SAO (Security Automation and Orchestration)

"You don't have to run faster than the bear to get away. You just have to run faster than the guy next to you."

Jim Butcher, Author

Gartner's Definition:

"utilize machine-readable security data to provide analysis and management capabilities to support operational security teams"

La amenaza es una realidad

- Los Ataques Avanzados van en aumento
- Bien financiados (Estados y Corp.), dirigidos, persistentes y ocultos
- Los ataques organizados representan un riesgo mucho mayor que el malware convencional
- Grupos de ataque sofisticados con una misión concreta: ataques dirigidos

Cada vez nos cuestan más

LOS INCIDENTES CADA VEZ SON MAS COSTOSOS

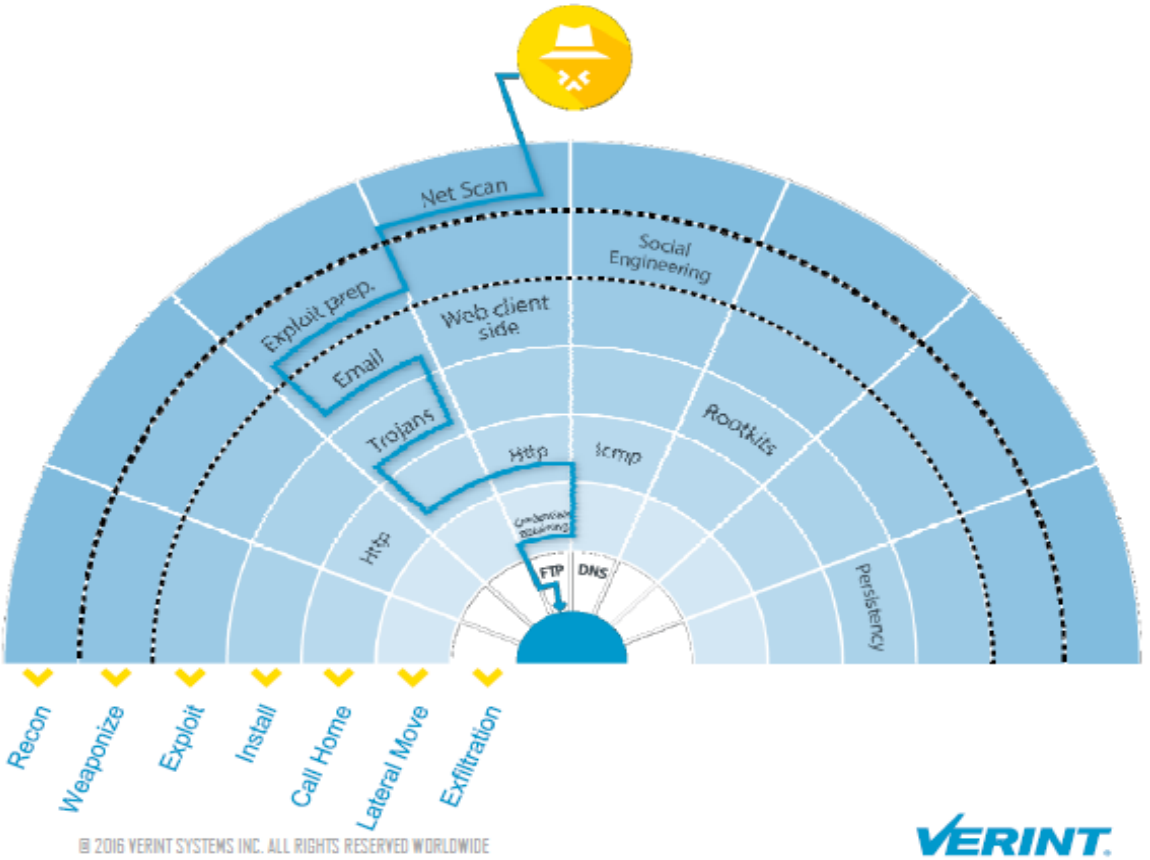
- 2060 Millones de datos de clientes comprometidos
- 146 días de media para la detección de infiltraciones
- $3,000 Millones de valor de mercado destruido
- 1,000 Millones de $ negocio en RANSOMWARE
- 1 Millón de elementos de Malware creados al día.
- Para 2019, el gasto en remediación de brechas de seguridad se multiplicará x4

