Příloha č. 6 Zadávací dokumentace
Příloha A smlouvy

Požadavky na technické řešení

1 Popis celkového řešení

Národní centrum kybernetické bezpečnosti (dále jen *„NCKB“*) buduje se zapojenými partnerskými organizacemi (dále také jako *„Partneři“*) Systém sledování provozu a detekce bezpečnostních událostí (dále jen *„Systém“*) s cílem **zvýšit pravděpodobnost detekce pokročilých kybernetických útoků a bezpečnostně nežádoucího chování**. Toto výběrové řízení je jen jednou z částí celkového řešení.

V rámci Systému budou Partneři s vládním pracovištěm GovCERT.CZ, které je součástí NCKB, sdílet

- nezpracované údaje o síťovém provozu z perimetru jejich sítě,
- vybrané detekované bezpečnostní události z jejich sítě.

NCKB bude výše uvedené údaje od Partnerů a z externích informačních zdrojů automaticky i manuálně zpracovávat a vzájemně korelovat, což umožní upozornit i na události, které by v rámci jedné organizace nebyly vyhodnoceny jako nežádoucí.

Partneři nebudou s NCKB sdílet ani lokální detailní aktivitu, ani obsah komunikace uživatelů ve své vnitřní síti. Všechny dodatečné prvky informační infrastruktury instalované v rámci Systému v sítích Partnerů budou v plné správě jejich pracovníků kybernetické bezpečnosti.

NCKB následně poskytne zapojeným partnerským organizacím aktualizace, které jim pomohou lépe identifikovat hrozby v jejich sítích. Hrozbami, proti kterým je Systém detekce namířen, jsou především:

- DoS/DDoS útoky,
- zapojení do BOTNET sítí,
- komunikace do sítí a na adresy se špatnou reputací,
- malware,
- skenování sítě,
- brute-force pokusy o prolomení autentizace u služeb nabízených sítí.

Pro zapojené partnerské organizace tak bude mít Systém dvojí význam:

- zvýší bezpečnost sítě,
- umožní splnit část požadavků kladených zákonem č. 181/2014 Sb., o kybernetické bezpečnosti, konkrétně technická opatření „nástroj pro detekci kybernetických bezpečnostních událostí“ a „nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí“.

Systém má dvě hlavní části, které jsou soutěženy v rámci samostatných výběrových řízení (VŘ):

- **Samostatné systémy sběru síťových dat a detekce anomálií**, nasazené v rámci zapojených partnerských organizací s integrací do centrály GovCERT.CZ. Tato část *NENÍ* součástí tohoto výběrového řízení.
- **Analytický systém**, který bude zpracovávat bezpečnostní události a síťové toky z jednotlivých partnerských organizací. **Tato část *JE* předmětem tohoto VŘ.**

Přibližné vizuální zobrazení poptávaného řešení je v Příloze G smlouvy – Nákres celkové architektury systému.

2 Vstupní data pro Analytický systém

Poptávaný Analytický systém musí umožnit plnohodnotnou práci se všemi druhy dat, popsanými v této kapitole. Není-li stanoveno jinak, označuje termín *„data“* všechny druhy popsané v této kapitole.

2.1 NetFlow/IPFIX data

Analytický systém bude zpracovávat data o síťovém provozu NetFlow/IPFIX, včetně následujících doplňujících informací z vrstvy L7:

http-metoda,
http-user-agent,
http-hostname,
http-url,
DNS requests,
detaily protokolu SMB.

V celé zadávací dokumentaci jsou tedy termínem *„NetFlow/IPFIX“* míněna data obohacená o L7 data uvedená výše. NetFlow data budou přicházet z perimetrů sítí Partnerů přes bezpečný přípojný bod ve formátu IPFIX podle IETF RFC7011. Analytický systém musí NetFlow/IPFIX data:

- umět zpracovat minimálně 6 měsíců zpětně (přičemž maximální taková kapacita datového úložiště je 50TB),
- licenčně umožnit retenci dat po dobu minimálně 6 měsíců.

2.2 Kybernetické bezpečnostní události

Přesný formát včetně jednotlivých datových polí zasílaných kybernetických bezpečnostních událostí bude znám až po skončení druhého výběrového řízení na Samostatné systémy sběru síťových dat a detekce anomálií. Zadavatel proto požaduje 50 mandays na integraci, které jsou součástí poptávkové ceny.

Bezpečnostní události detekované v sítích Partnerů

Půjde o události detekované Samostatnými systémy sběru síťových dat a detekce anomálií umístěnými v ICT infrastruktuře Partnerů, které jsou předmětem jiného výběrového řízení. Tyto systémy budou v sítích Partnerů mimo jiné provádět síťovou behaviorální analýzu (NBA) sloužící k vyhodnocování NetFlow/IPFIX statistik a následné detekci útoků a anomálií. Někteří Partneři budou data o síťovém provozu nejdříve integrovat do svého SIEM řešení, a teprve poté ze SIEM předávat vládnímu pracovišti GovCERT.CZ.

Události detekované v sítích Partnerů tak mohou přicházet jak z analytického modulu kolektoru sondy, tak ze SIEMu, vždy však přes bezpečný přípojný bod ve formátu syslog. Událostí musí být z Analytického systému exportovatelné zejména ve formátech

syslog,
CSV,

případně dalších.

Bezpečnostní události detekované Analytickým systémem

Půjde o události detekované až Analytickým systémem v rámci infrastruktury GovCERT.CZ. Událostí musí být z Analytického systému exportovatelné zejména ve formátech

syslog,
CSV,

případně dalších.

