FORCEPOINT
POWERED BY Raytheon

Protecting the human point.

FORCEPOINT UEBA-PLATTFORM
Architekturübersicht

FUNKTIONELLE ARCHITEKTUR – EINBLICK IN KRITISCHEN DATENFLUSS UND ANWENDERVERHALTEN

Die Forcepoint User and Entity Behavior Analytics (UEBA)-Plattform ist eine verteilte, fehlertolerante und umfassende Anwendung, die Einblick in Ihre kritischen Datenflüsse und damit Schutz vor Insider-Bedrohungen bietet. Dieses Dokument beschreibt die wesentlichen Komponenten von Forcepoint UEBA. Darüber hinaus erfahren Sie, welchen Beitrag die einzelnen Komponenten zur Forcepoint UEBA-Gesamtlösung leisten und welche jeweiligen technischen Vorteile sich dadurch ergeben.

Wie nachstehend beschrieben und auf der folgenden Seite dargestellt fließen Rohdaten von zahlreichen Quellen in die Ingest-Architektur und schließlich in die Anwendungsebene, wo die durch zusätzliche Informationen ergänzten Forcepoint UEBA-Ereignisse gespeichert, untersucht und an Analysten zur weiteren Prüfung weitergeleitet werden.

ARCHITEKTUREBENEN

Ebene I: Daten › Forcepoint UEBA sammelt Rohdaten aus einer Vielfalt von Datenströmen des Unternehmens, einschließlich Kommunikation, Muster über physischen Zugang sowie Endpunkt- und Netzwerkaktivitäten. Forcepoint DLP und Forcepoint Insider Threat werden als Datenquellen empfohlen, sind jedoch nicht zwingend erforderlich.

Ebene II: Ingest › Auf der Ingest-Ebene werden Rohdatenströme transformiert und für nachfolgende Analyseschritte vorbereitet. Mithilfe einer flexiblen Datenerfassungsplattform (d. h. TCP-Listener, FTP-Download) sammelt Forcepoint UEBA Rohdaten, transformiert diese in das anwendungseigene Ereignisformat und leitet Daten über die Ingest-Pipeline und Analyse-Engine weiter.

Ebene III: Anwendung › Die Anwendungsebene bietet höchst skalierbare Datenspeicher- und Abfragefunktionen, Analysen von Benutzerverhalten zur Laufzeit, eine Analysten- und Administratoroberfläche sowie eine externe API (Outbound API).

ANALYSE-FRAMEWORK VON FORCEPOINT UEBA

Der Analyseansatz von Forcepoint UEBA basiert auf drei wesentlichen Elementen, die folgende Faktoren festlegen: Welche Daten sollen und können erfasst werden? Wie können Aktivitätsdaten und ergänzende Informationen erfasst werden? Und welche Analysemodelle sind zur Identifizierung von Risiken durch Insider auszuführen? Jedes einzelne Element wird nachfolgend kurz beschrieben.

Audit-Leitfaden › Gibt Empfehlungen für optimale Protokollierungs- und Erfassungseinstellungen angesichts des Netzwerk- und Sicherheitsökosystems eines bestimmten Kunden.

Datenmodell › Stellt ein einheitliches Datenmapping über viele unterschiedliche Datenquellen hinaus sicher.

Basis-Analysemodelle › Bietet vordefinierte Analysekonfigurationen für Funktionen, Modelle und Szenarien.

ARCHITEKTUR – GRAFISCHE DARSTELLUNG

DATEN

E-KOMMUNIKATIONSEREIGNISSE
(Exchange, Office 365, Lync, Bloomberg Chat)

- E-Mail
- IM
- Voice
- SMS

NETZWERK- UND ENDPUNKTEREIGNISSE

EDR
(Forcepoint Insider Threat, Carbon Black, Dtex)

- Dateiaktivität
- Website-Aktivität
- Prozessaktivität

SIEM
(Forcepoint DLP, Carbon Black, Dtex)

- Authentifizierungsprotokolle
- VPN-Protokolle
- Proxy-Protokolle
- Druckprotokolle
- usw.

