IT Webinars

Bitdefender ExtraHop Forcepoint RAPID7

Mayo 2021

Descubriendo SASE y las últimas tecnologías de detección de amenazas

La visibilidad, que se fue perdiendo conforme avanzaba la movilidad y el BYOD, y se complicó con el cloud y el trabajo en remoto, acelerados el año pasado debido a la pandemia, se ha convertido en un punto débil para las empresas. Para detectar amenazas y responder a ellas, necesitamos visibilidad de los múltiples entornos y capas de tecnología que utilizan nuestras organizaciones. Los centros de operaciones de seguridad (SOC) utilizan herramientas como la detección y respuesta de puntos finales (EDR), la detección y respuesta de red (NDR) y la gestión de eventos e información de seguridad (SIEM), una combinación de tecnologías comúnmente conocida como "la triada del SOC", para hacer frente a esta necesidad.

Al mismo tiempo, el mercado está impulsando una nueva arquitectura, bautizada como SASE (Secure Access Service Edge), que permite proporcionar un acceso seguro con independencia de la ubicación de los usuarios, los datos, las aplicaciones o los dispositivos.

Tres tecnologías: EDR, NDR, SIEM y una arquitectura, SASE, que están llamados a proporcionar la seguridad que toda empresa digital necesita y sobre las que debatimos con un grupo de expertos, empezando por Lucas Rey, Channel Manager Spain & Portugal de Forcepoint; Christian Buhrow, Sales Director DACH, IBERIA & ITALY de Extra-Hop; Daniel Vaquero, Cybersecurity Engineer de Ingecom y experto en Rapid7 y Horatiu Bandoiu,

DESCUBRIENDO SASE Y LAS ÚLTIMAS TECNOLOGÍAS DE DETECCIÓN DE AMENAZAS

CLICAR PARA VER EL VÍDEO

> "La mejor manera de detectar una anomalía, una brecha o una amenaza de seguridad es a través del análisis de tráfico"
>
> Christian Buhrow, Sales Director DACH, IBERIA & ITALY, ExtraHop

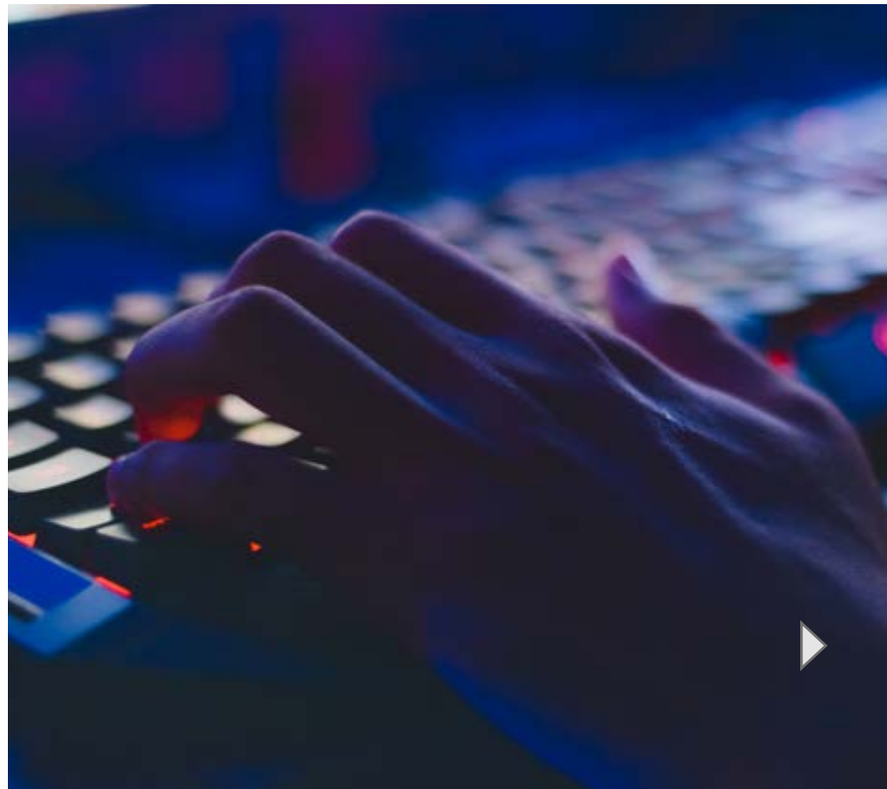
Channel Marketing Manager, SE & LATAM de Bitdefender.

