Dohledové centrum eGovernmentu

Aplikace ZoKB v praxi

Česká pošta
odštěpný závod ICT služby

Česká pošta
odštěpný závod ICT služby

Zák.181/2014Sb - opatření

Označení	Znění zákona	OPATŘENÍ
§ 4		DCeGOV
§ 5, 1 a), b)		SOCCR
§ 5, 2 b)	řízení rizik	nástroj RAMSES pro Risk a BC Management
§ 5, 2 h)	řízení provozu a komunikací kritické informační infrastruktury nebo významného informačního systému	Service Desk, Provozní a Bezpečnostní monitoring
§ 5, 2 i)	řízení přístupu osob ke kritické informační infrastruktuře nebo k významnému informačnímu systému	Identity Management, VPN, 2FA, JIP
§ 5, 2 k)	zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů	Service Desk, Risk a Business Continuity Management
§ 5, 2 l)	řízení kontinuity činností	Risk a Business Continuity Management
§ 5, 3 a)	fyzická bezpečnost	zajištěno smluvně technickými prostředky dodavatelů prostředí datových center a organizačně
§ 5, 3 b)	nástroj pro ochranu integrity komunikačních sítí	Firewall, IDS/IPS, HonePot, NetFlow, AntiMalware, AntiSpam, Anti DDoS, VPN, Provozní a Bezpečnostní monitoring, NTP, Patch Management
§ 5, 3 c)	nástroj pro ověřování identity uživatelů	Identity Management a 2FA, JIP
§ 5, 3 d)	nástroj pro řízení přístupových oprávnění	Identity Management a 2FA, JIP
§ 5, 3 e)	nástroj pro ochranu před škodlivým kódem	AntiMalware, AntiSpam, Firewall, IDS/IPS, , NetFlow, Patch Management
§ 5, 3 f)	nástroj pro zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů	Provozní a Bezpečnostní monitoring,Service Desk, 2FA,Identity management, Nástroje řízení přístupu, NTP
§ 5, 3 g)	nástroj pro detekci kybernetických bezpečnostních událostí	jsou Firewall, IDS/IPS, HonePot, NetFlow, AntiMalware, AntiSpam, Anti DDoS, VPN, Provozní a Bezpečnostní
§ 5, 3 h)	nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí	Provozní a Bezpečnostní monitoring, Service Desk, NTP, Risk a Business Continuty Management
§ 5, 3 i)	aplikační bezpečnost	Firewall, IDS/IPS, AntiDDoS, Vurnerability Scaner
§ 5, 3 j)	kryptografické prostředky	VPN
§ 5, 3 k)	nástroj pro zajišťování úrovně dostupnosti informací	Vulnerability Scaner, Balancery, Zálohování, Clustering, Provozní a Bezpečnostní monitoring, Archivace, AntiDDos a architektura tedy Redundance důležitých součástí

DCeGOV - popis

Dohledové centrum eGovernmentu zajišťuje pro resort MV provozní a bezpečnostní dohled, monitoring ICT, řízení jednotlivých událostí a incidentů ICT.

