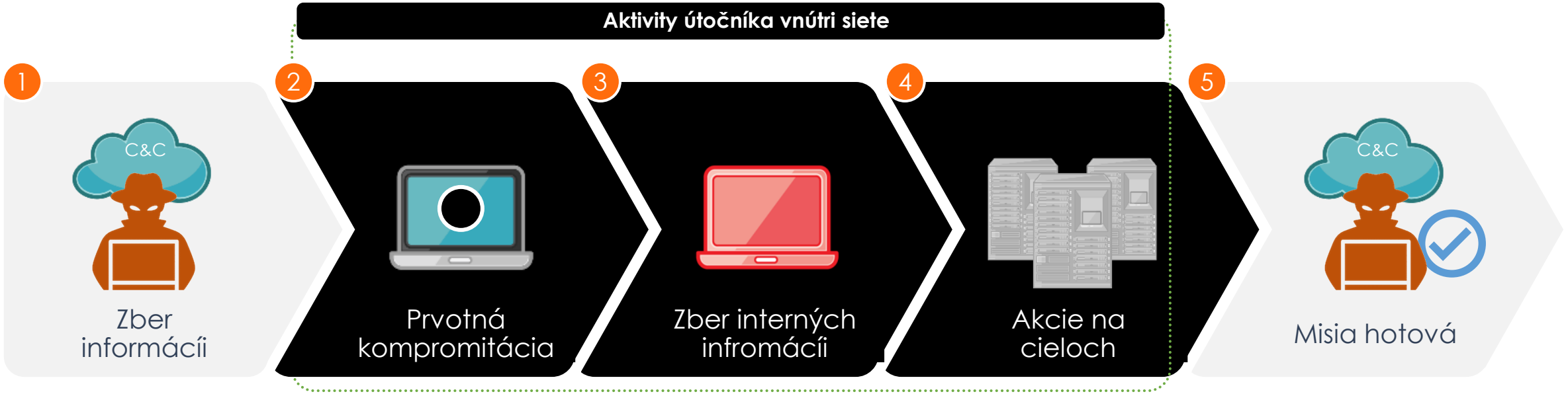
COMGUARD
communication security

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

Ondrej Malík | Security Consultant

Priebeh útoku a metódy



- 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

Premýšlaj ako útočník, následne aplikuj deception

- Prihlasovacie údaje v pamäti
- Prepojenia na ďalšie systémy
- Dotazovanie Active Directory
- Pohyb in the network
- Priestupom siete
- Prístup k dokumentom

