opentext™

The Information Company

NIS2 megfelelés támogatása OpenText termékekkel

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.

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 Endpoint Security Mgmt
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				

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.

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.

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**.

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

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	

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.

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.