Cisco Tetration Analytics bringt Transparenz in Anwendungen

Tetration Analytics unterstützt Unternehmen, alle Vorgänge im Rechenzentrum transparent zu machen – Datenpakete, Flows und Geschwindigkeiten bis auf Prozessebene von Applikationen. ISPIN AG ist der erste Schweizer Cisco Partner, der Tetration Analytics Dienstleistungen anbietet. Unter anderem verfügt der Bassersdorfer Security-, Netzwerk- und Datacenter-Spezialist über die europaweit erste mobile Tetration Analytics-Plattform zur Durchführung von lokalen Proof of Concepts bei interessierten Unternehmen.

Cisco Tetration Analytics sammelt Telemetriedaten von Hardware- und Software-Sensoren und untersucht diese mittels moderner Datacenter-Analytic und weitreichendem automatischen Machine Learning. Tetration Analytics ermittelt aufgrund der Analyse der Datenflüsse die Abhängigkeiten von Applikationen und Netzwerkbeziehungen, macht basierend auf diesen Erkenntnissen Vorschläge zur Gestaltung eines Regelwerks (Application Policy Whitelisting) und setzt sie durch automatische Konfiguration der Betriebssysteme, Firewalls und Netzwerkkomponenten durch.

Architektur und Aufbau

Die Tetration-Plattform ist eine integrierte Plattform: Die Server und Switches sind bereits verbunden und die Software vorinstalliert. Die Informationen werden über Host-, VM- oder Hardware-Sensoren gesammelt, welche die Daten an den Cisco Tetration Analytics Cluster weiterleiten. Die Host- und VM-Sensoren werden manuell oder über bestehende Softwareverteilungslösungen auf den Servern installiert. Die Hardwaresensoren sind in den Cisco Nexus 9k Switches der neuesten Generation integriert. Die Plattform wird via ein anpassbares Web-GUI bedient. Cisco bietet jedoch zusätzliche, offene Schnittstellen an, um Tetration Analytics in bestehende Systeme, wie zum Beispiel ein SIEM oder eine Ticketing-Lösung, zu integrieren. Individuelle Analyse-Algorithmen erzeugen je nach Geschäftsanforderungen individuelle Datenexports und Benachrichtigungen in offenen Formaten, welche sich mit externen Lösungen von Drittanbietern weiterverarbeiten lassen: Zur Entwicklung von Anwendungen und Integrationen arbeitet Cisco mit Partnern wie Algosec, Citrix, Dell EMC, F5, Infoblox, Servicenow und Tufin zusammen.

Die Installation und Inbetriebnahme von Tetration Analytics geschieht durch spezialisierte Cisco Partner. ISPIN AG ist in der Schweiz der erste und momentan einzige Partner, der diese Dienstleistungen anbietet.

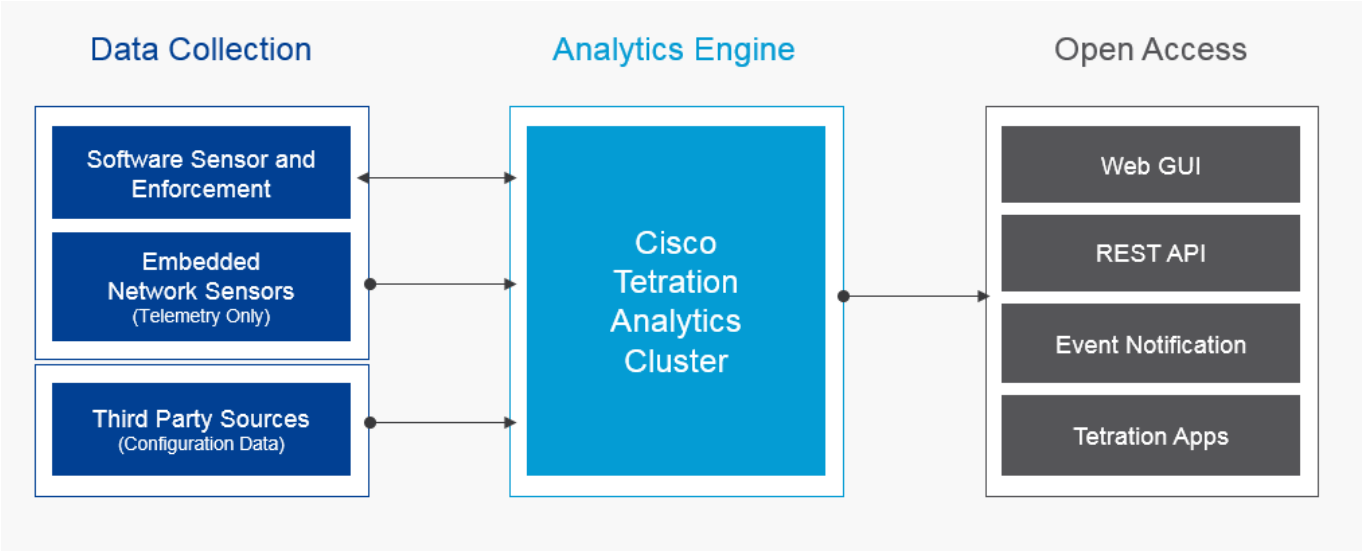

Abb1: Die Tetration Analytics Architektur (Quelle: Cisco)

Anwendungsfälle und Vorteile

Geschäftsanwendungen laufen heute oft auf Hunderten von Servern in einer heterogenen Infrastruktur im Rechenzentrum und in Clouds. Diese Komplexität wird erhöht durch Virtualisierung, mobile Applikationen und sich permanent verändernde Anwendungen aufgrund von DevOps-Modellen und Microservice-Architekturen. Dies stellt die Betreiber von Datacenters vor grosse Herausforderungen bei der Nachvollziehbarkeit der Applikationsbeziehungen und –abhängigkeiten sowie bei der Gewährleistung von Compliance- und Sicherheitsvorgaben.

