SIEM (Log menedzser) rendszer korszerűsítése projekt műszaki leírása

Előzmény: Az Országgyűlés Hivatala (a továbbiakban: OGYH) jelenleg a Microfocus Sentinel 8.1.x SIEM rendszert használja, amelyet korszerűsíteni kíván Micro Focus ArcSight SIEM rendszerre a korábbi logok megtartása nélkül.

A rendszer megvalósításának folyamata és eredménytermékei

- Az eddigi felméréseink alapján a kiépítendő Micro Focus ArcSight SIEM rendszerhez minimum 80 CPU core-ra, 232 GB memóriára és 9,6 TB háttértárra van szükség legfeljebb 6 virtuális szerverre vonatkozóan, amely erőforrások az OGYH VMware virtuális környezetében rendelkezésre állnak.
- A kiépítendő Micro Focus ArcSight SIEM rendszer kivitelezésének véghatárideje: 2022.12.10.
- A kiépítendő Micro Focus ArcSight SIEM rendszer kiépítéséhez felmérésre kell kerüljenek a bevonandó rendszerek, amelyek a következők: *Apache webszerverek, Microsoft Active Directory and Windows, Microsoft IIS, Microsoft SQL Server, NetIQ eDirectory, NetIQ iManager, Oracle Audit Database, RSA Authentication Manager, Red Hat Enterprise Linux, Suse Linux Enterprise Server, Symantec Endpoint Protection, Novell NSS Fájl audit, Barracuda Web Access Firewall, VMWare ESXi, CheckPoint Firewall, FortiGate Firewall, Cisco ISE, Cisco switch-ek és router-ek.*
- A fentebb felsorolt eseményforrások vonatkozásában megtervezésre kerül a Windows, Linux, hálózati és egyéb alkalmazásszintű naplók gyűjtése, illetve megtervezésre kerül a CEF eseményfolyam.
- A felmérést követően a Szállító feladata a SIEM rendszerhez tartozó Rendszerterv elkészítése.
- A Micro Focus ArcSight SIEM rendszer kiépítéséhez telepítésre kerülnek Kubernet-es környezet (CDF) és a tároló réteghez tartozó Vertica adatbázis (elkészítésre kerül a Container Deployment Foundation (CDF) telepítési konfigurációs yaml fájl, ami alapján létrehozásra kerül a Kubernet-es cluster és létrehozásra kerül a Vertica adatbázishoz tartozó séma), valamint a Kubernet-es master, worker és DB node-ok operációs rendszerei, illetve a Windows és Linux gyűjtőréteg operációs rendszerei.
- Telepítésre kerülnek a gyűjtést végző SmartConnectorok, a disztribúciót végző Transformation HUB, a keresést és tárolást végző Recon, az elemzést végző ESM és a végrehajtást végző SOAR. Az ArcSight termékek telepítése után a CDF ITOM felületén keresztül hozzáadásra kerülnek a termékekhez tartozó label-ek, hogy ezáltal a rendszerhez tartozó összes pod elinduljon.

- A rendszerkonfiguráció során el kell végezni a Windows kiszolgálók esemény továbbítási architektúra kialakítását, a szolgáltatások környezeti illesztését (LDAP, SMTP, Monitoring) és a Linux auditd konfigurációs feladatokat is.
- A rendszerkonfiguráció során el kell végezni a telepített SmartConnector-ok ArcSight Management Center-be való bevonását és a Connector-ok alapvető rendszermonitoring konfigurációs támogatási feladatait is.
- A SIEM rendszer kialakítása közben illesztésre kerülnek a fentebb felsorolt eseményforrások. Az eseményforrás típusok naplógyűjtési integrációját a szállító és a megrendelő munkatársai közösen végzik. A szállító eseményforrás típusonként 2-3 példány integrációját végzi el, ezzel mintegy gyakorlatban is bemutatva a folyamatot a megrendelő munkatársai számára.
- A következő jogosultsági körök kialakítása: *ArcSight adminisztrátor*: ArcSight rendszer konfigurációinak módosítása és bármilyen naplóadat keresése *Auditor*: bármilyen naplóadatot kereshet, rendszerkonfigurációkhoz nem fér hozzá
- A tartalmi elemek implementálása közben felülvizsgálatra és implementálásra kerülnek a jelenlegi Sentinel SIEM rendszerben definiált korrelációk, riportok és dashboard-ok.

