GREYCORTEX

Síla analýzy síťového provozu

aneb viditelnost, kterou jste možná netušili

| ESET Security Days 2024 |

Ondřej Hubálek

GREYCORTEX **MENDEL**

Visibility

All the network communication, devices with inventory details, and user behavior

Detection

From misconfigurations, performance problems, or policy violations to undetected malware, ransomware, and hacker activities which are able to bypass existing security tools

Response

Rapid attack response, and incident investigation and management

\+

SCADA/ICS Monitoring

Application Performance Monitoring

Asset Inventory (2021)

Network Detection and Response / NDR

Advanced artificial intelligence, machine learning, data analysis and more traditional detection methods

GREYCORTEX

Endpoint | EDR | Server | Workload protection | Cloud | Email | Mobile | Firewall | Switch | Wireless | ZTNA

Network Detection and Response

Open APIs

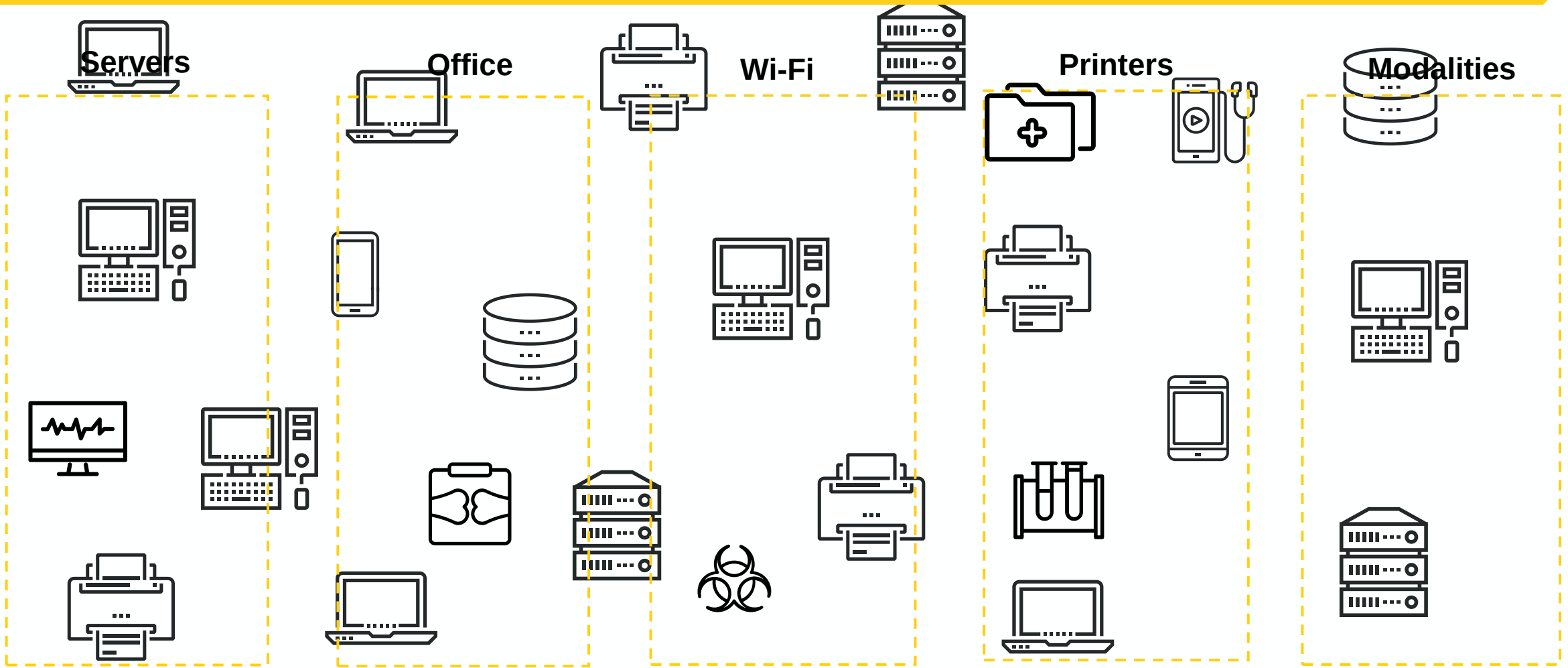
- Industry/Developer
- Service Provider
- Administrator
- Security Operations

