

COMGUARD
communication security

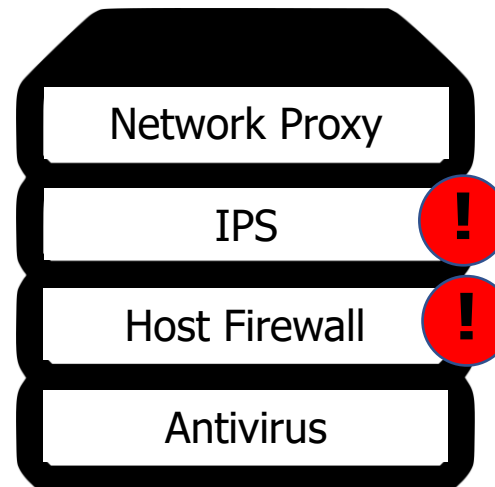
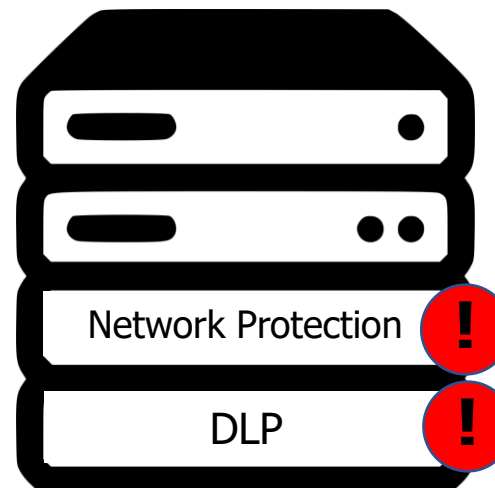
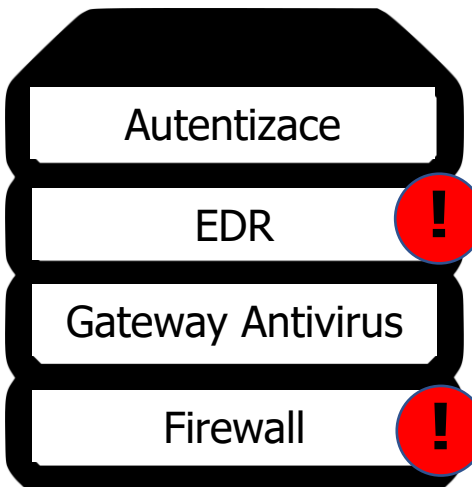


