

The image features a dark background with various neon-colored geometric shapes and lines. A central white-outlined tag contains the text 'CYBER SECURITY'. A pink arrow points towards the tag from the top left. Several cyan lines and shapes, including triangles, crosses, and a horizontal line, are scattered around the central tag. The text 'CYBER SECURITY' is in a white, sans-serif font, with the 'Y' having a small circle above it.

# CYBER SECURITY

Blue team

Red team

Pourquoi étudier la chaîne de **cyber sécurité** :

1. Comprendre ce qu'il se passe lors d'un test de pénétration, ou encore **pentest**.
2. Déterminer quelles sont les étapes d'une **évaluation de sécurité**.
3. La cybersécurité est en hausse constante depuis une dizaine d'année. Et encore plus après la pandémie : **+600%**. (février 2021)
4. Il est donc important de savoir analyser, comprendre et se protéger contre les menaces grandissantes.
5. Ce cours contient :
  - Visualisation graphique de la chaîne de cybersécurité et plusieurs **ressource infographique**.
  - Un lexique des termes techniques utilisés.

A collection of glowing geometric shapes in the top-left corner: a small magenta triangle, a cyan triangle, a cyan plus sign, and a large cyan trapezoid with a handle.

?

N'hésitez pas à poser toutes les  
questions nécessaires

# GLOSSAIRE

01

## LOCKHEED MARTIN

Introduction de la  
société créatrice de  
la killchain.

03

## OBJECTIF

Quelles sont les  
objectifs d'une  
attaque.

02

## KILL CHAIN

Présentation du  
modèle de la  
killchain.

04

## FOURTH SECTION

Here you could  
describe the topic of  
the section



“This is a quote. Words full of wisdom that someone important said and can make the reader get inspired.”

—SOMEONE FAMOUS



01

LOCKHEED  
MARTIN

Les créateurs de la kill  
chain.

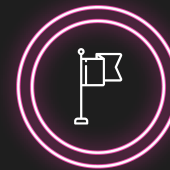
01

# LOCKHEED MARTIN KEY-NUMBER



## FIRST

Première entreprise  
américaine et mondiale de  
défense et de sécurité.



## BORN IN THE USA

Client principale : le  
Pentagone.



## Chiffre d'affaire

66 milliards de dollars  
(prévisionnel 2022).



## Créateur du modèle

Le modèle killchain inventé  
en 2011 par des informaticien  
de LM.

02

02

# KILL CHAIN

Présentation du modèle de la  
killchain.

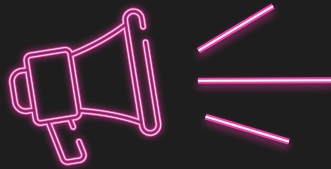


## ON DÉMARRE !

Nous avons vu les but de la cyber attaque, mais pourquoi avoir besoin d'un modèle. Pourquoi avoir besoin de le visualiser ?

- La visualisation contribue à soulager les manifestations de la plupart des problèmes.
- Connaître le processus permet l'organisation.
- Permet de partager le concept

# 7



La killchain se découpe en 7  
phases..



# Reconnaissance



Le hacker va rassembler des informations par rapport à sa cible. Repérer des failles de sécurité à exploiter.



Blue team

# Reconnaissance



Le hacker va rassembler des informations par rapport à sa cible. Repérer des failles de sécurité à exploiter.

Red team



# Arsenalisation



Le hacker va créer des malwares et des moyens d'exploiter les failles et vulnérabilités.

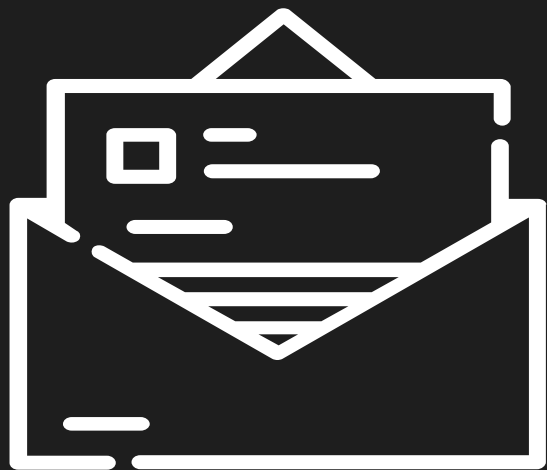
# Arsenalisation



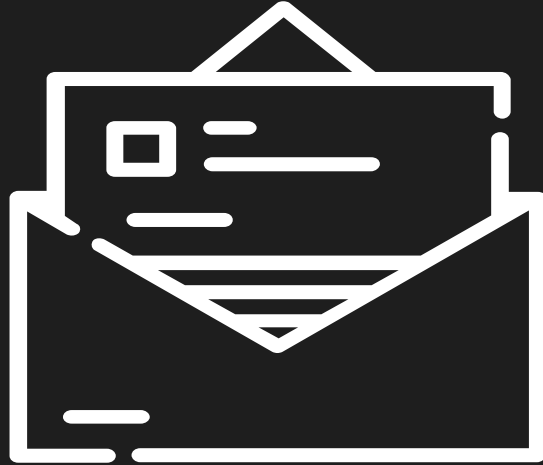
Le hacker va créer des malwares et des moyens d'exploiter les failles et vulnérabilités.





