Digitisation and cyber security

Lessons learned from the blackout in the Ukraine

30 August 2022, Swissgrid Grid Forum, Museum of Transport, Lucerne

cyrill.brunschwiler@compass-security.com

How secure is our power supply ?

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

Substation (Mettlen)

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

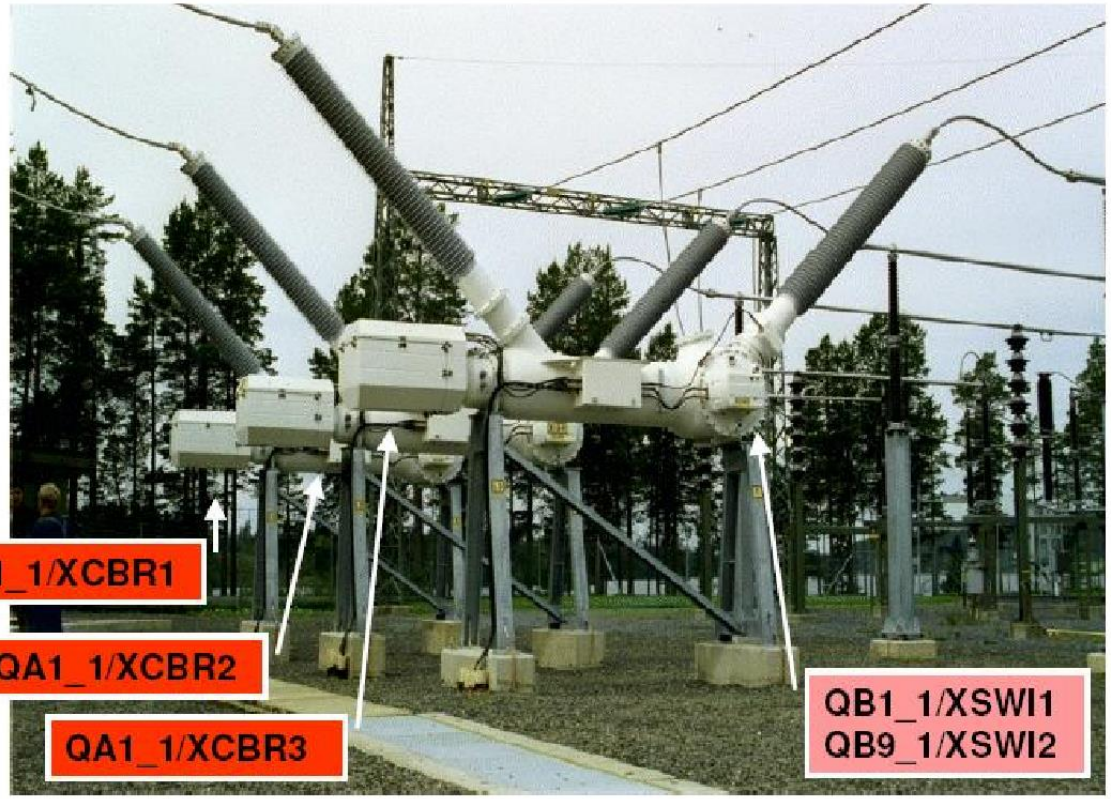
How secure is our power supply?

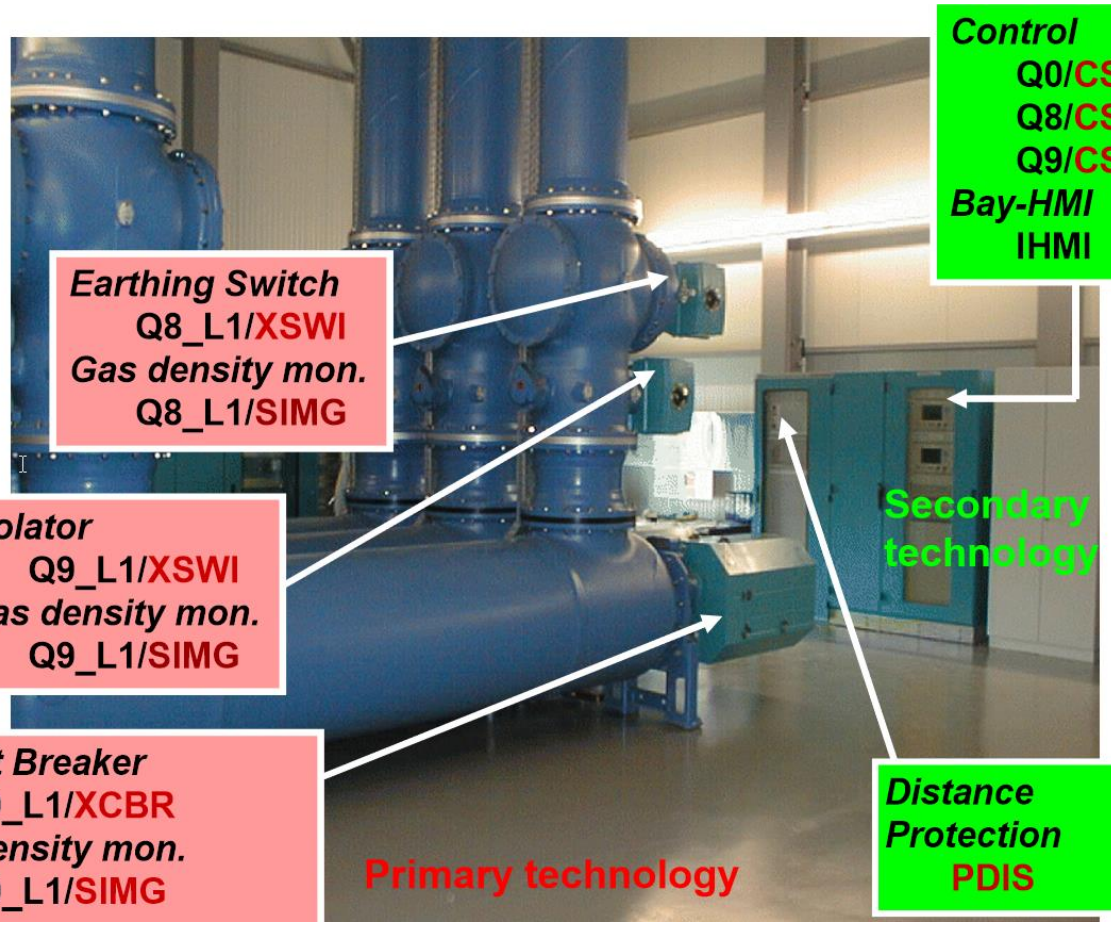
https://www.youtube.com/watch?v=UF5EDV6T7es

