RELACION
PËR ARGUMENTIMIN E SPECIFIKIMEVE TEKNIKE

LËNDA: Argumentim për specifikimet teknike për procedurën e prokurimit me objekt: "Parandalimi i rrjedhjes së të dhënave (DLP-Data Leakage Prevention) dhe Monitorim dhe Vizibilitet i pikave fundore (EDR-Endpoint Detection and Response) ", sipas Urdhrit të nr. 146 Prot., datë 18.03.2026

grupi i punës ka hartuar specifikimet teknike për procedurën me objekt "Parandalimi i rrjedhjes së të dhënave (DLP-Data Leakage Prevention) dhe Monitorim dhe Vizibilitet i pikave fundore (EDR-Endpoint Detection and Response)", sipas procedurave të prokurimit referuar Ligjit nr. 162, datë 23.12.2020 "Për Prokurimin Publik", i ndryshuar; VKM-së nr. 285, datë 19.05.2021, "Për Miratimin e Rregullave të Prokurimit Publik", e ndryshuar, dhe akteve të tjera nënligjore në fuqi.

Argumentimet dhe specifikimet teknike të zgjidhjeve "Parandalimi i rrjedhjes së të dhënave (DLP-Data Leakage Prevention) dhe Monitorim dhe Vizibilitet i pikave fundore (EDR-Endpoint Detection and Response)" janë hartuar bazuar në teknologjitë më të fundit në treg, duke mbajtur parasysh objektin e prokurimit dhe gjendjen aktuale teknologjike të kompanisë.

DLP (*Data Leaking Prevention*)
Duke përfshirë një spektër të gjerë aplikimesh në sistemet aktuale, zgjidhje të mundshme që ofrojnë shërbimin e kërkuar për të evidentuar elementët dhe specifikat më aktuale të software-t DLP që i përshtaten dhe nevojave të Shoqërisë IdentiTek sh.a, grupi i punës ka argumentuar zgjedhjen e këtyre specifikimeve si më poshtë:

Përzgjedhja e një sistemi të parandalimit të humbjes së të dhënave (DLP) është një vendim kyç për mbrojtjen e të dhënave sensitive brenda organizatës. Për të garantuar që zgjidhja DLP të përmbushë kërkesat specifike teknike dhe të sigurisë, është thelbësore të analizohen funksionet kyçe që duhet të përmbajë sistemi. Një zgjidhje DLP e implementuar "On-Premise" i jep organizatës kontroll të plotë mbi të dhënat e saj, duke garantuar që informacioni nuk kalon në duar të palëve të treta, duke minimizuar kështu rreziqet që vijnë nga vendosja e të dhënave në cloud ose në mjedise të jashtme. Sistemi duhet të ketë aftësinë për të zbatuar politika bazuar në URL-të, domeinet ose kategoritë e URL-ve, të integrohet me zgjidhje të sigurisë së web-it, të monitorojë dhe të kontrollojë trafikun e web-it për të parandaluar rrjedhjet e të dhënave përmes internetit, përfshirë trafikun tuneluar mbi HTTPS, si dhe të identifikojë dhe të bllokojë rrjedhjet e mundshme të informacionit përmes blogjeve, forumeve dhe kanaleve të tjera të komunikimit online, duke përfshirë trafikun e imazheve dhe përmbajtjeve të tjera që mund të përmbajnë të dhëna sensitive.

Adresa: "Identitek" SH.A, Rruga "Xhanfize Keko", ish Tipografia Ushtarake, Tiranë
NIPT: M31613043O
website: www.identitek.al
email: info@identitek.al

