ARBOR NETWORKS
The Security Division of NETSCOUT

Cinco puntos para mejorar la detección y respuesta ante amenazas avanzadas

Carlos Ayala, Consulting Engineer LATAM | @caar2000
CISSP, GCIA, GCFA, GNFA, GCIH, GMON, GPEN, GCCC

Agenda

1. Introducción: Conceptos y problemática
2. Tendencias (Arbor WISR 2016, SANS Institute y RAND)
3. Soluciones para mejorar la detección y contención de amenazas avanzadas
   - *Ciber inteligencia de amenazas*
   - *Respuesta a incidentes*
   - *Priorización (triaje)*
   - *Mejorar las capacidades de la gente*
   - *Equipo y técnicas de caza*
4. La plataforma Arbor Spectrum.
5. Conclusiones

© Arbor Networks, Inc. All rights reserved.

El ciber espacio

- El ciber espacio es el sistema más grande en la historia de la humanidad 3,326 millones de usuarios en 2016*
  - Básicamente es nuestro *teatro de operaciones*
- Los ciber criminales gozan de ventajas inalcanzables en este medio, es difícil identificarlos técnicamete, son muy competentes y cuesta mucho más procesarlos legalmente
  - *Características inherentes del ciber espacio (4A's)*

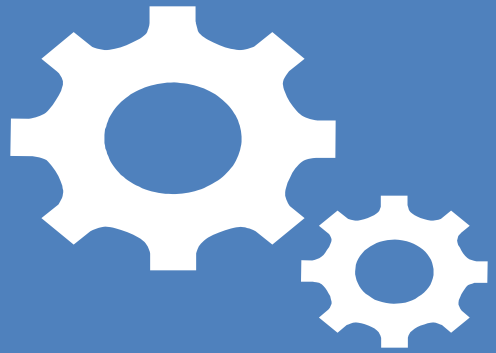
Anónimo	Abierto
Anárquico	Armamentizado

ARBOR NETWORKS
The Security Division of NETSCOUT

http://www.internetlivestats.com/internet-users/

I. Herramientas de detección temprana

Obtener observables de múltiples fuentes de red (NSM) para la detección temprana y respuesta oportuna



©2015 ARBOR® CONFIDENTIAL & PROPRIETARY

ARBOR® NETWORKS

2. Integración de Ciber inteligencia de amenazas y Respuesta a Incidentes

Multiples fuentes de información para agregar contexto y mejorar el proceso de Respuesta a Incidentes

