Enterprise Strategy Group | Getting to the bigger truth.™

# Abordando la Detección de Ataques y la Respuesta a Incidentes

## Investigación y Análisis por Intel Security y ESG

*Por Jon Oltsik, Analista en Jefe*

**2015 de Abril**

Este trabajo de ESG fue encomendado por Intel Security y se distribuye bajo licencia de ESG.

# Contenido

## Resumen Ejecutivo

Enterprise Strategy Group (ESG) recientemente ha trabajado con Intel Security para analizar los resultados de un proyecto de investigación basado en los resultados de una encuesta de 700 profesionales de TI y seguridad en organizaciones de mercado medio (i.e., 500 a 999 empleados) y empresas grandes (i.e., más de 1.000 empleados) que se encuentran en Asia, Norteamérica, EMEA, y Sudamérica. Enterprise Strategy Group (ESG) recientemente ha trabajado con Intel Security para analizar los resultados de un proyecto de investigación basado en los resultados de una encuesta de 700 profesionales de TI y seguridad en organizaciones de mercado medio (i.e., 500 a 999 empleados) y empresas grandes (i.e., más de 1.000 empleados) que se encuentran en Asia, Norteamérica, EMEA, y Sudamérica. Se formularon a los encuestados una serie de preguntas sobre las políticas de seguridad de información, procesos y tecnologías de su organización, así como sus actuales desafíos de seguridad y estrategias futuras.

Con base en esta investigación, ESG concluye:

- **Los profesionales de la seguridad permanecen ocupados y son desafiados por los ataques dirigidos.** En promedio, los encuestados de seguridad indicaron que sus organizaciones realizaron 78 investigaciones de seguridad el año pasado, y cerca del 28% de esas investigaciones se enfocaron en ataques dirigidos. Las investigaciones de ataques dirigidos son especialmente complicadas ya que requieren analistas de seguridad experimentados, una vista completa de los recursos de TI, y seguridad y análisis de datos. Estas investigaciones en particular pueden ser extremadamente laboriosas y obstaculizar las acciones de corrección, así como generar fugas de datos pese a los mejores esfuerzos del equipo de seguridad. Los datos de Intel Security señalan la necesidad de cambiar de simplemente recolectar volúmenes de datos, a encontrar valor en los datos, esta es la ruta para abordar los ataques más eficientemente.
- **Mientras abundan los ataques dirigidos, la detección y respuesta a incidentes se plaga más de calles de un sólo sentido, barricadas y desvíos.** Los ciberatacantes están utilizando una combinación de técnicas de ingeniería social, servicios de actividad en redes sociales disponibles públicamente, y malware sigiloso para engañar a los usuarios finales, burlar los controles de seguridad, y poner en riesgo sus sistemas. Aunque estas tácticas ofensivas son bastante sencillas, las defensas de ciberseguridad siguen siendo desordenadas, en el mejor de los casos. Los profesionales de seguridad a menudo tienen conocimientos limitados sobre las últimas tácticas, técnicas y procedimientos (TTPs) del hacking. La detección de incidentes y la respuesta se detienen por una serie de tareas que consumen mucho tiempo, procesos manuales e ineficiencias que alargan el tiempo de respuesta, lo que conduce a control de daños y limpieza Las herramientas de monitoreo de seguridad tienen visibilidad limitada de usuarios y tecnologías, mientras que a las herramientas de punto de seguridad les falta el nivel de integración necesario para coordinar y monitorear las defensas de seguridad a lo largo de la red. Alarmantemente, los datos de Intel Security retratan una injusta lucha donde las brechas a la ciberseguridad a menudo sobrepasan a las defensas de ciberseguridad. Las empresas necesitan cambiar sus estrategias de seguridad para poder hacer frente a los incidentes dentro del plazo más crucial, después de la infección y antes de que se pueda provocar un daño grave. Intel Security se refiere a esta ventana ideal de detección/respuesta de incidentes como la "hora dorada".
- **Los profesionales de seguridad solicitan ayuda en varias áreas.** Los profesionales de seguridad encuestados para este proyecto tienen una multitud de sugerencias para ayudar a mejorar las defensas de ciberseguridad, la detección de incidentes y las eficiencias de respuesta. Más de la mitad señalan la necesidad de mejores herramientas de seguridad para detección de incidentes y los análisis de seguridad, mientras que alrededor del 40% recomiendan más formación para profesionales de la ciberseguridad y el equipo de SOC. Y dado que el 80% de las organizaciones creen que sus procesos de detección/respuesta se ven obstaculizados por la falta de integración de tecnologías de seguridad, muchos profesionales de la seguridad creen que sus organizaciones se beneficiarían de una arquitectura de seguridad empresarial de principio a fin perfectamente integrada. En total, se necesitan avances en ciberseguridad a lo largo de personas, procesos y tecnología.

