Ataques Cibernéticos y Cuentas Privilegiadas

- George Alvarez SE Regional Director LATAM & Carribean
- George.Alvarez@Cyberark.com

El nuevo campo de batalla cibernético: La red interna

Más del 90% de las organizaciones han sido atacadas

- En el pasado: “Puedo detener todo en el perímetro”
- Ahora: “No puedo detener todo en el perímetro”

El foco de seguridad de la información cambia hacia el interior de la red

- Más del 45% de los ataques son internos – dirigidos maliciosamente o accidentalmente
- Credenciales comprometidas aumentan las posibilidades de un atacante para actuar como interno

Requerimientos de auditoria y cumplimiento se centran en cuentas privilegiadas

- Las cuentas privilegiadas otorgan acceso a los activos más sensibles e importantes
- La exposición de información daña la reputación y confianza de los clientes.

CYBERARK

Los hechos hablan por si mismos:

No existe la seguridad perfecta.

Los atacantes se vuelven más inteligentes y cambian sus tácticas todo el tiempo

100%

De las victimas tienen antivirus actualizado

94%

De los ataques son reportados por terceras partes

416

El número de días que los atacantes permanecen en la red antes de ser detectados

100%

De los ataques involucran robo de credenciales.

Mandiant, 2017

CYBERARK

Las defensas perimetrales no son suficientes

Former FBI Director Robert Mueller

"Hay solo 2 tipos de compañias: Aquellas que han sido atacadas y aquellas que serán atacadas. Incluso estan convergiendo en una sola categories': Aquellas que han sido atacadas y volverán a ser atacadas."

"FBI Director: Cybercrime Will Eclipse Terrorism" CNN Money

CYBERARK

CYBERARK

Gartner Top 10 Security

Secure | gartner.com/smarterwithgartner/gartner-top-10-security-projects-for-2018/

Apps | CyberArk bookmarks | Audiogon | ★ 6 in 1 ★ Multifunc | Login : New Audio & | B&W Group North A | B&W Group North A | Dailymoilegear™ 10 | My eBay | Houses | Other bookmarks

Smarter With Gartner

What are you looking for?

Gartner Top 10 Security Projects for 2018

June 6, 2018
Contributor: Jill Beadle

SECURITY

CISOs should focus on these ten security projects to reduce risk and

Related

Gartner Top 10 Security

Secure | gartner.com/smarterwithgartner/gartner-top-10-security-projects-for-2018/

Apps | CyberArk bookmarks | Audiogon | ★ 6 in 1 ★ Multifunc | Login : New Audio & | B&W Group North A | B&W Group North A | Dailymoilegear™ 10 | My eBay | Houses | Other bookmarks

Smarter With Gartner

What are you looking for?

Neil MacDonald, Gartner vice president and distinguished analyst, explains the Gartner top 10 security projects for CISOs to focus at the Gartner Security and Risk Management Summit 2018.

No. 1: Privileged account management

This project is intended to make it harder for attackers to access privileged accounts and should allow security teams to monitor behaviors for unusual access. At a minimum, CISOs

2018

Top Trends in the Gartner Hype Cycle for Emerging Technologies, 2017

Gartner Predicts a Virtual World of Exponential Change

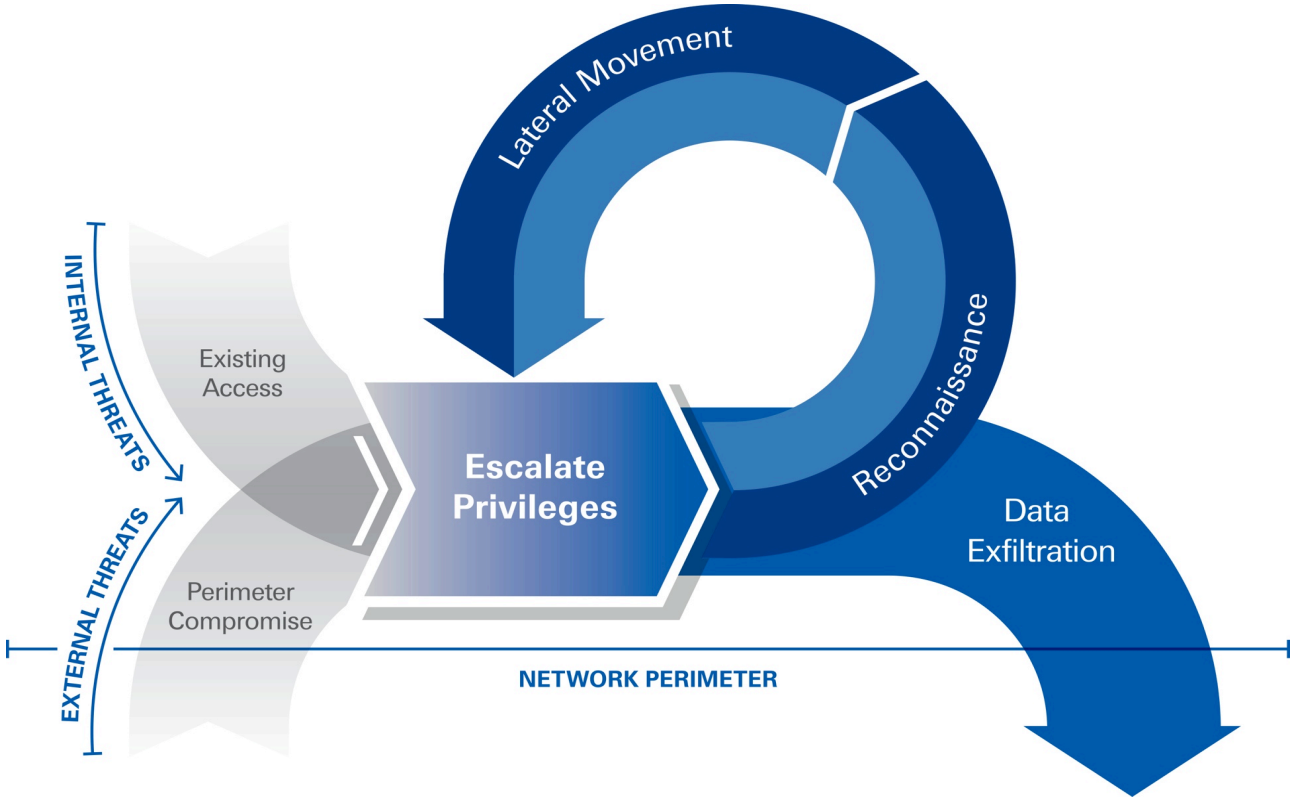
3 Trends Appear in the Gartner Hype Cycle for Emerging Technologies, 2016

8:58 AM
7/26/2018

CYBERARK

Morfología de los ataques cibernéticos

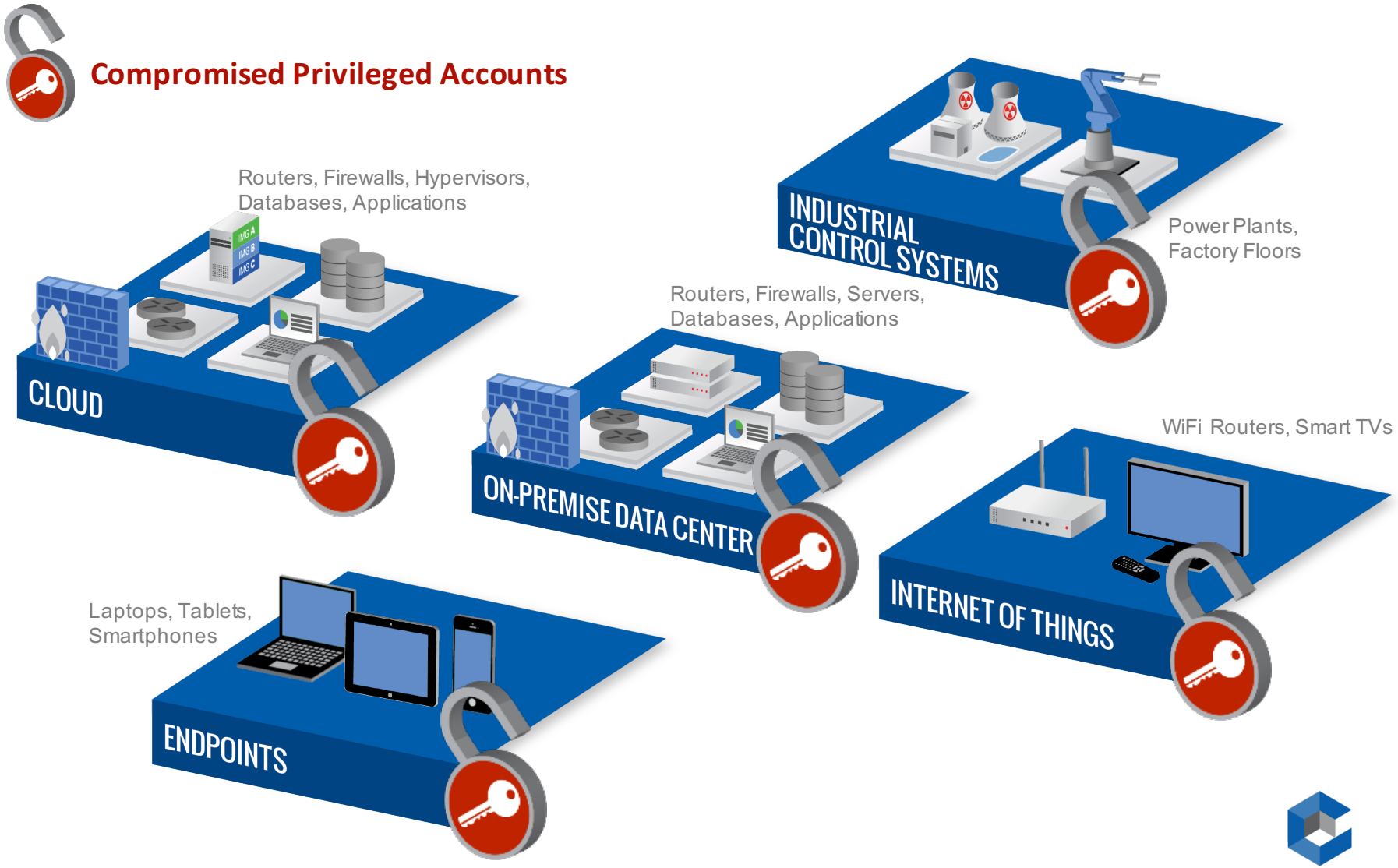
Los privilegios están en el centro del ciclo de vida de los ataques



