Závazné parametry řešení projektu

1. Název projektu

PANDDA: Pasivní objevování a analýza zařízení na síti

2. Doba zahájení a ukončení projektu

Datum zahájení projektu: 1. 10. 2024

Datum ukončení projektu (lhůta, v níž má být účelu dosaženo): 30. 4. 2025

3. Cíl(e) projektu (účel projektu)

Navrhovaný projekt se zaměřuje na integraci a přizpůsobení sady open source nástrojů, které jsou v současné době využívané pro monitorování a bezpečnostní analýzu v rámci akademické počítačové sítě CESNET3. Cílem je vytvořit veřejně dostupný a snadno nasaditelný ekosystém vysokorychlostních monitorovacích sond s centrálním kolektorem síťových toků. Usnadnění instalace a provozu těchto bezpečnostních nástrojů podpoří mezisektorovou spolupráci s oblastmi, kde je nedostatek kapacit potřebných odborníků na kyberbezpečnost, což posílí odolnost vůči potenciálním kybernetickým hrozbám. Mezi výsledky projektu vzniknou materiály pro prezentaci a školení technologií a tyto materiály budou použity pro budování povědomí o kyberbezpečnosti a nástrojích, které zlepšují přehled o stavu a provozu spravované síťové infrastruktury. Vedle základní funkcionality monitorovacího systému je hlavním přínosem projektu funkcionalita shromažďování a aktualizace seznamu aktivních zařízení (asset discovery) v monitorovaných sítích a zobrazení získaných provozních a statistických dat obsluze, např. bezpečnostním týmům, analytikům a správcům. Kvalitní síťová monitorovací infrastruktura je důležitým doplňkem k nástrojům pro bezpečnost a obranu počítačových systémů a sítí. Projekt proto podpoří možnost nasazení výkonné monitorovací infrastruktury do vysokorychlostních sítí i na menší a pomalejší sítě, přičemž instalace a nastavení budou připraveny tak, aby byl ekosystém použitelný uživateli bez expertních znalostí. Projekt tak reaguje na složitou instalaci a konfiguraci, které v současné době brání masivnějšímu nasazení těchto bezpečnostních nástrojů. Nasazený systém bude automaticky přispívat k vyšší automatizaci správy zařízení (asset management), tedy další důležité složce kyberbezpečnosti.

4. Klíčová osoba řešitelského týmu

5. Plánované výstupy/výsledky projektu

Výstup/výsledek:

Číslo výstupu/výsledku: V001

Název výstupu/výsledku: Instalační nástroj infrastruktury PANDDA

Popis výstupu/výsledku: Existující instalační Ansible Playbook pro monitorovací sondu vyžadují expertní znalosti pro správnou konfiguraci a nastavení. Navrhovaný výsledek rozšíří existující Playbook o instalaci a konfiguraci serveru sloužícího jako kolektor. Server kolektor sbírá data a provádí jejich zpracování a analýzu. Dokáže odhalovat aktivní zařízení na monitorovaných sítích, ukládat jejich historii a poskytuje tyto informace bezpečnostním analytikům a správcům sítí.

Výstup umožní automaticky nakonfigurovat jak sondu, tak kolektor, a tedy celou infrastrukturu potřebnou pro monitorování sítí a asset discovery. Součástí bude také konfigurace samotných nástrojů na serveru kolektor pro tyto účely. Hlavním dopadem tohoto výstupu je zjednodušení procesu nasazení bezpečnostních nástrojů pro monitorování provozu a automatické pasivní objevování zařízení na síti. Tím se posílí motivace k budování odolného kybernetického prostředí, které poskytne důležité informace k obraně proti kybernetickým hrozbám. Složitost a náročnost nasazení aktuálního stavu nástrojů je překážkou, kterou výsledek minimalizuje. Primárním klíčovým indikátorem je dosažení otestovaného výsledku a jeho nasazení u pilotního uživatele. Dalším klíčovým indikátorem je získání zpětné vazby od pilotního uživatele, která bude využitelná pro další rozvoj výsledku.

Druh výstupu/výsledku: R — Software

Výstup/výsledek:

Číslo výstupu/výsledku: V002

Název výstupu/výsledku: Generátor konfigurace

Popis výstupu/výsledku: Instalační nástroj (uvedený jako výsledek V001) stále vyžaduje konfiguraci vycházející ze znalostí cílového prostředí (síťové infrastruktury) operátora. Druhý navrhovaný výsledek je tedy průvodcem pro vytvoření samotné konfigurace tak, aby byl systém jednoduše použitelný i běžnými uživateli. Součástí průvodce bude i generátor konfigurace pro instalační nástroj, která by jinak musela být vytvořena manuálně.Generátor získá od uživatele informace o serverech, na které se má systém nainstalovat, zjistí jaké sítě a jaká síťová rozhraní se budou monitorovat. Nástroj uživateli napoví, jak požadované informace zjistit (např. najít v operačním systému) nebo odvodit technické parametry. Generátor pokryje vytvoření konfigurace všech částí systému, tedy sondy, kolektoru a všech použitých softwarových nástrojů.

