NetDescribe

NetDescribe Use Case

SIEM | Entertainment und E-Commerce

mit Splunk Enterprise Security

www.**netdescribe**.com

1. Die Ausgangssituation

Der Kunde ist mit der vorhandenen SIEM (Security Information and Event Management) Plattform Logrythm an seine Grenzen gekommen. Die langfristigen Security-Ziele konnten nicht mehr erreicht werden. Das betraf zum Beispiel

- neue Logformate, die nicht unterstützt wurden,
- variable Logformate, die eine größere Dynamik erforderten,
- aber auch technische Skalierungs- und Stabilitätsprobleme.

Wie kann die Ausfallsicherheit der Systeme maximiert werden?

Mit einem optimierten SIEM kann die Ausfallsicherheit Ihrer Systeme maximiert werden. Eine einfache, standardisierte Erweiterung der Monitoring-/SIEM-Funktion, schnelle Integration komplexer Umgebungen, sowie Schnittstellen und Dashboards „out of the box“ sichern höhere Qualität, mehr Flexibilität und Effizienz sowie eine erhebliche Kostenreduzierung.

Der Schlüssel dazu:
Automatisierung und Visualisierung der Datenauswertung!

Obwohl die Menge der Maschinendaten steigt, fehlt zur Analyse und Bewertung eine einheitliche Datenbasis. Ziel ist die Zentralisierung, Korrelation und Analyse der Daten im gesamten IT-Netzwerk, um Sicherheitsprobleme zu erkennen und in Echtzeit reagieren zu können.

2. Der Use Case

Das Unternehmen aus der Medienbranche ist einer der führenden Entertainment- und E-Commerce-Anbieter im deutschsprachigen Raum. Ergänzt wird das Entertainment-Portfolio durch digitale Verbrauchermarken in den Segmenten Commerce & Ventures sowie Dating & Video.

Das Ziel des Unternehmens war die Erhöhung der IT-Sicherheit durch die Erkennung von Bedrohungen, der Compliance regulatorischer Vorgaben und ganz allgemein dem Incident Management in der IT-Security.

Die Lösung von NetDescribe

Der Einsatz von Splunk Enterprise Security ermöglicht Unternehmen verteilte Daten konsequent per Log-Analyse zentral zu überwachen, auszuwerten und zu visualisieren und somit wertvolle Erkenntnisse aus den Maschinendaten bereitzustellen.

Es können Korrelationsregeln und Berichte erstellt werden, um Unregelmäßigkeiten und Bedrohungen sofort zu identifizieren und automatisch Bereiche mit Verstößen zu erkennen.

Splunk SIEM (Security Information and Event Management)

Volle Transparenz in all Ihren Umgebungen

Schnellere Bedrohungserkennung und -untersuchung

Mehr Flexibilität und Kompatibilität unterschiedlicher Tools und Technologien

3. Die Umsetzung

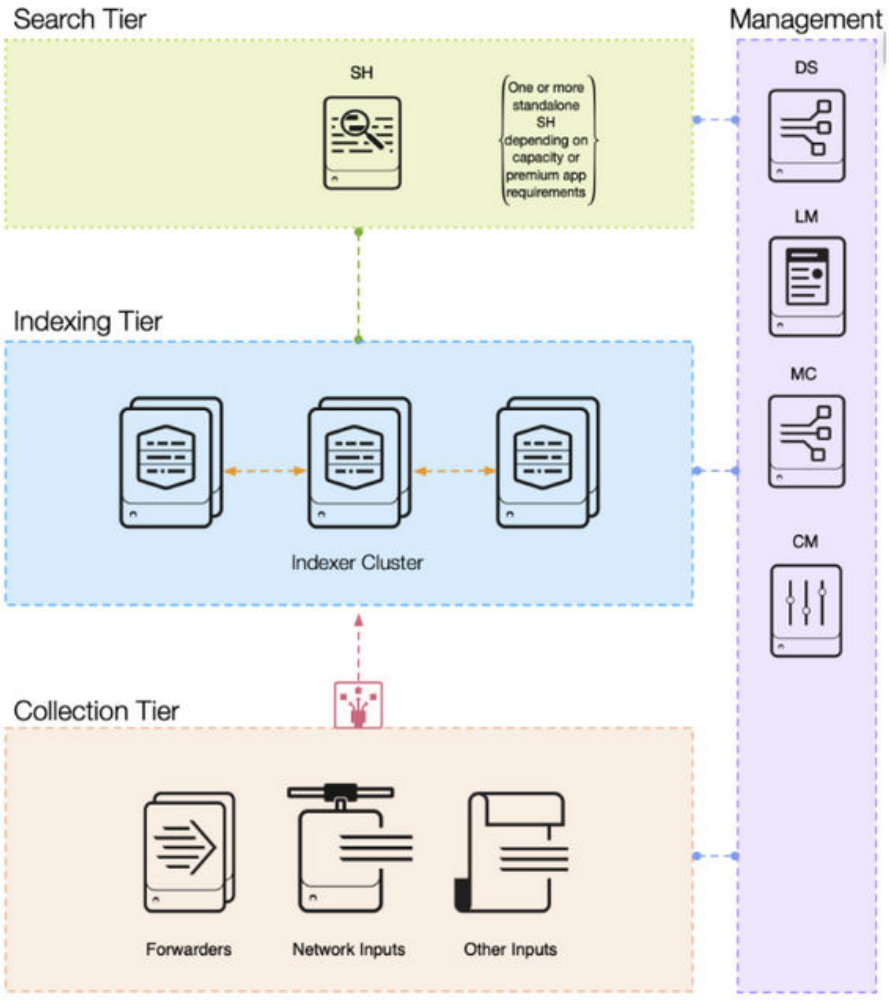
Die erste Demo der Enterprise-Security-Lösung vor Ort beim Kunden mit Hilfe von "Splunk SHOW/ House of Demos" verlief sehr erfolgreich und Fragen konnten umfänglich beantwortet werden.

