



Řešení kybernetické bezpečnosti v podmínkách Integrovaného Záchranného Systému

IT4P - Information Technology for Practice
2023

Thursday, October 9th 2023

David Klíma, Martin Votava



V čem vynikáme

Specializace:

ICT a komplexní outsourcing

kybernetická bezpečnost

vývoj a úprava software

fyzická bezpečnost

průmyslová automatizace

integrované záchranné systémy

Gold
Microsoft Partner



CISCO
Partner
Premier Certified

JUNIPER
NETWORKS

SELECT PARTNER

NAKIVO
GOLD PARTNER

 Sophos
Gold
Partner

DELL EMC
PARTNER
GOLD

VEEAM | PRO PARTNER
Silver Reseller

 Business
Partner

vmware
PARTNER
ENTERPRISE
SOLUTION PROVIDER

riverbed
Klasifikace informací: Neveřejně

Referenční projekty - fyzická bezpečnost

cBIS - Centrální biometrický systém Policie ČR

Nový centrální biometrický a identifikační informační systém PČR



EES - Entry Exit System – Cizinecká policie ČR

Nový evropský IS, pro biometrický záznam údajů příslušníků třetích zemí, kteří vstupují do schengenského prostoru přes naše mezinárodní letiště



EasyGO (eGate) – Ředitelství služby cizinecké policie

Dodávka a servis biometrických bran na Letišti Praha Ruzyně



NKA - Národní kontrolní autorita

Systém národní infrastruktury MV ČR pro ověření integrity a autenticity elektronických cestovních dokladů s biometrickými prvky, (tzv. ePasy)



Zvýšení bezpečnosti klíčových komponent TCTV112

Změna aplikační části na HA systém, simulátor nehlasových tísňových výzev a externích rozhraní, persistence dat v případě havárií systému, DLOC pro chytré hodinky, modul Předzpracování přijatých SMS-T pomocí deterministického algoritmu

ZOS Zlínského kraje

Modernizace informačního systému a technologií zdravotnického operačního střediska



Zajímavosti ze záchranky

- ▼ V roce 2022 přijali dispečeri 104 534 hovorů (286 hovorů denně), ale pouze 52 % z nich končí výjezdem záchranářů.
- ▼ Přes 8 tisíc hovorů zvládnou vyřešit dispečeri přes telefon radou nebo doporučením.



Ostravské vodárny a kanalizace

V rámci posílení ochrany před kybernetickými hrozbami byla u zákazníka provedena segmentace sítě, tedy oddělení aplikační sítě od sítě technologické. Oddělení těchto sítí pomohlo izolovat kritické systémy a data od potenciálních hrozeb.

Biskupství Ostravsko-opavské

Dodávka a implementace centrálního logovacího kolektoru

Střední škola techniky a služeb Karviná

Zpracování auditu kybernetické bezpečnosti

Ostravská univerzita

Posílení bezpečnosti síťové infrastruktury - implementace dle standardů 802.1X. řízení přístupu k sítí



KYBERNETICKÁ BEZPEČNOST

od VÍTKOVICE IT SOLUTIONS a.s.

v podmínkách integrovaného

záchranného systému



Cíle projektu

- ▼ Dodávka komplexního systému bezpečnosti v souladu s nejnovějšími trendy
- ▼ Pokrytí stěžejních vektorů
 - Firewalling a segmentace sítě
 - Endpoint protection včetně EDR
 - Ochrana dat (DLP a šifrování)
 - Privileged Access Management (PAM)
 - Dvoufaktorová autentizace
 - Vulnerability management
 - Lokální Threat Intelligence
 - Sběr a vyhodnocování událostí
 - Identity Management (IDM)
- ▼ Maximální úroveň integrace a automatizace
- ▼ Naplnění nově příchozích norem (např. NIS2)



