# Evolución del Modelo de Ciberseguridad en tiempos de Transformación Digital

panda

pandasecurity.com

# Transformación

# Consecuencias

Perímetros de la compañía tienden a difuminarse

Endpoints como activo crítico de las compañías

Aumento Dramático del volumen de datos

Incremento de los esfuerzos operativos

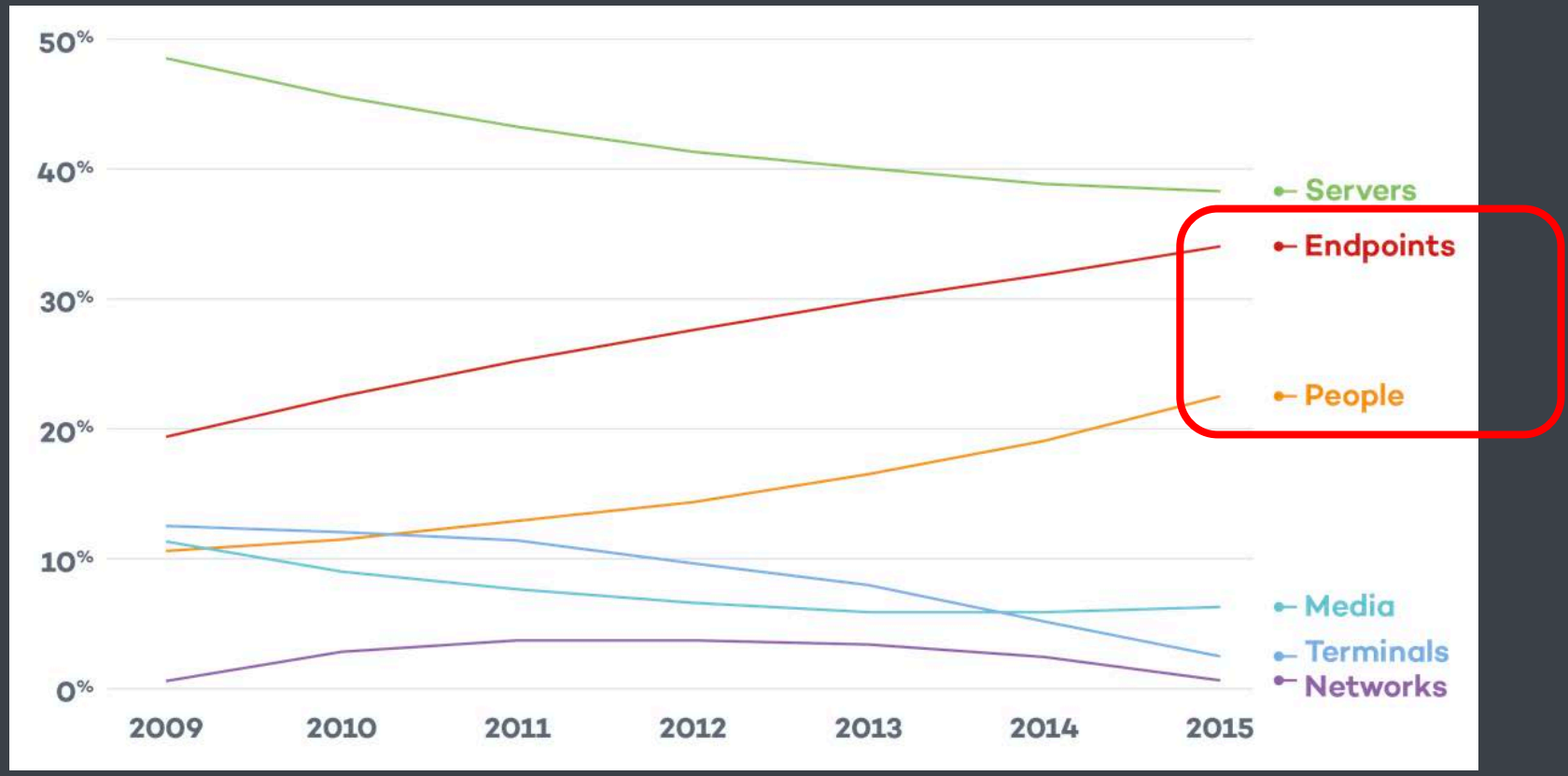
Incremento de la superficie de ataque

Mayor exposición a amenazas avanzadas

# El objetivo es el Endpoint…

…pero solo recibe un 3-4% del presupuesto de seguridad

% Incidencias por objetivo




Fuente: Verizon Data Breach Investigations Report

