Nabídka uchazeče: Greycortex			
Systém pro analýzu síťového provozu – obecné požadavky			**Plnění parametrů (Ano /Ne)**
1.	Systém složený z hardwarových zařízení musí monitorovat síťovou aktivitu v reálném čase a identifikovat potenciální kybernetické hrozby, bezpečnostní rizika a anomální chování a musí o nich v reálném čase vytvářet upozornění.		Ano
2.	Dodaný systém musí analyzovat síť na základě zrcadleného síťového provozu ze SPAN portů nebo TAPů (nikoliv jen na základě statistických protokolů typu NetFlow) a zároveň bez potřeby nasazovat agenty na koncové stanice nebo další zařízení v síti.		Ano
3.	Systém musí analyzovat obsah datových paketů v reálném čase a detekovat protokol nebo aplikaci na základě obsahu provozu prostřednictvím DPI (Deep Packet Inspection), nikoli pouze čísla portu.		Ano
4.	Dodaný systém musí být schopen analyzovat síť také na základě zpracování statistických protokolů typu NetFlow, IPFIX, NetStream, Cisco NSEL a případně dalších obdobných.		Ano
5.	Systém musí být plně funkční v offline prostředí objednatele bez využití cloudového prostředí pro sběr, ukládání a zpracování dat a veškeré konfigurace a reporting jsou k dispozici přímo v systému.		Ano
6.	Aktualizace systému musí být možné provádět uživatelsky v offline režimu.		Ano
Systém pro analýzu síťového provozu – zpracování a ukládání síťových toků			
7.	Systém ukládá síťové toky ve formátu, který umožní analýzu síťové komunikace na úrovni jednotlivých toků, včetně dohledání informací o aplikačních transakcích a jejich metadatech z L2 až L7, obsažených v daném síťovém toku.		Ano
8.	Požadované protokoly pro ukládání aplikačních metadat z jednotlivých transakcí jsou: DHCP, DNS, SMB, HTTP, HTTPS, SMTP, SMTPS, POP3, IMAP, SSH, LDAP, LDAPS, KERBEROS, SNMP, CIFS, MSSQL, RDP, SIP, TELNET, FTP, FTP-DATA, TFTP, TFTP-DATA, NFS, ARP, SSL/TLS zapouzdření.		Ano
9.	Je požadováno vysokorychlostní úložiště pro uchování historie datových toků minimálně 700 GB v technologii SSD.		Ano
10.	Analýza aplikačních a systémových logů		Ano
	Systém musí být schopen sbírat a analyzovat aplikační a systémové logy ve formátu syslog z dohledovaných zařízení a identifikovat nebezpečné nebo potenciálně škodlivé aktivity, jakož i obohatit data v systému o informace z nástrojů třetích stran (zejména identita uživatelů z logů v SIEMu nebo firewallu).		Ano
11.	Všechna data jsou uložena v relační databázi (nikoli souborovém systému), všechna pole a položky přijaté systémem jsou automaticky indexovány. Nad všemi položkami je možné ihned provádět vyhledávání bez nutnosti dodatečného ručního indexování administrátorem a výsledky hledání jsou k dispozici okamžitě, i když se vyhledává v časovém intervalu několika týdnů.		Ano
Systém pro analýzu síťového provozu – uživatelské rozhraní			
12.	Systém musí poskytovat jednotné grafické uživatelské rozhraní pro veškerou práci uživatelů, včetně všech detekcí, analýzy síťových statistik, nastavení systému, konfiguraci alertů, reportů a dashboardů.		Ano
13.1.	Systém musí být schopen vytváření profilů a skupin uživatelů pro omezení funkcionality produktu a viditelnosti uložených dat s podporou minimálně:	Granulárního nastavení přístupu k analytickým i konfiguračním/administrativním komponentám systému s definovanými úrovněmi přístupu (alespoň read, write, execute)	Ano
13.2.		Granulárního nastavení přístupu k datům z různých segmentů sítě organizace s definovanými úrovněmi přístupu (alespoň read, write, execute)	Ano
13.3.		Vytváření vlastních filtrů veškerých dat a jejich sdílení mezi uživateli a skupinami uživatelů	Ano
13.4.		Vytváření vlastních uživatelských pohledů, reportů, dashboardů apod.	Ano
Systém pro analýzu síťového provozu – automatické hlášení (alerty) a reporting			