Pomoc se splněním technických opatření NIS2

Bezpečnostní opatření poskytovatele regulované služby

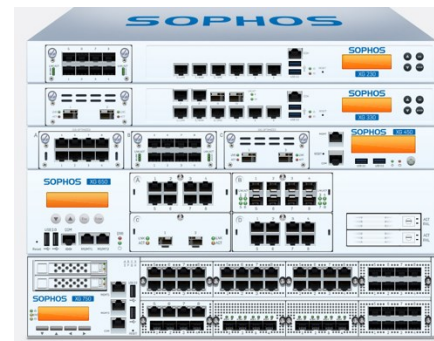
	v režimu vyšších povinností	v režimu nižších povinností	
organizační opatření	§ 4 Systém řízení bezpečnosti informací	§ 4 Zajišťování kybernetické bezpečnosti	
	§ 5 Povinnosti Vrcholného vedení	§ 5 Povinnosti vrcholného vedení	
	§ 6 Bezpečnostní role		
	§ 7 Řízení bezpečnostní politiky a bezpečnostní dokumentace		
	§ 8 Řízení aktiv		
	§ 9 Řízení rizik		
	§ 10 Řízení dodavatelů		
	§ 11 Bezpečnost lidských zdrojů	§ 6 Bezpečnost lidských zdrojů	
	§ 12 Řízení změn		
	§ 13 Akvizice, vývoj a údržba		
	§ 14 Řízení přístupu	§ 8 Řízení přístupu	
	§ 15 Zvládnání kybernetických bezpečnostních událostí a incidentů	§ 11 Řešení kybernetických bezpečnostních incidentů	
	§ 16 Řízení kontinuity činností	§ 7 Řízení kontinuity činností	
	§ 17 Audit kybernetické bezpečnosti		
	technická opatření	§ 18 Fyzická bezpečnost	
		§ 19 Bezpečnost komunikačních sítí	§ 12 Bezpečnost komunikačních sítí
		§ 20 Správa a ověřování identit	§ 9 Řízení identit a jejich oprávnění
§ 21 Řízení přístupových oprávnění		§ 18 Řízení přístupových oprávnění	
§ 22 Detekce kybernetických bezpečnostních událostí			
§ 23 Zaznamenávání událostí		§ 10 Detekce a zaznamenávání kybernetických bezpečnostních událostí	
§ 24 Vyhodnocování kybernetických bezpečnostních událostí			
§ 25 Aplikační bezpečnost		§ 13 Aplikační bezpečnost	
§ 26 Kryptografické algoritmy		§ 14 Kryptografické algoritmy	
§ 27 Zajišťování dostupnosti regulované služby			
§ 28 Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv			

- ▼ § 19 Bezpečnost komunikačních sítí
 - FW a segmentace, VPN
- ▼ § 20 Správa a ověřování identit
 - PIM s MFA
- ▼ § 21 Řízení přístupových oprávnění
 - PAM
- ▼ § 22 Detekce kybernetických bezpečnostních událostí
 - FW s IPS, AV, Device Control, Application Control, HostIPS, Machine learning, EDR
- ▼ § 23 Zaznamenávání událostí
 - Log management
- ▼ § 24 Vyhodnocování kybernetických bezpečnostních událostí
 - SIEM s aktualizovanými nastaveními, pravidly a varováním
- ▼ § 25 Aplikační bezpečnost
 - Vulnerability Management



Firewalling a segmentace sítě

- ▼ Sophos XGS Firewall:
 - AntiMalware
 - AntiSpam
 - URL Filter
 - IPS/Application Detection
 - Web Application Firewall
 - Sandbox
- ▼ Orientované na uživatele a aplikace (z pohledu tvorby pravidel)
- ▼ Definice pravidla a návazných bezpečnostních modulů v jednom kroku
- ▼ Sdílení a provázání informací se Sophos Cloud (Security Heartbeat)
- ▼ Unikátní provázání Network & Endpoint Security