Los CISOs deben utilizar los datos presentados en este informe de dos maneras:

1. **Como una guía de evaluación de seguridad.** Este informe destaca una serie de problemas que dificultan los procesos de detección de incidentes y su efectividad. Los CISOs deben evaluar si esos problemas existen dentro de sus organizaciones y, en caso afirmativo, tratar de identificar y medir las ramificaciones.
2. **Como un plan de acción para la planificación estratégica.** Los datos señalan la necesidad de mejorar mucho los análisis de datos de seguridad y de una arquitectura de tecnología de seguridad empresarial integrada. Los CISOs deben investigar sus planes en estas y otras áreas identificadas en este documento.

## Siempre Activos

La mayoría de los profesionales de la seguridad de la información estarían dispuestos a admitir que existe una ciber-guerra constante en curso, donde sus organizaciones se enfrentan a un constante bombardeo de ataques En promedio, los profesionales de seguridad de TI afirman que sus organizaciones realizaron 78 investigaciones de seguridad individuales en 2014. No es de sorprender que la frecuencia de investigación de seguridad estaba estrechamente relacionada con el tamaño de una organización: mientras más grande era la organización, más investigaciones de seguridad llevó a cabo (ver Tabla 1).

*Tabla 1 Número Promedio de Incidentes de Seguridad en 2014*

| | Estudio de población total (n= | 500 a 999 empleados (n = 196) | 1,000 a 4999 empleados | Más de 5.000 empleados (n = 256) |
|---|---|---|---|---|
| Número Promedio de Incidentes de 2014 | 78 | 31 | 41 | 150 |

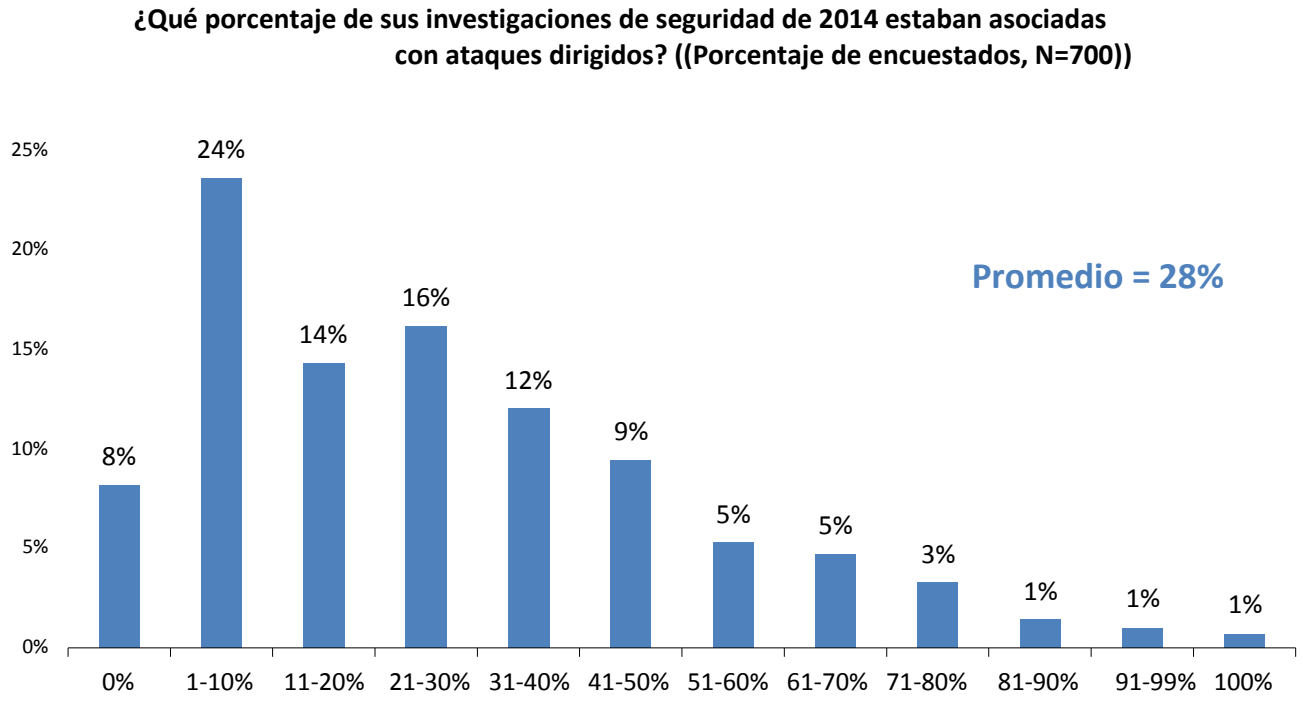
*Fuente:Intel Security, 2015.*

En casi la mitad de las compañías encuestadas, la mayoría de estas investigaciones de seguridad se enfocaron en incidentes de seguridad de rutina donde las PCs de usuarios finales se infectaron con adware, spyware y virus volumétricos comúnmente descargados desde diversas fuentes. Sin embargo, la otra mitad pasó la mayoría de su tiempo investigando problemas más sofisticados y a menudo interrelacionados: ataques dirigidos (por un adversario externo dirigido a un determinado individuo, grupo o tipo de sitio o servicio), brechas de datos y ataques internos maliciosos. De hecho, el 28% de las investigaciones de seguridad están asociadas directamente con ataques dirigidos más peligrosos y potencialmente dañinos (ver Figura 1).

