VU Fraud Analysis®

VU

www.vusecurity.com

VU Fraud Analysis

La solución es el complemento ideal para entornos con métodos de autenticación robusta en los que sea necesario contemplar un modelo de análisis de comportamiento de usuarios a través de reglas generadas.

¿Qué es VU Fraud Analysis?

Este módulo genera perfiles de usuarios en base a la información provista por el core del cliente. La solución funciona bajo la modalidad de WebServices/ REST/ SOAP recibiendo y procesando la información. Este módulo puede ser personalizado para adaptarse a los campos que el cliente solicite evaluar y las reglas de detección también podrán personalizarse desde la consola de administración de la solución a través de operadores lógicos definidos en conjunto, además de contar con una base de conocimiento generada en función del historial transaccional que posea la empresa.

¿Cómo funciona VU Fraud Analysis?

En base al almacenamiento y procesamiento de información como importes, fecha de transacción, tipo de transacción, frecuencia de operación y datos de conexión del usuario, el sistema identifica posibles casos de fraude o de comportamiento sospechoso, pudiendo alertar de forma pasiva o bien de forma activa disparando proceso de autenticación robusta personalizados para ese perfil de usuarios. El producto permite recibir, mediante WebServices, la información de distintos campos y agregarle a cada uno valores para así llegar a un “umbral” que indique una operación fraudulenta.

Los canales y medios de información de los cuales puede valerse la plataforma son:

Canales de operación: VU Fraud Analysis puede identificar los distintos canales de los que recibe información para así evaluar el comportamiento de cada usuario. La cantidad de canales no tiene un límite prefijado y puede ser personalizado según las preferencias de cada empresa.

Perfil de comportamiento: la solución almacena el historial de transacciones de cada usuario y genera un perfil único. En base a esta información es capaz de calcular los umbrales de desvío con un efectividad superior al 95%.

Información de dispositivos: al momento de transaccionar cada dispositivo deja sus huellos digitales virtuales, ya sea por el tipo de navegador, dirección IP o sistema operativo, VU Fraud Analysis puede recolectar y comparar esta información contra su base de datos de dispositivos seguros.

Geo localización: la solución interactúa con cada canal y permite co- relacionar la información otorgando la posibilidad de evaluar zonas seguras, distancias recorridas entre una operación y otra, evaluando la viabilidad física de la misma, además de las cuestiones de seguridad asociadas a cada área geográfica.

Categorías de operación: en función de la información recolectada por canales, el sistema puede generar categorías de riesgo, las cuales relacionadas aportan el nivel total de la operatoria del usuario. A modo de ejemplo, un usuario no corre el mismo riesgo en una transferencia a una cuenta de terceros asociada a su cuenta, que el pago de una tarjeta de crédito del exterior.

VU Labs: nuestro equipo de trabajo actualiza periódicamente los listados de patrones con reglas de prevención de fraude, IPs baneadas y sitios fraudulentos conocidos. A través de estos esfuerzos, se apunta a minimizar las tareas de administración por parte de la empresa. Transacciones críticas: se recopila está información con el objetivo de elevar el nivel de detección de transacciones fraudulentas. Las mismas pueden ser identificadas en base a distintas características tales como fecha, monto, cuenta destino.

Transacciones no críticas: en cada acceso a los sistemas online no siempre se realizan transacciones, a veces simplemente son consultas de saldo, información o cambio de configuraciones. Estos son datos de sumo valor, dado que nos permiten recopilar información del perfil de cada usuario.

¿Cómo se integra con el framework de autenticación?

VU Fraud Analysis se integra con las modalidades de VU Mobile Tokens con el objetivo de implementar en tiempo real mecanismos que permitan mitigar transacciones maliciosas. El *framework* de autenticación VU Omnichannel Authentication Framework cuenta con una amplia gama de soluciones de autenticación activas y pasivas.

Las tecnologías con las cuales se integra la solución son:

Implementación de HOTP

Las soluciones de VU implementan las especificaciones del algorítmo HOTP. HOTP es un algorítmo generador de contraseñas de única vez, basado en HMAC especificado por la IETF. Como una regla general, en VU trabajamos basados en estándares y especificaciones avaladas a nivel mundial.

.

Especificación Técnica: RFC 4226
http://tools.ietf.org/html/rfc4226

Implementación de TOTP:

TOPT (Time Based One Time Password): por sus siglas en inglés Time Based One Time Password Algorithm es una extensión del ya probado algoritmo HMAC-Based one Time password. TOPT utiliza un esquema de implementación mediante el cual permite darle una tiempo corto de vida a cada OTP.

Especificación Técnica: RFC 6238
http://tools.ietf.org/html/rfc6238

Implementación de VUOTP:

VUOTP (VU One Time Password): VU cuenta con un método de generación, validación y autenticación de OTPs propietarios, mediante el cual permite trabajar de forma simultánea con un sistema por eventos, por tiempo y por patrones de autenticación. Esta modalidad otorga al cliente la posibilidad de optar por una amplia variedad de opciones y generar así su propie esquema de autenticación robusta.

Implementación OATH:

OATH: sistema de autenticación abierto, que permite a proveedores de soluciones robustas de autenticación convivir bajo una misma infraesctructura. Las soluciones de VU son compatibles con dicho estándar lo uqe le permite integrarse con otras marcas y soluciones existentes en el mercado.

Especificación Técnica: Release 2.0 http://www.openauthentication.org/webfm_send/1

Diferenciales:

- **Económico:** solución anti fraude de bajo costo para la evaluación personalizada de fraude

- **Performance:** Permite evaluar la información tanto online como offline.

- **Rangos de detección:** La solución crea un perfil del usuario y aplica las reglas generales de filtrado generadas por el cliente.

VU

VU es la empresa líder en desarrollo de soluciones de seguridad que previenen el fraude online y el robo de identidad. Proveemos soluciones enfocadas en la seguridad de la información tanto a individuos como a empresas y organismos gubernamentales. Nuestras soluciones brindan protección contra ataques de pharming, phishing, man in the middle, vishing y botnets, entre otros. La misión de VU es mantener la confidencialidad, integridad y disponibilidad antes, durante y luego de realizar una transacción de validación de credenciales.

Capacidad de innovación

Desde sus inicios los fundadores de la empresa se enfocaron en desarrollar soluciones tecnológicas que se adapten a las necesidades de los usuarios, simplificando y flexibilizando su utilización con fines de seguridad. Recientemente, Bancos y organismos Gubernamentales de Argentina eligieron a VU al haber comprobado el nivel de innovación, compromiso y tiempo de respuesta.

Escenarios de implementación:

Las soluciones de VU pueden integrarse dentro de cualquier proceso de autenticación o validación de operaciones que utilice sistemas informáticos. Algunos de los más comunes y utilizados diariamente son: Sistemas de pagos y financieros, acceso a redes corporativas, sistemas contables, accesos VPNs, Intranets, Correo electrónico, Home Banking, sitios Web, Sistemas de seguridad física (molinetes, accesos a bóvedas) o cajeros automáticos, CRMs, y/o IVRs. Fabricantes como Cisco Systems, Juniper, Citrix, Fortinet y Microsoft, entre otros recomiendan y certifican las soluciones de VU.