



KORPORATA ELEKTROENERGJITIKE SHQIPTARE SH.A

**" Krijimi i programit të menaxhimit të aktivitetit të operimit
tregtar "**

1 FAQJA E KONTROLLIT TË DOKUMENTIT

1.1 Historiku i Versioneve dhe Ndryshimeve të Dokumentit

Data	Autori	Versioni	Shënime mbi Rishikimet
12.04.2021	Grupi i punës	1.1	

2 NËNSHKRIMET MIRATUESE

Përgatiti:

Përgatiti:

Përgatiti:

Përgatiti:

Miratoi:

Miratoi:

3 PËRMBAJTJA

SPECIFIKIMET TEKNIKE	1
1 FAQJA E KONTROLLIT TË DOKUMENTIT	2
1.1 Historiku i Versioneve dhe Ndryshimeve të Dokumentit	2
2 NËNSHKRIMET MIRATUESE	2
3 PËRMBAJTJA.....	3
4 Përfituesi /Autoriteti Kontraktues	5
4.1 Hyrje.....	5
5 Përshkrimi i Përgjithshëm i kërkesave.....	5
5.1 Kërkesat funksionale të sistemit (modulet).....	6
5.1.1 Moduli i krijimit të përdoruesve	6
5.1.2 Moduli i krijimit të klienteve	6
5.1.3 Moduli i garancise bankare	6
5.1.4 Moduli i kapaciteteve nderkufitare	7
5.1.5 Moduli i publikimit të tenderave.....	7
5.1.6 Moduli i dorezimit të ofertave	7
5.1.7 Moduli i vleresimit të ofertave.....	7
5.1.8 Moduli i gjurmëve (log) dhe sigurisë së modulit të portalit	8
5.1.9 Moduli i fiskalizimit të faturave	8
6 Specifikime teknike të sistemit	9
6.1 Frontend	9
6.2 Backend.....	10
6.3 Databaza.....	10
6.4 Arkitektura	10
6.5 Kodi burim	10
6.6 Ndërveprimi me sistemet e tjera.....	11
6.7 Komponenti i fiskalizimit.....	11
6.8 Proceset e biznesit (Workflows) që platforma duhet të ndjekë në funksionimin në tërësi të saj.....	11
6.8.1 Aplikimi për regjistrimin e shoqërive tregtare.....	11
6.8.2 Administrimi i kalendarit të kërkesave/ftesave për shitje/blerje.....	12
6.8.3 Administrim i ankesave	13
6.9 Proceset e biznesit (Workflows) të tregtimit të energjisë elektrike të detajuara	13
6.10 Siguria e sistemit	16
7 Logjistika dhe Koha.....	24

7.1	Vendndodhja	24
7.2	Afati kohor për zbatimin e projektit.....	24
8	PLANIFIKIMI I BUXHETIT PËR NDËRTIMIN E SISTEMIT.....	24
9	Zbatimi i projektit dhe shërbimet.....	25
9.1	Menaxhimi i Projektit.....	25
9.2	TRAJNIMI	25
9.3	Pranimi i sistemit.....	25
10	PËRGGJIGJA DHE SHKALLËZIMI I SHËRBIMIT	25

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 rëndësi të 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 ulët 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, mirëmbajtjes 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

Në kuadër të përmirësimit të vijueshëm të aktivitetit të operimeve tregtare të përditshme në Korporatën Elektro-Energjetike Shqiptare, është identifikuar nevoja për të investuar në teknologjinë e informacionit, më konkretisht në digjitalizimin, unifikimin dhe harmonizimin e aktiviteteve të shit-blerjes së energjisë elektrike. Më konkretisht, nëpërmjet një programi modular software do të mundësohet digjitalizimi dhe automatizimi i procesit të shitblerjes që nga momenti i publikimit të procedurave tenderuese të shitjes dhe blerjes së energjisë elektrike nga ana e KESH, ku të gjithë operatorëve vendas apo të huaj tu mundësohet të japin ofertat e tyre për keto procedura, marrjen e ofertave online nëpërmjet programit, gjenerimin e faturave financiare, ekzekutimin e tyre në përputhje me regjimin tatimor, fiskalizimi i faturave dhe arkëtimet e transaksioneve, regjistrimi i të gjitha të dhënave të transaksioneve financiare në këtë program. Programi gjithashtu do të bëjë të mundur sugjerimin në mënyrë automatike të ofertave me të favorshme për KESH për të maksimizuar të ardhurat dhe për të ulur shpenzimet. Në kushtet ku KESH sh.a. është pajisur me licensë në aktivitetin e furnizimit me energji elektrike si dhe ku parashikohet që procedurat e shit-blerjes së energjisë elektrike do të kryhen me mjete elektronike, lindë nevoja për hartimin e rregullave të reja të tregtimit të energjisë 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 kërkojë të skanojë me anë të një aplikacioni për autentikim një kod QR i cili duhet të gjenerojë fjalëkalime njëpërdorimshme. 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 të klienteve

