El ROS de Q1 Labs QRadar© Plataforma de seguridad Inteligente

Retorno a la Seguridad de IANS (ROS)
Junio de 2011

MEJORANDO LAS EFICIENCIAS OPERATIVAS EN EL GOBIERNO FEDERAL

AUSPICIADO POR:

Contenido

Resumen Ejecutivo

En nombre de Q1 Labs, IANS llevó a cabo un análisis del Retorno a la Seguridad (ROS) del producto de Q1 Labs: la Plataforma de Seguridad Inteligente QRadar©. Para facilitar dicho estudio, IANS entrevistó a dos clientes de Q1 Labs que utilizaban QRadar para evaluar el retorno a la seguridad. Los dos clientes proveían servicios al Gobierno de los Estados Unidos en la zona de Washington, D. C. Ambas organizaciones contaban con ambientes de alta seguridad y manejaban datos extremadamente sensibles. Además de las entrevistas, IANS también utilizó encuestas y modelos de costo de tecnología de seguridad de su base de clientes existente.

Los datos que se obtuvieron mediante las entrevistas permitieron a IANS crear un cálculo cuantificado de los costos y beneficios totales, sacando conclusiones con relación al valor de Q1 Labs QRadar y haciendo cálculos razonables de los beneficios netos en un período de tres años.

El retorno total es la suma del objetivo, infraestructura, riesgo y retornos de agilidad. Con base en las suposiciones anteriores, contamos con dos cálculos del retorno total en un período de tres años, uno para cada uno de los casos de riesgo genérico:

RETORNO TOTAL NETO “PROMEDIO” ESTIMADO: +$14,083,000

RETORNO TOTAL NETO “MÍNIMO” ESTIMADO: +$673,000

Los dos casos anteriores producen un retorno positivo a la seguridad de tres años para QRadar, después de incluir el costo total de la adquisición y del despliegue del sistema.

Es preciso notar que el retorno objetivo por si solo no sólo es positivo sino que varias veces es mayor al costo de adquisición y de despliegue. En otras palabras, aunque no hubiera infraestructura o retorno de agilidad, y aun cuando se sobre estimara de forma considerable el retorno del riesgo de seguridad, el retorno total de QRadar resultaría positivo y bastante considerable.

Asimismo, el producto proporcionó grandes beneficios inesperados para ambos clientes. En general, el producto crea eficiencia y eso permite que el equipo de seguridad se enfoque en su misión de forma más eficaz, a un costo significativamente menor a los beneficios que proporciona.

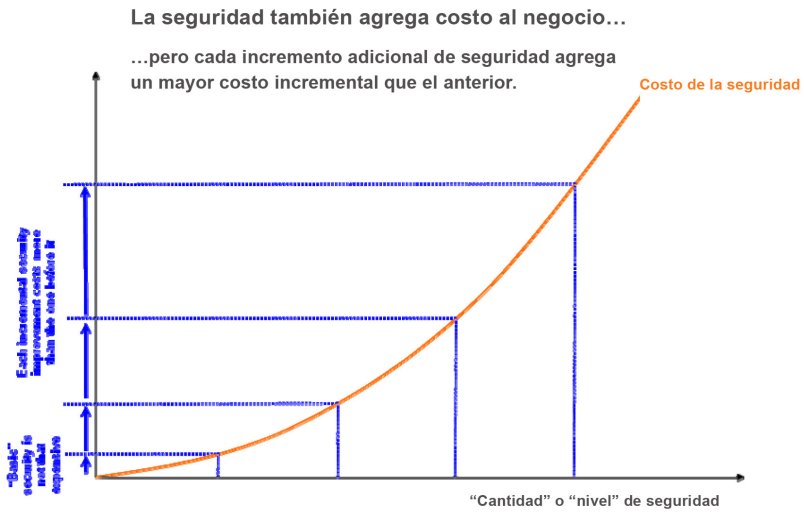
En el caso de ambos clientes, el personal de seguridad operativa está muy satisfecho con el desempeño del producto Q1 Labs QRadar, que no sólo cumplió sino que excedió todas sus expectativas, y sigue proporcionando un beneficio sustancial a la organización por su costo, tanto en dinero como en tiempo del personal, que la organización considera razonable y costeable.

