Příloha G smlouvy:

NÁKRES CELKOVÉ ARCHITEKTURY SYSTÉMU

GUI: ANALYT. SW
(připraví dodavatel analyt. SW, včetně datových zdrojů)

operátor GovCERT.CZ

GUI: REQUEST TRACKER

TICKETOVACÍ SYSTÉM
(připraví GovCERT.CZ)

API

TVORBA ALERTŮ
• připraví email k rozeslání z RTIR

ZALOŽENÍ TICKETU
• připraví ticket pro RTIR

SOUČÁSTI DODÁVKY VŘ *„ANALYTICKÝ SYSTÉM GovCERT.CZ“*

VYTVOŘÍ ZÁZNAM „ZAKÁZANÁ IP“ NEBO „ZAKÁZANÁ DOMÉNA“

VYTVOŘÍ ZÁZNAM „SIGNATURA“

ZAKÁZANÁ IP / DOMÉNA

SIGNATURA

KYBERNETICKÝ BEZP. INCIDENT

ANO

JDE O INCIDENT ?

NE

POVÝŠÍ *„UDÁLOST“* NA *„INCIDENT“*

UDĚLÁ Z INCIDENTU POUHOU *„UDÁLOST“*

PŘÍMO O(D)ZNAČÍ IP ADRESU / DOMÉNU ZA ZAKÁZANOU

PŘÍMO VYTVOŘÍ/UPRAVÍ SIGNATURU

VYTVOŘÍ NOVOU *„UDÁLOST“*

KYBERNETICKÁ BEZPEČNOSTNÍ UDÁLOST

VIZUALIZACE
• SPI graph • Graf spojení
• SPI View • NFSEN • IP/CIDR
• vynesení na mapu
+
SPRÁVA DAT
• odmazávání • zálohy

PROCHÁZENÍ DAT
• tagování • komentáře
• vyhledávání • agregace
• drill-down

POKROČILÁ PRÁCE S DATY
• korelace
• NBA

KORELACE NAD INCIDENTY Z REZORTŮ + VLASTNÍMI

3) EXISTUJÍCÍ ZÁZNAM UDÁLOSTI ZTRÁCÍ TAG *„INCIDENT“*

2) EXISTUJÍCÍ ZÁZNAM UDÁLOSTI ZÍSKÁ TAG *„INCIDENT“*

1) VYTVOŘÍ ZÁZNAM *“UDÁLOST“*

KORELACE NETFLOW Z VÍCE REZORTŮ + EXT. ZDROJŮ

NBA NAD NETFLOW

BLACKLISTY
• IP adresy
• domény

SIGNATURY ÚTOKŮ
• IP adresa • doména • TCP flagy • URL • user agent • kombinace polí NetFlow/IPFIX

API

INTEL MQ
gray/blacklisty IP a domén

INTEL MQ DB
(připraví GovCERT.CZ)

otevřený internet: závadné IPs / domény

API

Systémy GovCERT.CZ (připraví GovCERT.CZ)

API

UDÁLOSTI & INCIDENTY detekované v sítích partnerů • incident = událost s příznakem

UDÁLOSTI & INCIDENTY detekované v GovCERT.CZ
• incident = událost s příznakem

NETFLOW/IPFIX ÚDAJE + L7:
• http-metoda
• http-user-agent • http-uri
• http-url • DNS requests
• detaily protokolu SMB

UDÁLOSTI
syslog

SÍŤOVÝ PROVOZ
NetFlow/IPFIX + L7

Threat DB server
• blacklisty
• signatury

Update server
nový firmware

THREAT DB
(dodavatel sond)

IPSEC TUNEL
variantně SSH / TLS
KIVS LINKY / OTEVŘENÝ INTERNET

↑ infrastruktura NBÚ
↓ infrastruktura partnerů

KOLEKTOR:
- FILTRUJE NetFlow/IPFIX + L7 DATA A DO GovCERT ZASÍLÁ JEN TA PROCHÁZEJÍCÍ VNĚJŠÍM PERIMETREM
- DETEKUJE KYBERNETICKÉ BEZP. UDÁLOSTI POMOCÍ NBA A DDoS MODULU; VŠECHNY ZASÍLÁ DO GovCERT
- STAHUJE SI AKTUALIZOVANÉ BLACKLISTY IP ADRES / DOMÉN Z ThreatDB
- STAHUJE SI AKTUALIZOVANÉ SIGNATURY ÚTOKŮ Z ThreatDB

KIVS/internet: aktualizace HW

DODAVATEL SOND (DS)

BLACKLISTY/ SIGNATURY / INCIDENTY (XML)

PARTNEŘI GovCERT
CERT-EU
BotnetFeed
Shadow Server

KOLEKTOR (DS)

interní linka: NetFlow/IPFIX + L7

ICT expert partnerské organizace plně ovládá kolektor

SOUČÁST DODÁVKY VŘ *„TECHNOLOGIE SLEDOVÁNÍ SÍŤOVÉHO PROVOZU“*

SPAN (DS)

TAP (DS)

TAP / SPAN PRVKY PASIVNĚ ODKLÁNÍ PROVOZ K ANALÝZE KOLEKTOREM