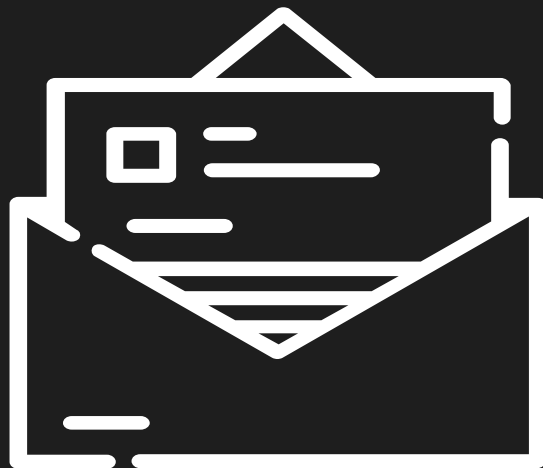


# Livraison



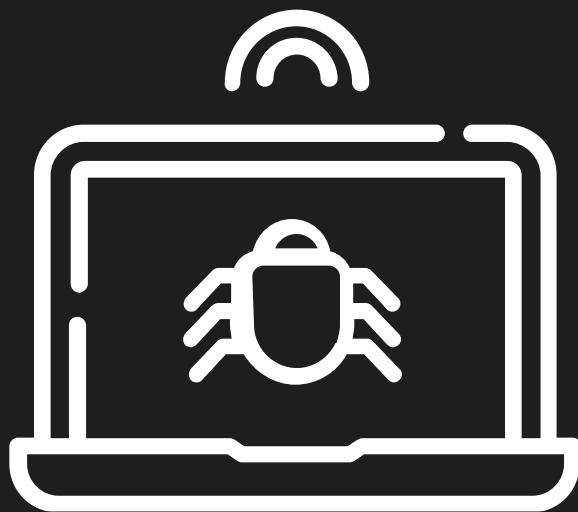
Le hacker va délivrer son malware dans le système de la cible.

# Livraison

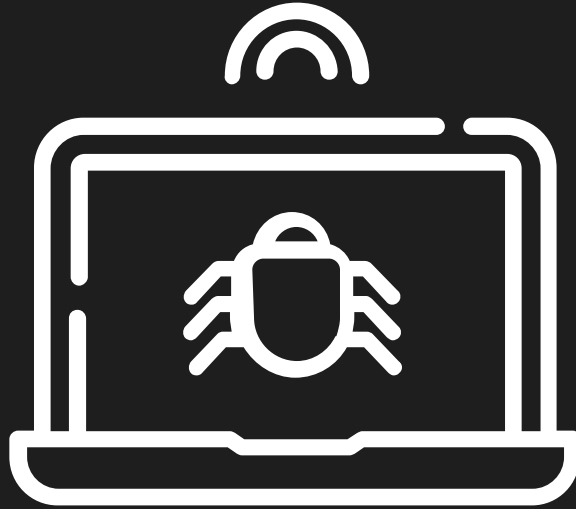


Le hacker va délivrer son malware dans le système de la cible.



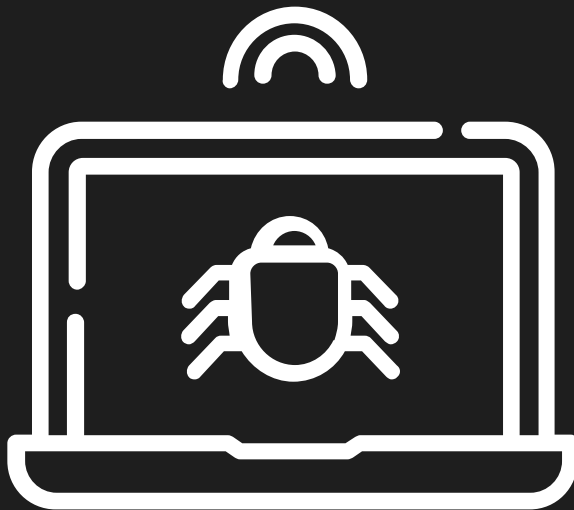


# Exploitation



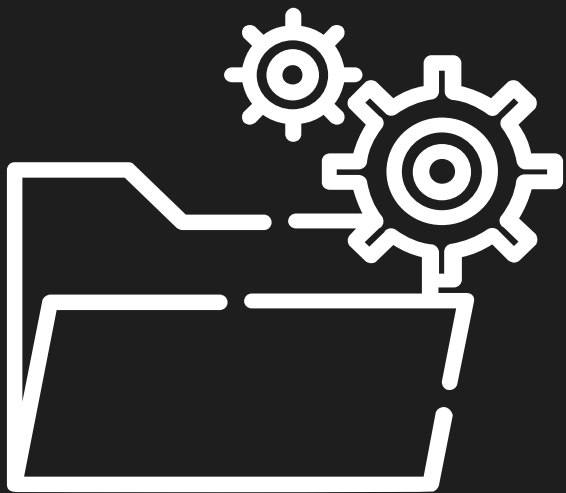
Utiliser une faille identifié lors des précédents processus pour exécuter le malware développer par l'attaquant.

# Exploitation

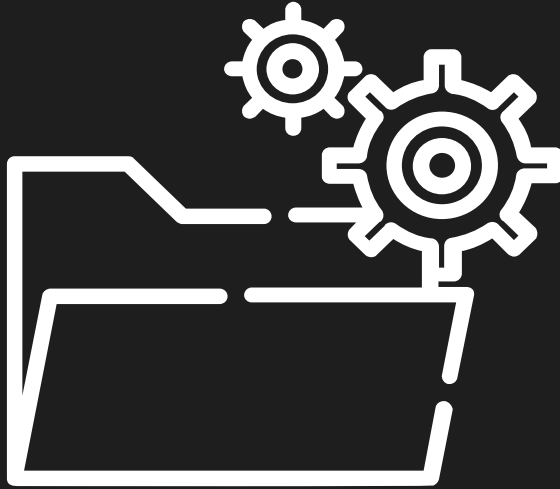


Utiliser une faille identifié lors des précédents processus pour exécuter le malware développer par l'attaquant.