Një DLP i fuqishëm duhet të monitorojë dhe të inspektojë të gjitha dërgesat e emailit përmes SMTP-së, duke zbatuar politika të sigurisë për të parandaluar rrjedhjet aksidentale ose qëllimshme të informacionit, të karantinojë emailet për inspektim përpara dërgimit, të mbështesë një gamë të gjerë platformash dhe të integrohet me shërbime të ndryshme të email-it për të ofruar një mbrojtje gjithëpërfshirëse. Një sistem DLP efektiv duhet të ofrojë një panel të centralizuar menaxhimi që lejon një pamje të unifikuar të të gjithë aktiviteteve DLP, përfshirë rrjetin, të dhënat e ruajtura dhe pikat fundore, duke lejuar kështu menaxherët e IT-së dhe sigurisë të zbatojnë politika të qarta dhe të koherente në të gjithë mjedisin e IT-së.
Sistemi duhet të monitorojë dhe të kontrollojë pajisjet e lëvizshme, duke përfshirë media si USB, disqe të jashtme dhe pajisje të tjera të ngjashme, për të parandaluar transferimin e paautorizuar të të dhënave dhe të sigurojë enkriptim të të dhënave të transferuara në këto pajisje, si dhe të mbështesë një gamë të gjerë aplikacionesh dhe platformash cloud, duke përfshirë shërbime të njohura si Dropbox, Google Drive dhe Amazon Cloud Drive, për të siguruar që të dhënat të mos lihen të pambrojtura gjatë transferimeve në cloud.
Sistemi duhet të përmbajë politika dhe shabllone të avancuara për identifikimin dhe klasifikimin e të dhënave sensitive, të zbulojë skedarët e koduar dhe të mbrojtur me fjalëkalim, të identifikojë rrjedhjet e të dhënave përmes protokolleve të ndryshme dhe të monitorojë trafikun keqdashës, duke përfshirë edhe mësimin automatik të avancuar për identifikimin dhe mbrojtjen automatike të informacionit sensitiv. Funksionaliteti për të zbuluar të dhënat sensitive në skedarët e imazheve përmes teknologjisë OCR është thelbësor për të siguruar që të gjitha llojet e përmbajtjeve, përfshirë skedarët e skanuar, të monitorohen dhe të mbrohen.

Një zgjidhje DLP e avancuar duhet të integrohet me sistemet ekzistuese të sigurisë, duke përfshirë SIEM, për të ofruar një pamje të plotë dhe të unifikuar të sigurisë, si dhe të mbështesë pseudonimizimin dhe anonimizimin e të dhënave personale për të përmbushur kërkesat e rregulloreve të privatësisë dhe për të mbrojtur të dhënat kundër aksesit të paautorizuar. Sistemi duhet të ofrojë mbrojtje për serverat e printimit dhe të mbështesë zbulimin e të dhënave sensitive në dosje të përbashkëta dhe servera SharePoint, të mbështesë një gamë të gjerë sistemesh operative, duke përfshirë Windows, Mac OS dhe Linux, për të siguruar një mbrojtje gjithëpërfshirëse për të gjitha pajisjet brenda organizatës, dhe të ofrojë mbështetje të plotë për instalimin, konfigurimin dhe trajnimin e përdoruesve fundorë dhe stafit teknik të organizatës, duke garantuar që zgjidhja të implementohet dhe menaxhohet në mënyrë efektive.

Duke siguruar që zgjidhja e përzgjedhur përmbush të gjitha specifikimet teknike dhe kërkesat e sigurisë të përmendura më sipër, IdentiTek mund të mbrojë të dhënat sensitive, të përmbushë kërkesat e rregulloreve të privatësisë dhe të mbrojë kundër rrjedhjeve të paautorizuara të informacionit.

Identitek aktualisht perdor nje zgjidhje të pjesshme DLP nga Trellix **për mbrojtjen e pajisjeve periferike** (si USB, printerë, media të lëvizshme) që mundëson: Bllokimin ose lejen e përdorimit të

Adresa: "Identitek" SH.A, Rruga "Xhanfize Keko", ish Tipografia Ushtarake, Tiranë
NIPT: M31613043O
website: www.identitek.al
email: info@identitek.al

USB-ve; Monitorimin e skedarëve të kopjuar në media të lëvizshme; Kontrollin e aksesit fizik ndaj pajisjeve

Për të përmiresuar sigurinë e kompanise IdentiTek kërkohet që kjo zgjidhje të plotësohet me një **arkitekturë e plotë DLP nga Trellix**, e cila permireson dukshem mbrojtjen ndaj rrjedhjeve të të dhënave duke parandaluar:

- Dërgimi i të dhënave me email.
  Punonjësit mund të dërgojnë të dhëna sensitive me email personal si psh.Gmail, Outlook, etj.
- Ngarkimi në Cloud si psh OneDrive, Dropbox.
  Të dhënat mund të ngarkohen në aplikacione jo të autorizuara
- Screenshot ose printime.
  Informacioni konfidencial mund të shpërndahet përmes pamjeve ose printimeve
- Aplikacione të palëve të treta.
  Përdorimi i aplikacioneve të titpit të Skype, TeamViewer për të shpërndarë të dhëna
- Kopjimi në clipboard ose komanda të sistemit.
  Të dhënat mund të kopjohen dhe ngjiten në vende të paautorizuara

Gjithashtu një zgjidhje e plotë Trellix DLP lejon:

- Monitorim gjithëpërfshirës i të dhënave
  Gjurmim dhe kontroll i të dhënave në lëvizje (network), në pushim (storage), dhe gjatë përdorimit (endpoints)
- Identifikim i të dhënave sensitive
  Përdor klasifikime të automatizuara (PII, financiare, IP, etj.) për të zbuluar dhe mbrojtur informacionin kritik
- Zbatim i politikave të centralizuara
  Politikat DLP aplikohen njëherësh në endpoint, email, web, cloud, dhe storage
- Auditim dhe Forenzikë
  Raportim i detajuar mbi incidentet dhe sjelljet që cenojnë politikat e sigurisë
- Integrim me ePO dhe EDR/XDR
  Reagim i shpejtë dhe i koordinuar ndaj rrjedhjeve ose tentativave të shkeljes së të dhënave
- Reagim i automatizuar. (Bllokim, enkriptim, karantinim, ose njoftim automatik në varësi të skenarit

Konluzion:

Mbrojtja vetëm në nivel periferik është e nevojshme, por jo e mjaftueshme për të parandaluar rrjedhjen e të dhënave. Zgjidhja e plotë Trellix DLP siguron kontroll të plotë të ciklit të jetës së të dhënave, pavarësisht nga kanali i transmetimit apo mediumi.
Kjo zgjidhje gjithëpërfshirëse është thelbësore për një strategji të plotë të mbrojtjes së informacionit, veçanërisht në përputhje me standarde si ISO/IEC 27001, GDPR, (ligjit 144/24).

Adresa: "Identitek" SH.A, Rruga "Xhanfize Keko", ish Tipografia Ushtarake, Tiranë
NIPT: M31613043O
website: www.identitek.al
email: info@identitek.al

Duke qënë se aktualisht zgjidhja e Pjesshme DLP nga Trellix është për 492 klientë,

Options

DLP Operation Mode	Number of DLP Computer Properties
Device and removable Storage	492
Total	492

për pasojë kërkohet pajisja me Zgjidhjen e Plote DLP nga Trellix EDR të licensohet për të paktën **500** përdorues për një vit.

EDR (*Endpoint Detection and response*)

Duke kryer një analizë të thelluar në internet për të evidentuar elementët dhe specifikat më aktuale të sistemeve Endpoint Detection and Response (EDR), që i përshtaten nevojave të Shoqërisë IdentiTek sh.a, duke përfshirë integrimin me infrastrukturen harduare dhe softuare aktualisht ne perdorim nga IdentiTek, grupi i punës ka argumentuar dhe zgjedhjen e këtyre specifikimeve si më poshtë:

Një zgjidhje e fuqishme dhe e qëndrueshme për Endpoint Detection and Response (EDR), e cila të mund të instalohet "On-Premise", dhe të jetë e integruar me ekosistemin ekzistues Trellix që kryen aktualisht mbrojtjen Antivirus të pajisjeve fundore, duke shtuar kështu mundësimin e Hetimit dhe reagimit ndaj kërcënimeve të avancuara.
Aftësia për të izoluar një makinë të infektuar dhe për të kryer veprime korrigjuese automatikisht është kritike për ndalimin e përhapjes së kërcënimeve në rrjet, duke siguruar një mbrojtje të zgjeruar dhe një reagim të shpejtë në rast incidenti. Funksionaliteti i Remote Shell ofron një mjet të sigurt dhe të fuqishëm për hyrje dhe menaxhimin e incidenteve në distancë, duke mundësuar ekspertëve të sigurisë të ndërhyjnë dhe të zgjidhin problemet pa pasur nevojë për ndërhyrje fizike. Monitorimi dhe vizualizimi i rrjetit janë aspekte kyçe për identifikimin e trafikut të padëshiruar dhe për marrjen e masave parandaluese për të ndaluar sulmet para se ato të bëhen problem serioz.

Në të njëjtën kohë, sistemi EDR duhet të përmbajë aftësi për analizë të avancuar të inteligjencës së kërcënimeve dhe investigimin forensik, duke ofruar mjete për të hulumtuar incidentet e sigurisë dhe për të krijuar masa mbrojtëse më efektive, bazuar në një kuptim të thellë të mënyrës së funksionimit të sulmeve të ndryshme. Duke përmbushur të gjitha këto kërkesa, një zgjidhje e tillë EDR jo vetëm që ofron një mbrojtje gjithëpërfshirëse ndaj një game të gjerë kërcënimesh, por gjithashtu garanton një reagim të shpejtë dhe të mirëkoordinuar ndaj incidenteve të sigurisë, duke përmirësuar vazhdimisht aftësitë e mbrojtjes dhe duke ndihmuar organizatën të qëndrojë një hap përpara kërcënimeve të reja dhe në zhvillim.

