Compartir Inteligencia de Ciberamenazas

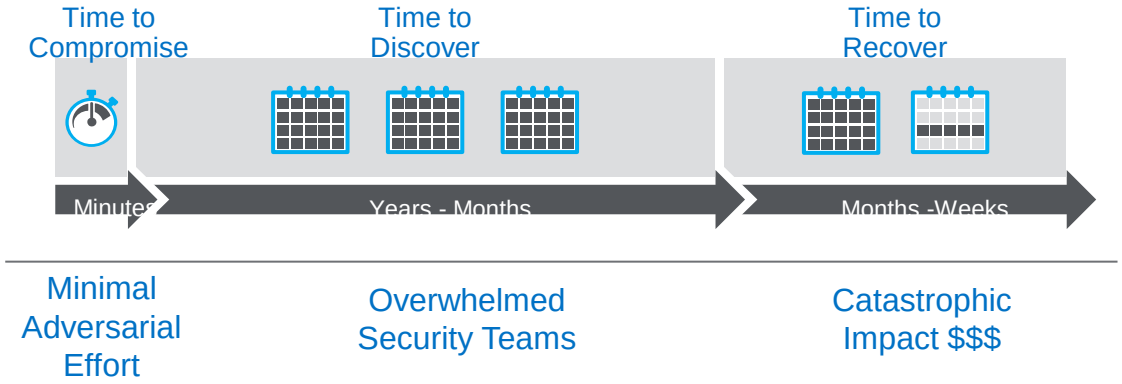
Barcelona, 03 de Mayo 2016

Roger Gallego | Business Manager Intel Security Catalunya

Realidades actuales en ciberamenazas

30 de Noviembre. Día internacional de la Ciberseguridad
5 de Mayo. World Password Day

- *Los ciberincidentes han aumentado un **116%** este año 2015 (INCibe)*
  - *18,000 incidentes en 2014*
  - *50,000 incidentes en 2015*
- *Los ciberdelitos aumentan a un ritmo del **12%** anual*
- *El cibercrimen origina pérdidas valoradas en más de **500,000 M€** al año a nivel mundial*
- *En 2020 se espera que el número de dispositivos inteligentes supere los **200.000 millones***
- *Tendencias esperadas en 2016: **ransomware** (cibersecuestro), ataques a **automóviles** o a **infraestructuras**, y el almacenamiento y venta de los datos robados*



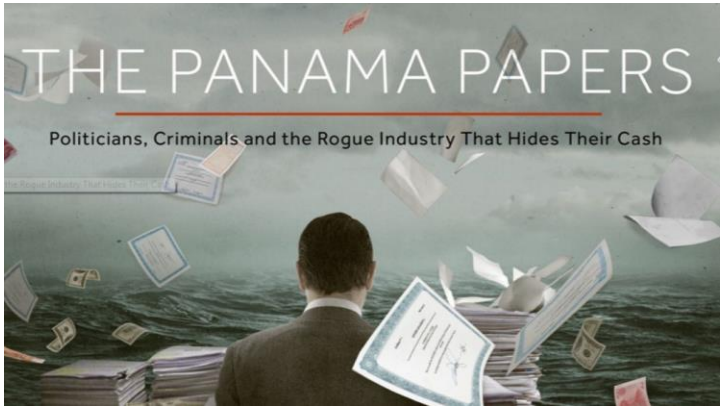
Un día en McAfee Labs

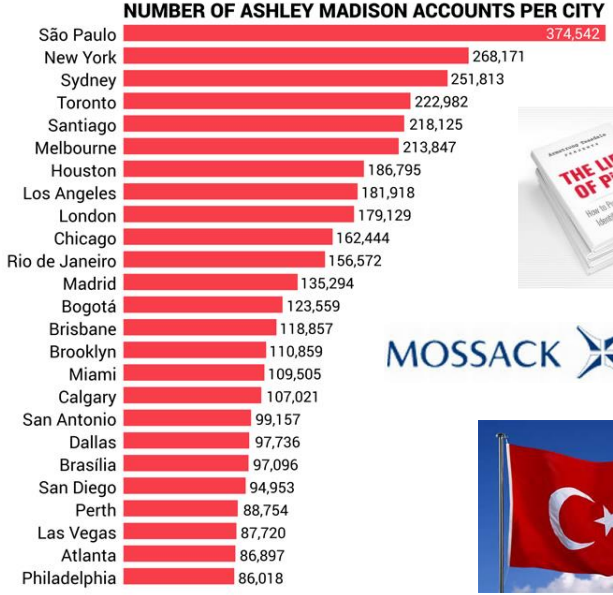
- McAfee GTI received on average **47.5 billion queries** per day.
- Every day more than **157 million attempts** were made (via emails, browser searches, etc.) to entice our customers into connecting to risky URLs.
- Every day more than **353 million infected files** were exposed to our customers' networks.
- Every day an additional **71 million potentially unwanted programs** attempted installation or launch.
- Every day **55 million attempts** were made by our customers **to connect to risky IP addresses**, or those addresses attempted to connect to customers' networks