CYBERARK

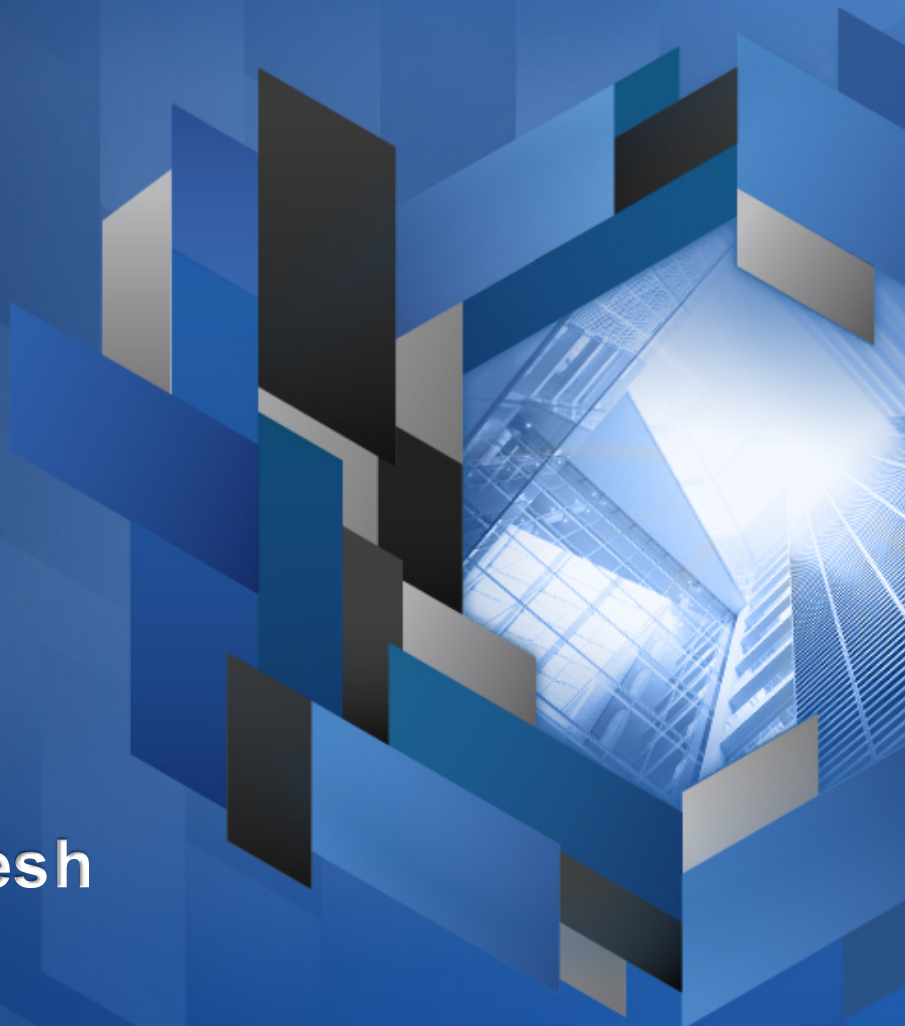
Las cuentas privilegiadas existen en todas partes…

Credenciales robadas o mal utilizadas ponen a la infraestructura de IT en riesgo…



CYBERARK

CYBERARK



Robo a Banco Central de Bangladesh

Criminales robaron $81 millones de USD del banco central de Bangladesh

BREACH OVERVIEW	
Objectivo	Bangladesh Central Bank
Atacante	Unknown
Motivación	Monetaria
Resultado	$81M robados y no recuperados

May 15, 2015:
Tres cuentas bancarias se abrieron en RCBC

January 29:
SysMon fue instalado en sistemas SWIFT-conectados

February 5 (AM):
Las impresoras del banco cayeron

Mid-January 2016:
Atacantes irrumpieron el perímetro

February 4:
Atacantes robaron credenciales de usuarios de SWIFT

February 5 (PM):
Se enviaron transacciones fraudulentas

The big Bangladesh Bank heist: How hackers managed to steal $81 million

Posted on: 11:24 AM IST Mar 17, 2016

IBNLIVE.COM

Bangladesh bank governor Atiur Rahman and two of the deputy governors have lost their jobs over the $81 million cyber heist that sent shockwaves through the banking world.

Now that more details are emerging it is becoming clearer how hackers managed to carry out one of the largest known bank thefts in history.

More details are emerging about how hackers managed to carry out one of the largest known bank thefts in history.

CYBERARK

Impacto

$81 millones de USD robados y no recuperados

Millones de USD lavados a través de casinos

El gobernador del banco central **renunció**

Investigador perdido por seis días

CYBERARK

Antecedente: Qué es SWIFT?

Society for Worldwide Interbank Financial Telecommunications

Miembro de propiedad cooperativo que permite a bancos centrales enviar y recibir de forma segura las transacciones monetarias