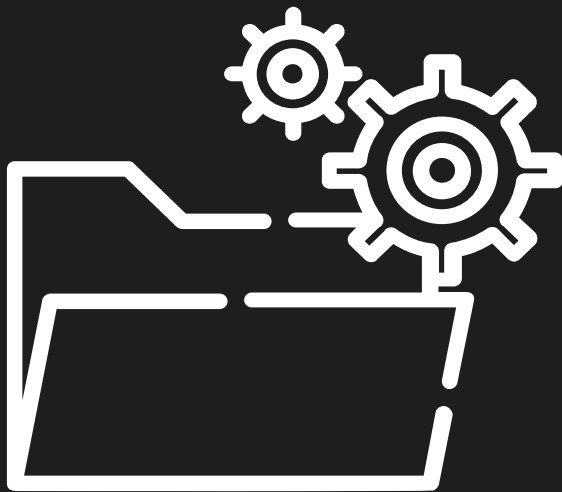
# Installation



Installer le malware sur le système afin d'avoir accès à la totalité de l'environnement.

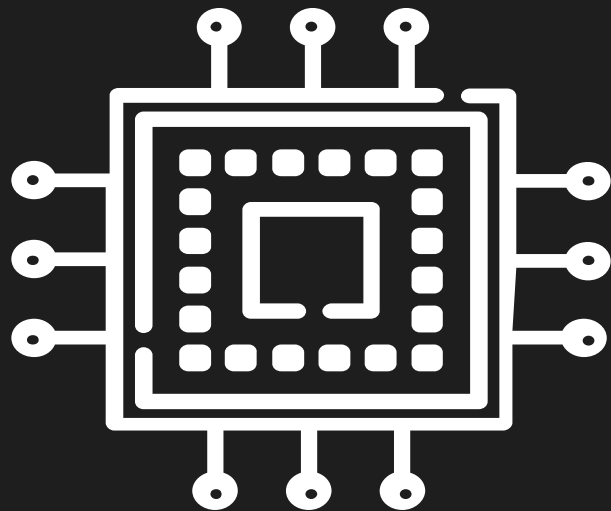


# Installation

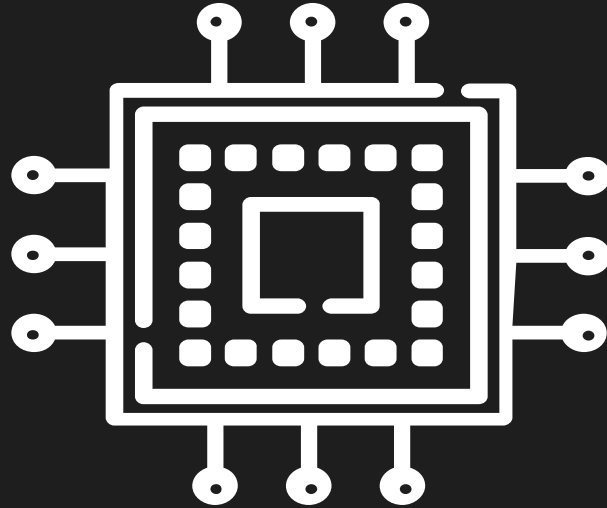


Installer le malware sur le système afin d'avoir accès à la totalité de l'environnement.



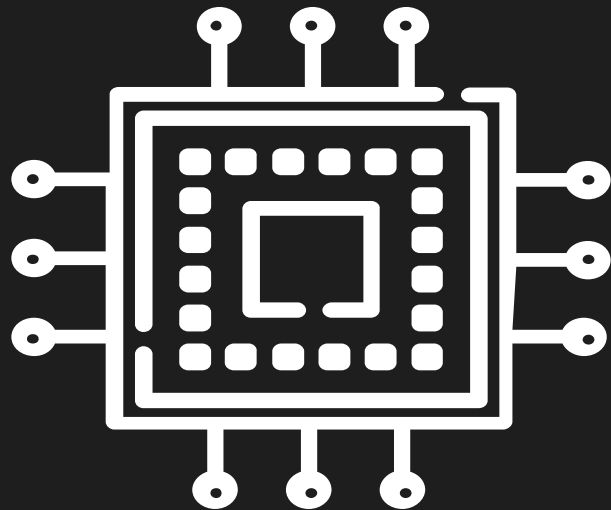


# Execution

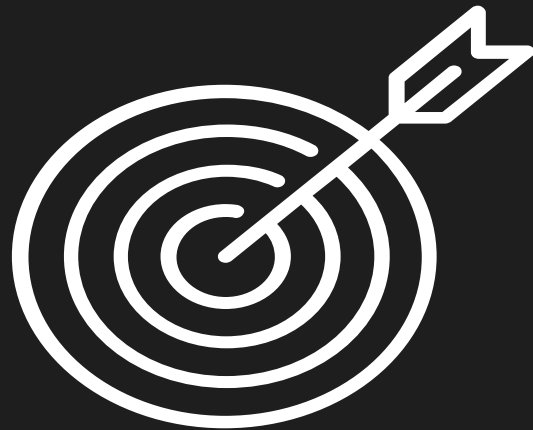


Le hacker profite de son accès à l'environnement pour exécuter des commandes à distance afin de maintenir et développer l'attaque.

