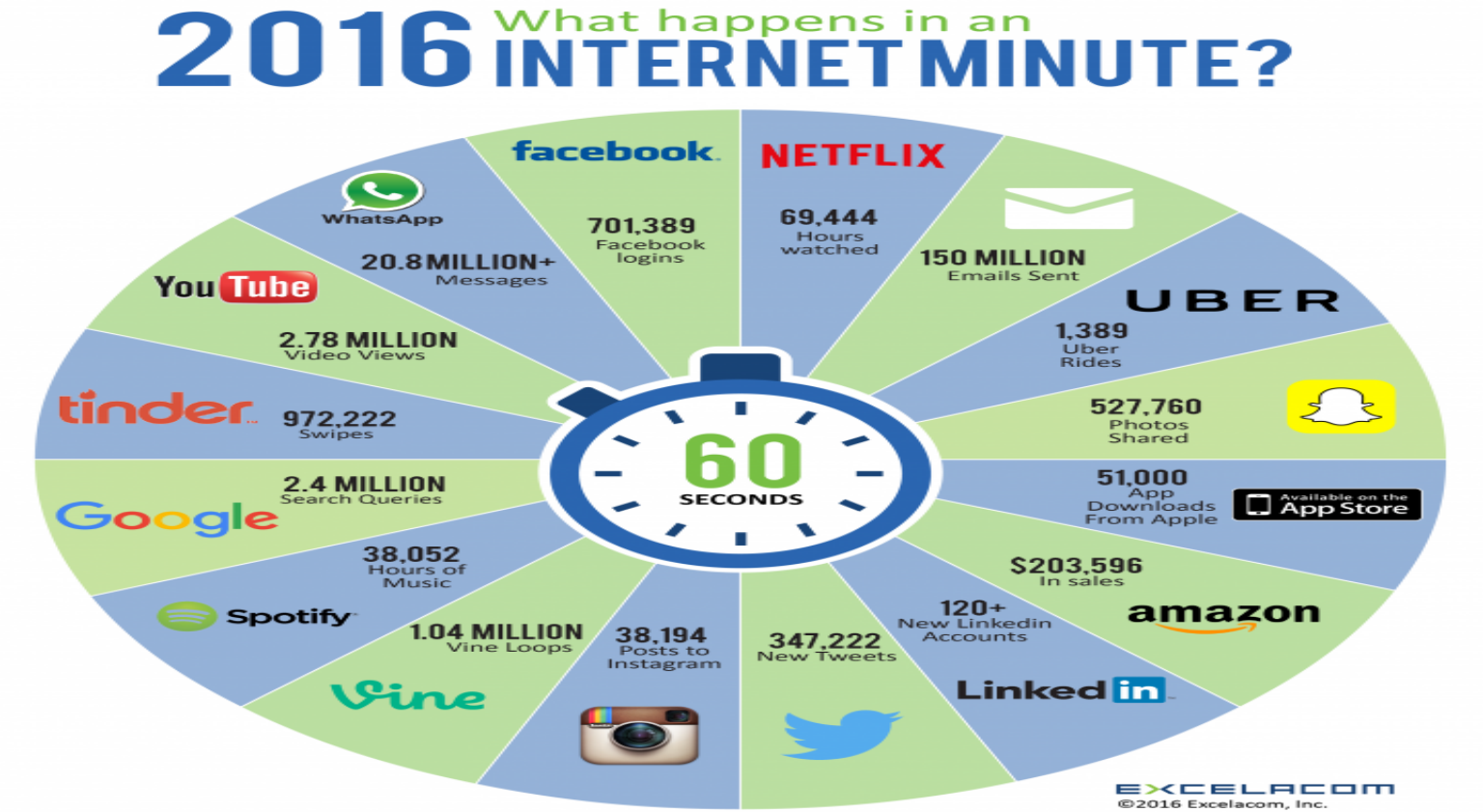
La importancia de los CISOs para la conuidad de negocio

Roberto Cruz
Responsable de Network Security
Mexico, Caribe y Centro América
Mayo 2016

FORCEPOINT
POWERED BY Raytheon

EL MUNDO AHORA (2016)



FORCEPOINT
POWERED BY Raytheon

NUEVAS ERA TECNOLÓGICA TRAE NUEVOS RETOS

IoT

Ambiente Empresarial en Evolución	Como adoptar tecnología que transforma de **manera segura y eficiente**