Në këtë sistem, klient do të quhet çdo operator vendas apo i huaj i cili është i interesuar të marrë pjesë në prokurimet e publikuara nga KESH për shitblerjen e energjisë elektrike. Për shkak të rëndësisë së sistemit klientet e interesuar duhet në fillim të kontaktojnë me KESH dhe të ndjekë procedurat përkatëse, i cili bën verifikimin e dokumenteve dhe më pas përdoruesit e brendshëm të KESH kanë mundësi të krijojnë llogari klienti për ta. Për të krijuar një klient përdoruesit e KESH regjistrojnë emrin e klientit, shtetin, aksionerët, ngarkojnë dokumentet përkatëse, vendosin të dhënat për përdoruesin i cili do të futet në sistem. Në çastin e krijimit të klientit paralelisht në mënyrë automatike sistemi duhet të krijojë dhe përdoruesin përkatës për atë klient. Pas krijimit të përdoruesit sistemi duhet të mundësojë të njëjtën rrjedhë për kyçjen e përdoruesit në sistem si në piken 5.1.1.

5.1.3 Moduli i garancisë bankare

Në këtë modul përdoruesit e financës kanë mundësinë të ngarkojnë në sistem një dokument i cili vërteton garancinë bankare të mbyllur nga një klient në benefit të KESH. Sistemi duhet ti mundësojë përdoruesve mundësinë e ngarkimit të këtij dokumenti si dhe ti japë mundësinë atyre që të plotësojnë fushat si, vlera totale e garancisë, datën e skadimit, vlera e mbetur që mbulon garancia. Kur një klient shpallet fitues për një tender dhe ai nuk i ka dërguar KESH-it vërtetimin e pagesës. KESH mund të përdorë garancinë bankare për të proceduar me proceset. Për ta bërë këtë gjë nevojitet që vlera e mbetur e garancisë bankare të jetë më e madhe se sa vlera që klienti i detyrohet KESH. Në çastin që klienti i dërgon KESH-it vërtetimin e pagesës për procedurën përkatëse dhe KESH ka përdorur garancinë bankare të klientit, atëherë vlera e pagesës i shtohet vlerës së garancisë bankare për klientin.

5.1.4 Moduli i kapaciteteve ndërkufitare

Në këtë modul përdoruesit e KESH duhet të kenë mundësinë që të regjistrojnë në sistem të gjithë blerjet që KESH bën për blerjet e kapaciteteve ndërkufitare. Në këtë modul regjistrohen të dhënat se kur është blerë një kapacitet ndërkufitar, drejtimin, kapacitetin e blerë (MW), datën e blerjes, dhe vlerën me të cilën është blerë ky kapacitet. Ky informacion do të përdoret në modulën e prokurimit në të cilin KESH do të përcaktojë nëse për një procedurë specifike kapaciteti ndërkufitar sigurohet nga KESH apo është përgjegjësi e klientit.

5.1.5 Moduli i publikimit të tenderave

Në këtë modul përdoruesit e KESH duhet të kenë mundësinë të publikojnë një tender për shitje apo për blerje energjie. Në këtë modul përdoruesit duhet të kenë mundësinë të hedhin informacion lidhur me një tender të caktuar. Informacioni përfshin një emërtim dhe përshkrim të tenderit, datën kur fillon pranimi i ofertave dhe datën kur mbaron pranimi i ofertave, datën kur fillon dhe kur mbaron shitblerja e energjisë, kapacitetin që do të blihet apo shitet si dhe informacion lidhur me kapacitetin ndërkufitar. Për çdo tender përdoruesit e KESH duhet të kenë mundësi të krijojnë profilet orare (ose lotet) në të cilët do të specifikohen saktë fashat orare kur KESH dëshiron të shesë dhe të blejë energji elektrike. Çdo tender qëndron fillimisht në statusin “DRAFT” dhe publikohet manualisht nga administratori i sistemit.

5.1.6 Moduli i dorëzimit të ofertave

Në këtë modul klientet kanë mundësi të japin ofertat e tyre për çdo tender. Klientet janë të detyruar që ofertën ta bëjnë për çdo profil (lot). Oferta e bërë nga klienti mund të mos jetë për të gjithë kapacitetin e kërkuar nga KESH ose mund ta tejkalojë kapacitetin që KESH kërkon. Një klient ka të drejtë të modifikojë ofertën e tij deri kur afati i dorëzimit të ofertave të ketë përfunduar. Pas përfundimit të afatit të dorëzimit të ofertave sistemi nuk duhet të lejojë më modifikimin e ofertës nga klienti. Për çdo ofertë të dërguar sistemi duhet të njoftojë me SMS klientin që oferta e tij u dorëzua me sukses.

