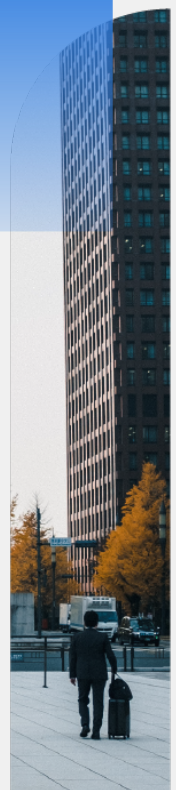
Fortibezpečnost Město Litoměřice zkušenosti a výhled

Horymír Šíma

Fortinet

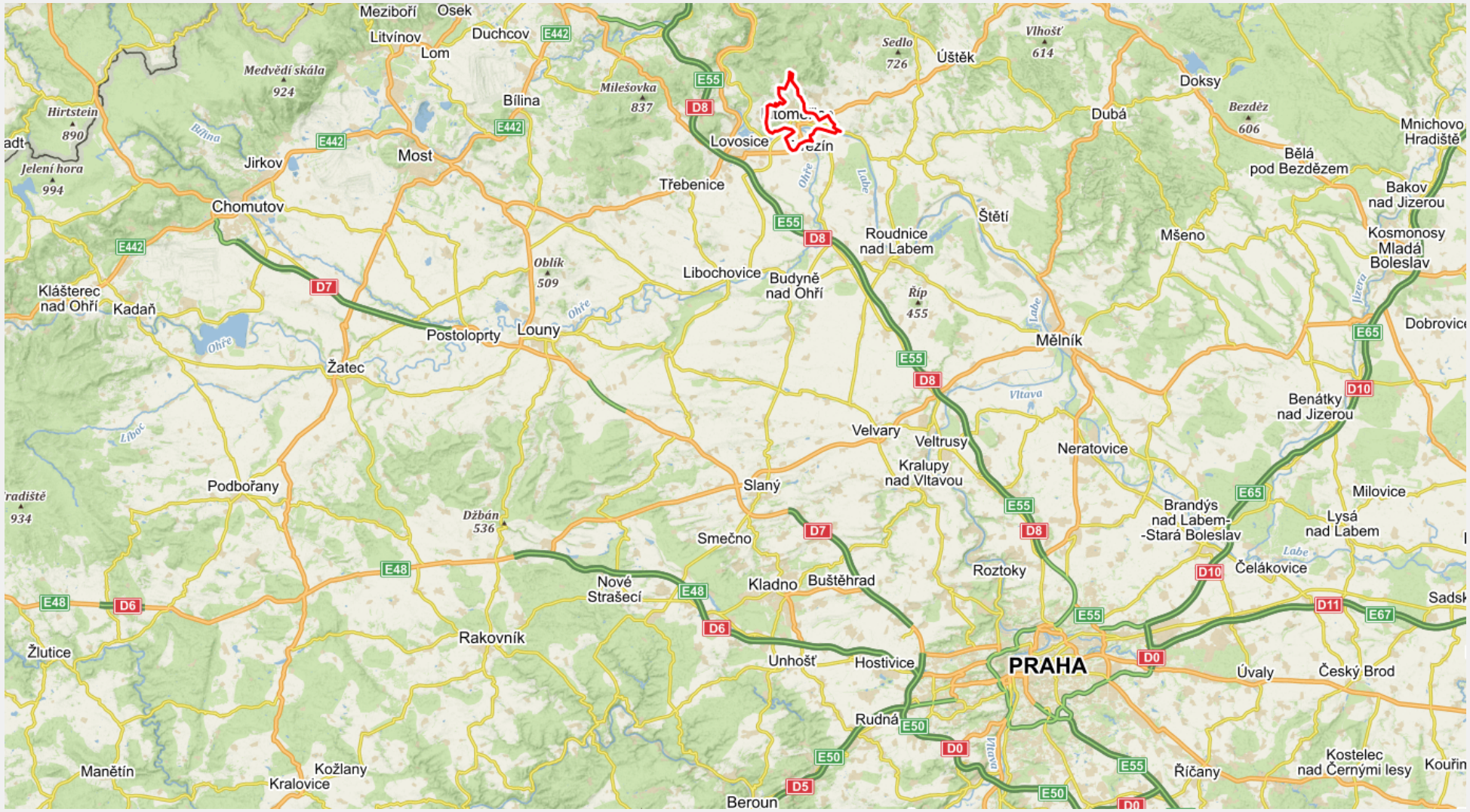
Jan Černý

Město Litoměřice



Město Litoměřice

