



GUÍA EJECUTIVA DE TI Para Seguridad Inteligente

Transición de la Administración de Registros y la SIEM a la Seguridad Inteligente

GUÍA EJECUTIVA DE TI SOBRE SEGURIDAD INTELIGENTE

Transición de la Administración de Registros y la SIEM a la Seguridad Inteligente

Índice

Resumen Ejecutivo	3
Introducción.....	3
Por qué Seguridad Inteligente	3
Definición del Problema.....	4
Más allá de La Administración de Registros y La SIEM.....	5
El Valor del Negocio de la Seguridad Inteligente	5
Consolidación de los Silos de Datos.....	6
Detección de Amenazas	6
Descubrimiento de Fraude.....	6
Administración/Evaluación de Riesgos.....	6
Conformidad de las Reglamentaciones.....	7
Abordaje del Resultado Final	7
Q1 Labs Permite la Seguridad Inteligente.....	8
Conclusión.....	8

Resumen Ejecutivo La Seguridad Inteligente, basada en los mismos conceptos que han hecho de la inteligencia empresarial una tecnología esencial, es el siguiente paso crítico para las organizaciones que reconocen la importancia de la seguridad de la información para la salud de su empresa.

Muy a menudo, la respuesta a nuevas amenazas de seguridad se basa en un enfoque en el que es “mejor prevenir que curar”, con una tecnología específica y singular o nuevas políticas o reglas reactivas. Esto se debe, en gran parte, a que un programa de seguridad unificada, basado en el análisis automatizado de información unificada de toda la infraestructura de TI es costoso, complejo, difícil de implementar e ineficaz. Como resultado, la mayoría de las organizaciones carecen de las capacidades de detección de amenazas precisas y administración de riesgos informados.

En este informe, usted aprenderá cómo la Seguridad Inteligente aborda estas deficiencias y autoriza a las organizaciones, ya sean las empresas del Fortune Five, empresas medianas o las agencias del gobierno, a mantener la seguridad de la información de manera completa y rentable. En particular, le mostraremos cómo la seguridad inteligente concentra las preocupaciones críticas en cinco áreas clave:

- 1 Consolidación de silos de datos
- 2 Detección de amenazas
- 3 Descubrimiento de fraude
- 4 Evaluación de riesgos/administración de riesgos
- 5 Conformidad con las reglamentaciones

Introducción

¿Por qué Seguridad Inteligente?

Las empresas de alto rendimiento se destacan en los negocios, en gran parte, debido a que saben cómo poner en práctica su información. Con la ayuda del uso automatizado de la tecnología de inteligencia empresarial, estas empresas aplican un análisis para extraer el valor máximo de las grandes cantidades de datos que tienen a su disposición.

El mismo enfoque se debe aplicar para asegurar esa información mediante la implementación de un programa de seguridad inteligente. De la misma manera que la inteligencia empresarial ayuda a las empresas a tomar decisiones que maximizan las oportunidades y minimizan los riesgos del negocio, la seguridad inteligente les permite una mejor detección de amenazas, identificación de los riesgos de seguridad y las áreas de incumplimiento, y establecer prioridades para su remediación.

El caso de la inteligencia empresarial es cautivador. Permite a las organizaciones soportar su toma de decisiones crítica mediante la automatización de los procesos de análisis de datos a un nivel apenas comparado con el análisis manual. Mediante la aplicación de un análisis de negocios automatizado para sus entornos únicos, las organizaciones

exitosas obtienen el mayor valor posible a partir de sus terabytes y petabytes de datos acumulados, desde los ingresos por ventas y demografía de los clientes hasta el costo de envío y las materias primas. Considere este extracto de un artículo del año 2010 de The Economist (“Data, Data Everywhere”): “Los datos se están convirtiendo en la nueva materia prima de los negocios: una entrada económica casi a la par con el capital y el trabajo. ‘Todos los días me despierto y me pregunto: ¿cómo puedo mejorar el flujo de datos, administrar mejor los datos, analizar mejor los datos?’ dice Rollin Ford, Jefe de los servicios de información de Wal-Mart”.

