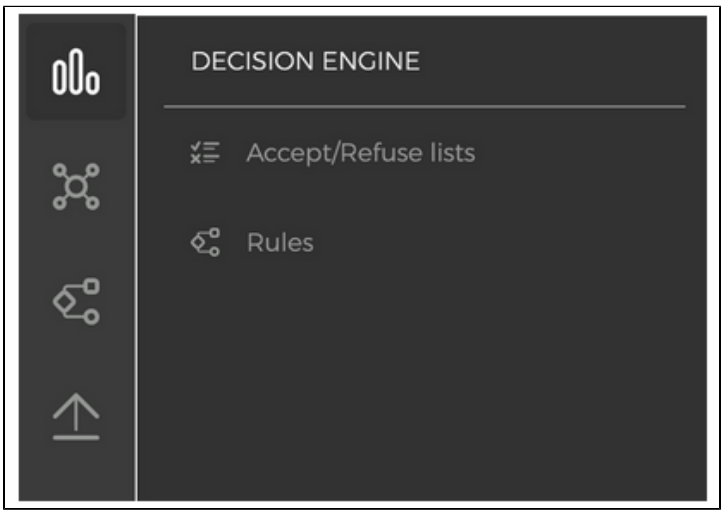
Entscheidungs-Engine

Die Ansicht der Entscheidungs-Engine besteht aus 2 Teilen:

- Akzeptanz-/Ablehnungslisten
- Regeln



Akzeptanz-/Ablehnungslisten

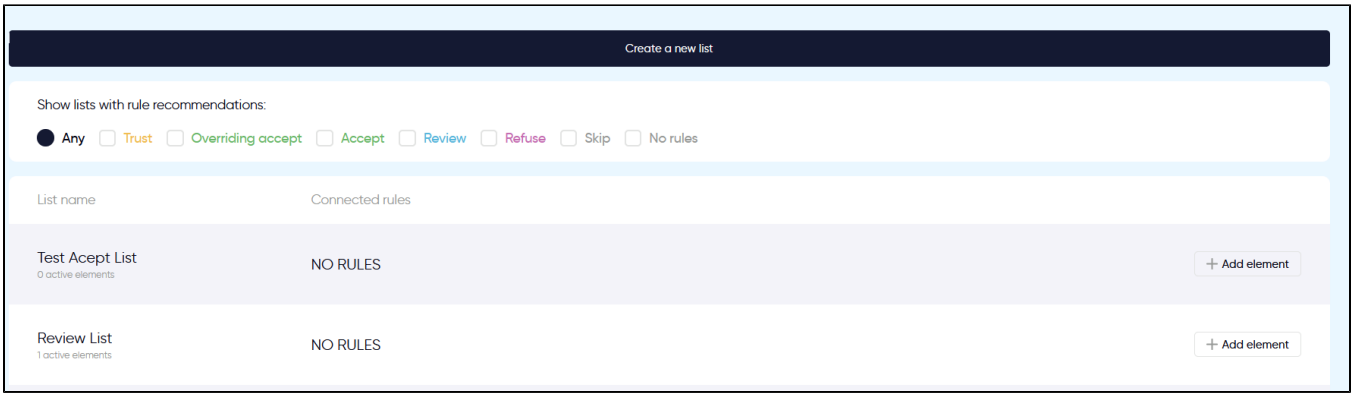
In der Ansicht sehen Sie alle in Ihrer Anwendung konfigurierten Listen. Jede Liste sollte mit einer „listenbasierten Regel“ verbunden sein. Hier finden Sie Informationen darüber, welche Empfehlungen verbundene Regeln im Falle einer Übereinstimmung erzeugen. Abhängig von der verbundenen Regel können wir drei Haupttypen von Listen unterscheiden:

Die Ablehnungsliste ist eine Liste, die mit einer listenbasierten Regel verbunden ist, die bei einer Übereinstimmung eine Emepfehlung Ablehnung generiert.

Die Überprüfungsliste ist eine Liste, die mit einer listenbasierten Regel verbunden ist, die bei einer Übereinstimmung eine Empfehlung Überprüfung generiert.

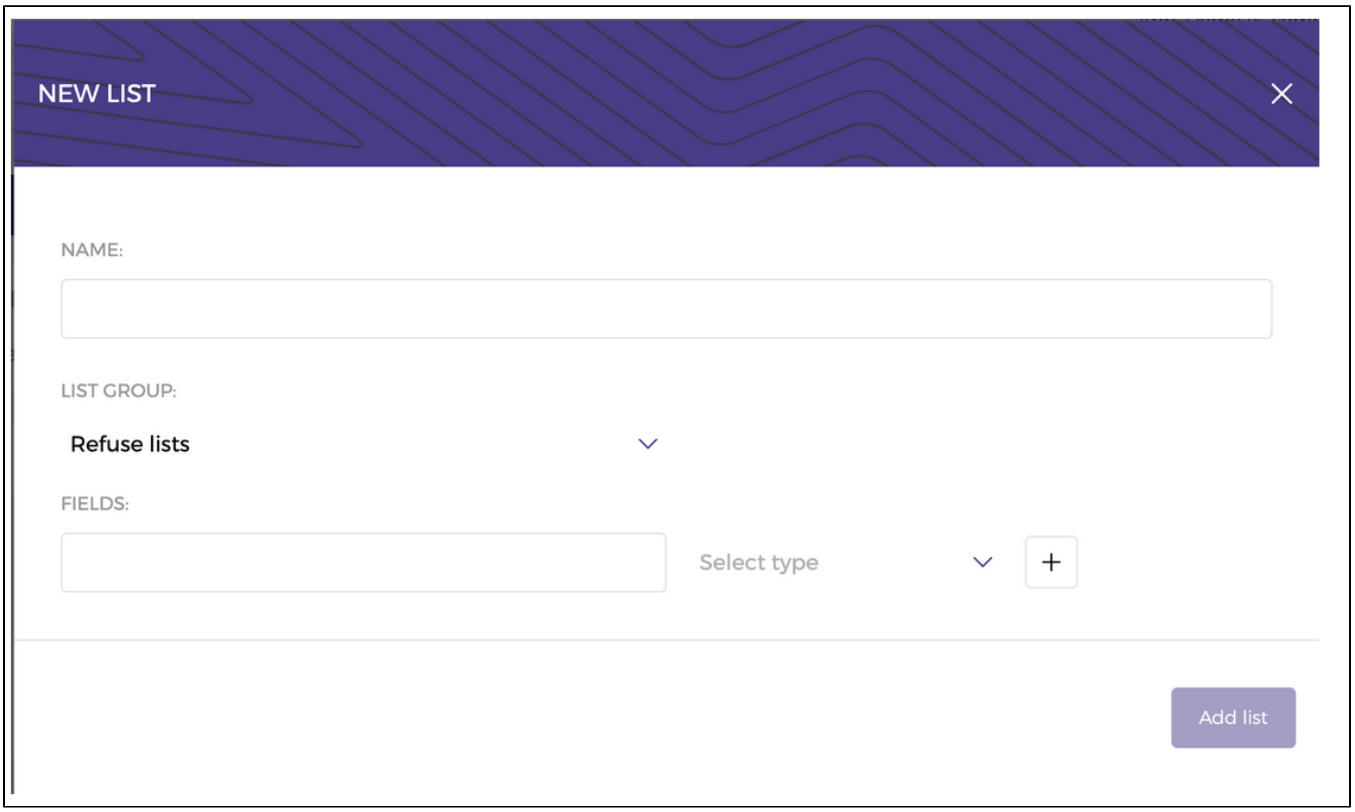
Die Annahmeliste ist eine Liste, die mit einer listenbasierten Regel verbunden ist, die bei einer Übereinstimmung entweder eine Empfehlung Overriding_Accept oder Akzeptanz generiert. Dadurch wird sichergestellt, dass die Transaktion immer akzeptiert wird und die Ergebnisse anderer Regeln ignoriert werden.

- Beachten Sie bitte, dass das Anlegen einer Liste allein keine Auswirkungen hat. Sie enthält nur Elemente. Um eine Liste in der Entscheidungslogik zu verwenden, muss ihr eine Regel zugeordnet werden.
- Die Überprüfungsliste erzeugt eine Überprüfungsempfehlung, bei der Transaktion wird dies jedoch als Ablehnung behandelt und die Zahlung wird abgelehnt. Die Überprüfungsempfehlung der zahlung muss individuell behandelt werden. Wenden Sie sich an den Helpdesk, um diesen Anwendungsfall zu unterstützen.



Neue Liste anlegen

Per Klick auf ‘Eine neue Liste anlegen’ können Sie eine neue Liste hinzufügen.



Zum Anlegen einer neuen Liste sind folgende Eingaben erforderlich:

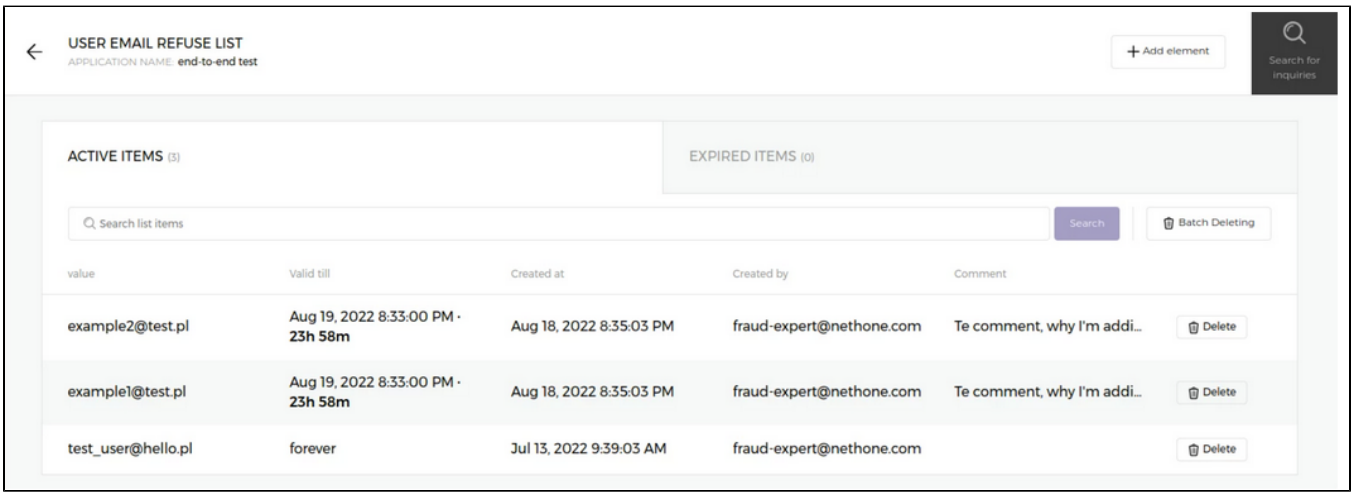
- Listenname,
- die Gruppe, zu der sie gehören soll (Ablehnungsliste, Überprüfungsliste oder Akzeptanzliste),
- die Liste der Felder, die die Elemente der Liste enthalten. Stellen Sie sicher, dass Sie den gewünschten Feldnamen manuell eingeben und den Feldtyp aus der Dropdown-Liste auswählen.

Sie können auch beim Erstellen einer listenbasierten Regel eine Liste anlegen. Weitere Informationen finden Sie unter Listenbasierte Regel.

Listendetails

Per Klick auf eine Liste gelangen Sie direkt zu den Listendetails und sehen:

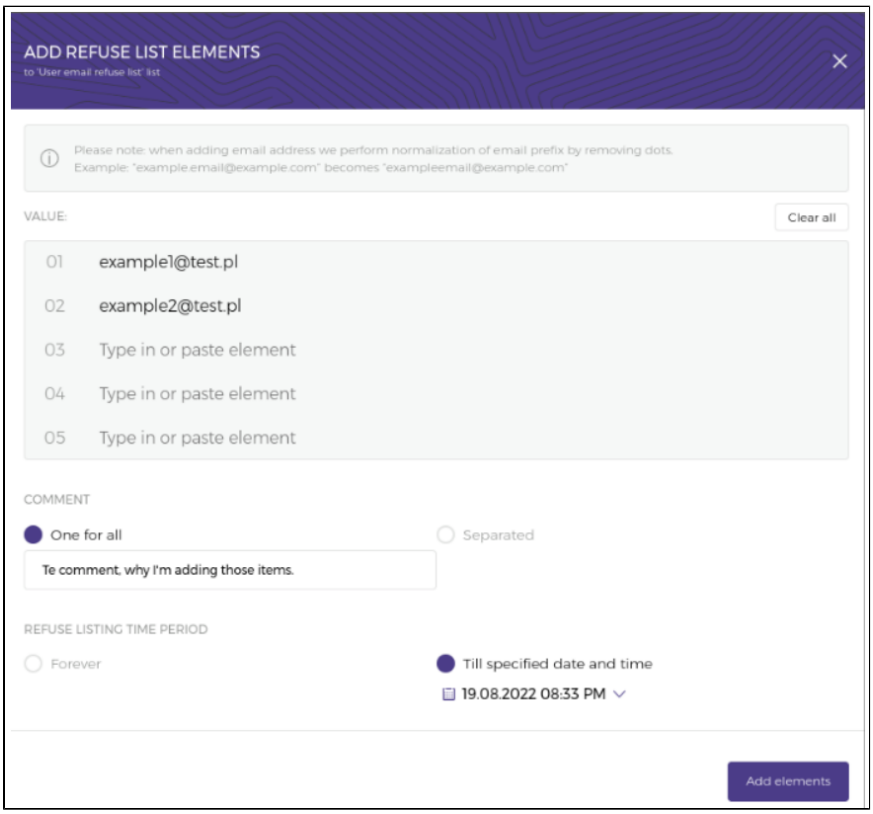
- die Listenelemente,
- wann das Element abläuft (Sie können Listenelemente entweder dauerhaft oder vorübergehend hinzufügen, indem Sie das Enddatum angeben),
- wer das Element erzeugt hat,
- wann das Elemente erzeugt wurde,
- den Kommentar des Elemente.