Substation protection devices, protocol converters, automation (IEDs)

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

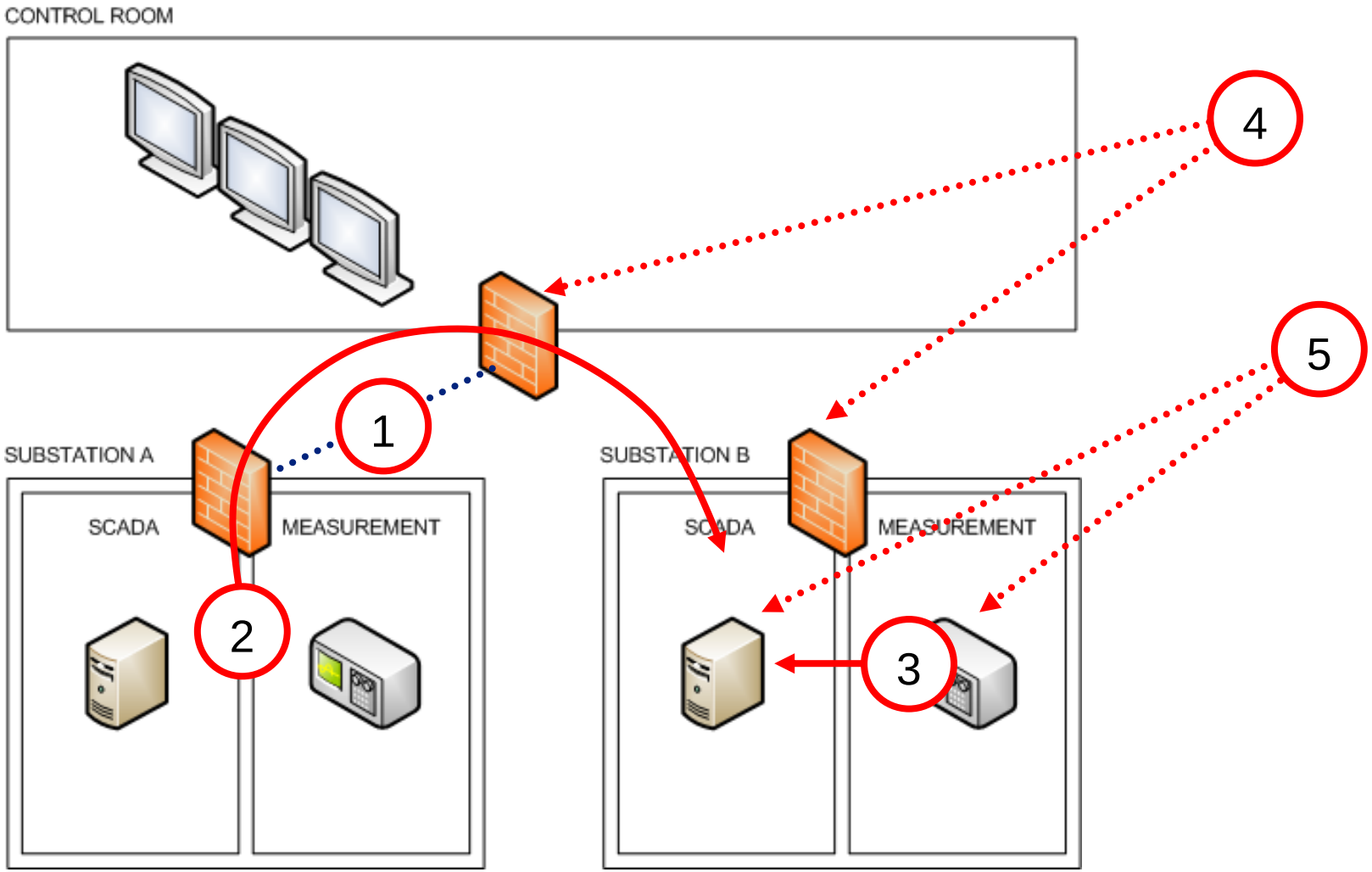
Naming via object model (IEC 61850 MMS)