5.1.7 Moduli i vlerësimit të ofertave

Në këtë modul sistemi duhet ti japë mundësinë përdoruesve të KESH të vlerësojnë ofertat e dhëna nga klientet për një tender të caktuar. Këto oferta mund të bëhen të dukshme nga KESH vetëm pasi afati i dorëzimit të ofertave ka përfunduar. Sistemi gjithashtu do të bëjë të mundur sugjerimin në mënyrë automatike të ofertave me të favorshme për të maksimizuar të ardhurat dhe për të ulur shpenzimet. KESH ka mundësinë të përzgjedhë si fitues klientë të ndryshëm për çdo profil (lot). KESH ka mundësinë të përzgjedhë në mënyrë të pjesshme një ofertë për një lot të caktuar (pra të marrë vetëm një pjesë të ofertës së dhënë nga një klient)

dhe jo të gjithë ofertën për çdo lot. Pas përzgjedhjes si fituese të një oferte për lot, KESH duhet të ketë të drejtë të shpallë 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 serverit qëndror duhet të jetë i sigurtë dhe i enkriptuar me TSL/SSL nëpërmjet protokollit HTTPS. Sistemi duhet 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 auditimi. Kodi dhe modulet e sistemit duhet që të sigurojnë një versionim dhe historik të ndryshimeve që do të bëhen në sistem. Aksesimi në sistem duhet të realizohet nga përdoruesit e jashtëm apo të brendshëm përmes autentifikimit 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.

5.1.9 Moduli i fiskalizimit të faturave

Pjesë e programit që duhet të implementohet duhet të jetë edhe komponenti i faturimit dhe fiskalizimit të faturave të shitjes, faturave të lëshuara nga blerësi dhe të transfertave apo faturave shoqeruese. I gjithë informacioni mbi faturat që do të fiskalizohen duhet të furnizohet direkt nga programi i shitblerjes, në bazë të veprimeve që regjistrohen nga përdoruesit. Komponenti që do të implementohet duhet të jetë i çertifikuar nga Drejtoria e Përgjithshme e Tatimeve dhe nga AKSHI, për ofrimin e shërbimit të fiskalizimit, bazuar në ligjin nr. 87/2019, datë 18.12.2019, "Për faturën dhe sistemin e monitorimit të qarkullimit", dhe të gjithë aktet normative reference të tij.

Komponentet e software të fiskalizimit që do të përdoren nga KESH, për aktivitetin e shitblerjes së energjisë do të jenë ato të përmendura më poshtë, bazuar vetëm në fiskalizimin e faturave pa para në dorë:

1. Fatura e Blerjes
 - a. Në rast të faturës së blerjes nga furnitorë vendas, sistemi duhet të lejojë mundësinë e regjistrimit manual të faturës së blerjes me informacionin e marrë nga platforma qëndrore e Administratës Tatimore
 - b. Në rast të faturës së blerjes nga furnitorë jashtë vendit, sistemi duhet të ofrojë mundësinë e regjistrimit të faturës së blerjes dhe fiskalizimin e saj në formën e

faturës së lëshuar nga blerësi (autofature), së bashku edhe me regjistrimin e faturës doganore të fiskalizuar.

2. Faturat e shitjes, qoftë në rastet e shitjeve brenda vendit, po ashtu edhe në ato jashtë vendit, sistemi duhet të ofrojë fiskalizimin e faturave të shitjes me të gjitha nivelet e TVSH së lejuar, si dhe në Eksport.
3. Faturat korigjuese, për të dy rastet më lart, sistemi do të mundësojë fiskalizimin e faturave të kthimit, të cilat gjithashtu duhet të fiskalizohen.
4. Faturat shoqëruese, duhet të jenë gjithashtu një nga dokumentet që duhet të fiskalizohet nga ky komponent. Transfertat jo vetëm në rastin e transferimit të brëndshëm në pronësinë e KESH sha, por edhe në rastin e transferimit me ndryshim pronësie, për ruajtjen e energjisë. E gjithë veprimtaria financiare e sistemit duhet të zhvillohet në KESH me fillimin e projektit.

Sistemi duhet të ofrojë një ambient të dedikuar për regjistrimin e të gjithë pagesave të realizuara me banke, për aktivitetin e shitblerjes së energjisë. Sistemi duhet të mundësojë regjistrimin manualisht të të gjithë informacionit të nevojshëm, numrat e llogarisë hyrëse/dalëse, por edhe lidhjen me faturat e blerjes apo të shitjes që do të jenë paraprakisht të regjistruara në sistem.

Të gjithë veprimet e regjistruara duhet të kenë mundësinë të lidhen domosdoshmërisht me një dokument referencë, në mënyrë që të ndiqet historiku i pagesave dhe debitorëve në blerje dhe në shitje. Në bazë të informacionit që do të regjistrohet në sistem, duhet të jepet mundësia e filtrimit dhe marrjes së informacionit të kërkuar në formën e raporteve statistikore.

Moduli i fiskalizimit dhe pagesave duhet të vendoset në dispozicion për 6 punonjës, ku 3 prej të cilëve duhet të kenë akses të pakufizuar në këtë modul, dhe 3 të tjerë për të hedhur të dhëna apo për të parë raporte.