Fuente:Juniper

Los ataques son multivector

LOS ATACANTES TIENEN MULTIPLES VECTORES DE ATAQUE

Las organizaciones necesitan cubrir toda la cadena del ataque

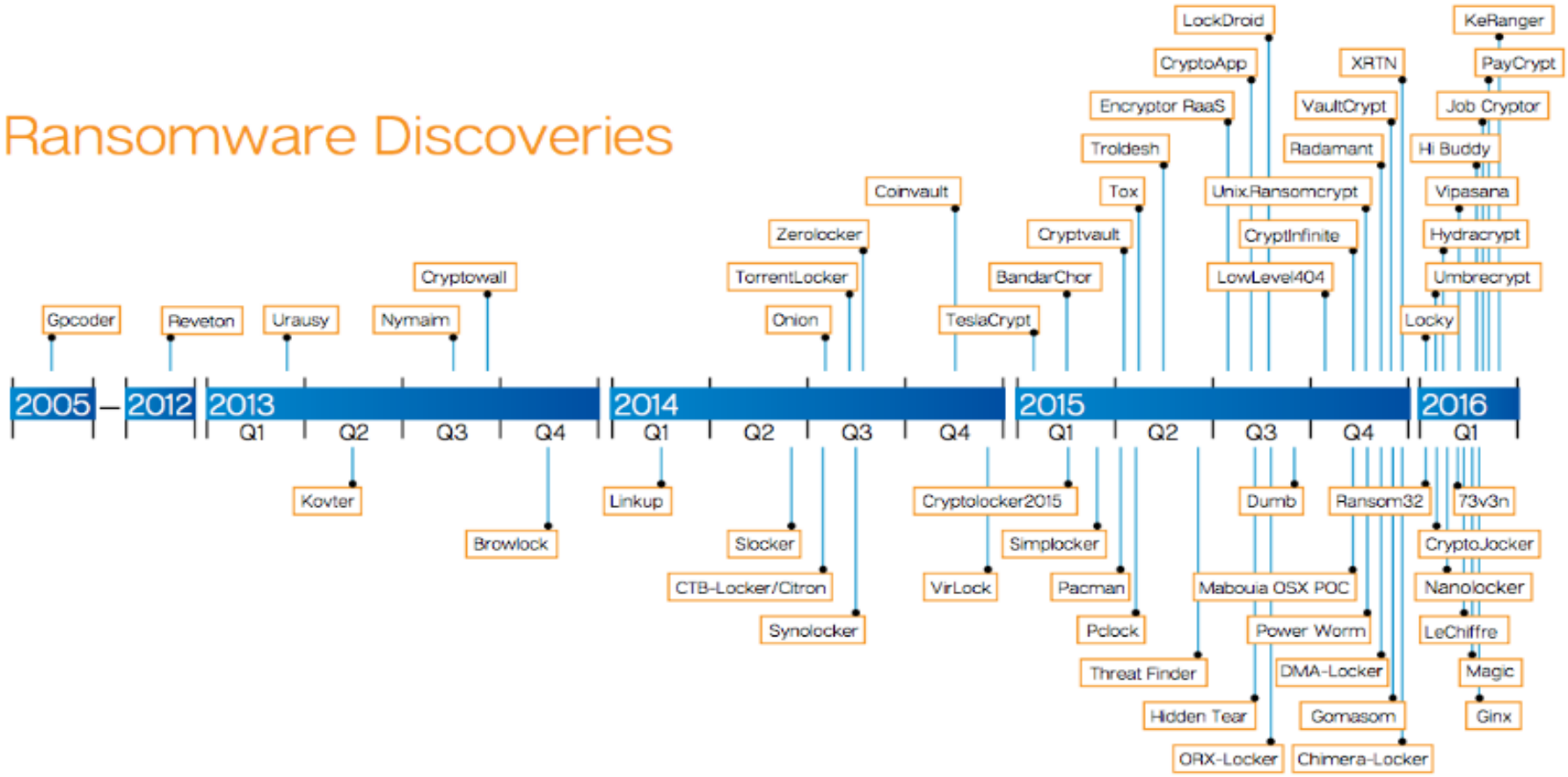


Necesitamos mucha tecnología distinta.

