axence®

A1 ICT Distribucija

Pet minut do polnoči: vaš končni seznam za preverjanje glede ZInfV-1



Govorniki



Miroslav Ekart

Pooblaščena oseba za varstvo podatkov (DPO) in Vodilni presojevalec tveganj informacijske varnosti za standard ISO/IEC 27005

Miroslav Ekart je diplomirani pravnik z opravljenim državnim pravniškim izpitom. Je tudi vodilni presojevalec (Lead Risk Manager) po standardu ISO 27005 (Information Security Risk Management).

Je soustanovitelj podjetja DATAINFO.SI, ki ponuja rešitve na področju varstva podatkov in informacijske varnosti več kot 300 strankam v Sloveniji, na Hrvaškem, v Srbiji, Švici, Nemčiji, Romuniji in na Malti. Sodeloval je pri več kot 50 projektih v okviru NIS2 in podobnih projektih, pri več kot 500 projektih v okviru GDPR ter v več kot 50 nadzornih postopkih pred slovenskim informacijskim pooblaščencem.

Poleg kvalifikacije ISO/IEC 27005 na področju upravljanja tveganj informacijske varnosti je pridobil mednarodna potrdila za pooblaščenca za varstvo podatkov, ki jih izdajajo Bureau Veritas, italijanski certifikacijski organ CEPAS in kanadski certifikacijski organ PECB. Poleg tega je član slovenskega združenja ISACA.



Marko Kašić

ICT inženir, A1 Slovenija, d.d.

Marko Kašić je vodilni inženir za informacijsko-komunikacijske tehnologije v podjetju A1 Slovenija z več kot 13 leti izkušenj na področju kibernetske varnosti. V svoji karieri je pridobil obsežno strokovno znanje na področju svetovanja o kibernetski varnosti, uvajanja rešitev ter tehnične podpore za stranke in partnerje.

Njegova ključna področja strokovnega znanja vključujejo varnost končnih naprav in omrežij, s posebnim poudarkom na uvajanju naprednih rešitev za odkrivanje incidentov kibernetske varnosti ter omogočanju organizacijam, da se na te hitro in učinkovito odzovejo s premišljenim sprejemanjem odločitev.

Marko aktivno podpira organizacije in tehnološke partnerje v celotni adrijski regiji, vključno s Slovenijo, Hrvaško, Črno goro, Bosno in Hercegovino ter Kosovom. Poleg tega, da partnerjem pomaga pri reševanju zapletenih varnostnih izzivov njihovih strank, redno deli svoje znanje in praktične izkušnje kot govornik na konferencah o kibernetski varnosti, strokovnih dogodkih in partnerskih prireditvah.

Ali je vaša organizacija pripravljena na ZInfV-1?

Kaj bi moralo biti že vzpostavljeno – in kaj lahko še popravite?



Preden začnete!

Zakaj ste postali zavezanci po ZInfv-1?

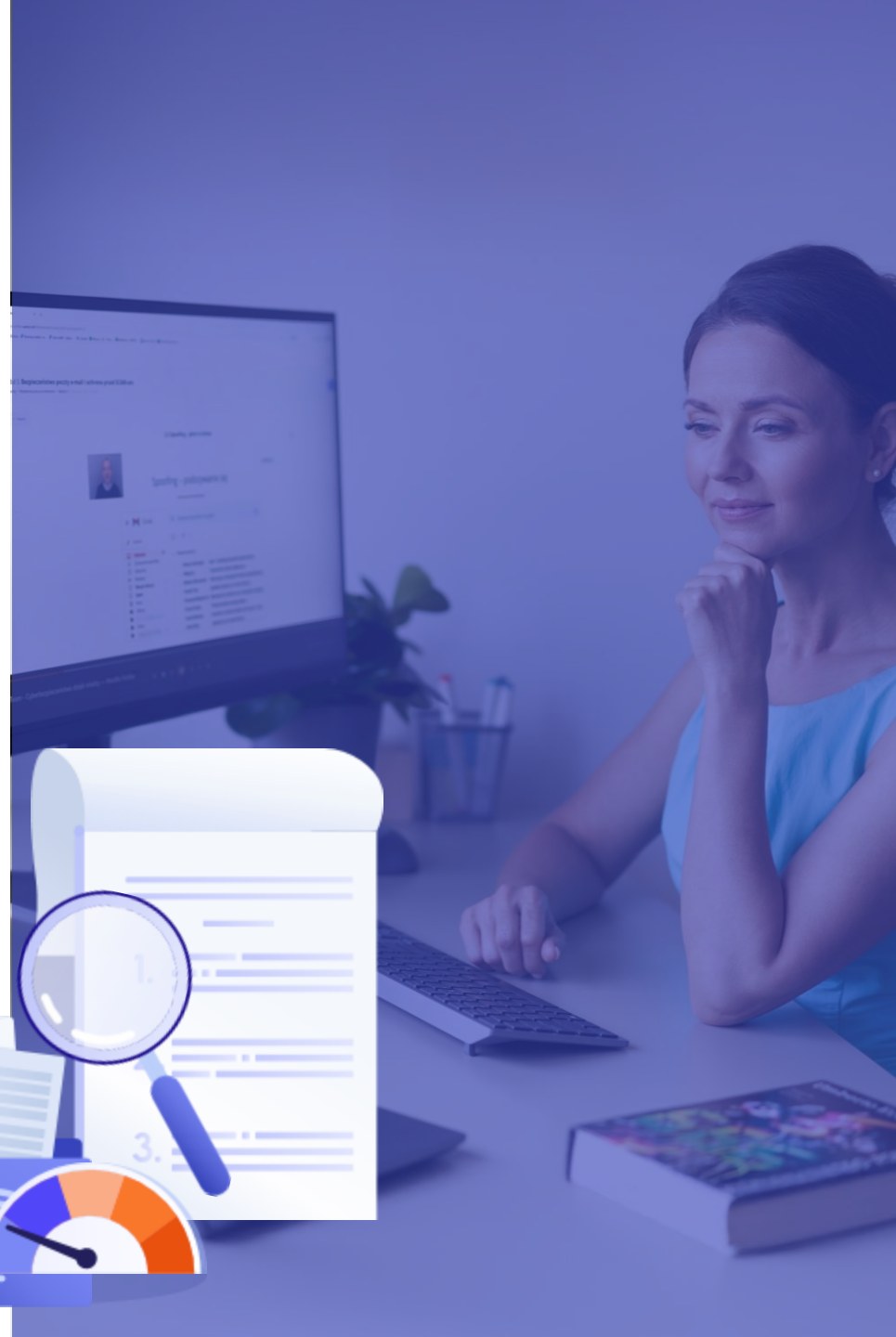
- Prilagodite zahteve, ukrepe,, dokumente, metodologije svoji organizaciji.
- Proizvodnja hrane ali strojegradnja ni enaka dobavi pitne vode.
- URSIV vzorci/predlogi so odlična osnova, niso pa (vsi) obvezni!