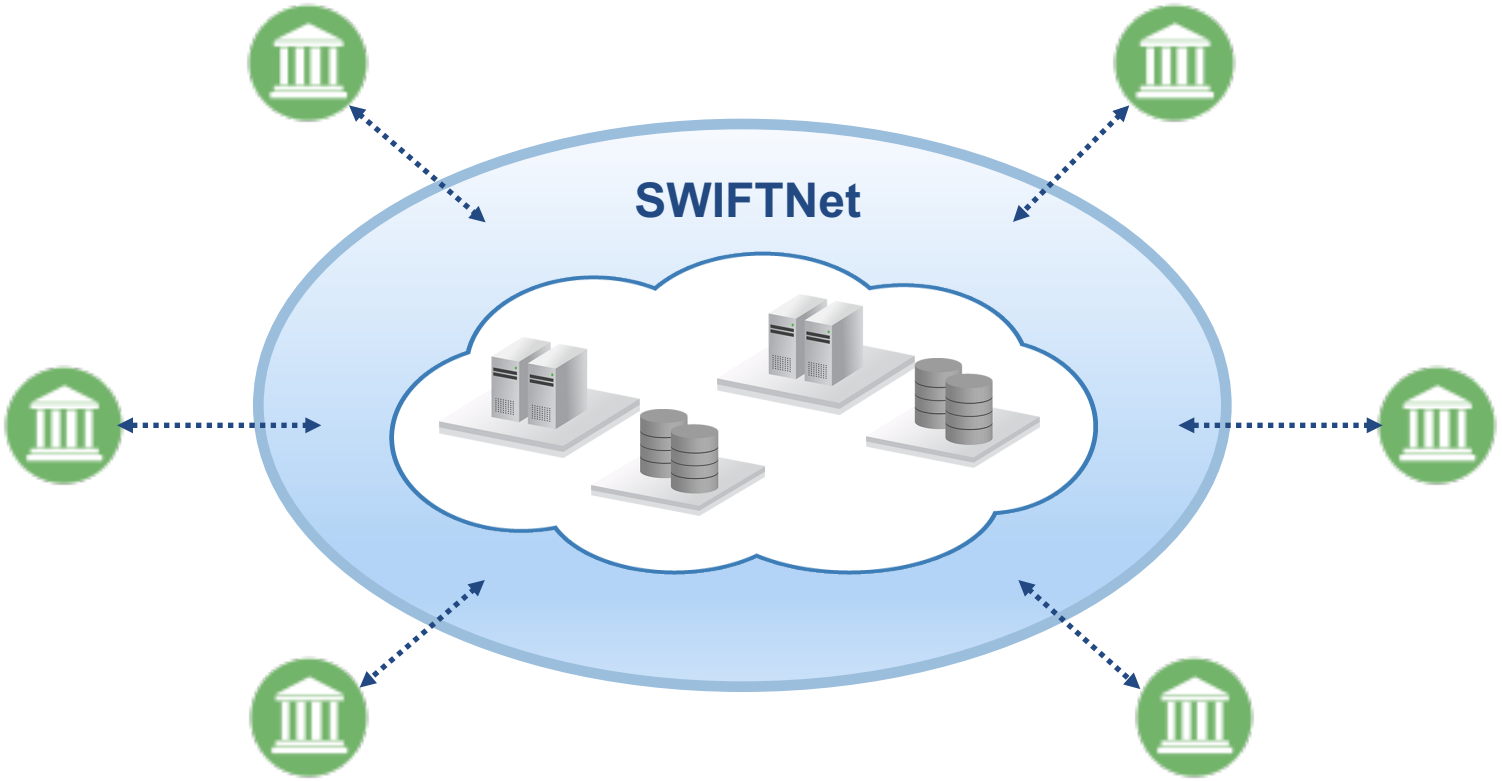
6.1+ billion
FIN messages

99.999%
SWIFTNet availability

99.999%
FIN availability

11,000+
Institutions connected to SWIFT

200+
Countries & territories connected



SWIFT: Construido por seguridad

Pero solo tan fuerte como sus usuarios lo sean

1. Usuarios autorizados reciben certificado digital

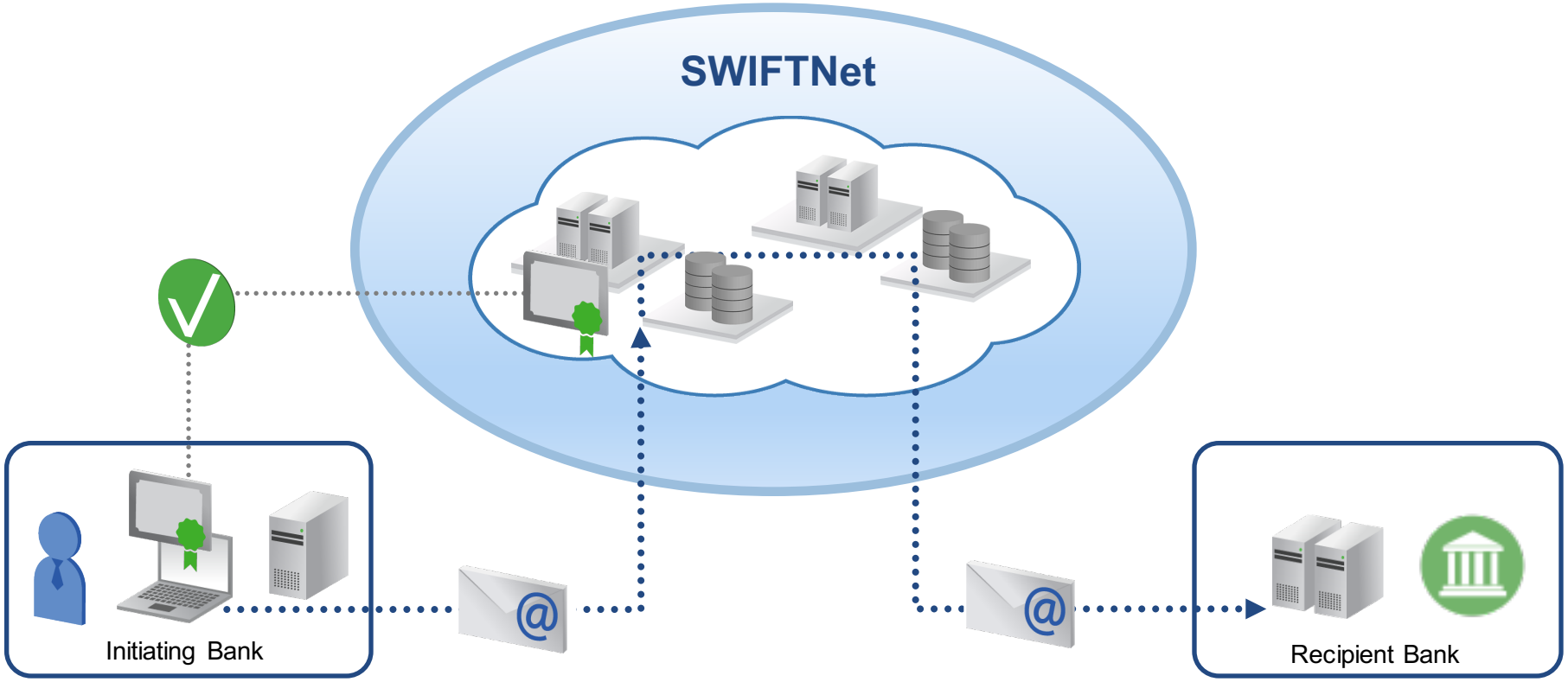
ACCESS CONTROL

2. SWIFT valida los certificados antes de enviar algún mensaje

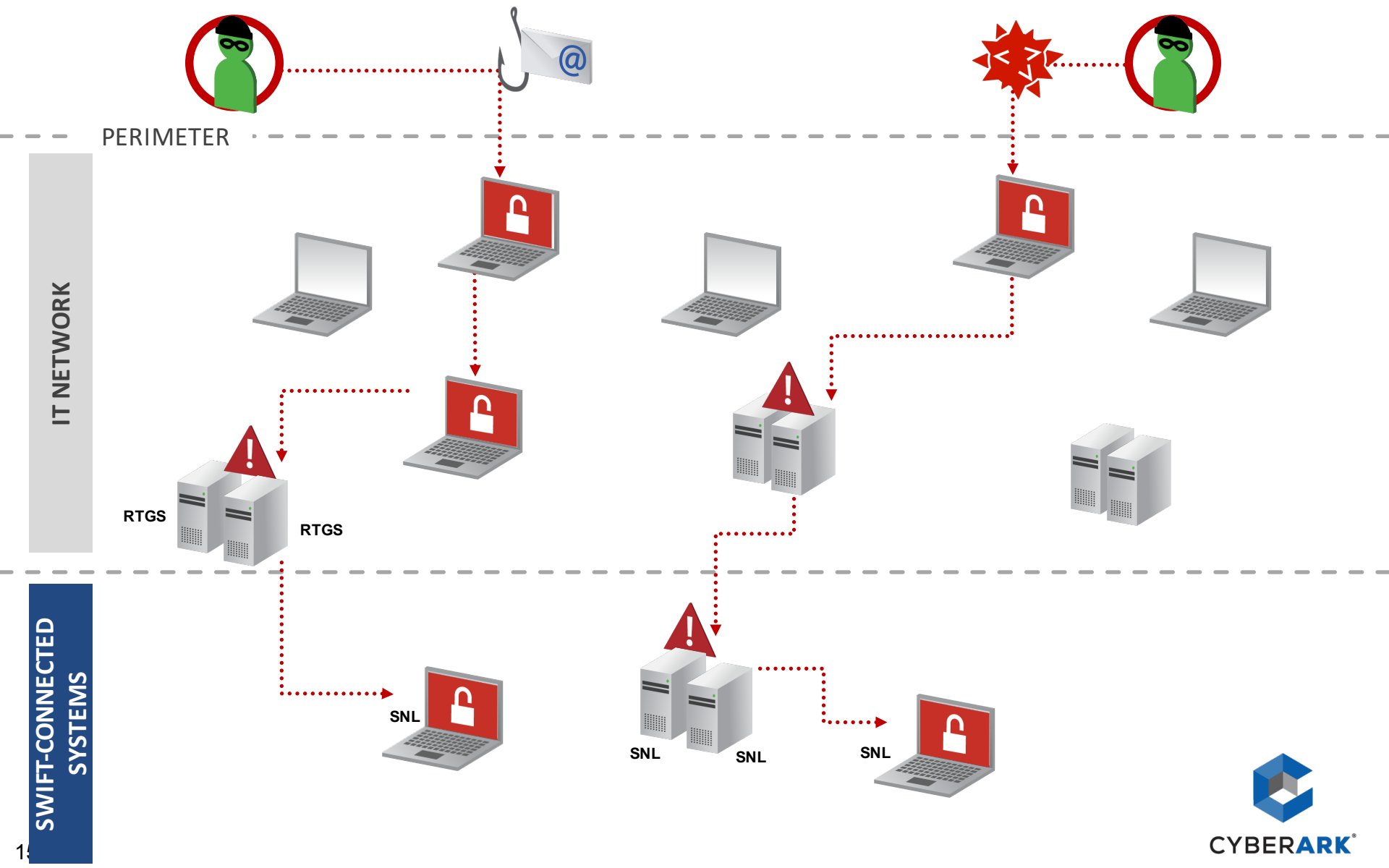
AUTHENTICATION

3. Una vez validados, los mensajes son enviados de forma segura a los destinatarios

ENCRYPTION

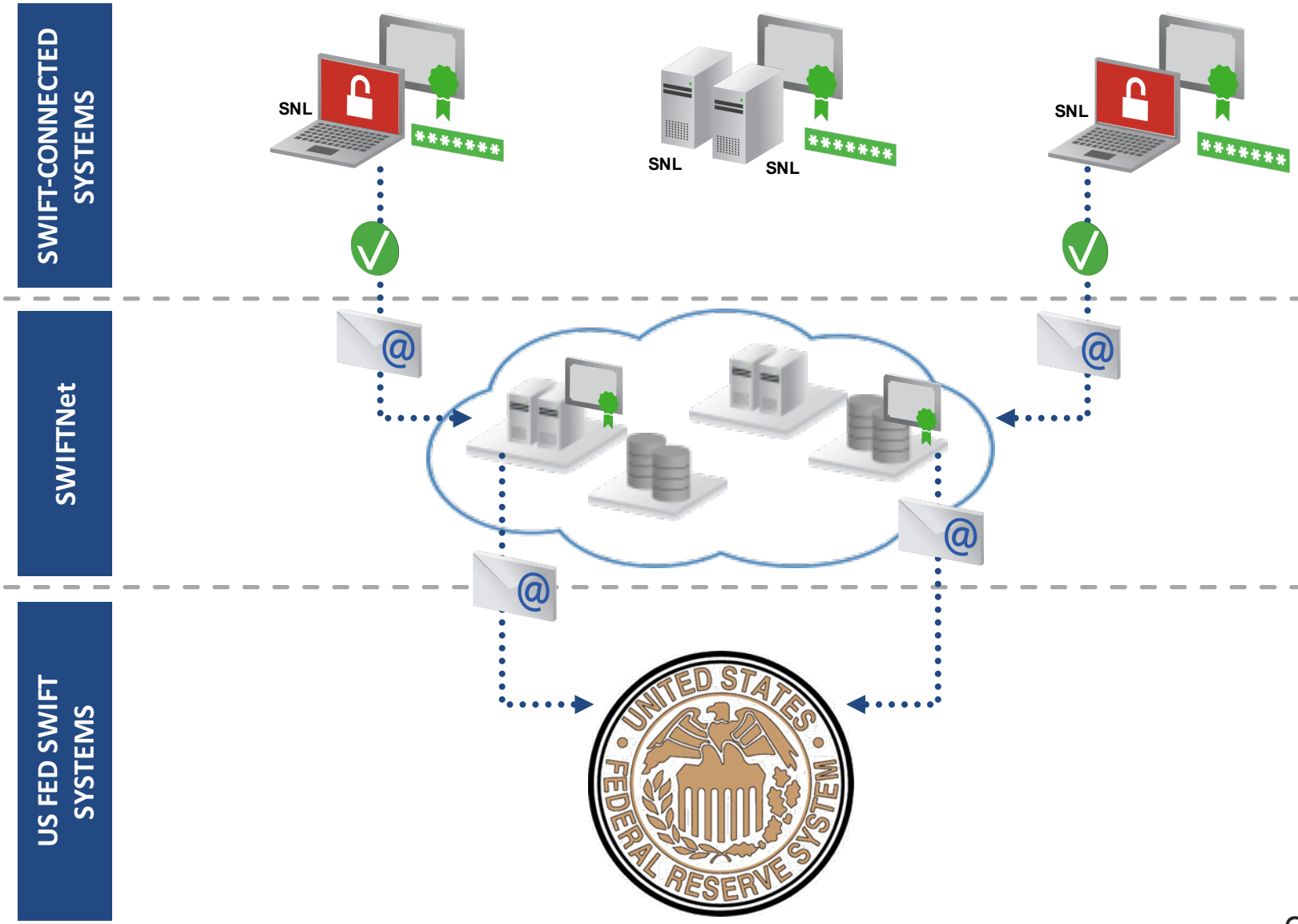


El camino hacia SWIFTNet inicia en el perimetro



CYBERARK

Privileged exploits enable a cyber bank robbery



CYBERARK

El daño pudo haber sido mucho peor

35 ORDENES CON VALOR DE $951 MILLONES FUERON ENVIADAS

