SERVICIUL TEHNOLOGIA INFORMAȚIEI

ȘI SECURITATE CIBERNETICĂ

MD-2012 mun. Chișinău, Piața Marii Adunări Naționale, 1 IDNO 1003600096694

tel.: + 373 22 820 900, fax: + 373 22 250 522 e-mail: stisc@stisc.gov.md, itsec@itsec.gov.md

SPECIFICAȚIA TEHNICĂ

Soluția de analiză și vizibilitate a traficului de rețea

IP STISC

stisc@stisc.gov.md

Introducere

Descrierea Soluției

Soluția de analiză și vizibilitate a traficului de rețea reprezintă o soluție software destinat Centrelor de operațiuni de securitate (SOC). Soluția reprezintă o platformă multifuncțională de detectare și răspuns la diferite tipuri de vulnerabilități și atacuri vizate care are ca scop reducerea timpului de detectare a atacurilor de rețea. Soluția permite să detecteze rapid și precis atacatorii, persoanele rău intenționate și malware deja în interiorul rețelei, să se angajeze cu atacatori și să neutralizeze amenințările cibernetice avansate. Cu această soluție administratorii pot crea în mod automat momeli (capcane) de sistem de operare reale, interactive, precum și servicii emulate și OS, inclusiv dispozitive IoT.

C1 Cerințe Generale

C1.01	Soluția trebuie să fie complet funcțională instalată și livrată la cheie
C1.02	Toate cerințele sunt minime și obligatorii
C1.03	Soluția trebuie sa includă toate licențele necesare funcționarii acesteia, la parametrii si valorile solicitate in prezentele specificații, inclusiv cele aferente extensibilității, si nu trebuie sa existe o careva limitare;
C1.04	Soluția trebuie să fie compatibilă și să ruleze pe infrastructuri de tip Cloud (VMware vSphere 6.0, 6.5, 6.7, 7.0)
C1.05	Soluția se va integra cu componentele de SDN ale platformei de virtualizare a beneficiarului si va asigura compatibilitatea cu cel puțin versiunile VMware NSX 6.2, 6.4;
C1.06	Perioada de implementare în producere a soluției nu va depăși 90 zile calendaristice
C1.07	Soluția trebuie să fie instalată exclusiv pe platformele beneficiarului în mediu virtualizat vSphere 7. Se admin componente hardware ce asigura decriptarea a traficului SSL/TLS, sau componentele ce asigura captarea traficului ca parte integrata a soluției.
C1.08	Ofertantul va asigura instruiri privind instalarea și utilizarea produsului livrat
C1.09	Soluția trebuie sa includă toate subscripțiile necesare pentru o perioada de minim 3 ani;
C1.10	Soluția trebuie sa includă accesul in portalul web al producătorului pentru a contacta suportul tehnic si descărca actualizările pentru o perioada de cel puțin 3 ani;

C2 Cerințe Funcționale

C2.01	Soluția trebuie să fie capabilă de a analiza traficul de rețea pentru detectarea atacurilor inclusiv a traficului criptat cel putin SSL, TLS1.1, 1.2, 1.3
C2.02	Soluția trebuie să fie capabilă de a capta traficul de rețea prin port mirror de pe infrastructura fizica și virtuala Vmware prin intermediul protocoalelor SPAN, RSPAN sau similare
C2.03	Soluția trebuie să fie capabilă de a detecta/inventaria corect toate resursele utilizate în rețea (servere, dispozitive finale, echipamente de rețea, IoT, Shadow-IT etc.), nu doar acelea care sunt implicate in procesul de atac.
C2.04	Soluția trebuie să fie capabilă de a detecta corect datele utilizate în rețea (Sistemul de Operare, subrețele, Aplicații, Porturi)
C2.05	Soluția trebuie să fie capabilă de a detecta Domeniile pentru integrarea cu Active Directory
C2.06	Soluția trebuie să fie capabilă de a construi vizual grafice de interacțiune între activele detectate
C2.07	Soluția trebuie să fie capabilă de a instala automat și manual momeli (clone a sistemelor reale) în infrastructuri clasice și de tip cloud
C2.08	Soluția trebuie să fie capabilă de a capta/intercepta cel puțin 500Mbps de trafic pentru analiză
C2.09	Soluția trebuie să permită extinderea capacității de analiză a traficului dacă aceasta este limitată de politica de licențiere
C2.10	Soluția trebuie să permită crearea regulilor individuale de reacție la incidente
C2.11	Soluția trebuie să detecteze acțiuni malițioase de diferite tipuri (sql injection, brute force atacuri, DLP etc.)
C2.12	Soluția trebuie să aibă consolă centralizată de gestiune și vizualizare a atacurilor
C2.13	Soluția trebuie să suporte utilizatori de diferite roluri și posibilitatea de a crea roluri individuale

C2.14	Soluția trebuie să permită atribuirea incidentelor către anumiți utilizatori din sistem pentru analiza;
C2.15	Soluția trebuie să suporte emularea celor mai des întâlnite sisteme de operare și capcane pentru a imita elementele din infrastructura reală;
C2.16	Soluția trebuie să permită captarea a cel puțin 200 surse de trafic
C2.17	Soluția trebuie să permită încărcarea manuală a fișierelor reale în capcane
C2.18	Soluția trebuie să fie capabilă de a înregistra și grupa în baza regulilor de corelație evenimentele analizate, în rezultatul cărora să genereze ”concluzii” pe baza acestor evenimente
C2.19	Soluția trebuie să permită generarea rapoartelor în baza șabloanelor cât și individuale în format cel puțin pdf
C2.20	Soluția trebuie să includă funcțional de notificare prin e-mail a rapoartelor preprogramate cât și a altor evenimente aferente soluției
C2.21	Soluția trebuie să permită autentificarea utilizatorilor în consola centralizată prin Radius, TACACS+ și LDAP