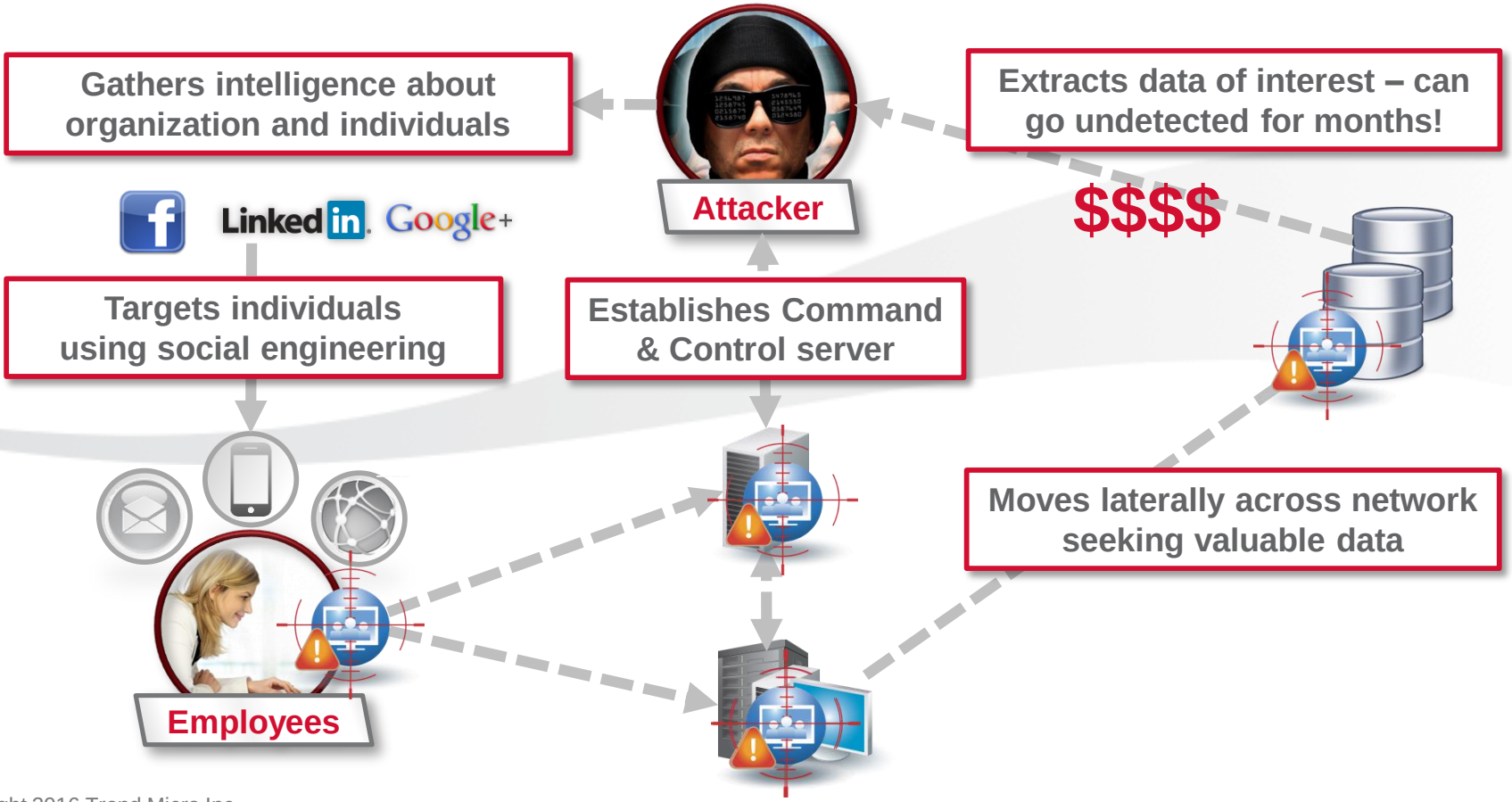
TREND MICRO

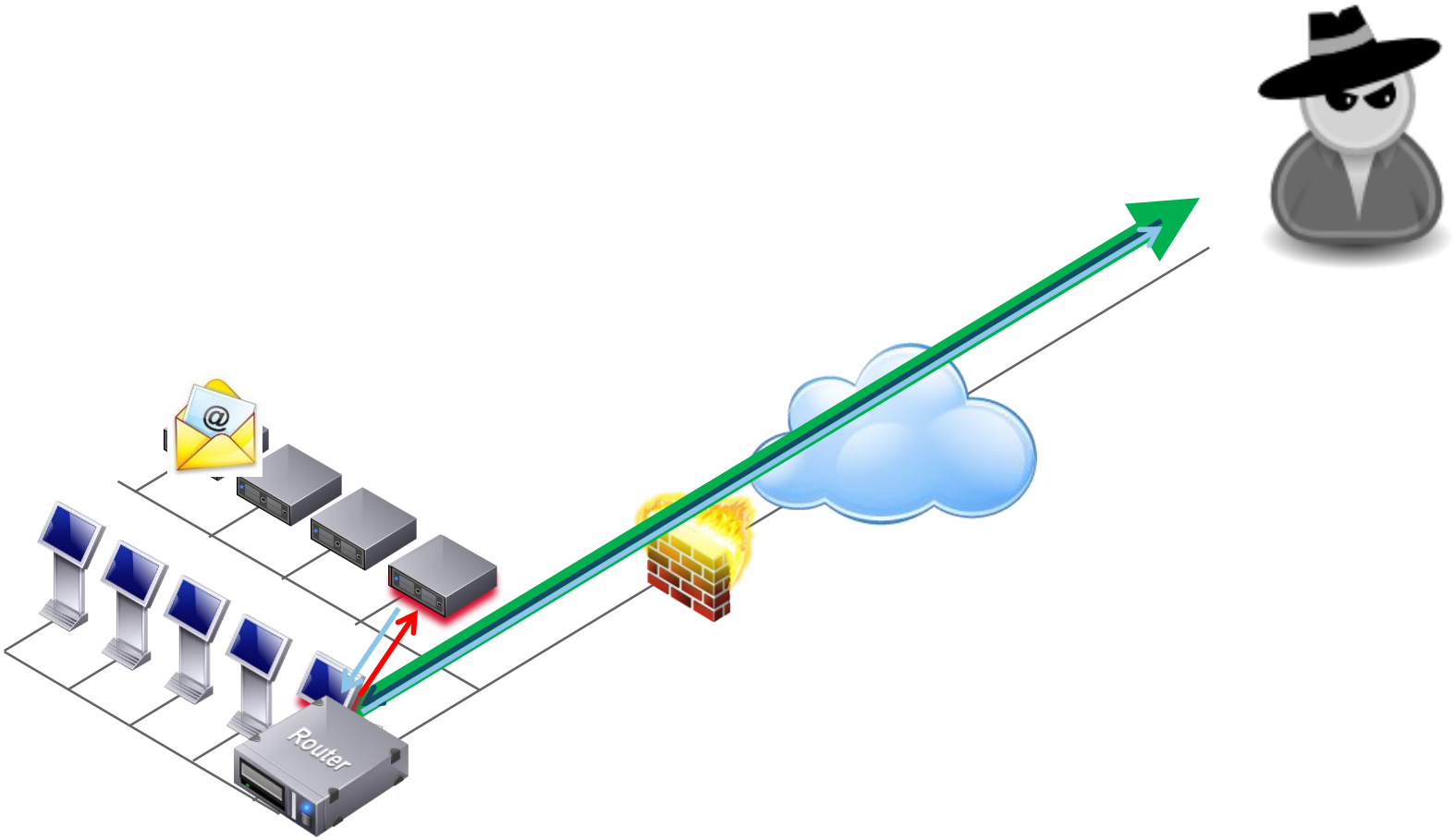
Securing Your Journey to the Cloud

# 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

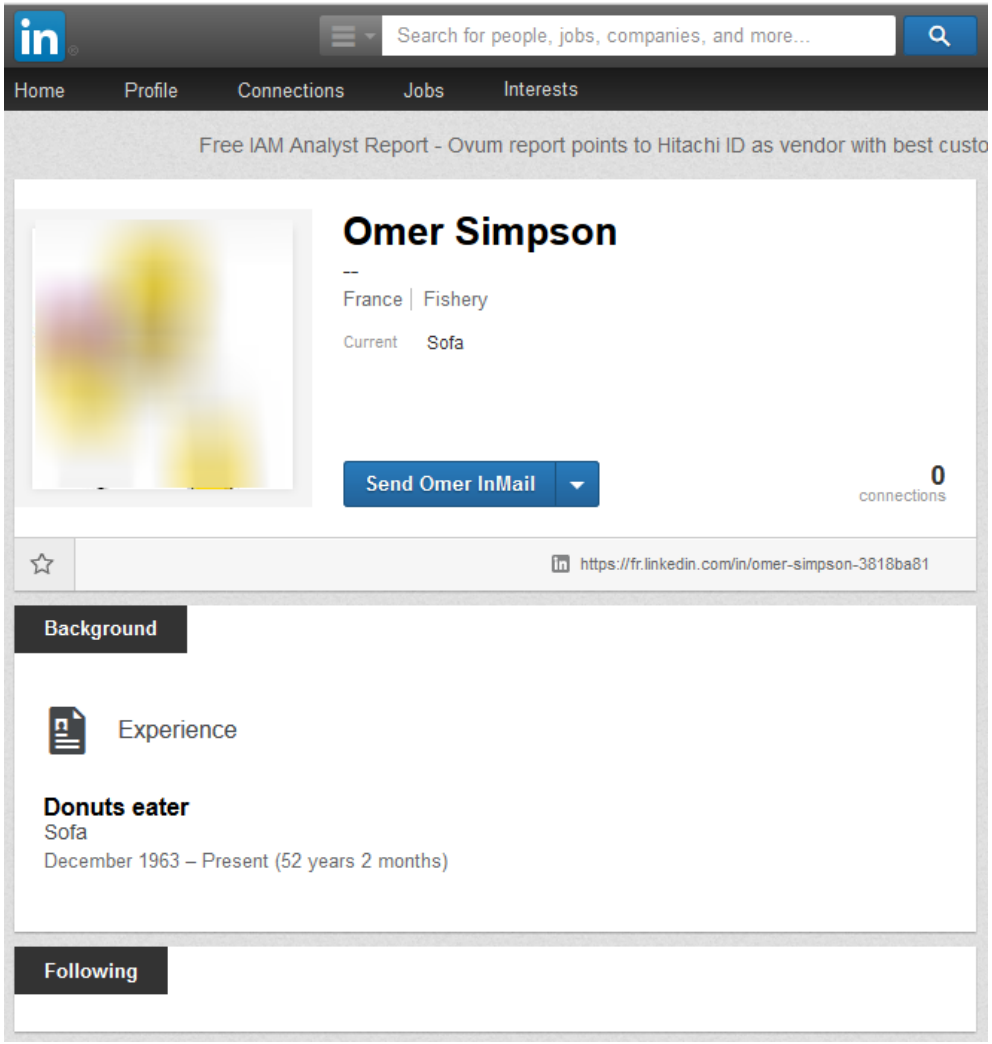
# Les phases d'une attaque ciblée





# Cible : Omer Simpson

# Reconnaissance



# Demo Time

IF ANYTHING
CAN
GO WRONG

**IT WILL !**

--

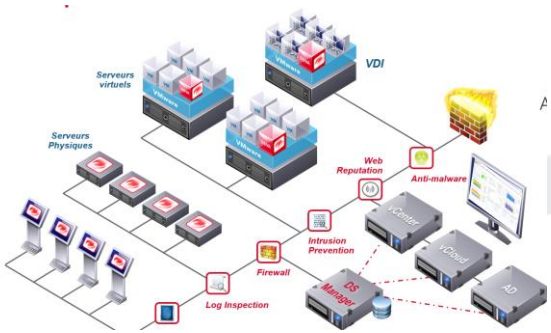
MURPHY'S LAW

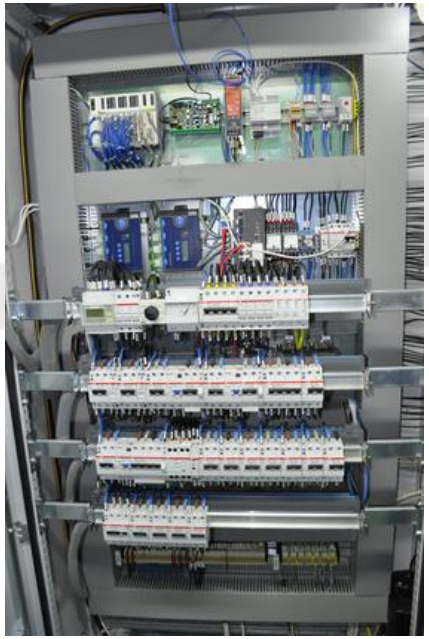
# Etat des lieux

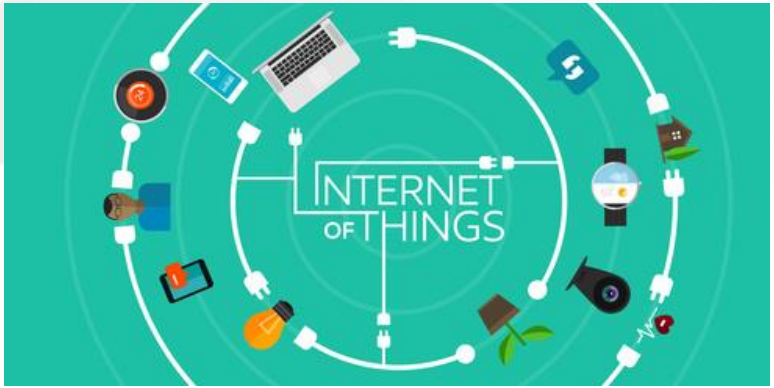
- Environnements IT complexes

