

668/2020



Ev. č. Objednatele: 52020/73

## Smlouva o poskytování služeb

### Smluvní strany:

#### **ANECT a.s.**

se sídlem: Vídeňská 204/125, Přízřenice, 619 00 Brno

zastoupena: Pavlem Srnkou, členem představenstva

IČO: 25313029

DIČ: CZ25313029

bankovní spojení: [redacted]

číslo bankovního účtu: [redacted]

kontaktní osoba: Ing. Petr Polášek

tel., email: [redacted]

dále jen „**Poskytovatel**“

a

#### **Česká republika – Kancelář Poslanecké sněmovny**

se sídlem: Sněmovní 176/4, 128 26 Praha 1 – Malá Strana

zastoupena: Mgr. Janem Morávkem, vedoucím Kanceláře Poslanecké sněmovny

osoba oprávněna jednat ve věcech smluvních: Ing. Mgr. Naďa Formanová, ředitelka

odboru hospodářské správy, na základě pověření vedoucího zaměstnance k jednání

jménem státu ze dne 1. 7. 2017

IČO: 00006572

DIČ: CZ00006572

bankovní spojení: [redacted]

datová schránka ID: bykaigw

kontaktní osoba: Ing. Monika Pravcová, ředitelka odboru informatiky

tel., email: [redacted]

dále jen „**Objednatel**“

(Poskytovatel a Objednatel dále též společně jako „Smluvní strany“ a každý jednotlivě jako „Smluvní strana“)



Smluvní strany ujednávají následující:

## **Článek I.**

### **Předmět smlouvy**

- 1.1 Předmětem této smlouvy je závazek Poskytovatele poskytnout Objednateli služby spojené s provozem vnitřní sondy typu IDS v síti Objednatele a závazek Objednatele zaplatit Poskytovateli za řádně poskytnuté služby sjednanou cenu. Bližší specifikace předmětu plnění je uvedena v příloze č. 1 smlouvy – Technická specifikace a Příloze č. 3 – Popis plnění.
- 1.2 Závazek Poskytovatele spočívá zejména v poskytnutí a implementaci vnitřní sondy včetně potřebných SW licencí, zaškolení administrátorů, zajištění služeb HW i SW produktové podpory a zajištění správy a provozu síťové sondy včetně pravidelných reportů.
- 1.3 Poskytovatel se dále zavazuje zajistit po celou dobu realizace předmětu plnění vzdálenou podporu v režimu 24x7 e-mailovou a telefonní hot-line v českém jazyce. Pro tyto účely uvádí Poskytovatel následující kontakty pro hot-line:
  - 1.3.1 [REDACTED]
  - 1.3.2 [REDACTED]
- 1.4 Poskytovatel se zavazuje poskytovat služby správy a provozu síťové sondy. Poskytovatel má právo odmítnout poskytnutí služeb, které by znamenalo překročení sjednaného rozsahu. Poskytnutí služby nad rámec sjednaného rozsahu nezakládá právo na vyšší úplatu.
- 1.5 Poskytovatel se zavazuje poskytovat služby způsobem, v rozsahu, kvalitě a termínech uvedených v této smlouvě včetně všech příloh a v jeho nabídce podané v rámci zadávacího řízení podlimitní veřejné zakázky s názvem „Vnitřní sonda“.

## **Článek II.**

### **Místo plnění**

- 2.1 Místem plnění předmětu smlouvy je sídlo Objednatele, služby podpory budou poskytovány vzdáleně.

## **Článek III.**

### **Termín plnění**

- 3.1 Poskytovatel se zavazuje zahájit plnění předmětu této smlouvy do dvou měsíců od uzavření smlouvy.

## **Článek IV.**

### **Smluvní cena a platební podmínky**

- 4.1 Smluvní strany se dohodly na ceně za řádně poskytnuté služby ve výši 47 000,00 Kč bez DPH/měsíc, DPH 9 870,00 Kč, tj. 56 870,00 Kč včetně DPH.



- 4.2 Měsíční sazba uvedená v odst. 4.1 smlouvy je konečná a nepřekročitelná a zahrnuje veškeré náklady vynaložené v souvislosti s plněním předmětu této veřejné zakázky.
- 4.3 K uvedené ceně bez DPH bude připočtena DPH v příslušné zákonné sazbě platné ke dni zdanitelného plnění.
- 4.4 Maximální výše plnění za celou dobu realizace této smlouvy (tj. 48 měsíců) nesmí přesáhnout částku 2 256 000,00 Kč bez DPH, DPH 473 760,00 Kč, tj. částku 2 729 760,00 Kč včetně DPH.
- 4.5 Platba za řádně poskytnuté služby bude prováděna měsíčně zpětně na základě faktury vystavené Poskytovatelem. Poskytovatel je povinen vystavit a doručit fakturu nejpozději do 15. dne měsíce následujícího po měsíci, v němž byly služby poskytnuty.
- 4.6 Faktura vystavená Poskytovatelem musí splňovat náležitosti daňového dokladu stanovené právními předpisy.
- 4.7 Fakturované částky budou hrazeny bezhotovostně, a to bankovním převodem na účet Poskytovatele uvedený v této smlouvě, nebo na účet Poskytovatele dodatečně písemně oznámený Objednateli, a to nejpozději ke dni doručení faktury.
- 4.8 Splatnost faktury je 30 kalendářních dnů ode dne doručení řádně vystavené faktury Objednateli. V případě, že faktura nebude obsahovat náležitosti daňového dokladu nebo nebude vystavena v souladu s podmínkami sjednanými v této smlouvě, je Objednatel oprávněn vrátit ji Poskytovateli k doplnění. V takovém případě se přeruší plynutí lhůty splatnosti a nová lhůta splatnosti začne plynout doručením opravené faktury Objednateli.
- 4.9 Objednatel umožňuje doručení faktury v písemné i elektronické podobě. Elektronická faktura musí být zaslána na [REDACTED]
- 4.10 Faktura se považuje za zaplacenou dnem, kdy bude fakturovaná částka odeslána z účtu Objednatele ve prospěch účtu Poskytovatele.
- 4.11 Poskytovatel prohlašuje a svým podpisem v závěru smlouvy potvrzuje, že ke dni uzavření smlouvy není veden v rejstříku nespolehlivých plátců DPH, a pro případ, že se stane nespolehlivým plátcem DPH až po uzavření této smlouvy, zavazuje se bezodkladně a prokazatelně po vydání rozhodnutí správce daně podle §106a zákona o DPH, informovat Objednatele o této skutečnosti.
- 4.12 Pokud Objednatel jako příjemce zdanitelného plnění zjistí po doručení daňového dokladu (faktury), že Poskytovatel je v evidenci plátců DPH označen jako nespolehlivý plátcem DPH, anebo bankovní účet, který Poskytovatel uvede na daňovém dokladu (faktuře), není zveřejněn v registru plátců DPH, je Objednatel oprávněn uhradit Poskytovatel pouze tu část peněžitého závazku vyplývajícího z daňového dokladu, jež odpovídá výši základu daně, a zbylou část pak ve smyslu §109a zákona o DPH uhradit přímo správci daně. V případě uplatnění výše uvedeného postupu zaniká nárok Poskytovatele, který je na seznamu nespolehlivých plátců DPH, na zaplacení částky odpovídající výši DPH.



## **Článek V.**

### **Další podmínky plnění předmětu smlouvy**

- 5.1 Poskytovatel je povinen poskytovat služby sjednané v této smlouvě řádně, včas, s odbornou péčí, podle svých nejlepších znalostí a schopností a v souladu s obecně závaznými právními předpisy, přičemž je povinen sledovat a chránit oprávněné zájmy Objednatele.
- 5.2 Poskytovatel postupuje při poskytování služeb samostatně, je však povinen dbát pokynů Objednatele, pokud Objednatel pokyny uděluje.
- 5.3 Poskytovatel je povinen upozornit Objednatele na zřejmě nesprávný pokyn, a to bez zbytečného odkladu, a s jeho plněním vyčkat až do doby, než Objednatel potvrdí Poskytovateli, že na splnění pokynu přesto trvá.
- 5.4 V případě prodlení Objednatele se zaplacením jakéhokoliv finančního plnění Poskytovateli podle této smlouvy nemá Poskytovatel právo přerušit poskytování služeb.
- 5.5 Poskytovatel nemá právo přenechat poskytování služeb poddodavatelům, s výjimkou poddodavatelů uvedených v nabídce Poskytovatele.
- 5.6 V případě, že Poskytovatel bude pro řádné poskytování služeb potřebovat informace od Objednatele, má Objednatel povinnost poskytnout Poskytovateli součinnost, zejména mu sdělit veškeré požadované informace, a to bez zbytečného odkladu.
- 5.7 Objednatel se zavazuje zajistit Poskytovateli veškeré podmínky nezbytné pro řádné poskytování služeb, zejména zajistit či poskytnout všechny potřebné přístupy.
- 5.8 Poskytovatel se zavazuje předat Objednateli veškeré informace o změnách v realizačním týmu. Dále se zavazuje evidovat všechny jím provedené změny v konfiguraci formou provozního deníku nebo komentářů k jednotlivým konfiguračním dokumentům.

## **Článek VI.**

### **Autorská práva**

- 6.1 Součástí poskytovaných služeb jsou SW licence včetně produktové podpory na dobu poskytování služeb.
- 6.2 Součástí plnění podle této smlouvy není vývoj aplikací ani SW. Podpůrné aplikace a skripty budou řešeny ad hoc.
- 6.3 Objednatel nemá právo udělit třetím osobám podlicence.
- 6.4 Poskytovatel nemá právo na jakoukoli dodatečnou odměnu v souvislosti s autorskými právy souvisejícími s poskytováním služeb.



## **Článek VII. Komunikace**

- 7.1 Poskytovatel a Objednatel budou komunikovat zejména prostřednictvím kontaktních osob uvedených definici Smluvních stran, preferovaným způsobem komunikace je komunikace elektronická.
- 7.2 Změna kontaktních osob je možná jen na základě předchozího písemného upozornění.