El caso de seguridad inteligente es igual, si no más, de cautivador. Las empresas y las organizaciones gubernamentales tienen grandes cantidades de datos que pueden ayudar a detectar las amenazas y las zonas de alto riesgo, siempre y cuando tengan los medios y el compromiso de recogerlos, agregarlos y, lo que es más importante, analizarlos. Estos datos no sólo provienen de los productos de seguridad específicos, sino también de fuentes, tales como configuraciones de dispositivos de red, servidores, telemetría de tráfico de la red, aplicaciones y usuarios finales y sus actividades.

Seguridad inteligente reduce el riesgo, facilita la conformidad, muestra un ROI demostrable y maximiza la inversión en las tecnologías de seguridad existentes. Por analogía con la inteligencia empresarial, los objetivos de la seguridad inteligente son los siguientes:

- Destilar grandes cantidades de información en un proceso de toma de decisiones eficaz, al reducir millones de piezas de datos a un puñado de asuntos a tratar.
- Poner en práctica la recolección y el análisis de datos a través de la automatización y la facilidad de uso.
- Ofrecer aplicaciones de alto valor que ayuden a las organizaciones a obtener los mayores beneficios de sus datos, a fin de comprender y controlar el riesgo, detectar problemas y priorizar las mejoras.
- Validar que tiene las políticas adecuadas.
- Asegurar que los controles que usted ha implementado están cumpliendo con esas políticas de manera eficaz.

Las organizaciones tienen un largo camino por recorrer en la comprensión del entorno de seguridad de su TI. Considere la encuesta realizada en el 2010 por la revista CSO, patrocinada por Deloitte, que informó que 7 de cada 10 incidentes de seguridad nunca se informan. De acuerdo con Deloitte, los indicios revelan que en la mayoría de los casos, las organizaciones que han sido víctimas ni siquiera se dan cuenta de que han sido comprometidas.

Además, el informe Verizon Data Breach Investigations del 2010 reveló que más de un tercio de las violaciones de datos investigados se mantienen ocultos durante meses. Además, tres quintos de los descubrimientos son de terceros, no de la organización que ha sido víctima. El informe también cita como factores “desconocidos” al 43 % de las violaciones: Activos desconocidos; datos de los que no se tenía conocimiento en un activo específico; activos que tenían conexiones de red o de accesibilidad desconocidas y privilegios o cuentas de usuario desconocidos.

Métodos simplificados de incumplimiento descubiertos por porcentaje de violaciones

Fuente:
Informe Verizon Data Breach Investigations del 2010

Definición del Problema

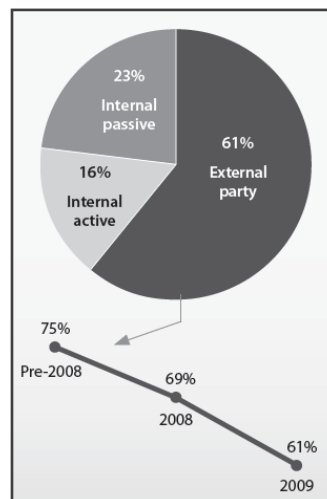
El modelo de seguridad de hace 10 o 12 años ya no es lo suficientemente adecuado para enfrentar los desafíos actuales, ya que el “vandalismo por Internet” ha dado lugar a la actividad delictiva organizada. El modelo es anticuado y no se adapta a las amenazas y los entornos de TI actuales. La seguridad basada en el perímetro se ha convertido en un modelo altamente distribuido, a medida que los empleados, los socios y los clientes realizan negocios, a distancia, a través de Internet y los criminales explotan nuevas áreas de ataque y echan a perder la confianza del usuario.

Las obligaciones reglamentarias del gobierno y la industria surgieron o fueron reforzadas a través de sanciones firmes y una imposición más rápida.

La industria de la seguridad respondió con nuevos y mejores productos para abordar cada amenaza. Todas estas herramientas añaden un valor a la seguridad empresarial en general, pero son, en efecto, islas de tecnología de seguridad. No son propicias para un programa de seguridad basado en el riesgo para toda la empresa, y el esfuerzo general tiende a estar fragmentado.

En muchos casos, las organizaciones tienen que lidiar con datos incompletos debido a que una herramienta de seguridad puede no reconocer una amenaza o riesgo sin la correlación de otras fuentes de datos. Por otra parte, aún cuando los datos se obtienen de fuentes dispares, los analistas se ven desafiados por la gran cantidad de volumen, lo que hace que sea extremadamente difícil extraer la información procesable.

