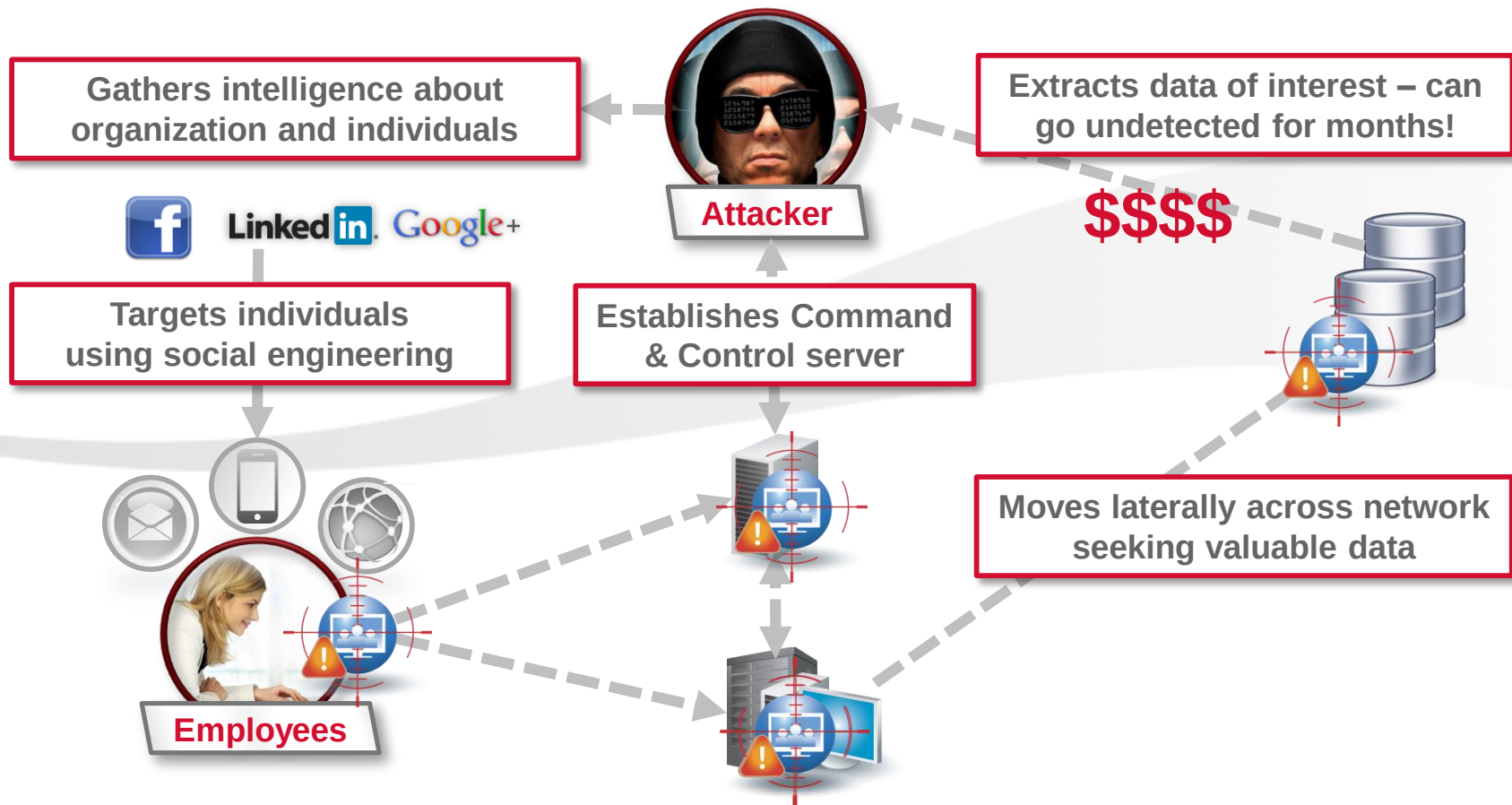
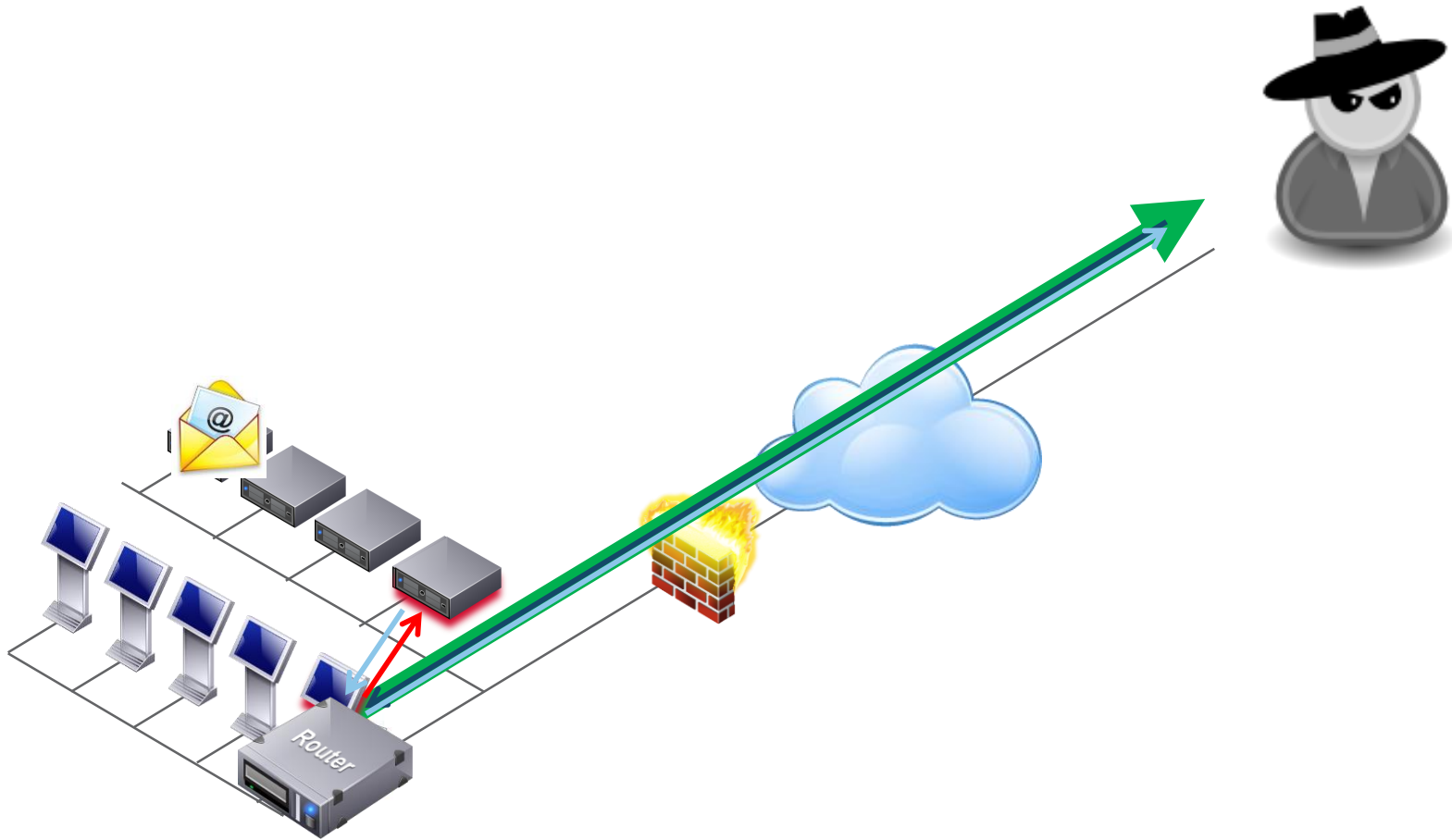