Der nächste Schritt war die Definition eines Proof of Concept, der die wichtigsten Quellen sowie die Umsetzung einiger Use Cases, die in der bisherigen Lösung nicht abgebildet werden konnten, beinhalten sollte.

Diese POC Phase fand im Rahmen von Workshops statt, um bereits von Anfang an möglichst viel Know-how zu vermitteln. Damit konnte der Kunde sehr schnell selbständig Use Cases umsetzen.

Nach der Beauftragung wurde der Projektplan erstellt.
Die Installation von Splunk Enterprise und Splunk Enterprise Security erfolgte im Rechenzentrum des Kunden.

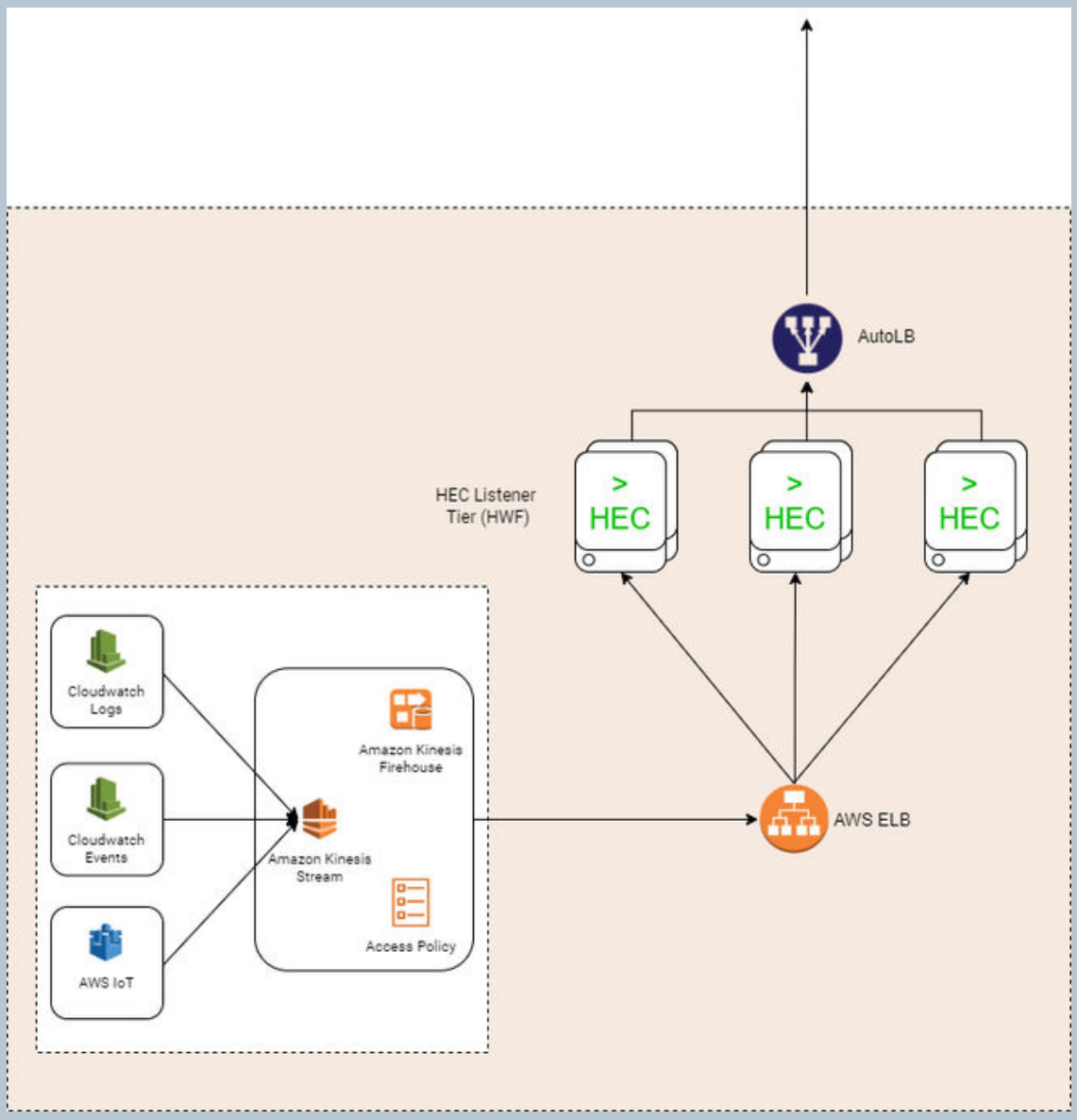
Splunk Architecture*



*Quelle: Splunk

- Splunk Enterprise Security wurde als verteilte Umgebung aufgesetzt
- Indexcluster mit lokalem Storage (1 Jahr Retention)
- 4 stellige Anzahl an Universal Forwarder, gemanged über den Deploymentserver
- 2 Searchhead (Adhoc + Splunk Enterprise Security)
- Integration Splunk-Configs mit Versionierungssoftware (GIT)
- Skizzenhafte Architektur

Kinesis AWS Infrastructure



Folgende Datenquellen wurden angebunden:

- Endpoint Security / mehrere Anti-Virus-Lösungen im Einsatz
- Virtualisierungsinfrastruktur
- Custom-Applikationen
- Cloud - Azure und AWS (mit AWS Firehose / ELB / Lambda)
- Server OS Logs
- Proxy Logs
- Loadbalancer Logs
- ERP System

4. Die Ergebnisse

- Auf Grund der langjährigen Erfahrungen der Mitarbeiter von NetDescribe konnte der enge Zeitplan eingehalten werden.
- Auch nach Abnahme des Projektes erfolgte eine kontinuierliche Weiterbetreuung im Rahmen eines Betriebs-Unterstützungsservice. Neue Datenquellen wurden hinzugenommen und weitere Security Use-Cases umgesetzt.
- Datenquellen, die Format-technisch nicht an die vorige Lösung angebunden werden konnten, wurden in sehr kurzer Zeit (0,5-2 Tage je Quelle) erfolgreich an Splunk Enterprise Security angebunden.
- Datenquellen, die in der vorigen Lösung extra lizenziert werden mussten, erforderten in Splunk Enterprise Security keine weiteren Zusatzlizenzen.
