Nabídka služby bezpečnostního dohledu interní sítě Krajského úřadu Plzeňského kraje

Zákazník: Krajský úřad Plzeňského kraje

Dodavatel: GREYCORTEX s.r.o.

Datum: 3. srpen 2020

Autoři: [redacted]

Obsah

1. Identifikační údaje dodavatele

Obchodní jméno	**GreyCortex s.r.o.**
Právní forma	společnost s ručením omezeným
Rok založení	2016
Sídlo společnosti	Purkyňova 649/127, 61200 Brno, CR
Adresa kanceláří	[redacted]
Seznam statutárních zástupců	
Kontaktní údaje	
IČ	
DIČ	
Zápis v OR	
Bankovní spojení	
Číslo účtu	
Zástupce v tomto jednání	
Zástupce pro technický kontakt	

2. Vybrané reference

3. Specifikace nabízeného řešení

Nasazení řešení v rámci služby síťového dohledu vnitřní sítě bude tvořeno:

1x VA Kolektor p/n **MA-SC-1k-G2-VA: senzor + kolektor / 1000Mbps / 700 toků za sekundu /**

4. Popis nabízené služby

Navrhovaná služba na úrovni SILVER je tvořena dvěma oblastmi zajišťovanými dodavatelem:

Bezpečnostním dohledem

- Analýza komunikace v intervalu vždy jednoho měsíce s označením důležitých incidentů ve vztahu k interní bezpečnosti
- Vytváření bezpečnostních reportů identifikovaných nedostatků v interní síti zadavatele ve specifikovaných segmentech.
- Dostupnost bezpečnostního analytika v režimu 8x5 v době 9:00 – 17:00.

Zajištění správné konfigurace:

- Průběžná odborná konfigurace systému
- Průběžné ladění detekce
- Zajištění updatů a upgradů zařízení

5. Cenová kalkulace

Produktový kód	*Položka*	*Ceníková cena*	*Jednotka*	*#*	*Sleva*	*Koncová cena*
VA appliance + služby bezpečnostního dohledu						
Kolektor + sensor						
MA-SC-1k-G2-VA	**Pronájem na 12 měsíců SW licenci: senzor + kolektor / 1000Mbps / 700 toků za sekundu / 2xGE monitorovací porty**	61 000	Měsíc	12	55%	329 400 Kč
Služby bezpečnostního dohledu						
MSS-M-SILVER	**Prémiové bezpečnostní služby, úroveň SILVER** - Měsíční audity síťového provozu (zpráva o stavu sítě, bezpečnostních rizicích) - Podpora cyber security analityka (Po-Pá 9:00-17:00)	18 000	Měsíc	4	20%	57 600 Kč
MSS-IMPL	Implementace a zaškolení	15 000	Manday	1	15%	12 750 Kč
Celková cena pronájmu VA appliance a bezpečnostního dohledu (12 měsíců)						**399 750 Kč**

- *Cena je uvedena bez DPH*
- *Celková cena je splatná při objednání služeb, se splatností 30 dnů.*
- *Klient při objednání potvrzuje souhlas s veřejnou referencí pro dodavatele*

