SPECIFIKIMET TEKNIKE

KORPORATA ELEKTROENERGJITIKE SHQIPTARE SH.A

"Platforma për menaxhimin e shit-blerjes së energjisë si dhe modulet mbështetëse"

1 FAQJA E KONTROLLIT TË DOKUMENTIT

1.1 Historiku i Versioneve dhe Ndryshimeve të Dokumentit

Data	Autori	Versioni	Shënime mbi Rishikimet

2 NËNSHKRIMET MIRATUESE

Përgatiti:

Përgatiti:

Përgatiti:

Pergatiti:

Miratoi:

Miratoi:

3 PËRMBAJTJA

4 Përfituesi /Autoriteti Kontraktues

Korporata Elektroenergjetike Shqiptare (KESH sh.a), është një shoqëri tregtare aksionere shtetërore dhe është prodhuesi kryesor dhe më i rëndësishëm i energjisë elektrike në Shqipëri, që administron dhe operon hidrocentralet e kaskadës së lumit Drin (HEC-Fierzë, HEC-Koman, HEC-Vau i Dejës).

4.1 Hyrje

Korporata Elektroenergjetike Shqiptare (KESH) sh.a e zhvillon aktivitetin e saj duke administruar dhe operuar hidrocentralet e kaskadës së lumit Drin (tre njësive të prodhimit HEC-Fierzë, HEC-Koman, HEC-Vau i Dejës) të cilët kanë rëndësisë së veçantë për ekonominë e vendit) dhe personelit në zyrat e administratës qendrore, Blloku Vasil Shanto Tiranë.

Misioni kryesor i KESH sh.a është plotësimi i kërkesës së vendit për energji elektrike me kosto sa më të ulet duke shfrytëzuar me efektivitet burimet ujore ekzistuese dhe duke zhvilluar burime të reja. Gjithashtu monitorimi dhe garantimi i jetëgjatësisë dhe sigurisë së veprave nëpërmjet administrimit të kujdesshëm dhe efektiv të tyre, mirembajtjes dhe modernizimit të sistemeve të monitorimit është një sfidë që KESH sh.a. ka ndërmarrë veçanërisht vitet e fundit.

5 Përshkrimi i Përgjithshëm i kërkesave

Qellimi i ketij projekti eshte ndertimi i nje sistemi i cili do te beje te mundur publikimin e tenderave te shitjes dhe blerjes se energjise elektrike nga ana e KESH, ku me pas te gjithe operatoret vendas apo te huaj te cilet deshirojne te japin ofertat e tyre per keto tender ate kene mundesine te ofertojne online ne kete sistem. Sistemi gjithashtu do te beje te mundur sugjerimin ne menyre automatike te ofertave me te favorshme per KESH per te maksimizuar te ardhurat dhe per te ulur shpenzimet. Ne kushtet ku KESH sh.a. eshte pajisur me license ne aktivitetin e furnizimit me energji elektrike si dhe ku parashikohet qe procedurat e shit-blerjes se energjise elektrike do te kryhen me mjete elektronike/platforme, linde nevoja per hartimin e rregulla te reja te tregtimit te energjise elektrike.

5.1 Kërkesat funksionale të sistemit (modulet)

5.1.1 Moduli i krijimit të përdoruesve

Në këtë modul sistemi duhet ti japë mundësi administratorit të krijojë përdorues të tjerë në sistem. Gjatë krijimit të përdoruesve duhen plotësuar saktë fushat Emër, Mbiemër, roli i përdoruesit në sistem, email, numër telefoni dhe password. Në çastin e krijimit të përdoruesit sistemi duhet të dërgojë në adresën e email të regjistruar për këtë përdorues një lidhje për të verifikuar llogarinë. Nëse përdoruesi nuk e klikon linkun e dërguar në email atëherë ai nuk mund të kyçet në sistem. Pasi përdoruesi klikon linkun dhe verifikon llogarinë atëherë ai mund të kyçet në sistem. Sistemi duhet të detektojë nëse ky përdorues po kyçet për herë të parë apo jo. Nëse përdoruesi po kyçet për herë të parë atëherë sistemi duhet ti kërkojë përdoruesit të aktivizojë opsionin e kyçjes me dy hapa (two step authentication) në të cilin

përdoruesit duhet ti kërkohet te skanojë me anë të një aplikacioni për autentikim një kod QR i cili duhet të gjenerojë fjalëkalime njëperdorimshme. Pasi përdoruesi ka aktivizuar opsionin e kyçjes me dy hapa dhe ka vendosur kodin e saktë atëherë ai do mund të kyçet në sistem. Sistemi nuk duhet të lejojë kyçjen pa aktivizimin e këtij opsioni për efekt të rritjes .

5.1.2 Moduli i krijimit te klienteve

Ne kete sistem klient do te quhet cdo operator vendas apo i huaj i cili eshte i interesuar te marre pjese ne prokurimet e publikuara nga KESH per shitblerjen e energjise elektirike. Pershkak te rendesise se sistemit klientet e interesuar duhet ne fillim te kontakojne me KESH, i cili ben verifikimin e dokumentave dhe me pas perdoruesit e brendshem te kesh kane mundesi te krijojne llogari klienti per ta. Per te krijuar nje klient perdroeusit e KESH regjistrojne emrin e klientit, shtetin, aksioneret, ngarkojne dokumentat perkatese, vendosin te dhenat per perdoruesin i cili do te futet ne sistem. Ne castin e krijimit te klientit paralelisht ne menyre automatike sistemi duhet te krijoje dhe perdoruesin peraktes per ate klient. Pas krijimit te perdoruesit sistemi duhet te mundesoje te njejten rrjedhe per kycjen e perdoruesit ne sistem si ne piken 1.

5.1.3 Moduli i garancise bankare

Ne kete modul perdoruesit e finances kane mundesine te ngarkojne ne sistem nje dokument I cili verteton garancine bankare te mbyllur nga nje klient ne benefit te KESH. Sistemi duhet ti mundesoje perdoruseve mundesine e ngarkimit te ketij dokumenti si dhe ti japi mundesine atyre qe te plotesojne fushat si, vlera totale e garancise, daten e skadimid, vlera e mbetur qe mbulon garancia. Kur nje klient shpallet fitues per nje tender dhe ai nuk I ka derguar KESH-it veretitmin e pageses keshi mund te perdore garancine bankare per te proceduar me dergimin e energjise. Per ta bere kete gje nevojitet qe vlera e mbetur e garancise bankare te jete me e madhe se sa vlera qe klienti I detyrohet KESH. Ne castin qe klienti I dergon KESH vertetimin e pageses per tendering perkates dhe KESH ka perdorur garancine bankare te klientit, atehere velra e pageses I shtohet vleres se garancise bankare per klientin.

5.1.4 Moduli i kapaciteteve nderkufitare

Ne kete modul perdoruesit e kesh duhet te kene mundesine qe te regjistrojne ne sistem te gjith blerjet qe kesh ben per blerjet e kapaciteteve nderkufitare. Ne kete modul regjistrohen te dhenat se kur eshte bler nje kapacitet nderkufitar, drejtimin, kapacitetin e blere (MW), daten e blerjes, dhe vleren me te cilen eshte blere ky kapacitet. Ky informacion do te perdoret ne modulin e prokurimit ne te cilin KESH do te percaktoje nese per nje tender specifik kapaciteti nderkufitar sigurohet nga KESH apo eshte pergjegjesi e klientit.

5.1.5 Moduli i publikimit te tenderave

Ne kete modul perdoruesit e KESH do te kene mundesine te publikojne nje tender per shitje apo per blerje energjie. Ne kete modul perdoruesit do te kene mundesine te hedhin informacion lidhur me nje tender te caktuar. Informacioni perfshin nje emertim dhe pershkrim te tenderit, daten kur fillon pranimi I ofertave dhe daten kur mbaron pranimi I ofertave, daten kur fillon dhe kur mbaron shitblerja e energjise, kapacitetin qe do bliehet apo shitet si dhe informacion lidhur me kapacitetin nderkufitar. Per cdo tender perdoruesit e

KESH do te kene mundesi te krijojne profilet orare (ose lotet) ne te cilet do te specifikohen sakte fashat orare kur KESH deshiron te shese dhe te bleje energji. Cdo tender qendron fillimisht ne statusn DRAFT dhe publikohet manualisht nga administratori I sistemit.