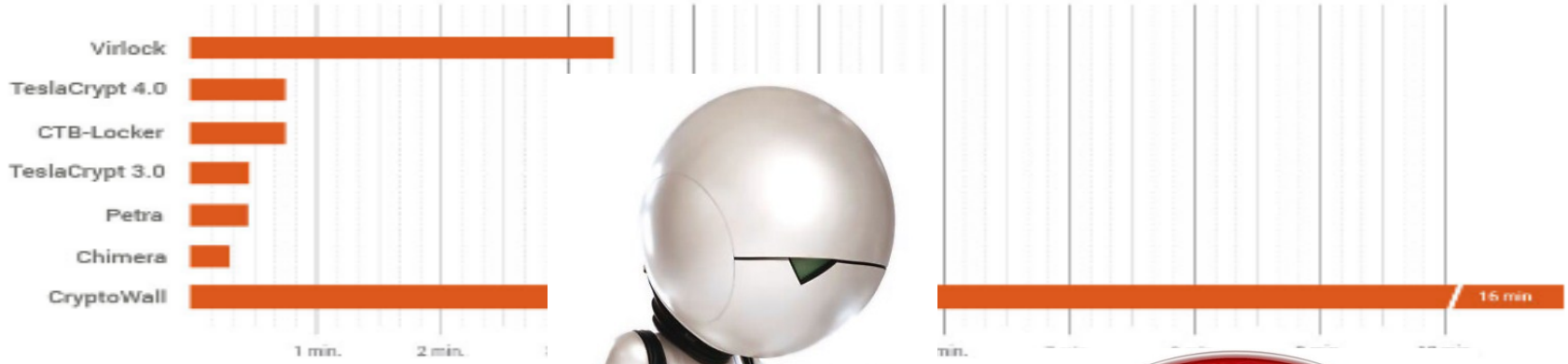
A nivel de las organizaciones...

Demasiadas soluciones de nicho Enfocadas en un solo vector de ataque	98% de los ataques **se origina en el entorno IT**
Avalancha de alertas **IEC**: 400,000 malware alertas al día, solo un 19% se consideran reales	Sólo el **4%** de las alertas son investigadas
Recursos Insuficientes En 2019, se prevé un deficit de 1.5M de analistas ciber	Imposible extraer información relevante de este panorama. Las investigaciones toman **82 días** en promedio (a añadir a los 146...)

Velocidad del ransomware



Encriptación del disco



- Chimera: 18 seconds
- Petya: 27 seconds
- TeslaCrypt 4.0: 28 seconds
- CTB-Locker: 45 seconds
- TeslaCrypt 3.0: 45 seconds
- Virlock: 3 minutes 21 secon
- CryptoWall: 16 minutes

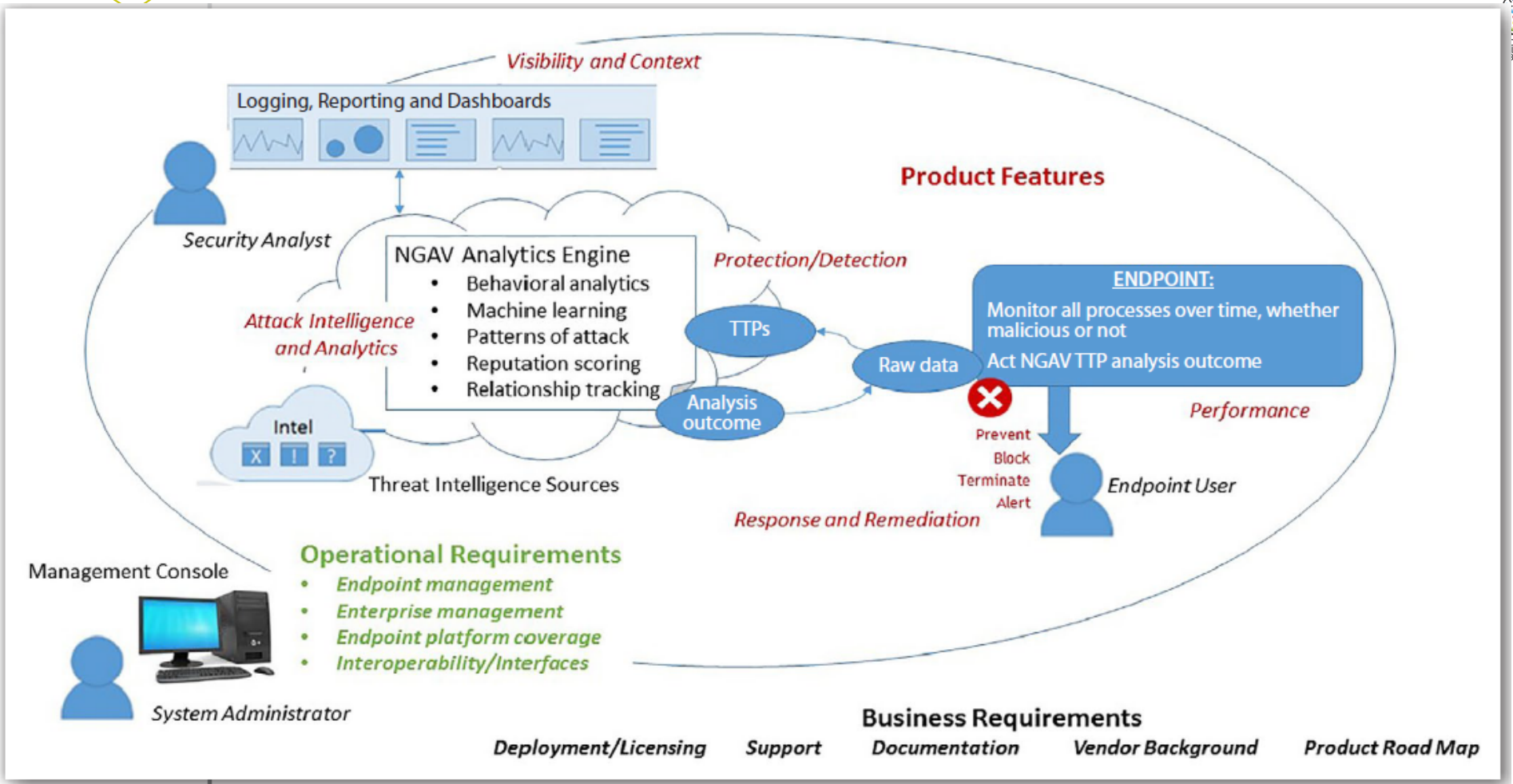
Five out of the seven samples finished the encryption process in under a minute.