panda

# Evolución de los Atacantes

Sofisticación de ataques dirigidos y específicos

Aumento de capacidades de computo y proceso

Malware y ransomware como servicio

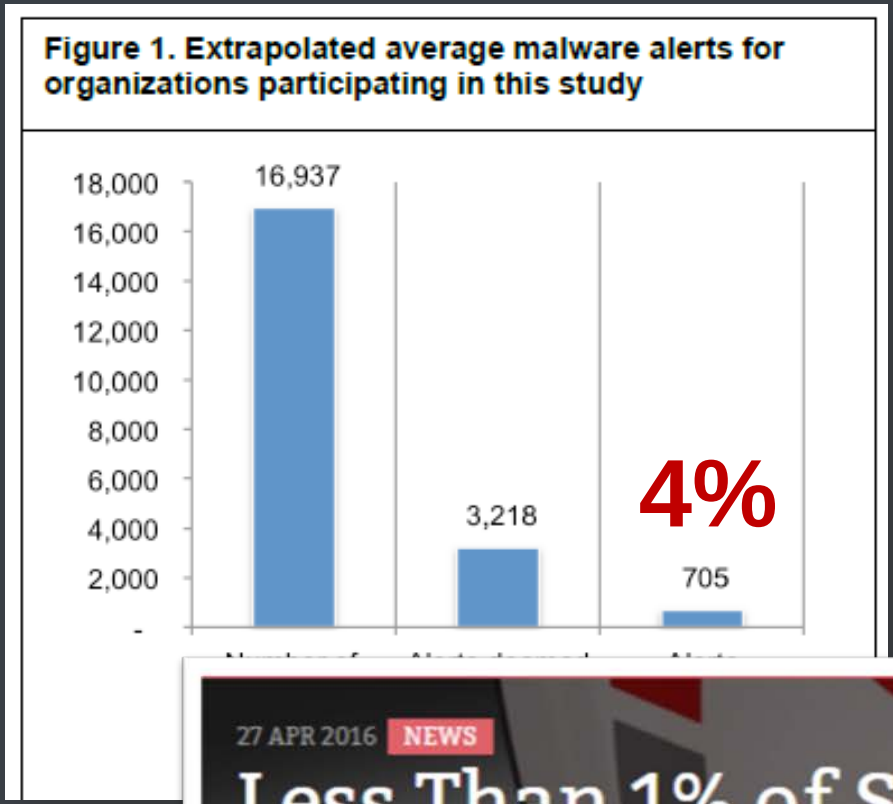
Sensible aumento del volumen de muestras

Uso de goodware para evitar detecciones

Incremento de exposición al Insider Threat

# Transformar el Modelo de seguridad

# Demasiadas alertas a investigar




**"Solo el 4% de las alertas recibidas son investigadas."**

***"Two-thirds of the time spent by security staff responding to malware alerts is wasted because of faulty intelligence"***

