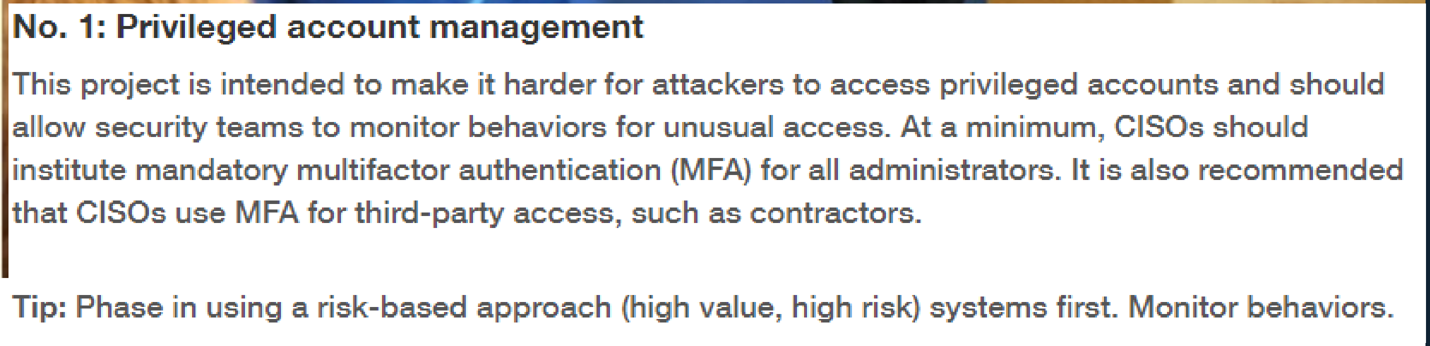
CYBERARK

common
Romandie

CYBER SECURITE

POURQUOI LE PAM EST-IL LA PRIORITÉ NUMÉRO UN ?

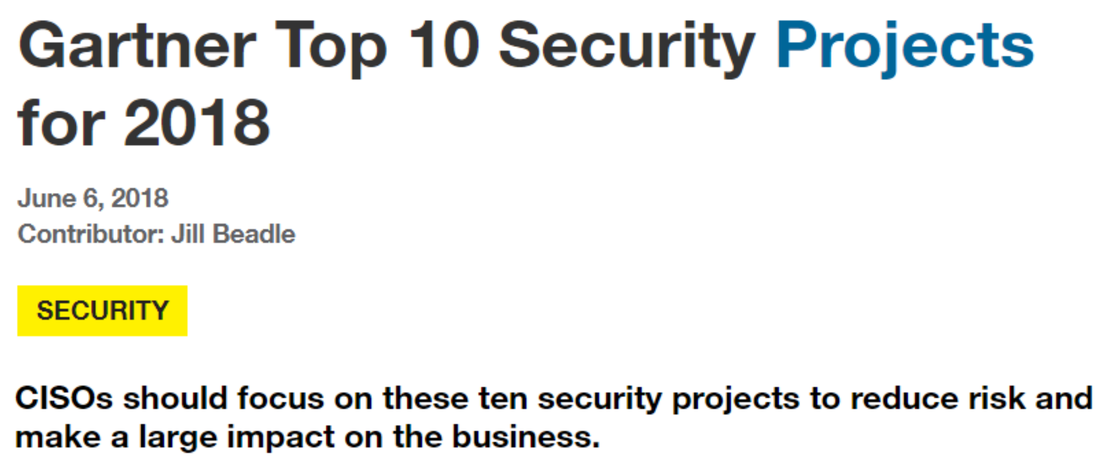
LES RECOMMANDATIONS DE GARTNER



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 should institute mandatory multifactor authentication (MFA) for all administrators. It is also recommended that CISOs use MFA for third-party access, such as contractors.

Tip: Phase in using a risk-based approach (high value, high risk) systems first. Monitor behaviors.



Gartner Top 10 Security Projects for 2018

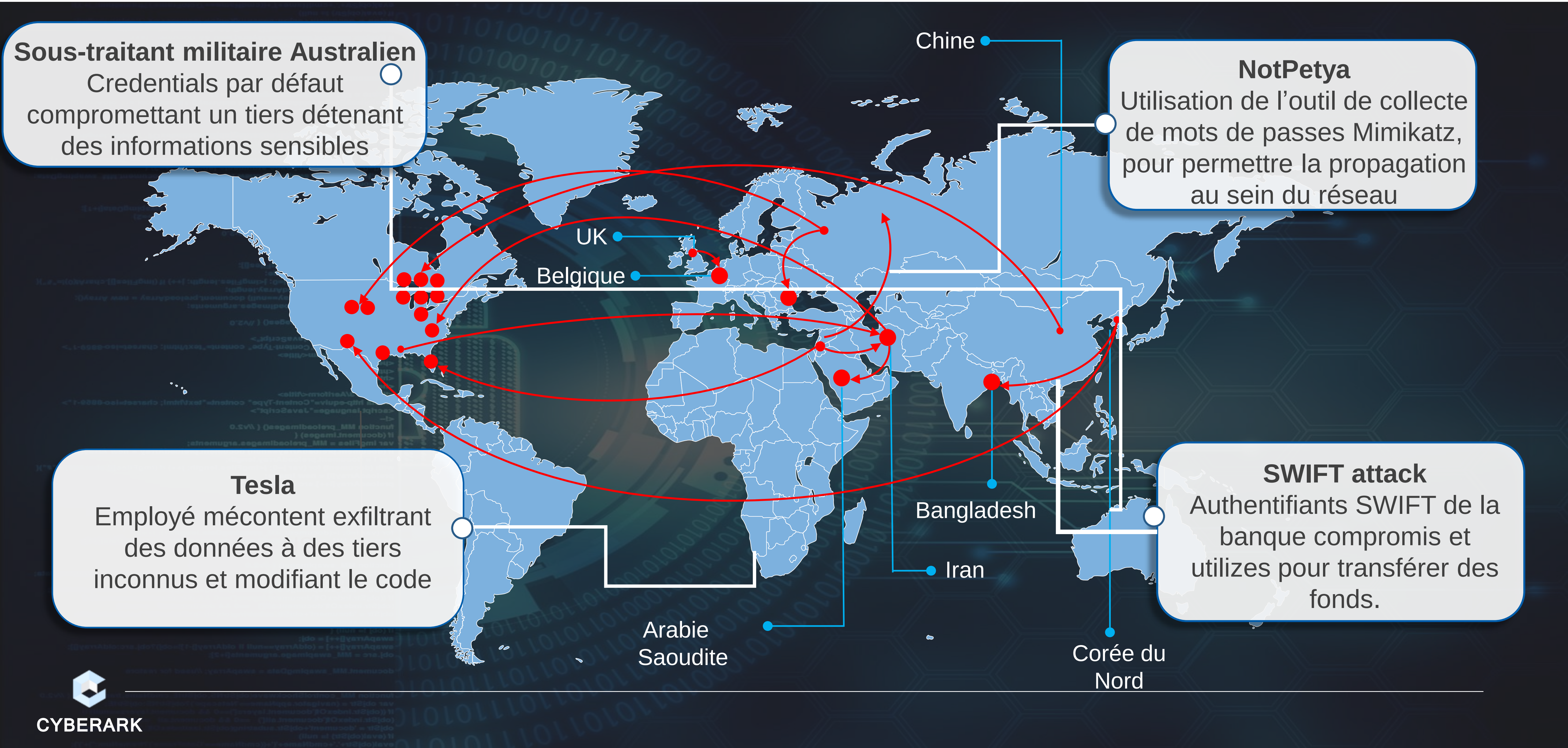
June 6, 2018
Contributor: Jill Beadle

SECURITY

CISOs should focus on these ten security projects to reduce risk and make a large impact on the business.

