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"

De que estamos hablando : Ciberamenazas

Copyright © 2017 Acuntia

Cada vez nos cuestan más

LOS INCIDENTES CADA VEZ SON MAS COSTOSOS

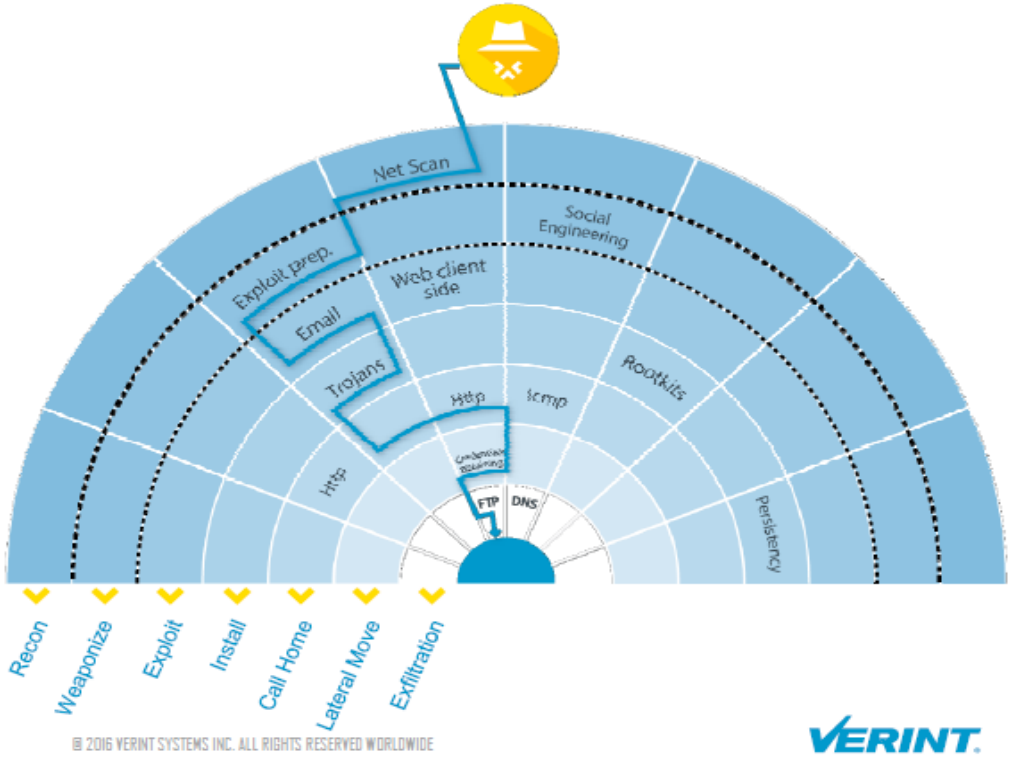
- 2060 Millones de datos de clientes comprometidos
- 146 días de media para la detección de infiltraciones
- $3,000 Millones de valor de mercado destruido
- 1,000 Millones de $ negocio en RANSOMWARE
- 1 Millón de elementos de Malware creados al día.
- Para 2019, el gasto en remediación de brechas de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

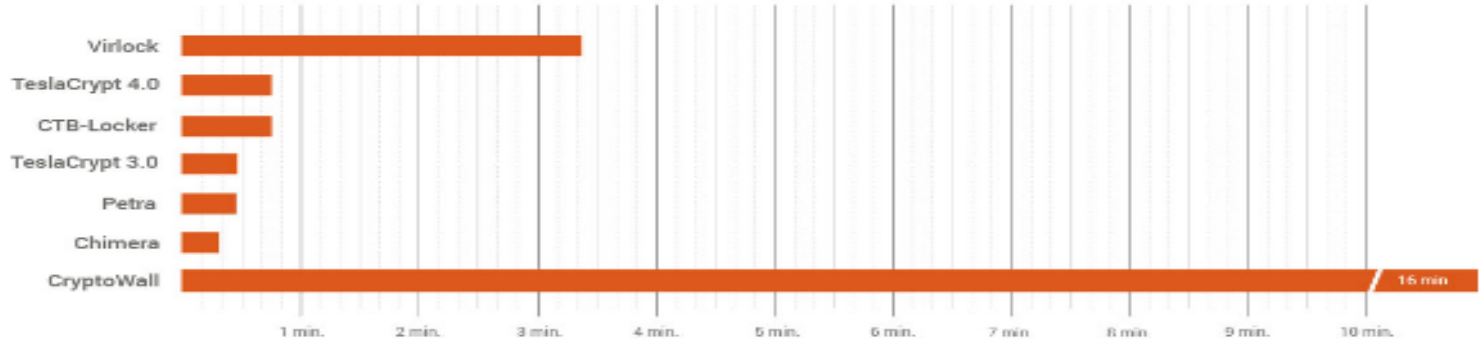


Necesitamos mucha tecnología distinta.