14.	Systém musí být schopen upozorňovat uživatele prostřednictvím minimálně emailu a logu o všech identifikovaných událostech a dále o událostech filtrovaných minimálně dle IP a MAC adresy, podsítě, závažnosti události, kategorie události, země, uživatele, síťové služby, čísla portu, provozu do/z internetu.		Ano
15.	Tyto alerty musí být systém schopen dodávat i ve strojově čitelném formátu pro vyžití 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 systému.		Ano
16.	Systém musí mít možnost vytváření automatizovaných manažerských reportů o stavu kybernetické bezpečnosti z pohledu zprávy kybernetických incidentů ideálně dle oblastí jejich vzniků (např.: doména, web, email apod.).		Ano

17.	Je požadováno vytváření automatizovaných reportů v českém jazyce.		Ano
Systém pro analýzu síťového provozu – integrace systému			
18.1.	Systém musí poskytovat hotové nástroje umožňující integraci se softwarem třetích stran bez použití API systému, a to minimálně:	Syslog, CEF a LEEF pro export událostí včetně plné podpory filtrů (exportování pouze požadovaných dat)	Ano
18.2.		Přímé URL odkazy na libovolnou obrazovku grafického uživatelského rozhraní a filtrovaná zobrazení v grafickém uživatelském rozhraní	Ano
18.3.		Export informací o toku ve formátu IPFIX nebo podobném formátu včetně plné podpory filtrů (exportovat lze pouze požadovaná data)	Ano
18.4.		Integrace se službami identity uživatelů bez nutnosti konfigurace zasílání logů do systému Microsoft Active Directory	Ano
18.5.		Integrace s firewally pro automatické a manuální reakce vyvolané systémem	Ano
18.6.		Integrace s nástroji pro řízení přístupu k síti, pro automatickou a manuální reakci systému	Ano
Systém pro analýzu síťového provozu – podpora EDR			
19.	Systém musí poskytovat nástroje umožňující přímou integraci se softwarem EDR třetích stran pro získání informací a zkvalitnění detekce.		Ano
Architektura nasazení – obecné požadavky			
20.	Pro všechny HW komponenty senzor a kolektor je požadován formát 1U nebo 2U server o velikosti 19“.		Ano
21.	Pro všechny HW komponenty senzor a kolektor je požadován duální zdroj napájení se schopností hot-swap.		Ano
22.	Pro všechny HW komponenty senzor a kolektor je požadováno samostatné síťové rozhraní pro vzdálenou správu serveru v případě výpadku systému typu IPMI, IDRAC, ILO apod.		Ano
Architektura nasazení –požadavky pro pokrytí IT prostředí			
23.1.	Je požadován 1x HW zařízení, které kombinuje datový kolektor a sensor o minimální celkové schopnosti zpracovat 0,5 Gbps průměrného provozu pro alespoň 1500 monitorovaných IP adres.		Ano
	Monitorovací rozhraní jsou požadována minimálně 4x1GbE a 2x10/25GbE optická, vč. kompatibilních SFP modulů.		Ano
	Na zařízení je požadována dostupná historie dat uložená na rychlém úložišti o čisté velikosti alespoň 700 GB s technologií SSD a RAID1.		Ano
Schopnost detekce bezpečnostních událostí – monitorování zařízení, segmentů sítě a využívaných síťových služeb			
24.1.	Dodaný systém musí identifikovat všechna zařízení připojená	Změna IP/MAC adresy hosta	Ano
24.2.		Duplicitní IP/MAC adresa	Ano
24.3.		Změna VLAN	Ano
24.4.		Vytvoření nové podsítě	Ano

24.5.	Součástí systému musí identifikovat všechna zařízení připojená do sítě včetně koncových zařízení, serverů, IoT zařízení apod. Zároveň musí být systém schopen identifikovat změny v síti – minimálně:	Připojení nového zařízení	Ano
24.6.		Použití nebo vznik nové služby	Ano
24.7.		Nedostupnost dříve dostupné a komunikující služby nebo dříve dostupného a komunikujícího zařízení	Ano
24.8.		Přístup nového zařízení ke službě či zařízení	Ano
24.9.		Ověřování platnosti interních certifikátu pro validní TLS šifrování u HTTPS a upozornění před datem jejich vypršení	Ano