5.1.6 Moduli i dorezimit te ofertave

Ne kete modul klientet kane mundesi te japin ofertat e tyre per cdo tender. Klientet jane te detyruar qe oferten ta bejne per cdo profil (lot). Oferta e bere nga klienti mund te mos jete per te gjithe kapacitetin e kerkuar nga KESH ose mund ta tejkaloje kapacitetin qe KESH kerkon. Nje klient ka te drejte te modifikoje oferten e tij deri kur afati i dorezimit te ofertave te kete perfunduar. Pas perfundimit te afatit te dorezimit te ofertave sistemi nuk lejon me modifikimin e ofertes nga klienti. Per cdo oferte te derguar sistemi njofton me SMS klientin qe oferta e tij u dorezua me sukses.

5.1.7 Moduli i vleresimit te ofertave

Ne kete modul sistemi i jep mundesine perodruesve te KESH te vleresojne ofertat e dhena nga klientet per nje tender te caktuar. Keto oferta mund te behen te dukshme nga KESH vetem pasi afati i dorezimit te ofertave ka perfunduar. Sistemi gjithashtu do te beje te mundur sugjerimin ne menyre automatike te ofertave me te favorshme per te maksimizuar te ardhurat dhe per te ulur shpenzimet. KESH ka mundesine te perzgjedhe si fitues Kliente te ndryshem per cdo profil (lot). KESH ka mundesine te perzgjedhe ne menyre parciale nje oferte per nje lot te caktuar (pra te marri vetem nje pjese te ofertes se dhene nga nje klient) dhe jo te gjithe oferten per cdo lot. Pas perzgjedhjes si fituese te nje oferte per lot KESH ka te drejte te shpalle fituesit zyrtarisht.

5.1.8 Moduli i gjurmëve (log) dhe sigurisë së modulit të portalit

Aplikacioni duhet të ofrojë funksionalitete për monitorimin dhe auditimin e të gjithë veprimeve në sistem. Për çdo veprim duhet të ruhet data, autori (përdoruesi), rekordi i ndryshuar, fushat e ndryshuara për çdo rekord, vlerat para modifikimit dhe ajo pas modifikimit, IP, sesioni etj. Gjurmët e auditimit duhet të jenë të aksesueshme por të pa modifikueshme nga ndërfaqja e sistemit. Të ofrohet mundësia që të krijohen rregulla auditimi në bazë të ambienteve dhe përdoruesve. Të përcaktohen veprimet që duhet të auditohen si lexim, modifikim, krijim, fshirje, rrjedhë pune. Komunikimi me databazën duhet të jetë i sigurtë dhe çdo rekord që ruhet të jetë i enkriptuar bazuar në një algoritëm të fortë enkriptimi. Kanali i lidhjes midis shfletuesit (browser-it) dhe Server Qendror duhet të jetë e sigurtë dhe i enkriptuar me TSL/SSL nëpërmjet protokollit HTTPS. Sistemi duhe të gjenerojë loget e sigurisë në një format raporti apo file i lexueshëm nga administratori kryesor i sistemit. Rekordet duhet të duplikohen dhe në një databazë të jashtme auditi. Kodi dhe modulet e sistemit duhet që të sigurojnë një versionim dhe historik të ndryshimeve që do të bëhen në sistem. Aksesi në sistem duhet të realizohet nga përdoruesit e jashtëm apo të brendshëm përmes autentikimit me dy faktorë: username/password dhe token. Sistemi duhet të ofrojë mundësinë e monitorimit të aksesit në sistem përmes logeve. Moduli i portalit duhet të suportojë përdorimin e token mobile për iOS apo Android për përdoruesit e jashtëm.

6 Specifikime teknike të sistemit

Sistemi duhet të funksionojë bazuar në mikroservise si dhe të ketë dy nën projekte: ***front end*** dhe ***back end.***

6.1 Frontend

Frontend duhet te suportoje standartet web te programimit CSS 3, HTML 5, dhe te jete kompatibel me te gjithe shfletuesit (browsers). Front end duhet te jete ne gjendje te marre te dhena nga backend duke konsumuar webserviset REST. Duhet te jete ne gjendje te menaxhoje tokenat e sigurise si dhe te menaxhoje refresh token per cdo perdorues. Sistemi front-end duhet te ndertoje funksionalitetet e tij si komponente te cilet te kene mundesi te riperdoren ne cdo modul te sistemit. Sistemi frontend duhet te ndertohet i tille qe te jete totalisht i pavarur nga backend dhe te jete funksional pa qen nevoja e nderhyrjeve te metejshme nese teknologjia e sistemit backend ndryshon. Sistemi duhet ti shfaqe qarte perdoruesve erroret dhe mesazhet e suksesit. Frontend duhet gjithashtu te suportoje javascript.

6.2 Backend

Backend duhet te ndertohet ne nje gjuhe programimi e cila suporton arkitekturen MVC. Te gjithe modulet e sistemit duhet te konceptohen si mikroservise dhe te dergojne te dhena tek Frontend nepermjet web-serviseve REST. Backend duhet te mbroje web-serviset REST nga perdorimi i pautorizuar duke kerkuar nje security token per cdo te dhene qe eshte sensitive. Backend duhet te suportoje nderveprimin me databazat RDBS. Backend duhet te jete ne gjendje te prodhoje dokumentacionin e nevojshem per konsumimin e web-serviseve qe nevojiten per funksionimin e sistemit.

6.3 Databaza

Databaza duhet te jete e llojit RDBS dhe te jete kompatibel me teknologjine qe do te perdoret per sistemin e backend. Duhet te jete ne gjendje te ruaje logs per te gjithe veprimet qe ndodhin ne databaze si dhe te gjithe query-t qe ekzekutohen ne te.

6.4 Arkitektura

Sistemi duhet te hostohet ne nje arkitekture e cila suporton auto scaling (rritjen automatike te kapaciteteve bazuar ne nevojat e sistemit). Autoscaling duhet te ndodhe ne menyre automatike pa qene nevoja e nderhyrjes manuale. Databaza duhet te jete e replikuar te pakten ne nje lokacion tjeter pervec lokacionit primar, dhe te garantoje sigurine dhe konsistencen e te dhenave ne cdo kohe. Infrastruktura e rrjetit ne te cilen do te hostohet aplikacioni duhet te beje te mundur aksesimin e databazes vetem nga serveri ku do te ruhet sistemi i backend. Aksesi i databazes nuk duhet te jete i mundur pa kriteret e sigurise.

Infrastrkutura duhet gjithashtu te suportoje adaptimin automatik. Cdo modul i ri apo permiresim qe kryhet ne sistem duhet te kete mundesine te behet adaptim ne menyre automatike nga infrastruktura pasi eshte bere bashkimin me kodin burim aktual.

Arkitektura duhet te jete ne gjendje te mbroje sistemin nga sulmet nga jasht si dhe sulmet DDoS, dhe te pershtatet me standartet dhe te dhenat e sigurise kibernetike.

6.5 Kodi burim

Kodi burimi nderfaqes dhe jo praktikave apo te dhenave, duhet te ruhet ne platformen git (Gitlab, Github ose ekuivalente). Kodi burim duhet te kete dy ndarje kryesore, main dhe development. Ku main do te perdoret per te mbajtur kodin i cili eshte ne sistemin live dhe development do te perdoret per te mbajtur kodin i cili eshte ne sistemin test. Teknologjia git duhet te beje te mundur qe gjate hedhjes se funksionaliteteve te reja ne kodin burim te beje kontrollet e nevojshme dhe teste automatike te kodit burim per te garantuar funksionalitetin e sakte te sistemit. Cdo funksionalitet i sistemit duhet te ndertohet ne nje dege(branch) te vecante dhe te jete kollaj I kthyeshem nese ndonje ndonje problematike e cila pengon funksionalitetin e sistemit.