Sie können sowohl aktive als auch abgelaufene Elemente von Listen prüfen, indem Sie zwischen den entsprechenden Registern navigieren. Sie können auch ein einzelnes Element aus der Liste löschen oder die Batch-Löschfunktion verwenden, um mehrere Punkte auf einmal zu löschen. Die Suchleiste hilft Ihnen, bestimmte Elemente zu finden.

Sie können Elemente aus Listen auch löschen, indem Sie rechts auf die Schaltfläche „Löschen“ klicken. Vor dem Löschen eines Elements werden Sie um Bestätigung gebeten.

In der oberen rechten Ecke finden Sie die Schaltfläche „Element hinzufügen“.



Sie können mehrere Elemente gleichzeitig hinzufügen. Die Elemente können dem Panel auch bereitgestellt werden, indem Sie sie aus der Zwischenablage einfügen, getrennt durch eine neue Zeile.

Die Datentypen, die einer Liste hinzugefügt werden können, hängen von der API-Integration Ihrer Plattform ab. Normalerweise sind dies:

- E-Mail-Adresse
- Cookie
- Kartentoken

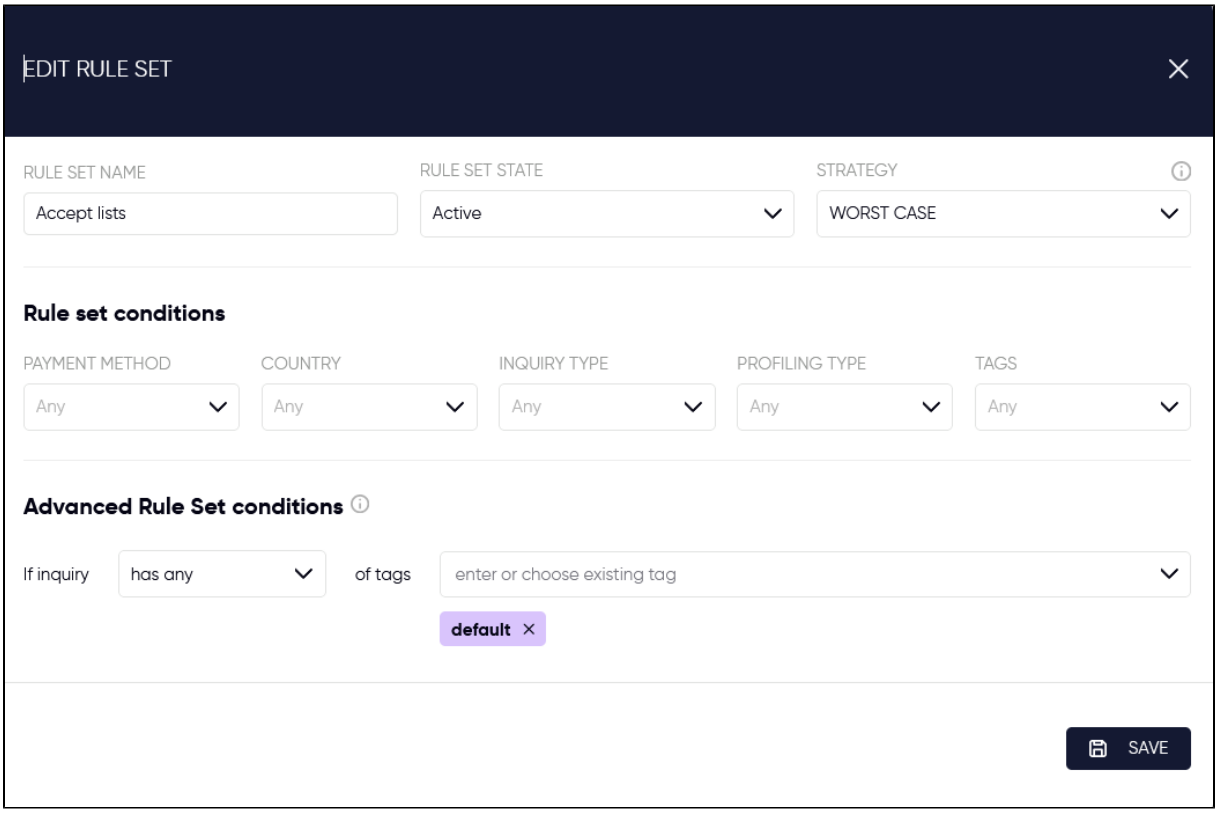
- Telefonnummer

Regeln

Die Ansicht zeigt alle in Ihrer Anwendung konfigurierten Regelsätze mit grundlegenden Informationen:

- Regelsatzstatus: 'aktiv' / 'inaktiv' / 'Simulation'
- die für den Satz konfigurierte Strategie
- Ausführungsbedingungen
- Anzahl der aktiven Regeln im Satz
- Verknüpfung zum Hinzufügen einer neuen Regel.

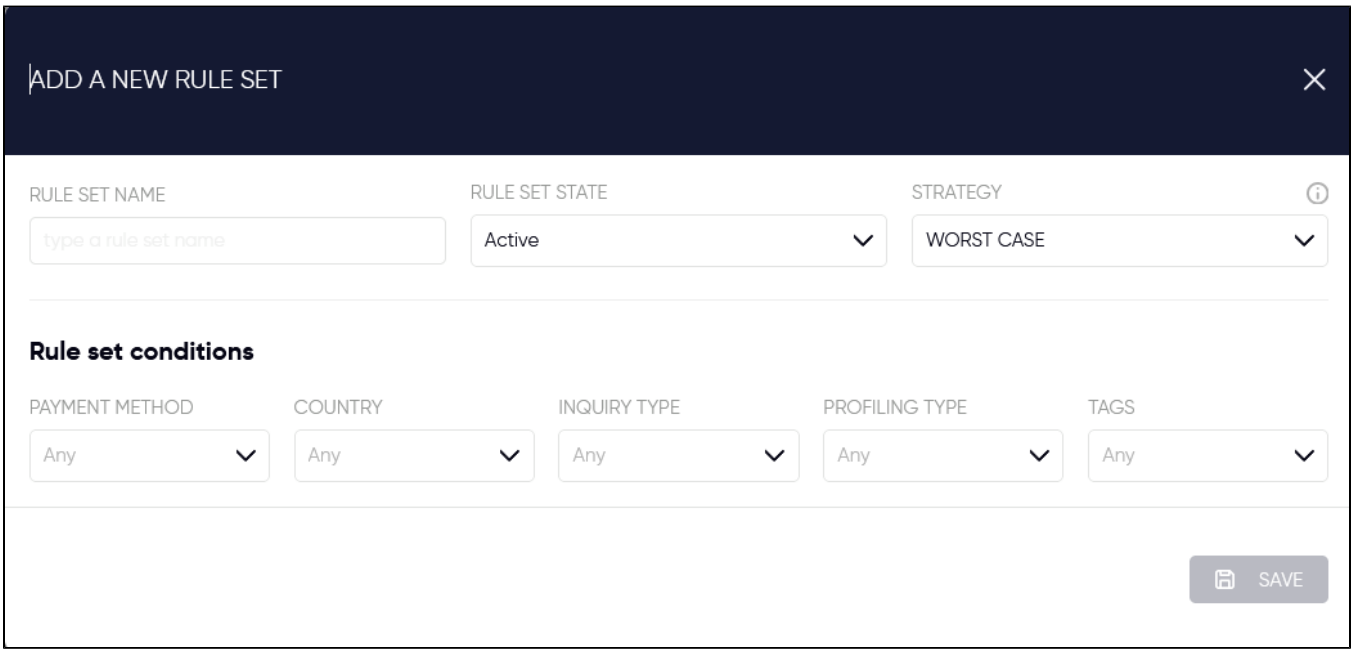
Sie können diese Regelsatzparameter bearbeiten, indem Sie in der Regelsatzansicht auf die Schaltfläche „Bearbeiten“ klicken. Dadurch wird der folgende Bearbeitungsbereich geöffnet:



Um einen neuen Regelsatz hinzuzufügen, klicken Sie einfach unten in der Ansicht auf die Schaltfläche „Neuen Regelsatz hinzufügen“.

Neuen Regelsatz hinzufügen

Per Klick auf die Schaltfläche 'Neuen Regelsatz hinzufügen' wird das Fenster zum Hinzufügen eines neues Regelsatzes geöffnet:



Geben Sie dem erzeugten Regelsatz einen Namen, wählen Sie einen Anfangszustand und eine Strategie und fügen Sie noch einige Ausführungsbedingungen für den Regelsatz hinzu.

Sie können weitere Ausführungsbedingungen hinzufügen, indem Sie auf die Schaltfläche „+ UND“ klicken:

Der Regelsatz wird sofort nach dem Klicken auf die Schaltfläche 'Speichern' erzeugt.

Regelsatzzustände

Regelsatzzustände können folgende Werte annehmen:

- Aktiv – Regeln innerhalb des Regelsatzes werden ausgelöst und das Ergebnis beeinflusst das Endergebnis
- Inaktiv – Regeln innerhalb des Regelsatzes werden nicht ausgelöst
- Simulation – Regeln innerhalb des Regelsatzes werden ausgelöst, aber das Ergebnis beeinflusst das Endergebnis nicht.

Strategien

Wenn mindestens eine Regel „overriding_accept“ zurückgibt, lautet die endgültige Empfehlung immer „akzeptieren“ (alle anderen werden überschrieben), unabhängig von der konfigurierten Strategie.

Strategie “Worst Case” – ein Satz gibt die schlechteste Regelempfehlung zurück:

- falls eine Regel 'ablehnen' zurückgibt – gibt der Satz 'ablehnen' zurück
- falls eine Regel 'überprüfen' zurückgibt – gibt der ganze Satz 'überprüfen' zurück
- falls alle Regeln 'akzeptieren' oder 'übersprungen' zurückgeben – gibt der Satz 'akzeptieren' zurück

Strategie “Best Case” – ein Satz gibt die beste Regelempfehlung zurück:

- nur wenn alle Regeln 'ablehnen' zurückgeben – gibt der Satz 'ablehnen' zurück
- falls alle Regeln 'überprüfen' zurückgeben – gibt der ganze Satz 'überprüfen' zurück
- falls mindestens eine Rgel 'akzeptieren' zurückgibt – gibt der Satz 'akzeptieren' zurück

Das System gibt die endgültige Empfehlung auf Grundlage der Empfehlungen der Sätze. Die angewandte Strategie ist immer die „Worst-Case"-Strategie (allerdings hat „overriding_accept" weiterhin Vorrang).

Sie können die Ergebnisse der Entscheidungs-Engine im Widget „Entscheidungslogik" in der Abfrageansicht sehen.

Ausführungsbedingungen

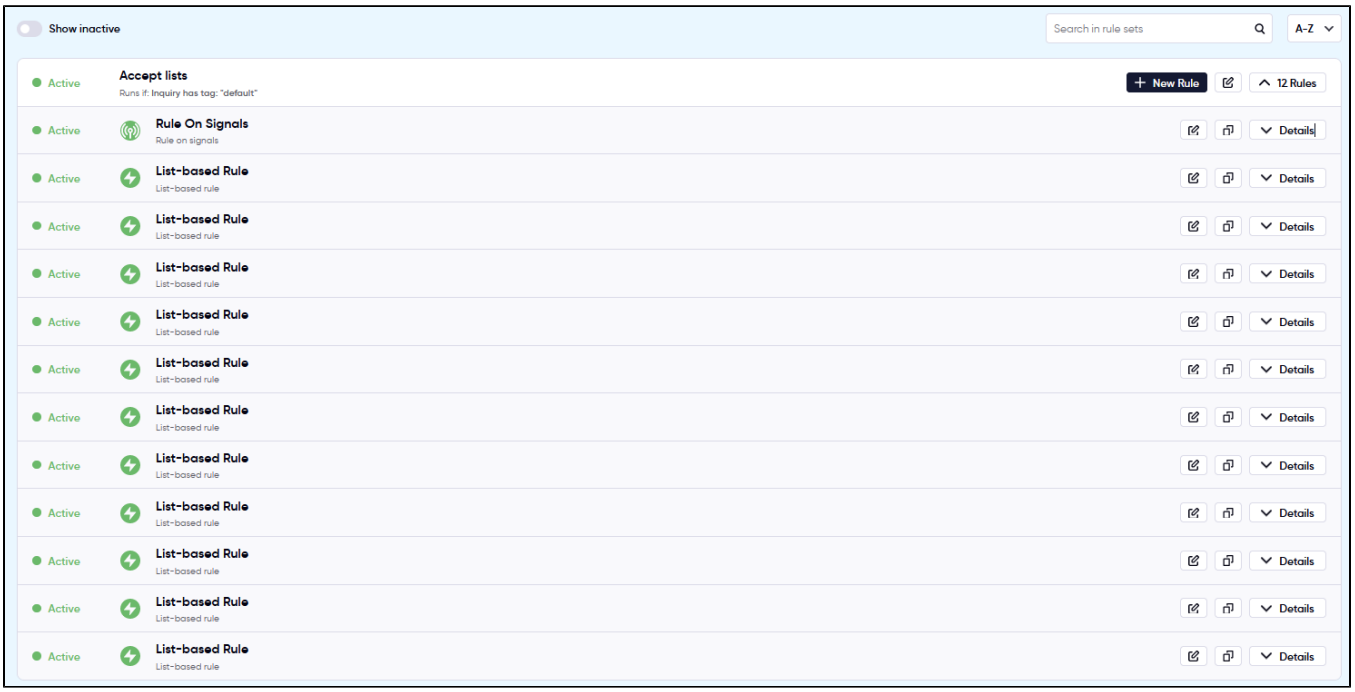
Ausführungsbedingungen sind einfache Selektoren, die angeben, wann der Regelsatz ausgeführt werden soll. Wenn Sie unterschiedliche Regelsätze für unterschiedliche Anwendungsfälle (z. B. verschiedene Länder, Herkunft) starten möchten, können Sie dies mit Selektoren tun. Sie basieren auf Tags, die einer Anfrage zugewiesen sind. Es gibt zwei Arten der Bedingungskonfiguration:

- "hat irgendeine" – erfüllt, wenn die Anfrage mit IRGENDEINEM der angegebenen Tags markiert ist
- "hat keine" – erfüllt, wenn die Anfrage mit KEINEM der angegebenen Tags markiert ist.