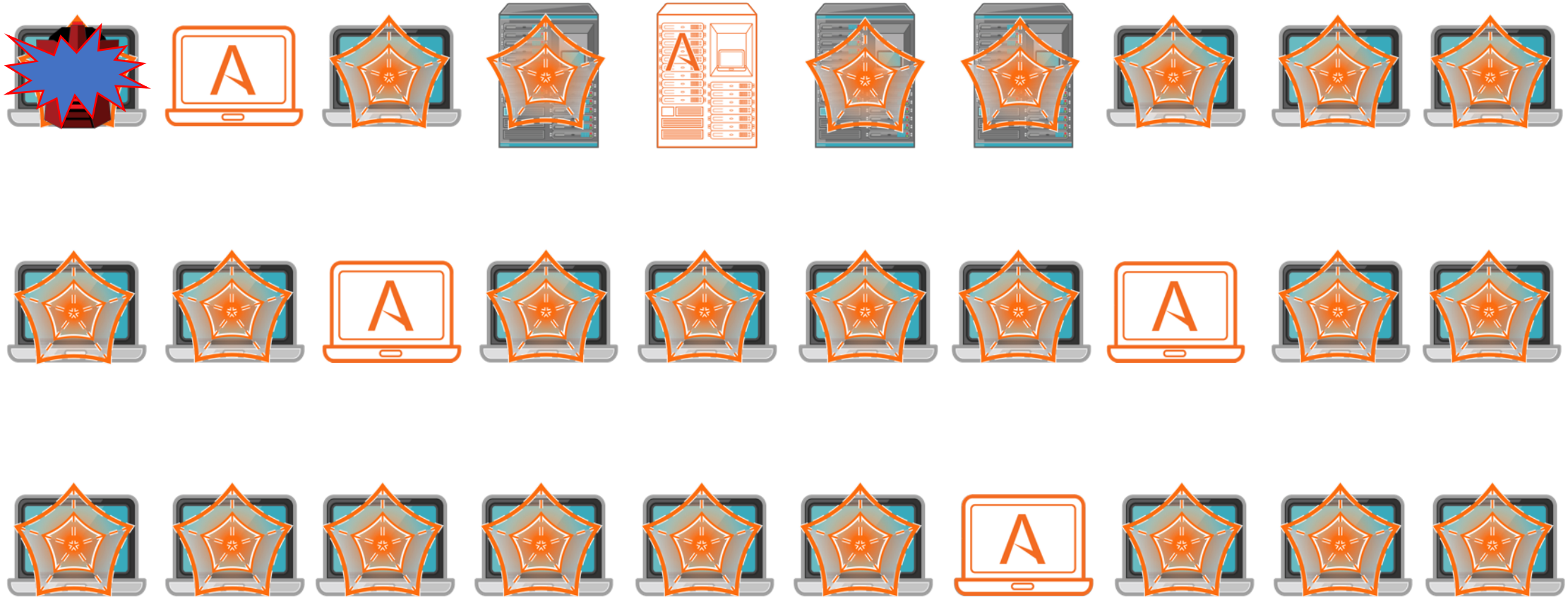
FAKE

ALERTY!

Autentické systémy - Decoys

Endpoint Detection Net

Z každého endpointu sa stane pasca



