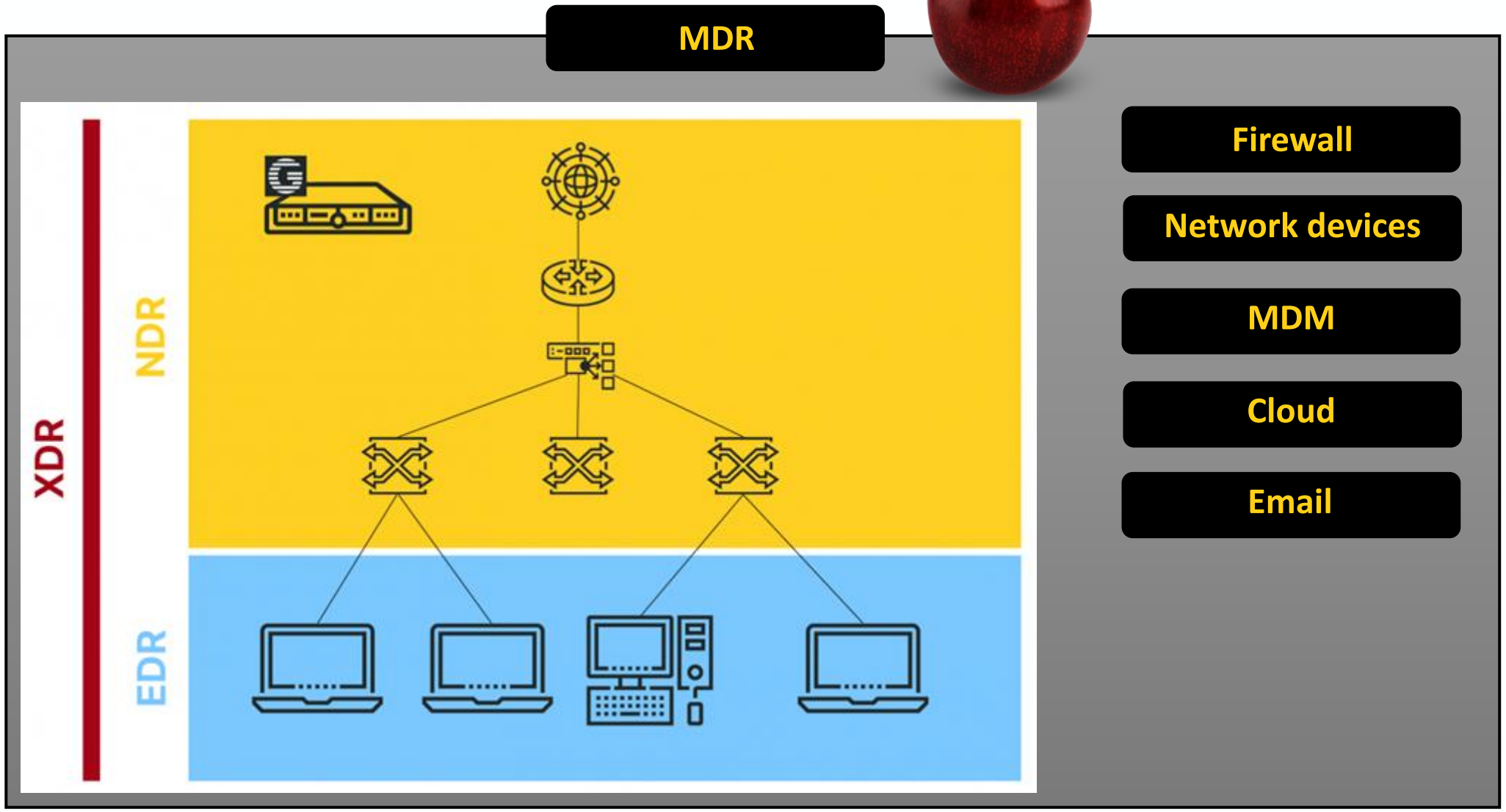
GREYCORTEX

Bezpečnostní audit sítě za 30 minut
aneb co se skrývá ve vašich IT a OT sítích

| ITAPA 2023 |

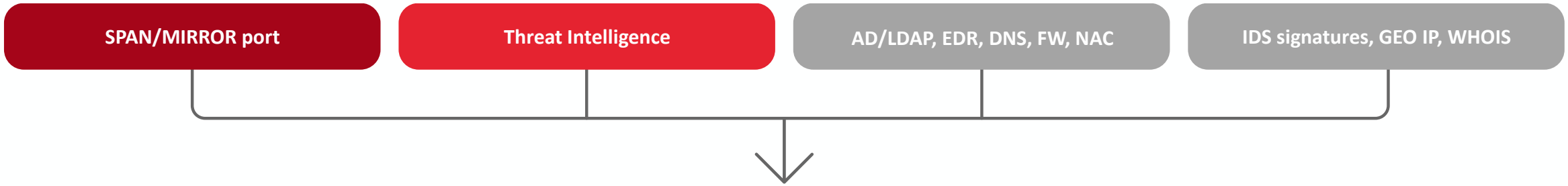
Ondřej Hubálek

Wave of EDR, XDR, NDR and MDR



GREYCORTEX

Architecture



Signatures & DPI
Signatures & Deep Packet Inspection

Signature-based detection

- Known malware
- Known attacks
- Known exploitations
- Policy violations
- High performance packet capture

NBA
Network Behavior Analysis

Behavior-based detection

- Malware activity propagation, downloading, spamming
- Attacker activity - scanning, brute-forcing, exploitation
- C&C activity - RAT, APT, AVT, bots, worms, rootkits
- Data exfiltration