La seguridad inteligente aborda estos problemas a través del espectro de seguridad del ciclo de vida, mediante la centralización de datos de silos dispares, la normalización de este y la ejecución de un análisis automatizado. Esto permite a las organizaciones priorizar los riesgos e implementar, de manera rentable, los recursos de seguridad para la detección, prevención, respuesta y recuperación.



Más Allá de La Administración de Registros y La SIEM

El concepto de seguridad inteligente está parcialmente materializado en las herramientas de la información de seguridad y la administración de eventos (SIEM), que correlacionan y analizan los datos de registro agregados y normalizados. Las herramientas de administración de registros centralizan y automatizan el proceso de consulta, pero carecen de la flexibilidad y de las capacidades sofisticadas de correlación y análisis de la SIEM y, en última instancia, de la seguridad inteligente.

Pero la SIEM debe ser considerada como un punto de paso en lugar de un destino. El objetivo final es la seguridad inteligente completa. La SIEM es muy fuerte desde el punto de vista de administración de eventos, y desempeña un papel especialmente importante en la detección de amenazas. La seguridad inteligente completa debe abarcar y analizar una gama mucho más amplia de información: Esta requiere de un monitoreo continuo de todas las fuentes de datos relevantes de toda la infraestructura de TI y la evaluación de la información en contextos que van más allá de las capacidades típicas de la SIEM.

La seguridad inteligente debe incluir una gama de datos mucho más amplia para aprovechar todo el contexto en el que los sistemas funcionan. Este contexto incluye, pero no está limitado a: registros de dispositivos de red y seguridad; vulnerabilidades; datos de configuración; telemetría de tráfico de la red; eventos y actividades de la aplicación; identidades de los usuarios; activos, geolocalización y contenido de la aplicación.

Esto produce una asombrosa cantidad de datos. La seguridad inteligente proporciona un gran valor en la utilización de esos datos para establecer un contexto muy específico alrededor de cada área posible de preocupación y ejecución de análisis sofisticados para detectar con precisión una mayor cantidad y diferentes tipos de amenazas.

Un punto de valor clave para la seguridad inteligente, más allá de la SIEM, es la capacidad de aplicar el contexto desde toda una amplia gama de fuentes.

Esto reduce:

- 1 Falsos positivos
- 2 Le indica no solo lo que ha sido explotado sino qué tipo de actividad se lleva a cabo como resultado.
- 3 Ofrece una detección y respuesta a incidentes de una manera más rápida.

Por ejemplo, el informe de explosión potencial de un servidor Web por el IDS se puede validar mediante la actividad de red de salida inusual detectada por la capacidad de detección de una anomalía conductual de la red (NBAD), y viceversa.

O bien, usted tiene un informe acerca de que un servidor tiene una vulnerabilidad potencial que acaba de ser divulgada. Pero se trata de uno de cientos en su organización, así que ¿cómo evalúa la amenaza de este servidor específico? La seguridad inteligente puede analizar todos los datos disponibles y le informará de:

- La presencia o la ausencia de la vulnerabilidad
- El valor que la organización le asigna a los activos o los datos
- La posibilidad de explosión según los modelos de amenaza de la ruta de ataque
- La información de configuración, que puede indicar, por ejemplo, que no se puede acceder al servidor debido a que se ha cambiado un valor predeterminado
- La presencia de controles de protección, tal como un IPS

Los 250.000 cables diplomáticos que se entregaron a WikiLeaks fueron obtenidos por un usuario, el Soldado de primera clase Manning, quien actuó dentro de sus privilegios autorizados. Es muy probable que ningún mecanismo de seguridad hubiera podido detectar este tipo de acción, pero el análisis de datos correlacionados, que aplica contextos de múltiples fuentes, podría haber detenido la filtración antes de que pudiera causar algún daño.

El Valor Comercial de la Seguridad Inteligente

Uno de los argumentos más convincentes de la seguridad inteligente está en la eficacia del funcionamiento: un mejor uso de las personas, el tiempo y la infraestructura. Es la capacidad de incorporar diferentes tecnologías de seguridad y de red en un sistema integrado en lugar de productos que operan de forma independiente.