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

Attacks against substations – scenarios



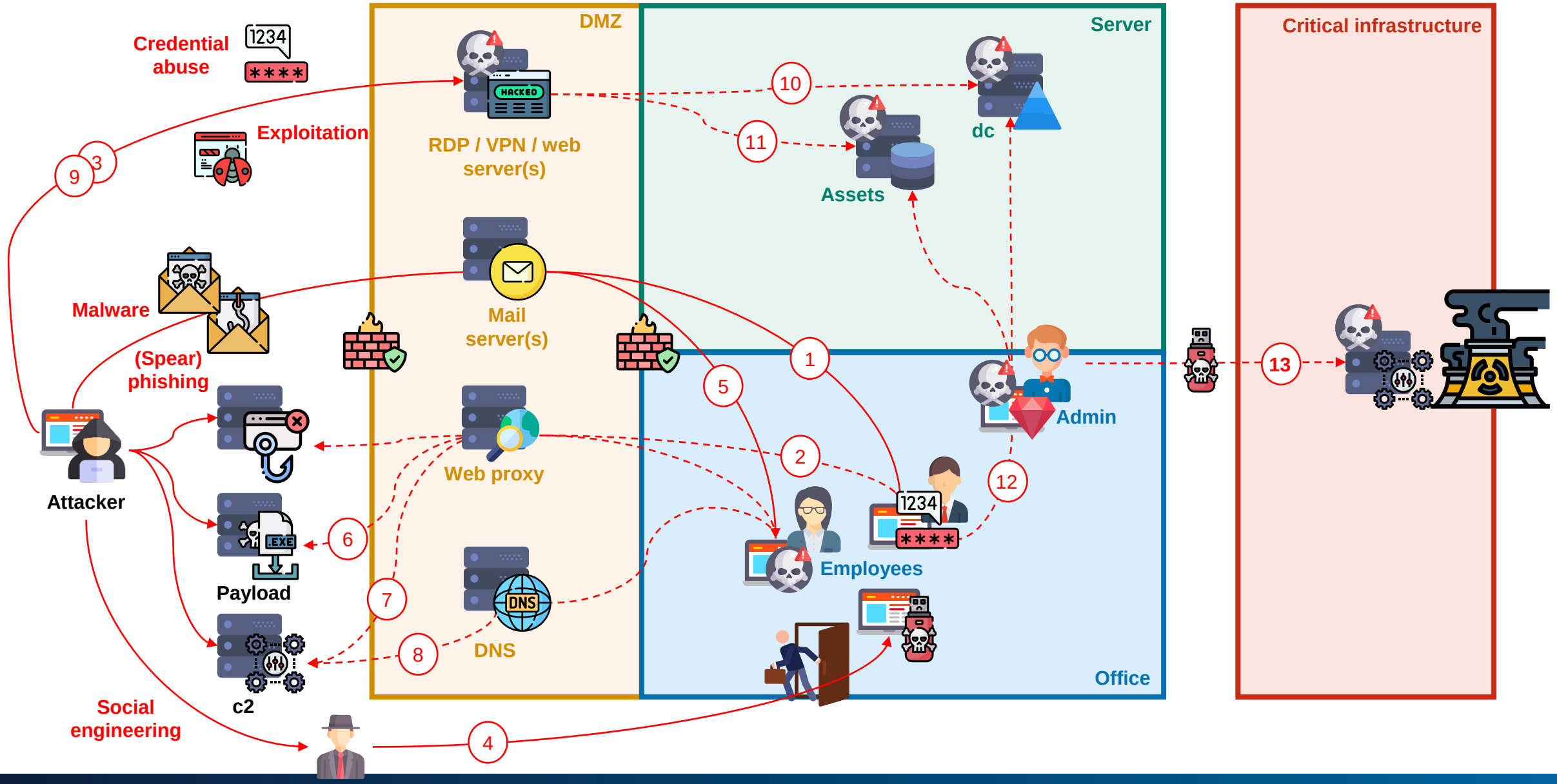
Typical intrusion patterns

Not every intrusion is as ingenious as the media are led to believe.