Tento výsledek pomáhá správně nakonfigurovat použité bezpečnostní nástroje pro nasazení podle potřeb cílové sítě, přičemž Generátor konfigurace odstíní uživatele od technických a odborných detailů. Dopadem tudíž bude snazší použitelnost nástrojů a využití zkušenosti a nejlepší praktiky získané sdružením CESNET v jiných sférách, což posílí budování odolného kybernetického prostředí. Primárním klíčovým indikátorem je dosažení otestovaného výsledku

a jeho použití při nasazování systému u pilotního uživatele. Dalším klíčovým indikátorem je získání zpětné vazby od pilotního uživatele, která bude využitelná pro další rozvoj výsledku.

Druh výstupu/výsledku: R — Software

Výstup/výsledek:

Číslo výstupu/výsledku: V003

Název výstupu/výsledku: Dokumentace a návody pro uživatele

Popis výstupu/výsledku: Třetí výsledek představuje vytvořenou webovou prezentaci a dokumentaci systému PANDDA. V rámci dokumentace bude primárně obsažen srozumitelný popis instalačního procesu pomocí Ansible Playbooku, podle kterého bude schopen systém zprovoznit běžný technicky zdatný uživatel. Pro pokročilejší scénáře nasazení bude dokumentace obsahovat technické podrobnosti a odkazy do podrobné technické dokumentace použitého softwaru, což umožní přizpůsobit infrastrukturu specifickým požadavkům pokročilými uživateli a vývojáři. Důležitou částí dokumentace bude sada návodů a popisů konkrétních příkladů nasazení (Case Studies). Díky těmto příkladům bude možné zprovoznit monitorovací infrastrukturu PANDDA přímočaře pomocí předpřipravených kroků a využít již hotovou konfiguraci. Možné příklady pro “Case Studies”:

1. Malá síť, kde jsou sonda i kolektor nasazeny na jednom společném stroji

2. Vlastní server pro sondu a vlastní server pro kolektor

3. Více sond s centrálním kolektorem

Hlavním dopadem tohoto výsledku a souvisejících propagačních aktivit je zvýšení povědomí uživatelů z jiných sfér (akademická, soukromá, veřejná) o kyberbezpečnosti a dostupných nástrojích, které podpoří schopnost detekovat nové bezpečnostní hrozby, čímž se zvýší odolnost kybernetického prostředí. Primárním klíčovým indikátorem je spuštění veřejně dostupné webové prezentace sdokumentací a souvisejícími materiály. Dalším klíčovým indikátorem je získání zpětné vazby od pilotního uživatele. Po spuštění webové prezentace bude jako indikátor sledován vývoj počtu přístupů uživatelů. Důležitým indikátorem bude počet akcí a PR výstupů, pomocí kterých budou propagovány dosažené výsledky projektu.

Druh výstupu/výsledku: O — Technická zpráva, web dokumentace

6. Identifikační údaje účastníků

Hlavní příjemce: CESNET, zájmové sdružení právnických osob

Role uchazeče na projektu: Hlavní řešitel

IČ: 63839172

DIČ / VAT-ID: CZ63839172

Obchodní jméno/název organizace: CESNET, zájmové sdružení právnických osob

Právní forma: Zájmové sdružení právnických osob

7. Náklady

Náklady - Souhrn		2024	2025
Osobní náklady [Kč]	**560 000,00**	**240 000,00**	**320 000,00**
Osobní náklady [Kč]	560 000,00	240 000,00	320 000,00
Úvazek [člověko-rok]		0,20	0,27
Průměrné osobní náklady na úvazek [Kč / člověko-rok]		1 200 000,00	1 200 000,00
Ostatní přímé náklady [Kč]	**0,00**	**0,00**	**0,00**
Cestovní náklady	0,00	0,00	0,00
Nákup služeb, materiálu, drobného hmotného a nehmotného majetku	0,00	0,00	0,00
Další přímé náklady	0,00	0,00	0,00
Nepřímé náklady [Kč]	**39 200,00**	**16 800,00**	**22 400,00**
Náklady celkem [Kč]	**599 200,00**	**256 800,00**	**342 400,00**
Zdroje			
Podpora [Kč]	**599 200,00**	**256 800,00**	**342 400,00**
Neveřejné zdroje [Kč]	**0,00**	**0,00**	**0,00**
Zdroje celkem [Kč]	**599 200,00**	**256 800,00**	**342 400,00**
Intenzita podpory [%]	100,00%	100,00%	100,00%