2.3 Blacklistované IP adresy / domény

Blacklistované IP adresy/domény budou sdíleny do databáze hrozeb – ThreatDB, kterou bude vládní pracoviště GovCERT.CZ sdílet se svými partnery. Dodavatel Analytického systému po dokončení Threat DB serveru, který je předmětem jiného výběrového řízení, připraví v rámci fáze II. napojení na tento server.

Analytický systém musí umožnit přiřadit ke každé IP adrese/doméně v ThreatDB další libovolné údaje, zejména:

who is údaje,
geo ip,
CIDR,
AS systém,
uživatelské tagy,
komentář.

2.4 Signatury útoků

Signatury útoků budou sdíleny do databáze hrozeb – ThreatDB, kterou bude vládní pracoviště GovCERT.CZ sdílet se svými partnery. Signatura je pro účely poptávaného systému definována jako souhrn informací identifikující hrozbu, zejména:

IP adresa,
doména,
TCP flagy,
URL,
user agent,
libovolná kombinace položek z NetFlow/IPFIX.

2.5 Napojení na jiné samostatné systémy sběru síťových dat a detekce anomálií

V rámci paralelně soutěžené dodávky samostatných systémů pro sběr síťových dat a detekci anomálií s názvem *„Technologie sledování síťového provozu“* bude do infrastruktury GovCERT.CZ vítězný dodavatel instalovat bezpečný přípojný bod a zajistí:

- přeposílání NefFlow/IPFIX záznamů ze systémů mimo ICT infrastrukturu NBÚ na zadanou IP adresu v rámci GovCERT.CZ,
- přeposílání syslog ze systémů mimo ICT infrastrukturu NBÚ na zadanou IP adresu v rámci GovCERT.CZ.

Analytický systém zajistí bezproblémový příjem Neflow/IPFIX a syslog na definovaných IP adresách a portech a

jejich následné zpracování.

3 Popis funkcí Analytického systému

Analytický systém bude nasazen v rámci infrastruktury NCKB. Musí disponovat nativními SIEM funkcionalitami, tedy schopností parsovat a normalizovat příchozích data z různých informačních zdrojů a v různých formátech, dále je obohacovat (enrichment) o jiná data z různých informačních zdrojů, na základě uživatelem určených pravidel je agregovat, analyzovat a nalézat v nich souvislosti a výsledky v předem dané struktuře předat dalším částem celkového řešení.

Analytický systém musí být schopen zpracovávat všechny druhy dat popsané v předchozí sekci. **Zadavatel požaduje, aby měl jednotné grafické rozhraní (webové GUI),** přístupné pomocí HTTPS s autentizací do všech svých komponent pomocí AD/LDAP. Funkcionality GUI jsou rozděleny do skupin z uživatelského hlediska. Celkové řešení musí být dodáno jako jeden integrální systém, ne jako funkční kombinace více oddělených modulů a/nebo systémů od různých výrobců.

GUI musí umožnit provádění funkcí, které lze shrnout do následujících podskupin:

- procházení dat,
- vizualizace dat,
- tvorba reportů,
- pokročilá práce s daty:
  - korelace,
  - detekce anomálií (NBA),
  - vytváření signatur a další funcionality „typu SIEM“,
- příprava alertů a zakládání ticketů pro Request Tracker, ticketovací systém GovCERT.CZ,
- správa zdrojů dat, zejména jejich automatické odmazávání.

3.1 Procházení dat

Modul slouží pro uživatelsky přívětivé procházení a zobrazování zdrojových dat. Modul musí umožnit tyto funkce:

Vyhledávání a agregace

Vyhledávání a agregace dat je předpokládána dle libovolného pole v datech obsažených, zejména však dle:

- zdrojové IP adresy,
- cílové IP adresy,
- zdrojového portu,
- cílového portu,
- domény,
- zadaného časového okna,
- CIDR,
- ASN,
- země,
- geoip,

- portu,
- vlastníka,
- abuse kontaktu,
- údaje, kdy byla IP adresa poprvé viděna v některé z externích databází (přes Intel MQ) nebo interních databází připojených do Analytického systému
- všechny informace dostupné ke konkrétní IP adrese/doméně dohledatelné mezi všemi daty systémem zpracovávanými (příslušnost do blacklistu/whitelistu, údaje z Threat DB, související bezp. události),
- interní informace ze systémů vládního CERT,
- tagů (přidělených v Analytickém systému),
- textu v komentářích (přidělených v Analytickém systému).

Komentář [A1]: vymazáno

vyhledané a agregované skupiny jsou následně základem pro další funkce a tvorbu reportů. Zadavatel nechává na Uchazeči, jakým způsobem navrhne způsob práce. Například lze vyhledané seznamy ukládat a pak s nimi dále pracovat nebo vše dělat dynamicky vkládáním podmínek.

Drill-down analýza

Drill down analýza umožní rozpad zvolených ukazatelů do většího detailu jedním proklikem a tedy postup od obecnějších informací k detailnějším s využitím minimálního počtu kroků.

Tagování a komentáře

Data lze opatřit libovolnými tagy, a to:

ručně,
automaticky na základě definovaných pravidel, a to i do minulosti.

Následně je možné podle těchto tagů záznamy přeskupovat a vyhledávat v nich. Jeden záznam může být opatřen více tagy zároveň. Předpokládá se použití krátkých názvů.