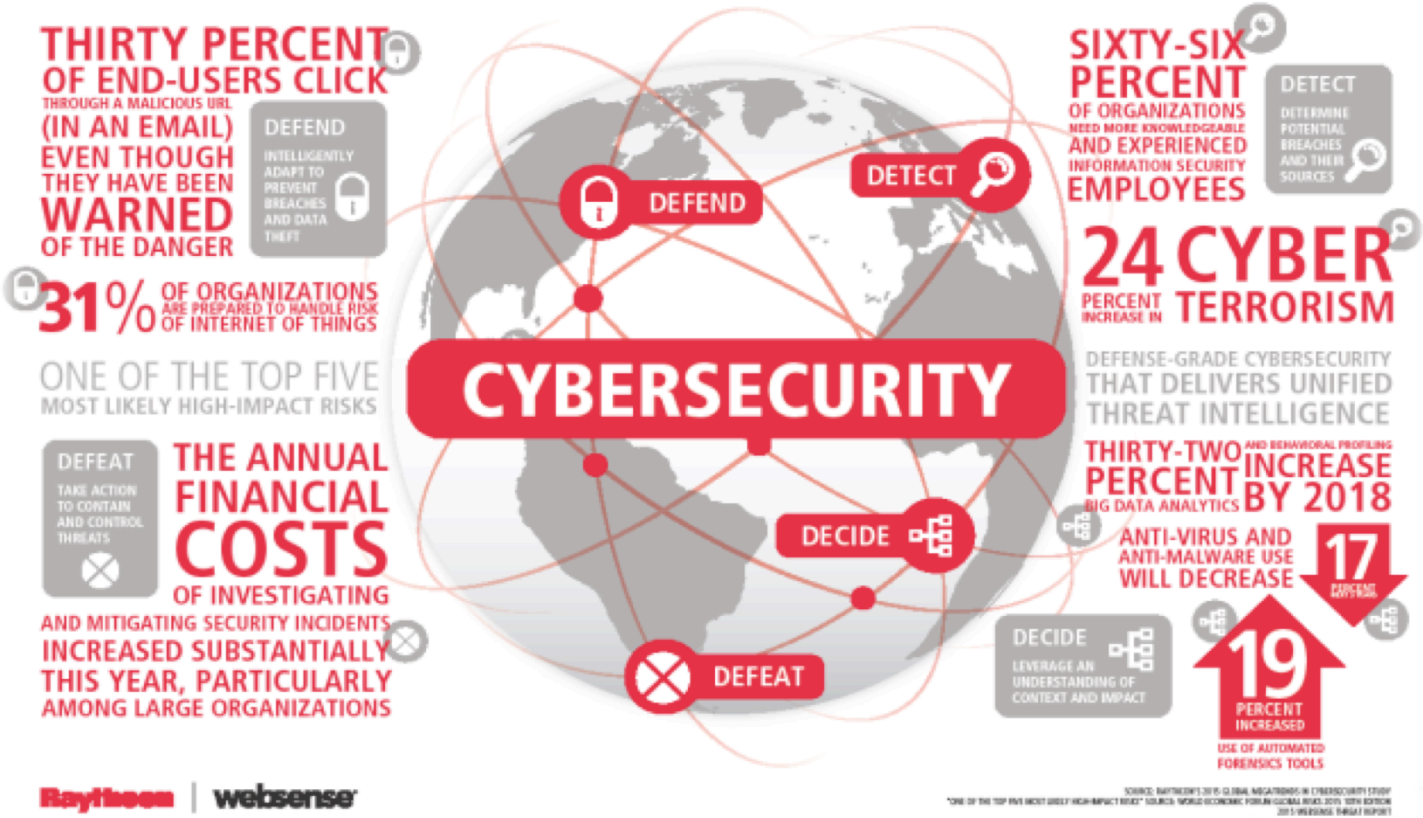
PANORAMA DE AMENAZAS EN EVOLUCION	**Amenazas internas** (accidentales o a propósito) y amenazas avanzadas hacen que las penetraciones sean inevitables

450+ empresas
En RSAC 2016

COMPLEJIDAD & FRAGMENTACION	Demasiados **productos**, demasiada **información**, **pocas personas** con los conocimientos necesarios