6. Popis produktu GreyCortex MENDEL

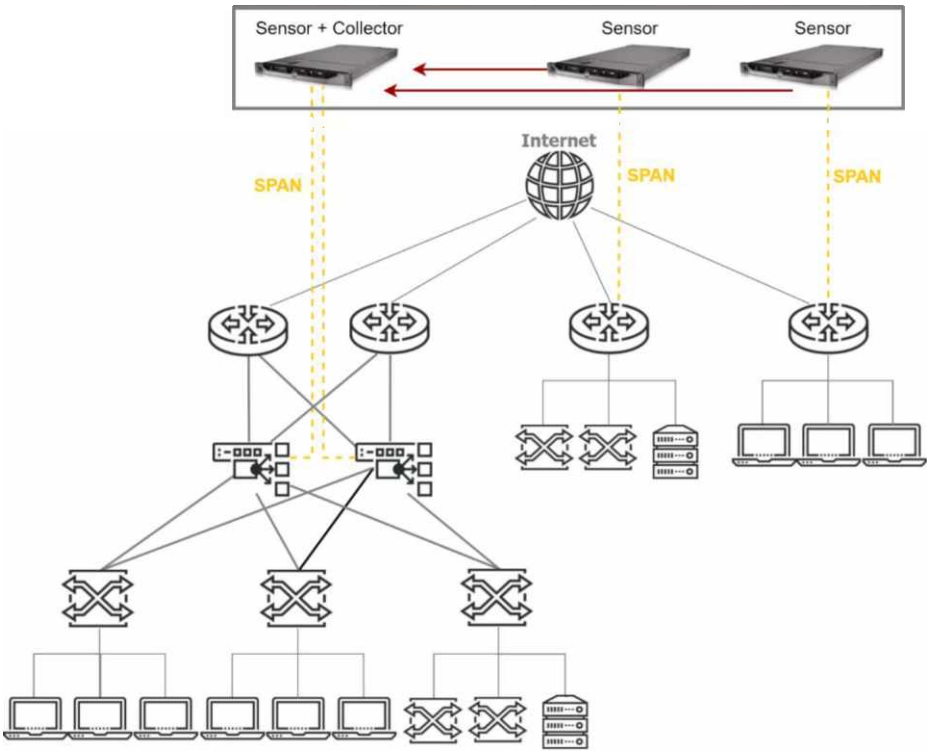
GREYCORTEX MENDEL je nástroj pro monitoring a analýzu síťového provozu, který identifikuje známé i neznámé kybernetické hrozby, provozní nedostatky a anomálie v chování síťové komunikace. Nástroj je určen k zajištění unikátní viditelnosti do interní infrastruktury včetně detailní viditelnosti do vybraných protokolů v rámci interní sítě.

Hlavní schopnosti

Nasazení GREYCORTEX Mendel zvyšuje bezpečnost a spolehlivost IT infrastruktury organizace, a to především v těchto oblastech (více v sekci Analýza síťového provozu):

- Detailní viditelnost do síťového provozu (jednotlivé komunikační vektory, přehled o zařízení, vytížení aplikací, atd)
- Detekce cílených a neznámých útoků pomocí pokročilých behaviorálních metod
- Detekce známého malware, virů, zranitelností a dalších známých útoků a hrozeb
- Ověření souladu s vybranými firemními politikami vč. GDPR a obecnými bezpečnostními zásadami
- Detekce anomálií ve výkonnosti sítě a aplikací
- Detekce špatných síťových konfigurací a porušení best practices

Zařízení analyzuje zrcadlený provoz ve vnitřní síti a detekuje bezpečnostní a provozní incidenty. Zařízení je pasivní a neovlivňuje síťový provoz a další síťovou infrastrukturu. Příprava prostředí pro jeho nasazení a vlastní nasazení je velmi jednoduché.



Obrázek 1: Schéma nasazení produktu

Popis řešení

Řešení je tvořeno hardwarovou nebo virtuální appliance umístěnou v prostředí uživatele (on-premis řešení), která dle konfigurace a nasazené licence slouží jako:

- **SÍŤOVÝ SENSOR** – sběr síťových dat, kompletní rekonstrukce provozu na aplikační úrovni, detekce výskytu známých hrozeb na základě detekčních signatur, dešifrování provozu a extrakce meta dat (síťových metrik) pro další analýzu. Všechny tyto informace jsou zasílány na kolektor v komprimované a šifrované podobě zamezující podvržení dat a jejich případnou modifikaci či zcizení.
  Sensor má volitelně jeden nebo více rozhraní typu 1GE nebo 10GE.

Výstupem sensoru jsou datové sady ASNM (Advanced Security Network Metrics) principiálně podobné protokolu NetFlow. ASNM jsou toky ukládány jako obousměrné (bi-direkcionální) a obsahují zhruba 10x více parametrů než běžné NetFlow. Jeden tok může být popsán až 900 parametry v závislosti na jeho typu a obsahu. Metriky předávané protokolem ASNM jsou rozděleny do šesti kategorií – výkonnostní, bezpečnostní, statistické, behaviorální, lokační a aplikační.
Sensor je neviditelné na L2 a L3 vrstvě (monitorovací porty nemají IP a je zcela pasivní.