Ein Regelsatz wird ausgeführt, wenn alle auf Tags basierenden Bedingungen erfüllt sind.

Regelsatz-Details

Durch Drücken des Symbols mit der Anzahl der Regeln in einem bestimmten Regelsatz gelangen Sie direkt zur Regelsatzübersicht.



Die Ansicht zeigt eine Liste der in diesem Satz konfigurierten Regeln. Sie können die deaktivierten Regeln auch auf der Registerkarte „Deaktivierte Regeln" sehen. Beachten Sie, dass diese Regeln nicht ausgelöst werden.

Wenn Sie eine Regel ausprobieren möchten, können Sie sie auf „Simulationsmodus" einstellen. Das Regelsymbol wird grau. Die Regel wird ausgeführt, das Ergebnis der Regel wird jedoch bei der Berechnung des Endergebnisses nicht berücksichtigt.

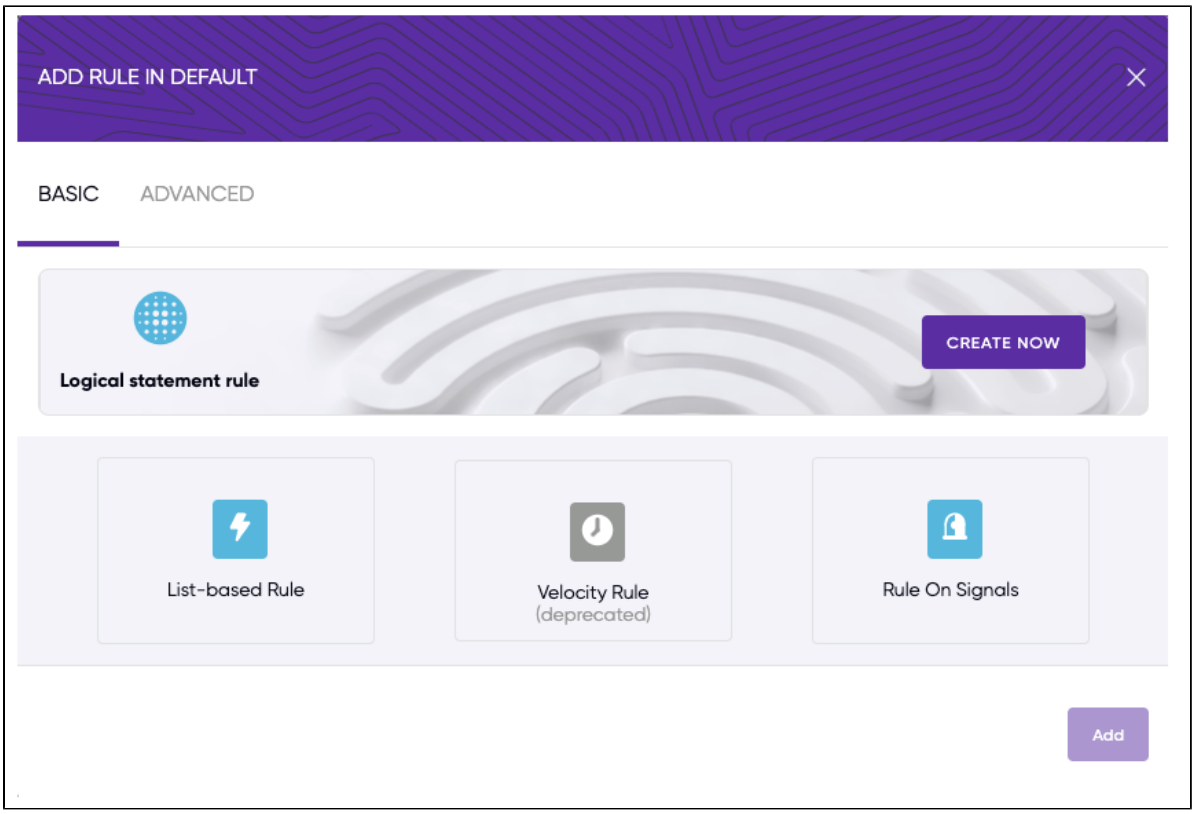
Sie können eine Regel bearbeiten, indem Sie darauf klicken oder mit der Schaltfläche „Regel hinzufügen" eine neue erstellen

Neue Regel hinzufügen

Der erste Schritt bei der Regelerstellung besteht darin, einen Regeltyp auszuwählen. Regeltypen werden in zwei Kategorien unterteilt: Einfach und Erweitert.

Die Gruppe „Einfach" enthält die am häufigsten verwendeten Regeltypen. Jeder dieser Typen verfügt über eine eigene, benutzerfreundliche Oberfläche.

Die Gruppe „Erweitert" enthält einen Katalog aller anderen im System verfügbaren Regeln. Diese Regeln haben Namen in einem technischen Format und die Bearbeitungsoberfläche basiert auf einem einfachen Texteditor.



Es gibt 4 Arten von einfachen Regeln:

- Regel für logische Anweisungen
- Listenbasierte Regel
- Geschwindigkeitsregel (veraltet)
- Regel bei Signal

Jede Regel kann eingestellt werden als:

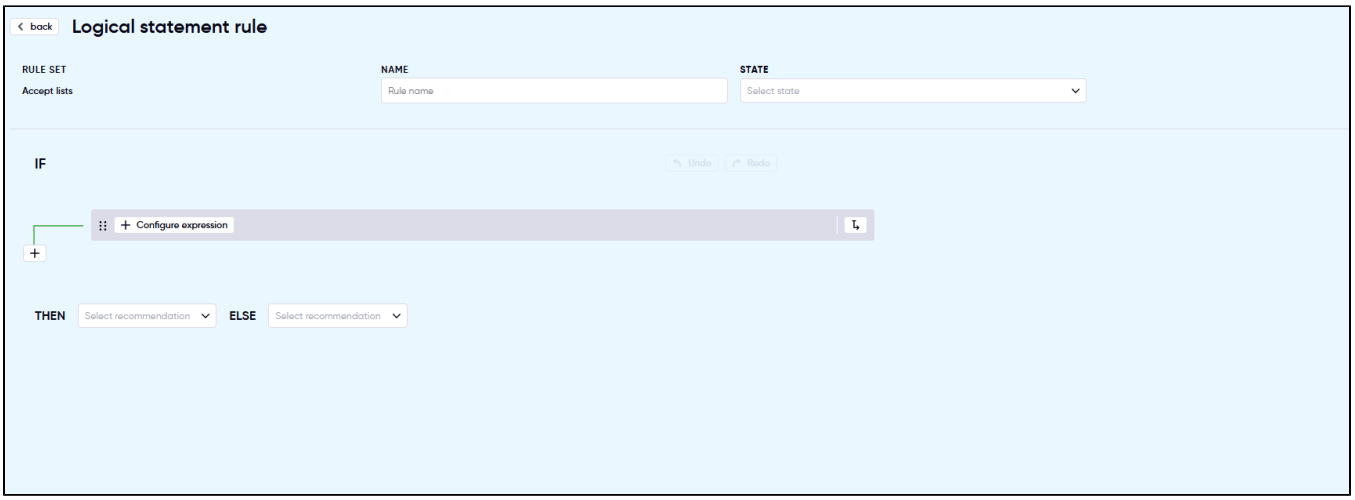
- Aktiv – die Regel wird ausgelöst und das Ergebnis beeinflusst das Endergebnis
- Inaktiv – die Regel wird nicht ausgelöst
- Simulation – die Regel wird ausgelöst, aber das Ergebnis beeinflusst das Endergebnis nicht.

Beachten Sie bitte, dass der Regelsatzstatus Vorrang vor einem einzelnen Regelstatus hat.

Regelsatz/Regel	Inaktiv	Aktiv	Simulation
Inaktiv	Inaktiv	Inaktiv	Inaktiv
Aktive	Inaktiv	Aktive	Simulation
Simulation	Inaktiv	Simulation	Simulation

Regel für logische Anweisungen

Klicken Sie auf „Jetzt erzeugen“, um den Generator für logische Anweisungsregeln zu öffnen. Mit diesem leistungsstarken Tool können Sie auf einfache Weise komplexe Ausdrücke erstellen. Sie können mehrere Ausdrücke mit logischen Operatoren verbinden: UND und ODER mit einer unbegrenzten Verschachtelungsebene.

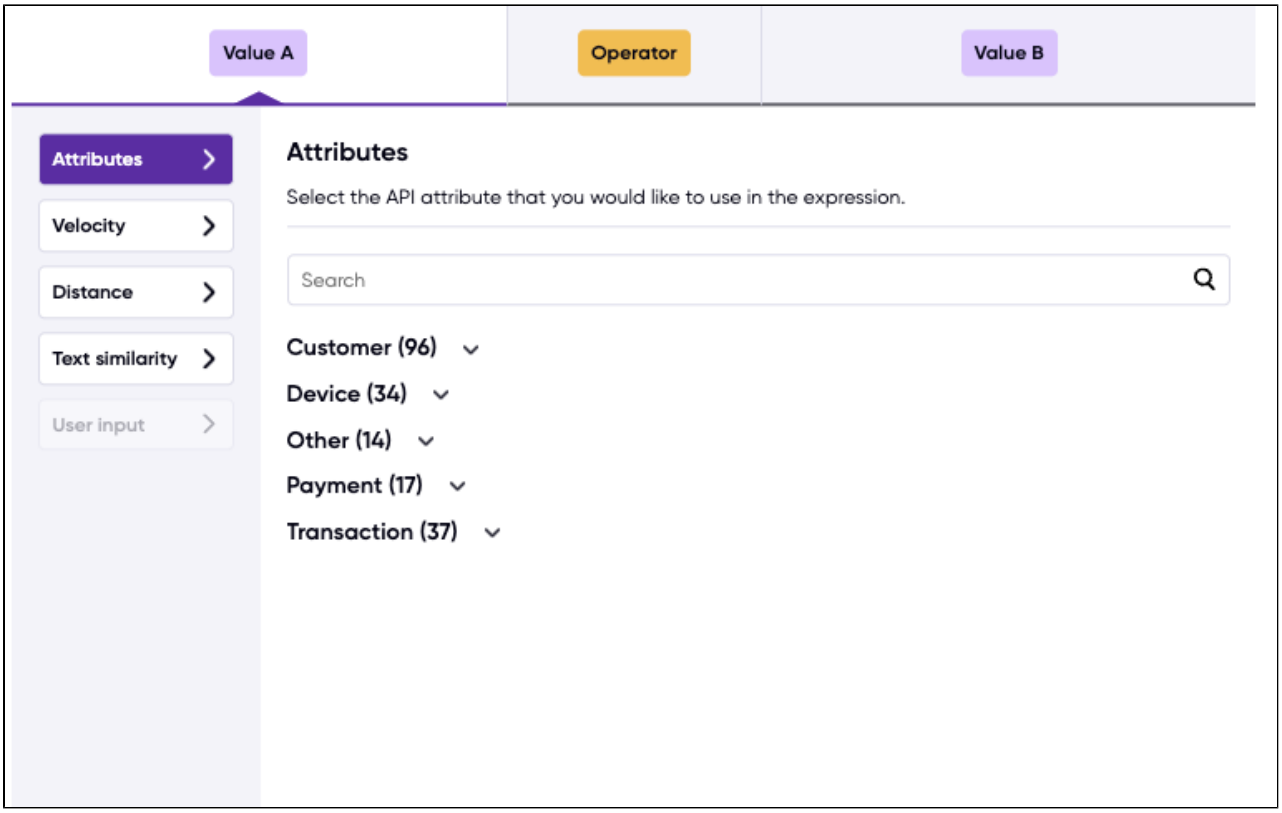


Schritt 1

Geben Sie den Regelnamen ein und wählen den Status aus

Schritt 2

Klicken Sie auf „Ausdruck konfigurieren“.