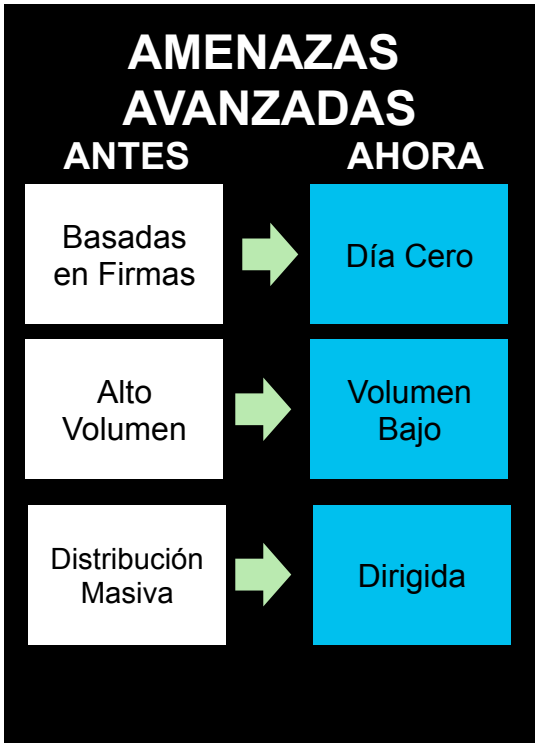
FORCEPOINT
POWERED BY Raytheon

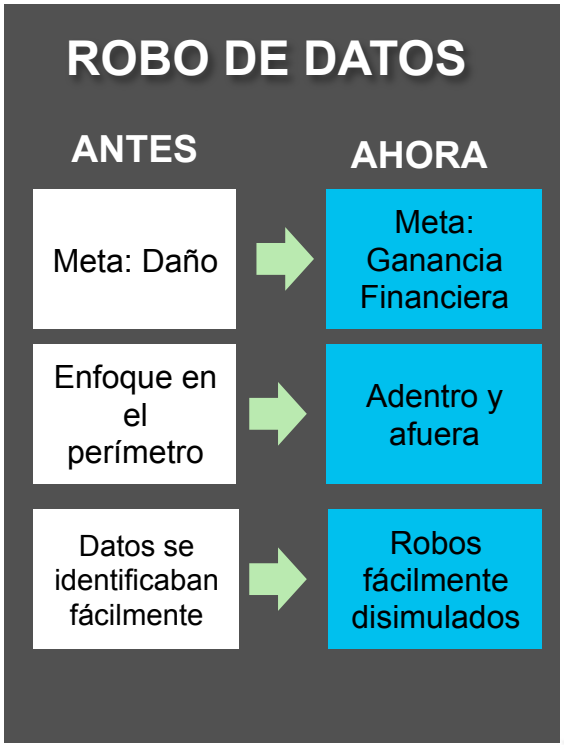
EL PROBLEMA



FORCEPOINT
POWERED BY Raytheon

HOY: DOS GRANDES PROBLEMAS DE SEGURIDAD





FORCEPOINT
POWERED BY Raytheon

LA BRECHA PARA CONSEGUIR PERSONAL CALIFICADO CRECE

2.25 millones

2017

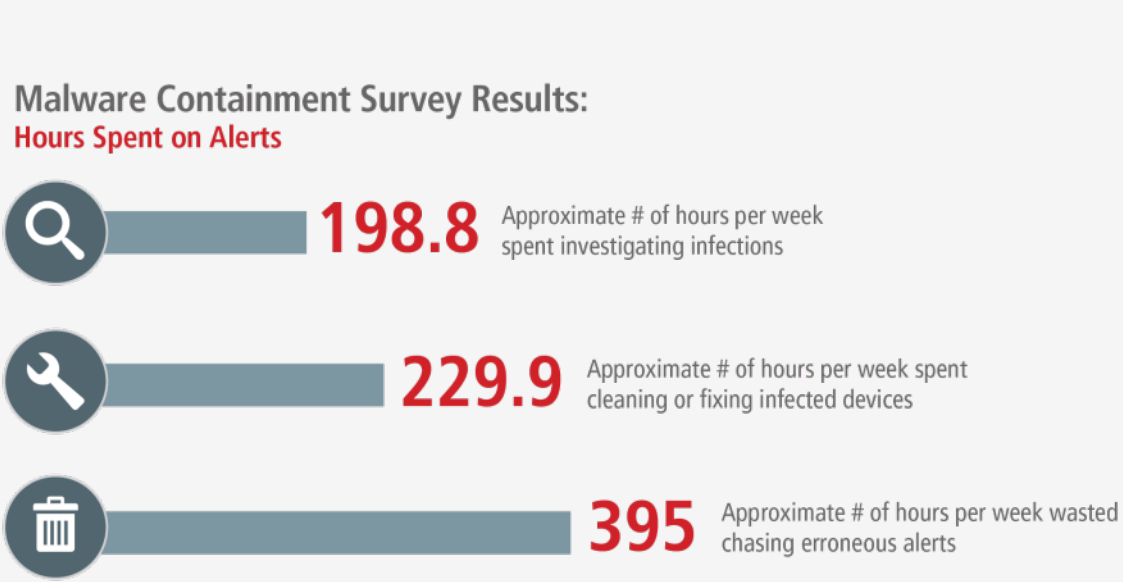
4.25 millones

La brecha de habilidades causa mas penetraciones

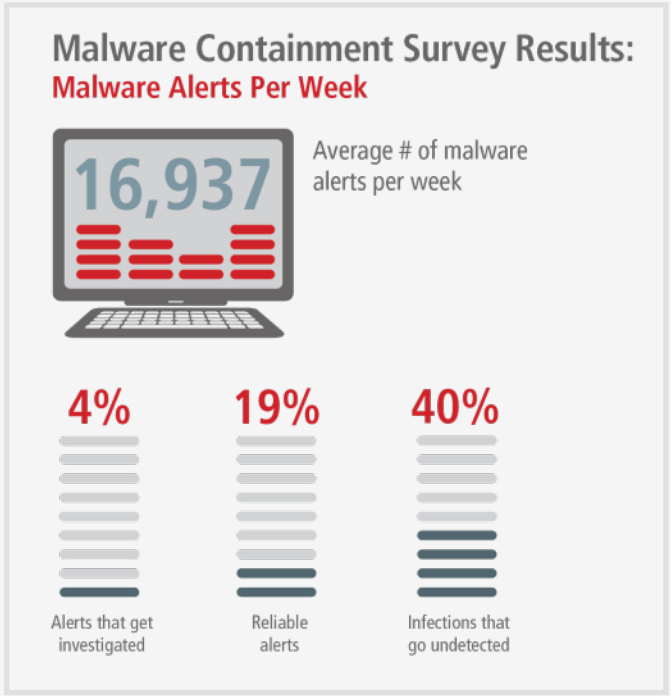
Fuente: 2013 (ISC)2 Global Information Workforce Study

= 250,000

PERSEGUIR LAS ALERTAS ES UNA ESTRATEGIA FALLIDA



Source: Ponemon Institute, 2015



FORCEPOINT
POWERED BY Raytheon

RETOS PARA RESOLVER EL PROBLEMA DE LAS AMENAZAS INTERNAS

INSIDER THREATS

88%
OF ORGANIZATIONS RECOGNIZE THAT INSIDER THREATS ARE **CAUSE FOR ALARM**

69%
DO NOT HAVE ENOUGH **CONTEXTUAL INFORMATION**

56%
OF THEIR TOOLS YIELD **TOO MANY FALSE POSITIVES**

TOO MANY RELY ON DLP AND SIEM - TRADITIONAL TOOLS FOCUSED MORE ON EXTERNAL THREATS

VISIBILITY

42%
are not confident they have enterprisewide visibility for privileged user access

16%
are very confident they have this visibility

BUDGET

88%
recognize budget as a **top priority**

Less than 40%
have a dedicated budget for insider threat

72% stated they use authentication and identity management tools to manage privileged user abuse - most use existing cybersecurity tools not designed to combat insider threat