(https://www.gartner.com/smarterwithgartner/gartner-top-10-security-projects-for-2018/)

Les attaques continuent d’exploiter des failles



Sous-traitant militaire Australien
Credentials par défaut compromettant un tiers détenant des informations sensibles

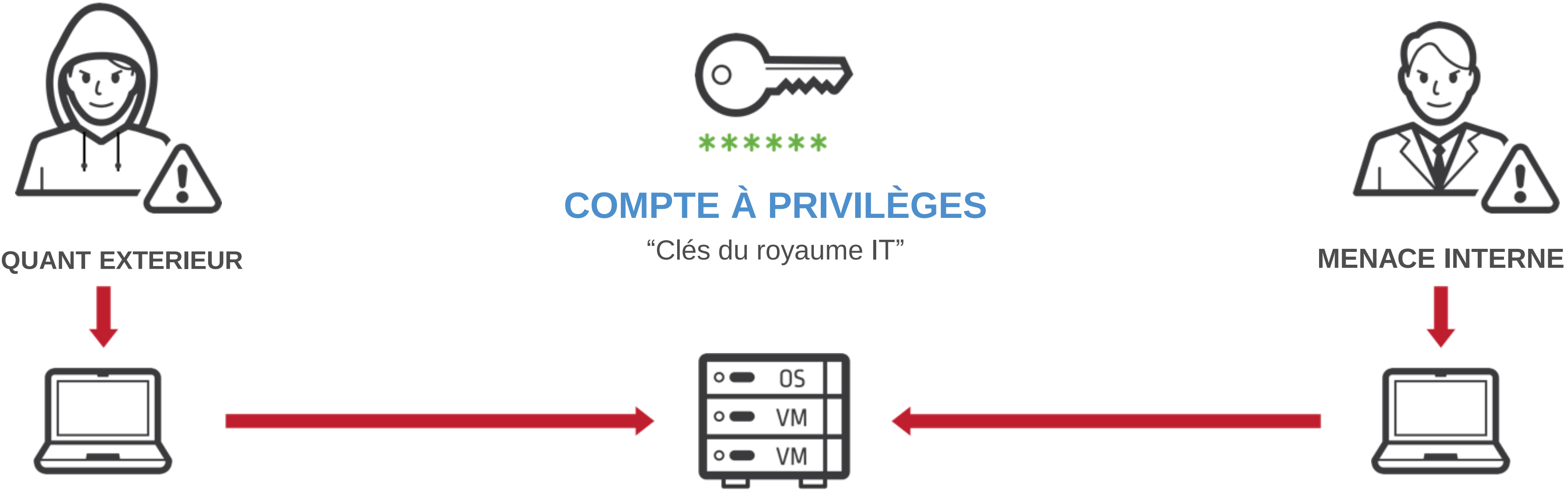
NotPetya
Utilisation de l’outil de collecte de mots de passes Mimikatz, pour permettre la propagation au sein du réseau

Tesla
Employé mécontent exfiltrant des données à des tiers inconnus et modifiant le code

SWIFT attack
Authentifiants SWIFT de la banque compromis et utilizes pour transférer des fonds.

CYBERARK

LES COMPTES A PRIVILÈGES, CLÉS DU ROYAUME !



ATTAQUANT EXTERIEUR

******

COMPTE À PRIVILÈGES

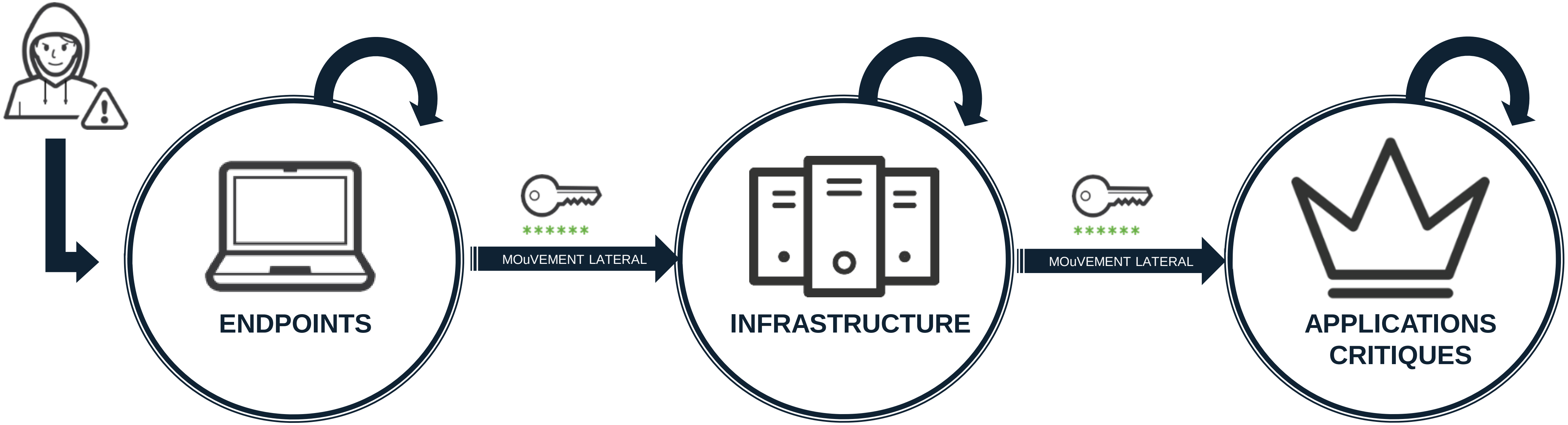
“Clés du royaume IT”

MENACE INTERNE

LES ATTAQUANTS ENTRERONT…

…OU SONT MÊME DÉJÀ PRÉSENTS

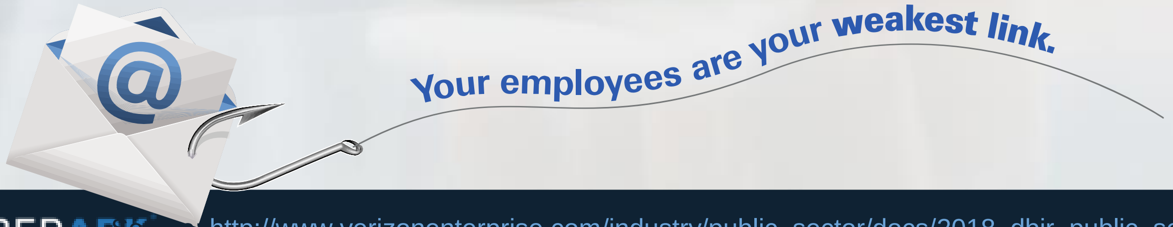
LA VOIX LA PLUS EMPRUNTÉE…

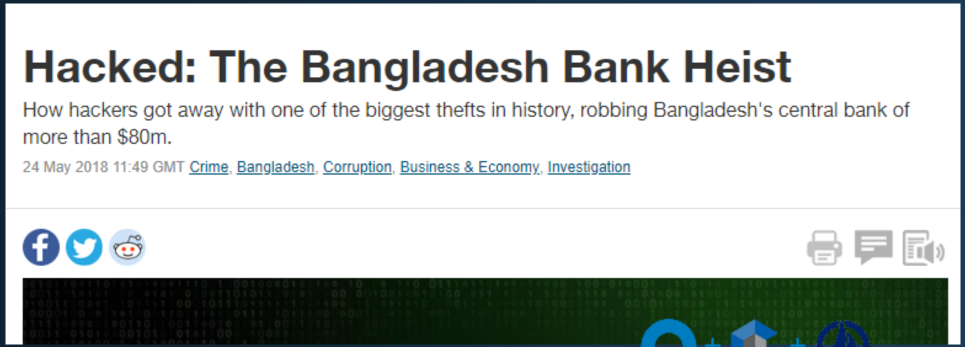


LE MAILLON FAIBLE

4% of people will click on any given phishing campaign.

"This is something we've been saying for the last three years, and sadly it's still true today—people are still falling for phishing campaigns"





Hacked: The Bangladesh Bank Heist

How hackers got away with one of the biggest thefts in history, robbing Bangladesh's central bank of more than $80m.