- **KOLEKTOR** – kolektor provádí analýzu získaných dat na základě získaných informací ze zdrojů. Zdrojem jsou informace získané z:
    - **NetFlow / IPFIX zdroj** – kolektor dokáže analyzovat a vizualizovat data přímo z protokolu NetFlow a jemu příbuzných, Detekce je však výrazně ochuzená a omezená vůči pokročilým metrikám generovaných sensory GreyCortex ve formátu ASNM
    - **Síťový sensor GreyCortex**

  Na kolektoru jsou veškerá získaná data rovněž dlouhodobě ukládána dle potřeby uživatele, případně je možné je ukládat a zálohovat mimo appliance na libovolném datovém úložišti dostupném prostřednictvím síťového připojení.
  Na kolektor lze připojit dle potřeby různé množství sensorů nebo zdrojů NetFlow,
  Kolektor podporuje protokoly NetFlow v9 a IPFIX. Podporuje pro sběr a analýzy sFlow. Rovněž obsahuje plnou podpora pro IPv4, IPv6, VLAN.

- **ALL–IN–ONE** – zařízení skládající se ze síťového sensoru a kolektoru v rámci jedné HW nebo virtuální appliance.

- **CENTRÁLNÍ KONZOLE** – slouží pro vizualizaci dat v jedné konzoly získaných z více kolektorů nebo All-in-One appliance.

Schopnosti analýzy síťového provozu

Analýza síťového provozu je rozdělena mezi kolektor a sensor, níže jsou popsané jednotlivé detekční a vizualizační metody včetně jejich principu.

1. Detekce neznámých a cílených útoků a hrozeb	
Typy útoků a hrozeb	Metoda
Pokročilé neznámé útoky • útoky na uživatelské účty • komunikace s botnetem • úniky dat • obecně anomální chování uživatelů a zařízení	***Prediktivní analýza =*** detekce anomálií na základě změny automaticky naučeného chování na různých úrovních monitorované sítě. Jedná se o odchylky od normálu na úrovni sítě, podsítě, daného zařízení a aktivních služeb na daném zařízení.
Cílené hrozby • RAT - Remote Access Trojan • APT – Advanced Persistent Threat • AVT – Advanced Volatile Threat	***Detekce strojového chování =*** odlišení projevů malware od lidské legitimní komunikace prostřednictvím periodických vzorů chování

2. Detekce známých útoků a hrozeb	
Typy útoků a hrozeb	Metoda
Známé projevy škodlivého chování • skenování sítě a zařízení • enumerace dat • detekce hádání hesel • DoS a DDoS útoky apod.	Behaviorální detekce na úrovni toků za pomoci pravidel pro detekci očekávatelných projevů útoků.
Známé hrozby a dříve popsané útoky • malware pro běžná zařízení • malware pro mobilní zařízení • trojské koně • útoky na aplikační a DB servery	Detekce známých útoků na základě denně aktualizované *sady detekčních pravidel* (přes 40.000) a blacklistů (60.000 až 100.000 záznamů). Příklady detekčních kategorií:

• zranitelnosti na straně klientských aplikací (JAVA, Flash, MS Office, prohlížeče…) • aktuální hrozby – phishing, trojans, … • komunikace s blacklistovanými zařízeními (IP adresa, doména)	Attack Response, Botcc, Chat, Current Events, DNS, DOS, Exploit, File, FTP, Games, ICMP, IMAP, Malware, Mobile Malware, Netbios, POP3, P2P, Policy, RPC, SCADA, Scan, Shellcode, SQL, TELNET, TFTP, TLS-Events, TOR, Trojans, User Agents, VOIP, Web Client, Web Server, Worms.

3. Ověření s bezpečnostními zásadami a politikami	
Příklady nálezů	Ověřované politiky
Porušení vybraných politik pro ochranu dat GDPR • využívání dat nepovolenými osobami/způsoby • rizika úniku osobních údajů	Ověření souladu identifikovaných komunikací a komunikačních vektorů obsahujících osobní údaje s předem definovanými politikami pro ochranu dat.
Porušení komunikační politiky • Nedostupné služby a zařízení • Vznik nových nepovolených služeb a zařízení • Nepovolené komunikační vektory	Kontrola povolených a zakázaných služeb, prostupů a sítových politik – srovnání pozorované komunikační matice a uživatelem definovaných politik.
Porušení bezpečnostních politik • používání anonymizačních (Tor) a P2P sítí • hraní her a používání nepovolených aplikací • prověrka šifrovaná komunikace • nepovolené DNS servery • tunelovaný DNS provoz • používání zranitelných a zastaralých aplikací apod.	Zásady dobré praxe v síťové bezpečnosti