Schritt 3

Jeder Ausdruck besteht aus:

- Wert A
- Operator
- Wert B

Wert A

Die möglichen Elemente, die Sie unter Wert A eingeben können, sind:

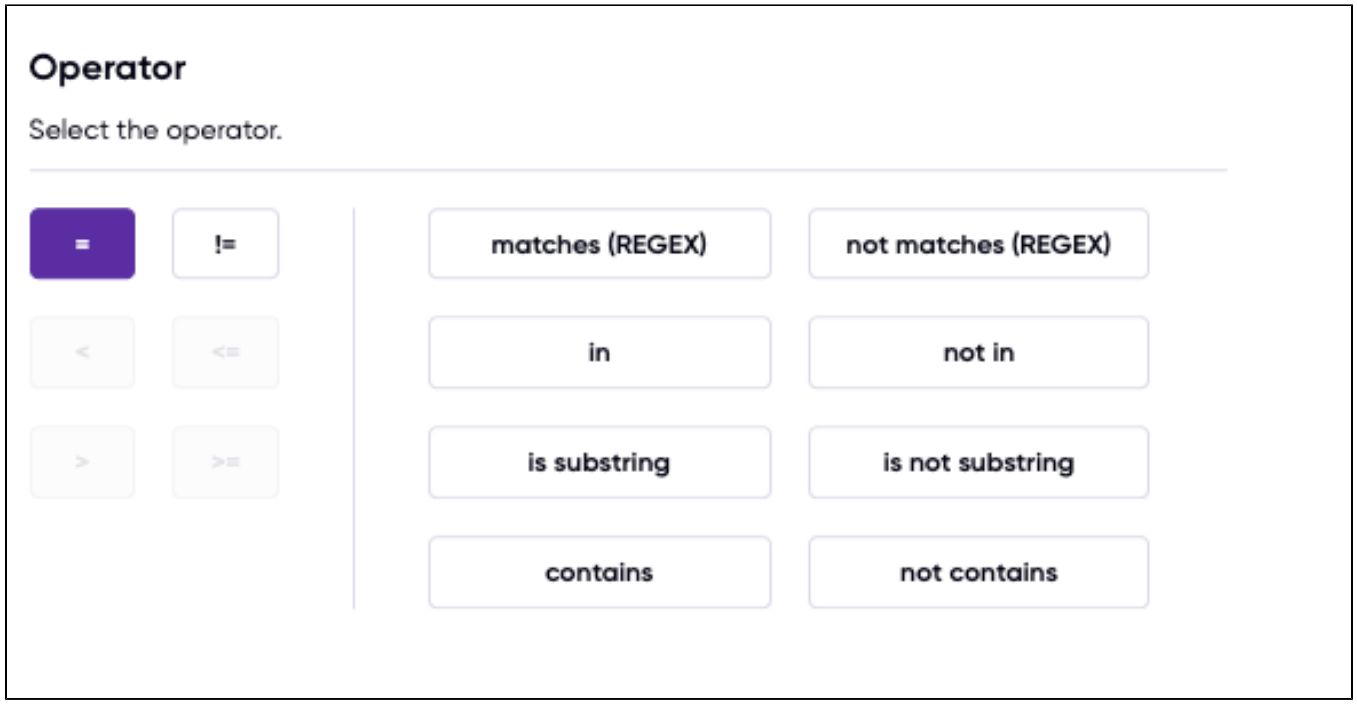
- **Attribute** – eines der Attribute, die das System von Ihnen über die Inquiry API-Integration erhält, z. B. Kunde/E-Mail
- **Geschwindigkeit** – eine Formel, mit der Sie z. B. die Anzahl der Anfragen oder den Transaktionsbetrag oder eine eindeutige BIN-Nummer usw. aus den Anfragen mit demselben Wert eines anderen Parameters, z. B. derselben IP, zählen können. Es ist auch obligatorisch, den Zeitrahmen zu definieren, z. B. in den letzten 24 Stunden. Optional können Sie zusätzliche Filter hinzufügen, die nur einen Teil der Anfragen in die Formel aufnehmen.
- **Entfernung** – wählen Sie 2 Attribute aus, die sich auf den Standort beziehen. Das System zählt die Differenz zwischen den Werten dieser Attribute.
- **Textähnlichkeit** – wählen Sie die Parameter aus, um das Ähnlichkeitsverhältnis zu überprüfen, das basierend auf Gestaltmustervergleich berechnet wird, wobei 0 keine Ähnlichkeit und 1 vollständige Ähnlichkeit bedeutet.

Wert B

Mögliche Elemente, die Sie unter Wert B eingeben können, variieren je nachdem, was als **Wert A** ausgewählt wurde. Sie können wählen aus:

- Attribute
- Benutzereingabe

Operator

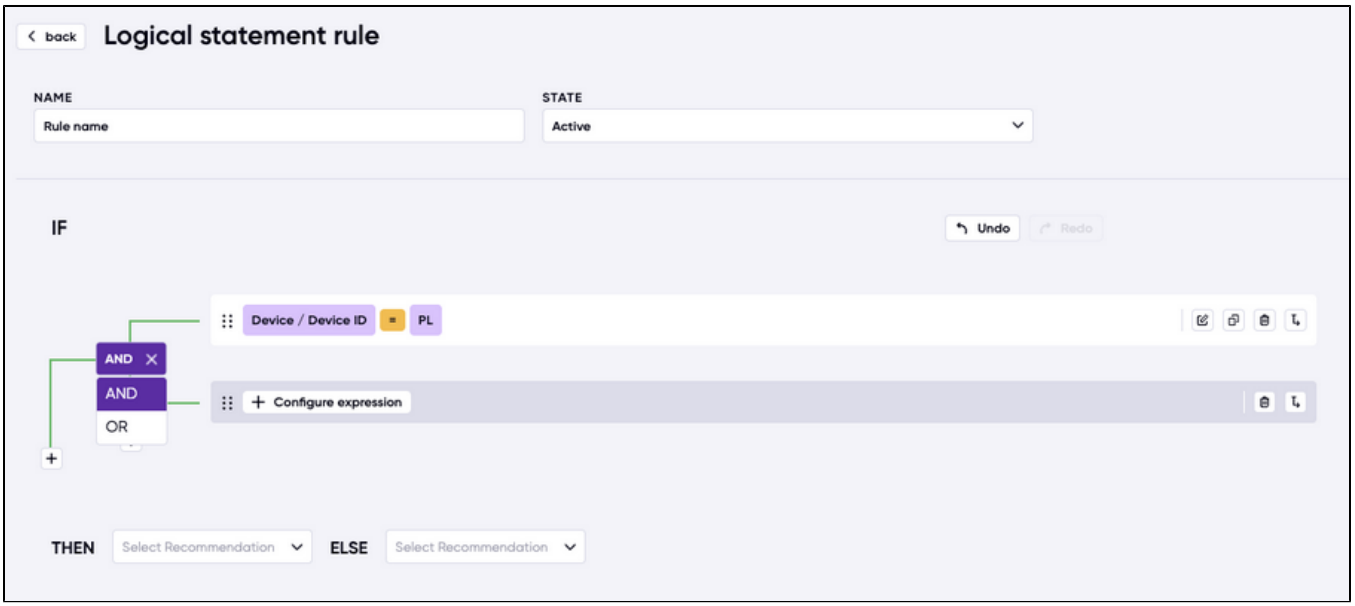


Die Operatoren, die für den Vergleich im Ausdruck verwendet werden, sind:

- Relationala Operatoren: **=**, **!=**, **<**, **<=**, **>**, **>=**
- **Übereinstimmungen (REGEX)** und **Nichtübereinstimmungen (REGEX)** – dieser Operator vergleicht den Wert des Attributs, das in Wert A ausgewählt wurde, mit der Eingabe, die Sie als Wert B angeben. Die Eingabe unter Wert B sollte das Format des regulären Ausdrucks beibehalten. Sie können Metazeichen verwenden:
    - **[ ]** – entspricht einem einzelnen Zeichen, das in den Klammern enthalten ist. Beispielsweise entspricht „[abc]“ „a“, „b“ oder „c“
    - **^** – markiert den Anfang der Zeichenfolge. Beispielsweise entspricht „^Com“ „Computop“
    - **$** – markiert den Anfang der Zeichenfolge. Beispielsweise entspricht „utop$“ „Computop“
    - **** – markiert das nächste Zeichen als Literal. Beispielsweise entspricht "\(" "("
    - ***** – entspricht dem vorhergehenden Zeichen null oder mehrmals. Beispielsweise entspricht "Compu*op" "Compuop" und "Computop"
    - **+** – entspricht dem vorhergehenden Zeichen ein oder mehrmals. Beispielsweise entspricht "Compu+op" "Computop" und "Computtop"
    - **?** – entspricht dem vorhergehenden Zeichen null oder einmal. Beispielsweise entspricht "Compu?op" "Compuop" und "Computop"
    - **.** – entspricht einem beliebigen einzelnen Zeichen
    - **|** – "a|b" entspricht "a" oder "b"
- **in** und **nicht in** – dieser Operator vergleicht den Wert des Attributs, das in Wert A ausgewählt wurde, mit den verschiedenen Eingaben, die Sie als Wert B angeben
- **ist Teilstring** und **ist nicht Teilstring** – dieser Operator prüft, ob der Wert des Attributs unter Wert A eine Teilzeichenfolge des Werts des Attributs oder der Benutzereingabe unter Wert B ist
- **enthält** und **enthält nicht** – dieser Operator prüft, ob der Wert des Attributs unter Wert A den Wert des Attributs oder die Benutzereingabe unter Wert B enthält

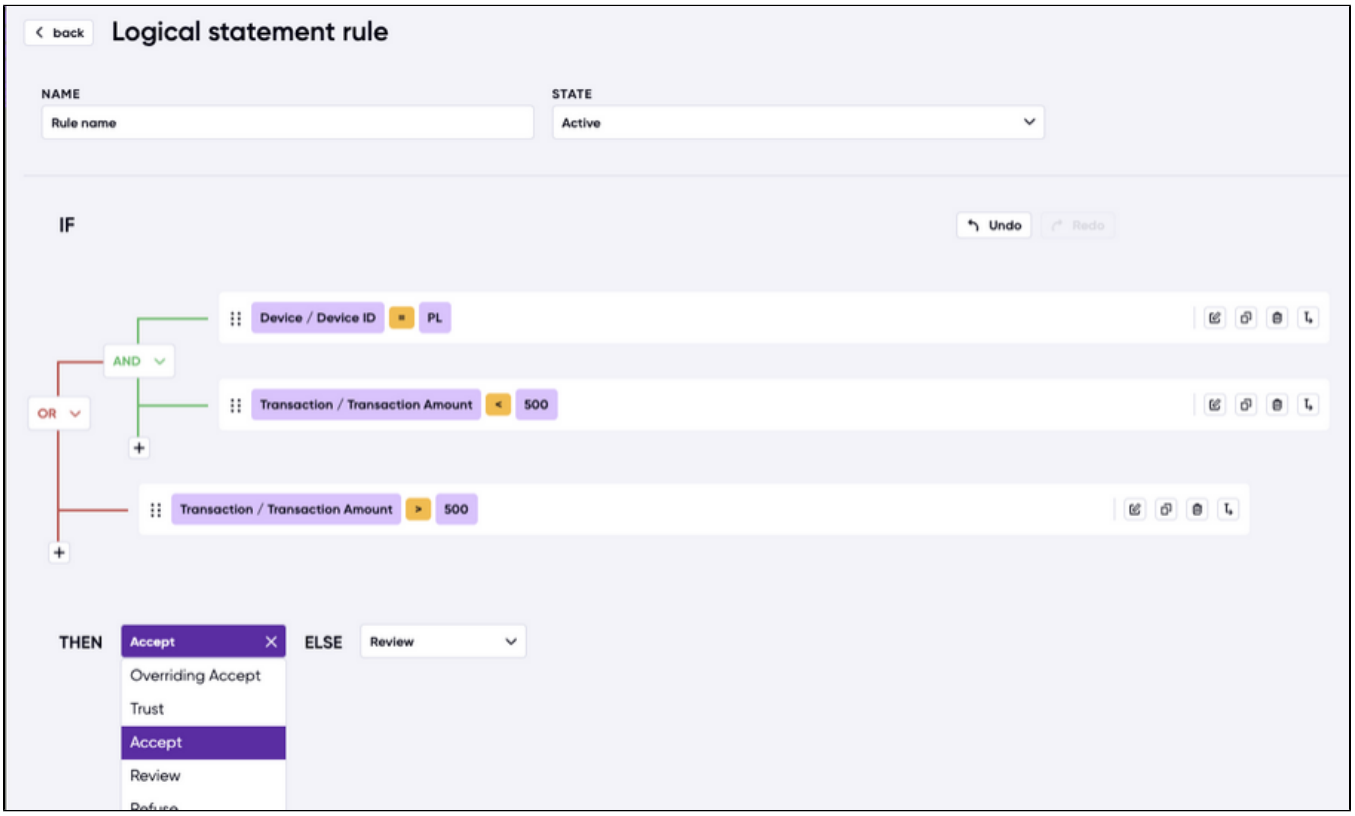
Schritt 4

Sobald Sie den Ausdruck erzeugt haben, können Sie einen weiteren hinzufügen. Sie können mehrere Ausdrücke mit logischen Operatoren verbinden: UND und ODER mit einer unbegrenzten Verschachtelungsebene, z. B.:



Schritt 5

Wählen Sie als letzten Schritt die Empfehlung aus, die ausgegeben werden soll, wenn alle Bedingungen der Regel erfüllt sind und was andernfalls passieren soll, z. B.:



Listenbasierte Regel

Um eine listenbasierte Regel zu konfigurieren, müssen Sie 3 Schritte ausführen:

Schritt 1: Abfrageattribute auswählen

Wählen Sie eines oder mehrere Attribute aus, nach denen in der Liste gesucht werden soll.