De l'hameçonnage ciblé à la compromission totale du domaine : Démonstration, état des lieux et comment le principe de la résilience peut aider à limiter les impacts

Johanne Ulloa
@julloa

Les phases d'une attaque ciblée





Cible : Omer Simpson

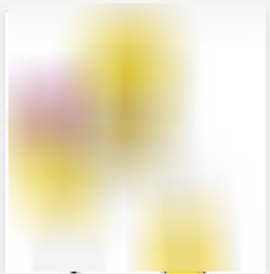


Reconnaissance



Home Profile Connections Jobs Interests

Free IAM Analyst Report - Ovum report points to Hitachi ID as vendor with best custo



Omer Simpson
—
France | Fishery
Current Sofa
[Send Omer InMail](#) 
0 connections

  <https://fr.linkedin.com/in/omer-simpson-3818ba81>

Background

 Experience
Donuts eater
Sofa
December 1963 – Present (52 years 2 months)

Following

Demo Time

IF ANYTHING
CAN
GO WRONG

IT WILL !

--

MURPHY'S LAW

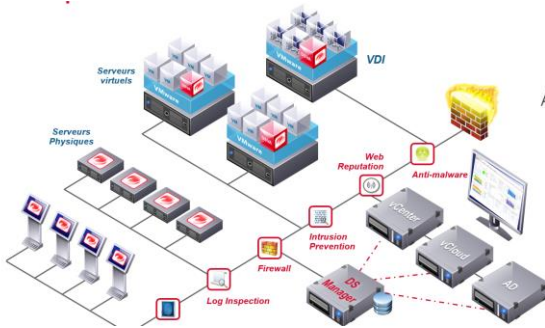
Etat des lieux

- Environnements IT complexes



Etat des lieux

- Démultiplication de la surface d'exposition



Etat des lieux

- Données dispersées

Consumerization

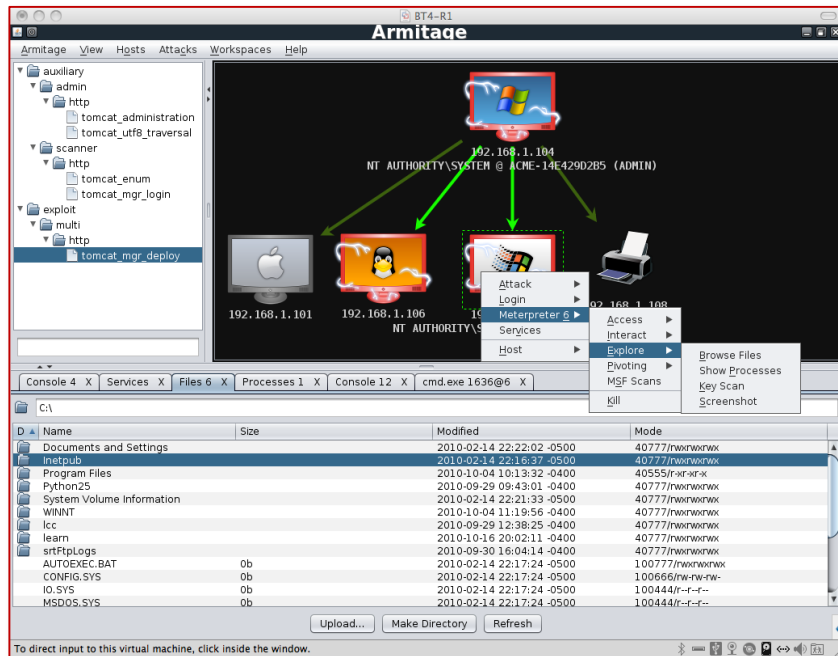


Cloud



Etat des lieux

- Professionnalisation des attaquants



Etat des lieux

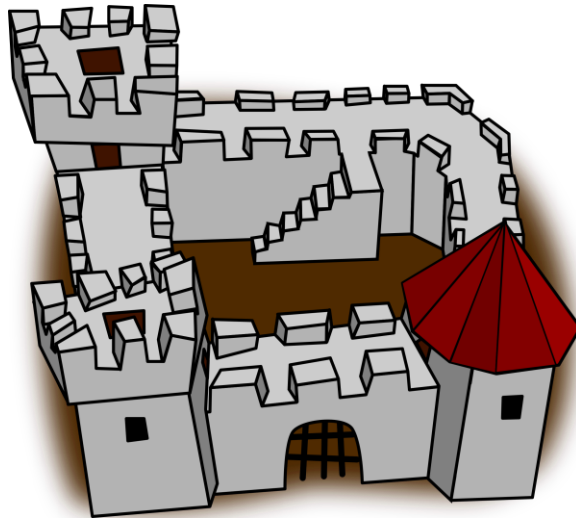
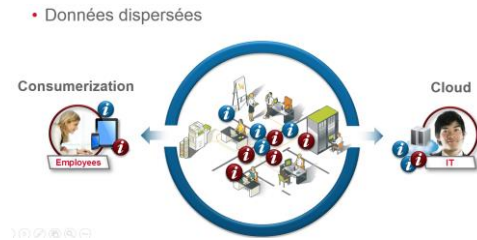
- Contournement des moyens de défense traditionnels



La personnalisation est rentable pour les attaquants



Citadelle



Résilience

- L'impact va inévitablement survenir
- L'impact va altérer nos capacités
- => Reprendre une activité normale le plus rapidement possible



Classification des données



Détection



Réponse à incident



Résilience : Pourquoi ?