Krátké představení



Krátké představení

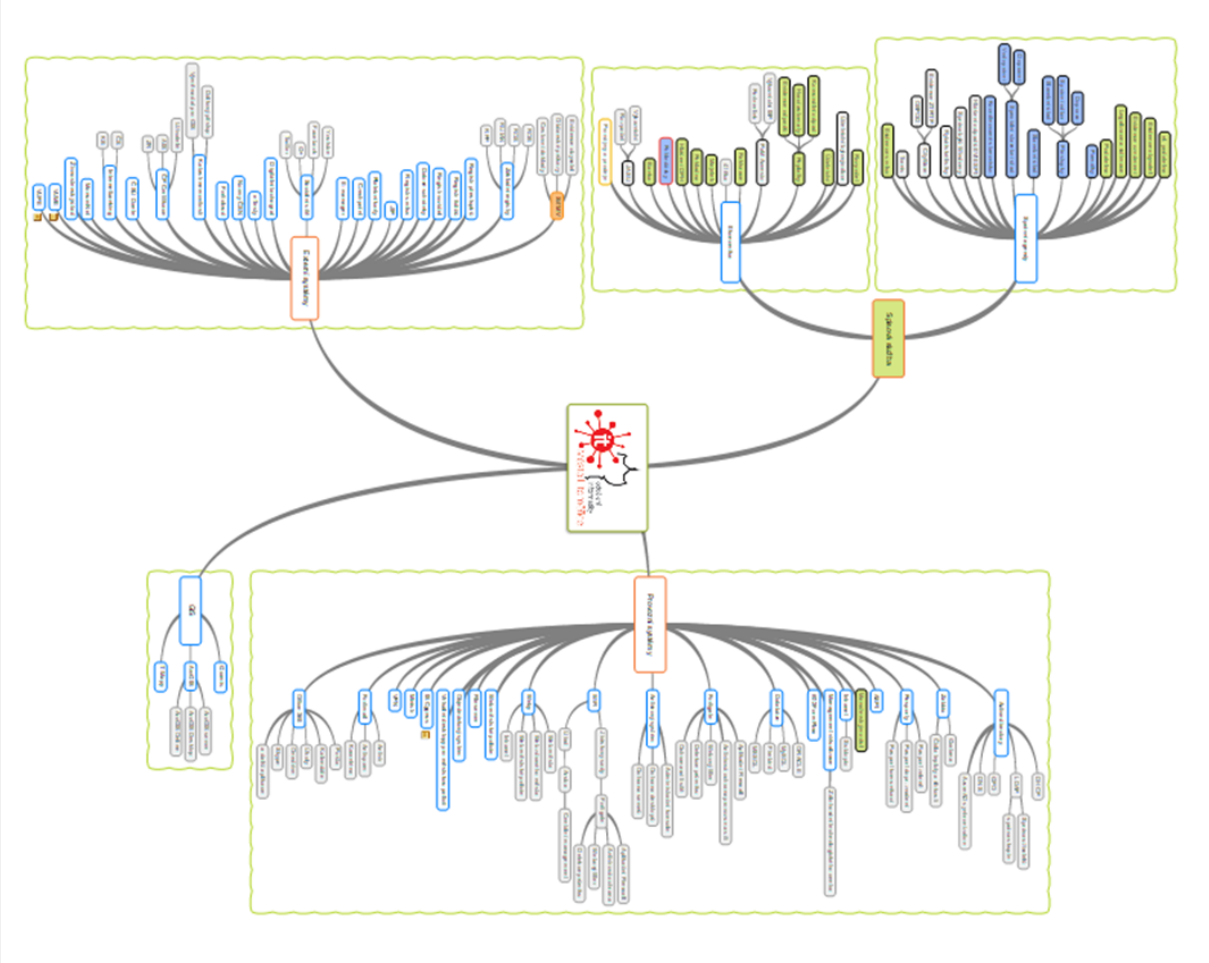
Litoměřice

- ORP III typu
- 40 Obcí ve správním obvodu
- Město má cca 25 000 obyvatel
- Letos slavíme 802 let od založení