Metodología

Es probable que un proyecto de seguridad (que utiliza un producto, mejora una política, lanza un programa de creación de conciencia, etc.) produzca valor en forma de beneficios que pesen más que los costos. Mantener dichos costos y beneficios bajo control también puede ayudar a los ejecutivos a tomar mejores y más informadas decisiones con respecto a la asignación de recursos. En la última década, los ejecutivos de seguridad han experimentado con una gran variedad de análisis costo beneficio y han tenido en general poco éxito. La metodología IANS ROS tiene como objetivo corregir las desventajas de otros análisis costo beneficio y producir un sistema de medición que se adapte específicamente a las cualidades específicas de un proyecto de seguridad.

En teoría, calcular el valor del producto, proyecto o procedimiento de seguridad no debería ser diferente a valuar cualquier otra cosa; para ponerlo en términos sencillos: agregar beneficios y restar costos y si aplica, ajustarse al tiempo de los beneficios y de los costos. La diferencia en la esfera de la seguridad consiste en que tanto los beneficios como los costos son más complejos de analizar, más difíciles de identificar con precisión y tienen relaciones complejas entre sí. Asimismo, existen fuentes con mayor potencial de incertidumbre que en otras inversiones, especialmente con respecto al valor de los beneficios. El punto más crítico consiste en que el valor de un proyecto o producto de seguridad específico puede variar con base en otros proyectos de seguridad que estén disponibles así como proyectos de seguridad alternos. Adicionalmente, muchas veces vemos casos en los cuales un cierto nivel mejorado de seguridad ofrece la posibilidad de ir tras una oportunidad de negocio totalmente nueva que en otros casos pudiera resultar impráctica. En este caso, podría decirse que el valor de cualquier producto o proyecto necesario para alcanzar ese nivel de seguridad es el valor total de la oportunidad de negocio, tomando en cuenta el importe neto sin considerar otros costos; sin embargo, en el caso de que haya opciones disponibles, el valor adecuado de la decisión del negocio estará basada en la diferencia en valor entre las diferentes opciones.

Costo de Seguridad Incremental



Asimismo, hay casos en los cuales cierto nivel de seguridad mejorado ofrece la posibilidad de ir tras una nueva oportunidad de negocio que pudiera resultar impráctica en otras circunstancias. En este caso el valor de los productos y proyectos necesarios para alcanzar ese nivel de seguridad podría estar constituido por el valor total de la oportunidad de negocios, tomando en cuenta el valor neto libre de otros costos; sin embargo, en el caso de que haya opciones disponibles, el valor adecuado para la decisión del negocio se basará en la diferencia en valor entre las diferentes opciones.

El Método ROS

En el caso de un proyecto de seguridad, los beneficios incluyen:

- **Valor del Objetivo.** El logro de alguna meta de negocios, por ejemplo: Instalar un firewall conforme al requerimiento del auditor
- **Valor del Riesgo.** La reducción del riesgo, por ejemplo: Se reducirá significativamente el riesgo de robo de los datos bancarios de los clientes.

- **Valor de la Infraestructura.** La mejora de inversiones anteriores, por ejemplo: Al instalar este firewall, el servidor de correo operará de forma más eficiente.

- **Valor de Agilidad.** Hacer posible la creación de nuevos negocios o nuevos procesos de negocios, por ejemplo: Los empleados pueden trabajar en casa de forma segura.

Los costos de un proyecto de seguridad incluyen lo siguiente:

- **Costo del Objetivo.** El precio de compra, despliegue y mantenimiento del programa, por ejemplo: Cuota de licencia $ 100,000 + 15% de mantenimiento anual + 1.5 de meses hombre de mano de obra

- **Costo de la Infraestructura.** La degradación de inversiones anteriores, por ejemplo: Al instalar este firewall, el servidor de aplicaciones será menos utilizable.

- **Costo de Agilidad.** La inhibición del negocio, por ejemplo: Los empleados ya no podrán realizar investigaciones por Internet sin restricciones.