5 ORDINES CON VALOR DE $101 MILLONES FUERON EJECUTADAS POR NY FED

$20 millones se transfirieron a Pan Asia Banking Company

- $20 millones hacia “Shalika **Fandation**” fueron detenidos

$81 millones transferidos a RCBC en Filipinas

- $29 millones a una compañia de entreteniemiento
- $31 millones entregados a un huesped de un hotel
- $21 millones enviados a un casino

30 ORDENES CON VALOR DE $850 MILLONES FUERON BLOQUEADAS POR FALTA DE DATOS

CYBERARK

SWIFT CSP program

SWIFT's reaction : **Customer Security Program** (CSP)

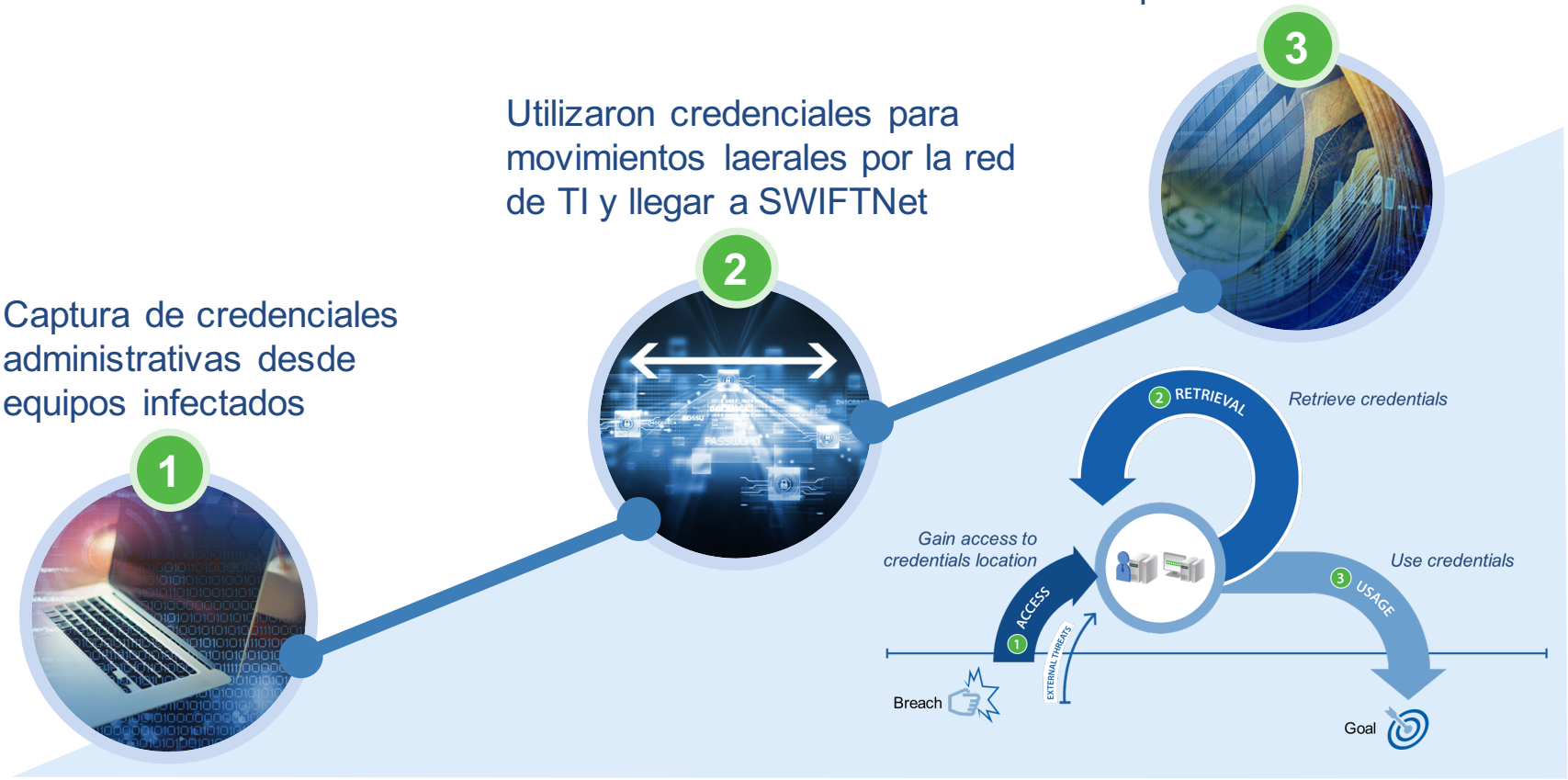
- Takes effect in the **second quarter of 2017**,
- SWIFT's customers will have to attest to complying with 16 mandatory controls.
- In **January 2018**, SWIFT will start **sharing information on non-compliance**
- **Privilege Account Security** takes a large part of the 16 controls