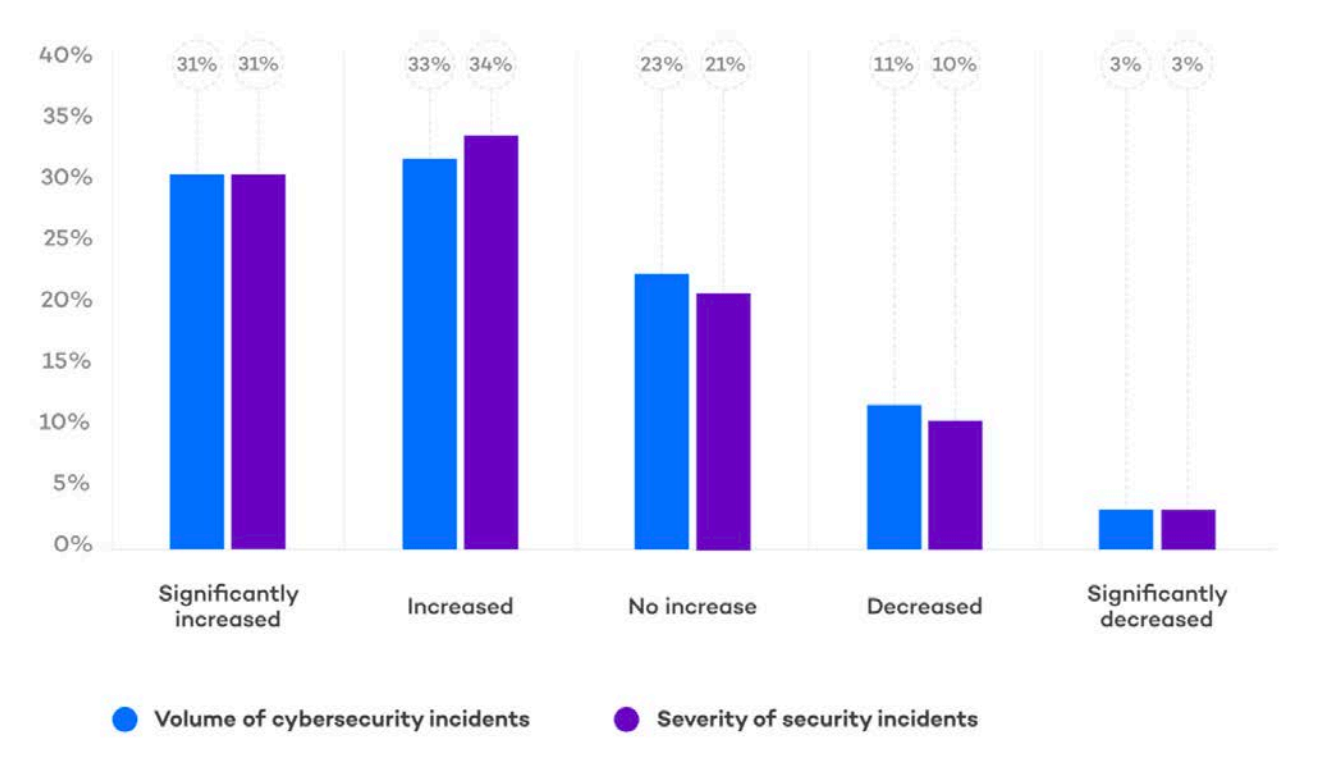
***"It costs organizations an average of $1.27 million annually in time wasted responding to erroneous or inaccurate malware alerts"***