Oddělení IT

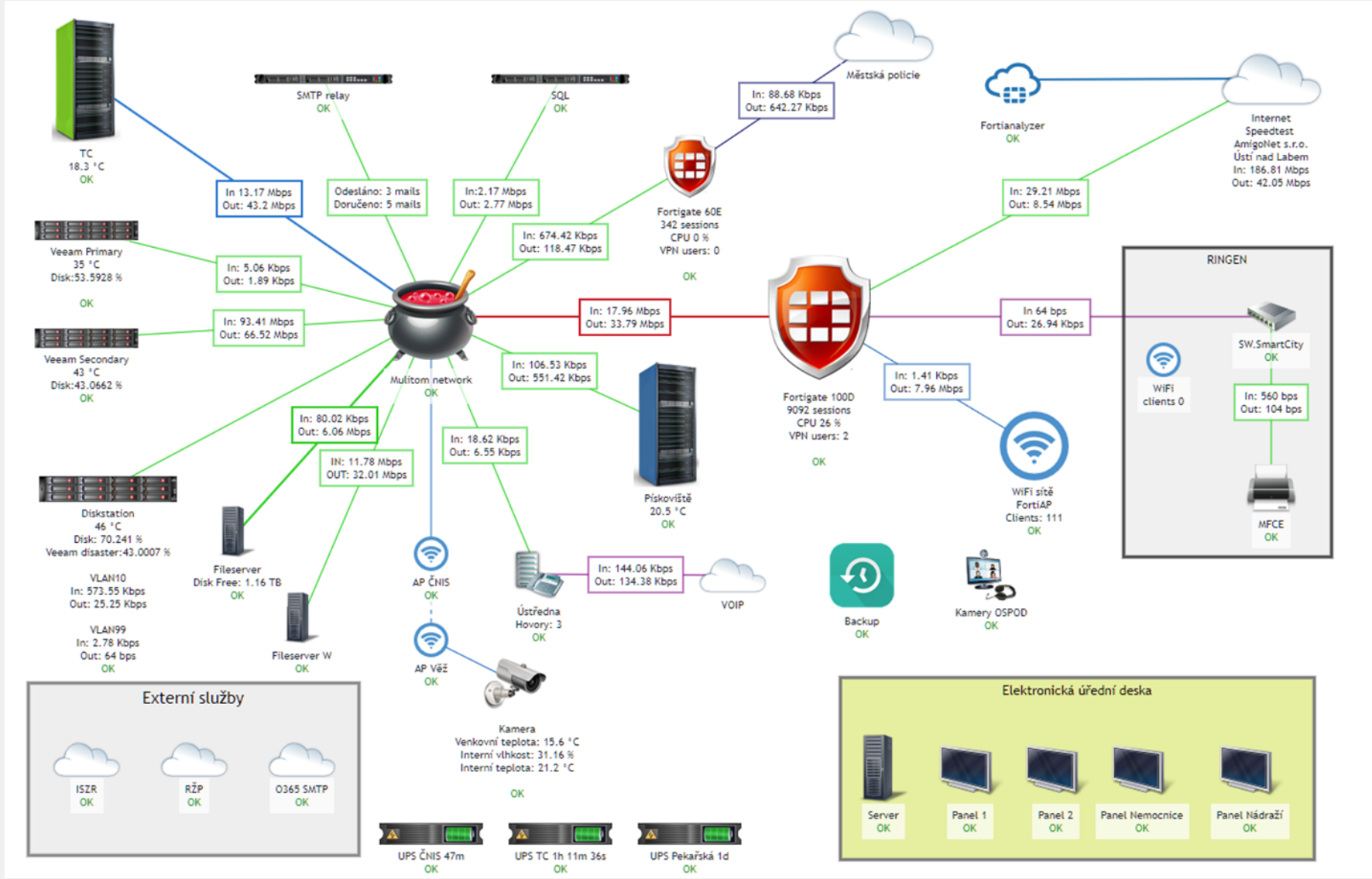
- 8 Budov
- Cca 240 uživatelů
- 5 Informatiků a 1 GISák