# Etat des lieux

- Démultiplication de la surface d’exposition

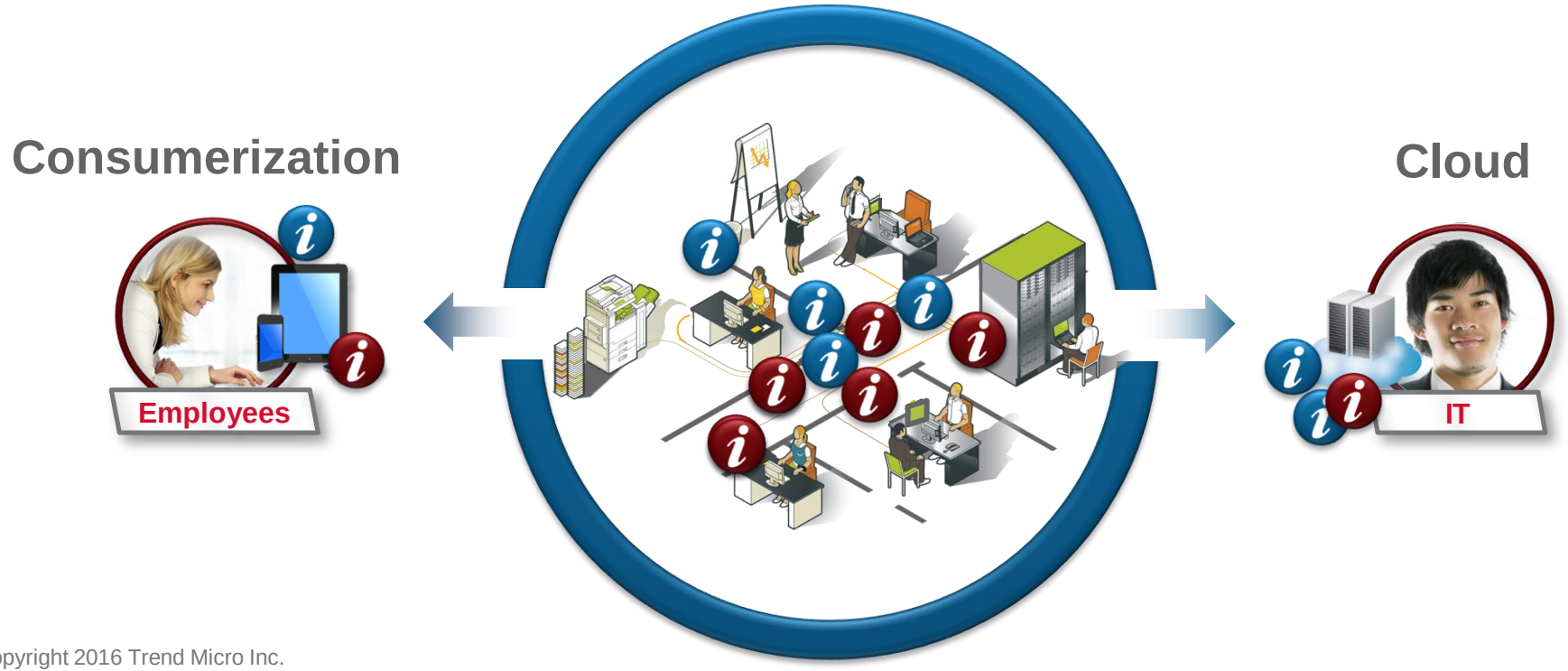




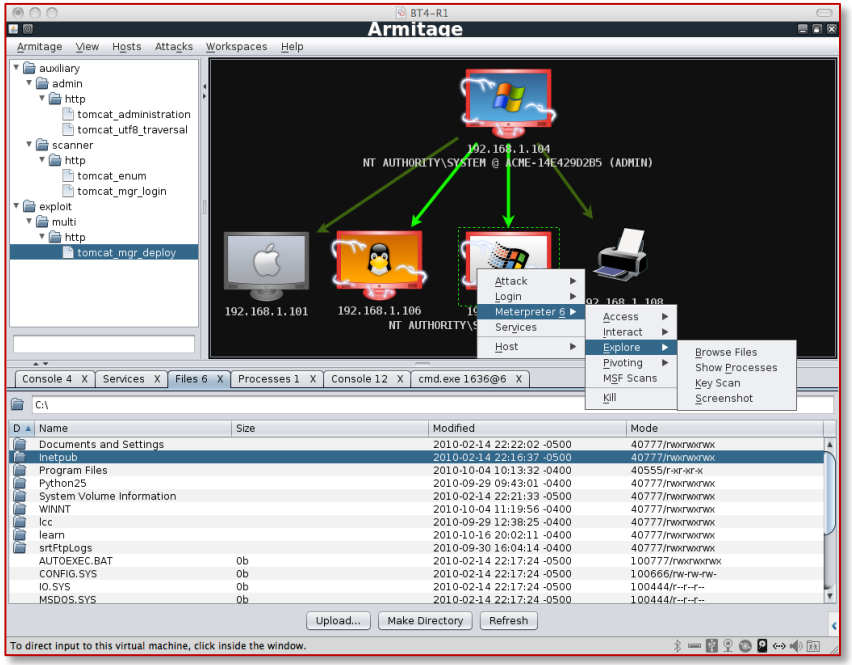
# Etat des lieux

- Données dispersées



# Etat des lieux

- Professionnalisation des attaquants

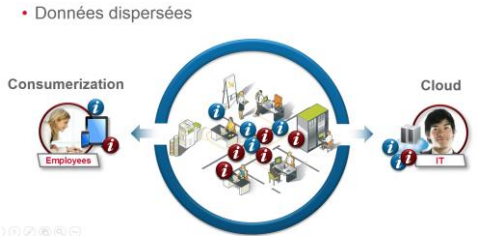


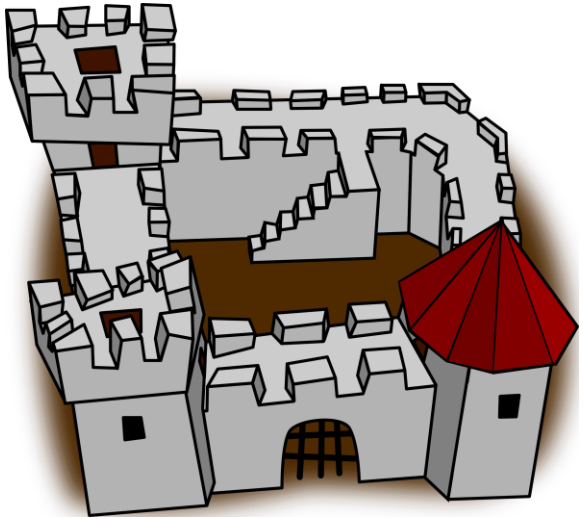
# Etat des lieux

- Contournement des moyens de défense traditionnels

# La personnalisation est rentable pour les attaquants

# Citadelle



# Résilience

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

