opentext™

The Information Company

NIS2 megfelelés támogatása OpenText termékekkel

1 NIS2 megfelelés támogatása

A NIS2 direktíva számos fejezetre osztva taglalja azokat a követelményrendszereket, amelyekkel szemben a vonatkozó szervezeteknek meg kell felelniük. Ezen követelmények között több olyan is található, amiket egy megfelelő eszköz hiányában szinte lehetetlen teljesíteni.

Az OpenText portfóliójában számos olyan termék található, amelyek segítenek több, a NIS2 által megfogalmazott követelményeknek megfelelni. Az alábbiakban olvashatóak azok a NIS2 fejezetek és követelmény csoportok, amelyekben a megjelölt OpenText termékek támogatást nyújtanak a megfelelés elérésében. A dokumentum 2. fejezetében bővebb leírás található az egyes termékekről további forrás megjelölésekkel.

1.1 Hozzáférés-felügyelet

A Hozzáférés-felügyelet követelményrendszer a NIS2 direktíva 2. fejezetében található. Az alábbi táblázat első oszlopa tartalmazza azokat a követelmény csoportokat, amelyekben a megjelölt OpenText termékek támogatást nyújtanak a megfelelés teljesítésében.

	Identity Manager	Access Manager	ZENworks Configuration Management	Advanced Authentication	ZENworks ESM
Fiókkezelés	X	X			
Hozzáférési szabályok érvényesítése	X	X			
Felelősségek szétválasztása	X				
Legkisebb jogosultság elve	X				
Sikertelen bejelentkezési kísérletek			X	X	
Külső rendszerek használata					X
Információmegosztás	X				

1.2 Naplózás, elszámoltathatóság

A “Naplózás, elszámoltathatóság” a NIS2 direktíva 4. fejezetében található. Az **OpenText™ Security Log Analytics**, valamint az **ArcSight Logger** termék segíti a felhasználókat a naplóállományok összeggyűjtésében, elemzésében, védelmében, archiválásában.

1.3 Értékelés, engedélyezés és monitorozás

Az “Értékelés, engedélyezés és monitorozás” követelményrendszert a NIS2 direktíva 5. fejezete tartalmazza. Ebben a fejezetben olvasható a “Behatolásvizsgálat” követelmény, mely rendszeres sérülékenységvizsgálatot ír elő a szervezet alkalmazásaival szemben.

Az OpenText portfóliójában található a **OpenText Fortify** termékcsalád, mely számos piacelemzőnél vezető pozíciót tölt be az alkalmazások sérülékenységvizsgálatát végző termékek csoportjában. Segítségével rendszeres sérülékenységvizsgálat végezhető az alkalmazásokkal szemben.

1.4 Konfigurációkezelés

A “Konfigurációkezelés” a NIS2 direktíva 6. fejezetében található. A konfiguráció változások kezelését, a rendszerelem leltárt, a szoftverhasználat menedzselését, korlátozását az alábbi OpentText termékek támogatják: **Service Management X (SMAX), Asset Management X (AMX), Universal Discovery and CMDB (UD/UCMD), valamint a ZENworks termékcsalád**.

1.5 Azonosítás és hitelesítés

Az “Azonosítás és hitelesítés” a NIS2 direktíva 8. fejezetében található. Az alábbi táblázat tartalmazza azon követelmény csoportokat és OpenText termékeket, melyek támogatást nyújtanak a megvalósításban.

	Access Manager	Advanced Authentication
Azonosítás és hitelesítés (felhasználók)	X	X
A hitelesítésre szolgáló eszközök kezelése		X
Helyzetfüggő hitelesítés		X

1.6 Biztonsági események kezelése

A “Biztonsági események kezelése” a NIS2 direktíva 9. fejezetében található. Az alábbi táblázat tartalmazza azon követelmény csoportokat és OpenText megoldásokat, melyek támogatást nyújtanak a megfelelősség elérésében.

	OpenText™ Enterprise Security Mgr	OpenText™ Core Behavioral Signals
Automatizált eseménykezelő folyamatok	X	
Dinamikus újrakonfigurálás	X	
Információk korrelációja	X	
Rendszer automatikus leállítása	X	
Belső fenyegetések	X	
Viselkedéselemzés		X
Biztonsági műveleti központ	X	
Automatizált nyomon követés, adatgyűjtés és elemzés	X	
Automatizált jelentés	X	
Eseményekkel kapcsolatos sérülékenységek	X	
Segítségnyújtás a biztonsági események kezeléséhez	X	
Információszivárgásra adott válaszlépések – Illetéktelen hozzáférés	X	

1.7 Karbantartás

A „Karbantartás” a NIS2 direktíva 10. fejezetében található. Ez a fejezet előírja a távoli bejelentkezés során használt autentikáció megerősítését. Ebben az **OpenText Advanced Authentication** megoldása nyújt támogatást.

1.8 Adathordozók védelme

Az „Adathordozók védelme” a NIS2 direktíva 11. fejezete tartalmazza. Az adathordozók használata során felügyelni kell, hogy csak az engedélyezett eszközök kerüljenek engedélyezésre a szervezetben található felhasználói végpontokon. A ZENworks termékcsaládban lévő **ZENworks Endpoint Security Management** többek között ezt a szolgáltatást is biztosítja.