6.6 Ndërveprimi me sistemet e tjera

Sistemi duhet te jete ne gjendje te ndervepoje me sistemet e tjera si: Dogana, Tatimet apo sistemet bankare. Integrimi me sistemin e doganes duhet te behet ne castin e blerjes se energjise elektrike. Integrimi me sistemin e tatimeve duhet te behet per deklarimin e faturave ne sistemin e fiskalizimit ndersa integrimi me sistemet bankare duhet te kryhet per te bere te mundur vertetimin automatik te pagesave. Keto integrime do te zhvillohen sipas kerkesave te KESH sh.a. ne diskutim me stafin e operatorit ekonomik qe do te zhvilloje projektin.

6.7 Proceset e biznesit (Workflows) që platforma duhet të ndjekë në funksionimin në tërësi të saj.

6.7.1 Aplikimi për regjistrimin e shoqërive tregtare

- Aplikimi bëhet me komunikim zyrtar me KESH sh.a.
- Aplikantët plotësojnë formën e aplikimit.
- Upload dokumentat për regjistrim
    - Kërkesa e shoqërisë për rregjistrim;
    - Dokumentacionin që vërteton regjistrimin e shoqërisë në regjistrat përkatës tregtar gjyqësor të shtetit përkatës në të cilin shoqëria është regjistruar.
    - Licencen për tregtimin/furnizimin e energjisë elektrike të lëshuar nga autoritete përgjegjëse.
    - Dokumentacionin e lëshuar nga institucionet kompetente të shtetit përkatës të cilët vërtetojnë se:
        - Subjekti i licencuar nuk është ne proces likuidimi/falimentimi dhe kapitalet/asetet e tij nuk janë objekt i procedurave përmbarimore;
        - Subjekti i licencuar dhe administratori nuk janë të dënuar nga gjykata dhe as nuk ndiqen penalisht për shkelje penale për çeshtje që lidhen me aktivitetin e tregtimit të energjisë elektrike apo vepra të tjera penale (pjesëmarrje në organizatë kriminale, korrupsion, mashtrim, pastrim parash, falsifikim, shpërdorim detyre, vjedhje, pengime për ekzekutimin e vendimeve të gjykatës dhe veprat penale në fushën e falimentit);
        - Subjekti i licencuar ka përmbushur detyrimet për pagimin e tatimeve, taksave dhe kontributeve të sigurimeve shoqërore/shëndetësore në përputhje me legjislacionin e shtetit përkatës

        - Pasqyrat financiare të subjektit të licencuar , të vitit të fundit, të çertifikuara sipas rregullave të shtetit përkatës ku shoqëria ushtron aktivitetin.
- Stafi i KESH i cili meret me operimet tregtare, zbaton procedurat e brendeshme per krijim e përdoruesit në sistem
- Sistemi dërgon njoftimet përkatëse sipas procedurave, nëpërmjet platformës në adresat elektronike të regjistruara të subjektit.
- Aprovimi i regjistrimit sipas kritereve, referuar udhëzimeve ligjore duke e shoqëruar me dërgimin e kontratës tip.
- Aprovimi/mosaprovimi i regjistrimit shoqërohet me ruatjen e komenteve dhe dokumentave bashkëngjitur.
- Aprovimi i regjistrimit shoqërohet me krijimin e llogarive në sistem.

Dokumentacioni i mësipërm duhet përditësuar nga shoqeritë sipas kërkesës së shoqërisë KESH sh.a., bazuar në rregullat e tregtimit të energjisë elektrike nga KESH SH.A.
Sistemi elektronik duhet të mundësojë gjenerimin e njoftim të marrjes së aplikimit ose jo të shoqërive të interesuara që kërkojnë të rregjistrohen në procedurat e shit-blerjes së energjisë elektrike nga KESH sh.a. sipas nevojës së stafit menaxhues të sistemit. Në rast të mos marrjes së aplikimit, dhe evidentimit të zërave që nuk janë plotësuar sipas kërkesës për rregjitrim (kjo me qëllim që shoqëria e interesuar të riplotesojë zërin për të cilën sistemi elektronik i ka kthyer mbrapsh kerkesen per rregjistirm).

6.7.2 Administrimi i kalendarit të kërkesave/ftesave për shitje/blerje

- Ndërtimi i kalendarit sipas kërkesave/ofertës për shitje (ask)/blerje (request for bid).
- Krijimi i kategorisë së procedurës shitje/blerje.
- Përcaktimi i vlefshmërisë së kërkesë/ofertës sipas periudhave, fashave orare.
- Përcaktimi i lote-ve së kërkesë/ofertës sipas periudhave, fashave orare:
    - kapaciteteve shit/blerje
    - sasive shit/blerje
    - çmimeve të shit/blerjeve
    - pikave të lëvrimit të shit/blerjes
- Vlerësimi i kërkesë/ofertës dhe menaxhimi i procedurës në të gjithë fazat e saj.
- Mirëmbajtja e kalendarit , përditësimi i tij.
- Mbledhja dhe shqyrtimi i kuotimeve për shitje/blerje.
- Formati i kërkesave për shitje/blerje.
- Publikimi i informacioneve zyrtare, i gjithë informacionit mbi procesin e shitjes/blerjes së energjisë elektrike.
- Rikonfirmimi i dokumentave ligjore dhe administrative për çdo procedurë/ kërkesë për shitje/blerje që publikohet rishtas.
- Mundësi listimi përzgjedhje të ofertave për shitje/blerje mbi bazën e kritereve të vlerësimit sipas nevojave të stafit të operimit.
- Komunikimi dhe ndërveprimi i operatorit KESH me pjesëmarrësit nëpërmjet platformës.
- Menaxhimi i procedurave të shitjes/blerjes.
- Njoftimi i fituesit dhe raportimi i informacionit.

- Dashboard administrativ i cili duhet të përbledhë aktivitet historik të transaksioneve dhe mundësia për shfaqe interaktive.

6.7.3 Administrim i ankesave

a. Hartimi i ankesave referuar kalendarit të kërkesave për shitje/blerje/shitje .
b. Përsëritja e procesit të dërgimit të kërkesës.
c. Publikimi ankesave në sistem dhe transparenca për tregtarët pjesëmarrës.

6.8 Proceset e biznesit (Workflows) te tregtimit te energjise elektrike të detajuara

Me poshtë po paraqesim proceset e tregtimit të energjisë elektrike të detajuara sipas rasteve:

Per shitje te energjise elektrike. Kerkesa/ftesa per oferte duhet te permbaje:

- Periudha/dita e shitjes se energjise elektrike e cila mund te jete:
  - Periudhe ne blloke;
  - Periudhe e kushtezuar (psh. Shitje energji elektrike 1-30 Prill 2019, por periudhen 1-10 Prill eshte e konfirmuar,ndersa periudhat 11-20 dhe 21-30 Prill do rikonfirmohen respketivisht ne datat 8 dhe 18 Prill 2019);
  - Peridhe me dite te ndara;

- Profili i levrimit te energjise elektrike nga ora 00: 00deri me 24:00 e cila mund te jete:
  - Profile ne blloke;
  - Profile me ore te ndara;

- Kapaciteti i shitjes se energjise elektrike e cila mund te jete:
  - Kapacitetin maksimal i kerkuar per tu ofertuar/deri ne... MW;
  - Kapacitet i kushtezuar (Psh: shitje energji elektrike per periudhen 11-20 Prill 2019 ne kapacitetin 50 MW,por KESH sh.a. i rezervon te drejten vetes qe me date 8 Prill 2019 ku do te konfirmoje periudhen e shitjes te zgjidhe edhe kapacitetin e levrimit e cila mund te jete nga 0 MW deri me 50 MW)
  - Kapacitet ne blloke;
  - Kapacitet me ore te ndara;

- Sasia e energjise elektrike mund te jete:
  - Sasia maksimale e kerkuar per tu ofertuar/ deri ne .... MWh;
  - Sasia e kushtezuar (Psh: shitje energji elektrike per periudhen 11-20 Prill 2019 ne kapacitetin 50 MW dhe sasine 1200 MWh, por KESH sh.a. i rezervon te drejten vetes qe me date 8 Prill 2019 ku do te konfirmoje periudhen e shitjes te zgjidhe edhe kapacitetin e levrimit e cila mund te jete nga 0 MW deri me 50 MW respektivisht edhe sasia e energjise elektrike)
  - Sasia ne blloke;
  - Sasi me ore te ndara;