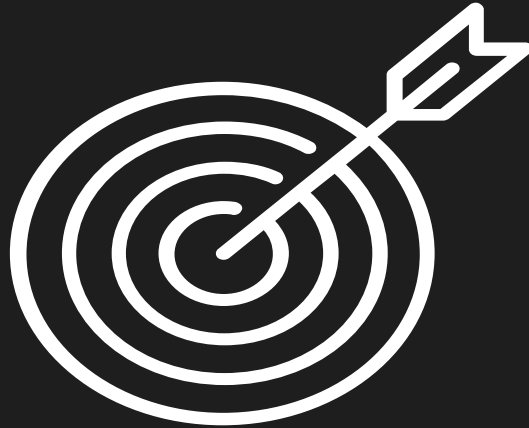
# Execution



Le hacker profite de son accès à l'environnement pour exécuter des commandes à distance afin de maintenir et développer l'attaque.

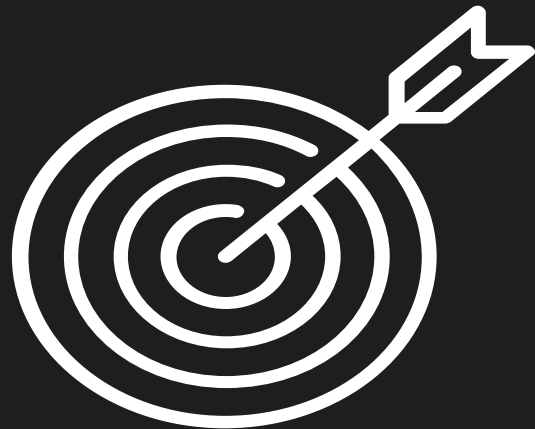


# Objectifs



Le hacker continue de poursuivre les objectifs de l'attaque.

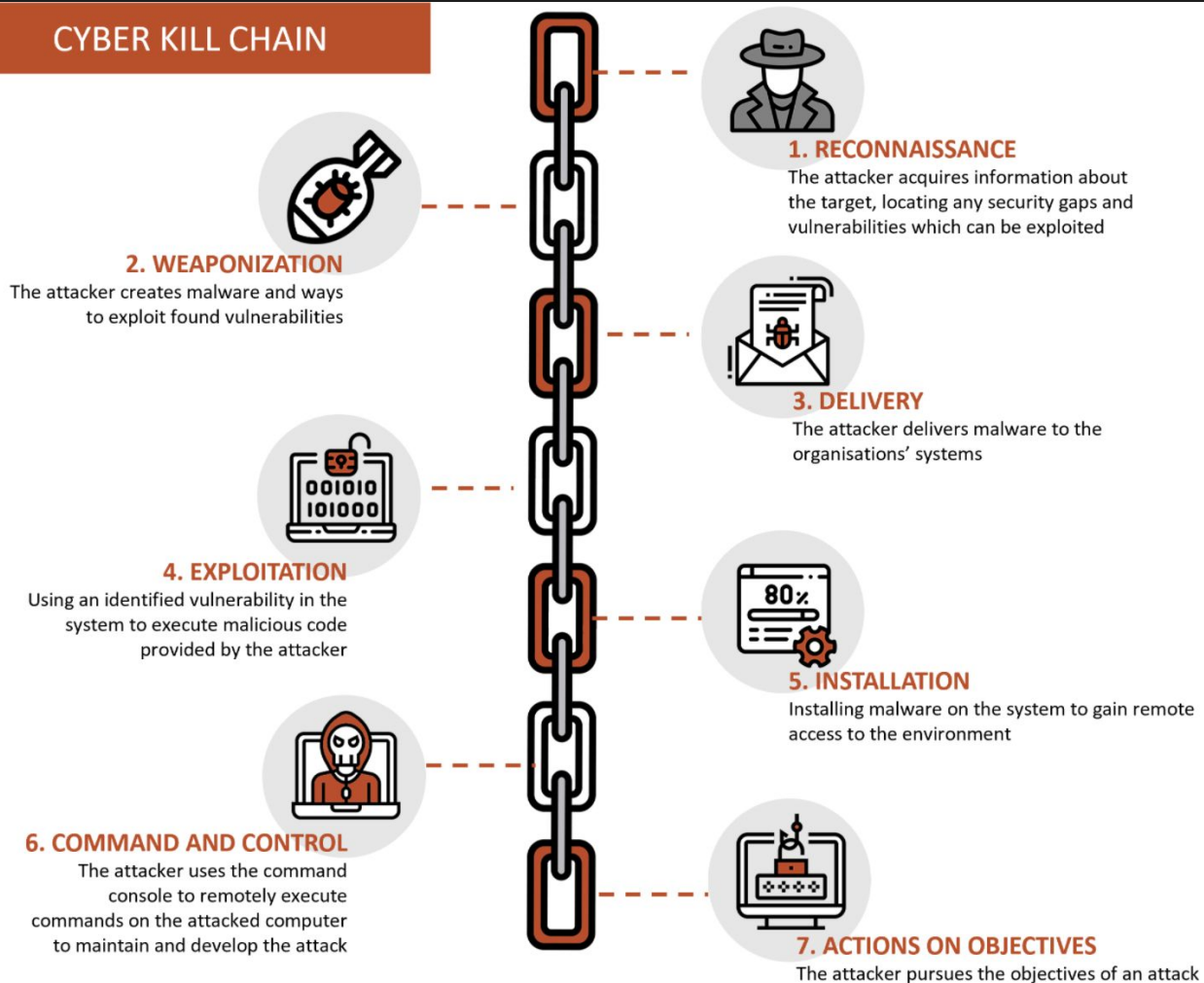
# Objectifs



Le hacker continue de poursuivre les objectifs de l'attaque.