# Classification des données


# Détection

# Réponse à incident

# Résilience : Pourquoi ?

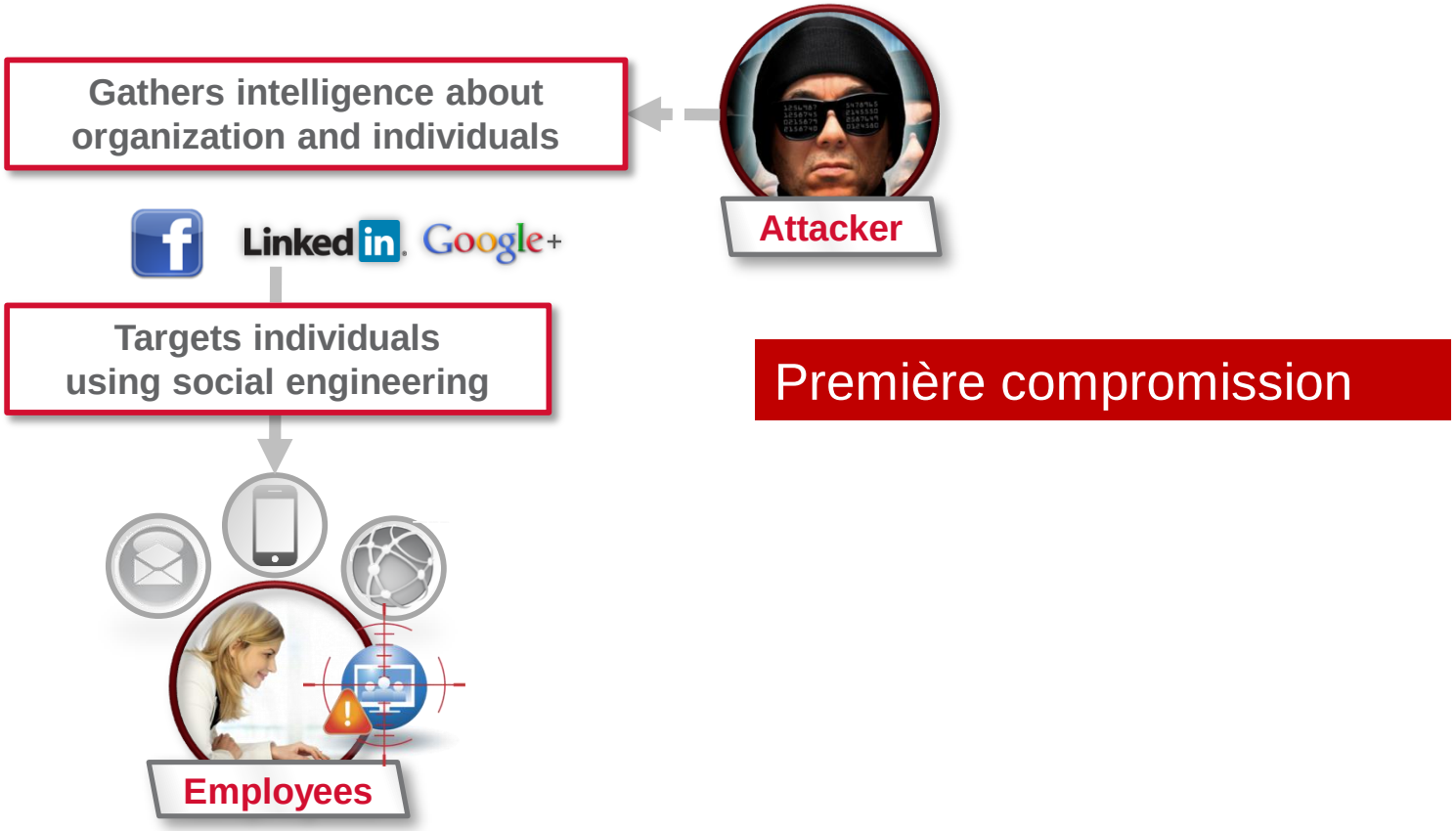
- ✓ Diminuer les risques de fraude
- ✓ Préserver l'image de votre entreprise

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

- ✓ Préserver la disponibilité des données (Ransomware)



# Détection première compromission




Première compromission

# Principe de l’analyse statique

USC Administrative Operations

USC University of Southern California

**Department of Public Safety**

*A Division of Administrative Operations*

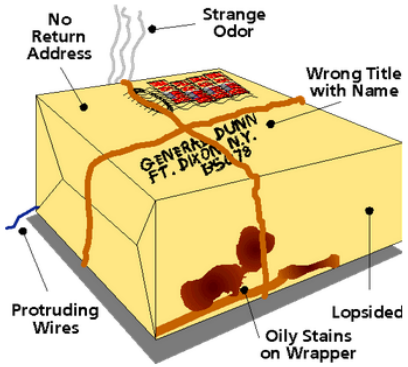
Enter keyword »