©2015 ARBOR® CONFIDENTIAL & PROPRIETARY

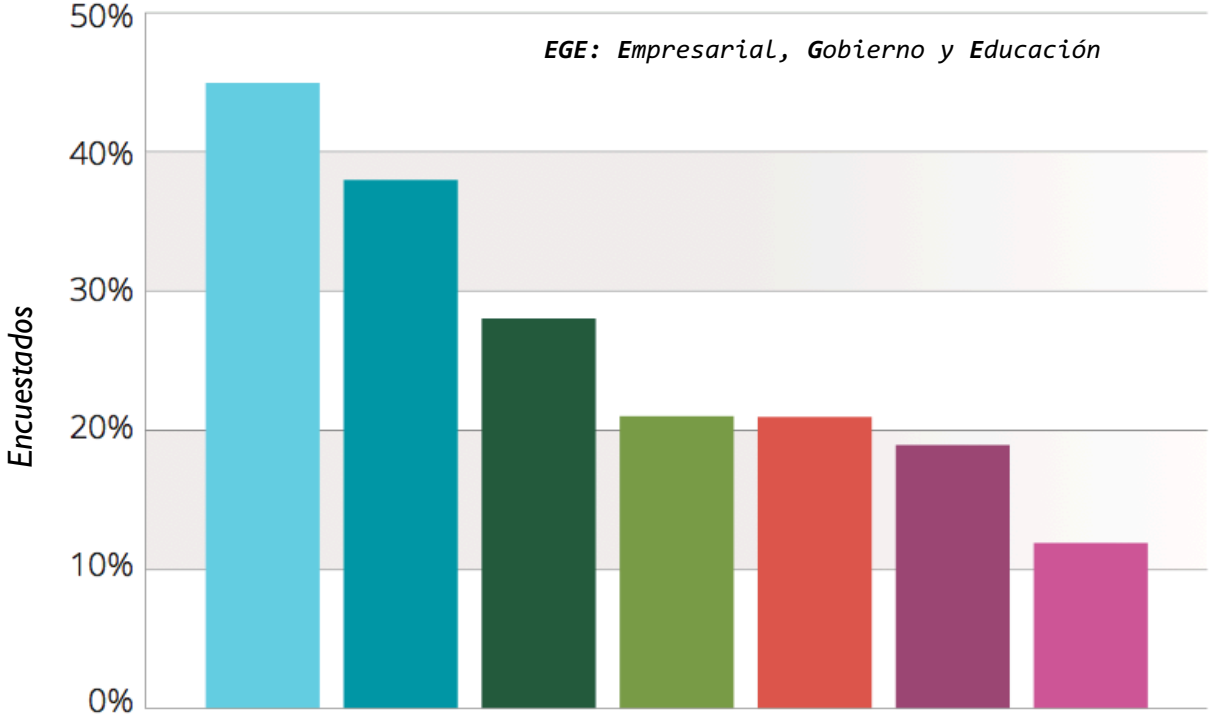
ARBOR® NETWORKS

3. Mejorar el proceso de priorización

Muchos datos por analizar y enfocarse en lo importante

©2015 ARBOR® CONFIDENTIAL & PROPRIETARY

Monitorización interna de la red (BYOD)



- **38%** de los encuestados aún **no tienen nada implantado** para la monitorización interna de la red (BYOD) http://www.arbornetworks.com/insight-into-the-global-threat-landscape

ARBOR NETWORKS
The Security Division of NETSCOUT

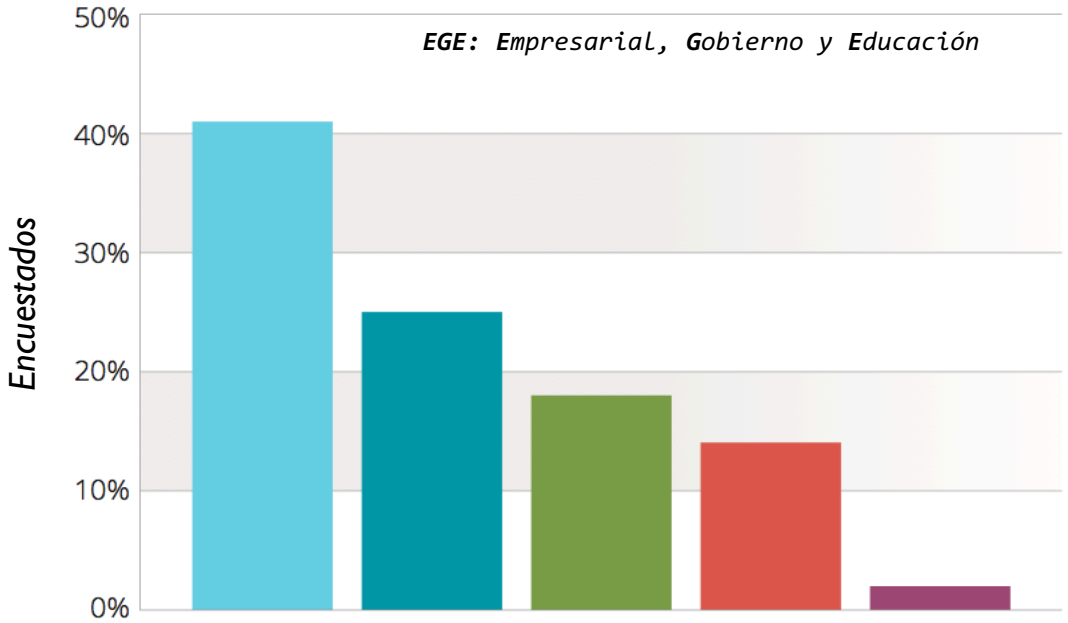
4. Incrementar el personal de seguridad

Mejorar las capacidades analíticas y desarrollar el talento de los analistas

©2015 ARBOR® CONFIDENTIAL & PROPRIETARY

ARBOR® NETWORKS

Postura de Respuesta a Incidentes (RI)



- 41% Tienen un plan de RI con recursos limitados
- 25% Tienen un plan de RI con recursos suficientes
- 18% No tienen un plan de RI
- 14% Tienen un plan de RI sin recursos
- 2% Un tercero les proporciona los servicios de IR