Q4 2015 Vincent Weafer, Senior Vice President, McAfee Labs

McAfee Labs
Threats Report
March 2016

www.mcafee.com/us/mcafee-labs.aspx





MOSSACK FONSECA

dadaviz.com

Madurez de la Seguridad percibida

Madurez de la Seguridad real

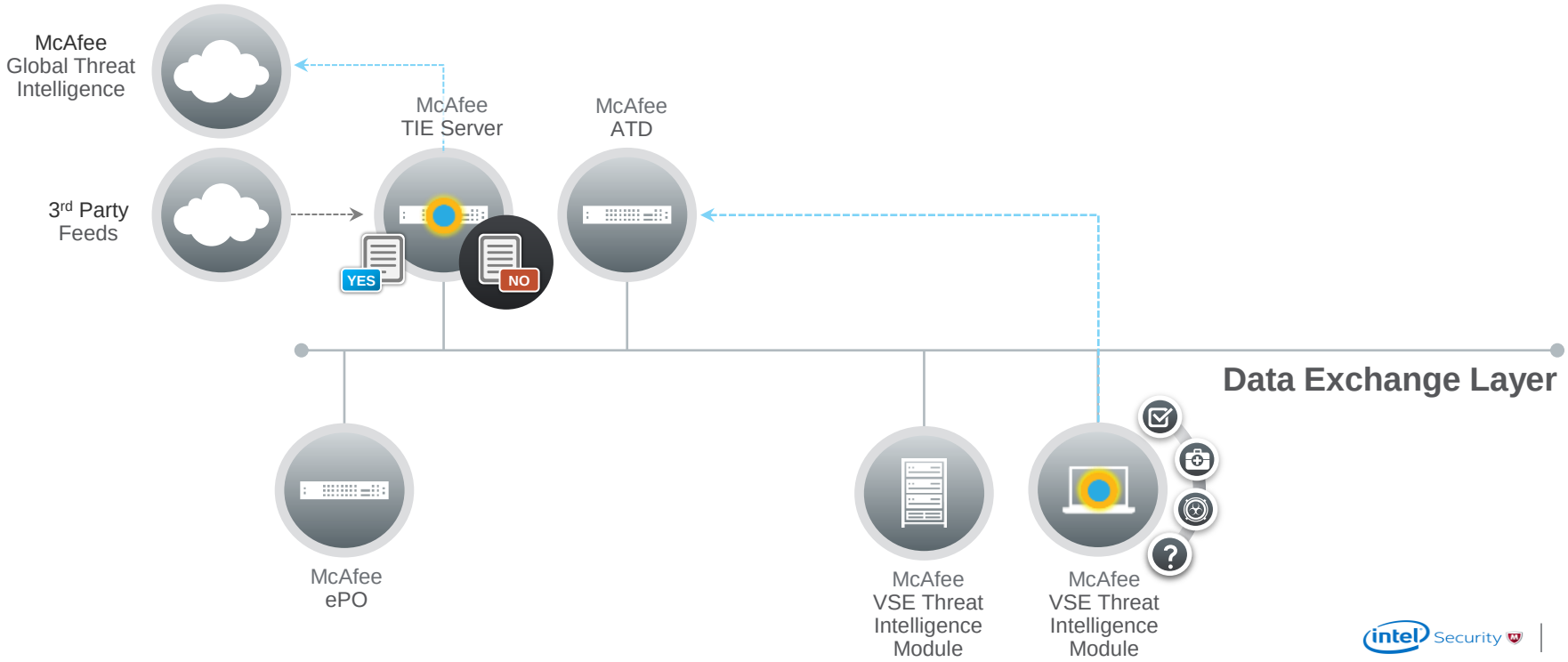
Security's Perfect Storm
Limitaciones del negocio

Increasing Complexity
- Exponential growth in data and devices
- "Shift to cloud" erodes visibility and control
- Fragmented security environment