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



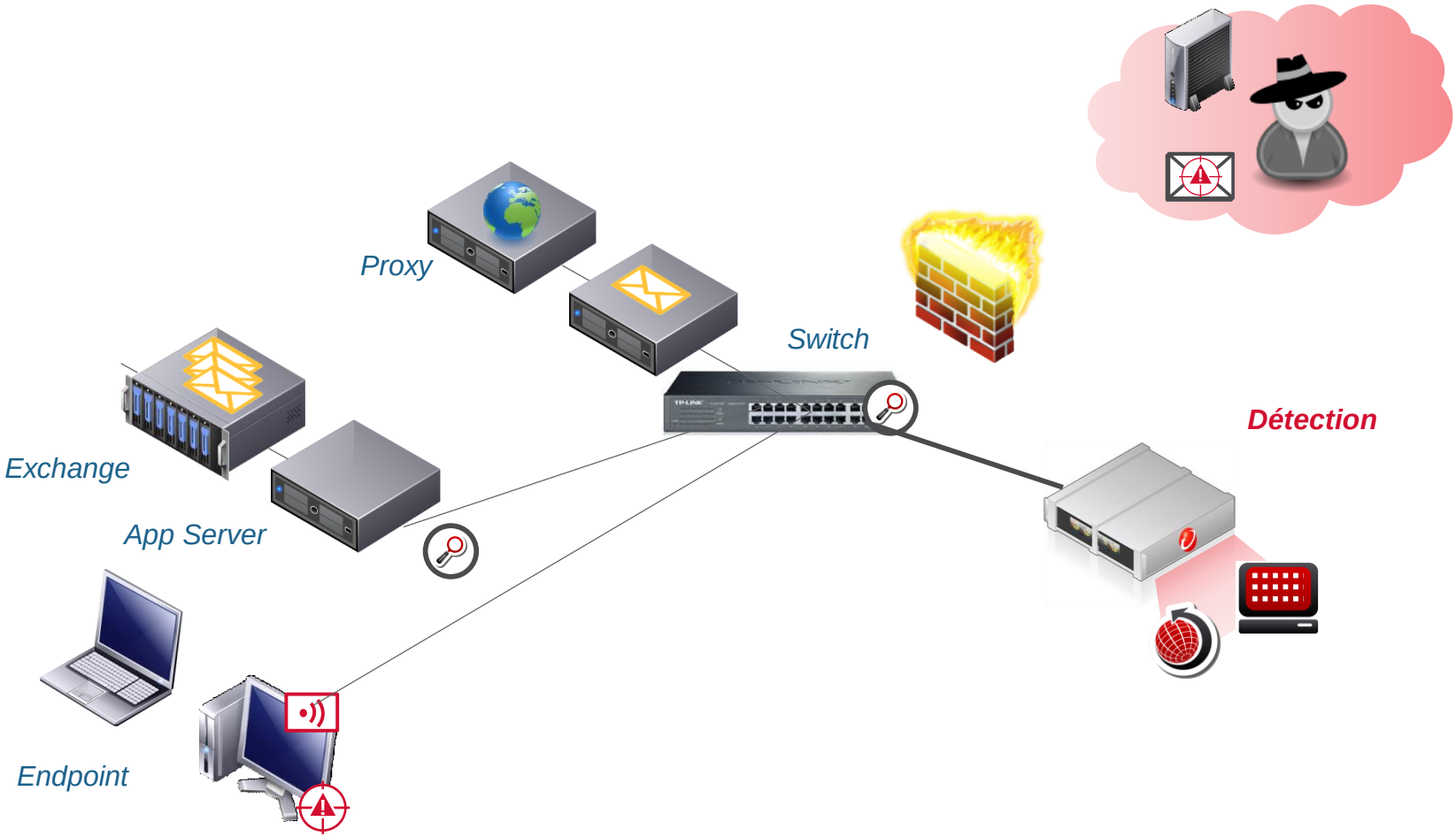

**Typical characteristics of a mail or package bomb.**

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

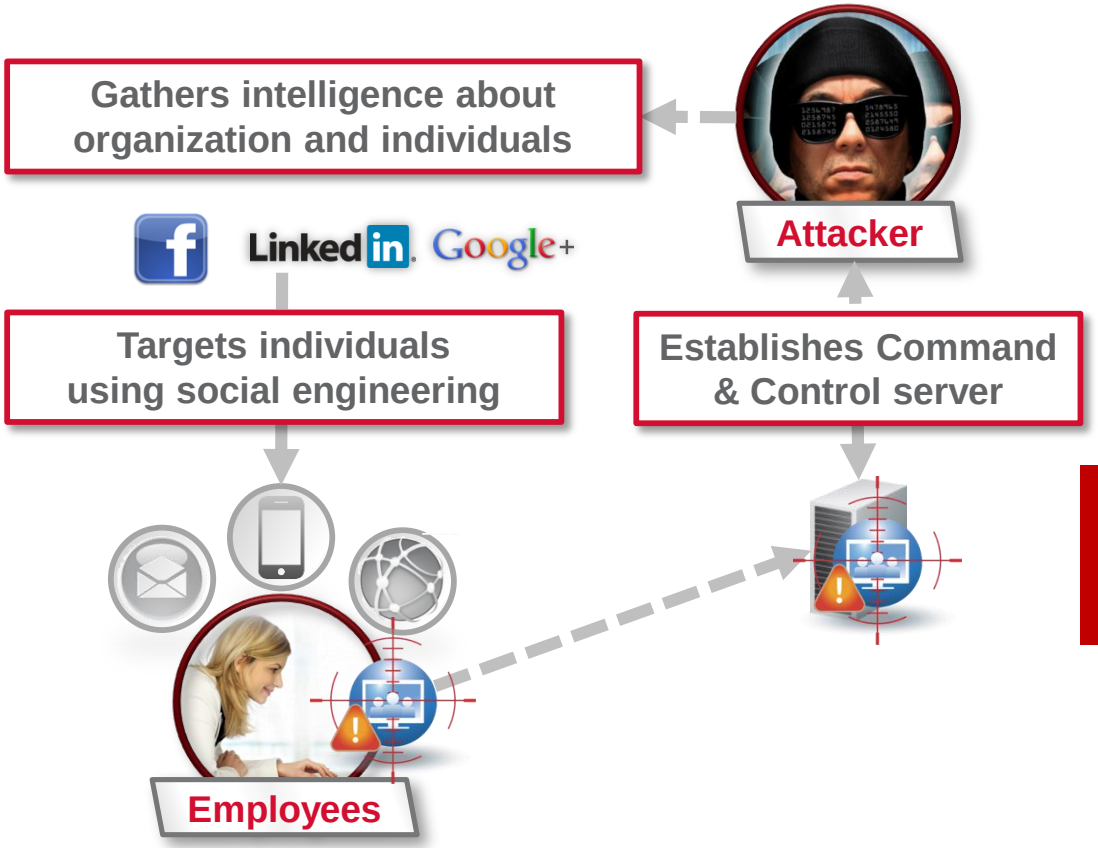
Links
Campus Access Policy
Trojans Alert
Bicycle Policy
Lost & Found
Gone But Not Forgotten
more

Online Forms
Bicycle Registration
Commendation Form
Complaint Form
Silent Witness
TC4T
more