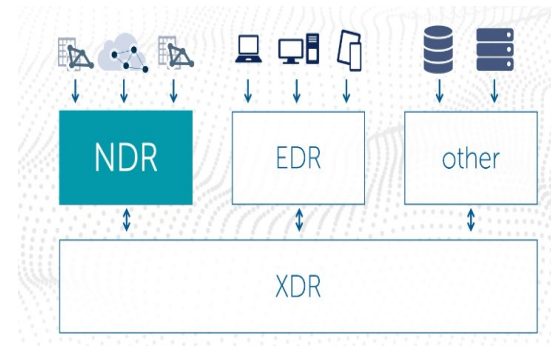


Klíčové vlastnosti Sophos InterceptX Advanced with XDR

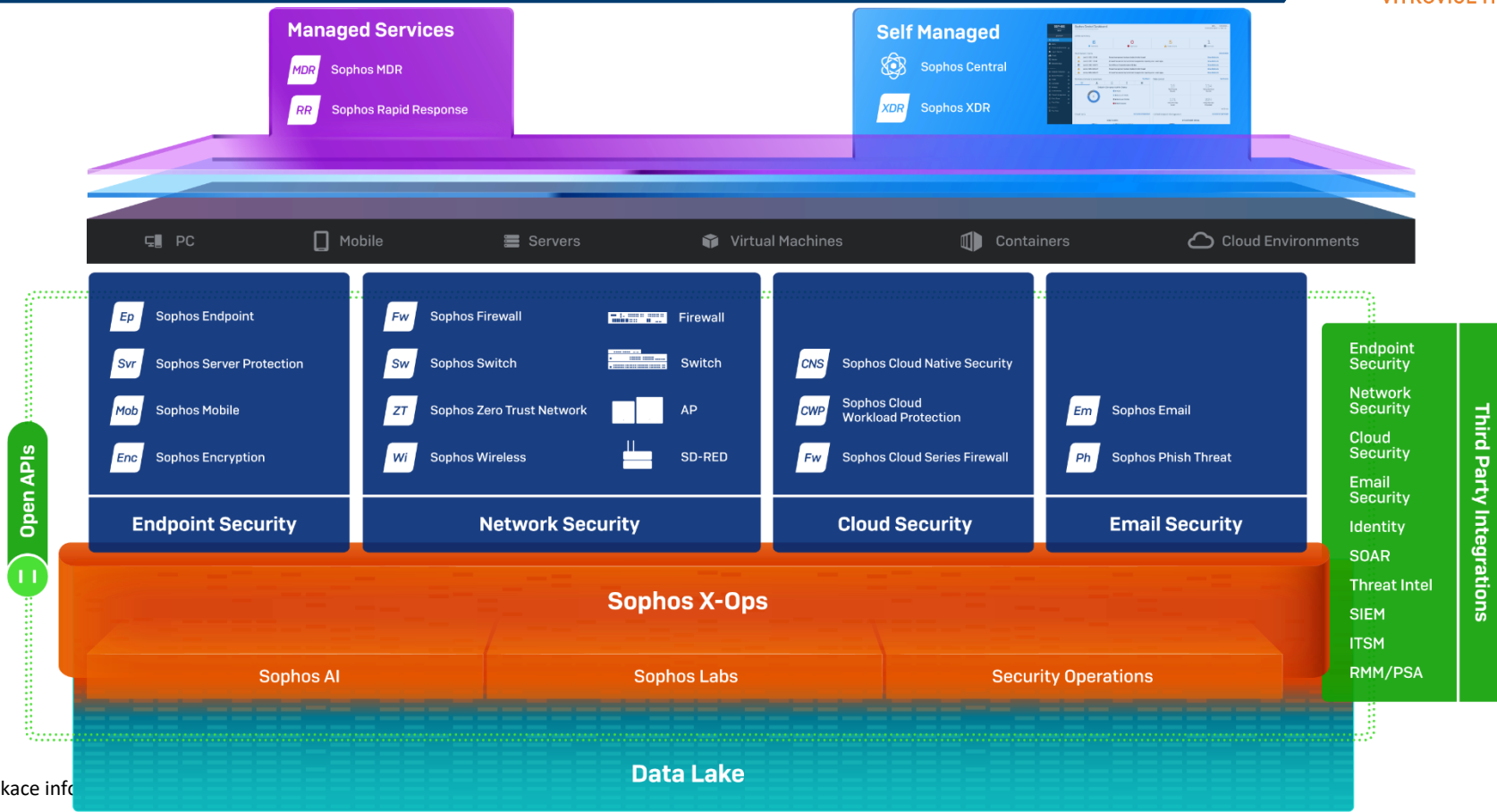
- ▼ Cryptoguard – dedikovaná ochrana proti zašifrování
- ▼ Deep learning poskytuje ochranu proti zero-day zranitelnostem bez nutnosti využívání sandboxu
- ▼ Anti-Exploit ochrana proti exploitačním technikám
- ▼ IPS + Malicious Traffic Detection včetně TLS/SSL inspekce
- ▼ Server lockdown