- Cmimi njesi i kerkuar per tu ofertuar mund te jete:
  - Cmime/njesi ne blloke;
  - Cmime/njesi orar;

- Cmime/njesi dysheme;

➢ Pika e levrimit te energjise elektrike e cil mund te jete:
- Brenda rrjetit te transmetimit
- Ne kufirin Shqiperi-Mali i Zi/Serbi/Greqi

➢ Siguruesi i kapacitetit mund te jete:
- Nga shoqerite ofertuese;
- Nga KESH sh.a.;

➢ Kriteri vleresimit te ofertave eshte:
- cmimi/njesi me i larte deri ne permbushjen e sasise se kerkuar per shitje te energjise elektrike;
- i kushtezuar sipas cmimit dysheme tevendosur ne oferte;
- Ne rast kur kemi dy oferta me te njejtin cmimi do te ndiqet parimi i pari qe vjen i pari sherbehet/pranohet;

➢ Kriteri financiar lidhur me menyren e pageses mund te jete:
- Me parapagim;
- Garanci financiare;
- Mjete te jera financiare;

➢ Afati i hapjes dhe e mbylljes se mjetit elektronik te perdoruar nga KESH sh.a. per zhvillimin e procedures se shit-blerjes se energjise elektrike per ofertimin e shoqerive tregtare;

➢ Kushte te tjera te vendosura nga Autoriteti Kontraktues;

➢ Raporti i mbylljes se procedures/rezultatet e procedures se shitjes duke publikuar cmimet dhe sasite mesatare te ofertuara dhe ato te fituara.

➢ Ankimimi. Brenda afatit te percaktuar ne kerkesen/ftesen per oferte shoqerite kane te drejte qe nepermjet sistemit elektronik te dergojne ankesen dhe sipas afateve te percaktuara do ti kthehet pergjigje, duke mos penguar aktivitetin e tregtimit te energjise elektrike.

<u>Per blerje te energjise elektrike. Kerkesa/ftesa per oferte duhet te permbaje:</u>

➢ Periudha/dita e blerjes se energjise elektrike e cila mund te jete:
- Periudhe ne blloke;
- Periudhe e kushtezuar (psh. Blerje energji elektrike 1-30 Prill 2019, por periudhen 1-10 Prill eshte e konfirmuar,ndersa periudhat 11-20 dhe 21-30 Prill do rikonfirmohen respketivisht ne datat 8 dhe 18 Prill 2019);
- Peridhe me dite te ndara;

➢ Profili i marrjesse energjise elektrike nga ora 00:oo deri me 24:oo e cila mund te jete:
- Profile ne blloke;
- Profile me ore te ndara;

➢ Kapaciteti i blerjes se energjise elektrike e cila mund te jete:
- Kapacitetin maksimal i kerkuar per tu ofertuar/deri ne... MW;

- Kapacitet i kushtezuar (Psh: blerje energji elektrike per periudhen 11-20 Prill 2019 ne kapacitetin 50 MW,por KESH sh.a. i rezervon te drejten vetes qe me date 8 Prill 2019 ku do te konfirmoje periudhen e blerjes te zgjidhe edhe kapacitetin e levrimit e cila mund te jete nga 0 MW deri me 50 MW)
- Kapacitet ne blloke;
- Kapacitet me ore te ndara;

➢ Sasia e energjise elektrike mund te jete:
- Sasia maksimale e kerkuar per tu blere/ deri ne .... MWh;
- Sasia e kushtezuar (Psh: blerje energji elektrike per periudhen 11-20 Prill 2019 ne kapacitetin 50 MW dhe sasine 1200 MWh, por KESH sh.a. i rezervon te drejten vetes qe me date 8 Prill 2019 ku do te konfirmoje periudhen e blerjes te zgjidhe edhe kapacitetin e levrimit e cila mund te jete nga 0 MW deri me 50 MW respektivisht edhe sasia e energjise elektrike)
- Sasia ne blloke;
- Sasi me ore te ndara;

➢ Cmimi njesi i kerkuar per tu ofertuar mund te jete:
- Cmime/njesi ne blloke;
- Cmime/njesi orar;
- Cmime/njesi tavan;

➢ Pika e levrimit te energjise elektrike e cil mund te jete:
- Brenda rrjetit te transmetimit
- Ne kufirin Shqiperi-Mali i Zi/Serbi/Greqi

➢ Siguruesi i kapacitetit mund te jete:
- Nga shoqerite ofertuese;
- Nga KESH sh.a.;

➢ Kriteri vleresimit te ofertave eshte:
- cmimi/njesi me i ulet deri ne permbushjen e sasise se kerkuar per blerje te energjise elektrike;
- i kushtezuar sipas cmimit tavan te vendosur ne oferte;
- Ne rast kur kemi dy oferta me te njejtin cmimi do te ndiqet parimi i pari qe vjen i pari sherbehet/pranohet;

➢ Kriteri financiar lidhur me menyren e pageses mund te jete:
- Me parapagim;
- Garanci financiare;
- Mjete te jera financiare;

➢ Afati i hapjes dhe e mbylljes se mjetit elektronik te perdoruar nga KESH sh.a. per zhvillimin e procedures se shit-blerjes se energjise elektrike per ofertimin e shoqerive tregtare;

➢ Kushte te tjera te vendosura nga Autoriteti Kontraktues;

➢ Raporti i mbylljes se procedures/rezultatet e procedures se sblerjes duke publikuar cmimet dhe sasite mesatare te ofertuara dhe ato te fituara.

➢ Ankimimi. Brenda afatit te percaktuar ne kerkesen/ftesen per oferte shoqerite kane te drejte qe nepermjet sistemit elektronik te dergojne ankesen dhe sipas afateve te percaktuara do ti kthehet pergjigje, duke mos penguar aktivitetin e tregtimit te energjise elektrike.

6.9 Siguria e sistemit

Pajisja e monitorimit të zgjidhjes duhet të jetë në gjendje të mbështesë mënyrat e mëposhtme të vendosjes për të monitoruar trafikun e aplikacioneve në ueb në rrjet:
- Nëpërmjet një modaliteti nuhatës të portit SPAN/TAP
- Modaliteti i urës së brendshme transparente të shtresës 2 (duhet të jetë mbështetje vendase dhe jo përmes integrimit të palës së tretë)
- Modaliteti i përfaqësuesit të kundërt
- Modaliteti Transparent Layer-2 Reverse Proxy (Layer-2, por që përfundon sesionet përkatëse TCP)

Për modalitetin e vendosjes së urës së brendshme të shtresës 2 dhe për pajisjet fizike, zgjidhja duhet të ketë një anashkalim të integruar për të mbështetur modalitetin "hapja e dështuar". Zgjidhja duhet të ketë gjithashtu aftësinë për të mbështetur modalitetin "fail-close". Kjo duhet të jetë një veçori e mbështetur në mënyrë origjinale në zgjidhje dhe jo nëpërmjet një integrimi të palës së tretë.
E gjithë zgjidhja duhet të menaxhohet nga qendra për operacionet e përditshme. Raportimi, krijimi i politikave, menaxhimi i sinjalizimeve, konfigurimi i mbrojtjes së aplikacionit në ueb, etj duhet të menaxhohen nga serveri i menaxhimit. Serveri i menaxhimit duhet të menaxhojë në mënyrë qendrore të gjitha portat e ndryshme të monitorimit. Zgjidhja duhet t'i lejojë përdoruesit të përdorë një shfletues standard për të hyrë në ndërfaqen e menaxhimit.
Gjatë shkallëzimit të zgjidhjes, zgjidhja duhet të mbështesë një qasje të zmadhuar duke u mjaftuar vetëm të shtojë më shumë porta monitorimi sipas nevojës dhe të regjistrojë portat në serverin e menaxhimit.
Zgjidhja duhet të mbështesë një model vendosjeje të shpërndarë WAN/global, ku mund të vendosen shumë Serverë Menaxhimi për çdo rajon gjeografik. Të gjithë serverët e menaxhimit duhet të jenë në gjendje të menaxhohen në mënyrë qendrore nga një "Menaxheri i Menaxherëve". "Menaxheri i Menaxherëve" duhet të ofrojë aftësitë e mëposhtme:
- Menaxhimi dhe administrimi i unifikuar i mjediseve të federuara në të gjithë serverët e menaxhimit
- Krijimi, konfigurimi dhe shpërndarja e politikave në të gjithë sistemin në të gjithë serverët e menaxhimit
- Pika e vetme e aksesit në çdo Server Menaxhimi
- Monitorimi i shëndetit të zgjidhjes për të gjithë vendosjen
- Pamje e gjerë e sistemit të aktiviteteve të sigurisë