O co se staráme



- Interní agendové systémy
- Dohledový systém
- Weby města
- Externí cloudové aplikace
- Office 365
- Bezpečnost

Všechno máme pod dohledem

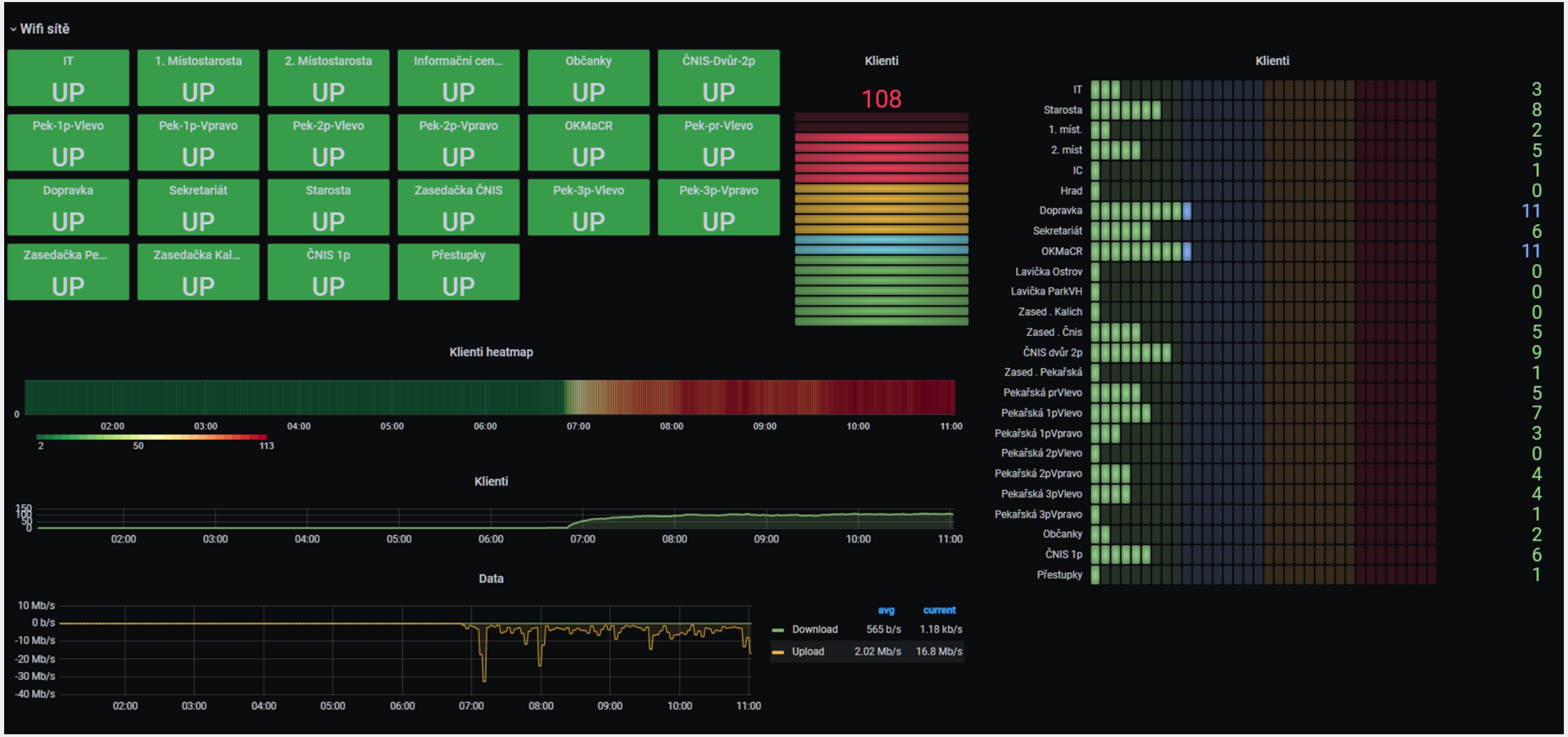


Zabbix

Počet zařízení	353
Počet položek	160 603
Počet spouštěčů	11 221

Grafana

Grafana



Něco máme i na zdi

Televize

+

Raspberry Pi

Postupná evoluce

Pravěk

- IPchains firewall
- Sendmail + ClamAV
- AVG antivirus na windows bez centrální správy
- Dva Linuxové servery
- Žádná wifi