Extended Detection and Response (XDR)

- ▼ Jaký je rozdíl oproti EDR?
 - Umožňuje nahlížet na incident v širších souvislostech
 - Koreluje informace z velkého množství zdrojů dat
 - Mapování útoku na MITRE ATT&CK framework



Firewalling a segmentace síť



Ochrana dat (DLP a šifrování)

Trellix



Endpoints

Windows & Mac
Ochrana všech
komunikačních kanálů

Ochrana před
použitím
neautorizovaných
periferií



Device Control

Incident
Management



Classification
Engine



Discover

Discovery
Klasifikace
Náprava
Fingerprinting

ICAP integrace
Ochrana před
odesláním
citlivých souborů



Prevent - Web

ePolicy
Orchestrator

Policy
Management



Prevent - Email

SMTP
Ochrana citlivých dat
v emailovém provozu



Monitor

SPAN / TAP
Monitoring
veškerého
provozu

SSO vstupní brána

- ▼ Obstarání autentizace a poskytnutí přístupu k cílovým aktivům
 - ▼ Podpora MFA
- ▼ Spolupracuje se zabezpečeným úložištěm přihlašovacích údajů
- ▼ Umožňuje nastavení rozšířených přístupových pravidel
 - ▼ Časové rámce, schvalovací procesy

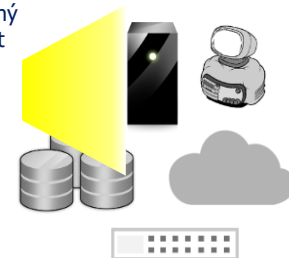
Monitoring uživatelských aktivit

- ▼ Sledování či sdílení relace
- ▼ Monitoring aktivit
- ▼ Detekce nežádoucího chování
- ▼ Podpora ICAP pro kontrolu souborů
 - ▼ DLP
 - ▼ Antimalware



RDP, SSH, VNC, TELNET,
RLOGIN, HTTP, HTTPS, Raw
TCP/IP

Dočasný
agent



Audit a dohledatelnost

- ▼ Pořízení nepozměnitelného záznamu a logování relací
- ▼ Obohacení nahrávky o metadata z relační sondy

Dvoufaktorová autentizace

- ▼ Britský výrobce zaměřený zejména na multifaktorovou autentizaci
- ▼ Uživatelský komfort - stávající zařízení uživatele (mobilní telefon, nositelná elektronika, ...) jako autentizační token
- ▼ Uživatelský portál pro správu tokenů (změna typu tokenu nebo přenos na jiné zařízení bez interakce IT oddělení)
- ▼ Integrace s jakoukoliv technologií podporující RADIUS protokol
- ▼ Licence pouze dle počtu uživatelů (licenční model již dále neřeší typ autentizačního tokenu a počet SecurEnvoy serverů)
- ▼ Možnost provozovat vlastní GSM brány



Dvoufaktorová autentizace

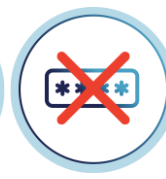
Široké možnosti autentizačních metod



Tablet AppPush



Push



Passwordless



Phone App



Biometrics



OTP Hardware
Token



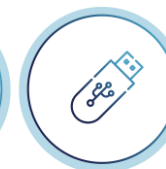
Email



Desktop App



SMS
Realtime



USB



- ▼ Zranitelné systémy jsou otevřenou branou do společnosti

Výčet nejznámějších za poslední dobu

- Útok NTLM Relay nazvaný PetitPotam
- Remote Code Execution ve VMware ESXi a vSphere Client
- Zero-Day zranitelnosti v Microsoft Exchange
- Zranitelnost "PrintNightmare" v Microsoft Windows Print Spooler
- Kritická zranitelnost v Apache Log4j s názvem Apache Log4Shell

- ▼ Kvalitní Vulnerability Management by měl zajišťovat

- Prioritizaci zranitelností (nespoléhat se jen na CVSS)
- Dávat nalezené zranitelnosti do souvislostí
- Workflow řešení zranitelností