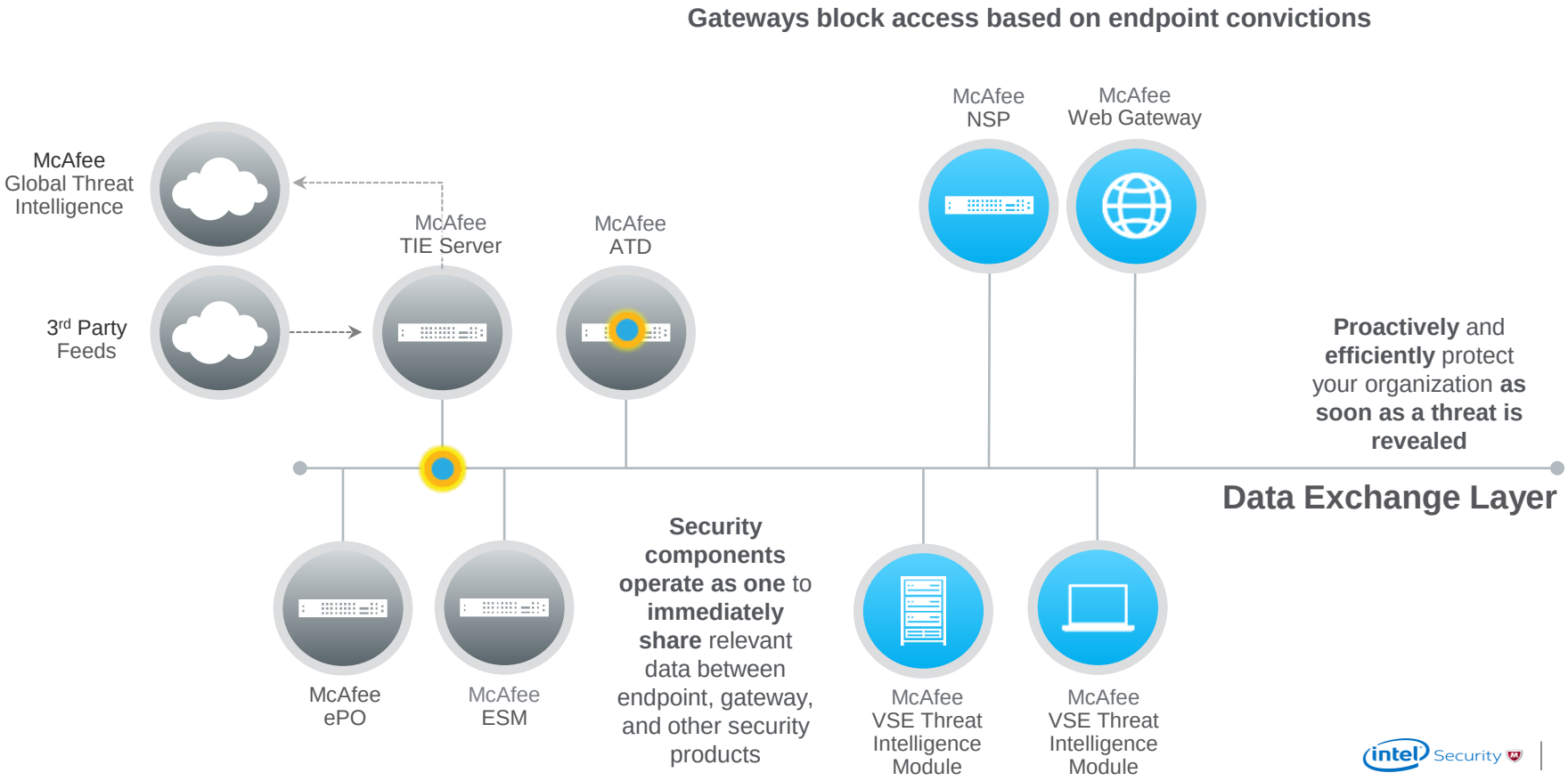
Time Imperative
- Organizations compromised in minutes
- Dwell times lasting for months
- Damage can be catastrophic

Resource Constraints
- Acute staffing and skills shortages
- Competitive pressures
- Linear budgets

Threat Intelligence Exchange Architecture



Threat Intelligence Exchange - Advance Malware Sandboxing



Tecnologías de Protección

Blacklisting

Known bad files
Anti-Virus Technology
Intelligence is Global
Daily updates

¿Qué hacemos con el resto?

IoA (Indicators of Attack)
IoC (Indicators of Compromise)

