Numérisation et Cyber Security

Leçons tirées du black-out en Ukraine

30 août 2022, Forum des réseaux de Swissgrid, Musée des transports de Lucerne

cyrill.brunschwiler@compass-security.com

Quel est le niveau de sécurité de notre approvisionnement en électricité?

Neue Zürcher Zeitung

Ein längeres Blackout hätte katastrophale Folgen – doch undenkbar ist es nicht

Eine Welt ohne Elektrizität können wir uns kaum vorstellen. Doch das Szenario einer anhaltenden Strommangellage ist keineswegs abwegig. Und die Politik tut zu wenig, um es abzuwenden.

01.06.2021, 05.30 Uhr David Vonplon

Gaëtan Bally / Keystone

Kommt es zu einer Verkettung unglücklicher Umstände, ist eine

Sous-station (SS Mettlen)

https://www.solutec.ch/de/aktuelles/referenzen/hs-netze/380-220kV-Schaltanlage-UW-METTLEN.php

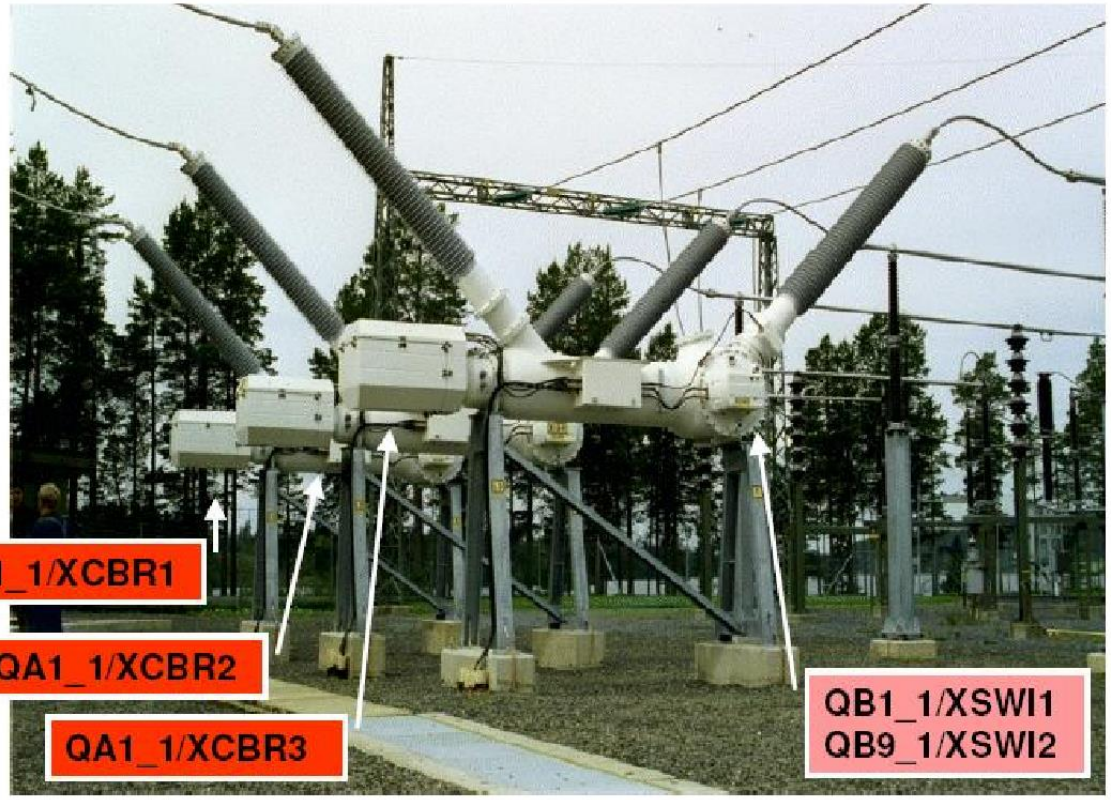
Quel est le niveau de sécurité de notre approvisionnement en électricité?