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...)

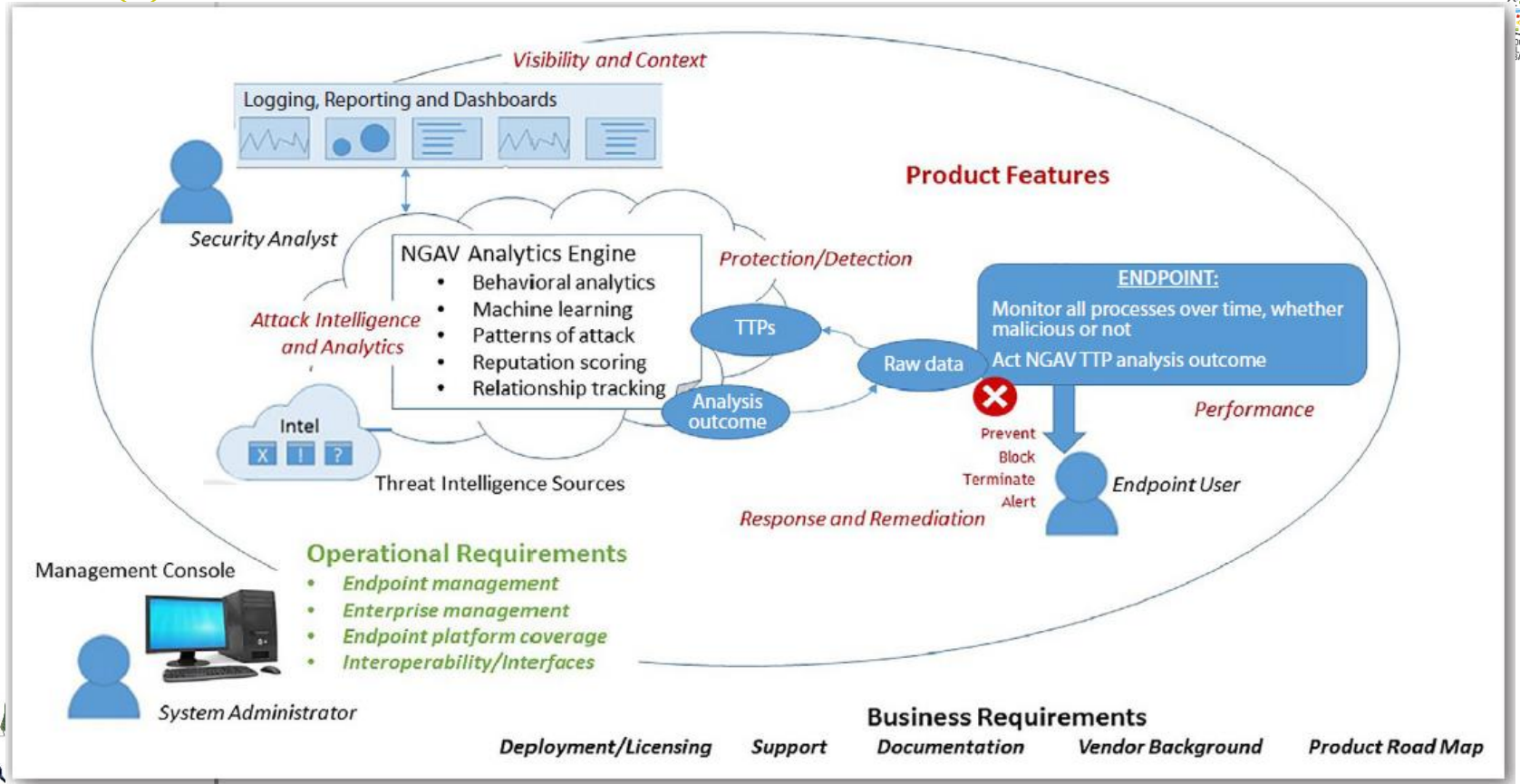
Encriptación del disco



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

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

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

Nube

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

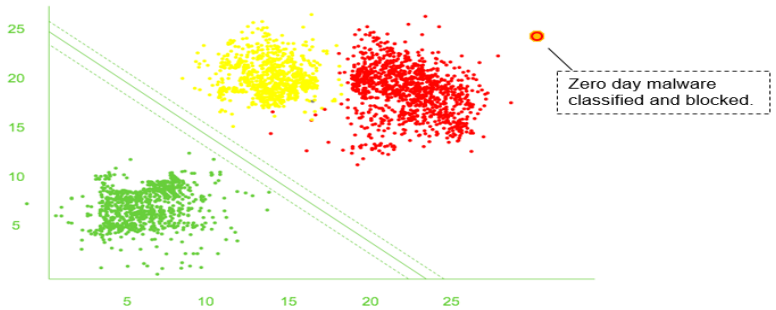