Data lze opatřit libovolnými komentáři. Následně je možné fulltextově vyhledávat podle textu v komentářích. Oproti tagům se v komentářích předpokládají delší texty.

3.2 Vizualizace dat

Modul slouží pro grafické a tabulkové zobrazení zdrojových nebo vyhledaných (filtrovaných) dat. Vizualizace je požadována zejména nad:

surovými NetFlow/IPFIX záznamy,
kybernetickými bezpečnostními událostmi.

Základní požadavky jsou:

- různé typy vizualizací dat, zejména síťový provoz za daný čas, vztahové vazby mezi IP, atp. s možností úpravy stávajících a tvorby nových,
- podpora agregované vizualizace (např. komunikace jednotlivých organizací mezi výchozími uzly),
- vizualizace na základě geografických dat dané IP (zobrazení na mapě světa),
- vizualizace pouze *„detekovaných útoků“*, tj. takových, které byly vytvořeny až v Analytickém systému ze zaslaných NetFlow/IPFIX dat,
- možnost drill down do detailních dat,

- možnost filtrace dat v sestavách (podle jednotlivých parametrů NetFlow),
- filtrování výsledků s pomocí ohraničení časového okna, kde čas se zadává ve tvaru DD-MM-YYYY HH:MM:SSS – dvě pole, *„od“* a *„do“*,
- pro filtraci využívat syntaxe vycházející z některých široce používaných nástrojů (např. syntaxe nfdump nebo wireshark),
- ve filtrech umožnit použití regulárních výrazů,
- proklik mezi vytvořenou událostí (korelovaný alert) a odpovídajícím NetFlow/událostí (zaslanou z instituce) a naopak,
- vytvářet časové řady průběhu provozu s možností filtrace (například spojení na jednu konkrétní IP adresu) a tyto vizualizovat formou časových grafů.

Požadované typy diagramů a grafů, které tento modul dokáže vykreslit již v rámci základní dodávky:

Sankeyův diagram

Také *„Sankey diagram/Re-usable Sankey“* diagram znázorňující tok dat, reprezentovaných šipkami. Šipky jsou odlišeny jak směrově, tak svou tloušťkou, která odpovídá objemu dat nebo jiné zvolené metrice.

Chord diagram

Kruhový diagram, na jehož obvod jsou vynesena zkoumaná data či kategorie, a v jehož středu jsou znázorněny jejich vzájemné vztahy. Zadavatel požaduje Chord diagram s možností vizuálního zjednodušení v případech přílišného počtu vazeb (metoda Hierarchical Edge Bundling).

Sequences sunburst

Kruhový diagram, od středu k okraji postupně rozkládající zkoumanou množinu dat podle společných charakteristik.

SPI graph po vzoru Moloch

Časový graf zobrazující výskyty a počty výskytů dané položky. Jako položky jsou brány jednotlivé elementy obsažené ve flow nebo události:

zdrojová/cílová ip
zdrojový/cílový port
protokol
doménové jméno
http url
typ události

a další pole ze zaslaných dat. Funkce:

dynamické vytváření vlastního grafu pro každou položku,
možnost specifikovat kolik maximálně bude vytvořeno grafů,
zobrazit výskyt vybraných položek v čase (časové diagramy),

viz http://molo.ch.

Graf spojení (NetFlow i události)

Graf vytvářející síť komunikujících stran podle zadaných parametrů kdy možnosti jsou:

- zdrojová_ip -> cílová_ip,
- zdrojová_ip -> cílová_ip:cílový_port,
- zdrojová_ip:zdrojový_port -> cílová_ip,
- zdrojová_ip:zdrojový_port -> cílová_ip:cílový_port,
- výše uvedené, kdy je ip adresa nahrazena doménou, např.:
  - doména -> doména,
  - zdrojová_ip -> doména,
- spojnice má svoji šířku přizpůsobenou podle množství komunikace a to podle volitelného kriteria:
  - počet spojení,
  - počet paketů celkem,
  - počet přenesených bytů,
- barevné nebo jiné odlišení zdroje a cíle komunikace (klient vs. server),
- logické seskupování uzlů, aby vytvářely *"ostrůvky"* vzájemných spojení:
  - lepší orientace v tom, které uzly mají spojitost s ostatními,
  - minimalizace křížení hran,
- možnost pohybovat s libovolným uzlem (a po přesunutí tam uzel zůstane) a zpřehlednit tak vizualizaci,
- zobrazování TOP uzlů podle počtu:
  - spojení,
  - přenesených paketů,
  - přenesených bytů,
  - případně dalších statistických polí,
- zobrazování posledních X spojení:
  - hodnota X volitelná v řádech stovek, tisíců a více podle výkonnosti HW na kterém řešení poběží,
  - možnost specifikovat minimální počet spojení s uzlem, aby byl do zobrazení zařazen po najetí/kliknutí na uzel zobrazení detailních informací (bráno z uzlu do všech ostatních kam komunikoval):
    - ip,
    - port,
    - počet spojení,
    - počet bytů přesenených celkem, odeslané, přijaté,
    - počet paketů,
    - zda jde o zdroj nebo cíl komunikace,
    - další využitelná pole ze zaslaných dat,
  - po najetí/kliknutí na hranu zobrazení detailních informací (bráno mezi danou dvojicí uzlů):
    - zdrojová ip,
    - cílová ip,
    - porty,
    - počet spojení,
    - počet bytů přesenených celkem, odeslané, přijaté,
    - počet paketů,

        - další využitelná pole ze zaslaných dat,
    - kliknutí pravým talčítkem (na uzel nebo hranu) nebo jiné vhodné zobrazení dalších možností:
        - možnost odfiltrovat daný uzel/hranu ze zobrazení,
        - přidání daného uzlu/hrany do filtru zobrazované komunikace,
        - ponechání pouze daného uzlu s jeho spojeními,
        - přejití na detail daných komunikací z uzlu/mezi uzly,
        - výpis daných NetFlow záznamů (pokud půjde o vizualizaci NetFlow dat) a možnost drill-down analýzy.