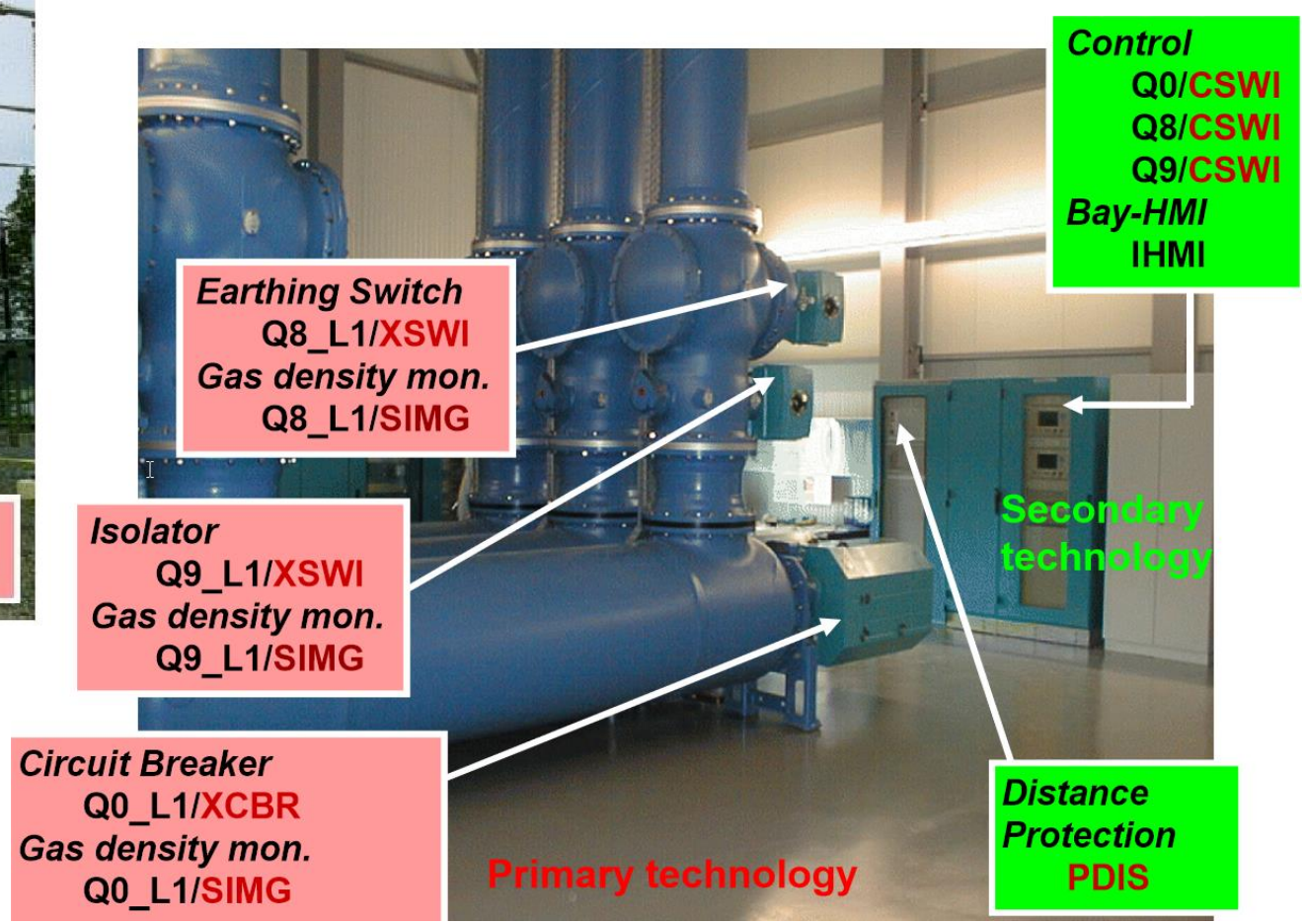
https://www.youtube.com/watch?v=UF5EDV6T7es

Sous-station: appareils de protection, convertisseurs de protocole, automatisation (IED)

https://new.abb.com/substation-automation/products/the-power-of-one
https://www.directindustry.fr/prod/siemens-energy-automation-and-smart-grid/product-30064-589133.html
https://www.se.com/in/en/work/products/product-launch/easergy/easergy-p3.jsp

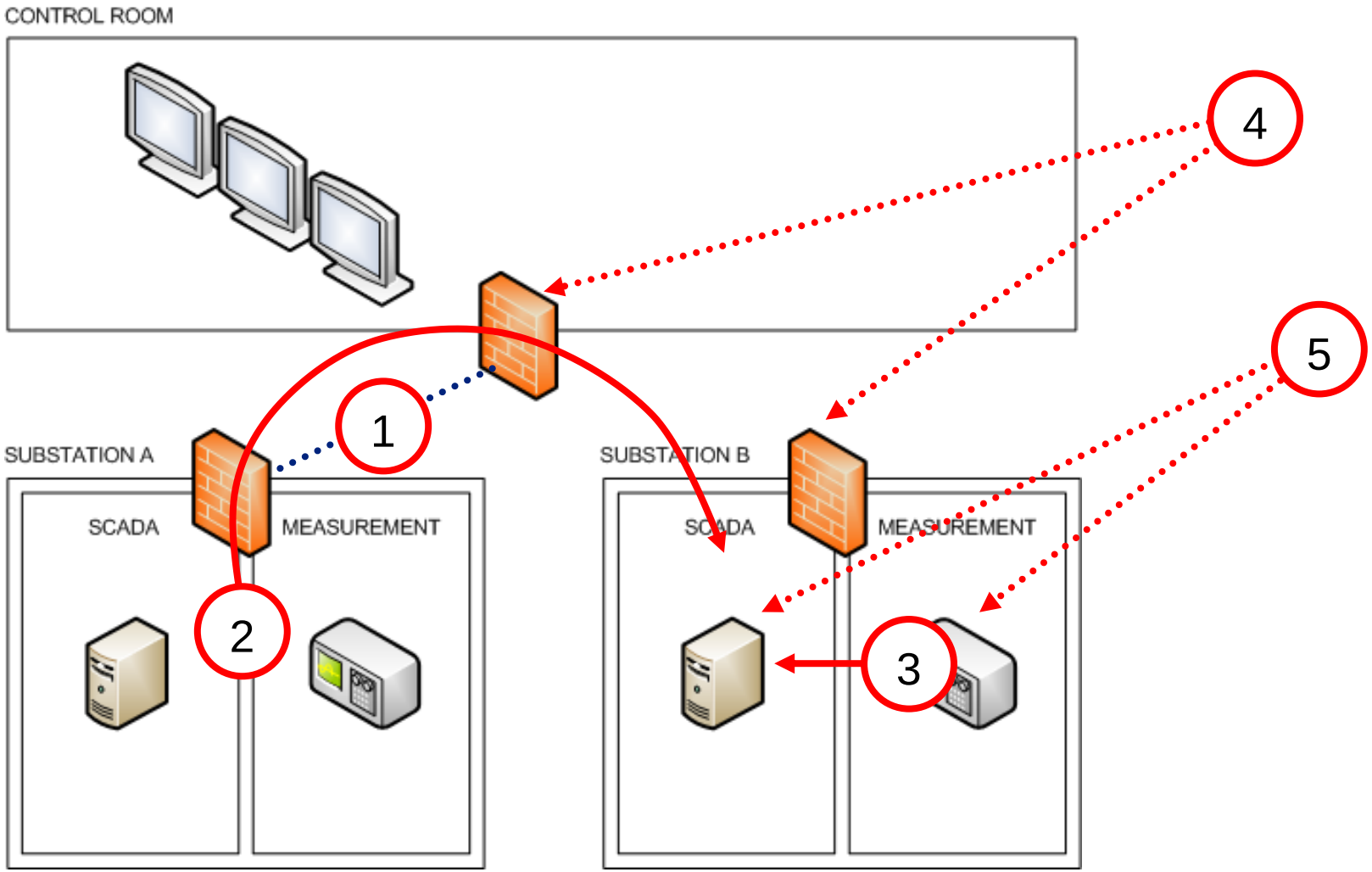
Dénomination au moyen d’un modèle d’objet (CEI 61850 MMS)