4. Výkonnost sítě a aplikací	
Příklady měřených veličin	Monitorovaná oblast
NPM – Network Performance Monitoring • objem a rychlost přenesených dat, síťových toků a paketů • počet komunikačních partnerů, aktivních hostů, ...	Výkonost sítě na úrovni celé sítě, jednotlivých podsítí, hostů a na nich běžících službách.
APM – Application Performance Monitoring • rychlost přenosu dat na síti • rychlost aplikační odezvy	Rychlost odezvy aplikací měřitelných na síti vč. automatické detekce anomálií

5. Vizualizace sítě a forenzní analýza	
Příklady využití	Monitorovaná oblast
Filtrování a zobrazení libovolných dat v reálném čase dle potřeb uživatele např.: • kdo s kým, kdy, jak komunikuje (komunikační partneři) • bezpečnostní incidenty vč. příslušných síťových toků a případně obsahu zachycených škodlivých paketů • využívané síťové služby vč. aplikačních metadat • komunikace uživatelem vybraných zařízení • výkonost aplikací a sítě apod.	Kompletní viditelnost na úrovni síťových toků: celá síť, podsítě, zařízení/hosti, služby (na všech síťových portech) vč. škodlivých payloadů Příklady parametrů pro filtrování: IP address, Host name , MAC address, Subnet , User name, Domain string, Service location, Traffic direction, Port, Protocol, Tunneled traffic, VLAN ID , Event, Event category, Incident status
Viditelnost proxy	Zobrazení cílových IP adres komunikace od zdrojových hostů na základě X-Forwarding-for
Rychlá analýza příčin a následků v reálném čase	Viditelnost do aplikačních metadat komunikačních protokolů

	Příklady protokolů: DNS, HTTP, HTTPS, TLS, MODBUS, SMB, SMB2, SSH, SSL, SMTP, FTP, DCERPC IRC, VNC, POP3, Oscar, SIP, MS-SQL DHCP
Jednoduché vyšetřování incidentů – bezpečnostních i provozních	Informace pro forenzní analýzu – bohatá metadata o síťovém provozu uchovávaná po požadovanou dobu (v řádu měsíců)
Záznam vybrané podezřelé komunikace pro analýzu	Volitelný záznam provozu (on-deman full packet capture) dle zařízení, komunikačního partnera, portu/služby, času atd.