PHYSISCHE AKTIVITÄTSEREIGNISSE

- Geolokalisierung/GPS-Protokolle
- Gebäudezugangsprotokolle

ENTITÄTSERGÄNZUNGEN

MITARBEITERATTRIBUTE (Active Directory, Workday)

- Vorgesetzter
- Unternehmenseinheit
- usw.

DRITTANBIETERATTRIBUTE (salesforce.com, Workday)

- Kundenseitige CRM-Systeme
- Anbietermanagement

NETZWERK-ENTITÄTSATTRIBUTE

- Attribute von Endpunktgeräten
- Attribute mutwilliger Akteure
- Attribute hochriskanter Domains

INGEST

1 **PLATTFORM ZUR DATENFLUSSVERARBEITUNG** (Apache NiFi)

- Ingest-Workflows
- Daten-Templates
- Pre-Ingest-Prozess; Ergänzung und Markup
- Metriken

2 **ÖFFENTLICHE API**
(Dropwizard)

- Batch-Modus
- Echtzeit

3 **INGEST-ANALYSEN** (Rabbit MQ, Queue Worker)

- Validierung des Ereignisdatums
- Deduplizierung
- Entitätsauflösung
- Administration

ANWENDUNG

4 **DATENSPEICHER** (Elasticsearch)

- Indizierte Ereignisse
- Strukturiert und unstrukturiert
- Referenzielle Entitätsdaten

7 **EXTERNE API**

5 **STAMMDATENQUELLE**

LAUFZEITANALYSEN (Java)

- Abfragen
- Bewertungsmodelle
- Analytische Szenarien (Sammlungen)

DATENEBENE (Postgres, Redis)

- Anmeldedaten
- Berechtigungen
- Rollen
- Zwischengespeicherte Anwendungsdaten

DATEIEN/ANHÄNGE (Dateisystem)

- Dateianhänge
- Native Dateiformate

6 **UI-SERVICES** (Node.js)

- Reporting
- Forensik
- Analyse-Tuning
- Administration

EBENE I: DATENVERARBEITUNGSPLATTFORM

Forcepoint UEBA verwendet Feeds aus vorhandenen Sensoren, Protokollen und Netzwerksicherheitsstrukturen, um Verhaltensanalysen zur Erkennung von Insider-Bedrohungen zu liefern. Zur Verarbeitung von Rohdaten nutzt die Datenverarbeitungsplattform von Forcepoint UEBA eine Reihe von Mechanismen, darunter Abhören eingehender TCP- oder UDP-Verbindungen (d. h. syslog), API-Abfragen (d. h. Splunk API) oder Massendatenausgaben über FTP, Dateifreigaben usw.

EBENE II: INGEST

Die erste Gruppe der Plattformkomponenten beinhaltet Ingest- und Ergänzungsprozesse. Nachdem die in Forcepoint UEBA zu analysierenden Datentypen gemäß den Vorgaben des Audit-Leitfadens bestimmt wurden, werden diese Datenquellen dem Datenmodell in der Pre-Ingest-Datenflussverarbeitungsplattform zugeordnet und dann in Forcepoint UEBA über die öffentliche API eingespeist. Anschließend durchlaufen die Daten eine Reihe von Ergänzungs- und Analyseprozessen. Die einzelnen Komponenten und ihre jeweiligen Vorteile werden nachfolgend beschrieben.

1 **Pre-Ingest-Datenflussverarbeitungsplattform ›** Forcepoint UEBA nutzt hauptsächlich das Apache NiFi-Framework, um Daten vor der Einspeisung zu verarbeiten. Apache NiFi wurde ursprünglich durch die National Security Agency (NSA) entwickelt und 2014 als Open-Source-Software freigegeben. Die Schlüsselkonzepte des NiFi-Frameworks wie Herkunftsermittlung und Transformation von Daten, lose Kopplung, hohe Parallelität und Metriken stimmen eng mit den Ingest-Prozessen von Forcepoint UEBA überein und die Forcepoint UEBA/NiFi-Produktlösung bietet Kunden einen Satz an standardisierten, optimierten und resilienten Workflows, Templates und Prozessoren zum Konsolidieren von Datenquellen und Ausgeben von Daten über die öffentliche API von Forcepoint UEBA. Die Plattform zur Datenflussverarbeitung ermöglicht Kunden außerdem die Entwicklung und Implementierung umgebungsspezifischer Ergänzungsprozessoren, um Ereignisse vor der Übergabe an Forcepoint UEBA zu kennzeichnen. Datenfeeds können damit ohne zusätzliche Kosten professioneller Forcepoint UEBA Services angepasst werden. Zusammenfassend lässt sich also sagen, dass die Pre-Ingest-Datenflussverarbeitungsplattform mehr Erweiterungsmöglichkeiten und Flexibilität bietet, ohne zusätzliche Kosten zu verursachen oder die Komplexität zu erhöhen.

