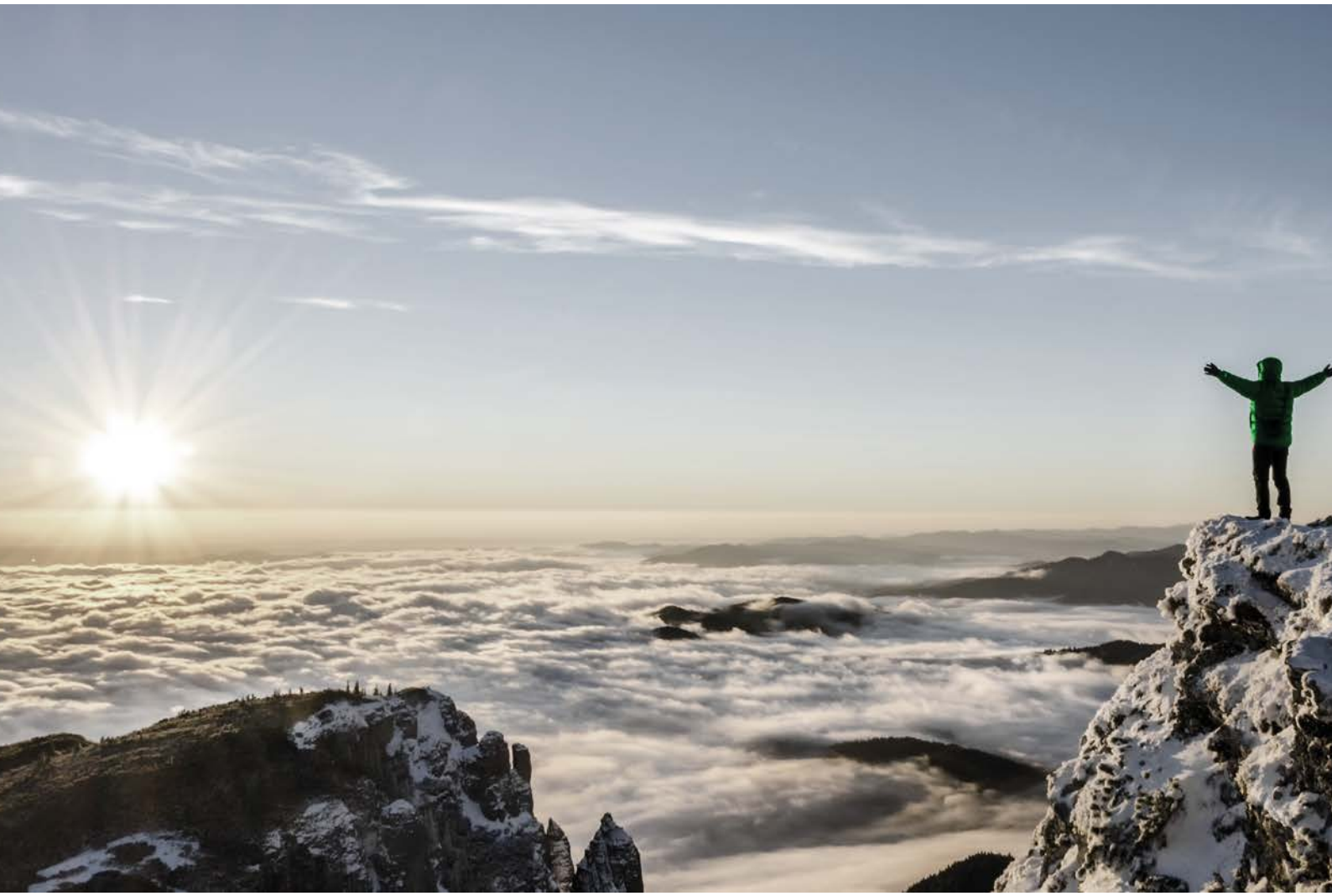
mayato®

Was wir vorhersagen, soll auch eintreffen!



Case Study ||

Einführung von Big Data Security Intelligence für ein Finanzdienstleistungsunternehmen

Einführung von Big Data Security Intelligence für ein Finanzdienstleistungsunternehmen

Management Summary

Stichworte

✓ IT Security Analytics ✓ Big Data ✓ Incident-Prozesse ✓ SOC
✓ IT-Angriffe ✓ Security Operations

Ausgangssituation

Ein Finanzdienstleistungsunternehmen, welches mehr als 10.000 Mitarbeiter in vielen Ländern weltweit beschäftigt, strebt durch seinen hohen Anspruch an Nachvollziehbarkeit und Sicherheit einen optimierten Schutz der IT vor Angriffen an. Ein aktives, nachvollziehbares Reporting soll hierbei nicht nur Angriffe frühzeitig erkennen, sondern auch Erfolgswahrscheinlichkeiten und Ziele potentieller Angreifer identifizieren. Darüber hinaus sollen nachhaltige und technologiegestützte Incident-Prozesse für den Ausbau des Security Operations Center (SOC) etabliert werden.