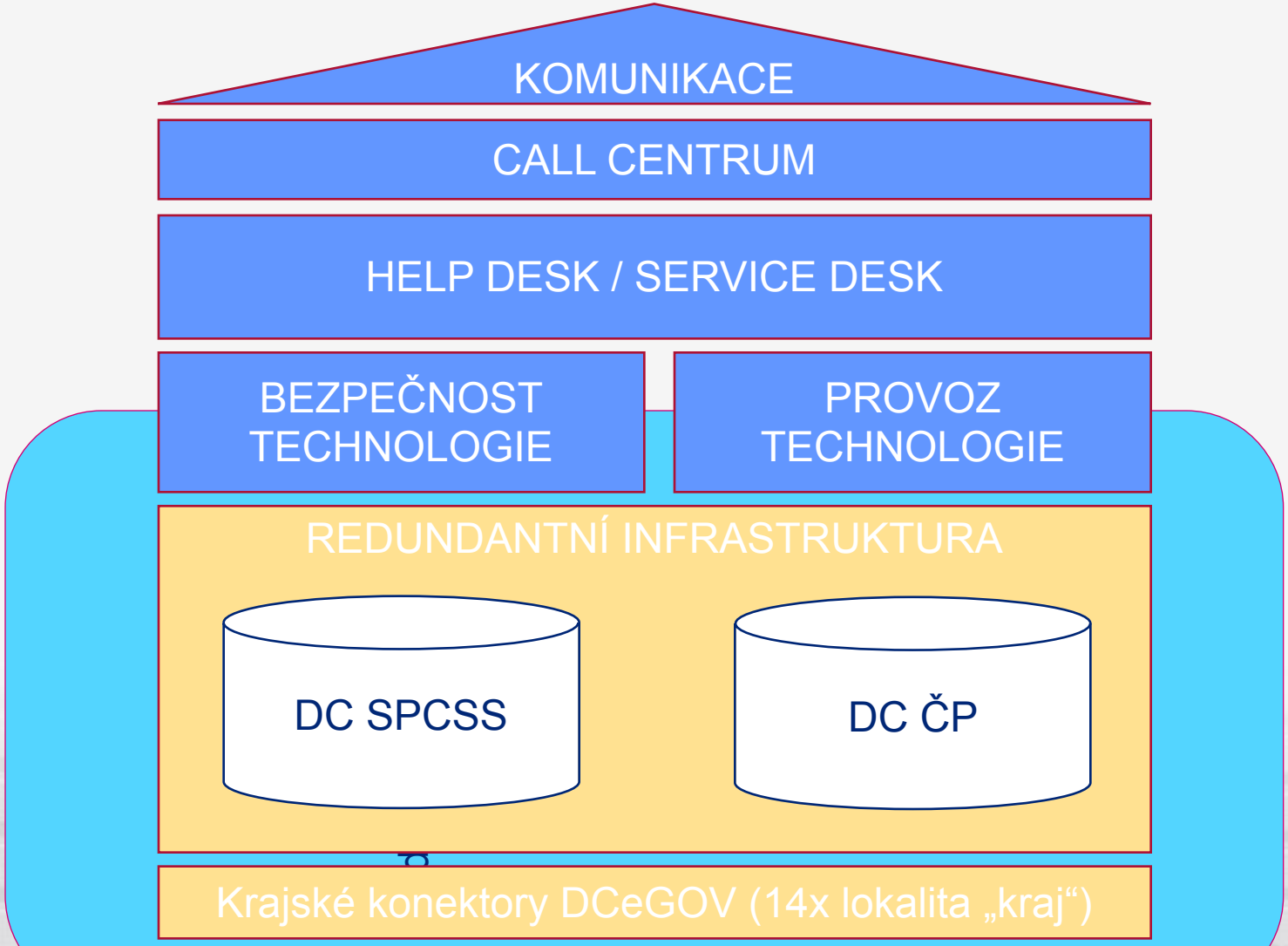
Cíle DCeGOV

- Sběr a vyhodnocování událostí nad IS a infrastrukturou resortu MV
- Identifikace a řešení provozních a bezpečnostních událostí a incidentů
- Zajištění komunikace s NCKB

Základní pilíře DCeGOV

- CALL CENTRUM / příjem událostí
- SOCCR / bezpečnostní proaktivní dohled
- NOC / provozní proaktivní dohled

DCeGOV - schéma



DCeGOV - základní vlastnosti

- Soulad se ZoKB (Zák.181/2014Sb.)
- Soulad s ISO standardy
- Provoz 24x7x365
- Proaktivní dohled
- Vysoká dostupnost
- Koordinace týmů (SOCCR, TKB, …)
- Modulární architektura
- Vlastní aktivní ochrana
- Zdroj znalostní báze

DCeGOV - základní funkcionality

pro IS a infrastrukturu resortu MV (KII, VIS …)

- Dohled a monitoring
- Řízení procesů dohledu a monitoringu
- Identifikuje, řídí, řeší události a zavádí nápravná a preventivní opatření
- **Identifikuje, řídí, řeší zavádí nápravná a preventivní opatření k KBU/KBI**
- Podpora řízení rizik a kontinuity
- Identifikace zranitelností a hrozeb
- Komplexní reporting, log management (ukládání, analýza, korelace, agregace, archivace)