Obveznosti po 21. členu ZInfV-1

dokumentacija

1. **Politika informacijske varnosti**
2. **Popis sredstev** – ažuren seznam informacijskih in drugih sredstev ter podatkov, potrebnih za delovanje, z navedbo skrbnikov.
3. **Analiza tveganj**
4. **Neprekinjeno poslovanje (BCP Business Continuity Plan)** – politika in načrt z oceno vpliva (BIA Business Impact Analysis), minimalno ravnjo poslovanja, upravljanje varnostnih kopij
5. **Obnovitev sistemov** (DRP Disaster Recovery Plan)
6. **Odziv na incidente** – načrt z zaznavo in odzivom, vlogami ter protokolom obveščanja pristojnega CSIRT (SI CERT ali SIGOV CERT). Opredelite vloge, osebe, reakcijski čas, eskalcijo, krizno komuncirianje, način vodenja odziva, dokumentiranje...
7. **Načrt varnostnih ukrepov** – ukrepi za zaupnost, celovitost, razpoložljivost in avtentičnost, prilagojeni tveganjem in posebnostim subjekta.
8. **Merjenje učinkovitosti** – politika in postopki za presojo učinkovitosti ukrepov, s kazalniki (KPI) in analizo zbranih podatkov.



Popis sredstev - kaj pravi URSIV

Povzeto po predavanju/spletni delavnici URSIV z dne 17.9.2026 in dne 28.1.2026.

ZAKAJ JE UPRAVLJANJE SREDSTEV POMEMBNO?

Ustrezno načrtovan in izveden popis informacijskih sredstev omogoča organizaciji, da na pregleden način poveže storitve, informacijske sisteme, podatke, infrastrukturo, uporabniške in skrbniške račune ter dobavitelje v enotno sliko.

Brez ažurnega registra sredstev organizacija ne more:

- pravilno izvajati analize tveganj,
- vzpostaviti nadzora dostopa ali sledljivosti,
- učinkovito odzivati se na incidente,
- zaščititi kritične poslovne funkcije,
- dokazovati skladnosti z ZInfV-1, ISO 27001 ali NIST.



Popis sredstev - kaj pravi URSIV

- Povzeto po predavanju/spletni delavnici URSIV z dne 17.9.2026 in dne 28.1.2026.
- Seznam informacijskih sredstev se šteje za popolnega, če je popisanih najmanj 98 % kritičnih sredstev in najmanj 95 % vseh sredstev.
- Seznam informacijskih sredstev se šteje za pravočasnega, če so lastniki kritičnih sredstev 95 % zapisov potrdili v manj kot 3 mesecih od nastale spremembe in ostalih sredstev v manj kot 6 mesecih.Seznam informacijskih sredstev se šteje za točnega, če je zaznano 2 % ali manj odstopanj pri naključnih preverjanjih.
- Seznam informacijskih sredstev se šteje za skladnega, če je 100 % sprememb zabeleženih prek zahtevkov in je 100 % zapisov z dodeljenim lastnikom.



Obveznosti po 22. členu v ZInfV-1

Varnostni ukrepi

1. **Podpora vodstva** – zavezanost vodstva in vključitev inf. Varnosti v letni načrt poslovanja ali program dela.
2. **Integriteta kadrov** – preverjanje pred zaposlitvijo, med njo in ob prenehanju ali spremembi (23. člen).
3. **Kibernetska higiena in usposabljanje** – osnovne prakse in redno izobraževanje zaposlenih.
4. **Človeški viri in dostopi** – preverjanje identitete, določanje dostopnosti informacij, upravljanje pooblastil.
5. **Varnostne kopije** – izvajanje in upravljanje varnostnega kopiranja.
6. **Dnevniški zapisi** – beleženje in hramba logov o delovanju sistemov (24. člen).
7. **Upravljanje omrežnih in informacijskih sistemov**
8. **Kriptografija**
9. **Promet in komunikacije** – upravljanje omrežnega prometa in komunikacij.



Obveznosti po 22. členu v ZInfV-1

Varnostni ukrepi

10. **Dobavna veriga** – minimalne varnostne zahteve za ključne neposredne dobavitelje.
11. **Fizično varovanje** – fizična in tehnična zaščita prostorov
12. **Varnost aplikacij in razvoja** – varnostni mehanizmi v aplikacijah, varnost pri nabavi, razvoju in vzdrževanju, obravnava in razkrivanje ranljivosti.
13. **Tehnične ranljivosti** – upravljanje ranljivosti in preprečevanje njihove izrabe.
14. **Zlonamerna koda in vdori** – zaščita pred zlonamerno kodo, zaznavanje vdorov in preprečevanje incidentov.
15. **MFA** – večfaktorska ali neprekinjena avtentikacija
16. **Varne komunikacije** (kjer je to primerno)
17. **Oblačne storitve** – politike in postopke za uporabo oblaka.



Nadzorni posotpki so že v teku

Možne posledice in kazni

- Bistvenemu ali pomembnemu subjektu se bodo zaradi neizpolnjevanja obveznosti, ki izhajajo iz zakona, naložile / bi se lahko naložile kazni v naslednjih višinah:
  - primeru bistvenega **subjekta do 10 milijonov EUR** oziroma do 2 % prihodkov v preteklem letu;
  - primeru **pomembnega subjekta do 7 milijonov EUR** oziroma do 1,4 % prihodkov v preteklem letu.
- **OSEBNA ODGVORNOST VODSTVA** (globe do 10.000 EUR)
- Začasna prepoved opravljanja vodstvenih funkcij.
- Zamuda prijave v roku 24 ur je samostojen prekršek!



Uredili smo dokumentacijo in uvedli varnostne ukrepe. Kaj sedaj?

- Preglejte seznam vseh dokumentov in ga primerjajte z zahtevami 21. člena ZInfv-1
- Preglejte seznam vseh varnostnih zahtev in ga primerjajte z zahtevami 22. člena ZInfv-1. Posebej preverite ali imate popisana vsa sredstva.
- Dokumentirajte v obliki dokumenta, ki ga lahko predložite revizorjem/URSIV; tudi česa ne boste uvedli.
- Naredite načrt za informacijsko varnost za leto 2027 (KPI, naložbe, vloge, revizije/notranji nadzor, poročanja, izobraževanja, testiranje odziva na incidente...)
- Načrt 2027 sprejmite.



Uredili smo nekaj dokumentacije in uvedli nekaj varnostnih ukrepov. Kaj sedaj?

- Preglejte seznam vseh dokumentov in ga primerjajte z zahtevami 21. člena ZInfv-1. Dokončajte osnutke. Fokus na vašo dejavost, zaradi katere ste zvezanci.
- Preglejte seznam vseh varnostnih zahtev in ga primerjajte z zahtevami 22. člena ZInfv-1. Fokus na vašo dejavost, zaradi katere ste zvezanci.
- Dokumentirajte, kaj je v fazi uvajanja, nabave, razpisa, česa ne bo, kaj manjka... in kdaj predvidoma bo to končano (tudi če bo v 2027!) Dokumentirajte v obliki dokumenta, ki ga lahko predložite revizorjem/URSIV.
- Naredite načrt za informacijsko varnost za leto 2027 (varnostni ukrepi, KPI, naložbe, vloge, revizije/notranji nadzor, poročanja, izobraževanja, testiranje odziva na incidente...). Začnite 2027 s preveritvijo popisa sredstev.