## **Článek VIII. Odpovědnost za škodu**

- 8.1 Poskytovatel plně odpovídá za škodu způsobenou Objednateli Poskytovatelem jakýmkoli porušením povinností Poskytovatele uvedených v této smlouvě a jejich přílohách.
- 8.2 Poskytovatel je povinen mít po celou dobu trvání smlouvy uzavřené platné pojištění odpovědnosti za škodu způsobenou třetí osobě s pojistným limitem minimálně 5 000 000,- Kč. V případě, že pojistný vztah mezi Poskytovatelem a pojistitelem skončí, je Poskytovatel povinen sjednat nový pojistný vztah ve stejném rozsahu tak, aby byla zachována podmínka existence pojištění v předmětném rozsahu po celou dobu trvání tohoto smluvního vztahu. Existenci pojištění je poskytovatel povinen na žádost Objednatele kdykoliv prokázat.

## **Článek IX. Důvěrnost**

- 9.1 Poskytovatel je vázán Dohodou o mlčenlivosti, která tvoří přílohu č. 2 této smlouvy.
- 9.2 Poskytovatel není oprávněn užívat data uživatelů ani aplikací, s výjimkou auditních záznamů, konfigurací a nastavení potřebných pro řešení PMR. Data mohou být vydána jen se souhlasem manažera kybernetické bezpečnosti.
- 9.3 Mezi důvěrné informace nepatří žádné informace, které jsou v době jejich zpřístupnění nebo použití běžně dostupné veřejnosti.
- 9.4 Objednatel dává souhlas Poskytovateli, aby jej Poskytovatel uváděl jako svého zákazníka.

## **Článek X. Smluvní pokuta**

- 10.1 V případě porušení povinností ohledně mlčenlivosti a důvěrnosti informací (dle čl. IX. A přílohy č. 2 této smlouvy), se Poskytovatel zavazuje uhradit Objednateli smluvní pokutu ve výši 50.000, - Kč za každé jednotlivé porušení povinnosti.
- 10.2 V případě, že Poskytovatel nedodrží podmínky SLA (zejména reakční doba a lhůta pro opravu) stanovené v Příloze č. 1 této smlouvy, zavazuje se uhradit Objednateli smluvní pokutu ve výši 1.000, - Kč za každou započatou hodinu prodlení.



- 10.3 V případě prodlení Objednatele s úhradou řádně vystavené faktury, je Poskytovatel oprávněn účtovat Objednateli úrok z prodlení v zákonné výši z fakturované částky za každý započatý den prodlení.
- 10.4 Smluvní pokuta a úrok z prodlení jsou splatné do 15 kalendářních dnů ode dne doručení jejich vyúčtování.
- 10.5 Zaplacením smluvní pokuty není dotčeno právo oprávněné strany na náhradu škody vzniklé v příčinné souvislosti s porušením smluvní povinnosti, za jejíž nedodržení je smluvní pokuta vymáhána a účtována.
- 10.6 Objednatel je oprávněn jednostranně započíst splatné smluvní pokuty vzniklé Poskytovateli vůči splatné úhradě za poskytování služeb dle této smlouvy.

## **Článek XI. Platnost smlouvy**

- 11.1 Tato smlouva nabývá platnosti dnem podpisu oprávněnými zástupci obou Smluvních stran.
- 11.2 Tato smlouva se uzavírá na dobu 48 měsíců ode zahájení poskytování služeb dle této smlouvy.
- 11.3 Obě Smluvní strany jsou oprávněny ukončit tuto smlouvu písemnou výpovědí i bez udání důvodů. Výpovědní doba činí jeden (1) měsíc a počíná běžet prvním dnem měsíce následujícího po měsíci, v němž došlo k doručení výpovědi druhé Smluvní straně.
- 11.4 Objednatel si vyhrazuje právo odstoupit od smlouvy také v případě opakovaného nedodržení SLA.

## **Článek XII. Ostatní ujednání**

- 12.1 Objednatel si vyhrazuje právo na provedení auditu kybernetické bezpečnosti u Poskytovatele. Tento audit lze nahradit poskytnutím výroční auditní zprávy v souladu s ČSN EN ISO/IEC 2700X.
- 12.2 Všichni jednotliví poddodavatelé se zavazují dodržovat v plném rozsahu ujednání mezi povinnou osobou a Poskytovatelem a nebudou v rozporu s požadavky povinné osoby (dle Dohody o mlčenlivosti). Součástí této povinnosti je podpis Dohody o mlčenlivosti poddodavatelem.
- 12.3 Poskytovatel se zavazuje dodržovat veškerá pravidla vyplývající z obecné bezpečnostní politiky a systémové bezpečnostní politiky, případně její odsouhlasení po jejím zpracování.
- 12.4 Poskytovatel se zavazuje informovat Národní úřad kybernetické a informační bezpečnosti a Objednatele o kybernetických bezpečnostních incidentech souvisejících s poskytováním služeb podle této smlouvy.



- 12.5 Poskytovatel se dále zavazuje informovat Objednatele o způsobu řízení rizik na straně Poskytovatele a o zbytkových rizicích souvisejících s plněním smlouvy.
- 12.6 Poskytovatel se zavazuje informovat Objednatele a Národní úřad kybernetické a informační bezpečnosti o významné změně ovládnutí Poskytovatele podle zákona o obchodních korporacích nebo o změně vlastnictví základních aktiv, změně oprávnění nakládat s těmito aktivy, využívanými Poskytovatelem k plnění této smlouvy.
- 12.7 Objednatel si vyhrazuje právo v případě havárie nebo kybernetického bezpečnostního incidentu požádat Poskytovatele o zajištění účasti jeho zaměstnanců do ISIRT týmu Objednatele. Poskytovatel se zavazuje poskytnout Objednateli matici kontaktních údajů zaměstnanců Poskytovatele, kteří mohou být zařazeni do ISIRT týmu, včetně jejich odborného zaměření.
- 12.8 Poskytovatel bere na vědomí, že podle ustanovení § 3 odst. 2 písm. f) zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), nebude tato smlouva uveřejněna v registru smluv.

### **Článek XIII.**

#### **Vyšší moc**

- 13.1 Smluvní strany se zprošťují veškeré odpovědnosti za nesplnění svých povinností z této Smlouvy po dobu trvání vyšší moci do té míry, pokud po nich nebylo možné požadovat, aby neplnění svých povinností z této smlouvy v důsledku vyšší moci předešly.
- 13.2 Za vyšší moc je pro účely této Smlouvy považována každá událost nezávislá na vůli Smluvních stran, která znemožňuje plnění smluvních závazků a kterou nebylo možno předvídat v době vzniku této Smlouvy. Za vyšší moc se z hlediska této Smlouvy považuje zejména přírodní katastrofa, požár, výbuch, silná vichřice, zemětřesení, záplavy, válka, stávková akce nebo jiné události, které jsou mimo jakoukoliv kontrolu Smluvních stran.
- 13.3 Po dobu trvání vyšší moci se plnění závazků podle této smlouvy pozastavuje do doby odstranění následků vyšší moci.

### **Článek XIV.**

#### **Závěrečná ustanovení**

- 14.1 Tato smlouva, jakož i práva a povinnosti vzniklé na základě této smlouvy nebo v souvislosti s ní se řídí právním řádem České republiky, zejména zák. č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.
- 14.2 Nevymahatelnost či neplatnost kteréhokoliv ustanovení této smlouvy nemá vliv na vymahatelnost či platnost zbývajících ustanovení této smlouvy, pokud z povahy nebo obsahu takového ustanovení nevyplývá, že nemůže být odděleno od ostatního obsahu této smlouvy.



14.3 Tato smlouva představuje úplné ujednání Smluvních stran ve vztahu k předmětu této smlouvy.

14.4 Tato smlouva může být měněna jen vzestupně číslovanými Dodatky.

14.5 Nedílnou součástí smlouvy tvoří tyto přílohy:

**Příloha č. 1** – Technická specifikace

**Příloha č. 2** – Dohoda o mlčenlivosti

**Příloha č. 3** – Popis plnění

14.6 Tato smlouva je uzavřena v pěti (5) vyhotoveních, z nichž Objednatel obdrží tři (3) vyhotovení a Poskytovatel dvě (2) vyhotovení.

14.7 Smluvní strany si smlouvu přečetly, souhlasí s jejím obsahem a prohlašují, že je ujednána svobodně.

V Praze dne (uvedeno v elektronickém podpisu)

28-05-2020

25.5.2020  
V Praze dne (uvedeno v elektronickém podpisu)

Ing. Mgr. Naďa Formanová,  
ředitelka odboru hospodářské správy

Pavel Srnka  
člen představenstva

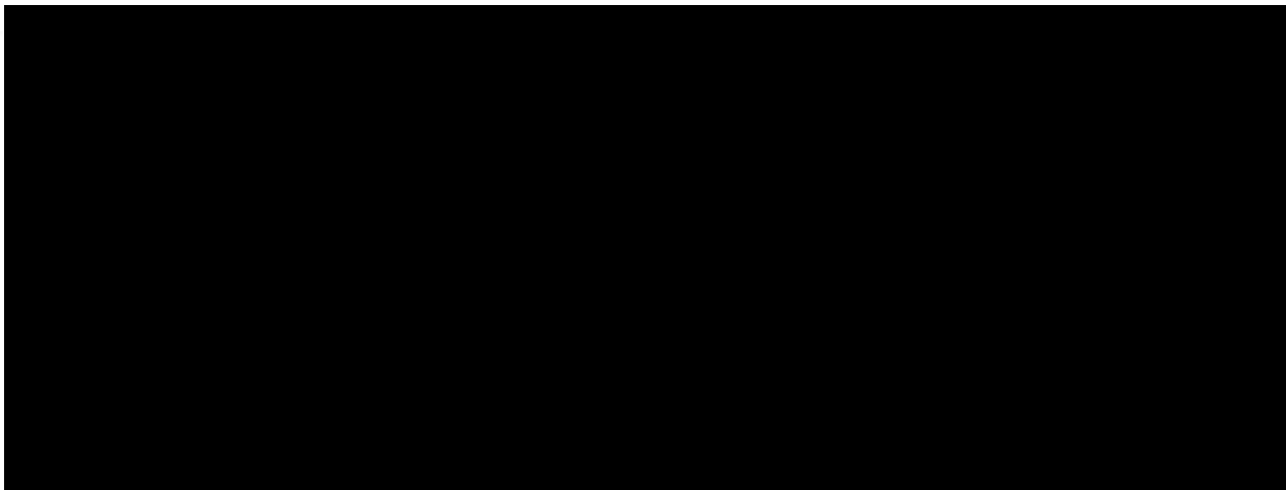
**ANECT**

ANECT a.s. | Vídeňská 204/125  
Přízřenice | 619 00 Brno  
T+420 547 100 100 | F+420 547 100 101  
www.anect.com      DIČ: CZ25313029