Starověk

- IPTABLES firewall
- Icewarp groupware
- Fortimail
- OpenVPN
- Dohledový systém Cacti
- Jeden Fortigate v transparentním módu
- ESET antivirus s centrální správou
- Několik serverů jak Windows tak Linux
- Decentralizovaná Wifi pro veřejnost chráněná Fortigate 50B

Postupná evoluce

Novověk

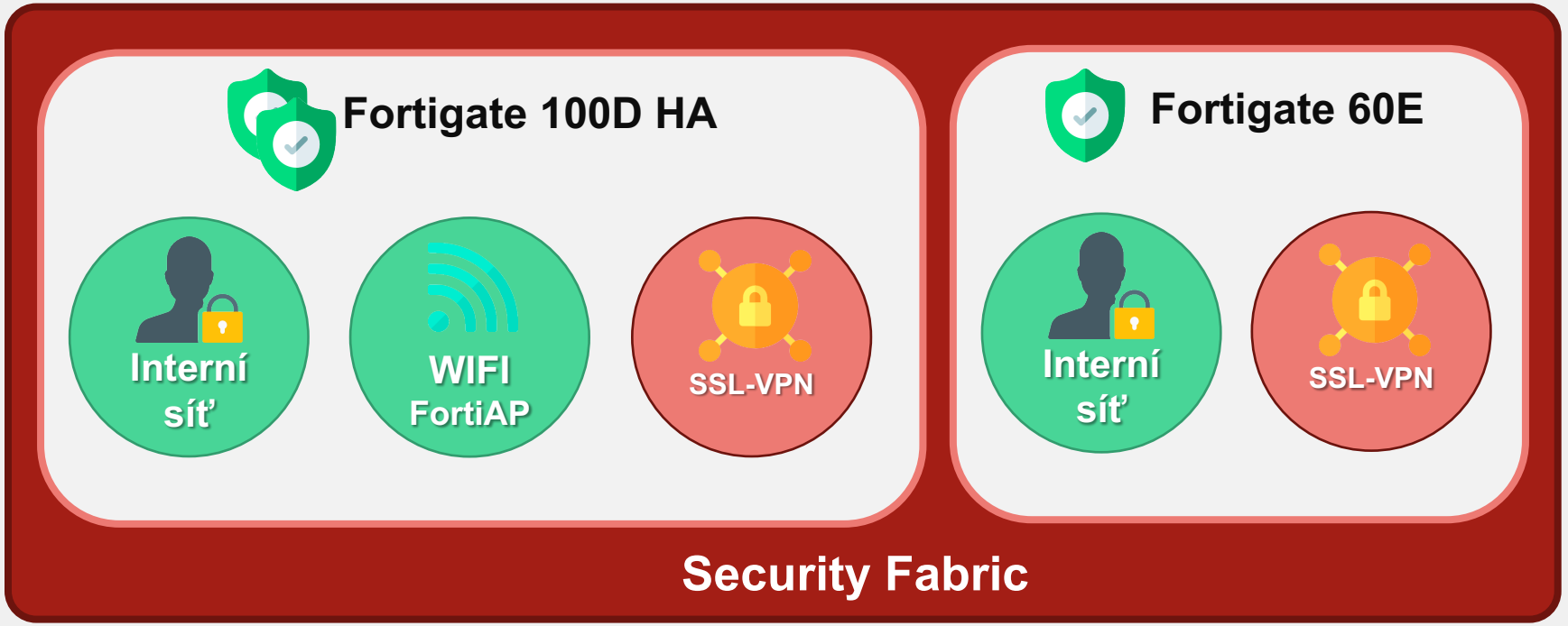
- IPTABLES firewall
- Jeden Fortigate v transparentním módu
- ESET antivirus s centrální správou
- Pár virtuálních serverů, zbytek fyzické
- Icewarp groupware
- Fortimail jako služba
- OpenVPN
- Wifi – Aruby s centrální správou
- Dohledový systém Zabbix