- **NIS2 in ZinfV-1 se ne začneta z dokumenti.**
- **Začneta se z poznavanjem lastnih sredstev.**
- **Če ne vemo, katere naprave, uporabniki in podatki so v organizaciji, ne moremo učinkovito upravljati kibernetske varnosti.**



Axence že 21 let podjetjem in institucijam po vsem svetu ponuja profesionalne rešitve za celovito upravljanje IT-infrastrukture.

dinamična rast prodaje

6000 strank

globalni doseg

na trgu od leta 2005

nagrajenec strokovnih nagrad

97% stranke našo tehnično podporo ocenjujejo pozitivno

Centralno upravljanje
Izberite svoje module

- Celovita inventarizacija in preglednost sredstev (asset management)
- Spremljanje infrastrukture in odkrivanje incidentov
- Upravljanje incidentov in zahtevkov (ITSM / HelpDesk)
- Varstvo podatkov in nadzor uporabnikov
- Poročanje in revizije

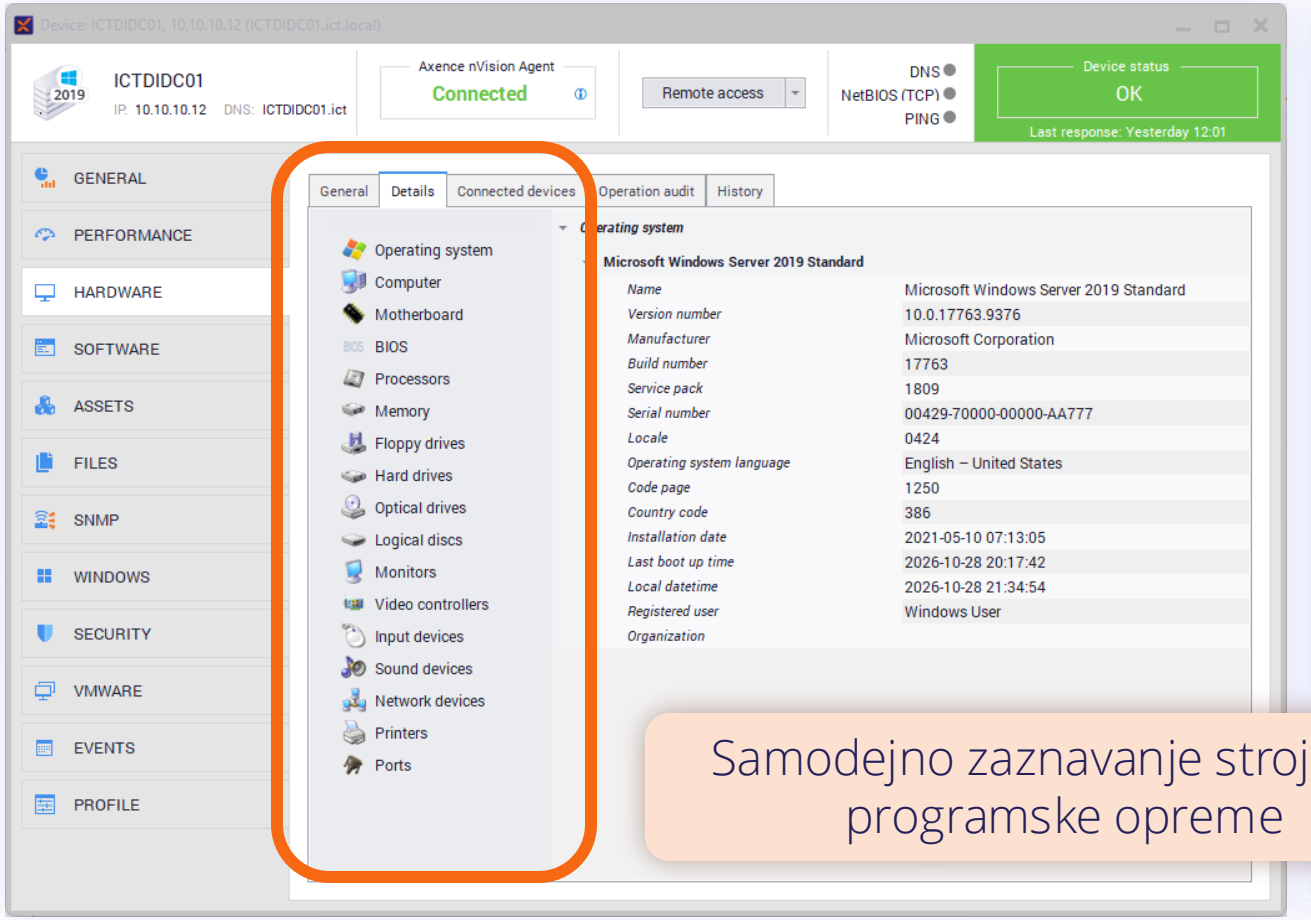


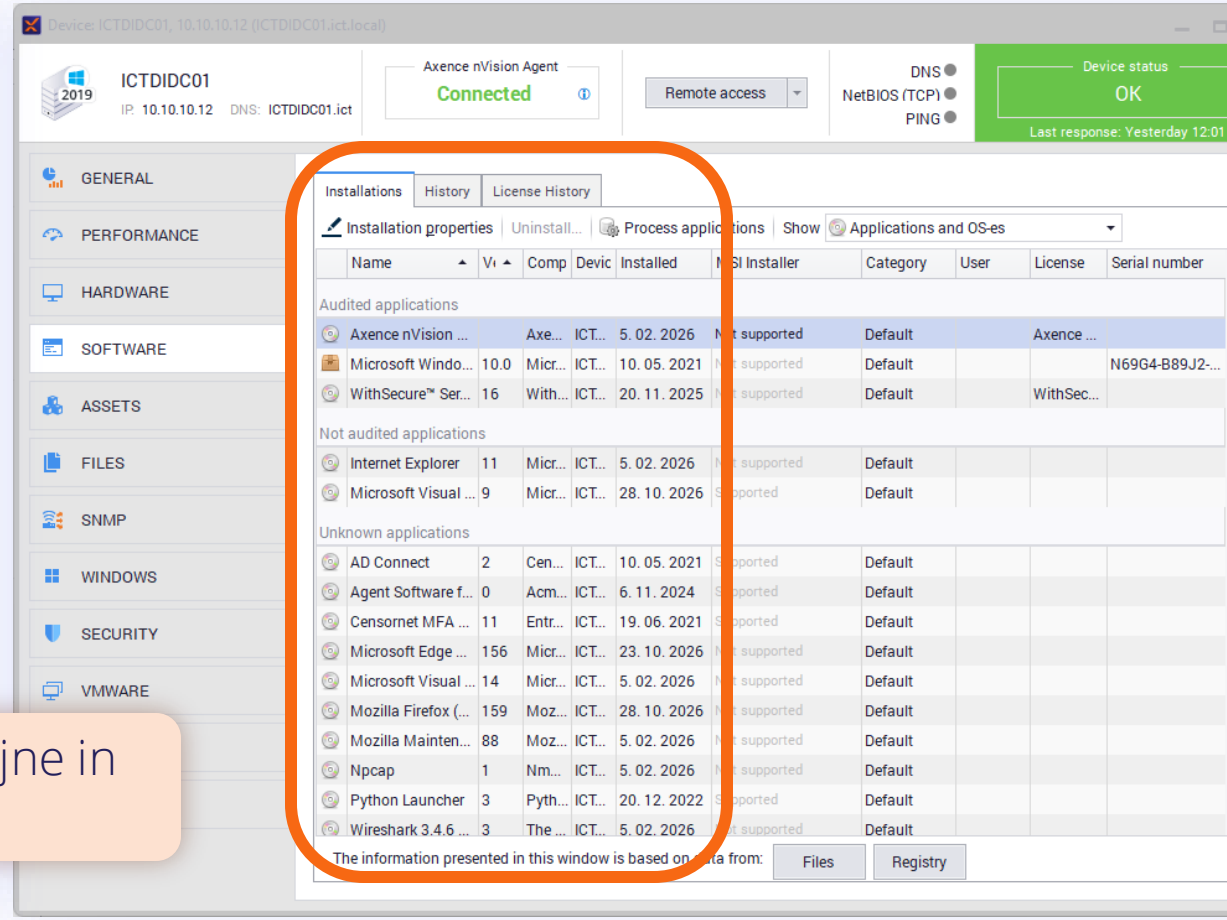


Live demo