## **Příloha smlouvy č. 1 – Technická specifikace**







	<p>bezpečnostní rizika a anomální chování a musí o nich v reálném čase vytvářet upozornění.</p>	<p>identifikuje kybernetické hrozby a provozní nedostatky.</p> <p>Zařízení je dodáváno formou předinstalovaných HW Appliance do 19" racku. Velikost zařízení je 1U.</p>
	<p><b>Analýza plného síťového provozu</b></p> <p>Dodaný systém musí analyzovat síť čistě na základě zrcadleného síťového provozu (nikoliv jen na základě statistických protokolů typu NetFlow) a zároveň bez potřeby nasazovat agenty na koncové stanice nebo další zařízení v síti.</p>	<p><b>Splňuje.</b></p> <p>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 jsou velmi jednoduché.</p>
	<p><b>Ukládání síťových toků</b></p> <p>Systém ukládá síťové toky ve formátu, který umožní uživatelsky přívětivou analýzu síťové komunikace, včetně dohledání informací o aplikačních transakcích a jejich metadatech z L2 až L7, obsažených v daném síťovém toku.</p>	<p><b>Splňuje.</b></p> <p>Zařízení umožňuje dohledání libovolné komunikace až na úroveň jednotlivých flow záznamů, průběžné grafy provozu, top statistiky, reporty, alerty, databáze aktivních zařízení na síti vč. identifikace zařízení.</p> <p>Zařízení GREYCORTEX MENDEL uchovává a analyzuje informace z:</p> <p>L2 – MAC, Ethernet.</p> <p>L3 – IPv4, IPv6, ARP, ICMP, ICMPv6, VLAN, MPLS, GRE a další.</p> <p>L4 – UDP, TCP.</p> <p>L5 – L7 – DNS, DHCP, HTTP, HTTPS, SSL, TLS, SMB, SMB2, SSH, SMTP, FTP, TFPT, TELNET, DCERPC, IRC, VNC, POP3, Oscar, SIP, MS-SQL, KERBEROS, LDAP, SNMP, MODBUS, DNP3 a řada dalších.</p>
	<p><b>Uchování a vyhledávání síťových toků</b></p> <p>Je požadováno úložiště pro uchování datových toků v délce minimálně 180 dnů.</p> <p>Dále je požadováno, aby uživatel mohl v reálném čase volně filtrovat a vyhledávat v plné historii uložených síťových toků a agregovaných síťových statistik na základě minimálně parametrů: IP a MAC adresa, hostname, username, příchozí a odchozí provoz, síťová služba, lokální nebo vzdálená služba (služba z pohledu klient nebo server), číslo portu, VLAN, země, ASN.</p>	<p><b>Splňuje.</b></p> <p>Zařízení uchovává data po dobu nejméně 180 dnů s úložnou kapacitou cca 22 TB. Nad uloženými daty lze v reálném čase provádět filtrování na základě všech požadovaných parametrů.</p>
	<p><b>Automatická identifikace důležitých systémů</b></p>	<p><b>Splňuje.</b></p>



	<p>Je požadována automatická detekce přítomnosti klíčových služeb monitorované infrastruktury, jako jsou doménové řadiče, webové, emailové a databázové služby apod. Systém musí být schopen upozornit na vznik nových služeb v interní síti a sledovat jejich změny. A to minimálně v rozsahu následujících služeb: DHCP, DNS, MS Active Directory služby, HTTP, HTTPS, SMTP, POP3, IMAP, SSH, CIFS, SMTS, POP3S, IMAPS, CDP, LLDP, MSSQL, MySQL, TELNET, FTP, TFTP.</p>	<p>Zařízení automaticky označuje systémy jako je doménový kontroler, web, e-mail, tiskárna, gateway apod. včetně upozornění na výskyt nového zařízení daného typu. Zařízení monitoruje chování u všech protokolů v interní síti včetně DHCP, DNS, MS Active Directory služby, HTTP, HTTPS, SMTP, POP3, IMAP, SSH, CIFS, SMTS, POP3S, IMAPS, CDP, LLDP, MSSQL, MySQL, TELNET, FTP, TFTP.</p>
<b>Hardwarové požadavky</b>		
	<p><b>Síťové porty</b></p> <p>Celkem požadujeme minimálně 2 LAN rozhraní 1 Gbps metalika pro sběr dat a 1 LAN rozhraní 1 Gbps metalika pro práci s centrální konzolí.</p>	<p><b>Splňuje.</b></p> <p>Zařízení obsahuje 4x 1 GE</p>
<b>Požadavky na schopnost detekce bezpečnostních událostí</b>		
	<p><b>Monitorování zařízení, segmentů sítě a využívaných síťových služeb</b></p> <p>Poskytovaný systém musí identifikovat zařízení připojená do sítě včetně koncových zařízení, serverů, IoT zařízení apod. Zároveň musí být systém schopen identifikovat změny v síti – minimálně: změna IP/MAC adresy hosta, duplicitní IP/MAC adresa, změna VLAN, vytvoření nové podsítě, připojení nového zařízení, použití nové služby, nedostupnost dříve dostupné a komunikující služby nebo dříve dostupného a komunikujícího zařízení.</p> <p>Systém musí uživateli umožnit pomocí těchto metod nastavovat bezpečnostní politiky pro různé segmenty sítě a na porušení těchto politik reagovat upozorněním.</p>	<p><b>Splňuje.</b></p> <p>GREYCORTX MENDEL identifikuje zařízení připojená do sítě včetně koncových zařízení, serverů, IoT zařízení apod.</p> <p>Systém je schopen identifikovat změny v síti, jako je změna IP/MAC adresy hosta, duplicitní IP/MAC adresa, změna VLAN, vytvoření nové podsítě, připojení nového zařízení, použití nové služby, nedostupnost dříve dostupné a komunikující služby nebo dříve dostupného a komunikujícího zařízení.</p> <p>Systém umožňuje pomocí těchto metod nastavovat bezpečnostní politiky pro různé segmenty sítě a na porušení těchto politik reaguje upozorněním.</p>
	<p><b>Detekce síťových služeb</b></p> <p>Systém musí být schopen detekovat síťové služby na základě síťových metadat získaných prostřednictvím DPI (Deep Packet Inspection), nikoliv pouze čísla portu.</p>	<p><b>Splňuje.</b></p> <p>Systém je schopen detekovat síťové služby na základě síťových metadat získaných prostřednictvím DPI (Deep Packet Inspection), nikoliv pouze čísla portu.</p>
	<p><b>Samostatné učení behaviorálních aktivit a detekce anomálií</b></p>	<p><b>Splňuje.</b></p> <p>Systém používá strojové učení pro analýzu standardní síťové aktivity,</p>



<p>System musí používat matematické metody samostatného učení (např. strojové učení) pro analýzu standardní síťové aktivity, musí vytvářet a v čase automaticky modifikovat modely chování na základě běžného chování organizace.</p> <p>Především systém musí mít schopnost identifikovat nestandardní síťové chování, a to zejména:</p> <ul style="list-style-type: none"><li>• anomální přenosy dat, toků a paketů,</li><li>• anomální počet komunikačních partnerů a entropie na portech,</li><li>• anomální počet síťových toků a využitých síťových služeb,</li><li>• anomálie výkonnosti sítě a aplikací.</li></ul> <p>Samostatné učení je požadováno na všech síťových službách (port číslo 0 až 65535 u TCP i UDP) na IPv4 a IPv6 a dalších protokolech L3 síťové vrstvy.</p>	<p>vytváří a v čase automaticky modifikuje modely chování na základě běžného chování organizace.</p> <p>System je schopen identifikovat nestandardní síťové chování jako:</p> <ul style="list-style-type: none"><li>• anomální přenosy dat, toků a paketů,</li><li>• anomální počet komunikačních partnerů a entropie na portech,</li><li>• anomální počet síťových toků a využitých síťových služeb,</li><li>• anomálie výkonnosti sítě a aplikací.</li></ul> <p>Samostatné učení je aplikováno na všech síťových službách (port číslo 0 až 65535 u TCP i UDP) na IPv4 a IPv6 a dalších protokolech L3 síťové vrstvy.</p>
<p><b>Identifikace neznámých hrozeb, podezřelých chování na síti a porušení politik</b></p> <p>System musí být schopen detekovat neznámé hrozby, které nelze identifikovat prostřednictvím detekčních signatur, jako jsou trojské koně, botnety, apod.</p> <p>Zejména musí být identifikovány tyto příznaky potenciálně škodlivého chování:</p> <ul style="list-style-type: none"><li>• průzkumné aktivity v síti,</li><li>• potenciální úniky dat,</li><li>• detekce strojového chování, které nevytvářejí lidští uživatelé sítě,</li><li>• detekce repetitivních vzorců chování na síti,</li><li>• detekce botnetů o ovládnutí kompromitované stanice,</li><li>• detekce zapojení do sítě pro těžení kryptoměn,</li><li>• útoky hrubou silou,</li><li>• rozpoznání tunelovaného síťového provozu – alespoň IPv4 prostřednictvím IPv6 a HTTP prostřednictvím DNS.</li></ul>	<p><b>Splňuje.</b></p> <p>System detekuje požadované aktivity:</p> <ul style="list-style-type: none"><li>• průzkumné aktivity v síti,</li><li>• potenciální úniky dat,</li><li>• detekce strojového chování, které nevytvářejí lidští uživatelé sítě,</li><li>• detekce repetitivních vzorců chování na síti,</li><li>• detekce botnetů o ovládnutí kompromitované stanice,</li><li>• detekce zapojení do sítě pro těžení kryptoměn,</li><li>• útoky hrubou silou,</li><li>• rozpoznání tunelovaného síťového provozu – IPv4 prostřednictvím IPv6</li><li>• rozpoznání DNS tunelů.</li></ul>