25.	Systém musí uživateli umožnit pomocí těchto detekčních metod nastavovat bezpečnostní politiky pro různé segmenty sítě a pro různá zařízení a na porušení těchto politik reagovat upozorněním.		Ano
Schopnost detekce bezpečnostních událostí – samostatné učení behaviorálních aktivit a detekce anomálií			
26.	Systém musí používat matematické metody samostatného učení pro analýzu síťové aktivity, vytvářet a v čase automaticky modifikovat modely chování na základě běžného chování jednotlivých zařízení a na nich provozovaných služeb v rámci celé organizace.		Ano
27.1.	Systém musí mít schopnost na základě matematického modelu daného zařízení a jeho služeb identifikovat nestandardní síťové chování, a to zejména odchylky od modelu normálního chování pro:	Odchylku od modelu pro přenos dat, toků a paketů	Ano
27.2.		Odchylku od modelu pro počet komunikačních partnerů	Ano
27.3.		Odchylku od modelu entropie na komunikačních portech	Ano
27.4.		Odchylku od modelu pro počet síťových toků a využitých síťových služeb	Ano
27.5.		Odchylku od modelu výkonnosti sítě (rychlost přenosu) a aplikací (doba odezvy)	Ano
28.	Samostatné učení je požadováno na všech síťových zařízeních a na nich provozovaných službách (port číslo 0 až 65535 u TCP i UDP) na IPv4 a IPv6 a dalších protokolech L3 a L4 síťové vrstvy.		Ano
Schopnost detekce bezpečnostních událostí – identifikace neznámých hrozeb a podezřelých chování			
29.1.	Systém musí být schopen detekovat neznámé hrozby, které nelze identifikovat prostřednictvím detekčních signatur, jako jsou trojské koně, botnety apod. Zejména musí být identifikovány tyto příznaky potenciálně škodlivého chování:	Průzkumné aktivity v síti	Ano
29.2.		Detekce podezřelého strojového chování, které nevytvářejí lidští uživatelé sítě	Ano
29.3.		Detekce repetitivních vzorců chování na síti	Ano
29.4.		Detekce botnetů a ovládání kompromitované stanice	Ano
29.5.		Detekce příznaků těžení kryptoměn	Ano
29.6.		Útoky hrubou silou a enumerace dat	Ano
29.7.		Rozpoznání tunelovaného síťového provozu – alespoň IPv4 prostřednictvím IPv6 a DNS tunely	Ano
Schopnost detekce bezpečnostních událostí – detekce na základě databáze známých hrozeb			

30.1.	Systém musí být schopen identifikovat hrozby a reportovat události na základě:	Detekční databáze známých hrozeb, tj. malware (trojské koně, viry, červy, rootkity, apod.), známých útoků (exploity) a zranitelností, porušení bezpečnostních pravidel a „best practices“ a dalších rizik	Ano
30.2.		Reputační databáze známých škodlivých IP adres, TLS certifikátů, záznamů DNS a hostname, URL adres a hashů souborů	Ano
31.	Tyto databáze musí být aktualizované minimálně na hodinové bázi. Nesmí se jednat pouze o volně dostupné/open-source databáze, ale musí se jednat o komerční databázi renomovaného vendora nebo poskytovatele těchto služeb.		Ano
32.	Uživatel musí být schopen importovat vlastní záznamy.		Ano
33.	Systém musí využívat tuto detekci pro veškerý monitorovaný provoz (na perimetru i v interní síti mezi všemi segmenty), nikoliv pouze pro omezený segment nebo podmnožinu celkové komunikace.		Ano
34.	Databáze detekčních pravidel (signatur) musí být založena na pokročilých regulárních výrazech pro zpracování řetězců, které dokáží provádět inspekci veškeré síťové komunikace od L2 (Ethernet apod.) po L7. Systém musí detekovat události na základě vysokého počtu signaturních pravidel (minimálně několik desítek tisíc).		Ano
	Systém musí umoňovat centrální správu detekčních pravidel z jednoho místa pro všechny senzory.		Ano
35.	Uživatel musí být schopen přidávat vlastní detekční pravidla v praktickém a obecně využívaném formátu, prostřednictvím grafického rozhraní s průvodcem (wizard), nikoliv jen textovou řádkou.		Ano
	Příklad možné syntaxe detekčního pravidla:		Ano