Popoln pregled nad vsemi sredstvi – jasna odgovornost

A1 ICT Distribucija

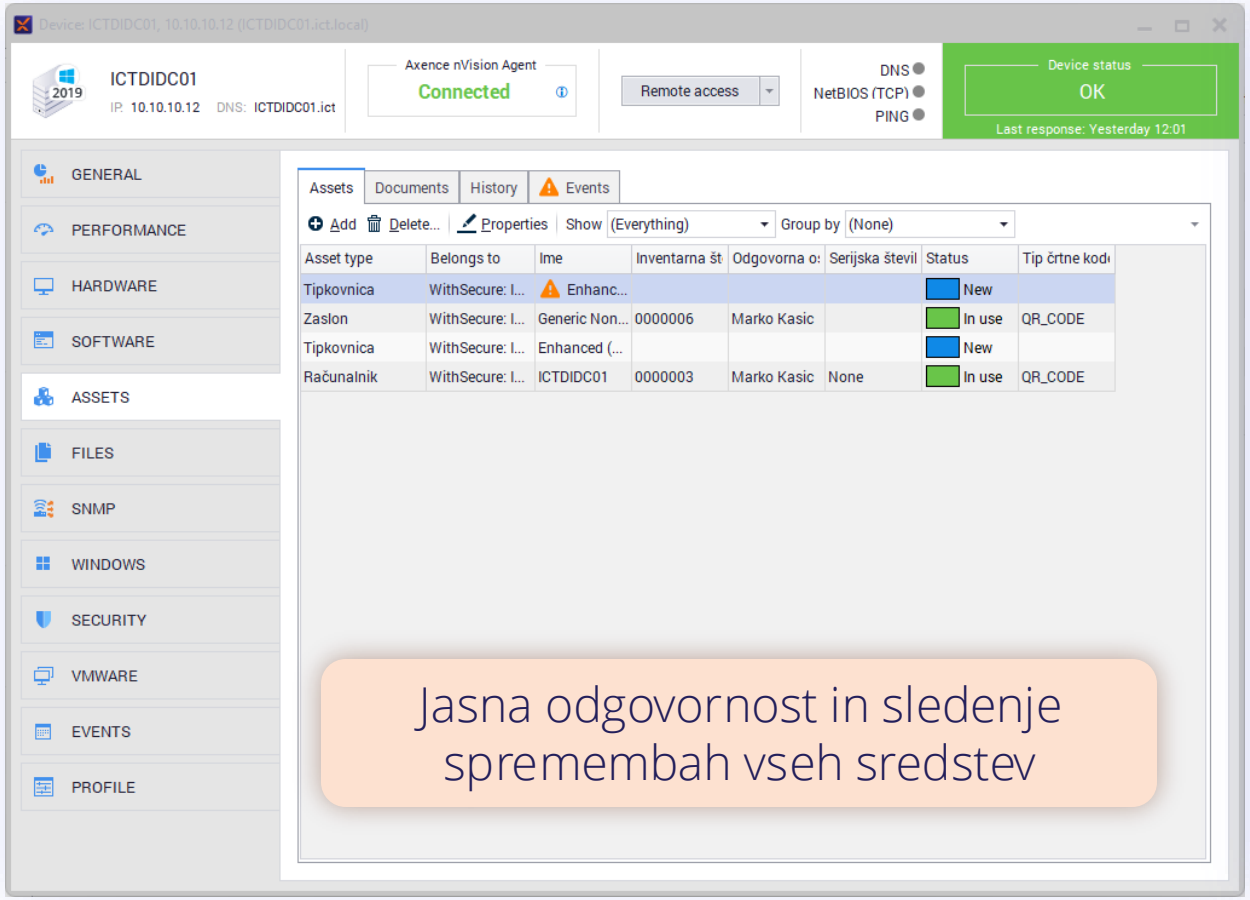


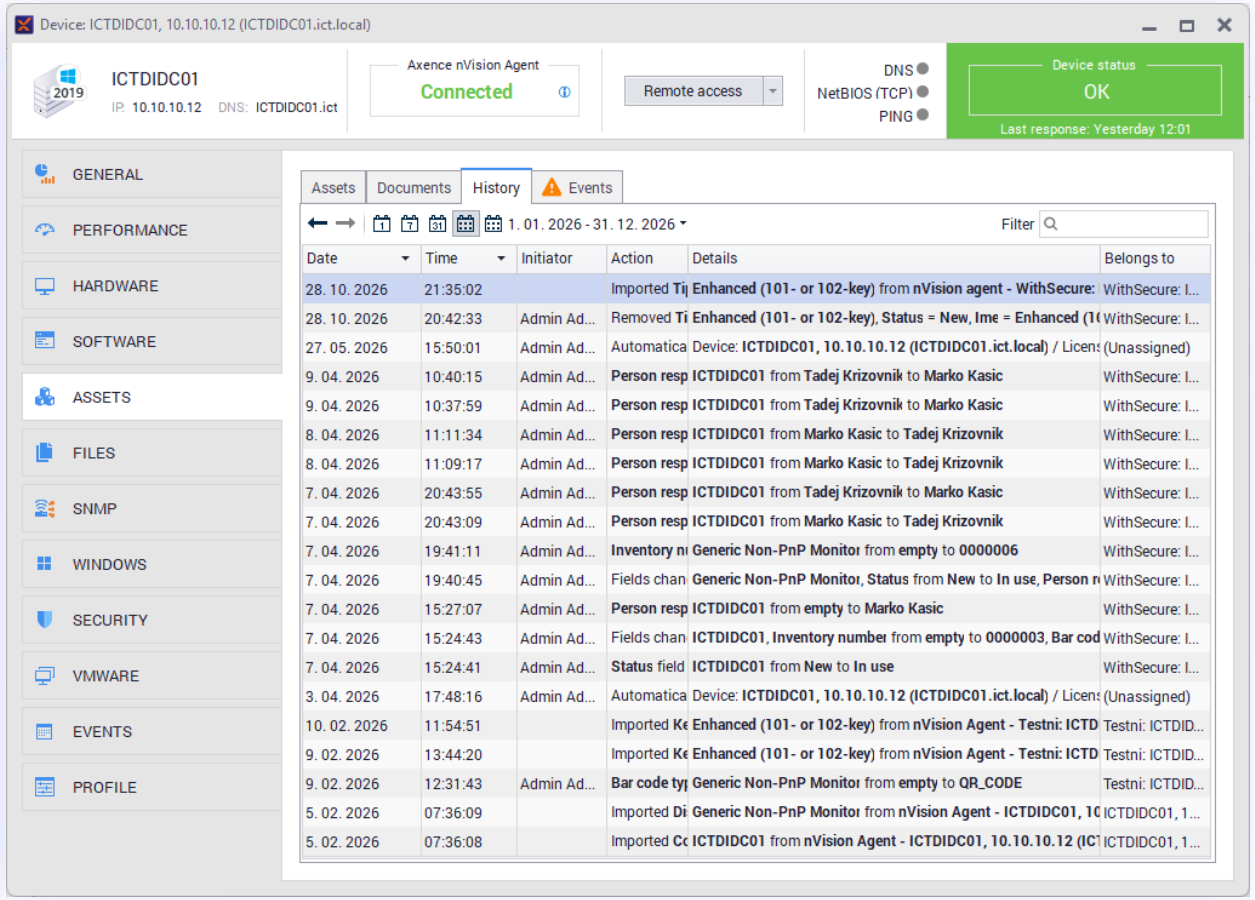


Samodejno zaznavanje strojne in programske opreme

Popoln pregled nad vsemi sredstvi – jasna odgovornost

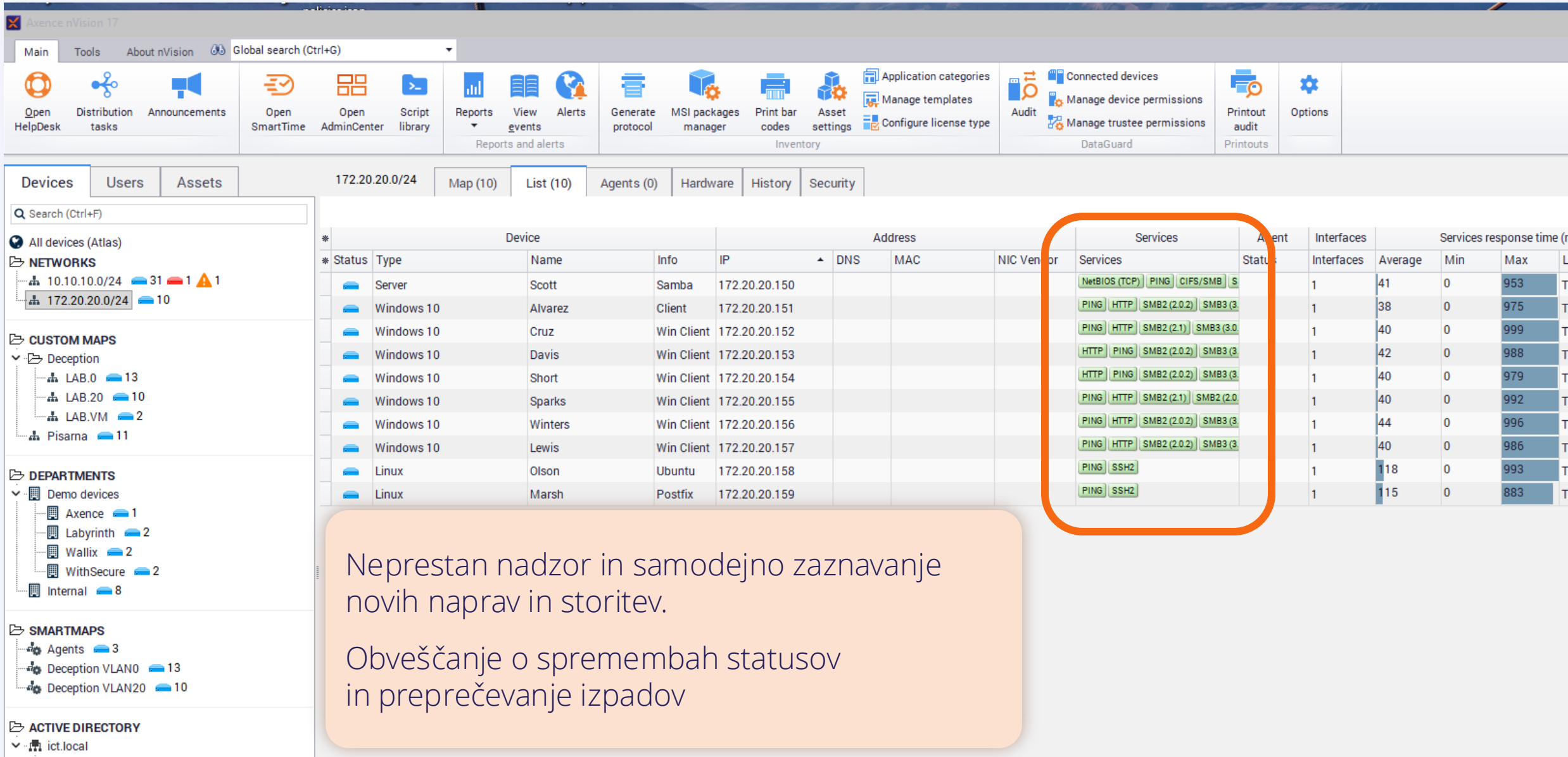
A1 ICT Distribucija





Neprestan nadzor in hitro zaznavanje incidentov

A1 ICT Distribucija

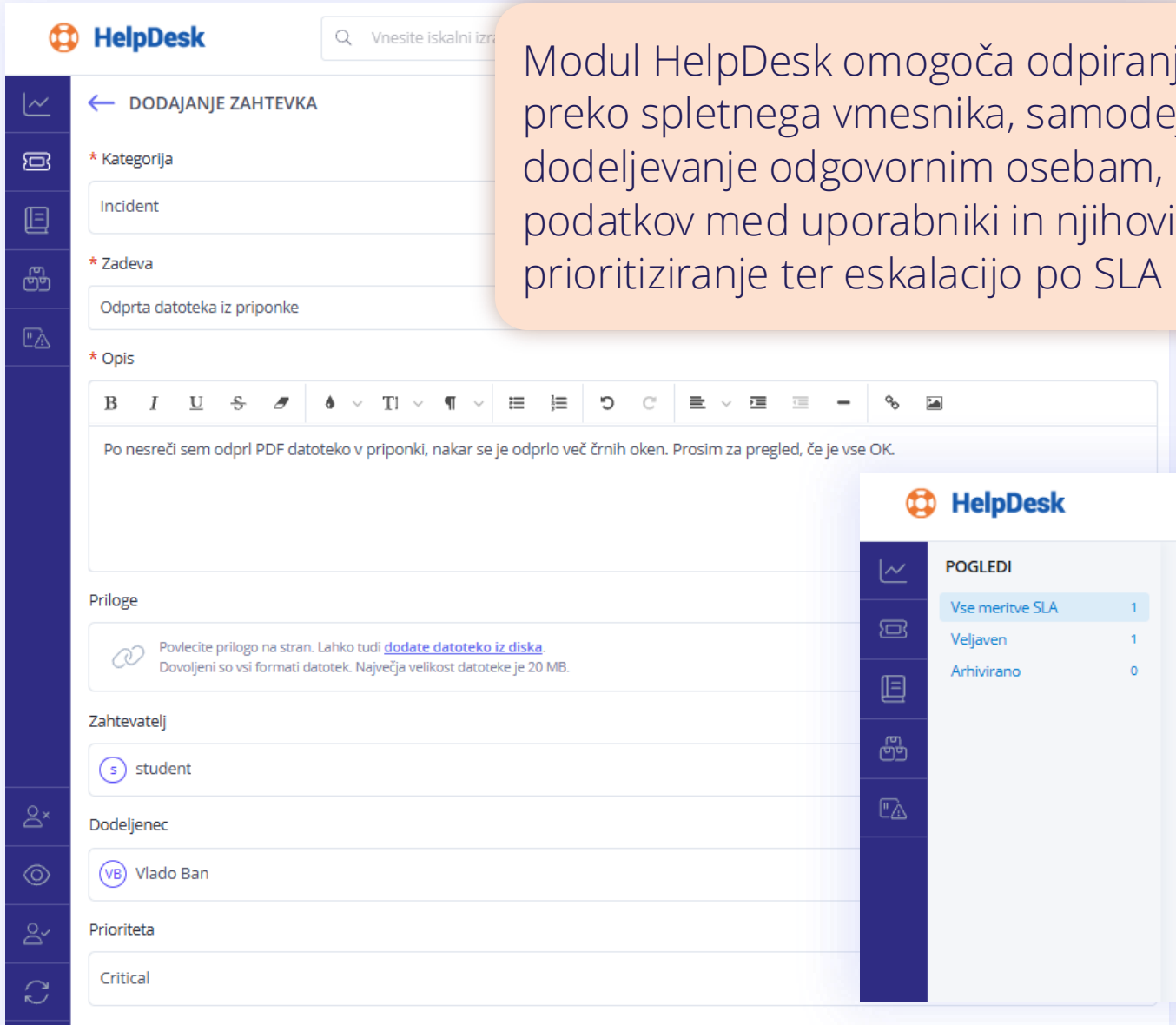