Mit dem Einsatz von Cisco Tetration Analytics können Unternehmen und Organisationen Folgendes erreichen:

- Verstehen, welche Applikationen im Rechenzentrum und in der Cloud voneinander abhängen (Application Dependency Mapping)
- Das Verhalten von Anwendungen kontinuierlich überwachen, um abweichende Kommunikationsmuster schnell zu identifizieren
- Fundierte Entscheidungen treffen und den Effekt von Richtlinienänderungen prüfen, bevor diese implementiert werden
- Milliarden Datenflüsse in Echtzeit mit Hilfe der Tetration Forensik-Suchmaschine durchsuchen und analysieren
- Konsistente Sicherheitsrichtlinien bei jeder Anwendung durchsetzen, unabhängig von ihrer Ablaufumgebung

Die folgende Grafik aus dem Anwendungsbeispiel „Application Dependency Mapping“ zeigt die Abhängigkeiten zwischen Anwendungen und Infrastrukturelementen. Diese „Landkarte“ kann beispielsweise zur Vorbereitung von Migrationen genützt werden.

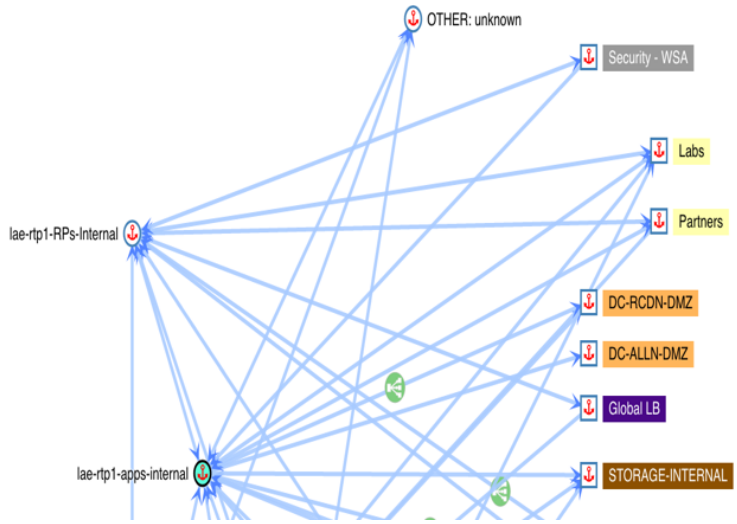

Abb2: Screenshot Tetration Analytics – Application Dependency Mapping

Sicherheit durch Applikationssegmentierung

Tetration Analytics erlaubt es, Workloads durch Applikationssegmentierung zu trennen und erreicht so eine automatische Mikrosegmentierung, unabhängig von der zugrundeliegenden Infrastruktur. Das Cisco-Tool wendet dabei Richtlinien auf jeder Anwendungsebene ortsunabhängig an. Es lässt sich in Firewalls jedes Herstellers integrieren und auf Netzwerkebene orchestrieren. Im Vergleich zu herkömmlichen statischen Lösungen basieren die Richtlinien auf realen Daten der Netzwerkkommunikation und der permanenten Durchführung dynamischer Verhaltensanalysen von Milliarden Flows, Prozessen und Workload-Charakteristiken.

Deployment Modelle und ISPIN-Angebot

Tetration Analytics ist in verschiedenen Versionen verfügbar. Die 39-Rack Unit Plattform unterstützt bis zu 10'000 Workloads, die kleinere 8-Rack Unit bis 1'000 Workloads. Des Weiteren ist eine Cloud-Appliance auf Amazon Web Services (AWS) angekündigt, welche ebenfalls bis 1'000 Workloads unterstützt, jedoch ohne Integration der Nexus 9k Hardwaresensoren.

ISPIN AG bietet mit der ersten in Europa verfügbaren Tetration-8-Rack-Unit ein standardisiertes Proof-of-Concept-Paket an. Das Paket beinhaltet während einer Laufzeit von insgesamt fünf Wochen:

- die Begleitung der Sensorinstallation
- die Integration von Tetration Analytics im Datacenter des Kunden
- die Durchführung des Application Dependency Mapping mit maximal 100 Sensoren
- Application Performance Analysis, Incident- und Anomalie-Analyse einer Applikation
- Policy Export (Whitelist und Micro-Segmentation)

Den Kunden stehen während der gesamten PoC-Phase ISPIN Datacenter Engineers, Datenanalysten und Softwareentwickler zur Verfügung, welche die Ergebnisse sicherstellen und die Vorzüge des Einsatzes von Tetration Analytics vor Ort aufzeigen können.

Falls Sie an einem PoC interessiert sind und mehr über Tetration Analytics erfahren wollen, kontaktieren Sie uns via info@ispin.ch. Und besuchen Sie auch unseren Security WakeUp am 7. Mai 2017 zum Thema „Schaffen Sie Transparenz im Datacenter mit Cisco Tetration Analytics". Anmelden unter marketing@ispin.ch.