FORCEPOINT
POWERED BY Raytheon

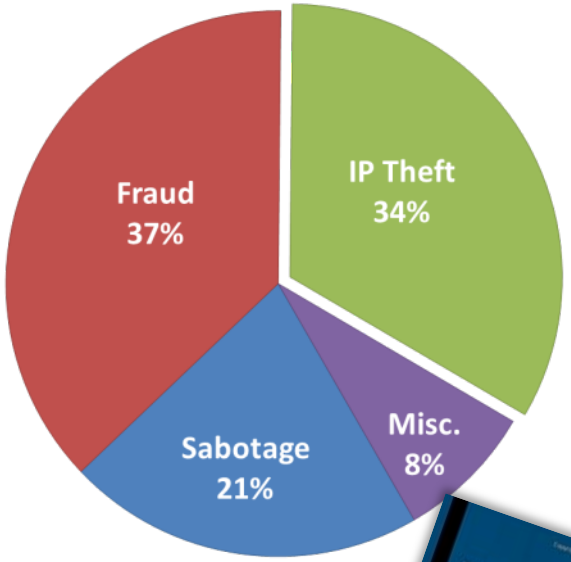
AMENAZAS INTERNAS – NO SOLAMENTE UN LADRON

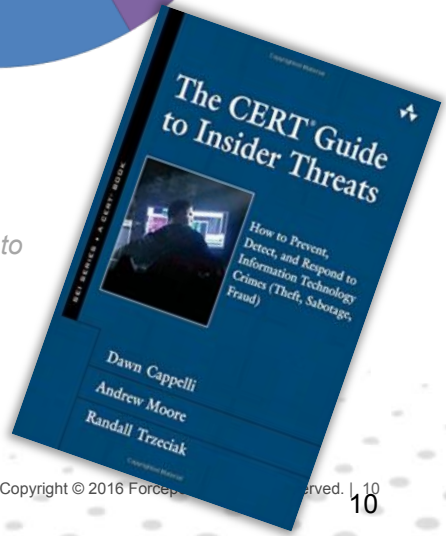
- Usuarios Autorizados
- A propósito
  - Fraude, Sabotaje y robo
- Accidental

Sistemas de IT: El testigo, la victima, o lo que facilita el problema

TIPOS DE AMENAZAS INTERNAS

- **Robo de propiedad intelectual**
- **Fraude**
- **Sabotaje** (administrador de sistemas molesto crea una backdoor antes de ser despedido y lo usa después para destruir sistemas IT)
- **Involuntario** (cuenta de usuario de un contratista usada por atacante para obtener acceso)
- **Misceláneo**
  - **Soborno Violencia** (amenazas y actos)





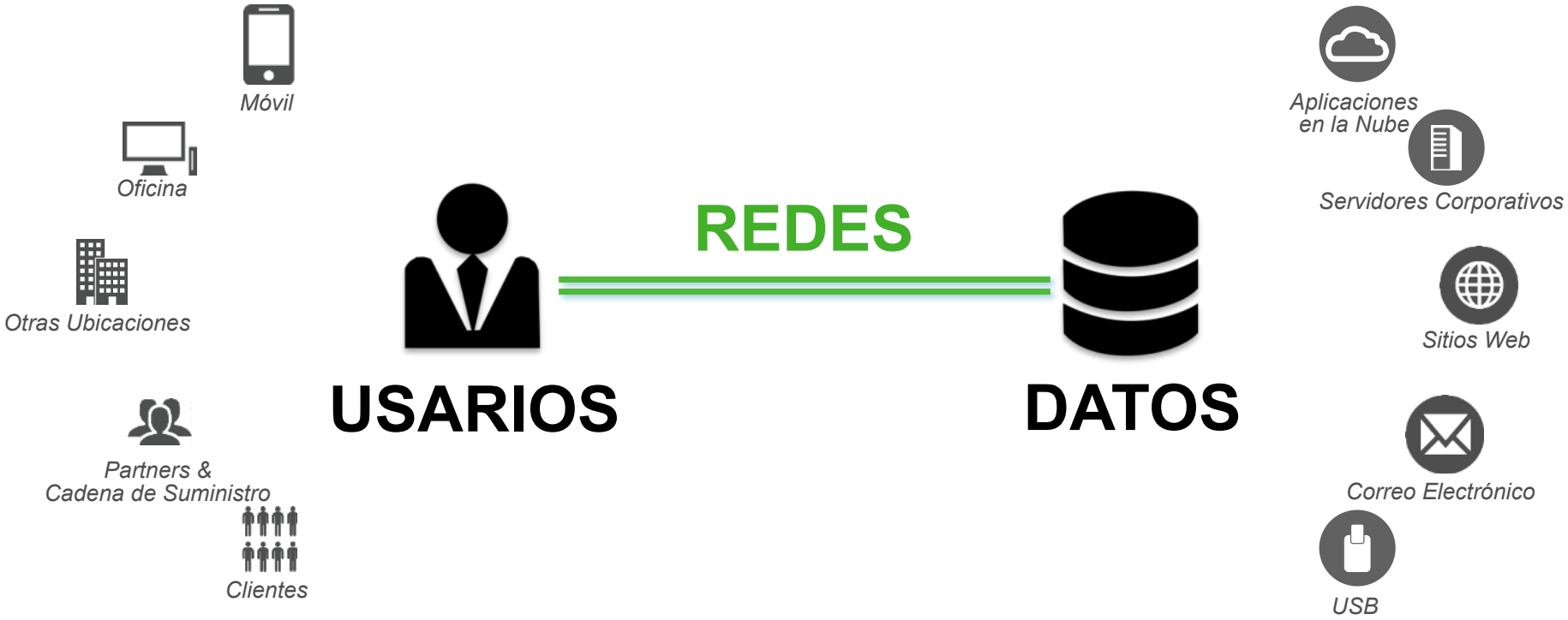
Fuente: *The CERT Guide to Insider Threats*, 2012

