aruba
a Hewlett Packard Enterprise company

RESUMEN DE LA SOLUCIÓN

ANALÍTICOS DE COMPORTAMIENTO DE USUARIOS Y ENTIDADES

Utilizando el aprendizaje de máquina para entregar una solución de seguridad más inteligente

Las organizaciones de TI de cualquier tamaño están invirtiendo más dinero que nunca para proteger su red y sus activos debido a la panorámica creciente de amenazas. De acuerdo con IDC, los presupuestos de seguridad crecerán en 40% para el año 2020. Y, en adición al creciente número de amenazas, el sistema de seguridad típico de TI está cambiando rápidamente debido a:

- El aumento en el número y en los tipos de dispositivos que un solo usuario puede desplegar para acceder a activos corporativos
- Aplicaciones basadas en nube (Box, Salesforce, etc.) a las cuales se puede acceder fuera del control del departamento de TI corporativo
- La necesidad de proporcionar acceso a activos de alto valor a entidades externas, como asociados y contratistas, para aumentar la eficiencia de los procesos de negocio clave
- Dispositivos IoT "no tradicionales" accediendo la red corporativa

El resultado es que antes era un asunto de defender el castillo (la red corporativa) con un foso (productos de seguridad en la entrada y en las salidas). Ahora, se trata de proteger una colección sin fronteras y sin contención de empleados, contratistas y asociados – todos utilizando múltiples dispositivos desde cualquier lugar y en cualquier momento – desde afuera y desde adentro de las fronteras seguras de la red corporativa.

Para poder manejar esta nueva panorámica de amenazas, la solución de Analíticos de Comportamiento de Usuarios y Entidades (UEBA por sus siglas en inglés) de Aruba, Aruba IntroSpect, detecta ataques identificando pequeños cambios en comportamiento que frecuentemente son indicativos de ataques que han evadido las defensas de seguridad tradicionales. Aruba IntroSpect integra aprendizaje de máquina avanzado basado en Inteligencia Artificial, visualizaciones puntuales y perspectiva forense instantánea en una sola solución. ataques que involucran a usuarios, sistemas y dispositivos maliciosos, comprometidos, o negligentes se encuentran y se reparan antes de que puedan dañar las operaciones y reputación de la organización. Con una plataforma Spark/Hadoop, IntroSpect integra en forma única la detección de ataques basados en comportamiento y la investigación forense de incidentes y respuesta a escala empresarial.

LA NECESIDAD DE UEBA

Los productos tradicionales de defensa cibernética no fueron diseñados para enfrentar los ataques sofisticados, cuidadosamente diseñados y enfocados que las empresas ahora enfrentan. Aún se requieren para enfrentar la gran mayoría de amenazas "estándar" que aparecen todos los días, pero requieren ayuda con el número más pequeño de ataques "avanzados" mortíferos que llegan sin advertencia y que evaden las defensas perimetrales. Denominamos estos ataques “attacks on the inside”.

Por definición, este tipo de ataques son "malos desconocidos"—utilizan técnicas y herramientas que no se han visto anteriormente. Esto significa que no existen "firmas" para comparar ni reglas para disparar, motivo por el cual IntroSpect incluye una nueva clase de analíticos de detección que utilizan aprendizaje de máquina - tecnología de inteligencia artificial que no requiere pre programación ni configuración. En lugar de eso, IntroSpect construye líneas base de comportamiento normal para un usuario, un sistema, o cualquier dispositivo con una dirección IP - conocida como una "entidad". Las líneas base se construyen mediante modelos de aprendizaje de máquina que operan en datos clave de logs, netflow y flujos de paquetes - cualquier cosa que caracterice el comportamiento de TI de una entidad. Estas líneas base entonces se utilizan para detectar comportamiento anormal que, agregado a lo largo del tiempo y colocado en contexto, indicarán un ataque que se está gestando.