Esta es una distinción importante. Con más de 1 de 4 investigaciones de seguridad vinculadas a ataques dirigidos, muchas organizaciones:

- **Enfrentaron ataques dirigidos frecuentemente.** Aunque el malware peatonal sigue siendo una importante molestia, los datos de Intel Security indican que nadie es inmune a los peligros de los ciberataques dirigidos de hoy. Las organizaciones pequeñas, medianas y grandes han informado de que el 28% de sus investigaciones de seguridad se enfocaron en ataques dirigidos y las organizaciones de todos los sectores se vieron afectadas. Claramente, las amenazas persistentes avanzadas (APTs) que una vez fueron el azote de los organismos gubernamentales y del sector de defensa/inteligencia, ahora se han generalizado, presentando una amenaza real para todas las organizaciones.
- **Requieren nuevos recursos y habilidades para llevar a cabo investigaciones de ataques dirigidos.** En general, los profesionales de la seguridad pueden obtener ayuda contra malware de sus proveedores AV IDS/IPS. Alternativamente, la investigación de malware dirigido que "vuela abajo del radar" puede requerir una combinación de herramientas de análisis de seguridad, feeds de inteligencia sobre amenazas, y habilidades avanzadas de ciberseguridad. Con base en esto, es seguro suponer que las investigaciones de ataques dirigidos son más difíciles y consumen más tiempo que las comunes, y muchas organizaciones simplemente no están preparadas con los recursos, habilidades o análisis adecuados.
- **Hay más en juego con las investigaciones de los ataques dirigidos.** El adware y el spyware pueden afectar la productividad de los empleados, pero los ataques dirigidos pueden generar brechas de datos costosas y dañinas. Esto ejerce presión sobre el equipo de analistas de seguridad para aislar y remediar los problemas tan pronto como sea posible, pero los mejores esfuerzos por sí solos no prevendrán la pérdida de datos.

*Figura 1. Porcentaje de Investigaciones de Seguridad Asociados con Ataques Dirigidos*




*Fuente: Intel Security, 2015.*

Todas estas investigaciones de seguridad plantean una pregunta obvia: ¿Por qué los ciber-adversarios son capaces de penetrar en las redes y poner en riesgo los sistemas con los ataques dirigidos? Desafortunadamente, los profesionales de seguridad señalan diversas raíces de causas - el 38% citan falta de conocimiento del usuario sobre los riesgos de ciberseguridad, el 32% dicen que es cada vez más difícil detectar malware persistente/moderno, 30% culpan al incremento del uso de las redes sociales y el 29% identifican a las tácticas sofisticadas de ingeniería social (ver Figura 2).

*Figura 2. Razones Citadas para el Éxito de un Ataque Dirigido*

**Si su organización ha sufrido uno o más ataques dirigidos avanzados exitosos en 2014, ¿cuál de las siguientes cosas cree que contribuyeron a que esos ataques fueran exitosos? (Porcentaje de encuestados, N=700, se admiten múltiples respuestas)**


*Fuente: Intel Security, 2015.*

Esta lista refleja un microcosmos del escenario de ciberseguridad de hoy. Los ciber-adversarios Inteligentes y astutos, emplean la ingeniería social y el malware sigiloso para tentar a los usuarios finales ingenuos a hacer clic en una URL o abrir un archivo adjunto de correo electrónico. Mientras tanto, casi una tercera parte (32%) de los profesionales de seguridad de luchan para detectar y responder a estos ataques.

