El SOC en acción: el ciclo de vida de una ciberamenaza

El centro de operaciones de seguridad (SOC) de SonicWall vela por la integridad de nuestros clientes 24x7. Cuando una alerta llega al SOC, el equipo se pone manos a la obra. Le explicamos cómo.



El centro de operaciones de seguridad de SonicWall supervisa 24x7 las alertas y comportamientos anormales para proteger a nuestros partners MSP y a sus clientes frente a las ciberamenazas. Cuando llegan alertas de las herramientas de seguridad, los analistas del SOC las investigan.



Las alertas se clasifican como menores, mayores o críticas. El equipo del SOC define reglas y configuraciones que clasifican las alertas automáticamente y después el analista escala o reduce el nivel de alerta según sea necesario.



Las alertas menores denotan actividades anormales en los endpoints, como archivos en cuarentena en carpetas inusuales. Es muy probable que sean falsos positivos. Si es recomendable investigar más, el SOC se pone en contacto con usted por email.



Las alertas mayores se utilizan cuando es seguro que se está produciendo una actividad maliciosa en el endpoint. A menudo, las herramientas de seguridad detienen esa actividad; por ej., un antivirus de nueva generación pone en cuarentena el malware automáticamente. El SOC lo contactará por email y le dirá qué pasos recomienda, como por ej. que los usuarios reciban formación adicional sobre phishing.



Cuando existe la certeza de que realmente está sucediendo una filtración o un incidente, la alerta es crítica. El equipo del SOC entra rápidamente en acción para minimizar los daños y evitar que el riesgo se expanda a través de la red.



Cuando hay una alerta crítica, durante la primera hora, el equipo del SOC llama cada 15 minutos al teléfono de emergencias que usted haya facilitado, y si nadie responde, sigue llamando cada hora. No obstante, los expertos del SOC no esperan a que usted responda para entrar en acción; inmediatamente toman las contramedidas necesarias para detener el ataque y proteger el resto del entorno, normalmente, aislando los endpoints.



El analista del SOC crea un informe para documentar lo sucedido, el alcance del incidente y cualquier otra área afectada. Asimismo, el SOC le hará recomendaciones sobre los siguientes pasos a seguir.



Cuando la amenaza activa se ha eliminado, puede trabajar con su cliente para reparar la red, devolver los endpoints aislados al último estado óptimo y hacer el seguimiento de otras medidas de resolución necesarias.

© 2024 SonicWall. Todos los derechos reservados.