A RelNet portfóliója a NIS2 irányelv tükrében

v1.1 – Frissítve 2024. március 6-án

MAGYARÁZAT

Ebben a dokumentumban a RelNet Kft. közli **a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről szóló MK rendelet** intézkedéskatalógusának kivonatát, kiegészítve azt a RelNet portfóliójába tartozó azon gyártókkal, amelyek egy-egy követelmény teljesítésében segíthetnek.

A rendelet értelmében 2024. október 18-i hatálybalépéssel:

„A kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény (Kibertantv.) hatálya alá tartozó elektronikus információs rendszert a Kibertantv. szerinti érintett szervezet az 1. mellékletben felsorolt szempontok szerint sorolja biztonsági osztályba.”

„Az elektronikus információs rendszer felett rendelkezni jogosult szervezet a 2. mellékletben meghatározott, az elektronikus információs rendszerére érvényes biztonsági osztályhoz rendelt követelményeket az abban meghatározott módon teljesíti.”

Az alábbiakban a rendelet által definiált követelménycsaládok megnevezését és sorrendjét követjük.

KÖVETELMÉNYCSOPORTOK

1. Programmenedzsment
2. Hozzáférés-felügyelet
3. Tudatosság és képzés
4. Naplózás és elszámoltathatóság
5. Értékelés, engedélyezés, monitorozás
6. Konfigurációkezelés
7. Készenléti tervezés
8. Azonosítás és hitelesítés
9. Biztonsági események kezelése
10. Karbantartás
11. Adathordozók védelme
12. Fizikai és környezeti védelem
13. Tervezés
14. Személyi biztonság
15. Kockázatkezelés
16. Rendszer- és szolgáltatásbeszerzés
17. Határvédelem
18. Rendszer- és információsértetlenség
19. Ellátási lánc kockázatkezelése

A teljesség kedvéért a fenti listában szerepeltetjük a 3., 14. és a 19. fejezetet, de az alábbiakban nem foglalkozunk velük, mert a bennük felsorolt követelmények és intézkedések nem relevánsak a RelNet Kft. megoldásportfóliója szempontjából.

1. PROGRAMMENEDZSMENT

Követelménycsoport megnevezése	Releváns technológia	RelNet megoldás
1.5. Elektronikus információs rendszerek nyilvántartása	Asset Management, Change Management	ManageEngine, Netwrix - NNT, SolarWinds
1.6. Biztonsági teljesítmény mérése	Vulnerability Scanner, Network Performance Monitoring (NPM), Analytics, Penetration Testing	Progress - Flowmon, ManageEngine, Pentera, SolarWinds
1.10. Kockázatmenedzsment stratégia	CMDB	ManageEngine, SolarWinds
1.15. Tesztelés, képzés és felügyelet	Penetration Testing	Pentera, Skybox Security, SolarWinds

2. HOZZÁFÉRÉSFELÜGYELET

Követelménycsoport megnevezése	Releváns technológia	RelNet megoldás
2.2.-2.14. Fiókkezelés	Identity Access Management (IAM), Privileged Access Management (PAM), Active Directory Management	Fortinet, ManageEngine, Netwrix, SSH.COM, WALLIX
2.15. Hozzáférési szabályok érvényesítése	Identity Access Management (IAM), Privileged Access Management (PAM), Active Directory Management	Fortinet, ManageEngine, Netwrix, SSH.COM, WALLIX
2.59. Felelősségek szétválasztása	Identity Access Management (IAM), Privileged Access Management (PAM), Active Directory Management	Fortinet, ManageEngine, Netwrix, SSH.COM, WALLIX
2.60.-2.70. Legkisebb jogosultság elve	Zero Trust	ManageEngine, SSH.COM, WALLIX
2.71. Sikertelen bejelentkezési kísérletek	Authentication	Fortinet, ManageEngine
2.75. A rendszerhasználat jelzése	IT Operations Management (ITOM), Analytics	ManageEngine, SolarWinds, SSH.COM, WALLIX
2.81. Egyidejű munkaszakasz kezelés	Session Management	ManageEngine, SSH.COM, WALLIX
2.82.-2.83. Eszköz zárolása	Device Management, Endpoint Detection and Response (EDR)	Acronis, ManageEngine
2.84. A munkaszakasz lezárása	Session Management	Fortinet, ManageEngine, Netwrix, SSH.COM, WALLIX
2.88. Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek	Identity Access Management (IAM), Privileged Access Management (PAM)	Fortinet, ManageEngine, Netwrix, SSH.COM, WALLIX
2.100.-2.104. Távoli hozzáférés	Remote Access, Privileged Access Management (PAM)	Juniper Networks, Fortinet, ManageEngine, Netwrix, SSH.COM, Stormshield, WALLIX
2.108.2.112. Vezeték nélküli hozzáférés – Hitelesítés és titkosítás		Extreme Networks, Juniper Networks, Tenda, Transition Networks, Stormshield
2.113.-2.114. Mobil eszközök hozzáférés-ellenőrzése	Mobile Device Management (MDM)	Acronis, ManageEngine
2.115.-2.117. Külső elektronikus információs rendszerek használata	Remote Access, Privileged Access Management (PAM)	Juniper Networks, Fortinet, ManageEngine, Netwrix, SSH.COM, Stormshield, WALLIX