Attivo Networks – Využití technik klamu k detekci post-breach aktivit

Lukáš Babčický | Vendor Manager
Ondrej Malík | Security Consultant



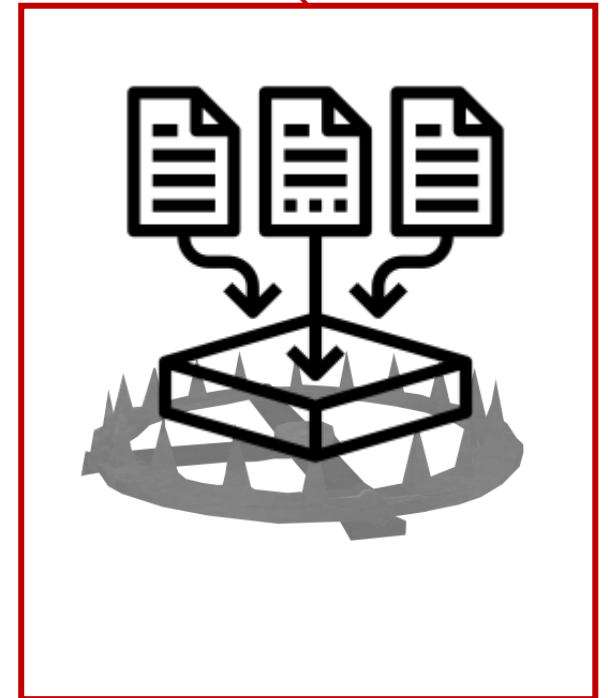
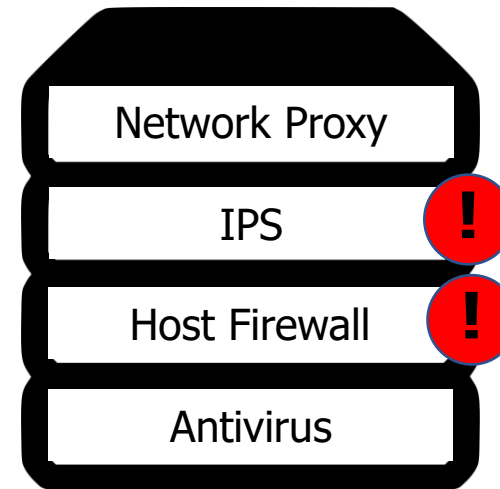
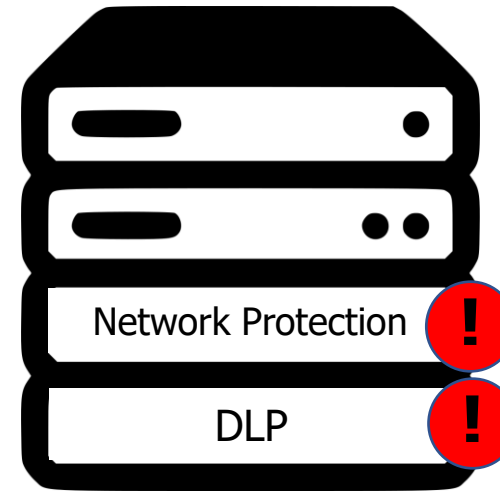
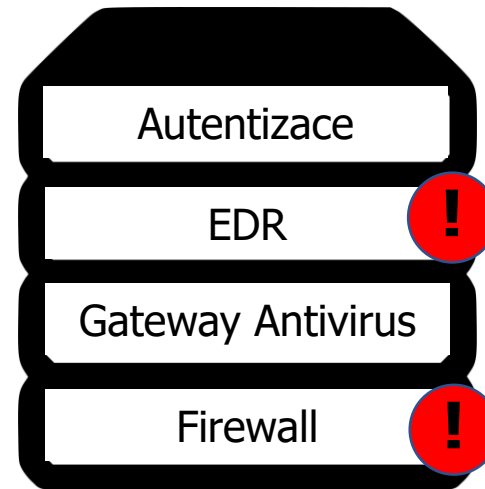
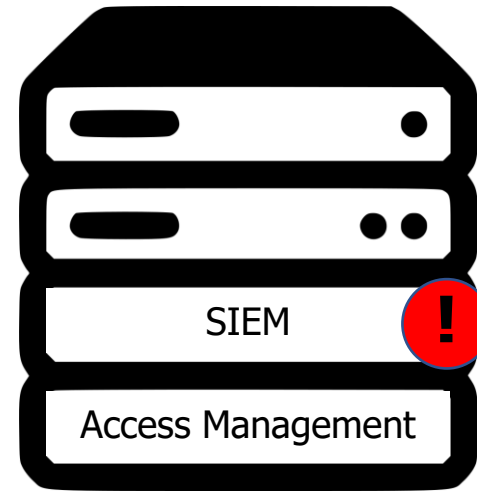
Externí útočníci
Insider Threats