ABB, Kirrmann, https://web.fe.up.pt/~asousa/sind/acetat/AI_EPFL/AI_421_IEC61850.pdf

Scénarios d’attaque contre les sous-stations



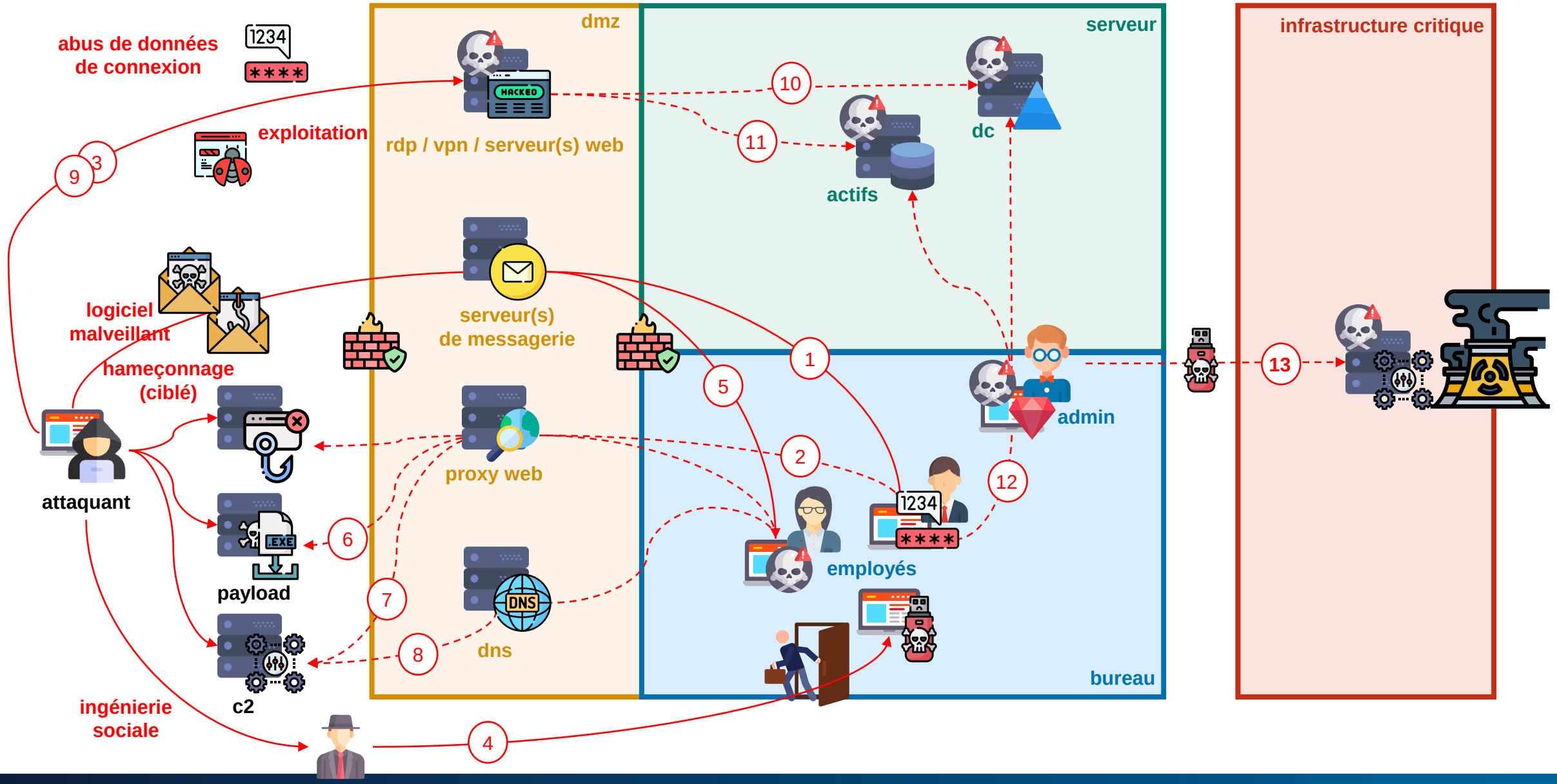
Schémas typiques d’intrusion

Tous les incidents ne sont pas aussi géniaux que ce que les médias veulent bien faire croire.

En général, les entreprises se font avoir par des pièges simples:

- spam malveillant
- mauvais mots de passe
- absence de 2FA
- vulnérabilité des appareils ou des logiciels (correctifs manquants)