<p><b>Detekce na základě databáze známých hrozeb (signaturní detekce)</b></p> <p>Systém musí být schopen identifikovat a reportovat události na základě detekční databáze malware, známých útoků a zranitelností, porušení bezpečnostních pravidel a „best practices“ a dalších rizik. Tato databáze musí být aktualizovaná minimálně na hodinové bázi.</p> <p>Databáze detekčních pravidel (signatur) musí být založena na pokročilých regulárních výrazech pro zpracování řetězců, které dokáží provádět inspekci veškeré síťové komunikace od L2 po L7</p> <p>Systém musí využívat tuto signaturní detekci pro veškerý monitorovaný provoz (na perimetru i v interní síti mezi všemi segmenty), nikoliv pouze pro omezený segment nebo podmnožinu celkové komunikace.</p> <p>Uživatel musí být schopen přidávat vlastní detekční pravidla v praktickém a obecně využívaném formátu.</p>	<p><b>Splňuje.</b></p> <p>Systém analyzuje veškerý provoz a porovnává jej se sadou detekčních signatur á la SNORT. Systém využívá asi 40 000–50 000 detekčních signatur, které jsou aktualizovány na hodinové bázi.</p>
<p><b>Detekce přenosu škodlivých souborů</b></p> <p>Systém musí být schopen v monitorovaném provozu porovnávat hash zachycených souborů s databázemi známých hashů škodlivých souborů.</p>	<p><b>Splňuje.</b></p> <p>Systém kontroluje přenášení souboru z pohledu jejich hash a ten kontroluje s databází škodlivých souborů.</p>
<p><b>Analýza šifrované komunikace</b></p> <p>Vedle samostatného učení musí systém používat další metody pro analýzu šifrované komunikace, minimálně TLS fingerprinting a s ní spojenou detekci známých hrozeb.</p>	<p><b>Splňuje.</b></p> <p>Systém provádí kontrolu šifrovacích certifikátů u SSL/TLS, provádí fingerprinting na základě algoritmů JA3 a provádí veškeré modelování šifrované komunikace, na základě které jsou detekovány anomální jevy.</p>
<p><b>Asistované učení a korelace událostí</b></p> <p>Systém musí být schopen korelace jakýchkoliv detekovaných událostí ze všech detekčních metod a úpravy samostatného učení a dalších detekčních metod tak, aby byly v maximální míře eliminovány falešné alarmy. Systém musí být schopen eliminovat falešné alarmy i pro události detekované v historii.</p> <p>Systém musí být schopen zobrazovat zařízení podle souhrnné kritičnosti identifikovaných</p>	<p><b>Splňuje.</b></p> <p>Systém je schopen korelace jakýchkoliv detekovaných událostí ze všech detekčních metod a úpravy samostatného učení a dalších detekčních metod s cílem v maximální míře eliminovat falešné alarmy.</p> <p>Systém je schopen eliminovat falešné alarmy i pro události detekované v historii.</p>



	událostí – minimálně v rozsahu kritické a důležité.	System je schopen zobrazovat zařízení podle souhrnné kritičnosti identifikovaných událostí.
	<b>Aktuální databáze blacklistů</b> System musí být schopen hodnotit IP adresy, se kterými komunikují vnitřní hosté v síti prostřednictvím minimálně denně aktualizovaných reputačních databází. Uživatel musí být schopen importovat vlastní reputační databáze.	<b>Splňuje.</b> System obsahuje reputační databáze, které jsou aktualizovány na hodinové bázi.
<b>Požadavky na zajištění síťové viditelnosti</b>		
	<b>Rychlé vyhledávání a filtrování všech dat</b> System musí být schopen podporovat okamžité vyhledávání a vizualizaci pro forenzní analýzu a podporu pro tzv. threat hunting (analýza bezpečnostních událostí při ověřování bezpečnostních incidentů). Jedná se o možnost okamžitě filtrovat a vyhledávat v plné historii všech uložených dat, tj. bezpečnostních událostí a zaznamenaných síťových toků, a to minimálně podle parametrů: IP a MAC adresa, hostname, username, příchozí a odchozí provoz, síťová služba, lokální nebo vzdálená služba (služba z pohledu klient nebo server), číslo portu, VLAN, země, ASN. System musí být schopen v reálném čase filtrovat a vizualizovat výsledky v grafech, výčtových tabulkách s možností řazení a TOP N statistikách. Uživatel musí mít možnost ukládat definované filtry a sdílet je s dalšími uživateli.	<b>Splňuje.</b> System podporuje okamžité vyhledávání ve všech částech aplikace. Příklady parametrů pro filtrování: IP Address, Host Name, MAC Address, Subnet, User Name, Domain String, Service, Application, Operating System, Location, Traffic Direction, Subnet, Network Interface, Protocol, Tunneled traffic, VLAN ID, Event, Event Category, Incident Status, Host Risk, Severity a fulltextové vyhledávání nad daty. Filtry je možné ukládat a sdílet.
	<b>Ukládání a vyhledávání aplikačních metadat</b> System musí být schopen ukládat a následně vyhledávat aplikační metadata (vždy dotaz i odpověď všech transakcí v toku) minimálně z následujících protokolů, které jsou nebo mohou být využívány ve vnitřní síti organizace: FTP, FTP-DATA, TFTP, TFTP-DATA, SSH, Telnet, SMTP, SMTPS, DNS, DHCP, HTTP, HTTPS, NTP, SMB, SNMP, LDAP, NFS, MS-SQL, SIP, Kerberos, SSL/TLS.	<b>Splňuje.</b> System je schopen ukládat a následně vyhledávat aplikační metadata (vždy dotaz i odpověď všech transakcí v toku) u následujících protokolů: FTP, FTP-DATA, TFTP, TFTP-DATA, SSH, Telnet, SMTP, SMTPS, DNS, DHCP, HTTP, HTTPS, NTP, SMB, SNMP, LDAP, NFS, MS-SQL, SIP, Kerberos, SSL/TLS.
	<b>Kontextuální informace</b>	<b>Splňuje.</b>



	<p>Systém musí být schopen získávat, vizualizovat a integrovat v jednotném grafickém rozhraní kontextuální informace pro detekované události a ukládané záznamy síťových toků a agregované síťové statistiky minimálně v tomto rozsahu:</p> <ul style="list-style-type: none"> <li>• Jméno uživatele a další jeho parametry z doménového řadiče (minimálně MS Active Directory)</li> <li>• Automatická detekce a zobrazování hostname na základě zpracování aktuálních dat z DNS a DHCP provozu</li> <li>• IP reputace, vč. údaje, jestli je IP adresa blacklistovaná nebo podezřelá</li> <li>• Zobrazování síťových toků příslušných k detekované události</li> <li>• MAC adresa a výrobce zařízení</li> </ul>	<p>Systém získává, vizualizuje a integruje v jednotném grafickém rozhraní kontextuální informace pro detekované události a ukládané záznamy síťových toků a agregované síťové statistiky rozsahu:</p> <ul style="list-style-type: none"> <li>• jméno uživatele a další jeho parametry z doménového řadiče (minimálně MS Active Directory),</li> <li>• automatická detekce a zobrazování hostname na základě zpracování aktuálních dat z DNS a DHCP provozu,</li> <li>• IP reputace vč. údaje, zda je IP adresa blacklistovaná nebo podezřelá,</li> <li>• zobrazování síťových toků příslušných k detekované události,</li> <li>• MAC adresa a výrobce zařízení.</li> </ul>
	<p><b>Monitoring výkonu aplikací</b></p> <p>Systém v celé monitorované síti, mezi všemi zařízeními a na všech službách měří a vytváří automaticky (bez nutnosti nastavovat manuálně limitní hodnoty (thresholdy) nebo jiné parametry) vytváří model normálního chování pro výkonnostní parametry minimálně odezva sítě, odezva aplikace a odezva z pohledu uživatele.</p>	<p><b>Splňuje.</b></p> <p>Systém plně monitoruje a vyhodnocuje výkonnostní parametry u všech zařízení v síti.</p>
	<p><b>Zaznamenávání a ukládání plného provozu</b></p> <p>Je požadováno volitelné nahrávání plného síťového provozu (full packet capture) na všech dodaných zařízeních minimálně na základě parametrů: cílová a zdrojová IP/MAC adresa, podsítě, využitý protokol, IPv4 nebo IPv6.</p>	<p><b>Splňuje.</b></p> <p>Systém umožňuje provádět záznam komunikace do PCAP souborů na základě uživatelem definovaných filtrů.</p>
	<p><b>Jednotné grafické rozhraní</b></p> <p>Systém musí poskytovat jednotné grafické uživatelské rozhraní pro veškerou práci uživatelů, včetně všech detekcí, analýzy síťových statistik, konfigurace alertů, reportů a dashboardů.</p>	<p><b>Splňuje.</b></p> <p>Systém poskytuje jedno GUI.</p>
	<p><b>Uživatelské profily a nastavení</b></p> <p>Systém musí být schopen vytváření profilů a skupin uživatelů pro omezení funkcionality</p>	<p><b>Splňuje.</b></p> <p>Systém je schopen vytváření profilů a skupin uživatelů pro omezení</p>



