SOC sin SIEM

by Jay Jay Davey

Jay Jay Davey

Líder global de SOC @ Marks and Spencer
30 de octubre de 2023

En un mundo que se aferra a la sabiduría convencional, desafié el statu quo, no por un mero deseo de atención, como pueden sugerir algunos que requerían conocimientos de alimentación con cuchara, sino para arrojar luz sobre ciertas verdades no examinadas. Abordemos la siguiente afirmación que hice:

"Existe la falsa creencia de que se requiere un SIEM para establecer una función de SOC".

Incluso el lector más básico puede discernir la verdad de esta afirmación, que pretendo desarrollar en este artículo. Si bien me esfuerzo por no usar el sarcasmo, dado el torrente de insultos y mensajes sarcásticos que he recibido, mantener la neutralidad aquí puede ser un desafío, así que aquí está mi disculpa de antemano.

El requisito de los SIEM emana principalmente de los proveedores que los venden. A lo largo de mi viaje de investigación, busqué información académica sobre los SOC que operan sin SIEM. Sin embargo, mis esfuerzos se encontraron principalmente con libros blancos, estudios y literatura escritos predominantemente por aquellos interesados en vender SIEM, lo que revela un sesgo inequívoco a su favor.

Volviendo a mi afirmación inicial, la génesis de una función SOC no tiene sus raíces en la adquisición de herramientas. Al explorar las motivaciones detrás de las

empresas que contemplan el inicio de un SOC, uno pronto se da cuenta de que las herramientas suelen entrar en la ecuación mucho más tarde. Sin embargo, hay matices a tener en cuenta, como si se trata de una respuesta instintiva a un incidente. Las innumerables razones por las que una empresa considera un SOC pueden variar, pero existe una esencia compartida:

"Monitorear el entorno técnico para eventos de seguridad. A continuación, analizar y examinar los eventos de seguridad dentro del dominio técnico, y actuar sobre aquellos que cumplan con el umbral de un incidente de seguridad". En resumen, Detectar y Responder.

A la hora de construir un SOC, es imprescindible entender nuestros objetivos, que están integrados en las necesidades de la empresa. Podemos navegar nuestro camino hacia adelante con una comprensión de nuestras limitaciones financieras. Esta comprensión fundamental nos permite evaluar varias estrategias y soluciones. Si bien hay más profundidad en la que profundizar, esto captura la esencia de la empresa

Gastos Operativos (Opex)

Cada decisión que tomo, que afecta las operaciones diarias, repercute con la preocupación de las implicaciones financieras. ¿De qué manera esta elección, o incluso la decisión de no tomar medidas, cambia nuestro gasto operativo, a menudo denominado simplemente Opex? En este intrincado arte de la toma de decisiones, es fundamental comprender los matices de las finanzas empresariales. Este conocimiento lo equipa a uno para comprender la asignación y el propósito de las asignaciones financieras dentro del negocio.

Sin alejarnos demasiado de nuestro tema principal, a la hora de seleccionar soluciones tecnológicas, es primordial protegerse de la escalada inadvertida de costes; Al fin y al cabo, la seguridad es un centro de costes; No genera dinero a menos que sea la misma cosa que se vende. El SIEM, por ejemplo, no es solo un costo singular. Es un mosaico de gastos, desde la ingesta de datos y el almacenamiento de registros hasta la asignación de recursos para el ajuste. Y no hay que pasar por alto el coste sutil pero significativo en el que se incurre por el tiempo dedicado a los falsos positivos. Todas estas facetas, cuando se combinan, pueden hacer que el atractivo de un SIEM no sea tan atractivo, lo que lleva a algunos a buscar soluciones alternativas, potencialmente menos onerosas desde el punto de vista financiero.

En el ámbito de la "detección y respuesta", nuestra misión es clara. Debemos identificar los comportamientos anormales y tener las herramientas para responder a ellos. Esta claridad de propósito simplifica nuestra búsqueda para seleccionar herramientas. Con un profundo conocimiento del entorno técnico, se pueden evaluar las soluciones en función de su rentabilidad y su alineación con los objetivos de la organización.

Entornos en la nube

Las construcciones milenarias de los perímetros tradicionales se han vuelto arcaicas. La metamorfosis provocada por la tecnología en la nube ha ampliado la superficie de ataque al tiempo que ha difuminado los límites de los perímetros. Esta progresión, si bien ha mejorado la eficiencia operativa, ha complicado el ámbito de la seguridad, dando paso a medidas de protección innovadoras. Desde el software como servicio hasta la plataforma como servicio, las soluciones en la nube vienen equipadas con controles de seguridad inherentes, entre los que se encuentran las capacidades de monitoreo.

