Best practices voor planning van update van beveiligde firewallinhoud

uitgeven

Organisaties die Firewall Threat Defense (FTD)-apparaten beheren met Firewall Management Center (FMC) hebben richtlijnen nodig voor best practices voor het toepassen van beveiligings- en inhoudsupdates. Er bestaat met name onzekerheid over hoe vaak verschillende soorten updates moeten worden toegepast, of updates kunnen worden gepland in plaats van onmiddellijk kunnen worden toegepast en wat de operationele effecten van deze updates zijn. De vraag rijst omdat Cisco regelmatig, soms wekelijks, content updates uitbrengt en beheerders moeten begrijpen of deze onmiddellijk na release moeten worden toegepast of dat ze kunnen worden gepland volgens de organisatieonderhoudsperioden en het wijzigingsbeheerbeleid.

milieu

- Cisco Secure Firewall Firepower, alle versies
- Firepower Management Center, alle versies

resolutie

Deze tabel toont het doel van elk updatetype in Firepower.

Type update	Doel	Opmerkingen
SRU/LSP	Updates van indringingsregels (respectievelijk Snort 2 en Snort 3)	Handhaaft regels voor inbraakdetectie/preventie
GeoDB	Geolocatiegegevens voor IP-adressen	Gebruikt voor op geolocatie gebaseerde

		verkeersfiltering
VDB	Informatie over kwetsbaarheid en vingerafdrukken van host	Gebruikt voor kwetsbaarheidsbeoordeling en risicoanalyse

Cisco Secure Firewall-contentupdates zijn onderverdeeld in drie verschillende typen, elk met verschillende releasefrequenties en aanbevolen planningspraktijken. Deze tabel bevat de aanbevelingen voor het plannen van best practices voor elk type update:

Type update	afgiftefrequentie	Voorgesteld schema	Standaard FMC-schema	Navigatiepad (wijzigen)
SRU/LSP	vaak	dagelijks	dagelijks	Systeem > Inhoudsupdates > Regelupdates
GeoDB	~Wekelijks	wekelijks	wekelijks	Systeem > Inhoudsupdates > Geolocatie-updates
VDB	~Maandelijks	wekelijks	wekelijks	Systeem > Hulpmiddelen: planning > Wekelijkse softwaredownload

Voor optimale beveiligingsconfiguraties en -houding is het de beste praktijk om deze updates toe te passen zodra ze door Cisco worden vrijgegeven. Sommige van deze updatebestanden kunnen vrij groot zijn en bandbreedtetoewijzingen moeten worden overwogen. Het wordt aanbevolen om de grotere updates buiten de piekuren te installeren, als u hetzelfde netwerk gebruikt.

SRU/LSP (Intrusion Rules)-updates

Snort Rule Updates (SRU) en Lightweight Security Packages (LSP) bevatten inbraakdetectie- en preventieregels. Deze updates moeten zo vaak worden toegepast als operationeel haalbaar is om bescherming tegen opkomende bedreigingen te behouden.

U kunt het schema voor de SRU/LSP als volgt wijzigen: Navigeer naar Systeem > Inhoudsupdates > Regelupdates in de FMC-interface om de instellingen voor tijd, datum en frequentie aan te passen.

SRU/LSP-updates ondersteunen geautomatiseerde implementatie en kunnen na het downloaden en installeren automatisch worden geïmplementeerd.

GeoDB (Geolocation Database)-updates

Geolocation Database-updates bieden actuele geografische locatiegegevens voor IP-adressen en worden doorgaans wekelijks vrijgegeven.

U kunt het GeoDB-schema als volgt wijzigen: Navigeer naar Systeem > Inhoudsupdates > Geolocatie-updates in de FMC-interface om de planningparameters aan te passen.

GeoDB-updates kunnen worden gepland voor download en installatie, maar implementatie op beheerde apparaten vereist handmatige push en kan niet volledig worden geautomatiseerd zoals SRU / LSP-updates.

VDB (Vulnerability Database)-updates

Kwetsbaarheid Database-updates worden ongeveer maandelijks uitgebracht en worden beheerd als software-updates in plaats van content-updates.

U kunt het VDB-schema als volgt wijzigen: Navigeer naar Systeem > Extra: Plannen en wijzig de taak Wekelijkse software downloaden om de downloadfrequentie en -timing aan te passen.

VDB-updates vallen onder software-updates en kunnen niet onafhankelijk worden geïmplementeerd. Deze worden meegenomen bij het uitvoeren van handmatige implementaties waarbij alle openstaande wijzigingen worden gecompileerd.

Overwegingen bij implementatie

Bij de implementatie van updates stelt de FMC alle openstaande configuratiewijzigingen samen en kan de FMC meerdere typen inhoudsupdates opnemen in één implementatiebewerking. Sommige updates kunnen leiden tot korte herstart van de Snort-service tijdens de implementatie, waarmee rekening moet worden gehouden bij het plannen van updates tijdens de productie-uren.

Organisaties moeten updateschema's afstemmen op hun wijzigingsbeheerbeleid en overwegen updates te plannen tijdens onderhoudsvensters als korte serviceonderbrekingen een probleem vormen voor hun operationele omgeving.

Oorzaak

Dit was een verzoek om configuratie en operationele richtsnoeren in plaats van een technische storing. De behoefte aan verduidelijking kwam voort uit onzekerheid over de planningspraktijken van updates, automatiseringsmogelijkheden en de operationele impact van verschillende typen inhoudsupdates in Cisco Secure Firewall-omgevingen.

Verwante inhoud

- Beheerdershandleiding Cisco Secure Firewall Management Center, 7.6: Updates
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.