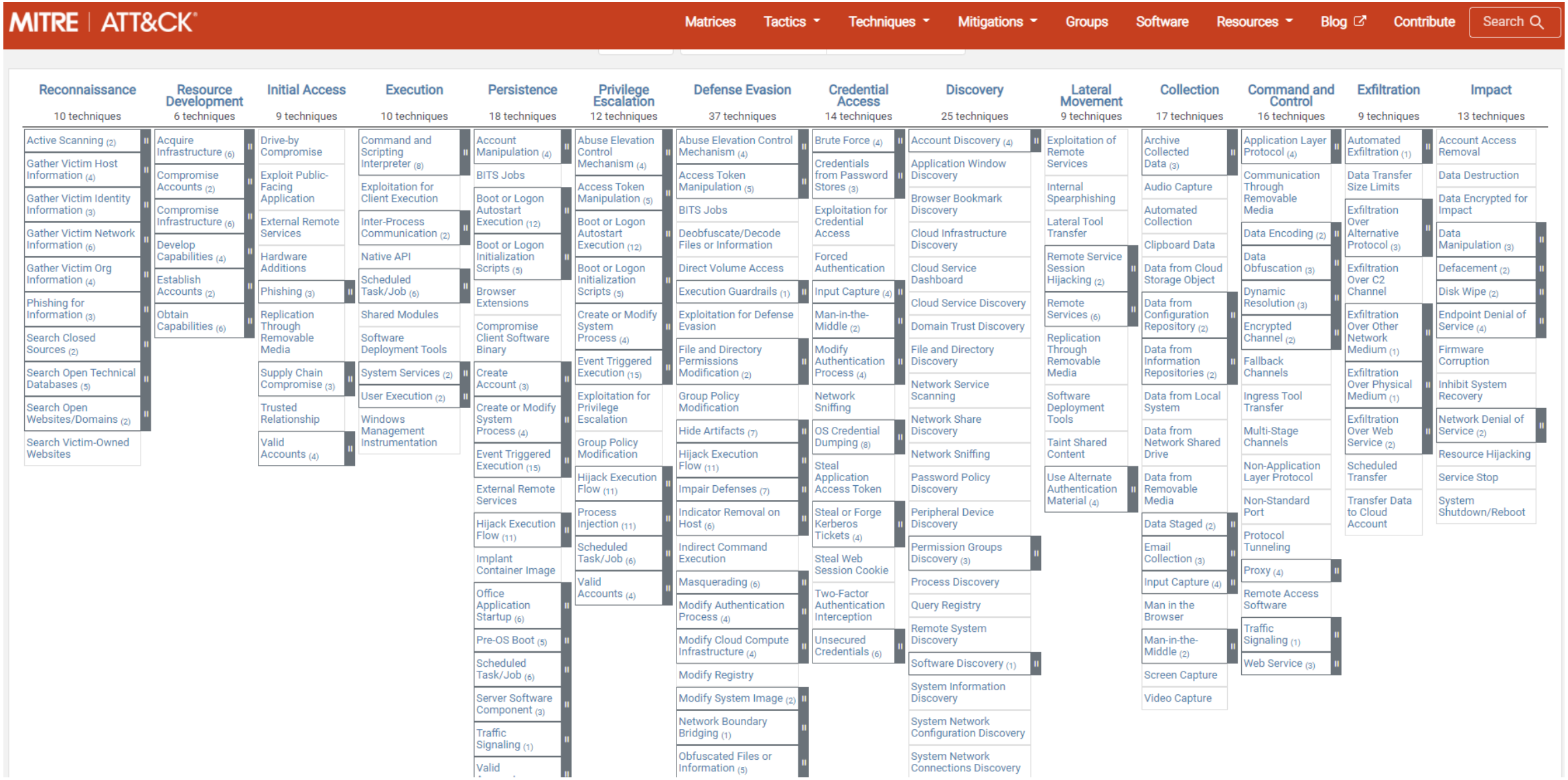
In most cases, security breaches have simple causes:

- Malspam
- Weak passwords
- No 2FA
- Vulnerability of equipment or software (lack of patches)

Typical intrusion patterns



MITRE ATT&CK framework



MITRE ATT&CK framework

Groups

			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'

Ukraine hack

Step 1

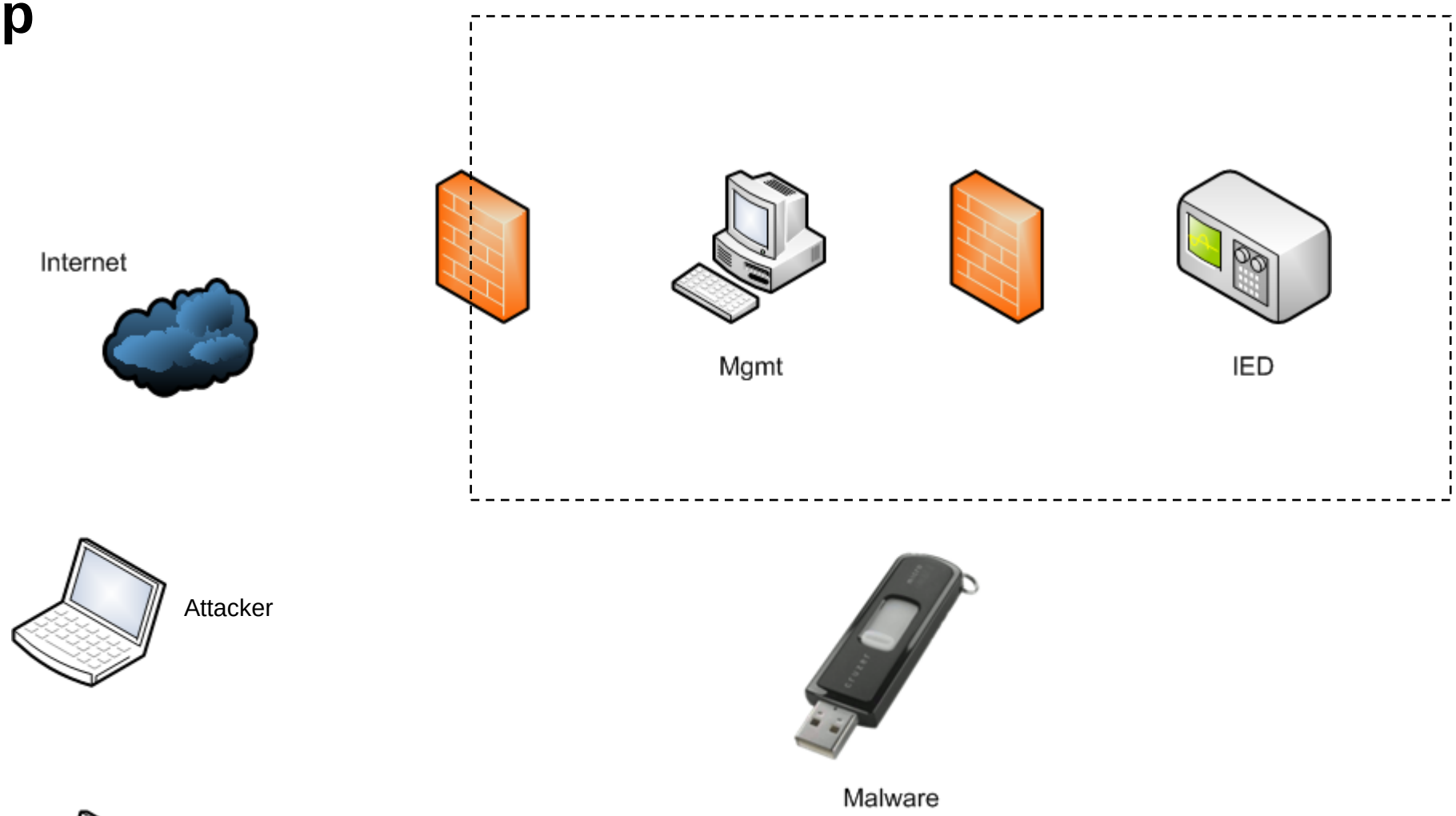
- Phishing e-mails with Word macro, BlackEnergy trojan loaded
- VPN logons and passwords stolen
- Network analysis and lateral movement