Business-critical prvky

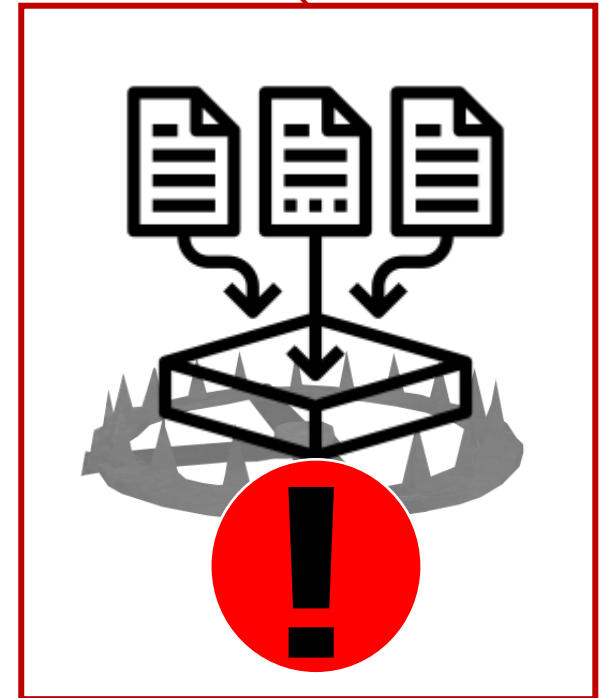
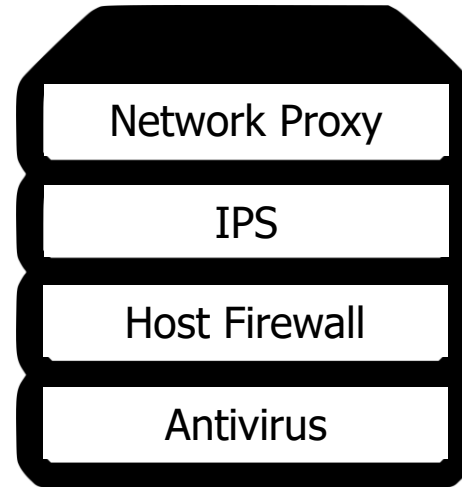
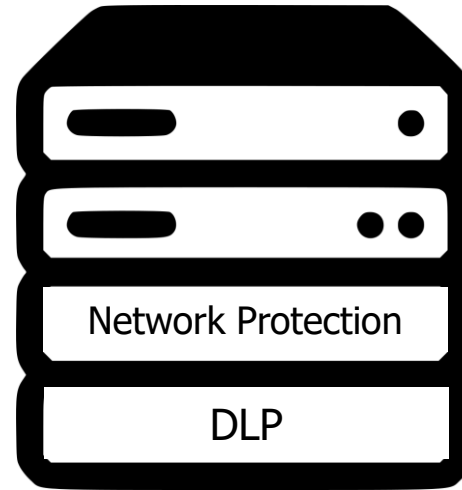
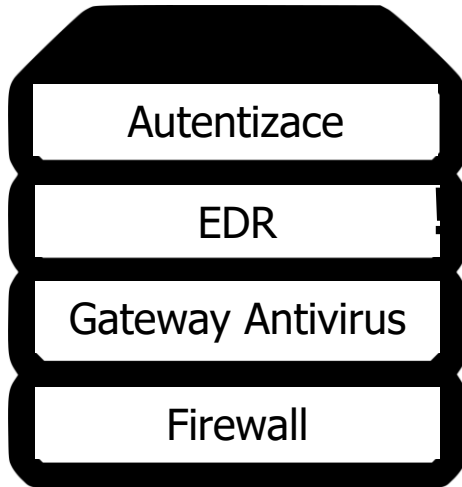


Externí útočníci
Insider Threats





Externí útočníci
Insider Threats



„Za války je pravda natolik drahocenná, že ji musí vždy doprovázet tělesná stráž lží.“

-Winston Churchill

- Operace Bodyguard
 - Spojenecká kampaň klamu zacílená na manipulaci strategie Německa
 - Zajistila úspěch invaze na Sicílii a vylodění v Normandii



The pathologist Sir Bernard Spilsbury, who assisted with the operation



The corpse of Glyndwr Michael, dressed as Martin, just prior to placement in the canister



A dummy Sherman tank



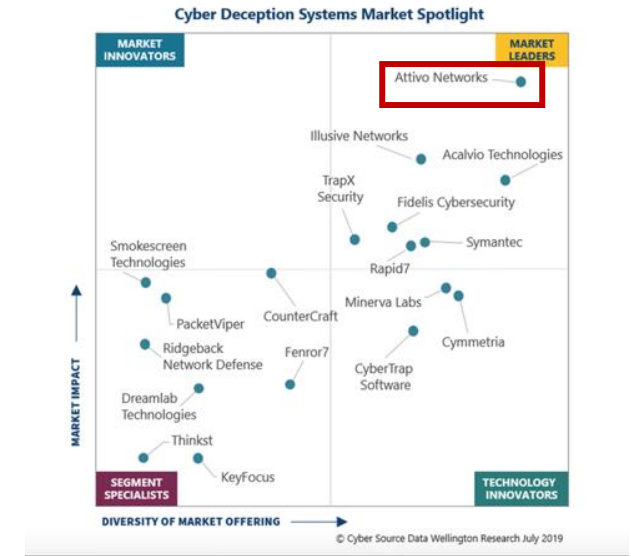
Dummy landing craft

- Útočník
 - Social engineering
 - Phishingové kampaně
 - Krádeže identit
 - Obfuskace aktivit