Schritt 2: Liste auswählen

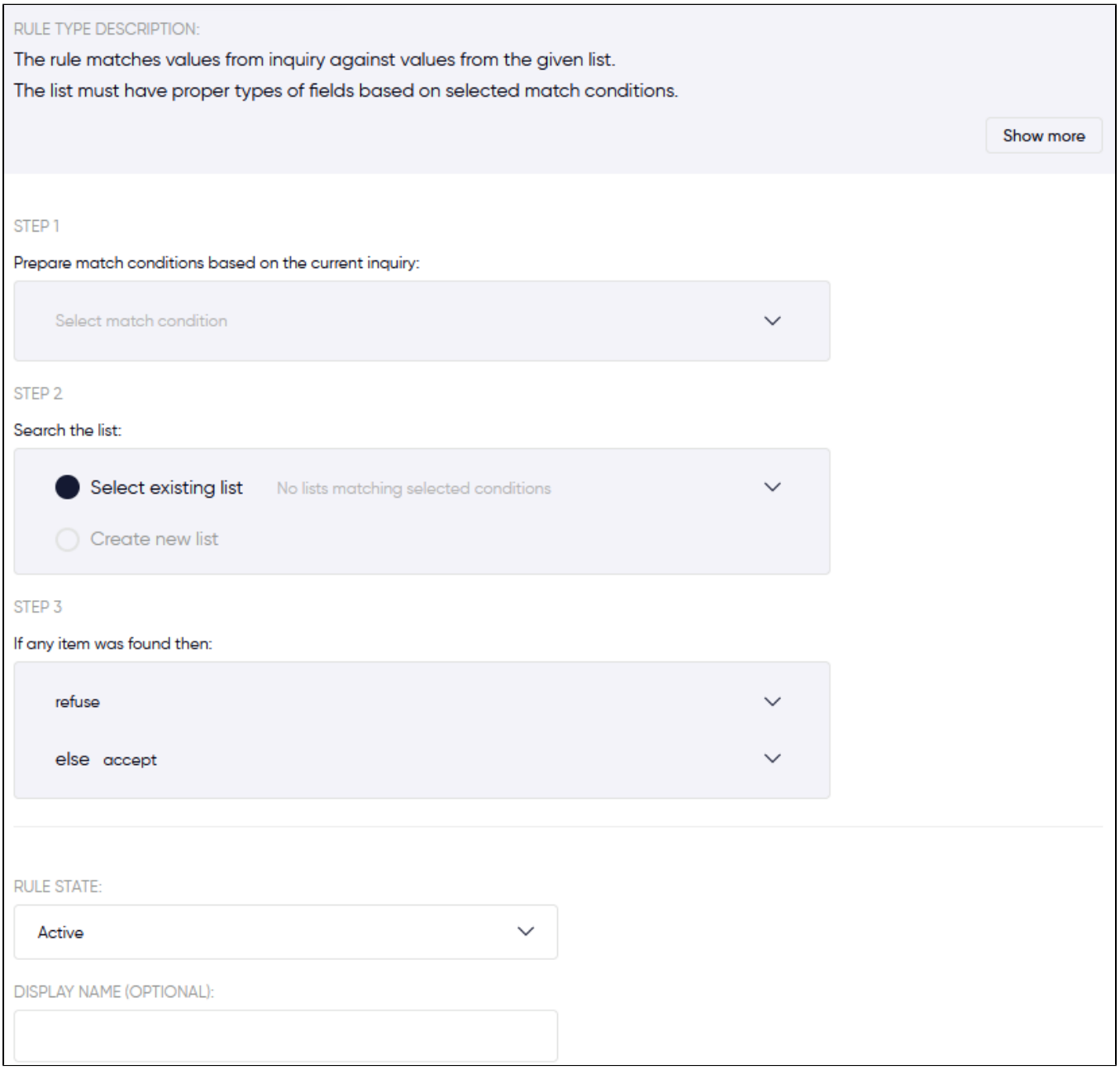
Wählen Sie eine vorhandene Liste aus oder erstellen eine neue. Die ausgewählte Liste muss eine gültige Struktur für die ausgewählten Übereinstimmungsbedingungen aufweisen.

Wenn Sie eine Liste anlegen, werden dieser automatisch dieselben Felder wie der Regel zugewiesen. Bestätigen Sie die Listenerstellung per Klick auf „Liste hinzufügen“. Der eindeutige Name der Liste wird validiert und die neu erzeugte Liste ausgewählt. Wenn der Name der Liste doppelt vorhanden ist, werden Sie aufgefordert, ihn zu ändern.

Wenn Sie beim Erstellen der Regel eine neue Liste erzeugt haben, wird die Liste in der Ansicht „Listen akzeptieren/ablehnen“ angezeigt.

Schritt 3: Ergebnis auswählen

Wählen Sie aus, was die Regel bei Übereinstimmung oder Nichtübereinstimmung zurückgeben soll. Dank dieser Funktion können Sie mehrere Szenarien mit nur einem Regeltyp erstellen.



Regel für Signale

Um eine Regel für Signale zu konfigurieren, müssen Sie 2 Schritte ausführen:

Schritt 1: Wählen Sie eines oder mehrere Profiler-Signale aus der Liste der verfügbaren Signale aus

Plattformunabhängige Signale

Name	Beschreibung
Tor-Netzwork	Tor ist eine Software zur anonymen Kommunikation. Durch die Nutzung von Tor wird es schwieriger, Internetaktivitäten auf den Benutzer zurückzuführen. Die Nutzung von Tor beim täglichen Surfen im Internet ist äußerst verdächtig.
Netzwerk-Adresse auf VPN-Blacklist	Die Netzwerkadresse erschien auf einer Liste bekannter VPNs. Dieses Signal zeigt an, dass die beobachtete IP-Adresse von einem VPN stammte; es sagt nicht aus, ob das VPN für Betrug verwendet wurde oder einen schlechten Ruf hat.
Netzwerkadresse eines Rechenzentrums	Die Netzwerkadresse scheint zu einem Rechenzentrum zu gehören.
Netzwerkadresse auf der Anonymisierer-Blacklist	Die Netzwerkadresse erschien auf einer möglichen Blacklist von Anonymisierern.
Netzwerkadresse auf der Bot-Blacklist	Die Netzwerkadresse erschien auf einer möglichen Bot-Blacklist.
Netzwerkadresse eines Server-Infrastrukturanbieters	Die Netzwerkadresse scheint einem Server-Infrastrukturanbieter zu gehören.
Mit VPN verbundene Netzwerkadresse	Die Netzwerkadresse bezieht sich auf VPN. Im angegebenen Netzwerk wurden einige Standorte beobachtet, die auf VPN hinweisen.
Netzwerkadresse im Zusammenhang mit Proxy	Die Netzwerkadresse ist mit dem Proxy verknüpft. Im angegebenen Netzwerk wurden einige Standorte beobachtet, die auf einen Proxy hinweisen.
Netzwerkadresse im Zusammenhang mit Apple Private Relay	Die Netzwerkadresse bezieht sich auf Apple Private Relay. Im angegebenen Netzwerk wurden einige Standorte beobachtet, die auf Apples Private Relay hinweisen.
keine Länderübereinstimmung	Es gibt eine Diskrepanz zwischen den aus den IP-Adressen ermittelten Ländern. Eine unterschiedliche Region könnte möglicherweise auf die Verwendung eines Proxys oder VPN hinweisen.
AnyDesk anhand der Netzwerkeigenschaften erkannt	Dieses Signal erkennt die AnyDesk-Nutzung basierend auf Netzwerkeigenschaften.

Web-Signale

Name	Beschreibung
Kein JavaScript	Der JavaScript -Code wurde heruntergeladen, er wurde jedoch nicht ausgeführt. Dies könnte bedeuten, dass JavaScript deaktiviert wurde.
Kein User-Agent	Es gab keinen User-Agent-Header. Alle Standardbrowser sollten ihn senden.
Keine Header	Mit der Anfrage wurden keine Header geschickt. Alle Standardbrowser sollten sie senden.
Unvollständige Daten	Es fehlten einige fehlende Datenteile. Das könnte durch eine schlechte Netzwerkverbindung oder durch eine extrem langsame Maschine verursacht worden sein. Es kann aber auch eine absichtliche Handlung sein.
Keine Plugins	Viele grundlegende Funktionen von Webbrowsern werden normalerweise als Plugins implementiert. Ein legitimer Browser sollte zumindest einige von ihnen haben. Das Gegenteil ist verdächtig.
Kein WebGL	Mit WebGL können Browser 2D- und 3D-Grafiken rendern. Es wird in Webdesign und Spielen häufig verwendet. WebGL ist vollständig in alle modernen Browser integriert, und es ist standardmäßig aktiviert.
Virtuelle Maschine	Eine virtuelle Maschine ist eine Nachahmung eines Computersystems. Das kann hilfreich sein, wenn jemand verschiedene Betriebssysteme auf demselben Computer ausführen muss. Virtuelle Maschinen werden jedoch von einem durchschnittlichen Web-Surfer nicht verwendet.

Virtuelle Maschine GPU	Eine virtuelle Maschine ist eine Nachahmung eines Computersystems. Das kann hilfreich sein, wenn jemand verschiedene Betriebssysteme auf demselben Computer ausführen muss. Virtuelle Maschinen werden jedoch von einem durchschnittlichen Web-Surfer nicht verwendet.
Mobile Emulation	Jemand gibt vor, ein mobiles Gerät zu verwenden. Tatsächlich ist das reale Gerät ein Desktop-Computer und das mobile Gerät wird gerade emuliert. Es ist eine gängige Technik des Identitätsverstecks.
User-Agent-Spoofing	Der User-Agent ist, wie sich ein Browser selbst vorstellt. Er enthält Informationen über das Betriebssystem, den Browser und manchmal sogar über das Gerätemodell. Daher ist das Spoofing vom User-Agent eine Möglichkeit, um eine Identifizierung zu vermeiden.
Kein Flash	Flash ist eine beliebte Multimedia-Plattform für die Herstellung von Animationen, Internetanwendungen oder Spielen. Einige Browser haben es standardmäßig aktiviert. Das Signal 'kein Flash' tritt nur auf, wenn der Browser standardmäßig Flash aktiviert hat, es jedoch absichtlich deaktiviert wurde.
Sprachfehlanpassung	An vielen Stellen im Browser gibt es Spracheinstellungen. Normalerweise sollten sie zueinander passen. Andernfalls ist dieses Signal vorhanden.
Zwischenablage für sensible Felder verwendet	Bei der Eingabe von Kreditkartendaten nimmt ein typischer Benutzer die Karte aus seiner Brieftasche und beginnt mit der Eingabe. Es ist ungewöhnlich, Daten zu kopieren, die als sensibel gekennzeichnet sind.
Zwischenablage für nicht-sensible Felder verwendet	Der Benutzer hat Daten wie Name oder Adresse in nicht-sensible Felder kopiert. Kriminelle kopieren häufig Basisdaten, um den Betrugsprozess zu beschleunigen.
Inkognito-Modus	"Inkognito-Modus" oder "Privates Browsen" sind Funktionen, die in den beliebtesten Browsern verfügbar sind. Sie deaktivieren das Durchsuchen von Historien und Web-Cache.
Tastatur nicht verwendet	Es wurden keine Tastaturereignisse aufgezeichnet. Das ist ungewöhnlich, denn selbst das Eingeben mit der Tastatur auf dem Bildschirm (z. B. auf mobilen Geräten mit Touchscreen) erzeugt Tastaturereignisse.
Nur positive Flugzeit	Die Flugzeit ist der Begriff, der das Intervall zwischen dem Loslassen einer Taste und dem Drücken einer anderen bezeichnet. Beim Tippen mit zwei Händen entstehen normalerweise zumindest einige negative Flugzeiten. Das Vorhandensein dieses Signals kann auf ein wirklich langsames Tippen oder die Verwendung automatisierter Skripte hinweisen.
Maus nicht verwendet	Es wurden keine Mausereignisse aufgezeichnet. Es sollte erwähnt werden, dass Aktionen auf Touchsbildschirmen wie Tippen und Schieben auch Mausereignisse ausgeben. Daher sind fehlende Mausereignisse verdächtig.
Keine Canvas-Schriftarten	Verschiedene Anwendungen und Betriebssysteme verwenden verschiedene Schriftsätze. Einige halten es für eine Bedrohung für ihre Privatsphäre und blockieren den Einsatz von nicht-grundlegenden Schriftarten. Andererseits verschlechtert das die Benutzererfahrung, sodass die Schriftblockierung für einen durchschnittlichen Benutzer ungewöhnlich ist.
Keine Berührungen auf dem Handy	Das Gerät sieht aus wie ein Mobiltelefon und sein User-Agent zeigt dies an, aber es gab keine Berührungsereignisse. Dies kann auf die Verwendung von Skripten hinweisen.
Übermittlung auf versteckter Seite	Als das Formular eingereicht wurde, war das entsprechende Browser-Tab oder das entsprechende Fenster nicht sichtbar. Dies kann auf die Verwendung von Skripten hinweisen.
Proxy verwendet	Ein Proxy-Server ist ein Server, der als Vermittler für Anfragen von Clients fungiert, die Ressourcen von anderen Servern suchen. Betrüger können Proxies verwenden, um ihre echte Netzwerkadresse zu verbergen.
Kein Origin	Dieses Signal zeigt eine Anomalie an, bei der der Origin-Header nicht vorhanden ist. Dies kann durch einen Bot verursacht werden.
Single-Core-CPU	Heute ist eine Single-Core-CPU in einem Desktop-PC oder mobilen Gerät sehr ungewöhnlich. Es könnte darauf hinweisen, dass eine virtuelle Maschine verwendet wird.
Keine Mime-Typen	MIME-Typen informieren über Arten von Dateien, die von Browser-Plugins unterstützt werden. Ein legitimer Browser sollte zumindest einige von ihnen haben. Das Gegenteil ist verdächtig.
Betrugswerkzeug verwendet	Betrüger erzeugen speziell gefertigte Tools, um Anti-Fraud-Systeme auszutricksen. Dieses Signal zeigt an, dass ein solches Tool versucht hat, das Verhalten des Browsers zu ändern.
Server-Betriebssystem	Dieses Signal zeigt an, dass bei diesem Versuch ein Serverklassensystem verwendet wurde. Kriminelle verwenden solche Systeme, um Betrug zu automatisieren.
Crawler-Aktivität	Bekanntes automatisches Tool wurde verwendet, um diesen Versuch zu erstellen.
Veralteter Browser	Heute verfügt jeder Browser über eine Auto-Update-Funktion, daher sind wirklich alte Versionen sehr ungewöhnlich. Es besteht eine hohe Gefahr, dass alte Browser schwerwiegende Sicherheitslücken haben, die bereits von Malware oder Botnets ausgenutzt wurden.

