingen en bedrijfsclouds.

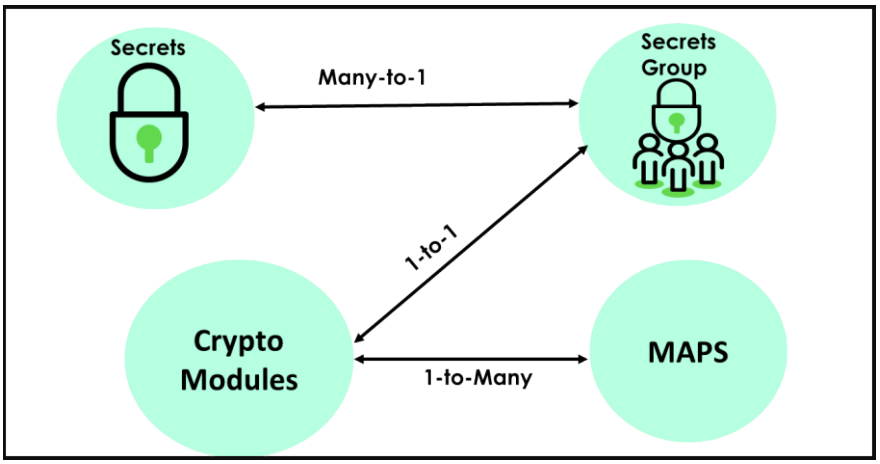
Geheimen worden door gebruikers en machines gebruikt voor verificatie en omvatten zaken als wachtwoorden, versleutelingssleutels, certificaten en tokens. Volgens Cyber Ventures zou het aantal door gebruikers en machines gebruikte wachtwoorden in 2020 meer dan 300 miljard zijn. Het alsmaar groeiende aantal geheimen wordt in veel verschillende contexten gebruikt, waardoor het uiterst moeilijk is ze te traceren en consequent in de onderneming toe te passen.

Organisaties hebben behoefte aan een goed doordachte strategie voor gecentraliseerd beheer van geheimen met krachtige bescherming en toegangscontrole om problemen op het gebied van cyberbeveiliging te voorkomen, zoals ongeoorloofde toegang tot kritieke gegevens en gegevensverlies of -inbreuk.

De ServiceNow-oplossing

Geheimenbeheer van ServiceNow is een centraal beheerde geheimenoplossing en een belangrijk onderdeel van het ServiceNow Vault-aanbod. Het biedt granulair beheer van toegang tot wachtwoorden, digitale certificaten en API-tokens (application programming interface) met behulp van geheime groepen die kunnen worden gedefinieerd om aan de bedrijfsbehoeften van een organisatie te voldoen.

Geheimen worden opgeslagen in een geheime groep, een container die de geheimen versleutelt aan de hand van een gemeenschappelijke sleutel. Een geheime groep kan veel geheimen opslaan en gebruikt cryptografische modules om de versleutelings- en ontsleutelingssleutels voor afzonderlijke geheimen op te slaan. Elke geheime groep wordt gekoppeld aan een enkele cryptografische module.



Afbeelding 1: Geheimenbeheer ServiceNow

Voordelen

Granulaire toegangscontrole voor toegang tot referenties per record

Veilige opslag met innovatieve versleuteling van geheimen aan clientzijde

De onderliggende architectuur verbeteren door organisaties in staat te stellen een granulair toegangsbeleid op PW2-velden te bieden

Compliance: Hardwarebeveiligingsmodules van FIPS 140-2 niveau 3 gebruiken om ervoor te zorgen dat versleutelingssleutels beveiligd worden opgeslagen

Cryptografische modules worden gekoppeld aan een of meer beleidslijnen voor moduletoegang (MAP). Deze MAP's worden toegepast op cryptografische modules en bieden de toegangscontrolemechanismen die bepalen wie toegang krijgt tot een bepaald geheim.

Dashboard voor geheimenbeheer

Organisaties kunnen met behulp van het dashboard voor geheimenbeheer beveiligingsproblemen met betrekking tot hun geheimenbeheer monitoren of de op hun respectievelijke instanties geconfigureerde beveiligingsgroepen bekijken. Met het direct inzetbare dashboard kunnen beheerders snel en eenvoudig informatie analyseren over geconfigureerde geheime groepen, zoals het aantal specifieke geheimen, geheime groepen per type en inactieve beveiligingsgroepen.

Use cases

Veilige ITOM Discovery waarborgen

In afbeelding 2 is een vereenvoudigde referentiearchitectuur te zien van hoe ServiceNow IT Operations Management (ITOM) Discovery door organisaties kan worden ingezet. Zoals in afbeelding 2 te zien is, maken meerdere Windows- en Linux-servers verbinding met de MID Server en maken verschillende MID Server-agenten het voor het detectieproces mogelijk om de CMDB bij te werken. Voor elke MID Server-transactie is een veilige verificatie nodig, waardoor het beheer van de verificatiereferenties vanuit veiligheidsoogpunt van cruciaal belang is.

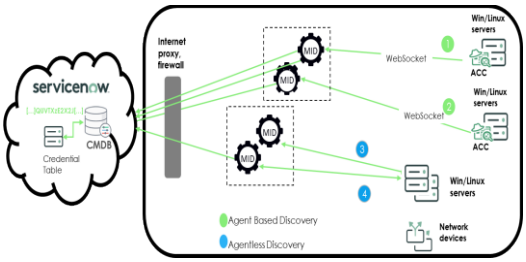
Workflowconnectiviteit veilig versnellen met Integration Hub

Organisaties gebruiken de Integration Hub van ServiceNow om verbinding te maken met verschillende systemen via geautomatiseerde API's (application programming interfaces). Telkens wanneer Integration Hub via een API verbinding maakt met een systeem, is een verificatiereferentie nodig om de verbinding tot stand te brengen. Aangezien organisaties allerlei toepassingen en API's voor connectiviteit beheren, hebben zij een oplossing voor geheimenbeheer nodig.

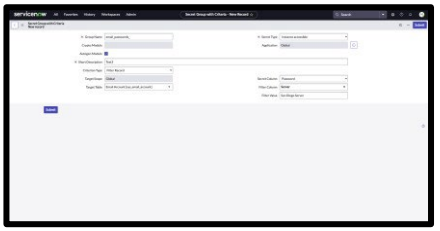
Geheimenbeheer is essentieel voor het waarborgen van de cyberveiligheid van een organisatie. Het omvat alle processen en tools voor het creëren, opslaan, verzenden en beheren van digitale referenties zoals versleutelingssleutels, API-tokens en wachtwoorden. Om geheimen zowel veilig als effectief te beheren, moeten organisaties een kernbeleid voor geheimenbeheer ontwikkelen dat standaardregels en -procedures vaststelt voor alle fasen van de levenscyclus van een geheim. Met geheimenbeheer van ServiceNow kunnen organisaties hun referenties met vertrouwen beveiligen voor alle toepassingen en gebruikers.

Meer informatie:

servicenow.com/nl/products/vault.html



Afbeelding 2: Geheimenbeheer voor ITOM Discovery



Afbeelding 3: Detailpagina geheime groep met criteria

servicenow

SN-DataSheet-Name-01012022