	<p>produktu a viditelnosti uložených dat s podporou minimálně:</p> <ul style="list-style-type: none"> <li>• granulární nastavení přístupu k analytickým i konfiguračním/administrativním komponentám systému s definovanými úrovněmi přístupu,</li> <li>• granulární nastavení přístupu k datům z různých segmentů sítě organizace s definovanými úrovněmi přístupu (alespoň read, write, execute),</li> <li>• vytváření filtrů veškerých dat a jejich sdílení mezi uživateli a skupinami uživatelů,</li> <li>• vytváření vlastních uživatelských pohledů, reportů, dashboardů apod.</li> </ul>	<p>funkcionality produktu a viditelnosti uložených dat s podporou minimálně:</p> <ul style="list-style-type: none"> <li>• granulární nastavení přístupu k analytickým i konfiguračním/administrativním komponentám systému s definovanými úrovněmi přístupu,</li> <li>• granulární nastavení přístupu k datům z různých segmentů sítě organizace s definovanými úrovněmi přístupu (read, write, execute),</li> <li>• vytváření filtrů veškerých dat a jejich sdílení mezi uživateli a skupinami uživatelů,</li> <li>• vytváření vlastních uživatelských pohledů, reportů, dashboardů apod.</li> </ul>
<b>Požadavky na procesní zpracování kybernetických událostí</b>		
	<p><b>Management bezpečnostních událostí a incidentů</b></p> <p>Systém musí poskytovat integrované rozhraní pro:</p> <ul style="list-style-type: none"> <li>• reporting bezpečnostních incidentů (prohlášení identifikované události za bezpečnostní incident),</li> <li>• spolupráci a sdílení informací při analýze identifikovaných bezpečnostních incidentů včetně potřebného workflow mezi jednotlivými uživateli s podporou automatizovaných oznámení o změně stavu události či přiřazení řešitele,</li> <li>• jednoduché sdílení informací o bezpečnostních incidentech,</li> <li>• možnost vyhledávání a filtrování nad všemi událostmi z pohledu workflow bezpečnostního incidentů (reportovaná událost, událost v řešení, vyřešená událost, události v řešení daného uživatele apod.).</li> </ul>	<p><b>Splňuje.</b></p> <p>Systém poskytuje integrované rozhraní pro:</p> <ul style="list-style-type: none"> <li>• reporting bezpečnostních incidentů (prohlášení identifikované události za bezpečnostní incident),</li> <li>• spolupráci a sdílení informací při analýze identifikovaných bezpečnostních incidentů včetně potřebného workflow mezi jednotlivými uživateli s podporou automatizovaných oznámení o změně stavu události či přiřazení řešitele,</li> <li>• jednoduché sdílení informací o bezpečnostních incidentech,</li> <li>• možnost vyhledávání a filtrování nad všemi událostmi z pohledu workflow bezpečnostního incidentu (reportovaná událost, událost v řešení, vyřešená událost, události v řešení daného uživatele apod.).</li> </ul>
	<p><b>Účast v ISIRT týmu.</b></p>	<p><b>Splňuje.</b></p>



	Tato skupina činností představuje řešení kybernetických bezpečnostních událostí a incidentů ve spolupráci s NÚKIB.	System umožňuje spolupráci v ISIRT týmu.
<b>Požadavky na integraci, reporting a alerting</b>		
	<b>Integrace</b> System musí být schopen rychlé a jednoduché uživatelské integrace s nástroji třetích stran bez využití složitých nástrojů jako API minimálně s: <ul style="list-style-type: none"><li>• nástrojem typu SIEM prostřednictvím minimálně syslog, CEF a LEEF,</li><li>• nástroji pro generování nebo zpracování síťových statistik ve formátu IPFIX/NetFlow, včetně možnosti filtrovat IPFIX/NetFlow exportované statistiky dle všech filtrovaných parametrů jako výše,</li></ul>	<b>Splňuje.</b> System umožňuje rychlé a jednoduché uživatelské integrace s nástroji třetích stran bez využití složitých nástrojů jako API minimálně s: <ul style="list-style-type: none"><li>• nástrojem typu SIEM prostřednictvím minimálně syslog, CEF a LEEF,</li><li>• nástroji pro generování nebo zpracování síťových statistik ve formátu IPFIX/NetFlow, včetně možnosti filtrovat IPFIX/NetFlow exportované statistiky dle všech filtrovaných parametrů jako výše.</li></ul>
	<b>Automatické bezpečnostní hlášení (alerty)</b> System musí být schopen upozorňovat uživatele prostřednictvím minimálně emailu a SNMP trap o: <ul style="list-style-type: none"><li>• všech identifikovaných událostech,</li><li>• událostech filtrovaných minimálně dle IP a MAC adresy, podsítě, závažnosti události, kategorie události, země, uživatele, síťové služby, čísla portu, provozu do/z internetu.</li></ul> Tyto alerty musí být systém schopen dodávat i ve strojově čitelném formátu pro využití v nástrojích typu SIEM a musí obsahovat minimálně kompletní informace o detekované události včetně URL odkazu na danou událost v reportovaném období do grafického rozhraní aplikace.	<b>Splňuje.</b> System je schopen upozorňovat uživatele prostřednictvím e-mailu a SNMP trap o: <ul style="list-style-type: none"><li>• všech identifikovaných událostech,</li><li>• událostech filtrovaných minimálně dle IP a MAC adresy, podsítě, závažnosti události, kategorie události, země, uživatele, síťové služby, čísla portu, provozu do/z internetu.</li></ul> Alerty je systém schopen dodávat i ve strojově čitelném formátu pro využití v nástrojích typu SIEM.
	<b>Možnost automatizovaného reportingu</b> Možnost vytváření automatizovaných manažerských reportů o stavu kybernetické bezpečnosti z pohledu zprávy kybernetických incidentů ideálně dle oblastí jejich vzniků (např.: doména, web, email, apod.).	<b>Splňuje.</b> System poskytuje možnost vytváření automatizovaných manažerských reportů o stavu kybernetické bezpečnosti z pohledu zprávy kybernetických incidentů.



	Je požadována podpora reportů v českém jazyce.	Je dostupná podpora generování reportů v českém jazyce.
<b>Implementační práce a dokumentace</b>		
	Instalace veškerých dodaných hardwarových komponent do racku včetně instalace veškeré kabeláže	<b>Splňuje.</b> Systém bude plně instalován a integrován v prostředí zákazníka včetně potřebné kabeláže.
	Konfigurace systému, včetně definice pravidel pro detekci událostí, nastavení alertů, nastavení reportů.	<b>Splňuje.</b> Součástí dodávky je konfigurace systému, včetně definice pravidel pro detekci událostí, nastavení alertů, nastavení reportů.
	Součástí dodávky je školení pro min. 2 administrátory v rozsahu min. 2x6 hodin (může být součástí implementačních prací)	<b>Splňuje.</b> Součástí dodávky je školení administrátorů v požadovaném rozsahu.
	<p>Aktuální implementace a konfigurace řešení je dokumentovaná v elektronické podobě (DOCx, XLSx, PDF anebo HTML). Dokumentace je požadovaná v českém jazyce.</p> <p>Dokumentace musí obsahovat minimálně:</p> <ul style="list-style-type: none"> <li>• Popis dodaného nástroje a jeho případných komponent (výrobce, typ, sériové číslo, servisní číslo, licence).</li> <li>• Schematický náčrt zapojení do počítačové sítě Zadavatele.</li> <li>• Textový popis fungování řešení jako celku.</li> <li>• Název nástroje (zařízení) v síti Zadavatele, jeho IP adresy a všechna přidělená jména.</li> <li>• Detailní náčrt a popis zapojení (porty nástroje a jejich konfigurace, VLAN, konfigurace portů aktivních prvků, ke kterým je nástroj připojen).</li> <li>• Popis přístupů ke správě nástroje: použité rozhraní (LAN, USB apod.), adresa rozhraní, způsob přístupu (webový prohlížeč, SSH apod.).</li> <li>• Přehled přístupových údajů k nástroji tak, aby Zadavatel měl po převzetí neomezený přístup ke všem částem a komponentám nástroje.</li> <li>• Popis přístupu k technické podpoře nástroje: kontaktní údaje, autentizační</li> </ul>	<b>Splňuje.</b> Součástí dodávky je vytvoření dokumentace nasazení.



	údaje, pravidla pro komunikaci s technickou podporou.	
<b>Technická podpora</b>		
	Dodavatel garantuje vzdálenou podporu min formou emailu a telefonní hot-line v režimu 24x7 v českém jazyce	<b>Splňuje.</b> Zákazník si může podporu vyžádat pomocí on-line přístupu do trouble-ticket systému ServiceDesk, použitím bezplatné zelené linky nebo mobilního čísla, případně e-mailu na adresu dodavatele.  Pro poskytování služby budou vytvořeny příslušné kategorie s požadovanými parametry služby a všechny požadavky budou odbavovány kvalifikovanými pracovníky dodavatele v rámci definovaného SLA.
	Dodavatel garantuje servisní podporu v režimu 9x5 na hardware a software s opravou on-site, s garantovanou odezvou 4h od nahlášení případné závady, včetně výměny a plné implementace náhradního zařízení on-site NBD (Next Business Day, následující pracovní den)	<b>Splňuje.</b> Zákazník si může podporu vyžádat pomocí on-line přístupu do trouble-ticket systému ServiceDesk, použitím bezplatné zelené linky nebo mobilního čísla, případně e-mailu na adresu dodavatele.  Pro poskytování služby budou vytvořeny příslušné kategorie s požadovanými parametry služby a všechny požadavky budou odbavovány kvalifikovanými pracovníky dodavatele v rámci definovaného SLA.
	Dodavatel zajišťuje možnost eskalovat kritické incidenty na podporu výrobce	<b>Splňuje.</b> Dodavatel je certifikovaným partnerem výrobce a je oprávněn eskalovat řešení incidentů na L3 podporu výrobce.
	Servisní podpora výrobce na aktualizaci SW na. 4 roky. Podpora obsahuje vždy aktuální verze SW a opravy chyb.	<b>Splňuje.</b> Je součástí nabízené maintenance výrobce.