Sin embargo, esta evolución presenta su propio conjunto de dilemas. Dado que cada solución en la nube genera alertas únicas y especificidades de registro, la información a menudo se redirige al SIEM, que inadvertidamente se convierte en un mero mecanismo de emisión de tickets. Dada la falta de datos de correlación, especialmente si la plataforma funciona de forma autónoma del entorno principal, se podría cuestionar la lógica detrás de la canalización de estas alertas a través de un SIEM. ¿Por qué no emplear un sistema SOAR u otra plataforma de venta de entradas?

Se podría argumentar que los SIEM podrían proporcionar correlación utilizando fuentes de inteligencia de amenazas. Sin embargo, este contraargumento parece superficial cuando se examina. Si una alerta ya significa una amenaza potencial, la mera yuxtaposición con indicadores de compromiso parece redundante. Profundizar en la inteligencia de amenazas revela su naturaleza intrincada,

Los entornos modernos en la nube son autosuficientes y cuentan con sus propios mecanismos de monitoreo, prevención y respuesta, lo que cuestiona la indispensabilidad de los SIEM. Endpoint Detection and Response es un testimonio de ello, ya que ofrece información completa y capacidades de respuesta para los dispositivos supervisados. He sido testigo de entornos que canalizan hábilmente

las alertas de una variedad de plataformas en la nube directamente a un sistema de gestión de servicios de TI, evitando los SIEM y, sin embargo, brindando un servicio eficiente.

Una pequeña aclaración: no me opongo a SIEM. Lo uso a diario, elaborando modelos para aumentar su eficacia y reducir los gastos. Sin embargo, mi enfoque se inclina hacia el pragmatismo. Reconozco que cada SOC tiene matices únicos, y las empresas navegan por la seguridad técnica con perspectivas variadas influenciadas por muchos factores.

A los SIEM les gustan los problemas

La Multitud empuñando horcas de disidencia, defendiendo ferozmente a su señor y salvador, los SIEMs, les ofrezco una propuesta: realizar una evaluación fría y sin prejuicios de sus despliegues de SIEM. Si se analizan las implicaciones financieras de los falsos positivos, junto con la frecuencia de su aparición, y se tienen en cuenta las horas invertidas por personal altamente capacitado en descifrarlos, la sobrecarga de ajustar las reglas analíticas, calibrar los registros en sus orígenes y en el momento de la entrada, y los costos de la ingesta, surge un retrato financiero bastante crudo. En ciertas implementaciones, la ineficacia del SIEM se hace evidente, eclipsada por una proporción abrumadora de falsos positivos.

Sin embargo, es innegable que los SIEM sobresalen en proporcionar visibilidad, un elemento primordial aquí. Sin embargo, la tragedia radica en la ambigüedad de esta visibilidad. Muchas organizaciones, al carecer de la comprensión para priorizar, adoptan una filosofía general: ingerir registros indiscriminadamente y contemplar los detalles más tarde. Sin el conocimiento de sus procesos y activos fundamentales, un soldado encargado de proteger las murallas de un castillo equivale a recibir instrucciones continuas de vigilar cada piedra y grieta sin razón ni tono.

Irónicamente, este enfoque ofusca la visibilidad, enturbiando las aguas que busca aclarar. Así que planteo esto: "¿Visibilidad de qué?" y las respuestas a menudo se hacen eco de generalidades huecas y mediocres como "hackers" o "malware". La esencia de la detección clara y concisa es buscar anomalías y luego crear reglas para producir detecciones significativas, lo que lamentablemente se pierde en la traducción. La detección de malware es predominantemente el dominio de las soluciones de punto final. ¿Y en cuanto a los hackers? Si el último bastión de uno contra sus nefastas actividades es un SIEM, entonces que la fortuna favorezca a los valientes.

Desplazar a la izquierda

El principio de "desplazamiento a la izquierda" ejemplifica una postura proactiva, en la que las medidas preventivas se adoptan antes y no como meras respuestas reaccionarias en etapas posteriores. En el contexto de la seguridad, "desplazarse a la izquierda" implica reenfocar nuestra detección y respuesta a fases anteriores del ciclo de vida del ataque. Es similar a abordar posibles vulnerabilidades o hallazgos en las primeras etapas del marco MITRE ATT&CK o durante los pasos iniciales de la cadena de eliminación. En lugar de simplemente introducir controles en las últimas etapas, el énfasis gira hacia una postura defensiva coherente y significativa que aborde las vulnerabilidades y las rutas de ataque identificadas en las etapas iniciales de un ataque.