24 May 2018 11:49 GMT Crime, Bangladesh, Corruption, Business & Economy, Investigation

CYBERARK

http://www.verizonenterprise.com/industry/public_sector/docs/2018_dbir_public_sector.pdf

LA MENACE INTERNE

Se produit dans 26% des attaques, dont les coûts sont importants

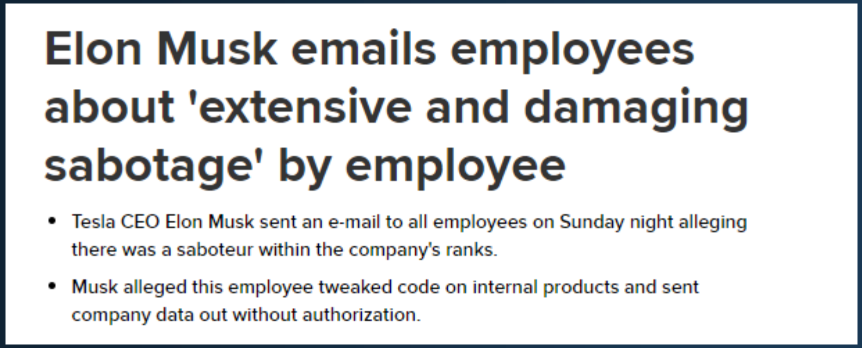
Les motivations les plus courantes:

FRUSTRATION

FINANCIERES

HACKTIVISME

INFLUENCE EXTERIEURE

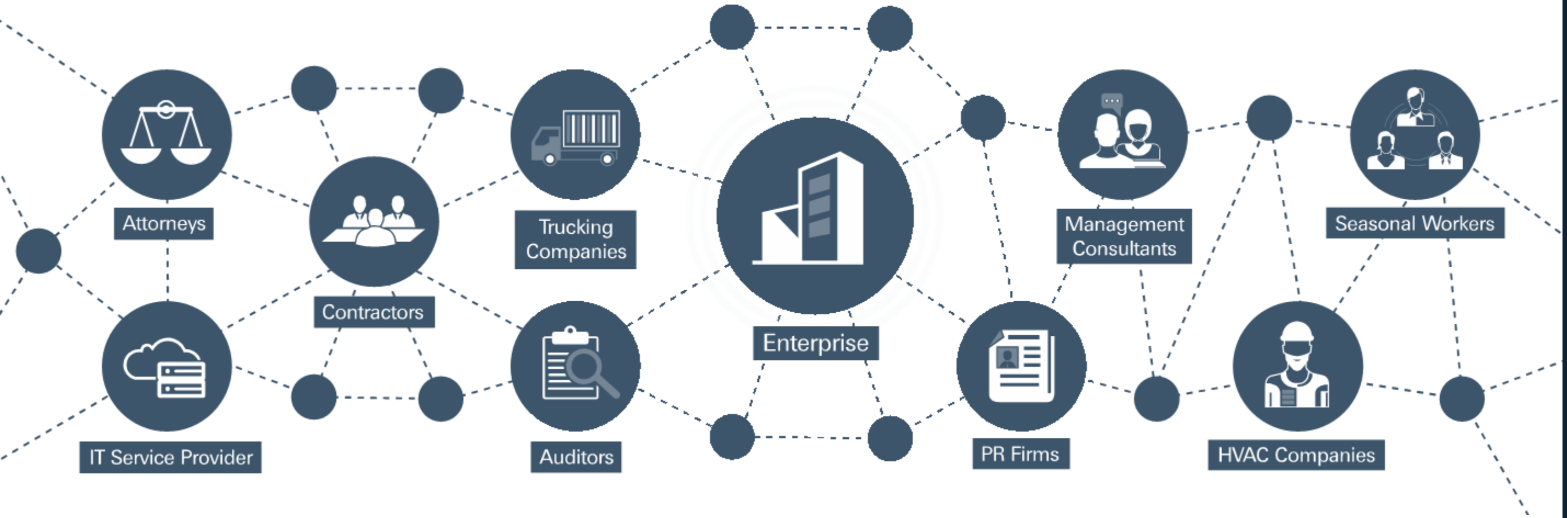


Elon Musk emails employees about 'extensive and damaging sabotage' by employee

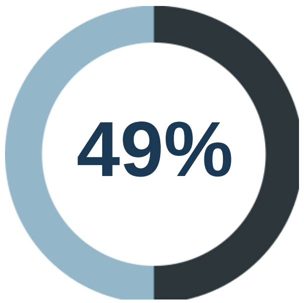
- Tesla CEO Elon Musk sent an e-mail to all employees on Sunday night alleging there was a saboteur within the company's ranks.
- Musk alleged this employee tweaked code on internal products and sent company data out without authorization.

LA MENACE EXTERNE

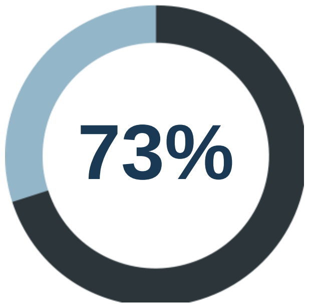
Au moins 60% des organisations autorisent les accès distants à des tiers.