2 **Öffentliche API zum Einspeisen von Daten in UEBA ›** Bei der öffentlichen API von Forcepoint UEBA handelt es sich um eine RESTful API zum Einspeisen von Ereignis- und Entitätsdaten in die Anwendung – entweder in Echtzeit oder über einen Massen-Upload. Die API umfasst zahlreiche vordefinierte Endpunkte, die mit den Mappings von Datenmodellen übereinstimmen (auch genutzt in der Pre-Ingest-Datenflussverarbeitungsplattform), und bietet außerdem einen standardisierten Satz an Metriken zur Ermittlung der Anfragelatenz. Zwei wesentliche Vorteile der öffentlichen API sind die Vereinfachung und Transparenz des Ingest-Prozesses. (Hinweis: Bestimmte Datenquellen können direkt in die unten beschriebenen Ingest-Pipelines eingespeist werden. Forcepoint UEBA empfiehlt jedoch dringend die Verwendung der öffentlichen API.)

3 **UEBA Ingest-Pipeline (Validierung › Ergänzung › Analysen) ›** Nachdem die Ereignis- und Entitätsdaten über die öffentliche API eingespeist wurden, werden sie zur weiteren Bearbeitung und Ergänzung in die Nachrichtenwarteschleife eingefügt und an den Queue Worker weitergeleitet. Alle Prozessoren im Queue Worker bieten Vorteile für nachfolgende Analyseschritte und forensische Untersuchungen. Nachstehend betrachten wir jeden einzelnen Prozessor:

- **Validierung des Ereignisdatums:** Ermöglicht Forcepoint UEBA, ausschließlich Ereignisse einzuspeisen, die für das konfigurierte Analysezeitfenster relevant sind.
- **Deduplizierung:** Ermöglicht das Entfernen duplizierter Ereignisse, um Aufwand zu reduzieren. Damit werden Anwendern unnötige Arbeitsschritte erspart.
- **Entitätsauflösung:** Bietet die Auflösung von Ereigniskennungen im Zusammenhang mit einer bestimmten Entität. So kann eine einzelne Entität einfach mit mehreren Kennungen und Aktivitätsmodi verbunden werden.
- **Erkennung von Haftungsausschlüssen:** Reduziert Aufwand, indem für die Analyse irrelevanter Text (nämlich Haftungsausschlüsse) aus Kommunikationsereignissen entfernt wird.
- **Kennzeichnung:** Ermöglicht die Kennzeichnung von Ereignissen basierend auf einer bestimmten Gruppe von Richtlinien.
- **Bewertung:** Bewertet als erster Baustein im Analyseprozess jedes Ereignis basierend auf dem konfigurierten Satz an Basis-Analysemodellen, die in das System geladen wurden.

EBENE III: FORCEPOINT UEBA-ANWENDUNG

Nach dem Ingest-Vorgang werden die in das System eingespeisten Ereignisse und Entitäten gespeichert, um in der Anwendung verwendet zu werden. Dieser Abschnitt erläutert die Funktionen und Vorteile der einzelnen Anwendungskomponenten.

4 **Datenspeicher ›** Forcepoint UEBA nutzt Elasticsearch (ES) als primären Datenspeicher für Ereignis- und Entitätsdaten. Elasticsearch hat sich weithin bewährt und bietet im Vergleich zu anderen Datenbanktechnologien bedeutende Anwendervorteile bei Textsuche, Analyse und Aggregation.

