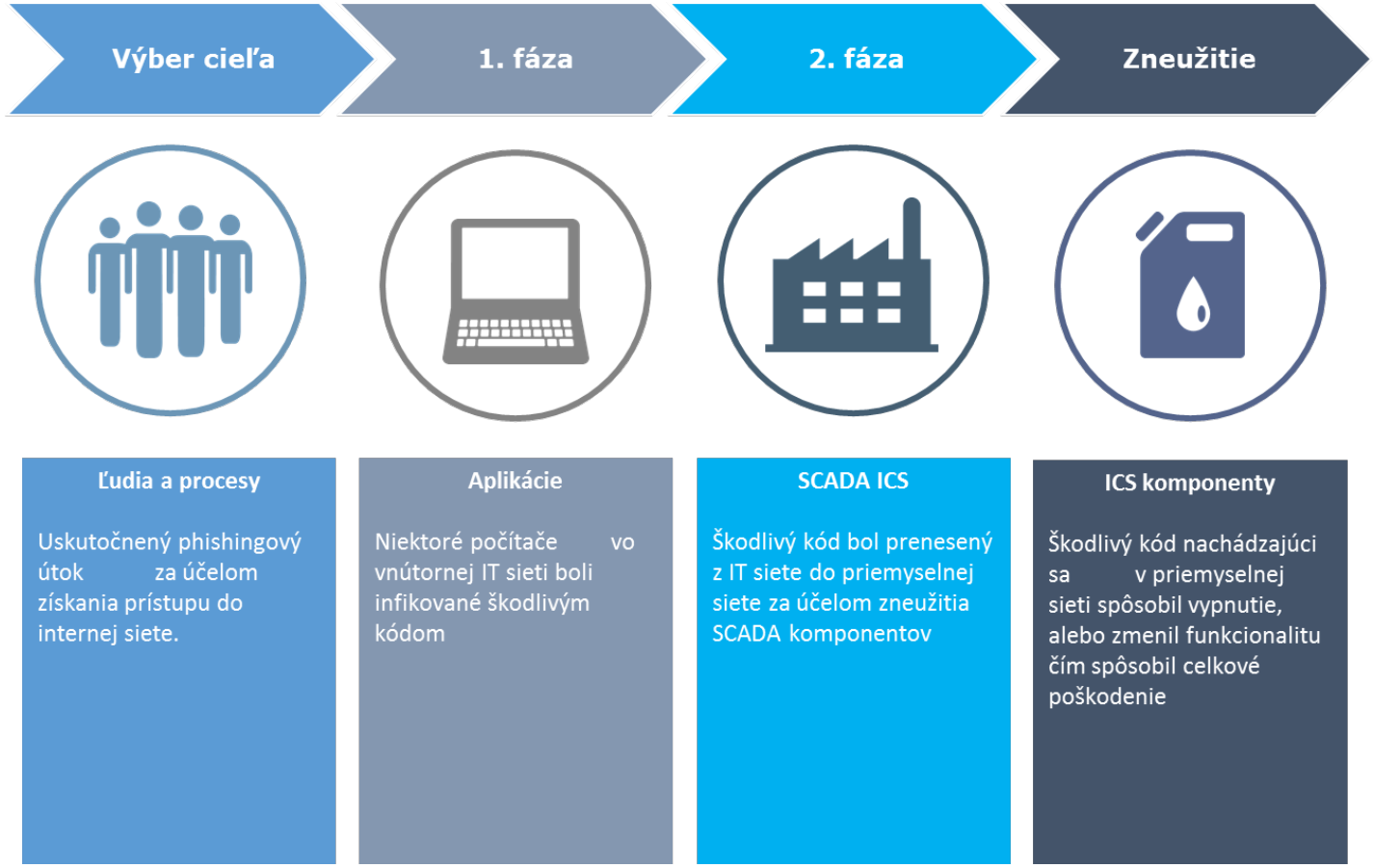
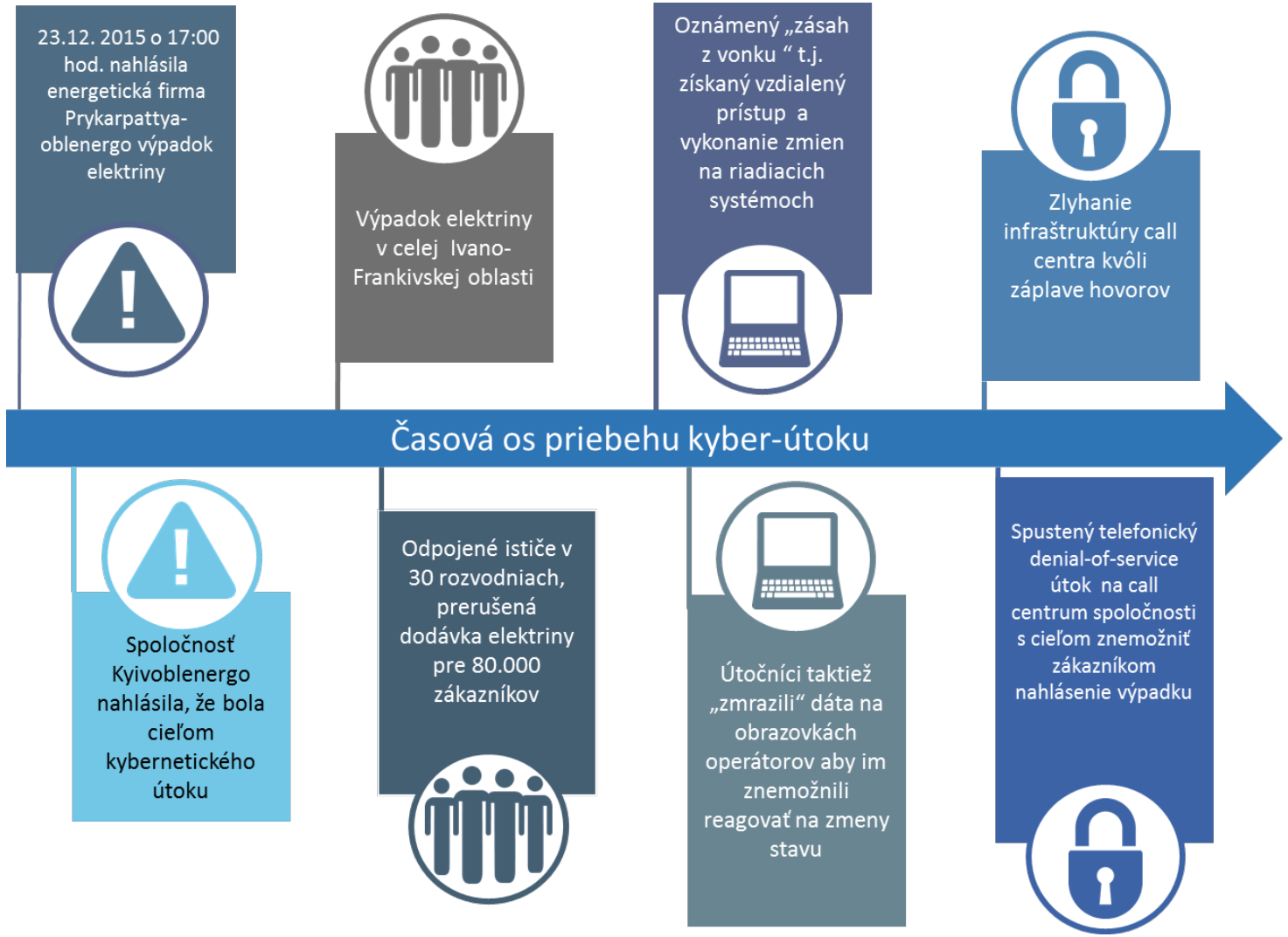
Komplexný prístup ku kybernetickej bezpečnosti