Necesidad de inversión

"If you protect your paper clips and diamonds with equal vigour, you'll soon have more paper clips and fewer diamonds."

Dean Rusk, US Secretary of State, 1961-1969

NGAV, EDR, ...



Necesidad de computo más allá del endpoint

Modelo matemático

- Aprendizaje automático para la clasificación

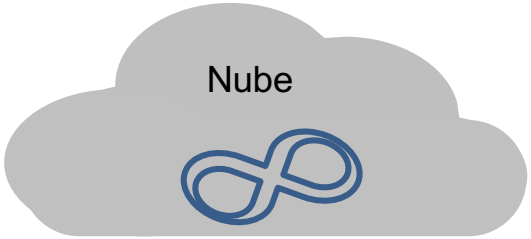
COLLECT

EXTRACT

X = [63796c616e6365]
X = [70726576656e74]
X = [70726f74656374]

TRANSFORM, VECTORIZE AND TRAIN

CLASSIFY AND CLUSTER



We build the model with **100,000,000** good and **100,000,000** bad files.

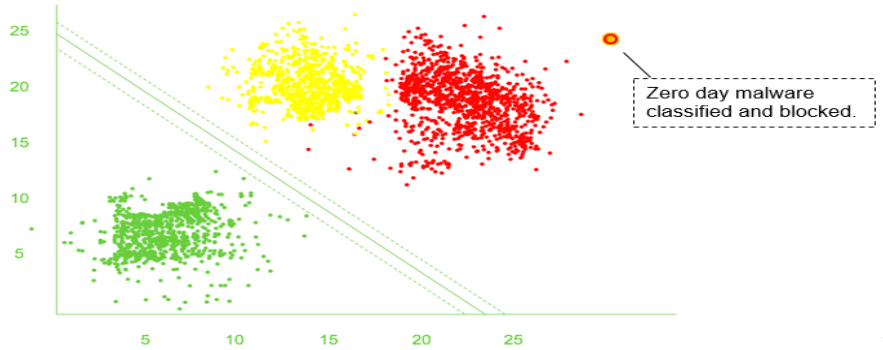
We test on **100,000,000** new good and **100,000,000** new bad files.

We train on **100,000,000** good and **100,000,000** bad files.

>6,000,000 features.

>600,000,000 data samples.