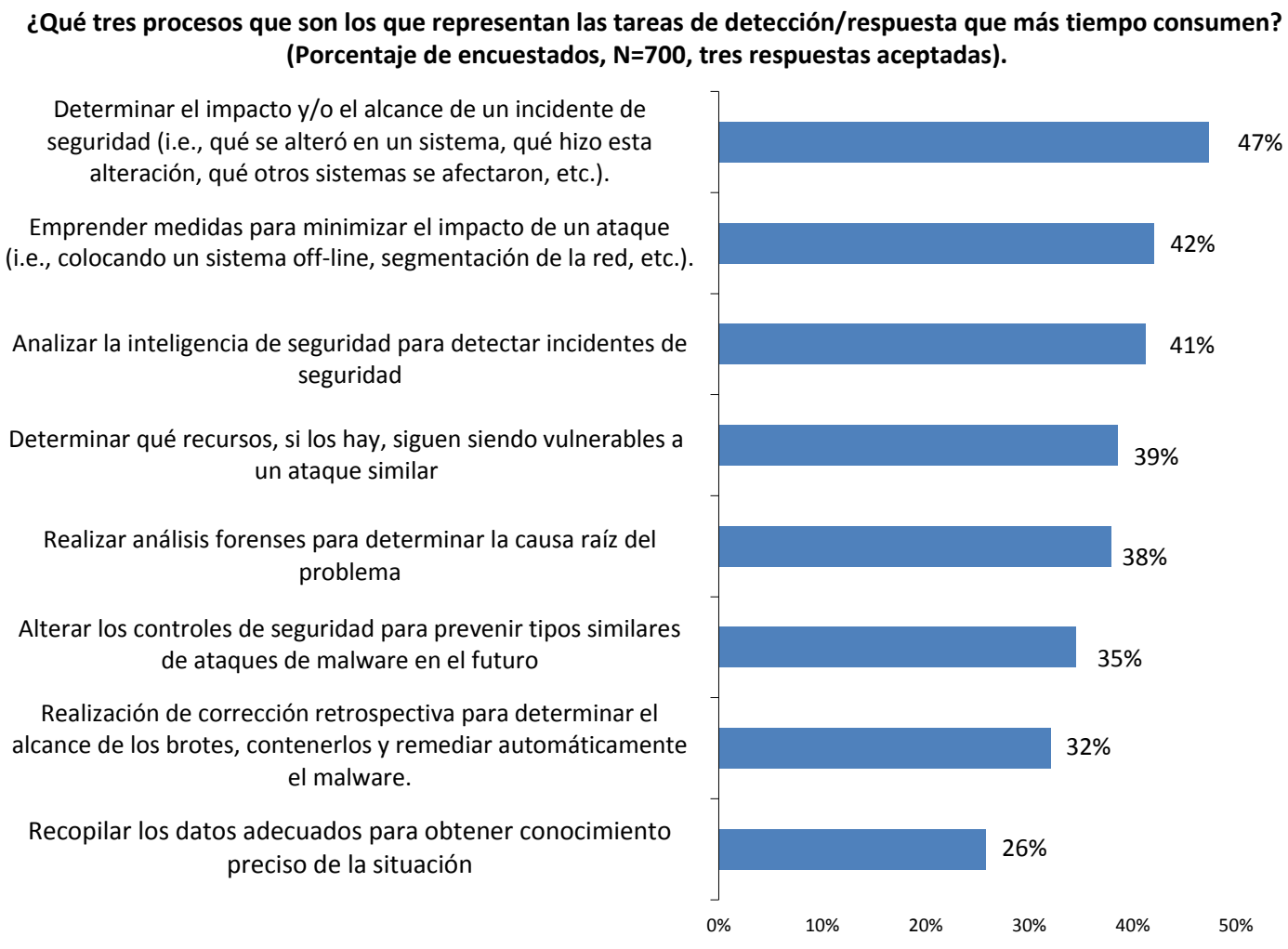
La investigación señala un claro desajuste entre las amenazas a la ciber seguridad ofensivas y las defensas de ciberseguridad tradicionales. Este desequilibrio es motivo de alarma y debe ser abordado por todas las organizaciones tan rápido como sea posible. Es importante que los profesionales de la seguridad comprendan que el volumen de datos por sí mismo no los hace más inteligentes, de lo que se necesita es de más análisis y acción sobre eventos aparentemente no relacionados que agregan a incidentes significativos.

## Defensa de Ciberseguridad

La investigación de Intel Security parece señalar que es relativamente fácil para los ciber-adversarios lanzar ataques dirigidos, evadir las defensas de seguridad, y poner en riesgo los sistemas. Los profesionales de seguridad reconocen esta situación y siguen siendo diligentes en sus esfuerzos por prevenir, detectar y responder a los ataques dirigidos, pero comúnmente son obstaculizados por procesos manuales, controles de seguridad aislados, o análisis de seguridad limitados.

Por ejemplo, los procesos de detección y respuesta a incidentes dependen de una serie de tareas que toman mucho tiempo, incluyendo determinar el impacto/alcance de un incidente de seguridad (47% dicen que esta es una tarea que toma mucho tiempo), emprender acciones para minimizar el impacto de un ataque (42%), y analizar inteligencia de seguridad para detectar incidentes de seguridad (41%) (ver Figura 3). Cuando se juntan todos estos procesos que llevan mucho tiempo, a menudo pasan días, semanas o meses antes de que los ciberataques sean identificados y remediados.

*Figura 3. Tareas que Consumen Mucho Tiempo Asociadas con Detección/Respuesta de Incidentes*




*Fuente: Intel Security, 2015.*

Cuando se trata de detección y respuesta a incidentes, el tiempo tiene una siniestra correlación con el daño potencial, mientras más tarda una organización en identificar, investigar y responder a un ciberataque, lo más probable es que sus acciones no serán suficientes para evitar una costosa brecha de datos delicados. Para enfrentar esta situación, muchas organizaciones se están trasladando hacia monitoreo continuo de usuarios, sistemas, aplicaciones y datos delicados ubicados en redes internas y externas de recursos (i.e., SaaS, IaaS, PaaS, sistemas de partners de negocios, etc.). Un monitoreo eficaz y continuo demanda recolección de principio a fin, procesamiento y análisis de volúmenes de datos de seguridad como archivos de registro, flujos de red, datos forenses de endpoint/red, feeds de inteligencia de amenazas, etc. Ser capaz de identificar y responder a un incidente dentro de la primera hora (i.e., la "hora dorada" de Intel Security) pueden reducir significativamente el impacto de la brecha.