Zgjidhja duhet të jetë në gjendje të mbështesë rastin e përdorimit ku disa aplikacione ueb mbrohen në modalitetin Transparent Reverse Proxy dhe disa aplikacione ueb për t'u mbrojtur në modalitetin e urës së brendshme transparente Later-2. Kjo duhet të mbështetet në mënyrë origjinale në zgjidhje dhe jo nëpërmjet integrimit të zgjidhjeve të tjera nga palët e treta. Përshkruani se si arrihet kjo.
Zgjidhja duhet të jetë e thjeshtë dhe intuitive për t'u konfiguruar dhe konfiguruar. Me të gjitha miratimet e kërkuara të menaxhimit të ndryshimeve në vend dhe informacionin e rrjetit në dispozicion.

Duhet të ketë ndikim minimal në aplikacionet ekzistuese të Uebit dhe arkitekturën e rrjetit gjatë vendosjes ose heqjes së zgjidhjes nga rrjeti. Përshkruani se si arrihet kjo.
Kur vendoset në platformën Amazon Web Services, zgjidhja duhet të mbështesë aftësinë e shkallëzimit automatik.
Kur vendoset në platformën Google Cloud, zgjidhja duhet të mbështesë aftësinë e shkallëzimit automatik.
Kur vendoset në platformën Microsoft Azure, zgjidhja duhet të mbështesë aftësinë e shkallëzimit automatik.
Zgjidhja duhet të vijë me opsionin për të zgjeruar fushën e mbrojtjes në renë kompjuterike me një WAF të bazuar në renë kompjuterike. WAF i bazuar në renë kompjuterike duhet gjithashtu të vijë me zbutjen e rrjetit DDoS, Mbrojtjen DNIS, Sigurinë API, Mbrojtjen e Avancuar të Bot-it, Mbrojtjen nga ana e klientit CDN dhe aftësinë e balancimit të ngarkesës me shtresa-7. Cloud WAF dhe premisa duhet të integrohen me një model të unifikuar të panelit të raportimit dhe alarmit.

Kërkesat e Sigurisë
Zgjidhja duhet të mbështesë mekanizmin e mëposhtëm të vërtetimit për të hyrë në UI-në e menaxhimit të zgjidhjes:
- Autentifikimi i integruar në zgjidhje
- Autentifikimi Kerberos
- Autentifikimi dhe autorizimi i LDAPS me platformat e mëposhtme të Windows: 2008, 2008 R2, 2012 dhe 2012 R2.
- Autentifikimi RADIUS
- Autentifikimi i bazuar në kartën inteligjente
Zgjidhja duhet të jetë e certifikuar me kritere të përbashkëta.
Zgjidhja duhet të ofrojë kontroll të aksesit të bazuar në role ose role të shumta përdoruesish që lehtësojnë ndarjen e detyrave.
Zgjidhja duhet të mbështesë aftësitë e mëposhtme të menaxhimit të fjalëkalimit pa u mbështetur në ndonjë sistem të jashtëm:
a. Periudha e vlefshmërisë së fjalëkalimit në ditë
b. Gjatësia e fjalëkalimit (numri minimal i kërkuar i karaktereve në fjalëkalim.)
c. Nëse një fjalëkalim duhet të jetë dukshëm i ndryshëm nga fjalëkalimi i fundit i përdorur.
d. Nëse një fjalëkalim duhet të përfshijë shkronja të mëdha, numra, shkronja të vogla dhe karaktere jo alfa-numerike apo jo.
Zgjidhja duhet të jetë në gjendje të mbështesë konfigurimin e cilësimeve të mëposhtme të bllokimit nga ndërfaqja e përdoruesit të menaxhimit të zgjidhjeve:
a. Periudha e përpjekjeve të dështuara të hyrjes (në minuta) në të cilën futja e një fjalëkalimi të pasaktë disa herë bllokon një llogari
b. Numri i përpjekjeve të dështuara të hyrjes që rezultojnë në bllokimin e një llogarie
c. Kohëzgjatja e kyçjes në minuta
Zgjidhja duhet të mbështesë aftësinë e komunikimit të bazuar në besimin ndërmjet komponentëve të ndryshëm në zgjidhje. dmth. Komunikimi ndërmjet komponentëve të zgjidhjes duhet të bëhet duke përdorur certifikata.
Zgjidhja duhet të mbështesë openssl 1.0.2

Kërkesat e zgjidhjes WAF
WAF duhet të jetë lider në kuadrantin magjik Gartner për muret e zjarrit të aplikacioneve në ueb të paktën për 7 vitet e fundit.
Zgjidhja duhet të mbështesë qasjen e modelit pozitiv të sigurisë. Një model sigurie pozitive deklaron se çfarë hyrje dhe sjellje lejohet dhe çdo gjë tjetër që devijon nga modeli pozitiv i sigurisë sinjalizohet dhe/ose bllokohet.

Zgjidhja duhet të mbështesë qasjen e modelit negativ të sigurisë. Një model negativ sigurie përcakton në mënyrë eksplicite nënshkrimet e njohura të sulmit.
Zgjidhja duhet të ofrojë një normë false-pozitive pothuajse zero duke përdorur politika të para-konfiguruara OOTB (Out Of The Box) që lejon që WAF të vendoset në modalitetin e bllokimit pa pasur nevojë të sintonizohen politikat.
Zgjidhja duhet të jetë në gjendje të bllokojë transaksionet me përmbajtje që përputhet me nënshkrimet e njohura të sulmit duke lejuar çdo gjë tjetër.
Zgjidhja duhet të jetë në gjendje të mbështesë simulimin inline dhe jo-inline dhe mënyrën aktive të zbatimit. Në modalitetin e simulimit, administratori mund të shikojë sinjalizimet, sulmet, gabimet e serverit dhe aktivitete të tjera të paautorizuara. Në modalitetin e zbatimit aktiv, zgjidhja mund të kryejë gjithçka që bëhet në modalitetin e simulimit dhe gjithashtu të jetë në gjendje të bllokojë sulmet.
Zgjidhja duhet të jetë në gjendje të ekzekutojë veprimet e mëposhtme me zbulimin e një sulmi ose ndonjë aktiviteti tjetër të paautorizuar:
- Aftësia për të hequr kërkesat dhe përgjigjet,
- Blloko seancën TCP,
- Blloko përdoruesin e aplikacionit, ose
- Blloko adresën IP