Honeypoty VS Deception

Honeypoty

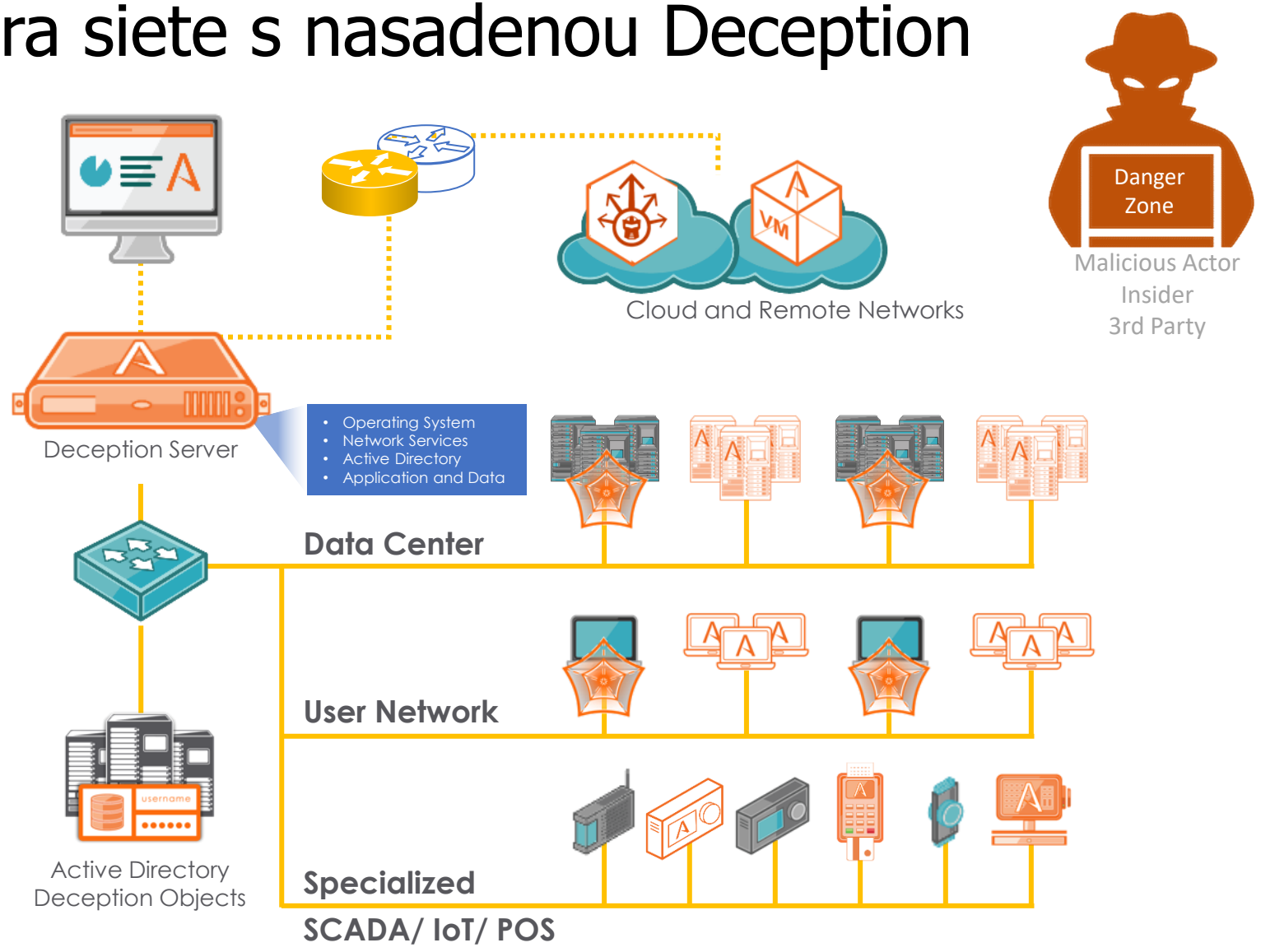
- Malá interakcia
- Imitácia prostredia
- Mimo skutočnú sieť