- **Solo el 25%** de las organizaciones tienen un plan de **Respuestas a Incidentes con recursos suficientes**
- Un plan de Respuestas a Incidentes sin recursos o con recursos a medias **no es funcional**
  - http://www.arbornetworks.com/insight-into-the-global-threat-landscape

ARBOR NETWORKS
The Security Division of NETSCOUT

5. Crear un equipo de caza

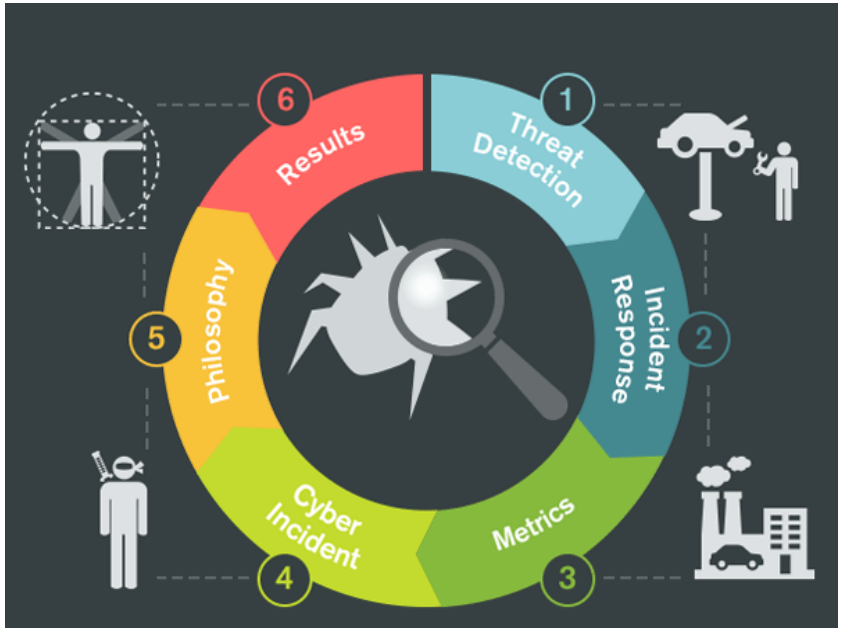
Detección proactiva de IOC para reducir el impacto de las operaciones de los ciber adversarios

©2015 ARBOR® CONFIDENTIAL & PROPRIETARY

ARBOR® NETWORKS

Crear un equipo de caza

- Si no tenemos un equipo de caza en la organización **estamos perdiendo**
  - Necesitamos tener un equipo activo de caza para que la ciber inteligencia de amenaza tenga un impacto positivo en la organización
- Necesitamos entender las amenazas de cada organización analizando las intrusiones usando modelos como
  - Cadena de progresión de la amenaza (*Cyber Kill Chain*)
  - Modelo diamante
- Inclusión de las **técnicas de caza al flujo operativo** del proceso de **Respuesta a Incidentes**
- Ayudar al **"Blue Team"** a **priorizar los esfuerzos**

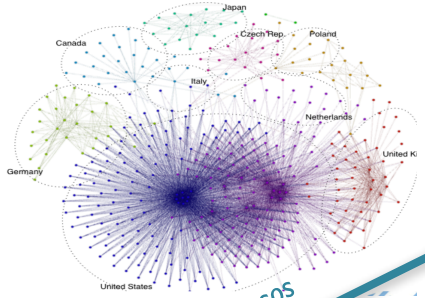


Evaluación: ¿Cómo estás cazando?
http://bit.ly/1f0dbwl

ARBOR NETWORKS
The Security Division of NETSCOUT

Business benefits of threat hunting
http://www.arbornetworks.com/blog/insight/business-benefits-of-threat-hunting/

Modelo diamante de Neverquest



Adversario

- **Distribuido geográficamente**

Alemania
Japón
Polonia
Canada
EEUUAA
República Checa
Reino Unido

usan

desarrolla

Implantada a través de

Infraestructura

- **Infraestructura C2**
- **Actualizaciones de TOR**
  - 453pn6kasexkbqxiztbio2mnh2p gl6nrxdqgylngcyw4dehz
  - 453pn6kasexkbqxiztbio2mnh2p gl6nrxdqgylngcyw4dehz
  - 5h3ejaxii4fshu4e7qpxfodfh6fvpq yckfz2wdsf45s42mempt3ayo2bn 7inhq6