# CYBER KILL CHAIN





# VICTIMIZE AND SECURITY BREACH

La kill chain dans l'actu :

- 
- 
- 

Maintenant, nous allons rentrer beaucoup plus dans le détails de la kill chain.

# RECONNAISSANCE

## Reconnaissance active

Trouver des informations en interagissant avec le système.

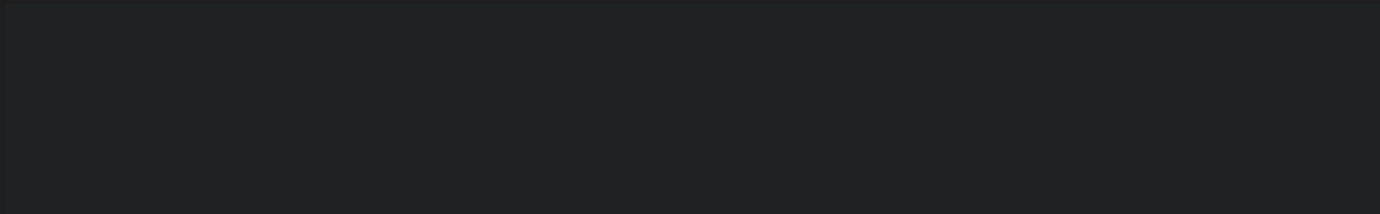


## Reconnaissance passive

Trouver des informations sans interagir avec le système.

# RECONNAISSANCE PASSIVE

Trouver des informations publiques :



Il y a des milliards de scénarii possible. Il faut savoir s'adapter. Potentielle cours sur le DOXING  
La récolte est à durée variable.

# RECONNAISSANCE PASSIVE

Trouver des informations publiques :

- Whois, cmd
- Nom de domaine
- Google, DW
- Personne composant le système

Il y a des milliards de scénarii possible. Il faut savoir s'adapter. Potentielle cours sur le DOXING  
La récolte est à durée variable.

## RECONNAISSANCE ACTIVE

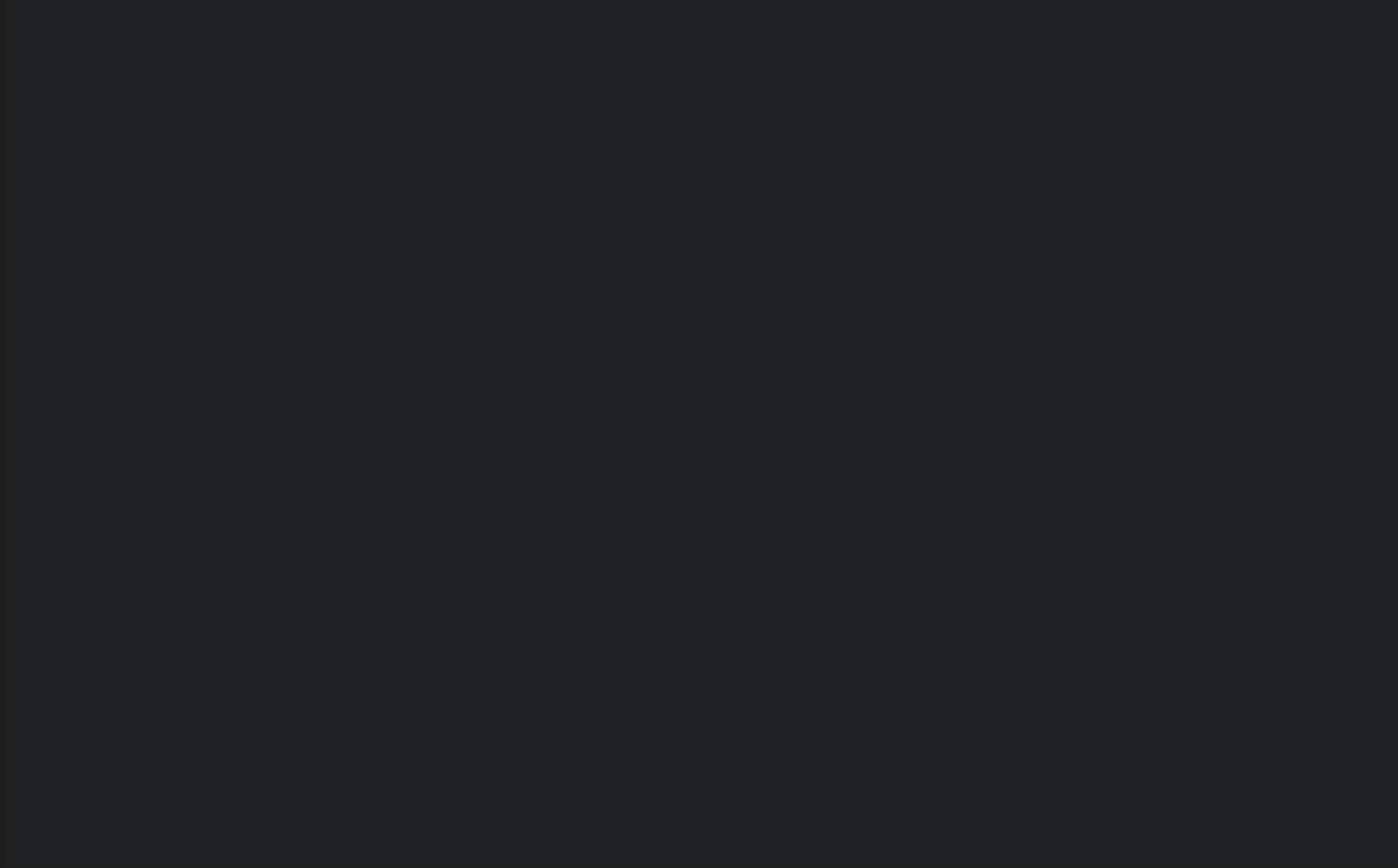
Sonder un système pour obtenir des informations.