Jednorázový sken zranitelností

Jednorázový

Chybějící vývoj ve společnosti

Cena



Vulnerability Management

Reakce na Zero-Day

Prioritizace assetů

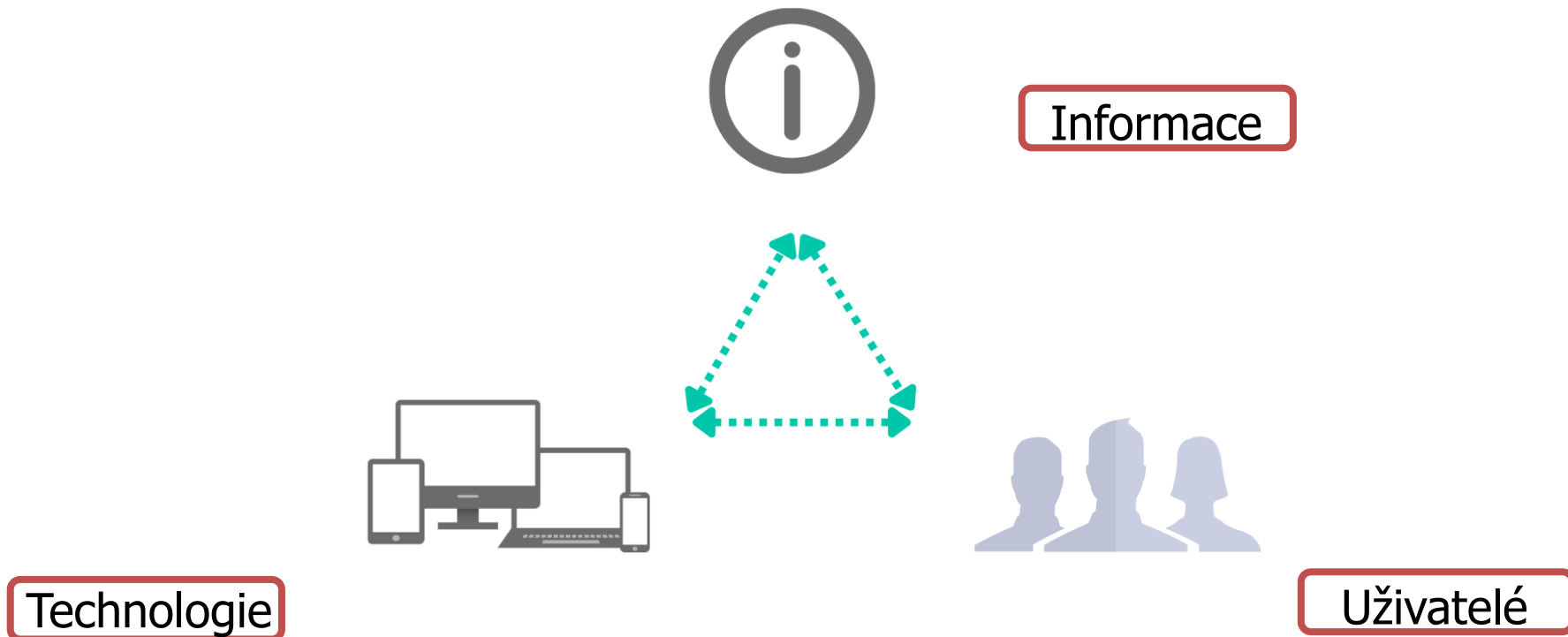
Řízení oprav

Neustálý přehled o trendech

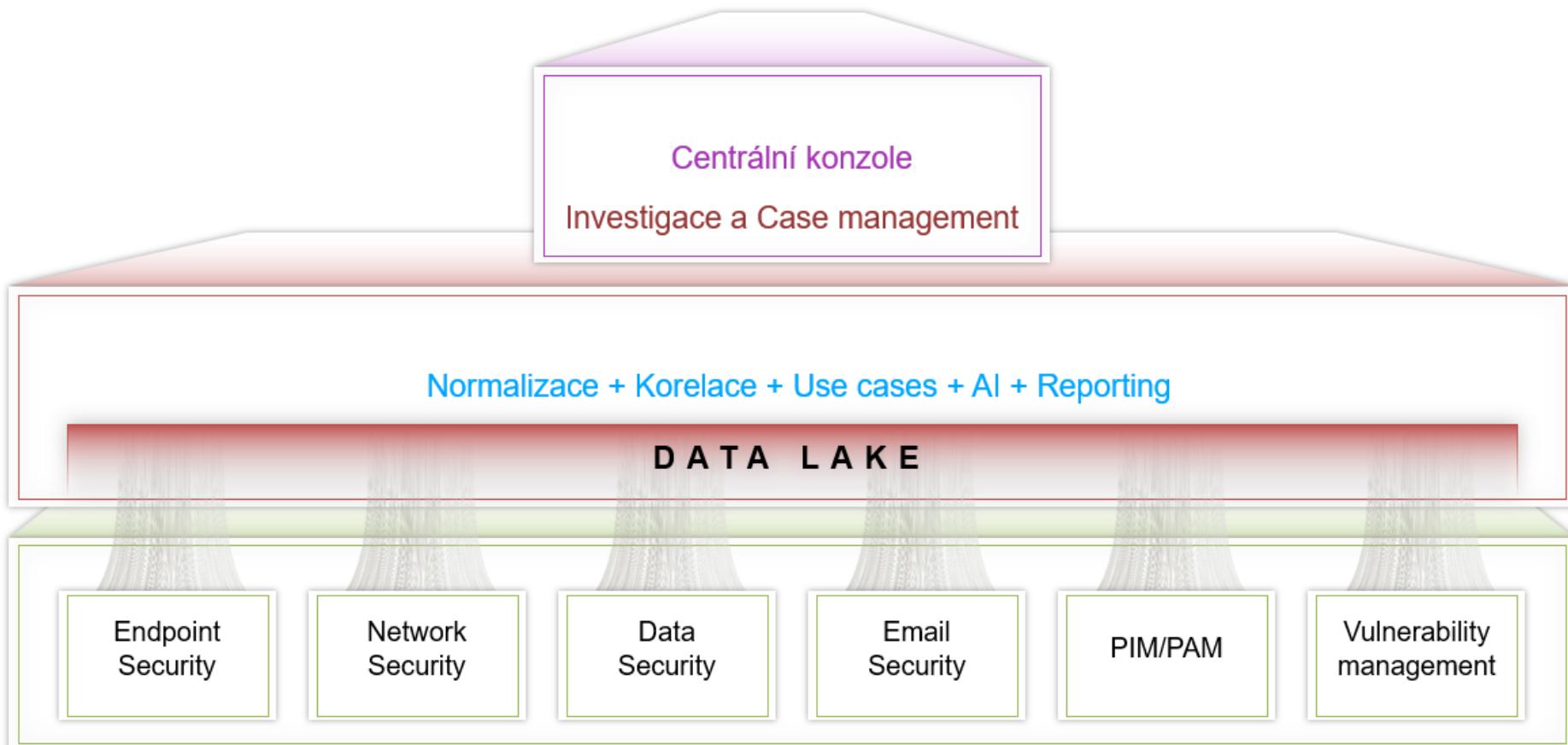
Pravidelné skeny

Cena

Stolička bezpečnosti



SIEM - Sběr a vyhodnocování událostí



ThreatGuard je zdroj informací!

- ▼ Stále dostupná, aktuální a strukturovaná databáze hrozeb a opatření
- ▼ Přehled kritických a nebezpečných hrozeb pro Vaše technologie, vč. rad a doporučení, jak se správně bránit

Tým vyhodnocuje informace z různých zdrojů:

- ▼ Webové stránky, databáze exploitů, sociální sítě
- ▼ Newsfeedy vendorů, CSIRT týmy, darkweb, aktuálně řešené incidenty v našem regionu

O jaké hrozby se jedná?