  Implementálásra kerül:

  — a Gépvándorlás korreláció, amely a MAC címek hálózati portok közötti mozgásának detektálását végzi a NAC rendszer, valamint a hálózati eszközök naplói alapján,
  — az Egypontos hozzáférési kapuk megkerülésének figyelése korreláció, amely az Egypontos hozzáférés (SCB, jump station) megkerülése esetén generál figyelmeztető riasztást.
  — az IDM technikai felhasználó megkerülésének figyelése korreláció, amely az IDM technikai felhasználó megkerülésével az Active Directory-ban és az eDirectory-ban végzett tevékenységek megfigyelését végzi,
  — az Alert Dashboard, amely segítségével vizualizálni lehet a kiváltott riasztásokat,
  — a távolról bejelentkező felhasználók tevékenységéről szóló riport (havi és heti), amely a munkaidőn belüli és kívüli szolgáltatások bejelentkezési statisztikáját mutatja felhasználókra bontva, a használt VPN csatorna és szolgáltatás alapján (számosságban),
  — vírusos levelek esetében a küldő e-mail címe automatikus tiltása és a kapcsolódó riport,
  — SMTP kapcsolati hibák elemzése (TRANS_FAILURE típusú Symantec Messaging Gateway naplók) - napi riportként,
  — Groupwise bejelentkezések kereshetősége, melyik felhasználó mikor lépett be
  — mintalekérdezések készítése: tipikus és atipikus események dokumentálása a hibakeresés és a hibaelhárítás érdekében (pl. authentikációk; fájl műveletek, különös tekintettel a törlésre; kizáródás jelszó hiba miatt, és a

kapcsolódó visszaengedés; gyárilag támogatott WAF és tűzfalak eseményeinek értelmezése)
  - implementálásra kerül a Top Network Issues from previous day riport, amely megmutatja az előző napon bekövetkezett magas súlyosságú hálózati támadásokat,
  - a Top Attacks By Sources from previous day riport, amely megmutatja az előző napon bekövetkezett támadások forrásait top 10-es listába rendezve,
  - a Firewall traffic Trends riport, amely megmutatja az aktuális hónap tűzfal statisztikái alapján a Sikertelen adminisztrátori bejelentkezéseket, a konfigurációs változásokat és az egy forrásból érkező többszörös sikertelen bejelentkezéseket,
  - az Adminisztrátori bejelentkezések (hálózati eszközök) riport, amely egy napi riport és egy perces késleltetésű korreláció a hálózati eszközön végbemenő adminisztrátori bejelentkezésekről és konfiguráció módosításokról,
  - az Unallowed HTTP Access riportok (Ilias, Liferay), amelyek megmutatják az adott webszerver naplók alapján az előző héten bekövetkezett adminisztrátori bejelentkezéseket az előre meghatározott hálózati szegmensen kívülről a rendelkezésre álló információk alapján,
  - a Hálózati eszközök rendellenes működése riport, amely megmutatja a hálózati eszközök rendellenes működésének kritikus eseményeit.
- A tartalmi elemek implementálása közben implementálásra kerül 3 darab intelligens beavatkozási folyamatot biztosító SOAR playbook:
  - a Gépvándorlást figyelő playbook, amely figyeli, hogyha egy adott MAC címmel rendelkező gép a szokásostól eltérő port-on kerülne csatlakoztatásra. Az észlelés és riasztás generálása után jóváhagyást/elutasítást kér a kijelölt személytől. Jóváhagyás esetén a MAC címhez tartozó hálózati port frissítésre kerül, míg elutasítás esetén a MAC cím nem kap hozzáférést a támogatott integrációval rendelkező hálózati hozzáférés vezérlőn a jelzett port-on keresztül a hálózathoz,
  - az Egypontos hozzáférés (SCB, jump station) megkerülését figyelő playbook, amely figyeli, hogyha egy kiszolgálóhoz egypontos hozzáférés megkerülésével csatlakoztak. Az észlelés és riasztás generálását követően jóváhagyást/elutasítást kér a kijelölt személytől. Jóváhagyás esetén nem történik művelet, míg elutasítás esetén a hozzáféréshez használt felhasználói objektum letiltásra kerül a címtárban,
  - az IDM technikai felhasználó megkerülésével végzett Active Directory és eDirectory tevékenységet figyelő playbook, amely figyeli, hogyha nem IDM technikai felhasználó segítségével történt tevékenység az Active Directory-ban és eDirectory-ban. Az észlelés és riasztás generálása után jóváhagyást/elutasítást kér a kijelölt személytől. Jóváhagyás esetén nem történik művelet, míg elutasítás esetén a hozzáféréshez használt felhasználó letiltásra kerül a címtárban.
- A SIEM rendszer kialakítását követően el kell készíteni a Megvalósulási, telepítési és az üzemeltetési dokumentációt