FORCEPOINT
POWERED BY Raytheon

Recomendación

FORCEPOINT
POWERED BY Raytheon

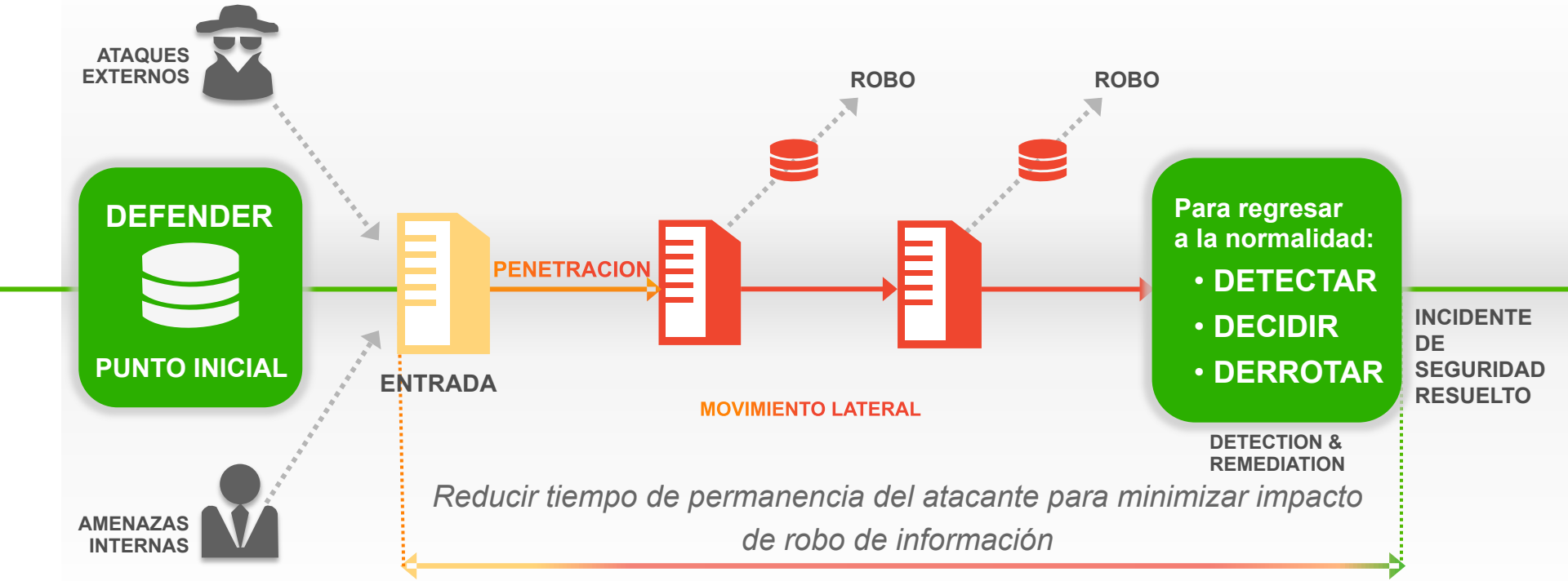
RECOMENDACIÓN: CONECTAR A LOS USUARIOS DE FORMA SEGURA A LOS DATOS ES PRIMORDIAL