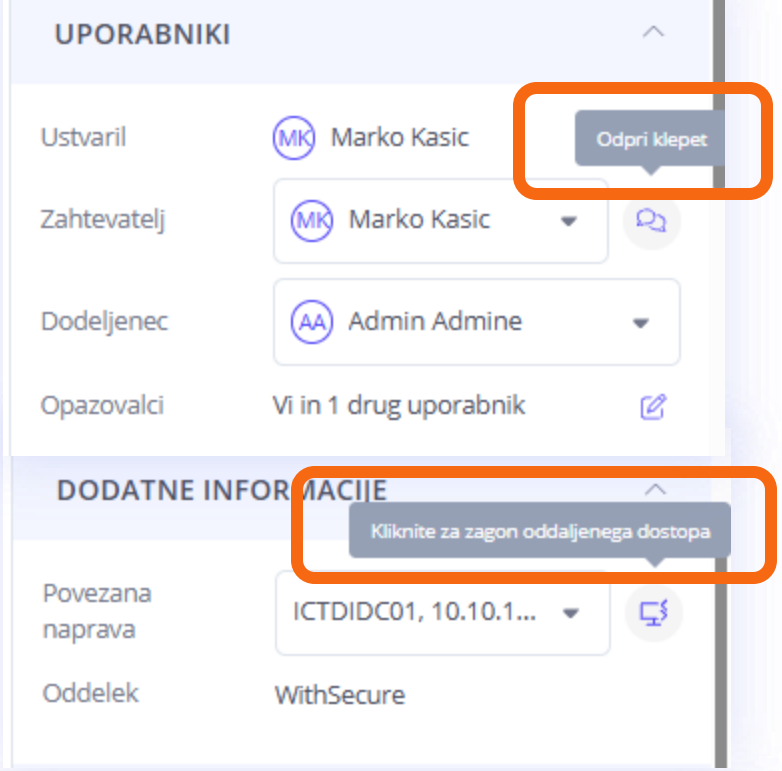
Neprestan nadzor in samodejno zaznavanje novih naprav in storitev.

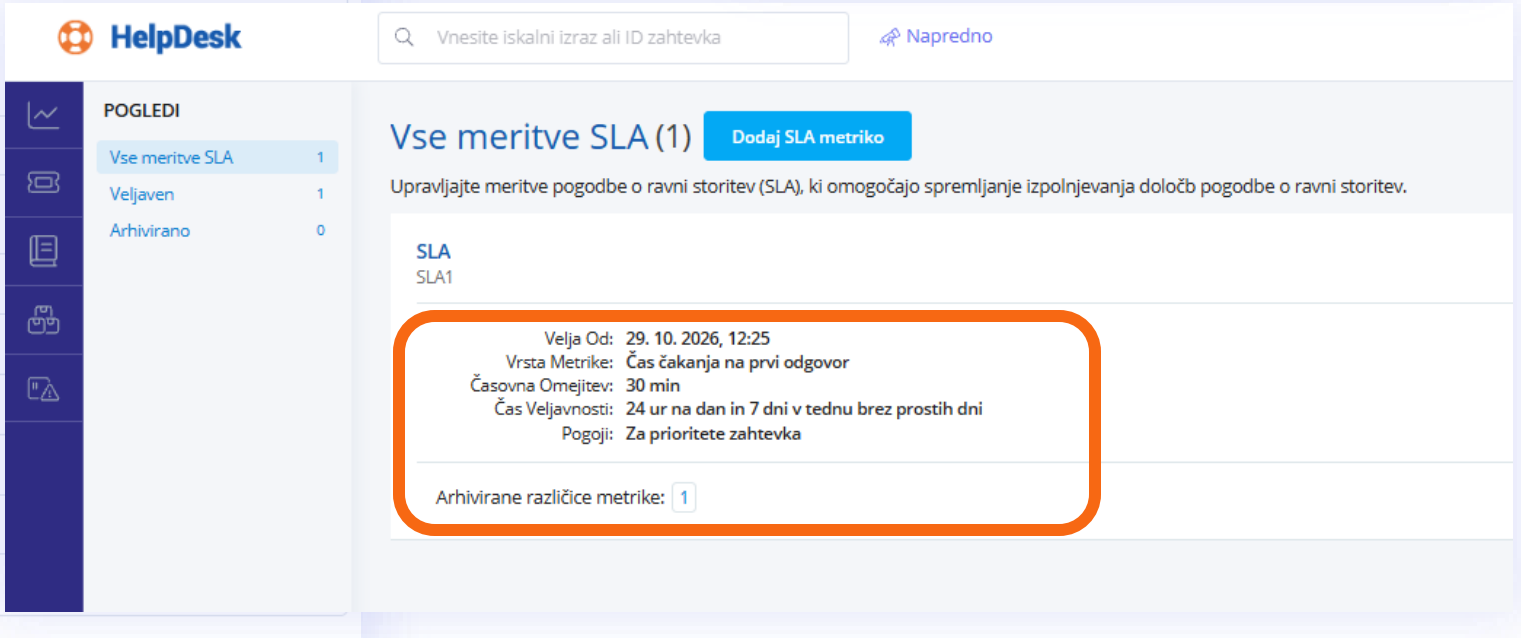
Obveščanje o spremembah statusov in preprečevanje izpadov

Upravljanje z incidenti in proces odzivanja

Modul HelpDesk omogoča odpiranje primerov preko spletnega vmesnika, samodejno dodeljevanje odgovornim osebam, povezovanje podatkov med uporabniki in njihovimi sredstvi in prioritiziranje ter eskalacijo po SLA metrikah.

