Tetration Analytics

Eine von der existierenden Infrastruktur unabhängige Telemetrie- und Analytics-Lösung für das Rechenzentrum, welche auf Basis der Netzwerkkommunikation zwischen Systemen in Echtzeit die bestehende Anwendungslandschaft auf logischer Ebene kartografiert.

Sie erkennt Abhängigkeiten zwischen Anwendungen und ermittelt durch maschinenbasiertes Lernen den „Normalzustand“ der Kommunikation und registriert Abweichungen anhand verschiedener Kriterien. Die ermittelten realen Kommunikationsprofile innerhalb und zwischen Applikationen können automatisiert in Sicherheitsrichtlinien überführt werden, die entweder in bestehende Security-Umgebungen exportiert oder direkt in der Lösung umgesetzt werden.

Aufgrund der Granularität und Umfänglichkeit der Informationserhebung und der Vorhaltung historischer Kommunikationsdaten über mehrere Monate ist Tetration Analytics insbesondere zum Nachweis der Einhaltung von Compliance-Richtlinien (z.B. zur Segmentierung von Applikationen) prädestiniert.

Application Dependency Mapping und Erzeugung von White-List-Policies

Umsetzen von Sicherheitsrichtlinien über Server-Firewall

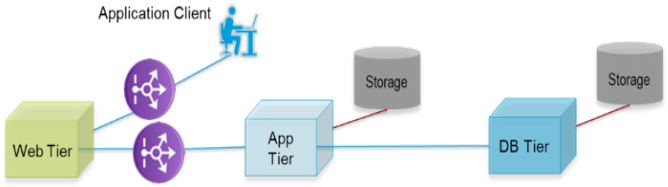
Policy und auditierbare Compliance

Forensik und Troubleshooting - Zeitmaschine für das RZ

Anwendungsfelder

Cisco Tetration Analytics zeichnet in Echtzeit sämtliche Kommunikationsbeziehungen im und zwischen Rechenzentren auf Datenpaket-Ebene auf, analysiert diese und hält sie für bis zu 12 Monate vor. Durch intelligente Maschinenlernverfahren und vorprogrammierte Big-Data-Mechanismen können darauf basierend folgende Auswertungen „out-of-the-box“ durchgeführt werden:

Automatisches Kartografieren aller Applikationsbeziehungen und Abhängigkeiten untereinander.



Automatische Detektierung neuer Endpunkte und maschinengestütze Zuordnung zu existierenden Applikationsclustern.

Abgleich mit Compliance-Vorgaben z.B. zur Separierung von Applikationslandschaften – Nachweisführung im Falle von Auditierungen.

Export der Kommunikationsprofile in Form von maschinell verwertbaren Sicherheitsrichtlinien auf Basis eines White List-Modells („nur erlauben, was tatsächlich benötigt wird”), z.B. zur direkten Einspielung in Firewalls (herstellerunabhängig) oder als „Access Control Lists“ in die Netzwerk-Infrastruktur.

Abgleich des realen Kommunikationsverhaltens mit den existierenden Regelwerken in den Firewalls zur automatischen Ermittlung von ggf. überflüssigen Einträgen.

Vermessung der Abweichung vom „Normalverhalten“ zur gezielten Ermittlung von Anomalien, möglichen Sicherheitsvorfällen und Erstellung von Trendanalysen zur Verminderung der operationellen Risiken.

Durchführen von Simulationen des Kommunikationsverhaltens vor Einführung oder Änderung von Sicherheitsrichtlinien auf Basis von historischen Echtdaten („was-wäre-gewesen-wenn“).

Gezielte Suche nach bestimmtem Kommunikationsverhalten in aktuellen und historischen Kommunikationsdaten.

Umsetzung von Sicherheitsrichtlinien

Darüber hinaus kann Tetration dazu verwendet werden, zentral Kommunikationsrichtlinien vorzugeben und direkt auf den Endpunkten zu „enforcen“ (unter Verwendung der jeweiligen lokalen Host-Firewall). Die Definition der Richtlinien erfolgt dabei über die Eigenschaften („Tags“) der einzelnen Endpunkte und nicht über IP-Adressen und ist daher unabhängig von existierenden Netzwerk-Topologien. Damit wird es möglich, Sicherheitsrichtlinien über alle Rechenzentren, Co-Location-Standorte bis in die Public Cloud konstant zu erzwingen und deren Einhaltung nachzuweisen.