2 Termékismertetők

2.1 OpenText IAM (Identity and Access Management) termékcsalád

2.1.1 OpenText Access Manager

Az Access Manager segítségével egypontos hozzáférés kezelés valósítható meg, melynek segítségével szabályozható, hogy a belső felhasználók, külső ügyfelek-partnerek milyen időszakban, honnan, és milyen autentikációs metódussal férhetnek hozzá a vállalat webes erőforrásaihoz. Külső vagy belső eszközről történő biztonságos hozzáférés kialakításához támogatja a multi-factor autentikációt, a szabályrendszer alapú alkalmazás hozzáférést és az adattitkosítást is. Továbbá egypontos bejelentkezést (Web Single Sign-On) nyújt, mely segítségével a felhasználók az első autentikációt követően automatikus belépéssel érhetik el további webes alkalmazásaikat. A külső, third party (SaaS) alkalmazások vagy szolgáltatások egyszerű és biztonságos eléréséhez biztosított a federáció lehetősége, melyhez olyan ipari szabványok támogatottak, mint a Secure Assertions Markup Language (SAML) és Liberty Alliance protokollok.

Termék főbb jellemzői:

- **Autentikációs metódusok széleskörű támogatása:** az igen elterjedt jelszavas védelmen túl x.509, RADIUS token-based, smart card, Kerberos, NMAS, OpenID, Time-Based One-Time Password (TOTP), Risk-based authentication, Social authentication, valamint egyedi fejlesztésű osztályok is támogatottak pl. SMS alapú azonosítás. Az autentikációs metódusok tetszés szerint kombinálhatóak, így létrehozva a multi-factor alapú autentikációt
- **Központi hozzáférés-kezelés webes alkalmazásokhoz**: vállalati webes alkalmazásokhoz történő külső vagy belső hozzáférések kezelhetősége és ellenőrizhetősége rendkívül nehézkessé válhat egy megfelelő eszköz hiányában. Az Access Manager lehetőséget ad ezen alkalmazások központi hozzáférés kezelésére és ellenőrzésére. A hozzáférés vezérlés történhet felhasználói csoporttagság, konténertagság vagy tetszőleges attribútum értéke, megléte alapján. Mindezt kiegészítve olyan kritériumokkal, mint a kliens IP-je, lokációja vagy a belépés időpontja
- **Egypontos bejelentkezés (Single Sign-On):** webes Single Sign-On, a felhasználóknak, partnereknek és ügyfeleknek egy jelszót vagy autentikációs rutint kell megjegyezniük, majd az első hitelesítést követően nincs szükség további autentikációra mindaddig, amíg a pillanatnyi biztonsági szintje elegendő az adott alkalmazás vagy szolgáltatás eléréséhez
- **Federáció támogatása:** federáció segítségével a felhasználók biztonságos hozzáférést kaphatnak a szervezeten kívüli, third party által nyújtott szolgáltatásokhoz és alkalmazásokhoz, illetve felhő alapú szolgáltatásokhoz (pl. Office 365, Salesforce, ServiceNow,

Google Apps) anélkül, hogy újra be kellene jelentkezniük. Valamint a federáció segítségével nincs szükség redundáns identitás forrás fenntartására és ezzel további felhasználói adminisztrációra

- **Ügyfelek és partnerek hozzáférés kezelésének (B2C) széleskörű támogatása:** alkalmazottak hozzáférés kezelése mellett egyre inkább igényként jelentkezik a külsős felhasználók (pl. ügyfelek, partnerek) hozzáférés menedzselésének lehetősége is. Az Access Manager számos funkcióval támogatja és egyszerűbbé teszi a B2C hozzáférés kezelést. Ilyen például a felhasználók önregisztrációjának támogatása és eszközeinek, alkalmazásainak adminisztrációja belső adminisztrációs erőforrás bevonása nélkül
- **Risk-based authentication:** kockázatalapú hitelesítési megoldásának segítségével biztonságosabbá tehetőek a web alapú szolgáltatások és alkalmazások. Az adminisztrátorok különféle kapcsolati jellemzők (felhasználó, kliens IP, lokáció, belépés időpontja, stb.) alapján kockázati profilokat hozhatnak létre, amelyek alapján meghatározhatják a személyazonosság-ellenőrzési szinteket
- **Mobil hozzáférés:** web alapú alkalmazások mobil eszközökön történő egyszerű elérhetőségére is megoldást nyújt. Támogatja a MobileAccess megoldást, amely gondoskodik a felhasználók biztonságáról és az egyszerű hozzáférésről
- **Alkalmazás portál:** beépített alkalmazás portálja segítségével a felhasználók akár laptopról, táblagépről vagy okostelefonról egy központi webes felületen keresztül érhetik el a jogosult alkalmazásaikat, illetve onnan indíthatják is azokat. A portál felülete könnyen áttekinthető, ezáltal gyorsabb navigálást tesz lehetővé
- **Önkiszolgáló jelszókezelés:** A Self Service Password Reset megoldás integrációjával a felhasználók önállóan, az ügyfélszolgálat közreműködése nélkül állíthatják vissza jelszavukat, vagy oldhatják fel fiókjaik zárolását
- **Testre szabható felhasználói portál**
- **Forgalom naplózás:** Teljes körű és testre szabható naplózás, valamint integrációs lehetőség OpenText ArcSight, illetve egyéb SIEM vagy Syslog szerver felé

Gyártói weboldal: Access Management Software | OpenText Access Manager
Data sheet: NetIQ Access Manager Data Sheet
Gyártói dokumentációk: Access Manager - Documentation | Micro Focus
Termék funkciókat bemutató videók: NetIQ Unplugged - YouTube
Termék funkciókkal kapcsolatos bemutató és konfigurációs videók: Access Manager - YouTube