- ✓ Diminuer les risques de fraude
- ✓ Préserver l'image de votre entreprise



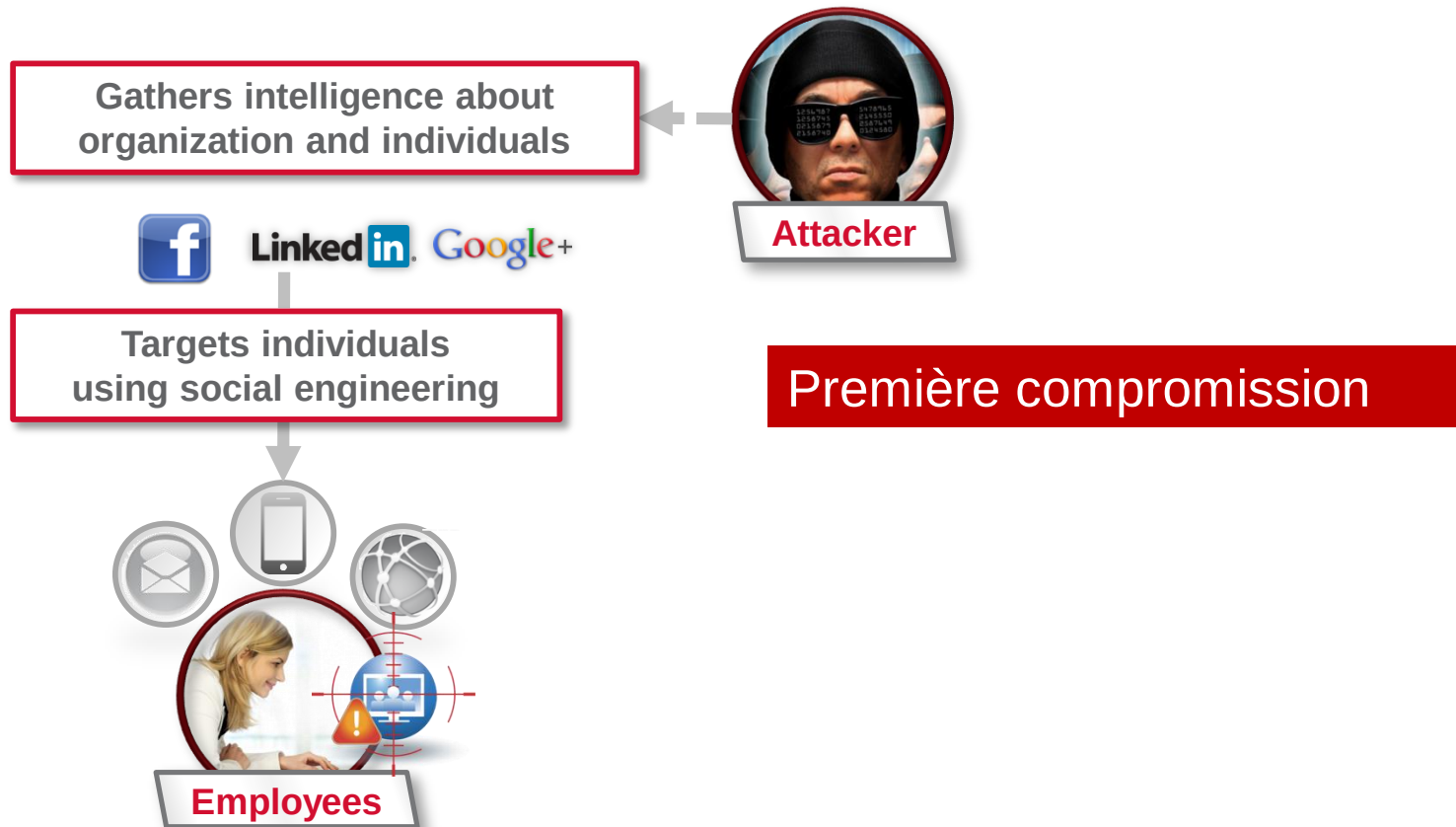
- ✓ Préserver votre capital informationnel (Espionnage et/ou divulgation)



- ✓ Préserver la disponibilité des données (Ransomware)



Détection première compromission



Principe de l'analyse statique

USC Administrative Operations



Department of Public Safety
A Division of Administrative Operations

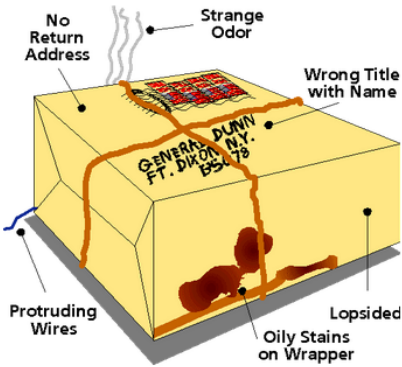
Enter keyword »

[Home](#)
[Message from the Chief](#)
[About Us](#)
[Clery Compliance](#)
[Crime Prevention](#)
[Crime Stats](#)
[FAQ](#)
[Services](#)
[Contact Us](#)
[In Remembrance of Keith and Monica](#)
[Sept 11th Memorial Installation Ceremony](#)

Quick links

- ▶ [Annual Security Report](#)
- ▶ [Bias Reporting](#)
- ▶ [Daily Incident Log](#)
- ▶ [DPS Facebook](#)

Bombs and Bomb Threats
LETTER AND PACKAGE BOMBS



The diagram shows a yellow rectangular box representing a package. Several red lines and dots indicate warning signs: a red dot at the top left labeled 'No Return Address'; a red dot at the top center labeled 'Strange Odor'; a red dot at the top right labeled 'Wrong Title with Name'; a red dot at the bottom left labeled 'Protruding Wires'; a red dot at the bottom center labeled 'Oily Stains on Wrapper'; and a red dot at the bottom right labeled 'Lopsided'. The box has a red label that reads 'GENERAL DUNN, NY. FT. DIXON, N.Y. 178'. The box is shown from a three-quarter perspective, with a red line running along the top edge and another red line running along the bottom edge.

Typical characteristics of a mail or package bomb.