	alert tcp $HOME_NET any -> any any (msg:“Command Shell Access”; content:“C:\\Users\\Administrator\\Desktop\\hfs2.3b”; sid:1000001; rev:1;)		Ano
36.	Analýza šifrované komunikace		Ano
	Vedle samostatného učení musí systém používat další metody pro analýzu šifrované komunikace, minimálně TLS fingerprinting a s ní spojenou detekci známých hrozeb.		Ano
Schopnost detekce bezpečnostních událostí – asistované učení			
37.1.	Je požadován uživatelsky přívětivý proces vytváření pravidel pro zpřesnění detekce a eliminaci falešně pozitivní detekce, a to na základě minimálně následujících parametrů:	IP adresa	Ano
37.2.		MAC adresa	Ano
37.3.		Hostname	Ano
37.4.		Segment sítě / podsíť	Ano
37.5.		Lokalita – ASN, země, apod.	Ano
37.6.		Směr komunikace – určení klienta, nebo serveru	Ano
37.7.		Detekovaná událost – kategorie, název apod.	Ano
37.8.		Použité služby, protokolu, portu	Ano
37.9.		Libovolné kombinaci výše popsaných	Ano
38.	Systém musí být schopen eliminovat falešné alarmy i pro události detekované v historii.		Ano

Požadavky na zajištění síťové viditelnosti – vyhledávání, filtrování a vizualizace dat			
39.	Systém musí být schopen okamžitého (v řádu vteřin) vyhledávání a vizualizace pro forenzní analýzu a podporu threat hunting bez zvláštního dotazovacího jazyka.		Ano
40.1.	Jedná se o možnost okamžitě filtrovat a vyhledávat v plné historii všech uložených dat, tj. bezpečnostních událostí, síťových toků a agregovaných síťových statistikách (tabulky a grafy), a to minimálně:	Podle parametrů IP a MAC adresa, hostname, username (identita uživatele), příchozí a odchozí provoz, síťová služba, lokální nebo vzdálená služba (služba z pohledu klient nebo server), číslo portu, VLAN, země, ASN	Ano
40.2.		Prostřednictvím full-textového vyhledávání v datech a vyhledávání na základě definice směru (zdroj, cíl) a logických výrazů and, or, not	Ano
41.	Systém musí pro vyhledávání poskytovat již předpočítané hodnoty výkonnostních a behaviorálních charakteristik pro každé zařízení v síti a pro všechny na něm provozované služby, bez nutnosti zpracování surových dat ze síťových logů.		Ano
42.	Systém musí být schopen filtrovat a vizualizovat výsledky v grafech, výčtových tabulkách s možností řazení a TOP N statistikách.		Ano
43.	Systém 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, RDP, ARP, MS-SQL, SIP, Kerberos, SSL/TLS.		Ano
	Metadata jsou v tomto případě chápána jako přenášená aplikační metadata nebo vlastní data servisních protokolů. U protokolu HTTP například http hlavička s metodou, URI, host, user-agent, cookies apod. V odpovědi pak návratový kód a další http parametry.		Ano
44.	Systém umožnuje provádět uživatelsky jednoduché a okamžité vizualizace síťových prostupů mezi zařízeními a podsítěmi. Využitím uživatelského datového filtru lze vizualizační pohledy libovolně modifikovat.		Ano
45.	Zaznamenávání a ukládání plného provozu		Ano
	Je požadováno volitelné nahrávání plného síťového provozu (full packet capture) ve formátu PCAP na všech dodaných zařízeních minimálně na základě parametrů: cílová a zdrojová IP/MAC adresa, podsíť, využitý protokol, IPv4 nebo IPv6. Zaznamenávání je možno zapínat automaticky dle detekovaných událostí, nebo uživatelskou aktivací.		Ano
Monitorování politik kybernetické bezpečnosti			
48.1.	Systém musí umožňovat vytváření komplexních komunikačních a bezpečnostních politik, a to minimálně:	Monitorovat definovanou komunikační matici a detekovat, kdy jsou tyto matice porušeny – alespoň jaké zařízení smí komunikovat s jakým zařízením, přes jaký protokol, v jakém čase.	Ano
48.2.		Detekce změn v síti – přinejmenším nové komunikační vektory, nová nebo změněná zařízení a podsítě, obcházení perimetru.	Ano