Threat Intelligence

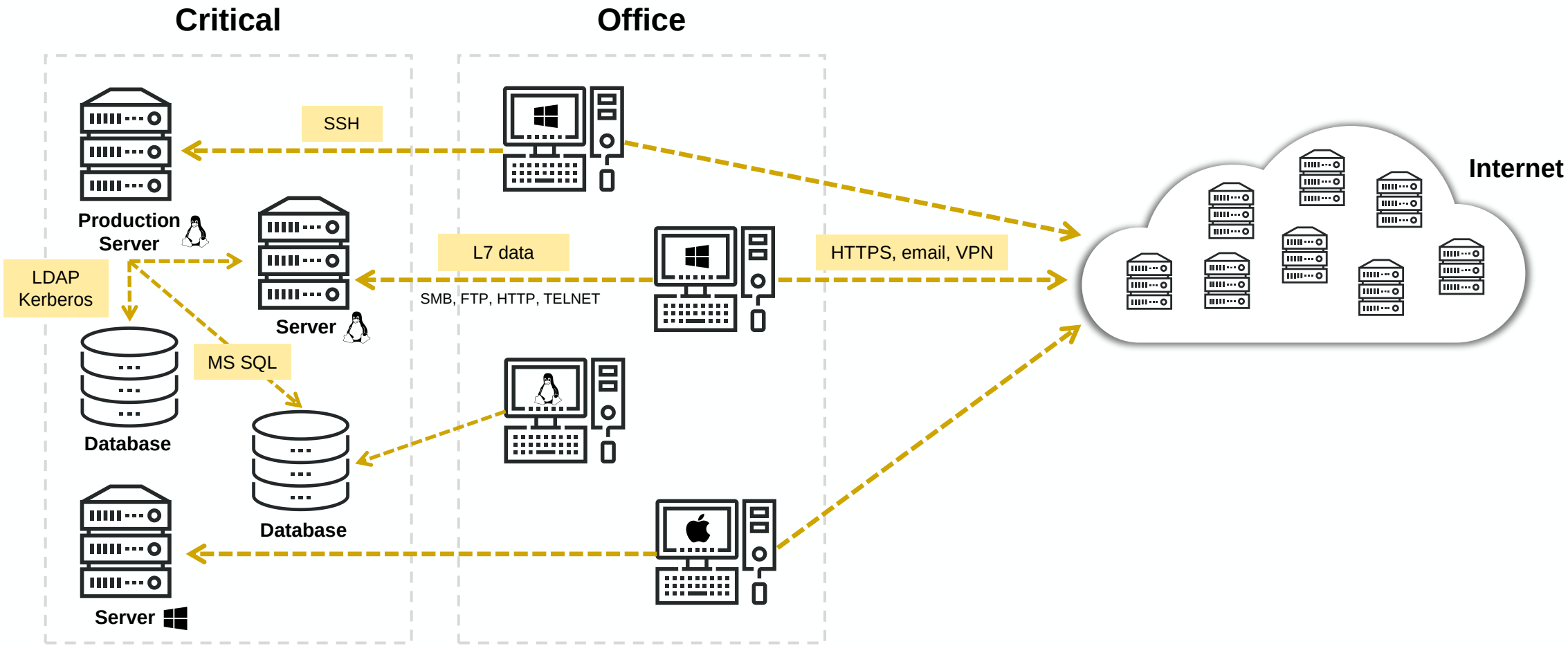
Artificial Intelligence

Data Lake

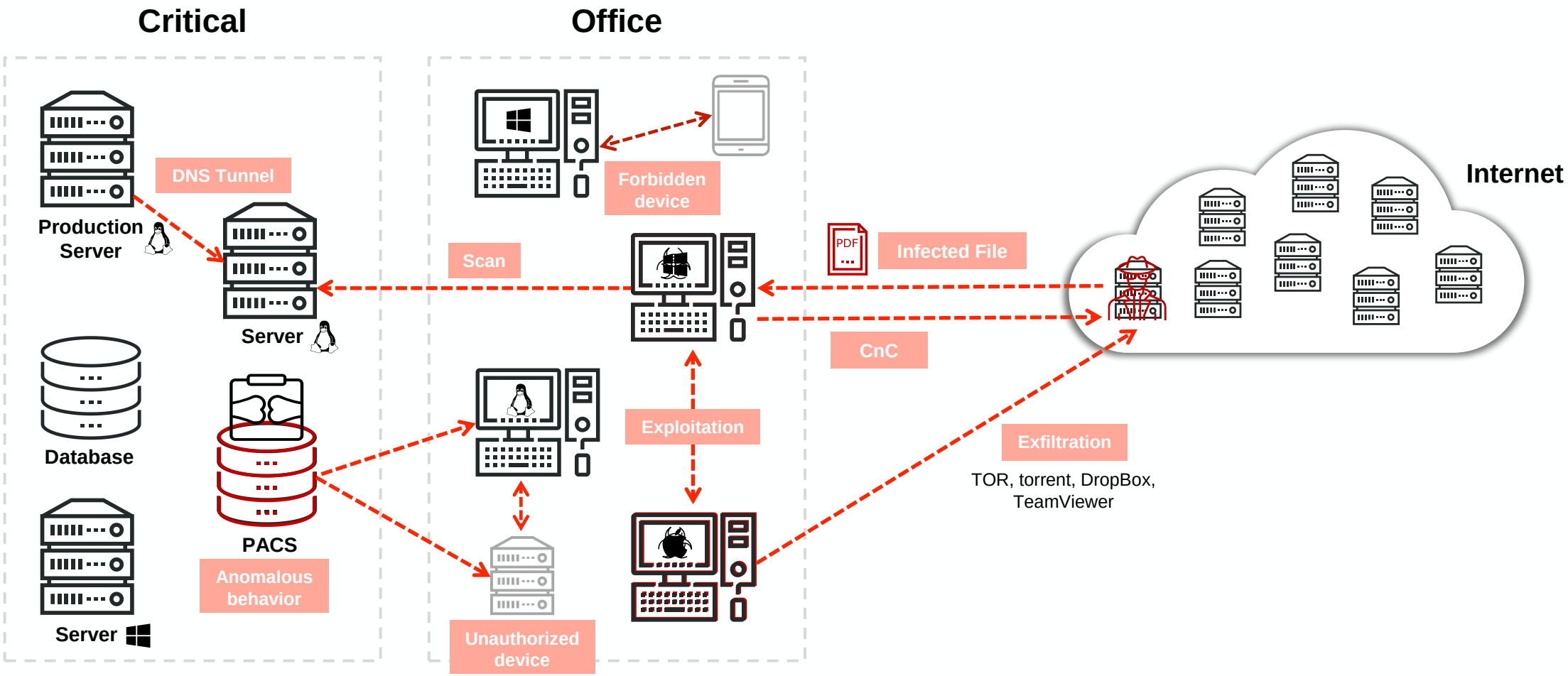
Visibility



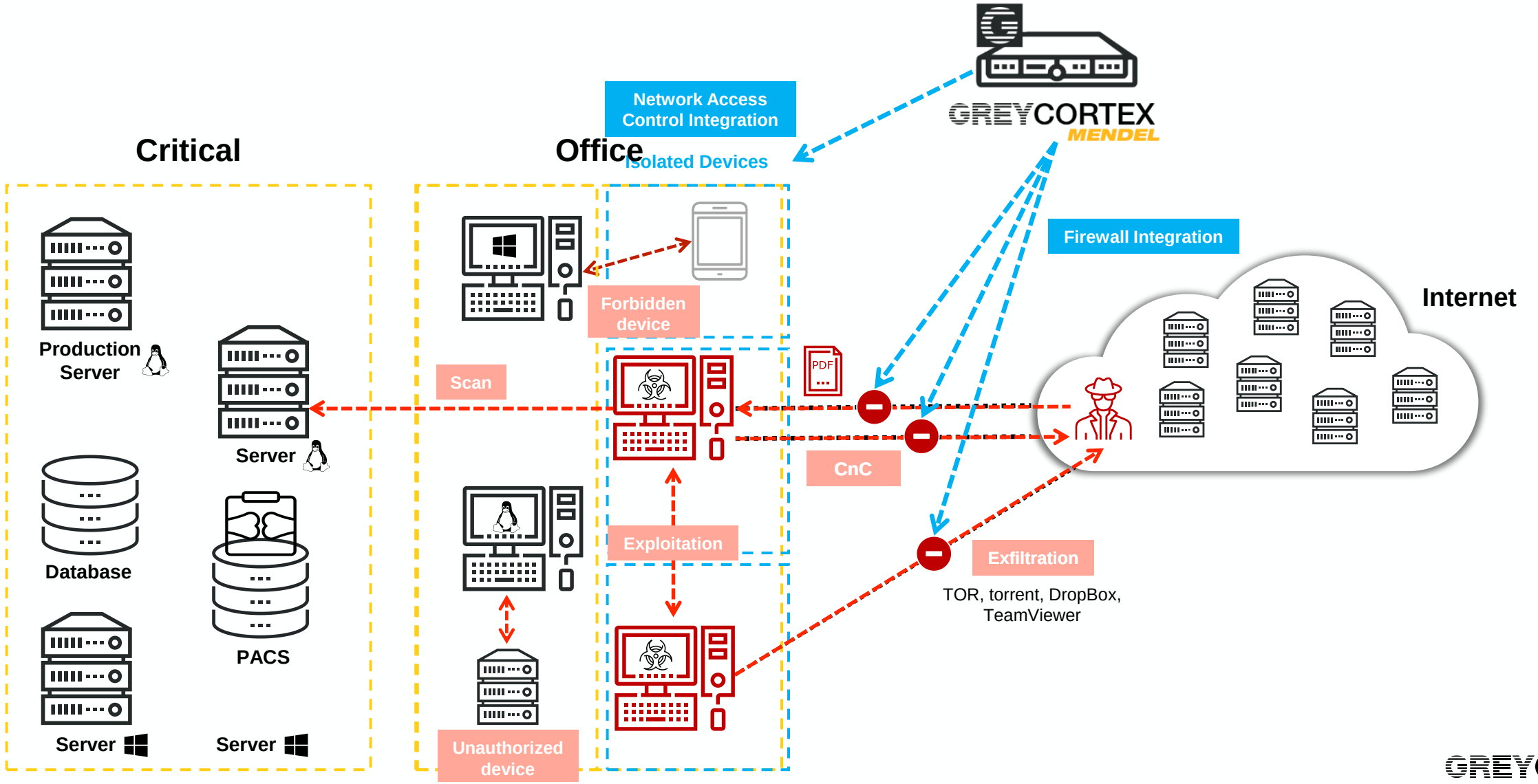
Visibility


Critical
Office
SSH
Production Server
LDAP Kerberos
Server
L7 data
SMB, FTP, HTTP, TELNET
HTTPS, email, VPN
Internet
MS SQL
Database
Database
Server