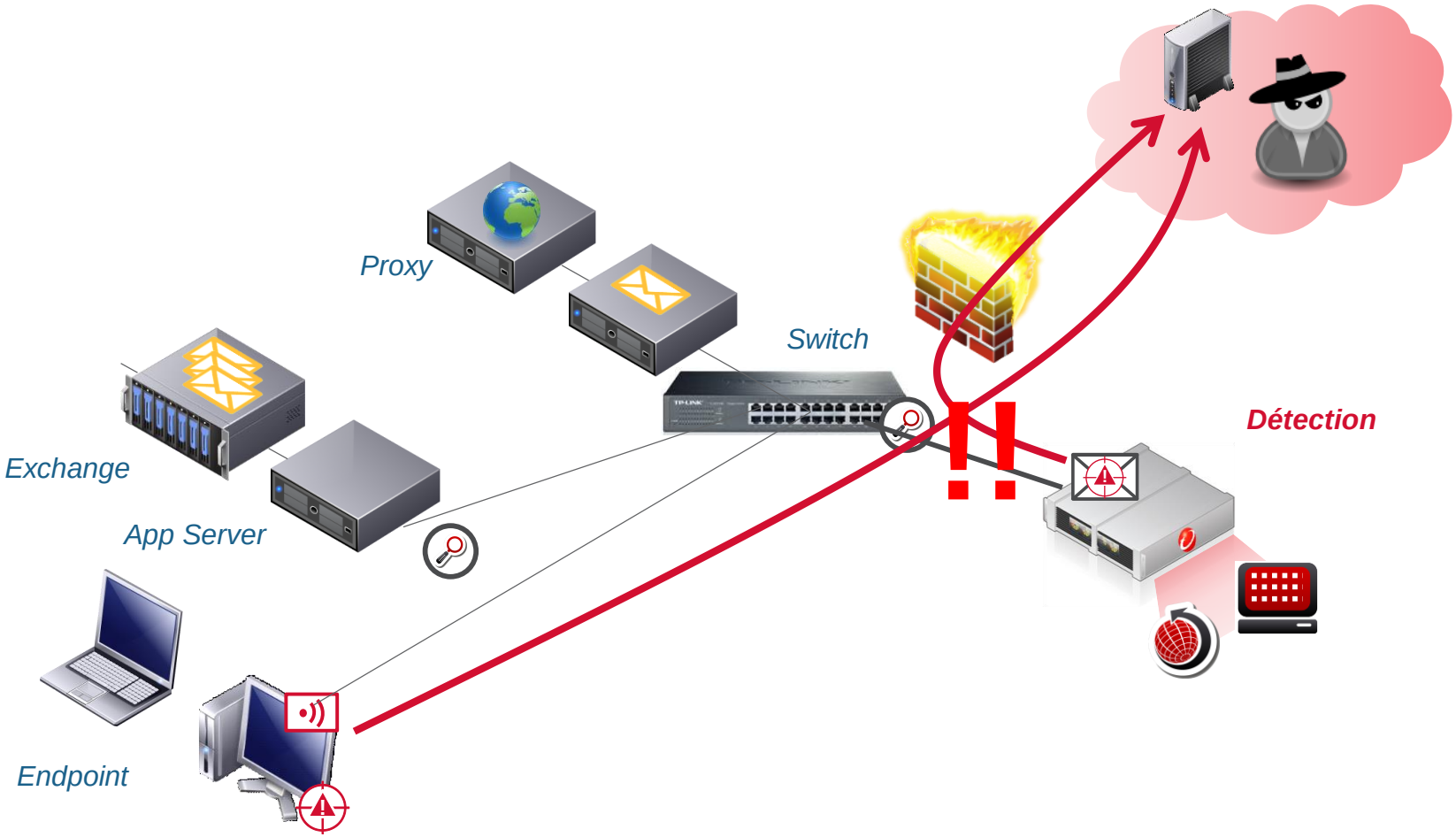
# Principe de l’analyse dynamique



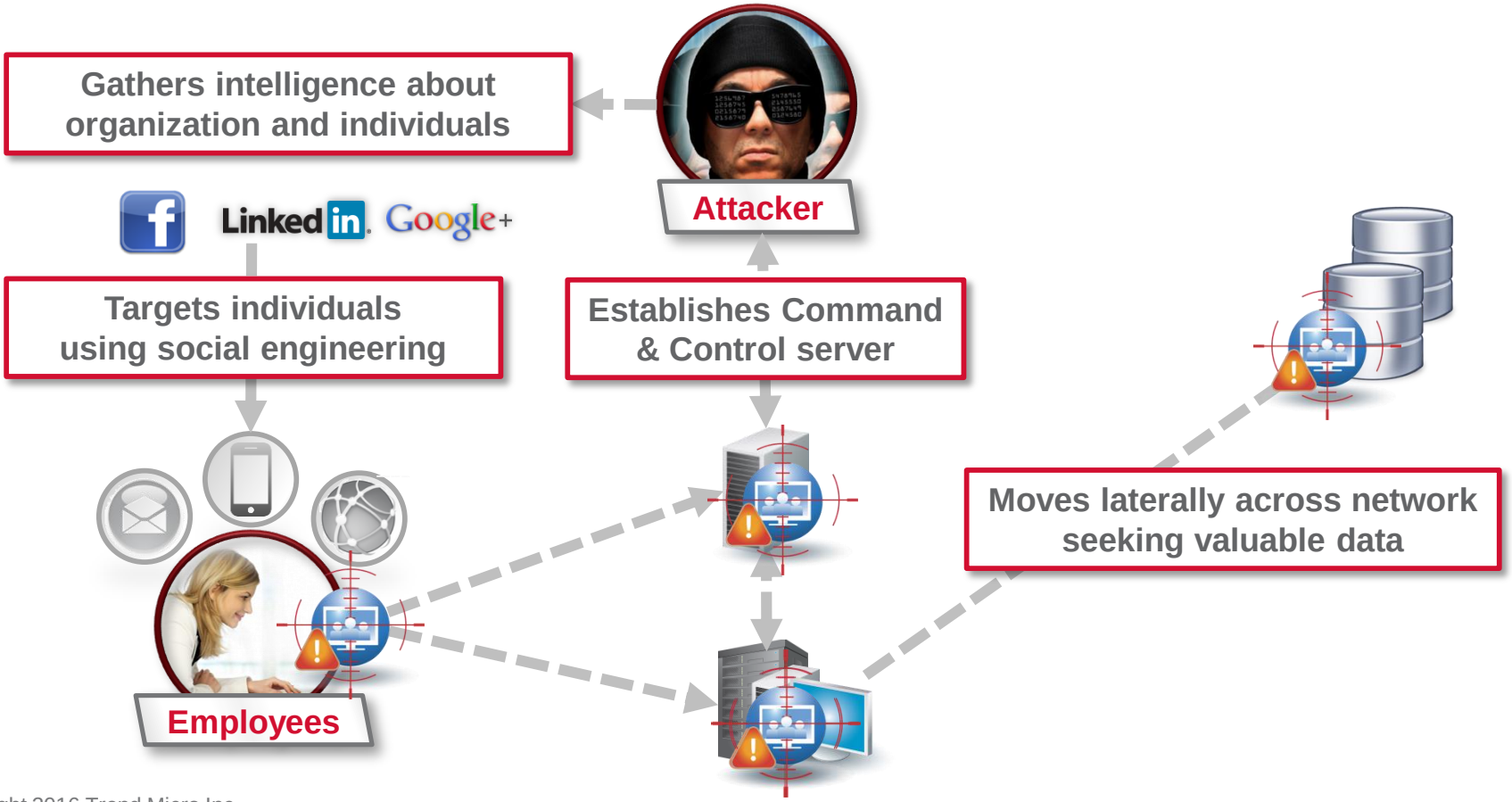
# Détection des communications avec les C&C




Détecter les communications avec les C&C



# Détection des mouvements latéraux

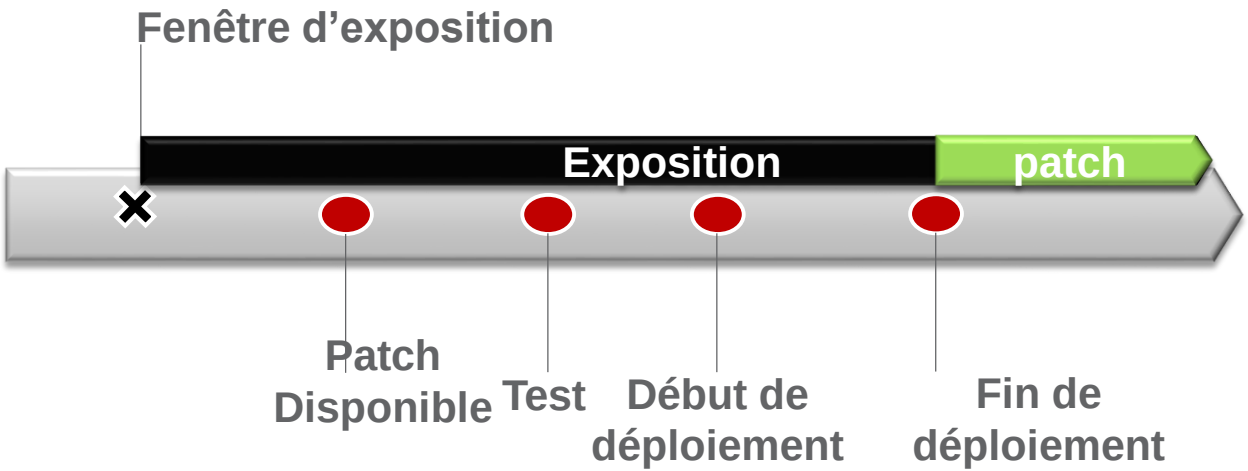