Por consiguiente, medir el valor de un proyecto de seguridad requiere lo siguiente:

Sumar;
Valor del Objetivo + Valor del Riesgo + Valor de la Infraestructura + Valor de Agilidad

Y restar;
Costo del Objetivo + Costo de la Infraestructura + Costo de Agilidad

Hallazgos

Evaluación y Análisis de los Resultados

Retorno del Objetivo – ¿Cuáles son los costos y beneficios de sencillamente lograr el objetivo que los clientes se fijaron en un lapso de tres años?

Los clientes deseaban una solución gerencial de información que les permitiera recibir alertas en tiempo real de eventos específicos desde una variedad de fuentes de cómputo y de red, que investigara y diera respuesta en tiempo real. Los principales motivadores para la compra de QRadar consistían en aumentar la eficiencia del personal de seguridad, reducir los tiempos de respuesta a los incidentes, evitar amenazas de seguridad y administrar el cumplimiento con los requerimientos NIST.

Para ambos clientes, QRadar cumplió o excedió todas las expectativas, y en ambos casos, el personal de seguridad operativa quedó muy satisfecho con su desempeño.

El costo inicial de QRadar, el mantenimiento anual y el soporte de servicios profesionales estuvo dentro del rango presupuestado asignado por cada cliente. La instalación y el soporte tomaron más tiempo del que se había presupuestado inicialmente, pero una vez que llegaron los servicios profesionales, la configuración dio resultados rápidos. Los clientes estimaron que QRadar tardaba menos tiempo, requería menos esfuerzo y costo que las opciones de la competencia que estaban considerando.

Calculamos el retorno neto relativo a los precios de lista para una instalación típica. Dichos precios eran de $128,700 para la aplicación y software QRadar, un 18% continuo ($23,166) de cuota de mantenimiento que inicia al segundo año así como la cuota única de $7,500 por concepto de capacitación del usuario y del administrador.

El uso de QRadar por parte de cada cliente varia de acuerdo con el tamaño de su red y la intensidad de uso. El costo total del cliente incluye no sólo el costo del hardware, software y de capacitación sino también el costo del tiempo del personal que se encarga a la configuración inicial y el uso continuo del producto. Con base en nuestras entrevistas, calculamos los costos adicionales de un cliente "típico" que asume un costo de mano de obra de $ 140 por hora (con carga total) y una semana de trabajo de 40 horas.

Calculamos un costo total de instalación que incluye equipo, servicios profesionales, capacitación y tiempo del personal (tanto para la configuración inicial como para el seguimiento) de aproximadamente $141,000.

Calculamos que un cliente "típico" incurrirá en un costo continuo incluyendo tiempo del personal de aproximadamente $58,000 al año con QRadar (incluyendo tanto la cuota de mantenimiento como el tiempo del personal), comparado con $280,000 al año de tiempo del personal para realizar una parte de la misma tarea sin QRadar. Estos cálculos incluyen tanto la cuota de mantenimiento anual y el tiempo de uso del personal, y esto se basa en nuestras entrevistas.

Bajo las suposiciones anteriores, para un ciclo de vida de tres años del producto, el retorno objetivo total consiste de los costos siguientes:[1]

Costo de adquisición inicial y de despliegue:	-$141,000
Cuota de mantenimiento anual (2 años @23,000):	-$46,000
Uso anual por parte del personal (3 años @35,000)	-$105,000
COSTO TOTAL:	-$292,000

… así como los siguientes beneficios:

Tiempo anual del personal sin QRadar (3 años @280k)	$840,000

Y combinando estas cifras, tenemos lo siguiente:

RETORNO DEL OBJETIVO NETO CALCULADO A 3 AÑOS:	+$548,000

1 Los costos de los componentes se redondean a miles de dólares.

Retorno de la infraestructura –¿Cómo se logra que los sistemas preexistentes sean más eficientes o eficaces como resultado en un período de tres años?

Mientras que QRadar se desplegó originalmente para manejar y monitorear eventos de seguridad, frecuentemente QRadar detectaba eventos que en realidad eran el resultado de sistemas de red mal configurados. Un cliente descubrió un servidor que se estaba tratando de contactar consigo mismo cientos de veces por segundo. Por el hecho de que QRadar detectara este evento de "seguridad", el operador de seguridad pudo contactar al administrador del servidor para que arreglara la configuración del servidor; y como resultado, el servidor y los interruptores de la red ahora funcionan de forma más eficiente, sin los costos operativos de una gran cantidad de tráfico inútil.