Mientras que muchas organizaciones se esfuerzan en monitorear continuamente a lo largo de la TI, muchas siguen teniendo visibilidad limitada hacia una o más áreas de TI. Cuando se les preguntó acerca de los mayores inhibidores para contar con visibilidad hacia la seguridad integral y en tiempo real, 41% de las organizaciones dijeron que necesitan una mejor comprensión del comportamiento del usuario, 37% afirmaron que necesitan una mayor integración entre la inteligencia de seguridad y las herramientas de operación de TI, 37% necesitan una mejor comprensión del comportamiento de la red, y un tercio (33%) necesitan mejores herramientas para colocar el punto de referencia del comportamiento normal, de manera que puedan detectar anomalías (ver Figura 4).

*Figura 4. Qué se Necesita para Obtener Visibilidad Integral y en Tiempo Real de la Seguridad*


*Fuente: Intel Security, 2015.*

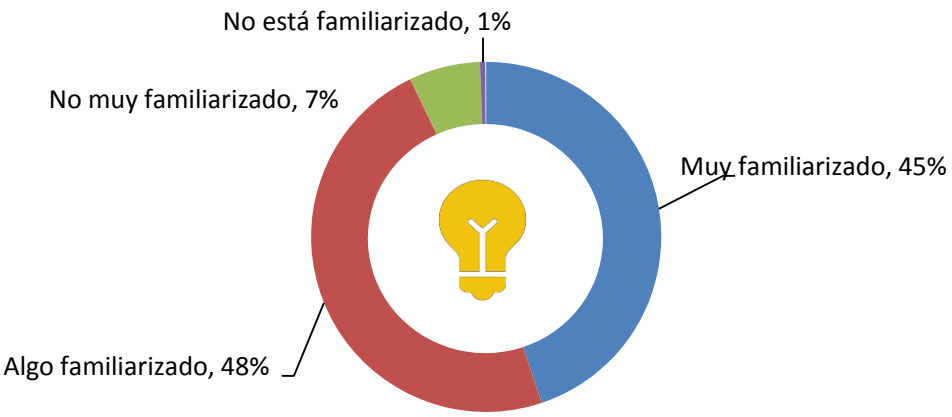
Abordar estas deficiencias de visibilidad y comprensión es fundamental. Por ejemplo, la falta de conocimiento sobre el comportamiento del usuario podría brindar a los ciber-adversarios la oportunidad de crear cuentas de usuario falsas o derrepente descargar volúmenes de documentos delicados hacia una PC de usuario. De manera similar, cuando los analistas de seguridad no están seguros sobre las actividades de la red, tienen más probabilidad de pasar por alto conexiones sospechosas, tráfico de salida, o comportamiento de DNS. Los CISOs deben abordar estas lagunas de visibilidad para armar a los analistas de seguridad con los datos que necesitan para pasar través de aplicaciones, redes y sistemas conforme realizan investigaciones de ataques dirigidos.

La visibilidad de la seguridad de principio a fin es fundamental, pero los datos de seguridad no tienen sentido por sí mismos si los analistas de seguridad no pueden comprender la información o sus consecuencias. De hecho, la detección y respuesta efectiva a incidentes es realmente anclada por la experiencia, los instintos y las habilidades del equipo de analistas de seguridad mientras observan el contenido, monitorean el comportamiento, analizan los datos, y reparan de punto de datos a punto de datos como parte de sus investigaciones.

Dada la necesidad de una robusta base de conocimientos de seguridad, a ESG le parece algo preocupante que sólo el 45% de los profesionales de seguridad se consideren muy conocedores de las técnicas de ofuscación de malware, mientras que el 8% no están muy familiarizados o no está en absoluto familiarizados con las técnicas de ofuscación de malware (ver Figura 5). Con escasos conocimientos en esta área, es fácil conocer el motivo de que los sobrecargados analistas de seguridad hagan caso omiso de las alertas de seguridad, minimicen los esfuerzos de investigación o clasifiquen erróneamente un archivo malicioso como benigno. Esto es especialmente preocupante ya que muchas organizaciones tienen lagunas de visibilidad y deficiencias técnicas, lo que limita su capacidad para detectar y responder a los ciberataques.

*Figura 5. Los Profesionales de Seguridad no están Familiarizados con las Técnicas de Ofuscación de Malware*

**Muchos de los ataques de malware utilizan herramientas sofisticadas para ofuscar u ocultar determinados aspectos de sus explotaciones de vulnerabilidades, cargas, comunicaciones y otras tácticas y procesos. ¿Usted está familiarizado con estos tipos de técnicas? (Porcentaje de encuestados, N=700)**




*Fuente: Intel Security, 2015.*

Las actividades de seguridad empresariales que giran en torno de prevención, detección y respuesta de incidentes se basan a menudo en una multitud de herramientas de punto dispares, que se utilizan para la gestión de amenazas, la aplicación de políticas, el control de acceso y el monitoreo de seguridad. En muchos casos, estas herramientas fueron añadidas a la red de manera orgánica a lo largo del tiempo, en respuesta a los nuevos tipos de ciber-riesgos.