Richard Kiškováč, CISSP

Nemecko – útok voči zlievarenskej spoločnosti



Ukrajina – kybernetický útok na prenosovú sústavu



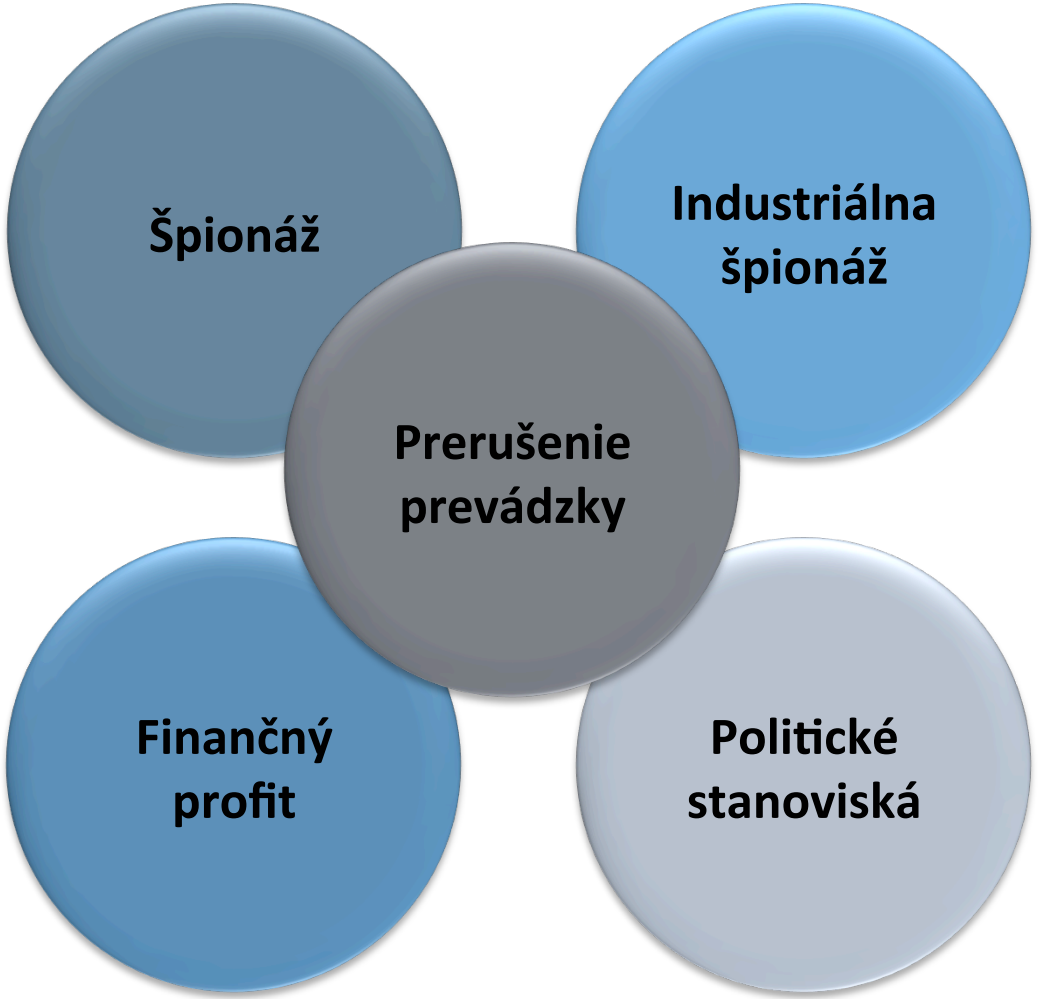
Aktéri a motivácia

Štátom sponzorované skupiny

Kyber-kriminálnici

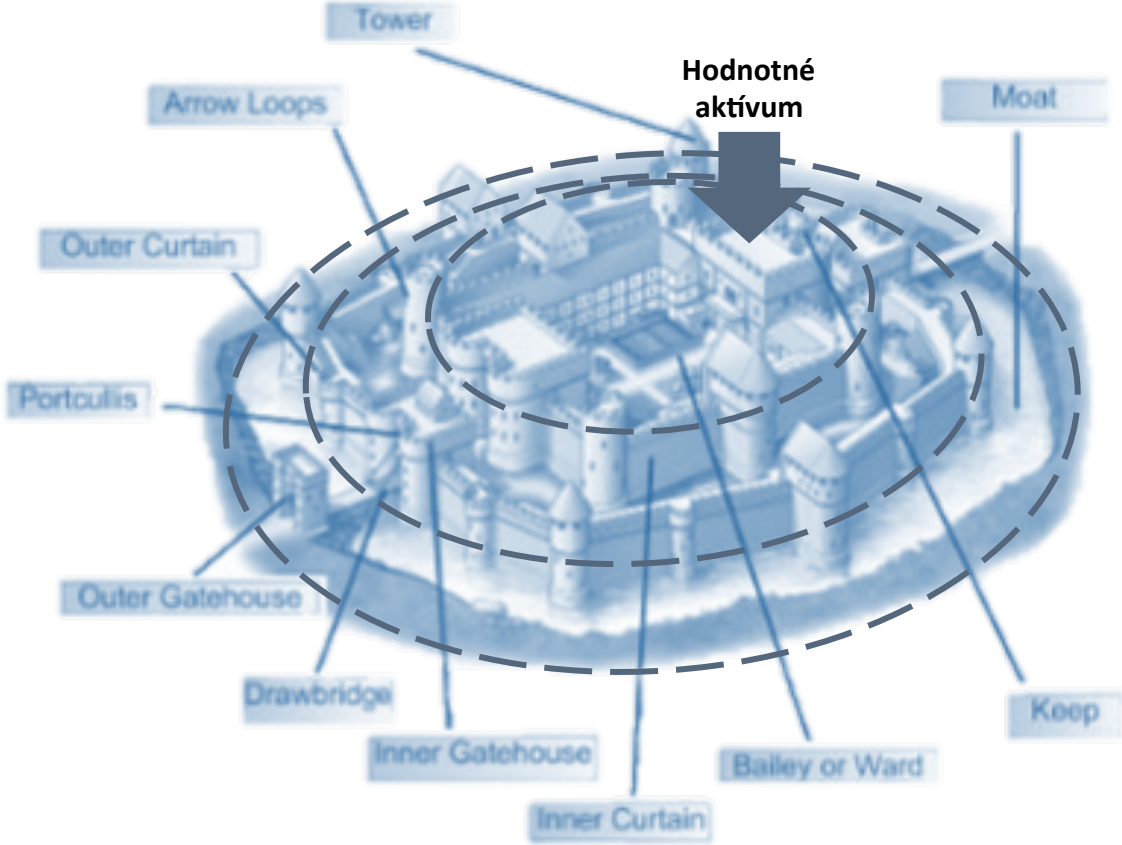
Haktivisti

Insideri

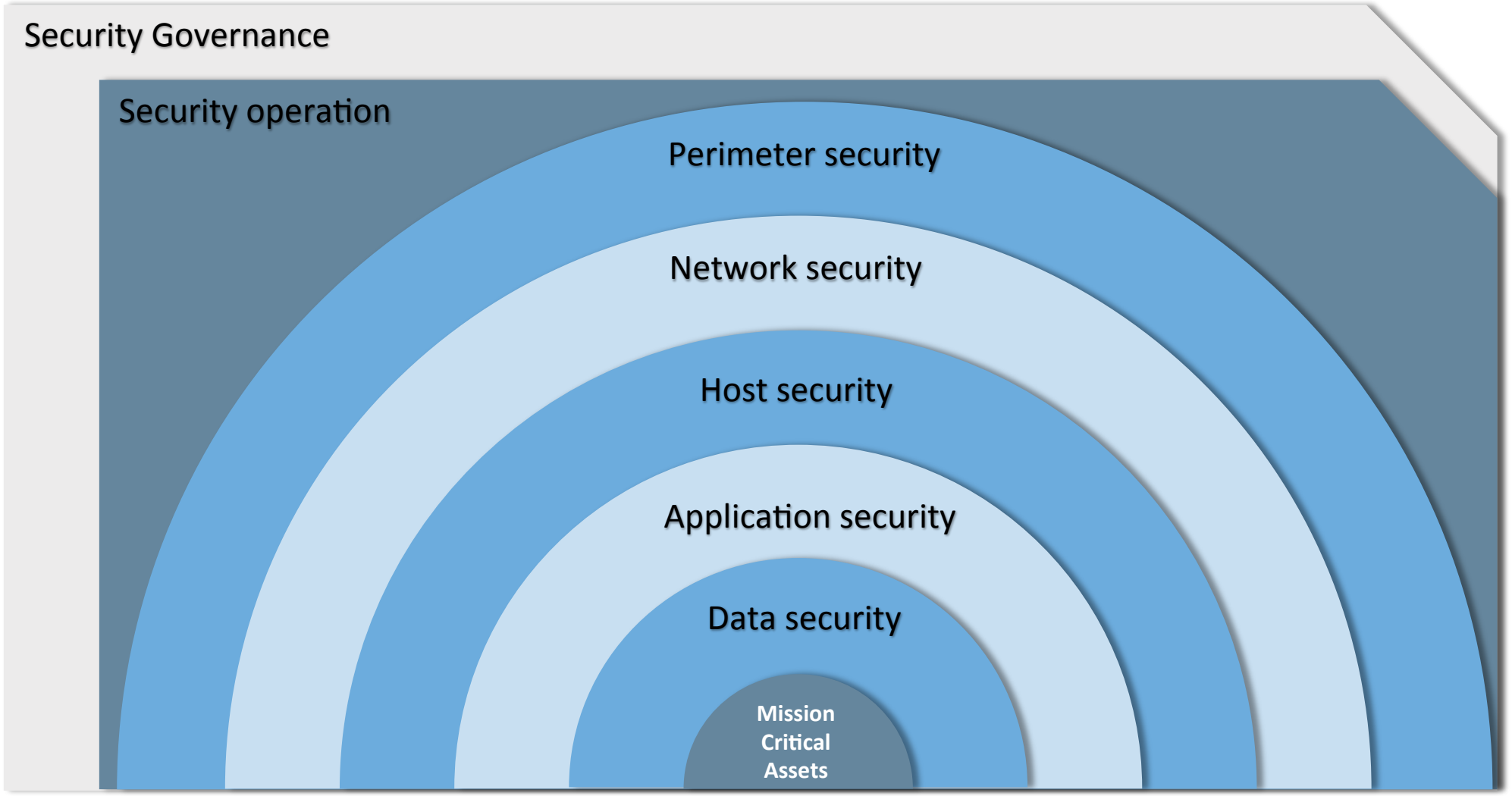


Bezpečnosť ako komplexný systém

- Komplexné hrozby si vyžadujú komplexné riešenia
- Je potrebné koordinované používanie viacerých bezpečnostných opatrení pre ochranu informačných aktív organizácie – koncepcia hĺbkovej ochrany (Defence in Depth)
- Vojenský princíp - Je ťažšie prekonať nepriateľov komplexnú viac vrstvovú obranu ako preniknúť iba jednou bariérou.
- Hĺbková ochrana minimalizuje pravdepodobnosť úspešnosti škodlivého útočníka.
- Dobre navrhnutá stratégia pomáha identifikovať škodlivé aktivity
- V prípade, že útočník získa prístup umožní minimalizáciu následkov a poskytne čas na odpoveď