2.1.2 OpenText Advanced Authentication

Az OpenText Advanced Authentication termék egy olyan multi-faktor autentikációt biztosító megoldás, mely több mint 20 autentikációs metódust támogatásával (pl. Smart Card, TOTP, Fingerprint, PKI, Radius, Smartphone, Voice OTP) és a számos integrációs lehetőség biztosításával (pl. SAML, OAuth, Radius, API, ADFS, Advanced Authentication Client) képes megvalósítani a multi-faktor autentikációt akár olyan alkalmazás esetén is, melyek alapvetően nem támogatják a multi-faktor típusú autentikációt. A központi webes konzolon keresztül menedzselhető a teljes autentikációs folyamat. Továbbá számos VPN megoldáshoz is jól illeszthető a többfaktoros autentikáció kialakításához. Az autentikációs láncok alkalmazásonként, felhasználónként és felhasználói csoportonként is egyénileg állíthatóak. Az Advanced Authentication megoldás on-prem és felhő alapú szolgáltatásként is igénybe vehető. Az integrációs interfészek mellett natív klienssel is rendelkezik, ezzel együtt segítségével megerősíthetőek a Windows, egyes Linux (SSH) és MacOS operációs rendszereken történő felhasználói belépések.

Termék főbb jellemzői:

- Széleskörű platform támogatás: Windows, OS X, Linux, Android és iOS
- Iparági szabványokon alapuló alkalmazásintegráció (pl. HSPD11, PKI12, OAuth, FIDO, OATH, RADIUS, FIPS 140, NFC ISO/IEC)
- On-Prem vagy SaaS alapú szolgáltatás implementáció és elérés lehetősége
- Magas rendelkezésre állású infrastruktúra biztosítása már meglévő terheléselosztó mellett
- Számos autentikációs metódus támogatása (pl. Smart Card, Soft and Hard token, Fingerprint, PKI, Radius, Smartphone, SMS OTP, Voice Call)
- Felhasználók megfelelő támogatásához külön Help Desk modul érhető el, melyen keresztül segíthetjük a felhasználókat például az eszköz és felhasználó párosításban, illetve egyszeri belépési jelszó generálást is biztosít
- Egyszeri ideiglenes jelszó generálása az azonnali belépéshez, ezzel áthidalva az esetleges autentikációs problémákat
- Kockázat alapú autentikáció támogatása, mely során a felhasználó egyes jellemzői (pl. beosztás, lokalizáció, történeti adatok) alapján dől el, hogy milyen szigorú autentikációt várunk el a sikeres belépéshez
- Multi-tenant támogatás

Gyártói weboldal: Multifactor Authentication | OpenText Advanced Authentication
Data Sheet: NetIQ Advanced Authentication Data Sheet | OpenText
Gyártói dokumentáció: Advanced Authentication 6.4
Rövid termékbemutató videó: NetIQ Advanced Authentication - Brief Intro
Videó bemutató VPN autentikáció integrációjához: Securing VPNs with Multi-Factor Authentication

2.1.3 OpenText Identity Manager

Az OpenText Identity Manager egy átfogó identitáskezelő megoldás, amely automatizálja a felhasználói identitások és hozzáférési jogosultságok kezelését. Segít a szervezeteknek a biztonság növelésében, a megfelelőség biztosításában és az adminisztratív terhek csökkentésében.

A termék főbb jellemzői:

- **Automatizált felhasználóéletciklus-kezelés:** A felhasználók létrehozása, módosítása és törlése automatikusan történik, a vállalati szabályoknak megfelelően.
- **Szerep alapú hozzáférés-szabályozás (RBAC):** A felhasználók hozzáférése a szerepeikhez igazodik, minimalizálva a túlzott jogosultságok kockázatát.
- **Hozzáférésellenőrzés és auditálás:** Rendszeres ellenőrzésekkel biztosítható, hogy a felhasználók csak a szükséges hozzáférésekkel rendelkezzenek, és ezzel kapcsolatban részletes auditnaplók is rendelkezésre állnak.
- **Jelszókezelés:** Biztonságos jelszókezelési szabályzatok, önkiszolgáló jelszóvisszaállítás és többfaktoros hitelesítés.
- **Integrációk:** Számos vállalati alkalmazással és rendszerrel integrálható, beleértve a felhőalapú szolgáltatásokat is.
- **Megfelelőség:** Segít a szervezeteknek a különböző megfelelőségi követelmények teljesítésében, mint például a GDPR, a NIS2 vagy a HIPAA.
- **Hozzáférési kérések és jóváhagyások:** Az alkalmazottak egyszerűen kérhetnek hozzáférést a szükséges erőforrásokhoz, és a jóváhagyási folyamat is automatizált.
- **Testre szabható megoldás.** A beépített fejlesztőeszközökkel a felhasználók minden jogosultságkezeléssel kapcsolatos igénye megvalósítható.

Az OpenText Identity Manager csökkenti a manuális adminisztrációt, növeli a biztonságot és segít a szervezeteknek a megfelelőségi követelmények teljesítésében.

Gyártói weboldal: OpenText Identity Manager
Data sheet: Identity Manager termékismertető
Gyártói dokumentációk: Identity Manager - Documentation
Termék funkciókat bemutató videók: NetIQ Unplugged - YouTube

2.1.4 OpenText Identity Governance

Az OpenText Identity Governance egy olyan megoldás, amely az identitások és hozzáférési jogosultságok felügyeletét automatizálja, így segít a szervezeteknek a megfelelőség biztosításában és a biztonsági kockázatok csökkentésében.