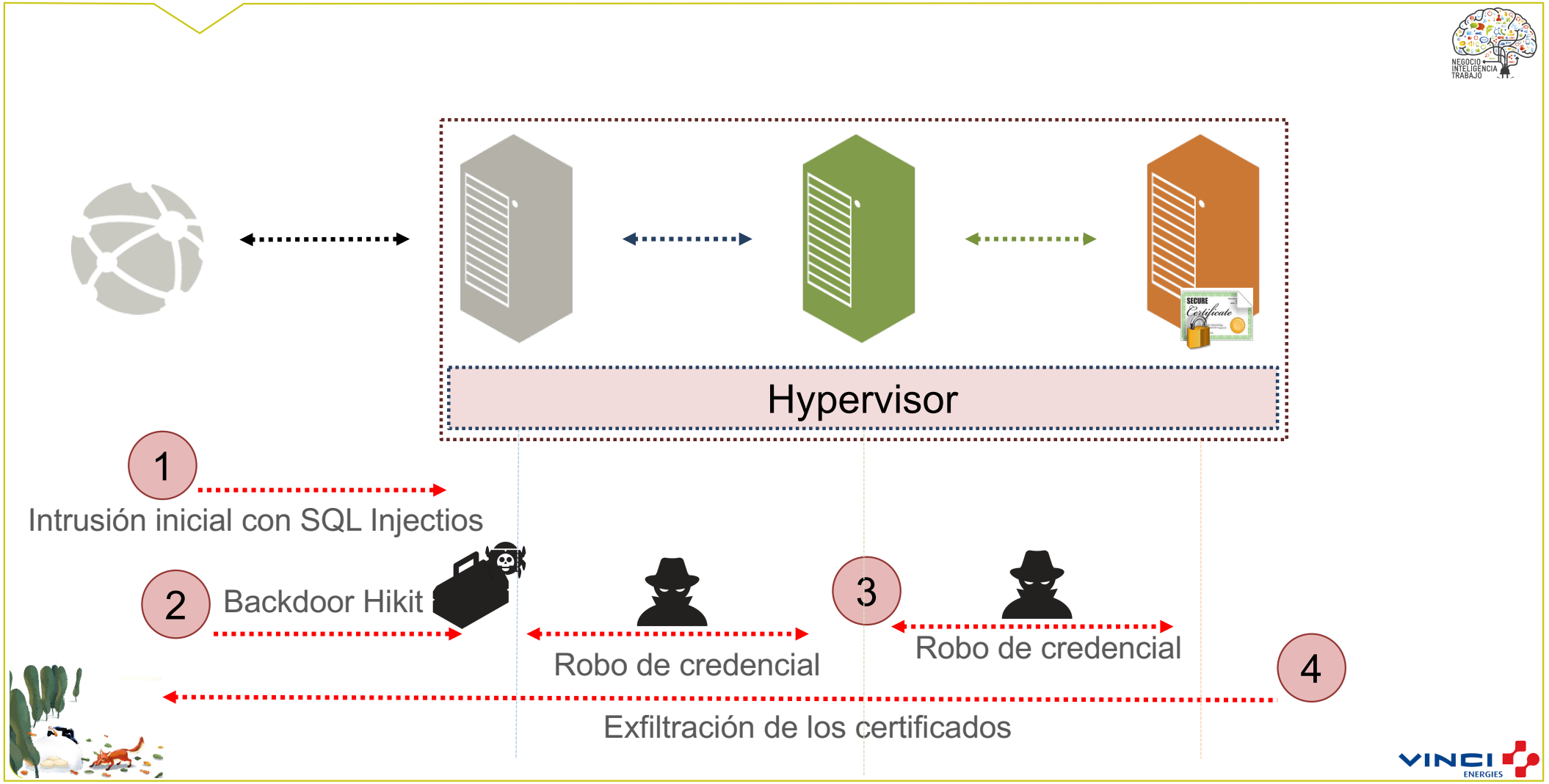
3,600,000,000,000,000
(3 quadrillion) data points in total.