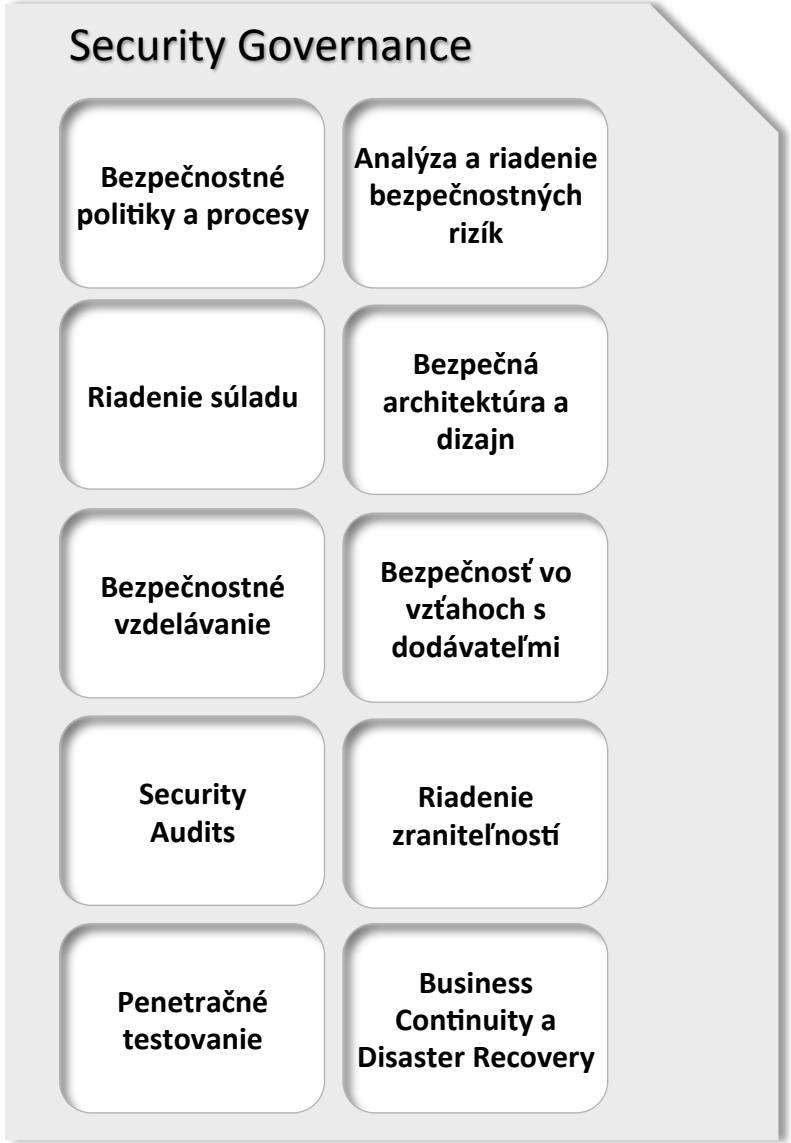


Koncepcia hĺbkovej ochrany - vrstvy



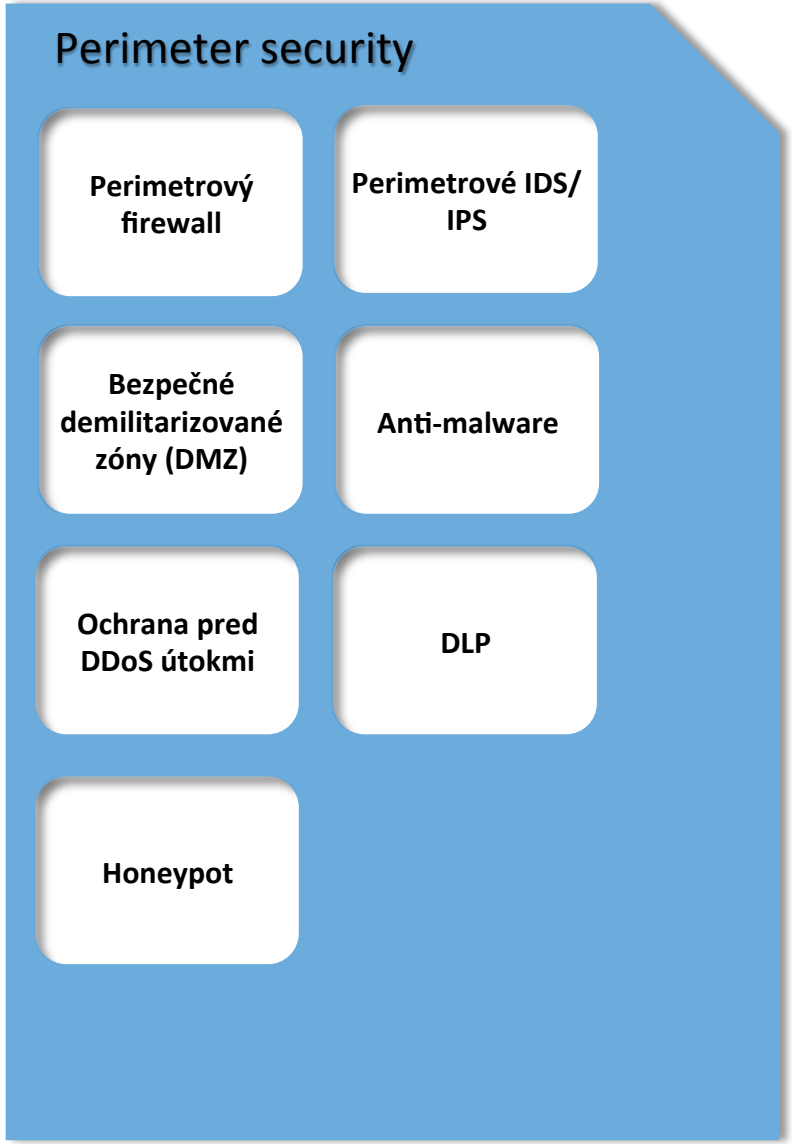
Security Governance

- Bezpečnostné politiky a procesy
- Analýza a riadenie bezpečnostných rizík
- Riadenie súladu
- Bezpečná architektúra a dizajn
- Bezpečnostné vzdelávanie
- Bezpečnosť vo vzťahoch s dodávateľmi
- Riadenie zraniteľností