DCeGOV - nástroje

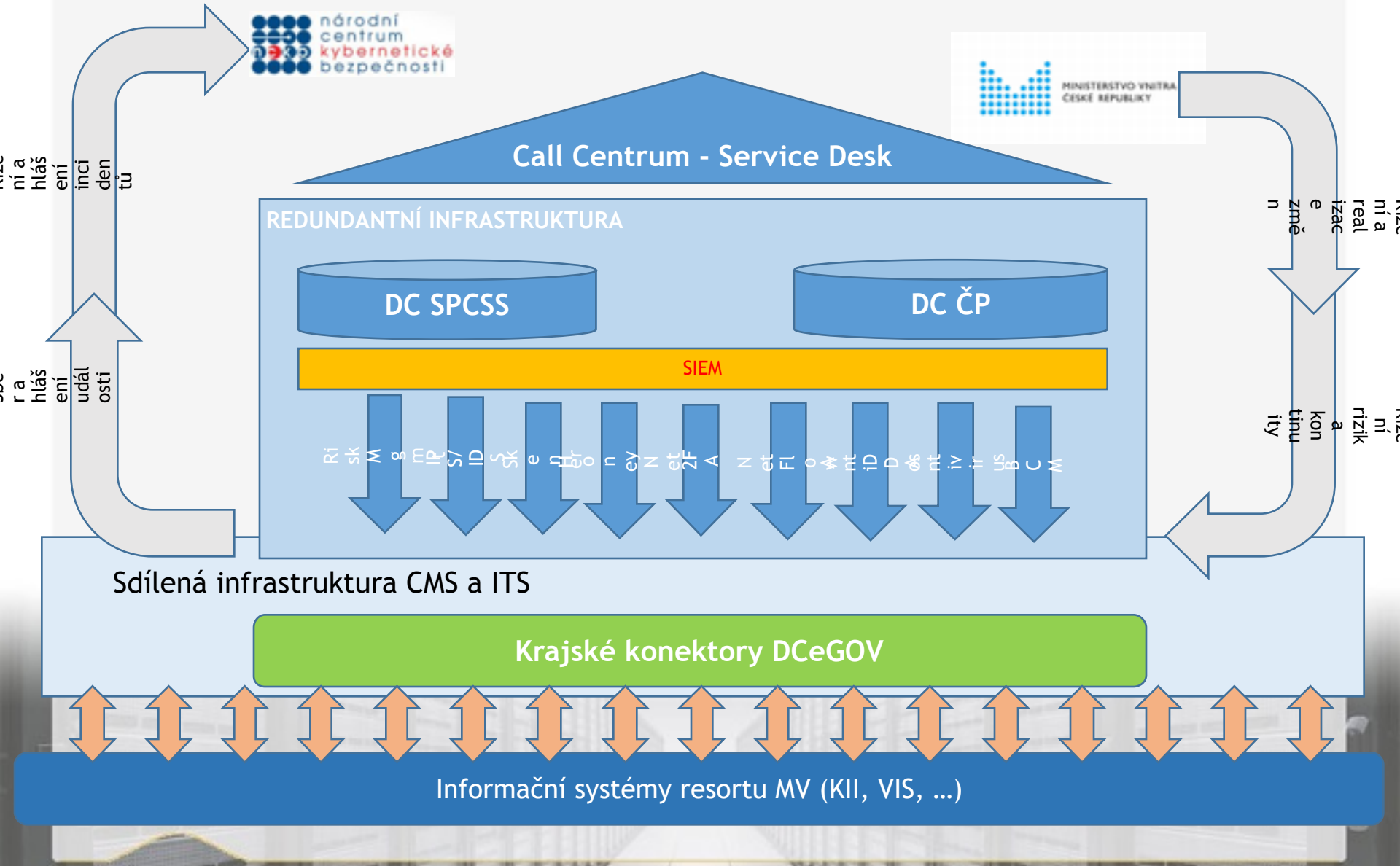
Technologické nástroje

- CallCentrum
- ServiceDesk
- SIEM
- Logger
- Vulnerability Management
- HoneyNet
- Net Flow
- Řízení rizik a kontinuity
- Antivirus
- AntiDDos
- IDS/IPS
- 2 FA