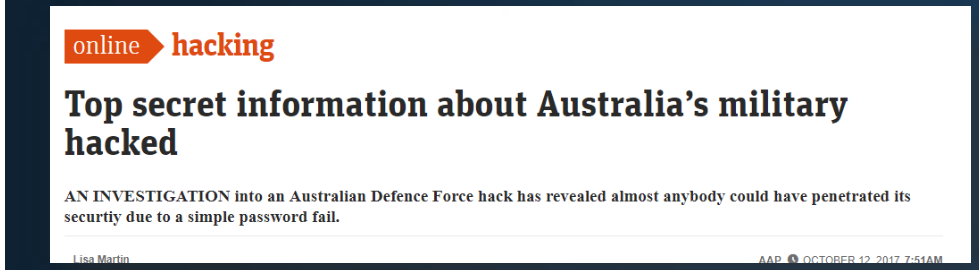
D’après une étude Ponemon…



Des répondants on subit des fuites de données causées par des tiers



Pensent que le problème s’aggrave



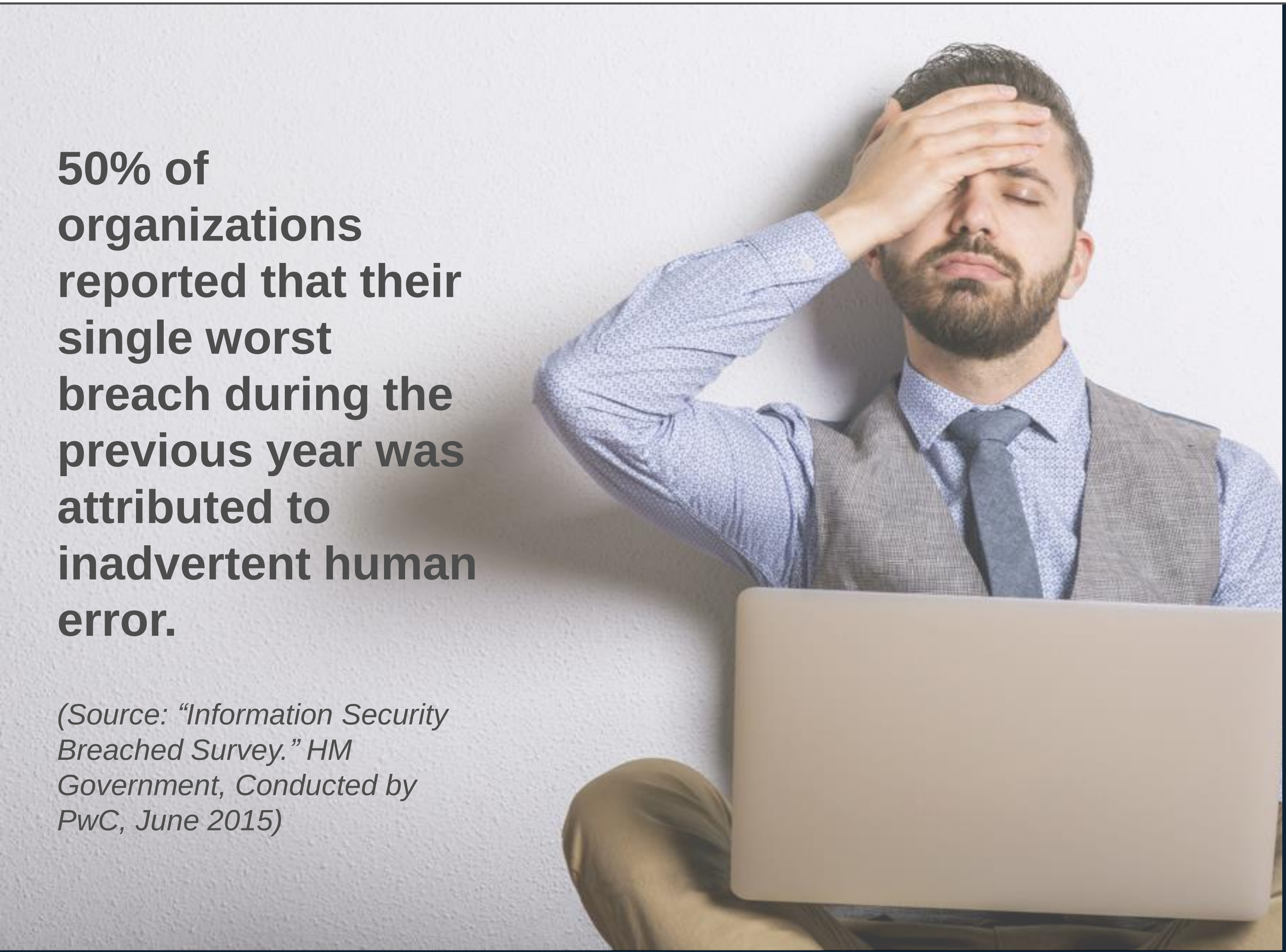
online hacking

Top secret information about Australia’s military hacked

AN INVESTIGATION into an Australian Defence Force hack has revealed almost anybody could have penetrated its securtiy due to a simple password fail.

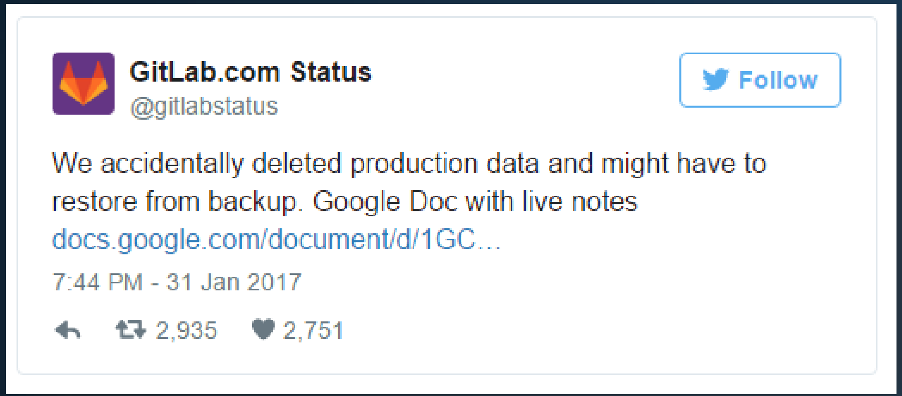
Lisa Martin AAP OCTOBER 12 2017 7:51AM

LES INCIDENTS



50% of organizations reported that their single worst breach during the previous year was attributed to inadvertent human error.

(Source: "Information Security Breached Survey." HM Government, Conducted by PwC, June 2015)



GitLab.com Status
@gitlabstatus

We accidentally deleted production data and might have to restore from backup. Google Doc with live notes docs.google.com/document/d/1GC...

