Q1Labs®
Total Security Intelligence

S1 CORPORATION

QRadar® presenta Mejoras para las Emergentes Amenazas de Seguridad

A principios de 2007, el equipo de seguridad de S1 tuvo la difícil tarea de garantizar que S1 estuviera en conformidad con el estándar PCI DSS cuando se realizara la auditoría a fin de año. Al igual que otros gestores de pago, debían desarrollar un sistema compatible y eficaz, de lo contrario, podrían recibir fuertes multas, suspensiones y, posiblemente, la revocación de los privilegios de procesamiento de tarjetas de crédito.

S1 CORPORATION (NASDAQ: SONE) BRINDA SOFTWARE DE INTERACCIÓN CON EL CLIENTE PARA SERVICIOS FINANCIEROS Y DE PAGO. Más de 3.000 clientes en todo el mundo usan las soluciones de software de S1, las cuáles incluyen aplicaciones para casi todos los segmentos del mercado y todos los canales de entrega. Los bancos comunitarios, los bancos regionales, los bancos nacionales, las cooperativas de crédito, los minoristas, las telecomunicaciones y los procesadores confían en el software bancario y de pago que ofrecen las siguientes tres marcas: Postilion, S1 Enterprise y FSB Solutions. S1 cuenta con más de 1.400 empleados de operaciones en las regiones de América del Norte, Europa, Medio Oriente, África y Asia Pacífico. S1 trabaja junto con las mejores organizaciones de la industria para brindarles a sus clientes soluciones de software flexibles y escalables. En el 2007, la ganancia total superó los 200 millones de dólares, y entre los productos más importantes para clientes que se incorporaron en el 2007 se encuentran tres de los 15 principales bancos de los Estados Unidos, una de las compañías de comidas rápidas más grande del mundo, una de las compañías de telecomunicaciones más grande del mundo y el fabricante de cajeros automáticos (ATM) más grande del mundo.

Cumplimiento del estándar PCI

Los principales analistas de seguridad de S1, David Screws y Bill Baker, fueron los encargados de identificar una herramienta de administración de monitoreo de seguridad y redes que ayudara a satisfacer los próximos requisitos de conformidad. Además, S1 se preocupaba por cómo proteger correctamente los activos, las inversiones; así como su propiedad intelectual y la de sus clientes. Aunque muchas de las ofertas de administración de registros podían ser de utilidad para satisfacer los próximos requisitos de conformidad del estándar PCI. DSS, David y Bill también tenían en cuenta las necesidades de S1 a largo plazo, y querían una solución que fuera más allá del simple cumplimiento de los requisitos: ofrecer una visibilidad y un análisis completo de las actividades de seguridad de la red.

Bill y Dave habían asumido el compromiso de implementar una oferta integral de monitoreo de seguridad, pero esta solución era "muy difícil": la visibilidad total en las actividades de red también implicaría una excesiva carga de datos. A menos que encontraran una solución que incluyera un motor de correlación integral para priorizar la información, creían que no iban a poder aislar las amenazas debido al gran volumen de datos.

Y Así Comenzó la Evaluación

Hasta ahora, S1 usaba una antigua oferta de seguridad de redes de primera generación de otro proveedor. La frustración con esta tecnología deriva del hecho que no podían extraer datos útiles y precisos del producto sin tener que usar más de 10 profesionales de operaciones y seguridad dedicados a mantener y ejecutar la solución. Para empeorar más la situación, los elementos identificados por la solución anterior generaron

S1 CORPORATION

QRadar® presenta Mejoras para las Emergentes Amenazas de Seguridad

falsos positivos. Debido a que la solución no se basaba en dispositivos, S1 también tuvo que hacer inversiones significativas de capital en equipos y recursos de soporte adicionales.

Después de analizar muchas críticas e informes de la industria, y de evaluar el informe del Cuadrante Mágico de Gartner para la Información de Seguridad y la Administración de Eventos (SIEM), S1 se encontró con que QRadar® SIEM de Q1 Labs parecía ser la solución más integral. Aunque se preparaban para evaluar la oferta de Q1 Labs, David y Bill se comunicaron inmediatamente con otros profesionales de seguridad de la industria para saber qué pensaban de la Plataforma de Inteligencia de Seguridad de QRadar® en su totalidad. Obtuvieron excelentes opiniones del producto y de la compañía.

Cuando S1 comenzó con la evaluación del producto, se fascinaron con lo que vieron. Se impresionaron inmediatamente al ver que QRadar SIEM iba más allá del simple cumplimiento del estándar PCI, ya que se podía escalar a un módulo de evento de seguridad integral que podía ayudarlos a satisfacer sus necesidades y requisitos de informes de incidentes. Además, descubrieron que, gracias a la facilidad de QRadar SIEM para crear reglas personalizadas, el proceso de evaluación se simplificó, a diferencia de las otras soluciones que obligaban al equipo de seguridad de S1 a ingresar una asombrosa cantidad de reglas individualmente. QRadar SIEM también le proporcionó a S1 un sistema flexible que les permitió "profundizar" en datos forenses y, al mismo tiempo, permitirle a los analistas de seguridad encontrar resúmenes ejecutivos de alto nivel en los resultados de incidentes. Bill y David estaban impresionados con el panel de instrumentos SIEM totalmente configurable de QRadar, el cual ofrece un resumen general del estado de la red.