- Útočník
 - Social engineering
 - Phishingové kampaně
 - Krádeže identit
 - Obfuskace aktivit
- Obránce
 - Honeypots
 - Tarpits
 - Beacons
 - Traps



- Globální leader na poli Deception Technologies
 - Inovátor v oblasti detekce post-breach aktivit
 - Nejrozsáhlejší Deception Technology vendor na trhu
 - Široká škála partnerských integrací pro orchestraci reakcí
-
- Desítky ocenění nezávislých agentur
 - Pokrytí 50% Fortune 100 companies



Threat Deception Platform Comparison Summary

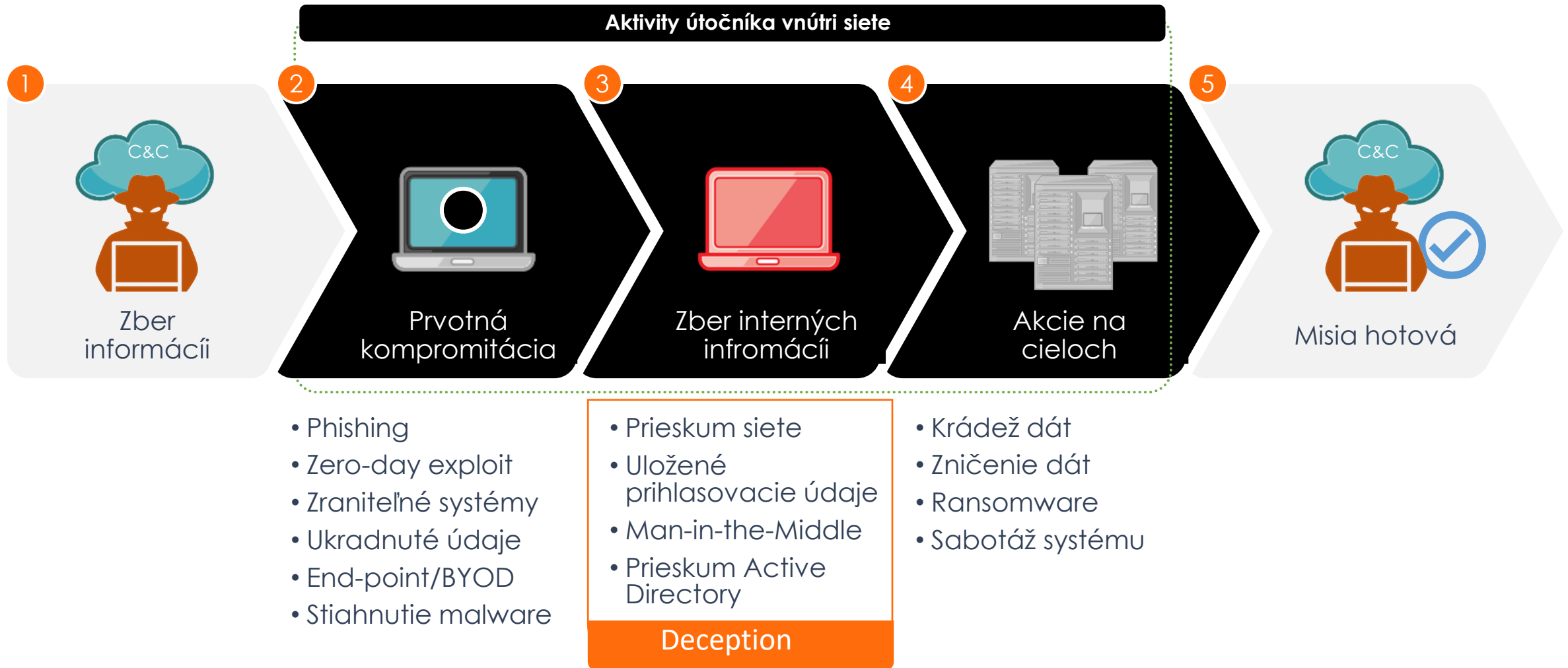
	Acalvio	Attivo Networks	Cymmetria	Illusive Networks	Smokescreen	TrapX
Assessment Criterion						
Supported Deception Types						
Network IT Decoys	H	H	H	H	H	H
Network Device Decoys	M	M	H	M	H	H
Endpoint Lures	H	H	H	H	H	H
Other Deception Types	M	H	H	M	H	H
Deployment Management Capabilities						
Traffic Delivery to Decoys	H	H	M	M	H	M
Lure Deployment Machinery	M	H	M	H	M	H
Environment Learning Capabilities	H	H	M	H	H	M
Automated Deception Customization	H	H	L	H	H	M
Enterprise Management Features	M	H	M	H	M	M
Threat Detection and Response						
Decoy Data Gathering	H	H	H	H	H	H
Additional Data Gathering	H	H	L	H	H	H
Containment Actions Capabilities	H	H	L	M	H	H
Exporting Attack Data Capabilities	H	H	H	M	H	M
Deception Credibility and Authenticity	H	H	M	H	H	H