Step 2

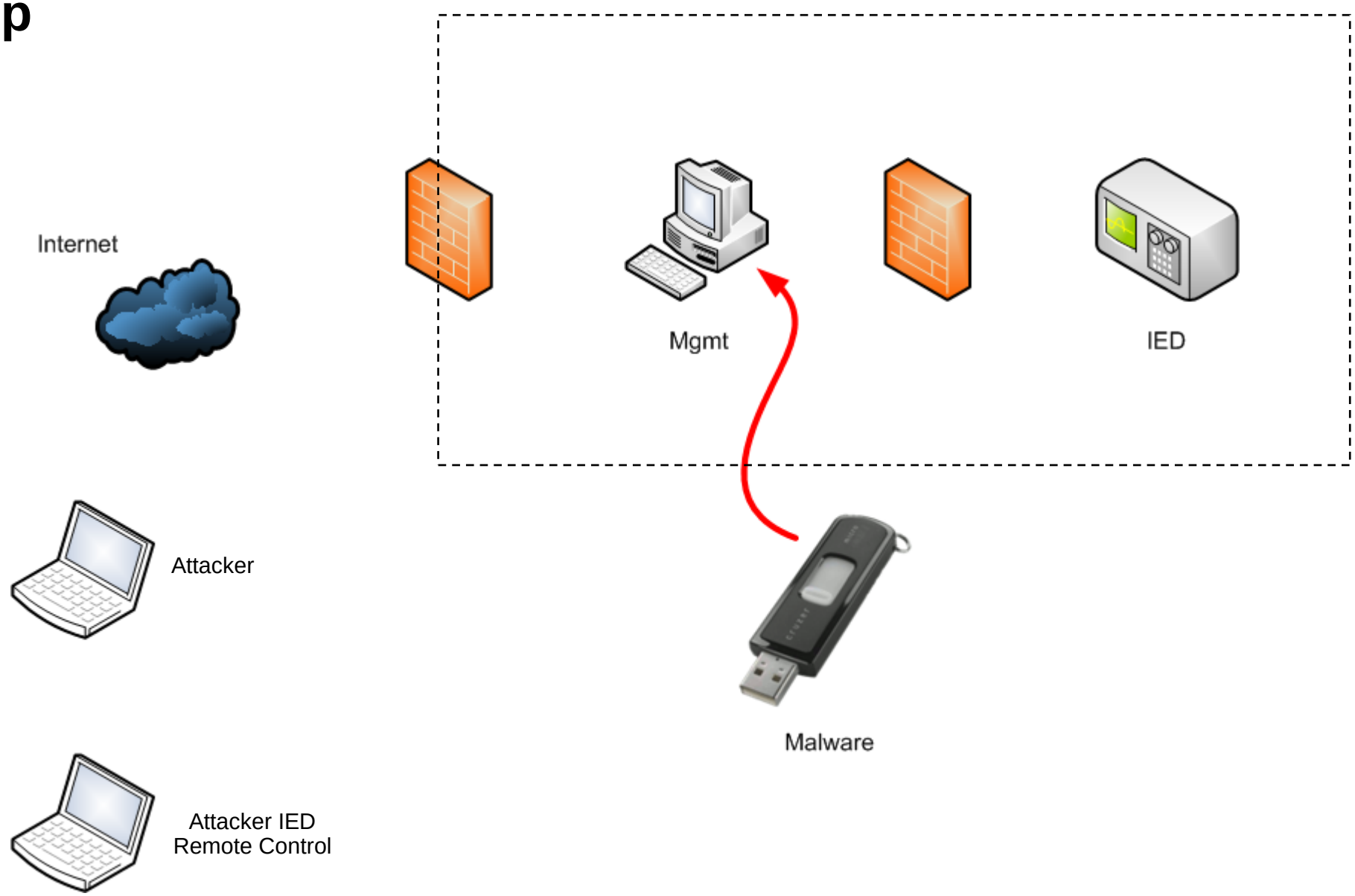
- Malicious firmware developed
- SCADA environment taken over via user interface
- Disconnecting switch opened
- UPS shutdown orchestrated, firmware loaded onto converter, logs and disks deleted
- Denial of telephony service