Současnost

- Dva Fortigate firewally v HA
- Jeden Fortigate pro Městskou policii
- 15 Fortiswitchů
- Office 365
- ESET antivirus s centrální správou
- Mraky virtuálních serverů
- Několik Wifi sítí - FortiAP
- SSL VPN + Forticlient
- Active directory + Radius + GPO
- Dohledový systém Zabbix + Grafana pro prezentaci dat
- Fortianalyzer jako služba

S čím nám Fortinet pomáhá

3x Fortigate
15x FortiSwitch
27x FortiAP z toho 2 externě v chytrých lavičkách
1x Fortianalyzer jako služba



Fortianalyzer jako služba

Kam dál

Vlastní Fortianalyzer

Nasazení dalších FortiAP

Obměna stávajících switchů za Fortiswitche

Generační obměna Fortigate

SIEM

Monitoring a vyšší zabezpečení koncových stanic

Co se mi na Fortinetu líbí

a občas nelíbí ☺

Škálovatelnost

Vzájemné provázanost jednotlivých produktů

Jednoduchá správa

Rychlá identifikaci hrozeb

Přehled o provozu na síti

Dobrá dokumentace

Bugy ve firmware

Lagování webového rozhraní

Cena ☺

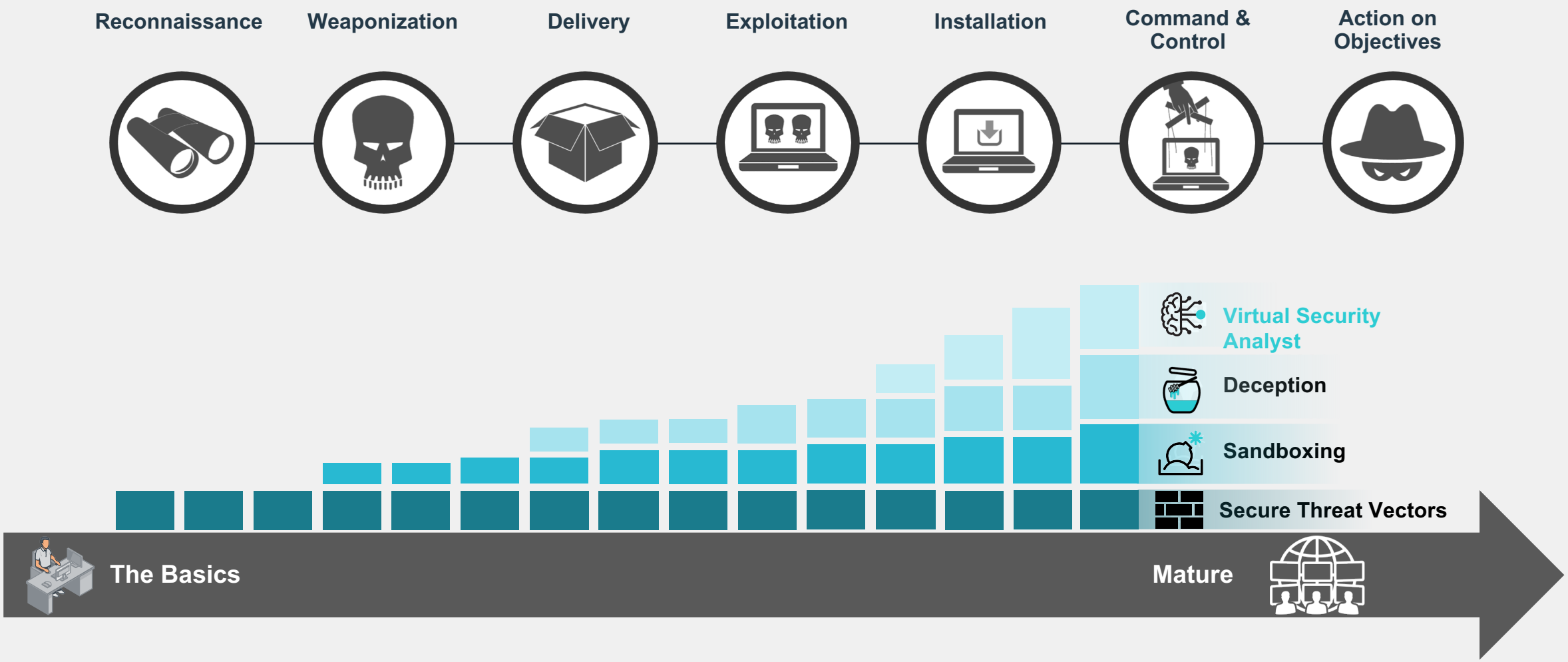
Věta na závěr

Je dobré mít po ruce někoho kdo vám pomůže, když něco nevíte nebo „seto“ rozbije.