- Bezpečnostné audity
- Penetračné testovanie
- Business Continuity a Disaster Recovery procesy



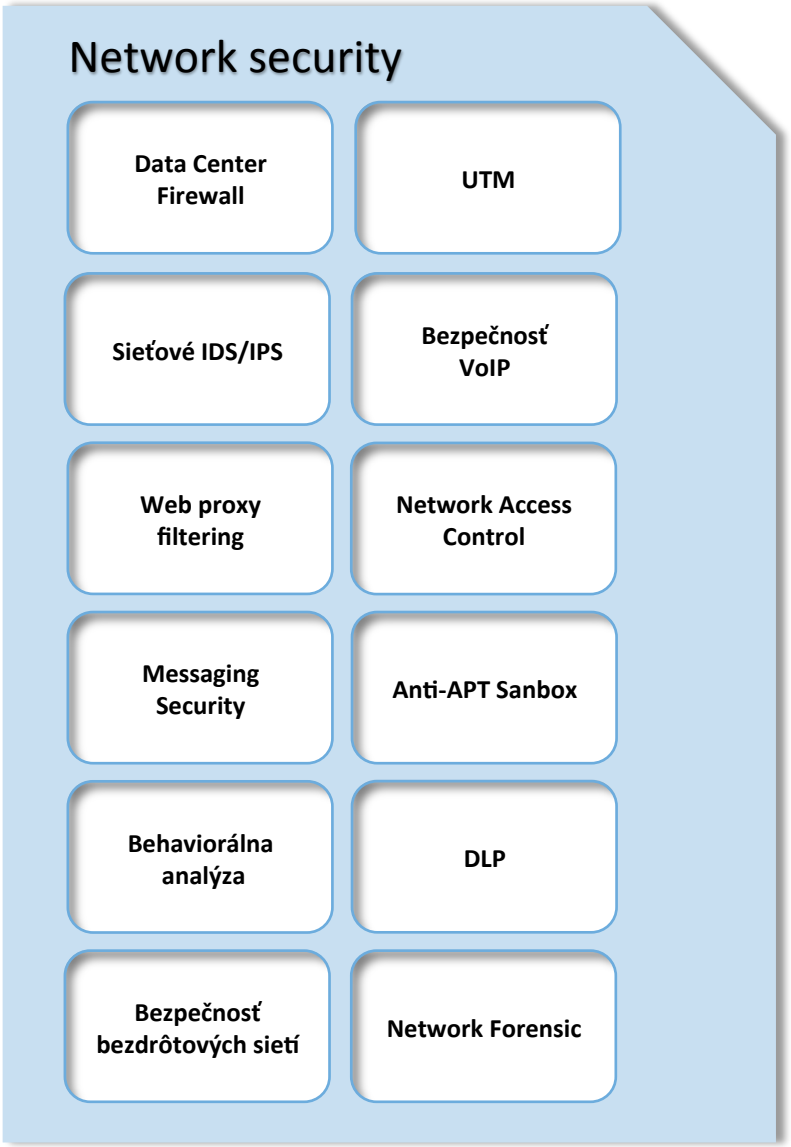
Perimeter Security

- Perimetrový firewall
- Perimetrové IDS/IPS
- Bezpečné demilitarizované zóny (DMZ)
- Perimetrové anti-malware riešenie
- Ochrana pred DDoS útokmi
- Data Leak Protection (DLP)
- Honeypot