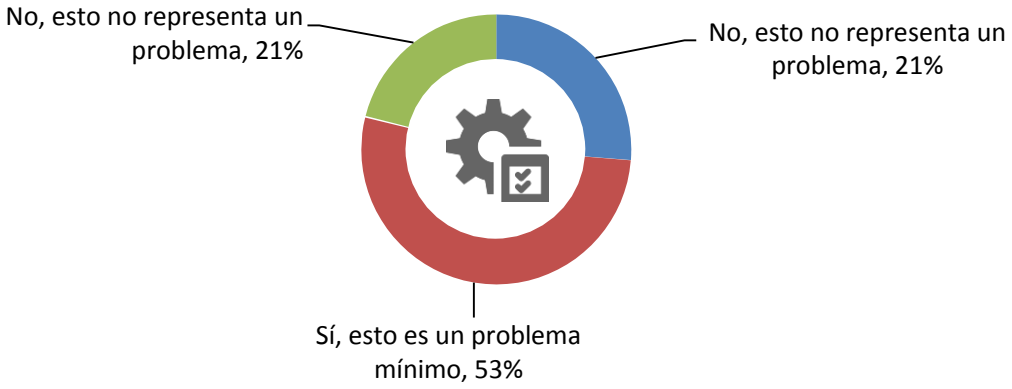
Cada herramienta está diseñada para una función específica y puede ser efectiva por sí misma, pero el equipo de seguridad de la información es en última instancia el responsable de proteger todos los activos de TI, independientemente de su ubicación o los tipos de amenazas que enfrentan. Frecuentemente es difícil, si no imposible, crear y aplicar políticas de seguridad o monitorear el estado de seguridad empresarial al armar los informes generados a partir de decenas de herramientas independientes.

La compleja naturaleza inter-vectorial de los ataques, hace que el modelo de herramienta de punto sea aún menos aceptable. Múltiples eventos detectados por diferentes sensores deben ser agregados para correlacionar eventos en una secuencia de ataque, permitir un flujo de trabajo de investigación, o comunicar la contención adecuada y la corrección a los controles pertinentes.

¿Esta falta de integración es la que obstaculiza los esfuerzos en torno a la detección y respuesta a incidentes? Según la investigación, la desafortunada respuesta es "sí", el 26% de las organizaciones dicen que la falta de integración y comunicación entre las tecnologías/herramientas de seguridad, crea un gran problema para la detección y respuesta a incidentes, mientras que el 53% afirman que la falta de integración y comunicación entre las tecnologías/herramientas de seguridad sigue siendo un problema marginal (ver Figura 6).

*Figura 6. La Falta de Integración de Tecnologías de Seguridad Genera Problemas de Detección/Respuesta a Incidentes*

**¿Su organización tiene dificultad con detección y respuesta de incidentes debido a la falta de integración y comunicación entre sus tecnologías/herramientas de seguridad? (Porcentaje de encuestados, N=700)**