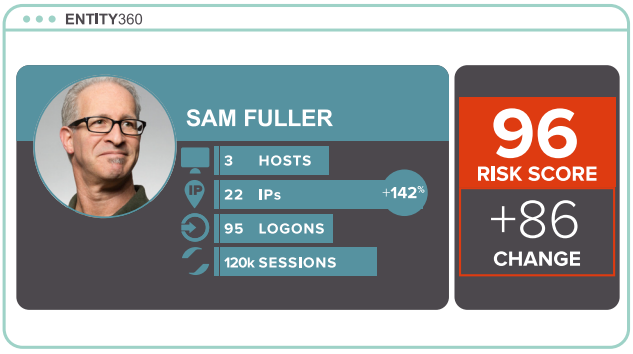

Figura 1: El Aprendizaje de Máquina de IntroSpect detecta ataques antes de que provoquen daños

Dado este enfoque, Gartner apodó la categoría UBA (User Behavior Analytics) y después extendió esto a UEBA (User and Entity Behavior Analytics) para reflejar productos como IntroSpect que perfilan no tan sólo a usuarios y a sistemas, sino a cualquier cosa con una dirección IP (esto es, IoT).

UNA DESCRIPCIÓN GENERAL RÁPIDA DEL APRENDIZAJE DE MÁQUINA

El Aprendizaje de Máquina (Machine Learning) es un término paraguas que abarca técnicas utilizadas para aprender y para hacer juicios sin ser programado explícitamente para cada escenario. A diferencia de productos basados en firmas, los modelos de aprendizaje de máquina aprenden de los datos y sus resultados se reportan como una probabilidad. La probabilidad de que una decisión sea exacta se expresa como un porcentaje y se puede interpretar como una medida de confianza en esa conclusión.

IntroSpect tiene más de 100 modelos de aprendizaje de máquina (algoritmos) en su arsenal que contienen dos técnicas diferentes:

1. **Aprendizaje de Máquina Supervisado.** Estos modelos son entrenados en un laboratorio con grandes cantidades de datos para encontrar tipos de ataques específicos. Una vez que se desarrolla el modelo, entonces se puede utilizar para predecir un ataque para cualquier conjunto nuevo de entradas. Por ejemplo, IntroSpect utiliza modelos de aprendizaje de máquina supervisados para detectar sistemas que se controlan por un externo malicioso, detectando URLs insólitos que son típicos de esta situación.
2. **Aprendizaje de Máquina sin Supervisión.** En este tipo de modelo, el algoritmo "auto aprende," lo cual significa que no existe ninguna capacitación o preparación previa requerida antes de que se despliegue. El algoritmo construye automáticamente una "línea base" para detectar pequeños cambios en comportamiento que son indicativos de ataques inminentes.
   Las líneas base se pueden establecer para usuarios, sistemas, o dispositivos en forma individual. Por ejemplo - se notará si un empleado accede a un nuevo sistema en un horario raro del día, o si un dispositivo IoT en una fábrica aumenta su uso de tráfico de red por un factor de 5.

CASOS DE USO TÍPICOS

IntroSpect UEBA se implementa en una amplia variedad de verticales de industria y de organizaciones de todos los tamaños.

- **SALUD:** La instalación requiere procesar logs de 300,000 usuarios que resultan en miles de millones de eventos por día. Casos de uso clave incluyen monitorear a usuarios de alto valor, como sysadmins por comportamiento anormal y para detectar credenciales compartidas.
- **FINANZAS:** Un cliente SIEM necesita soporte de analíticos adicionales para detectar exfiltración basada en correo electrónico y para ayudar a los analistas a priorizar alertas de correlación, al tiempo que acelera la investigación de incidentes.
- **LEGAL:** Un bufete jurídico de 2,000 empleados con 14 oficinas alrededor del mundo no cuenta con visibilidad del tráfico de la red LAN, lo cual bloquea su capacidad de ver comportamiento negligente, como compartir contraseñas y uso anormal de la nube.

DIFERENCIADORES CLAVE

Aruba es el único proveedor de networking que cuenta con la solución UEBA líder de la industria.

1. **Monitoreo continuo y detección de ataques.** Más de 100 modelos supervisados y sin supervisión que detectan el rango más amplio de ataques.
2. **Visibilidad total.** IntroSpect incorpora en forma singular todas las fuentes de datos relevantes de TI en los analíticos y en la inspección forense, incluyendo paquetes, flujos, logs, alertas, puntos terminales, nube, etc.
3. **Investigación acelerada de incidentes.** IntroSpect combina la detección de ataques vía aprendizaje de máquina supervisado y sin supervisión con datos forenses integrados en un perfil de seguridad denominado Entity360. Entity360 es clave para reducir el tiempo y el esfuerzo requeridos para entender, diagnosticar y responder a un ataque. Entity360 proporciona calificación de riesgo exhaustiva y continua e información de seguridad enriquecida que los analistas de otra forma tendrían que invertir horas o días en buscar – meses y años de datos de seguridad hasta el nivel de paquete.