7:44 PM - 31 Jan 2017

Un employé de GitLab supprime Accidentellement des données importantes

COMMENT ISOLER LES ÉQUIPEMENTS SENSIBLES

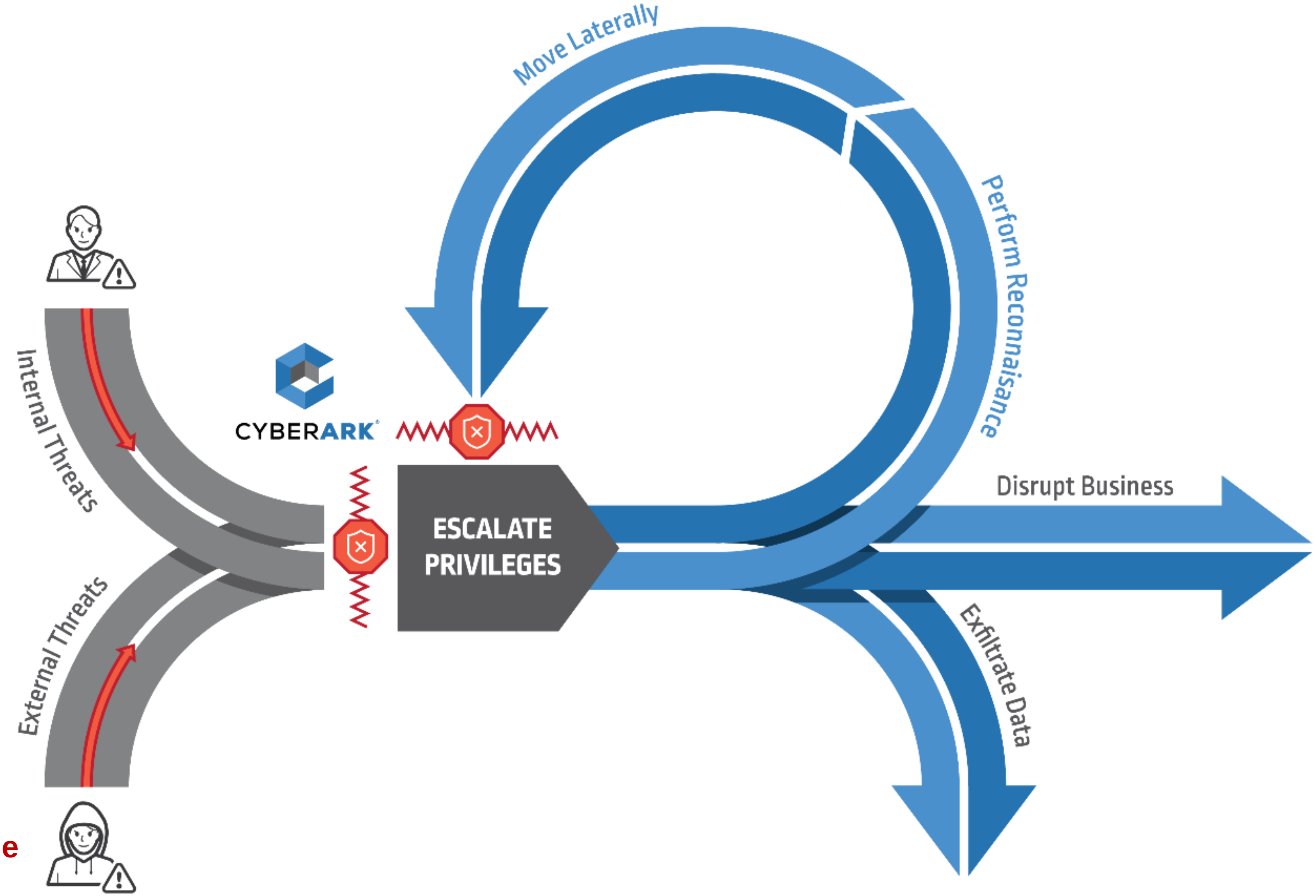
Accès Existants

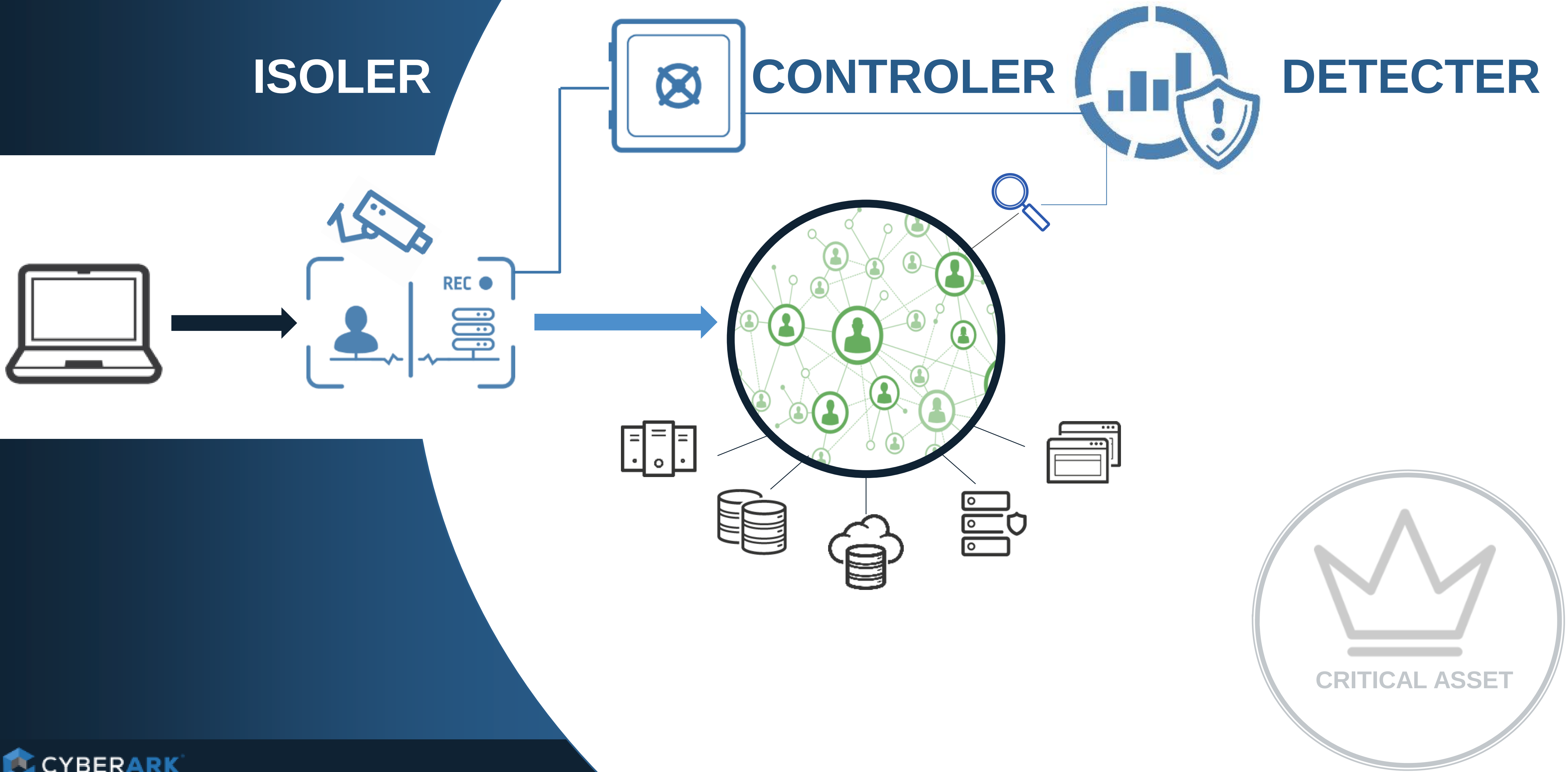
On-Premises

Hybrid

Cloud

Compromission externe





ISOLER

CONTROLER

DETECTER

CRITICAL ASSET

LE FUTUR DES VOLS D’IDENTIFIANTS

Cloud

Environnements DevOps

AUTOMATISATION

Automatic Scale Services

TECHNOLOGIES “SERVERLESS”

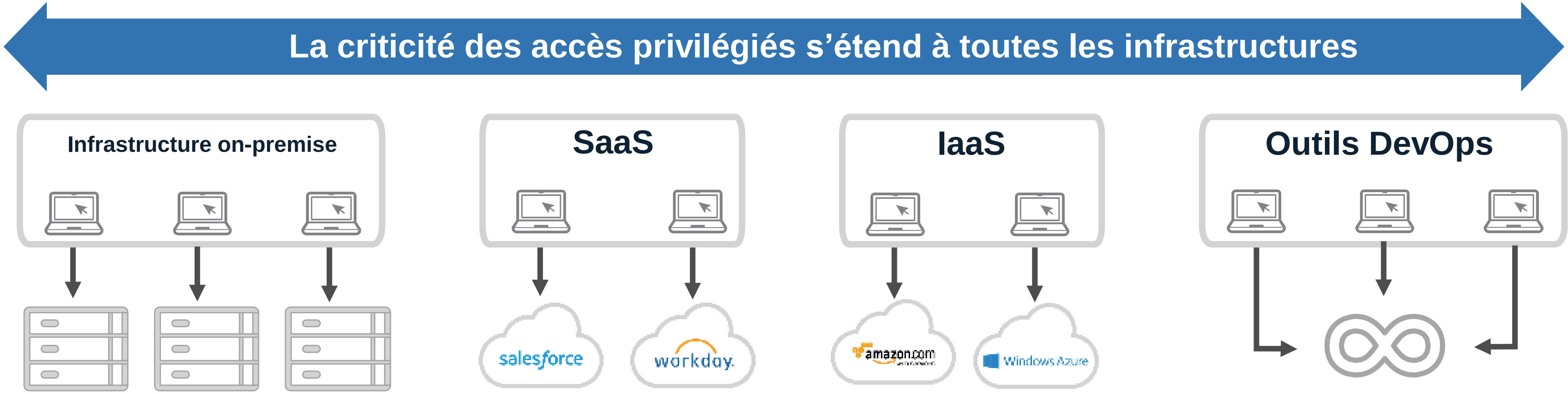
Fonctions & Containers

NOUVEAUX CREDENTIALS

Identité et Rôles Machine

LA TRANSFORMATION DIGITALE MODIFIE LES ACCÈS

La transformation digitale s'accompagne de nouveaux processus d'administration des infrastructures, s'appuyant notamment sur des accès tiers, de l'automatisation et de l'orchestration.