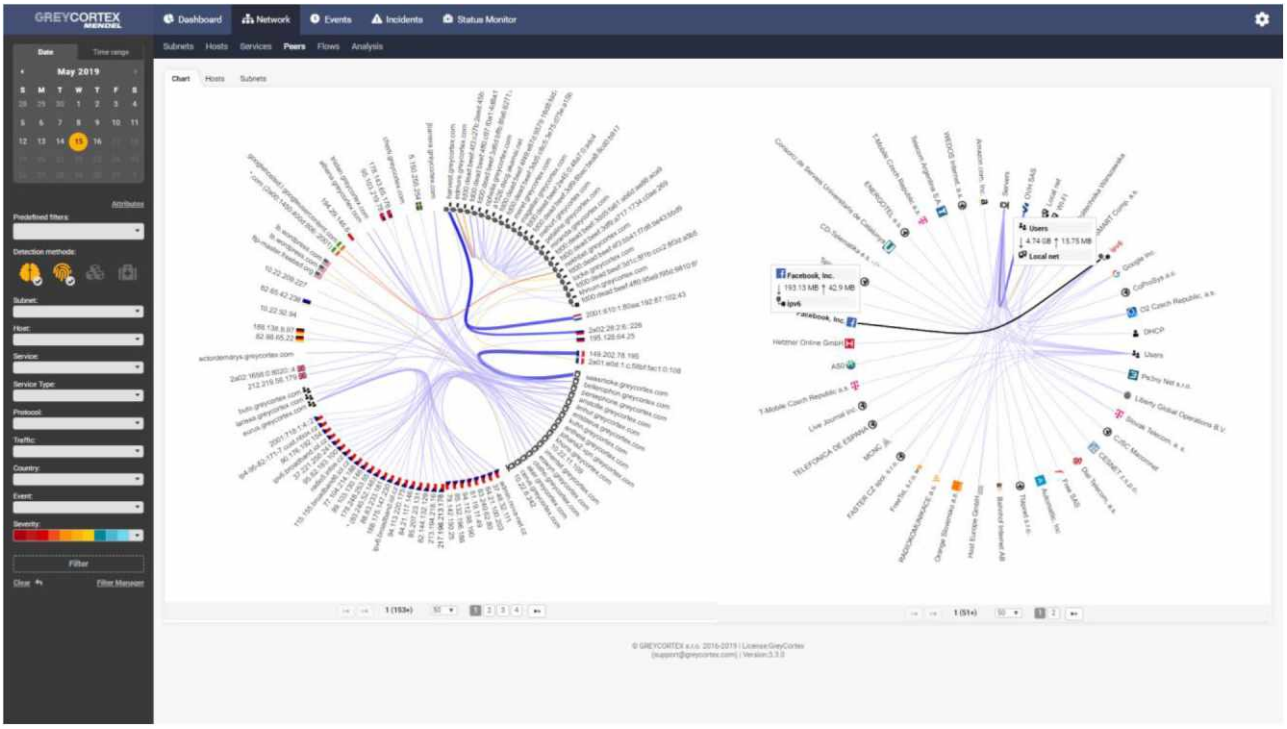
Doplňující vlastnosti analýzy a detekce

- Detailní sběr a zpracování statistik o síťovém provozu na úrovni celé sítě, jednotlivých podsítí, všech hostů v síti a služeb na každém hostu. To vše libovolně kombinovatelné, včetně směrů provozu a umístění služeb.
- Možnost sběru informací z NetFlow sond na základě uživatelské konfigurace.
- Schopnost detekce nežádoucích vzorů chování na síti (útoky, anomálie datového provozu, nežádoucí aplikace, detekce virů a botnetů ve vnitřní síti, detekce odchozího spamu, provozních problémů).
- Detekce anomálií vzhledem k dlouhodobému profilu chování zařízení na síti na základě dynamického modelování endpointů - metoda EDM.
- Předdefinovaná sada pravidel pro odhalování obecných anomálií v síti, včetně možnosti uživatelem definovaných pravidel.
- Vyhodnocování na základě implementace standardu Bidirectional flows (RFC 5103).
- Okamžitá integrace informací ze služeb DNS, DHCP, DC, Threat Intelligence, WHOIS a geo lokační služby.