EN LA NUBE, EN EL CAMINO, EN LA OFICINA

FORCEPOINT
POWERED BY Raytheon

RECOMENDACION: ENFOCARSE EN REDUCIR TIEMPO DE PERMANENCIA DEL ATACANTE

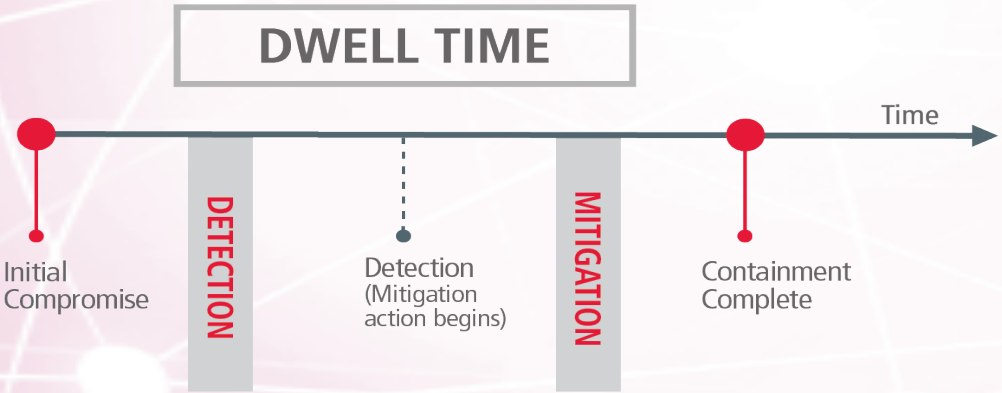


FORCEPOINT
POWERED BY Raytheon

REDUCIR TIEMPO DE PERMANENCIA

206 Days Mean time to identify a breach[1]

69 Days Mean time to contain a breach[1]

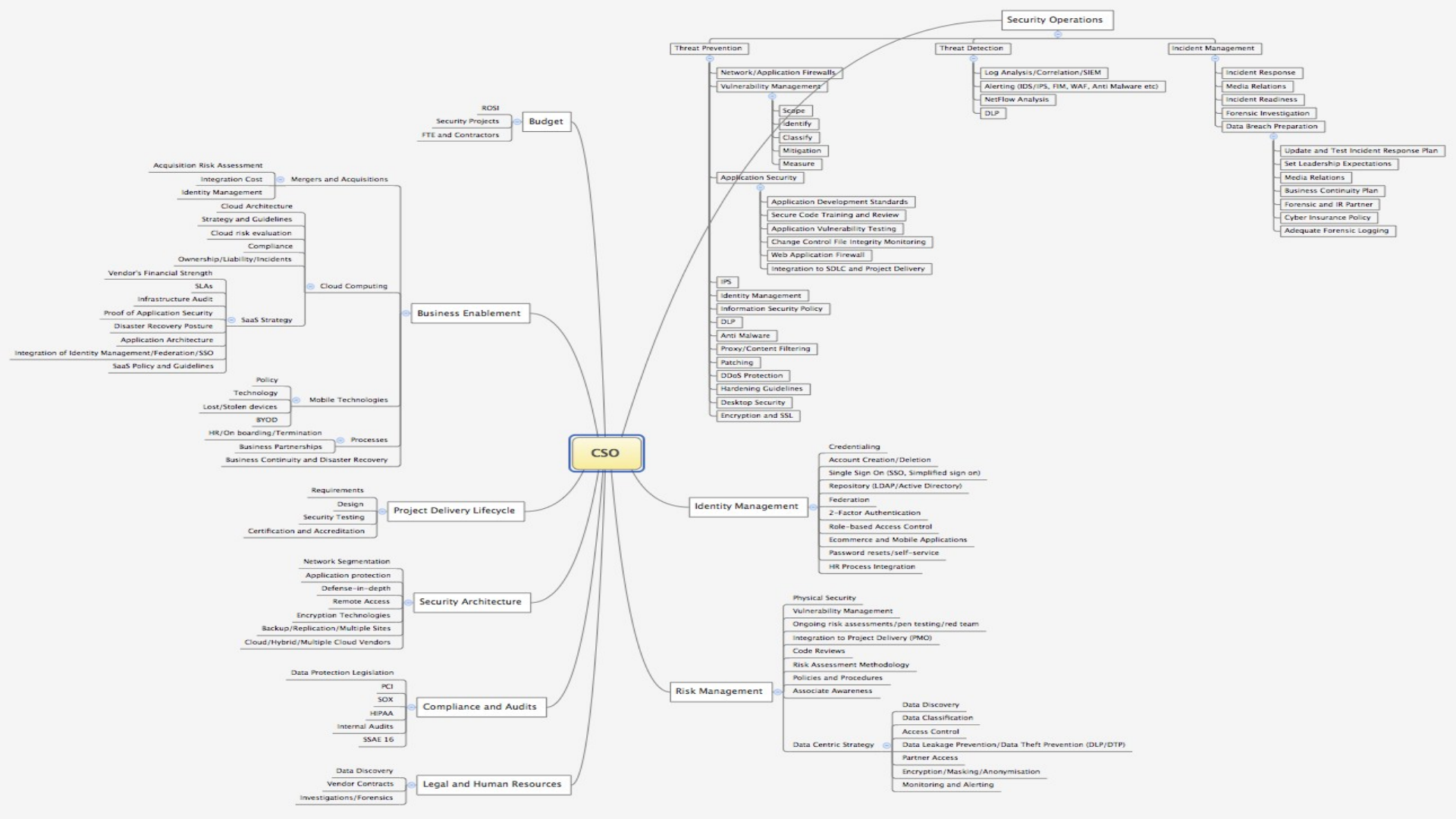


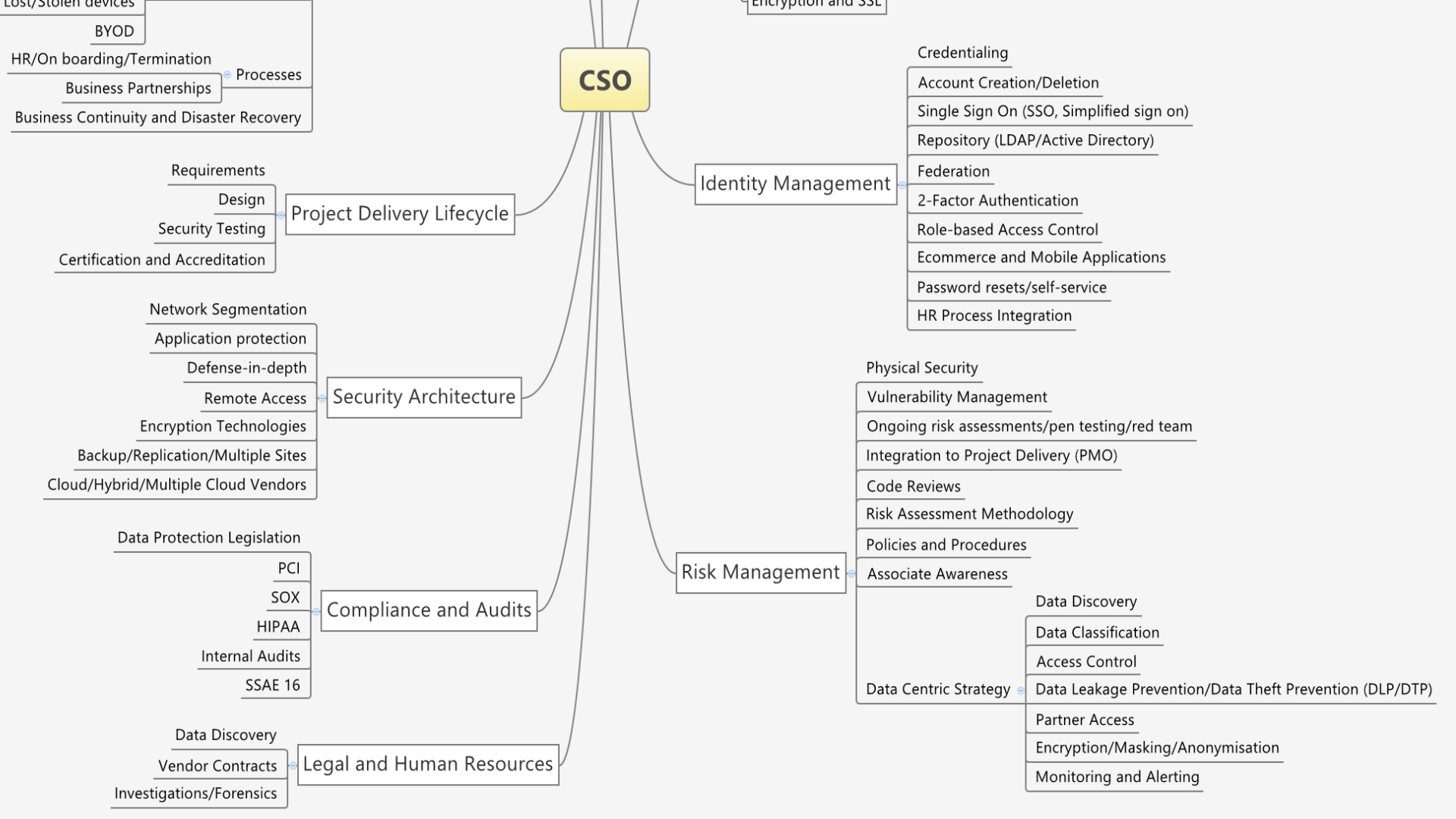
"Si el tiempo de permanencia se está reduciendo, la ciberseguridad esta mejorando"