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

UŽÍVATEĽSKÉ 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

Windows XP 7 8 10 2008 2012 2016

ubuntu 12.04 & later

CentOS

redhat 6.5

Cisco IOS SOFTWARE

PLATFORMY

amazon web services

Microsoft Azure

openstack.

ORACLE CLOUD

Microsoft Hyper-v

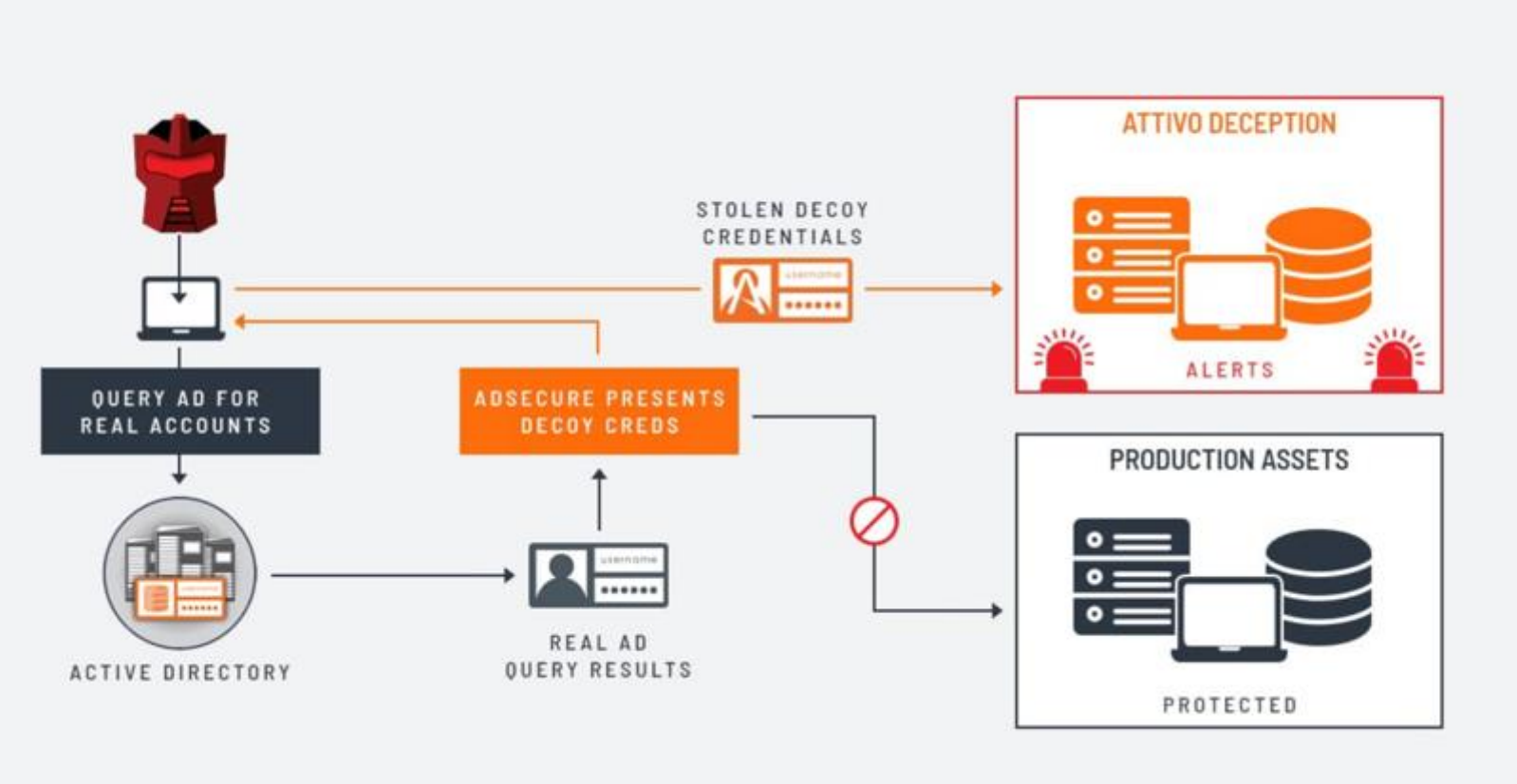
vmware

Google Cloud Platform

Appliance

ADSecure

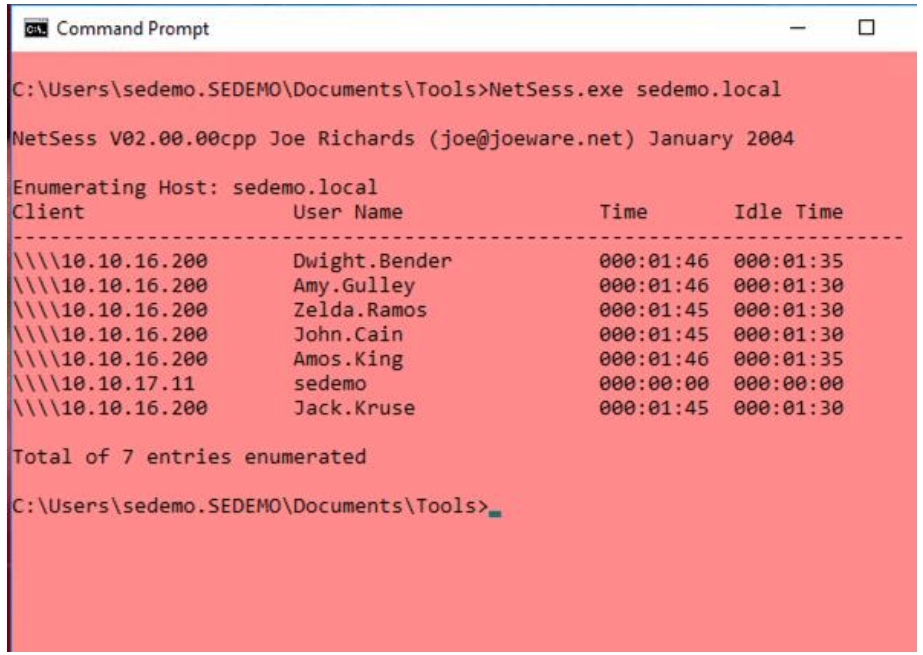
Ochrana pred útokom na Active Directory



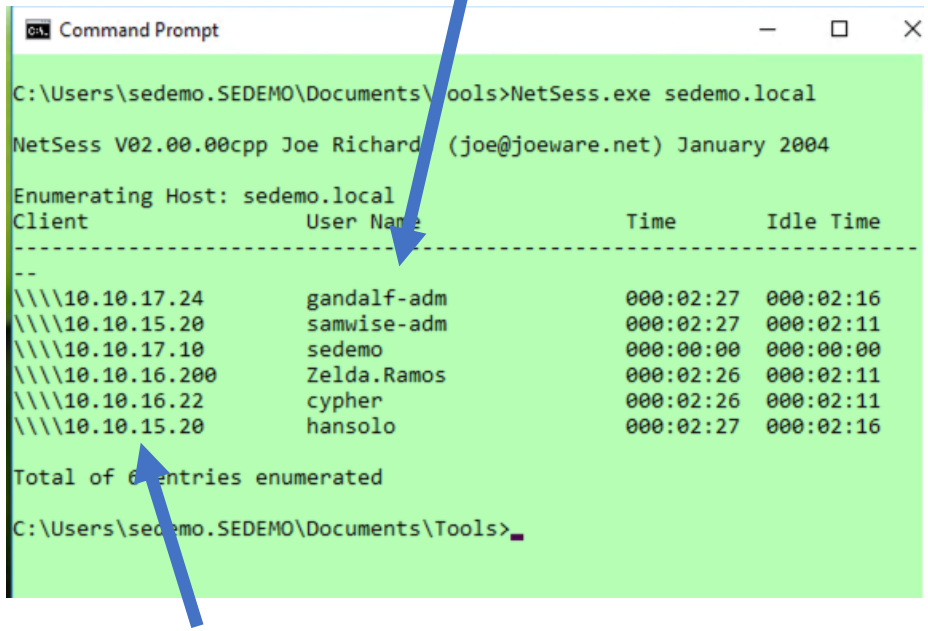
* Podporuje známe AD objekty (admins, service accounts, critical computers, net sessions)

Netsess.exe

Odkiaľ sú doménový admini prihlásení?



Falošní užívatelia



Decoy systémy

- Útočník použije Nesess pre zistenie, odkiaľ sú prihlásení doménoví administrátori
- ADSecure ukryje reálné 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

Check Point SOFTWARE TECHNOLOGIES LTD.
CISCO
FORTINET
JUNIPER NETWORKS
paloalto networks
BROADCOM

Endpoint Distribution

CROWDSTRIKE *
McAfee
TANIUM

Endpoint management solutions (ECM, WMI, Casper, etc.)

Integrations to Attivo API

Digital Defense by HelpSystems
Quantea

Investigate: Analysis & Hunting

FIREEYE
FORESCOUT
IBM QRadar
LogRhythm
McAfee
MICRO FOCUS
REVERSINGLABS
splunk>
TANIUM
ThreatConnect
VirusTotal
WEBROOT an opentext company

Orchestration

CORTEX XSOAR BY PALO ALTO NETWORKS
IBM Security
splunk> phantom
SWIMLANE

Respond: Endpoint Quarantine

aruba a Hewlett Packard Enterprise company
CISCO
CROWDSTRIKE
FIREEYE
FORESCOUT
GoSECURE POWERED BY COUNTERTACK
McAfee
SentinelOne
TANIUM
vmware Carbon Black.

Cloud Monitoring

box
Google Drive
Office 365
salesforce

Redirection

McAfee

Ticketing

servicenow

COMGUARD
communication security

Ďakujem za pozornosť!

Ondrej Malík | ondrej.malik@comguard.cz

28.4.2022