Legend: 3 High, 2 Medium, 1 Low, 0 None

Source: Gartner © 373459



Priebeh útoku a metódy



Premýšľaj ako útočník, následne aplikuj deception



Prihlasovacie údaje v pamäti

Prepojenia na ďalšie systémy

Dotazovanie Active Directory

Prístup k dátam v sieti

Prieskum siete

Prístup k dokumentom

FAKKE



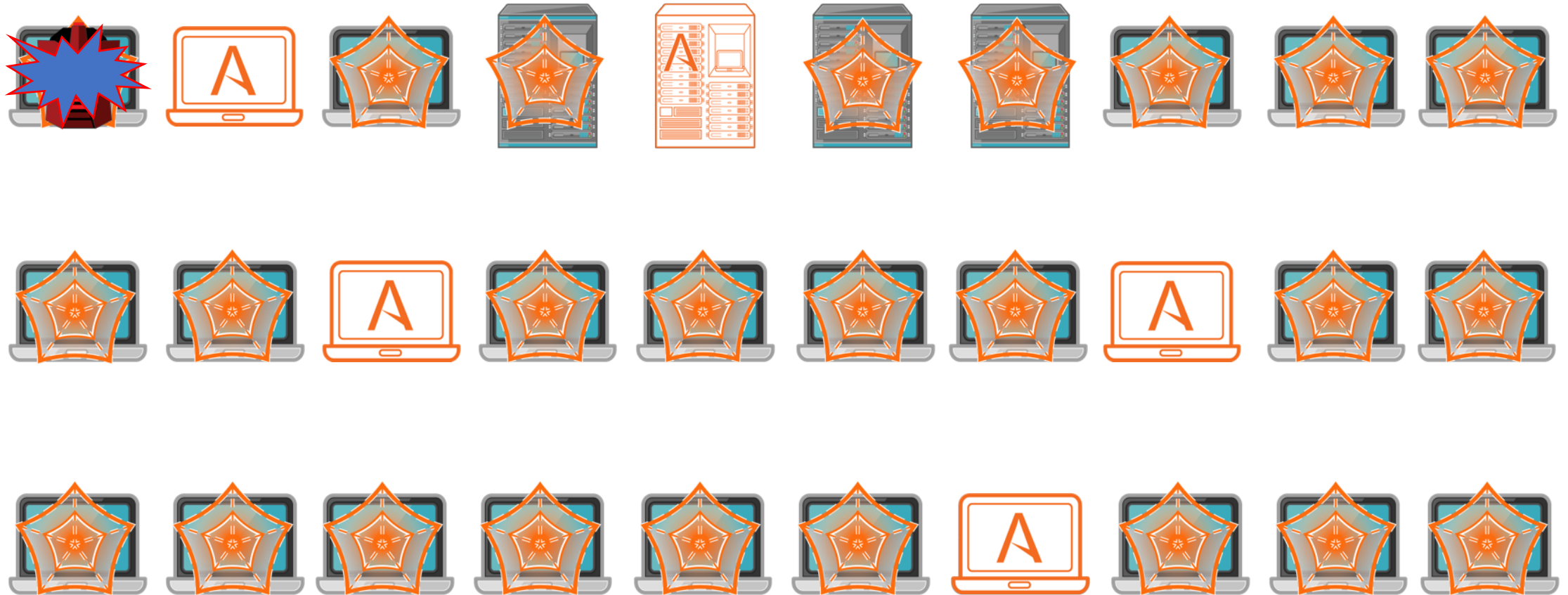
ALERTY!