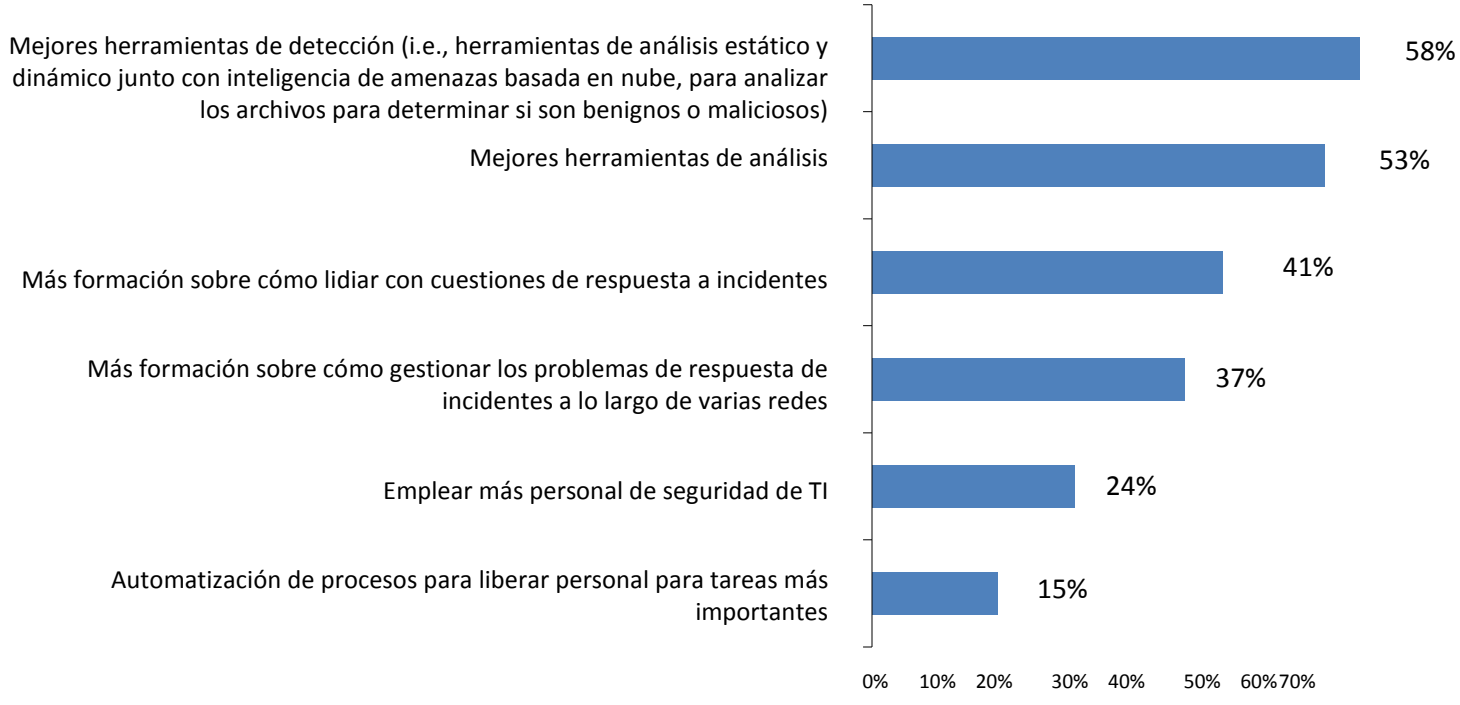



*Fuente: Intel Security, 2015.*

A los profesionales de seguridad se les pidieron sus opiniones acerca de cómo sus organizaciones pueden mejorar la eficiencia y efectividad del personal de seguridad de la información. La investigación demuestra que existe un deseo real de herramientas de análisis de seguridad más eficaces, el 58% de los encuestados desean mejores herramientas de detección, mientras que el 53% dicen que necesitan mejores herramientas de análisis para convertir los datos de seguridad en inteligencia procesable. Existe el deseo de mejorar el conjunto de habilidades de seguridad de la organización con más formación de respuesta a incidentes y una necesidad general de hacer crecer al personal de seguridad de la información (ver figura 7). En conjunto, estos datos demuestran la necesidad de mejoras en personas, procesos y tecnología.

*Figura 7. Lo que Se Necesita para Mejorar Eficiencia y Efectividad del Personal de Seguridad de la Información*

**En su opinión, ¿cuál de los siguientes elementos podría hacer más para mejorar la eficiencia y efectividad de su personal? (Porcentaje de encuestados, N=700, se aceptan varias respuestas)**




*Fuente: Intel Security, 2015.*

## Lo Que Hay de Fondo

Intel Security expone algunas debilidades fundamentales y generalizadas de la ciberseguridad:

1. Las organizaciones llevan a cabo docenas de investigaciones de seguridad cada año, y alrededor de una cuarta parte de estas investigaciones se centran en ataques dirigidos. Estas investigaciones en particular, tienden a requerir habilidades avanzadas y herramientas de análisis de seguridad, así como una arquitectura integrada.
2. A pesar de los productos de "bala de plata" desplegados en los últimos años, los ataques dirigidos tienen éxito y demuestran un desequilibrio entre la ofensiva del ciber-adversario y las defensas correspondientes de las grandes y pequeñas organizaciones. Mientras que las campañas de ataque sigilosas de los ciber-adversarios se basan en tácticas de ingeniería social, para las empresas es difícil prevenir, detectar, o responder a estos ataques de manera oportuna.
3. Muchas organizaciones carecen del monitoreo continuo integral que necesitan para identificar y responder a comportamiento sospechoso durante el lapso de tiempo posterior a la explotación de vulnerabilidades donde todavía no ocurren daños graves (ej., la "hora dorada" de Intel Security).
4. Los datos también señalan problemas organizacionales y tecnológicos. Muchas organizaciones carecen de habilidades de ciberseguridad avanzadas, mientras que las tecnologías de seguridad en las que dependen generan gastos ya que les falta el nivel adecuado de integración técnica. Como resultado, los procesos de detección y respuesta a incidentes están cargados con múltiples tareas que consumen mucho tiempo y gastos operacionales.
5. Los profesionales de seguridad creen que necesitan mejores tecnologías de análisis de seguridad, integración y formación adicional para mejorar la eficiencia y la efectividad de sus equipos de seguridad.