Personál

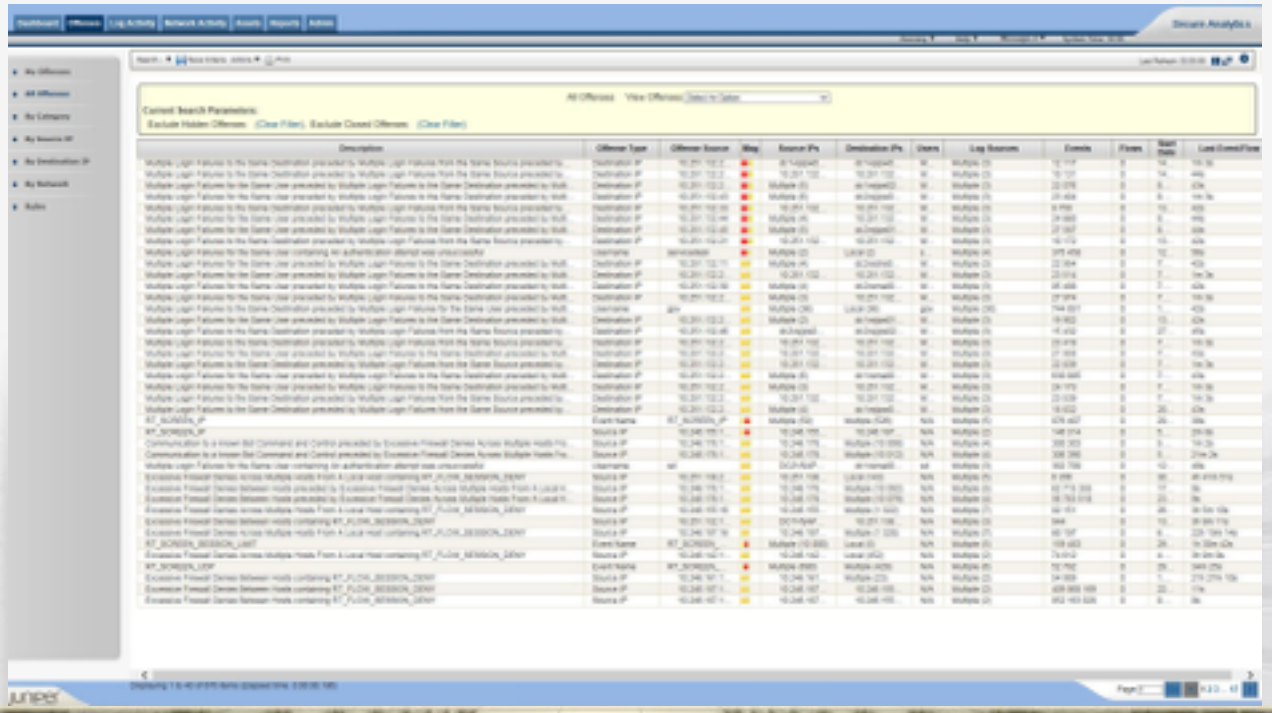
- Operátoři
- Analytická skupina
- Administrátoři
- Správci
- Analytici
- Kompetenční zázemí
- Architekti
- Vývoj
- Bezpečnost
- Tým kybernetické bezpečnosti
- Externí podpora
- Dodavatelé
- Partneři