He observado que aprovecha la potencia de los lagos de datos para agregar métricas e información clave. Utilizando herramientas como PowerBi, crean un sistema similar a SIEM y una visión más profunda del entorno. El propósito trasciende la mera generación de alertas. En su lugar, busca proporcionar conocimientos profundos que proporcionen a los responsables de la toma de decisiones información crítica, lo que les permite dirigir de forma preventiva el curso de acción. Piense en ello menos como una alarma de incendio que suena durante las llamas, sino más bien como un sistema de alerta meteorológica temprana que pronostica condiciones adversas. ¿No sería mejor identificar un posible incendio mientras se enciende una chispa? En lugar de luchar perennemente contra los incendios y arriesgarse al agotamiento de su equipo y de los recursos empresariales, ¿no sería más sabio mitigar la chispa que los produce? ¿No es ese el sello distintivo de un SOC eficiente?

Reiterando mi punto anterior, numerosas plataformas hoy en día tienen capacidades de monitoreo sólidas. Se pueden extraer datos sin problemas para crear cuadros de mando significativos a través de herramientas como PowerBi aprovechando las API. La mayoría de las veces, las alertas SIEM tradicionales se fijan en dominios de monitoreo como Active Directory o DNS. Sin embargo, cuando una alerta de este tipo resuena, es posible que el intruso ya esté en lo más profundo de su entorno técnico y se enfrente a una crisis ya materializada. Más allá de esto, hay una narrativa convincente en torno a la gestión proactiva de vulnerabilidades y la evaluación de controles, aunque tal discurso merece su artículo dedicado, tal vez para otro momento.

La preocupante dependencia de las herramientas

Imagina, por un momento, que estás en un escenario de incógnita, donde las mismas herramientas en las que has confiado se vuelven inútiles. Es una idea que he discutido con algunas de las mentes más expertas en respuesta a incidentes. La hipótesis es clara: ¿qué pasa si nuestras herramientas estándar fallan? Supongamos que no ofrecen ninguna información. O bien, ¿qué pasa si surge un incidente más allá del alcance de las capacidades de registro y monitoreo de nuestro SIEM? ¿Poseen nuestros analistas la capacidad de entender e interpretar la situación sin la ayuda de SIEM o EDR?

Lamentablemente, el consenso a menudo se inclina hacia el "No". Se ha cultivado una dependencia prevalente en el dominio de los kits de herramientas, dejando de lado la habilidad más rudimentaria pero vital de la detección manual de amenazas. En mi viaje, me he encontrado con casos en los que el SIEM era ineficaz o estaba ausente, lo que me obligó a realizar un ejercicio manual para identificar la presencia de una amenaza (piense en Digital Forensics

Si nuestro SIEM flaqueara, ¿nos mantendremos firmes y competentes en nuestros deberes como profesionales de SOC? ¿O nos desmoronaríamos, atrapados por una dependencia general de la herramienta? Este es un oficio que considero fundamental. Nos dota de una perspectiva matizada, enriqueciendo el contexto más amplio de nuestros esfuerzos. Recuerda, no son las herramientas las que forjan al profesional, sino los conocimientos y habilidades. Si no eres maleable en tu enfoque, la efectividad sigue siendo solo un sueño, lo que te convierte en un pulsador de botones en el mejor de los casos.

Conclusión

Los SOC pueden funcionar sin problemas sin SIEM; No solo existen, sino que prosperan, demostrando una competencia encomiable. Su modus operandi se aparta de las normas convencionales y está esculpido por sus necesidades. Hablando en términos de madurez, a menudo rivalizan, si no superan, a sus contrapartes ancladas por SIEM desde una perspectiva de funcionalidad y costo. Fundamentalmente, un SOC encarna una tríada: personas, procesos y tecnología, todos orquestados hacia un objetivo singular y con propósito arraigado en los requisitos comerciales. Reconozca que no existe una plantilla universal para el éxito de SOC, no hay una talla única para todos; Es único para cada negocio y sus

desafíos. Comprender esta noción aumentará la eficacia y fomentará un enfoque más holístico de los desafíos del SOC. Hay que tener en cuenta muchas consideraciones a la hora de decidir el camino adecuado a seguir para formular un SOC.