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

SPECIFICAȚIE TEHNICĂ

Soluția de jurnalizare si analiză a evenimentelor de rețea în MCloud

IP STISC

stisc@stisc.gov.md

Introducere

Descrierea Soluției

Soluția de jurnalizare și analiză a evenimentelor de rețea în MCloud este destinată Centrelor de operare de securitate (SOC) care are ca scop colectarea evenimentelor de securitate din diferite sisteme și corelarea lor pentru a putea rapid detecta și preveni atacurile cibernetice.

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
C1.08	Ofertantul va asigura instruiri privind instalarea și utilizarea produsului livrat
C1.09	Ofertantul va oferi suport tehnic necesar in vederea instalării în producere a soluției și configurării colectării de la 10 surse de date
C1.10	Ofertantul va oferi suport tehnic necesar in vederea configurării corelării de evenimente pentru sursele de date de la C1.09
C1.11	Soluția trebuie sa includă toate subscripțiile necesare pentru o perioada de minim 3 ani;
C1.12	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 colecta evenimentele de securitate de pe diferite tipuri de sisteme sau echipamente (surse de date) în formate multiple;
C2.02	Soluția trebuie să includă funcționalități de analiză a comportamentului utilizatorilor și entităților;
C2.03	Soluția trebuie să fie capabilă de a se integra nativ cu cel puțin cele mai populare sisteme pentru colectarea evenimentelor cum ar fi: -Windows Event Logs; - Linux logs; - Domain Controllers; - Kaspersky Endpoint Security; - Cisco ASA, Cisco Routers, Cisco Switches, Juniper; - Fortigate, Fortianalyzer; - Collaboration: Zimbra, postfix, Microsoft Exchange, Nextcloud; - VMware, Netapp, Synology; - Kubernetes;
C2.04	Soluția trebuie să permită crearea adaptoarelor individuale/proprii pentru prelucrarea și înregistrarea evenimentelor
C2.05	Soluția trebuie să posede capabilități de corelare a evenimentelor colectate din diverse surse
C2.06	Soluția trebuie să fie capabilă de a prelucra evenimentele colectate și să facă corelare automatizat
C2.07	Soluția trebuie să fie capabilă de a colecta date prin protocolul Netflow/IPFIX

C2.08	Soluția trebuie să fie capabilă de a agrega datele colectate prin protocolul NetFlow/IPFIX pentru analiză și statistică
C2.09	Soluția trebuie să aibă consolă web centralizată de gestiune și vizualizare a evenimentelor. Accesul la consolă trebuie să fie doar prin protocoale securizate
C2.10	Soluția trebuie să posede capabilități de generare personalizata a statisticii
C2.11	Soluția trebuie să dispună de alerte pre-configurate și să permită configurarea alertelor în bază de triggere
C2.12	Soluția trebuie să dispună de capabilități de transmitere a notificărilor (alertelor) prin SMTP.
C2.13	Soluția trebuie să ofere posibilități de căutare interactivă atât într-o sursă de date, cât și simultan în surse multiple
C2.14	Soluția trebuie să suporte utilizatori de diferite roluri și posibilitatea de a crea roluri individuale
C2.15	Soluția trebuie să aibă funcțional de orchestrare, automatizare si răspuns a incidentelor identificate;
C2.16	Soluția trebuie sa permită setarea politicii de retenție a evenimentelor pentru stocare;
C2.17	Soluția trebuie sa suporte cel puțin 500 de hosturi monitorizate (surse de date);
C2.18	Soluția trebuie sa suporte volum nelimitat de evenimente analizate;
C2.19	Soluția trebuie să ofere posibilitatea de generare a rapoartelor, atât preconfigurate, cât și customizabile, în format PDF, HTML, CSV.
C2.20	Soluția trebuie să funcționeze la o capacitate de minim 5000 eps.