Zgjidhja duhet të jetë në gjendje të bllokojë përdoruesin ose adresën IP për një periudhë kohe të konfigurueshme.
Zgjidhja duhet të jetë në gjendje të dërgojë një paketë TCP RST në të dy skajet e një lidhjeje ueb kur ajo vendoset në modalitetin e nuhatjes në rast të modalitetit të vendosjes së zbatimit aktiv.
Zgjidhja duhet të jetë në gjendje të mbrojë si aplikacionet në ueb HTTP ashtu edhe aplikacionet ueb SSL (HTTPS).
Zgjidhja duhet të jetë në gjendje të inspektojë dhe mbrojë të dy protokollet HTTP/1.x dhe HTTP/2.
Zgjidhja duhet të jetë në gjendje të deshifrojë trafikun e internetit SSL midis klientëve dhe serverëve të uebit.
Zgjidhja duhet të jetë në gjendje të deshifrojë trafikun në ueb SSL që përdorin protokollet e shkëmbimit të çelësave Diffie-Hellman me pajisjen monitoruese të vendosur në modalitetin transparent të shtresës 2 të urës (Modaliteti i urës së avancuar).
Zgjidhja duhet të ofrojë aftësinë për t'u pajtuar me Certifikimin A+ me klikimin e një butoni.
Zgjidhja duhet të ofrojë aftësinë për të kontrolluar cilësimet SSL nëpërmjet një ndërfaqeje të bazuar në GUI.
Zgjidhja duhet të jetë në gjendje të deshifrojë trafikun e internetit SSL për inspektim pa ndërprerë ose ndryshuar lidhjen HTTPS. (Përjashtuar protokollet e shkëmbimit të çelësave Diffie-Hellman).
Zgjidhja duhet të ofrojë veçoritë dhe mbrojtjen e mëposhtme jashtë kutisë:
- Vlefshmëria e protokollit HTTP (1.x dhe 2).
- Vlefshmëria e sulmit të ndërlidhur me shtresën e shërbimit në ueb
- Nënshkrimet e sulmit të protokollit HTTP
- Mbrojtje e personalizuar e shtresës së shërbimit në ueb
- Vlefshmëria e nënshkrimit të cookie-ve
- Anti-skrapi i vendit
- Mbrojtja e profilit në ueb
- Mbrojtja nga krimbat e uebit
- Nënshkrimet e sulmit të aplikacionit në ueb
- Mbrojtje e personalizuar e shtresës së aplikacionit në ueb
- Vlefshmëria e protokollit OCSP
- Sfida CAPTCHA

Zgjidhja duhet të përfshijë një listë të para-konfiguruar të nënshkrimeve gjithëpërfshirëse dhe të sakta të sulmit në ueb.
Zgjidhja duhet të ketë një bazë të dhënash me minimalisht 6000+ nënshkrime që janë krijuar për të zbuluar problemet dhe sulmet e njohura në aplikacionet në ueb.
Zgjidhja duhet të sigurojë mbrojtje nënshkrimi kundër dobësive të njohura në softuerët e infrastrukturës komerciale si Apache, IIS, Oracle, e kështu me radhë. Përmbajtja e ofruar nga mekanizmi i zbulimit të nënshkrimit duhet të bazohet në kërkimin e bërë nga divizioni i inteligjencës së kërcënimeve të shitësve të zgjidhjeve dhe një kombinim burimesh të tjera si Snort, CVE etj. Ky grup nënshkrimesh duhet të përditësohet vazhdimisht dhe automatikisht.
Zgjidhja duhet të lejojë administratorët të shtojnë dhe modifikojnë nënshkrimet.
Zgjidhja duhet të mbështesë llojet e mëposhtme të përkufizimit të nënshkrimeve me porosi:

Burimi i përdoruesve me qëllim të keq duhet të përditësohet automatikisht dhe periodikisht (Përditësimi i bazës ditore).
Zgjidhja duhet të inspektojë dhe monitorojë të gjitha të dhënat HTTP(S) dhe nivelin e aplikacionit duke përfshirë kokat e HTTP(S), fushat e formularit dhe trupin HTTP(S).
Zgjidhja duhet të jetë në gjendje të inspektojë kërkesat dhe përgjigjet HTTP.
Zgjidhja duhet të jetë në gjendje të identifikojë lidhjet WebSocket.
Zgjidhja duhet të jetë në gjendje të vërtetojë të dhënat e koduara në trafikun HTTP.
Zgjidhja duhet të jetë në gjendje të kryejë vërtetimin në të gjitha llojet e hyrjeve, duke përfshirë URL-të, formularët, kukit, vargjet e pyetjeve, fushat e fshehura dhe parametrat, metodat HTTP, elementët XML dhe veprimet SOAP.
Zgjidhja duhet të jetë në gjendje të kryejë automatikisht profilizimin dinamik të aplikacioneve në internet.
Teknologjia e profilizimit dinamik të zgjidhjes duhet të jetë në gjendje të zbulojë dhe të mbrojë kundër kërcënimeve që janë specifike për kodin personal të aplikacionit në internet. Pas fazës dinamike të profilizimit/të mësuarit, zgjidhja duhet të jetë në gjendje të kuptojë strukturën e çdo URL të mbrojtur.
Zgjidhja duhet të ndërtojë/mësojë automatikisht profilet e aplikacionit në internet dhe t'i përdorë ato për të zbuluar devijime dhe anomali (ose shkelje) të ndryshme dhe të bllokojë sulmet në kodin personal të aplikacionit.
Zgjidhja duhet të jetë në gjendje të mësojë automatikisht përdorimin e uebit dhe strukturën e aplikacionit dhe elementet dhe sjelljet e pritshme të përdoruesit sapo të instalohet sistemi.
Struktura dhe elementet përfshijnë URL-të, drejtoritë, skedarët e skedarëve, fushat dhe parametrat e formularit dhe metodat HTTP. Sjelljet e përdoruesit përfshijnë gjatësinë e pritshme të vlerës; karaktere të pranueshme për fushë parametri; nëse vlera e parametrit është vetëm për lexim ose e modifikueshme nga përdoruesi dhe nëse parametri është i detyrueshëm ose opsional.
Zgjidhja duhet të jetë në gjendje të kalojë automatikisht në modalitetin e mbrojtjes (Modaliteti i bllokimit) pas një periudhe të përshtatshme mësimi, e cila mund të përcaktohet manualisht nga administratori.
Mënyra e të mësuarit të profilizimit dinamik të zgjidhjes duhet të jetë në gjendje të njohë ndryshimet në aplikacionin ueb dhe njëkohësisht të mbrojë aplikacionet e uebit në të njëjtën kohë.
Zgjidhja duhet të jetë në gjendje të kryejë profilizimin dinamik dhe të jetë në gjendje të vendoset në një modalitet bllokimi aktiv të zbatimit në të njëjtën kohë.
Zgjidhja duhet të lejojë që profilet dinamike të ndryshohen manualisht dhe informacioni mund të shtohet dhe hiqet për të rregulluar mirë profilet.
Zgjidhja duhet të mbështesë profilizimin dinamik vetëm nga një grup përdoruesish të besuar për të mësuar sjelljen dhe përdorimin normal të pranueshëm të aplikacionit në internet.

Zgjidhja duhet të lejojë ri-mësimin e një profili aplikacioni mbi bazën për URL ose për faqe. Administratorit nuk duhet t'i kërkohet të mësojë përsëri të gjithë aplikacionin kur kanë ndryshuar vetëm disa faqe.
Zgjidhja duhet të mbështesë konfigurimin për të lejuar që disa faqe në një aplikacion ueb të jenë në modalitetin e mbrojtur dhe disa faqe të jenë në modalitetin e të mësuarit të profilizimit dinamik.
Zgjidhja duhet të jetë në gjendje të kryejë profilizimin dinamik të aplikacioneve në internet në një mjedis ku ka një përzierje të trafikut të mirë dhe të keq. Zgjidhja duhet të jetë në gjendje të dallojë automatikisht trafikun e mirë dhe të keq kur mëson profilin. Trafiku i keq nuk duhet mësuar dhe shtuar në profil.
Zgjidhja duhet të jetë në gjendje të mësojë automatikisht të gjithë emrat e hosteve të aplikacioneve në internet që mbrohen.
Zgjidhja duhet të jetë në gjendje të kryejë profilizimin dinamik të JSON. Kërkesat HTTP në formatin JSON duhet të mësohen nga WAF me parametrat dhe vlerat.
Zgjidhja duhet të jetë në gjendje të mbrojë aplikacionet në internet që përfshijnë përmbajtjen e shërbimeve të uebit (XML).
Mbrojtja XML e ofruar nga zgjidhja duhet të jetë e ngjashme me mbrojtjen e aplikacionit në ueb të ofruar me aftësi të automatizuar të profilizimit/mësimit dinamik. Nuk ka nevojë të importoni skedarin WSDL.
Zgjidhja duhet të mbështesë rregullat e sigurisë me porosi. Administratorët duhet të jenë në gjendje të përcaktojnë rregullat për modelin pozitiv dhe negativ të sigurisë dhe të krijojnë rregulla korrelacioni me kritere të shumta.
Zgjidhja duhet të jetë në gjendje të nënshkruajë në mënyrë dixhitale kukit, të kodojë kukit dhe të rishkruajë URL-të kur vendoset në modalitetin e përfaqësuesit të kundërt.
Zgjidhja duhet të mbështesë si rishkrimin e URL-së, ashtu edhe rishkrimin e përmbajtjes për kokën dhe trupin http kur është në modalitetin e përfaqësuesit të kundërt.
Zgjidhja duhet të jetë në gjendje të kryejë korrigjimin virtual për aplikacionet e saj të mbrojtura në ueb në mënyrë që të sigurojë një korrigjim të menjëhershëm të një cenueshmërie aplikacioni.
Zgjidhja duhet të mbështesë të gjitha mjetet e mëposhtme të vlerësimit të cenueshmërisë së aplikacionit në ueb (skanuesit e aplikacioneve në internet) për të rregulluar praktikisht dobësitë e aplikacionit në ueb:
- Acunetix
- Përtej sigurisë
- Cenzic
- Grupi xhins
- HP Fortify WebInspect
- IBM AppScan
- OBJEKTIVAT NT
- Kualitet
- Shpejtë 7
- Trend Micro
- Veracode
- Kapelë e Bardhë

