COMGUARD

cyber security masters

Vlákejte útočníky do pasti

Tomáš Koutný | Product Manager
Ondrej Malík | Security Consultant

19.9.2024

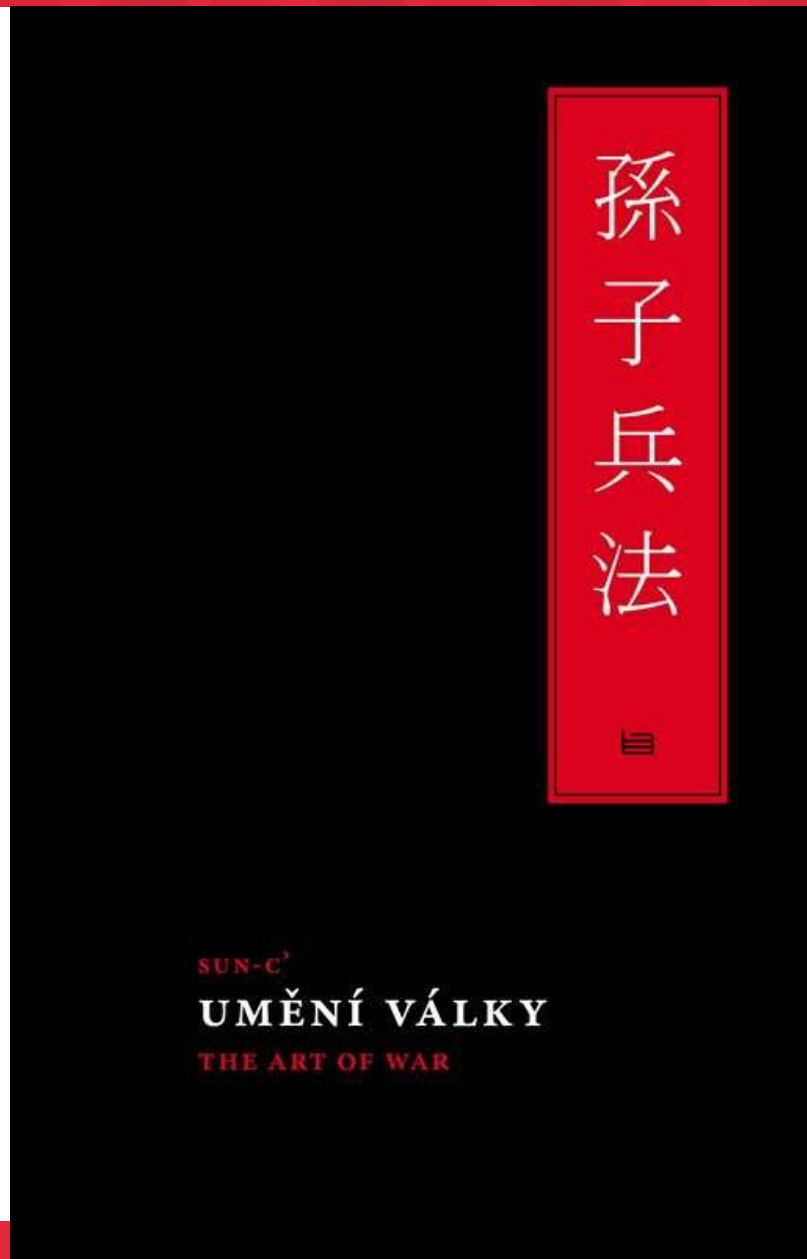
COMGUARD

Oklamání útočníka jako nová forma obrany to je

- Labyrinth byl založen v roce 2019
- HQ v Zabrze, Polsko
- Tým společnosti Labyrinth se zabývá penetračním testováním a Deception technologií, kterou tak testují.
- Oficiální stránky výrobce: www.labyrinth.tech

Techniky klamu

- Předpokládají nevyhnutelnost kompromitace
  - Předkládají útočníkovi podvržené informace pro ovlivnění jeho dalších kroků
  - Odklonění útoku, zdržení a vyčerpání útočníka
  - Okamžitá detekce při interakci s návnadou
  - Proaktivní přístup k horzbě



Dwell Time

Global Median Dwell Time, 2011-2023

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
All	416	243	229	205	146	99	101	78	56	24	21	16	10
External	—	—	—	—	320	107	186	184	141	73	28	19	13
Internal	—	—	—	—	56	80	57.5	50.5	30	12	18	13	9