We test on **100,000,000** new good and **100,000,000** new bad files.

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

>6,000,000 features.

>600,000,000 data samples.

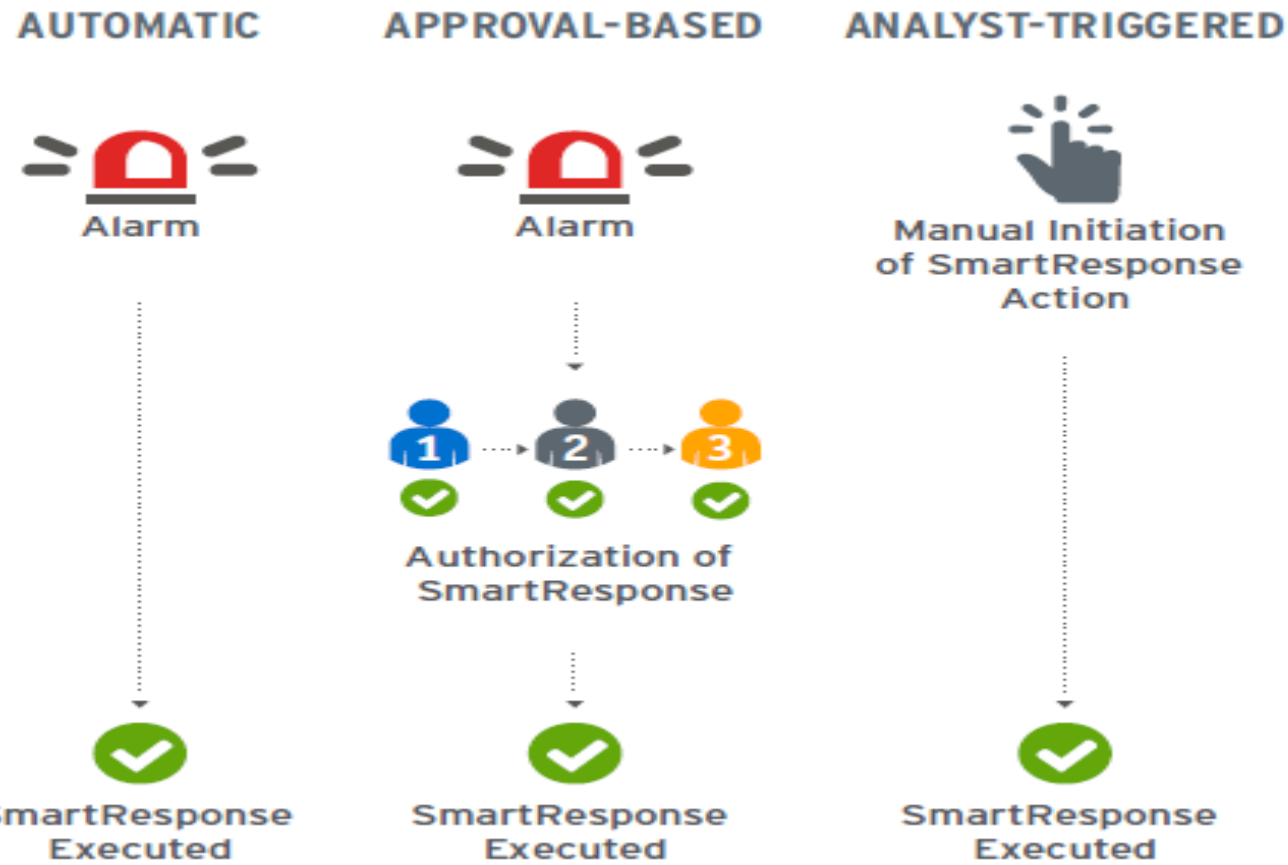
3,600,000,000,000,000
(3 quadrillion) data points in total.



(Algoritmo)
Agente SW

Objetivo a cumplir

¿Hasta donde dejar la automatización ?



www.acuntia.es