

GENERIERUNG VON ANGEREICHERTEN METADATEN FÜR SIEM

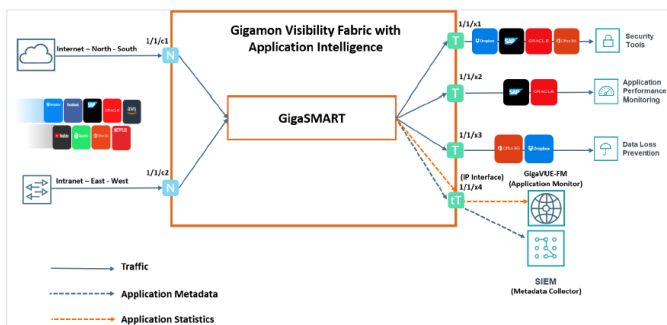
PROBLEM:

Die Sicherheits- und Überwachungstools werden oft nach der Bandbreite dimensioniert, die sie empfangen, daher ist es unerlässlich, über Lösungen zur Identifizierung der Anwendungen zu verfügen, die es uns ermöglichen, zu filtern, welchen Traffic jedes Tool empfängt, um die Bereitstellungskosten unserer Sichtbarkeits- und Sicherheitsstrategie zu kontrollieren. Aber möglicherweise ist es nicht genug, einen binären Filter auf jede Anwendung anzuwenden, um unsere Sicherheitsrichtlinien zu erfüllen, sodass wir eine zusätzliche Strategie benötigen, um Informationen an unsere Tools zu senden, die ausreichen, um zu identifizieren, was im Netzwerk vor sich geht, und gleichzeitig die Bandbreite, die wir versenden, so weit wie möglich zu reduzieren. Üblicherweise wollen wir Daten über Daten, also Metadaten, generieren.

Zudem brauchen wir einen Mechanismus, mit dem wir diesen Informationsversand automatisieren können, damit wir, wenn wir beispielsweise diese Daten an ein SIEM senden, automatisch die Metadatenstruktur, die übertragen wird, kommunizieren können.

Ebenso muss die Übertragung der Metadaten flexibel sein und verschiedene Formate unterstützen, die sich an den Exporter anpassen, der die Daten empfangen wird.

SCHEMA:



GENERIERUNG VON ANGEREICHERTEN METADATEN FÜR SIEM

LÖSUNG:

Das Anwendungserkennungsmodul der GigaSMART-Karte, Application Filtering Intelligence, enthält ein zusätzliches Modul zur Generierung von Metadaten namens Application Metadata Intelligence (AMI). Aktuell kann AMI über eine benutzerfreundliche grafische Benutzeroberfläche mehr als 5.800 Felder über die 3.200 bekannten Anwendungen erstellen.

Die Metadaten können sowohl im Netflow-Format als auch im CEF-Format erstellt werden, um sie an das Tool anzupassen, das sie empfangen soll.

Dank des umfangreichen Partnernetzwerks von Gigamon verfügen wir über native Integrationen mit SIEM-Herstellern (Qradar, Slunk) über die API der Verwaltungsplattform Fabric Manager, sodass wir die Übertragung des Formats der gesendeten Metadaten automatisieren können.

LIZENZEN:

- Application Metadata Intelligence