Jeff Brown, Raytheon CISO

[1]*Cost of Data Breach Study: Global Analysis, Ponemon Institute, 2015*

FORCEPOINT
POWERED BY Raytheon


CSO
Security Operations
Threat Prevention
Network/Application Firewalls
Vulnerability Management
Scope
Identify
Classify
Mitigation
Measure
Application Security
Application Development Standards
Secure Code Training and Review
Application Vulnerability Testing
Change Control File Integrity Monitoring
Web Application Firewall
Integration to SDLC and Project Delivery
IPS
Identity Management
Information Security Policy
DLP
Anti Malware
Proxy/Content Filtering
Patching
DDoS Protection
Hardening Guidelines
Desktop Security
Encryption and SSL
Threat Detection
Log Analysis/Correlation/SIEM
Alerting (IDS/IPS, FIM, WAF, Anti Malware etc)
NetFlow Analysis
DLP
Incident Management
Incident Response
Media Relations
Incident Readiness
Forensic Investigation
Data Breach Preparation
Update and Test Incident Response Plan
Set Leadership Expectations
Media Relations
Business Continuity Plan
Forensic and IR Partner
Cyber Insurance Policy
Adequate Forensic Logging
Budget
ROSI
Security Projects
FTE and Contractors
Business Enablement
Mergers and Acquisitions
Acquisition Risk Assessment
Integration Cost
Identity Management
Cloud Computing
Cloud Architecture
Strategy and Guidelines
Cloud risk evaluation
Compliance
Ownership/Liability/Incidents
SaaS Strategy
Vendor's Financial Strength
SLAs
Infrastructure Audit
Proof of Application Security
Disaster Recovery Posture
Application Architecture
Integration of Identity Management/Federation/SSO
SaaS Policy and Guidelines
Mobile Technologies
Policy
Technology
Lost/Stolen devices
BYOD
Processes
HR/On boarding/Termination
Business Partnerships
Business Continuity and Disaster Recovery
Project Delivery Lifecycle
Requirements
Design
Security Testing
Certification and Accreditation
Security Architecture
Network Segmentation
Application protection
Defense-in-depth
Remote Access
Encryption Technologies
Backup/Replication/Multiple Sites
Cloud/Hybrid/Multiple Cloud Vendors
Compliance and Audits
Data Protection Legislation
PCI
SOX
HIPAA
Internal Audits
SSAE 16
Legal and Human Resources
Data Discovery
Vendor Contracts
Investigations/Forensics
Identity Management
Credentialing
Account Creation/Deletion
Single Sign On (SSO, Simplified sign on)
Repository (LDAP/Active Directory)
Federation
2-Factor Authentication
Role-based Access Control
Ecommerce and Mobile Applications
Password resets/self-service
HR Process Integration
Risk Management
Physical Security
Vulnerability Management
Ongoing risk assessments/pen testing/red team
Integration to Project Delivery (PMO)
Code Reviews
Risk Assessment Methodology
Policies and Procedures
Associate Awareness
Data Centric Strategy
Data Discovery
Data Classification
Access Control
Data Leakage Prevention/Data Theft Prevention (DLP/DTP)
Partner Access
Encryption/Masking/Anonymisation
Monitoring and Alerting


Encryption and SSL
Lost/Stolen devices
BYOD
HR/On boarding/Termination
Business Partnerships
Processes
Business Continuity and Disaster Recovery
CSO
Credentialing
Account Creation/Deletion
Single Sign On (SSO, Simplified sign on)
Repository (LDAP/Active Directory)
Federation
2-Factor Authentication
Role-based Access Control
Ecommerce and Mobile Applications
Password resets/self-service
HR Process Integration
Identity Management
Requirements
Design
Security Testing
Certification and Accreditation
Project Delivery Lifecycle
Network Segmentation
Application protection
Defense-in-depth
Remote Access
Encryption Technologies
Backup/Replication/Multiple Sites
Cloud/Hybrid/Multiple Cloud Vendors
Security Architecture
Physical Security
Vulnerability Management
Ongoing risk assessments/pen testing/red team
Integration to Project Delivery (PMO)
Code Reviews
Risk Assessment Methodology
Policies and Procedures
Associate Awareness
Data Centric Strategy
Data Discovery
Data Classification
Access Control
Data Leakage Prevention/Data Theft Prevention (DLP/DTP)
Partner Access
Encryption/Masking/Anonymisation
Monitoring and Alerting
Risk Management
Data Protection Legislation
PCI
SOX
HIPAA
Internal Audits
SSAE 16
Compliance and Audits
Data Discovery
Vendor Contracts
Investigations/Forensics
Legal and Human Resources

¿DE QUÉ TE ESTAS PROTEGIENDO?