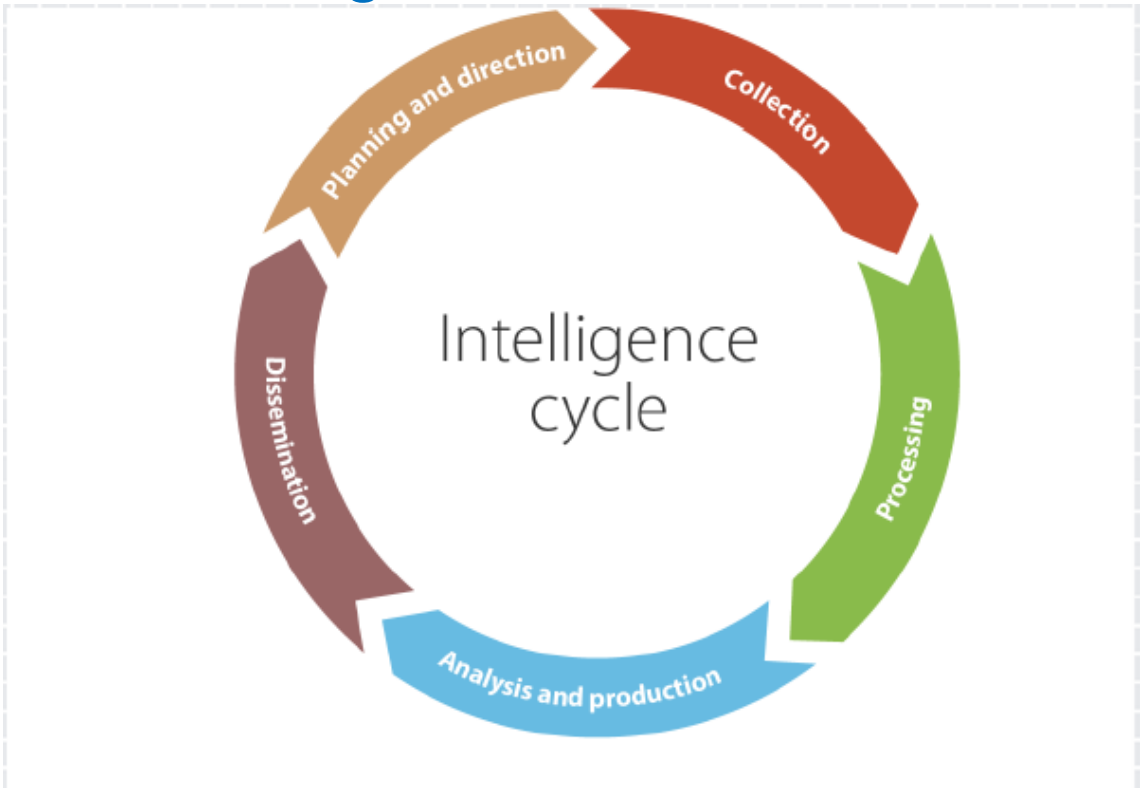
Whitelisting

Known good files
Application Whitelisting
Intelligence is Manual
Ad-Hoc Updates

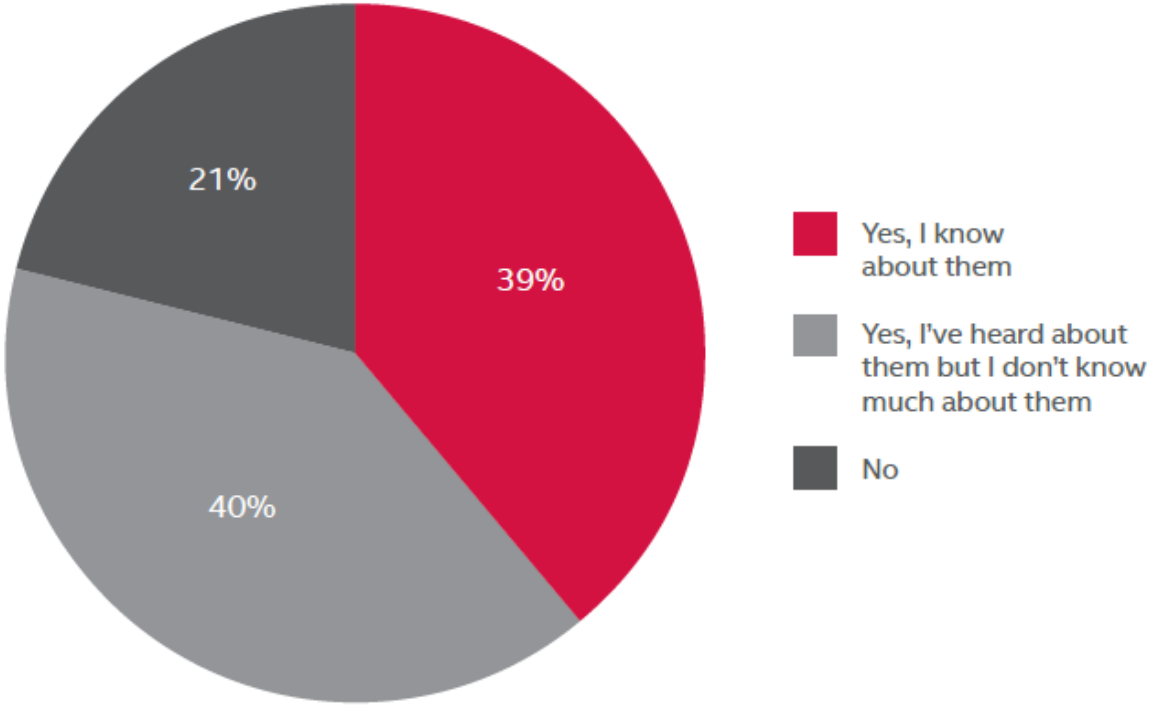
¿Qué es CTI (Cyber Threat Intelligence)?