- Alle Quellen wurden in Splunk Enterprise Security normalisiert. Dies hilft u. a. entscheidend bei der Use Case Erstellung, da alles Splunk CIM konform ist.

Was der Kunde über die Zusammenarbeit mit NetDescribe sagt:

> **Die kollegiale, effiziente und sorgfältige Arbeitsweise des NetDescribe Teams hat es uns ermöglicht, unsere komplette SIEM Infrastruktur in nur 3 Monaten aufzubauen und einen nahtlosen Hotswap von LogRhythm auf Splunk durchzuführen.**
>
> **Der Aufbau war hierbei nicht nur lediglich eine Duplizierung unserer alten Umgebung, sondern gleichzeitig auch eine Verbesserung mit neuen Netzwerkzonen-Konzepten zur Gewährleistung der Sicherheit unserer Logdaten.**

Splunk Enterprise - Business Benefits

Splunk Enterprise zeigt die Verfügbarkeit Ihrer IT-Dienste aus realer Anwendersicht. Sowohl die Verteilung auftretender Probleme jeglicher Art als auch die schnelle Identifizierung ihrer Ursachen.

Splunk Enterprise wächst mit Ihren Anforderungen und ist unbegrenzt skalierbar. Möglich sind die Lösung einzelner Probleme wie auch ganzheitlicher, strategischer Überwachungsszenarien, zum Beispiel für Application Delivery, IT Operations, Security Compliance & Fraud, Business Analytics, IoT & Industrial Data.

"Zentrale Überwachung aller Maschinendaten"
Martin Liebelt, Splunk®-Experte bei NetDescribe

Die Splunk-Funktionen auf einen Blick

Sammlung und Indizierung von Maschinendaten
Eventerfassung in Echtzeit, universelle Indizierung, Adapterentfall, Verwendung von Metrikdaten, Zeitstempel für Events

Suche und Überprüfung
Echtzeitsuche, Transaktionssuche, interaktive Ergebnisse

Korrelation und Analyse
Machine-Learning-basierte KI, Korrelation komplexer Events, Ereignisanmerkungen, Mustererkennung

Visualisierung und Reporting
Dashboard-Erstellung, Automatisierung von Berichten

Überwachung und Alarmierung
Monitoring von Ereignissen und KPIs, proaktive Benachrichtigungen

Sicherheit und Verwaltung
Verschlüsselter Zugriff auf Datenströme, gesicherter Benutzerzugriff