La criticité des accès privilégiés s'étend à toutes les infrastructures

Infrastructure on-premise

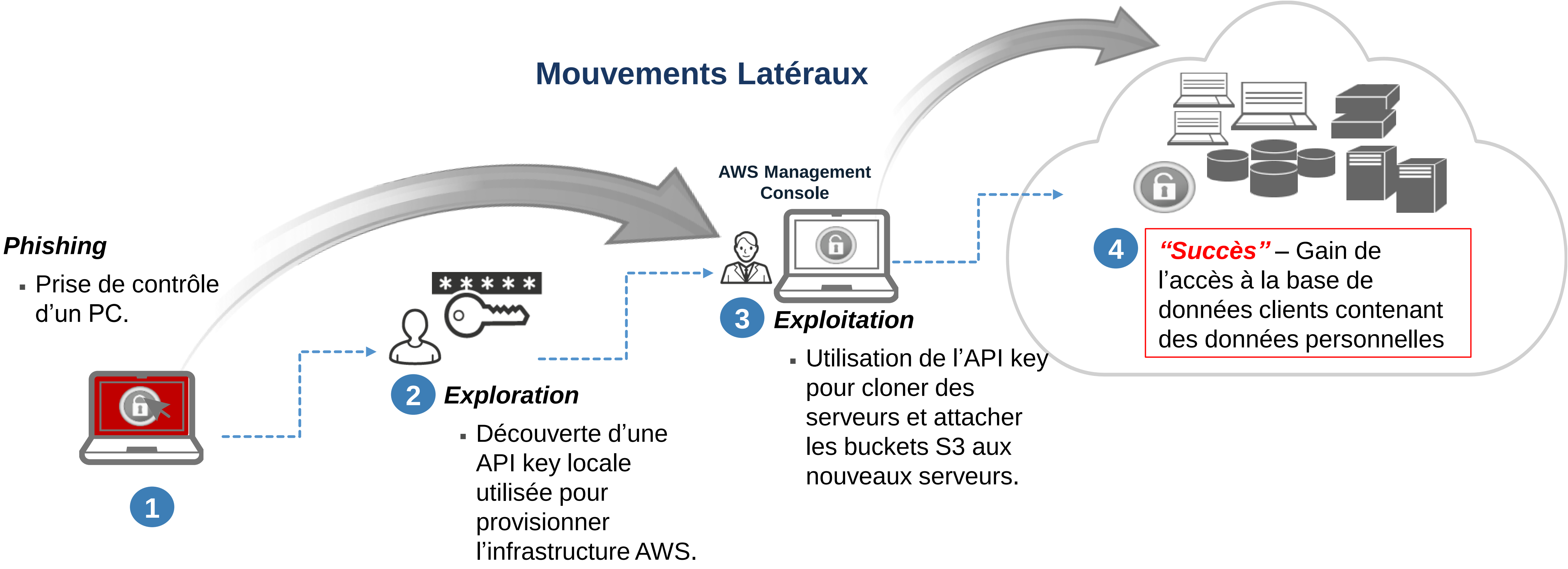
SaaS

IaaS

Outils DevOps

EXEMPLE SIMPLE D’EXERCICE RED TEAM : LES VULNÉRABILITÉS FACE AU CLOUD

Demande client d’un exercice Red Team afin d’identifier des vulnérabilités potentielles



Mouvements Latéraux

Phishing

- Prise de contrôle d’un PC.

1

2 ***Exploration***

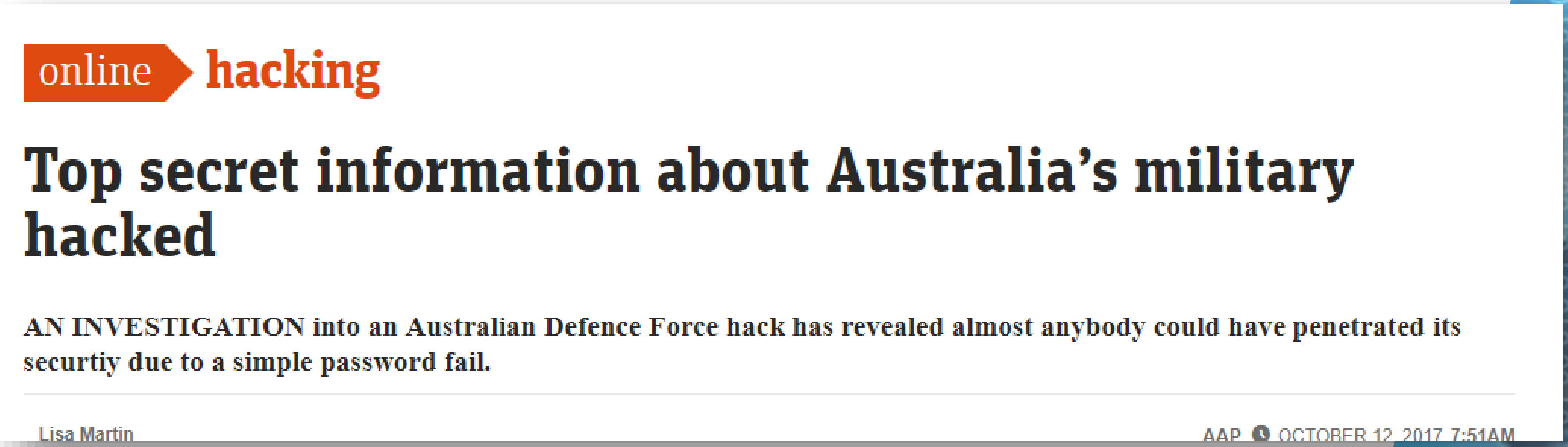
- Découverte d’une API key locale utilisée pour provisionner l’infrastructure AWS.

AWS Management Console

3 ***Exploitation***

- Utilisation de l’API key pour cloner des serveurs et attacher les buckets S3 aux nouveaux serveurs.

4 ***“Succès”*** – Gain de l’accès à la base de données clients contenant des données personnelles



online hacking

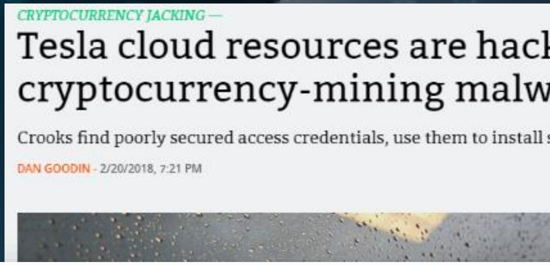
Top secret information about Australia's military hacked

AN INVESTIGATION into an Australian Defence Force hack has revealed almost anybody could have penetrated its securtiy due to a simple password fail.

Lisa Martin AAP OCTOBER 12, 2017 7:51AM

Nouveau Monde...