SOCCR - schéma



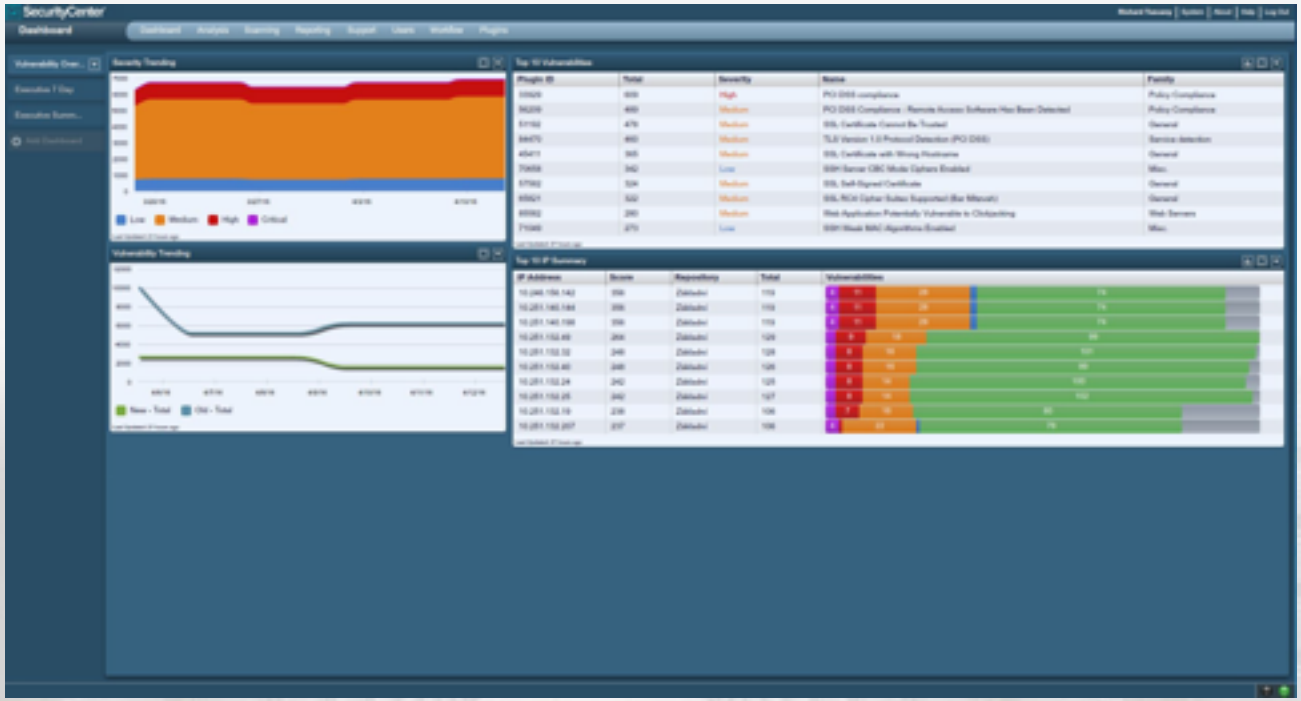
SIEM

- Redundantní nasazení
- Jádro bezpečnostního řešení, rozšířením konfigurace, navýšením kapacity možno pokrýt další systémy MV (DCeGOV)
- Pro získávání záznamů o provozu + doplňující informace z IPS/IDS, NBA - Netflow, Vulnerability scanneru
- Nedílnou součástí SIEM jsou analytické nástroje pro vyšetřování incidentů a reaktivní opatření
- Reporting bezpečnostních incidentů pomocí stanoveného rozhraní na NCKB



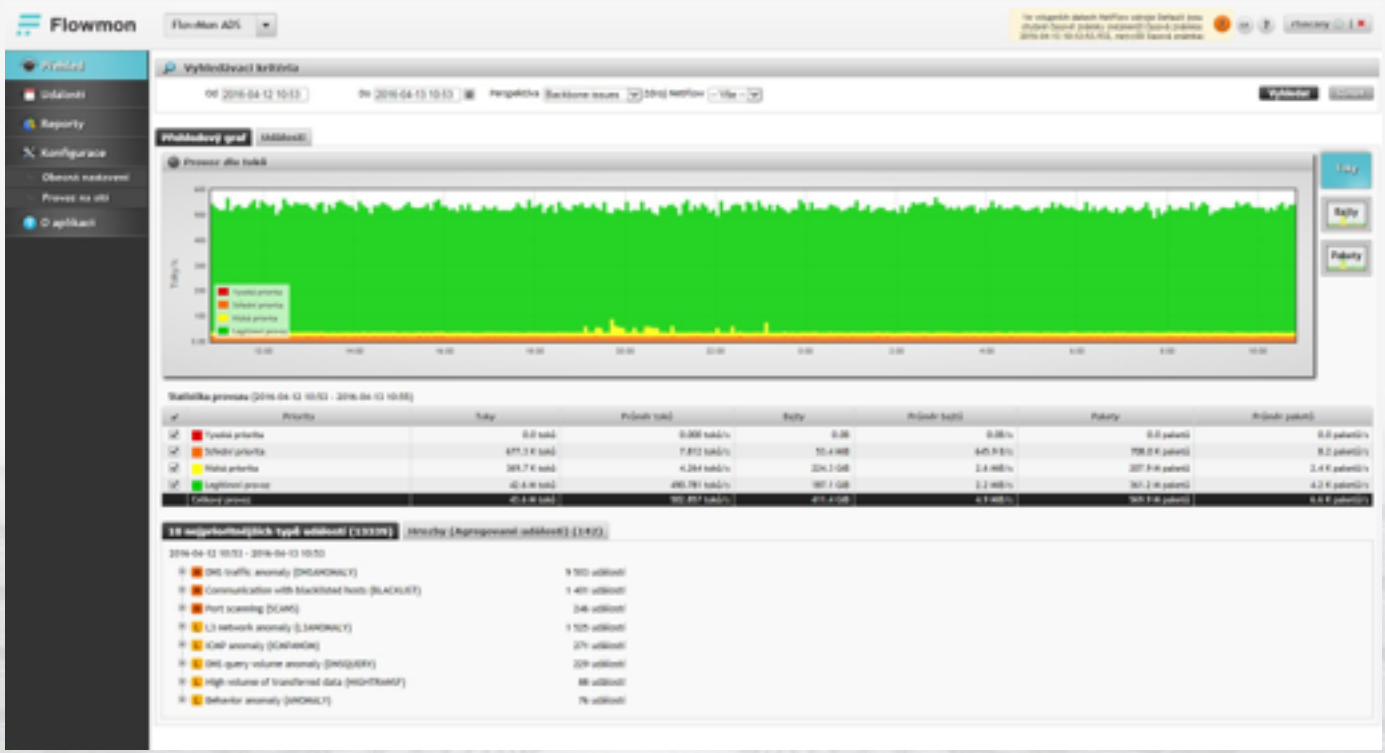
Vulnerability Management

- Kontrola konfigurace a aktualizací - umožňuje zkontrolovat na infrastrukturních komponentách nainstalované bezpečnostní aktualizace včetně nastavení politik a porovnat je s doporučenými parametry a databází všech dostupných aktualizací a doporučit doinstalování chybějících záplat (pokrytí bez. mezer, které mohou být exploitovány) nebo provedení změn nastavení.
- Kontrola bezpečnostní konfigurace systému - umožňuje zkontrolovat na infrastrukturních komponentách správnost nastavení a doporučit změny nastavení (pokrytí rizika neoprávněného přístupu k systému, zamítnutí služby)
- Skenování je prováděno na všech zařízeních v infrastruktuře do úrovně operačního systému.