El papel de los privilegios en este ataque

Utilizadas para ejecutar 35 operaciones financieras y para cubrir rastros

Utilizaron credenciales para movimientos laerales por la red de TI y llegar a SWIFTNet

Captura de credenciales administrativas desde equipos infectados

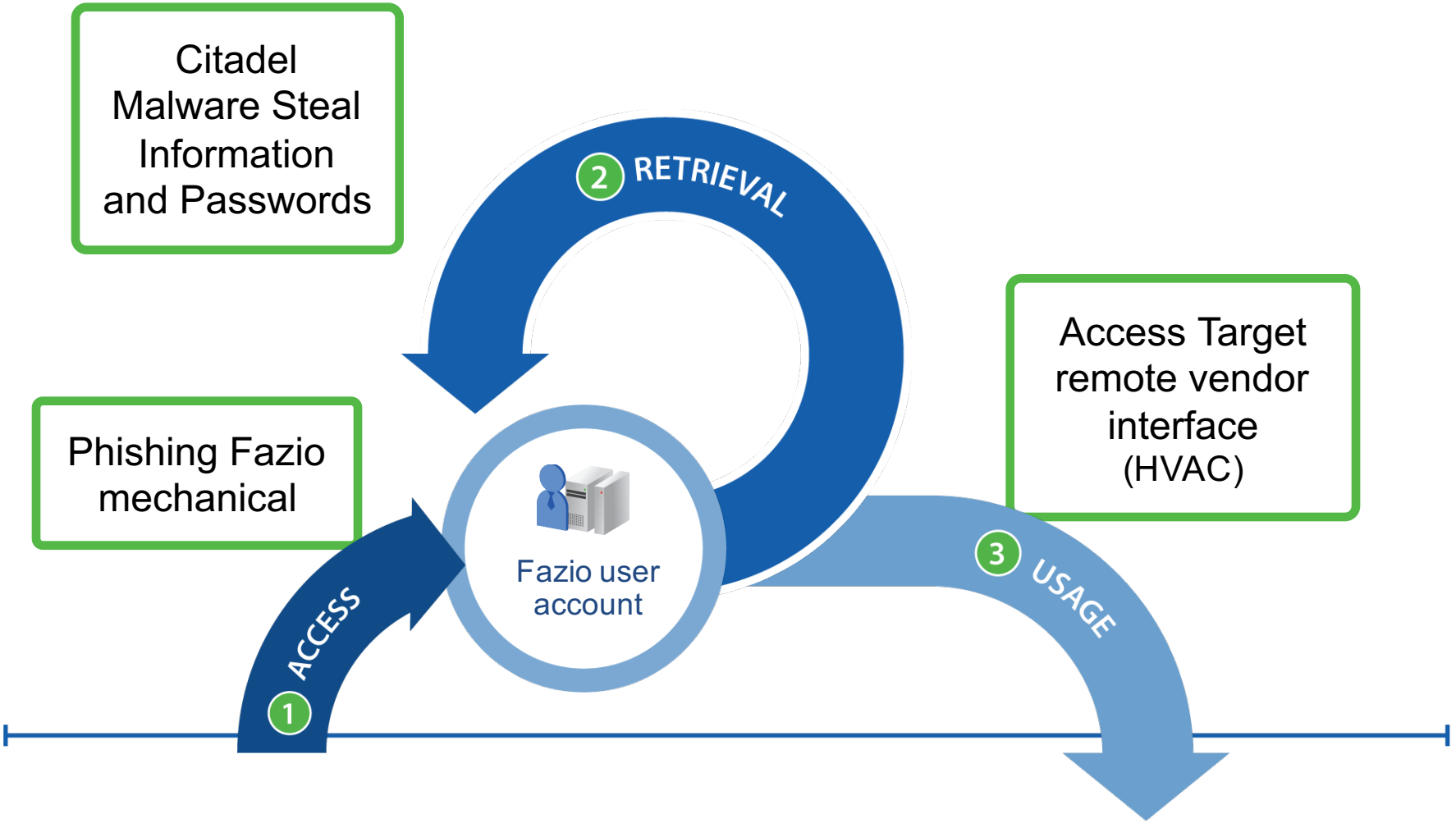


CYBERARK

CYBERARK

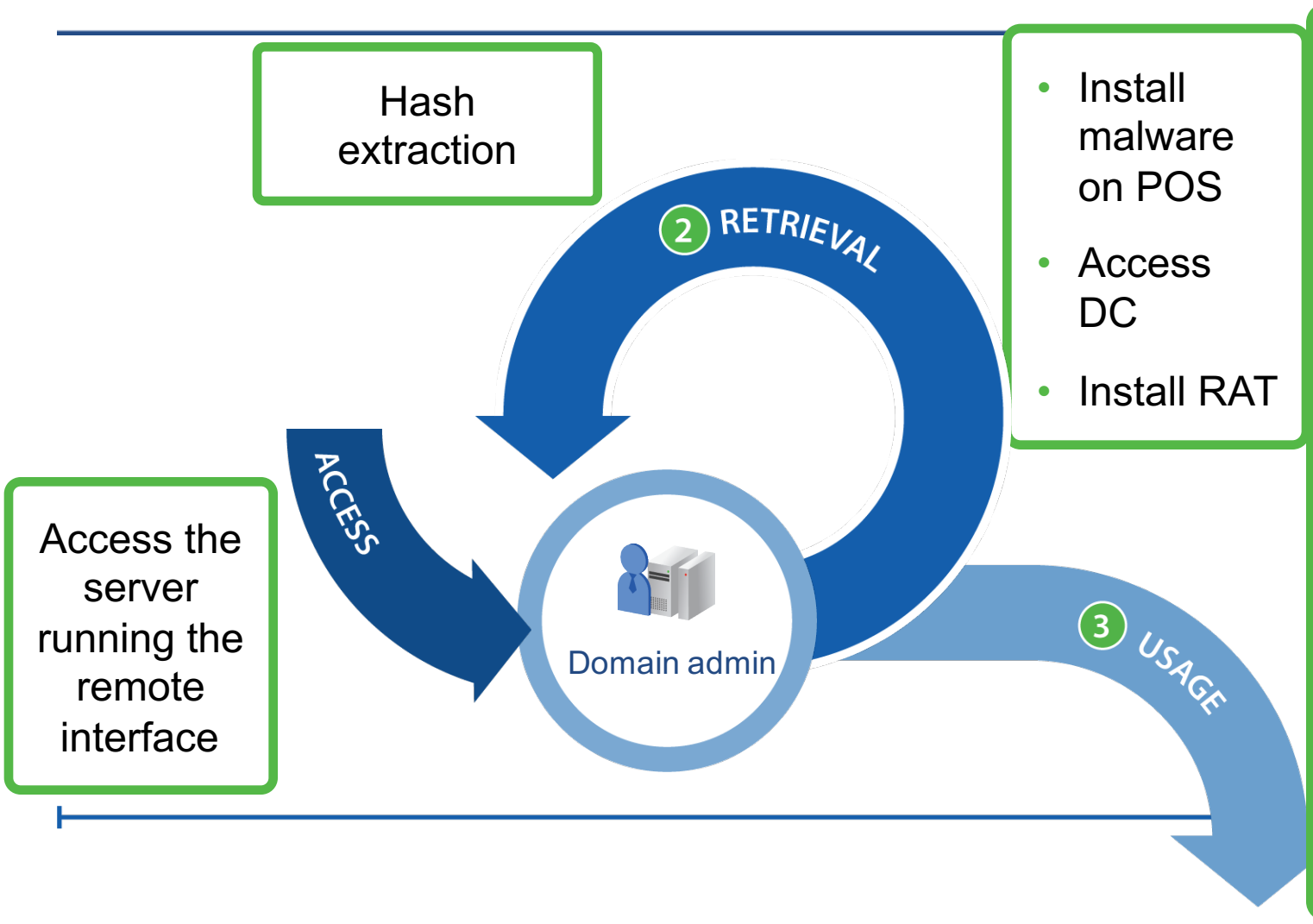
El Robo y la Brecha de Target

La Brecha de Target