Sistemi mbi të cilin duhet të implementohen këto funksionalitete duhet të ketë mundësinë e zgjerimit të mëtejshëm

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 të suportojë standartet web të programimit CSS 3, HTML 5, dhe të jetë kompatibël me të gjithë shfletuesit (browsers). Front end duhet të jetë në gjendje të marrë të dhëna nga backend duke konsumuar webserviset REST. Duhet të jetë në gjendje të menaxhoje tokenat e sigurisë si dhe të menaxhojë refresh token për çdo përdorues. Sistemi front-end duhet të ndërtojë funksionalitetet e tij si komponente të cilët të kenë mundësi të

ripërdoren në çdo modul të sistemit. Sistemi frontend duhet të ndërtohet i tillë që të jetë totalisht i pavarur nga backend dhe të jetë funksional pa qen nevoja e ndërhyrjeve të mëtejshme nëse teknologjia e sistemit backend ndryshon. Sistemi duhet të shfaqë qartë përdoruesve errortet dhe mesazhet e suksesit. Frontend duhet gjithashtu të suportoje javascript.

6.2 Backend

Backend duhet të ndërtohet në një gjuhë programimi e cila suporton arkitekturën MVC. Të gjithë modulet e sistemit duhet të konceptohen si mikroservise dhe të dërgojnë të dhëna tek Frontend nëpërmjet web-serviseve REST. Backend duhet të mbrojë web-serviset REST nga përdorimi i pautorizuar duke kërkuar një security token për çdo të dhënë që është sensitive. Backend duhet të suportoje ndërveprimin me databazat RDBS. Backend duhet të jetë në gjendje të prodhojë dokumentacionin e nevojshëm për konsumimin e web-serviseve që nevojiten për funksionimin e sistemit.

6.3 Databaza

Databaza duhet të jetë e llojit RDBS dhe të jetë kompatibël me teknologjinë që do të përdoret për sistemin e backend. Duhet të jetë në gjendje të ruajë logs për të gjithë veprimet që ndodhin në databazë si dhe të gjithë query-t që ekzekutohen në të.

6.4 Arkitektura

Sistemi duhet të hostohet në një arkitekturë e cila suporton auto scaling (ritjen automatike të kapaciteteve bazuar në nevojat e sistemit). Autoscaling duhet të ndodhë në mënyrë automatike pa qenë nevoja e ndërhyrjes manuale. Databaza duhet të jetë e replikuar të paktën në një lokacion tjetër përveç lokacionit primar, dhe të garantojë sigurinë dhe konsistencën e të dhënave në çdo kohë. Infrastruktura e rrjetit në të cilën do të hostohet aplikacioni duhet të bëjë të mundur aksesimin e databazës vetëm nga serveri ku do të ruhet sistemi i backend. Aksesimi i databazës nuk duhet të jetë i mundur pa kriteret e sigurisë.

Infrastruktura duhet gjithashtu të suportoje adaptimin automatik. Çdo modul i ri apo përmirësim që kryhet në sistem duhet të ketë mundësinë të bëhet adaptim në mënyrë automatike nga infrastruktura pasi është bërë bashkimi me kodin burim aktual.

Arkitektura duhet të jetë në gjendje të mbrojë sistemin nga sulmet nga jashtë si dhe sulmet DDoS, dhe të përshtatet me standartet dhe të dhënat e sigurisë kibernetike.

6.5 Kodi burim

Kodi burimi ndërfaqes dhe jo praktikave apo të dhënave, duhet të ruhet në programin git (Gitlab, Github ose ekuivalente). Kodi burim duhet të ketë dy ndarje kryesore, main dhe development. Ku main do të përdoret për të mbajtur kodin i cili është në sistemin live dhe development do të përdoret për të mbajtur kodin i cili është në sistemin test. Teknologjia git duhet të bëjë të mundur që gjatë hedhjes së funksionaliteteve të reja në kodin burim të bëjë

kontrollet e nevojshme dhe teste automatike të kodit burim për të garantuar funksionalitetin e saktë të sistemit. Çdo funksionalitet i sistemit duhet të ndërtohet në një degë (branch) të veçante dhe të jetë kollaj i kthyeshëm nëse ndonjë problematikë e cila pengon funksionalitetin e sistemit.

6.6 Ndërveprimi me sistemet e tjera

Sistemi duhet të jetë në gjendje të ndërveprojë me sistemet e tjera si: Dogana, Tatimet apo sistemet bankare. Integrimi me sistemin e doganës duhet të bëhet në çastin e blerjes së energjisë elektrike. Integrimi me sistemin e tatimeve duhet të bëhet për deklarimin e faturave në sistemin e fiskalizimit ndërsa integrimi me sistemet bankare duhet të kryhet për të bërë të mundur vërtetimin automatik të pagesave. Këto integrimet do të zhvillohen sipas kërkesave të KESH sh.a. në diskutim me stafin e operatorit ekonomik që do të zhvillojë projektin.

6.7 Komponenti i fiskalizimit

Komponenti i fiskalizimit duhet të mundësojë integrimin me sistemin financiar të KESH sha. Integrimi duhet të mundësohet në një prej metodikave të mëposhteme:

1. Me anë dokumentave
2. Me anë të një Databaze të ndërmjetme
3. Me anë të shërbimeve web (web services)

Integrimi me sistemin financiar do të realizohet në dakordësi me KESH, në çdo moment që do të kërkohet gjatë kohezgjatjes së kësaj kontrate.