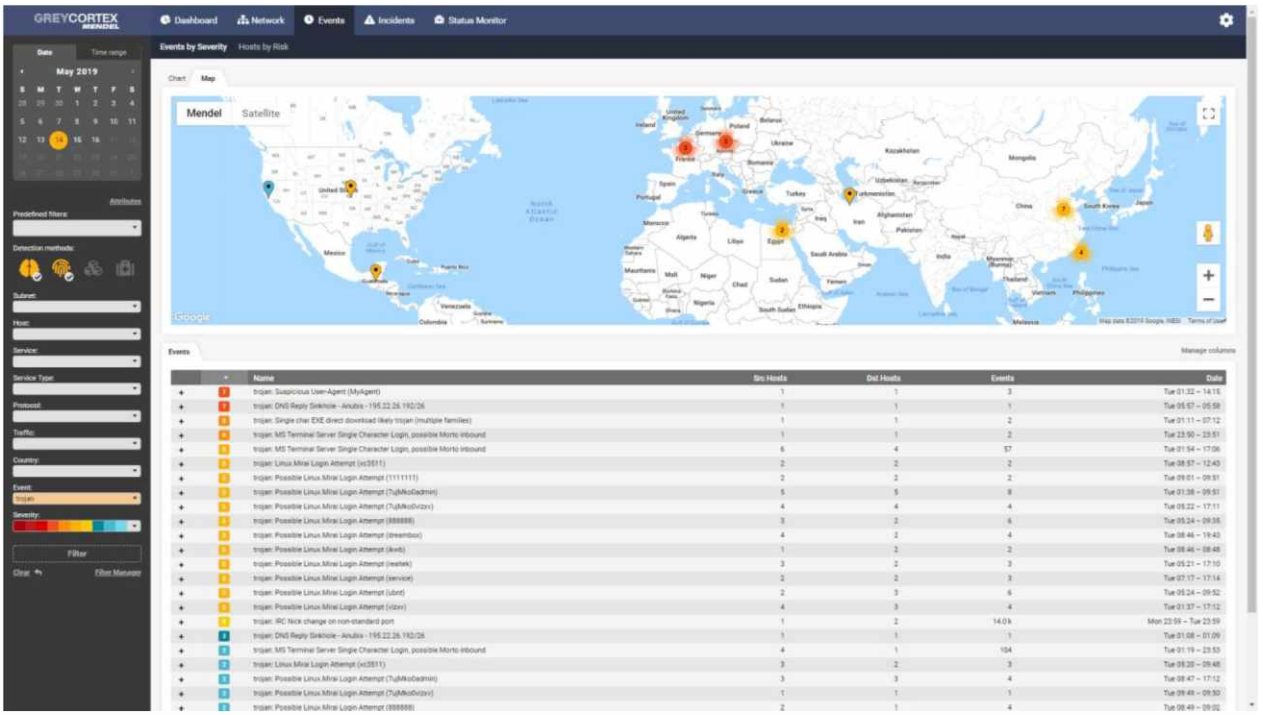
Uživatelský přístup a výstupy nástroje

Aplikace obsahuje webové grafické uživatelské rozhraní, které je dostupné prostřednictvím všech běžných internetových prohlížečů.

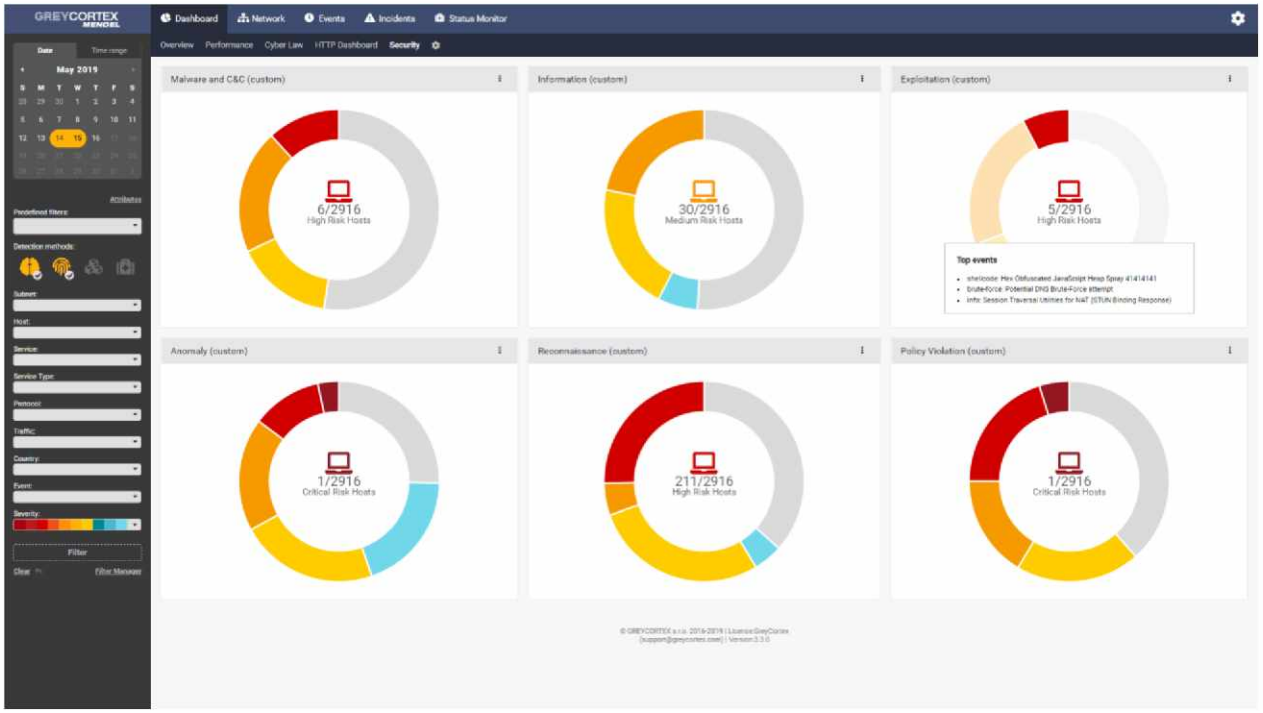
Obrázek 2: GUI s uživatelskými dashboardy