Detection

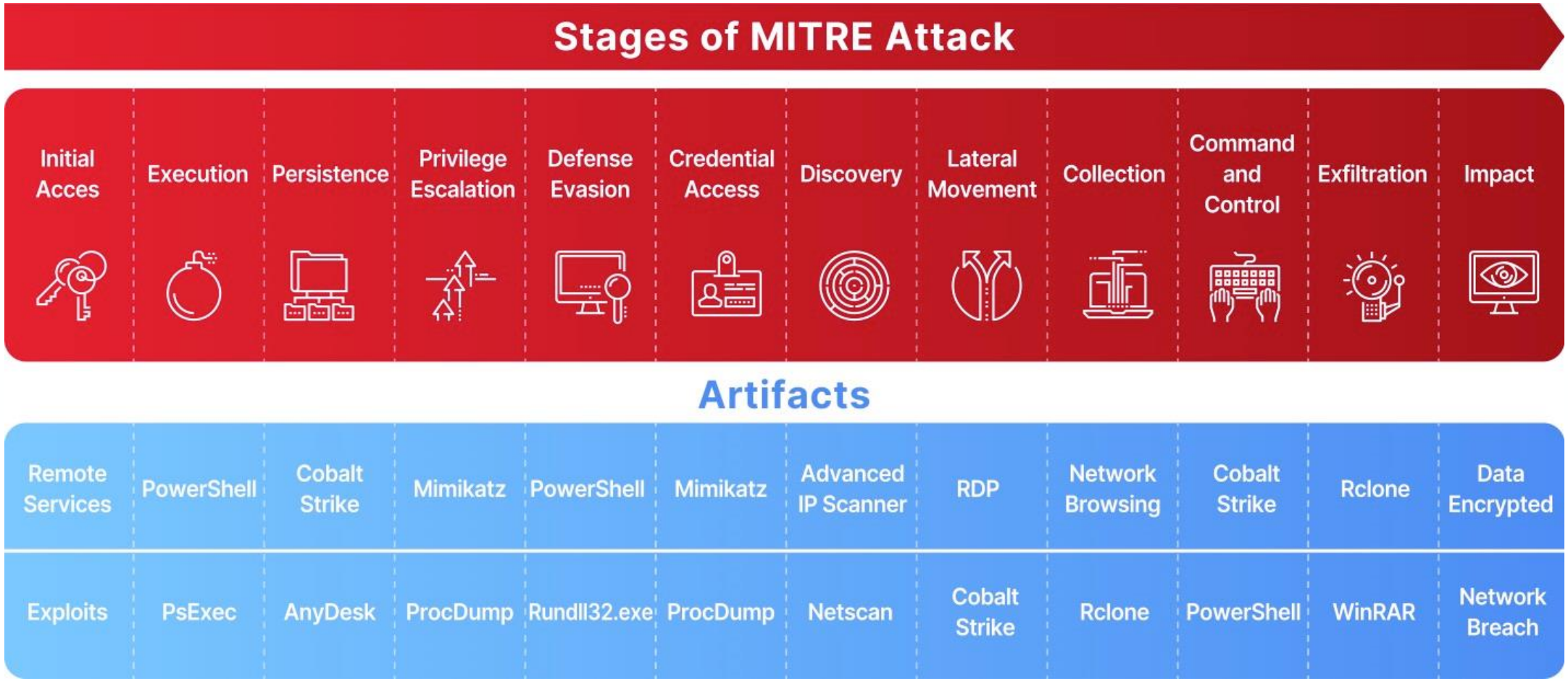

Critical
Office
Production Server
DNS Tunnel
Server
Database
PACS
Anomalous behavior
Server
Forbidden device
Scan
Infected File
CnC
Exploitation
Exfiltration
TOR, torrent, DropBox, TeamViewer
Unauthorized device
Internet

Response



GREYCORTEX

Adversaries Exploit Legitimate It Tools

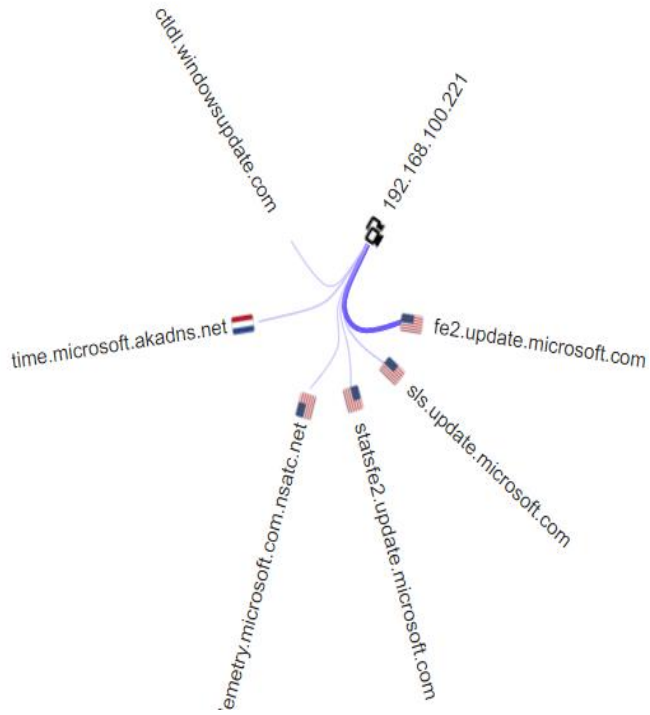


LIVE DEMO

www.greycortex.com

Discovery

- Inventory Link
- Sítě
- Zařízení
- Podklady pro analýzu rizik Link
- Služby Link



Discovery: New RDP Remote Access system 2

Signature: -50015 (Information, created: 2021-05-23 02:00:00)

Signature ID:	-50015	Description:	New RDP Remote Access system appeared in network.
Mitre:	Discovery/System Service Discovery		
Created:	2021-05-23 02:00:00 (Modified: 2021-12-03 15:08:59)		

Top Dst Hosts	Top Dst Subnets	Top Services
10.22.10.163	DB servers (10.22.10.0/24)	3389
10.22.10.249		

10 10 10

Malware, Exploits and Hacker’s activities

- Known Threats Link
- Projevy nebezpečného chování
  - C&C odchozí komunikace Link
  - Útoky hrubou silou Link
  - Skeny Link
  - Tunely
  - OT zařízení Link

Security Policies

- **Co neodpovídá best practices interní sítě?**
- Prostupy kritických segmentů a systémů
- Přístupy privilegovaných AD účtů Link
- Plain-textové autentizace a nešifrované protokoly Link
- Administrativní přístupy – vzdálená správa (TeamViewer, AnyDesk, …) Link Link
- VPN přístupy (SoftEther, přístupy z vnějšku)
- Aplikace – coin miners, TOR, P2P, … Link

GREYCORTEX

www.greycortex.com