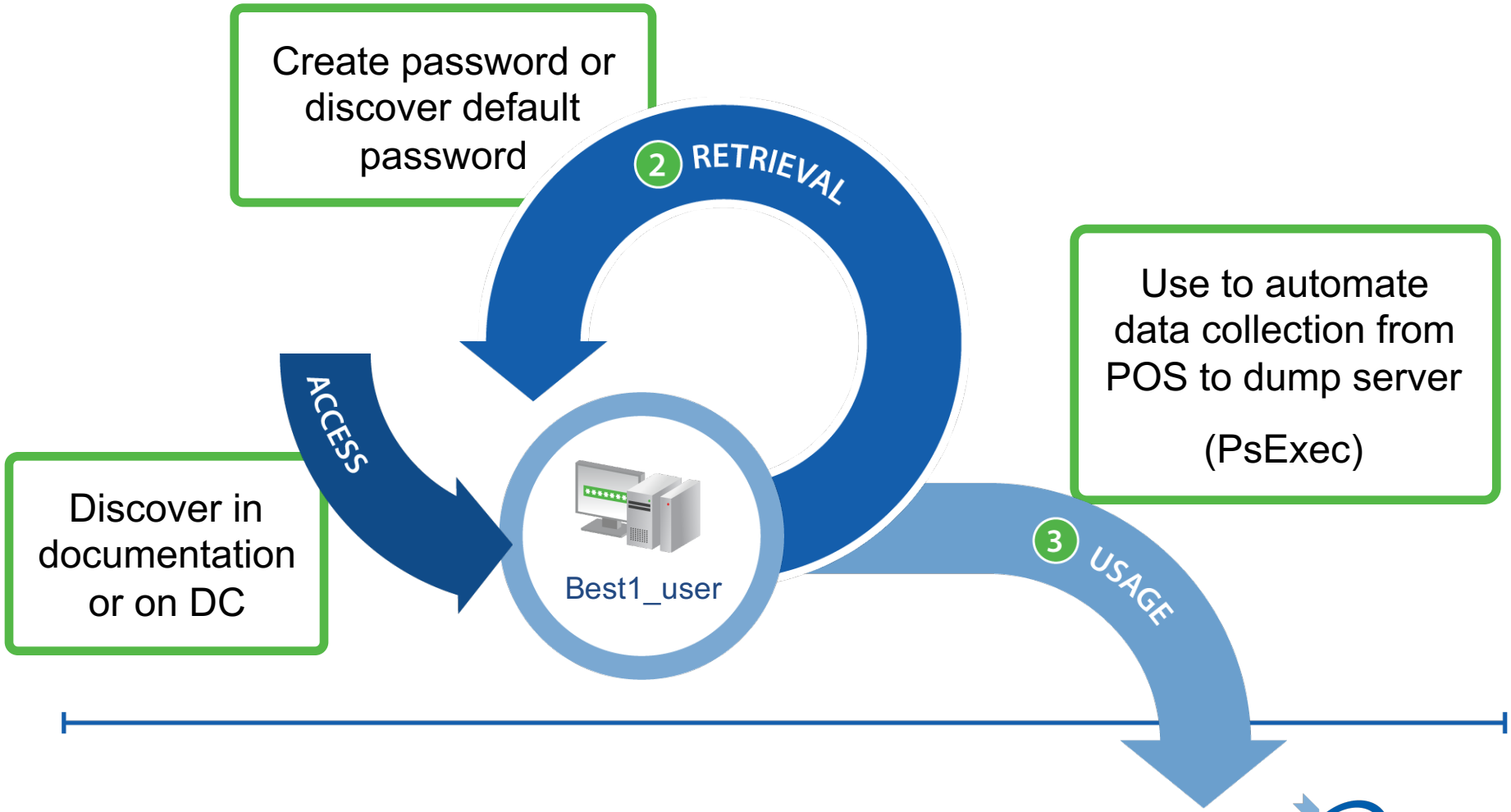
CYBERARK

La Brecha de Target



CYBERARK

La Brecha de Target

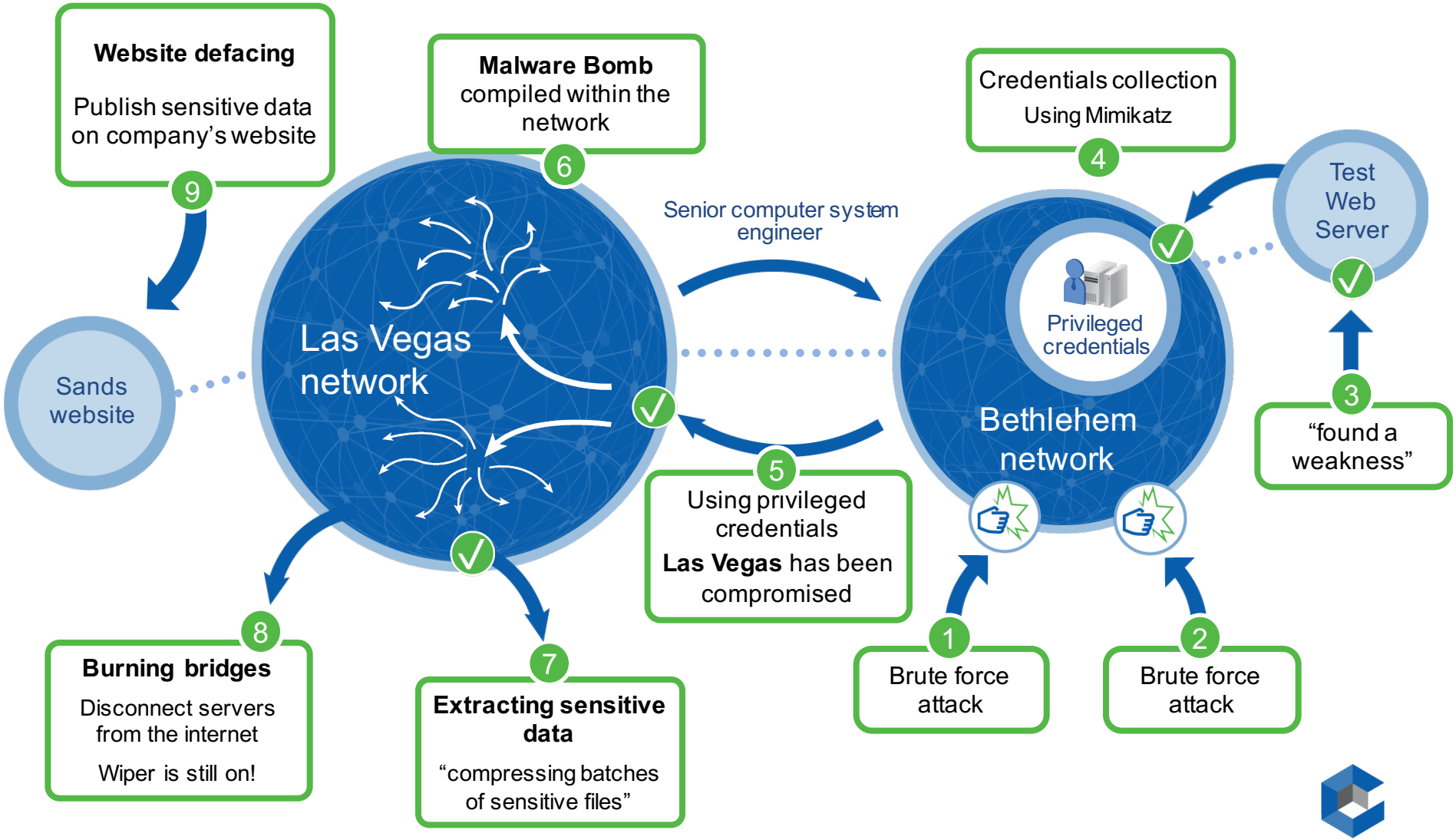


CYBERARK

CYBERARK

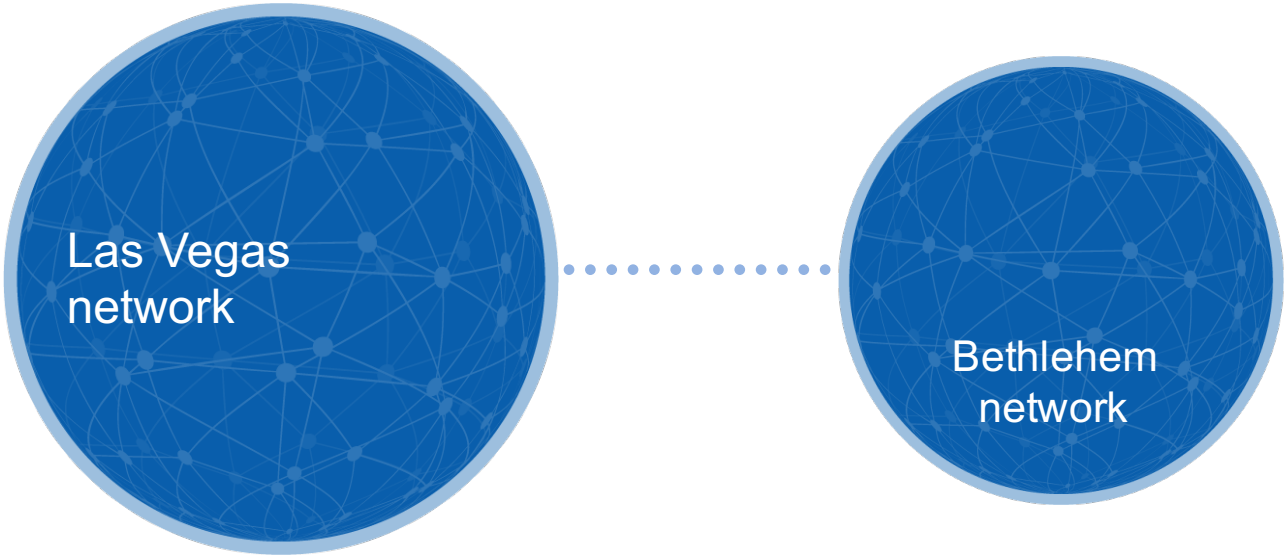
El Ataque del Casino Sands

El Ataque de Sands



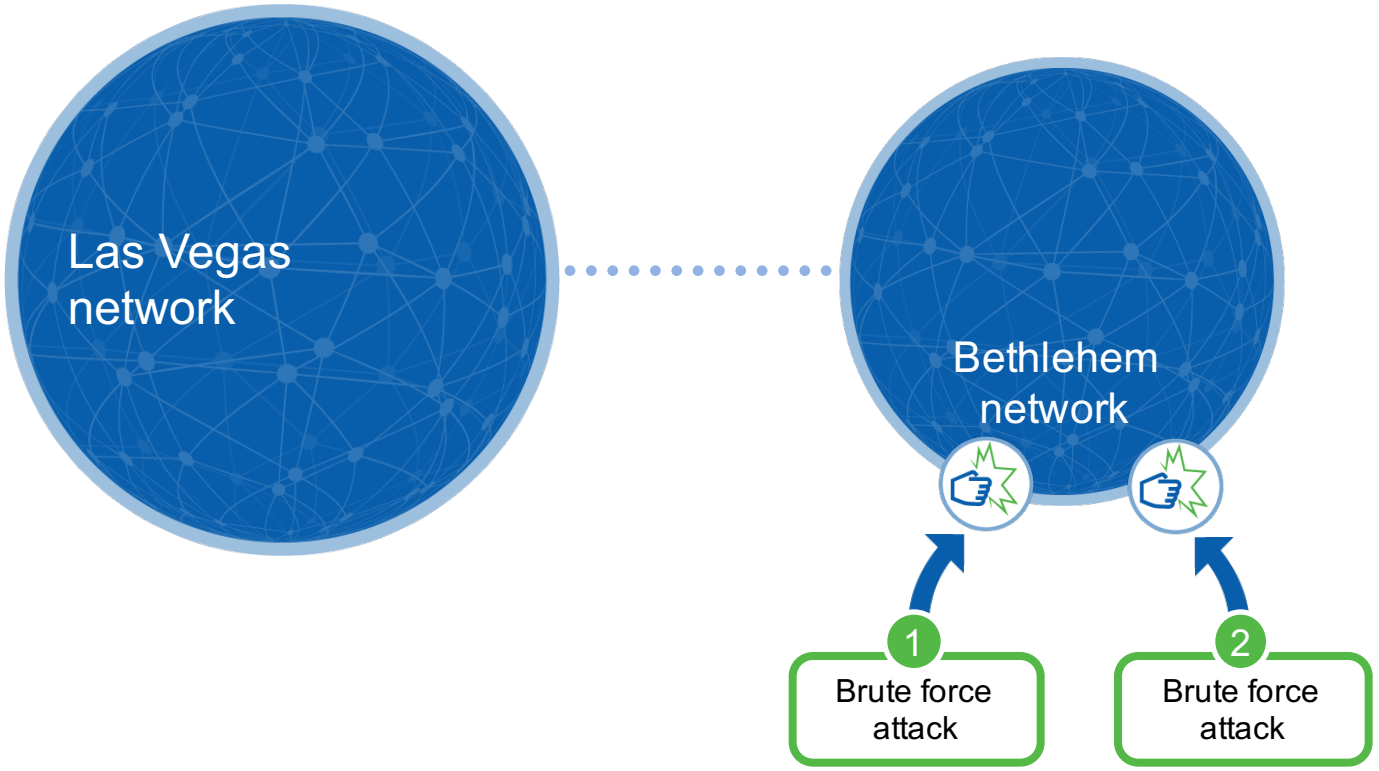
CYBERARK

El Ataque de Sands



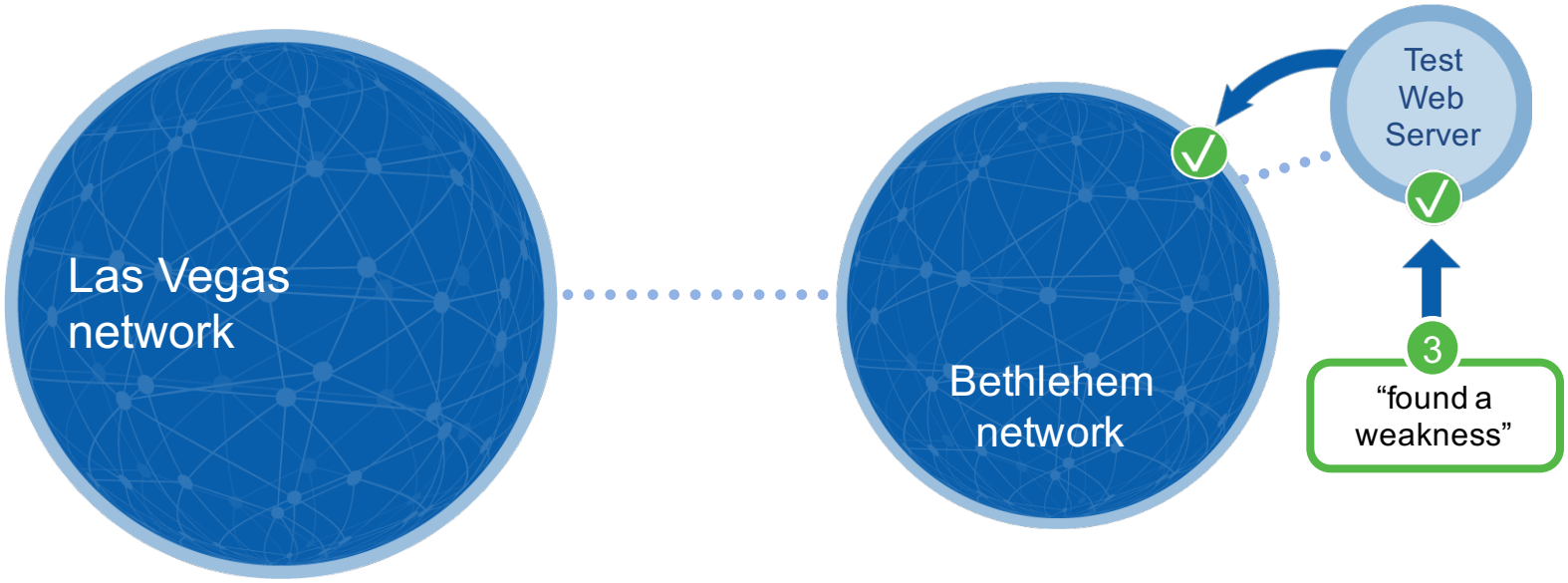
CYBERARK

El Ataque de Sands



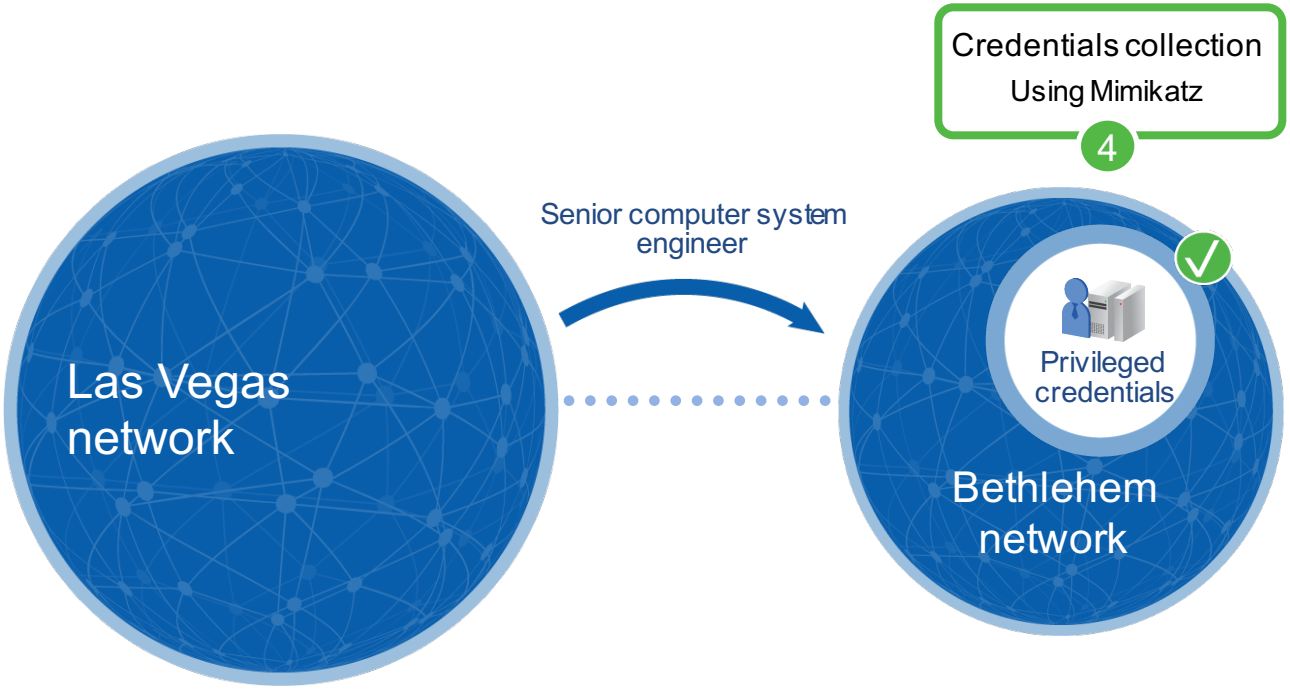
CYBERARK

El Ataque de Sands



