Servicio de Detección y Respuesta ante ciberamenazas ayuda a los MSPs de Latinoamérica a ofrecer grandes beneficios

Por: Juan Alejandro Aguirre, director de soluciones de Ingeniería para América Latina, SonicWall

La mayoría de las veces, cuando nuestro cuerpo nos alerta sobre algo inusual que lo está afectando preferimos pasar por alto los síntomas leves, pensando en que, si no es nada grave, los dolores pasarán por sí solos, apagando así nuestro sistema de alerta voluntariamente. Sin embargo, a menudo, cuando se trata de alguna afectación grave, nos suele tomar por sorpresa y ya en la sala de emergencias pensamos en que hubiéramos podido prestar más atención a esas pequeñas alertas o picos de actividad inusual para evitar una operación, un tratamiento a largo plazo o una intervención médica incomoda.

Hemos observado que en la ciberseguridad pasa lo mismo. Más de 75% de los ataques registrados se producen fuera del horario laboral, con picos durante la madrugada o cuando no estamos tan alerta por el desgaste que generan las alarmas informativas constantes; nuevamente, apagamos el sistema de detección de riesgos.

Para los proveedores de servicios gestionados (Managed Services Providers, **MSPs**, por sus siglas en ingles), que cada mañana se sienten aliviados al llegar al trabajo y comprobar que todo está en orden, tal vez la pregunta más acertada sería: *"Son las 4 de la madrugada. ¿Sabe quién está respondiendo a sus alertas?"*

Un grupo selecto de MSPs siempre sabe la respuesta a esta pregunta. Pueden estar tranquilos sabiendo que las redes de sus clientes están siendo monitoreadas por un equipo dedicado de expertos en ciberseguridad—ya sea porque han creado un SOC interno, lo cual supone un gasto considerable, o porque cuentan con los servicios de un equipo de detección y respuesta gestionadas (MDR).

MDR, equipo de expertos a su servicio

Los MSPs proporcionan a sus clientes servicios críticos de TI y de ciberseguridad. Los clientes de los MSPs, que no suelen contar con equipos de seguridad propios, confían en que les faciliten soluciones de ciberseguridad efectivas.

Sin embargo, el panorama de las ciberamenazas cambia constantemente: emergen nuevas vulnerabilidades y los cibercriminales utilizan nuevas tácticas, técnicas y procedimientos. De hecho, según el Informe Anual de Ciberamenazas 2024 de SonicWall, aunque el *ransomware* sigue predominando, se detectaron más de 19.000 amenazas al día dirigidas específicamente a pymes, gobiernos y empresas.

Ante esta perspectiva, ¿cómo puede un MSP ofrecer una seguridad más avanzada a sus clientes? Añadir un servicio de detección y respuesta gestionadas (MDR) puede ayudar, no solo porque suma una capa de ciberseguridad, sino también porque facilita el trabajo del MSP.

¿Qué pueden ofrecer los servicios MDR a su negocio?

A continuación, exponemos cinco ventajas de MDR para los MSPs, especialmente para aquellos que sirven a empresas pequeñas y medianas:

1. Monitoreo por parte del SOC 7*24

Dado que los cibercriminales claramente prefieren perpetrar ataques fuera del horario laboral y durante las vacaciones, las alertas de ciberseguridad de herramientas como las de detección de los *end point* o estaciones de trabajo, a menudo se emiten cuando nadie está prestando atención.

Elegir el momento oportuno también es crítico a la hora de responder a los ataques; tan solo unos minutos pueden marcar la diferencia entre una alerta molesta, sin importancia, y un grave incidente de ciberseguridad.

La mayoría de los MSPs simplemente no cuentan con los recursos necesarios para monitorear las alertas a todas horas.

Los servicios MDR como la de **SonicWall** ofrecen monitoreo las 24 horas con el fin de que ninguna alerta pase desapercibida, independientemente de cuándo llegue. Como resultado, la respuesta es inmediata y tanto el MSP como sus clientes pueden disfrutar de una mejor ciberseguridad en general.

2. Análisis de comportamiento realizado por expertos

Por lo general, los MSPs suelen cubrir una amplia variedad de tareas de TI, desde el aprovisionamiento de computadores portátiles hasta la implementación de software empresarial y la gestión de las redes. No todos los MSPs conocen a fondo el cambiante panorama de las ciberamenazas. Además, aunque lo conozcan, suelen estar ocupados con otras tareas.

Lamentablemente, para los MSPs que quieren aumentar su negocio, contratar a los expertos necesarios para mejorar su oferta de ciberseguridad no siempre es tan sencillo como ampliar la nómina de personal. No es ningún secreto que hay escasez de talento en el sector de la ciberseguridad: el número de puestos que requieren talento cualificado en materia de ciberseguridad supera con creces la cantidad de personas cualificadas. Incluso si un MSP cuenta con los recursos necesarios para contratar a analistas de amenazas y crear un equipo para un SOC, a menudo el proceso de contratación les resulta frustrante, por no hablar de lo caro que puede ser.