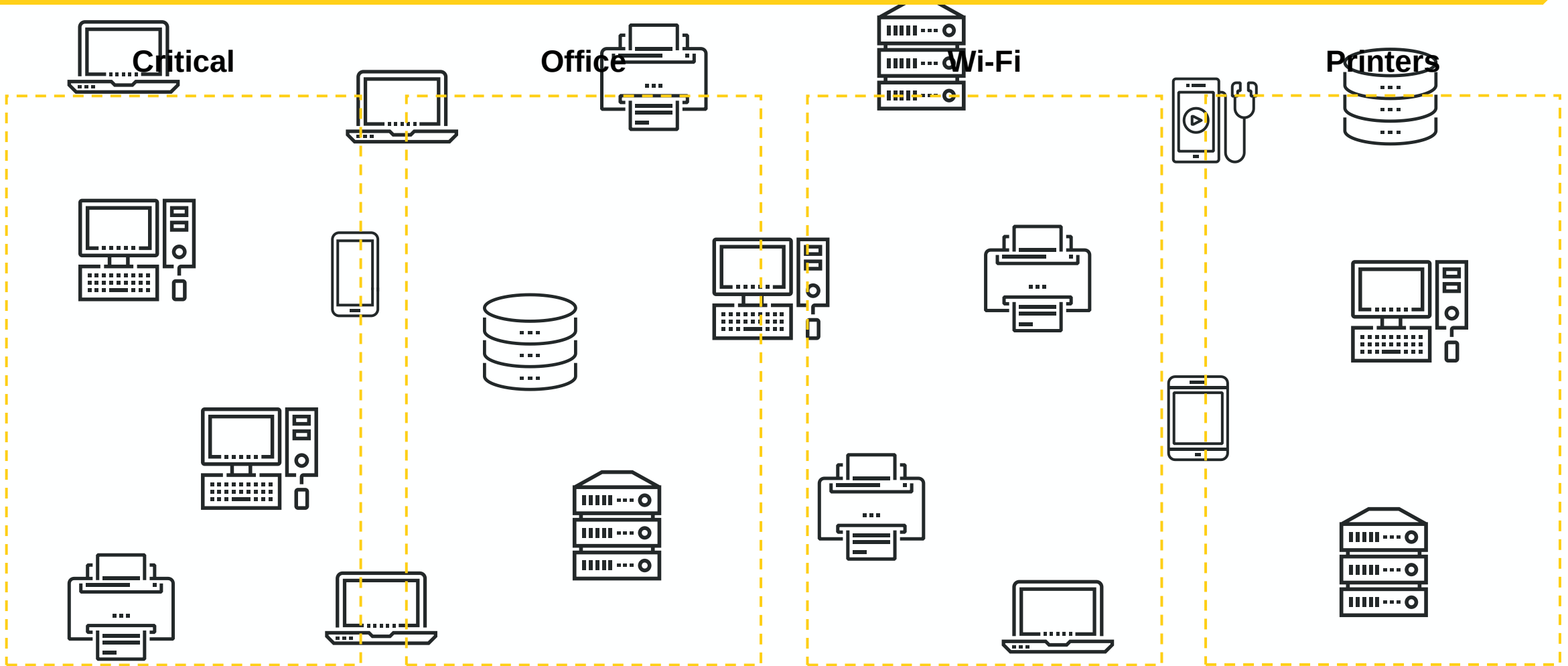
Stats
Network Statistics

Visibility & Performance

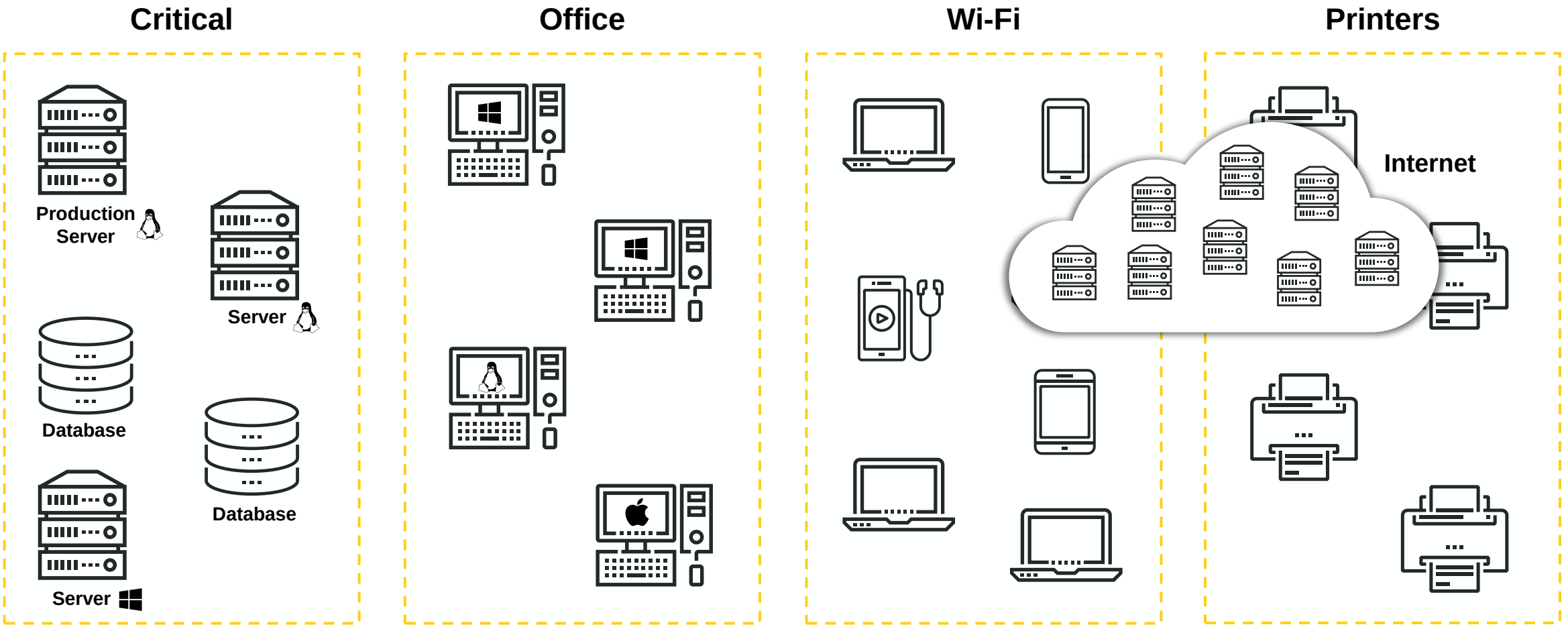
- Complete network visibility
- Application performance
- Network performance
- Application & user awareness