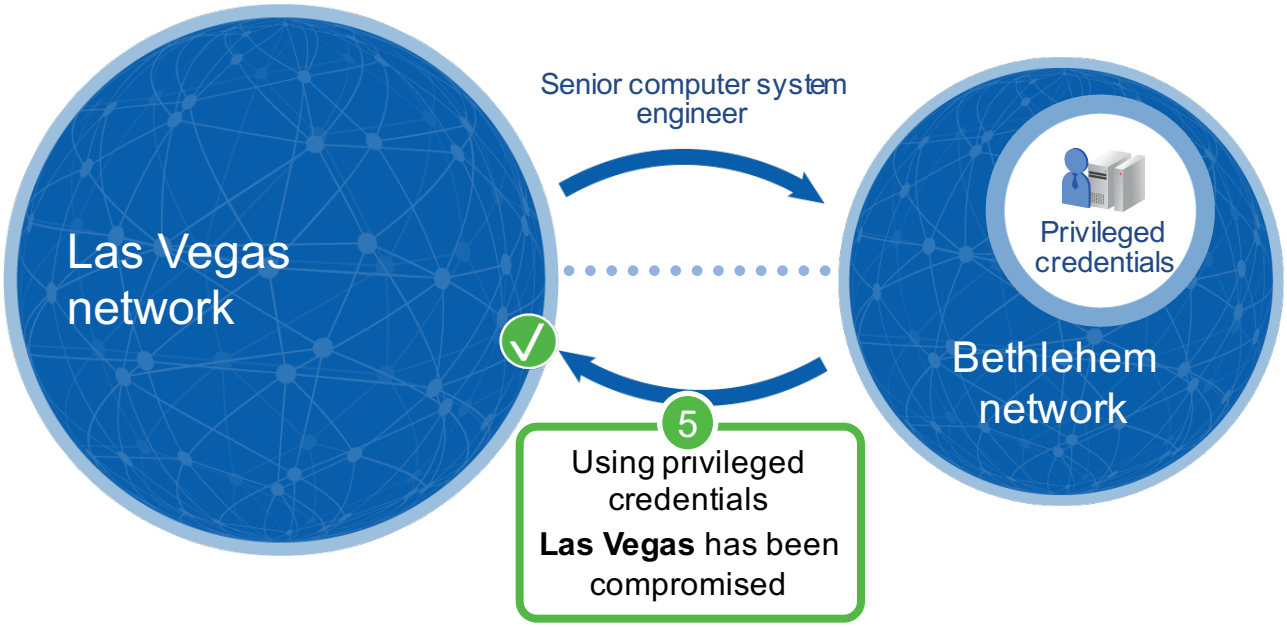
CYBERARK

El Ataque de Sands



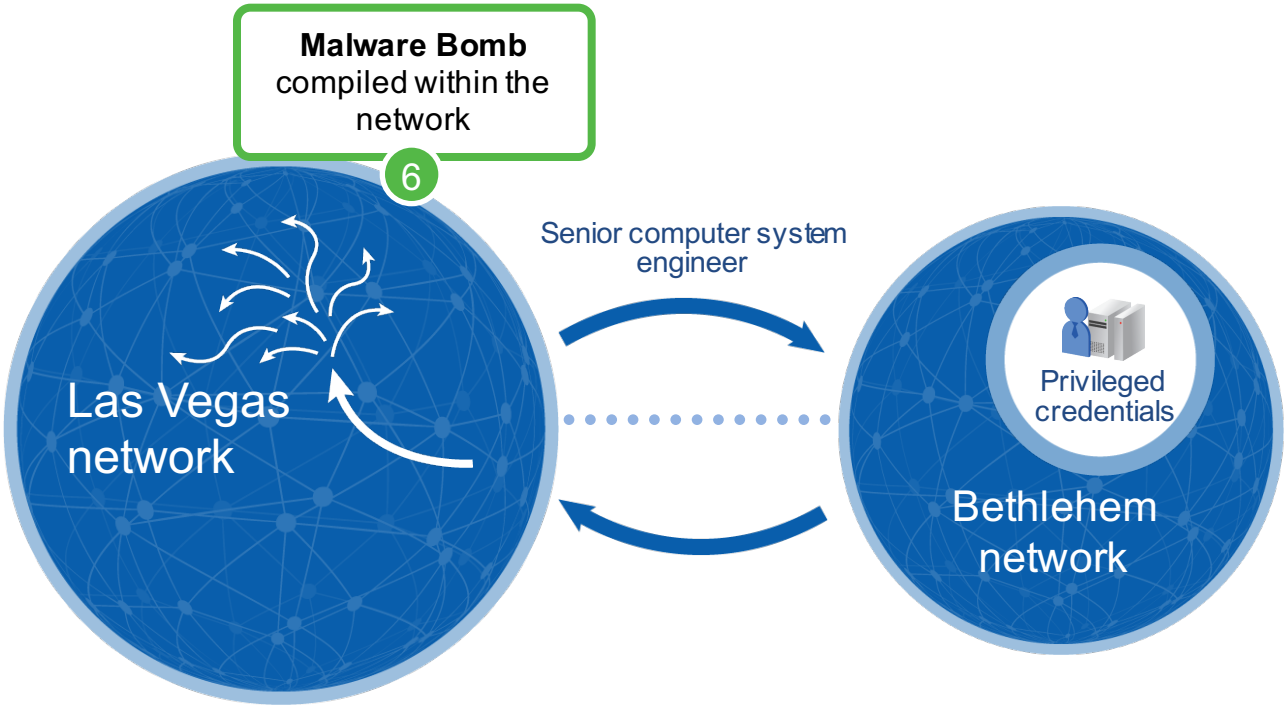
CYBERARK

El Ataque de Sands



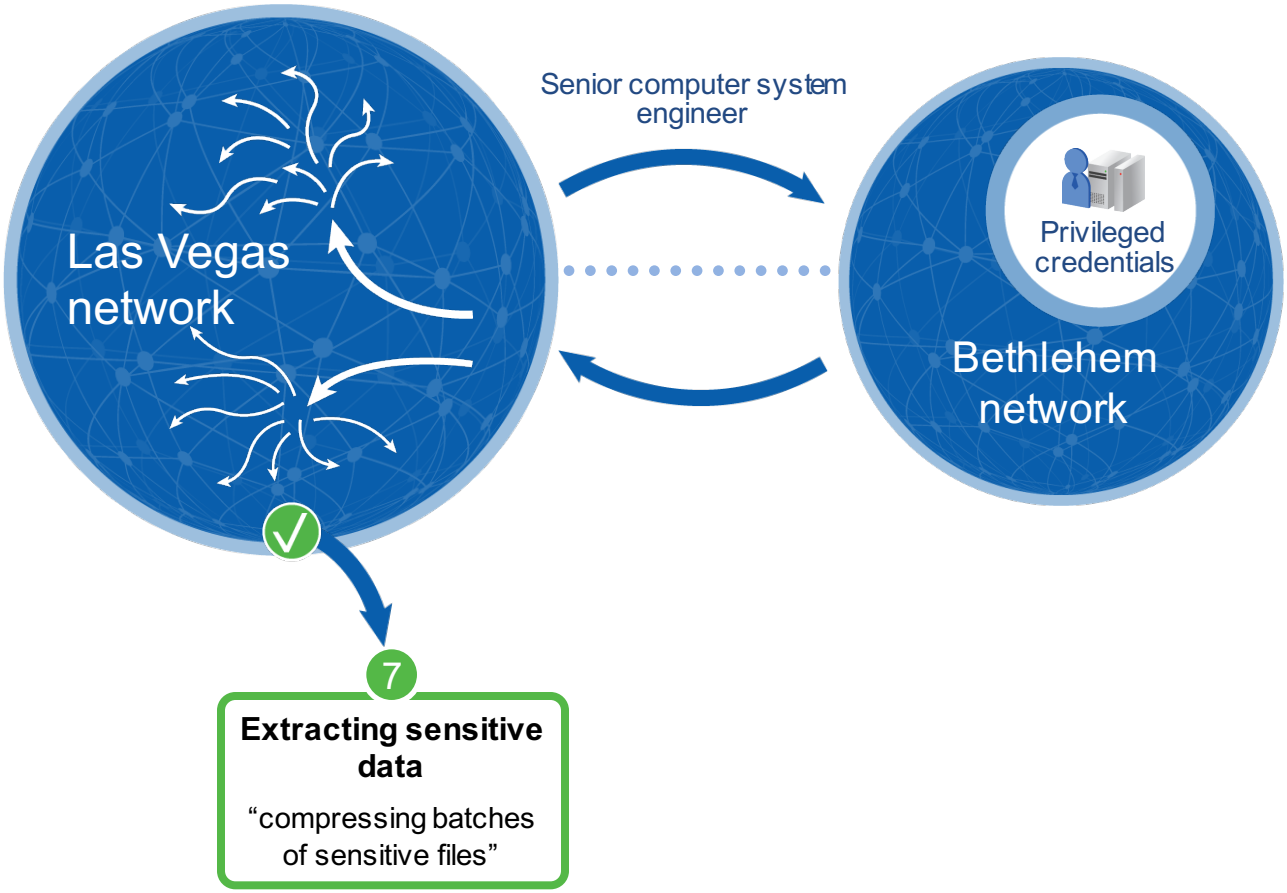
CYBERARK

El Ataque de Sands



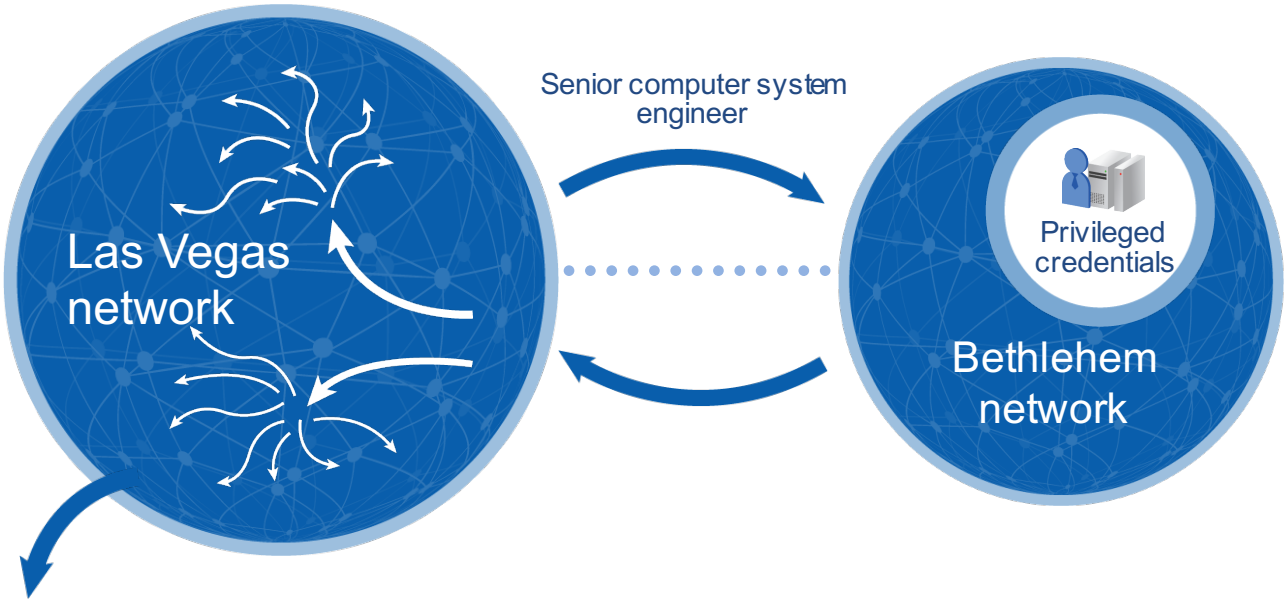
CYBERARK

El Ataque de Sands



CYBERARK

El Ataque de Sands



8

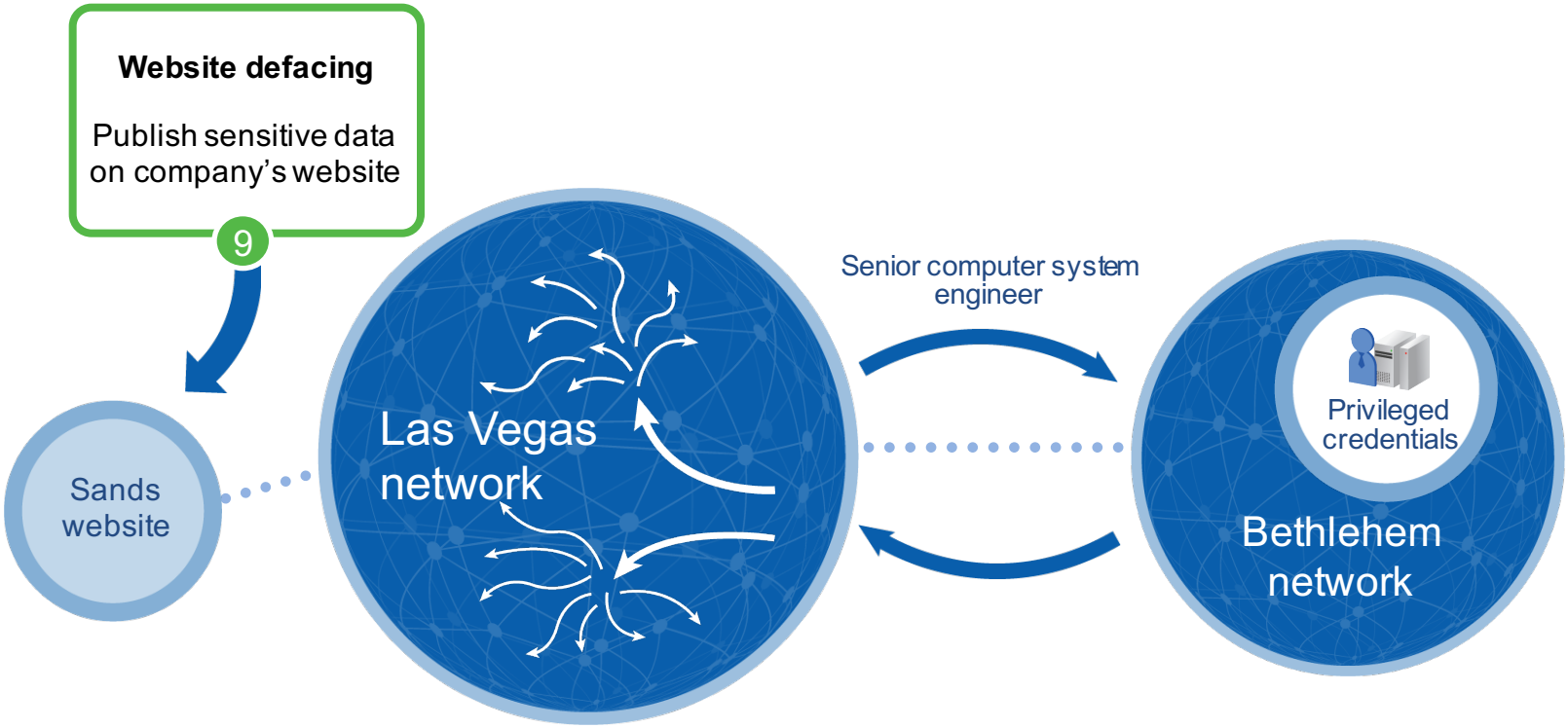
Burning bridges

Disconnect servers from the internet

Wiper is still on!