Se conecta a

explota

Capacidades (TTP)

- **Ciber adversario avanzado**
  - Inyección web
    - (‘client.schwab.com/Accounts/’, ‘</body>’, ‘<script>\r\nLoadPageGood();\r\n</script>\r\n</body>’, ‘\x0c\x07 ‘)
  - Armamentización con esteganografía
  - Semillas de cifrado dinámicas

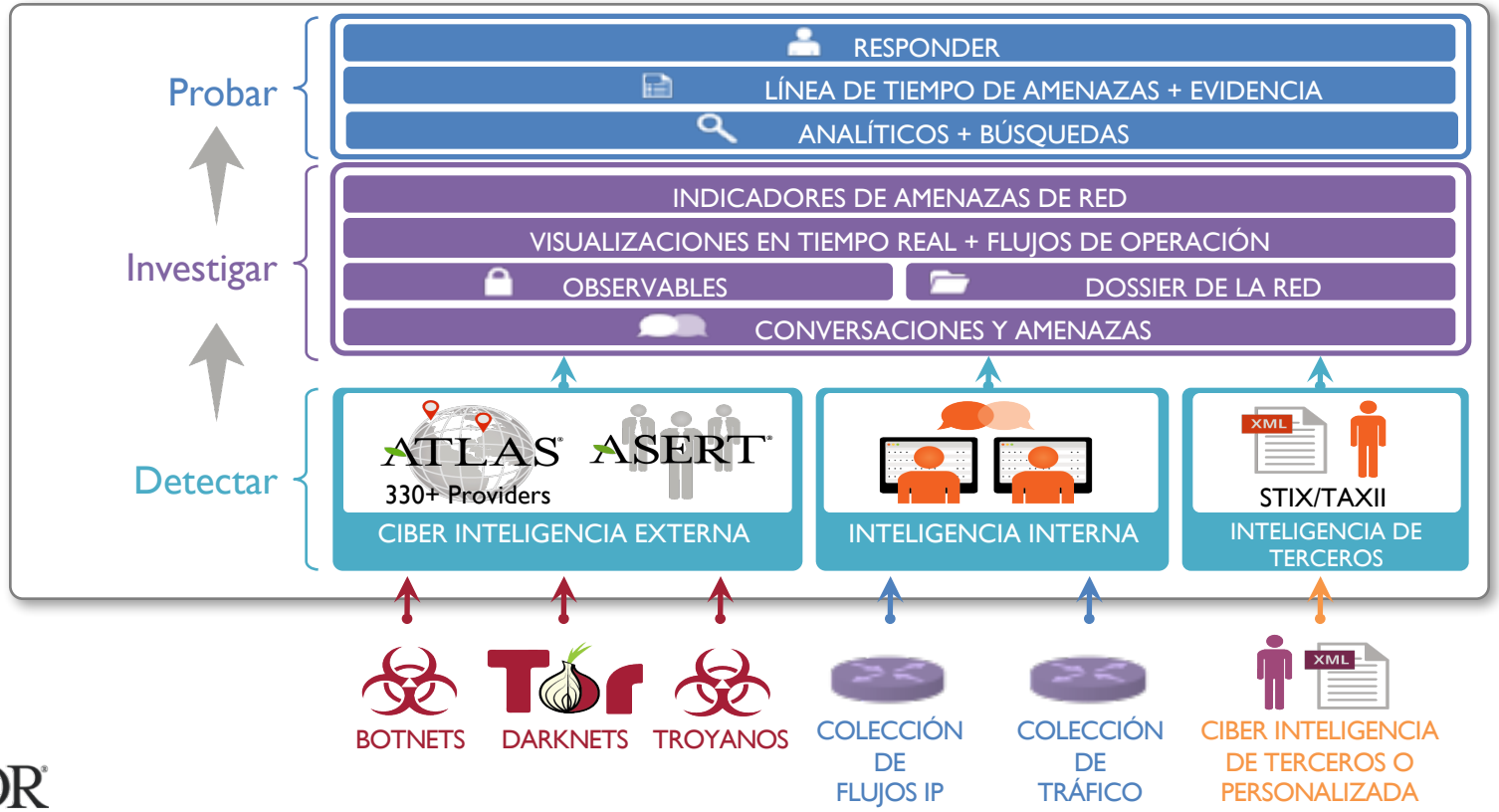
Víctima

- **Por nombre**
  - 53.com
  - accessmycardonline.com
  - accountonline.com
  - accurint.com

http://www.arbornetworks.com/blog/asert/neverquest-a-global-threat-targeting-financials/