Iniciamos el debate preguntando a Lucas Rey qué es SASE y qué viene a solucionar. Asegura este directivo que SASE es un modelo de entrega de seguridad como servicio que está orientado a cubrir problemas de adopción de servicios cloud en modalidad SaaS, PaaS o IaaS con un conjunto de tecnologías.

Las soluciones de Network Detection and Response, NDR, empiezan a imponerse en el mercado. Se trata de una tecnología "bastante novedosa que cubre la necesidad de tener visibilidad de lo que está pasando en las redes de las empresas", asegura Christian Buhrow. Explica el directivo que los ataques son cada vez más sofisticados y difíciles de detectar y que "la mejor manera de detectar una anomalía, una brecha o una amenaza de seguridad es a través del análisis de tráfico". Asegura también que son muchas las empresas que "se dan cuenta de que tienen falta de visibilidad, que no saben realmente quién está comunicando en mi red, en mi datacenter, y quién se está moviendo dentro de mi infraestructura". NDR viene a solucionar este problema.

Igual que NDR se va imponiendo, las soluciones de EDR (Endpoint Detection and Response) ya están más asentadas en el mercado. Evolución de las soluciones de seguridad de puesto de trabajo, los EDR se están volviendo imprescindibles porque "las empresas se dan cuenta de que el paradigma tradicional de 'tengo un cortafuego y un antivirus y estoy cubierto' ya no funciona", explica Horatiu Bandoiu. Añade este directivo que los EDR son ideales porque trabajan en tiempo real con alertas que proporcionan visibilidad a los analistas de seguridad, pero también ofrecen contención automática para muchas de las incidencias detectadas.

Pasamos a hablar de SIEM preguntando a Daniel Vaquero qué solucionan este tipo de tecnologías y para qué tipo de clientes están pensadas. Frente a las distintas propuestas de seguridad que se han ido planteando dice este experto que se necesita una herramienta que los gobierne a todos, un



centro de mando capaz de recopilar la información de las distintas fuentes y además aportar información relevante que permita ejecutar algún tipo de acción para poder contener las brechas que estamos detectando. Añade que la mayoría de las soluciones hacen la detección y respuesta, “pero cuando queremos automatizar esas respuestas entre distintas herramientas de ciberseguridad, necesitamos que algo los orqueste y en este caso son los SIEM los que toman este liderazgo para poder desplegar acciones lo más automáticas posible”.

Las empresas se enfrentan a cada vez más retos de seguridad, más amenazas y más avanzadas sin un incremento de los prepuestos de seguridad, ¿cómo puede un CISO hacer más con menos? Para el responsable de canal de Forcepoint para España

"La diferencia principal entre las herramientas de gestión de logs y los SIEM es la inteligencia"

Daniel Vaquero, Cybersecurity Engineer de Ingecom y experto en Rapid7

y Portugal, la clave está en utilizar un modelo de plataforma que pueda ajustarse a los desafíos de los propios clientes. “Buscamos una homogeneización de las tecnologías que no sólo genera una mejor operativa, sino que genera ahorros al conseguir una predictibilidad del gasto”, asegura Lucas Rey, apuntando a que esto ya genera ciertos ahorros, a lo que se añade la menor complejidad que conlleva contar con un único fabricante.