Ziele

- ✓ Optimierung des Schutzes der IT vor Angriffen
  - ✓ Aktives Reporting
  - ✓ Frühzeitige Erkennung von versuchten oder erfolgten Angriffen
  - ✓ Identifikation möglicher Ziele
  - ✓ Ermittlung von Erfolgswahrscheinlichkeiten
- ✓ Ausbau des Security Operations Center
  - ✓ Etablierung nachhaltiger und technologiegestützter Incident-Prozesse

Ansatz

Im Rahmen des Projekts wurden zunächst eine Bestandsaufnahme der gesamten IT-Umgebung und eine Erfassung möglicher Datenquellen durchgeführt. Hierbei erfolgte gleichzeitig eine Bewertung zur Komplexität der Einbindung der jeweiligen Quellen. Aus den ermittelten Daten wurde eine Chancen- und Nutzenanalyse abgeleitet, die die spezifische Infrastruktur des Kunden reflektiert und als Basis für eine Aufwandsschätzung sowie die Definition des mehrstufigen Vorgehens diente.

Die darauf folgende initiale Anforderungsanalyse wurde auf ein Einvernehmen mit Datenschutz, Sicherheit, Betrieb, Risikomanagement und Betriebsrat fokussiert. Das detaillierte Vorgehen wurde in Abgleich der Ergebnisse der Chancen- und Nutzenanalyse unter Berücksichtigung bestehender Lösungen und deren mögliche Integration ausgearbeitet. Eine Entscheidungsvorlage zur Einführung der kundenspezifischen Lösung zur Erreichung einer Big Data Security Intelligence zielte auf eine stufenweise, budgetoptimierte Implementierung über einen Zeitraum von 2 Jahren nach dem Reifegradmodell unserer Consulting Practise.

Einführung von Big Data Security Intelligence für ein Finanzdienstleistungsunternehmen

Erreichung des Reifegrades 1 der Umgebung

Auf Basis von Logging-Daten unterschiedlichster Netzwerk- und Sicherheitskomponenten, Systeme sowie Applikationen wurden erste Erkenntnisse über die Umgebung erfasst und mit Hilfe von Regelsätzen erste Reports und Analysen ermöglicht.

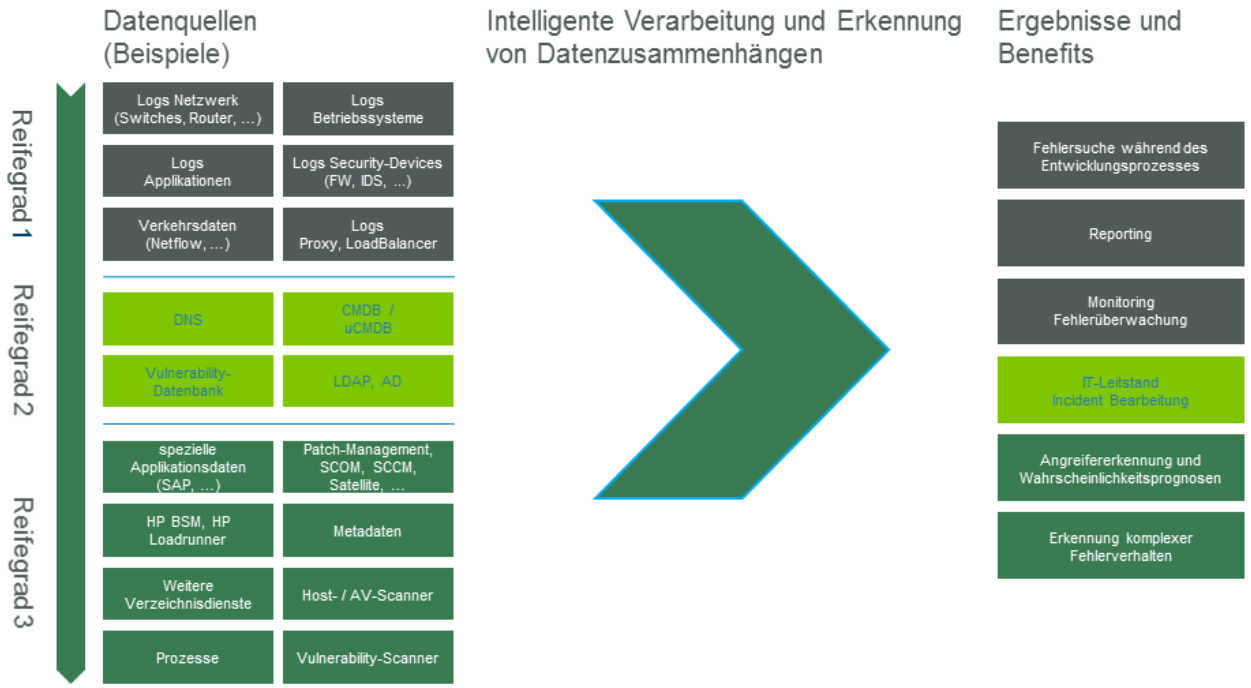
Erreichung des Reifegrads 2 der Umgebung