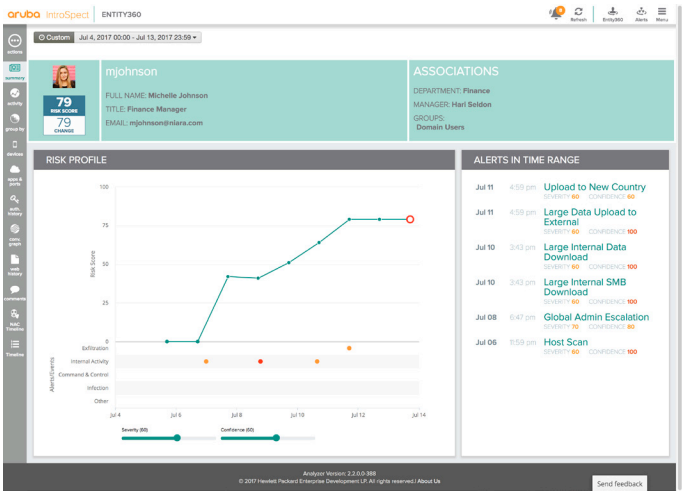

Figura 2: Información forense consolidada en un perfil Entity360

4. **Escalabilidad madura de clase empresarial.** Soporte para arquitectura de Big Data – IntroSpect tiene una ventaja de 3 años en perfeccionar esta tecnología.
5. **Integración transparente.** Con integración bidireccional con los sistemas importantes SIEM y de agregación de logs como ArcSight, McAfee ESM, QRadar y Splunk, IntroSpect aprovecha sus repositorios de datos centralizados, así como las alertas basadas en aprendizaje de máquina y los datos forenses que regresan a la consola y al flujo de trabajo SIEM.
6. **Respuesta a ataques basada en el contexto de negocio y en políticas.** La integración con sistemas de control de acceso, como ClearPass, le proporcionan a IntroSpect la capacidad de automatizar la respuesta a alertas de ataques en base a políticas establecidas por la organización. Y, debido a que IntroSpect correlaciona el significado de negocio a su calificación de riesgo, las políticas y las acciones se pueden afinar en base al valor de los activos y de los actores involucrados. En un mundo en donde es casi imposible bloquear todos los ataques, IntroSpect es un complemento de seguridad "post admisión" a la visibilidad y control "pre admisión" de ClearPass.

FAMILIA DE PRODUCTOS ARUBA INTROSPECT—OPTIMIZADA PARA LA RÁPIDA RECUPERACIÓN DE LA INVERSIÓN, DIMENSIONADA PARA LA GRAN EMPRESA

La familia de productos IntroSpect UEBA consiste en las Ediciones Standard y Advanced:

IntroSpect Standard es una versión optimizada para inicio rápido de la plataforma UEBA completa, perfecta para instalaciones de networking de Aruba. Requiere tan solo tres fuentes de datos (Active Directory o registros de autenticación equivalentes, información de identidad basada en LDAP y logs de firewall, como los logs AMON que se generan por los controladores inalámbricos de Aruba) para entregar detección de ataques enfocada en acceso anormal a activos, intentos de expandir ataques como beaconing e indicaciones de intentos de exfiltración de datos.

IntroSpect Avanzado proporciona todas las capacidades de detección de ataques, investigación de incidentes y cacería de amenazas en los cuales los clientes ya están confiando para la protección más amplia disponible en el mercado de UEBA. Si un cliente comienza con IntroSpect Standard, el actualizarse a alguna o a toda la funcionalidad de la Edición Advanced es transparente y no requiere ningún cambio al producto base.

figure 1.0_060617_clearpassintrospect

Figura 3: Cuando IntroSpect se integra con Aruba ClearPass, la solución combinada entrega tres innovaciones clave de seguridad: detección avanzada de ataques, investigación acelerada y cumplimiento automatizado basado en políticas.

aruba
a Hewlett Packard Enterprise company
3333 SCOTT BLVD | SANTA CLARA, CA 95054
1.844.473.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM
www.arubanetworks.com/latam