Zgjidhja EDR siguron që ajo do të përballojë volumin e lartë të aktivitetit pa degraduar performancën,

Adresa: "Identitek" SH.A, Rruga "Xhanfize Keko", ish Tipografia Ushtarake, Tiranë
NIPT: M31613043O
website: www.identitek.al
email: info@identitek.al

duke garantuar stabilitet dhe efikasitet në menaxhimin e ngarkesave të rënda, edhe në rastet kur përdoruesit janë shumë aktivë.

Integrimi i moduleve nga i njëjti prodhues është një element thelbësor që siguron koherencë dhe harmoni në funksionimin e sistemit, duke eliminuar konfliktet që mund të lindin nga përdorimi i zgjidhjeve nga ofrues të ndryshëm dhe duke minimizuar problemet që lidhen me ndërfaqet dhe komunikimin midis komponentëve të ndryshëm.

EDR fokusohet në zbulimin, hetimin dhe reagimin ndaj kërcënimeve të avancuara që kalojnë mbrojtjen tradicionale duke mundësuar:

- Gjueti ndaj kërcënimeve kibernetike dhe vizibilitet i thelluar – monitorim i proceseve, skedarëve, rrjetit dhe aktivitetit të përdoruesit.
- Hetim i avancuar i incidenteve – analizon zinxhirët e sulmit dhe prioritizon bazuar në rrezik.
- Të dhëna në kohë reale dhe historike – analizë forenzike dhe gjurmim i shkakut rrënjësor.
- Reagim i automatizuar – izolim i hosteve, ndalim i proceseve, karantinim i skedarëve.
- Zbulim i malware pa skedarë dhe sulmeve 'Living off the Land' – që nuk kapen nga antivirusi tradicional
- Integrim me XDR (Extended Detection and Response) dhe produkte të tjera Trellix – për një mbrojtje të bashkërenduar.

Konluzion:

• Ndërkohë që antivirusi aktual (Trellix ENS) është i domosdoshëm për mbrojtjen bazë dhe përputhshmërinë me kërkesat e sigurisë, EDR është thelbësor për plotësimin e kërkesave të sigurisë që kërkojnë zbulim të avancuar, reagim ndaj incidenteve dhe aftësi hetimore.
• Përdorimi i EDR së bashku me antivirusin aktual nga Trellix, ofron një strategji të plotë mbrojtjeje kundër kërcënimeve të njohura dhe të panjohura.
Specifikimet teknike të hartuara, për këtë objekt prokurimi, "Parandalimi i rrjedhjes së të dhënave (DLP-Data Leakage Prevention) dhe Monitorim dhe Vizibilitet i pikave fundore (EDR-Endpoint Detection and Response) ", përshkruajnë minimumin ose tërësinë e elementeve më të rëndësishme përbërëse, që garantojnë cilësinë e kërkuar, dhe që i vlerëson mallrat si të pranueshme për funksionet e kërkuara, në përputhje me parashikimet e nenit 4, pika 38/b dhe nenit 36, të LPP, si dhe nenit 40, pika 2, të VKM nr. 285, datë 19.05.2021, "Për miratimin e rregullave të prokurimit publik", duke argumentuar çdo kërkesë funksionale ose performancë, apo/dhe çdo standard të kërkuar, ku çdo referencë duhet të shoqërohet nga fjalët "ose ekuivalenti i tij/saj".

Duke qenë se aktualisht zgjidhja e aktuale nga Trellix (Enpoint Security ENS) që kërkohet të zëvendësohet nga zgjidhja EDR, ka aktualisht 578 klientë:

Adresa: "Identitek" SH.A, Rruga "Xhanfize Keko", ish Tipografia Ushtarake, Tiranë
NIPT: M31613043O
website: www.identitek.al
email: info@identitek.al

1st Level Group	Number of Systems
My Organization\Identitek\	574
My Organization\Lost and Found\	4
Total	578

për pasojë kërkohet që zgjidhja Trellix EDR të licesohet për të paktën **600** përdorues për një vit.

Arsyetim mbi domosdoshmërinë Ligjore të Implementimit të projekteve të sigurisë.