Integrimi do të jetë i njëanshëm, nga komponenti i fiskalizimit në sistemin financiar dhe dokumentet pjesë e këtij intergrimi do të jenë:

1. Faturat e Blerjes
2. Faturat e Shitjes
3. Faturat Korigjuese
4. Transaksionet Bankare
5. Transfertat e magazines (faturat shoqëruese)

6.8 Proceset e biznesit (Workflows) që programi duhet të ndjekë në funksionimin në tërësi të saj.

6.8.1 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.
 - Licencën 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 në proces likuidimi/falimentimi dhe kapitalet/asetet e tij nuk janë objekt i procedurave përbarimore;
 - 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 tregimit 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.
- Staf i KESH i cili merret me operimet tregtare, zbaton procedurat e brendshme për krijim e përdoruesit në sistem
- Sistemi dërgon njoftimet përkatëse sipas procedurave, nëpërmjet platformës në adresat elektronike të regjistruara të subjektit.
- Aprovimi i regjistrimit sipas kriterëve, referuar udhëzimeve ligjore duke e shoqëruar me dërgimin e kontratës tip.
- Aprovimi/mosaprovimi i regjistrimit shoqërohet me ruajtjen e komenteve dhe dokumentave bashkëngjitur.
- Aprovimi i regjistrimit shoqërohet me krijimin e llogarive në sistem.

Dokumentacioni i mësipërm duhet përditësuar nga shoqëritë sipas kërkesës së shoqërisë KESH sh.a., bazuar në rregullat e tregimit të energjisë elektrike nga KESH SH.A.

Sistemi elektronik duhet të mundësojë gjenerimin e njoftimit 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 regjistrim (kjo me qëllim që shoqëria e interesuar të riplotesojë zërin për të cilën sistemi elektronik i ka kthyer mbrapsh kërkesen për regjistrim).

6.8.2 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 kërkesës/ofertës sipas periudhave, fashave orare.
- Përcaktimi i lote-ve së kërkesës/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 shfaqje interaktive.

6.8.3 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.

6.9 Proceset e biznesit (Workflows) të tregtimit të energjisë elektrike të detajuara (shëmbull praktik)

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

Për shitje të energjisë elektrike. Kërkesa/ftesa për ofertë duhet të permbajë:

- Periudha/dita e shitjes së energjise elektrike e cila mund të jetë:
 - Periudhë në bllok
 - Periudhë e kushtëzuar (psh. Shitje energji elektrike 1-30 Prill 2019, por periudhën 1-10 Prill është e konfirmuar,ndërsa periudhat 11-20 dhe 21-30 Prill do rikonfirmohen respektivisht në datat 8 dhe 18 Prill 2019);
 - Periudhë me ditë të ndara;
- Profili i lëvrimit të energjisë elektrike nga ora 00: 00deri me 24:00 e cila mund të jetë:
 - Profile në bllok;
 - Profile me orë të ndara;

- Kapaciteti i shitjes së energjise elektrike e cila mund të jetë:
 - Kapacitetin maksimal i kërkuar për tu ofertuar/deri në... MW;
 - Kapacitet i kushtëzuar (Psh: shitje energji elektrike për periudhën 11-20 Prill 2019 në kapacitetin 50 MW,por KESH sh.a. i rezervon të drejtën vetës që më datë 8 Prill 2019 ku do të konfirmojë periudhën e shitjes të zgjidhe edhe kapacitetin e lëvrimit e cila mund të jetë nga 0 MW deri me 50 MW)
 - Kapacitet në bllok;
 - Kapacitet me orë të ndara;

- Sasia e energjisë elektrike mund të jetë:
 - Sasia maksimale e kërkuar për tu ofertuar/ deri në MWh;
 - Sasia e kushtëzuar (Psh: shitje energji elektrike për periudhën 11-20 Prill 2019 në kapacitetin 50 MW dhe sasinë 1200 MWh, por KESH sh.a. i rezervon të drejtën vetës që më datë 8 Prill 2019 ku do të konfirmojë periudhën e shitjes të zgjidhë edhe kapacitetin e lëvrimit e cila mund të jetë nga 0 MW deri më 50 MW respektivisht edhe sasia e energjisë elektrike)
 - Sasia në bllok;
 - Sasi me orë të ndara;

- Çmimi njësi i kërkuar për tu ofertuar mund të jetë:
 - Çmime/njësi në bllok;
 - Çmime/njësi orar;
 - Çmime/njësi dysheme;

- Pika e lëvrimit të energjisë elektrike e cila mund të jetë:
 - Brenda rrjetit të transmetimit
 - Në kufirin Shqipëri-Mali i Zi/Serbi/Greqi

- Siguruesi i kapacitetit mund të jetë:
 - Nga shoqëritë ofertuese;
 - Nga KESH sh.a.;
- Kriteri vlerësimit të ofertave është:
 - çmimi/njësi më i lartë deri në përmbushjen e sasisë së kërkuar për shitje të energjisë elektrike;
 - i kushtëzuar sipas çmimit dysheme të vendosur në ofertë;
 - Në rast kur kemi dy oferta me të njëjtin çmim do të ndiqet parimi i pari që vjen i pari shërbehet/pranohet;

- Kriteri financiar lidhur me mënyrën e pagesës mund të jetë:
 - Me parapagim;
 - Garanci financiare;
 - Mjete të tjera financiare;

➤ Afati i hapjes dhe e mbylles se mjetit elektronik të përdoruar nga KESH sh.a. për zhvillimin e procedurës së shit-blerjes se energjisë elektrike për ofertimin e shoqërive tregtare;

➤ Kushte te tjera të vendosura nga Autoriteti Kontraktues;

➤ Raporti i mbylles së procedurës/rezultatet e procedurës së shitjes duke publikuar çmimet dhe sasi të mesatare të ofertuara dhe ato të fituara.