Všechna dodavatelem instalovaná zařízení nebo komponenty musí být dodavatelem profesionálně nainstalována a zprovozněna a po jejich nasazení řádně dokumentována a otestována, vč. prokázání, že tato zařízení plní všechny požadované a výkonnostní parametry.

Všechna dodavatelem instalovaná zařízení budou zabezpečena a nebudou obsahovat zjevná rizika a zranitelnosti, a to po celou dobu provozu služby.

Řešení musí splňovat bezpečnostní kritéria podle zákona č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění



pozdějších předpisů, a nebude v rozporu s požadavky Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) pro provoz významných informačních systémů; Zadavatel je povinen dle § 5 vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů, provádět analýzu rizik a identifikovaná rizika řídit. Současně je zadavatel povinen zabývat se všemi hrozbami, které prostřednictvím varování vydává NÚKIB, těmito hrozbami se dále zabývat a zohlednit je v analýze rizik. Zadavatel proto provedl, s přihlédnutím k vydanému "varování" NÚKIB, analýzu rizik a v hodnocení se řídil pokyny uvedenými v dokumentu NÚKIB "Metodika k varování ze dne 17. prosince 2018". Veškerá bezpečnostní opatření, která bude nutné u dodaného řešení na základě výsledků analýzy rizik přijmout, nesmí pro zadavatele znamenat žádné další náklady.

### **Implementační služby**

Zadavatel požaduje implementaci řešení do vlastní infrastruktury pro provoz

- produkčního prostředí,
- testovacího prostředí funkčně ekvivalentního s produkčním prostředím.

Součástí implementace řešení bude:

- Vstupní analýza upřesňující nastavení cílového řešení a požadavky na infrastrukturu
- Příprava prostředí pro implementaci řešení dle závěrů vstupní analýzy
- Nasazení a konfigurace řešení do testovacího prostředí
- Ověření funkčnosti řešení v testovacím prostředí
- Nasazení a základní konfigurace produkčního prostředí
- Provedení akceptačních testů
- Konzultace pro podporu integrace
- Školení uživatelů
- Předání dokumentace a ukončení implementace

### **Produktová podpora výrobce**

Dodavatel musí zajistit produktovou podporu řešení v délce 48 měsíců od zahájení poskytování služeb.

### **Akceptační testy**

Součástí akceptačních testů bude prokázání funkčností dodaných rozhraní pro všechny typy požadovaných operací a formátů a předání formou akceptačního protokolu.

### **Provozní dokumentace**

V rámci realizace řešení služeb bude Dodavatelem zpracována a předána dokumentace řešení minimálně v tomto rozsahu:

- Provozně-technická dokumentace v rozsahu požadovaném vyhláškou č. 529/2006 Sb. § 10 a § 11,
- Plán zálohování a obnovy včetně doporučení pravidel pro pravidelné ověřování jednotlivých postupů,
- Bezpečnostní dokumentace dle zákona 181/2014 Sb. o kybernetické bezpečnosti, včetně jeho novel a jeho prováděcích právních předpisů, především pak analýza aktiv“ ve vazbě na metodiku PSP a plán obnovy.



- Integrovaná dokumentace popisující jednotlivá aplikační rozhraní (WS a API služby) používaná k integraci IS na jednotlivé funkce včetně funkčních prototypů volání jednotlivých funkcí.

### ***Administrátorské školení***

V rámci realizace bude Dodavatelem realizováno administrátorské školení pro zaměstnance Zadavatele.

### ***Termín plnění***

Dodavatel musí zajistit zahájení plnění služeb do 2 měsíců od podpisu smlouvy.



## **Příloha smlouvy č. 2 – Dohoda o mlčenlivosti**

### **Dohoda o mlčenlivosti**

#### **ANECT a.s.**

se sídlem: Vídeňská 204/125, Přízřenice, 619 00 Brno  
zastoupena: Pavlem Srnkou, členem představenstva  
IČO: 25313029  
DIČ: CZ25313029  
bankovní spojení: Komerční banka, a.s., pobočka Brno,  
číslo bankovního účtu: 27-6667590237 / 0100  
kontaktní osoba: Ing. Petr Polášek  
tel., email: +420 724 427 220, petr.polasek@anect.com  
dále jen „**Poskytovatel**“

a

#### **Česká republika – Kancelář Poslanecké sněmovny**

se sídlem: Sněmovní 176/4, 128 26 Praha 1 – Malá Strana  
zastoupena: Mgr. Janem Morávkem, vedoucím Kanceláře Poslanecké sněmovny  
osoba oprávněna jednat ve věcech smluvních: Ing. Mgr. Naďa Formanová, ředitelka  
odboru hospodářské správy, na základě pověření vedoucího zaměstnance k jednání  
jménem státu ze dne 1. 7. 2017  
IČO: 00006572  
DIČ: CZ00006572  
bankovní spojení: ČNB Praha, číslo bankovního účtu: 5622001/0710  
datová schránka ID: bykaigw  
kontaktní osoba: Ing. Monika Pravcová, ředitelka odboru informatiky  
tel., email: +420 257 174 151, PravcovaM@psp.cz  
dále jen „**Objednatel**“

Smluvní strany ujednávají následující:

1. Smluvní strany prohlašují, že veškeré důvěrné podklady a důvěrné informace, které od sebe navzájem získají, budou použity výhradně pro potřebu přípravy a realizace projektu. Tyto důvěrné informace nebudou poskytnuty v žádné formě třetím osobám ani nebudou použity Smluvními stranami k žádnému dalšímu účelu, pokud nedojde k písemné dohodě, která by nakládání s informacemi tohoto charakteru upravila způsobem odlišným.
2. Smluvní strany se zavazují po zde sjednanou dobu ochraňovat důvěrné informace obvyklým způsobem, přinejmenším však, jako by se jednalo o důvěrné informace jejich vlastní.

T



3. Za důvěrné podklady a důvěrné informace podle předchozího odstavce se bez ohledu na formu jejich zachycení považují veškeré podklady a informace, které byly některou ze Smluvních stran označeny jako důvěrné, a které se týkají zmíněného projektu jeho plnění anebo podklady a informace, které se týkají přímo některé ze Smluvních stran (zejména osobní údaje, obchodní tajemství, informace o činnosti, struktuře, hospodářských výsledcích, know-how, připravovaných projektech apod.).
4. Smluvní strany se dále zavazují považovat za důvěrné podle tohoto ustanovení taktéž veškeré neveřejné informace, mající povahu obchodního tajemství, vzájemně získané ústním podáním některé ze Smluvních stran.
5. Po skončení projektu, který bude po podpisu této dohody stanoven v plánu penetračního testu, zavazují se strany této dohody vrátit si vzájemně do tří pracovních dnů veškeré si v písemné či elektronické podobě poskytnuté důvěrné podklady a důvěrné informace, případně zničit jejich elektronický tvar na nosičích ve vlastním systému.
6. O postupu dle bodu 5. bude pořízen dvojmo zápis, v němž bude toto prohlášení obsaženo, a každá Smluvní strana obdrží jeden výtisk podepsaný přítomnými zástupci obou Smluvních stran.
7. Tato dohoda se netýká informací, obsažených ve veřejně dostupných materiálech, které Smluvní strany poskytují svým anonymním zákazníkům nebo klientům v jakékoli formě. Týká se však takových informací, které jsou vypracovány přímo pro druhou Smluvní stranu, jsou takto označeny a mají současně povahu informací, uvedených v čl. I této dohody.
8. Závazkem ochrany veškerých informací, uvedených v čl. I této dohody, jsou Smluvní strany vázány od okamžiku podpisu této dohody s tím, že závazek ochrany důvěrných informací zůstává v platnosti i po ukončení projektu.
9. Bez ohledu na výše uvedená ustanovení se za důvěrné nepovažují informace, které:
  - se staly veřejně známými, aniž by to zavinila záměrně či opomenutím strana přijímající dle této dohody důvěrnou informaci,
  - měla přijímající strana legálně k dispozici před uzavřením této dohody, pokud takové informace nebyly předmětem jiné, dříve mezi Smluvními stranami uzavřené smlouvy o ochraně informací,
  - jsou výsledkem postupu, při kterém k nim přijímající strana dospěje nezávisle a je to schopna doložit svými záznamy nebo informacemi třetí strany, bez ohledu na to, zda obsahuje důvěrné informace či nikoli,
  - po podpisu této dohody poskytne přijímající straně třetí osoba, jež takové informace přitom nezíská přímo ani nepřímo od strany, jež je jejich vlastníkem.

28-05-2020

V Praze dne (uvedeno v elektronickém podpisu)

ČESKÁ REPUBLIKA  
KANCELÁŘ POSLANECKÉ SNĚMOVNY  
110 27 PRAHA 1, SNĚMOVNÍ 176/4

Ing. Mgr. Naděžda Formanová,  
ředitelka odboru hospodářské správy

25.5.2020

V Praze dne (uvedeno v elektronickém podpisu)

Pavel Srnka

člen představenstva

ANECT Strana 24 z 24

ANECT a.s. | V Ideňská 204/125  
Přížbenice | 619 00 Brno  
T+420 547 100 100 | F+420 547 100 101  
www.anecl.com DIČ: CZ25313029

T



## Příloha smlouvy č. 3 – Popis plnění

**GREYCORTEX MENDEL** je nástroj pro pokročilý monitoring a analýzu síťového provozu, který prostřednictvím umělé inteligence a strojového učení identifikuje kybernetické hrozby a provozní nedostatky.