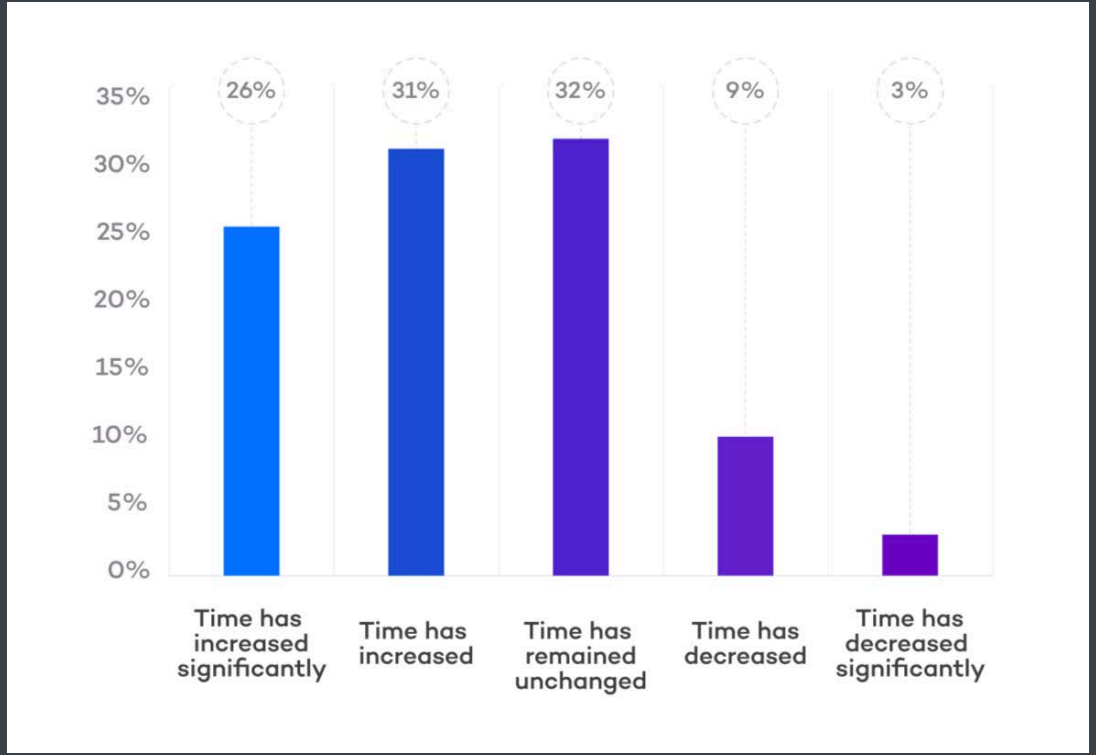

**Fuente: Ponemon Institute. "The cost of malware containment".**

**Fuente: EMA**

panda

# Aumento del Volumen y Severidad de Incidentes




# Aumento del tiempo de detección

**Fuente: Estudio Ponemon Institute. Evolución del volumen y la severidad de incidentes de seguridad en los últimos 12 meses (Hasta Marzo 2018)**

panda

# Indicadores de Obsolescencia

- Capacidad de análisis y proceso mermadas
- Perdida de visibilidad y ausencia de contexto
- Operación estática y poco flexible
- Falta de recursos para satisfacer demanda
- Falta de integración en la arquitectura de seguridad

- Perdida de efectividad en prevención y detección
- Incremento en los tiempos de respuesta
- Aumento en la exposición frente a amenazas
- Elevación de los indicadores de riesgo

panda

# Indicadores de Obsolescencia

En 2018 las inversiones en ciberseguridad han aumentado en solo el 7% mientras las superficies de ataque incrementan exponencialmente

Estimaciones indican que solo el 36% de los profesionales de la seguridad tienen comunicación directa con el CEO

Algunas estimaciones indican que solo el 35% de los profesionales de la ciberseguridad valoran un ecosistema de ciberseguridad integrado

Para 2020 se prevé que haya más de 1.5 millones de puestos en ciberseguridad sin cubrir

Profesionales del sector estiman que más de la mitad de las alertas de seguridad vienen mal categorizadas de los sistemas teniendo que realizar ajustes manuales