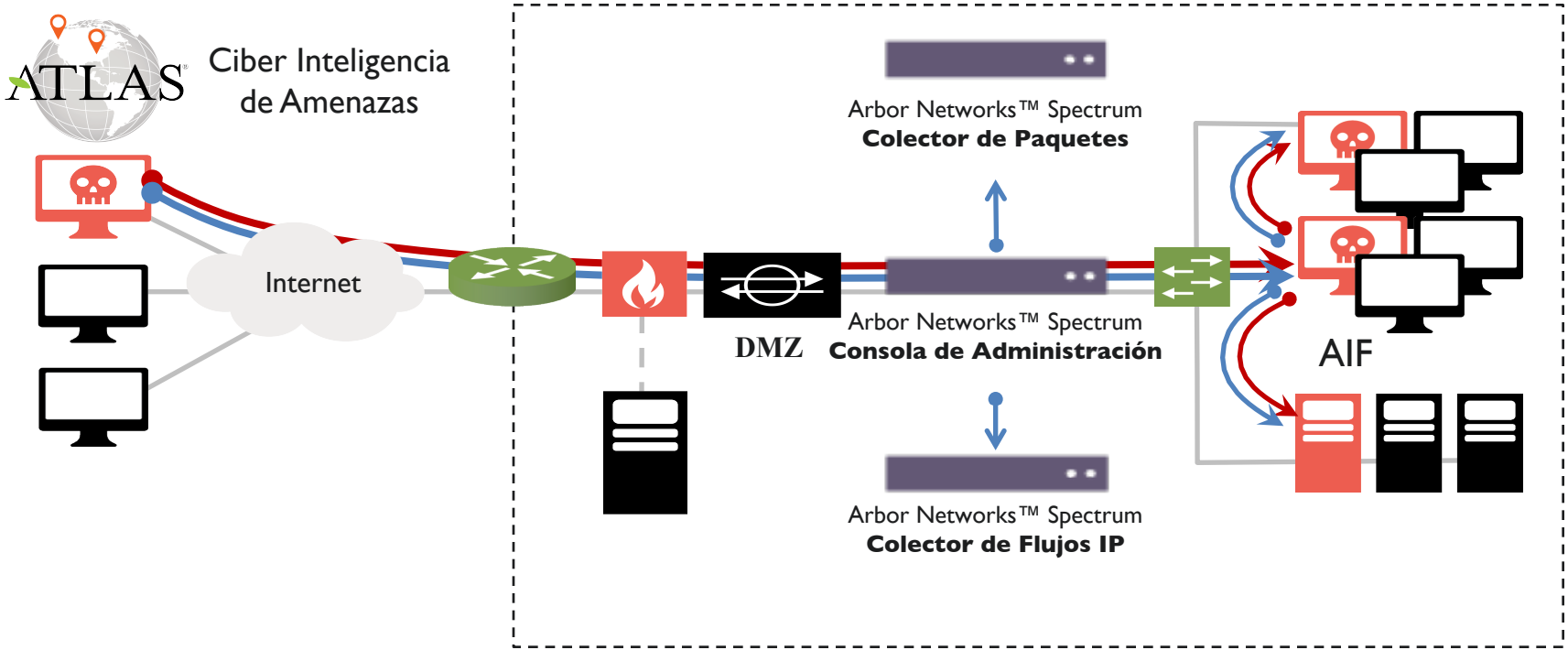
ARBOR NETWORKS
The Security Division of NETSCOUT

