Generazione di metadati arricchiti da SIEM

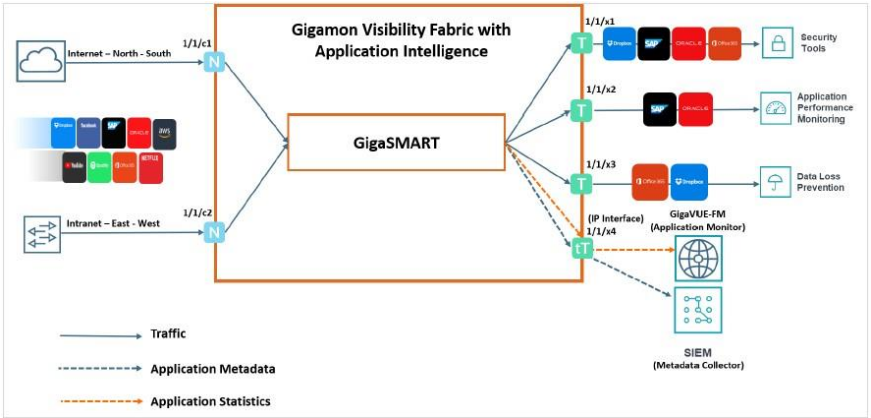
Problema

Gli strumenti di sicurezza e monitoraggio, che di solito sono dimensionati in base alla lunghezza di banda che ricevono e pertanto dispongono di soluzioni di identificazioni dell'applicazione che permettono di filtrare il tipo di traffico che riceverà ogni strumento, sono fondamentali per controllare i costi di distribuzione della propria strategia di visibilità e sicurezza. Però realizzare un filtro binario su ogni applicazione può non essere sufficiente a conformarsi con le proprie politiche di sicurezza, per cui è necessario adottare alcune strategie aggiuntive per inviare informazioni ai tool sufficienti per individuare ciò che sta attraversando la rete, riducendo il più possibile la larghezza di banda che sarà inviata. Di solito si desidera poter generare dati di dati, ossia metadati.
Inoltre è importante avere un meccanismo che permetta di automatizzare questo invio di informazioni, in modo che se per esempio si inviano questi dati a un SIEM si possa comunicare automaticamente la struttura di metadati in corso di trasferimento.
Allo stesso modo il trasferimento di metadati deve essere flessibile e supportare diversi formati che si adattino allo strumento di esportazione che riceverà i dati.

Soluzione

Il modulo di riconoscimento delle applicazioni della scheda Gigasmart Application Filtering Intelligence include un modulo aggiuntivo di generazione di Metadati denominato Application Metadata Intelligence (AMI). Attualmente AMI è in grado di generare più di 5800 campi sulle 3200 applicazioni riconosciute tramite un'interfaccia grafica più intuitiva. I metadati si possono generare sia in formato Netflow sia in formato CEF in modo da adattarli allo strumento che li riceverà. Grazie all'estesa rete di partner che ha Gigamon, disponiamo di integrazioni native con produttori SIEM (Qradar, Slunk) attraverso l'API della piattaforma di gestione Fabric Manager, in modo da potere automatizzare il cambiamento di formato dei metadati inviati.

Schema



Licenza

Application Metadata Intelligence

LINK