Frente a las soluciones de análisis de tráfico de red (NTA) más tradicionales, las soluciones de NDR implican una respuesta. Explica el responsable de ExtraHop en España que el análisis de tráfico es como parte ND antes de la R, y que “por una parte tienes que analizar y luego responder de forma automatizada”

“Aunque los EDR pueden ser tecnologías bastante democráticas, yo empezaría por recomendar dos pre-requisitos”, dice el representante de Bitdefender cuando el preguntamos qué se necesita tener para adoptar una solución de endpoint detection and response. “Para sacar provecho de la herramienta es importante tener al menos un equipo dedicado de seguridad y un proceso de incident response”, asegura Horatiu Bandoiu añadiendo que los EDR son herramientas en tiempo real y tienes que tomar decisiones al instante, por lo que “tienes que mantener una interacción continua con la herramienta,

ALINEADOS CON TU NEGOCIO

www.ingecom.net **Ingecom** info@ingecom.net

BILBAO C/ Elcano 9, 3ª pl - 48008 Bilbao - Tel.: +34 944 395 678 // **MADRID** C/ Infanta Mercedes 90, 8ª pl izq - 28020 Madrid - Tel: +34 915 715 196

algosec · ALIEN VAULT · allot See. Control. Secure. · Array NETWORKS · Bitdefender · CYBONET · Cymulate · efficient iP · ExtraHop · Forcepoint · FORESCOUT · GARLAND · Guardicore

Hdiv · KELA · MEDIGATE · mobileiron · okta · RAPID7 · sealpath · thycotic · Vicarius · viewtinet · wbsgo · ZEROFOX · ZIMPERIUM

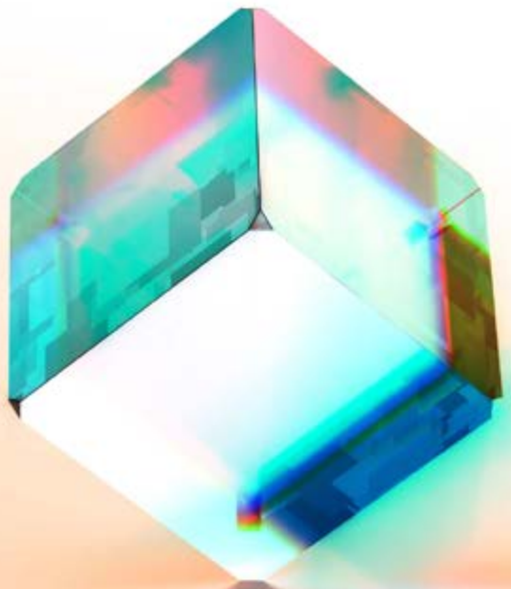
entender las alertas que te da, investigar y, en caso de necesidad, tienes que actuar cortando conexiones, terminando procesos, aislando equipos para su inspección y remediación, etc.”.

El nivel de integración es, en opinión de Daniel Vaquero, una de las características que tiene que tener un buen SIEM, que debe poder recoger información tanto de tecnologías heredadas como de nuevos servicios o productos para poder analizarla y convertirla en una información relevante para poder realizar una toma de decisiones que “debería hacerse de forma automática”.

El servicio SASE trata de consolidar la mayor cantidad de funciones de seguridad en sus nodos, y por tanto se han de considerar la protección en las comunicaciones y accesos y la protección de la información, explica Lucas Rey, añadiendo que una solución SASE debe tener en cuenta la gestión de identidades como uno de sus elementos claves a la hora de tener adoptar esta nueva arquitectura.

Junto con el EDR y el SIEM, el NDR es uno de los tres elementos que forman parte de lo que se denomina la “Triada del SOC” un concepto desarrollado por Gartner que para Christian Buhrow tiene mucho sentido porque son tres tecnologías y fuentes de datos muy diferentes que permiten conseguir en el SOC una visibilidad de 360 grados. “Las tres partes son esenciales”, asegura el directivo de Extra-Hop apuntando a que cronológicamente el SIEM ha sido la primera tecnología en la mayoría de las empresas, que el EDR ha llegado con muchísima inteligencia, conexión a la nube y tiempo real y que NDR cubre la parte de la red donde no se tiene la visibilidad.