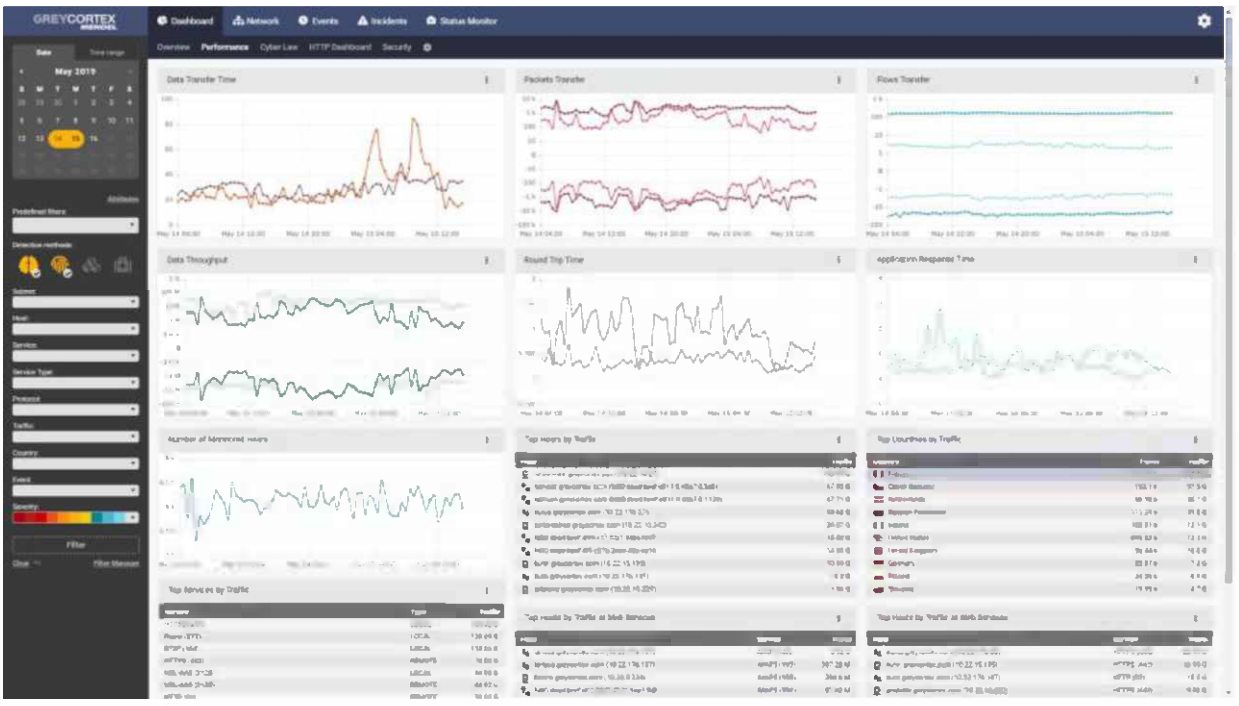
Obrázek 3: Graf komunikační partnerů (Peers graf)



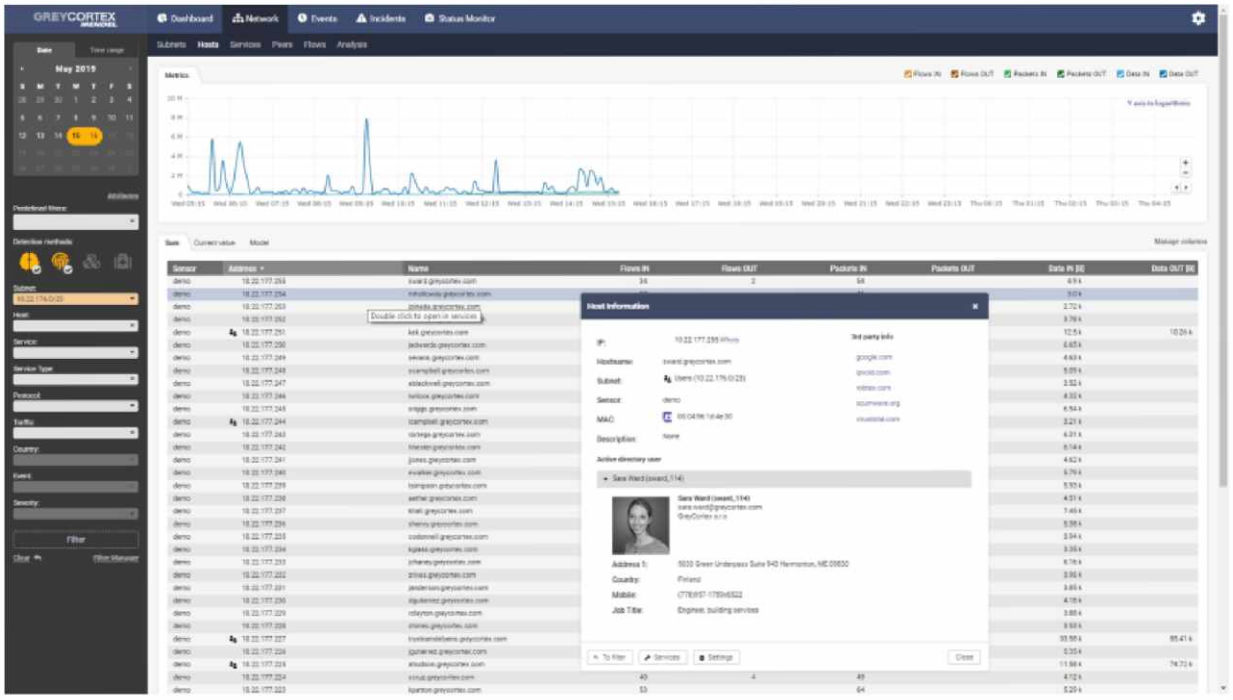
Obrázek 4: Příklad vizualizace bezpečnostních událostí na mapě