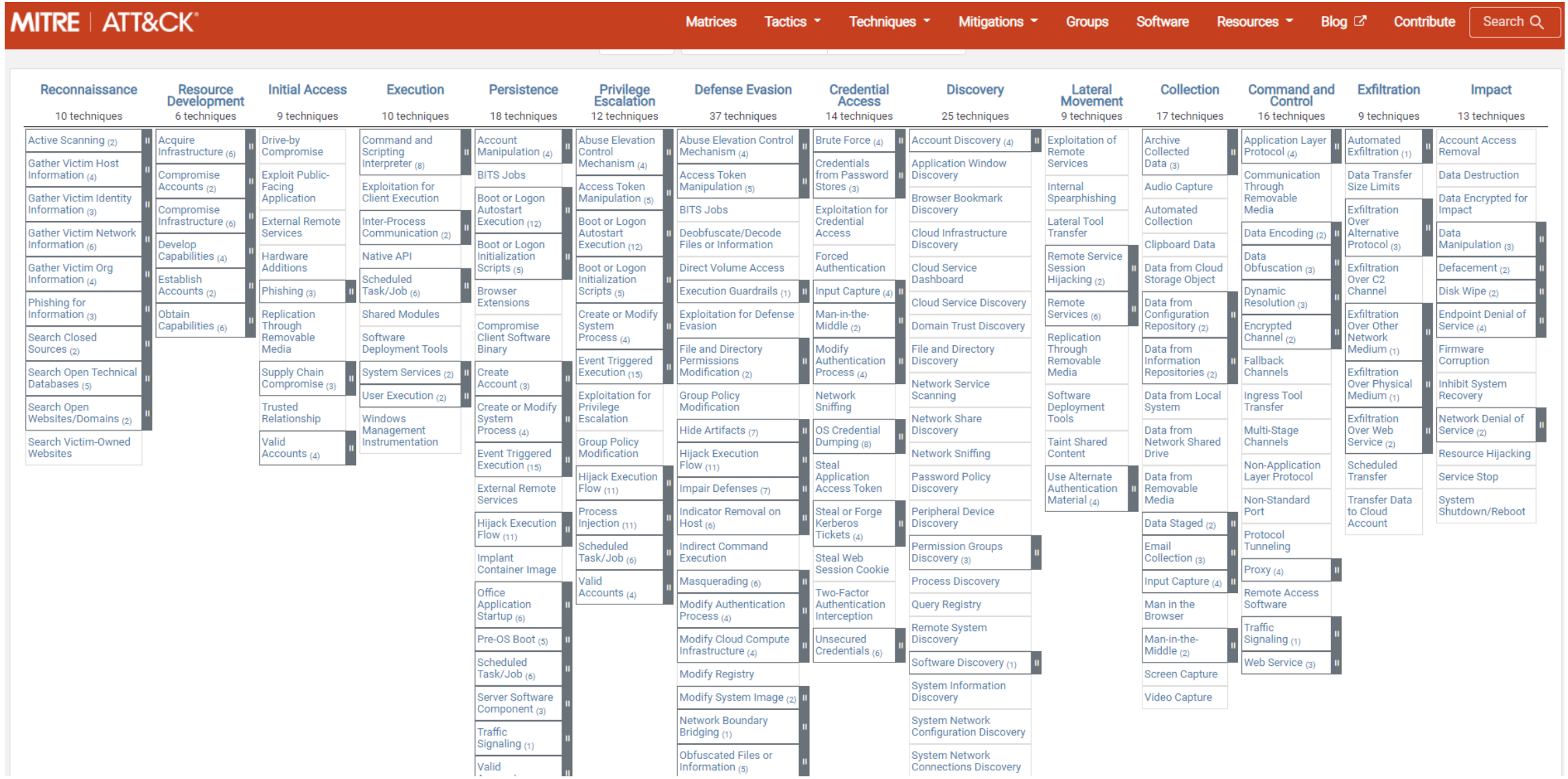
Schémas typiques d'intrusion



Qu’est-ce que cela veut dire plus précisément?

Cadre MITRE ATT&CK

Cadre MITRE ATT&CK



Cadre MITRE ATT&CK

Groupes

			primarily interested in users of remote banking systems in Russia and neighboring countries. The group uses a Trojan by the same name (RTM).
G0034	Sandworm Team	ELECTRUM, Telebots, IRON VIKING, BlackEnergy (Group), Quedagh, VOODOO BEAR	Sandworm Team is a destructive threat group that has been attributed to Russia's General Staff Main Intelligence Directorate (GRU) Main Center for Special Technologies (GTsST) military unit 74455. This group has been active since at least 2009. In October 2020, the US indicted six GRU Unit 74455 officers associated with Sandworm Team for the following cyber operations: the 2015 and 2016 attacks against Ukrainian electrical companies and government organizations, the 2017 worldwide NotPetya attack, targeting of the 2017 French presidential campaign, the 2018 Olympic Destroyer attack against the Winter Olympic Games, the 2018 operation against the Organisation for the Prohibition of Chemical Weapons, and attacks against the country of Georgia in 2018 and 2019. Some of these were conducted with the assistance of GRU Unit 26165, which is also referred to as APT28.
G0029	Scarlet Mimic		Scarlet Mimic is a threat group that has targeted minority rights activists.

Ukraine power cut 'was cyber-attack'