5 **Stammdatendienst (Master Data Service, MDS) ›** Der proprietäre Stammdatendienst von Forcepoint UEBA stellt einen Großteil der Analysefunktionen der Anwendung bereit und korreliert darüber hinaus Daten aus dem Elasticsearch-Datenspeicher mit anderen unterstützenden Technologien (z. B. werden Postgres und Redis zum Speichern relationaler und transaktionaler Daten genutzt). Ein Vorteil dieser separaten Datenspeicher liegt darin, dass sich die einzelnen Speicher unabhängig voneinander skalieren lassen.
So ergeben sich bei der Bereitstellung mehr Konfigurationsmöglichkeiten basierend auf der Menge an überwachten Anwendern und eingespeisten Daten und damit niedrigere Betriebskosten für unsere Kunden.

- **Analysen zur Laufzeit:** Diese Analysen ermöglichen Analysten die Ausführung von Ad-hoc-Abfragen in Echtzeit, entitätsorientierte Risikoberechnungen und szenariobasierte Verhaltensanalysen (d. h. szenariobasierte Rollups speziell zu Risiken wie Herausschleusen von Daten, Missbrauch von Daten durch privilegierte Benutzer oder Datenflucht).
- **Datenebene:** Anmeldedaten, Berechtigungen und Rollen werden im Stammdatendienst gespeichert. Außerdem werden hier Anwendungsdaten zwischengespeichert, um Abfragezeiten zu verkürzen.
- **Dateien/Anhänge:** Für Ereignis-Feeds mit Dateien und Anhängen indiziert der Stammdatendienst die Inhalte dieser Dateien oder Anhänge und bietet optional eine dauerhafte Speicherung der ursprünglichen Anhänge, um Anwendern einen einfachen Zugriff und Detailsuchen über die Benutzeroberfläche zu ermöglichen. Analysten können damit direkt vertiefende forensische Untersuchungen zu einem bewerteten Ereignis durchführen und so ihre Produktivität bedeutend steigern.

6 **UI-Services ›** Die Benutzeroberflächenebene von Forcepoint UEBA ist eine Web-Anwendung, während es sich beim Client um einen Browser handelt. Für alle Interaktionen zwischen Browser und Server wird ein Node.js HTTPS-Server genutzt. Anwendungsdaten und Anwendersitzungen werden mithilfe von Redis im Cache gespeichert.

7 **Externe API (Outbound API) ›** Forcepoint UEBA bietet außerdem einen Outbound-API-Service, mit dem externe Anwendungen verarbeitete Ereignisse und damit verbundene analytische Metadaten abrufen können (d. h. Merkmale und Modelle). Kunden können damit die Analyseergebnisse von Forcepoint UEBA in anderen Systemen nutzen (d. h. Sicherheitsorchestrierung oder Workflow).

WICHTIGSTE SCHLUSSFOLGERUNGEN ZUR ARCHITEKTUR

Zusammenfassend kann gesagt werden, dass der Forcepoint UEBA Ingest- und Anwendungs-Stack eine Reihe bewährter und anerkannter Open-Source-Technologien in Kombination mit proprietären Lösungen nutzt, um unseren Kunden die folgenden technischen Alleinstellungsmerkmale und Vorteile zu bieten:

- Moderne, erweiterbare Architektur, die eine horizontale Skalierung (Scale-out) bei wachsendem Datenvolumen bietet.
- Flexibles Entitäts- und Ereignisdatenmodell, das nahtlos in die Ingest-Pipeline von Forcepoint UEBA implementiert ist. Damit können sowohl strukturierte als auch unstrukturierte Daten verarbeitet, aufgelöst und analysiert und neue Feeds schnell integriert werden.
- Pipeline-Verarbeitung, bei der Inhaltsklassifizierung, Ereignisbewertung, Risikomodellierung und das Erstellen von Verhaltensprofilen sequenzialisiert werden.
- Stark konfigurierbare Echtzeit-Analysen ermöglichen den Einsatz von Forcepoint UEBA bei verschiedensten Anwendungsfällen – von kriminellen Geschäften über Marktmanipulation bis hin zum Herausschleusen von Daten und Unternehmensspionage.
- Abfrage-Engine für Echtzeitanalysen, die Analysten spontanes Durchführen von Untersuchungen und Verhaltensanalysen ermöglicht.

KONTAKT
www.forcepoint.com/contact