SPI View

Tedy obecný souhrn informací uvedených v NetFlow/událostech (počty i procentuelně) podobně jako SPI View:

- zastoupení jednotlivých protokolů,
- výskyt jednotlivých IP,
- využití jednotlivých portů,
- doménové názvy,
- hodnoty z certifikátu,

a další pole ze zaslaných dat. Viz http://molo.ch.

NFSEN

Tedy statistický přehled podobně jako nfsen:

- časové grafy využití sítě (filtr IP/CIDR/ASN) z pohledu počtu spojení/přenesných bajtů a paketů,
- možnost vracet se v historii (zadání času od-do, specifikace zadání času viz výše).

IP/CIDR

Tedy statistický přehled k IP/CIDR podobně jako ntopng (konkrétní IP) / Kibana. Přehled zejména:

- komunikujících IP adres (zdrojových, cílových),
- portů (zdrojových, cílových),
- domén na které zdrojové IP (adresy úřadů) komunikovaly,
- URL na které zdrojové IP (adresy úřadů) přistupovaly,
- poměru protokolů (L4 i L7).

Vynesení na mapu

Statistický přehled na geografické mapě (světa/ČR a jednotlivých kontinentů), agregované zobrazení spojení IP/CIDR/ASN podle GeoIP.

Vizualizace kyber. bezpečnostních událostí a incidentů

Vizuální odlišení a prezentace dat kybernetických bezpečnostních událostí a incidentů podle

- času – systém bude schopen pro vybranou událost nebo incident zobrazit timeline – časovou linku, kde bude přehledně zobrazeno datum jejího přijetí od Partnerů nebo jejího vytvoření operátorem GovCERT.CZ, datum změny z kybernetické bezpečnostní události na incident nebo naopak, data přidávání tagů, komentářů a dalších operací, které se k události nebo incidentu váží,
- ICT infrastruktury, ve které byla událost detekována – ze zobrazení bude jasně patrný podíl událostí jednotlivých sítí Partnerů na celkovém počtu událostí,
- volitelně i dalších kritérií a datových polí.

3.3 Tvorba reportů

Modul slouží pro zobrazení na obrazovce a následný export zdrojových dat, používaných ve vizualizacích. Zadavatel předpokládá úroveň standardních funkcionalit zavedených systémů pro reporting (např. IBM Cognos, Microsoft BI, BIRT, GoodData, Hyperion a další). Předpokládané základní funkcionality jsou:

zobrazení výsledků uvedených vizualizací ve formě zdrojových dat, ze kterých byly grafy a vizualizace vytvářeny,
v závislosti na typu vizualizace jsou do reportu zahrnuty zdrojová data NetFlow/IPFIX a/nebo bezpečnostní události,
vytváření reportu ve formě tabulky nebo jiného vhodného formátu přímo v prostředí společného GUI,
možnost zobrazovaný výsledek exportovat ve formátu CSV (nebo i jiném dalším vhodném) pro následné strojové zpracování.

3.4 Pokročilá práce s daty

V rámci všech pokročilých operací s daty popsaných v této kapitole musí Analytický systém v případě *„false-positive“* detekce vytvořit whitelist podle IP adresy, domény, portu a jejich libovolné kombinace.

Všechna nově vytvořená detekční pravidla musí být zpětně aplikovatelná i na historické události.

Korelace dat v úložišti kybernetických bezpečnostních událostí

Analytický systém bude přijímat a automaticky vyhodnocovat kybernetické bezpečnostní události popsané v sekci 2.2 Kybernetické bezpečnostní události, tedy

příchozí bezpečnostní události zaslané partnerskými organizacemi ve formátu syslog,
bezpečnostní události detekované Analytickým systémem v NetFlow/IPFIX datech.

Systém musí zejména umožnit:

zpracování kybernetických bezpečnostních událostí v rozsahu minimálně 2500 EPS (událostí za sekundu), rozšiřitelných až do 5000 EPS (tento limit se týká pouze kybernetických bezpečnostních událostí, limit pro NetFlow údaje je uveden dále v textu),
detekovat konkrétní události zadanou operátorem na základě stanovených kritérií (např. IP adresy, portu nebo jiných datových polí),
detekovat konkrétní hodnotu nebo textový řetězec v rámci události,
detekovat posloupnost událostí, tedy časovou souslednost jednotlivých bezpečnostních událostí (příklad souslednosti: nejdříve proběhl scan, následně proběhl pokus o přihlášení, následně proběhl anomální přenos dat – Systém bude schopen tuto souslednost vyhledat napříč daty i v minulosti),