CYBERARK

El Ataque de Sands

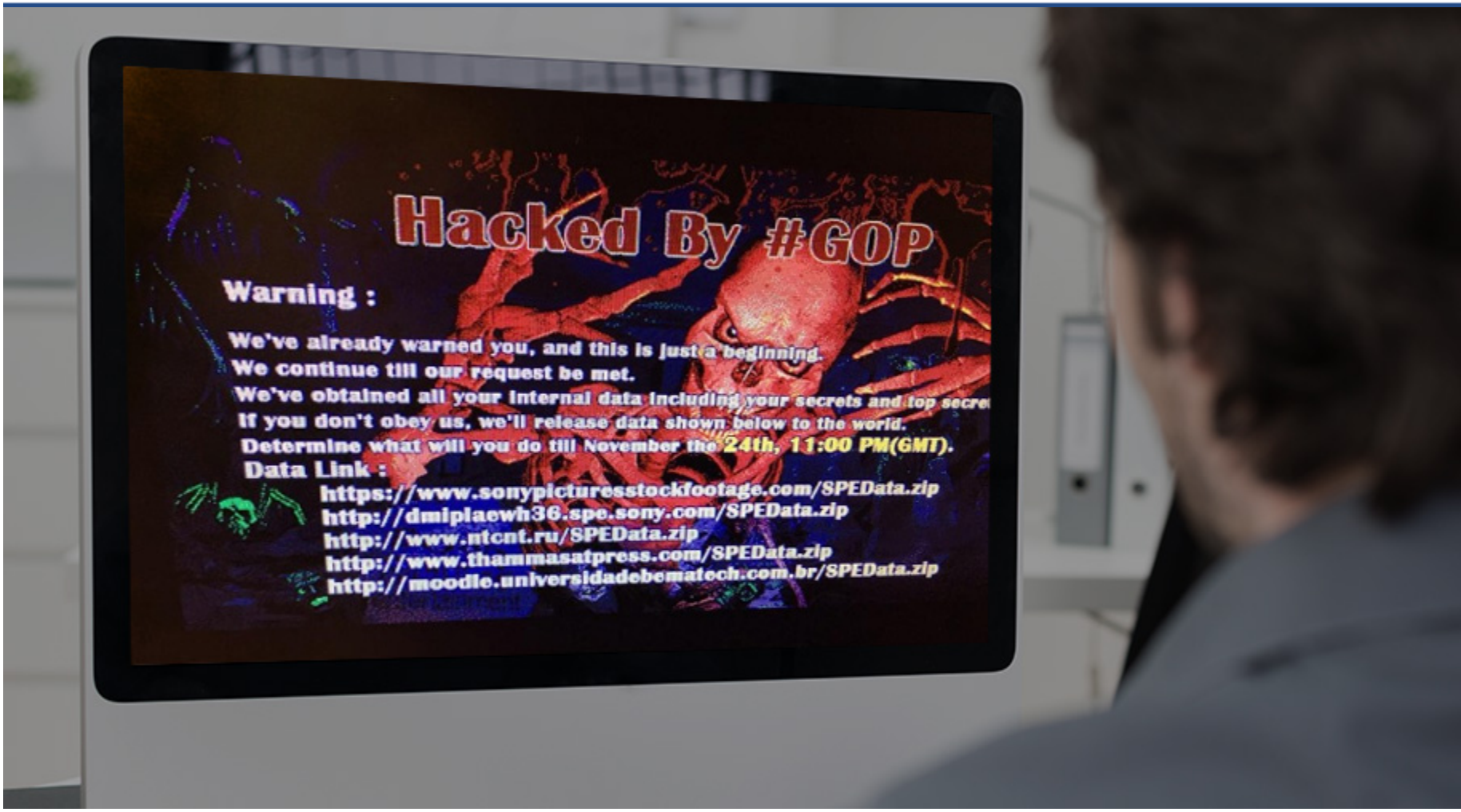


CYBERARK

CYBERARK

El Ataque de Sony Pictures and Entertainment

La Notificacion



CYBERARK

Detalles ofrecido por US Cert del gusano usado (SMB)

- Bruteforce passwords
- Lightweight backdoor
- Network propagation
- Destroys hard drives
- Listening implant

CYBERARK

Informacion Robada de Sony

5 UNRELEASED MOVIES

NETWORK INFORMATION

FTP passwords

SSH keys

Excel, Word and text files with passwords

Full dumps of SQL DBs

PERSONAL INFORMATION

Emails

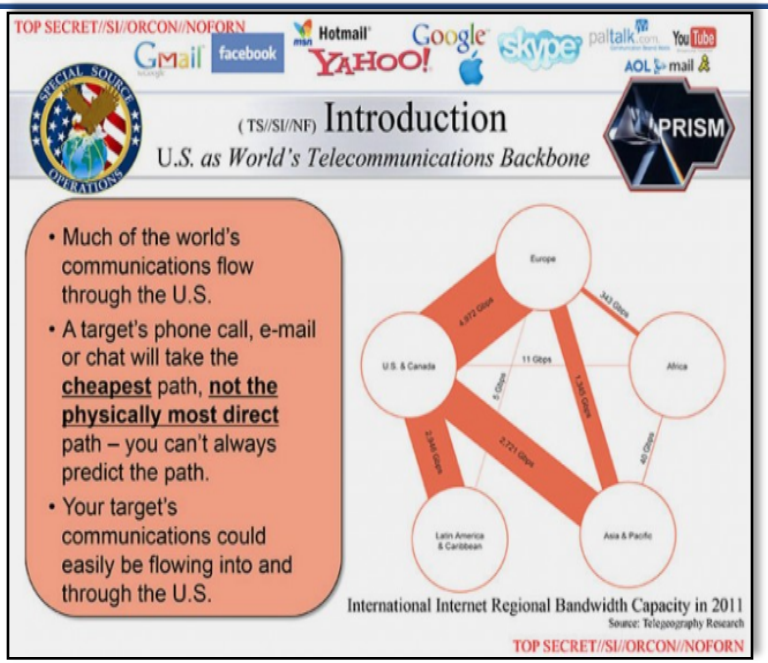
Salaries

Passport scans

CYBERARK

SNOWDEN

+



=Problemas

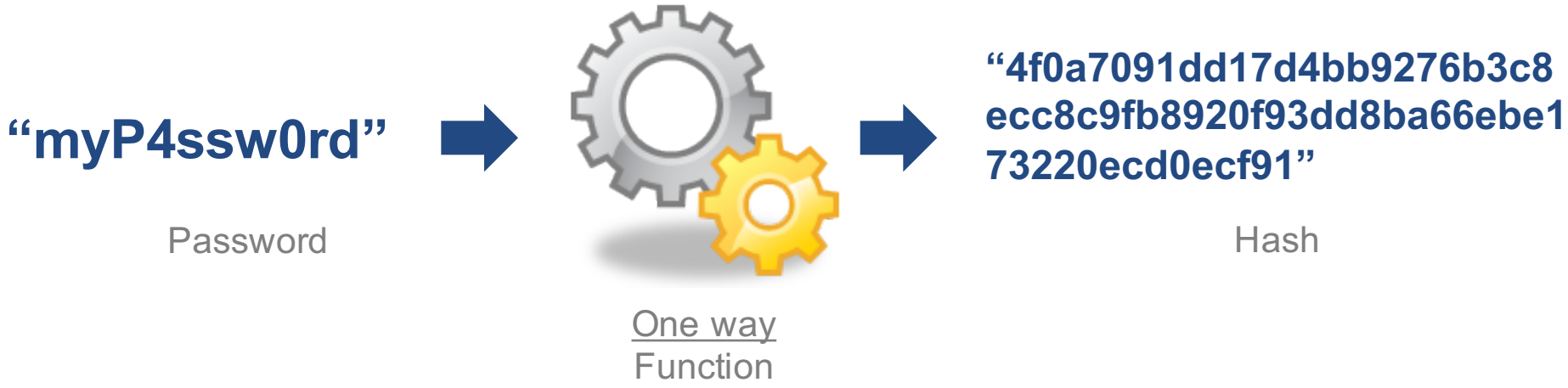
CYBERARK

CYBERARK

Protección y control de cuentas privilegiadas

Ataques comunes para obtener privilegios

- **PASS THE HASH**

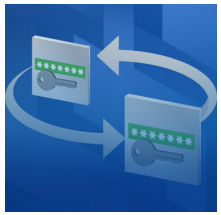


- **GOLDEN TICKET**
  - Ataque al protocolo **kerberos** que permite a los atacantes irrumpir en dominios de Windows copiando tickets de equipos comprometidos para obtener acceso ilimitado como administrador

CYBERARK

Qué hacer?

Asegurar proactivamente todas las credenciales privilegiadas



Rotar credenciales administrativas después de cada uso

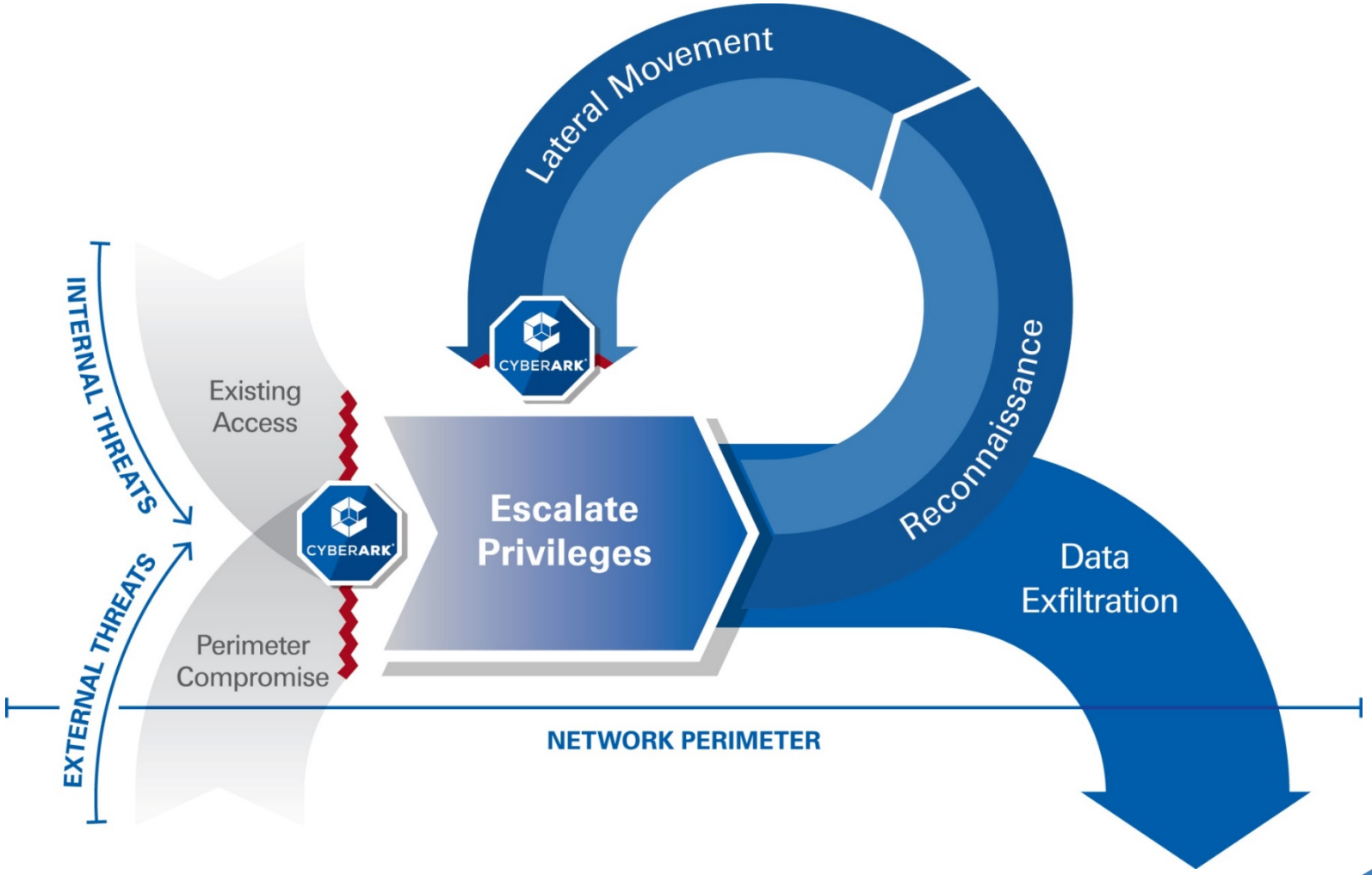
Establecer un punto de acceso hacia sistemas **críticos**

Monitorear el uso de cuentas privilegiadas para detectar anomalias

Controlar aplicaciones para reducir el riesgo de ataques basados en malware

CYBERARK

CyberArk Breaks the Attack Chain

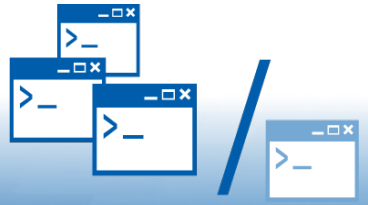


CYBERARK

Controles exhaustivos en la Actividad Privilegiada

Protección de Credenciales

Proteger contraseñas privilegiadas y llaves SSH



Aislar y Control De Sesiones

Aislando, controlando y grabando accesos privilegiados

Monitorización Contínua

Monitorear continuamente el comportamiento de las cuentas privilegiadas

Enterprise Password Vault Application Identity Manager SSH Key Manager	Privileged Session Manager On-Demand Privileges Unix OPM Windows	Privileged Threat Analytics

CYBERARK

¿Preguntas?