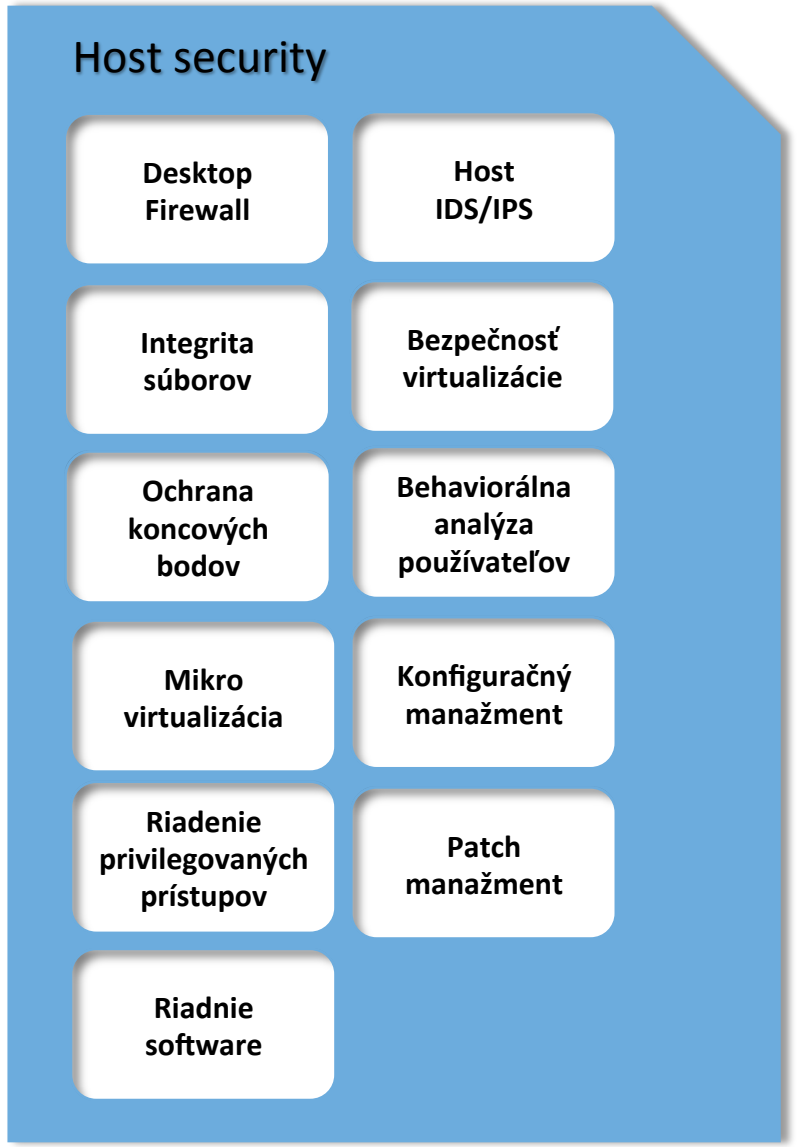
Network Security

- Data Center Firewall
- Sieťové IDS/IPS
- Jednotné riadenie hrozieb (UTM)
- Network Access Control (NAC)
- Bezpečnosť VoIP
- Web proxy filtering
- Bezpečnosť správ (messaging security)
- Anti-APT Sandbox
- Behaviorálna analýza
- Data Leak Protection (DLP)
- Bezpečnosť bezdrôtových sietí (Wireless Security)
- Network Forensic riešenia