Programs

- Active Shooter Training
- Adopt-a-Hall
- DPS Cadets
- Greek Liaison
- Protect Your Laptop

[more](#)

Links

- Campus Access Policy
- Trojans Alert
- Bicycle Policy
- Lost & Found
- Gone But Not Forgotten

[more](#)

Online Forms

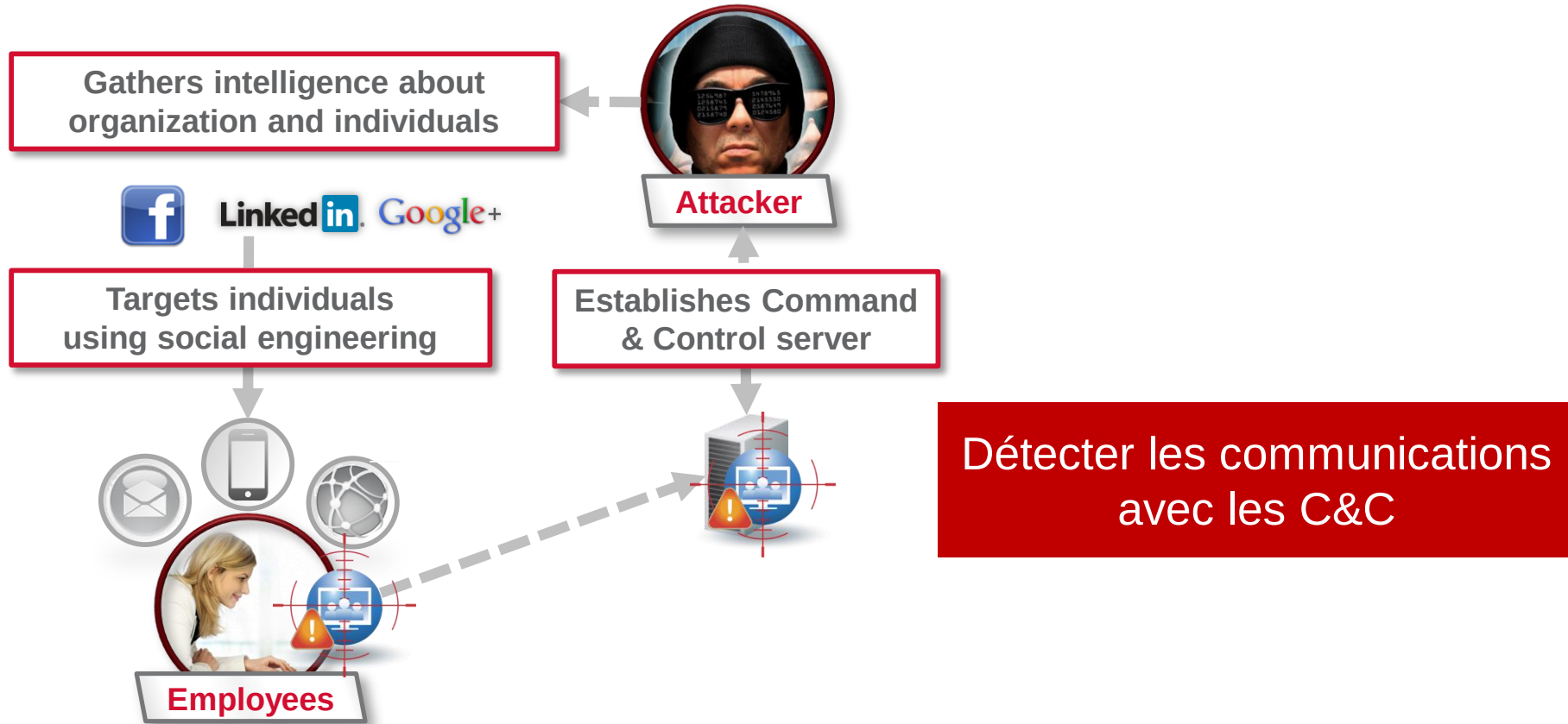
- Bicycle Registration
- Commendation Form
- Complaint Form
- Silent Witness
- TC4T

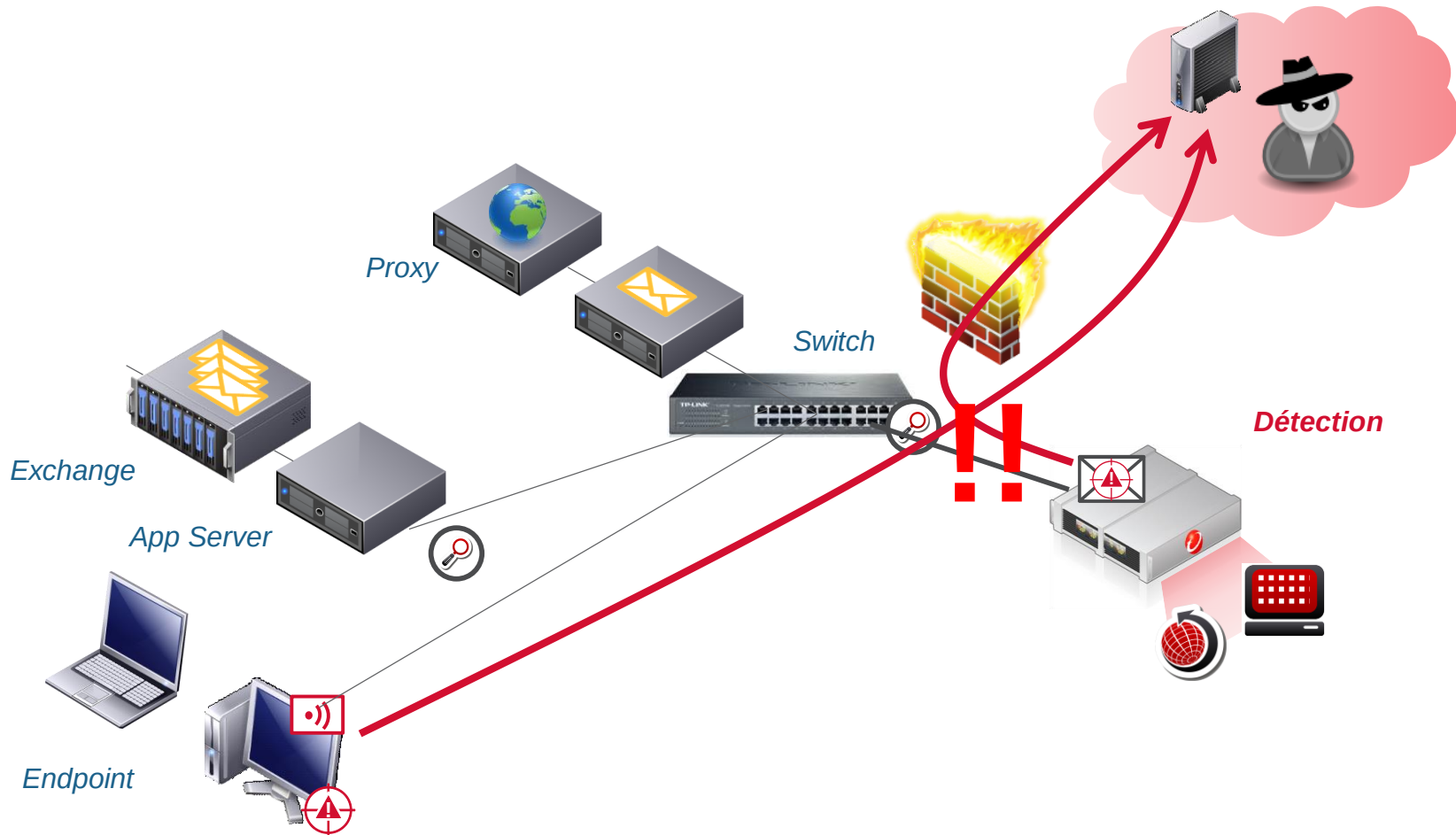
[more](#)