El enfoque en la seguridad inteligente es muy importante, ya que la responsabilidad operativa de la seguridad está cada vez más en manos de los equipos de operaciones de red. Tiene sentido reflejar esta consolidación de las responsabilidades operativas con la consolidación en el nivel de la inteligencia. Considere permitir múltiples tareas en una sola plataforma y el desarrollo multifuncional de habilidades en toda la organización, para luego implementar el acceso basado en roles.

Además, la seguridad inteligente añade valor en otras áreas de TI, tales como la resolución de problemas del sistema, problemas de red y análisis de autorización y soporte de usuarios.

La seguridad inteligente permite a las organizaciones utilizar herramientas integradas a través de una infraestructura común, y aprovechar un conjunto de datos unificados para abordar los problemas por todo el espectro de seguridad. Esto se puede ilustrar con los cinco casos de uso más destacados en los cuáles la seguridad inteligente genera un alto valor.

1 Consolidación de Silos de Datos

Sin la tecnología automatizada, los análisis de inteligencia empresarial son difíciles de llevar a cabo. Los datos que le permiten a usted comprender las devoluciones de inventario, cadenas de suministro, etc., están disponibles, pero se encuentran en silos, en diferentes aplicaciones y bases de datos. Corresponde al analista recopilar los datos de todas esas fuentes y verterlos en hojas de cálculo o bases de datos para realizar un análisis manual. Los análisis de seguridad plantean problemas similares y la seguridad inteligente proporciona eficacias similares. Desde una perspectiva de seguridad, pueden existir datos en tres tipos de silos:

- Datos bloqueados en dispositivos, aplicaciones y bases de datos de seguridad dispares
- Datos que se recogen desde productos, aplicaciones, etc. específicos y que, en efecto, crean otro silo. Es otra base de datos donde se almacenan los datos, pero no hay comunicación o coordinación entre, por ejemplo, la base de datos de configuración
- Silos organizacionales de datos segregados por unidad de negocio, grupo de operaciones, departamento, etc.

En los dos primeros casos, la seguridad inteligente acaba con los silos mediante la integración de fuentes de datos a partir de diversos productos en una estructura común para el análisis automatizado a través de diferentes tecnologías de TI y seguridad. Desde una perspectiva de seguridad, esto aporta todas las capacidades de detección y evaluación de riesgos mejoradas que la telemetría consolidada de seguridad inteligente pueden ofrecer. Desde una perspectiva de CIO, la reducción de estos silos permite la racionalización de productos de seguridad que de otra manera tendrían que ser administrados sobre la base de un producto específico. El tercer caso requiere una cooperación considerable entre los grupos que están generalmente separados, es decir, una realineación de procesos y responsabilidades, y quizás, un poco de presión ejercida por la dirección.

El abrumador volumen acumulado de todos estos datos dispares agrava el problema de manera exponencial. Cada uno de estos silos puede crear volúmenes de datos enormes, en diferentes formatos, con diferentes propósitos y, en algunos casos, diferentes políticas, e incluso, requisitos de conformidad. Solo la seguridad inteligente automatizada puede administrar con eficacia petabytes de datos relacionados con la seguridad y analizarlos a través de los silos organizacionales y operacionales.

2 Detección de Amenazas

En pocos años, debido a que las empresas se extendieron a un comercio basado en la Internet y en usuarios remotos, la seguridad ha pasado de un modelo basado en el perímetro con toda la política centrada en el firewall a una seguridad distribuida. La seguridad ahora se enfoca en los hosts, las aplicaciones y el contenido de la información que se mueve fuera de la organización.

Por otra parte, estamos viendo la creciente incidencia de ataques muy específicos, como los ataques a la NASDAQ y a otras empresas de renombre. Las intrusiones sofisticadas y específicas suelen ser multifacéticas y tener varias etapas, son difíciles de detectar y muy difíciles de erradicar. Las amenazas avanzadas persistentes (APT) se caracterizan por la tenacidad de los atacantes y los recursos a su disposición.

Se debería aplicar una inteligencia global a las diversas tecnologías de seguridad que se han desarrollado en respuesta al panorama cambiante de amenazas. Como se señaló en la discusión del contexto de seguridad, una actividad que parece inofensiva para una parte de una infraestructura puede revelarse como una amenaza cuando los datos se correlacionan con otras fuentes. Así, por ejemplo, un atacante puede deshabilitar el registro, pero no puede inhabilitar la actividad de red. Las aplicaciones propietarias pueden no producir registros; algunos tramos de la red pueden no tener firewall. La seguridad inteligente todavía puede identificar las aplicaciones y servicios que se ejecutan entre el host y la red en estos casos, y señalar una amenaza potencial.