V našem případě jsou to NetLANCERS

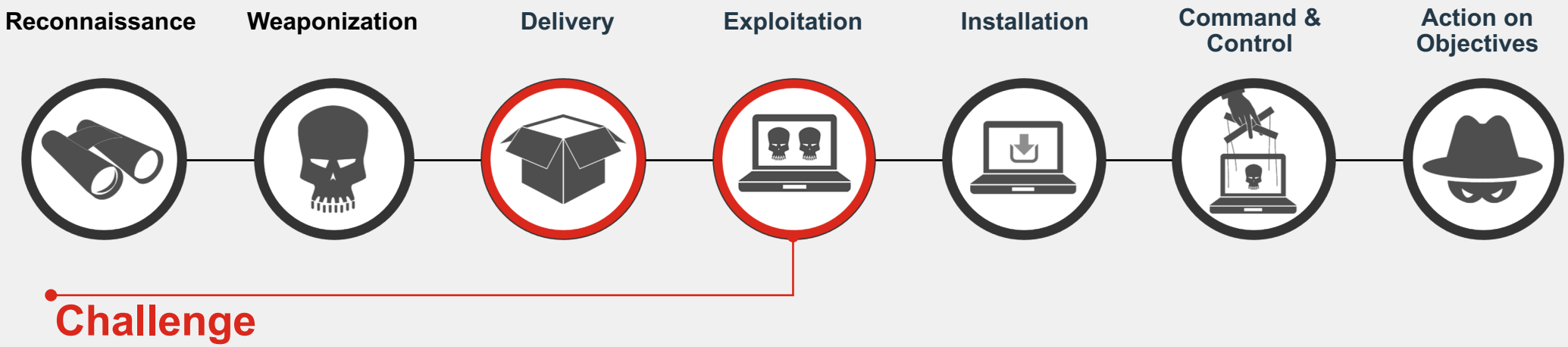
Security Framework for Digital Security

SOC Maturity Model

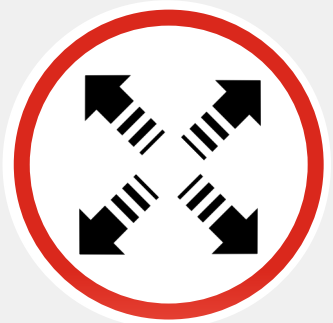


Sandboxing

Block Advanced Threats



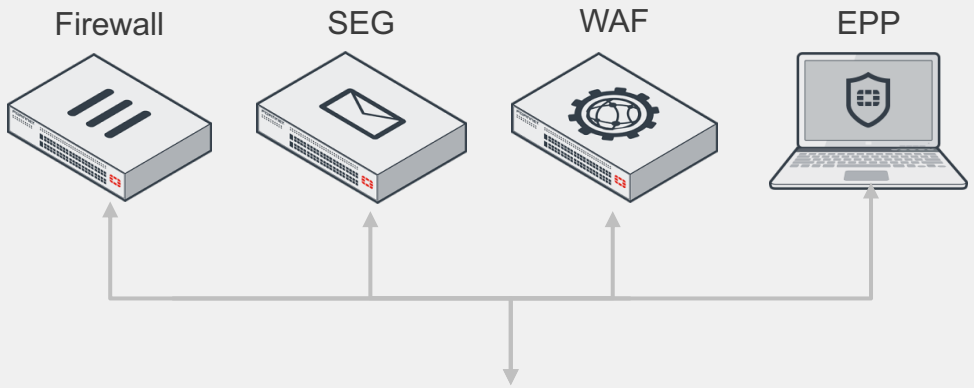
Advanced Ransomware & 0-day Threats



Lateral Spread

Manual & Slow Response

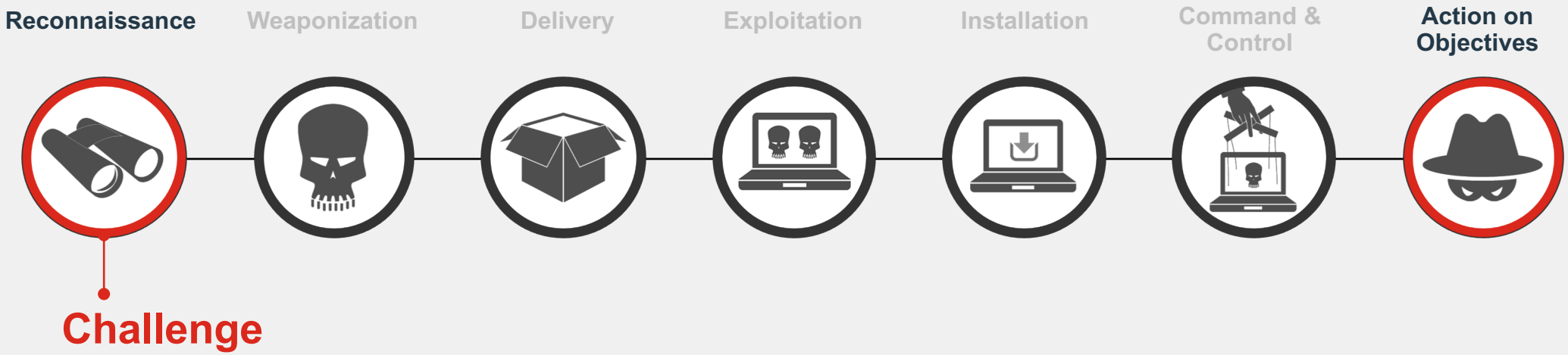
How Should We Address 0-day Threats?



Code Continuum	Known Good	Probably Good	Might be Good	Completely Unknown	Somewhat Suspicious	Very Suspicious	Known Bad
Security Technologies	**Whitelists**	**Reputation:** File, IP, App, Email App Signatures, Digitally singed files	Sandboxing			**Heuristics Reputation:** File, IP, App, Email Generic Signatures	**Blacklists Signatures**