detekovat určitý počet událostí za časové okno (např. výpis SSH scanů za všechny partnerské organizace za poslední měsíc, nebo komunikace na určených portech a určených IP adresách za poslední rok),,
korelovat proti manuálně zadaným seznamům IP adres/domén,
detekovat komunikaci na blacklistovanou IP adresu v rámci interní ThreatDB (nutná integrace a automatický export IP adres),
jako reakci na korelační pravidlo vygenerovat korelovanou událost a vytvořit návrh na bezpečností incident pro operátora Analytického systému, který bude obsahovat všechny bezpečností události, které vedly k pozitivní detekci,
jako reakci na korelační pravidlo automaticky blacklistovat IP adresu (vytvořit záznam v ThreatDB),
schopnost blacklistovat IP adresu manuálně (zadat do ThreatDB) v rámci práce v GUI,
možnost vyhledávat v zachycených i korelovaných událostech včetně drill-down funkcionality,
možnost tvorby vlastních reportů,
normalizovat příchozí data a ukládat normalizované i RAW data do uložiště,
manuální a automatické zakládání ticketů - integrace s interním ticketovacím systémem, včetně zpětné vazby (Napojení na Request Tracker API. Bude uveden příznak pro založení ticketu a volitelně odeslat email),
hledání a reporting s grafickým výstupem (tabulky, grafy),
integrace blacklistu do korelačních pravidel,
přiřazení informací k externí IP adrese (výtah z ThreatDB: základní info o IP, geolokace, záznamy v blacklistech, výsledky ze služeb typu Virustotal atp.), která byla vyhodnocena jako podezřelá (na základě korelačních pravidel) a uchování této informace v čase,
integraci s ThreatDB.

Korelace dat v úložišti NetFlow/IPFIX

Analytický systém bude přijímat a automaticky vyhodnocovat

NetFlow/IPFIX údaje zaslané všemi partnerskými organizacemi popsané v sekci 2.1 NetFlow/IPFIX data,

a porovnávat je s dalšími daty, zejména:

blacklistovanými IP adresami / doménami,
signaturami útoků,
příchozími bezpečnostními událostmi zaslanými partnerskými organizacemi ve formátu syslog,
bezpečnostními událostmi detekovanými Analytickým systémem v NetFlow/IPFIX datech.

Systém musí zejména umožnit:

zpracování příchozích NetFlow/IPFIX dat z jedné z partnerkých organizací v minimálním objemu 250 000 NetFlow/s,
jako reakci na korelační pravidlo vygenerovat korelovanou událost a vytvořit návrh na bezpečností incident pro operátora Analytického systému, který bude obsahovat všechny bezpečností události, které vedly k pozitivní detekci,
jako reakci na korelační pravidlo automaticky blacklistovat IP adresu (vytvořit záznam v ThreatDB),
schopnost blacklistovat IP adresu manuálně (zadat do ThreatDB) v rámci práce v GUI,
možnost vyhledávat v zachycených i korelovaných událostech včetně drill-down funkcionality,
možnost tvorby vlastních reportů,

normalizovat příchozí data a ukládat normalizované i RAW data do uložiště,
manuální a automatické zakládání ticketů - integrace s interním ticketovacím systémem, včetně zpětné vazby (Napojení na Request Tracker API. Bude uveden příznak pro založení ticketu a volitelně odeslat email),
integraci s ThreatDB.

Detekce síťových anomálií (NBA) v úložišti NetFlow/IPFIX

Požadována je schopnost detekovat anomálie přes všechny NetFlow/IPFIX toky s pomocí NBA (network behavioral analysis) metod. Analytický systém bude přijímat a automaticky vyhodnocovat

NetFlow/IPFIX údaje zaslané všemi partnerskými organizacemi,

k detekci anomálií může v závislosti na zvoleném řešení využívat i další data, zejména:

blacklistované IP adresy / domény,
signatury útoků,
příchozí bezpečnostní události zaslané partnerskými organizacemi ve formátu syslog,
bezpečnostní události detekované Analytickým systémem v NetFlow/IPFIX datech.

V rámci NBA funkcionality je požadována minimálně detekce následujících jevů:

anomálně dlouhé spojení z jedné nebo více organizací na jednu IP adresu s možností whitelistingu (IP adresa, doména, port a jejich libovolná kombinace),
spojení z jedné nebo více organizací na jednu IP či doménu, která je blacklistovaná (integrace s interní ThreatDB),
statistické anomálie v provozu jednotlivých organizací (možnost definování prahových hodnot).

Detekce jevů musí být založena na základě učení normálního chování sítě a hledání odchylek od tohoto normálního stavu. Zadavatel požaduje možnost nastavení délky doby učení časovým parametrem (např. týden, 14 dní, měsíc).

Dále požaduje schopnost vytvářet vlastní metody pro detekci anomálií, například pomocí skriptů spustitelných v rámci systému.

Systém musí zejména umožnit:

jako reakci na anomálii nalezenou pomocí NBA metody vygenerovat událost a vytvořit návrh na bezpečností incident pro operátora Analytického systému, který bude obsahovat všechny bezpečností události, které vedly k pozitivní detekci,
jako reakci na anomálii nalezenou pomocí NBA metody automaticky blacklistovat IP adresu (vytvořit záznam v ThreatDB),
schopnost blacklistovat IP adresu manuálně (zadat do ThreatDB) v rámci práce v GUI,
možnost vyhledávat v událostech nalezených pomocí NBA metody včetně drill-down funkcionality,
možnost tvorby vlastních reportů,
normalizovat příchozí data a ukládat normalizované i RAW data do uložiště,
manuální a automatické zakládání ticketů - integrace s interním ticketovacím systémem, včetně zpětné vazby (Napojení na Request Tracker API. Bude uveden příznak pro založení ticketu a volitelně odeslat email),
integraci s ThreatDB.

