nevisDetect – Risk Detection System

Der digitale Zugang sollte einfach und sicher sein, unabhängig davon, welchen Kanal Kunden wählen. Zugleich werden Angriffe immer raffinierter. Eine Zwei-Faktor-Authentisierung bietet deshalb keinen ausreichenden Schutz mehr vor Identitätsdiebstahl oder Man-in-the-Browser-Angriffen, die auf Schadprogrammen basieren. Hinzu kommt, dass eine Authentisierung mit mehreren Faktoren das Nutzererlebnis beeinträchtigt und so die Kundenbindung schwächt. Um die Sicherheit kritischer Dienste zu erhöhen, ohne Abstriche bei der Benutzerfreundlichkeit zu machen, sind deshalb ganzheitliche neue Sicherheitskonzepte gefragt. Genau diese Anforderungen standen bei der Entwicklung von nevisDetect im Mittelpunkt. nevisDetect ermöglicht es, führende Anomalieerkennungstechnologien auf einer einzigen Plattform zu vereinen. Es schützt digitale Dienste durch Mechanismen, die kontinuierlich das Risiko beurteilen und ein hohes Mass an Schutz gewährleisten, ohne das Nutzererlebnis zu schmälern.

Vorteile

- Entdeckt und verhindert Identitätsdiebstahl und Kontoübernahmen.
- Entdeckt und verhindert Session Hijacking.
- Bestimmt die wahre Identität einer Person anhand von deren Verhalten und Interaktion.
- Erhöht die Session-Sicherheit, ohne das Nutzerlebnis zu beeinträchtigen.
- Reduziert die False Positives, indem es verschiedene führende Technologien zur Anomalieerkennung optimal nützt.
- Verantwortliche für Forensik sind in der Lage, verdächtige Aktivitäten rasch zu analysieren und die Identitätsdaten in einem historischen Zusammenhang zu betrachten. Dies ermöglicht es Organisationen, ihr Meldewesen zu verbessern und neue regulatorische Vorgaben ohne grossen Aufwand einzuhalten.
- Sicherheitsteams können proaktiv verdächtige Identitäten ermitteln, bevor im Backend kritische Transaktionen ausgeführt werden.
- Die Scoring-Mechanismen anderer Systeme zur Anomalieerkennung (z.B. bei Zahlungen) lassen sich mit den von nevisDetect ermittelten Scores ergänzen. Dies reduziert den manuellen Aufwand der Betrugsabteilung beträchtlich und senkt zugleich Kosten und Verluste.
- Support-Desk-Teams können Kundenanfragen effizient bearbeiten, indem sie spezifische Benutzerinformationen abfragen. Support-Mitarbeiter können befähigt werden, Systemaktionen nach ordnungsgemässer Kundenidentifikation zu übersteuern.

Wichtigste technische Features

- Modularer und flexibler Aufbau
- Ausgelegt auf hohe Last und asynchrone Erkennung
- Ausgelegt für Deployments auf mehreren Linien
- Korrelation von TCP-, TLS- und HTTP-Features
- Einfache Integration neuer Erkennungsmodule dank Plug-in-Architektur
- Die Datenaufbewahrung von nevisDetect und BehavioSec lässt sich vollständig auf lokale Vorschriften abstimmen.
- Simulations- und Trainingsmodell für alle Erkennungsmodule
- Zentrales Verwaltungs-Cockpit für alle Erkennungsmodule
- Nahtlose Integration in bestehende NEVIS-Umgebungen
- Über TLS gesicherte Kommunikation zwischen Komponenten
- Die Zugriffskontrolle gewährleistet die Aufgabentrennung zwischen den Rollen Forensic Expert, Security Expert, Operator und Support Desk

Schweiz ▪ AdNovum Informatik AG ▪ Röntgenstrasse 22 ▪ 8005 Zürich ▪ Schweiz ▪ +41 44 272 6111 ▪ info@nevis-security.ch ▪ www.nevis-security.ch
Singapur ▪ AdNovum Singapore Pte. Ltd. ▪ 3 Shenton Way ▪ #23-03 Shenton House ▪ Singapore 068805 ▪ +65 6536 0668 ▪ info@adnovum.sg ▪ www.nevis-security.sg
Deutschland ▪ NEVIS Security GmbH ▪ Maximilianstraße 35 A ▪ 80539 München ▪ Deutschland ▪ +49 89 2421 8180 ▪ info@nevis-security.de ▪ www.nevis-security.de

Worum geht es?