A táblázatban használt különböző háttérszínek elkülönítik a többi követelménycsoporttól azokat a követelménycsoportokat, amelyekre ugyanabból a gyártói körből szállítunk megoldásokat.

4. NAPLÓZÁS ÉS ELSZÁMOLTATHATÓSÁG

Követelménycsoport megnevezése	Releváns technológia	RelNet megoldás
4.2. Naplózható események	Security Information and Event Management (SIEM), Security Operations Center (SOC), Analytics	CYREBRO, Fortinet, Juniper Networks, ManageEngine, Netwrix - NNT, SolarWinds
4.3.-4.4. Naplóbejegyzések tartalma	Security Information and Event Management (SIEM), Security Operations Center (SOC), Analytics	CYREBRO, Fortinet, Juniper Networks, ManageEngine, Netwrix - NNT, SolarWinds
4.5. Naplózás tárkapacitása	Security Information and Event Management (SIEM), Security Operations Center (SOC), Analytics	CYREBRO, Fortinet, Juniper Networks, ManageEngine, Netwrix - NNT, SolarWinds
4.7.-4.9. Naplózási hiba kezelése	Security Information and Event Management (SIEM), Security Operations Center (SOC), Analytics	CYREBRO, Fortinet, Juniper Networks, ManageEngine, Netwrix - NNT, SolarWinds
4.13.-4.18. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel	Network Performance Monitoring (NPM), Analytics	Progress - Flowmon, ManageEngine
4.22.-4.23. Naplóbejegyzések csökkentése és jelentéskészítés	Security Information and Event Management (SIEM), Security Operations Center (SOC), Analytics	CYREBRO, Fortinet, Juniper Networks, ManageEngine, Netwrix - NNT, SolarWinds
4.24. Időbélyegek	Time Server	Microchip - Microsemi
4.25.-4.29. Naplóinformációk védelme	Security Information and Event Management (SIEM)	Fortinet, Juniper Networks, ManageEngine, Netwrix - NNT, SolarWinds
4.33. Letagadhatatlanság	Security Information and Event Management (SIEM), Automated Security Validation (ASV), Network Performance Monitoring (NPM), Security Operations Center (SOC)	Acronis, CYREBRO, ExtraHop, Progress - Flowmon, Fortinet, ManageEngine, Skybox Security, SolarWinds
4.38. A naplóbejegyzések megőrzése	Backup	Acronis

A táblázatban használt különböző háttérszínek elkülönítik a többi követelménycsoporttól azokat a követelménycsoportokat, amelyekre ugyanabból a gyártói körből szállítunk megoldásokat.

5. ÉRTÉKELÉS, ENGEDÉLYEZÉS, MONITOROZÁS

Követelménycsoport megnevezése	Releváns technológia	RelNet megoldás
5.10. Az intézkedési terv és mérföldkövei		Szakértői tanácsadás
5.15.-5.18. Folyamatos felügyelet	Analytics, IT Operations Management (ITOM), Network Detection and Response (NDR), Security Operations Center (SOC)	CYREBRO, ExtraHop, Progress - Flowmon, ManageEngine, Skybox Security, SolarWinds
5.25. Belső rendszerkapcsolatok		Szakértői tanácsadás