Zdroj: Mandiant M-Trends 2024

COMGUARD

Reaktívna obrana

- Firewall
- Antivir
- IPS/IDS
- EDR
- SIEM

Aktívna obrana – šedá zóna

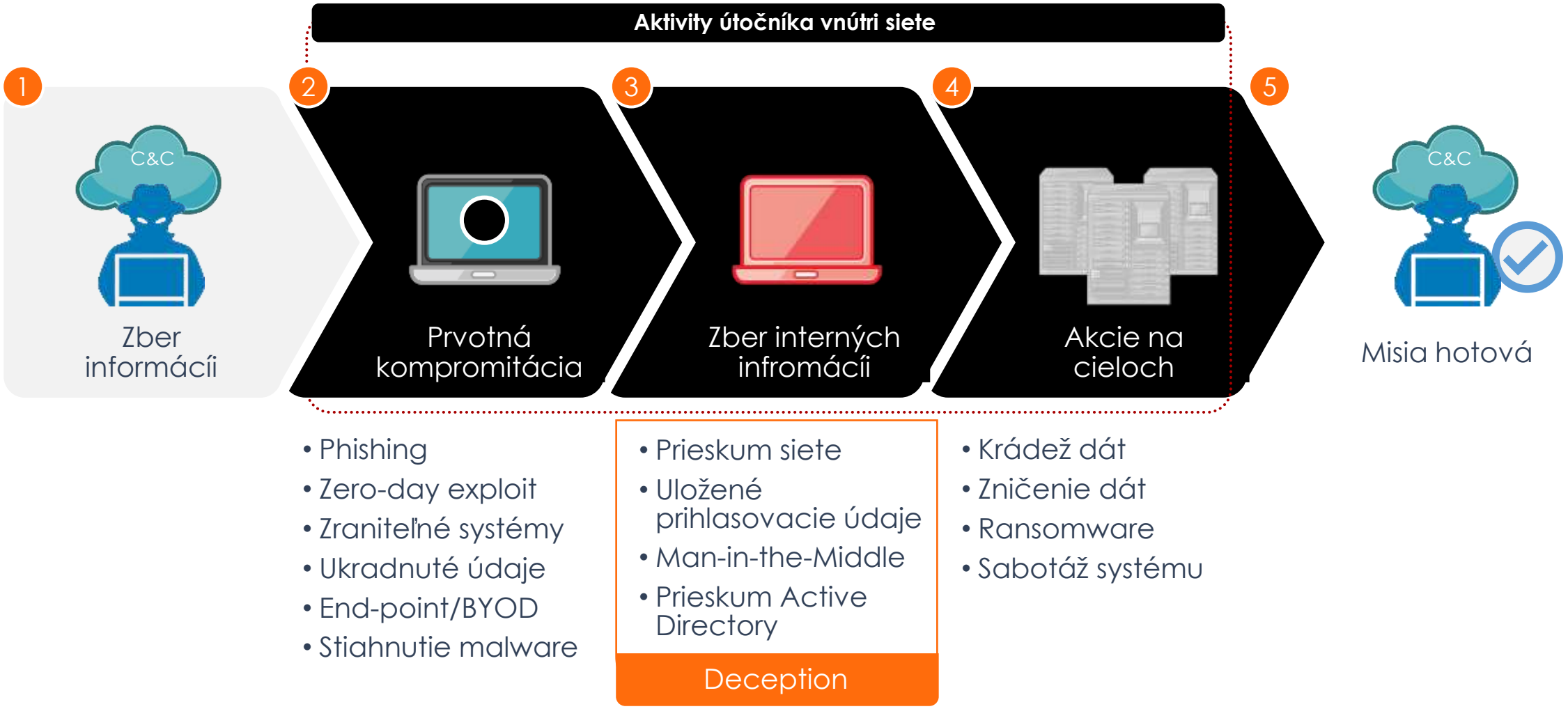
- Red Teaming
- Threat Intelligence
- Threat Hunting
- Deception
- Deterrence