3.5 Threat DB – sdílení dat s Partnery

Sdílení NBA signatur s partnerskými organizacemi

Přesný formát signatur včetně jednotlivých datových polí zasílaných Partnerům bude znám až po skončení druhého výběrového řízení na Samostatné systémy sběru síťových dat a detekce anomálií. Zadavatel proto požaduje 50 mandays na integraci, které jsou součástí poptávkové ceny, tak aby Samostatné systémy sběru síťových dat a detekce anomálií umístěné v partnerských organizacích byly schopné načítat signatury útoků vytvořené v Analytickém systému.

Předávání signatur partnerům nebude nikdy probíhat přímo. Analytický systém pouze data vystaví pro Threat DB server umístěný v ICT infrastruktuře NBÚ, odkud si je budou partnerské organizace stahovat (viz Příloha G – Nákres celkové architektury systému).

Předpokládá se Implementace GUI pro tvorbu takových signatur a umožnění jejich exportu (integrace) do partnerských NBA systémů. Zadavatel předpokládá využití univerzálního XML formátu (struktura XML se může lišit dle konkrétního výrobce partnerských NBA řešení). Pro splnění tohoto požadavku jsou pro II. realizační fázi požadovány člověkodny (MD) dodavatele, které budou v průběhu projektu využity, jakmile bude detailně známa struktura dat pro import signatur.

Požadavky na GUI jsou:

- jednoduché grafické rozhraní jako součást jednotného GUI celého systému,
- možnost vytvořit NBA signaturu na úrovni toků pro NBA nástroj (statická korelační pravidla definující signaturu na základě pevně daných hodnot z NetFlow/IPFIX záznamů),
- generování výstupního XML souboru obsahujícího signaturu a jeho vystavení do Threat DB updatovacího serveru (updatovací server *není* součástí tohoto VŘ),
- dodání jako virtuální appliance nebo modul celkového řešení,
- integrace s ThreatDB.

Sdílení blacklistovaných IP adres / domén s partnerskými organizacemi

ThreatDB musí být schopna integrace s externími databázemi Indicators of Compromise (dále „IOC“) vládního pracoviště GovCERT.CZ, zejména:

integraci na on-line databáze blacklistů IP adres/domén/ASN (autonomní číslo systému), strojů zapojených do botnetů, passive DNS, passive ssl (přes API z různých zdrojů na internetu a od partnerských organizací) a interních nástrojů GovCERT.CZ),
generování výstupního souboru obsahujícího blacklistovanou IP adresu / doménu a její vystavení pro stažení Threat DB updatovacím serverem (updatovací server *není* součástí tohoto VŘ),
integrace s IntelMQ (získávání/předávání informací partnerským organizacím),
zjištěné hrozby předávat do MISP (Malware Information Sharing Platform) pomocí API.

3.6 Tvorba alertů

Je požadována funkcionalita generovat alerty na základě korelačních nebo NBA funkcí Analytického systému a tyto alerty zasílat standardizovaným protokolem do externího tiketovacího systému GovCERT.CZ. Požaduje se minimálně:

integrace protokoly SNMP,
volání externí WebService.

Dále musí komponenta poskytovat API (např: RestFULL API) s možností vyhledávat v datech a zpracovat výsledky v jiném systému. Pro jednoduchost Zadavatel předpokládá využití stejného API i pro integraci s vizualizační komponentou.

3.7 Správa zdrojů dat

Analytický systém bude mít k dispozici úložný prostor do velikosti 50TB. Zadavatel požaduje, aby Analytický systém sám řídil retenci a automatické odmazávání dat, a to podle dvou klíčů:

objemového – tedy určením maximální velikosti ukládaných dat; pokud se velikost přiblíží určené maximální hranici, budou automaticky umazány nejstarší záznamy,
časového – tedy jsou promazávány libovolné položky starší určeného data (např. všechny položky starší než 1. 1. 2017), nebo položky starší než operátorem určený časový úsek (např. všechny položky vytvořené před více než 72 hodinami).

4 Scénáře použití

Níže jsou popsány scénáře použití, které musí být realizovatelné s nabízeným Analytický systémem jako celkem. Zadavatel striktně neurčuje, jaká komponenta má umožnit realizaci konkrétního scénáře.

4.1 Operativní scénáře

- Systém detekuje událost, která je nabídnuta operátorovi ke zkoumání. Operátor rozhodne, že se jedná o kybernetický bezpečnostní incident, který zatím postihl jednu/menší část sledovaných institucí, ale z charakteristiky je vidět postupné šíření. Systém přes API ticketovacího systému GovCERT.CZ předpřipraví hlášení pro cílové instituce o hrozícím nebezpečí. Hlášení je následně operátorem ticketovacího systému ručně odesláno jako e-mail příslušné ohrožené instituci nebo institucím.
- Na úrovni GovCERT.CZ je odhalen útok. Operátor vytvoří patřičnou signaturu, aby NBA moduly partnerských organizací byly schopny útok samostatně detekovat. Signatura je ve formátu XML vystavena do Threat DB updatovacího serveru (součást jiného VŘ).
- Na úrovni GovCERT.CZ je odhalen útok. Operátor blacklistuje IP adresu / doménu, aby síťové sondy partnerských organizací byly schopny útok samostatně detekovat. Blacklistovaná IP adresa / doména je vystavena do Threat DB updatovacího serveru (součást jiného VŘ).
- Na základě korelovaných událostí je zjištěno, že větší množství/všechny instituce komunikují s IP adresou (nebo doménou), která zatím nebyla považována za škodlivou. Pokud operátor rozhodne, že se jedná o nelegitimní provoz, IP adresu (nebo doménu) v Systému označí za podezřelou/škodlivou a zařadí ji na blacklist. Blacklistovaná IP adresa / doména je vystavena do Threat DB updatovacího serveru (součást jiného VŘ), skrze který si ji mohou stáhnout bezpečnostní zařízení jednotlivých partnerských institucí takovéto komunikaci zabránit/upozornit na ni.
- Jednotlivé detekované události i události vyhodnocené jako pravděpodobné incidenty jsou za specifikované časové období automaticky ukládány pro další využití v nadřazeném systému využívaném GovCERT.CZ.