# Mouvements latéraux

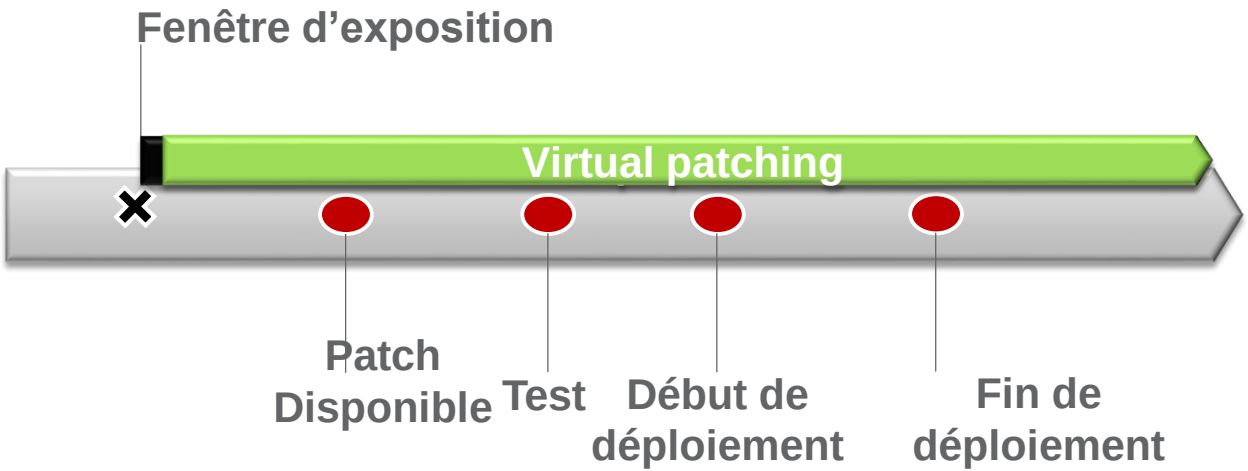
- Détection des exploitations de vulnérabilités
- Comportements suspicieux :
  - Usages d'outils utilisés lors d'attaques
  - Connections avec le réseau TOR
  - Upload de fichiers
  - Réponse volumineuse de bases de données
  - Drop de fichiers sur des partages administratifs
  - …