Los clientes manifestaron que con QRadar, "La seguridad y el desempeño van de la mano", y que el personal de seguridad a menudo descubre problemas operativos antes de que lo haga el personal de operaciones. Calculamos que cada cliente ha descubierto cinco posibilidades de ahorrarle 5 horas al personal de redes.

Tiempo ahorrado al personal de redes ($140 x 5 x 5)	+$1,400

Resulta difícil calcular la frecuencia de este tipo de evento o asignar un valor en dólares al beneficio de solucionarlo. Por consiguiente, adoptamos un enfoque conservador y asumimos que en un ciclo de vida de tres años del producto, el cliente promedio experimenta ese hecho una vez y el beneficio puede compararse con el ahorro que implica evitar una infección de virus en el software. Los analistas de la industria han estimado el costo de lo anterior en aproximadamente $2,000 y los proveedores de antivirus como Trend Micro lo han estimado en una suma hasta de $20,000 por incidente. Nosotros tomamos un cifra más conservadora (+$2,000). Ya que este problema se descubriría en el curso del uso normal de QRadar, no hay ningún costo adicional relacionado con este retorno.

RETORNO NETO EN INFRAESTRUCTURA ESTIMADO A 3 AÑOS:	+$10,200

Retorno del Riesgo – ¿Cuales son los costos y beneficios de la actitud en torno al manejo de seguridad y de riesgo para esta organización?

Definimos el "riesgo de seguridad" como el riesgo de daño al cliente debido al acceso no autorizado a información sensible, fraude financiero y actos mal intencionados similares. Mediante esta definición, estamos excluyendo riesgos sin objetivo fijo o accidentales, que se conocen mejor como virus o malas configuraciones de los servidores.

QRadar evita lo que un cliente llama "el problema Sony" que impide la divulgación no autorizada de información y hace posible responder de forma más rápida cuando ocurren ciertos eventos. En ese caso, un servidor Apache sin parches de seguridad tuvo un problema de vulnerabilidad de seguridad mientras que QRadar habría detectado el patrón de tráfico atípico provocado por la vulnerabilidad sin parches de seguridad, creando la posibilidad de que el problema se pudiera solucionar antes de que provocara daño.

Como resultado de recibir alertas en tiempo real en vez de reportes después de los hechos, el equipo de seguridad tiene la capacidad de evaluar y mitigar el riesgo, detener intrusiones y solucionar los ajustes que fallan en un sistema de forma inmediata, reduciendo sustancialmente la duración y el grado del probable daño. Ambos clientes reportaron por lo menos cinco casos en el primer año en los cuales QRadar había alertado al personal de seguridad de algún problema de seguridad que de no haber obtenido respuesta en tiempo real, habría tenido un efecto muy dañino.

El riesgo a la seguridad es uno de los retornos más difíciles de evaluar. La probabilidad de algún incidente varía ampliamente de un cliente a otro. De manera similar, el rango de costos potenciales va desde unos cuantos miles de dólares a muchos millones. Por consiguiente, proporcionamos dos estimaciones, una para un caso "promedio" que representa el retorno de un cliente promedio, y otra para un "caso de bajo retorno", con la intención de capturar el beneficio mínimo que un cliente en el mercado objetivo pudiera esperar.

El caso "promedio" tiene como objetivo un cliente que en ausencia de QRadar, experimenta un promedio de cinco fallas de seguridad al año, con un costo promedio de $1 millón de dólares por incidente. Asumimos que QRadar redujo la cantidad de incidentes en un 90%, sin cambiar el costo por incidente. El resultado de lo anterior redunda en ahorros esperados de $ 13.5 millones en un ciclo de vida de tres años:

RETORNO DEL RIESGO NETO ESTIMADO "PROMEDIO": +$13,500,000

El "bajo retorno" o caso "mínimo" tiene como objetivo a un cliente que en ausencia de QRadar, enfrenta una posibilidad del 10% de una sola falla de seguridad al año, con un costo promedio esperado por incidente de $300,000. De nuevo, asumimos que QRadar reduce el número de incidentes en un 90%, sin cambiar el costo por incidente. El resultado es un ahorro esperado de $90,000 en un ciclo de vida de tres años.