...Mêmes Problèmes

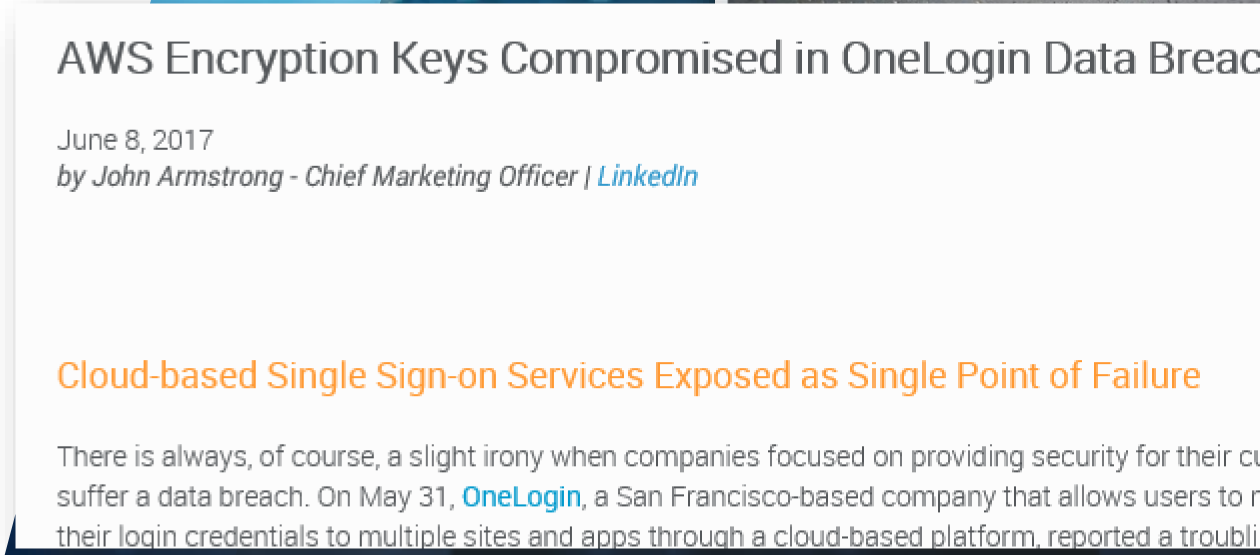


CRYPTOCURRENCY JACKING —

Tesla cloud resources are hack
cryptocurrency-mining malw

Crooks find poorly secured access credentials, use them to install

DAN GOODIN - 2/20/2018, 7:21 PM



AWS Encryption Keys Compromised in OneLogin Data Breac

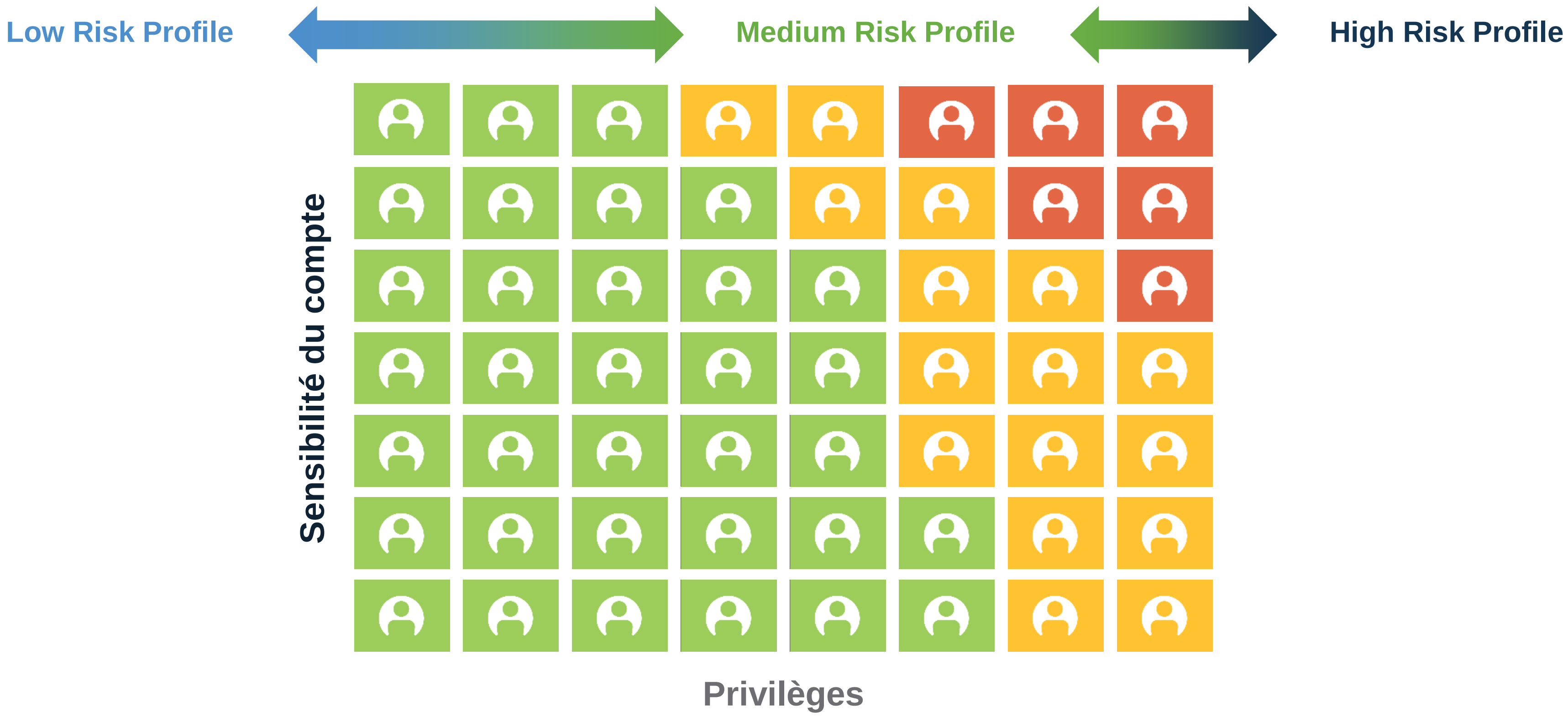
June 8, 2017
by John Armstrong - Chief Marketing Officer | LinkedIn

Cloud-based Single Sign-on Services Exposed as Single Point of Failure

There is always, of course, a slight irony when companies focused on providing security for their cu
suffer a data breach. On May 31, OneLogin, a San Francisco-based company that allows users to m
their login credentials to multiple sites and apps through a cloud-based platform, reported a troubli

LA METHODE

UNE APPROCHE BASÉE SUR LE RISQUE



Low Risk Profile

Medium Risk Profile

High Risk Profile

Sensibilité du compte

Privilèges

SE DÉFENDRE AVEC UNE APPROCHE BASÉE SUR LE RISQUE

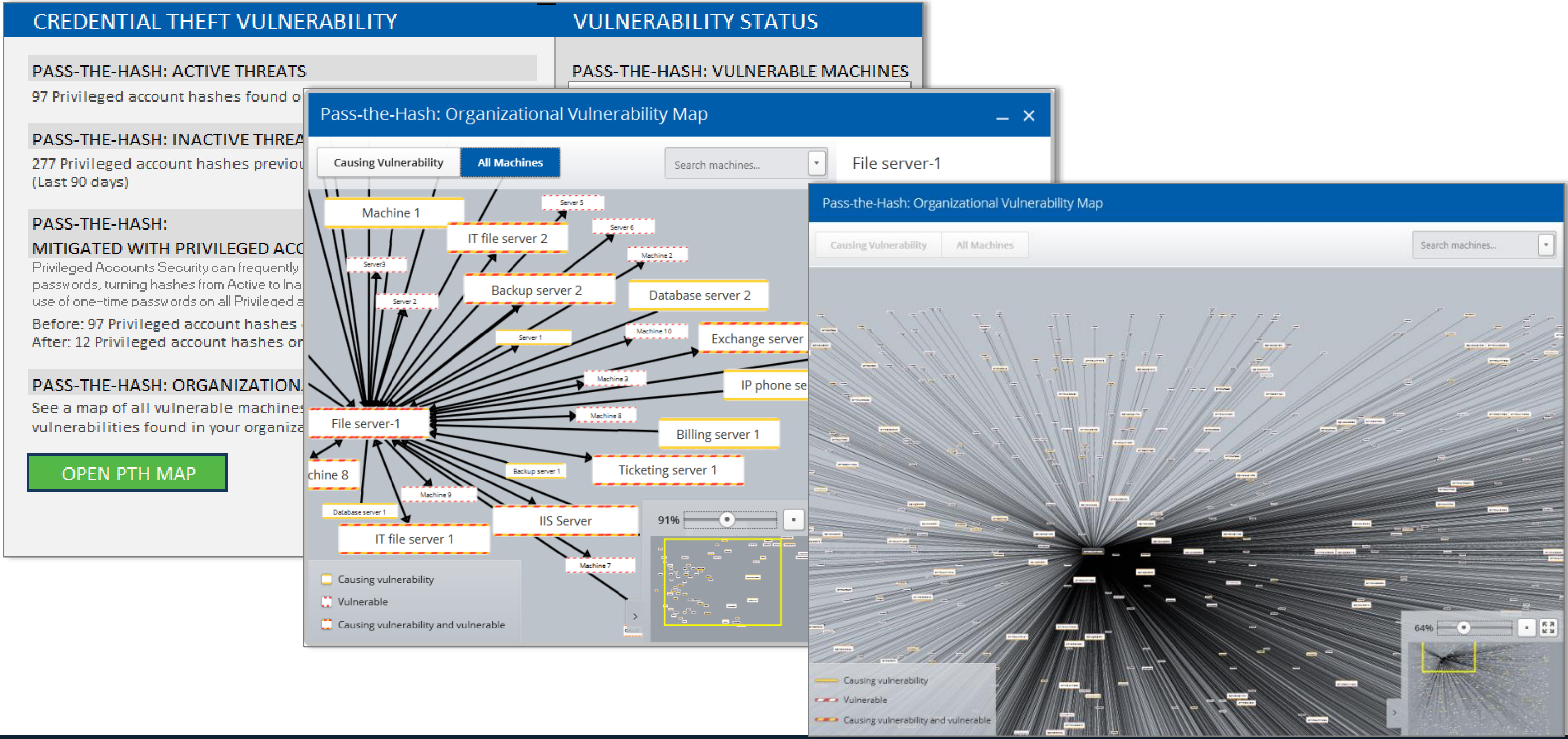
Systematically Address Organization’s Top Control Goals

- Eliminate Irreversible Network Takeover Attacks
- Control and Secure Infrastructure Accounts
- Limit Lateral Movement
- Secure SaaS Admins and Privileged Business Users
- Manage *NIX SSH Keys
- Defend DevOps Secrets in the Cloud and On-Premises
- Protect Credentials for Third-Party Applications

PAR OÙ COMMENCER ?