Betriebssystem-Nichtübereinstimmung	Es scheint, dass das Betriebssystem auf Netzwerkebene und Browserebene unterschiedlich aussieht. Es kann viele Gründe geben – mit einem Web-Proxy oder einem virtuellen privaten Netzwerk oder in einer virtuellen Maschine zu arbeiten – um nur die häufigsten zu erwähnen.
Netzwerk – User-Agent-Nichtübereinstimmung	Deklarationen von User-Agent und beobachtete Werten aus dem Netzwerk-Stack scheinen unterschiedlich zu sein.
WebRTC deaktiviert	WebRTC ist eine Funktion, die die Echtzeitkommunikation innerhalb des Browsers ermöglicht. Das Deaktivieren könnte verdächtig sein.
Plugins im Zusammenhang mit VM	Plugins, die auf die Verwendung von virtuellen Maschinen hinweisen können, wurden festgestellt.
Plugins im Zusammenhang mit VPN	Plugins, die auf die Verwendung von VPN hinweisen können, wurden festgestellt.
Plugins im Zusammenhang mit Malware	Es wurden Plugins erkannt, die auf Malware hinweisen können.
Anomalie der Bildschirmauflösung	Geräte berichten die Bildschirmauflösung in Pixel sowie die sogenannte verfügbare Auflösung als Menge des horizontal/vertikal verfügbaren Platzes für ein Fenster, was der Bildschirmauflösung abzüglich des verwendeten Platzes etwa für Leisten des Betriebssystems ist. Wenn die verfügbare Auflösung größer als die Bildschirmauflösung ist, ist das widersprüchlich zu den Definitionen.
WebGL-Anomalie	WebGL-Eigenschaften, die vom Browser zurückgegeben werden, sehen abnormal aus. Eine solche Situation kann z.B. durch Plugins zur Datenschutzverbesserung verursacht werden, die üblicherweise von Betrügern verwendet werden.
Leistungsmess-Anomalie	Die vom Browser gemeldeten Leistungsmetriken sehen ungewöhnlich aus. Dies kann bedeuten, dass der Browser in einem speziellen Anti-Fingerabdruck-Modus arbeitet oder Datenschutz-Plugins installiert wurde.
VPN-ähnliche Netzwerkeigenschaften	Netzwerkeigenschaften können auf die Verwendung von VPN hinweisen.
Falsche Systemzeit	Systemdatum und -zeit sind falsch. Es sollte automatisch eingerichtet werden. Daher zeigt dieses Signal manuelle Änderungen an.
Header – JavaScript User-Agent Deklarationsfehler	Die Deklaration des User-Agent in JavaScript stimmt nicht mit HTTP-Headern überein.
Ungewöhnlicher User-Agent	Deklarierter User-Agent ist ungewöhnlich. Es kann sich um ein ungewöhnliches Gerät handeln oder jemand versuchte, den User-Agent manuell zu ersetzen und hat den Wert falsch angegeben.
Offene Ports im Zusammenhang mit RDP	Auf diesem Computer erkannte offene Ports werden normalerweise vom Windows Remote Desktop Service verwendet. Dieses Protokoll hat Sicherheitslücken und wird von Betrügern häufig verwendet.
Offene Ports im Zusammenhang mit AnyplaceControl	Auf diesem Computer erkannte offene Ports werden normalerweise von der beliebten Remote-Desktop-Software namens AnyPlaceControl verwendet. Diese Anwendung wird manchmal von Betrügern verwendet, um auf einen gehackten Computer zuzugreifen.
Offene Ports im Zusammenhang mit VNC	Auf diesem Computer erkannte offene Ports werden normalerweise von der beliebten Remote-Desktop-Software namens VNC. Diese Anwendung wird manchmal von Betrügern verwendet, um auf einen gehackten Computer zuzugreifen.
Offene Ports im Zusammenhang mit TeamViewer	Auf diesem Computer erkannte offene Ports werden normalerweise von der beliebten Remote-Desktop-Software namens TeamViewer. Diese Anwendung wird manchmal von Betrügern verwendet, um auf einen gehackten Computer zuzugreifen. Team Viewer hat kürzlich 2 Milliarden Installationen auf Geräten auf der ganzen Welt überschritten, so dass dieses Signal in der Bevölkerung häufig auftreten kann.
Offene Ports im Zusammenhang mit AnyDesk	Auf diesem Computer erkannte offene Ports werden normalerweise von der beliebten Remote-Desktop-Software namens AnyDesk. Diese Anwendung wird manchmal von Betrügern verwendet, um auf einen gehackten Computer zuzugreifen.

Offene Ports Ports im Zusammenhang mit anderer Remote-Desktop-Software	Auf diesem Computer erkannte offene Ports werden normalerweise von der anderen beliebten Remote-Desktop-Software verwendet. Diese Art von Anwendungen wird manchmal von Betrügern verwendet, um auf einen gehackten Computer zuzugreifen.
Selenium-Nutzung erkannt	Selenium ist eines der beliebtesten Browser-Automatisierungswerkzeuge. Dieser Browser scheint von Selenium kontrolliert worden zu sein.
Automatisierter Browser	Browserautomatisierung wie z.B, durch Selenium hilft bei der Prüfung von Web-Apps oder bei der Ausführung von sich wiederholenden Aufgaben. Es könnte auch unerwünscht verwendet werden, z.B. zum automatischen Ausfüllen von Formularen mit gestohlenen Anmeldeinformationen.
Automatisierten Browser verstecken	Einige moderne Browser melden, dass automatisierte Tools sie mithilfe der integrierten Browser-API steuern. In diesem Fall wurde die oben genannte API manipuliert, um falsche Werte zu melden, die darauf hinweisen, dass ein automatisierter Browser nicht verwendet wurde.
Headless-Browser	Headless-Browser bieten automatisierte Steuerung einer Webseite in einer Umgebung, die den beliebten Webbrowsern ähnelt, jedoch ohne grafische Benutzeroberfläche. Sie waren für Testautomatisierung oder Website-Scraping gedacht. Andererseits werden sie häufig im Werbebetrug, bei DDoS-Angriffen oder zur Automatisierung von Websites (z. B. Ausfüllen von Formularen mit gestohlenen Anmeldeinformationen) auf unbeabsichtigte Weise verwendet.
Unstimmigkeiten der Zeitzone	Es gibt eine Diskrepanz zwischen den Zeiteinstellungen im Betriebssystem und der Zeitzone, die aus der IP-Adresse erhalten wurde. Das kann z.B. auf das Verwenden von VPN oder Proxy aus verschiedenen Regionen hindeuten.
Einhaken bei WebRTC	WebRTC ist ein Mechanismus, der die ursprünglichen IP-Adressen preisgeben kann, selbst wenn Sie ein VPN oder einen Proxy verwenden. Erfahreneren Betrügern ist diese Tatsache bekannt. Fälscher versuchen oft, Browsererweiterungen oder sogar spezielle Betrugsprogramme zu verwenden, um die WebRTC-Daten zu fälschen. Dieses Signal erkennt ein solches Verhalten.
Einhaken bei Mime-Typen	Mime-Typen informieren Sie über die Dateitypen, die von Browser-Plugins unterstützt werden. Ein legitimer Browser sollte zumindest einige davon haben. Sie werden häufig für einen Fingerabdruck vom Browser verwendet. Erfahreneren Betrügern ist diese Tatsache bekannt. Fälscher versuchen häufig, Browsererweiterungen oder sogar spezielle Betrugsprogramme zu verwenden, um Mime-Typ-Daten zu fälschen. Dieses Signal erkennt ein solches Verhalten.
Einhaken bei Bildschirmdaten	Bildschirmdaten enthalten verschiedene Informationen über Bildschirmeigenschaften – Breite, Höhe usw. Diese API wird häufig für Fingerabdruck-Zwecke verwendet, was einigen Betrügern bekannt ist. Diese Daten werden häufig durch Datenschutz-Plugins, spezielle Betrugstools oder verschiedene Arten von Bots gefälscht. Dieses Signal erkennt ein solches Verhalten.
Einhaken bei Plugins	In Browsern installierte Plugins werden häufig von Betrugsschutzsystemen verwendet, um Benutzer zu identifizieren. Erfahrenere n Betrügern ist diese Tatsache bekannt. Fälscher versuchen häufig, Browsererweiterungen oder sogar spezielle Betrugsprogramme zu verwenden, um Browser-Plugins zu fälschen. Dieses Signal erkennt ein solches Verhalten.
Einhaken bei der Storage-API	Ein typischer Browser bietet mehrere APIs, die zum Speichern von Informationen verwendet werden können. Betrugsbekämpfungssysteme verwenden APIs, um Informationen über die Identität eines Benutzers zu speichern. Erfahreneren Betrügern ist diese Tatsache bekannt. Fälscher versuchen häufig, Browsererweiterungen oder sogar spezielle Betrugsprogramme zu verwenden, um das Verhalten solcher APIs zu ändern und Betrugsbekämpfungs-Cookies zu entfernen. Dieses Signal erkennt ein solches Verhalten.
Einhaken bei der Inkognito-Erkennung	Fälscher verwenden den Inkognito-Modus, um von Betrugsschutzsystemen gespeicherte Cookies zu löschen. Einige Betrüger wissen, dass solche Systeme den Inkognito-Modus erkennen, und verwenden daher Browsererweiterungen oder sogar spezielle Betrugsprogramme, um das Verhalten der für diesen Zweck verwendeten APIs zu ändern. Dieses Signal erkennt solche Änderungen.
Einhaken bei der Geolokation	Betrugsbekämpfungssysteme verwenden Geolokalisierungsdaten aus verschiedenen Quellen, um verschiedene Inkonsistenzen zwischen dem Benutzerstandort und den vom Browser angegebenen Daten zu finden. Diese Inkonsistenzen sind oft ein Zeichen für die Verwendung von VPNs oder Proxys. Einige Betrüger sind sich dieser Tatsache bewusst und versuchen, mithilfe von Browsererweiterungen oder sogar speziellen Betrugsprogrammen das Verhalten solcher APIs zu ändern und solche Tatsachen zu verbergen. Dieses Signal erkennt solche Änderungen.
Einhaken bei der HTML-Objekterstellung	Betrugsbekämpfungssysteme verwenden häufig Verhaltensdaten, um Betrug aufzudecken. Einige Betrüger sind sich dessen bewusst und manipulieren die Browser-API, um das Betrugsbekämpfungssystem mit den falschen Daten zu füttern. Solche Manipulationen können mithilfe von Browsererweiterungen oder speziellen Betrugsbekämpfungstools durchgeführt werden. Auch einige Schadsoftware und Bots verwenden diese Technik. Dieses Signal erkennt solche Änderungen.
Einhaken bei der Zwischenablage	Die meisten Betrüger auf Anfängerniveau verwenden die Zwischenablage, um Karteninhaberdaten einzufügen. Einige fortgeschrittene Fälscher sind sich bewusst, dass dieses Verhalten von Betrugsbekämpfungssystemen überwacht wird, und versuchen, Browser-APIs zu manipulieren, um die Verwendung der Zwischenablage zu verbergen. Dieses Signal erkennt solche Änderungen.
Einhaken bei der allgemeinen Fingerabdruck-API	Betrugsbekämpfungssysteme verwenden verschiedene kleinere Browser-APIs, um Benutzer zu identifizieren. Erfahrenere Betrüger wissen das und versuchen, den Inhalt dieser APIs durch Browsererweiterungen oder sogar spezielle Betrugsprogramme zu ersetzen. Dieses Signal erkennt ein solches Verhalten.