Autentické systémy - Decoys



Endpoint Detection Net

Z každého endpointu sa stane pasca



Honeypoty VS Deception

Honeypoty

- Malá interakcia
- Imitácia prostredia
- Mimo skutočnú sieť

Technológia Deception

- Automatická IR
- Jednoduchá správa
- Dynamický klam
- Reálny OS, Služby
- Sieť, Prihl. údaje
- Priamo v sieti



BOTa a Brute Force útoky

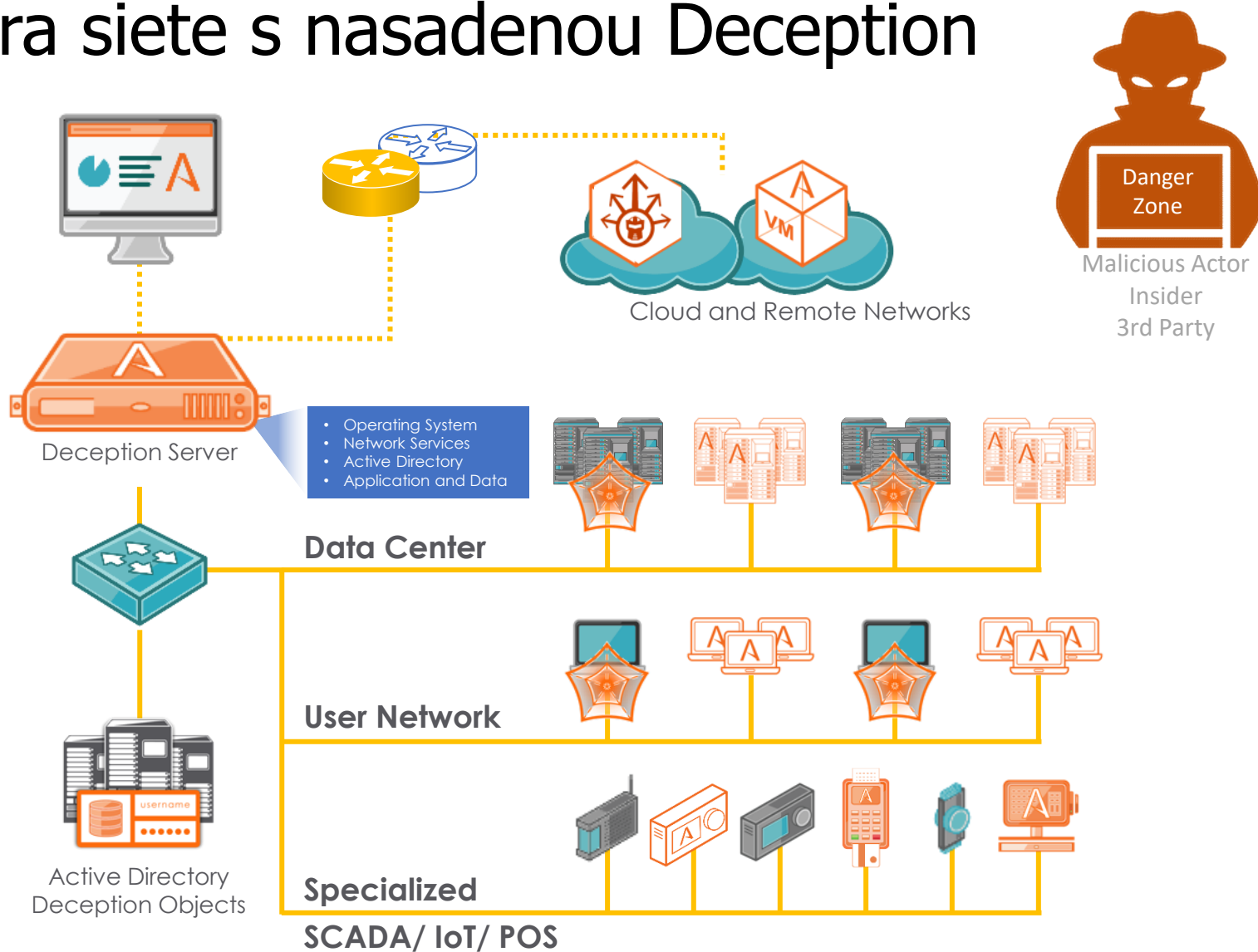


Navrhnuté pre



Skutočného útočníka

Architektúra siete s nasadenou Deception



Autenticita Attivo platformy



UŽIVATEĽSKÉ DATA



- Memory credentials
- Active connections
- Credential lures
- SMB shares lures
- Browser credentials, history, shortcuts
- Application credentials
- Vulnerable data in SMB Shares
- PC, Mac, Linux deceptive credentials



APLIKÁCIE | *PLNE KONFIGUROVATEĽNÉ*

- FTP/SFTP
- HTTP/HTTPS
- Print
- SMB
- NBNS
- SSH
- SMTP
- SWIFT Messaging
- SNMP
- Telnet
- RDP
- GIT
- mDNS
- MySQL
- Apache
- Tomcat
- Jboss
- SVN/CVS
- VPN
- Mongo DB, ES, Redis
- WinRM
- AD
- MSSQL

ICS/SCADA

- Modbus
- BACnet
- Siemens S7comm
- IPMI
- Common Industrial Protocol (CIP)

IoT/IoE

- MQTT
- CoAP
- XMPP
- Health Level-7
- Digital Imaging & Comms in Medicine (DICOM)