What activity are we seeing?	 Observable	What threats should I look for on my networks and systems, and why?	 Indicator
Where has this threat been seen?	 Incident	What does it do?	 TTP
What weaknesses does this threat exploit?	 Exploit Target	Why does it do this?	 Campaign
Who is responsible for this threat?	 Threat Actor	What can I do about it?	 Course of Action

Ciclo de ciber-inteligencia

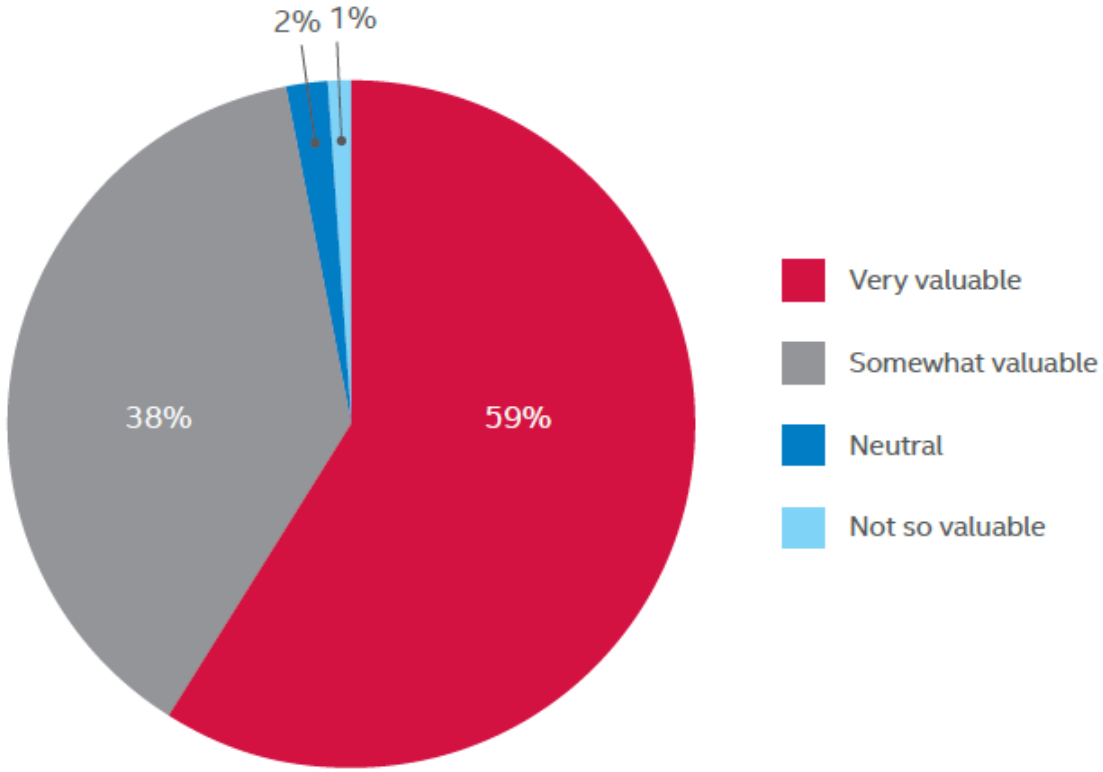


Are You Aware of Any Cyber Threat Intelligence Sharing Initiatives?