A termék főbb jellemzői:

- **Hozzáférési felülvizsgálatok és tanúsítványok:** Rendszeres felülvizsgálatokkal biztosítja, hogy a felhasználók csak a szükséges hozzáférésekkel rendelkezzenek.
- **Szerepkör-alapú hozzáférés kezelése (RBAC):** Automatizálja a hozzáférési jogosultságok kezelését a felhasználók szerepkörei alapján.
- **Szabálymegfelelőség és auditálás:** Részletes naplókat vezet a hozzáférési eseményekről, és segít a megfelelőségi követelmények teljesítésében.
- **Kockázatértékelés és elemzés:** Azonosítja a kockázatos hozzáférési mintákat és segít a kockázatok csökkentésében.
- **Hozzáféréskérések és jóváhagyások automatizálása:** Automatizálja a hozzáférési kérelmek és jóváhagyások folyamatát.
- **"Segregation of Duties" (SOD) követelmények kezelése:** Elemzi a feladatok szétválasztásának követelményeit, és segít az ütközések megelőzésében.
- **Integrációk:** Számos vállalati alkalmazással és rendszerrel integrálható.
- **Cloud alapú identitás felügyelet:** Felhő alapú rendszerek identitásainak kezelése.
- **Egyszerű bevezetés.** A szoftver legújabb verziója képes magától beolvasni a cégnél használatban lévő beállításokat és elemezni azokat, majd ezek alapján automatikusan ajánl kifejezetten a cég működésére optimalizált, intelligens jogosultságkezelési folyamatokat.

Az OpenText Identity Governance segít a szervezeteknek abban, hogy hatékonyan felügyeljék az identitásokat és hozzáférési jogosultságokat, ezzel csökkentve a biztonsági kockázatokat és biztosítva a megfelelőséget.

Gyártói weboldal: OpenText Identity Governance
Termékismertető: IGA Buyer's Guide
Gyártói dokumentációk: Identity Governance - Documentation
Termék funkciókat bemutató videók: NetIQ Unplugged - YouTube

2.2 OpenText Threat Detection and Response termékcsalád

2.2.1 OpenText™ Security Log Analytics (korábban ArcSight Recon)

Az OpenText Security Log Analytics egy átfogó naplókezelő és biztonsági elemző megoldás, amely segíti a szervezeteket a biztonsági események gyors és hatékony elemzésében, a fenyegetések proaktív felderítésében és a megfelelőségi követelmények teljesítésében.

- **Központosított naplókezelés:** Összegyűjti és tárolja a naplókat a szervezet különböző rendszereiből (tűzfalak, behatolás-érzékelő rendszerek, alkalmazások stb.). Nagy mennyiségű naplóadatot képes kezelni és hatékonyan indexelni.
- **Fejlett elemzési képességek:** Fenyegetésfelderítő és nyomozási funkciókat biztosít és segíti a felhasználókat a rendellenességek és a gyanús tevékenységek felismerésére.
- **Vizualizáció és jelentéskészítés:** Interaktív irányítópultokat és vizualizációkat kínál az elemzések eredményeinek megjelenítéséhez. Testreszabható jelentéseket készít a megfelelőségi követelményekhez és a biztonsági incidensekhez.
- **Integráció:** Integrálható más biztonsági eszközökkel és rendszerekkel (SIEM, SOAR stb.).
- **Gyors keresés:** Lehetővé teszi a biztonsági elemzők számára, hogy a naplók között nagyon gyorsan keressenek.

Előnyök:

- **Gyorsabb incidensreagálás:** Segít a biztonsági incidensek gyorsabb azonosításában és megoldásában.
- **Proaktív fenyegetésfelderítés:** Lehetővé teszi a fenyegetések korai felismerését és megelőzését.
- **Megfelelőség támogatása:** Segít a szervezeteknek a különböző szabályozási követelmények (például GDPR, NIS2, HIPAA) teljesítésében. Auditnaplókat és megfelelőségi jelentéseket készít.
- **Biztonsági kockázatok csökkentése:** Növeli a szervezet átláthatóságát és csökkenti a biztonsági kockázatokat.

További információ:

- Gyártói weboldal: OpenText Security Log Analytics
- Gyártói dokumentáció: ArcSight Recon - Documentation
- Videók a termékcsaládról: ArcSight Unplugged - YouTube

2.2.2 OpenText™ Enterprise Security Manager (korábban ArcSight ESM)

Az OpenText Enterprise Security Manager (ESM) egy átfogó biztonsági incidens- és eseménykezelő (SIEM) megoldás, amely segít a szervezeteknek a biztonsági fenyegetések valós idejű felismerésében, elemzésében és a rájuk való gyors reagálásban. Főbb jellemzők:

- **Valós idejű fenyegetésészlelés:** Folyamatosan figyeli a hálózati és rendszereseményeket, és azonnal riasztást küld a gyanús tevékenységekről. Korrelációs szabályok segítségével azonosítja a komplex fenyegetéseket.
- **Intelligens kockázatelemzés és priorizálás.** Több adatpontot és kritériumot megvizsgál egy egyedi prioritási képlet segítségével, hogy értékelje a kockázatot és meghatározza a biztonsági események súlyosságát.
- **Megfelelőség támogatása:** Segít a szervezeteknek a különböző szabályozási követelmények (például GDPR, NIS2. HIPAA) teljesítésében. Auditnaplókat és megfelelőségi jelentéseket készít.
- **SOAR képességek:** A SOAR (Security Orchestration, Automation and Response) funkciók révén automatizált munkafolyamatokat biztosít az incidensek gyors kivizsgálásához és megoldásához.
- **Jelentések, irányítópultok.** MITRE ATT&CK leképezést, moduláris irányítópultokat, több száz állítható korrelációs szabályt, valamint egyéni jelentéseket biztosít a nagyobb biztonság és a gyorsabb megtérülés érdekében.
- **Integráció:** Integrálható más biztonsági eszközökkel és rendszerekkel (tűzfalak, IDS/IPS, végpontvédelmi megoldások stb.).

