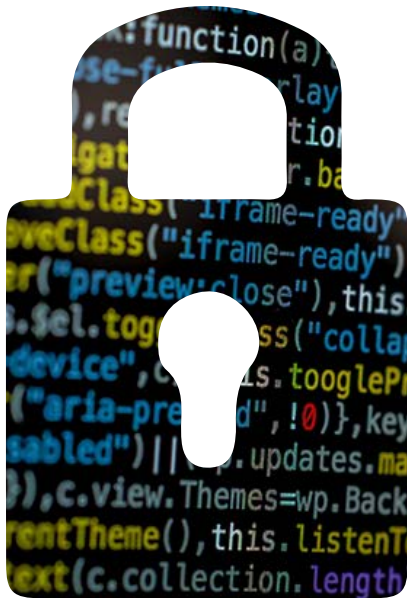


# Detección y respuesta ponen a **las amenazas en la mira**

Imaginemos el radar de un submarino de guerra que patrulla las aguas de su país. Todo está en aparente tranquilidad cuando detecta la presencia de un barco enemigo que podría resultar una amenaza. Una alerta se emite al instante y la tripulación se prepara para iniciar la ofensiva.

Si se lleva este escenario al entorno de negocios donde opera una organización, estaríamos hablando de un equipo completo de expertos en ciberseguridad que están atentos de manera permanente a detectar cualquier posible amenaza y aplicar los protocolos necesarios para responder a ellos, mucho antes de que afecten sus sistemas críticos.



Su misión es aún más contundente cuando el número de amenazas se multiplica, se abren nuevos vectores de ataque y se utilizan innovadoras técnicas y tácticas de ataque. Es por eso por lo que hoy no es suficiente monitorear y alertar sobre lo que sucede en los dispositivos, ni reaccionar a un incidente que ya haya ocurrido. Deben desarrollarse nuevos métodos de **detección y respuesta para detener en seco las amenazas y riesgos.**

### **Rumbo a la proactividad**

Los servicios de detección y respuesta se están convirtiendo en puntos medulares de las operaciones de los centros de operaciones de ciberseguridad. Entre sus principales componentes figuran tecnologías como Endpoint Detection and Response (EDR) o Extended Detection and Response (XDR), los cuales tienen un rol altamente relevante en la detección de comportamientos anómalos.

Tienen, por tanto, la capacidad de aislar, detectar y bloquear en tiempo real dichos comportamientos en los endpoints y servidores, así como cuando se identifica un vector de ataque en el perímetro a fin de aislar los equipos que puedan ser blancos potenciales. Los servicios administrados de detección y respuesta están siendo considerados por las empresas como una forma de elevar la proactividad en sus estrategias de protección.



En 2022, el tamaño del mercado global de Extended Detection and Response (XDR) estaba valorado en 754.8 millones de dólares, según datos de Grand Review Research, y se prevé que se expanda a una tasa de crecimiento anual compuesta de 20.7% de 2023 a 2030.

La fortaleza de la detección y respuesta es integrar técnicas y tácticas de nueva generación que realicen dichas labores de manera automática, utilizando y correlacionando la tecnología de ciberseguridad, y que no solamente se pueda alertar y esperar a que los operadores o administradores de la infraestructura realicen el análisis del comportamiento malicioso detectado.