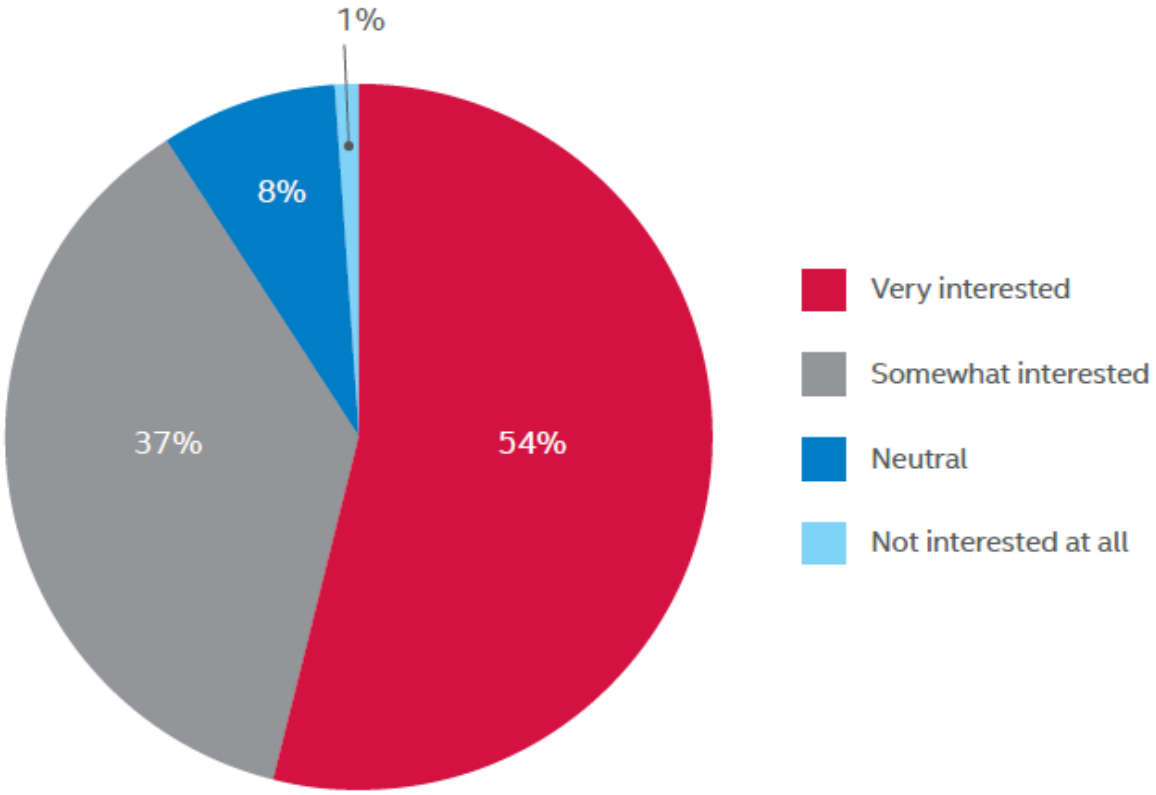
Source: Intel Security survey, 2015.

How Valuable Is Cyber Threat Intelligence Sharing to Your Organization?



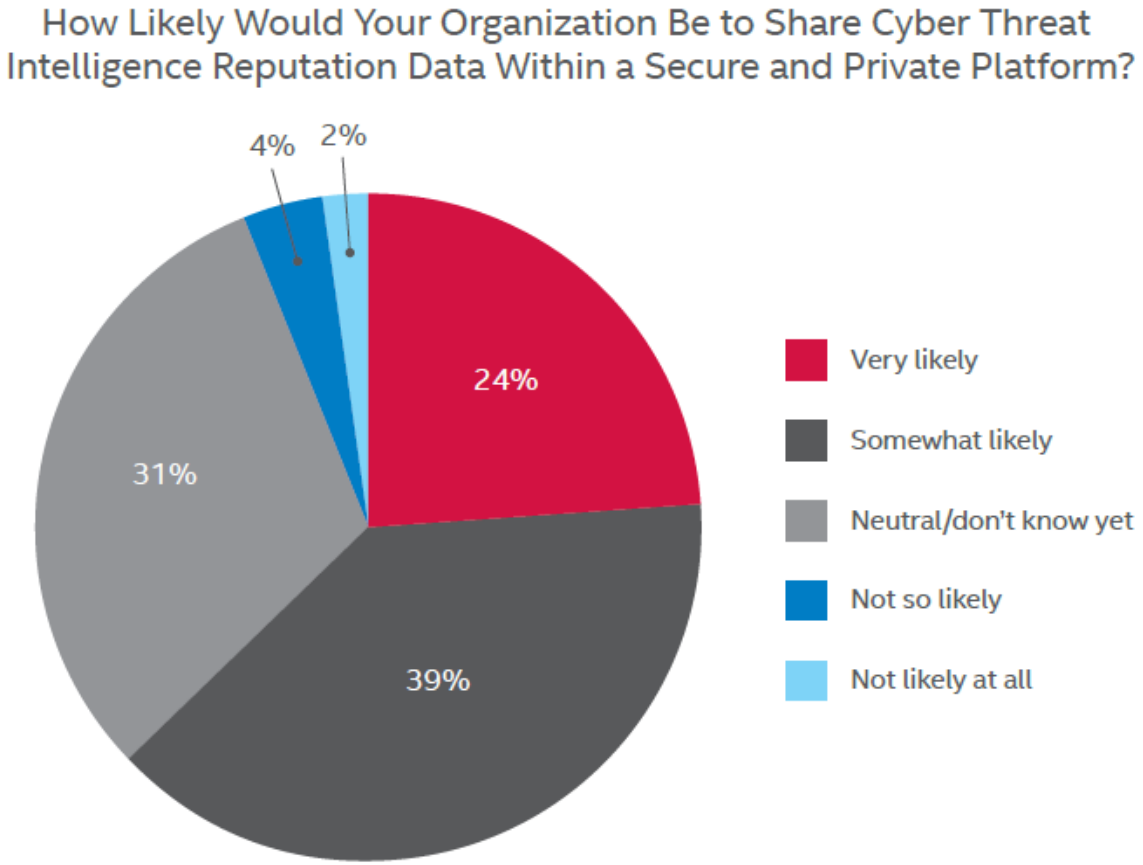
Source: Intel Security survey, 2015.