3 Descubrimiento de Fraude

La seguridad inteligente es absolutamente esencial para la detección eficaz del fraude. El ingrediente clave, además de la telemetría de la red, los datos del tejido de conmutación y enrutamiento y la capa de seguridad del dispositivo de la aplicación, es la comprensión de los usuarios y los datos de la aplicación.

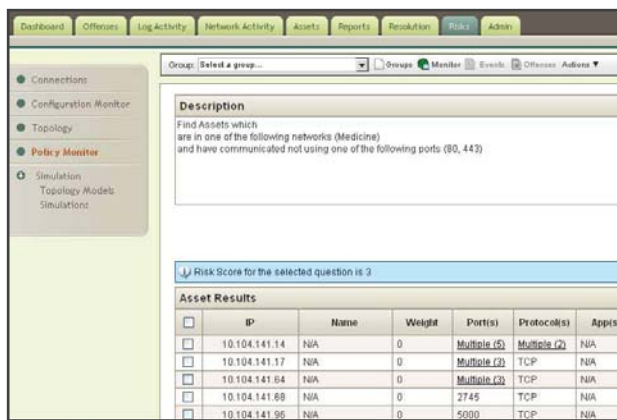
La detección del fraude requiere una supervisión de todo lo que sucede en la red: los eventos y actividad de la red, la actividad del host y las aplicaciones, y la actividad de cada usuario. La seguridad inteligente le permite enlazar el usuario a un activo específico. Al unir la red, el servidor DNS y la actividad de las aplicaciones con la información del directorio, por ejemplo, la seguridad inteligente puede vincular a un usuario específico a una dirección IP específica para una determinada sesión VPN.

4 Evaluación de Riesgos/Administración de Riesgos

La seguridad inteligente es la columna vertebral de la administración de riesgos a través del análisis de impacto y el modelo de amenaza. Es la diferencia entre reaccionar ante los ataques a la red y proteger, proactivamente, sus activos más importantes.

El análisis de impacto se basa en el valor que una empresa le asigna a un activo específico y las consecuencias negativas para el negocio si se ve comprometido. La seguridad inteligente se encarga de ello mediante el descubrimiento y la clasificación de datos y activos, a fin de identificar los activos críticos. Además, responde a preguntas tales como: ¿Cuán expuesto está el activo? ¿Tiene algún acceso directo a Internet? ¿Posee vulnerabilidades conocidas para las cuales existan explosiones conocidas?

El modelado de amenazas toma todos estos factores en cuenta y no solo identifica las vulnerabilidades en el sistema destino, sino las rutas de ataque posibles basadas en la explotación de las debilidades entre el destino e Internet: reglas de firewall mal diseñadas, ACL del enrutador mal configuradas, etc.



The screenshot shows a web interface with a navigation menu on the left (Dashboard, Offenses, Log Activity, Network Activity, Assets, Reports, Remediation, Risk, Admin) and a main content area. The main area displays a 'Description' box with a query: 'Find Assets which are in one of the following networks (Medicine) and have communicated not using one of the following ports (80,443)'. Below this, it states 'Risk Score for the selected question is 3'. An 'Asset Results' table is shown with columns for IP, Name, Weight, Ports, Protocol(s), and App(s).

IP	Name	Weight	Ports	Protocol(s)	App(s)
10.104.141.14	N/A	0	Multiple (0)	Multiple (2)	N/A
10.104.141.17	N/A	0	Multiple (0)	TCP	N/A
10.104.141.64	N/A	0	Multiple (0)	TCP	N/A
10.104.141.68	N/A	0	2745	TCP	N/A
10.104.141.96	N/A	0	5000	TCP	N/A

Priorizar El Riesgo: Consulta de Calificación de Riesgo

5 Conformidad con las reglamentaciones

La conformidad es un caso de uso fundamental para la seguridad inteligente. Aborda muchos requisitos de conformidad, especialmente de todos los aspectos de supervisión de la seguridad. Así, por ejemplo, la seguridad inteligente no satisface todos sus requerimientos de PCI, pero cumple con todos sus requerimientos de vigilancia de PCI de una manera que la SIEM y la administración de registro por sí solo no puede. La seguridad inteligente proporciona la información que sirve de base para ofrecer y demostrar los requisitos de auditoría para todas las regulaciones.