User interface, Reporting, Notification & Integration (SIEM, Firewall, …), Response

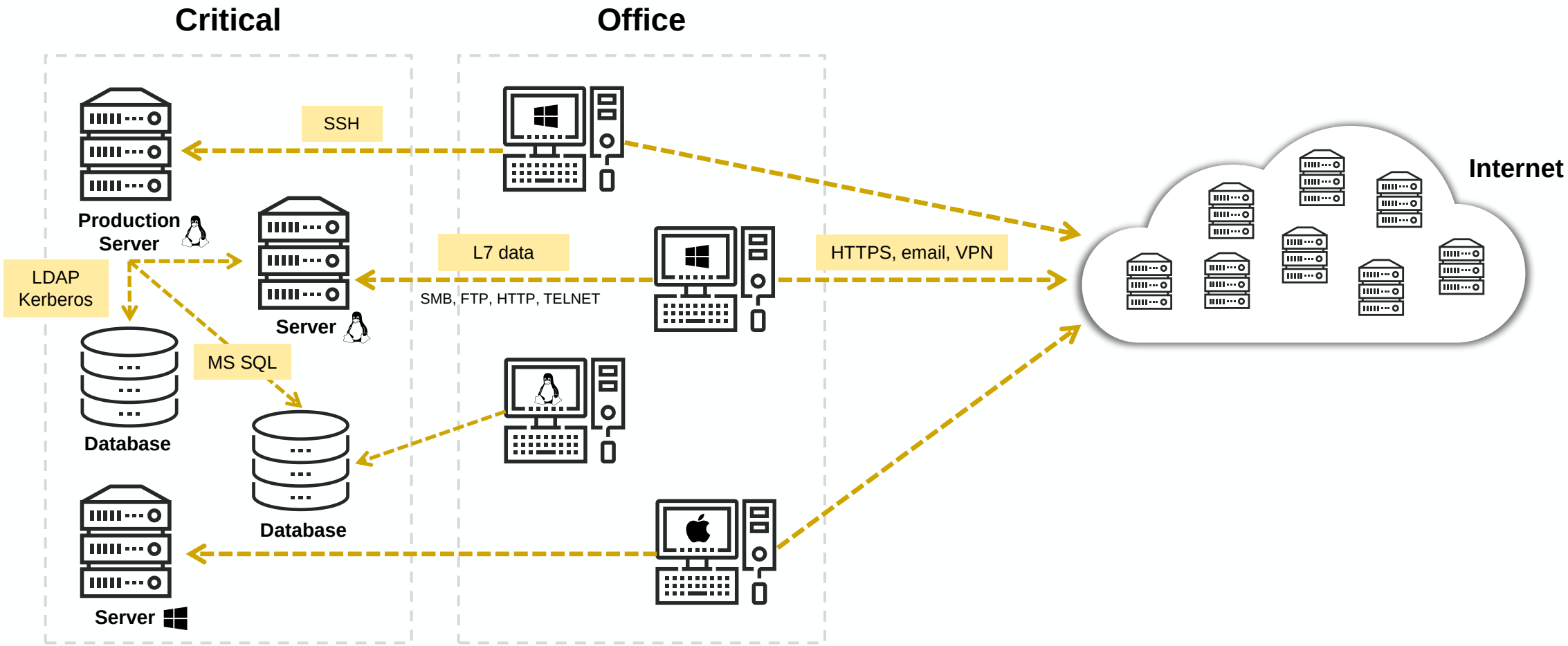
Visibility