- U každé kybernetické události je Systém schopen určit, na základě jakých dílčích událostí byla vytvořena, a u každého kybernetického incidentu musí být dohledatelné, proč bylo rozhodnuto, že se skutečně jedná o incident.
- Systém umožňuje dodatečně označit dříve detekované události či skupinu událostí jako incidenty, pokud bude na základě dodatečných analýz tato skutečnost zjištěna.

4.2 Analytické scénáře

Operátor může na základě nahlášeného incidentu z jedné instituce vyhledat podobné události z jiných institucí, a to na základě společných charakteristik, zejména množství dat/paketů/spojení přenesených v časovém okně, použitých portů nebo TCP flagů. Cílem je dohledat, zda se podobný incident nestal u více institucí, ale povedlo se ho detekovat pouze na jednom místě.
Operátor může proaktivně vyhledávat podezřelé komunikace na základě ručního procházení statistik o provozu a vizualizace jednotlivých statistik a charakteristik provozu. Jedná se o využití vizualizační funkcionality k ručnímu vyhledávání podezřelých událostí a komunikace.
Operátor může v rámci zpracovávaného incidentu, např. zasažení malware, dohledat další potenciální cíle útoku, zejména v případě, kdy malware do internetu komunikuje se stejnými nebo podobnými charakteristikami jako v případě napadené stanice. Pomocí Analytického systému operátor dohledá:
s jakými dalšími stanicemi probíhala komunikace z nakaženého stroje v době blízké incidentu,
ověří, zda došlo k nakažení dalších strojů, které se však zatím neprojevilo a zůstalo tak sondou neodhaleno.
Operátor má možnost procházet historická data za účelem ověření, zda aktuálně detekovaný incident nenastal i v minulosti, nebo zda ke stejnému incidentu nedošlo i na jiném stroji, avšak bez jeho detekování. Například zda stroj nekomunikoval s podezřelou sítí/adresou i v minulosti, kdy tato síť/adresa ještě nebyla uvedena jako podezřelá, avšak už mohla být využívána ke škodlivé činnosti. Operátor má možnost historické korelace a aplikace nově vytvořených pravidel i na historické události.
Během řešení incidentu komunikujícího malware/zapojení do botnetu je forenzní analýzou zjištěno, že škodlivý kód se do cílové instituce dostal určitým způsobem a je možno vytvořit signaturu (korelační pravidlo) pro takovouto komunikaci. Tato signatura (korelační pravidlo) je následně vystavena do Threat DB aktualizačního serveru, který ji distribuuje do dalších zapojených resortů tak, aby mohly být chráněny, pokud k infikaci ještě nedošlo, ale stále hrozí.
Na základě IoC (indicators of compromise) operátor prověří podle indikátorů kompromitace, jestli nedošlo ke stejné události i ve sledovaných sítích. Podle zjištění pak podnikne příslušné kroky.
Dohledání možnosti výskytu určitých znaků komunikace, která byla v některé z institucí detekována honeypotem (honeypot není součástí projektu). Data z honeypotu jsou analytikem zpracována mimo analytický software nezávisle na něm. V analytickém SW jsou vyhledány charakteristiky dané komunikace (IoC) a je hledáno, zda se stejným způsobem nesnažil útočník dostat i do sítí sledovaných poptávaným řešením.
Po nahlášení události do tiketovacího systému GovCERT.CZ operátor prověří, zda v datech nemá další relevantní informace k hlášení. Podle zjištění podnikne příslušné kroky.

5 Provozní požadavky na Analytický systém

5.1 Programový kód

Webové GUI musí být založeno na standardech HTML5, JS a CSS. Bude v českém nebo anglickém jazyce a přístupné z následujících prohlížečů – Firefox 50+, Chrome 54+, Safari 10+ a Edge 38+. K jeho zobrazení a využívání nebude třeba žádný externí plug-in nebo doplněk (Flash, Silverlight anebo Java).

Zadavatel požaduje k výslednému řešení neomezenou výhradní licenci.

5.2 Zálohování

Všechny komponenty musí být zálohované. Dodavatel zajistí:

- každodenní zálohování konfigurací a základních indexů Analytického systému na aplikační úrovni, které umožní obnovení systému v záložní lokalitě, na oddělenou část diskového pole poskytnutého NBÚ,
- zálohy pro obnovení systému budou k dispozici minimálně 5 dní zpětně, systém tedy v jakémkoliv daném bodě bude schopen obnovit jednu z pěti posledních záloh,
- kopie zdrojových dat (události, toky) Anatytického systému na aplikační úrovni za operátorem stanovenou dobu (např. posledních 24 hodin) na oddělenou část diskového pole poskytnutého NBÚ (zadavatel mimo to veškerá data replikuje na úrovni datového pole).