Előnyök:

- **Gyorsabb fenyegetésészlelés és reakció:** Csökkenti a fenyegetések okozta károkat.
- **Javított biztonsági helyzet:** Csökkenti a szervezet biztonsági kockázatait.
- **Hatékonyabb biztonsági műveletek:** Automatizálja a biztonsági feladatokat.
- **Megfelelőség javítása:** Segít a szervezeteknek a szabályozási követelményeknek való megfelelésben.
- **Költségcsökkentés:** Az automatizálás gyorsabb megoldást eredményez, ami által a költségek is csökkennek.

További információ:

- Gyártói weboldal: OpenText Enterprise Security Manager
- Gyártói dokumentáció: ArcSight - Documentation
- Videók a termékcsaládról: ArcSight Unplugged - YouTube

2.2.3 OpenText™ Core Behavioral Signals (korábban ArcSight Intelligence)

Az OpenText Core Behavioral Signals egy fejlett elemzési megoldás, amely a felhasználói viselkedés elemzésével segít a szervezeteknek a csalások, a belső fenyegetések és más biztonsági kockázatok felderítésében.

Főbb jellemzők:

- **Viselkedéselemzés:** A felhasználói tevékenységek (például bejelentkezések, fájlhozzáférések, alkalmazáshasználat) folyamatos elemzésével azonosítja a szokásostól eltérő viselkedéseket. Gépi tanulási algoritmusokat használ a normál viselkedési minták meghatározására és a rendellenességek felismerésére.
- **Csalásfelderítés:** Segít azonosítani a csalárd tevékenységeket, például a fiókátvételt, a pénzügyi csalásokat és az adathalászatot. Valós idejű riasztásokat küld a gyanús tranzakciókról és tevékenységekről.
- **Belső fenyegetések felderítése:** Segít azonosítani a belső fenyegetéseket, például az adatlopást, az ipari kémkedést és a szabályszegést. Elemzi a felhasználói viselkedést a vállalati adatokhoz való hozzáférés és a kommunikáció terén.
- **Adaptív kockázatértékelés:** A felhasználói viselkedés alapján dinamikusan értékeli a kockázatokat. Lehetővé teszi a biztonsági intézkedések adaptálását a kockázati szinthez.
- **Integráció:** Integrálható más biztonsági eszközökkel és rendszerekkel (SIEM, hozzáférés-kezelés stb.).
- **Felhasználói profilok:** A felhasználói viselkedés alapján profilokat állít fel.

Előnyök:

- **Proaktív fenyegetésfelderítés:** Lehetővé teszi a fenyegetések korai felismerését és megelőzését.
- **Csökkentett csalási kockázat:** Segít csökkenteni a csalások okozta károkat.
- **Belső fenyegetések csökkentése:** A belső fenyegetések időben való felismerése.
- **Megfelelőség javítása:** Segít a szervezeteknek a szabályozási követelményeknek való megfelelésben.
- **Valós idejű válaszadás:** Lehetővé teszi, hogy gyorsan reagáljon a biztonsági eseményekre.

Gyártói weboldal: Threat Detection Software & User and Entity Behavior Analytics
Gyártói dokumentáció: ArcSight Intelligence CE 24.2 - Documentation
Termékbemutató videó: ArcSight Intelligence

2.3 OpenText Fortify termékcsalád

2.3.1 OpenText Fortify Static Code Analyzer (SCA)

A OpenText Fortify Static Code Analyzer (SCA) megoldással végzett statikus értékelések segítségével a fejlesztők azonosíthatják a sérülékenységeket a bináris, a forrás- vagy a bájtkódban a biztonságosabb szoftverfejlesztéshez. A termék több, mint 950 egyedi sérülékenységkategóriát különböztet meg és több, mint 25 programozási nyelvet támogat. A vizsgálatot követő eredménylistában található álpozitív eredmények kiszűrését egy tudásbázis segítheti. A biztonsági vizsgálat nem csak az elkészült alkalmazáson végezhető, hanem már a fejlesztés során, a fejlesztők által használt integrált fejlesztési környezetben (IDE) is folyamatosan történhet, így fejlesztők azonnali visszajelzést kapnak. Az auditált vizsgálati eredmények (például a kódsorok részletei és a javításra vonatkozó tanácsok) segítenek kialakítani a biztonságos kódolás bevált gyakorlatát. Továbbá a hozzáadható nyílt forráskódú komponenselemzéssel (Software Composition Analysis) azonosíthatóak a sérülékeny Open Source komponensek használata is. A OpenText Fortify Static Code Analyzer zökkenőmentesen illeszkedik a már meglévő agilis vagy DevOps folyamatokhoz – „kulcsrakész" integrált fejlesztési környezettel, build szerverrel, a folyamatos integráció képességével és hibakövetési integrációkkal. Főbb jellemzők:

- Alkalmazás sérülékenységek korai felismerése és javaslat azok javítására
- Több, mint 25 nyelv támogatása, például ABAP/BSP, ActionScript, Apex, ASP.NET, C# (.NET), C/C++, Classic ASP (VBScripttel), COBOL, ColdFusion CFML, HTML, Java (Android is), JavaScript/ AJAX/Node.js, JSP, MXML (Flex), Objective C/C++, PHP, PL/SQL, Python, Ruby, Scala, Swift, T-SQL, VB.NET, VBScript, Visual Basic és XML
- Nyílt forráskódú komponensek (Open Source) elemzése
- Valós idejű sérülékenységazonosítás és álpozitív eredmények kiszűrése a Security Assistant segítségével
- Integrált fejlesztői környezetek (IDE) támogatása (pl.: Eclipse, IntelliJ, Visual Studio, Visual Studio Code)
- Illeszkedés a DevOps folyamatokhoz- Build, CI/CD szerver, ticketing rendszerekkel gyártói integráció
- Jól skálázható, optimalizálható architektúra a sérülékenységvizsgálat kiszolgálására (Fortify ScanCentral)