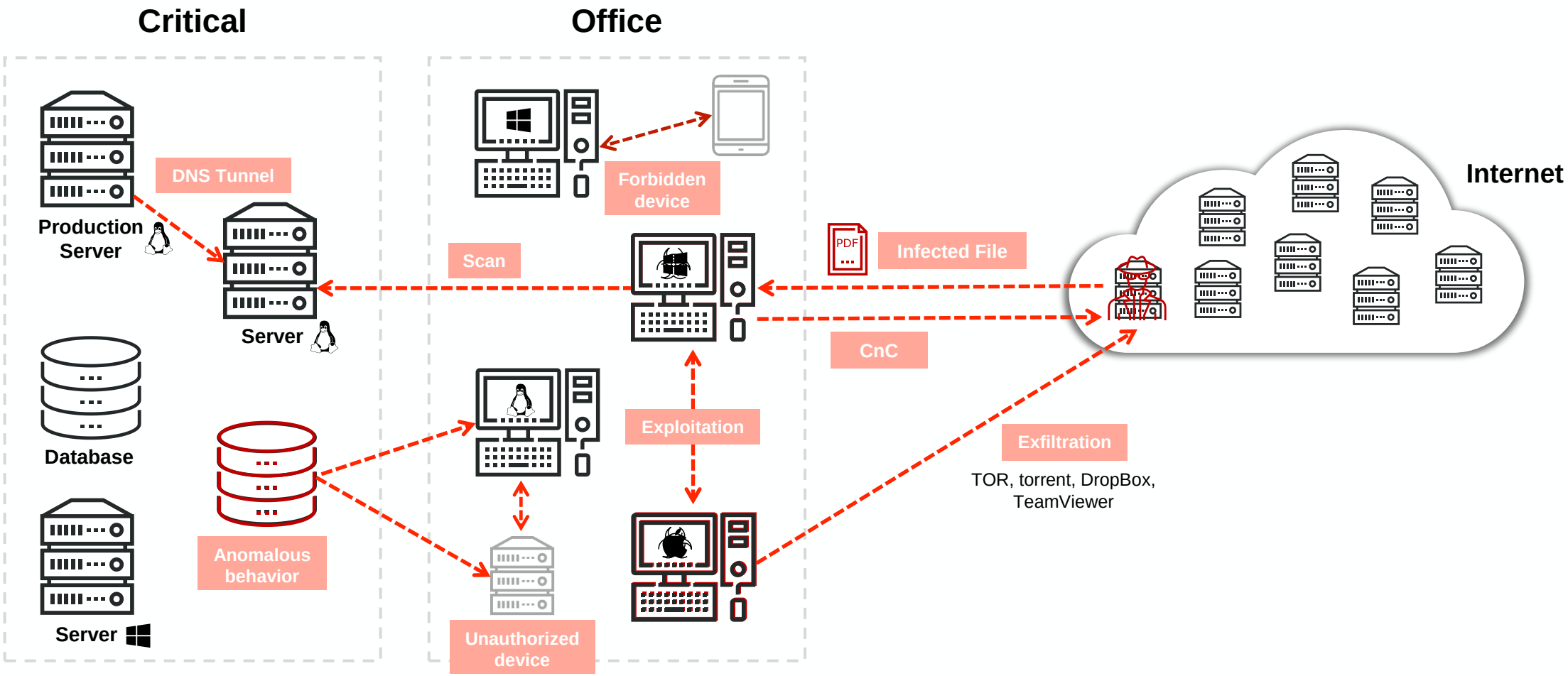
Vysibility


Critical
Office
Wi-Fi
Printers
Production Server
Server
Database
Database
Server
Internet