# RECONNAISSANCE ACTIVE

Sonder un système pour obtenir des informations.

- Ping
- IMAP
- Balayage de port
- Wireshark

# ARSENALISATION





## SCRIPT

Création de script malicieux



# ARSENALISATION



## SCRIPT

Création de script malicieux



## PHISHING

Malware dans un software  
existant ou page web  
infectée.

# ARSENALISATION



## SCRIPT

Création de script malicieux



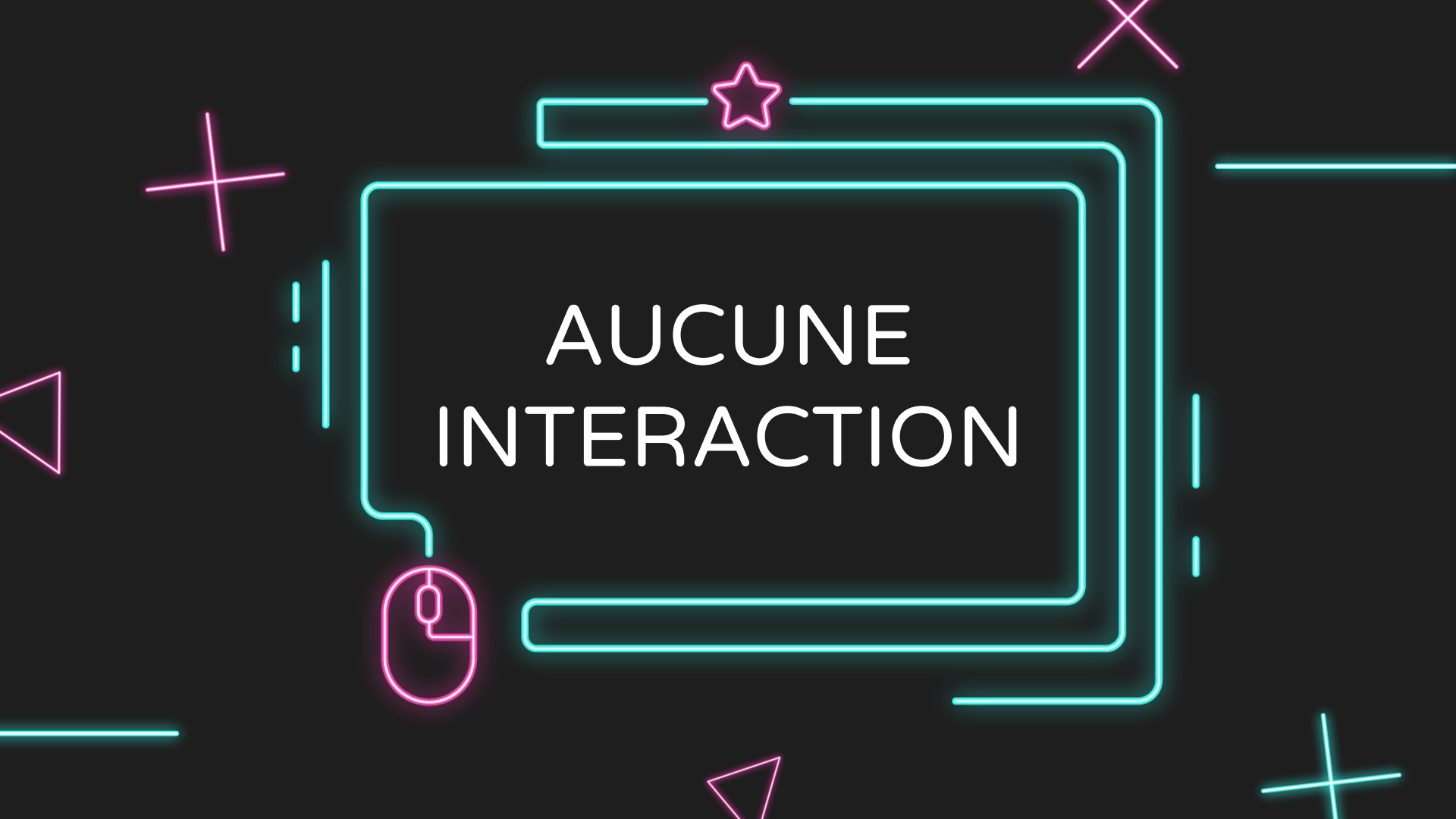
## PHISHING

Malware dans un software  
existant ou page web  
infectée.



## DEVICE

Malware sur une clé usb ou  
du hardware.



# AUCUNE INTERACTION

## LIVRAISON



La transmission de  
l'attaque à la victime.

## RECONNAISSANCE PASSIVE

Comment envoyez notre colis suspect ?

- Mail, Sms
- Hardware
- Site web

Pensez à votre cible et adapté la stratégie, soit vous avez un grand nombre de target générique, soit vous êtes précis sur un petit groupe d'individu.



## EXPLOITATION

Le script tourne maintenant sur le système de votre victime. Le public averti vérifie toujours que leurs systèmes sont mis à jour souvent. Il s'assure d'avoir toujours des outils de protection appropriés. Lorsque vous êtes ici, vous êtes déjà dans le système. Vous avez bypass toutes les sécurités, et vous avez accès à toutes les ressources de la cible.



QU'EST CE  
QUE VOUS  
FAITES ?