(Algoritmo)
Agente SW

Que debería hacerse …

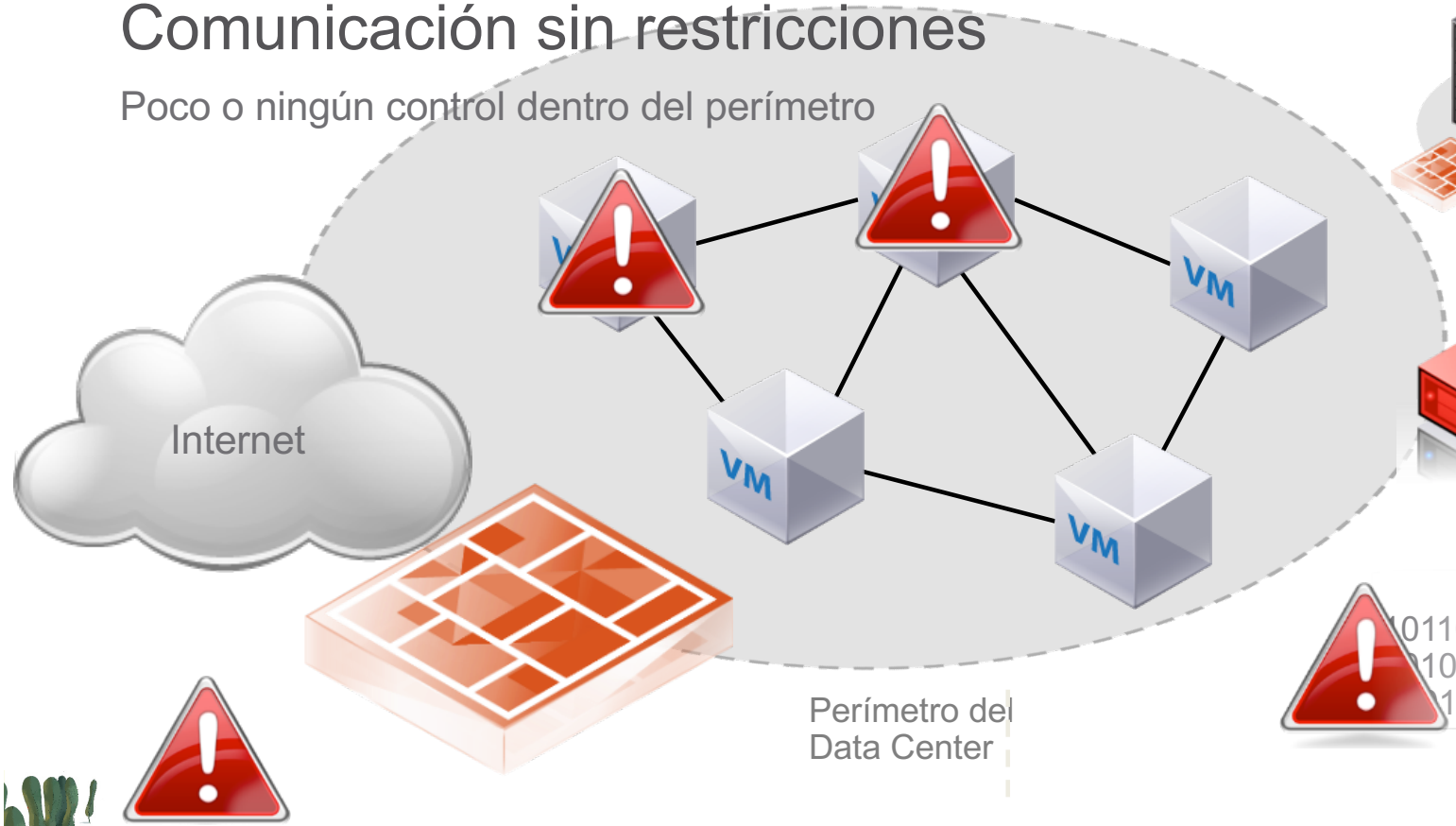
Propagación en la Nube / Virtual Hidden LYnx



¿Por qué ocurren los problemas de seguridad en entornos virtuales?