RETORNO DEL RIESGO NETO "MÍNIMO" CALCULADO: +$90,000

Los casos anteriores se basan en suposiciones genéricas; los clientes que poseen información más precisa de su propio perfil de riesgo deberán utilizar dicha información en vez de las suposiciones anteriores. Asimismo, vale la pena considerar que las evaluaciones de dichos casos están basadas en la pérdida (estadística) esperada, que constituye la base del concepto de "expectativa de pérdida anualizada". Un cliente racional con aversión al riesgo generalmente valorará una mejora en seguridad más que la reducción de la pérdida esperada.

Retorno de Agilidad

Ambos clientes reportaron cierto número de ocasiones en las que QRadar identificó errores en la red o errores de aplicación que habrían pasado desapercibidos o cuyas causas habrían permanecido como un misterio durante meses, consumiendo docenas o hasta cientos de horas hombre. Sin embargo, la característica de reportes eficaces del producto hizo posible que el equipo de seguridad solucionara los problemas de una manera muy directa.

Para un cliente, QRadar identificó por lo menos cinco problemas de seguridad al año que anteriormente habrían pasado desapercibidos, acceso no autorizado a aplicaciones y anomalías en el firewall.

Sin QRadar, se encontrarían en una situación "a ciegas pero feliz" en la cual muchos eventos de seguridad no se habrían detectado.

Adicionalmente, los clientes establecen reglas a la medida con base en información externa, por ejemplo: Los clientes fácilmente descargan listas web de computadoras principales sospechosas para activar alertas cuando hay tráfico de salida hacia destinos sospechosos. Los clientes creen que se habrían perdido de dichos eventos con el sistema anterior.

Como en el caso del retorno de la infraestructura, resulta difícil calcular la frecuencia de este tipo de evento o asignar un valor en dólares al beneficio de solucionarlo. De nuevo, adoptamos un enfoque que nos parece conservador en este caso y asumimos que en un ciclo de vida de tres años del producto, el cliente promedio experimentará tres de dichos casos, y el beneficio podrá compararse con el ahorro que implica evitar una infección de virus en el software. El resultado consiste en un retorno de $6,000 al año o de $18,000 a lo largo del ciclo de vida de tres años del producto.

RETORNO NETO DE AGILIDAD ESTIMADO:	+$18,000

Resultados

El retorno total consiste de la suma del objetivo, la infraestructura, el riesgo y el retorno de agilidad. Con base en las suposiciones anteriores, tenemos dos cálculos del retorno total en un período de tres años, uno para cada uno de los casos de riesgo genérico:

RETORNO TOTAL NETO “PROMEDIO” ESTIMADO:	+$14,076,000
RETORNO TOTAL NETO “MÍNIMO” ESTIMADO:	+$666,000

Estos dos casos producen un retorno positivo de seguridad a tres años relativo a QRadar, incluyendo el costo total de adquisición y de despliegue del sistema.

Cabe notar que el retorno objetivo en sí no solo resulta positivo sino que es varias veces mayor que el costo de adquisición y de despliegue. En otras palabras, aun en ausencia del retorno de infraestructura o de agilidad y aun cuando el retorno por riesgo de seguridad se hubiera calculado de más, el retorno total de QRadar resultaría positivo y bastante considerable.

Asimismo, el producto proporcionó beneficios impredecibles sustanciales a ambos clientes. En general, el producto crea un equipo de seguridad más eficiente y con mayor enfoque que resulta más eficaz en su misión, a un costo sustancialmente menor a los beneficios adquiridos.

En el caso de ambos clientes, el personal de seguridad operativa está muy satisfecho con el desempeño de QRadar de Q1Labs, que cumplió o excedió todas las expectativas, y proporciona un beneficio sustancial a la organización a un costo que la organización juzga razonable y costeable, tanto en dinero como en tiempo del personal.