Unabhängigkeit von der existierenden Infrastruktur

Tetration funktioniert völlig unabhängig von der zugrundeliegenden Netzwerk- oder Security-Infrastruktur, da es primär durch Sensoren in den Betriebssystemen gespeist wird. Entsprechende Software ist für Windows Server, die gängigen Linux-Server-Distributionen sowie für AIX und Solaris-Systeme verfügbar.

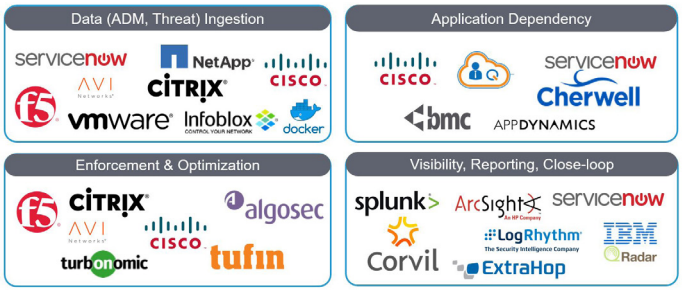
Multi-Data Center & Multi-Cloud Analytics

Tetration Analytics erlaubt nicht nur die Analyse im lokalen Rechenzentrum, sondern ist explizit konzipiert für Multi-Datacenter und Multi-Cloud-Umgebungen. Aufgrund der geringen Netzwerk-Belastung und der sicheren Verschlüsselung können die Sensor-Daten aus verschiedenen Rechenzentren über größere Entfernungen und aus Cloud-Umgebungen zu einem zentralen Tetration-System übermittelt und übergreifend verarbeitet werden. Selbst das zentrale Tetration-System kann wahlweise im Rechenzentrum oder in der Cloud betrieben werden

Offenheit und Integration mit Lösungen von Drittanbietern

Auswertungen und Analysen können nicht nur über die Benutzeroberfläche des Tetration-Systems, sondern auch programmatisch über eine offene REST-API durchgeführt werden.

Hierüber kann Tetration etwa in Incident-Management-Systeme, SIEM-Umgebungen oder jede Art von zentraler Überwachungsumgebung („Leitstand“) integriert werden. Derzeit integrieren über 20 strategische Partner Tetration Analytics mit ihren Lösungen.



Rollenbasierte Zugriffssteuerung

Der Zugriff auf die Daten und Auswertungen in Tetration Analytics wird über ein rollenbasiertes Zugriffs-Modell feingranular gesteuert. Damit können dediziert ausgewählte Sichten und Dashboards bestimmten Verantwortlichen zugänglich gemacht werden.

Einbettung in den Betrieb

Tetration Analytics ist als integriertes System konzipiert, welches von Cisco als solches beim Kunden aufgebaut und fertig übergeben wird. Das Ausrollen der Software-Sensoren erfolgt über die etablierten Prozesse beim Kunden. Spezielles Big-Data- oder Analytics-Know-How ist nicht erforderlich.

Datenschutz und Sicherheit

Die Sensoren (Software und Hardware-Sensoren) kommunizieren über individuelle Zertifikate stets verschlüsselt mit dem Tetration-System. Das „Einschleusen“ von nicht von Tetration selbst erzeugten Sensor-Instanzen wird dadurch wirksam verhindert.

Es werden ausschließlich sogenannte Header-Informationen der Datenpakete verarbeitet, angereichert mit Informationen über die kommunizierenden Server (Betriebssystem, Patch -Level, kommunizierender Prozess, etc). Eine Analyse oder Speicherung der Paketinhalte („Payload“) findet nicht statt.

Weitere Informationen

Interessiert? Weiterführende Informationen zu Cisco Tetration Analytics finden Sie hier:
www.cisco.de/tetration

Bei Fragen wenden Sie sich gerne an:
tetration-sales-germany@cisco.com