Gyártói weboldal: OpenText Fortify Static Code Analyzer | Static Code Analysis Security
Data sheet: Fortify Static Code Analyzer: Static application security testing Data Sheet
Open Source komponens vizsgálat rövid tájékoztató: micro-focus-fortify-and-sonatype-deliver-360-degree-view-of-application-security-brochure.pdf
Fortify fejlesztői eszközök integrációs oldal: Application Security Integration Ecosystem | CyberRes
Gyártói dokumentációk: Fortify Static Code Analyzer and Tools - Documentation | Micro Focus
Rövid bemutató videók az egyes funkciókról: Fortify Unplugged - YouTube

2.3.2 OpenText Fortify WebInspect

Az OpenText Fortify WebInspect egy hatékony és rugalmas eszköz, amely segít a webalkalmazások biztonságának növelésében és a sebezhetőségek gyorsabb felismerésében. A valós életből vett, automatikus és manuális hackelési technikákat és támadásokat utánozva, átfogóan elemzi a komplex webalkalmazásokat és webszolgáltatásokat (API) futás közben saját környezetében. Az automatikus dinamikus vizsgálat a Fortify termékcsaládból a WebInspect komponens segítségével érhető el. A tesztelés a jól felkészült hackerek által kihasznált sérülékenység típusokra összpontosít (pl. hitelesítés, hozzáférés-szabályozás, adatbevitel validálása, munkamenet-kezelés, üzleti logika tesztelése). A vizsgálat megkezdéséhez elég megadni egy URL-címet, és a WebInspect elvégzi a biztonsági tesztelést. Főbb jellemzők:

- **Dinamikus alkalmazásbiztonsági tesztelés (DAST):** A WebInspect a dinamikus alkalmazásbiztonsági tesztelés (DAST) technológiáját alkalmazza, amely a webes alkalmazások futás közbeni biztonsági kockázatait észleli.
- **A platform képes azonosítani a különböző sebezhetőségeket**, amelyeket az alkalmazás interaktív, valós környezetben történő használata során fedezhetünk fel, például a bejövő adatok kezelése, a session menedzsment vagy az autentikációs mechanizmusok gyenge pontjai.
- **Automatikus és manuális tesztelési módszerek:** A WebInspect képes teljesen automatizált módon tesztelni az alkalmazásokat, de lehetőség van manuális kiegészítésekre is, hogy a tesztelési folyamat a lehető legteljesebb legyen.
- **API biztonsági tesztelés:** Az API-k biztonsági problémái egyre nagyobb veszélyt jelentenek a webes alkalmazások számára. A WebInspect képes tesztelni a RESTful és SOAP API-kat, biztosítva, hogy az API-k ne legyenek a támadók célpontjai.
- **Integráció DevOps és CI/CD Környezetekkel:** A WebInspect könnyen integrálható a DevOps és CI/CD (folyamatos integráció, folyamatos fejlesztés) rendszerekbe, például Jenkins vagy Azure DevOps környezetekbe.
- **Makrókezelés:** egyéni makrók készítése, akár az automatizált autentikáció, akár egyéni alkalmazás folyamatok kezelésére
- **Kockázati pontszámítás:** Az eszköz egy kockázati pontszámítást biztosít, amely segít a sebezhetőségek prioritásának meghatározásában.
- **Részletes hibajelentés és javaslatok:** A WebInspect részletes riportokat generál a felfedezett biztonsági rések és sérülékenységek kategorizálásával. A rendszer automatikusan javaslatokat ad a problémák orvoslására, és megmutatja, hogyan javítható a biztonság az egyes hibák kiküszöbölésével.
- **Megfelelőségi riportok:** mint például PCI DSS, NIST 800-53, ISO 27K, OWASP, és HIPAA

Gyártói weboldal: OpenText Fortify WebInspect | DAST (Dynamic Application Security Testing) Analysis
Data sheet: Fortify WebInspect (DAST) Data Sheet | OpenText
Gyártói dokumentációk: Fortify WebInspect - Documentation | Micro Focus
Rövid bemutató videók az egyes funkciókról: Fortify Unplugged - YouTube

2.3.3 OpenText Fortify Software Security Center

A OpenText Fortify Software Security Center (SSC) megoldás segítségével egy központi felületen keresztül ellenőrizhetőek és követhetőek az alkalmazásbiztonsági programmal kapcsolatos események a teljes szoftverfejlesztési folyamat során. A felhasználók webes felületen keresztül tekinthetik meg, adminisztrálhatják és követhetik nyomon a szoftver biztonsági tesztelés eseményeit és eredményeit. A riport modul segítségével a beépített riportok mellett, egyedi riportokkal pontos és áttekinthető képet kaphatunk a biztonsági tesztelési folyamatról, valamint felhasználhatóak a folyamat optimalizálására is.