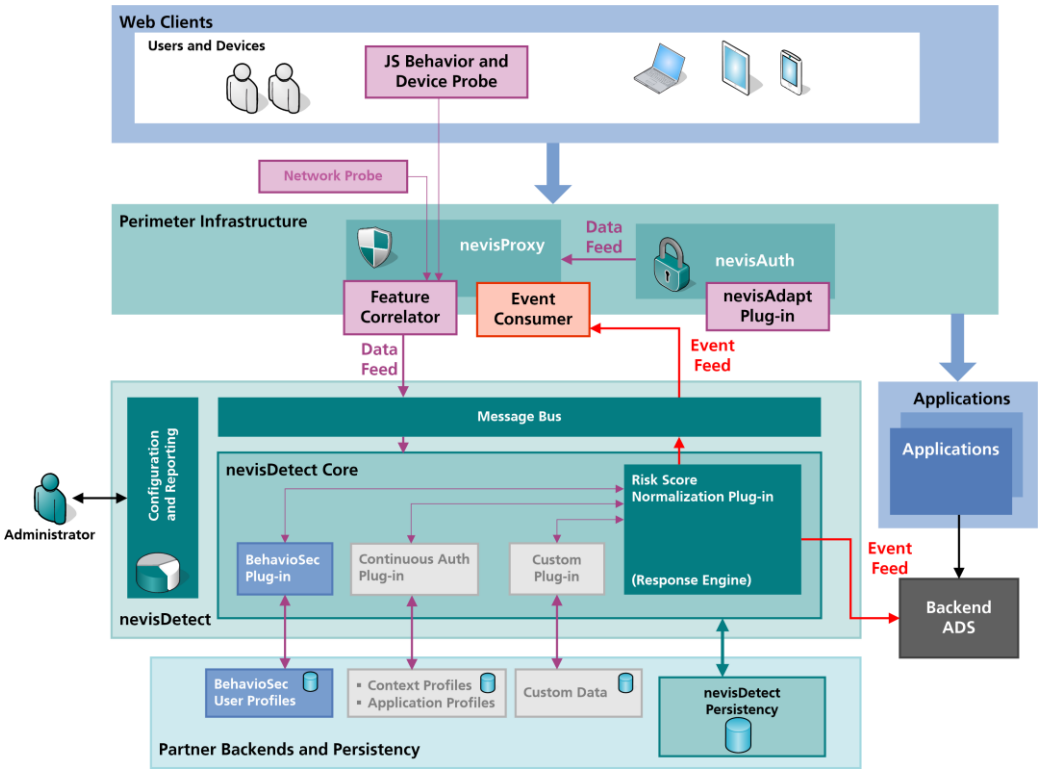

Abbildung 1: Architektur von nevisDetect

Die kontinuierliche, risikobasierte Benutzerauthentisierung von nevisDetect korreliert die Ausgaben mehrerer Anomalieerkennungsmodule. Sie basiert auf der Tatsache, dass die Korrelation mehrerer Attribute wie Verhaltensbiometrie, Geolokation oder Geräteinformation einen einzigartigen digitalen Fussabdruck erzeugt. Selbst wenn ein Angreifer ein Konto vollständig übernommen hat, ist das System in der Lage, diese Situation zu erkennen und darauf zu reagieren. Wurde beispielsweise am frühen Morgen ein gültiger Zugriff in Genf verzeichnet und derselbe Benutzer will sich eine Stunde später in Jakarta einloggen, kann es sich offensichtlich nicht um dieselbe Person handeln. Um zu entscheiden, ob eine bestimmte Benutzerinteraktion vertrauenswürdig ist, kombiniert nevisDetect die Ergebnisse mehrerer Anomalieerkennungsmodule zu einem flexiblen Risiko-Scoring. Auf der Grundlage des Risiko-Scoring kann das System Massnahmen zur Risikominderung einleiten, indem es beispielsweise den Benutzer bittet, sich neu zu authentisieren, die Session sofort abbricht oder ein Ticket für weitere Abklärungen eröffnet.

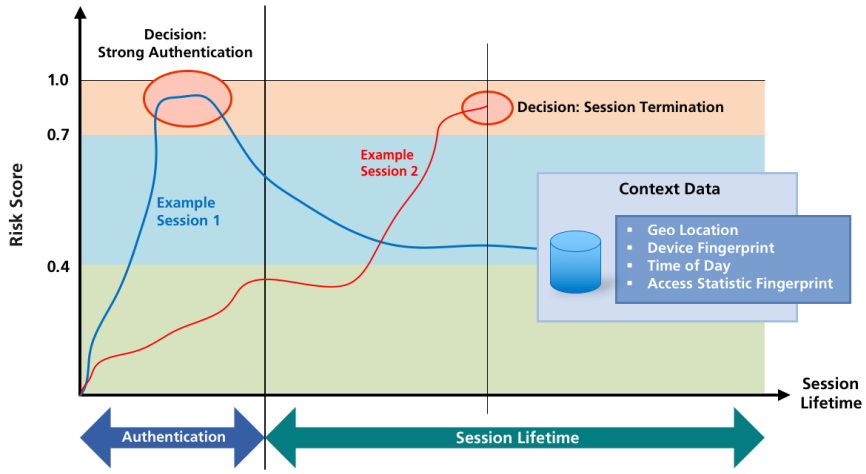

Abbildung 2: Kontinuierliche Authentisierung

Schweiz ▪ AdNovum Informatik AG ▪ Röntgenstrasse 22 ▪ 8005 Zürich ▪ Schweiz ▪ +41 44 272 6111 ▪ info@nevis-security.ch ▪ www.nevis-security.ch
Singapur ▪ AdNovum Singapore Pte. Ltd. ▪ 3 Shenton Way ▪ #23-03 Shenton House ▪ Singapore 068805 ▪ +65 6536 0668 ▪ info@adnovum.sg ▪ www.nevis-security.sg
Deutschland ▪ NEVIS Security GmbH ▪ Maximilianstraße 35 A ▪ 80539 München ▪ Deutschland ▪ +49 89 2421 8180 ▪ info@nevis-security.de ▪ www.nevis-security.de