Zgjidhja duhet të adresojë Kriteret e Vlerësimit të Firewallit të Ueb-Application (WAFEC), siç përcaktohet nga Konsorciumi i Sigurisë së Aplikacioneve në Ueb (www.webappsec.org).
Zgjidhja duhet të jetë në gjendje të ofrojë një furnizim dhe shërbim të inteligjencës së kërcënimit bazuar në reputacionin e burimit. Furnizimi duhet të sigurohet në kohë pothuajse reale për burimet e mëposhtme të njohura të sulmit:
- IP me qëllim të keq
- Anonim

Raportimi
Zgjidhja duhet të ofrojë aftësi raportimi të parapaketuara jashtë kutisë pa ndërhyrjen e përdoruesit/konfigurim të mëtejshëm:
- Analiza e alarmit (Për përdoruesin e aplikacionit, modelet e njohura të sulmit, ashpërsia, IP-ja e burimit me ashpërsinë dhe llojin, URL-ja, përdoruesi me ashpërsinë dhe llojin, llojet e shkeljeve)
- Top 10 shkeljet ditore dhe javore të WAF
- Përmbledhja ditore e lidhjeve të bllokuara
- Raporti i rrjedhjes së të dhënave
- Raporti i zbulimit të shfletimit të drejtorisë
- Lista e alarmeve
- Shkeljet e PCI - WAF
- Raporti i rrjedhjes së mesazheve të ndjeshme të gabimit
- Sinjalizime të ngadalta HTTP/S
- Raportet ditore, tremujore dhe mujore të Inteligjencës së Kërcënimit për përfaqësuesit anonimë, IP-të e postës elektronike të komenteve, IP-të me qëllim të keq, URL-të e phishing, nënshkrimet RFI, IP-të e injektimeve SQL, IP-të e skanerit dhe IP-të TOR.
- Raporti ditor i shkeljeve kryesore të robotëve
Zgjidhja duhet të mbështesë krijimin e raporteve të profilizimit dinamik të mëposhtëm:
- Biskota të mësuara
- Emrat e mësuar të hosteve
- Mësuan drejtoritë e ndjeshme
- Modelet e URL-ve të mësuara
- URL-të e mësuara
- Ndjekja e përdoruesve të aplikacionit në ueb
Zgjidhja duhet të ofrojë funksionalitet për të ndihmuar në mjekësinë ligjore të ngjarjeve të sigurisë.
Zgjidhja duhet të ketë aftësinë për t'u integruar me një mjet "Atack Analytics". Mjeti "Atack Analytic" duhet të tresë të gjitha sinjalizimet e sigurisë dhe të ndihmojë administratorët e sigurisë të verifikojnë sinjalizimet më të rëndësishme të sigurisë.
Mjeti i "Atack Analytics" duhet të jetë në gjendje të konsolidojë ngjarjet e sigurisë nga WAF të vendosura në cloud, WAF On-Premise dhe WAF Cloud Service.
Zgjidhja duhet të ketë funksionalitetin brenda UI-së jashtë kutisë që i mundëson administratorit të krijojë shabllone raportesh të personalizuara bazuar në raportet ekzistuese jashtë kutisë.
Zgjidhja duhet të mbështesë redaktimin dhe krijimin e politikave të sigurisë që drejtohet nga një UI miqësore për përdoruesit.
Zgjidhja duhet të mbështesë gjenerimin e raporteve me pamje tabelare dhe pamje grafike të analizës së të dhënave.
Zgjidhja duhet të mbështesë gjenerimin automatik të raporteve bazuar në një plan të përcaktuar.
Zgjidhja duhet të mbështesë planifikimin e gjenerimit të raportit për të filluar vetëm në një datë të ardhshme.

Administrata dhe Menaxhimi
Zgjidhja duhet të ketë një modul/pajisje të dedikuar të menaxhimit të centralizuar.
Zgjidhja duhet të sigurojë një instalues të bazuar në ueb të lehtë për t'u përdorur që mundëson vendosjen e WAF duke përdorur një proces të thjeshtë të bazuar në magjistar.
Zgjidhja duhet të ofrojë mbështetje API që lejon vendosjen e automatizuar të WAF në mjediset DevOps.

Pajisja e menaxhimit të zgjidhjeve duhet të jetë në gjendje të menaxhojë deri në 200 pajisje WAF.
Pajisja e menaxhimit të zgjidhjeve duhet të jetë në gjendje të trajtojë deri në 40,000 certifikata SSL të ngarkuara (madhësia e çelësit 1024-bit).
Menaxhimi i zgjidhjeve duhet të jetë në gjendje të mbështesë shumë qira për menaxhimin e pajisjes.
Zgjidhja duhet të vijë me një ndërfaqe administrimi të bazuar në ueb dhe GUI.
Zgjidhja duhet të ketë dy porte menaxhimi për të mbështetur menaxhimin jashtë brezit.
Pajisja e menaxhimit të zgjidhjeve duhet të mbështesë menaxhimin dhe raportimin e centralizuar për pajisje të shumta monitoruese.
Pajisja e menaxhimit në ambientet e zgjidhjes duhet të jetë në gjendje të menaxhojë një shembull të pajisjes WAF që është vendosur në platformën AWS dhe njëkohësisht të menaxhojë një pajisje WAF që është vendosur në mjedis.
Pajisja e menaxhimit në ambientet e zgjidhjes duhet të jetë në gjendje të menaxhojë një shembull të pajisjes WAF që është vendosur në platformën Microsoft Azure dhe në të njëjtën kohë të menaxhojë një pajisje WAF që është vendosur në premisë.
Kur ofrohet si një pajisje virtuale, zgjidhja duhet të vijë si një imazh i përgjithshëm VM (një çift .ovf & .vmdk). Dmth një imazh i vetëm VM për instalimin e të gjithë komponentëve (server menaxhues, pajisje porta, etj.)
Pajisja harduerike e zgjidhjes duhet të vijë me ekran LCD që shfaq minimalisht funksionet e mëposhtme:
- Shfaq informacione për emrin e hostit, modelin e zgjidhjes dhe versionin
- Shfaq statusin e zgjidhjes (i konfiguruar, në ekzekutim, i ndaluar, etj.)
- Informacioni i rrjetit: Adresa IP, IP e parazgjedhur e portës,
- Aftësia për të ping portën e paracaktuar; Pini një adresë IP; Cakto Adresën IP të Menaxhimit të pajisjes; Cakto portën e paracaktuar
- Rinisni dhe fikni pajisjen.
Zgjidhja duhet të sigurojë menaxhim të centralizuar të softuerit për të thjeshtuar vendosjen e patch-it dhe përmirësimet në
Porta e WAF.
Gjatë përmirësimit të zgjidhjes, zgjidhja nuk duhet të kërkojë ndonjë ndërhyrje njerëzore për të rindezur. Të gjitha rindezjet e sistemit gjatë përmirësimeve duhet të jenë automatike dhe sistemi duhet të rindizet vetë sipas nevojës.
Zgjidhja duhet të vijë me aftësitë e monitorimit të shëndetit të sistemit për të ofruar ndërgjegjësim në kohë reale për shëndetin e të gjithë elementëve në vendosjen e zgjidhjes. Monitorimi shëndetësor duhet të vijë minimalisht me alarme/alarme për çështjet e mëposhtme:
- Tepricë & Disponueshmëri e lartë
- Ngarkesa dhe Kapaciteti
- Lidhja me rrjetin
- Probleme harduerike
- Mospërputhjet e konfigurimit midis komponentëve të ndryshëm