# Résister aux exploitations de vulnérabilités

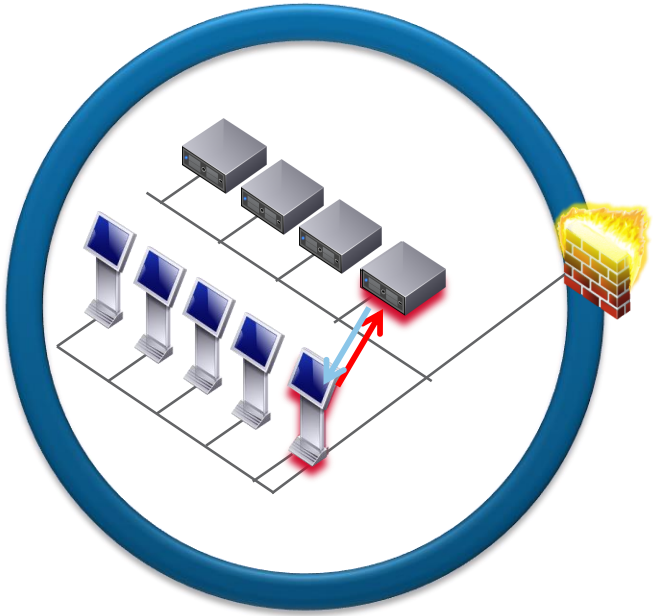
# Exploitation de vulnérabilités

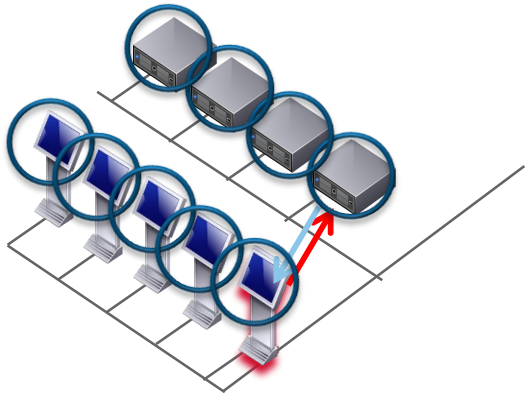



# Exploitation de vulnérabilités

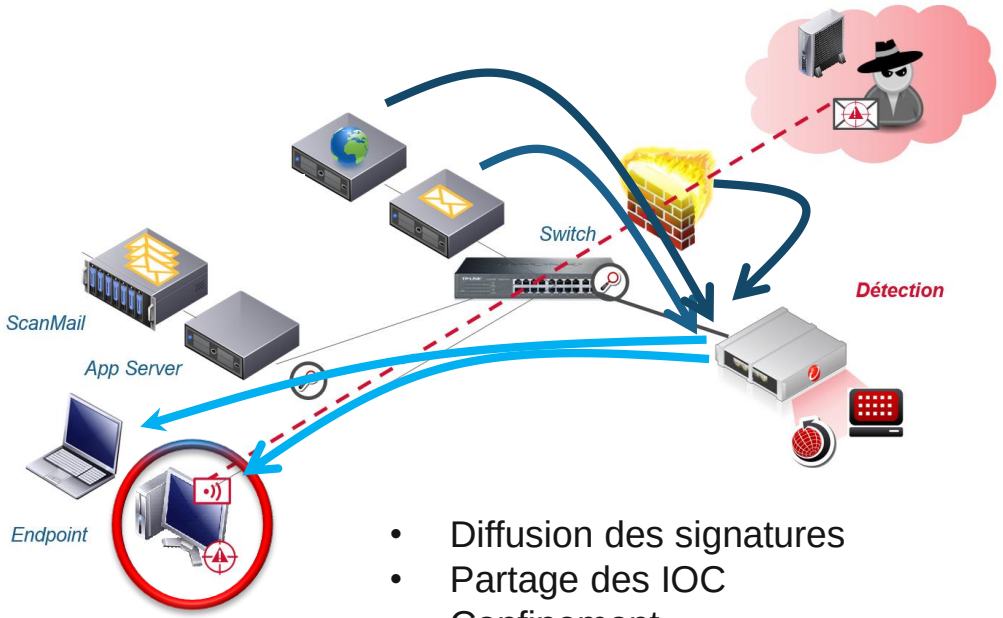



# IPS - HIPS





# Réponse à incident

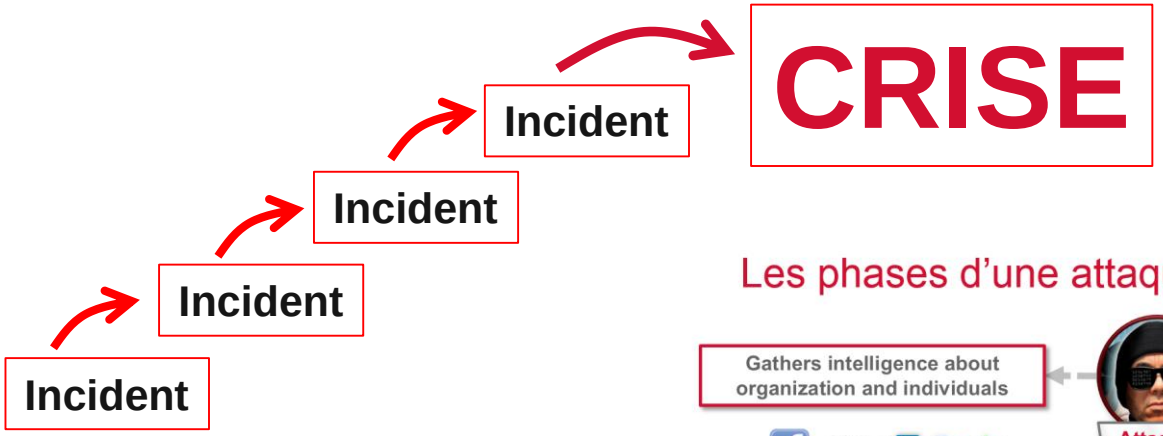



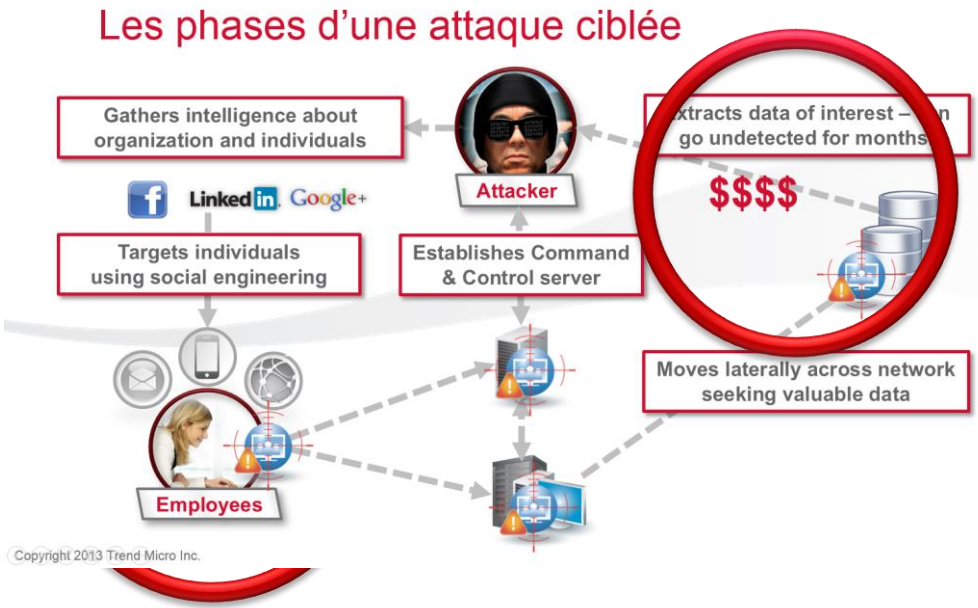

- Diffusion des signatures
- Partage des IOC
- Confinement

# Aspects organisationnels

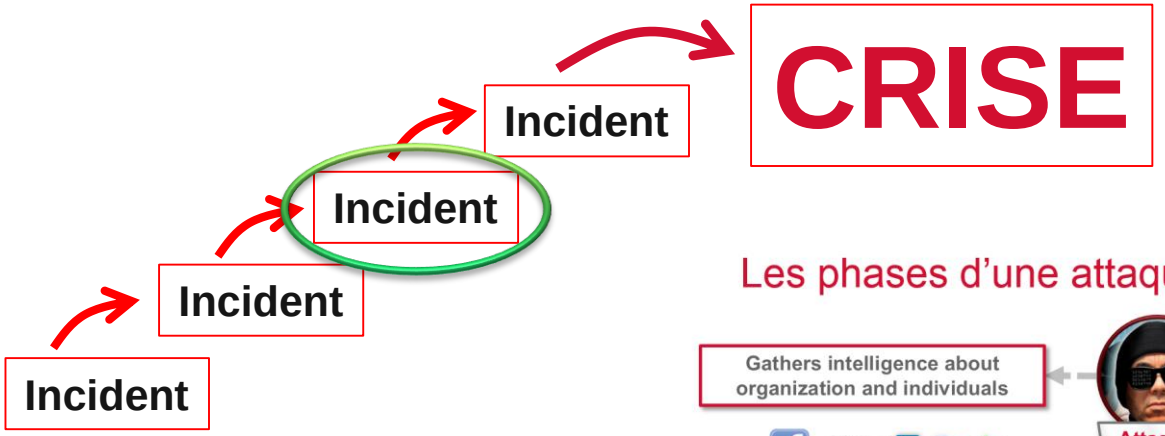
**Préparation**

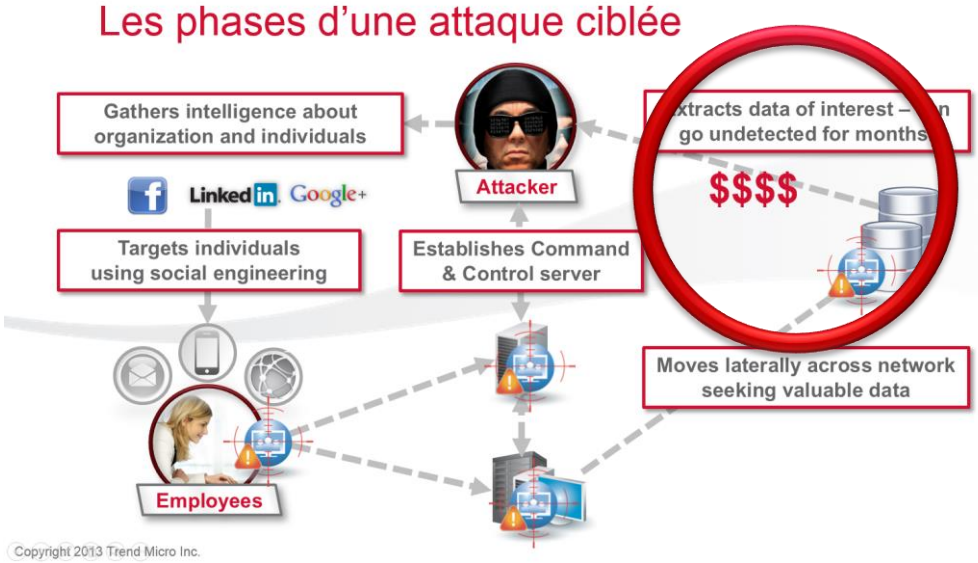