Netflow analyzer

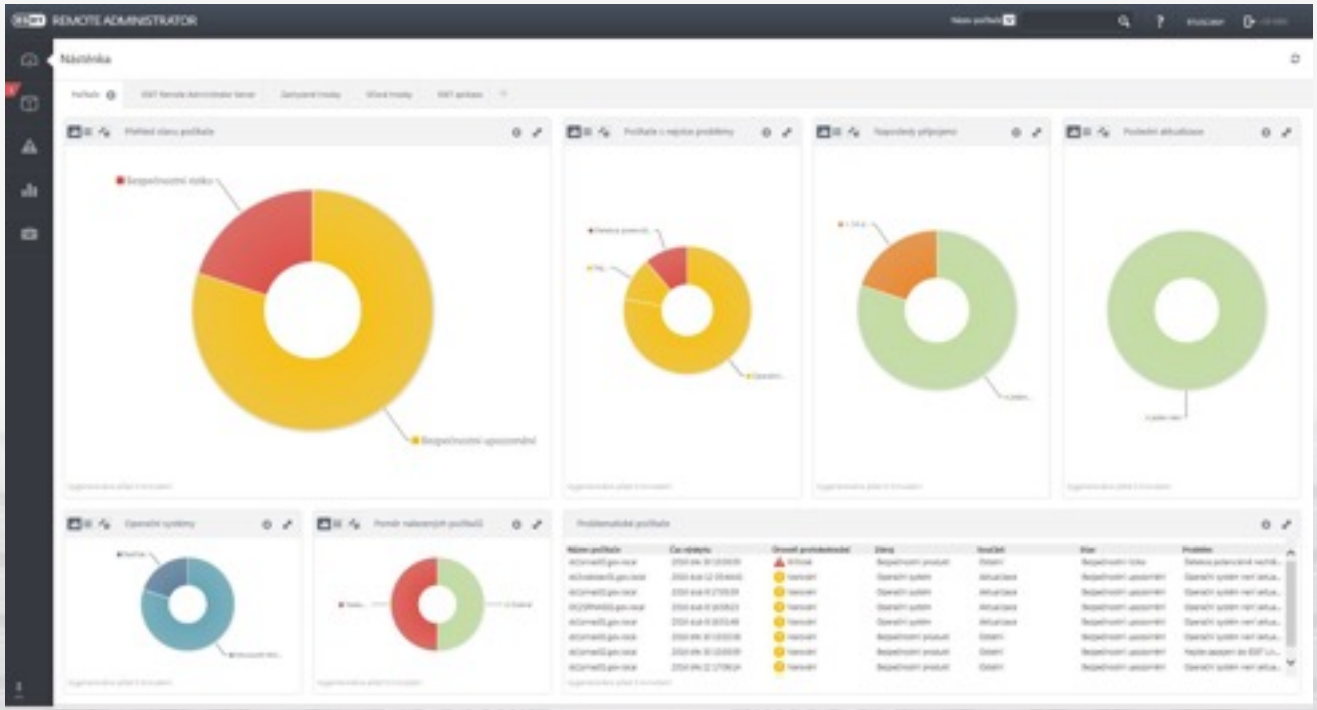
- Pokrývá riziko výskytu nestandartní komunikace, změny konfigurací
- Netflow analyzer analyzuje datové toky a jejich vývoj. Upozorní na existenci nových profilů chování
- Monitorování síťového provozu na základě IP toků, součástí autonomní sondy, kolektory pro uložení, zobrazení, analýzu síťových aktivit a další moduly