Acerca de IANS

IANS, fundado en junio de 2001 como el Instituto de Seguridad Aplicada de Redes; se inspiró en el método de Sócrates que consiste en llevar a cabo sesiones de discusión interactivas que promuevan el conocimiento profundo colectivo. IANS adaptó este formato para que se ajustará a las necesidades de los profesionales de la seguridad de la información, y se enfoca exclusivamente en los campos de seguridad de la información, cumplimiento regulatorio y administración de riesgo de TI. La misión de IANS consiste en proporcionar conocimiento profundo técnico y de negocios que ayude a sus clientes a resolver los problemas que más los presionan.

Acerca de Q1 Labs y de la Plataforma de Inteligencia de Seguridad QRadar

Fundada en 2001, Q1 Labs es un proveedor global de productos de inteligencia de seguridad de alto valor, costeables y de siguiente generación. El producto que representa el emblema, la Plataforma de Inteligencia de Seguridad QRadar, integra funciones previamente dispares, incluyendo a SIEM, administración de riesgo, administración de bitácoras, análisis de comportamiento de la red y administración de eventos de seguridad, en una solución total de inteligencia de seguridad, convirtiéndola en la solución de inteligencia de seguridad más inteligente, integrada y automatizada que existe.

QRadar, la Plataforma de Inteligencia de Seguridad de Q1 Labs, proporciona una solución de seguridad inteligente, integrada y automatizada que proporciona inteligencia de 360º en toda la red, sin importar su tamaño.

La Plataforma de Inteligencia de Seguridad QRadar proporciona una arquitectura unificada para recolectar, almacenar, analizar y consultar bitácoras y datos relacionados con las amenazas y con la vulnerabilidad y el riesgo. Como resultado, los operadores, analistas y auditores que utilizan cualquiera de los módulos de la Plataforma de Inteligencia de Seguridad obtienen beneficios como los que se muestran a continuación:

- Arquitectura unificada de colección, agregación y análisis para bitácoras de aplicación, eventos de seguridad, datos de vulnerabilidad, datos IAM, archivos de configuración y telemetría de flujo de red
- Una plataforma común para todos que busca, filtra, redacta reglas y reporta funciones
- Una sola interfase de usuario, o panel único y sencillo para toda la administración de bitácoras, modelaje de riesgo, priorización de vulnerabilidades, detección de incidentes y tareas de análisis de retorno

Apéndice – Síntesis de las Entrevistas

Entrevista #1

Proveedor: **Q1 Labs**
Producto: **Plataforma de Inteligencia de Seguridad QRadar (QRadar 2000, Aplicación Todo en Uno)**
Fecha de la Entrevista: Mayo 20, 2011

Introducción

La empresa del cliente es proveedor líder en tecnología y servicios y soluciones estratégicas de consultoría, principalmente para agencias gubernamentales. La organización de TI utiliza el dispositivo dentro de la empresa que da servicio a clientes externos; es decir, todas las demás organizaciones dentro de la empresa. Para lo anterior, el producto fue adquirido para su uso en un ambiente que no requiere funciones de dispositivo distribuido. Un requerimiento consistía en cumplir con el Control NIST AU-6(5) y con normas relacionadas. Un solo miembro del equipo desplegó la aplicación QRadar.

Proceso de Adquisición

El entrevistado no se involucró en el proceso de adquisición y no conoce las opciones que pudieron haberse considerado.

Evaluación y Análisis de Resultados

Retorno de Objetivos

La Aplicación QRadar 2000 Todo en Uno cumplió o excedió todas las expectativas y la persona responsable de la seguridad operativa está muy satisfecha con su desempeño. Recibe alertas en tiempo real de eventos específicos y utiliza el sistema no sólo para responder a eventos de seguridad sino para proporcionar ayuda a los clientes dentro de su organización. Se ha logrado el cumplimiento con la norma relevante NIST.