Identifier les accès à privileges légitimes…

IDENTIFIER LES RISQUES – MOUVEMENTS LATERAUX



CREDENTIAL THEFT VULNERABILITY

PASS-THE-HASH: ACTIVE THREATS

97 Privileged account hashes found o

PASS-THE-HASH: INACTIVE THREA

277 Privileged account hashes previou
(Last 90 days)

PASS-THE-HASH:
MITIGATED WITH PRIVILEGED ACC

Privileged Accounts Security can frequently
passwords, turning hashes from Active to Ina
use of one-time passwords on all Privileged a

Before: 97 Privileged account hashes
After: 12 Privileged account hashes or

PASS-THE-HASH: ORGANIZATION

See a map of all vulnerable machines
vulnerabilities found in your organiz

OPEN PTH MAP

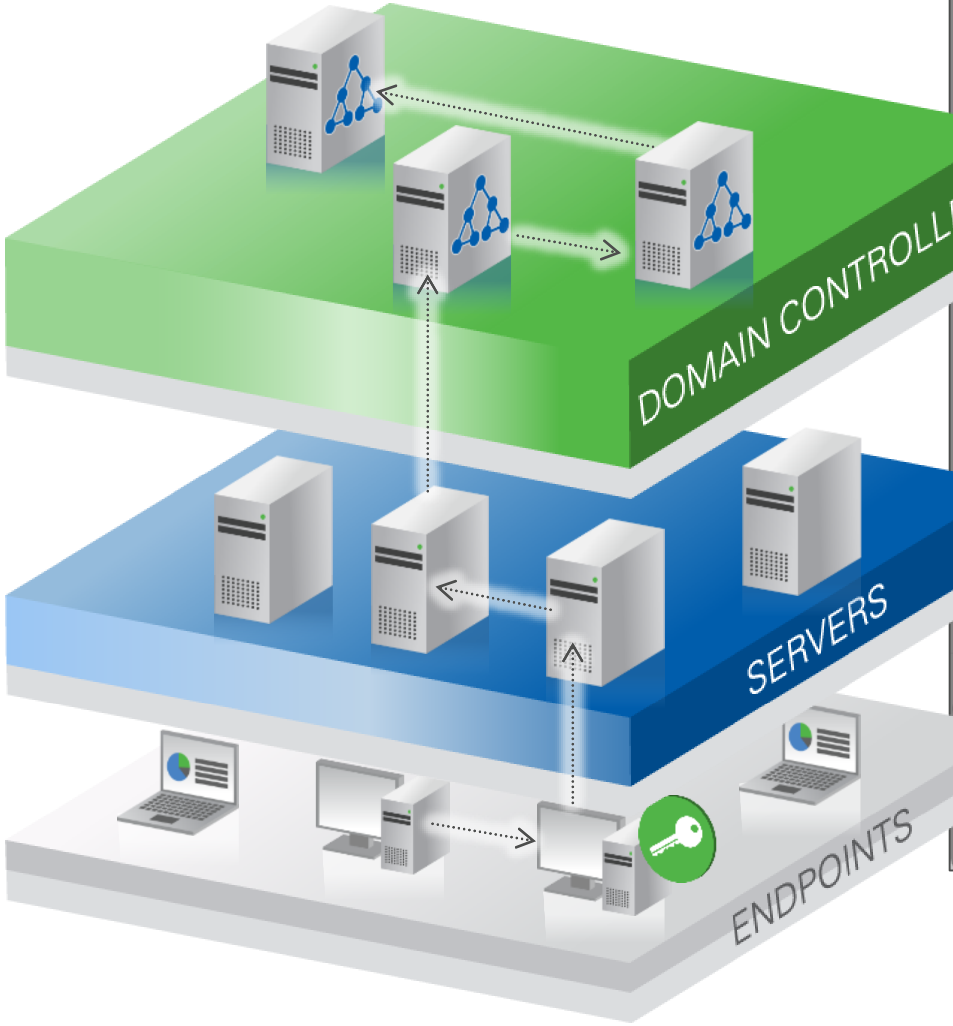
VULNERABILITY STATUS

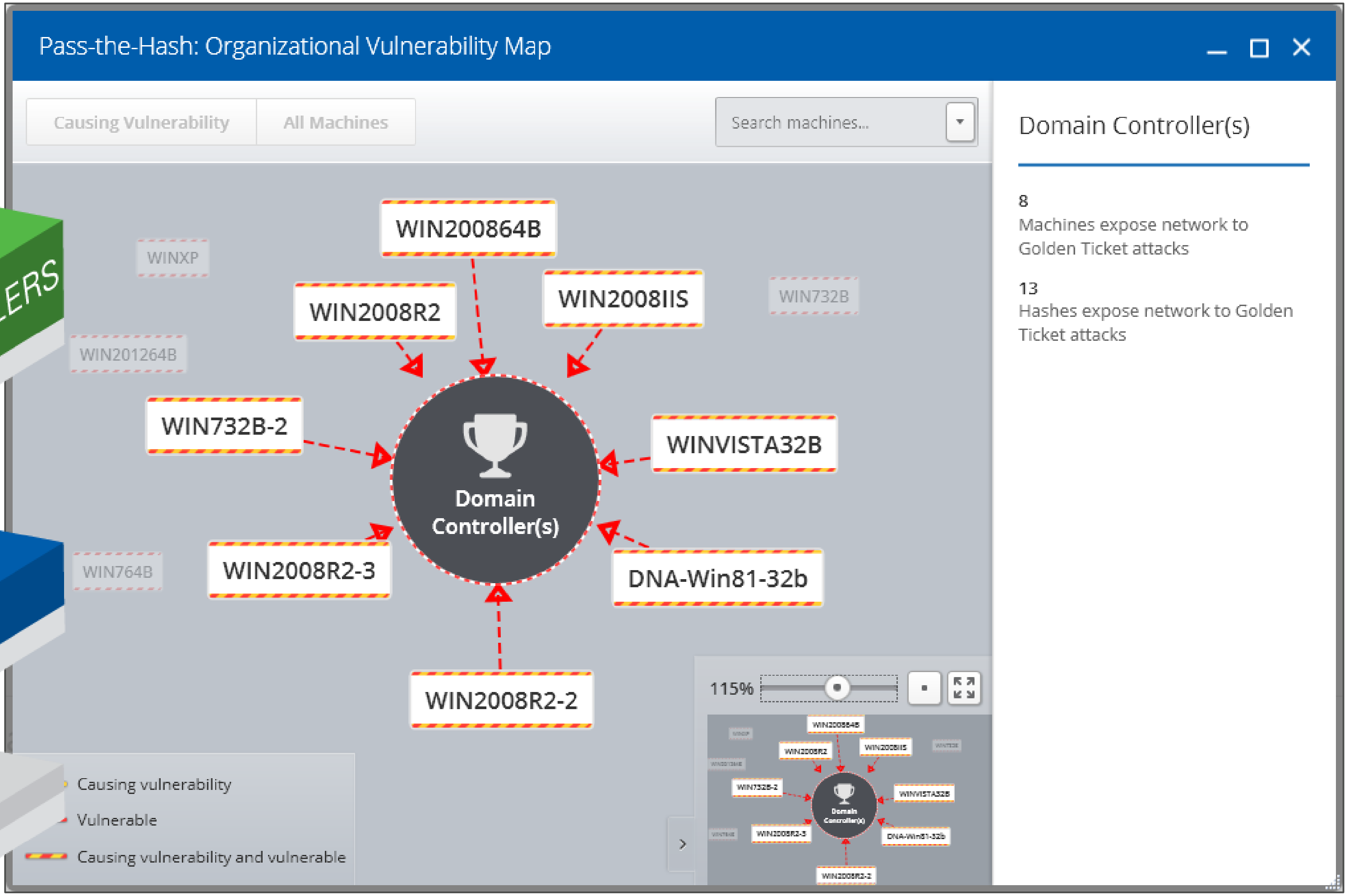
PASS-THE-HASH: VULNERABLE MACHINES

Pass-the-Hash: Organizational Vulnerability Map

Pass-the-Hash: Organizational Vulnerability Map

IDENTIFIER LES RISQUES– COMPROMISSION DE DOMAINE





Pass-the-Hash: Organizational Vulnerability Map

Domain Controller(s)

8
Machines expose network to Golden Ticket attacks

13
Hashes expose network to Golden Ticket attacks

QUESTIONS?

jc.vitu@cyberark.com