Im zweiten Schritt wurden die Grundlagen für die Erkennung von Zusammenhängen geschaffen. Hierbei wurden die in Schritt 1 erfassten Live-Daten mit Informationen unterschiedlichster Tools und Systeme wie Verzeichnisdienste oder Inventardatenbanken korreliert. Zur Klassifizierung des Sicherheitsniveaus von Systemen wurde eine Vulnerability-Datenbank eingebunden. Dadurch konnten Such- und Berichtsergebnisse verfeinert und ergänzende Auswertungsmöglichkeiten, insbesondere für das Security Operations Center, geschaffen werden. Mit diesen Möglichkeiten konnte eine erste Involvierung des Systems in die bestehenden Incident-Prozesse erfolgen.

Erreichung des Reifegrads 3 der Umgebung

Im dritten und letzten Schritt des Projekts wurden zusätzliche Datenquellen aus Systemen zum Patch-Management, Monitoring, AV- und Vulnerability-Scanning eingebunden. Hierdurch wurde eine Transparenz geschaffen, welche Systeme für bekannte Schwachstellen anfällig sind. Durch die Auswertung des Patch-Managements konnten gewollte von ungewollten Systemveränderungen unterschieden werden.

Zusätzlich wurden mit Hilfe von mathematischen Analysemethoden Auswertungen implementiert, die eine Erkennung abweichender Verhaltensmuster auch für bislang unbekannte und sehr spezifische Angriffsszenarien ermöglicht. Hierdurch können Ziele von Angriffen und Angreifer auch dann identifiziert werden, wenn die verwendeten Verfahren nicht in Regelwerken von AV- und Security-Scannern abgebildet sind.



Einführung von Big Data Security Intelligence für ein Finanzdienstleistungsunternehmen

Ergebnis

Das aufgebaute System und seine abgesicherte Architektur, welches auf einem Standard-Industrieprodukt basiert, ermöglicht es dem Kunden, Angriffe auf IT-Systeme frühzeitig und auch für bislang unbekannte Szenarien zu erkennen, potentielle Angreifer zu identifizieren sowie eine forensische Nachvollziehbarkeit über die gesamte IT-Infrastruktur zu gewährleisten. Darüber hinaus kann eine Auswertung erfolgen, welche Erfolgswahrscheinlichkeiten für Angriffe auf potentielle Ziele bestehen, die als Grundlage zur Härtung und Optimierung der IT-Landschaft dienen kann.

Über mayato

Die mayato GmbH unterstützt Unternehmen, den optimalen Nutzen aus verfügbaren Informationen zu ziehen. Gemeinsam mit seinen Kunden entwirft und realisiert mayato Lösungen in den Bereichen Financial Analytics, Customer Analytics, Industry Analytics und IT Security Analytics.

Von den Standorten Berlin, Bielefeld, Mannheim und Wien aus arbeitet ein Team von erfahrenen Prozess- und Technologieberatern. Diese analysieren und optimieren Ihre fachlichen Prozesse und erarbeiten mit Ihnen die Anforderungen an deren technische Umsetzung. Sie helfen bei der Auswahl der geeigneten Werkzeuge, entwickeln erfolgreiche Strategien und konzipieren bewährte und moderne Architekturen. Natürlich helfen mayato Berater auch bei deren praktischer Umsetzung. Technische Standards und methodische Vorgaben (Governance) ermöglichen sparsame, effektive Projekte und einen effizienten, nachhaltigen Betrieb.

Analysten und Data Scientists von mayato nutzen diese Lösungen in Ihrem Auftrag für die Ermittlung relevanter Zusammenhänge in unterschiedlichsten Daten sowie für die Prognose zukünftiger Trends und Ereignisse. Sie schaffen überzeugende Business Cases und einen spürbaren monetären Nutzen Ihrer Prozesse und Anwendungen. Ihre Mitarbeiter lernen den Umgang mit modernen Verfahren der Datenanalyse, mit Problemen der Datenqualität und bei der Interpretation und Visualisierung von Ergebnissen. Die Zusammenarbeit mit mayato macht Ihr Unternehmen fit für das Big-Data-Zeitalter.

Die mayato GmbH wurde 2007 gegründet. Zu den Kunden von mayato zählen namhafte große und mittelständische Unternehmen aus unterschiedlichen Branchen. Als Partner mehrerer Softwareanbieter ist mayato grundsätzlich der Neutralität und in erster Linie der Qualität seiner eigenen Dienstleistungen verpflichtet. Nähere Infos unter www.mayato.com.

Was wir vorhersagen, soll auch eintreffen!

Kontaktieren Sie uns //

mayato GmbH
Am Borsigturm 9
13507 Berlin

info@mayato.com

+49 / 30 4174 4270 10