Antes de instalar dicho dispositivo, la única manera de lograr el mismo objetivo consistía en escribir secuencias de comandos grep y perl para archivos syslog múltiples en sistemas distribuidos (no todos están disponibles para el personal de seguridad) y en dar seguimiento a cada hallazgo de forma manual. En la actualidad, el entrevistado pasa alrededor de una hora al día en procesar información producida por QRadar. Él estima que el seguimiento de alertas de seguridad que de otra manera habría llevado la mitad del día, ahora pueden terminarse en 15 minutos en promedio. Esto representa una reducción del 94% en el tiempo que el personal dedica a dicha función.

Calculamos el componente de tiempo del personal correspondiente al costo de instalación (tanto configuración inicial como seguimiento) en $5,000 aproximadamente. Calculamos el costo correspondiente al tiempo continuo del personal en $35,000 al año aproximadamente con QRadar, comparado con los $280,000 al año correspondientes al tiempo que el personal tarda en terminar una parte de la misma tarea (retorno básico de infraestructura) sin QRadar. Dichos cálculos se basan en un costo de mano de obra de $140 por hora (con carga completa) y una semana de 40 horas de trabajo.

Retorno de Infraestructura

Adicionalmente, QRadar detectó eventos que parecían ser eventos de seguridad pero que en realidad eran el resultado de sistemas mal configurados. Él utilizó el ejemplo de un servidor que está tratando de contactarse consigo mismo cientos de veces por segundo. Porque QRadar detectó este evento de "seguridad", el operador de seguridad pudo contactar al administrador del servidor para que arreglara la configuración del servidor; los interruptores del servidor y de la red ahora funcionan de manera más eficaz, sin los gastos fijos de una gran cantidad de tráfico inútil. El entrevistado afirmó que con QRadar, la "seguridad y el desempeño van de la mano" y que el personal de seguridad a menudo descubre problemas operativos aún antes de que lo haga el personal operativo.

La seguridad con QRadar evita lo que él llama "el problema Sony", que impide la divulgación no autorizada de información y hace posible responder más rápido cuando ocurren los eventos. En ese caso, un servidor Apache sin parches de seguridad sufrió una vulnerabilidad de seguridad; y aun cuando QRadar no determina directamente si los parches de seguridad del sistema están actualizados, habría detectado el patrón de tráfico atípico posibilitado por la vulnerabilidad sin parches de seguridad y eso hace posible arreglar el problema antes de que ocurra un daño mayor.

El costo inicial incluía cuatro horas de capacitación por parte de Q1 Labs, aun cuando el entrevistado no se dio cuenta de esto sino hasta cierto tiempo después, cuando el sistema ya estaba funcionando. Inicialmente pudo configurar el sistema en un día utilizando información obtenida del (los) manual(es) y de foros en línea. Agregó que estos últimos habían resultado especialmente útiles. Logró utilizarlo de manera más eficaz después de tomar el curso de capacitación.

Retorno de Riesgo

Debido a que ahora recibe alertas en tiempo real, tiene la capacidad de evaluar y de mitigar el riesgo, detener las intrusiones y arreglar los ajustes que fallen en el sistema, reduciendo sustancialmente la duración y grado del posible daño.

Retorno de Agilidad

La aplicación ayuda a manejar los rechazos del firewall, así como los incidentes de no repudio en los cuales los usuarios han intentado de forma intencional utilizarlo sin autorización y le han intentado dar otros usos. Sin QRadar, se encontrarían en una situación "ciega pero feliz",donde la mayor parte de los eventos de seguridad habrían pasado totalmente desapercibidos.

Supervisión

El equipo no cuenta con ningún sistema formal que se haya puesto en operación para medir o reportar el retorno de la aplicación QRadar. En el caso de tareas que inicia el cliente, éstas cuentan con un sistema de medición de desempeño con base en la rapidez con la que satisfacen al que llama.