Ofenzivní operace

- Hacking back
- Cyber operations

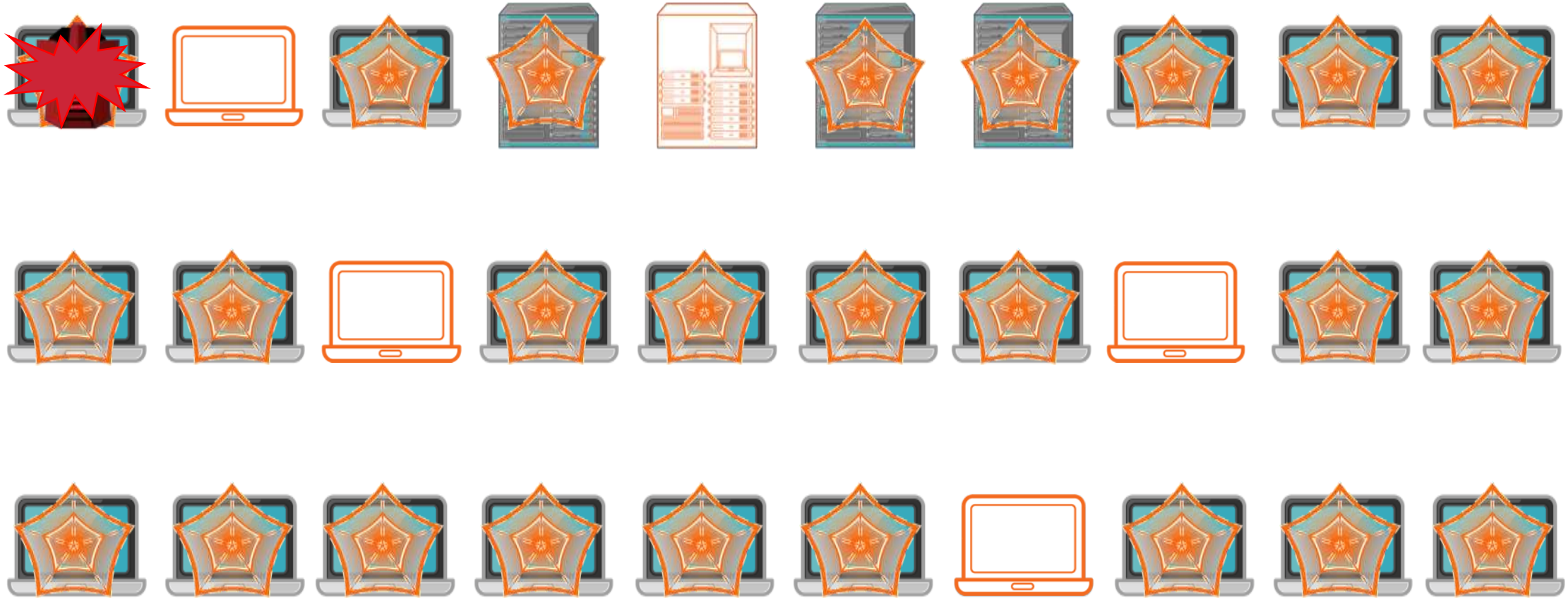
Šedá zóna Aktivní kybernetické obrany (vytvořili Ondřej Nekovář a Jan Pohl DCG420.org)

COMGUARD


Aktivity útočníka vnútri siete
1
2
3
4
5
C&C
Zber informácií
Prvotná kompromitácia
Zber interných infromácií
Akcie na cieloch
C&C
Misia hotová
• Phishing
• Zero-day exploit
• Zraniteľné systémy
• Ukradnuté údaje
• End-point/BYOD
• Stiahnutie malware
• Prieskum siete
• Uložené prihlasovacie údaje
• Man-in-the-Middle
• Prieskum Active Directory
Deception
• Krádež dát
• Zničenie dát
• Ransomware
• Sabotáž systému