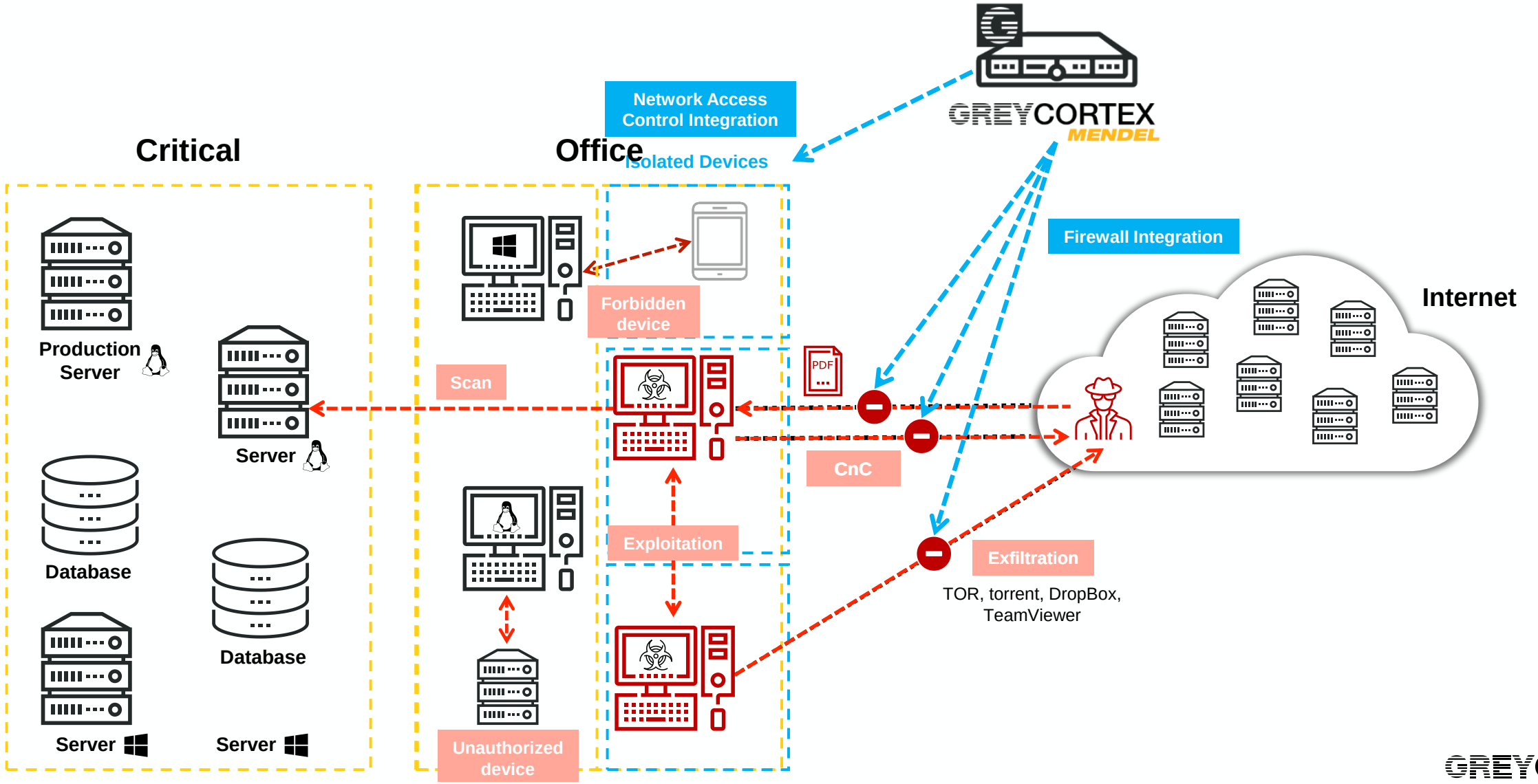
Visibility


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

Detection

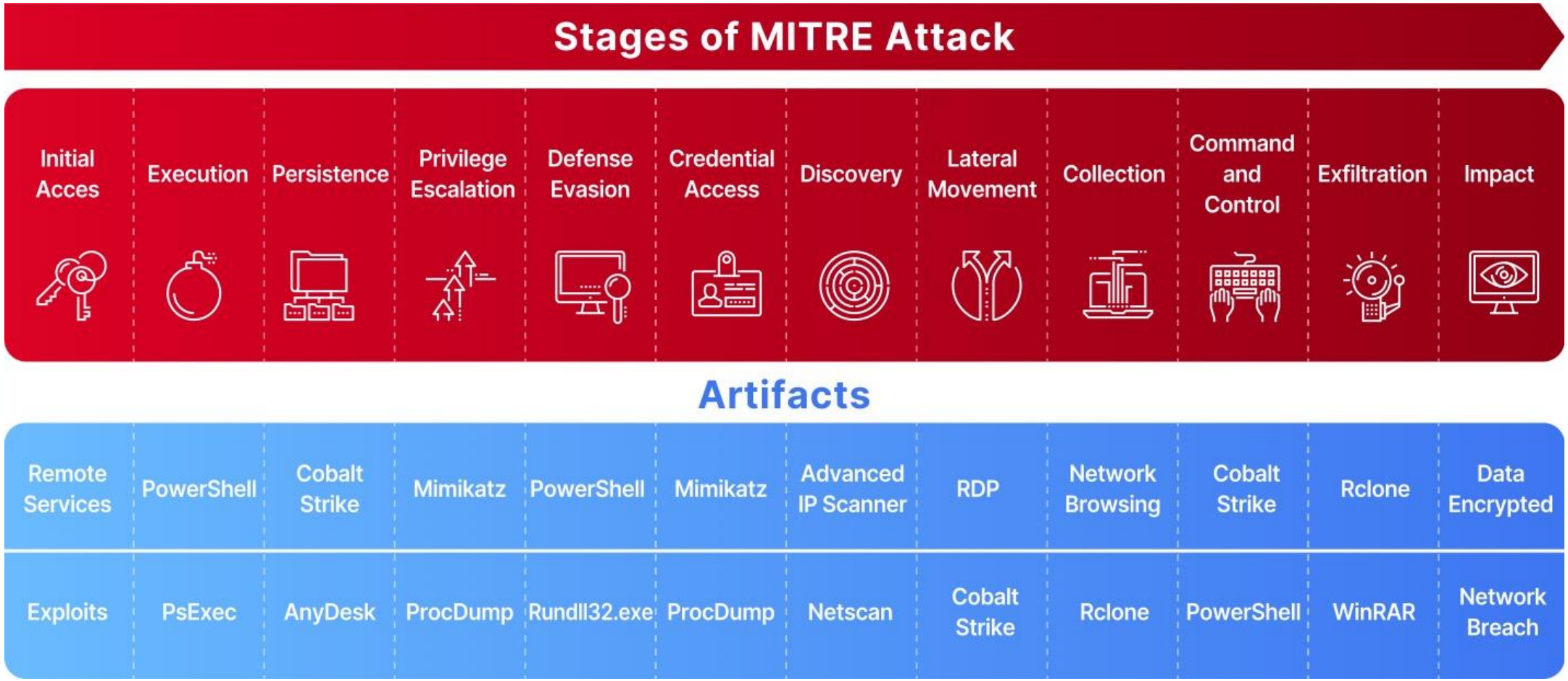

Critical
Office
Production Server
DNS Tunnel
Server
Database
Server
Anomalous behavior
Forbidden device
Scan