Entrevista #2

Proveedor: **Q1 Labs**
Producto: **Plataforma de Inteligencia de Seguridad QRadar (Aplicación QRadar 2100 y QRadar 3100)**
Fecha de la Entrevista: Mayo18, 2011

Introducción

La organización del cliente es una agencia gubernamental preocupada por la seguridad de su red y que administra el tráfico entre los hosts interno y externo, La agencia tiene un equipo de seguridad de operaciones que consiste de seis a ocho miembros. Anteriormente, la agencia tenía numerosos sistemas independientes ((IDS, firewall, web/AV, servidor proxy, etc.) que proporcionaban alertas y reportes de diferentes tipos en diferentes formatos, sin manera alguna de integrar todas las diferentes fuentes de información. Con base en los reportes después de los hechos, la información recibida no necesariamente resultaba oportuna y no había una manera fácil de buscar correlaciones entre los reportes de las diferentes fuentes. La agencia buscó una solución que integrara las diferentes fuentes de información y generara alertas en tiempo real procesables para poder manejar y resolver los problemas de forma inmediata.

Proceso de Adquisición

La empresa solicitó propuestas y recibió diferentes presentaciones de diversos proveedores. Ellos seleccionaron a QRadar principalmente por su costo razonable y bajos gastos fijos de administración. La agencia contaba con cierto financiamiento de fin de año disponible que iba de acuerdo con el precio, y el personal deseaba tener acceso a información en tiempo real y no tenía tiempo de vaciar los informes buscando la información que necesitaba. Una opción que rechazaron consistía en el sistema ArcSight, que se consideró demasiado caro y al parecer, requería demasiados gastos fijos de administración.

También les gusto el producto que venía como una sola aplicación con una plataforma Linux que iba de acuerdo con sus conocimientos.

Evaluación y Análisis de Resultados

Retorno de Objetivos

QRadar cumplió o excedió todas las expectativas, y el equipo de seguridad operativa está muy satisfecho con su desempeño. Reciben alertas en tiempo real de eventos específicos y pueden investigar y manejarlos en tiempo real, conforme a su objetivo.

La compra de QRadar incluía una cierta cantidad de horas de apoyo de servicios profesionales. Sin embargo, el equipo tuvo algunas dificultades para obtener el apoyo programado. No sabemos si lo anterior fue el resultado de la falta de comunicación o disponibilidad por parte del cliente o por parte del proveedor. En cualquier caso, el resultado consistió en que tuvieron a QRadar durante tres a cuatro meses antes de que el personal de apoyo viniera a capacitar al equipo en el uso del mismo. Durante este tiempo, se instaló la aplicación; sin embargo, ésta producía muy poco si no es que ningún valor. No obstante, una vez que se proporcionó el apoyo, el equipo pudo hacer que le configuraran la aplicación y que produjera información muy útil en un período breve.

Retorno de Infraestructura

Las capacidades de QRadar han proporcionado beneficios adicionales que exceden las metas relacionadas con seguridad que era el propósito inicial. Por ejemplo, ahora el equipo de seguridad puede identificar a usuarios y actividades que requieren un gran ancho de banda, y exhortar a los usuarios a trasladar dichas actividades a horas no pico, para mejorar la eficiencia global de la red. Adicionalmente, han podido responder a peticiones (enviadas por personal de apoyo de TI de bajo nivel) de usuarios con problemas de desempeño del servidor, que han podido solucionar con información de QRadar.

Retorno del Riesgo

Debido a que ahora recibe alertas en tiempo real en lugar de reportes después de los hechos, el equipo de seguridad tiene la capacidad de mitigar y detener las intrusiones de forma inmediata, reduciendo sustancialmente la duración y el grado del posible daño.

Retorno de Agilidad

El equipo puede establecer reglas a la medida con base en la información externa. Por ejemplo, puede descargar listas de hosts sospechosos y desencadenar alertas de sitios de Internet cuando hay tráfico de salida hacia destinos sospechosos. El equipo cree que se habría perdido completamente de dichos eventos con el sistema antiguo.

A unos 15-18 meses de la instalación de la aplicación, se integró al equipo un empleado adicional con experiencia previa que había trabajado con sistemas similares, y esto aumentó todavía más la capacidad del equipo de obtener valor de la aplicación (igual que su capacidad de aprovechar la experiencia del nuevo integrante del equipo).

Supervisión

El equipo no cuenta con ningún sistema formal para medir o reportar el retorno a la inversión de la aplicación QRadar. Sin embargo, cree que cuenta con la confianza de su administración, que entiende el valor que el equipo proporciona a la organización y confía en su capacidad para seleccionar las herramientas idóneas para el trabajo.