Einhaken bei Webkit-spezifischer API	Browser basieren auf einer sogenannten Engine. Eine der vielen Browser-Engines ist Webkit. Der Chrome-Browser verwendet den Nachfolger von Webkit als eigene Engine. Einige beliebte Betrugstools basieren auf der Firefox-Engine (Gecko). Solche Tools müssen Anti-Fingerprint-Systeme täuschen, die eine andere Engine verwenden. Eine Möglichkeit dazu besteht darin, Browserfunktionen so zu manipulieren, dass sie wie ein anderer Browser aussehen. Dieses Signal erkennt solche Änderungen.
Einhaken bei Batterie-API	Browser liefern Informationen über den Akkustand des Geräts. Betrugsbekämpfungssysteme nutzen diese Funktion häufig, um Benutzer zu identifizieren. Erfahrenere Betrüger wissen das. Fälscher versuchen häufig, Browsererweiterungen oder sogar spezielle Betrugsprogramme zu verwenden, um die Ergebnisse dieser API zu fälschen. Dieses Signal erkennt ein solches Verhalten.
Einhaken bei HTML Canvas	HTML-Canvas-Fingerprinting ist eine der besten und beliebtesten Methoden, um Benutzer zu identifizieren. Fälscher sind sich dieser Technik sehr bewusst. Viele Browsererweiterungen oder sogar spezielle Betrugssoftware werden verwendet, um das Ergebnis eines solchen Fingerprintings zu manipulieren, kurz bevor es an das Betrugsbekämpfungssystem gesendet wird. Dieses Signal erkennt ein solches Verhalten.
Einhaken bei Gamepads-API	Browser liefern Informationen über Gamepads, die mit dem Gerät verbunden sind. Betrugsbekämpfungssysteme nutzen diese Funktion häufig, um Benutzer zu identifizieren. Erfahrenere Betrüger wissen das. Fälscher versuchen häufig, Browsererweiterungen oder sogar spezielle Betrugsprogramme zu verwenden, um die Ergebnisse dieser API zu fälschen. Dieses Signal erkennt ein solches Verhalten.
Einhaken bei Service Worker API	Service Worker sind spezialisierte JavaScript-Assets, die zur Verbesserung des Offline-Erlebnisses auf Websites verwendet werden. Fälscher versuchen häufig, Browsererweiterungen oder sogar spezielle Betrugsprogramme zu verwenden, um die Ergebnisse dieser API zu fälschen und sich als anderer Browser auszugeben. Dieses Signal erkennt ein solches Verhalten.
Einhaken bei Media API	Mithilfe der Media API können Mediengeräte wie Mikrofone, Kameras und Headsets aufgelistet werden, die an das Gerät angeschlossen sind. Betrugsbekämpfungssysteme verwenden diese Funktion häufig, um Benutzer zu identifizieren. Erfahrenere Betrüger wissen das. Fälscher versuchen häufig, Browsererweiterungen oder sogar spezielle Betrugsprogramme zu verwenden, um die Ergebnisse dieser API zu fälschen. Dieses Signal erkennt ein solches Verhalten.
Einhaken bei Kommunikations-API	Einige von Betrügern verwendete Tools versuchen, APIs zum Senden von Daten durch ihren eigenen Code zu ersetzen. Dadurch können sie das Senden bestimmter Daten ändern oder sogar stoppen. Dieses Signal erkennt ein solches Verhalten.
WebGL-Hooking	WebGL-Fingerabdrücke sind eine der besten und beliebtesten Möglichkeiten, um Benutzer zu identifizieren. Fälscher sind sich dieser Technik sehr bewusst. Viele Browser-Erweiterungen oder sogar dedizierte Betrugssoftware werden verwendet, um das Ergebnis eines solchen Fingerabdrucks zu manipulieren, kurz bevor es an das Anti-Fraud-System gesendet wird. Dieses Signal erkennt ein solches Verhalten.
WebGL-Spoofing	WebGL-Fingerabdrücke sind eine der besten und beliebtesten Möglichkeiten, um Benutzer zu identifizieren. Fälscher sind sich dieser Technik sehr bewusst. Viele Browser-Erweiterungen oder sogar dedizierte Betrugssoftware werden verwendet, um das Ergebnis eines solchen Fingerabdrucks zu manipulieren, kurz bevor es an das Anti-Fraud-System gesendet wird. Dieses Signal erkennt ein solches Verhalten und konzentriert sich auf die anspruchsvollsten Tools.
HTML Canvas-Spoofing	HTML Canvas-Fingerabdrücke sind eine der besten und beliebtesten Möglichkeiten, um Benutzer zu identifizieren. Dieses Signal reagiert empfindlich gegenüber gängigen Fingerabdruck-Schutztechniken, wie sie im Firefox Resistfingerprinting-Modus oder dem Brave Fingerabdruckschutzmodus verwendet werden, es kann aber auch die Verwendung von anonymisierenden Browser-Erweiterungen und Betrugswerkzeugen indizieren.
Cookies deaktiviert	Anti-Fraud-Systeme speichern Informationen über die Identität eines Benutzers in seinem Browser mit Cookies. Fälscher möchten möglicherweise den Cookie-Mechanismus vollständig deaktivieren, um die Verfolgung zu verhindern. Für den ordnungsgemäßen Betrieb der Websites werden jedoch Cookies benötigt, sodass legitime Nutzer sie nicht deaktivieren.
Verhaltensmuster sieht aus wie TeamViewer	Geräte- und Verhaltensdaten geben an, dass TeamViewer verwendet wird. TeamViewer kann von Betrügern verwendet werden, um auf einen Computer aus der Ferne zuzugreifen. Das ist oft mit Social-Engineering-Angriffen verbunden.
Einhaken beim User-Agent	Der User-Agent ist eine charakteristische Zeichenfolge, mit der Server und Netzwerk-Peers die Anwendung, das Betriebssystem, den Anbieter usw. identifizieren können. AntiFraud-Systeme verwenden diese Eigenschaft häufig als Fingerabdruck für Benutzer. Sowohl Betrüger als auch Programmierer von Bots sind sich dessen bewusst und versuchen oft, dieses Feld zu manipulieren. Die ses Signal erkennt ein solches Verhalten.
Einhaken bei Anbieterinformationen	Der Anbieter-Feld enthält Informationen zum Hersteller des Browsers. Anti-Fraud-Systeme verwenden diese Eigenschaft häufig als Fingerabdruck für Benutzer. Sowohl Betrüger als auch Programmierer von Bots sind sich dessen bewusst und versuchen oft, dieses Feld zu manipulieren. Dieses Signal erkennt ein solches Verhalten.
Einhaken bei der App-Version	Das Feld der App-Version enthält Informationen zur Version des Browsers. Anti-Fraud-Systeme verwenden diese Eigenschaft häufig als Fingerabdruck für Benutzer. Sowohl Betrüger als auch Programmierer von Bots sind sich dessen bewusst und versuchen oft, dieses Feld zu manipulieren. Dieses Signal erkennt ein solches Verhalten.
Einhaken bei Betriebssysteminformationen	Diese Eigenschaft enthält Versionsinformationen zum Browser. Anti-Fraud-Systeme verwenden diese Eigenschaft häufig als Fingerabdruck für Benutzer. Sowohl Betrüger als auch Programmierer von Bots sind sich dessen bewusst und versuchen oft, dieses Feld zu manipulieren. Dieses Signal erkennt ein solches Verhalten.
Einhaken beim Plattformtyp	Das Plattformfeld enthält Informationen über das Betriebssystem und die CPU-Architektur. Anti-Fraud-Systeme verwenden diese Eigenschaft häufig als Fingerabdruck für Benutzer. Sowohl Betrüger als auch Programmierer von Bots sind sich dessen bewusst und versuchen oft, dieses Feld zu manipulieren. Dieses Signal erkennt ein solches Verhalten.

User-Agent inkonsistent	Der Wert User-Agent wurde manipuliert. Verschiedene Informationsquellen zum User-Agent zeigen unterschiedliche Werte an.
Geräteparameter inkonsistent	Werte der Geräteparameter wurden manipuliert. Verschiedene Informationsquellen zu Geräteparametern zeigen unterschiedliche Werte an.
Bevorzugte Sprache inkonsistent	Die am meisten bevorzugte Sprache wurde manipuliert. Verschiedene Informationsquellen über die am meisten bevorzugte Sprache zeigen unterschiedliche Werte an.
Sprachen inkonsistent	Vom Benutzer bevorzugte Sprachen wurden manipuliert. Verschiedene Informationsquellen zu bevorzugten Sprachen geben unterschiedliche Werte an.
Datenschutz-Erweiterung	Ein Muster im Zusammenhang mit einer Datenschutz-Erweiterung wurde in den Daten entdeckt. Da nicht alle Erweiterungen charakteristische Muster hinterlassen, werden nicht alle Erweiterungen festgestellt.
Einhaken beim Verstecken des automatisierten Browsers	Einige moderne Browser melden, dass sie automatisierte Tools mithilfe der integrierten Browser-API steuern. In diesem Fall wurde die oben genannte API manipuliert, um falsche Werte zu melden, die darauf hinweisen, dass ein automatisierter Browser nicht verwendet wurde.
WebRTC privater Modus	Mit der WebRTC-Technologie können Anti-Fraud-Systeme Situationen erkennen, in denen eine profilierte Person einen Proxy oder VPN verwendet, indem sie ihre IP-Adressen verlassen. Einige Betrüger sind sich dieser Tatsache bewusst und verwenden den privaten Modus von WebRTC, um diese Lecks zu verhindern. Dieses Signal erkennt den oben genannten privaten Modus von WebRTC.
Nichtübereinstimmung der Browser-Version	Die im User-Agent deklarierte Browserversion stimmt nicht mit der aus den Daten identifizierten Version überein. Dies kann bedeuten, dass der Benutzer die wahre Version des Browsers verbirgt oder Browserfunktionen durch den Benutzer aktiviert /deaktiviert.
Einhaken bei Zeitzonen	Anti-Fraud-Systeme verwenden häufig die Zeitzone, um Proxys oder VPNs zu erkennen. Betrüger und Bot-Programmierer kennen diese Tatsache und versuchen oft, dieses Feld zu manipulieren. Dieses Signal erkennt ein solches Verhalten.
Einhaken bei Zeit-API	Dieses Signal erkennt Manipulationen mit verschiedenen Browser-APIs, die Uhrzeit oder Datum berichten. Anti-Fraud-Systeme verwenden diese Felder, um Informationen über das Verhalten von Benutzern auf der Website zu sammeln, zum Beispiel das Timing des Tastenanschlags.
Verdächtiges mobiles Verhalten	Betrüger verwenden Remote-Desktop-Tools, um viele Betrugstechniken zu verwenden, beispielsweise: Kontoübernahme, Imitieren von Handlungen oder Trick-Opfer, um andere schädliche Handlungen auszuführen. Betrüger verwenden Remote-Desktop-Tools, Simulatoren und Emulatoren, um so zu handeln, als würden sie einen mobilen Browser verwenden.
Inkonsistentes mobiles Verhalten	Betrüger verwenden Remote-Desktop-Tools oder andere schädliche Programme, um Kontoübernahmen durchzuführen oder das als Aktion eines anderen auszugeben. Dieses Signal erkennt diese Techniken anhand von Verhaltensdaten.
Netzwerk als Proxy eingestuft	Erkannte Merkmale im Netzwerkverkehr, die üblicherweise mit der Proxy-Verwendung verbunden sind.
Netzwerk als VPN eingestuft	Erkannte Merkmale im Netzwerkverkehr, die üblicherweise mit der VPN-Verwendung verbunden sind.
Software-Renderer	Manchmal lädt die GPU Treiber nicht oder ist im System nicht vorhanden. Dann erfolgt ein Fallback-Mechanismus zum Software-Renderer. Dies kann entweder auf eine virtuelle Maschine oder eine schlecht konfigurierte Workstation hinweisen - insbesondere wenn jemand bei der automatischen Einrichtung der Maschinen, eines Emulators oder nur einem Problem mit dem GPU-Treiber nicht auf solche Details achtet. Einige dieser Fälle sind direkt mit der Aktivität von Bots und Betrügern verbunden.

iOS-Signale

Name	Beschreibung
Emulator	Das verwendete Gerät scheint ein Emulator anstatt eines echten Mobiltelefons oder Tablets zu sein.
Jailbreak	Das Gerät scheint einen Jailbreak zu haben. Das bedeutet, dass die von Apple auferlegten Softwarebeschränkungen vom Benutzer aufgehoben wurden. Dadurch kann Software installiert werden, die im App Store nicht verfügbar ist und für betrügerische Aktivitäten verwendet werden kann.
Kurze Betriebszeit	Die Betriebszeit ist kurz. Das bedeutet, dass das Gerät erst vor kurzem eingeschaltet wurde. Betrüger wechseln häufig die SIM-Karten in ihren Geräten und führen einen Hard-Reset durch, um alle Kennungen zu löschen.
Debugger	Die Anwendung scheint im Debug-Modus zu laufen. Debuggen hilft Programmierern, die Qualität ihres Codes zu verbessern, normale Benutzer sollten es jedoch niemals verwenden.