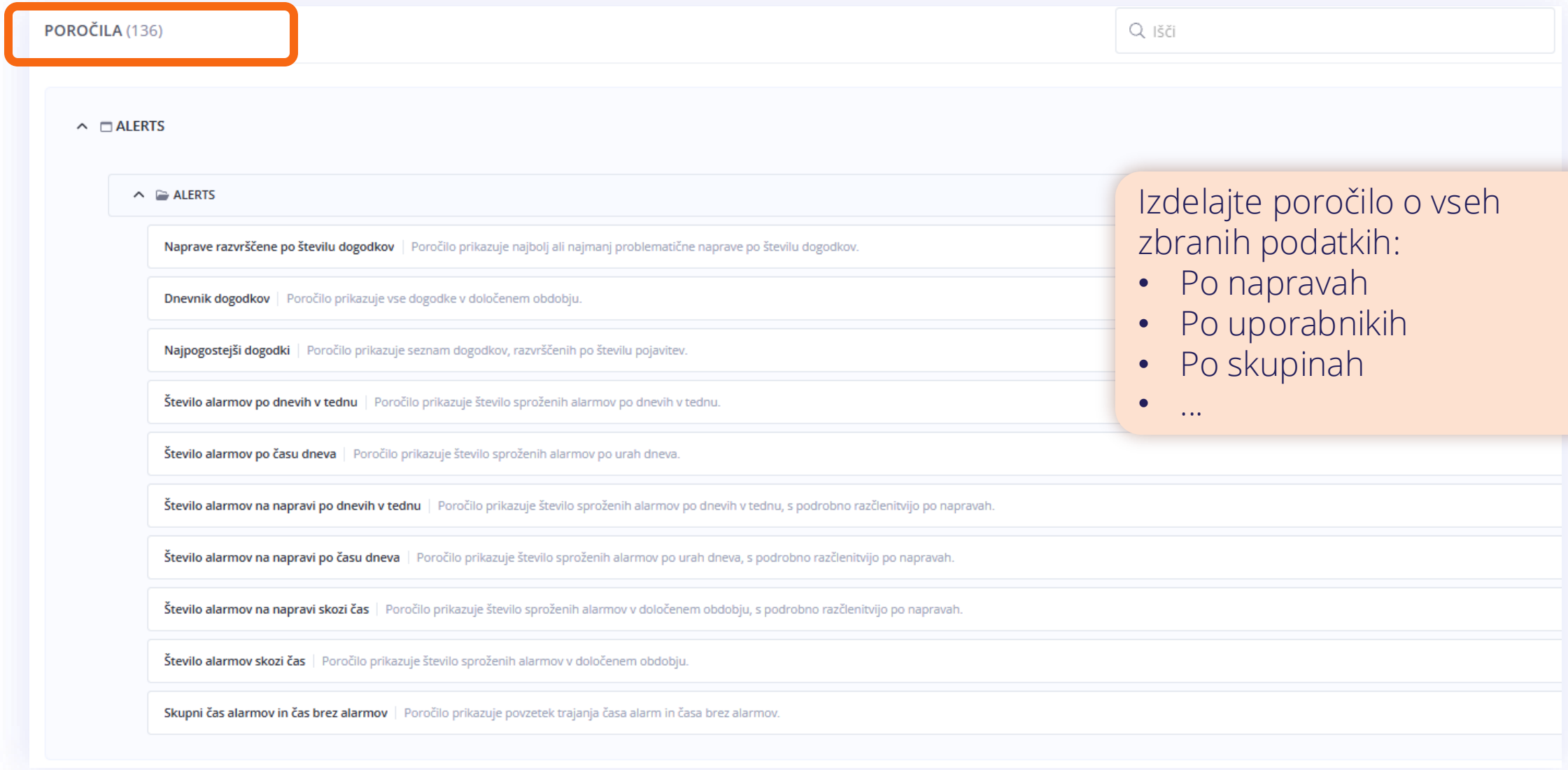






Poročanje, nazdorne plošče in revizijska sled

A1 ICT Distribucija

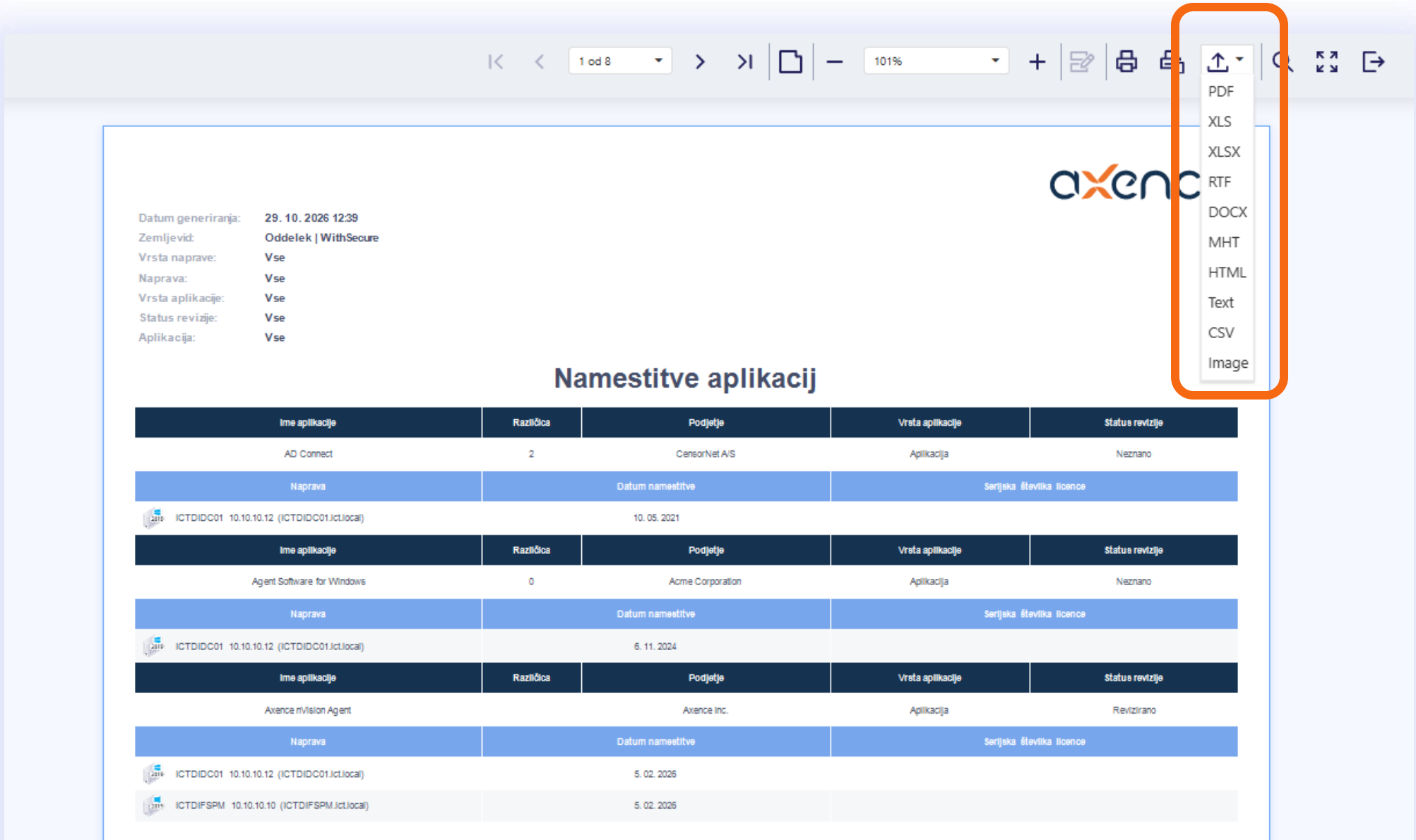


Izdelajte poročilo o vseh zbranih podatkih:

- Po napravah
- Po uporabnikih
- Po skupinah
- ...