➤ Ankimimi. Brenda afatit të përcaktuar në kërkesën/ftesën për ofertë shoqëritë kanë të drejtë që nëpërmjet sistemit elektronik të dërgojnë ankesën dhe sipas afateve të përcaktuara do ti kthehet përgjigje, duke mos penguar aktivitetin e tregtimit të energjisë elektrike.

Për blerje të energjisë elektrike. Kërkesa/ftesa për ofertë duhet të përmbajë:

➤ Periudha/dita e blerjes së energjisë elektrike e cila mund të jetë:

- Periudhë në bllok;
- Periudhë e kushtëzuar (psh. Blerje energji elektrike 1-30 Prill 2019, por periudhën 1-10 Prill është e konfirmuar, ndërsa periudhat 11-20 dhe 21-30 Prill do rikonfirmohen respektivisht në datat 8 dhe 18 Prill 2019);

- Periudhë me ditë të ndara;

➤ Profili i marrjes së energjisë elektrike nga ora 00:00 deri me 24:00 e cila mund të jetë:

- Profile në bllok;
- Profile me orë të ndara;

➤ Kapaciteti i blerjes se energjisë elektrike e cila mund të jetë:

- Kapacitetin maksimal i kërkuar për tu ofertuar/deri në... MW;
- Kapacitet i kushtëzuar (Psh: blerje energji elektrike për periudhën 11-20 Prill 2019 në kapacitetin 50 MW,por KESH sh.a. i rezervon të drejtën vetes që më datë 8 Prill 2019 ku do të konfirmojë periudhën e blerjes të zgjidhë edhe kapacitetin e lëvrimin e cila mund të jetë nga 0 MW deri me 50 MW)

- Kapacitet në bllok;
- Kapacitet me orë të ndara;

➤ Sasia e energjisë elektrike mund të jetë:

- Sasia maksimale e kërkuar për tu blerë/ deri në MWh;
- Sasia e kushtëzuar (Psh: blerje energji elektrike për periudhën 11-20 Prill 2019 në kapacitetin 50 MW dhe sasinë 1200 MWh, por KESH sh.a. i rezervon të drejtën vetes që më datë 8 Prill 2019 ku do të konfirmojë periudhën e blerjes të zgjidhë edhe kapacitetin e lëvrimin e cila mund të jetë nga 0 MW deri më 50 MW respektivisht edhe sasia e energjisë elektrike)

- Sasia në bllok;

- Sasi me orë të ndara;
- Çmimi njësi i kërkuar për tu ofertuar mund të jetë:
 - Çmime/njësi në bllok;
 - Çmime/njësi orar;
 - Çmime/njësi tavan;
- Pika e lëvrimin të energjisë elektrike e cile mund të jetë:
 - Brenda rrjetit të transmetimit
 - Në kufirin Shqipëri-Mali i Zi/Serbi/Greqi
- Siguruesi i kapacitetit mund të jetë:
 - Nga shoqërite ofertuese;
 - Nga KESH sh.a.;
- Kriteri vlerësimit të ofertave është:
 - çmimi/njësi më i ulët deri në përmbushjen e sasisë së kërkuar për blerje të energjisë elektrike;
 - i kushtëzuar sipas çmimit tavan të vendosur në ofertë;
 - Në rast kur kemi dy oferta me të njejtin çmimi do të ndiqet parimi i pari që vjen i pari shërbehet/pranohet;
- Kriteri financiar lidhur më mënyrën e pagesës mund të jetë:
 - Me parapagim;
 - Garanci financiare;
 - Mjete të jera financiare;
- Afati i hapjes dhe e mbylljes së mjetit elektronik të përdoruar nga KESH sh.a. për zhvillimin e procedurës së shit-blejjes së energjisë elektrike për ofertimin e shoqërive tregtare;
- Kushte të tjera të vendosura nga Autoriteti Kontraktues;
- Raporti i mbylljes së procedurës/rezultatet e procedurës së blerjes duke publikuar çmimet dhe sasi të mesatare të ofertuara dhe ato të fituara.

Ankimimi. Brenda afatit të përcaktuar në kërkesën/ftesën për ofertë shoqëritë kanë të drejtë që nëpërmjet sistemit elektronik të dërgojnë ankesën dhe sipas afateve të përcaktuara do të kthehet përgjigje, duke mos penguar aktivitetin e tregtimit të energjisë elektrike.