- A dokumentációk elkészítését követően egy alkalommal, egy napos terjedelmű oktatást kell tartani legfeljebb 5 fő rendszeradminisztrátor részére a Recon, ESM, SOAR és Eseményforrás illesztés témakörében.
- A projektben megvalósított tartalmi elemek (korrelációk, playbookok) funkcionalitása csak a megfelelő naplótartalom mellett garantálhatók.

A bevezetni kívánt SIEM rendszer által nyújtott gyűjtő, tároló, elemző és végrehajtó képességek

Az ArcSight Platform képességei (SIEM rendszer alapja)
A Kubernet-es alapoknak köszönhetően a rendszer egyszerűen és könnyen skálázható további master és worker node-ok bevonásával.
A rendszerhez széleskörű közösségi támogatás érhető el a MicroFocus Marketplace-en keresztül.
Egységes séma a rendszer komponensein belül, illetve SSO biztosítása a rendszeren belül.
Rendszer lehetőséget biztosít LDAP-on keresztül történő felhasználó hitelesítésre.
Az ArcSight SmartConnector képességei (gyűjtő komponens)
Az ArcSight SmartConnectorok gyári támogatással képesek gyűjteni a következő eseményforrásokat: - Apache webszerverek - Microsoft Active Directory and Windows - Microsoft IIS - Microsoft SQL Server - NetIQ eDirectory - NetIQ iManager - Oracle Audit Database - RSA Authentication Manager - Red Hat Enterprise Linux - Suse Linux Enterprise Server - Symantec Endpoint Protection - Novell NSS Fájl audit - Websense Web Security - VMWare ESXi

- CheckPoint Firewall - Fortigate Firewall - Barracuda WAF - Cisco ISE - Cisco switchek és routerek
Több mint 480 azonnal használható gyári támogatással rendelkező Connector.
A gyűjtő réteg, azaz a SmartConnectorok végzik az összegyűjtött események normalizálását és gazdagítását egy egységes CEF formátumra.
A telepített SMC-k menedzselése egy központi menedzsment felületen keresztül tehető meg. A központi felület az ArcSight Managment Center.
A gyűjtő réteg lehetségessé teszi a gyártó által nem támogatott alkalmazások, rendszerek illesztését egy FlexConnector Framework keretrendszer segítségével.
A rendszerbe telepíthető SmartConnectorok száma nincsen licenszeléshez kötve.

Az ArcSight Transformation HUB képességei (disztribúciós komponens)
Az összegyűjtött adatok eljuttatása egyszerűbb a megfelelő feldolgozó komponens felé (Tároló komponens, Elemző komponens).

Az ArcSight Recon képességei (Tároló komponens)
A feldolgozott naplóadatok bizalmassága, sértetlensége biztosítva van a tároló komponens által.
A rendszer adatbázisának köszönhetően a tároló komponens natív Big Data elemzést és jelentéskészítést tesz lehetővé.
Előre elkészített GDPR-nak megfelelő jelentéskészítési és dashboard lehetőségeket tartalmaz a tároló komponens.
Korai analízis a tárolt események között a fenyegetések felderítése érdekében.
A rendszer dinamikus lekérdezési javaslatokat ajánl a keresések írása közben a keresett események gyorsabb megtalálása érdekében.
A rendszer rendelkezik Nyers esemény nézettel.
A rendszer segítségével lehetséges mentett keresések készítése és futtatása.