**Mise en situation**



# Aspects organisationnels



# Aspects organisationnels


Incident

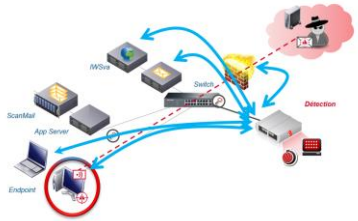
Incident

Incident

qualification

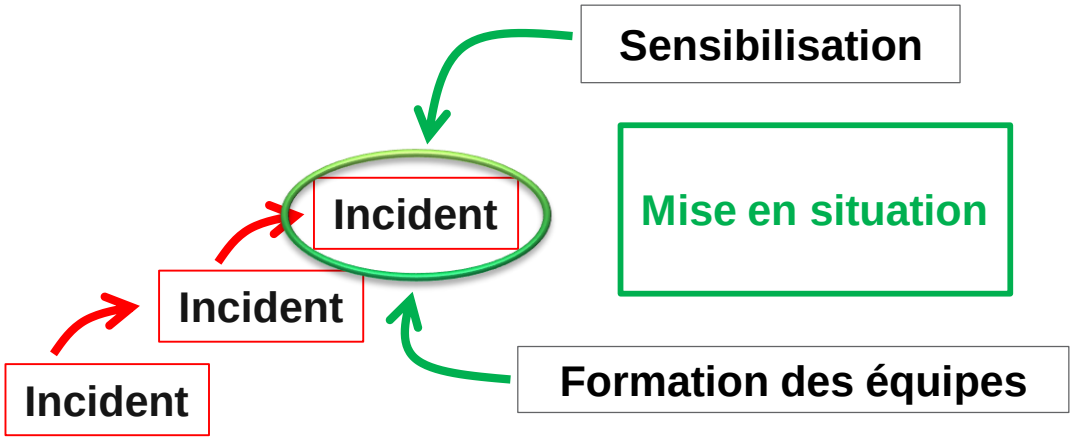
Limiter l'impact

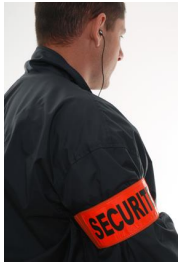
Investigations



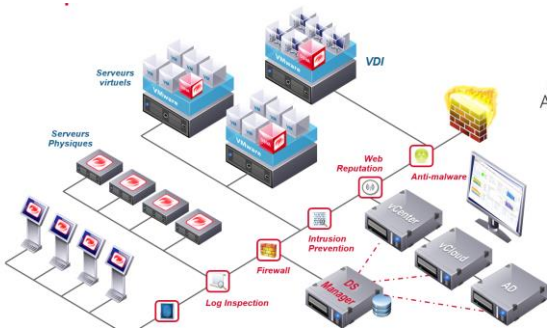
Préserver les preuves

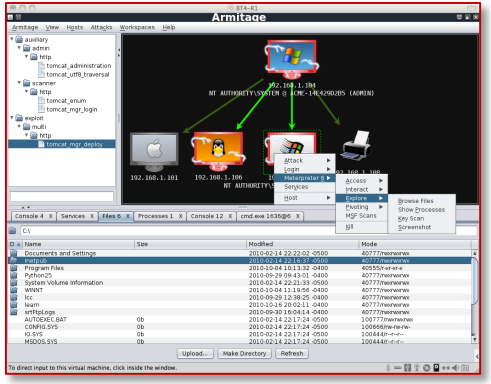
# Aspects organisationnels



# Conclusion





TREND MICRO™

Securing Your Journey to the Cloud

# Merci

Johanne Ulloa
@julloa