OPERAČNÉ SYSTÉMY

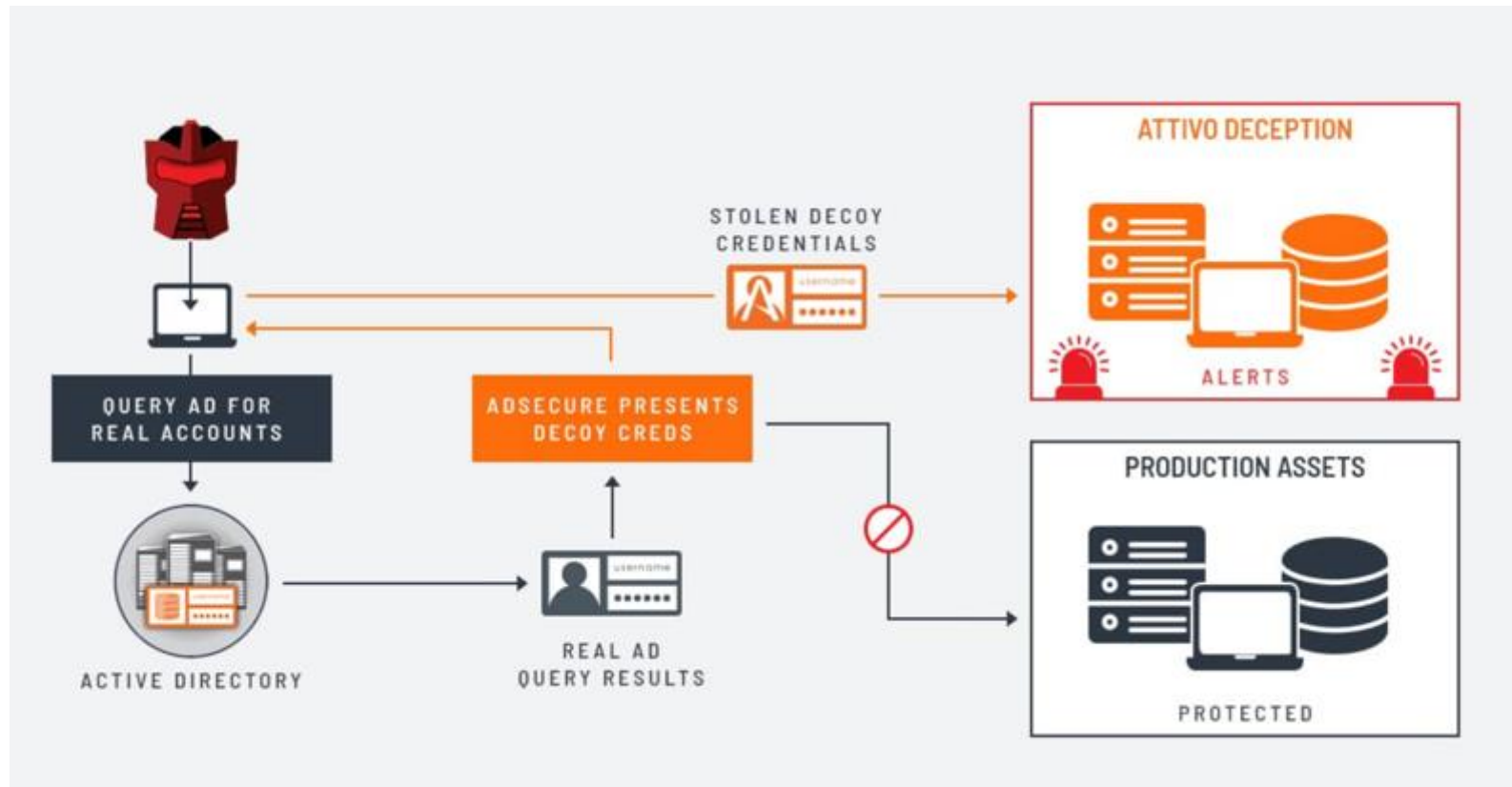


PLATFORMY



ADSecure

Ochrana pred útokom na Active Directory



* Podporuje známe AD objekty (admins, service accounts, critical computers, net sessions)

Netsess.exe

Odkiaľ sú doménový admini prihlásení?

```
Command Prompt
C:\Users\sedemo.SEDEMO\Documents\Tools>NetSess.exe sedemo.local
NetSess V02.00.00cpp Joe Richards (joe@joeware.net) January 2004
Enumerating Host: sedemo.local
Client      User Name      Time      Idle Time
-----
\\\\10.10.16.200    Dwight.Bender  000:01:46  000:01:35
\\\\10.10.16.200    Amy.Gulley     000:01:46  000:01:30
\\\\10.10.16.200    Zelda.Ramos    000:01:45  000:01:30
\\\\10.10.16.200    John.Cain     000:01:45  000:01:30
\\\\10.10.16.200    Amos.King     000:01:46  000:01:35
\\\\10.10.17.11     sedemo        000:00:00  000:00:00
\\\\10.10.16.200    Jack.Kruse    000:01:45  000:01:30
Total of 7 entries enumerated
C:\Users\sedemo.SEDEMO\Documents\Tools>
```











































Falošní uživatelé

```
Command Prompt
C:\Users\sedemo.SEDEMO\Documents\Tools>NetSess.exe sedemo.local
NetSess V02.00.00cpp Joe Richard (joe@joeware.net) January 2004
Enumerating Host: sedemo.local