Az ArcSight ESM képességei (Elemző komponens)
Az rendszer elemző komponense képes az eseményeket valós időben elemezni.
A rendszer rendelkezik dashboard felülettel.
Az elemző komponens képes riportok és dashboard-ok generálására.
A komponens rendelkezik beépített, azonnal használható, finomhangolható és módosítható riportokkal és dashboard-okkal.
A rendszer képes a korreláció teljesülésekor riasztás generálására és e-mailben történő kiküldésre.
Széles MITRE ATTACK integrációs lehetőség és beépített MITRE Dashboard.

Az Elemző komponens licenszéhez járó natív SOAR technológia.
Többszörös korrelációs technikák alkalmazása: Statisztikai, Fenyegetés agnosztikus, Termék agnosztikus, Munkamenet, Sebezhetőség, Eszköz.
Integrálási lehetőségek biztosítása fenyegetési hírcsatornákkal és keretrendszerekkel, mint például: MISP, Anomaly, RepSM+.

Az ArcSight SOAR képességei (Végrehajtó komponens)
100+ infrastruktúra és biztonsági eszköz integrációját teszi lehetővé a komponens.
Előre elkészített playbook-ok letöltésének lehetősége a Marketplace-ről.
Teljes és fél automatizált működési módot biztosít az incidensek osztályozásánál, kivizsgálásánál és az azokra való reagálásnál.

A rendszer komponensei által megvalósítható tartalmi elemek

Korrelációk
Gépvándorlás
Egypontos hozzáférési kapuk megkerülésének figyelése
IDM technikai felhasználó megkerülésének figyelése

Dashboard
Alert dashboard

Riportok
Riport az OTP autentikációval bejelentkező felhasználók, Direct Access felhasználók tevékenységéről
Top Network Issues from previous day
Top Attacks By Sources from previous day
Firewall traffic Trends
Adminisztrátori bejelentkezések (hálózati eszközök)

Unallowed HTTP Access – Ilias, Liferay stb.
Hálózati eszközök rendellenes működése

Intelligens beavatkozási folyamatok (Playbook-ok)
Gépvándorlás
Egypontos hozzáférés (SCB, jump station) megkerülés
IDM technikai felhasználó megkerülésével végzett Active Directory és eDirectory tevékenység.

A beszerzendő rendszer Mintakonfigurációja:

Cikkszám	**Megnevezés**	**Mennyiség**	**Mennyiségi egység**
SP-AI101	ArcSight Enterprise Security Manager Standard Edition 250 EPS SW E-LTU	1	db
SP-AI101-SUAA	ArcSight Enterprise Security Manager Standard Edition 250 EPS SW E-LTU Business Support*	1	db
SP-AN156	MF ArcSight Recon SE 2500 EPS SW E-LTU	1	db
SP-AN156-SUAA	MF ArcSight Recon SE 2500 EPS SW E-LTU Business Support*	1	db
MLIC_SZOLG 12	Rendszermérnök (óradíj)	824	óra

A megvalósított rendszerre a Szállítónak 1 év rendszergaranciát nyújt.

*A termékeket örökös licencelési konstrukcióval, 16 hónap termékkövetéssel kerülnek leszállításra (teljesítésre).

A Szállítónak az alábbi feladatokat kell elvégeznie az implementáció a rendszermérnöki óradíj keretében:

- felmérés, tervezés (fizikai, logikai)
- installáció, implementáció
- konfiguráció

- finomhangolás
- tesztelés
- üzemeltetői oktatás

A Szállítónak az alábbi dokumentációt kell átadnia az implementáció során

- Rendszerterv
- Megvalósulási dokumentáció (végleges rendszerterv és telepítési dokumentáció),
- Üzemeltetési dokumentáció.

A licence igazolás(ok) átadásának határideje: a szerződéskötéstől (a szerződés hatálybalépésétől) számított 30 napon belül.