Comunicación sin restricciones

Poco o ningún control dentro del perímetro



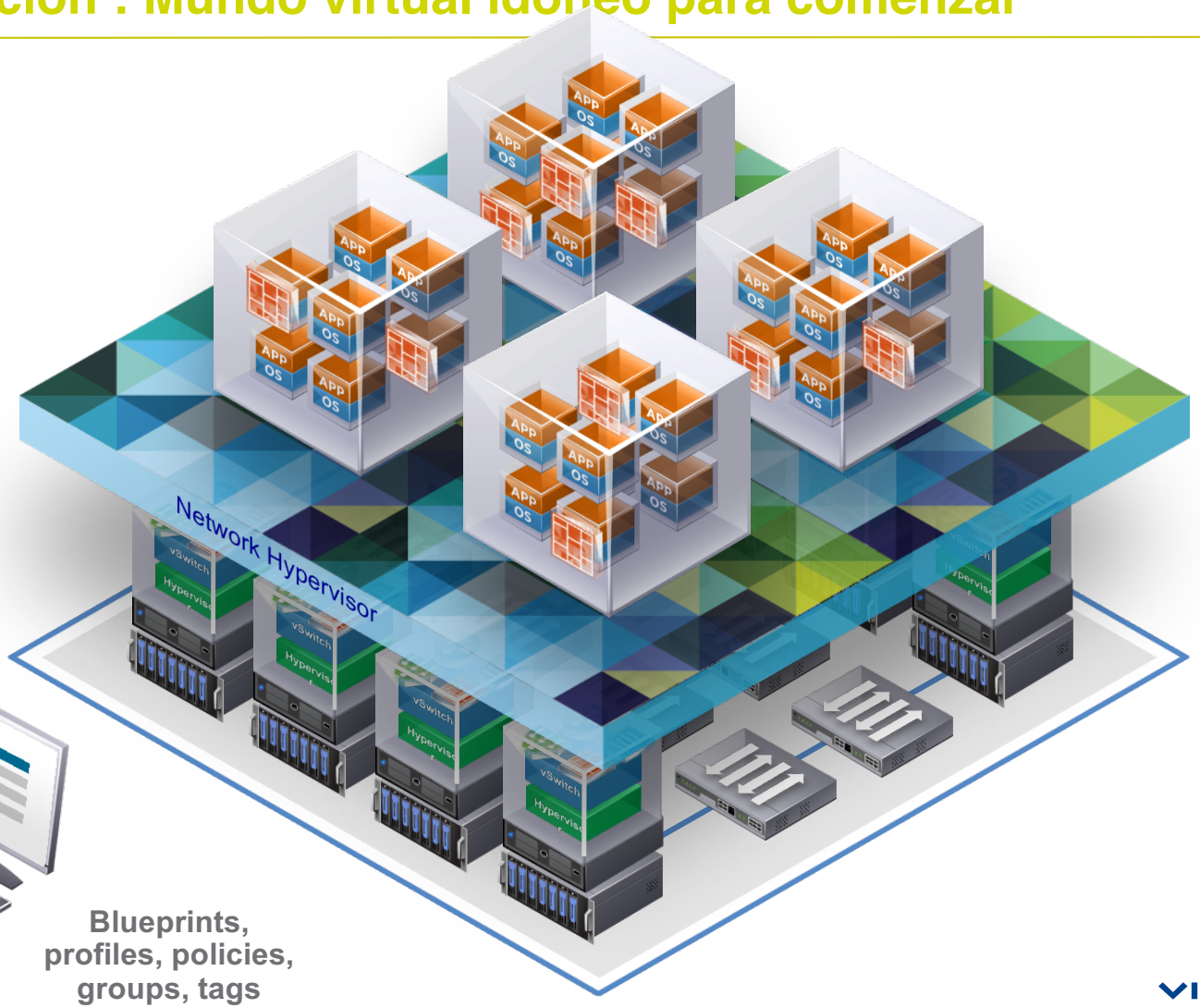
Los sistemas menos críticos son los que se atacan primero.

Los atacantes se pueden mover libremente dentro del DC

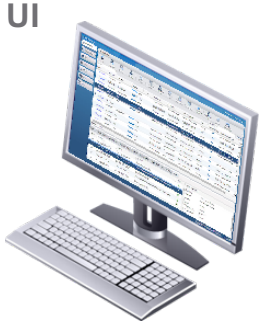
Los atacantes pueden causar daños sin que nos enteremos.

Automatización : Mundo virtual idóneo para comenzar

- Ventajas de automatización



Management APIs, UI



Blueprints, profiles, policies, groups, tags

Ventajas de Automatización

- Centraliza y asegura las investigaciones de seguridad (Forense)
- Estandariza los procesos de respuesta a incidentes
- Permite una colaboración eficiente (API)
- Automatiza flujos de trabajo y respuestas
- Reduce profundamente el tiempo medio de respuesta (MTTR)

Threat Lifecycle Management (TLM)

Detección

Las amenazas se pueden detectar a partir de plantillas de alarmas y baremaciones de amenazas. Los casos se pueden crear con un solo clic.

Cualificación

Las búsquedas se pueden ejecutar desde una alarma generada o un evento. Las informaciones aportadas en las visualizaciones aceleran el análisis.

Investigación

Detalles de alarmas, datos de los registros y las notas se pueden agregar fácilmente. Los analistas colaboran para abordar los casos.

Neutralización

Los playbooks automatizados aseguran una ejecución consistente. Los analistas pueden invocar automáticamente un volcado forense desde un punto final remoto.

Recovery

Las contramedidas pueden invocarse para mitigar la amenaza. Las listas de IoC se actualizan automáticamente para reducir el riesgo futuro.