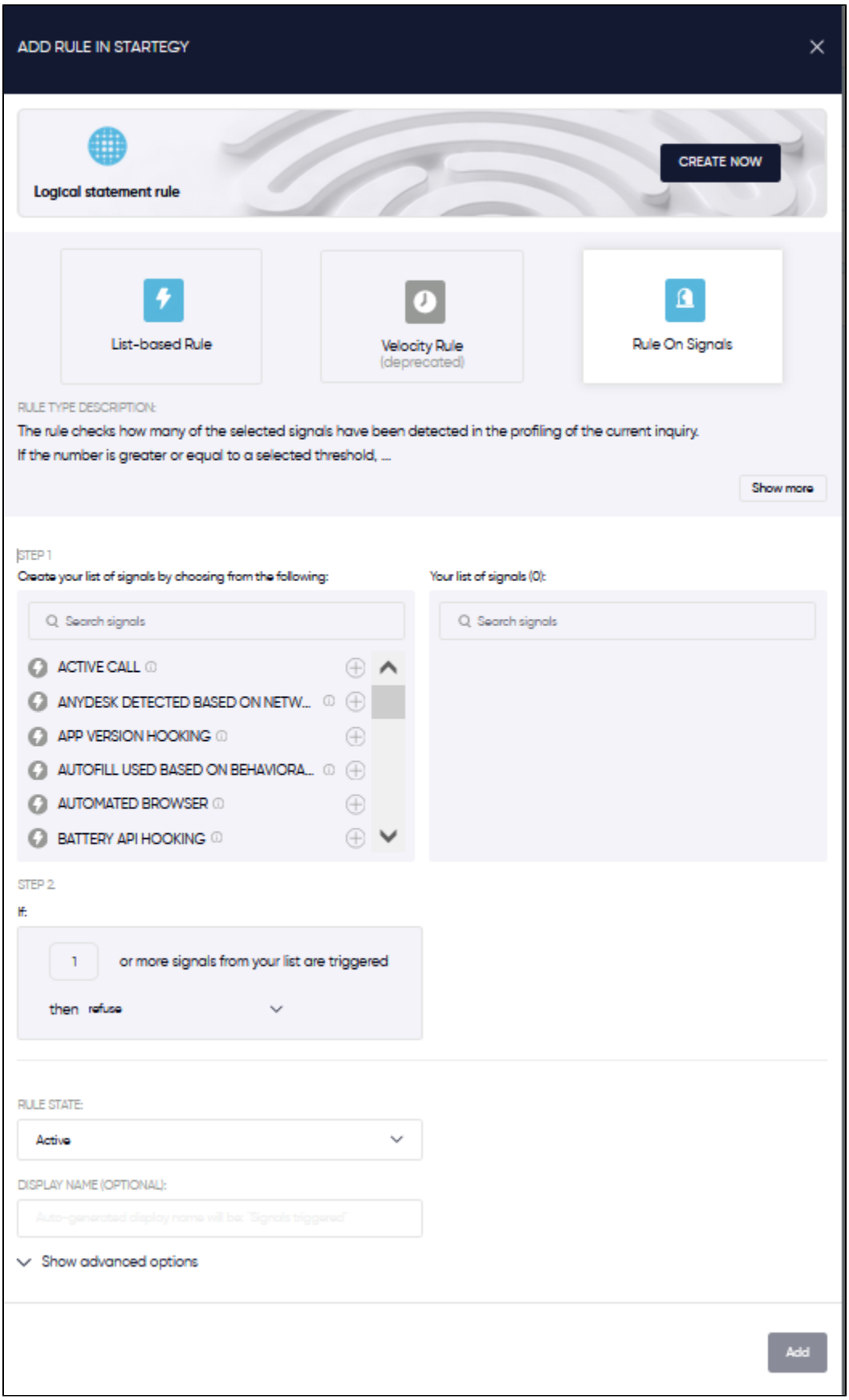
Software zum Verbergen von Jailbreaks	Auf dem Gerät des Benutzers wurde Software zum Verbergen eines Jailbreaks erkannt. Jailbreak bedeutet, dass der Benutzer die von Apple auferlegten Softwarebeschränkungen aufgehoben hat. Dies ist häufig für die Installation von Drittanbieteranwendungen erforderlich, die für verschiedene betrügerische Aktivitäten verwendet werden. Dieses Signal bedeutet, dass jemand versucht, diese Tatsache zu verbergen.
Hooking-Software	Auf dem Gerät des Benutzers wurde Hooking-Software erkannt. Diese Software ermöglicht die Manipulation der Anwendungsausführung, beispielsweise das Umgehen von Sicherheitsmaßnahmen oder das Vortäuschen von Daten.
GPS-Spoofing-Software	Auf dem Gerät des Benutzers wurde GPS-Spoofing-Software erkannt.
In-App-Kauf nicht autorisierter Software	Auf dem Gerät des Benutzers wurde nicht autorisierte In-App-Kaufsoftware erkannt. Mit dieser Software kann das In-App-Kaufsystem von Apple gehackt und umgangen werden, wodurch der Benutzer eine Bedrohung darstellen kann.
Nicht autorisierte App-Installationssoftware	Auf dem Gerät des Benutzers wurde nicht autorisierte Software zur App-Installation erkannt. Mit dieser Software können modifizierte Versionen der Anwendung oder im AppStore verbotene Anwendungen installiert werden.
Geringe Speicherplatznutzung	Die Speicherplatznutzung ist sehr gering. Dies kann ein Zeichen dafür sein, dass das Gerätesystem neu installiert wurde. Betrüger bereinigen ihre Geräte häufig, um Fingerprinting zu vermeiden.
Bildschirmaufnahme	Während der Profilerstellung wurde eine Bildschirmaufnahme erkannt. Die Bildschirmaufnahmefunktion wird während der Bildschirmaufzeichnung und von Anwendungen wie TeamViewer QuickSupport verwendet, die bei betrugsbezogenen Aktivitäten eingesetzt werden können.
Zeitzonen stimmen nicht überein	Es besteht eine Diskrepanz zwischen den Zeiteinstellungen im Betriebssystem und der aus der IP-Adresse ermittelten Zeitzone. Dies kann beispielsweise auf die Verwendung eines VPN oder Proxys aus einer anderen Region hinweisen.
Virtuelle Netzwerkschnittstellen auf dem Gerät	Auf dem Gerät des Benutzers wurden virtuelle Netzwerkschnittstellen erkannt.
Aktiver Anruf	Während der Profilerstellung wurde ein aktiver Anruf erkannt
Akku geladen und eingesteckt	Das Laden eines vollständig aufgeladenen Geräts während der Profilerstellung kann darauf hinweisen, dass dieses Gerät Teil einer Gerätefarm ist.
Offene Ports im Zusammenhang mit Frida	Die auf diesem Gerät erkannten offenen Ports können auf die Verwendung einer beliebten Hooking-Software namens Frida hinweisen. Diese Anwendung wird verwendet, um das Verhalten der Anwendung dynamisch zu ändern, was von Betrügern verwendet werden könnte.
Offene Ports im Zusammenhang mit Needle	Die auf diesem Gerät erkannten offenen Ports können auf die Verwendung einer beliebten Hooking-Software namens Needle hinweisen. Diese Anwendung wird verwendet, um das Verhalten der Anwendung dynamisch zu ändern, was von Betrügern verwendet werden könnte.
Offene Ports im Zusammenhang mit SSH	Offene Ports auf diesem Computer können auf die Verwendung eines SSH-Protokolls hinweisen. Dieses Protokoll wird zur Fernsteuerung des Geräts verwendet und könnte von Betrügern verwendet werden.
Keine nennenswerte Gerätebewegung	Während der Profilerstellung wurde keine nennenswerte Gerätebewegung beobachtet
Keine SIM-Karte oder nicht konfiguriert	Das Gerät hat keine physische SIM-Karte oder die Konfiguration der Mobilfunkfunktionen wie SMS ist nicht abgeschlossen.
Proxy-Konfiguration auf dem Gerät	Auf dem Gerät des Benutzers wurde eine Proxy-Konfiguration erkannt. Betrüger verwenden Proxys, um ihre wahre IP-Adresse zu verbergen, was es schwierig macht, sie zu verfolgen und zu identifizieren.
Zwischenablage für sensible Felder verwendet basierend auf Verhaltensdaten	Ein Signal, das auf Grundlage der Verhaltensdaten des Benutzers und seiner Interaktion mit der Anwendung und sensiblen Textfeldern ausgelöst wird
Zwischenablage für nicht sensible Felder verwendet basierend auf Verhaltensdaten	Ein Signal, das auf Grundlage der Verhaltensdaten des Benutzers und seiner Interaktion mit der Anwendung und nicht-sensiblen Textfeldern ausgelöst wird
Autofill verwendet basierend auf Verhaltensdaten	Ein Signal, das auf Grundlage der Verhaltensdaten des Benutzers und seiner Interaktion mit der Anwendung und den Textfeldern generiert wird

Android-Signale

Name	Beschreibung
Emulator	Das verwendete Gerät scheint ein Emulator anstatt eines echten Mobiltelefons oder Tablets zu sein.

Kurze Betriebszeit	Die Betriebszeit ist kurz. Das bedeutet, dass das Gerät erst vor kurzem eingeschaltet wurde. Betrüger wechseln häufig die SIM-Karten in ihren Geräten und führen einen Hard-Reset durch, um alle Kennungen zu löschen.
Rooten	Beim Rooten erhalten Benutzer von Smartphones, Tablets und anderen Geräten mit dem mobilen Betriebssystem Android privilegierte Kontrolle über verschiedene Android-Subsysteme. Rooten ermöglicht das Ändern von Systemeigenschaften, das Überschreiben von Dateien im Verzeichnis /system, das erneute Einbinden von Partitionen usw.
Anwendung zum Verbergen des Rootens	Auf dem Gerät wurde eine Anwendung erkannt, die versucht, das Rooten zu verbergen. Diese Apps können das Rooten verbergen, ohne es zu deaktivieren. Sie verbergen Superuser-Binärdateien, von Root ausgeführte Prozesse und vieles mehr. Dazu können sie ein Hooking-Framework verwenden.
Anwendung, die Root-Berechtigungen erfordert	Auf dem Gerät wurde eine Anwendung erkannt, die Root-Zugriff benötigt (vollständig oder nur teilweise – z. B. wären bestimmte Funktionen ohne Root nicht verfügbar). Einige der Apps ermöglichen das Ändern von Systemeigenschaften, das erneute Bereitstellen von Verzeichnissen, Flashen der benutzerdefinierten Wiederherstellung usw.
Anwendung für Fernzugriff	Diese Tools ermöglichen die Steuerung des PCs oder Mobilgeräts von einem anderen Gerät aus, die Erfassung und Aufzeichnung von Bildschirmaktivitäten sowie die Übertragung von Dateien. Dieses Signal bezieht sich nur auf den Fall des mobilen Fernzugriffs von einem anderen Gerät oder PC aus. Dieses Signal informiert darüber, dass eines dieser Tools auf dem Gerät installiert ist, was nicht unbedingt bedeutet, dass es während der Profilerstellung verwendet wurde.
Zeitzonen stimmen nicht überein	Es besteht eine Diskrepanz zwischen den Zeiteinstellungen im Betriebssystem und der aus der IP-Adresse ermittelten Zeitzone. Dies kann beispielsweise auf die Verwendung eines VPN oder Proxys aus einer anderen Region hinweisen.
Virtuelle Netzwerkschnittstellen auf dem Gerät	Netzwerkeinstellungen, die angeben, dass VPN verwendet wird.
Akku geladen und eingesteckt	Das Laden eines vollständig aufgeladenen Geräts während der Profilerstellung kann darauf hinweisen, dass dieses Gerät Teil einer Gerätefarm ist.
Keine SIM-Karte	Es kommt selten vor, dass normale Benutzer ein Telefon ohne SIM-Karte besitzen. Betrüger hingegen verwenden möglicherweise echte Geräte (um nicht als Emulatoren erkannt zu werden) und machen sich nicht die Mühe, eine SIM-Karte zu kaufen, da das Gerät nicht zum Telefonieren verwendet wird.
Erster Start	Dies zeigt den ersten Start nach dem Zurücksetzen auf Werkseinstellungen an. Betrüger verwenden das Zurücksetzen auf Werkseinstellungen häufig, um alle Kennungen und andere Daten zu löschen, die zur Identifizierung des Geräts verwendet werden können.
Präsentationsdisplay	Auf dem Gerät wurde mindestens ein Präsentationsdisplay gefunden. Ein solches Display kann verwendet werden, um Anwendungsinhalte an einem anderen Ort als dem Hauptbildschirm des Geräts oder mithilfe einiger Fernzugriffstools wie TeamViewer oder AnyDesk anzuzeigen.

Schritt 2: Legen Sie fest, wieviele Signale aus der Liste ausgelöst werden müssen, um eine ausgewählte Empfehlung abzugeben


ADD RULE IN STARTEGY
Logical statement rule
CREATE NOW
List-based Rule
Velocity Rule
(deprecated)
Rule On Signals
RULE TYPE DESCRIPTION:
The rule checks how many of the selected signals have been detected in the profiling of the current inquiry.
If the number is greater or equal to a selected threshold, ...
Show more
STEP 1
Create your list of signals by choosing from the following:
Your list of signals (0):
Search signals
Search signals
ACTIVE CALL
ANYDESK DETECTED BASED ON NETW...
APP VERSION HOOKING
AUTOFILL USED BASED ON BEHAVIORA...
AUTOMATED BROWSER
BATTERY API HOOKING
STEP 2
If:
1
or more signals from your list are triggered
then refuse
RULE STATE:
Active
DISPLAY NAME (OPTIONAL):
Show advanced options
Add