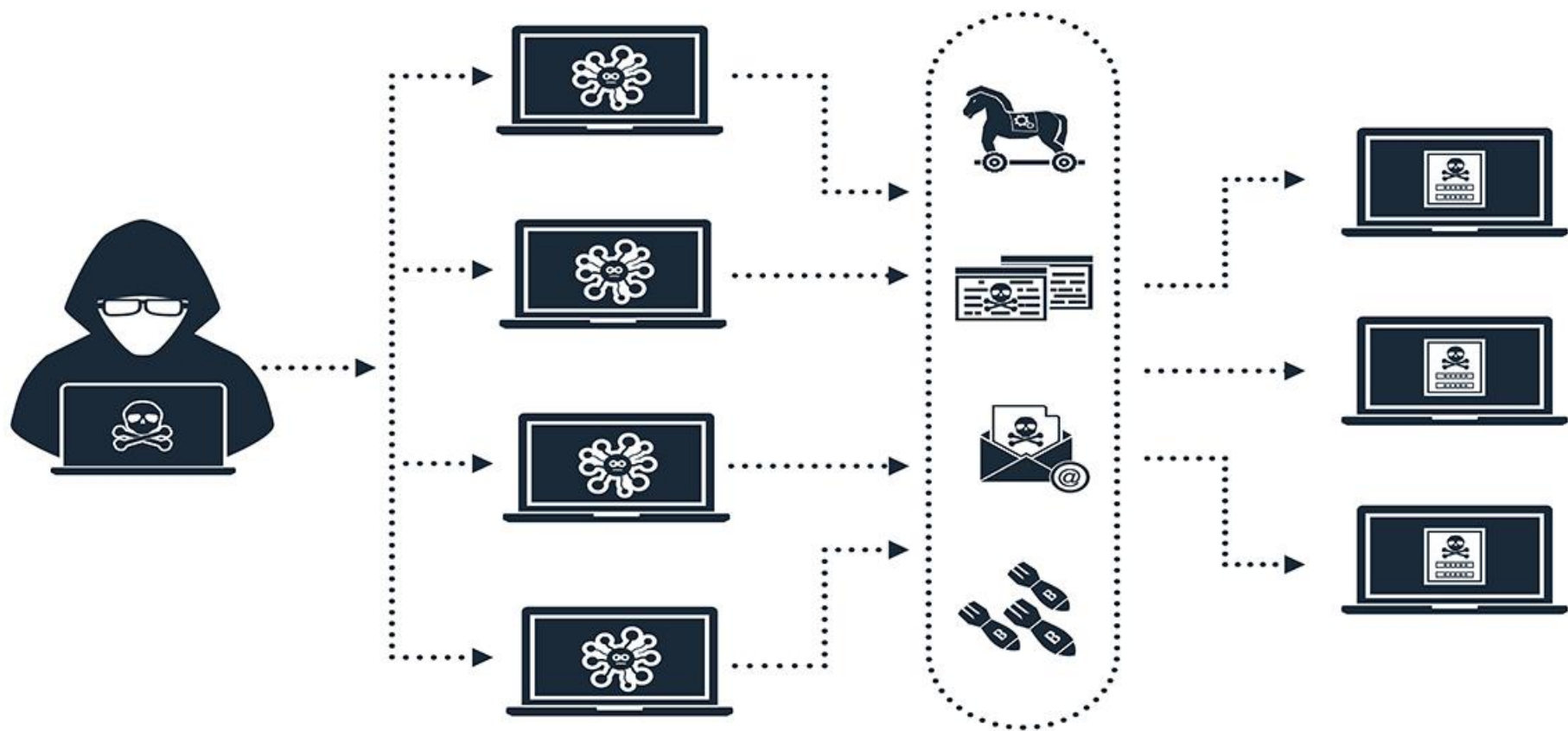


# INSTALLATION

Vous voulez avoir la possibilité de pouvoir installer/modifier/manipuler ce que vous voulez sur la machine. Pour créer de la persistance dans le système.

Faire en sorte que le malware reste actif peu importe le redémarrage, la mise à jour du système, etc.

APT : advanced persistent threat



# 03

03

OBJECTIF

Quelles sont les objectifs  
d'une attaque ?

## EXEMPLE D'OBJECTIF

### Extorsion de données

Intéressé par les organisations propriétaires de données comme les studio de création numérique (donc employé et client). On cible le produit, les DPI, etc.

### Déni de service

Attaque informatique ayant pour but de rendre indisponible un service.

### Destruction de service

J'ai pas vraiment besoin de plus d'explication ici.

## EXEMPLE D'OBJECTIF

### Extorsion de données

Intéressé par les organisations propriétaires de données comme les studio de création numérique (donc employé et client). On cible le produit, les DPI, etc.

### Déni de service

Attaque informatique ayant pour but de rendre indisponible un service.

### Destruction de service

J'ai pas vraiment besoin de plus d'explication ici.