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

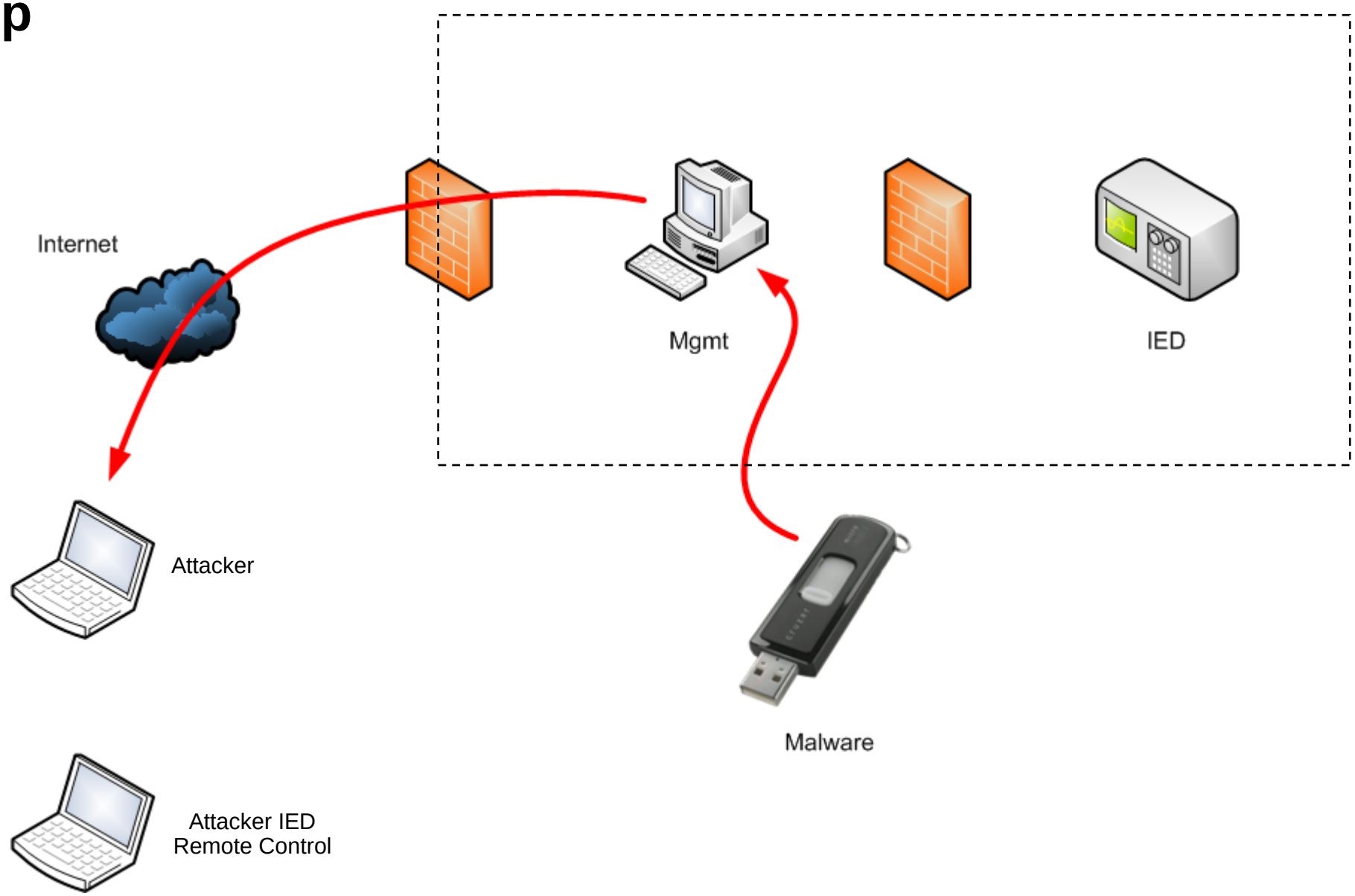
Demo set-up


Internet
Mgmt
IED
Attacker
Malware
Attacker IED
Remote Control

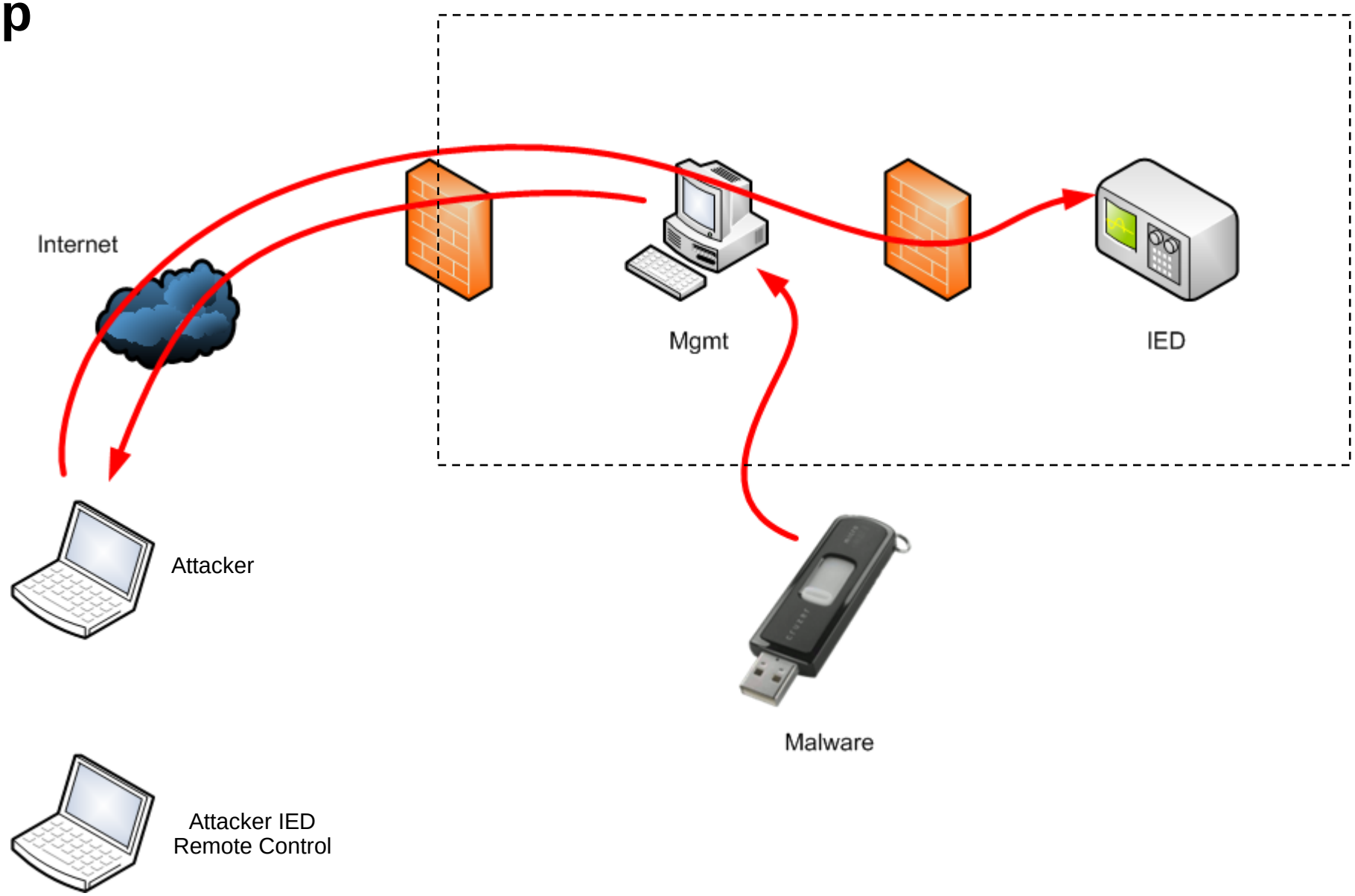
Demo set-up


Internet
Mgmt
IED
Attacker
Malware
Attacker IED
Remote Control

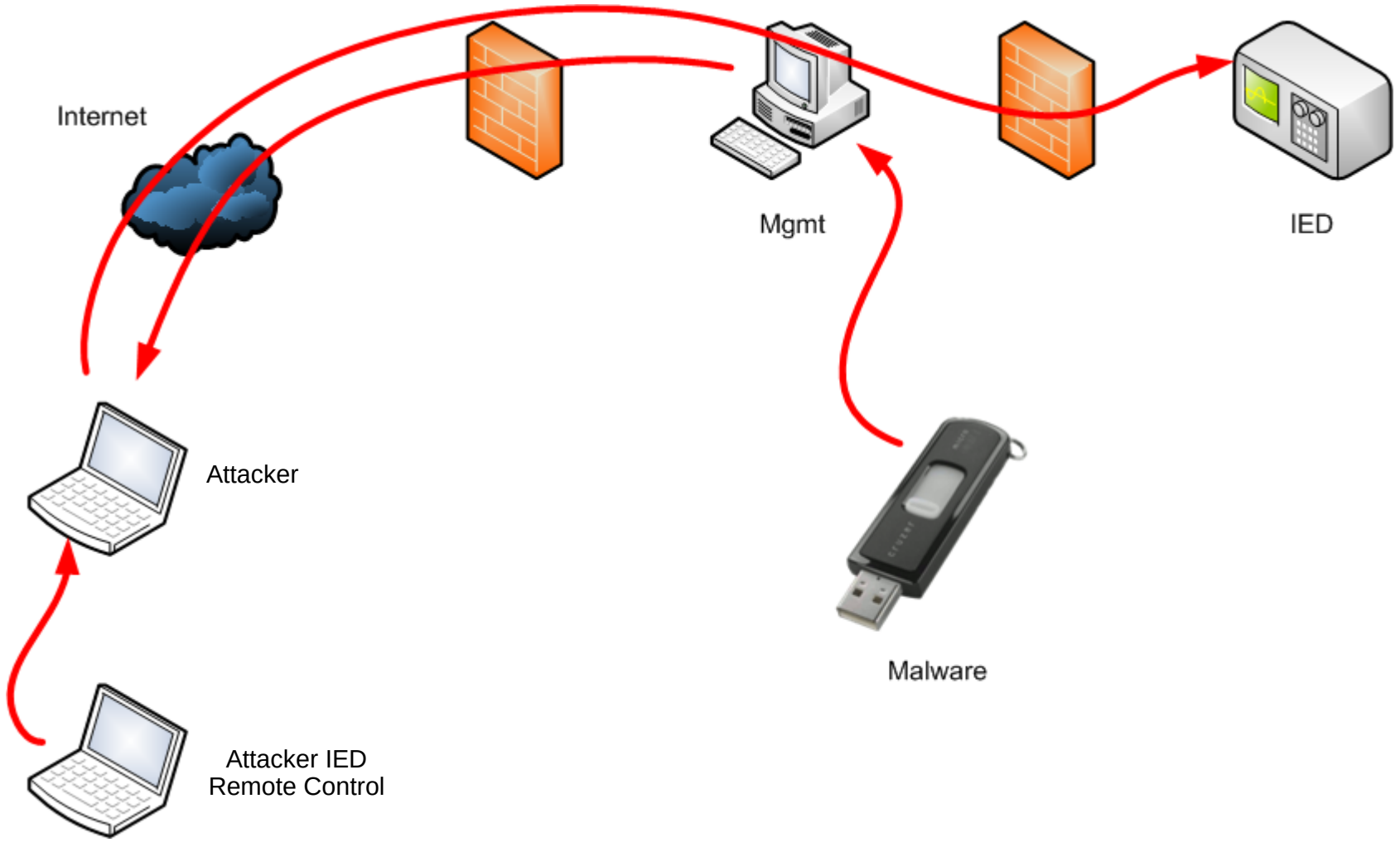
Demo set-up


Internet
Mgmt
IED
Attacker
Malware
Attacker IED
Remote Control

Demo set-up


Internet
Mgmt
IED
Attacker
Malware
Attacker IED
Remote Control

Demo set-up


Internet