Decoys

Z každého endpointu sa stane pasca

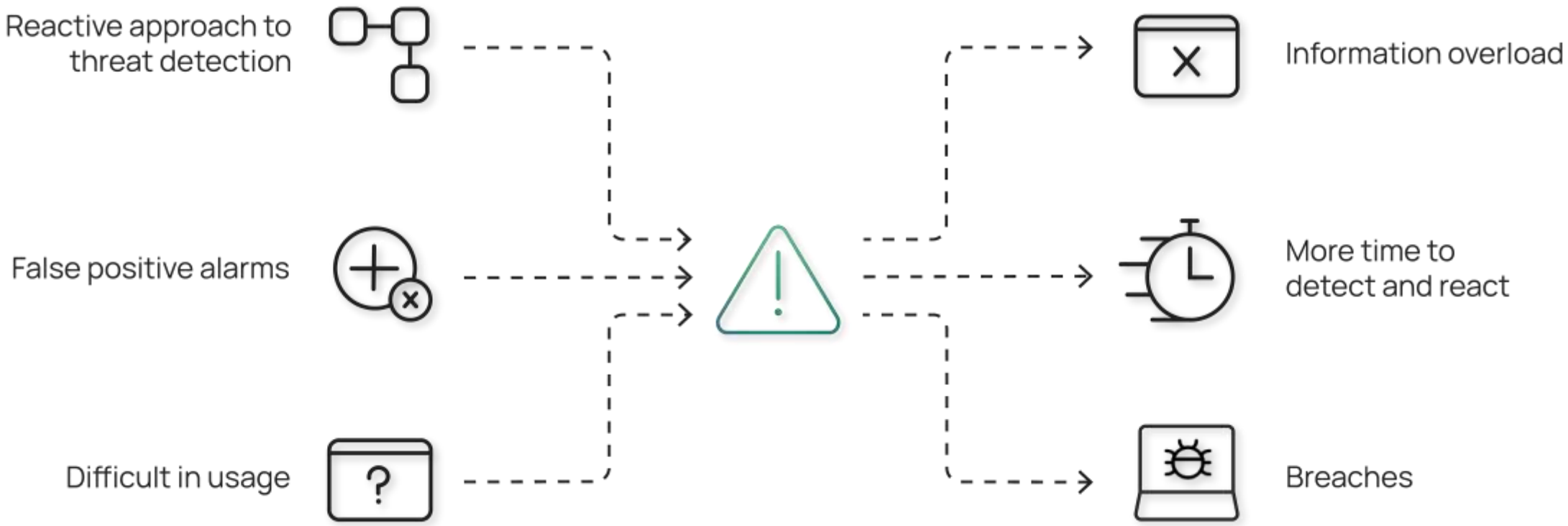


COMGUARD

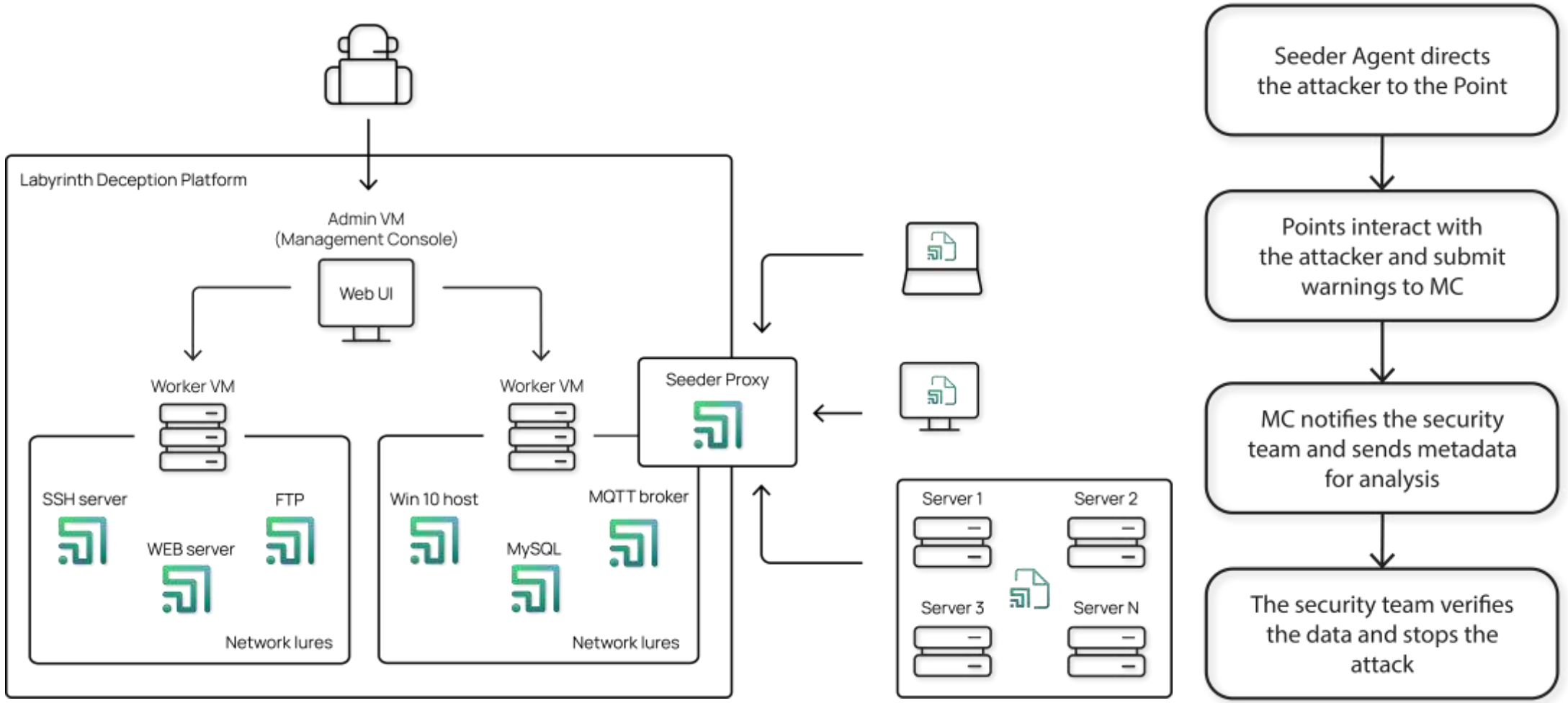
BOTa a Brute Force útoky ⟵ Navrhnuté pre ⟶ Skutočného útočníka