49.1.	Pro účely monitorování politik kybernetické bezpečnosti musí systém poskytovat uživatelský rámec pro definování pravidel pomocí:	Uživatelem definované podsítě na základě rozsahů IP adres	Ano
49.2.		Uživatelsky libovolně definovaných skupin zařízení	Ano
49.3.		Automaticky přiřazené značky/tagu zařízení, které popisují jejich účel a chování – alespoň server doménového řadiče, webový server, poštovní server, server DNS, server SSH, databázový server, tiskárna, administrátorské zařízení, datové úložiště, aktivní dohledy, skenery zranitelností a technologické systémy	Ano
Management bezpečnostních událostí a incidentů			
50.1.	Systém musí poskytovat funkcionalitu pro reporting bezpečnostních incidentů (prohlášení identifikované události za bezpečnostní incident), včetně:	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	Ano
50.2.		Jednoduché sdílení informací o bezpečnostních incidentech, včetně uživatelem zadaných komentářů	Ano
50.3.		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.)	Ano
50.4.		Možnost exportování dat do emailu, csv, pdf, syslogu a podobně	Ano
50.5.		Možnost exportu bezpečnostních událostí a incidentů do systémů typu ticket management třetích stran	Ano

Detekce úniku dat			
51.	Systém musí být schopen detekovat přenosy citlivých souborů a dat definovaných pomocí jejich názvů, hashů, specifického binárního obsahu (vodoznaku) nebo regulárních výrazů (např. rodné číslo).		Ano
52.	Systém musí být schopen detekovat přenosy citlivých souborů a dat alespoň u následujících protokolů: HTTP, FTP, SMTP, SMB, NFS.		Ano
53.1.	V rámci historických metadat u HTTP, FTP, SMTP, SMB a NFS je požadováno ukládání informací o všech po síti přenášených souborech alespoň v rozsahu:	Název souboru	Ano
53.2.		Velikost souboru	Ano
53.3.		HASH souboru	Ano
Monitoring výkonu aplikací a sítě			
54.1.	Systém v celé monitorované síti, mezi všemi zařízeními a na všech službách měří a vytváří automaticky (bez nutnosti nastavovat manuálně limitní hodnoty) model normálního chování pro výkonnostní parametry minimálně:	Přenosová rychlost sítě	Ano
54.2.		Rychlost odezvy aplikace	Ano
54.3.		Odezva systému z pohledu uživatele	Ano
55.1.	Výpočet uvedených výkonnostních parametrů a automatické detekce anomálií na základě odchylky od modelu normálního chování musí být prováděna pro:	Všechny porty a služby TCP	Ano
55.2.		Pro všechny kombinace služeb a zařízení	Ano
56.	Systém musí v celé monitorované síti, mezi všemi zařízeními a na všech službách měřit informace o retransmission paketech, out of order paketech, TTL, QoS a komunikaci blokované firewally.		Ano
Monitoring cloudových služeb			
57.	Systém musí být schopen monitorovat přístupy zařízení a uživatelů ke cloudovým službám, a to minimálně Google Workspace a Microsoft Office 365, vč. monitoringu operací se soubory, změn oprávnění a nastavení a neúspěšných přístupů.		Ano
58.	Systém musí být schopen tyto informace autonomně a průběžně získávat z aplikačních rozhraní těchto cloudových služeb bez nutnosti využití řešení třetích stran.		Ano
Inventarizace sítě a grafická vizualizace topologie			
59.	Systém musí být schopen zobrazit celý inventář monitorované sítě s počtem zařízení v jednotlivých lokalitách, segmentech, nebo podsítích. Včetně detailního přehledu zařízení.		Ano
60.	Systém musí být schopen graficky vykreslit celou topologii sítě, dle zaznamenané komunikace.		Ano
61.	Systém musí být schopen zobrazit inventář jednotlivých lokalit, přehledy zařízení, přehledy výrobců, tagy zřízení, uživatele.		Ano
62.	Systém umožnuje všechny inventory informace řadit dle různých parametrů.		Ano
Podpora výrobce			
63.	Součástí nabídky dodavatele bude vyjma zajištění instalace, zprovoznění nabízeného řešení, podpora výrobce na 60 měsíců.		Ano