Principe de l'analyse dynamique

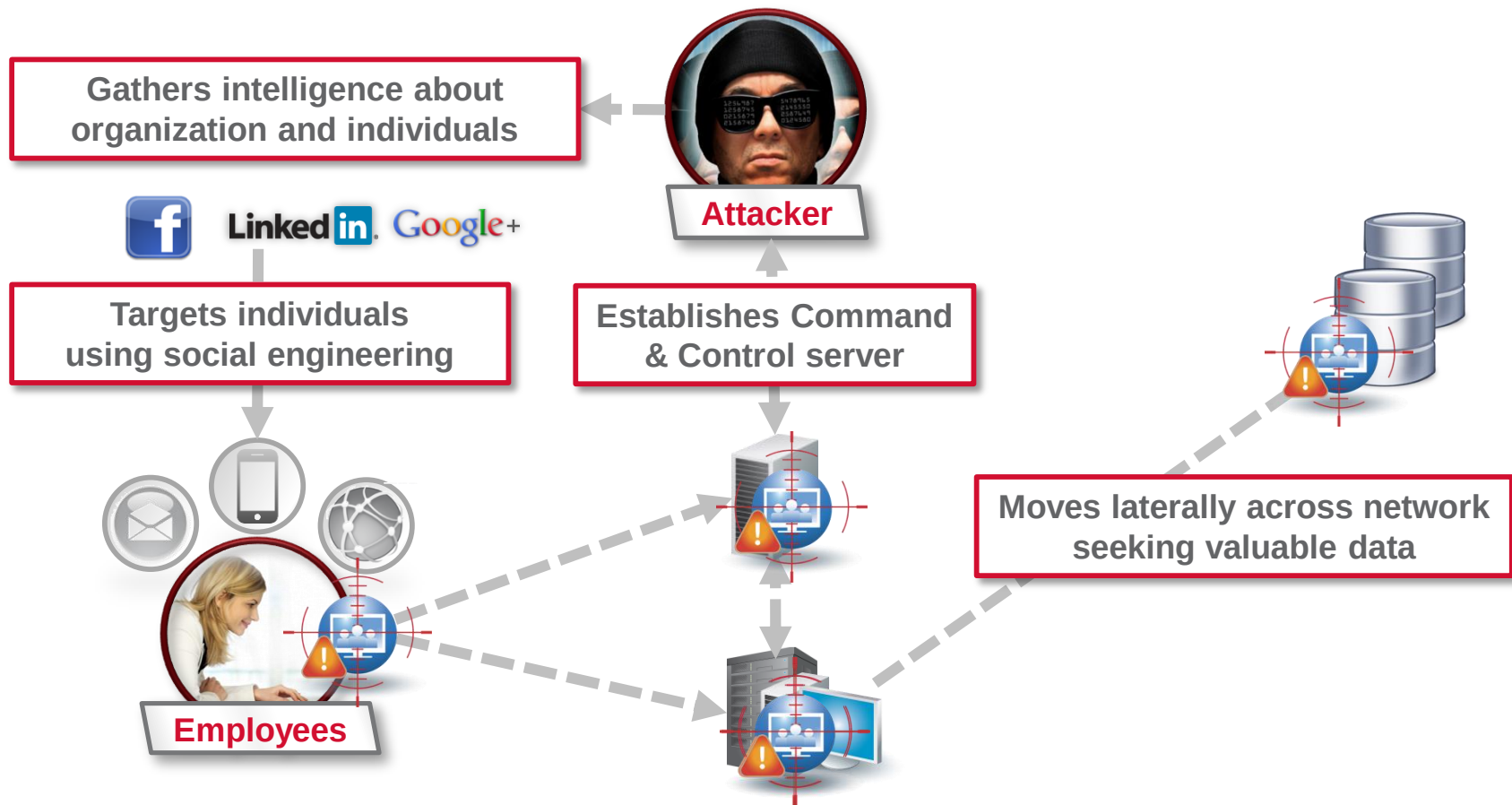


Détection des communications avec les C&C





Détection des mouvements latéraux



Mouvements latéraux

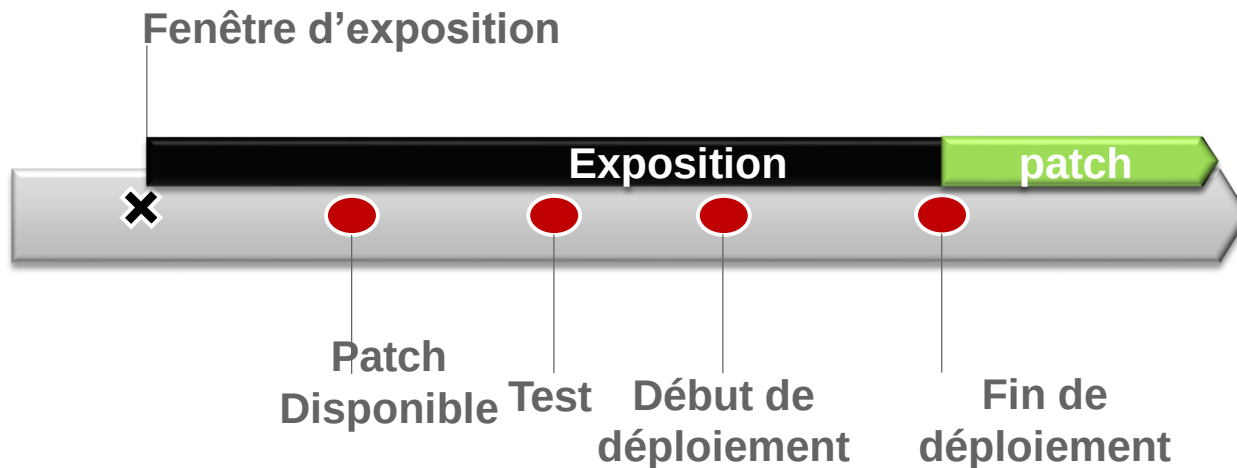
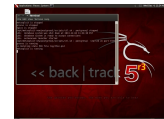
- Détection des exploitations de vulnérabilités
- Comportements suspects :
 - Usages d'outils utilisés lors d'attaques
 - Connexions avec le réseau TOR
 - Upload de fichiers
 - Réponse volumineuse de bases de données
 - Drop de fichiers sur des partages administratifs
 - ...