**Fuente: Panda Security Summit**

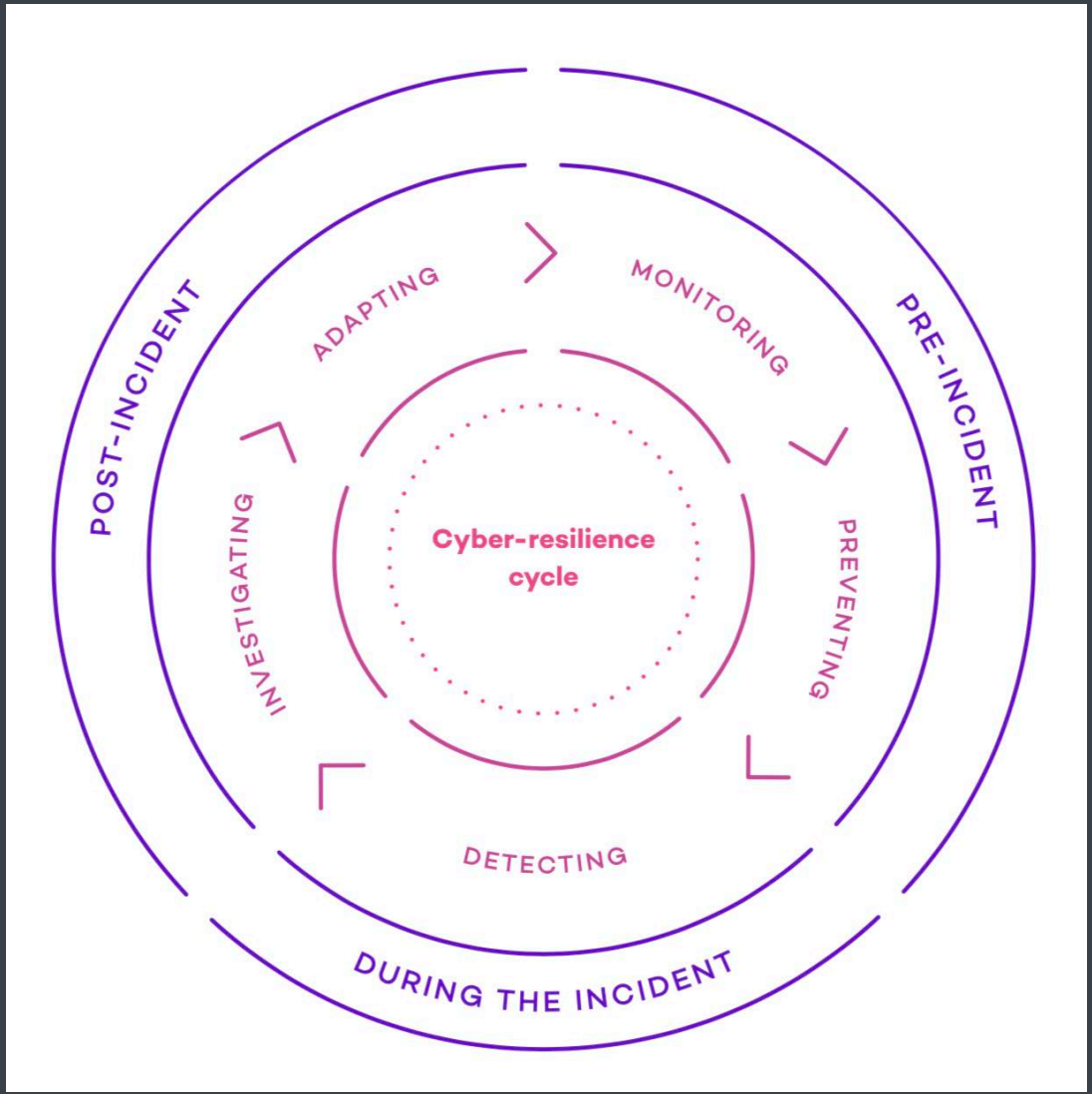
panda

# Como adaptar modelo de ciberseguridad en la era de la transformación digital?

- Gestionar el modelo de ciberseguridad y el manejo del riesgo a nivel de organización y no a nivel departamental
- Aumentar los niveles de interacción en las distintas capas que componen el modelo
- Apoyarse en productos y servicios que permitan establecer modelos de análisis automatizados y predictivos. **Inteligencia Artificial**
- Implementar un modelo flexible que se adapte continuamente a las nuevas tácticas y técnicas empleadas por los atacantes
- Reforzar los pilares de prevención detección y respuesta reduciendo exposición y superficie de ataque. ***Visibilidad, automatización***
- Dotar al modelo de carácter proactivo. Incluir servicios de ***Threat Hunting***

panda

# Ciber-Resiliencia




GRACIAS
panda
pandasecurity.com