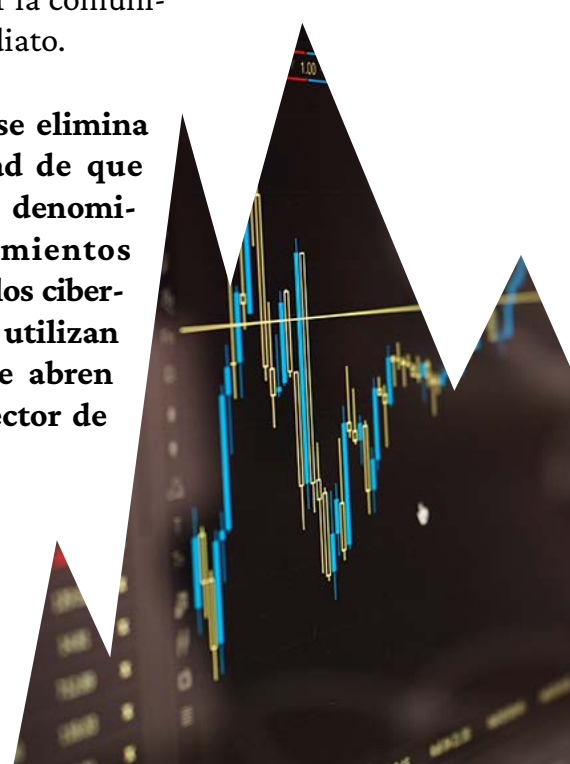
### Tácticas de defensa

La detección y respuesta son el siguiente nivel evolutivo de la seguridad de las organizaciones, que integra tecnología, metodologías, capacidades analíticas, la cacería de amenazas tanto dentro como fuera, así como un profundo conocimiento de las técnicas de ataque más utilizadas. De no tener este panorama, sería muy complicado anticiparse a serias situaciones de riesgo.

Para llevar a cabo las acciones requeridas, los libros de tácticas, o playbooks, son fundamentales para poner a aplicar los casos de uso que se requieren para fortalecer el entorno de protección. De hecho, la tecnología seguirá estas tácticas en caso de que se presente algún riesgo para la red.

Por ejemplo, al detectar que un endpoint o un servidor establece comunicación anómala con otro equipo fuera de la organización, los mecanismos automáticos de protección pueden aislar dichos dispositivos y detener la comunicación de inmediato.

De este modo, **se elimina toda posibilidad de que se realicen los denominados movimientos laterales que los ciberdelincuentes utilizan una vez que se abren paso por un vector de ataque.**



En esencia, un movimiento lateral permite saltar de un servidor vulnerable a otro que no lo es para infectarlo y tomar el control mediante relaciones de confianza. De salto en salto, puede llegarse a los activos críticos de la organización.

El componente de respuesta se encarga, por tanto, de detener por completo esos movimientos laterales que potencien el riesgo de un ataque, aislando el equipo, y cortando todo contacto con la red. Es entonces que el equipo responsable realiza un análisis exhaustivo del entorno para garantizar su seguridad.


### **Un componente esencial**

El entorno actual de riesgos y amenazas demanda que las capacidades de detección y respuesta sean parte tácita de los centros de operaciones de ciberseguridad. Deberían ser, por tanto, las capacidades mínimas necesarias que las organizaciones deberían establecer como requisito en el momento de colaborar con un tercero.

Al igual que las labores de inteligencia y de cacería de amenazas, las de detección y respuesta requieren una infraestructura integral y tecnología de punta que puede brindar un proveedor especializado que cuente con el personal capacitado y los procesos certificados que avalen que cuenta con las capacidades requeridas.

Cabe mencionar que los profesionales que deben liderar una iniciativa de esta naturaleza son los responsables de ciberseguridad, quienes trabajan en conjunto con los expertos en TI, y que deberán coordinar los esfuerzos de comunicación con los terceros que hospedan el centro de datos o los servicios de gestión de la infraestructura.





Los especialistas en ciberseguridad deben, asimismo, estar colaborando con el CISO, pues éste será el estratega con gran responsabilidad dentro de la organización, y el vínculo con la alta dirección.

### **Factores a considerar**

Si bien han ido permeando a más organizaciones, las actividades de detección y respuesta deben seguir una planeación bien estructurada, así como los recursos tecnológicos y operativos definidos por todas las partes.

En este sentido, los encargados de la ciberseguridad deben tener tres recomendaciones en mente.

Por un lado, es recomendable focalizar los esfuerzos de protección, detección y respuesta con base en los riesgos propios de su organización. De este modo, se evita incurrir en gastos tecnológicos innecesarios y se ayudará a implementar la protección idónea para los activos de información más críticos.

De igual manera, una vez que se han definido las áreas de riesgo claves, y se han identificado los activos que se protegerán, es posible determinar cómo la implementación tecnológica puede iniciar un ciclo de mejora continua.

Finalmente, las empresas necesitan fortalecer sus capacidades metodológicas de detección y respuesta para aprovechar al máximo la tecnología especializada al nivel de endpoints y servidores. Y, a la vez, llevarlo más allá de un ámbito tecnológico, para convertirlo en una práctica de protección permanente.

Fuente de información: [cio.com.mx](http://cio.com.mx)