El SOC 24*7 de **SonicWall**, ofrecido por *Solutions Granted*, cuenta con expertos que aplican la lógica y análisis de comportamiento a las alertas de ciberseguridad. Reconocen las alertas especialmente relevantes y qué cibercriminales o tipos de ataque puede haber detrás de ellas, y encuentran formas de ayudar al MSP a tomar las correspondientes medidas de defensa inmediatas.

3. Reducción de la fatiga por alertas

Las herramientas de ciberseguridad como los antivirus, EDRs, firewalls, IPSs, *Email Security Gategays*, herramientas de filtrado de contenido, etc., pueden generar una enorme cantidad de alertas, de las cuales no todas son realmente urgentes. En medio de esta avalancha de alertas, es fácil pasar por alto las que son verdaderamente importantes y requieren acciones, especialmente para los MSPs, que posiblemente se encuentren ocupados con cualquier otra tarea, desde reunirse con nuevos clientes hasta solucionar los problemas de una impresora.

Confiar en los expertos del SOC que hay detrás del servicio MDR de **SonicWall** puede reducir esta fatiga por alertas. Puesto que el SOC se ocupa del monitoreo y de notificar al MSP cuando una alerta requiere una acción específica, su equipo ya no debe preocuparse de leer todas las alertas, solo las que realmente requieren su atención.

4. Ciberseguridad avanzada para pymes

Muchos MSPs sirven a empresas pequeñas y medianas que no cuentan con sus propios equipos de ciberseguridad. Aunque es fácil caer en la creencia de que algunas empresas simplemente son demasiado pequeñas para ser el blanco de ciberataques, cualquier organización que utilice herramientas conectadas a internet está expuesta. De hecho, algunos cibercriminales dirigen sus ataques contra pymes intencionadamente, suponiendo (a menudo con razón) que están menos protegidas y, por ello, es más probable que paguen los rescates o extorsiones. Las empresas que colaboran con otras más grandes a menudo son blancos atractivos, ya que los perpetradores de ataques

tienen la esperanza de acceder a sus *partners* de mayor tamaño a través de ellas, mediante un ataque en cadena.

Al ofrecer servicios MDR, los MSPs que atienden al mercado de las pymes pueden brindar a sus clientes las ventajas de la inteligencia de ciberamenazas, los análisis avanzados y la mitigación de amenazas, a las que de otro modo posiblemente no tendrían acceso.

En consecuencia, estas pymes pueden adoptar un enfoque proactivo de la ciberseguridad, y el MSP puede proporcionar una rentabilidad continua para sus clientes.

5. Conoce a tu enemigo y conócete a ti mismo

Ya lo decía el general militar, estratega y filósofo chino, Sun Tzu, “si eres ignorante de tu enemigo y de ti mismo, vas a perder todas las batallas”. Y es que en el campo de la ciberseguridad el conocimiento es poder; ante un panorama de amenazas cada día más complejo y tácticas amenazadoras en continua evolución, resulta indispensable desarrollar capacidades sofisticadas de detección y respuesta. Este nuevo paradigma presenta una oportunidad para los canales de ciberseguridad de transferir estas capacidades de detección y respuesta de forma gestionada y como plataforma a sus clientes finales.

Independientemente de que soporte cientos o miles de *endpoints*, los clientes pueden acceder a niveles de ciberseguridad superiores y obtener soluciones escalables en función de las necesidades del negocio.

Al final del día, los clientes pueden estar tranquilos, porque, sea la hora que sea, siempre sabrán quién responde a sus alertas.

Acerca de SonicWall

SonicWall es una pionera en ciberseguridad con más de 30 años de experiencia y que está considerada el proveedor con un modelo de distribución centrado en partners líder del mercado. Gracias a su habilidad de crear, escalar y gestionar soluciones de seguridad en entornos de nube, híbridos y tradicionales en tiempo real, SonicWall ofrece una protección sin fisuras contra los ciberataques más evasivos en cientos de puntos de exposición para usuarios cada vez más remotos, móviles y basados en la nube. Al contar con su propio centro de investigación de amenazas, SonicWall puede proporcionar de forma rápida y económica soluciones de seguridad creadas específicamente para respaldar a cualquier organización—empresas grandes, agencias gubernamentales y Pymes—en cualquier lugar del mundo. Para obtener más información, visite www.sonicwall.com o síganos en Twitter, LinkedIn, Facebook y Instagram.

###

Contactos con medios:

Agencia de Prensa y Relaciones Públicas
Tel: (1) 434 2717
E-mail: prensa@syspertec.co
Bogotá – Colombia