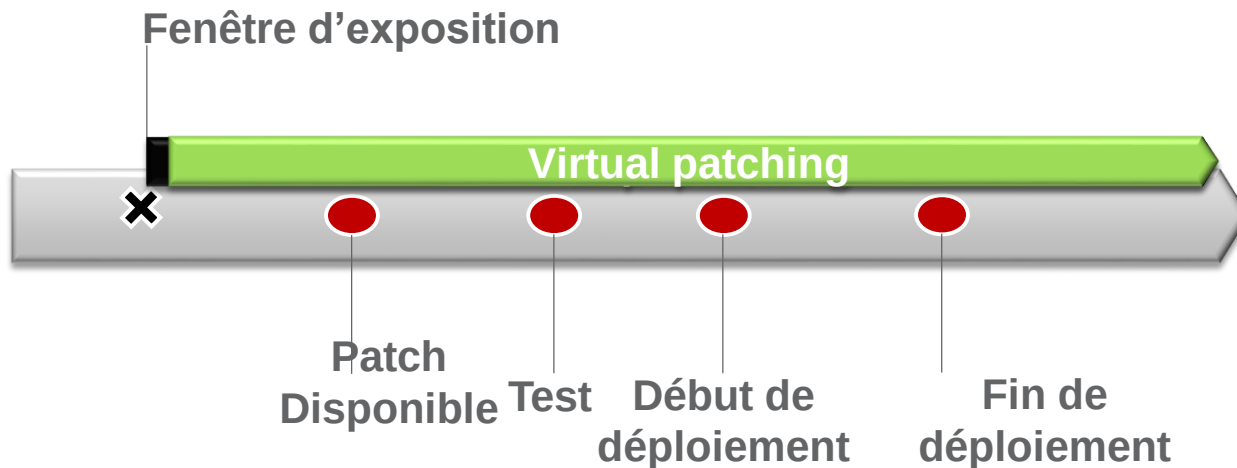
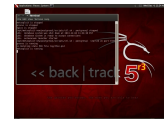
Résister aux exploitations de vulnérabilités



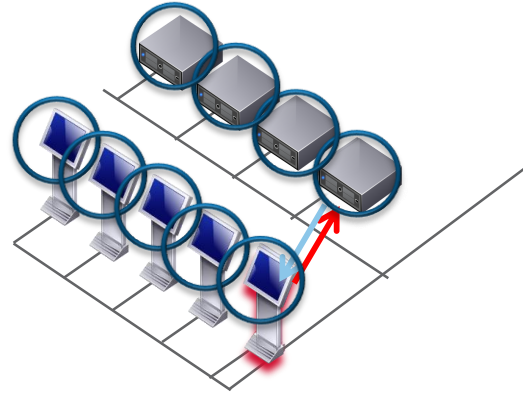
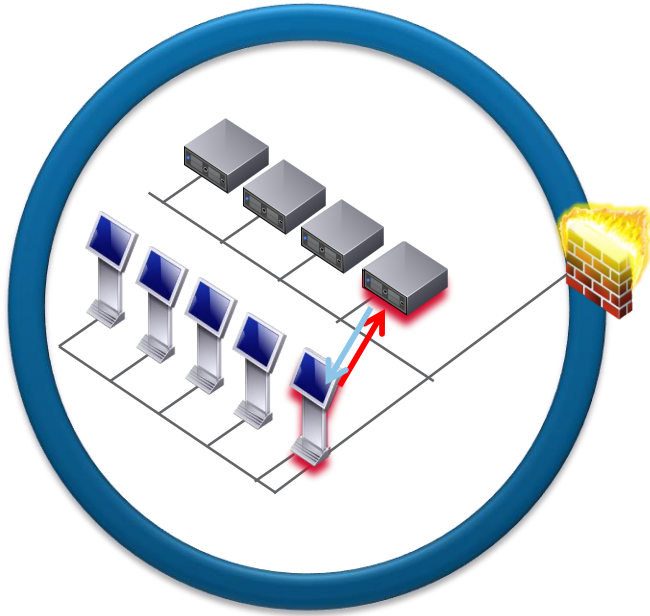
Exploitation de vulnérabilités