Mediante una supervisión general a través de la infraestructura de TI (eventos, cambios de configuración, actividad de la red, aplicaciones, actividad del usuario) la seguridad inteligente consolida las capacidades de conformidad en un conjunto de productos único, en lugar de depender de múltiples productos específicos y que cada uno colabore con su propia pieza del rompecabezas de la auditoría.

Abordaje del Resultado Final

La seguridad inteligente, así como la inteligencia empresarial, permite a las organizaciones tomar decisiones de negocios inteligentes. Permite a las organizaciones procesar más información, de manera más eficaz, a través de toda la infraestructura de TI. La aplicación de la tecnología de inteligencia empresarial permite a las organizaciones, literalmente, hacer más con menos: en lugar de tener analistas que dediquen valiosas horas al análisis minucioso y manual de una fracción de los datos disponibles, la inteligencia empresarial automatiza el análisis en todos los datos disponibles y proporciona información basada en roles y específica para la tarea.

La tecnología de la información se trata, después de todo, de la automatización del proceso empresarial: para compras, logística, ERP, etc. La seguridad inteligente se trata de la automatización de la seguridad: la comprensión del riesgo, la supervisión de la infraestructura para detectar amenazas y vulnerabilidades y la priorización de la remediación.

Al centralizar los datos y las herramientas de seguridad de la infraestructura de TI, la seguridad inteligente permite una administración consolidada y un uso más eficaz de los recursos destinados a la seguridad. Las organizaciones mejoran la postura de la seguridad sin costos operativos y de personal adicionales, y sin costos adicionales de adquisición, mantenimiento e integración de múltiples productos específicos.

La seguridad inteligente genera beneficios clave para el costo y la eficacia empresarial:

- Reduce el costo asociado con el despliegue y la operación. En lugar de añadir personas, las libera para hacer que la seguridad sea relevante para la empresa.
- Hace adquisición de productos de manera más simple y más barata. Las empresas compran una sola plataforma, en lugar de múltiples productos.
- Facilita la implementación a través de una plataforma unificada, en lugar de varios productos, que se deben integrar para acercarse a una capacidad de seguridad inteligente aceptable.
- Ofrece una amplia clase de capacidades de seguridad para las organizaciones, las cuales antes eran posibles solo para las empresas más sofisticadas.
- Automatiza la recopilación, la normalización y el análisis de grandes cantidades de datos de seguridad de silos técnicos y organizativos. Esta capacidad aplica un contexto valioso a cada análisis.
- Mejora la detección de amenazas, mediante la aplicación de contexto para detectar posibles ataques que podrían pasar inadvertidos por una tecnología de seguridad específica.
- Mejora la respuesta a incidentes a través de una detección precisa y rápida.

- Aprovecha el ROI del equipo de trabajo. Las organizaciones pueden implementar nuevos servicios de seguridad, tales como la supervisión de amenazas en todo el mundo, sin mano de obra adicional.
- Autoriza a las empresas a ejecutar programas de seguridad sólidos, que procesen miles de millones de registros por día y que produzcan una calificación o similar de asuntos a tratar de alta prioridad cada 24 horas.

Q1 Labs Permite la Seguridad Inteligente

La Plataforma de Seguridad Inteligente QRadar de Q1 Labs proporciona un conjunto de soluciones altamente integrado, diseñado para ayudar a las empresas a alcanzar la seguridad inteligente total, implementado en un sistema operativo unificado y administrado a través de una única consola.