6. KONFIGURÁCIÓKEZELÉS

Követelménycsoport megnevezése	Releváns technológia	RelNet megoldás
6.2.-6.6 Alapkonfiguráció	Configuration Management, Asset Management	ManageEngine, Netwrix - NNT, Skybox Security, SolarWinds
6.7.-6.12. A konfigurációváltozások felügyelete (változáskezelés)	Configuration Management, Asset Management	ManageEngine, Netwrix - NNT, Skybox Security, SolarWinds
6.15.-6.17. Biztonsági hatásvizsgálatok	Vulnerability Management	ExtraHop, ManageEngine, Netwrix, Pentera, Skybox Security, SolarWinds
6.18.-6.19. A változtatásokra vonatkozó hozzáférés-korlátozások		Szakértői tanácsadás
6.23.-6.25. Konfigurációs beállítások	Configuration Management	ManageEngine, Skybox Security, SolarWinds
6.26.-6.31. Legszűkebb funkcionalitás		Szakértői tanácsadás
6.36.-6.40. Rendszerelem leltár	Asset Management	ManageEngine, Skybox Security, SolarWinds
6.45. Konfigurációkezelési terv		Szakértői tanácsadás
6.47. A szoftverhasználat korlátozásai	License Management	ManageEngine
6.49. Felhasználó által telepített szoftver	Access Management	ManageEngine

A táblázatban használt különböző háttérszínek elkülönítik a többi követelménycsoporttól azokat a követelménycsoportokat, amelyekre ugyanabból a gyártói körből szállítunk megoldásokat.

7. KÉSZENLÉTI TERVEZÉS

Követelménycsoport megnevezése	Releváns technológia	RelNet megoldás
7.19.-7.22. Biztonsági tárolási helyszín	Backup, Storage	Acronis
7.23.-7.27. Alternatív feldolgozási helyszín	Disaster Recovery (DR)	Acronis
7.35.-7.45. Az elektronikus információs rendszer mentései és helyreállítása, újraindítása	Backup and Restore	Acronis

8. AZONOSÍTÁS ÉS HITELESÍTÉS

Követelménycsoport megnevezése	Releváns technológia	RelNet megoldás
8.2.-8.7. Azonosítás és hitelesítés (felhasználók)	User Management, Account Management	ManageEngine, SSH.COM, WALLIX
8.10. Eszközök azonosítása és hitelesítése	Device Management, Endpoint Detection and Response (EDR)	ManageEngine, Netwrix - CoSoSys
8.14.-8.16. Azonosítókezelés	Identity Management, Account Management	ManageEngine, SSH.COM, WALLIX
8.21.-8.25. A hitelesítésre szolgáló eszközök kezelése	Device Management	Fortinet, ManageEngine, SSH.COM, WALLIX
8.36. Hitelesítési információk visszajelzésének elrejtése	Authentication, Account Management	ManageEngine, SSH.COM, WALLIX
8.37. Hitelesítés kriptográfiai modul esetén	Authentication, Account Management	ManageEngine, SSH.COM, WALLIX
8.38.-8.39. Azonosítás és hitelesítés (szervezeten kívüli felhasználók)	Authentication, Account Management	ManageEngine, SSH.COM, WALLIX
8.43. Újrahitelesítés	Authentication, Password Management	ManageEngine, SSH.COM, WALLIX
8.44.-8.49. Személyazonosság igazolása	Authentication, Account Management	ManageEngine, SSH.COM, WALLIX

A táblázatban használt különböző háttérszínek elkülönítik a többi követelménycsoporttól azokat a követelménycsoportokat, amelyekre ugyanabból a gyártói körből szállítunk megoldásokat.

9. BIZTONSÁGI ESEMÉNYEK KEZELÉSE

Követelménycsoport megnevezése	Releváns technológia	RelNet megoldás
9.5.-9.7. Biztonsági események kezelésének tesztelése	Security Information and Event Management (SIEM), Security Operations Center (SOC), DR, Monitoring	CYREBRO, Fortinet, Juniper Networks, ManageEngine, Netwrix - NNT, Skybox Security, SolarWinds
9.9.-9.20. Biztonsági események kezelése	Security Information and Event Management (SIEM), Security Operations Center (SOC), DR, Monitoring	CYREBRO, Fortinet, Juniper Networks, ManageEngine, Netwrix - NNT, Skybox Security, SolarWinds
9.25.-9.26. A biztonsági események nyomonkövetése	Security Information and Event Management (SIEM), Security Operations Center (SOC), DR, Monitoring	CYREBRO, Fortinet, Juniper Networks, ManageEngine, Netwrix - NNT, Skybox Security, SolarWinds
9.27.-9.30. A biztonsági események jelentése	Security Information and Event Management (SIEM), Security Operations Center (SOC), DR, Monitoring	CYREBRO, Fortinet, Juniper Networks, ManageEngine, Netwrix - NNT, Skybox Security, SolarWinds
9.31.-9.32. Segítségnyújtás a biztonsági események kezeléséhez	Security Information and Event Management (SIEM), Security Operations Center (SOC), DR, Monitoring	CYREBRO, Szakértői tanácsadás
9.34. Biztonsági eseménykezelési terv		Szakértői tanácsadás

A táblázatban használt különböző háttérszínek elkülönítik a többi követelménycsoporttól azokat a követelménycsoportokat, amelyekre ugyanabból a gyártói körből szállítunk megoldásokat.