La plataforma Arbor Spectrum



ARBOR NETWORKS
The Security Division of NETSCOUT

Implantación de Arbor Spectrum



ARBOR NETWORKS
The Security Division of NETSCOUT

En resumen

- Combatimos contra **personas talentosas** y el talento humano es difícil de mitigar
- Las amenazas aumentan en complejidad y **requerimos más observables** para **reducir puntos ciegos**
- Requerimos mejores **soluciones que automaticen el proceso de detección** e indicadores tempranos
- Necesitamos **priorizar** para enfocarnos en lo importante
- Requerimos desarrollar **capacidades analíticas** y de **Respuesta a Incidentes** en nuestro personal
- Necesitamos crear **equipos de caza** para bucar proactivamente el compromiso
- **Arbor Spectrum** instrumenta la **detección de múltiples fuentes internas,** la **ciber inteligencia de amenazas del ASERT** y sintetiza la información **de manera visual** para **responder rápidamente** ante **amenazas y mitigarlas con Pravail APS**

ARBOR NETWORKS
The Security Division of NETSCOUT

Referencias

1. http://www.internetlivestats.com/internet-users/
2. http://dl.acm.org/citation.cfm?id=1996332
3. http://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1354/RAND_RR1354.pdf
4. http://www.arbornetworks.com/insight-into-the-global-threat-landscape
5. www.gartner.com/id=1960615
6. https://www.sans.org/reading-room/whitepapers/analyst/eliminating-blind-spots-paradigm-monitoring-response-36712
7. https://nemesis.training.arbor.net
8. https://www.sans.org/reading-room/whitepapers/analyst/cyberthreat-intelligence-how-35767
9. https://atlas.arbor.net/briefs/
10. Threat Intelligence: Collecting, Analysing, Evaluating mwrinfosecurity.com | CPNI.gov.uk | cert.gov.uk
11. https://asert.arbornetworks.com/defending-the-white-elephant/
12. http://www.arbornetworks.com/blog/asert/ntp-attacks-continue-a-quick-look-at-traffic-over-the-past-few-months/
13. http://pages.arbornetworks.com/rs/arbor/images/Uncovering_PoS_Malware.pdf
14. http://www.digitalattackmap.com
15. https://atlas.arbor.net/summary/fastflux
16. www.sans.org/reading-room/whitepapers/analyst/analytics-intelligence-survey-2014-35507survey-2014-35507
17. http://taosecurity.blogspot.mx/2014/09/a-brief-history-of-network-security.html
18. http://www.forbes.com/sites/davidkwilliams/2013/02/19/what-a-fighter-pilot-knows-about-business-the-ooda-loop/#538433766650
19. http://www.arbornetworks.com/advanced-threat-arbor-spectrum
20. http://www.arbornetworks.com/more-than-one-target-point-of-sale-malware-campaigns-continue
21. Assessment: How are you hunting? http://bit.ly/1f0dbwI
22. http://www.arbornetworks.com/blog/insight/business-benefits-of-threat-hunting/
23. https://www.sans.org/reading-room/whitepapers/bestprac/threat-hunting-open-season-adversary-36882
24. http://cyber.lockheedmartin.com/solutions/cyber-kill-chain
25. http://www.dtic.mil/get-tr-doc/pdf?AD=ADA586960
26. http://www.arbornetworks.com/blog/asert/neverquest-a-global-threat-targeting-financials/
27. http://www.arbornetworks.com/images/documents/Data%20Sheets/DS_AIF_EN.pdf
28. https://www.researchgate.net/publication/220450035_The_Financial_Impact_of_IT_Security_Breaches_What_Do_Investors_Think
29. https://cybertab.boozallen.com

¿ Preguntas ?

107 países
Donde las soluciones de Arbor han sido implementadas

15 años siendo líderes
De innovación, desarrollo, visibilidad de la red y ciber intel

Ciber inteligencia de amenazas
Con fuentes de información diversas con más de 140 terabytes del tráfico global de Internet

+ 90% de ISPs del mundo
Proveedores Tier 1

8 / 10 proveedores de nube
Más grandes del mundo

9 / 10 MSSPs de seguridad
De los proveedores más grandes del mundo

55% de los ingresos
Provienen de clientes Globales en Asia, Europa y Latinoamérica

Proveedor #1
En mitigación de DDoS en Carrier, Enterprise, Mobile, IHS Infonetics, June 2015

5 Juegos olímpicos
Protegidos por Arbor Networks

3 / 5 redes sociales
Más grandes

5 / 6 más grandes
Proveedores de banda ancha por cable de EE.UU.

4 del top 6
Bancos de Estados Unidos

ARBOR NETWORKS
The Security Division of NETSCOUT

The Security Division of NETSCOUT

©2015 ARBOR® CONFIDENTIAL & PROPRIETARY