Objetivo a cumplir

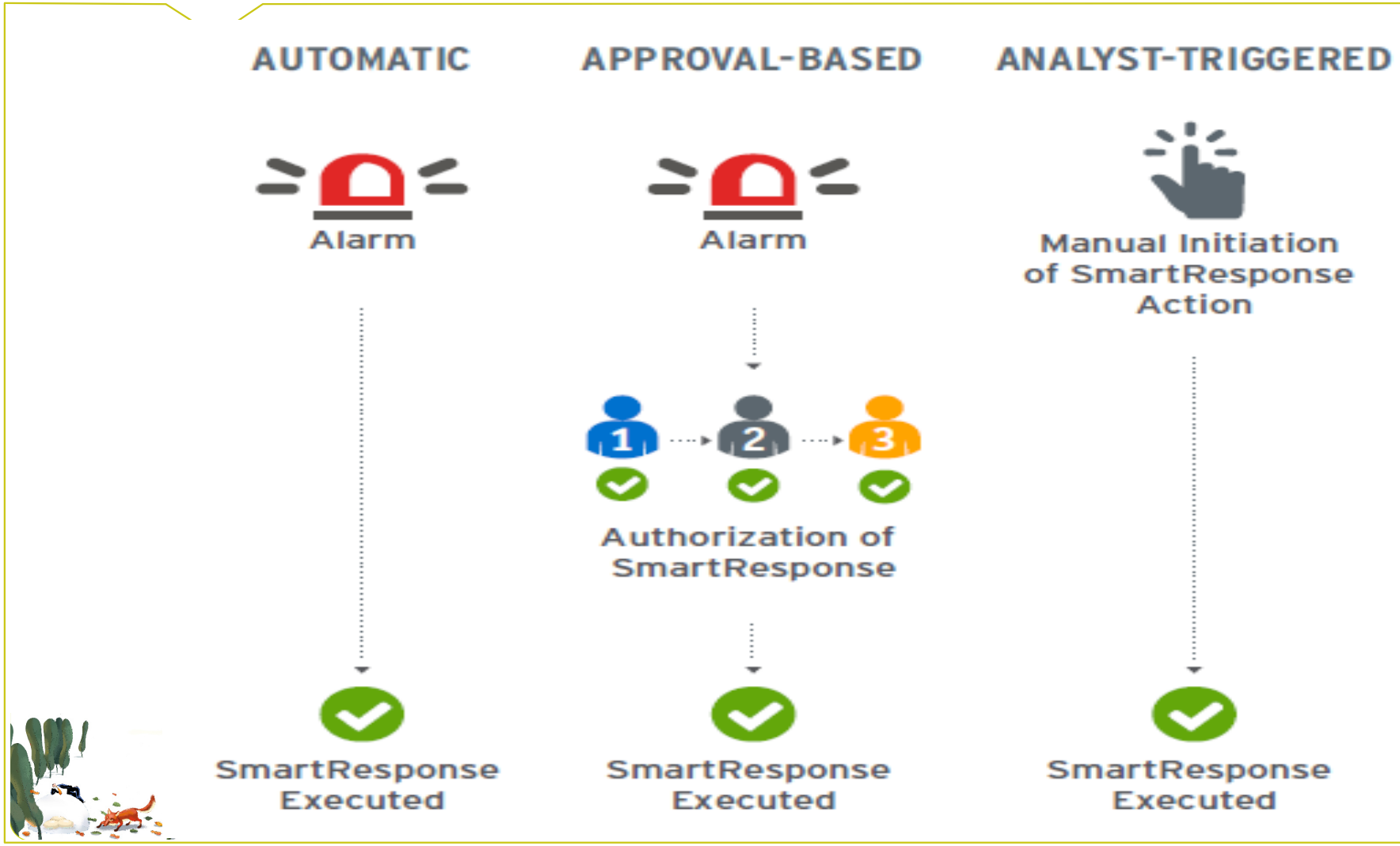
¿Qué aporta un mecanismo de estas características?

TPS: mimetizando al analista SOC

Reconstrucción de tramas de ataque completas

1. Indicio de anomalía
2. El TPS lo divide en componentes a investigar
3. Se crea una hipótesis de investigación
4. Se inicia la recolección de evidencias para probarlo /descartar
5. Se visualiza la trama completa del ataque
6. El analista recibe la informacion enriquecida y prosigue análisis / toma acciones

¿Hasta donde dejar la automatización ?



acuntia 3.0

www.acuntia.es