6.10 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 web në rrjet:

- Nëpërmjet një modaliteti nuhatës të portit SPAN/TAP
- Modaliteti i urës së brëndshme transparente të shtresës 2 (duhet të jetë mbështetje vendase dhe jo përmes integritit 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 integriti 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 disa paisje Server Menaxhimi për çdo pikë. Të gjithë serverët e menaxhimit duhet të jenë në gjendje të komandohen në mënyrë qendrore nga një "Sistem monitorimi dhe kontrolli". "Sistemi i monitorimit dhe Kontrollit" duhet të ofrojë kapacitetet teknike si më poshtë:

- Menaxhimi dhe administrimi i unifikuar për çdo pikë të implementuar në të gjithë serverat
- Krijimi, konfigurimi dhe shpërndarja e politikave në të gjithë serverat e menaxhimit
- Pika e vetme e aksesit në çdo Server Menaxhimi
- Monitorimi i të dhënave teknike të zgjidhjes
- Pamje e gjerë e sistemit të aktiviteteve të sigurisë

Zgjidhja duhet të jetë në gjendje të mbështesë rastin e përdorimit ku disa aplikacione web mbrohen në modalitetin "Transparent Reverse Proxy" (term teknik për rikthimin transparent të sistemeve proxy) dhe disa aplikacione web për t'u mbrojtur në nivelin e rrjetit Layer-2. Kjo duhet të mbështetet në zgjidhje nga prodhues të cilët meren me sigurinë kibernetike dhe jo nëpërmjet integritit të zgjidhjeve të tjera nga palët e treta.

Zgjidhja duhet të jetë e thjeshtë dhe intuitive për t'u 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 dhe arkitekturën e rrjetit gjatë vendosjes ose heqjes së sistemit nga rrjeti.

Zgjidhja duhet të vijë me opsionin për të zgjeruar fushën e mbrojtjes në renë kompjuterike, duhet gjithashtu të mundësojë mbrojtjen nga sulmet DDoS, mbrojtjen nga sulmet e tipit DNIS, të ofrojë sigurinë API, mbrojtjen e avancuar nga Bot (programe rrobotë që sulojnë faqet e internetit), mbrojtjen nga ana e klientit CDN dhe aftësinë e balancimit të ngarkesës me shtresa.

Kërkesat e Sigurisë për sistemin e mbrojtjes:

Zgjidhja duhet të mbështesë mekanizmin e mëposhtëm të verifikimit për të hyrë në ndërfaqjen e menaxhimit:

- Autentifikimi i integruar
- Autentifikimi Kerberos
- Autentifikimi dhe autorizimi i LDAP (active directory) me platformat e mëposhtme të Windows: 2008, 2008 R2, 2012 dhe 2012 R2.
- Autentifikimi RADIUS
- Autentifikimi i bazuar në kartën autentikuese

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:

- a. Periudha e përpjekjeve të dështuara të hyrjes (në minuta) në të cilën futja e një fjalëkalimi të pasaktë disa herë bllokun 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 të saj. Komunikimi ndërmjet komponentëve të zgjidhjes duhet të bëhet duke përdorur certifikata sigurie të mbështetura në standartin openssl 1.0.2

Kërkesat për mbrojtësin e aplikimit WAF

WAF- i cili do të ofrohet duhet të jetë lider në kuadrantin Gartner për paisjet “firewall” mbrojtësit e aplikacioneve në web të paktën për 7 vitet e fundit.

Zgjidhja duhet të mbështesë qasjen e modelit pozitiv të sigurisë. Një model sigurie pozitiv 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 tipet e njohura të sulmit.

Zgjidhja duhet të ofrojë një normë false-pozitive pothuajse zero duke përdorur politika të konfiguruar paraprakisht OOTB (Out Of The Box) që lejon që WAF të vendoset në modalitetin e bllokimit pa pasur nevojë që administratori të rinovojë politikat e sigurisë.

Zgjidhja duhet të jetë në gjendje të bllokojë transaksionet me përmbajtje që përputhet me tipet 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,
- Bllokimi i seancës TCP,
- Bllokimi i përdoruesit të aplikacionit, ose
- Bllokimi i adresës 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 web kur ajo vendoset në modalitetin e ruajtjes në rast të modalitetit të vendosjes së zbatimit aktiv.

Zgjidhja duhet të jetë në gjendje të mbrojë si aplikacionet në web HTTP ashtu edhe aplikimet web 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 web SSL që përdorin protokollet e shkëmbimit të çelësave Diffie-Hellman me pajisjen monitoruese të vendosur në modalitetin transparent të shtresës Layer2 (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. (Përfshijë 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 web
- Nënshkrimet e sulmit të protokollit HTTP
- Mbrojtje e personalizuar e shtresës së shërbimit në web
- Vlefshmëria e nënshkrimit të cookie-ve
- Mbrojtja e profilit në web
- Mbrojtja nga infektimet e webit (worms)
- Nënshkrimet e sulmit të aplikacionit në web
- Mbrojtje e personalizuar e shtresës së aplikacionit në web
- Vlefshmëria e protokollit OCSP
- Sfida CAPTCHA