La enorme escasez de especialistas de seguridad está impulsando la adopción de servicios de seguridad. Y el hecho de que uno de los retos de la adopción de un EDR sea la necesidad de contar con personal dedicado, ha llevado a algunas empresas, entre ellas Bitdefender, a crear soluciones de MDR



> "Una solución SASE debe tener en cuenta la gestión de identidades como uno de sus elementos claves a la hora de tener adoptar esta nueva arquitectura"
>
> Lucas Rey, Channel Manager Spain + Portugal, Forcepoint

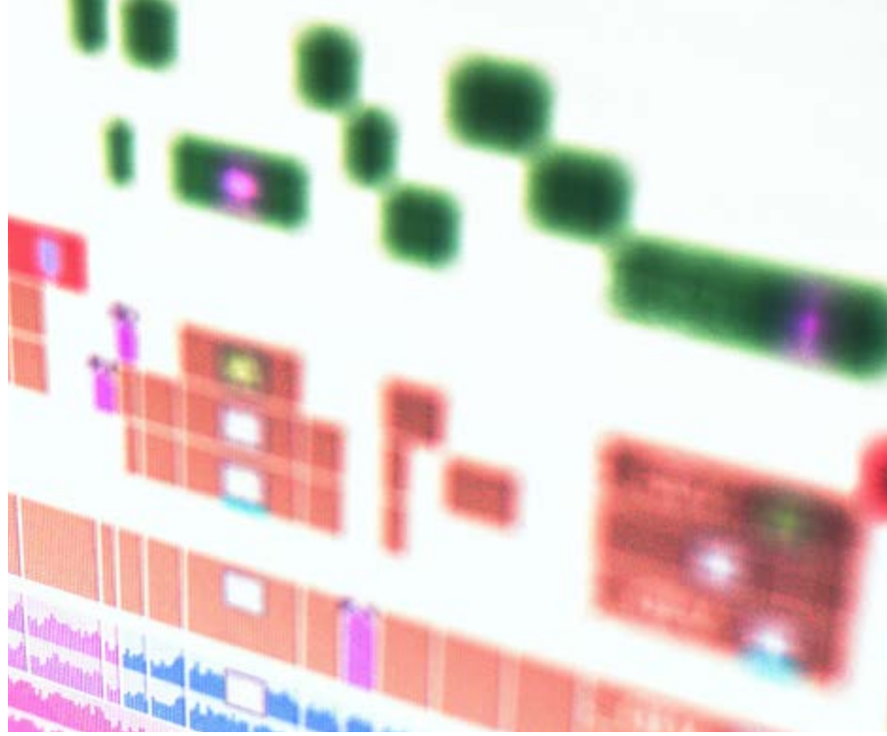
"La tendencia es incorporar las dos tecnologías, EDR y antivirus, y evolucionar hacia el XDR para conseguir una visibilidad completa y una respuesta rápida"

Horatiu Bandoiu, Channel Marketing Manager, SE & LATAM, Bitdefender

(Managed Detection and Response) que ponen a disposición de las empresas "los expertos que pueden hacerse cargo de varios aspectos, desde la detección e investigación y notificación hasta el Incident Response; intervenir y arreglar el problema en su lugar". Cuando el cliente es más avanzado se añaden servicios más avanzados, como el de Threat Hunting, que empieza identificado los activos más importantes del cliente para que después los expertos desarrollen escenarios avanzados de ataque; o la monitorización de la Dark Web para buscar indicios de que uno va a ser atacado o ya le han robado los datos y los quieren vender, por ejemplo.

Al igual que planteábamos la diferencia ente un NDR y una herramienta de análisis de tráfico de red, plantamos cuál es la diferencia entre un SIEM y una solución de gestión de logs. Para Daniel Vaquero estas últimas son importantes y no se suelen tener en cuenta. Asegurando que en algún momento toda empresa será ciberatacada, dice que es importantes analizar qué ha pasado, "y para ello vamos a necesitar la evaluación de los logs. La diferencia principal de estas herramientas con los SIEM es la inteligencia porque "de nada sirve tener logs y eventos infinitos si no podemos utilizarlos". Añade que el SIEM permite hacer correlaciones y "poder desarrollar las respuestas lo más automáticamente posible y con fundamento".