Poročanje, nazdorne plošče in revizijska sled

A1 ICT Distribucija



Poročanje, nazdorne plošče in revizijska sled

A1 ICT Distribucija

Najpogostejši dogodki

	Dogodek	Sprožen dogodki
1	Sprememba inventarja programske opreme	14
2	User breached a blockade	1
3	Najdena nova naprava	1
4	Windows threshold	
5	Naprava ne deluje	

Podrobnosti o zasobah

Ime	Tip	Status	Pripada	Odgovorna oseba
ICTDIDC01	Računalnik	In use	WithSecure	Marko Kasic

Ime polja	Vrednost polja
Garancija do	
Ime	ICTDIDC01
Inventarna številka	0000003
Lokacija	
Odgovorna oseba	81
Serijska številka	None
Status	In use
Tip črtne kode	QR_CODE
Vrednost	0,00
Zadnje mobilno shranjevanje	
Zadnje mobilno skeniranje	
Informacije 1	ict.local

Poročanje, nazdorne plošče in revizijska sled

A1 ICT Distribucija

nVision AdminCenter

Default

Uredi nadzorno ploščo

Dnevnik dogodkov Axence nVision v All devices (Atlas) (Vsi dogodkov)

Ime dogodka	Naprava		Prioriteta	Čas začetka	Stanje
Zaznano odstranitev aplikacije Mozilla Firefox (x64 sl)	ICTDIDC01	10.10.10.12	običajna	28.10.2026 17:25	zaprt
Zaznana aplikacija Mozilla Firefox (x64 sl)	ICTDIDC01	10.10.10.12	običajna	28.10.2026 17:25	zaprt
Zaznana aplikacija Microsoft Visual C++ 2008 Redistributable	ICTDIDC01	10.10.10.12	običajna	28.10.2026 16:41	zaprt
vezanih in/ali odklopljenih (28. 10. 2026 14:39:39) Veliko naprav je bil	ICTDIDC01	10.10.10.12	običajna	28.10.2026 14:40	zaprt
Zaznano odstranitev aplikacije Mozilla Firefox	ICTDIDC01	10.10.10.12	običajna	28.10.2026 14:23	zaprt
Zaznana aplikacija Mozilla Firefox (x64 sl)	ICTDIDC01	10.10.10.12	običajna	28.10.2026 14:23	zaprt
Zaznano odstranitev aplikacije Microsoft Edge WebView2 Runtime	PRTG	10.10.10.18	običajna	28.10.2026 12:47	zaprt
Zaznana aplikacija Microsoft Edge WebView2 Runtime	PRTG	10.10.10.18	običajna	28.10.2026 12:47	zaprt
rabnika Administrator@ICT: Poskus prenosa datoteke (28. 10. 2026 12	ICTDIDC01	10.10.10.12	običajna	28.10.2026 12:20	zaprt
rabnika Administrator@ICT: Poskus prenosa datoteke (28. 10. 2026 12	ICTDIDC01	10.10.10.12	običajna	28.10.2026 12:20	zaprt

DC01 1h



PRTZH 15m



Nedavni dogodki na zasobah v All devices (Atlas)

Prilagodljiva nadzorna plošča, ki prikazuje dogodke po vaših zahtevah

Ni rezultatov

Tickets priority 24h

Prioriteta	Zgłosila
Blocker	0
Critical	1
Major	0
Minor	0

tickets status 24h

Stanje	Zgłosila
Novo	1
Odprto	0
Čaka na odgovor	0
Začasno ustavljeno	0

Slovenščina ▲ | Pomoč | Politika zasebnosti | Copyright © 2026 Axence Sp. z o.o. Sp. j.

Neprestano se razvijamo!
17. novembra bo premiera Axence nVision® 18.0

Patch Management

Prevzemite nadzor nad posodobitvami programske opreme. Preverite, katere aplikacije so nameščene in na katerih napravah, ter na daljavo posodobite izbrane aplikacije na želene različice na določenih delovnih postajah.

Avtomatizirana poročila

Ni vam več treba vsak dan preverjati konzole, da bi vedeli, kaj se dogaja v vašem imperiju.
Določite, katero poročilo naj se pošlje, kdaj in komu, nVision pa bo poskrbel za ostalo.

Cloud Relay

Ostanite povezani s svojimi napravami tudi zunaj lokalnega omrežja. Cloud Relay omogoča preprosto oddaljeno povezovanje brez potrebe po nastavljanju omrežnih vrat, ročnega usmerjanja prometa ali zapletene konfiguracije omrežja.

Izboljšan prikaz povezav med IT-sredstvi

Pridobite še več podatkov, ki vam bodo pomagali pri analizi vaše IT-infrastrukture, dejavnosti uporabnikov in IT-sredstev organizacije.

Centralno upravljanje ITv okviru NIS2 in ZinfV-1

- Celovita inventarizacija in preglednost sredstev (asset management)
- Spremljanje infrastrukture in odkrivanje incidentov
- Upravljanje incidentov in zahtevkov (ITSM / HelpDesk)
- Varstvo podatkov in nadzor uporabnikov
- Poročanje in revizije



Načrt izvedbe

Seznanite se z načrtom za uvedbo skladnosti s standardi ISO in NIS2 v vašem podjetju s pomočjo priročnika Axence v angleškem jeziku

Dokumentacija je na voljo strankam, ki uporabljajo programsko opremo v angleškem jeziku, od 17. novembra pa tudi uporabnikom slovenske različice.



Izpolnjujemo varnostne standarde

ISO/IEC 27001:2022

Certificiran sistem upravljanja z varnostjo informacij (ISMS). Zagotavljamo skladnost procesov z mednarodnim varnostnim standardom.



Certificate PL26/00000026

The management system of

Axence Sp. z o.o. Sp. j.

ul. Na Zjeździe 11, 30-527 Kraków, PL

has been assessed and certified as meeting the requirements of

ISO/IEC 27001:2022

For the following activities

Design, development, and delivery of on-premise and SaaS software, provision of a training platform service, software delivery, technical support for the delivered software, as well as conducting marketing activities and managing IT community portals.

Accordance with the Statement of Applicability dated on 7.01.2026, ver. 1.0

This certificate is valid from 26 February 2026 until 25 February 2029 and remains valid subject to satisfactory surveillance audits.

Issue 1. Certified since 26 February 2026

L. Moran

Authorised by

Liz Moran

Business Manager

SGS United Kingdom Ltd

Rossmore Business Park, Ellesmere Port, Cheshire, CH65 3EN, UK

t +44 (0)151 350-6666 - www.sgs.com

This document is an authentic electronic certificate for Client business purposes use only. Printed version of the electronic certificate are permitted and will be considered as a copy. This document is issued by the Company subject to SGS General Conditions of certification services available on Terms and Conditions | SGS. Attention is drawn to the limitation of liability, indemnification and jurisdictional clauses contained therein. This document is copyright protected and any unauthorized alteration, forgery or falsification of the content or appearance of this document is unlawful.

Page 1 / 1

UGODNOST ZA UDELEŽENCE SEMINARJA

20% POPUST

NA LICENCE

Posebna ponudba velja do 31. 12. 2026.

Q&A

Hvala za pozornost!



A1 ICT Distribucija

A1 Slovenija, d.d. je uradni pooblaščeni distributer podjetja Axence.

Ostanimo v stiku!

E: ict-partners@A1.si
T: 040 440 373
W: www.varnostne-resitve.si