Exemple

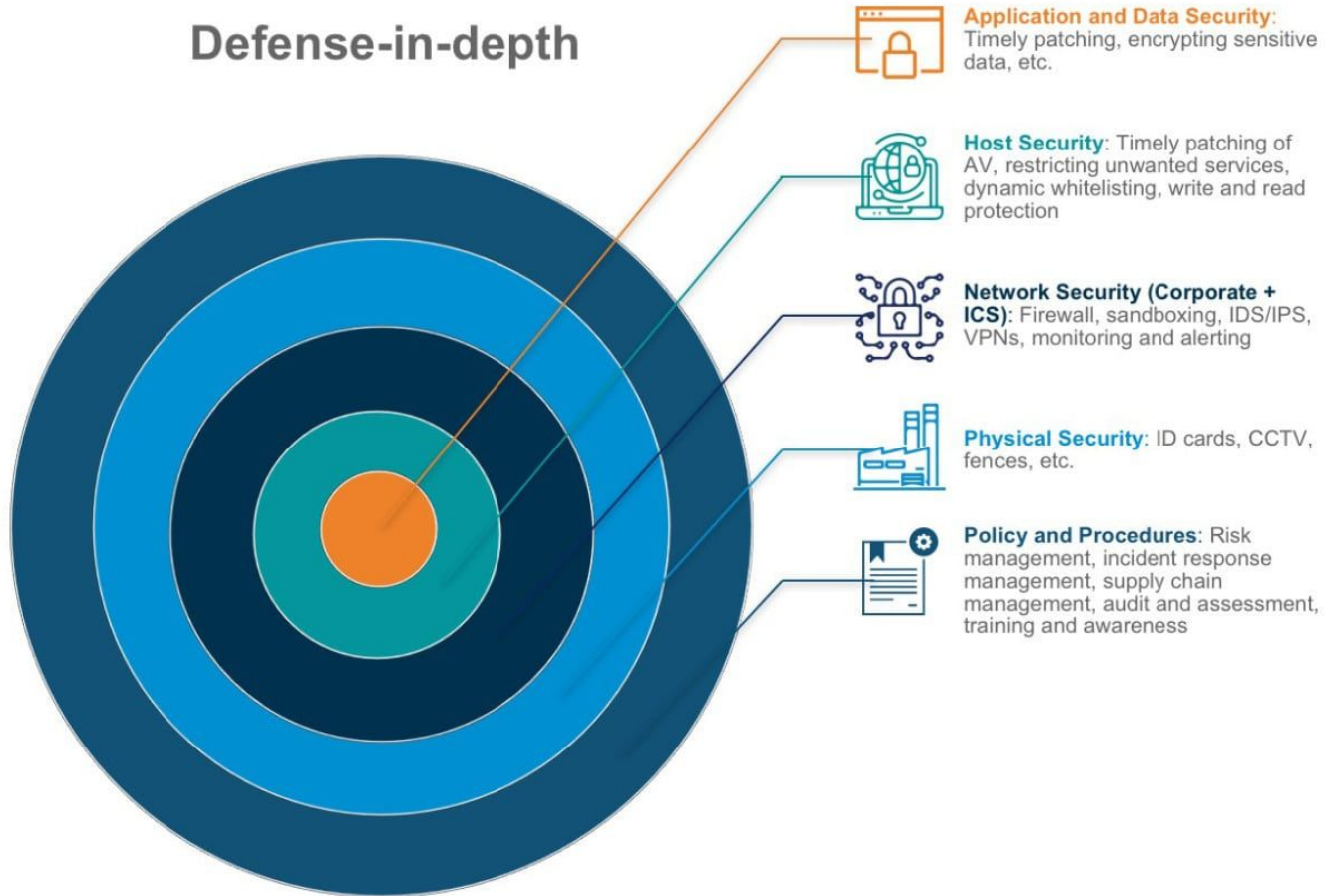
## DEFENSE IN DEPTH

Le concept de défense en profondeur est un terme d'origine militaire, où une multitude de couches sont implémentées pour sécuriser l'actif. Comme cela, si une couche est corrompue, une autre est encore en capacité de protéger le système et mitiger le risque. (Blindage de char multicouche).

Ses couches sont implémentées dans le hardware, dans le software ou sur les gens.

On doit toujours avoir un moyen de ralentir l'attaque. (antivirus, plateforme de surveillance IPS IDS, firewall, et autre)

# Defense-in-depth





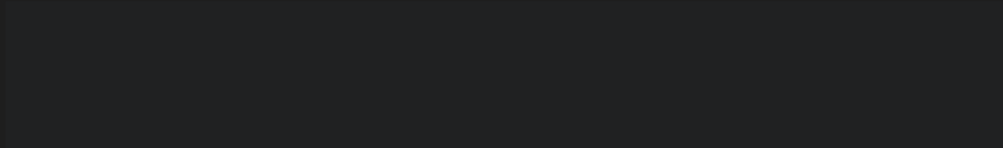
# UNE PERTURBATION

...



Avec cette méthode de visualisation, quelle team à l'avantage ?

La bleu ! Car pour qu'une cyberattaque soit réussie, il faut que les 7 étapes soit validés. Ce qui donne 7 opportunités au bleu de briser la chaîne.



Avec cette méthode de visualisation, quelle team à l'avantage ?

La bleu ! Car pour qu'une cyberattaque soit réussie, il faut que les 7 étapes soit validés. Ce qui donne 7 opportunités au bleu de briser la chaîne.

mais c'est faux....

Pourquoi ?

04

04

CHIFFRES

Chiffres clés d'une  
cyber-attaque

# What is happening in the threat landscape - The challenges of keeping up with a perpetually evolving cyber security environment.

61%



of organizations say  
**data theft and cybercrime**  
are the greatest threats  
to their reputation

2012 IBM Global Reputational Risk & IT Study



70%

of security execs  
are concerned about **cloud  
and mobile security**

2013 IBM CISO Survey



80%

of enterprises  
have difficulty finding the  
security skills they need

2013 Forrester Consulting, "Surviving the  
Technical Security Skills Crisis"



Average data  
breach in the  
US cost

**\$6.5**million

2015 Cost of Data Breach Study: Global Analysis  
Ponemon Institute

**Mobile malware** is affecting

**11.6M**

mobile devices



IBM X-Force® Threat Intelligence Quarterly IQ 2015

**85**

tools from



**45**

vendors



IBM client example