La protección de los usuarios remotos frente al contenido web malicioso y el uso indebido de las aplicaciones en nube es uno de los aspectos a tener en cuenta a la hora de escoger una plataforma



SASE, dice Lucas Rey. Añade el directivo de Forcepoint la capacidad de acceder a las aplicaciones privadas sin necesidad de utilizar VPN, simplemente a través del acceso a nuestra plataforma cloud: "el tercero es la protección del uso de la información en cualquier lugar" y un cuarto aspecto sería "la adopción progresiva con la capacidad de comenzar con unas necesidades inmediatas de SASE y poder ir incrementando otro tipo capacidades a lo largo del tiempo". Menciona Lucas Rey que también debe tenerse en cuenta que la plataforma sea nativa en cloud y capaz de evolucionar para adoptar todas las capacidades que se necesitan actualmente y en el futuro, y que el acceso a los servicios sea flexible.

"Para nosotros análisis de tráfico se refiere a analizar paquetes y hacerlo en detalle y no de manera superficial", dice Christian Buhrow cuando le preguntamos en qué hay que fijarse a la hora de escoger un buen NDR. ExtraHop analiza los paquetes que corren el red desde la capa 2 a la capa 7, se analiza "cada comunicación, cada transacción con la posibilidad de, con dos clics de ratón, entrar en

los paquetes para tener la prueba" de una brecha o de una amenaza. "Para nosotros es imprescindible al hacer análisis de paquetes para llegar al fondo y diferenciar entre sospechar y saber", añade el directivo.

Las soluciones de EDR, ¿reemplazan elementos o tecnologías de seguridad endpoint existentes? Dice Bandoiu que es más lo que aportan que lo que reemplazan. De forma que se puede tener la solución antivirus de toda la vida y montar encima un EDR para que aporte la visibilidad o incluso la capacidad de actuar. Asegura el Channel Marketing Manager de Bitdefender que "la tendencia es de incorporar las dos tecnologías" evolucionando hacia el XDR, o Extended Detection and Response que la compañía ha empezado a proponer al mercado "para conseguir una visibilidad completa y una respuesta rápida".

"La flexibilidad y la escalabilidad son los principales beneficios que aportan los SIEM que han migrado al cloud", dice Daniel Vaquero, añadiendo que constantemente vamos evolucionando y que lo que antiguamente nos parecía que era óptimo se nos ha quedado pequeño y cada vez tenemos más herramientas, más sistemas o incluso más usuarios. Un entorno cloud, dice también este ejecutivo, también nos va a aportar "las actualizaciones de ciberseguridad y la inteligencia en el mismo momento en el que el fabricante las incluye", así como aprovechar toda la capacidad del cloud "para hacer un procesamiento en profundidad, analizar el comportamiento de los usuarios (UEBA o UBA)", y la posibilidad de hacer una orquestación de todas las herramientas de ciberseguridad para no trabajar en silos de forma que se puedan tomar esas decisiones de una manera consciente y con confianza. it

Enlaces de interés...

- Guía para la integración de SecOps y NetOps
- Forcepoint SASE
- Prevención y mitigación de ransomware con Bitdefender GravityZone
- Impulsando el valor de un SIEM en la nube

Compartir en RRSS

itds

IT Webinars

¿Cómo puedo proteger la empresa digital?

“INSIGHTIDR REVOLUCIONA EL CONCEPTO DE SIEM” (RAPID7)

“TRABAJAMOS CON LOS CLIENTES EN UN GASTO PREDECIBLE Y FLEXIBILIDAD FRETE A LOS CAMBIOS” (FORCEPOINT)

“NDR ES EL PILAR FUNDAMENTAL DE LAS TECNOLOGÍA DE DETECCIÓN DE AMENAZAS Y ANOMALÍAS” (EXTRAHOP)

“BITDEFENDER PROPORCIONA UNA PLATAFORMA UNIFICADA DE SEGURIDAD BASADA EN VARIAS CAPAS” (BITDEFENDER)

Clicar para ver los vídeos

Mayo 2021