Los CISOs deben estudiar esta investigación y evaluar si sus organizaciones se enfrentan a los mismos desafíos de ciberseguridad en todos los aspectos del dominio de seguridad de la información y estrategia. Además, ESG cree que existe una historia oculta dentro de la investigación de Intel Security que alude a mejores prácticas y lecciones aprendidas. Estos datos sugieren fuertemente que los CISOs:

- **Se comprometen con la formación continua en ciberseguridad.** Como los médicos, los profesionales de ciberseguridad deben mantenerse al día con las últimas novedades en materia de investigación y desarrollo en el ámbito de sus competencias. Esto incluye avances en técnicas de malware, vectores de amenazas y nuevas innovaciones en ciber-defensas. Lamentablemente, la educación continua frecuentemente no se contempla ya que el equipo de seguridad está casi siempre demasiado ocupado yendo a la par de su carga de trabajo o reaccionando a alertas de emergencia. Esto genera la situación descrita en el presente informe, donde menos de la mitad de los profesionales de la seguridad encuestados estaban muy familiarizados con las técnicas de ofuscación de malware Los CISOs deben buscar un equilibrio entre estas diversas actividades, ya que los profesionales de ciberseguridad no serán efectivos si no saben cómo identificar o corregir los últimos tipos de ciber-amenazas Algún tipo de ciber-formación debe ser requisito para toda la organización de manera anual, y ser apoyada por un programa continuo dirigido por el equipo de seguridad y RR. HH. Los programas de ciber-formación serán más exitosos cuando la alta dirección tome un papel de liderazgo subrayando su importancia y alentando el esfuerzo en todo momento.
- **Anclan su estrategia de ciberseguridad con análisis robustos pasando de volumen a valor.** Si bien los controles de prevención de amenazas como el SANS top 20 son críticos, los CISOs deben asumir que los ataques dirigidos eludirán las defensas de seguridad, penetrarán en las redes y pondrán en riesgo los sistemas. Para abordar esta inevitabilidad, la estrategia de ciberseguridad debe basarse en análisis de seguridad robustos. Esto significa recopilar, procesar y analizar enormes cantidades de datos internos (i.e., registros, flujos de paquetes, análisis forense de endpoint, análisis estáticos/dinámicos de malware, etc.), inteligencia organizacional (i.e., comportamiento de usuarios, comportamiento de negocios, etc.) y datos externos (i.e., inteligencia de amenazas, notificaciones de vulnerabilidad, etc.). Los análisis de seguridad deben basarse en algoritmos inteligentes, en la medida de lo posible, que puedan detectar comportamientos anómalos, identificar a los sistemas afectados, y ayudar a los analistas a determinar la causa raíz y el alcance con la mayor rapidez y precisión posibles. Los CISOs deben recordar que la recolección y el tratamiento de los datos es un medio hacia la acción, mejorando la efectividad y eficiencia de la detección y respuesta ante amenazas.
- **Crean una arquitectura de tecnología de seguridad empresarial estrechamente integrada.** Casi el 80% de las organizaciones creen que la falta de integración entre las herramientas de seguridad crea un cuello de botella e interfiere con su capacidad para detectar y responder a amenazas de seguridad. Esto debe ser percibido como una bandera roja brillante. Los CISOs deben mitigar esta limitación mediante el desarrollo de

- una arquitectura de seguridad empresarial, que reemplace a las herramientas de punto de seguridad con una arquitectura de seguridad empresarial integrada durante los próximos tres años. Esta arquitectura de seguridad debe abarcar redes internas y activos de TI basados en nube. El plan del proyecto debe comenzar inmediatamente con los puntos problemáticos o tecnologías de seguridad completamente amortizadas, y posteriormente introducir nuevos puntos de integración en fases a lo largo del tiempo. Cada fase debe incluir métricas de éxito en torno a la eficacia y eficiencia operativa de la seguridad. Si bien está más allá del alcance de este trabajo el proporcionar detalles acerca de arquitectura de seguridad empresarial, las características clave incluyen comando y control centrales (i.e., gestión de políticas, gestión de la configuración, análisis de seguridad, etc.) y la aplicación distribuida hacia arriba y hacia abajo de la pila tecnológica.
- **Automatizan la detección y respuesta a incidentes siempre que es posible.** Mientras las ciber-amenazas crecen exponencialmente, las herramientas de seguridad y el personal existentes sólo pueden aumentar su capacidad aritméticamente. En otras palabras, la mayoría de las organizaciones no tienen la posibilidad ir al paso del malware o de las técnicas de ciber-ataque siempre cambiantes. Para nivelar el campo de juego, los CISOs deben comprometerse a más automatización. Para la detección de incidentes, esto requiere de análisis avanzados de malware, algoritmos inteligentes, aprendizaje de máquina y el consumo de inteligencia de amenazas, para comparar el comportamiento interno con incidentes de puesta en riesgo (IoCs) y tácticas, técnicas y procedimientos (TTPs) utilizados por los ciber-adversarios. Además, los equipos de seguridad y de operaciones de TI deben instrumentar infraestructura de TI y automatizar tareas y flujos de trabajo para obtener corrección continua, para colocar en cuarentena a los sistemas que estén en riesgo o para bloquear URLs y direcciones IP maliciosas recientemente descubiertas, tan rápidamente como sea posible. La meta a corto plazo aquí, debería ser la reducción de la carga de trabajo de seguridad de bajo riesgo, para liberar al personal de SOC y permitirle enfocarse en tareas de alta prioridad.

Enterprise Strategy Group | **Getting to the bigger truth.**

20 Asylum Street | Milford, MA 01757 | Tel: 508.482.0188 Fax: 508.482.0218 | www.esg-global.com