Mgmt
IED
Attacker
Malware
Attacker IED
Remote Control

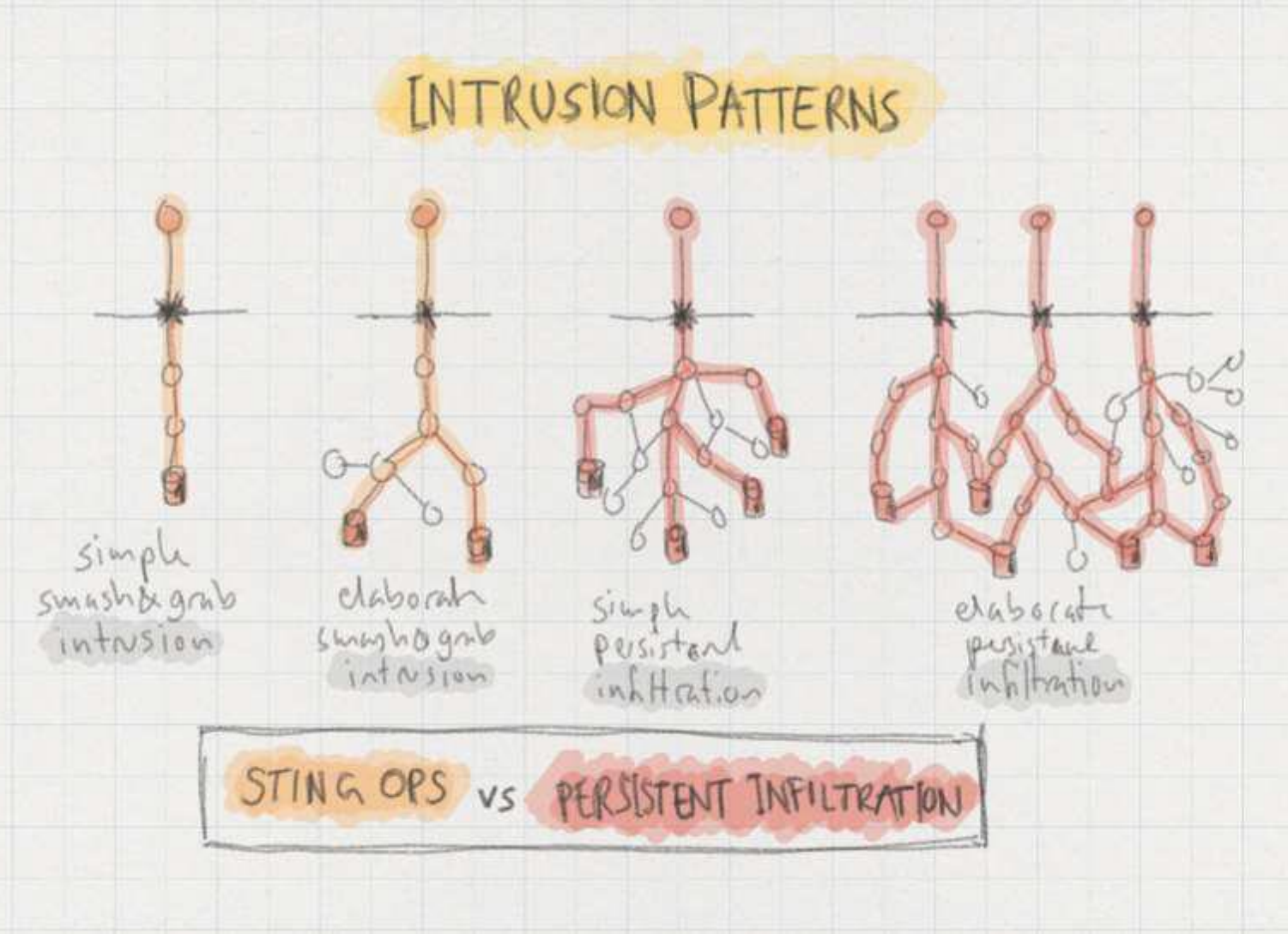
How to react ?

Behaviour of attackers

Intrusion patterns

Sting operation
Also called «smash and grab».
A direct attack to obtain a certain piece of information or to carry out an action.

Persistent infiltration
A prolonged campaign in which your adversary gains and maintains unauthorised access to your infrastructure over an extended period of time.



[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 Physical security principles

(11) ... laptops, portable parameterising or remote-controlled PCs and handheld devices have to be strictly secured and not used outside the ICS network.

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

2.8.3 Remote access and authentication

(3) ... access to the jump stations have to take place by means of two-factor authentication and be monitored and controlled at all times. …

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

alk:~$ Thank you for your attention...