Durante la evaluación, el objetivo principal era garantizar que todo "se adaptara bien al resto". Era autoritario que cualquier solución que implementaran fuera compatible con todos los elementos de la red, dispositivos, enrutadores, conmutadores, firewalls, y con los cientos de servidores Unix y Windows que hospedan su infraestructura corporativa y los datos de los clientes.

> "Evaluamos muchas soluciones de seguridad y conformidad, pero para todas era necesario usar un profesional interno o externo durante tres horas para que desarrollara, de forma personalizada, los conjuntos de reglas y parámetros para que sean compatibles con todos los sistemas operativos y dispositivos. Debido a los próximos requisitos de PCI, necesitábamos una solución que no requiriera el compromiso de tantos recursos para implementarla. De todos los productos que consideramos, QRadar SIEM fue la única solución lista para usar que probamos y que funcionó inmediatamente".

Además, como QRadar SIEM está basada en dispositivos, S1 no tuvo que invertir en equipos para implementar la iniciativa de seguridad; se sorprendieron que pudiera implementarse en los sistemas actuales sin tener que incurrir en gastos adicionales de capital.

Entusiasmo por QRadar SIEM:

> *"Nos quedamos sorprendidos al ver las ventajas de usar QRadar SIEM. El sistema viene con un conjunto de capacidades de gestión de registros preinstaladas y, además, es flexible y fácil de programar, por lo que pudimos modificar las reglas existentes o, simplemente, usar el asistente crear reglas nuevas. Es más, como las reglas están basadas en un sistema modular "de componentes", era lo suficientemente flexible como para crear reglas para cada componente en nuestra red (por ejemplo, base de datos, servidores, clientes, etc.), y nos permitió ajustar la sensibilidad para obtener, en mayor medida, positivos falsos".*

> Toda nuestra infraestructura sigue funcionando correctamente con QRadar SIEM y, además, les avisa a las personas correctas cuando hay algún problema.
>
> **- BILL BAKER,**
> Analista principal de seguridad de S1 Corporation

S1 CORPORATION

QRadar® presenta Mejoras para las Emergentes Amenazas de Seguridad

Los ataques son cada vez más sofisticados, por lo tanto, Bill y David tenían que adelantarse a los intrusos que intentaban destruir la integridad de su red.

> ***"Nos gustó el concepto de ' infracción' de QRadar SIEM", con el que podíamos detectar actividades sospechosas en nuestra red. Con nuestra herramienta de seguridad anterior, era todo un desafío identificar verdaderos comportamientos sospechosos entre la gran cantidad de datos no útiles, y teníamos que depender de un proceso lento y usar otras herramientas para poner la información en contexto. QRadar SIEM fue un alivio porque correlacionaba los datos automáticamente en todos los dispositivos asociados con actividades sospechosas, lo que nos permitió responder, de manera más eficaz, ante posibles amenazas. Si había un intento de intrusión u otra actividad sospechosa, podíamos identificar, inmediatamente, la infracción y ubicar la fuente", dijo Bill Baker.***

S1 Implementa QRadar SIEM:

Después de que S1 seleccionara QRadar SIEM, la implementación se llevó a cabo sin problemas. S1 instaló el dispositivo y puso el sistema en funcionamiento en un día. Más sorprendente aún fue el incomparable soporte de ventas y productos de Q1 Labs. David Screws dice al respecto: "Estoy muy impresionado con su soporte y capacidad de respuesta. Son uno de los mejores proveedores con los que he trabajado en los últimos ocho años. Ojalá otros proveedores fueran como Q1 Labs".

El objetivo de S1 era satisfacer los requisitos de conformidad de PCI DSS y reemplazar un sistema que requería de mucho trabajo para mantenerlo. A pesar de las restricciones de tiempo, S1 pudo implementar y poner en funcionamiento el QRadar SIEM de Q1 Labs sin contratiempos. El soporte posventa fue muy eficaz y brindó mucha ayuda de seguimiento.

> ***Desde que instalaron QRadar, S1 se dio cuenta de que era la solución que estaban buscando. Bill Baker dijo: "El primer día que instalamos QRadar SIEM, identificamos, inmediatamente, una configuración de red incorrecta que hubiera significado el incumplimiento del estándar PCI. Pero pudimos solucionar eso y otros problemas antes de que se hiciera la auditoría de PCI. Desde entonces, toda nuestra infraestructura ha seguido funcionando correctamente con QRadar SIEM, y también les notifica a las personas correctas cuando hay algún problema". Gracias a QRadar SIEM, S1 se pudo cumplir los siguientes requisitos de conformidad: PCI DSS, FFIEC, Sarbanes-Oxley, SAS 70, GLBA y HIPAA.***

> Estoy muy sorprendido con el soporte y capacidad de respuesta. Son uno de los mejores proveedores con los que he trabajado en los últimos ocho años. Ojalá otros proveedores fueran más como Q1 Labs.
>
> **- DAVID SCREW,**
> Analista principal de seguridad de S1, Inc.

Q1 Labs
890 Winter Street, Suite 230
Waltham, MA 02451 USA
1.781.250.5800; info@Q1Labs.com
www.Q1Labs.com

S1CS0311