Client      User Name      Time      Idle Time
-----
--
\\\\10.10.17.24     gandalf-adm    000:02:27  000:02:16
\\\\10.10.15.20     samwise-adm    000:02:27  000:02:11
\\\\10.10.17.10     sedemo        000:00:00  000:00:00
\\\\10.10.16.200    Zelda.Ramos    000:02:26  000:02:11
\\\\10.10.16.22     cypher        000:02:26  000:02:11
\\\\10.10.15.20     hansolo       000:02:27  000:02:16
Total of 6 entries enumerated
C:\Users\sedemo.SEDEMO\Documents\Tools>
```

Decoy systémy

- Útočník použije Netsess pre zistenie, odkiaľ sú prihlásení doménový administrátori
- ADSecure ukryje reálne Netsess a nahradí ich falošnými užívateľmi a decoy systémami
- **ADSecure presmeruje útočníka do existujúcej decoy infraštruktúry**

Attivo Networks: Integrácie s natívnymi partnermi

Respond: Network Blocking	Investigate: Analysis & Hunting	Respond: Endpoint Quarantine
     	         	         
Endpoint Distribution	 	Cloud Monitoring
   <p>Endpoint management solutions (ECM, WMI, Casper, etc.)</p>	Orchestration	   
Integrations to Attivo API	   	Redirection
 	Ticketing	 

COMGUARD
communication security



Děkujeme za pozornost!

Lukáš Babčický | lukas.babcicky@comguard.cz

Ondrej Malík | ondrej.malik@comguard.cz