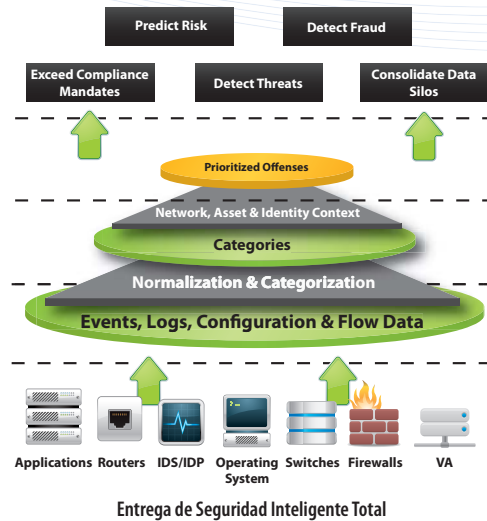
QRadar, asegurado por una poderosa SIEM, presenta una capacidad de seguridad inteligente única que integra un conjunto de aplicaciones de alto valor de seguridad y de supervisión a través de la red en una solución unificada, que permite a las empresas implementar los recursos de operaciones de seguridad y de red basados en el análisis de un conjunto completo de datos fuentes.

La solución QRadar está basada en el Sistema Operativo de Seguridad Inteligente de Q1 Labs, que permite a Q1 Labs ofrecer un conjunto de servicios comunes en torno de la integración, la normalización, el almacenamiento, el archivado y el análisis de datos. Esta estructura unificada produce una capacidad uniforme de flujo de trabajo, informes, alertas y panel de instrumentos. Éstas soportan las políticas y los procesos de toda la organización, identifican rápidamente las amenazas y evalúan los riesgos, y soportan los requisitos de respuesta e información de seguridad de nivel de auditoría, operacional, administrativo y ejecutivo.

Además del fuerte núcleo de las capacidades de administración de registros y SIEM, la tecnología QRadar QFlow ofrece una supervisión profunda de la red con capacidades sofisticadas de detección de anomalías del comportamiento que añaden un contexto valioso a los análisis que, de otro modo, podrían basarse únicamente en los datos de registro. La supervisión de red de QRadar consciente de las aplicaciones permite indicar la información completa del estado de todas las conversaciones en la capa de aplicación.

Además, la Plataforma de Seguridad Inteligente QRadar extiende sus capacidades de seguridad inteligente hacia los entornos de redes virtuales con la tecnología VFlow de QRadar, que asegura un alto nivel de detección de amenazas y administración de riesgos, como apoyo a la consolidación del centro de datos y a las iniciativas de nube pública y privada.

El módulo de evaluación de riesgos, QRadar Risk Manager, proporciona una auditoría de configuración detallada que añade un contexto de postura de riesgo que la SIEM no puede proporcionar por sí sola. QRadar Risk Manager evalúa el riesgo y los modelos de amenazas potenciales en comparación con activos de alto valor, y determina las posibles rutas de ataque basado en la riqueza de datos sobre la cual se basa.



El Sistema Operativo de la Seguridad Inteligente ofrece una plataforma para seguir añadiendo nuevos módulos de seguridad para dar cabida a nuevos casos de uso en torno de la protección inteligente y de la evaluación de riesgos inteligente de la infraestructura de la empresa. Esto elimina la carga de nuevas capas de integración de datos, requisitos de almacenamiento diferentes, motores de análisis nuevos e infraestructura de información diferente para dar cabida a nuevas aplicaciones de seguridad y fuentes de datos potenciales.

Conclusión

Las organizaciones con visión de futuro han reconocido y adoptado el valor de la tecnología de inteligencia empresarial, debido a que su éxito se basa en la capacidad de análisis y actuación sobre la información esencial derivada de los sorprendentes volúmenes de datos. Del mismo modo, la seguridad inteligente es esencial porque la seguridad de la información es parte integral de los negocios en el siglo 21. Los análisis potentes y automatizados de datos centralizados de fuentes que cubren todo el espectro de la infraestructura de TI hacen que la seguridad económica y de alto nivel no solo sea posible, sino indispensable.

Q1 Labs, an IBM company
 890 Winter Street, Suite 230
 Waltham, MA 02451 USA
 1.781.250.5800, info@Q1Labs.com

Copyright 2012 Q1 Labs, an IBM company. Todos los derechos reservados. Q1 Labs, el logotipo Q1 Labs, Total Security Intelligence, y QRadar son marcas o marcas registradas de Q1 Labs, Inc. Todos los otros nombres de productos o empresas mencionados pueden ser marcas, marcas registradas o marcas de servicios de sus respectivos propietarios. Las especificaciones y la información expresadas en este documento están sujetas a cambios sin previo aviso.
 WPEGSIO220