Deception

Disrupt Threat Actors

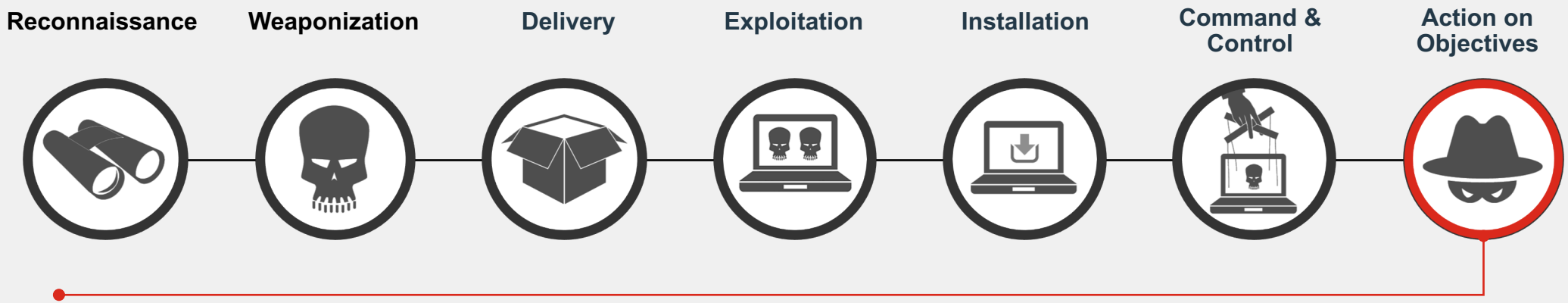


External & Internal Actors

Mitigation Cost

Virtual Security Analyst – FortiAI

Bolster Security Operations (SecOp)



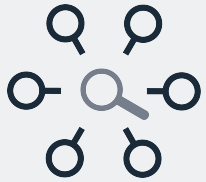
Challenge

Too Many Alerts

Manual Investigation

Lack of Trained People

Fortinet Transforms Security with Virtual Security Analyst™

01	Powerful Security		Secure business continuity against sophisticated malware
02	Broad Coverage		Close gaps and secure the dynamic attack surface
03	Automated Protection		Ability to scale and increase SOC efficiency without increasing budgets


FORTINET