Obrázek 5: Uživatelské dashboardy



Obrázek 6: Uživatelské dashboardy



Obrázek 7: Přehled zařízení s aktivními uživateli

Obrázek 8: Ukázka automaticky generovaných reportů

Webové rozhraní aplikace se skládá z:

Datových filtrů – prostřednictvím filtru lze vytvářet libovolné pohledy na potřebná data. Filtr je uživatelský nastavený a funguje v reálném čase. Lze s ním ovládat veškerá grafická a tabulková zobrazení v aplikaci.

Uživatelských dashboardů – každý uživatel může vytvářet vlastní uživatelsky definované dashboardy. Existuje několik desítek typů dashboardů, které slouží pro vizualizaci různých typů dat a pohledů na ně. Na každý dashboard je možné aplikovat libovolný filtr.

Vizualizace sítě – modul umožňující realizovat libovolné pohled do sítě a vizualizaci sítových dat na úrovni celé sítě, jednotlivých podsítí, jednotlivých hostů a jejich služeb, vizualizace komunikačních partnerů, vizualizace sítových toků a analytický modul pro libovolnou grafickou vizualizaci uživatelem vybraných dat.

Vizualizace bezpečnostní události – slouží pro informaci o detekovaných událostech, popis hostu, podsítí, služeb a uživatelů, kterých se incident týká. Detailu jednotlivých událostí – zachycená data ze sítě, nebo

konkrétní statistiky na základě byla daná událost detekována. Poslední úrovní vizualizace je výčet síťových toků, které stály za vznikem událostí. Součástí každé události je plná intepretace detekční příčiny

Management bezpečnostních incidentů – procesní management identifikovaných bezpečnostních incidentů. Umožňuje řídit stav incidentů mezi stavy reportováno, řešeno, vyřešeno, nevyřešeno, včetně možnosti přiřazovat řešitele a sdílet odkazy incidentu.

Konfigurace a management aplikace

Uživatelský přístup, reporting, alerting

Uživatelský přístup lze řídit prostřednictvím uživatelských politik definovaných ve webovém rozhraní aplikace. Politiky vycházejících z přímé definice práv uživatele, nebo na základě informací z doménového kontroléru.

Data zobrazovaná jednotlivým uživatelům lze omezit na základe definovaných politik. Politikami lze omezit přístup uživatele k datům z definovaných:

- Detekčních modulů
- Podsítí
- IP adres
- MAC adres
- Uživatel (Identit doménového kontroléru)

Každý uživatel může plně definovat své uživatelské prostředí. Jedná se především o definici dashboardů, barvy rozhraní a jazyka.

Aplikace umožňuje vytvářet:

- uživatelsky definované reporty a grafů ve formátu PDF,
- dlouhodobé grafy a přehledy s různými typy pohledů rozdělených do kategorií podle objemu (počet přenesených bytů, toků, paketů), IP provozu (TCP, UDP, ICMP, ostatní) nebo protokolu (HTTP, IMAP, SSH), aplikačních protokolů.
- Generování statistik a podrobných výpisů nad volitelnými časovými intervaly.
- Alerty na základě uživatelem nastavených filtrů a pravidel.
- Uživatelsky filtrované logy nebo emaily v různých formátech zasílané na uživatelem definované prostředí.