FORCEPOINT
POWERED BY Raytheon

UN FALSO SENTIDO DE SEGURIDAD…

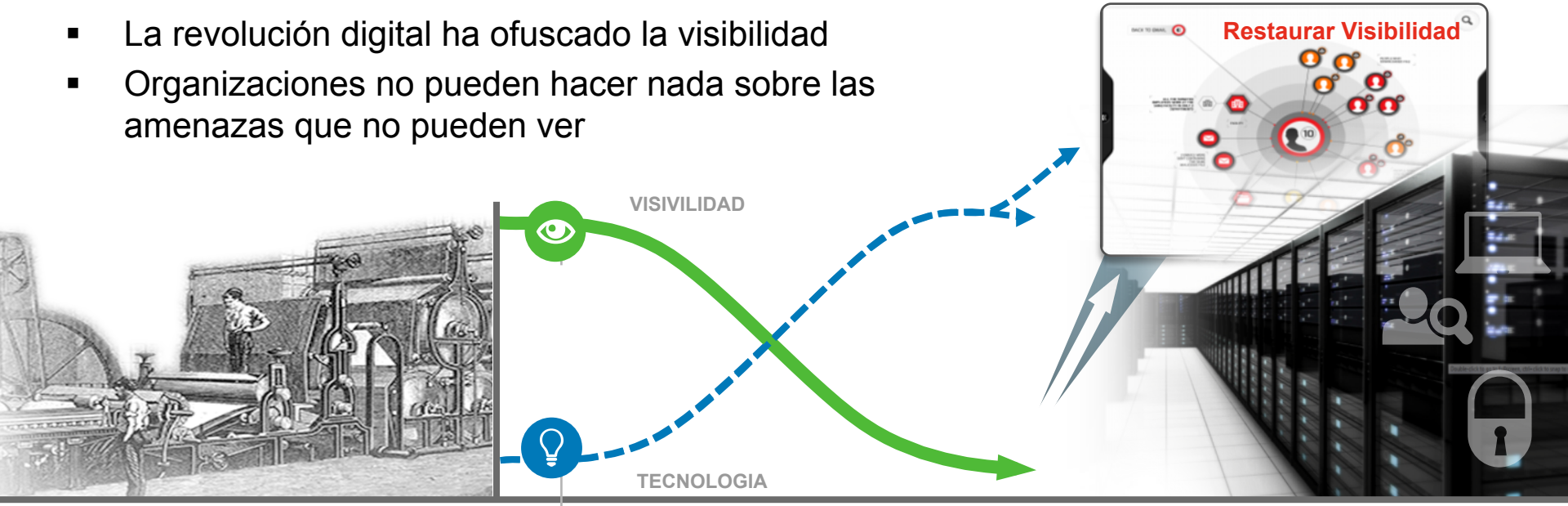
COMO ABORDAR EL PROBLEMA

Visibilidad + Contexto + Programa Formal

Photo: Jeramey Jannene

VISIBILIDAD ES PRIMORDIAL

- La revolución digital ha ofuscado la visibilidad
- Organizaciones no pueden hacer nada sobre las amenazas que no pueden ver



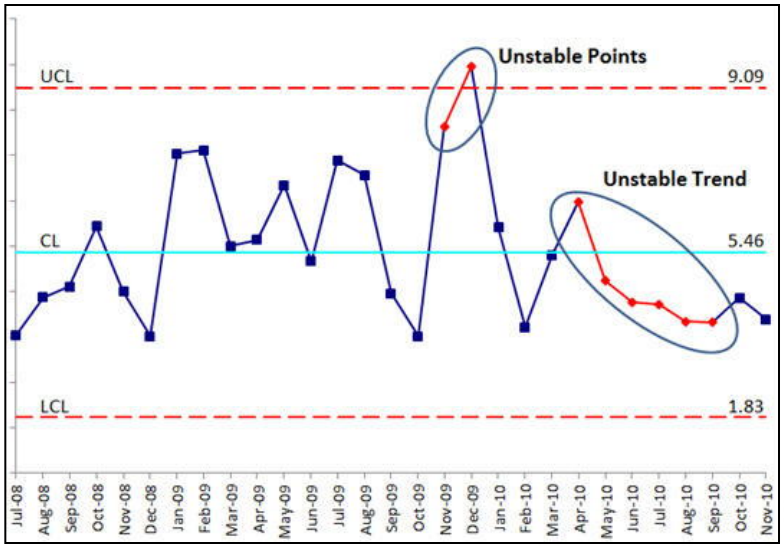
Necesidad de **tecnología** que recauda y analiza las actividades de los usuarios, **restaurando la visibilidad sobre acciones** que puedan tener riesgo

FORCEPOINT
POWERED BY Raytheon

CONSEJOS PARA SELECCIONAR HERRAMIENTA ADEQUADA

1. Visibilidad y correlacionar las fuentes de información necesarias
2. Que pueda definir ”comportamiento base” estadísticamente y detectar cambios anormales
3. Guardar un histórico

Seleccionar herramienta que funciona para las necesidades de la organización



FORCEPOINT
POWERED BY Raytheon

GRACIAS

Roberto Cruz
rcruz@forcepoint.com

FORCEPOINT
POWERED BY Raytheon