How Interested Would You Be in Receiving Cyber Threat Intelligence Related to Your Industry?



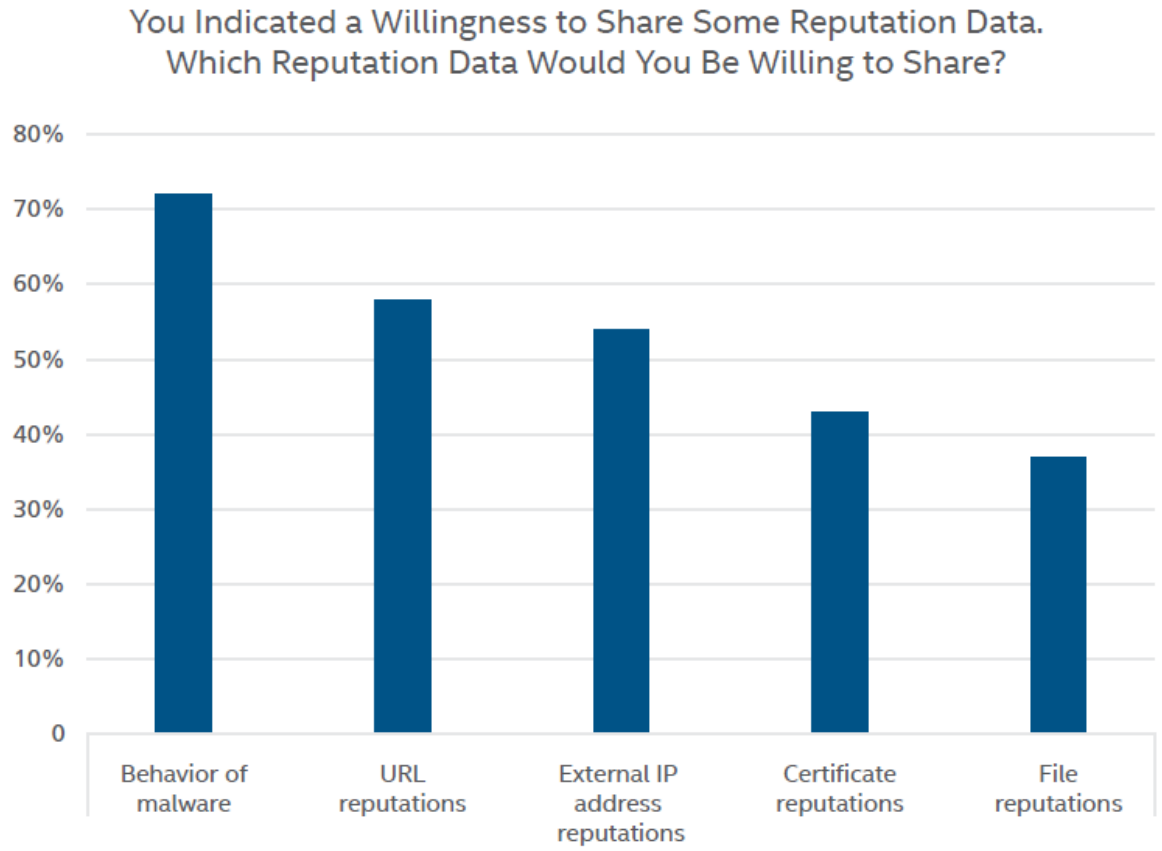
Source: Intel Security survey, 2015.

- Comportamiento del malware
- Reputaciones URL
- Reputaciones de Ficheros



Source: Intel Security survey, 2015.

- Políticas Corporativas



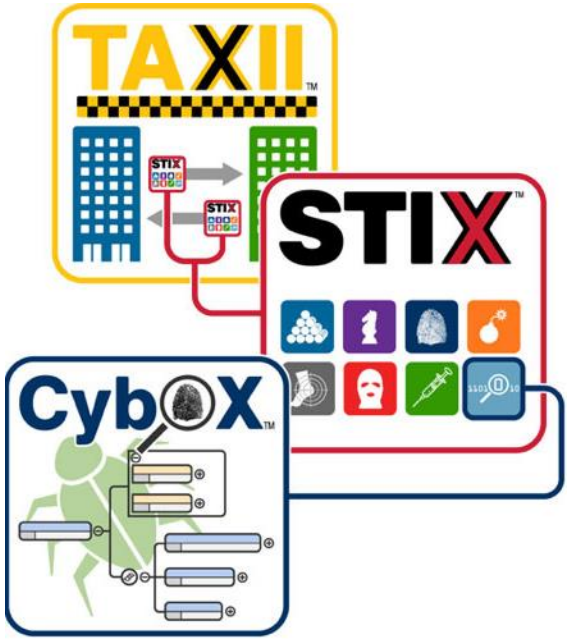
Source: Intel Security survey, 2015.

