Anexa Nr 1 la Anx. 22, oferta Tehnica.

Soluția de analiză și vizibilitate a traficului de rețea

Digitally signed by Cojocari Andrei
Date: 2022.01.14 15:04:42 EET
Reason: MoldSign Signature
Location: Moldova

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

Nr.	Cerința	Răspuns
C1.01	Soluția trebuie să fie complet funcțională instalată și livrată la cheie	Confirmam indeplinirea, acoperit de ExtraHop Reveal(x)
C1.02	Toate cerințele sunt minime și obligatorii	Confirmam indeplinirea, acoperit de ExtraHop Reveal(x)
C1.03	Soluția trebuie sa includă toate licențele necesare funcționarii acesteia, la parametrii sivalorile solicitate in prezentele specificații, inclusiv cele aferente extensibilității, si nu trebuie sa existe o careva limitare;	Confirmam indeplinirea, acoperit de ExtraHop Reveal(x)
C1.04	Soluția trebuie să fie compatibilă și să ruleze pe infrastructuri de tip Cloud (VMwarevSphere 6.0, 6.5, 6.7, 7.0)	Confirmam indeplinirea, acoperit de ExtraHop Reveal(x)
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;	Confirmam indeplinirea, acoperit de ExtraHop Reveal(x)
C1.06	Perioada de implementare în producere a soluției nu va depăși 90 zile calendaristice	Confirmam indeplinirea, acoperit de ExtraHop Reveal(x)
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.	Confirmam indeplinirea, acoperit de ExtraHop Reveal(x)
C1.08	Ofertantul va asigura instruiri privind instalarea și utilizarea produsului livrat	Confirmam indeplinirea, acoperit de ExtraHop Reveal(x)
C1.09	Soluția trebuie sa includă toate subscripțiile necesare pentru o perioada de minim 3 ani;	Confirmam indeplinirea, acoperit de ExtraHop Reveal(x)
C1.10	Soluția trebuie sa includă accesul in portalul web al producătorului pentru a contactasuportul tehnic si descărca actualizările pentru o perioada de cel puțin 3 ani;	Confirmam indeplinirea, acoperit de ExtraHop Reveal(x)

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	Confirmam indeplinirea, acoperit de ExtraHop Reveal(x)
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 sausimilare	Confirmam indeplinirea, acoperit de ExtraHop Reveal(x)
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.	Confirmam indeplinirea, acoperit de ExtraHop Reveal(x)
C2.04	Soluția trebuie să fie capabilă de a detecta corect datele utilizate în rețea (Sistemul deOperare, subrețele, Aplicații, Porturi)	Confirmam indeplinirea, acoperit de ExtraHop Reveal(x)
C2.05	Soluția trebuie să fie capabilă de a detecta Domeniile pentru integrarea cu Active Directory	Confirmam indeplinirea, acoperit de ExtraHop Reveal(x)
C2.06	Soluția trebuie să fie capabilă de a construi vizual grafice de interacțiune între activele detectate	Confirmam indeplinirea, acoperit de ExtraHop Reveal(x)
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	Confirmam indeplinirea, acoperit de TrapX
C2.08	Soluția trebuie să fie capabilă de a capta/intercepta cel puțin 500Mbps de trafic pentruanaliză	Confirmam indeplinirea, acoperit de ExtraHop Reveal(x)
C2.09	Soluția trebuie să permită extinderea capacității de analiză a traficului dacă aceasta estelimitată de politica de licențiere	Confirmam indeplinirea, acoperit de ExtraHop Reveal(x)
C2.10	Soluția trebuie să permită crearea regulilor individuale de reacție la incidente	Confirmam indeplinirea, acoperit de ExtraHop Reveal(x)

C2.11	Soluția trebuie să detecteze acțiuni malițioase de diferite tipuri (sql injection, brute forceatacuri, DLP etc.)	Confirmam indeplinirea, acoperit de ExtraHop Reveal(x)
C2.12	Soluția trebuie să aibă consolă centralizată de gestiune și vizualizare a atacurilor	Confirmam indeplinirea, acoperit de ExtraHop Reveal(x)
C2.13	Soluția trebuie să suporte utilizatori de diferite roluri și posibilitatea de a crea roluriindividuale	Confirmam indeplinirea, acoperit de ExtraHop Reveal(x)

C2.14	Soluția trebuie să permită atribuirea incidentelor către anumiți utilizatori din sistem pentruanaliza;	Confirmam indeplinirea, acoperit de ExtraHop Reveal(x)
C2.15	Soluția trebuie să suporte emularea celor mai des întâlnite sisteme de operare și capcanepentru a imita elementele din infrastructura reală;	Confirmam indeplinirea, acoperit de TrapX
C2.16	Soluția trebuie să permită captarea a cel puțin 200 surse de trafic	Confirmam indeplinirea, acoperit de ExtraHop Reveal(x)
C2.17	Soluția trebuie să permită încărcarea manuală a fișierelor reale în capcane	Confirmam indeplinirea, acoperit de TrapX
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 acestorevenimente	Confirmam indeplinirea, acoperit de ExtraHop Reveal(x); ExtraHop oferă, printre altele, briefing-urile despre amenințări, oferind îndrumări despre potențialele amenințări la adresa rețelei dvs. (este atasat la licitatie)
C2.19	Soluția trebuie să permită generarea rapoartelor în baza șabloanelor cât și individuale înformat cel puțin pdf	Confirmam indeplinirea, acoperit de ExtraHop Reveal(x)
C2.20	Soluția trebuie să includă funcțional de notificare prin e-mail a rapoartelor preprogramatecât și a altor evenimente aferente soluției	Confirmam indeplinirea, acoperit de ExtraHop Reveal(x)

C2.21	Soluția trebuie să permită autentificarea utilizatorilor în consola centralizată prin Radius,TACACS+ și LDAP	Confirmam indeplinirea, acoperit de ExtraHop Reveal(x)

Semnat:_____
Numele, Prenumele: Andrei Cojocari
În calitate de: Chief Commercial Officer
Ofertantul: S&T MOLD SRL
Adresa: Calea Iesilor 8, MD-2069 Chisinau, Republica Moldova