Főbb jellemzők:

- **Centralizált biztonsági központ:** A Fortify Software Security Center központi irányítópultot biztosít, amely egyesíti az alkalmazásbiztonsági tesztelés és a kockázatkezelési funkciókat. Ez lehetővé teszi a csapatok számára, hogy az összes szoftverbiztonsági adatot egyetlen platformon követhessék és kezelhessék.
- **Integrált statikus és dinamikus tesztelés:** A termék kombinálja a statikus (SAST) és dinamikus (DAST) tesztelést egy központi platformon, biztosítva ezzel, hogy a fejlesztők és a biztonsági szakemberek mindkét tesztelési módszert alkalmazhassák a különböző szintű alkalmazások esetén.
- **Kockázatkezelés és prioritáskezelés:** A Fortify Software Security Center nemcsak a hibák azonosítására, hanem azok priorizálására is lehetőséget ad. A rendszer elemzi a sebezhetőségek súlyosságát és segíti a csapatokat a legfontosabb kockázatok kezelésében.
- **Automatikus és testreszabható jelentéskészítés:** A platform automatikusan generál részletes riportokat, amelyek áttekinthetően ábrázolják a szoftverek biztonsági állapotát, a felfedezett hibákat és azok javítási állapotát.
- **SDLC integráció:** A Fortify Software Security Center integrálható a legnépszerűbb fejlesztői és CI/CD (folyamatos integráció, folyamatos fejlesztés) környezetekkel, mint például Jenkins, GitLab, és Azure DevOps, így a biztonsági tesztelés zökkenőmentesen illeszkedik a fejlesztési folyamatokba.
- **Könnyen használható és átlátható platform:** A Fortify Software Security Center felhasználói felülete intuitív és könnyen navigálható, lehetővé téve a csapatok számára, hogy gyorsan hozzáférjenek a szükséges információkhoz.

Gyártói weboldal: OpenText Enterprise Cybersecurity Solutions
Data sheet: Fortify Software Security Center Data Sheet | OpenText
Gyártói dokumentációk: Fortify Software Security Center - Documentation | Micro Focus
Rövid bemutató videók az egyes funkciókról: Fortify Unplugged - YouTube

2.4 Az OpenText IT Service Management termékcsalád

2.4.1 OpenText Service Management X (SMAX)

Az OpenText SMAX (Service Management Automation X) egy modern szolgáltatásmenedzsment platform, amely a mesterséges intelligencia és az automatizálás erejét használja a hatékonyság növelésére és a felhasználói élmény javítására.

Főbb jellemzők:

- **Mesterséges intelligencia (AI) és gépi tanulás (ML):** Automatizálja a rutinfeladatokat, mint a hibajegyek kategorizálása és az egyszerű problémák megoldása. AI-alapú javaslatokat ad a technikusoknak a problémák gyorsabb megoldásához.
- **Enterprise Service Management (ESM):** Nem csak az IT, hanem más vállalati területek (HR, létesítménygazdálkodás) szolgáltatásmenedzsmentjére is alkalmazható.
- **Önkiszolgáló portál:** Felhasználóbarát felület a problémák bejelentésére, szolgáltatások kérésére és hibajegyek nyomon követésére.
- **Mobilalkalmazás:** Hozzáférést biztosít az SMAX funkcióihoz mobileszközökről is.
- **Integrációk:** Könnyen integrálható más OpenText termékekkel és külső rendszerekkel.
- **Low code fejlesztési platform:** Testreszabható anélkül, hogy mélyreható programozási ismeretekre lenne szükség.

Előnyök:

- **Gyorsabb problémamegoldás:** Az automatizáció és az AI csökkenti az állásidőt.
- **Jobb felhasználói élmény:** Az önkiszolgáló portál és a mobilalkalmazás kényelmes szolgáltatáselérést biztosít.
- **Fokozott hatékonyság:** Az automatizálás csökkenti az IT-szakemberek terheit.
- **Költségcsökkentés:** Az automatizálás és a hatékonyságnövelés csökkenti a szolgáltatásmenedzsment költségeit.
- **Jobb döntéshozatal:** Átfogó jelentések és elemzések segítik a döntéshozatalt.

Az OpenText SMAX egy modern és innovatív megoldás a szolgáltatásmenedzsment optimalizálására és a digitális átalakulásra.

- Gyártói weboldal: OpenText Service Management (SMAX)
- Gyártói dokumentációk: SMAX Documentation - ITOM Practioner Portal
- Rövid bemutató videók az egyes funkciókról: OpenText SMAX - YouTube

2.4.2 OpenText Asset Management X (AMX)

Az OpenText Asset Management X egy átfogó eszközgazdálkodási megoldás, amely segíti a vállalatokat az eszközeik teljes életciklusának hatékony kezelésében. Ez magában foglalja az eszközök beszerzését, nyomon követését, karbantartását és leselejtezését.

Főbb jellemzők:

- **Eszközéletciklus-kezelés:** Az eszközök teljes életciklusának nyomon követése a beszerzéstől a leselejtezésig. Az eszközök állapotának és helyzetének valós idejű nyomon követése.
- **Karbantartásmenedzsment:** A karbantartási tevékenységek tervezése, ütemezése és végrehajtása. A karbantartási költségek és az állásidő csökkentése.
- **Eszközleltár:** Részletes információk az eszközökről, beleértve a hardver- és szoftverkonfigurációkat. A leltárpontosság és a megfelelőség javítása.
- **Munkafolyamat-automatizálás:** Az eszközgazdálkodási folyamatok automatizálása a hatékonyság növelése érdekében. A manuális munka csökkentése és a hibák minimalizálása.
- **Mobil hozzáférés:** Hozzáférés az eszközgazdálkodási információkhoz mobileszközökről. A terepen dolgozó technikusok támogatása.
- **Integrációk:** A vállalati adatok egységesítése. integráció más vállalati alkalmazásokkal pl. vállalatirányítási rendszerekkel.