- Confianza
- Responsabilidad ante terceros

Source: Intel Security survey, 2015.

Por qué las organizaciones no comparten CTI

- Política corporativa *(Hash)*
- Atrapar a los malos
- Temas legales (NDA, MOU)
- Temas de Privacidad (Evitar multas)
- Estándares de intercambio
  - TAXII,™ Trusted Automated eXchange of Indicator Information.
  - STIX,™ Structured Threat Information eXpression.
  - CybOX,™ Cyber Observable eXpression.
  - OASIS *Organization for the Advancement of Structured Information Standards*



El futuro de CTI

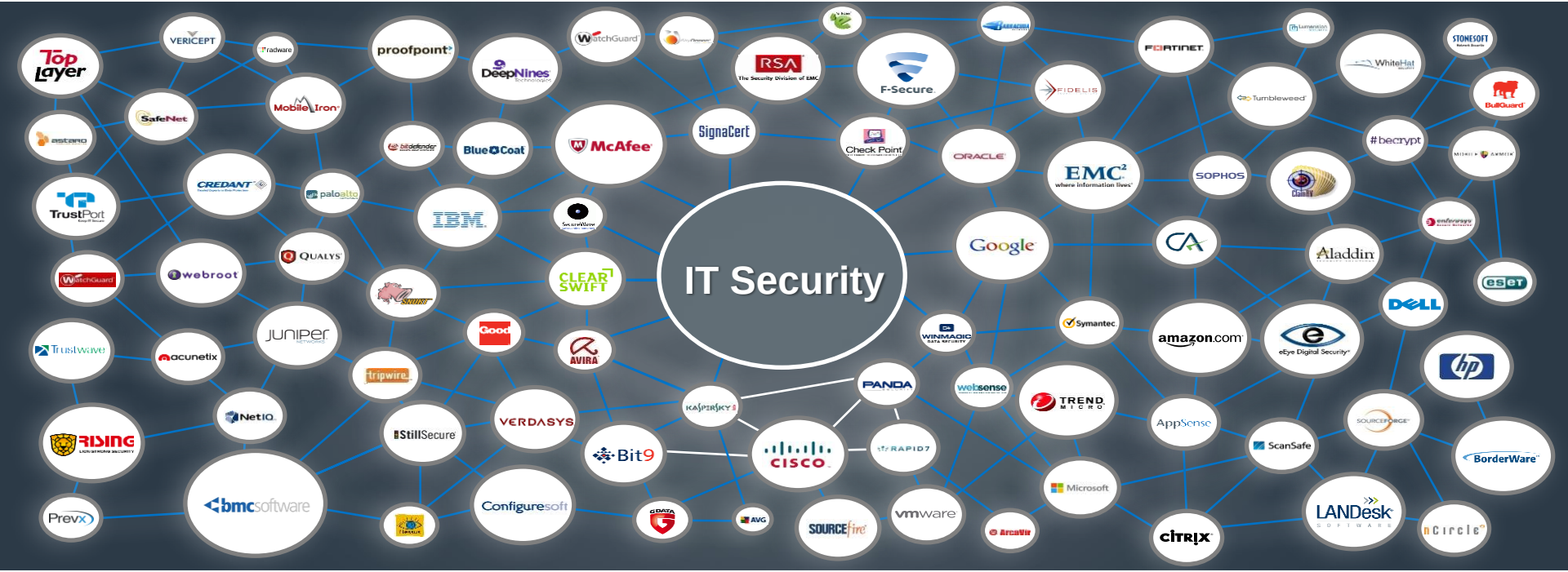
- Marcos legales HS. Cybersecurity Act 2015
- Aumento de compartición en la comunidad
- Integración de la automatización
- Organizaciones innovadoras y servicios alrededor de CTI
  - Consistency, Type & Quality
  - Enrich the data
- CTA (Cyber Threat Alliance)
  - Vulnerabilities and Exploits, new Malware samples, and Botnet control infrastructure
  - Specific campaigns, including in-depth technical analysis and the development of recommendations for prevention and mitigation.

CYBER THREAT ALLIANCE

FORTINET
intel Security
paloalto NETWORKS
Symantec.
Barracuda
Eleven Paths
REVERSING LABS
zscaler

Fabricantes de Seguridad

El proceso habitual de adquisición de tecnologías ha provocado un Caos en el entorno de Seguridad



Entretenimiento

- **El año de la garrapata** (Jorge Coira, 2004)
  “¡Voy a venderlo todo!”

- **Mr Robot** (Sam Esmail, 2015)

- **The Blacklist** (NBC Sony Pictures, 2013)

Gràcies

roger.gallego@intel.com