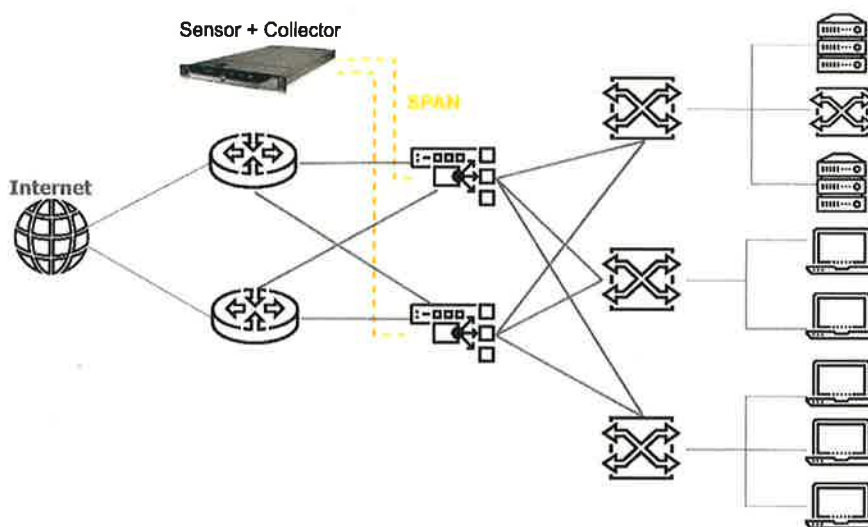
### Hlavní schopnosti

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

- 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
- Detailní viditelnost do síťového provozu

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.

Následující schéma znázorňuje příklad nasazení.



### 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.

Sensor zpracovává a analyzuje veškerá data zachycená na úrovni síťových vrstev ISO/OSI modelu v rozsahu L2 – L7.

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 neviditelný na L2 a L3 vrstvě (monitorovací porty nemají IP a jsou 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/IPFIX, Kolektor podporuje generování a odesílání síťových statistik protokolem NetFlow v9 a IPFIX. Rovněž obsahuje plnou podporu pro IPv4, IPv6, VLAN, Ethernet a další.

**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.

### Analýza síťového provozu

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

1. Detekce neznámých a cílených útoků a hrozeb	
Typy útoků a hrozeb	Metoda
<b>Pokročilé neznámé útoky</b> <ul style="list-style-type: none"><li>• útoky na uživatelské účty</li><li>• komunikace s botnetem</li><li>• úniky dat</li><li>• obecně anomální chování uživatelů a zařízení</li></ul>	<b>Prediktivní analýza</b> = 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.
<b>Cílené hrozby</b> <ul style="list-style-type: none"><li>• RAT - Remote Access Trojan</li><li>• APT – Advanced Persistent Threat</li><li>• AVT – Advanced Volatile Threat</li></ul>	<b>Detekce strojového chování</b> = odlišení projevů malware od lidské legitimní komunikace prostřednictvím periodických vzorů chování



## 2. Detekce známých útoků a hrozeb

Typy útoků a hrozeb	Metoda
<p>Známé projevy škodlivého chování</p> <ul style="list-style-type: none"><li>• skenování sítě a zařízení</li><li>• enumerace dat</li><li>• detekce hádání hesel</li><li>• DoS a DDoS útoky apod.</li></ul>	<p>Behaviorální detekce na úrovni toků za pomoci pravidel pro detekci očekávatelných projevů útoků.</p>
<p>Známé hrozby a již popsané útoky</p> <ul style="list-style-type: none"><li>• malware pro běžná zařízení</li><li>• malware pro mobilní zařízení</li><li>• exploitace a zneužití zranitelností</li><li>• trojské koně</li><li>• útoky na aplikační a DB servery</li><li>• zranitelnosti na straně klientských aplikací (JAVA, Flash, MS Office, prohlížeče...)</li><li>• aktuální hrozby – phishing, trojans, ...</li><li>• komunikace s blacklistovanými zařízeními (IP adresa, doména)</li></ul>	<p>Detekce známých útoků na základě denně aktualizované <i>sady detekčních pravidel</i> (přes 40.000) a blacklistů (60.000 až 100.000 záznamů).</p> <p>Příklady detekčních kategorií: 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.</p>

## 3. Ověření s bezpečnostními zásadami a politikami

Příklady nálezů	Ověřované politiky
<p>Porušení vybraných politik pro ochranu dat GDPR</p> <ul style="list-style-type: none"><li>• využívání dat nepovolenými osobami/způsoby</li><li>• rizika úniku osobních údajů</li></ul>	<p>Ověření souladu identifikovaných komunikací a komunikačních vektorů obsahujících osobní údaje s předem definovanými politikami pro ochranu dat.</p>
<p>Porušení komunikační politiky</p> <ul style="list-style-type: none"><li>• Nedostupné služby a zařízení</li><li>• Vznik nových nepovolených služeb a zařízení</li><li>• Nepovolené komunikační vektory</li></ul>	<p>Kontrola povolených a zakázaných služeb, prostupů a síťových politik – srovnání pozorované komunikační matice a uživatelem definovaných politik.</p>
<p>Porušení bezpečnostních politik</p> <ul style="list-style-type: none"><li>• používání anonymizačních (Tor) a P2P sítí</li><li>• hraní her a používání nepovolených aplikací</li><li>• prověrka šifrovaná komunikace</li><li>• nepovolené DNS servery</li><li>• tunelovaný DNS provoz</li><li>• používání zranitelných a zastaralých aplikací apod.</li></ul>	<p>Zásady dobré praxe v síťové bezpečnosti</p>

T



#### 4. Výkonnost sítě a aplikací

##### Příklady měřených veličin

##### NPM – Network Performance Monitoring

- objem a rychlost přenesených dat, síťových toků a paketů
- počet komunikačních partnerů, aktivních hostů, ...

##### APM – Application Performance Monitoring

- rychlost přenosu dat na síti RTT, SRT, URT.
- rychlost aplikační odezvy ART, EUT.

##### Monitorovaná oblast

Výkonost sítě na úrovni celé sítě, jednotlivých podsítí, hostů a na nich běžících službách.

Rychlost odezvy aplikací měřitelných na síti vč. automatické detekce anomálií, případně porušení uživatelem definovaných SLA. Možnost sledování vývoje výkonnosti v čase u všech aplikací v interní síti na portech TCP/0-65535.



## 5. Vizualizace sítě a forenzní analýza

Příklady využití	Monitorovaná oblast
<p>Filtrování a zobrazení libovolných dat v reálném čase dle potřeb uživatele např.:</p> <ul style="list-style-type: none"><li>• kdo s kým, kdy, jak komunikuje (komunikační partneři)</li><li>• bezpečnostní incidenty vč. příslušných síťových toků a případně obsahu zachycených škodlivých paketů</li><li>• využívané síťové služby vč. aplikačních metadat</li><li>• komunikace uživatelem vybraných zařízení</li><li>• výkonost aplikací a sítě apod.</li></ul>	<p>Kompletní viditelnost na úrovni síťových toků: celá síť, podsítě, zařízení/hosti, služby (na všech síťových portech) vč. škodlivých payloadů</p> <p>Příklady parametrů pro filtrování: IP Address, Host Name, MAC Address, Subnet, User Name, Domain String, Service, Application, Operating System, Location, Traffic Direction, Subnet, Network Interface, Protocol, Tunneled traffic, VLAN ID, Event, Event Category, Incident Status, Host Risk, Severity a fulltextové vyhledávání nad daty.</p> <p>Zobrazení cílových IP adres komunikace od zdrojových hostů na základě X-Forwarding-for</p>
<p>Viditelnost proxy</p>	<p>Viditelnost do uložených aplikačních metadat komunikačních protokolů s možností fulltextového vyhledávání.</p> <p>Příklady protokolů: DNS, DHCP, HTTP, HTTPS, SSL, TLS, SMB, SMB2, SSH, SMTP, FTP, TFPT, TELNET, DCERPC, IRC, VNC, POP3, Oscar, SIP, MS-SQL, KERBEROS, LDAP, SNMP, MODBUS, DNP3 a další.</p>
<p>Rychlá analýza příčin a následků v reálném čase díky ukládání bohatých metadat</p>	<p>Informace pro forenzní analýzu – bohatá metadata o síťovém provozu uchovávaná po požadovanou dobu (v řádu měsíců).</p>
<p>Jednoduché vyšetřování incidentů – bezpečnostních i provozních</p>	<p>Volitelný záznam provozu (on-deman full packet capture) dle zařízení, komunikačního partnera, portu/slужby atd.</p>
<p>Záznam vybrané podezřelé komunikace pro analýzu</p>	