Piratage en Ukraine

Étape 1

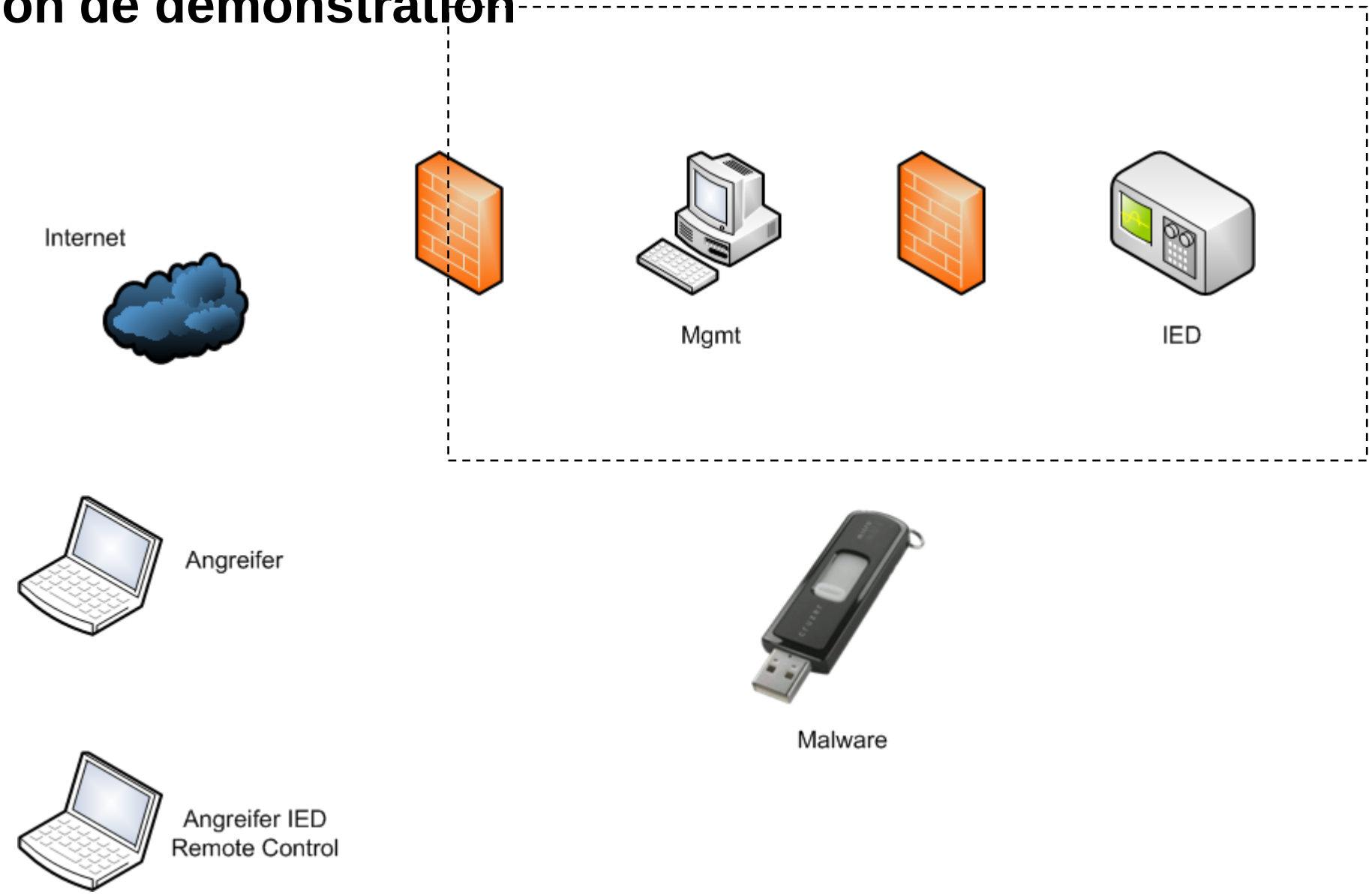
- E-mails de phishing avec des macros Word et des chevaux de Troie BlackEnergy
- Données d’accès VPN et mots de passe volés
- Analyse de réseau et mouvement latéral

Étape 2

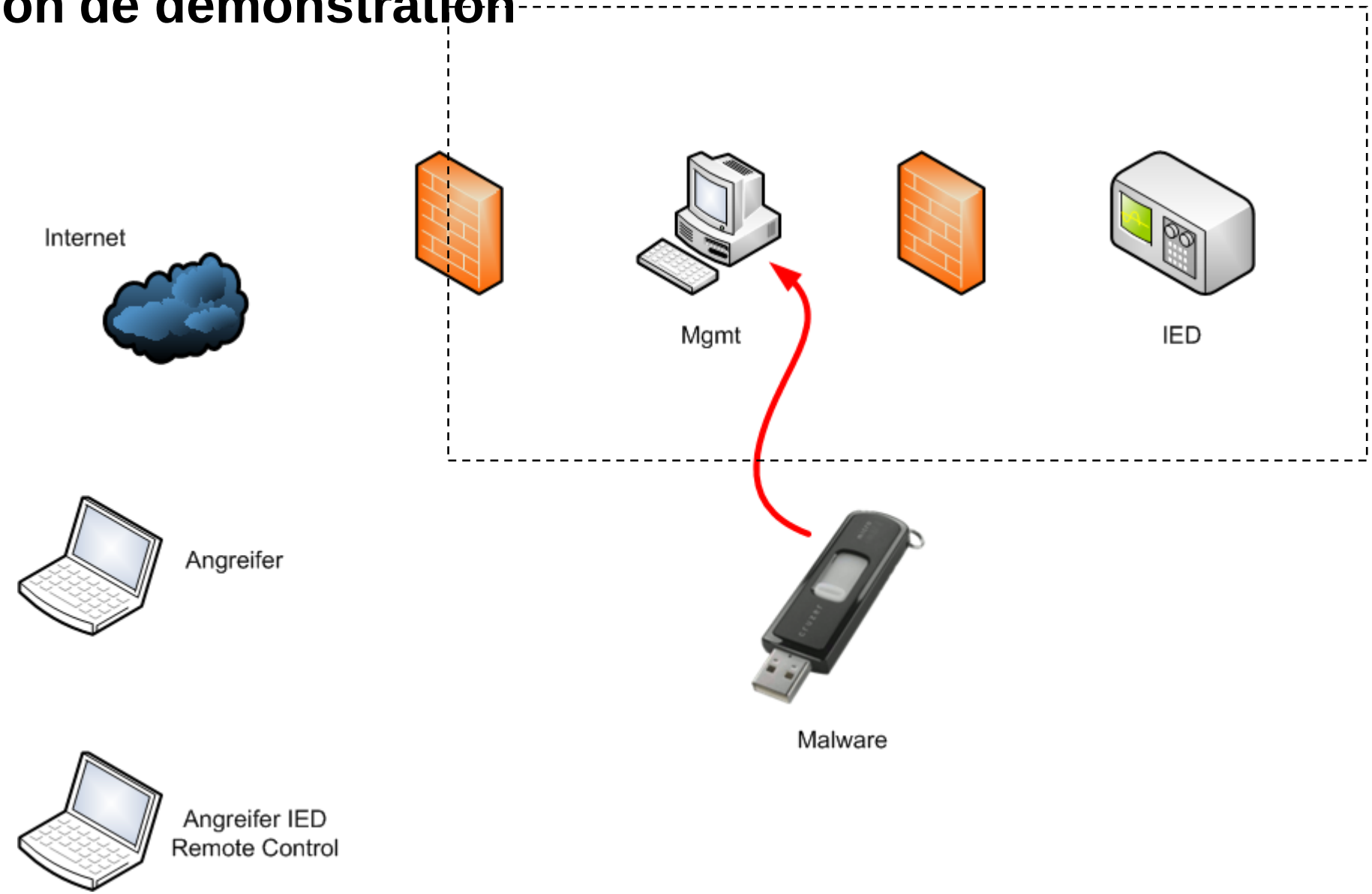
- Micrologiciel malveillant développé
- Environnement SCADA repris via l’interface utilisateur
- Sectionneur ouvert
- Coupure UPS orchestrée, micrologiciel chargé sur le convertisseur, journaux et disques effacés
- Déni de service téléphonique