Duke qenë se IDENTITEK SHA është klasifikuar nga ana e Autoritetit Kombëtar për Sigurinë Kibernetike AKSK si Organizatë e Infrastrukturës Kritike të Informacionit (OIKI).
(*AKSK Ref. Nr. 2445 Prot. Dt. 26.08.2025/ Identitek Nr. 1343 Prot. Dt. 29.08.2025*),

Realizimi i këtyre projekteve përfaqëson detyrime të qarta ligjore dhe rregullatore, dhe më konkretisht:

1. ***LIGJ Nr. 25/2024 Për Sigurinë Kibernetike,*** Neni 31 - Detyrimet e operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit**.**

2. ***VKM Nr. 531, datë 25.09.2025*** përcakton masa të detyrueshme teknike të sigurisë kibernetike për OIKI, duke përfshirë një listë masash te domosdoshme, mosrespektimi i të cilave përbën shkelje të detyrimeve ligjore dhe ekspozon institucionin ndaj sanksioneve administrative.

3. ***VKM Nr. 606, datë 23.10.2025,*** "Për Miratimin e Strategjisë Kombëtare Për Sigurinë Kibernetike 2025–2030 dhe të Planit të Veprimit 2025-2027".

   Përputhshmëria me të cilin ka këto qëllime kryesore:
   - Mbrojtja e infrastrukturës digjitale
   - Mbrojtja online e qytetarëve dhe nxitja e kulturës kibernetike
   - Forcimi i bashkëpunimit ndërkombëtar:
   - Mbrojtja ndaj kërcënimeve hibride

4. **Certifikimi ISO/IEC 27001:2022.** IDENTITEK SHA mban certifikimin ISO/IEC 27001:2022 për Sistemin e Menaxhimit të Sigurisë së Informacionit (ISMS);

   Në përputhje me Kërkesat e ligjit 25/2024, për Sigurinë Kibernetike, ky certifikim, është i detyrueshëm për *Organizatat e Infrastrukturave Kritike të Informacionit OIKI***.**

   Ky standard i sigurisë së informacionit kërkon Specifikisht zbatimin e masave, (kontrolleve të Annex A), përfshirë:
   - A.5.37 - Menaxhimi i vulnerabiliteteve (Zgjidhja Vulnerability Scanner);
   - A.5.19 / A.5.29 - Siguria e rrjeteve (Zgjidhja WAF/DDoS);
   - A.5.15 - Menaxhimi i aksesit të privilegjuar (Zgjidhja PAM);
   - A.8.16 / A.5.30 - Monitorimi dhe parandalimi i rrjedhjeve (Zgjidhja EDR/DLP).

Adresa: "Identitek" SH.A, Rruga "Xhanfize Keko", ish Tipografia Ushtarake, Tiranë
NIPT: M31613043O
website: www.identitek.al
email: info@identitek.al

- Moszbatimi i këtyre masave brenda afateve të përcaktuara rrezikon certifikimin ISO/IEC 27001:2022, me impakt të drejtpërdrejtë në funksionimin ligjor të IDENTITEK si operator i infrastrukturës kritike kombëtare, pasi mungesa apo vonesa e implementimit të këtyre projekteve krijon ekspozim të drejtpërdrejtë ndaj:
    - Sulmeve kibernetike (DDoS, Web Application Attacks, Ransomware);
    - Rrjedhjeve të të dhënave personale (biometrike, te dhëna sensitive);
    - Kompromet imit të sistemeve nga vulnerabilitete të paidentifikuara;
    - Akseseve jo të autorizuara nga përdorues të brendshëm (insider threats).

DETAJET E KONTRATËS:

Sipas specifikimeve bashkëngjitur të hartuara, vendosur dhe përllogaritur nga struktura të posacme të specializuara, e konkretisht nga: "Grupi i punës për hartimin e specifikimeve teknike dhe përllogaritjen e fondit limit", mbështetur në Vendimit të Këshillit të Ministrave Nr.285, datë 19.05.2021 "Për miratimin e Rregullave të Prokurimit Publik":

Kohëzgjatja e kontratës: 5 muaj nga nënshkrimi i saj

Licensa aktive: 12 Muaj

Plani i implementimit:

Ofertuesi duhet të instalojë zgjidhjen në ambientet e IdentiTek sipas kalendarit të mëposhtëm të dakordesuar në bashkëpunim me ekipin e IT. Shërbimi do të ndahet në faza dhe afati për secilën fazë është si në tabelën më poshtë:

Nr	Faza	Muaj 1	Muaj 2	Muaj 3	Muaj 4	Muaj 5
1	Marrja e të dhënave paraprake	■				
2	Implementimi	■	■	■		
3	Testimi i shërbimit			■	■	
4	UAC (User Acceptance)				■	
5	Dorëzimi i shërbimit				■	
6	Trajnimi për stafin					■

Adresa: "Identitek" SH.A, Rruga "Xhanfize Keko", ish Tipografia Ushtarake, Tiranë
NIPT: M31613043O
website: www.identitek.al
email: info@identitek.al