Zgjidhja duhet të ketë një bazë të dhënash me minimalisht 6000+ tipe sulmesh 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 tipit të sulmit 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 tipet e sulmit. Zgjidhja duhet të mbështesë llojet e mëposhtme të përkufizimit të tipeve të sulmit 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 parametrat 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 web dhe njëkohësisht të mbrojë aplikacionet e webit 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 kërkohej 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/mësimin 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 web (skanuesit e aplikacioneve në internet) për të rregulluar praktikisht dobësitë e aplikacionit në web:

- Acunetix
- Beyond security
- Cenzic
- Denim group
- HP Fortify WebInspect
- IBM AppScan
- OBJEVES NT
- Quality
- Fast 7
- Trend Micro
- Veracode

- White hat

Zgjidhja duhet të adresojë Kriteret e Vlerësimit të Firewallit të Web-Application (WAFEC), siç përcaktohet nga Konsorciumi i Sigurisë së Aplikacioneve në Web (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:

- Malicious IP
- Anonymous

Raportimi

Zgjidhja duhet të ofrojë aftësi raportimi të (out-of-the-box) 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 (qëllim dashakeq), 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:

- Cookies
- Emrat e mësuar të hosteve
- Emrat e skedarëve me të dhëna sensitive
- Modelet e URL-ve të mësuar (adresa të faqeve web)
- URL-të e mësuar (adresat e faqeve web)
- Ndjekja e përdoruesve të aplikacionit në web

Zgjidhja duhet të ofrojë funksionalitet për të ndihmuar gjetjen e provave të detajuara

Zgjidhja duhet të ketë aftësinë për t'u integruar me një model "Attack Analytics". Modeli "Attack Analytic" duhet të fshijë të gjitha sinjalizimet e sigurisë dhe të ndihmojë administratorët e sigurisë të verifikojnë sinjalizimet më të rëndësishme të sigurisë.

Modeli i "Attack 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 (out of the box) që i mundëson administratorit të krijojë shabllone raportesh të personalizuar bazuar në raportet ekzistuese jashtë kutisë.

Zgjidhja duhet të mbështesë redaktimin dhe krijimin e politikave të sigurisë që drejtohet nga një UI (ndërfaqje) 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 differencim ekzekutues.

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

7 Logjistika dhe Koha

7.1 Vendndodhja

- Sistemi duhet të instalohet në një infrastrukturë hardware të siguar nga KESH. Për të mundësuar vënien në dispozicion të parametrave të nevojshëm teknik, Kontraktori duhet të qartësojë në kërshen teknike nevojat nga pikpamja e burimeve hardware për të implementuar platformen. Çdo licensë software e nevojshme në kuader të platformës duhet të sigurohet nga Kontraktori.
- Kontraktori do të jetë përgjegjës për vazhdueshmërinë e sistemit në 24x7 dhe të njoftojë paraprakisht për ndërhyrje apo raste difektesh.
- Sistemi duhet të ofrojë ruajtje të informacionit arshivor deri në 2 vite.

7.2 Afati kohor për zbatimin e projektit

Afati kohor- për zbatimin e këtij shërbimi do të jetë 60 ditë, nisur nga data e nënshkrimit të kontratës.

Mirëmbajtja- do të jetë 1 (një) vit nga momenti i lëshimit të Çertifikatës 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 pa TVSH
1	Dizenjimi dhe implementimi i Programit të Menaxhimit të Aktivitetit të Operimeve Tregtare	1	Copë	

2	Sistemi i sigurisë	1	Copë	
3	Trajnim mirëmbajtje	30	Orë	
4	Mirëmbajtje e sistemit	12	Muaj	
	TOTALI PA TVSH			
	TVSH			
	TOTALI ME TVSH (LEKË)			

9 Zbatimi i projektit dhe shërbimet

9.1 Menaxhimi i Projektit

1. Kontraktori 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. Kontraktori duhet të sigurojë një plan zbatimi të projektit me piketa të qarta.

9.2 TRAJNIMI

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

9.3 Pranimi i sistemit

- Kontraktori duhet të kryejë testet e pranimit të sitit të sistemit pas implementimit të tij.
- Kontraktori i duhet të demonstrojë që sistemi është dorëzuar dhe instaluar në përputhje me specifikimet dhe kërkesat teknike.
- Kontraktori 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 ndjekës së kontratës
- Një çertifikatë duhet të lëshohet pas përfundimit dhe të suksesshëm të pranimit.

10 PËRGJIGJA DHE SHKALLËZIMI I SHËRBIMIT

Në tabelën e mëposhtme përcaktohet kategorizimi i seriozitetit të problemeve të lindura në platformen software të Menaxhimit të Aktivitetit të Operimeve Tregtare, 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		
<u>Nuk ka një mënyrë alternative</u> të përkohshme dhe të pranueshme për zgjidhjen e problemit	<u>Ka pjesërisht një mënyrë alternative</u> të përkohshme dhe të pranueshme për zgjidhjen e problemit.	<u>Ka një mënyrë alternative</u> 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.