https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

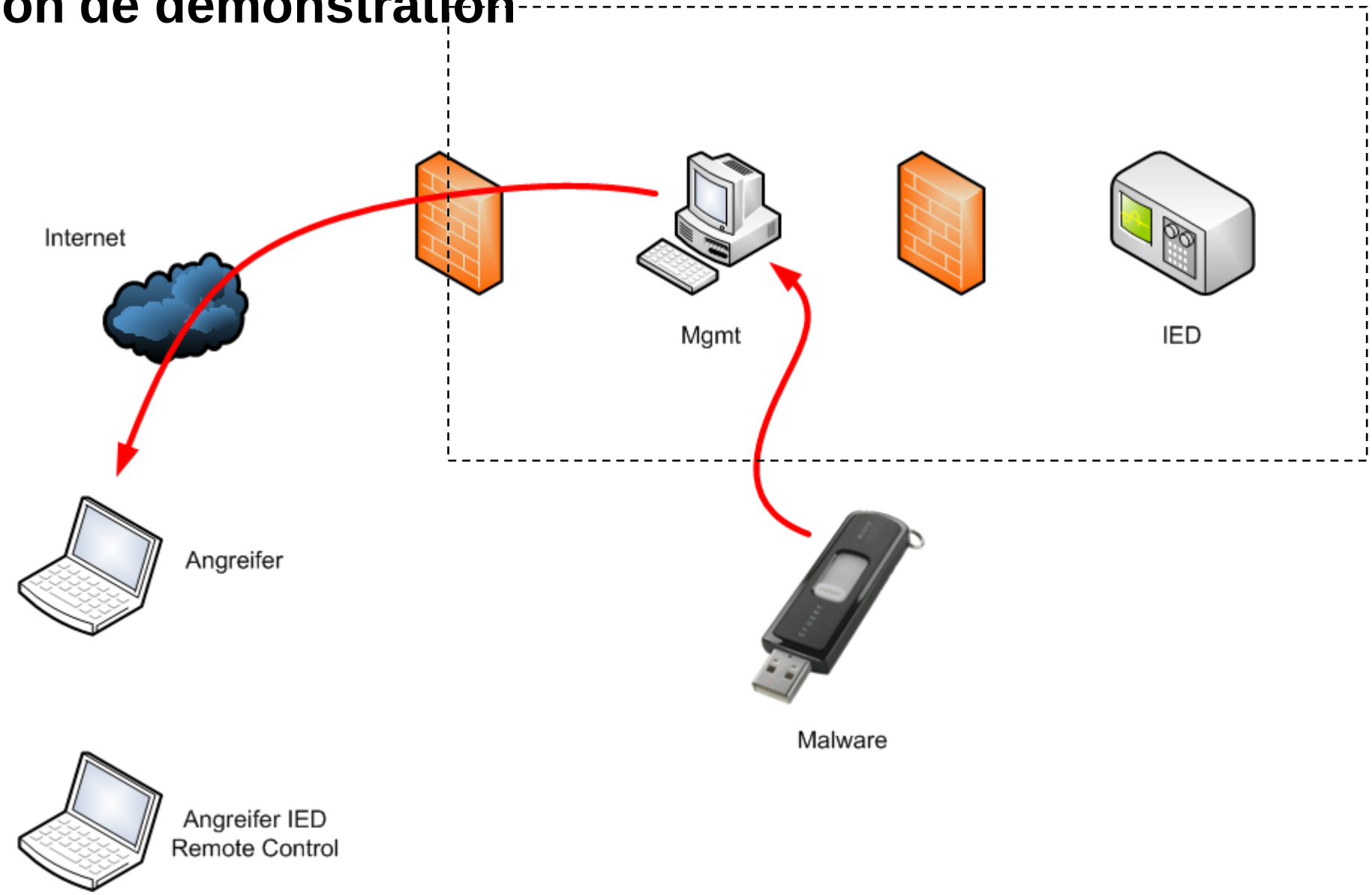
Configuration de démonstration



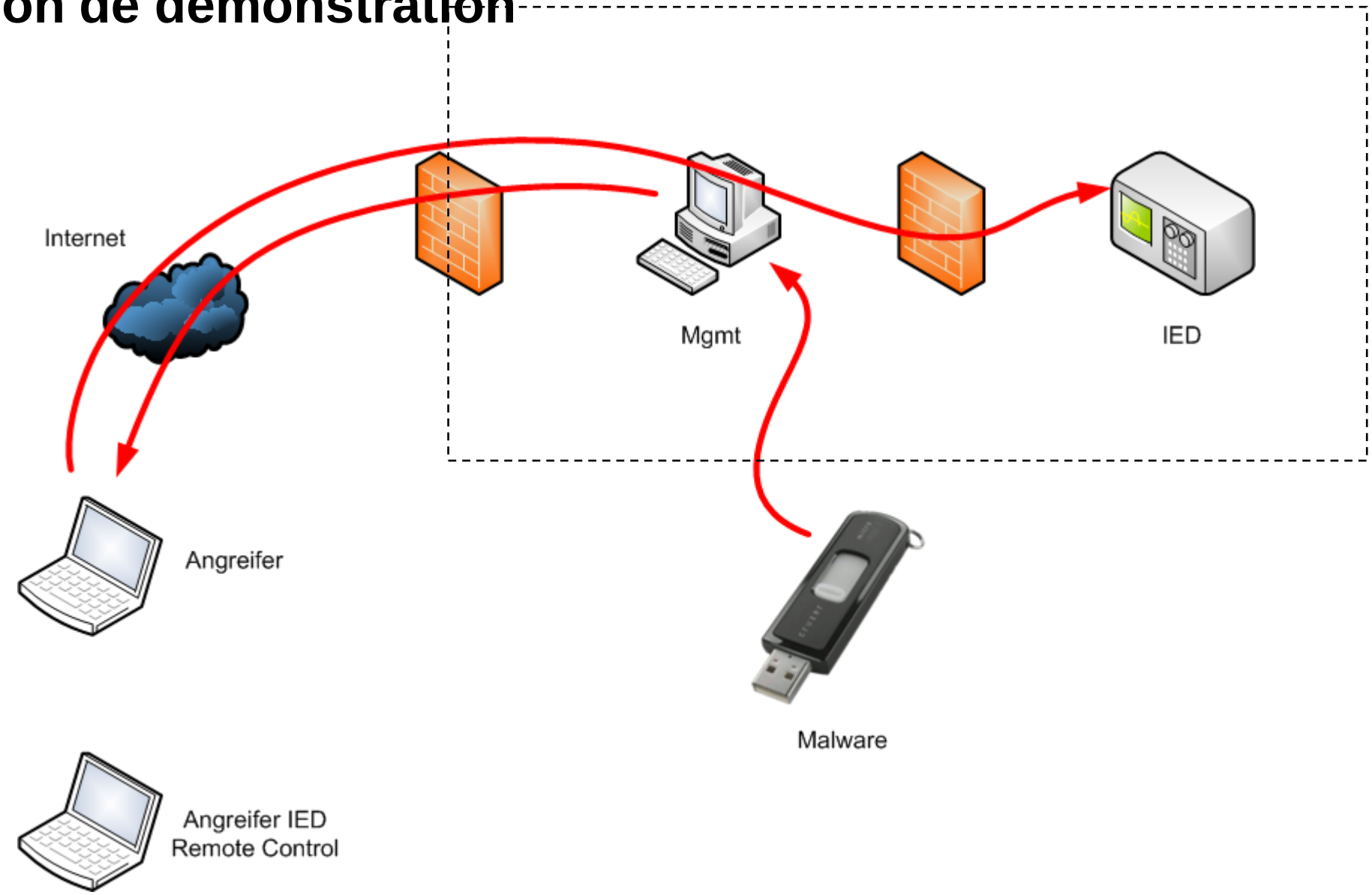
Configuration de démonstration



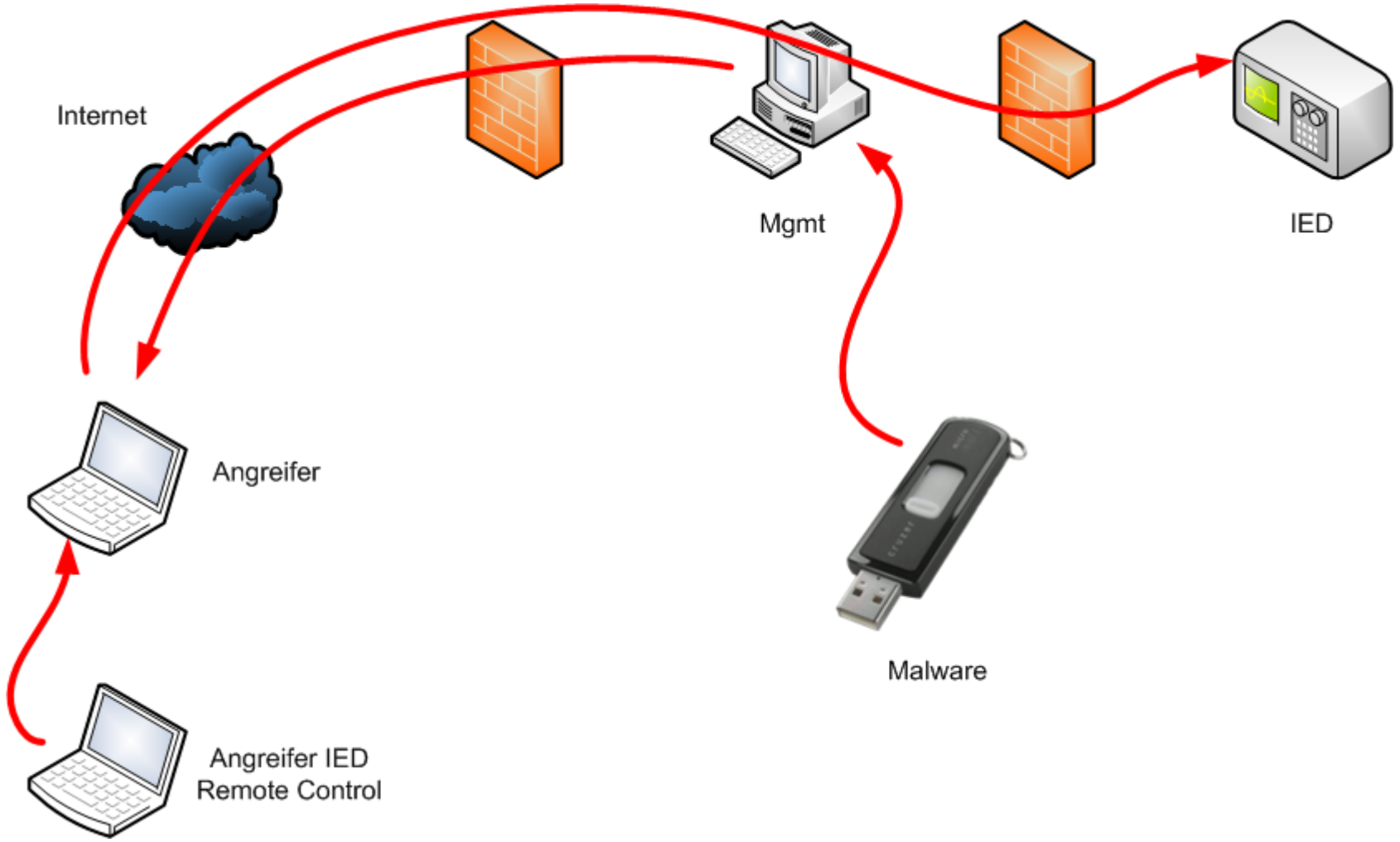
Configuration de démonstration



Configuration de démonstration



Configuration de démonstration



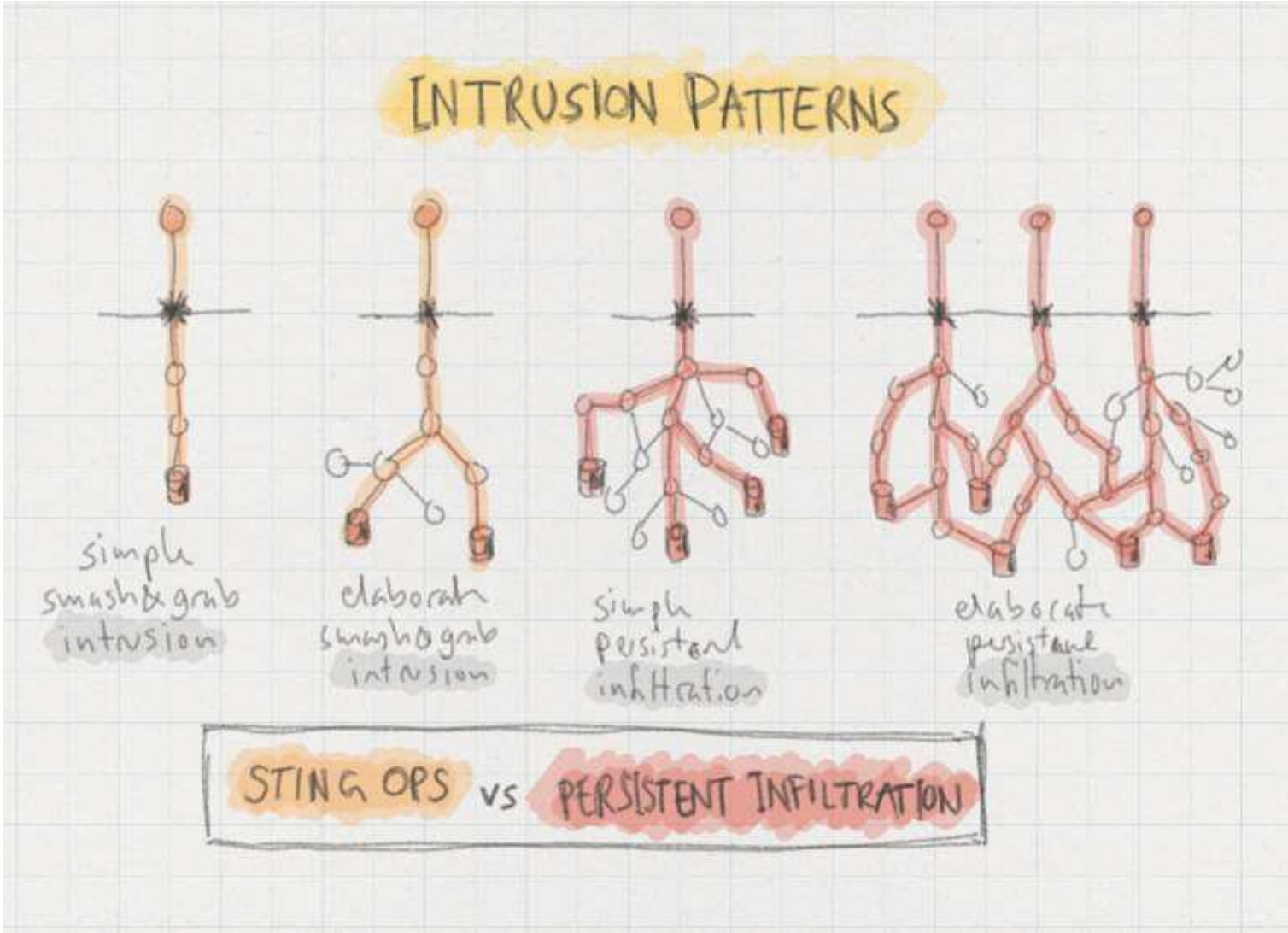
Et si cela arrivait?

Comportements des attaquants

Modèles d'intrusion

Opération Sting
Aussi appelée «smash and grab» («fracasser et saisir» en français). Une attaque directe pour obtenir une information spécifique ou effectuer une action.

Infiltration persistante
Une campagne de longue durée pendant laquelle votre adversaire obtient et maintient un accès non autorisé à votre infrastructure.



[Source]: https://www.slideshare.net/FrodeHommedal/taking-the-attacker-eviction-red-pill
https://www.youtube.com/watch?time_continue=3&v=WAvO0Y0nOws

Fix the Grid!

2.6.1 Principes de sécurité physique

(11) ... les ordinateurs portables, les PC portables de paramétrage ou de commande à distance et les ordinateurs de poche doivent être strictement sécurisés et ne pas être utilisés en dehors du réseau ICS.

https://www.strom.ch/de/media/8302

2.8.3 Accès à distance et authentification

(3) ... Les accès aux stations Jump doivent être effectués au moyen d’une authentification à deux facteurs et peuvent être surveillés et contrôlés à tout moment. (…)

https://www.strom.ch/de/media/8302

alk:~$ Merci de votre attention...