COMGUARD

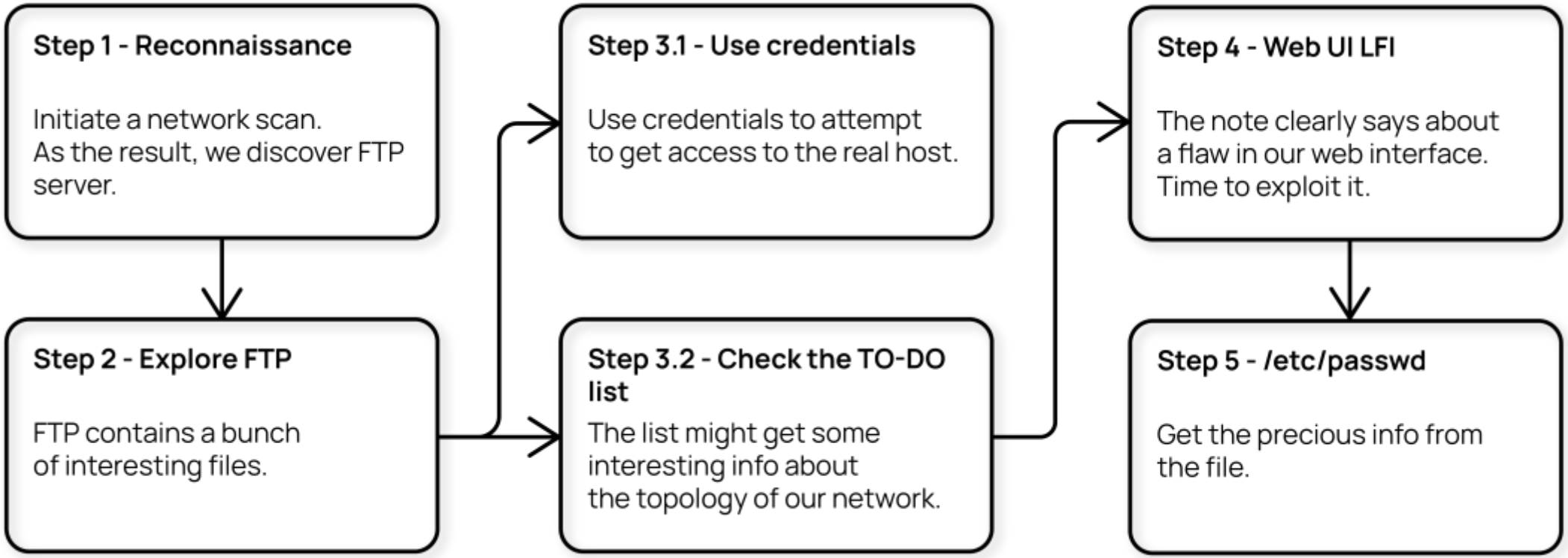
Výzvy v kyberbezpečnosti



Architektúra Labyrinth



Use case – FTP


Step 1 - Reconnaissance
Initiate a network scan.
As the result, we discover FTP server.
Step 2 - Explore FTP
FTP contains a bunch of interesting files.
Step 3.1 - Use credentials
Use credentials to attempt to get access to the real host.
Step 3.2 - Check the TO-DO list
The list might get some interesting info about the topology of our network.
Step 4 - Web UI LFI
The note clearly says about a flaw in our web interface. Time to exploit it.
Step 5 - /etc/passwd
Get the precious info from the file.

Trellix

COMGUARD

cyber security masters

Děkujeme za pozornost!

Tomáš Koutný | tomas.koutny@comguard.cz

Ondrej Malík | ondrej.malik@comguard.cz