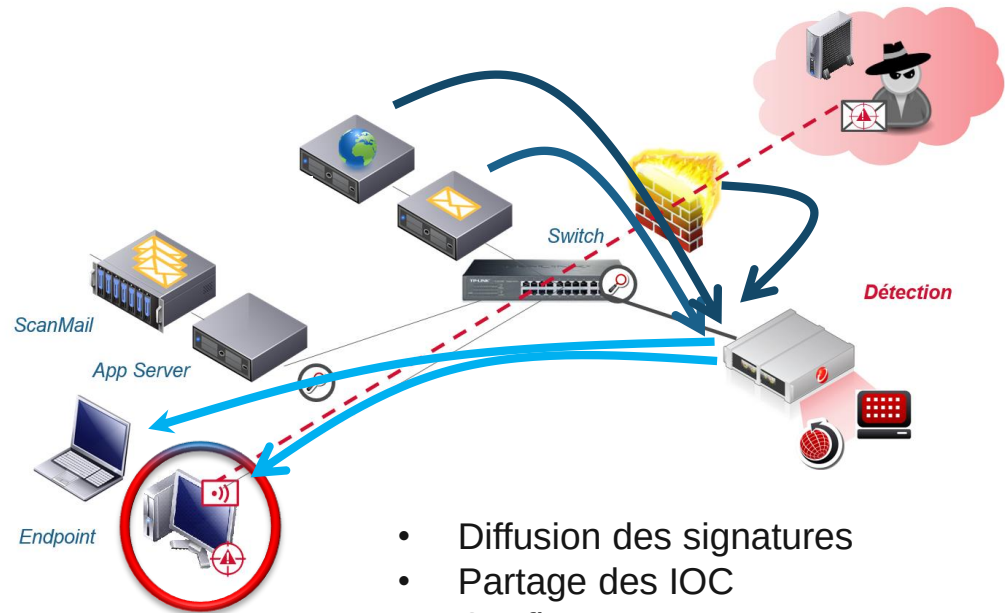
Exploitation de vulnérabilités



IPS - HIPS

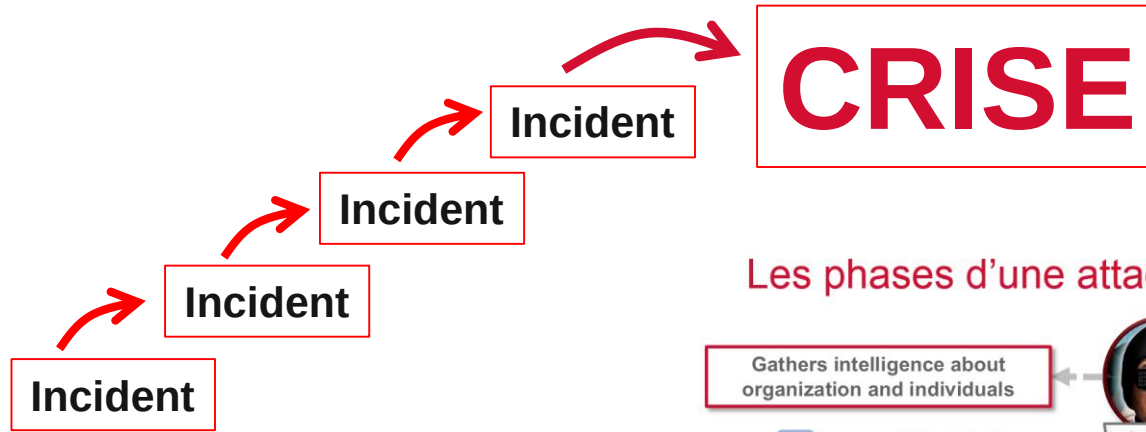


Réponse à incident



- Diffusion des signatures
- Partage des IOC
- Confinement

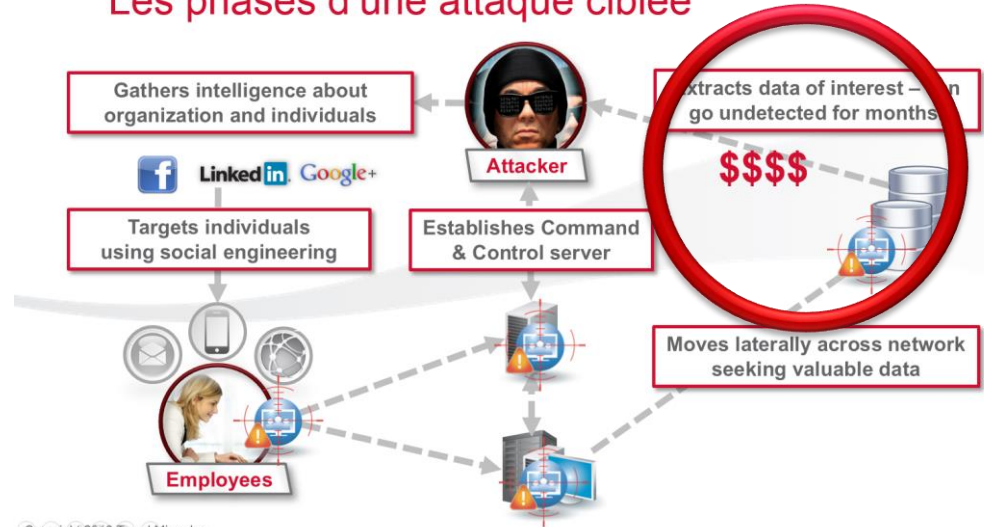
Aspects organisationnels



Préparation

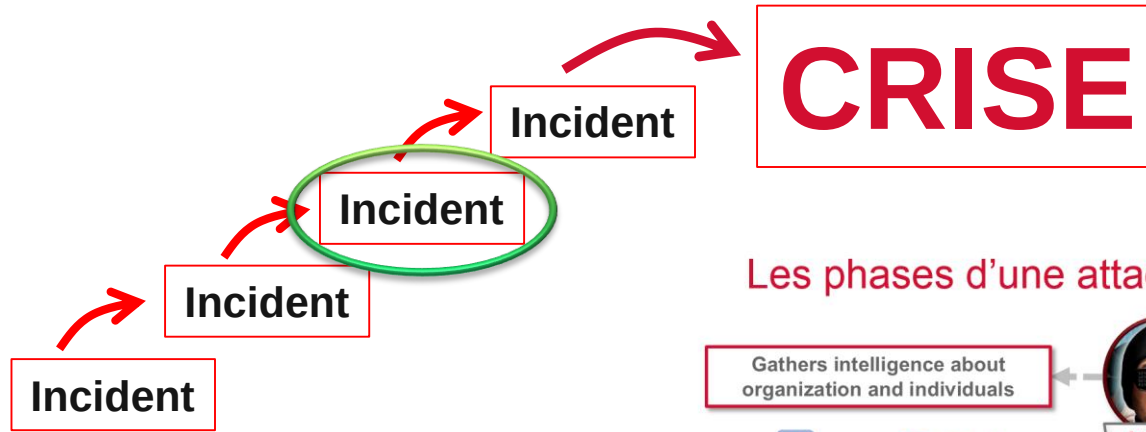
Mise en situation

Les phases d'une attaque ciblée

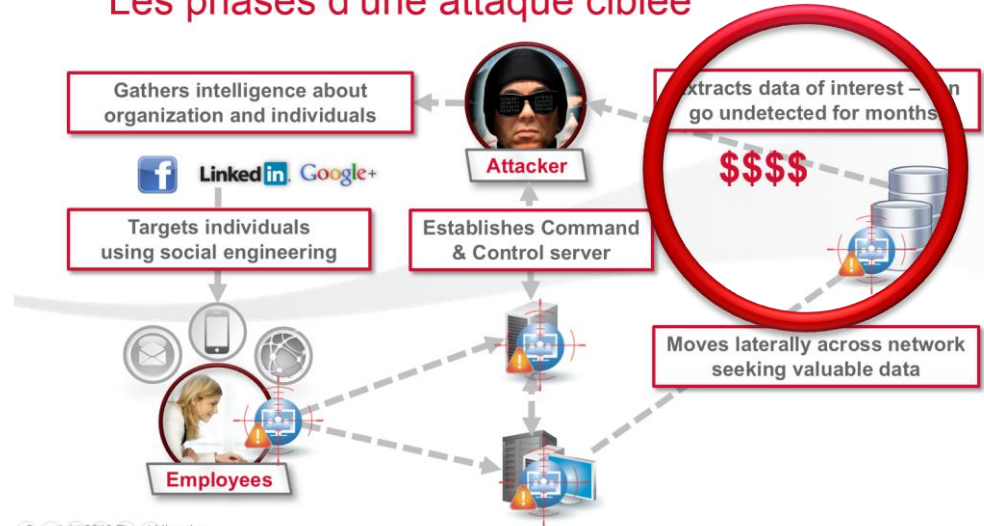


Copyright 2013 Trend Micro Inc.