Antivirus

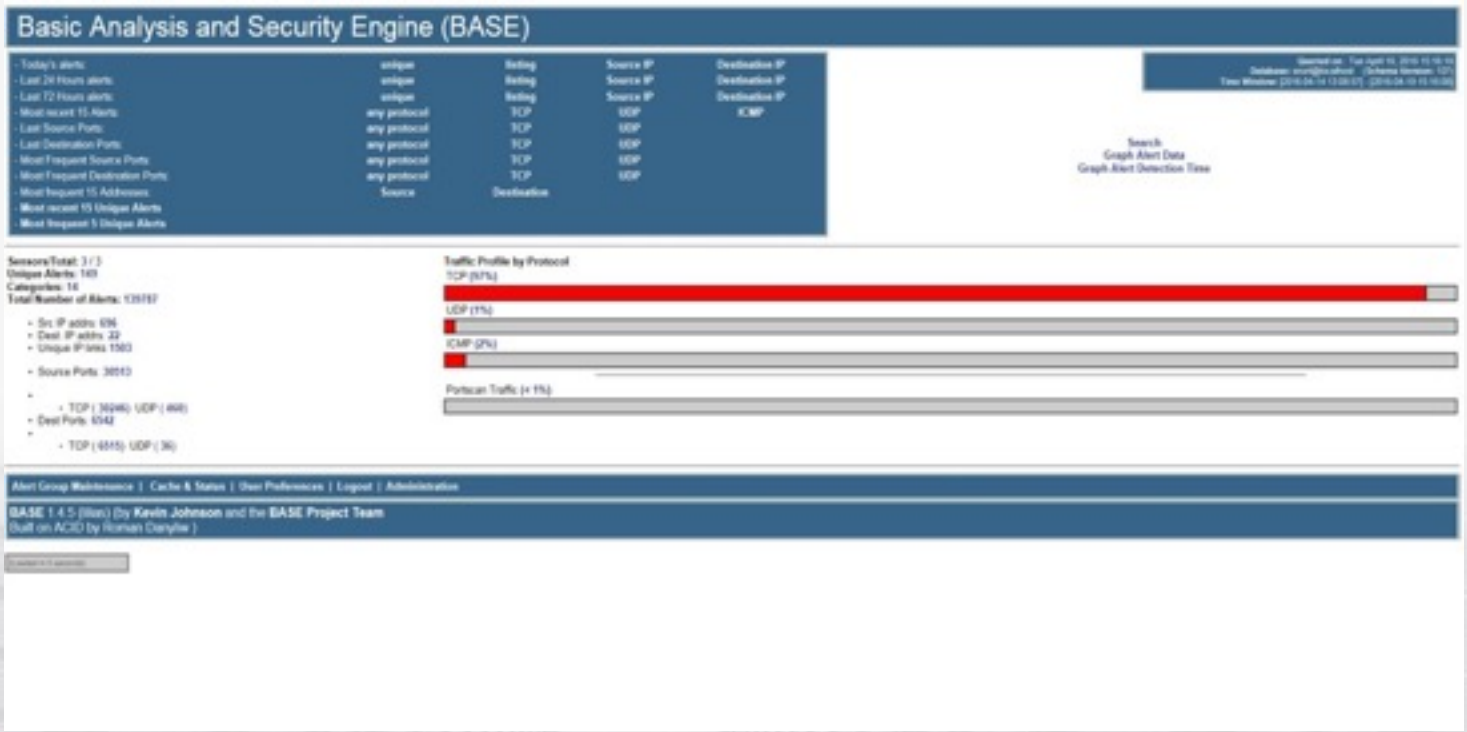
Chrání před škodlivým obsahem

- App/db servery
- OS serverů
- počítače dohledového centra



HoneyNet

- Účinná návnada
- Simulace kritických služeb
- Umožní studovat a získat vzorce chování útočníka
- Komplikuje pokusy o kompromitaci systému
- Technologicky „živé“ prostředí



Řízení rizik IS resortu MV (KII, VIS)

Analýza rizik na systémech určených k dohledu

- Výstup tvoří podklad pro sestavení rozsahu a režimu dohledu
- Hodnocení aktiv = rámec dohledu
- Hodnocení hrozeb = platforma stanovení SLA
- Plán kontinuity = koncept procesů Recovery a Redundance

Interaktivní RISK MANAGEMENT

- Automatizovaný přístup k informacím – aplikace RAMSES
- Události vyhodnocujeme v korelaci s nastavenými parametry
- Ukazatele rizik a hrozeb jsou aktualizovány ve vazbě na reálný provoz
- Četnosti a rozsah událostí určují úroveň opatření
- Dle úrovně znalostí o hrozbách upravujeme režim dohledu
- Změny konzultujeme a sdílíme se správci aktiv

Řízení kontinuity IS resortu (KII, VIS)

- Pro každou službu / proces / aktivum, je stanovena maximální tolerovatelná doba výpadku, doba obnovy po přerušení a požadovaná úroveň funkčnosti
- Jsou identifikovány podpůrné aplikace, nástroje, aktiva a případně další zdroje (vstupy) procesu
- Strategie vychází z provedené analýzy dopadů.
- Plány kontinuity a obnovy nastavují postupy reakce a eskalace při mimořádných událostech Součástí plánů je určení odpovědností za jednotlivé činnosti při odstraňování následků mimořádných událostí, eskalační matice, důležité kontakty...