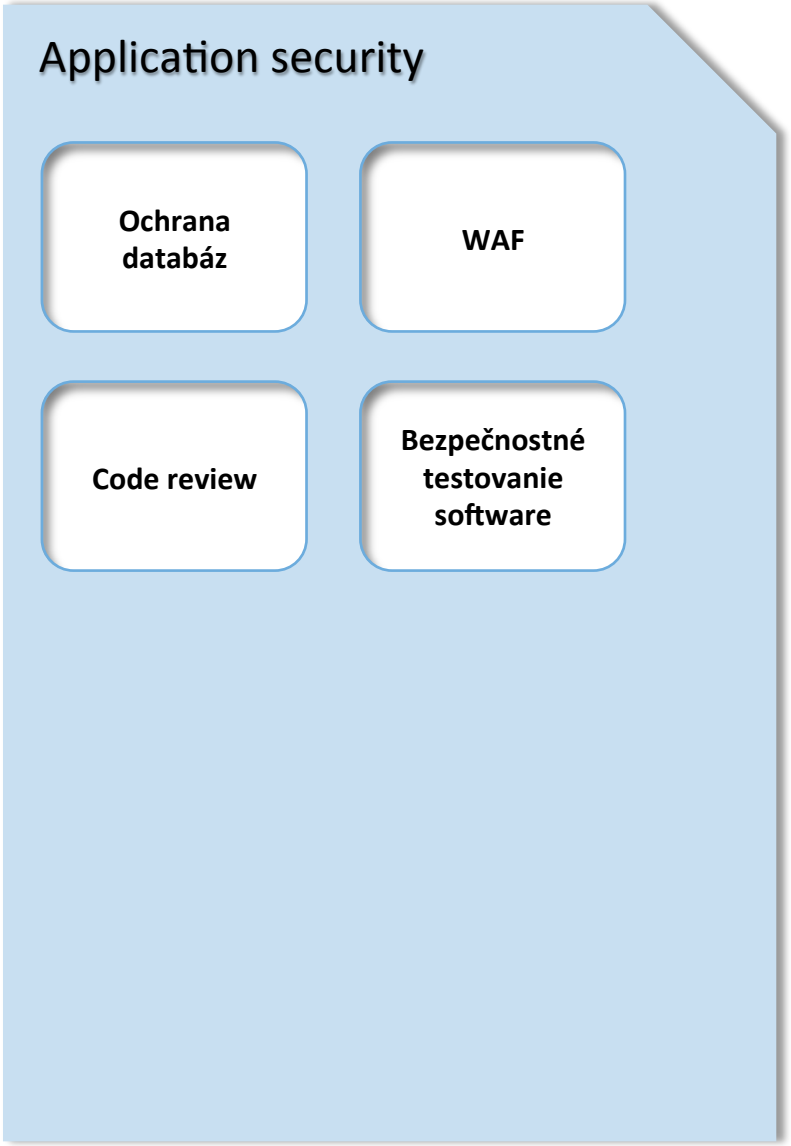
Host Security

- Desktop firewall
- Host IDS/IPS
- Integrita súborov
- Bezpečnosť virtualizácie
- Ochrana koncových bodov
- Behaviorálna analýza používateľov
- Mikro-virtualizácia
- Konfiguračný manažment
- Riadenie privilegovaných prístupov
- Riadenie software
- Patch manažment



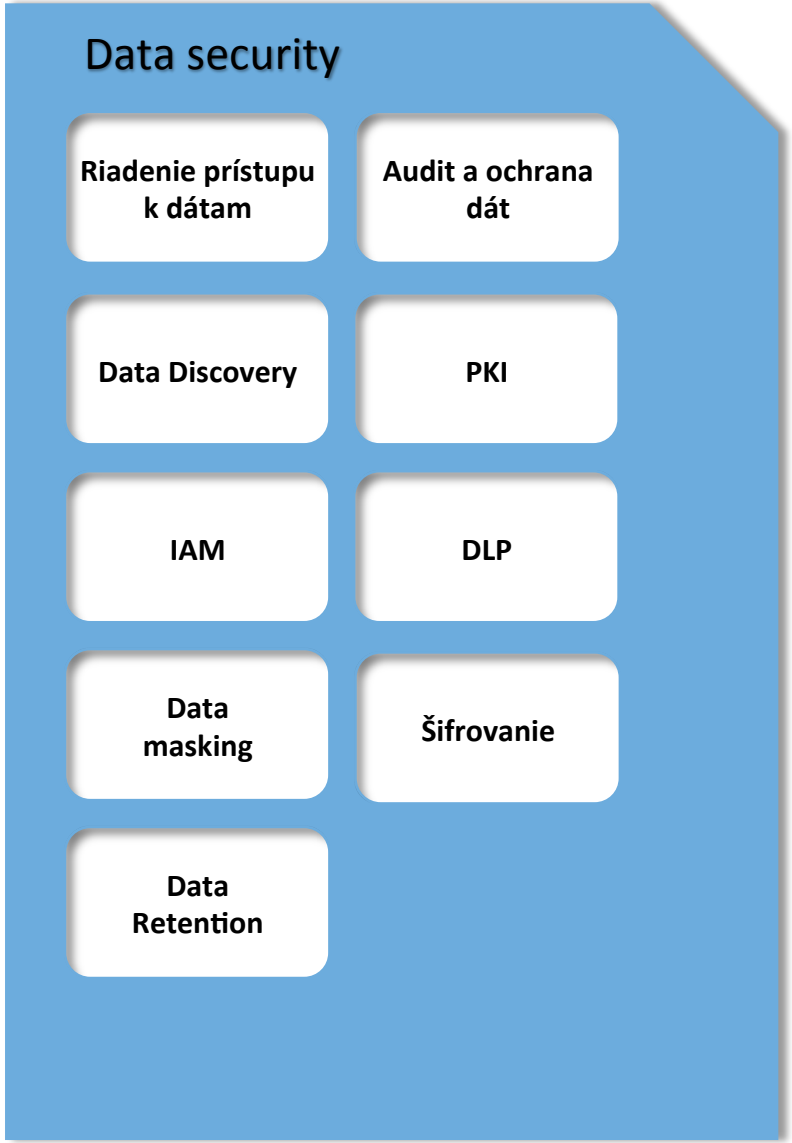
Application Security

- Ochrana Databáz
- Web Application Firewall (WAF)
- Code review
- Bezpečnostné testovanie software