Aspects organisationnels

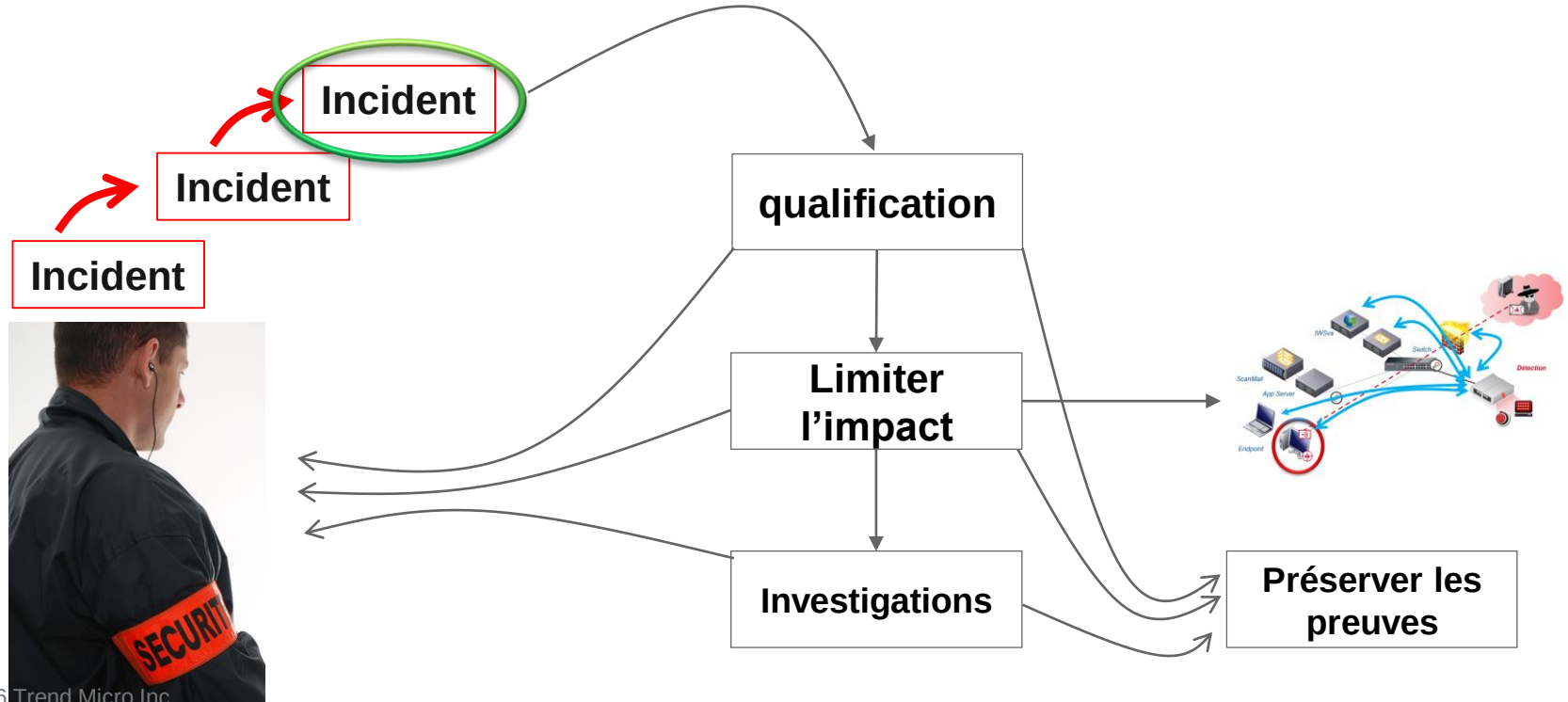


Les phases d'une attaque ciblée

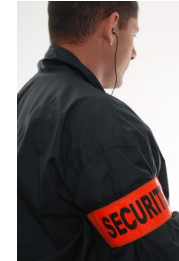
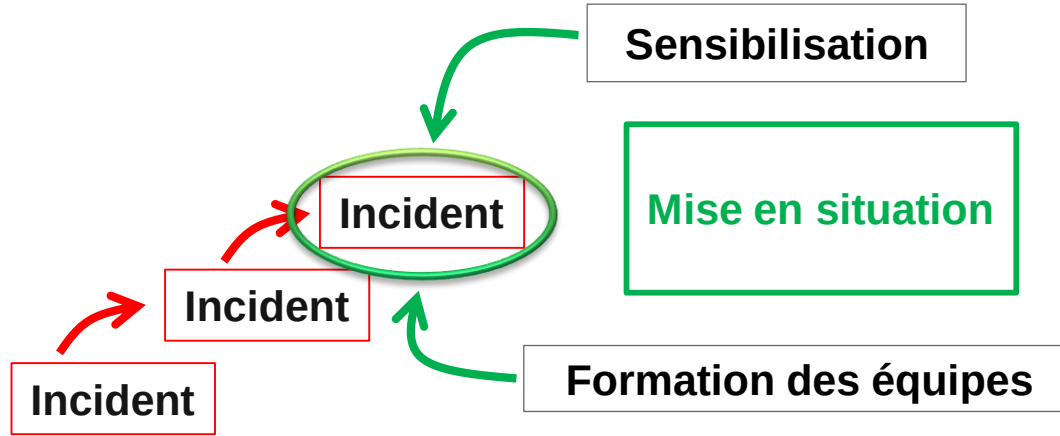


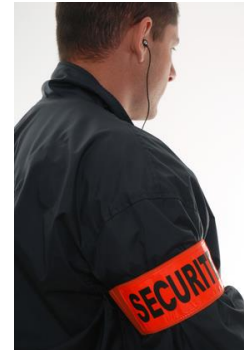
Copyright 2013 Trend Micro Inc.

Aspects organisationnels



Aspects organisationnels





Merci

Johanne Ulloa
@julloa