Disponueshmëria dhe Performanca e Lartë
Zgjidhja duhet të mbështesë disponueshmërinë e lartë.
Zgjidhja duhet të ketë një modul anashkalimi të integruar (i hapur) kur pajisja harduerike vendoset në modalitetin inline.
Pajisja harduerike duhet të ketë të paktën 2 segmente të brendshme anashkaluese.
Zgjidhja duhet të jetë në gjendje të mbështesë operacionet me shumë nyje dhe

SERVER	
Form Factor	Të montueshëm në rack
Procesor:	Minimumi 1 CPU x 12 core minimum 2 GHz.
Chipset	Intel or AMD
Slote memorje RAM	Min 12 DIMMs of DDR4 memory
Memorja "RAM":	Minimum 64 GB Memory te perfshira.
Madhësia e Hard Diskut	2 x 2TB 10k rpm SAS
"RAID Controller":	Hardware Raid Controller.
"Network"	Minimumi 1 kartë dual port 1GB Ethernet
"Management Network"	Portë menaxhimi e dedikuar e cila bën menaxhimin edhe nëse serveri është i fikur. Të japë mundësi për fikje/ndezje/logs etj.
Operating systems support	vMware , Microsoft,Linux
GARANCIA	3 vite

6.10 Server

7 Logjistika dhe Koha

7.1 Vendndodhja

- Vend instalimi i sistemit duhet të jetë në një infrastrukturë fizike e përbërë nga dy server me gadishmëri të lartë dhe standarte të sigurisë kibernetike.
- Operatori ekonomik do të jetë pergjegjës për vazhdueshmërinë e sistemit në 24x7 dhe të njoftojë paraprakisht për ndërhyrje apo raste difektesh.
- Platforma duhet të ofrojë ruajtje të informacionit arshivor deri në 2 vite.

7.2 Afati kohor për zbatimin e projektit

Afati kohor- për zbatimit e këtij projekti do të jetë 30 ditë, nisur nga data e nënshkrimit të kontratës.

Mirembajtja- do te jetë 1 (një) vit nga momenti i lëshimit të Certifikatës së marrjes në dorëzim të sistemit. Shërbimet e mirëmbajtjes do të realizohen konform kërkesave bashkëlidhur këtyre specifikimeve teknike.

8 PLANIFIKIMI I BUXHETIT PËR NDËRTIMIN E SISTEMIT

Nr.	Emërtimi	Sasia	Njësia	Çmimi
1	Dizenjimi dhe implementimi i sistemit menaxhimit te shit-blerjes	1	Copë	
2	Server	2	Copë	
3	Platforma e sigurisë	1	Copë	
4	Trajnim mirëmbajtje	30	Orë	
5	Mirëmbajtje e sistemit (HW/SW SLA)	12	Muaj	
TOTALI ME TVSH (LEKË)				

9 Zbatimi i projektit dhe shërbimet

9.1 Menaxhimi i Projektit

1. Furnizuesi duhet të jetë përgjegjës implementimin, adaptimin, testimin, shpërndarjen dhe instalimin e të gjitha informacioneve teknike të sistemit si dhe duhet të ofrojë trajnim për përdoruesit.

2. Furnizuesi duhet të sigurojë një plan zbatimi të projektit me piketa të qarta.

3. Projekti duhet të përfundojë plotësisht brenda 30 ditëve, nga data e firmosjes së kontratës.

9.2 TRAJNIMI

Trajnimi i përdoruesve duhet të jetë për të gjithë përdoruesit e sistemit. Operatori ekonomik duhet gjithashtu të ndërtoje prezantime me shpjegime shteruese për përdorimin e sistemit në mënyrë që të kuptohet lehtësisht nga operatorët të cilët do ta përdorin platformën.

9.3 Parnimi i sistemit

- Furnizuesi duhet të kryejë testet e pranimit të sitit të sistemit pas implementimit të tij.

- Furnizuesi duhet të demonstrojë që sistemi është dorëzuar dhe instaluar në përputhje me specifikimet dhe kërkesat teknike.
- Furnizuesi duhet të sigurojë planet dhe procedurat e testimit për miratim para kryerjes së pranimit të sitit.
- Hapat e testit të përmendur në Planin e Testit duhet të miratohen paraprakisht nga grupi ndjekjes së kontratës
- Një çertifikatë duhet të lëshohet pas përfundimit dhe të suksesshëm të pranimit.

Garancia teknike për pajisjet do të jetë 3 vjet.

10 PËRGJIGJA DHE SHKALLËZIMI I SHËRBIMIT

Në tabelën e mëposhtme përcaktohet kategorizimi i seriozitetit të problemeve dhe koha e përgjigjes për zgjidhjen e tyre.

Kategoria A (Kritik/ I Larte)	**Kategoria** A **(I Mesem)**	**Kategoria C (I Ulet)**
Mos funksionimi i aplikacionit krijon apo rrezikon shumë aktivitetin normal	Mos funksionimi i aplikacionit krijon vonesa në aktivitetin normal	Mos funksionimi i aplikacionit pengon në mënyrë minimal aktivitetin
Numri i përdoruesve të ndikuar		
Mos funksionimi i sistemit ndikon një numër ***shumë të madh*** të përdoruesve	Mos funksionimi i sistemit ndikon një numër ***të vogël*** të përdoruesve	Mos funksionimi i sistemit ndikon pjesërisht në disa përdorues
Pezullimi i punës		
Mos funksionimi i sistemit pengon përdoruesit ***të realizojnë pjesën më të madhe të punës së tyre.***	Mos funksionimi i sistemit pengon përdoruesit ***të realizojnë pjesë te punës së tyre***	Mos funksionimi i sistemit pengon përdoruesit ***të realizojnë disa pjesë të vogla të punës së tyre***,
Zgjidhje alternative e përkohshme		
Nuk ka një mënyre alternative të përkohshme dhe të pranueshme për zgjidhjen e problemit	***Ka pjesërisht një mënyre alternative*** të përkohshme dhe të pranueshme për zgjidhjen e problemit.	***Ka një mënyrë alternative*** të përkohshme dhe të pranueshme për zgjidhjen e problemit..
Koha e përgjigjes		
○ *1 orë për të kthyer përgjigje* ○ *Në vend brenda 4 orëve*	○ *2 orë për të kthyer përgjigje* ○ *Në vend brenda 8 orëve*	○ *4 orë për të kthyer përgjigje* ○ *Në vend brenda 24 orëve*
Koha e zgjidhjes		
Maksimumi i pranimit Kjo zgjidhjes është 1 dite pas kërkesës.	Maksimumi i pranimit Kjo zgjidhjes është brenda 5 ditëve të punës.	Maksimumi i pranimit Kjo zgjidhjes është 10 ditë kalendarike.

a) **Shërbime të mirëmbajtjes parandaluese**

Kompania duhet të ndërmarrë, në mënyrë periodike **një herë në muaj**, shërbime të Mirëmbajtjes Parandaluese për të gjitha pajisjet e listuara në tabelën mësipër.

b) **Shërbime Riparimi në vendndodhje**

Kompania duhet të jetë e disponueshme gjatë interval kohor, nga e Hëna në të Dielë, 24x7, për të ofruar Shërbime të Riparimit në përgjigje të "Alarmeve Madhore" të raportuara nga personeli i autorizuar. Për këtë qëllim, me termin "Alarm Madhor" do të kuptohet parashtrimi i kërkesës për Shërbime Riparimi të ndërmarra në rast të keqfunksionimit të Sistemeve të mbuluara, që i pengon ato të operojnë në përputhje me Specifikimet dhe shkaktojnë ndërprerje të menjëhershme e të konsiderueshme të proceseve të punës në KESH.