Vlastností řešení bude, že při selhání systémů NBÚ (virtualizace, fyzické ICT infrastruktury atd.) bude možné obnovit provoz řešení v záložní lokalitě v rozsahu next-business-day, a to jen s minimálním zásahem administrátora (spuštění virtuálních serverů, spuštění připravených startovacích skriptů atp.). Tento požadavek lze řešit v rámci implementace dodávkou obslužných skriptů, které zaručí obnovu systému v záložní lokalitě v případě nedostupnosti lokality primární.

Dodavatel dále v rámci nabídky popíše postup, jakým způsobem bude řešit zálohování a jak bude požadavek na obnovu realizován. V rámci implementace zadavatel požaduje dodání Disaster Recovery postupů (DR plán). DR plán bude soubor postupů pro co nejrychlejší zajištění obnovy analytického SW. Popíše reinstalaci SW, jak z důvodu selhání samotného selhání samotného SW, tak infrastruktury zadavatele.

5.3 Logování

Všechny komponenty systému musí zaznamenávat svou vnitřní systémovou činnost v souladu s vyhláškou 316/2014, §21 a vytvářet auditní logy. Tyto auditní logy pokrývají pouze funkci samotného Analytického systému a vytváří se nezávisle na příchozích nebo odchozích provozních datech. Musí být chráněny proti modifikaci. Jedná se především o zaznamenávání:

a) přihlášení a odhlášení uživatelů a administrátorů,

b) činnosti provedené administrátory,

c) činnosti vedoucí ke změně přístupových oprávnění,

d) neprovedení činností v důsledku nedostatku přístupových oprávnění a další neúspěšné činnosti uživatelů,

e) zahájení a ukončení činností technických aktiv informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému,

f) automatická varovná nebo chybová hlášení technických aktiv,

g) přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech a změny nastavení nástroje pro zaznamenávání činností a

h) použití mechanismů identifikace a autentizace včetně změny údajů, které slouží k přihlášení.

5.4 Virtualizace Vmware

Celkové řešení Zadavatel požaduje dodat jako virtuální appliance pro prostředí Vmware vSphere 6.0. Pro systém bude vyhrazeno virtuální prostředí s následujícími parametry:

Vmware vSphere 6.5,
Vmware ESXi 6.0U2.

Pro běh systému jsou alokovány tyto HW prostředky:

- Praha – typu blade,
- Dva procesory Intel Xeon CPU E5-2680 v3 – každý 12 jader, celkem tedy 24 jader,
- RAM 768GB – nesdílená,
- 8Gb FC Adapter do SAN,
- Brno – typu blade. Stejné parametry jako Praha.

Disková pole:

zcela redundantní v rámci lokality, tj. v případě výpadku jednoho přebírá hlavní roli druhé,
čistá maximální kapacita 50TB,
8Gb FC Adapter do SAN,
kapacita je distribuovaná přes systém diskové virtualizace IBM SVC 2145,
podpora zadavatele je 10x5, tj. pracovní dny od 8:00-18:00,
obnova do 4 hodin od nahlášení závady a její zaevidování.

5.5 Integrace

s ticketovacím systémem

GovCERT.CZ aktuálně využívá produkt Request Tracker s nadstavbou Incident Response (viz https://bestpractical.com/rtir/). Systém musí umět používat REST API, které tento ticketovací systém nabízí (viz https://rt-wiki.bestpractical.com/wiki/REST).

obecné REST API

Analytický systém musí nabízet obecné REST API, které umožní napojení dalšího softwaru využívaného NCKB, neveřejné části webového portálu GovCERT.CZ, a dalších systémů. API musí na dotaz těchto systémů vrátit zejména:

aktuální blacklist IP adres/domén,
kybernetické bezpečnostní incidenty za určité časové období,
kybernetické bezpečnostní incidenty za konkrétní subjekt,
kybernetické bezpečnostní incidenty v rámci určeného IP rozsahu.

5.6 Licenční omezení

Celý Analytický systém musí technicky a licenčně umožňovat:

založení až 100 rozdílných uživatelských profilů/účtů,
souběžnou práci 10 fyzických uživatelů,
podporu vytvoření uživatelských skupin a přidělování oprávnění.

Požaduje se podpora propojení s AD/LDAP. Server AD/LDAP tedy musí být jediné místo, kde probíhá definice uživatelů.

Systém musí zajistit, aby při překročení maximálního povoleného objemu příchozích dat nedošlo k jejich zastavování/zahazování (vztahuje se na licenční omezení, HW požadavky řeší zadavatel). Zadavatel musí mít možnost tyto jednorázové problémy vyřešit, aniž by byla ovlivněna funkcionalita celého řešení.

5.7 Provozní monitoring

Provozní dohled bude realizován přes vlastní dohled zadavatele – System Center Operation Manager (SCOM). Nepředpokládá se zřízení přístupu pro externisty. Uchazeč musí jasně popsat jak monitorovat dodané řešení přes SNMP protokol.

6 Příloha – struktura dat Threat DB

Zadavatel pro Threat DB počítá s tímto tvarem dat:

0x00000.skoreabeefimports.info

0x00x0x0x3453.weedns.com

0x1.privserver.com

0x90.devtech.us

1.ns10.xxxy.info

10.mtmyza.net

120.nigr.biz

1337.reipmav.net

2.irc.su

2418.zwned.com

3.hackarmy.tk

3.irc.su

3rb.no-ip.biz1.178.179.217

1.179.170.7

1.93.0.224

101.187.28.8

103.13.29.158

103.16.26.228

103.16.26.36

103.224.83.130

103.228.200.37

103.228.200.44