Előnyök:

- **Költségcsökkentés:** Az eszközök jobb kihasználása, karbantartási költségek és az eszközvesztés csökkentése.
- **Hatékonyságnövelés:** Az eszközgazdálkodási folyamatok automatizálása, optimalizálása. Nagyobb átláthatóság az eszközök állapotáról.
- **Megfelelőség:** A szabályozási követelményeknek való megfelelés támogatása. A pontos adatok biztosítása az auditokhoz.
- **Jobb döntéshozatal:** Valós idejű adatok az eszközgazdálkodási döntések támogatására. Nagyobb rálátás az eszközpark állapotára.
- **Csökkentett kockázat:** Eszközleállások és a biztonsági kockázatok csökkentése.

További információ:

- Gyártói weboldal: OpenText Asset Management
- Gyártói dokumentációk: OpenText Asset Management Documentation
- Rövid bemutató videók az egyes funkciókról: OpenText AMX - YouTube

2.4.3 OpenText Universal Discovery and CMDB

Az OpenText Universal Discovery and CMDB (Configuration Management Database) termék egy átfogó megoldás, amely lehetővé teszi a szervezetek számára az informatikai infrastruktúrájuk automatikus feltérképezését, konfigurációjának nyomon követését és a konfigurációs elemek (CI-k) közötti kapcsolatok feltárását.

Főbb jellemzők:

- **Automatikus feltérképezés:** Automatikusan felfedezi a hardver- és szoftvereszközöket, a hálózati eszközöket, a virtuális gépeket és a felhőalapú erőforrásokat. A feltérképezés egyaránt történhet ügynökprogrammal vagy anélkül.
- **CMDB adattár:** Központi adattárat biztosít az összes konfigurációs elem (CI) és azok közötti kapcsolatok tárolására. Biztosítja a konfigurációs adatok pontosságát és naprakészségét.
- **Kapcsolatok feltárása:** Vizualizálja a CI-k közötti kapcsolatokat, segítve az incidensek okainak gyorsabb azonosítását és a változások hatásainak elemzését.
- **Szolgáltatásmodellezés:** Lehetővé teszi olyan szolgáltatásmodellek létrehozását, amelyek tükrözik az üzleti szolgáltatások informatikai függőségeit.
- **Integrációk:** Integrálható más ITSM (IT Service Management) eszközökkel, például incidens- és változáskezelő rendszerekkel. Több hibrid és multicloud környezeteket is támogat.

Előnyök:

- **Jobb rálátás az informatikai infrastruktúrára:** Teljes képet nyújt az eszközökről, az alkalmazásokról és a függőségekről.
- **Gyorsabb problémamegoldás:** Segít az incidensek okainak gyorsabb azonosításában és a változások hatásainak felmérésében.
- **Hatékonyabb változáskezelés:** Csökkenti a változásokkal járó kockázatokat és leállásokat.
- **Megfelelőség biztosítása:** Segít a szabályozási követelményeknek való megfelelésben.
- **Költségcsökkentés:** Optimalizálja az erőforrás-kihasználást és csökkenti a felesleges kiadásokat.

További információ:

- Gyártói weboldal: OpenText Universal Discovery and CMDB
- Gyártói dokumentációk: OpenText™ Universal Discovery and CMDB Documentation
- Rövid bemutató videók az egyes funkciókról: OpenText Universal Discovery & UCMDB (CMS) - YouTube

2.5 OpenText ZENworks termékcsalád

A Unified Endpoint Management (UEM) olyan integrált eszközkezelő megoldások átfogó készlete, amelyek automatizálják az informatikai feladatokat ezen eszközök teljes életciklusa során, beleértve a felderítést, az üzembe helyezést, a szoftverek telepítését és frissítését, a konfigurációkezelést, az adat- és végpontbiztonságot, valamint a javítócsomagok kezelését. Az OpenText ZENworks termékcsaládja ezeket a szolgáltatásokat biztosítja Windows, Linux, Mac, iOS és Android eszközökre a legkülönbözőbb vállalati környezetekben. (Pl. Active Directory vagy eDirectory alapú címtárak esetén.)

Legfontosabb termékjellemzők és előnyök

- Teljes körű munkaállomás felügyelet mind az asztali desktop, mind pedig a mobil eszközök esetében, akár eszköz, akár felhasználó alapon. (**ZENworks Configuration Management**)
- Hardver-szoftver leltár, távoli alkalmazás telepítés, távoli segítségnyújtás, imaging a minél hatékonyabb eszközfelügyelet érdekében. (**ZENworks Configuration Management**)
- Licencfelügyelet (Asset Management) biztosítása, eszköz felfedezés, leltár adatok, szoftver licencek rögzítésének lehetősége, megfelelőségi riportok. (**ZENworks Asset Management**)
- Végpontvédelmi megoldás biztonsági konfigurációk és előírások betartásának biztosítására (tűzfal, alkalmazás futtatási engedélyek, munkaállomás eszközök (USB, Bluetooth, Wifi stb.) engedélyezése v. tiltása, helyszín alapú felügyelet). (**ZENworks Endpoint Security Management**)
- Patch Management. A felügyelt eszközök operációs rendszerének (Windows, Linux) és az azokon lévő alkalmazások egy részének automatizált frissítése. (**ZENworks Endpoint Software Patch Management**)
- Teljes diszk vagy diszk partíciók titkosítása. (**ZENworks Full Disk Encryption**)

Termékismertető: https://www.microfocus.com/hu-hu/media/data-sheet/zenworks_configuration_management_ds_hu.pdf

Angol nyelvű terméklapok:

https://www.opentext.com/products/zenworks-configuration-management

https://www.opentext.com/products/zenworks-endpoint-software-patch-management

https://www.opentext.com/products/zenworks-asset-management

https://www.opentext.com/products/zenworks-full-disk-encryption

https://www.opentext.com/products/zenworks-endpoint-security-management

Dokumentáció: https://www.novell.com/documentation/zenworks-24.4/