10. KARBANTARTÁS

10. KARBANTARTÁS		
Követelménycsoport megnevezése	**Releváns technológia**	**RelNet megoldás**
10.3. Rendszeres karbantartás – Automatizált karbantartási tevékenységek	IT Operations Management (ITOM), Diagnostics, Patch Management, Firewall Management	Acronis, ManageEngine, Skybox Security, SolarWinds
10.11.-13. Távoli karbantartás	IT Operations Management (ITOM), Asset Management	ManageEngine, SolarWinds, SSH.COM, WALLIX
10.18.-10.19. Karbantartó személyek	Privileged Access Management (PAM)	Fortinet, ManageEngine, Netwrix, SSH.COM, WALLIX

11. ADATHORDOZÓK VÉDELME

Követelménycsoport megnevezése	Releváns technológia	RelNet megoldás
11.2. Hozzáférés az adathordozókhoz	Device Management, Data Loss Prevention (DLP), Endpoint Detection and Response (EDR)	Acronis, ManageEngine, Netwrix - CoSoSys, Stormshield
11.8.-11.11. Adathordozók törlése	Device Management, Data Loss Prevention (DLP), Endpoint Detection and Response (EDR)	Acronis, ManageEngine, Netwrix - CoSoSys, Stormshield
11.14. Adathordozók használata	Device Management, Data Loss Prevention (DLP), Endpoint Detection and Response (EDR)	Acronis, ManageEngine, Netwrix - CoSoSys, Stormshield

12. FIZIKAI ÉS KÖRNYEZETI VÉDELEM

Követelménycsoport megnevezése	Releváns technológia	RelNet megoldás
12.24. Áramellátó berendezések és kábelezés		CTS, Transition Networks
12.28.-12.29. Vészhelyzeti tápellátás		CTS, Transition Networks
12.44. Az információs rendszer elemeinek elhelyezése		Szakértői tanácsadás

13. TERVEZÉS

Követelménycsoport megnevezése	Releváns technológia	RelNet megoldás
13.2. Rendszerbiztonsági terv		Szakértői tanácsadás
13.3.-13.4. Viselkedési szabályok		Szakértői tanácsadás
13.6. Információbiztonsági architektúra leírása		Szakértői tanácsadás
13.10.-13.11. Biztonsági követelmények kiválasztása és testre szabása		Szakértői tanácsadás

15. KOCKÁZATKEZELÉS

Követelménycsoport megnevezése	Releváns technológia	RelNet megoldás
15.2. Biztonsági osztályba sorolás	CMDB	Szakértői tanácsadás
15.4.-15.5. Kockázatelemzés	Penetration Testing, Automated Security Validation (ASV), Analytics	ManageEngine, Netwrix, Pentera, Skybox Security, SolarWinds
15.9. Sérülékenységek ellenőrzése	Penetration Testing, Automated Security Validation (ASV), Analytics	ManageEngine, Netwrix, Pentera, Skybox Security, SolarWinds
15.10.-15.18. Sérülékenységmenedzsment	Penetration Testing, Automated Security Validation (ASV), Analytics	ManageEngine, Netwrix, Pentera, Skybox Security, SolarWinds
15.20. Kockázatokra adott válasz	Penetration Testing, Automated Security Validation (ASV), Analytics	ManageEngine, Netwrix, Pentera, Skybox Security, SolarWinds
15.21. Rendszerelemek kritikusságának elemzése	Penetration Testing, Automated Security Validation (ASV), Analytics	ManageEngine, Netwrix, Pentera, Skybox Security, SolarWinds

A táblázatban használt különböző háttérszínek elkülönítik a többi követelménycsoporttól azokat a követelménycsoportokat, amelyekre ugyanabból a gyártói körből szállítunk megoldásokat.