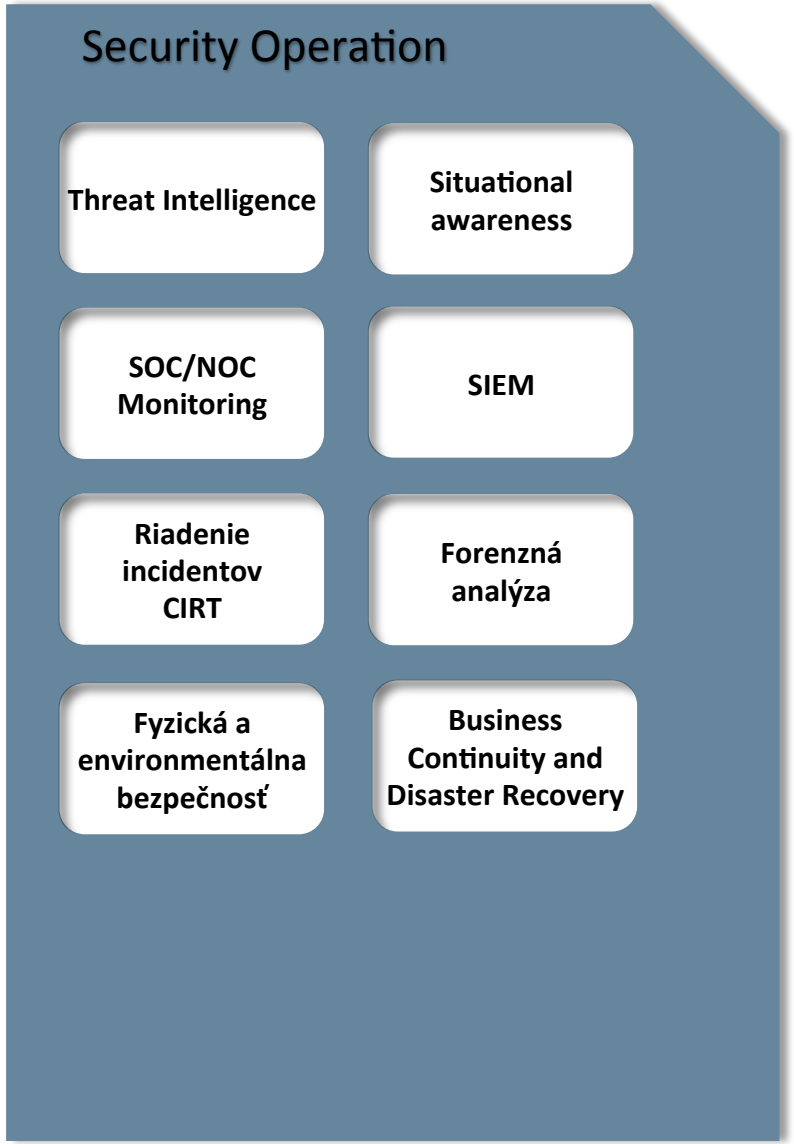
Data Security

- Riadenie prístupu k dátam
- Audit a ochrana dát
- Data Discovery
- PKI – Public Key Infrastructure
- IAM – Identity and Access Management
- DLP – Data Leak Prevention
- Data masking
- Šifrovanie
- Data Retention

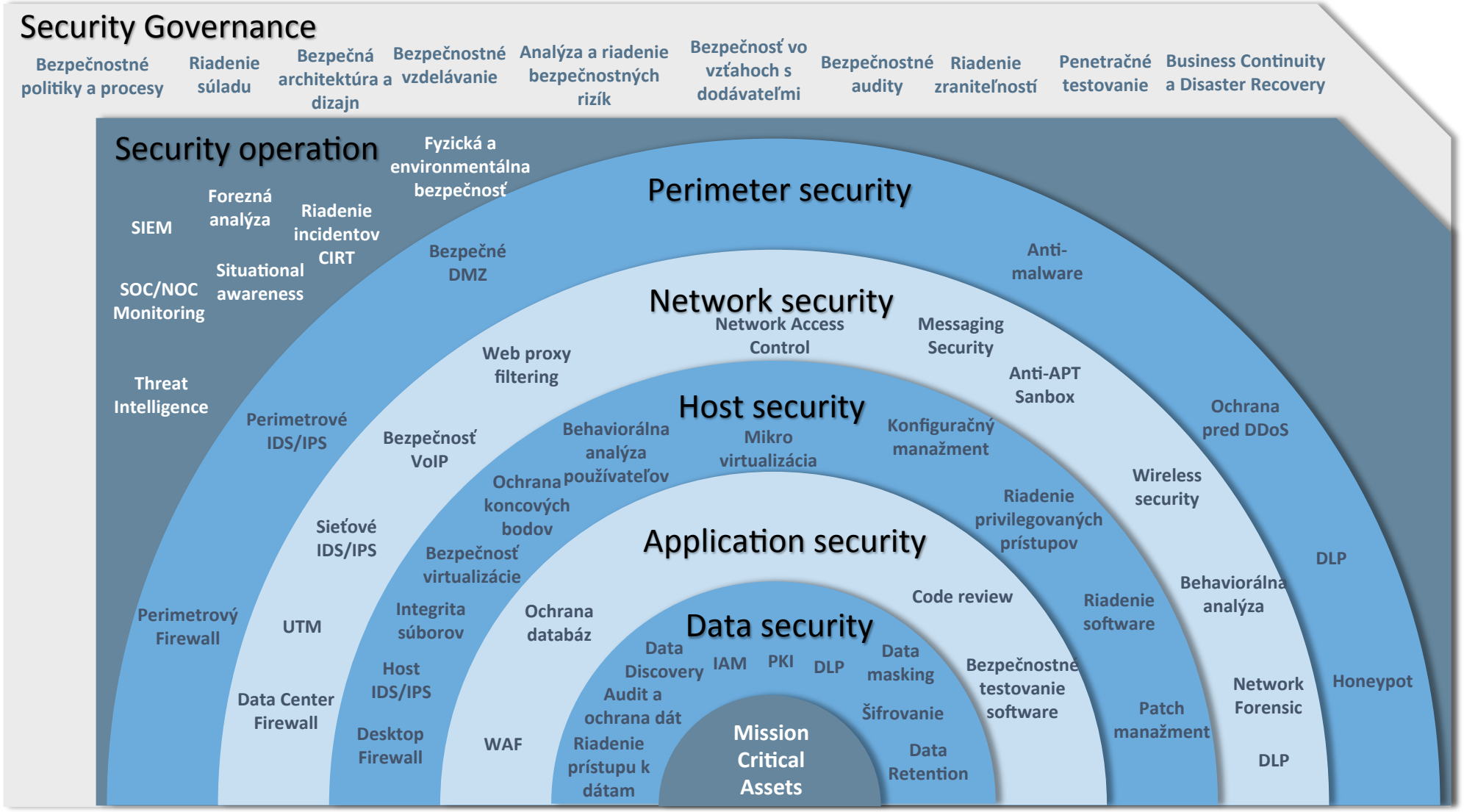


Security operation

- Threat Intelligence
- Situational Awareness
- Security/Network Operation Center (SOC/NOC)
- SIEM – Security Information and Event Management
- CSIRT – Riadenie incidentov
- Forenzná analýza
- Business Continuity and Disaster Recovery
- Fyzická a environmentálna bezpečnosť



Komplexný prístup ku kybernetickej bezpečnosti



ALITER TECHNOLOGIES

Ďakujeme za pozornosť