### 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 lokální služby.

### Uživatelský přístup a výstupy nástroje

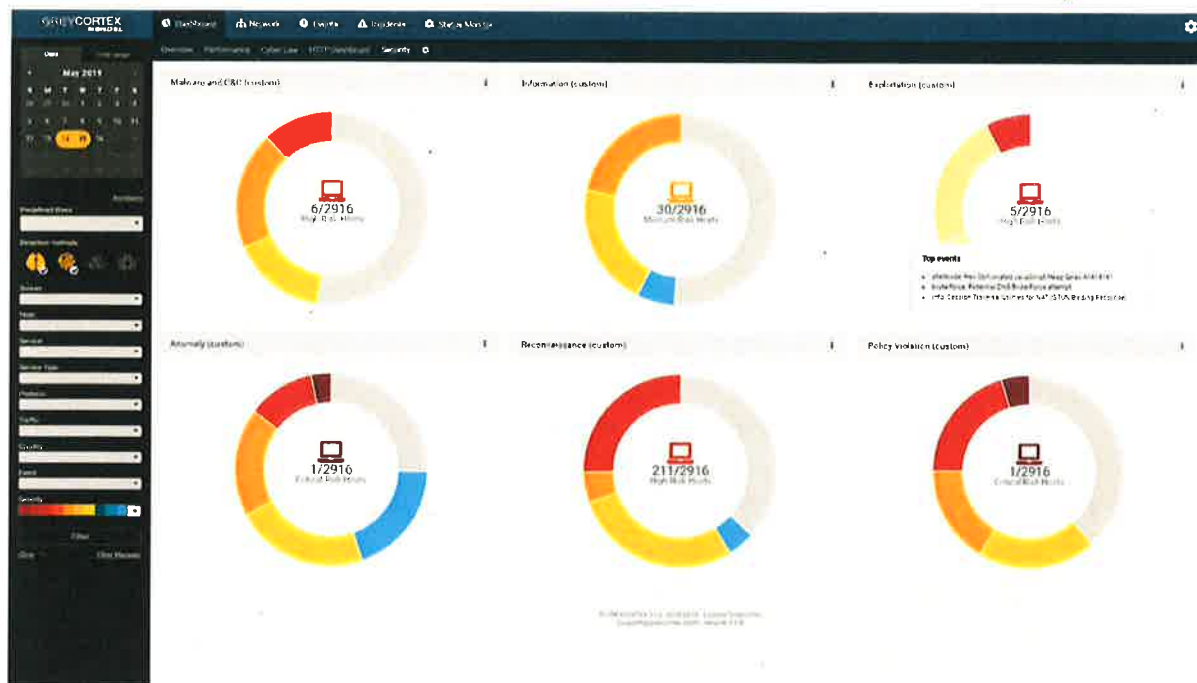
Aplikace obsahuje webové grafické uživatelské rozhraní, které je dostupné prostřednictvím všech běžných internetových prohlížečů.



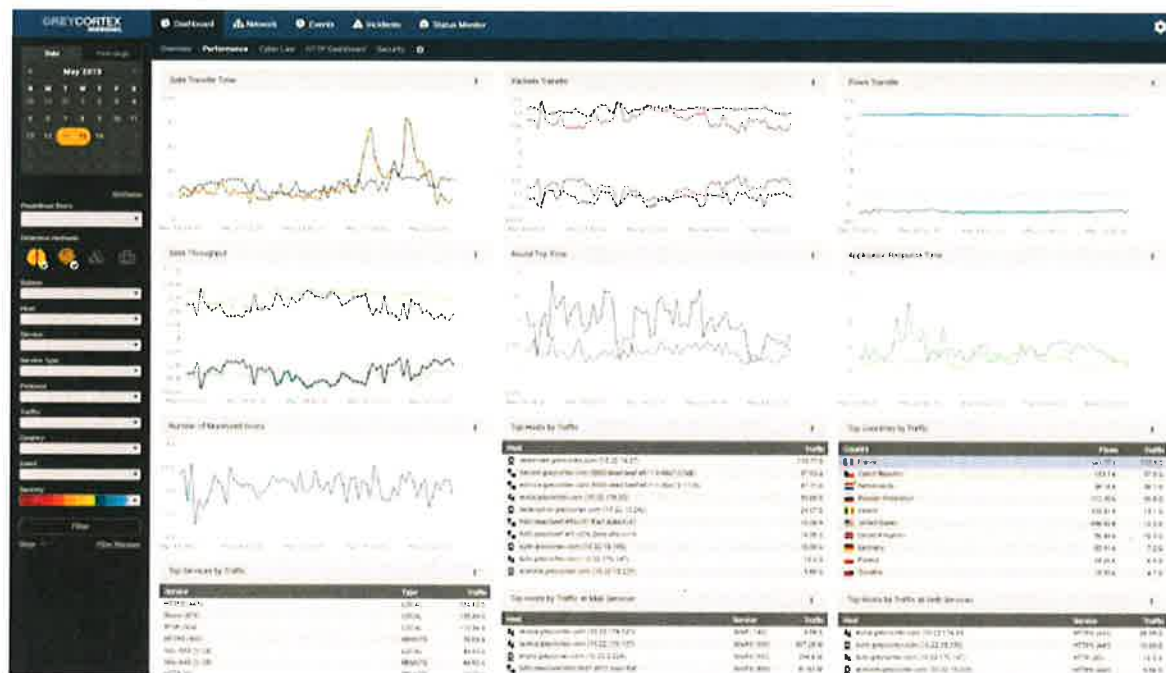
Obrázek 1: GUI s uživatelskými dashboardy

T

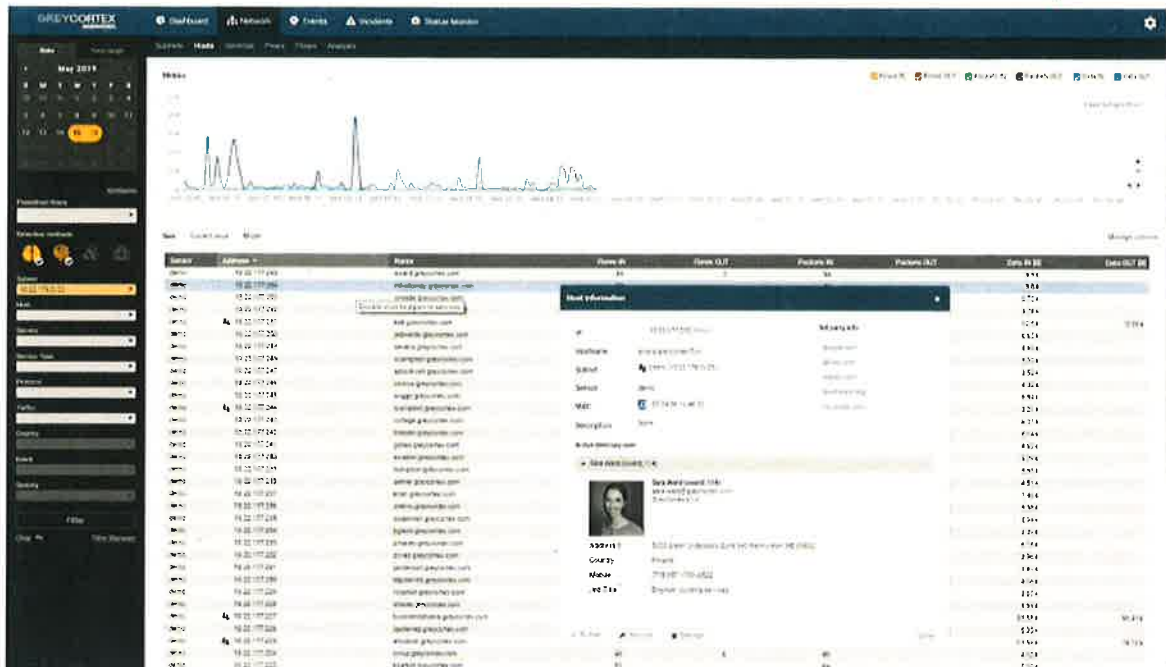




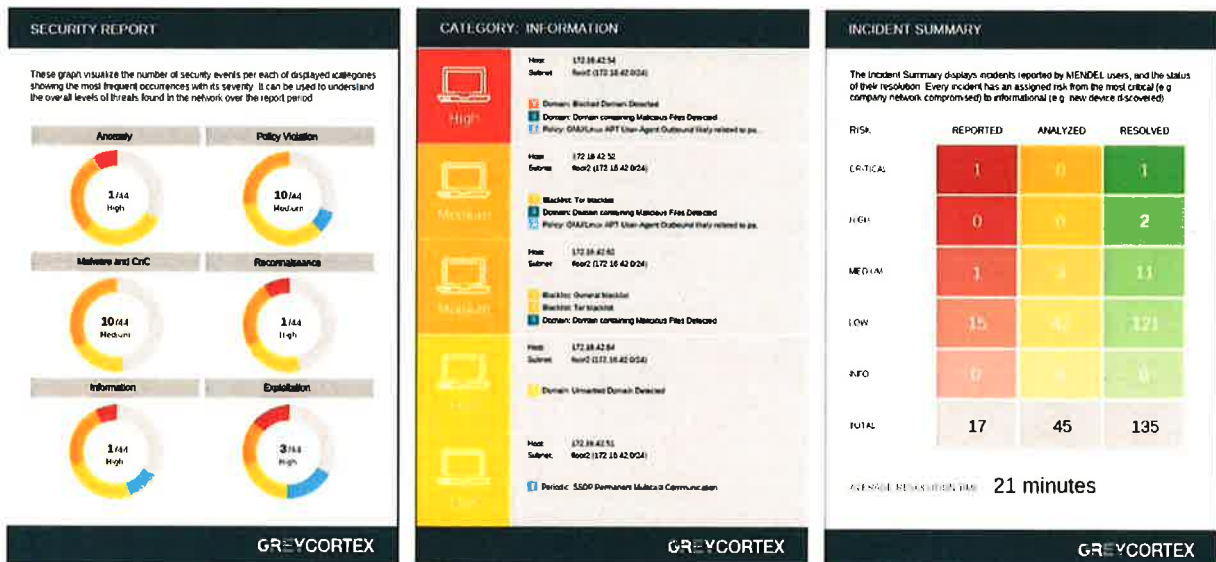
Obrázek 4: Uživatelské dashboardy



Obrázek 5: Uživatelské dashboardy



Obrázek 6: Přehled zařízení s aktivními uživateli



Obrázek 7: Ukázka automaticky generovaných reportů

Webové rozhraní aplikace se skládá z:

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

T



**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 síťových dat na úrovni celé sítě, jednotlivých podsítí, jednotlivých hostů a jejich služeb, vizualizace komunikačních partnerů, vizualizace síťových 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 úroveň vizualizace je výčet síťových toků, které stály za vznikem událostí. Součástí každé události je plná interpretace 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 základě 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 (čeština, polština, angličtina, korejština, čínština, japonština).

Aplikace umožňuje vytvářet:

- uživatelsky definované reporty a grafy 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.