- zranitelnosti
- DDOS útoky
- malware
- ransomware
- phishing

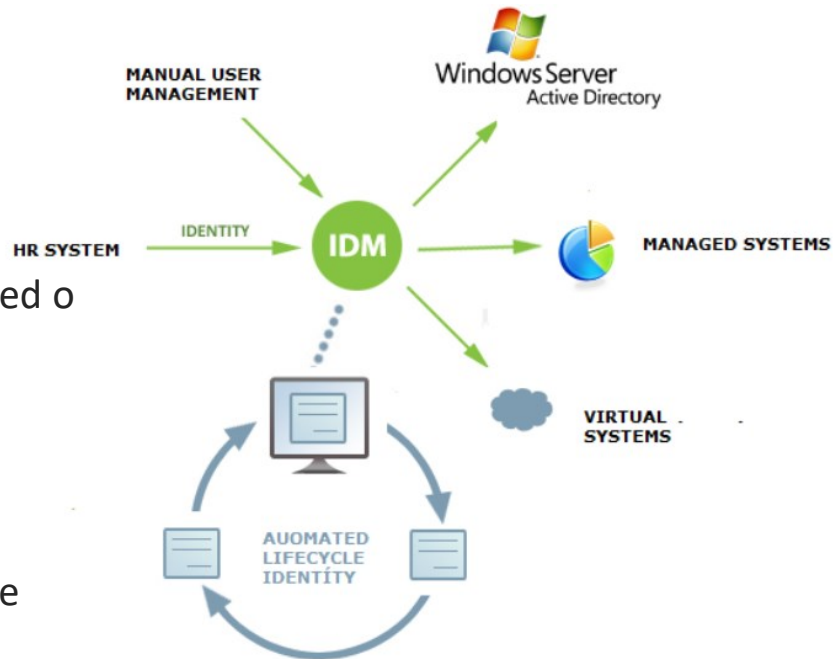
Virtuální bezpečnostní analytik =



ThreatGuard

Řízení identit IDM

- ▼ Automatizuje rutinní procesy správy identit
- ▼ Ulevuje administrátorům od rutinních procesů
- ▼ Centralizuje systémy pod jedinou správu – získáte přehled o přístupech v systémech
- ▼ Delegujte správu účtů na business vlastníky
- ▼ Eviduje, audituje operace nad účty a právy. Získáte rychle podklady pro auditu IT.
- ▼ Zvýší bezpečnost například zamezením existence mrtvých duší



Bezpečnostní portál - Dashboard

DASHBOARD

Hledej zde

Admin

Bezpečnostní portál v.1.1

Dashboard

Inventory

Bezpečnostní události

Virtualizace a uložště

Monitorování události

Protokol záloh

Antivirus

Výkonnost sítě

STRÁNKY

Logy

Reporty

Znalostní báze

Bezpečnostní testy

DOKUMENTY

Základní

Komponenty

Nápvěda

Poslední incidenty
115

Zobrazit více

ULOŽIŠTĚ
125 GB
+12% využito za poslední měsíc



LOGY
14 254
-36% využito za poslední měsíc



NAVÁZENÉ SESSIONS
2684
+29% využito za poslední měsíc



UDÁLOSTI
589
-16% využito za poslední měsíc



KATEGORIE

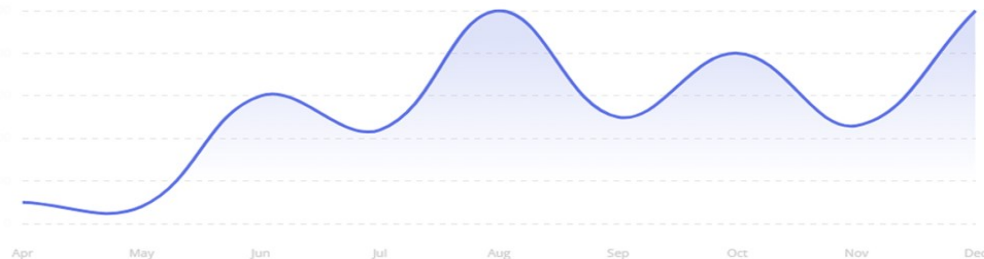
ZAŘÍZENÍ

SERVISNÍ UDÁLOSTI

VM STANIC

Vývoj události

+72% od roku 2022



LOGY
480

60%



PROJEKTY
115

- Hotovo
- V řešení





VÍTKOVICE

VÍTKOVICE IT SOLUTIONS

A network diagram with a central white circle containing the text 'Děkujeme za pozornost'. The diagram consists of a complex web of black lines connecting various icons: orange, purple, red, and blue circles with white person silhouettes, and blue circles with white person silhouettes. Some icons are enclosed in rounded rectangles with arrows, suggesting a flow or process. The background is a light gray gradient.

**Děkujeme
za
pozornost**