DCeGOV - služby

Primární služby

- Log management
- Provozní monitoring

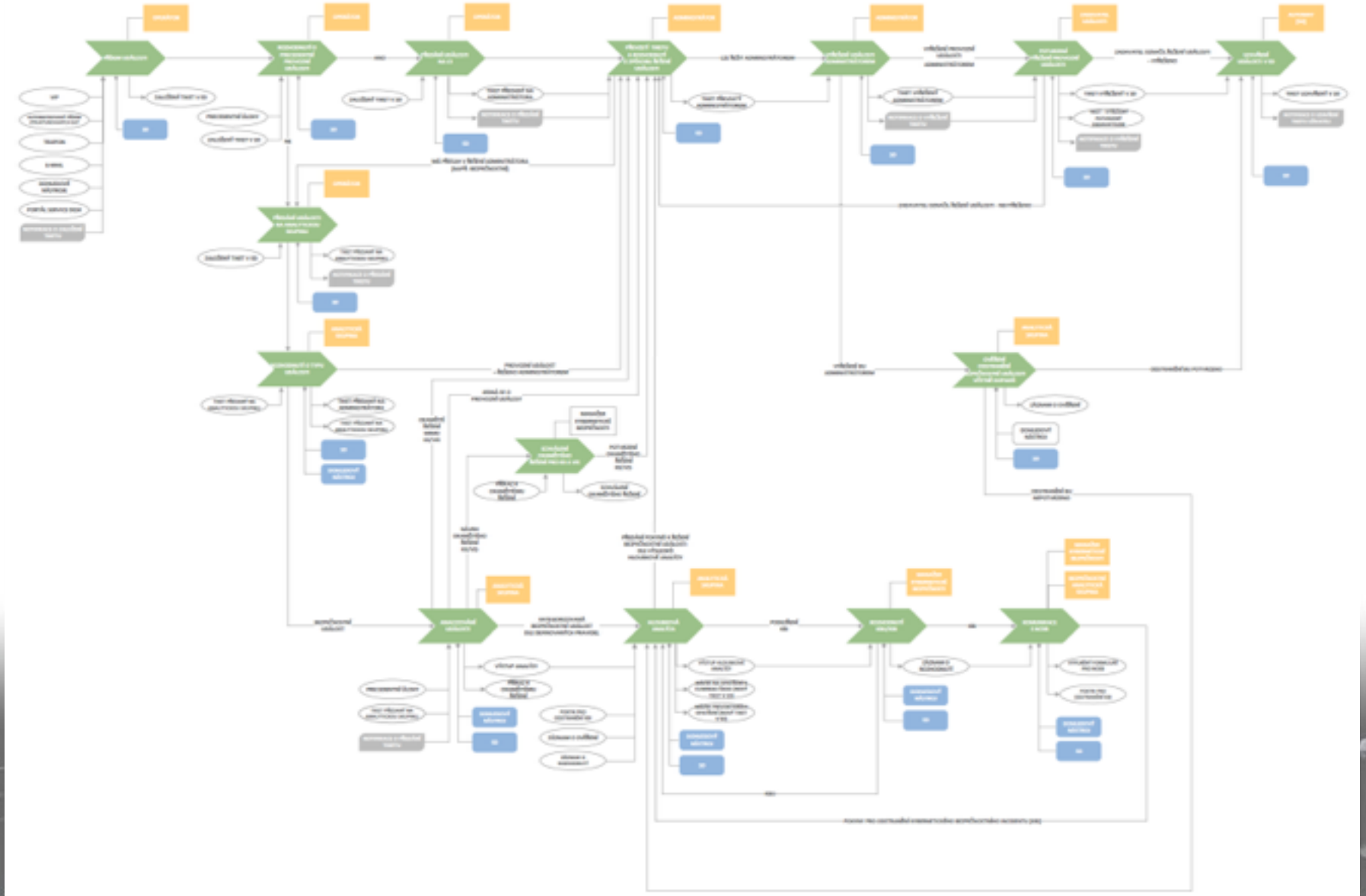
Podpůrné služby

- Patch management
- Release management
- Zálohování
- Archivace
- IDM
- NTP (řízení přesného času)
- Zabezpečený vzdálený přístup
- SMS notifikace
- e-mailové služby
- Vícefaktorová autentifikace
- Atd.

Bezpečnostní služby

- Zabezpečení perimetru
- Kontrola obsahu
- Analýza datových toků
- Analýza kapacitních ukazatelů
- Aktualizace bezpečnostních opatření
- Risk management
- Řízení kontinuity
- Analýza hrozeb
- Proaktivní dohled

Proces řešení Tiketu - základní schéma



DĚKUJI ZA POZORNOST …

Luděk Tichý

Vedoucí oddělení Bezpečnost ČP OZ ICTs

Kontakt: tichy.ludek@cpost.cz