16. RENDSZER- ÉS SZOLGÁLTATÁSBESZERZÉS

Követelménycsoport megnevezése	Releváns technológia	RelNet megoldás
16.2. Erőforrások rendelkezésre állása	Resource Management	Extreme Networks, ManageEngine, Skybox Security, SolarWinds
16.58. Fejlesztői változáskövetés	DevOps, Configuration Management	ManageEngine, SolarWinds
16.66. Fejlesztői biztonsági tesztelés	Test Management, Penetration Testing	Pentera
16.87. Fejlesztői biztonsági architektúra és tervezés		Szakértői tanácsadás
16.99. Támogatással nem rendelkező rendszerelemek	Asset Management	ManageEngine, SolarWinds

17. HATÁRVÉDELEM

Követelménycsoport megnevezése	Releváns technológia	RelNet megoldás
17.2. Rendszer és felhasználói funkciók szétválasztása		SolarWinds
17.4. Biztonsági funkciók elkülönítése	Privileged Access Management (PAM), Network Management	Fortinet, ManageEngine, Netwrix, SSH.COM, Stormshield, WALLIX
17.10. Információk az osztott használatú rendszererőforrásokban		Radware
17.12. Szolgáltatásmegtagadással járó támadások elleni védelem	DDoS Protection, Network Detection and Response (NDR)	Allot, ExtraHop, Progress - Flowmon, ManageEngine, Radware
17.17.-17.35. A határok védelme	Firewall, Privileged Access Management (PAM), Network Detection and Response (NDR)	Extreme Networks, Fortinet, Juniper Networks, ManageEngine, Netwrix, SSH.COM, Stormshield, WALLIX
17.40.-17.41. Az adatátvitel bizalmassága és sértetlensége	Privileged Access Management (PAM), Quantum-Safe Encryption	Fortinet, ManageEngine, Netwrix, SSH.COM, WALLIX
17.49.-17.50. Kriptográfiai kulcs előállítása és kezelése	Key Management	ManageEngine, SSH.COM
17.53. Kriptográfiai védelem	Key Management, Encryption, Quantum-Safe Encryption	ManageEngine, SSH.COM
17.54. Együttműködésen alapuló informatikai eszközök távoli aktiválásának tiltása	Mobile Device Management (MDM), Asset Management	ManageEngine, SolarWinds
17.62. Nyilvános kulcsú infrastruktúra tanúsítványok	Key Management	ManageEngine, SSH.COM, WALLIX
17.63. Mobilkód korlátozása	Mobile Device Management (MDM)	ManageEngine
17.73. Munkaszakasz hitelessége	Session Management	ManageEngine, SSH.COM, WALLIX
17.77. Ismert állapotba való visszatérés	Disaster Recovery (DR)	Acronis
17.81.-17.82. Tárolt (at rest) adatok védelme	Data Loss Prevention (DLP), Secure File Transfer	Acronis, ManageEngine, SSH.COM

A táblázatban használt különböző háttérszínek elkülönítik a többi követelménycsoporttól azokat a követelménycsoportokat, amelyekre ugyanabból a gyártói körből szállítunk megoldásokat.

18. RENDSZER- ÉS INFORMÁCIÓSÉRTETLENSÉG

Követelménycsoport megnevezése	Releváns technológia	RelNet megoldás
18.2.-18.3. Hibajavítás	Patch Management	Acronis, ManageEngine, SolarWinds
18.8. Kártékony kódok elleni védelem	Anti-Malware, Anti-Ransomware, Penetration Testing, Endpoint Detection and Response (EDR), Network Detection and Response (NDR), XDR	Acronis, ExtraHop, Progress - Flowmon, Fortinet, Juniper Networks, ManageEngine, Pentera, Radware, Stormshield
18.13.-18.33. Az EIR monitorozása	IT Operations Management (ITOM)	Progress - Flowmon, ManageEngine, Skybox Security, SolarWinds
18.37.-18.38. Biztonsági riasztások és tájékoztatások	Endpoint Detection and Response, Security Operations Center (SOC), Network Detection and Response (NDR), Security Information and Event Management (SIEM)	CYREBRO, Progress - Flowmon, ExtraHop, ManageEngine, Skybox Security, SolarWinds
18.39. Biztonsági funkciók ellenőrzése	Change Management	ManageEngine, Netwrix - NNT, Skybox Security, SolarWinds
18.42.-18.53. Szoftver-, firmware és információsértetlenség	Asset Management, Change Management	ManageEngine, SolarWinds, Netwrix - NNT
18.66. Hibakezelés	Patch Management, Remediation	Acronis, ManageEngine, SolarWinds

A táblázatban használt különböző háttérszínek elkülönítik a többi követelménycsoporttól azokat a követelménycsoportokat, amelyekre ugyanabból a gyártói körből szállítunk megoldásokat.