Infected File
CnC
Exploitation
Exfiltration
TOR, torrent, DropBox, TeamViewer
Unauthorized device
Internet

Response



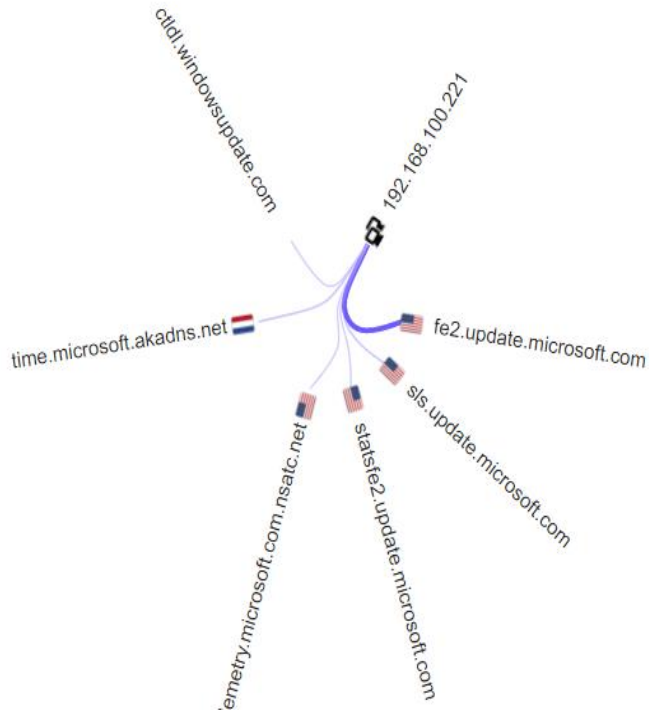
GREYCORTEX

Adversaries Exploit Legitimate It Tools



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