Akronime:

Shkurtimi	**Përkufizimi**
APD	Autoriteti Portual Durres
SIEM	Security Information and Event Management
UEBA	User and Entity Behavior Analytics
SOAR	Security Orchestration, Automation and Response
EDR	Endpoint Detection and Response
VSCAN	Vulnerability Scanning
FV	Furnizim Vendosje

Hyrje

Për të realizuar qëllimet themelore të saj, APD kryen një sërë veprimtarish, të cilat janë të lidhura ngushtë me interesat e saj, me interesat kombëtarë dhe me interesat e subjekteve ose të personave juridikë që kanë marrëdhënie me të.

Është i domosdoshëm monitorimi dhe mbrojtja e pjesëve të ndryshme të sistemeve informatike për te cilat APD është përgjegjëse, në varësi të vëllimit, të vlerës financiare, të ndjeshmërisë dhe të rrezikshmërisë që ato kanë. Në veçanti duhen mbrojtur në nivel sa më lartë burimet e informacionit, për të garantuar saktësinë dhe disponueshmërinë e tij në kohën e duhur.

APD ka investuar në drejtim të zhvillimit të teknologjisë së informacionit dhe pretendimet e tij për shkëmbimin dhe thellimin e këtij procesi janë gjithnjë në rritje. Administrimi i matur i aseteve dikton nevojën e mbrojtjes së këtij investimi nga kërcënimet e mundshme. Për më tepër, me mbështetjen gjithnjë e më të madhe që po i japin sistemet e informacionit aktivitetit të institucioneve te ndryshme, siguria e informacionit në këto sisteme është gjithmonë dhe më e rëndësishme si për institucionin ashtu edhe për institucionet te cilat mbështesin kapacitete te tyre informatike ne të.

Objektivat më të rëndësishëm në lidhje me sigurinë e informacioneve janë garantimi dhe mbrojtja e integritetit, e disponueshmërisë dhe e konfidencialitetit. Niveli i përshtatshëm i mbrojtjes mund të arrihet vetëm duke garantuar që të gjitha aspektet e sigurisë së informacionit mbulohen në mënyrë të vazhdueshme dhe metodike.

Informacioni i APD ekziston në një ekosistem kompleks, i implementuar me një mori teknologjish të cilat prodhojnë, ruajnë, përpunojnë, shpërndajnë dhe transmetojnë informacion nëpërmjet rrjeteve informatike, mjeteve dhe pajisjeve të transmetimit në përdorim ose në pronësi të saj. Është e domosdoshme mbrojtja e sistemeve informatike për të cilat APD është përgjegjëse në varësi të vëllimit, të vlerës financiare, të ndjeshmërisë dhe të rrezikshmërisë që ato kanë. Mbrojtja në fjalë duhet të plotësojë tre parimet e sigurisë së informacionit: disponueshmërinë, integritetin dhe konfidencialitetin.

APD po zhvendoset nga monitorimi dhe mbrojtja e një perimetri tradicional të rrjetit (mbajtja e aseteve të biznesit në një vend të sigurt) në strategji më efektive duke menduar mbrojtjen e përdoruesit, të dhënat dhe asetet e biznesit. Ky transformim sjell ndryshime të teknologjisë dhe kërkesë për të mbrojtur në nivel sa më lartë burimet e informacionit, për të garantuar saktësinë dhe disponueshmërinë e tij në kohën e duhur.

Niveli i përshtatshëm i mbrojtjes mund të arrihet vetëm duke garantuar që të gjitha aspektet e sigurisë së informacionit mbulohen në mënyrë të vazhdueshme dhe metodike.

Në vijim të aplikimit të strategjive APD synon zbatimin e Politikes së Sigurisë me anë të zgjidhjeve inteligjente bashkohore. Në fokus do të jete përdoruesi dhe infrastruktura në teresi, duke implementuar të gjitha fazat e monitorimit, menaxhimit proaktiv të sigurisë kibernetike. Zgjidhjet e lart-përmendura duhet të mbeshtesin, por jo të limitohen në arritjen e implementimit të suksesshem të fazave: Mbrojtja, Parashikimi, Hulumtimi, Zbulimi dhe Reagimi.

Qëllimi

Menaxhimi proaktiv i sigurisë kibernetike synon minimizimin e riskut të sigurisë kibernetike duke zbatuar Politikën e Sigurisë së APD përmes vleresimit të infrastruktures dhe përmiresimit të cdo pike të dobët të zbuluar gjatë procesit të pafundëm me fazat si mëposhtë:

Figure 1-Menaxhimi Proaktiv i Sigurisë Kibernetike

Modulet e propozuara në vazhdimësi te këtij dokumentacioni, synojnë të përmbushin këtë qasje në mënyrë të vazhdueshme dhe në kohë reale, për të avancuar nivelin e sigurisë në APD.

Implementimi

Qëllimi i këtij projekti është përmirësimi i sigurisë ne mënyrë të vazhdueshme. Për të arritur këtë do të kryhet fillimisht vleresimi i nivelit të sigurisë aktuale. Kjo do arrihet përmes aplikimit të platformë e automatizuar SIEM, sistemin EDR si dhe VSCAN. Këto platforma do të kryejnë monitorim proaktiv 24/7 për të krijuar një sistem masash të cilat do të jenë rregullisht duke vepruar. Në rast se lind nevoja për të vlerësuar gjendjen e sigurisë pas ndryshimeve në infrastrukturë ose konfigurime të tjera të diktuara nga procesest e punës së APD, kjo zgjidhje duhet të bëhet “run” me periodicitet minimalisht një mujor dhe duhet të raportojë dobesitë dhe rekomandimet për mitigimin e këtyre të fundit.

Hapi parë i implementimit të këtij projekti është qendërzimi i logeve në një platformë SIEM. Vetë aktiviteti i APD dhe tërësia e infrastrukturës së rrjetit informatik që ajo përfshin, dikton nevojën e qendërzimit të logeve, për të monitoruar të gjithe infrastrukturën duke prioritarizuar asetet sipas rëndesise së tyre dhe aktivitetit. Eshte shume e rëndësishme që kjo zgjidhje të intergrojë dhe sigurojë korrelimin e logeve për këto asete si me poshte: Firewall, Web Servera, EDR, Mail Servera, Databaze, Endpoint, Active Directory, paisje rrjeti, servera, sisteme prodhimi, sisteme mbeshtetese etj.

Gjithashtu, impelementimi i kësaj zgjidhje do mundesojë shtimin e logeve të aseteve në rritje të APD sipas kërkesës. Sipas nevojes duhet të konfigurohen alerte dhe njoftime për grupin tonë të sigurisë, për rreziqe të vërejtura në loge në kohë reale. Kjo do i mundesojë ekipit të APD të jetë i përditesuar dhe të rrisë nivelin e sigurisë në të gjithë infrastukturën dhe të ketë mundesinë të korrelojë loge nga shumë paisje për të identifikuar asete të mundëshme të kompromentuar.

Pjesë shumë e rëndësishme e këtij projeki është mbrojtja e aseteve të kompansisë dhe nga përdorues të mundshem keqdashës të brendshëm. Kjo do arrihet përmes zgjidhjes së Analizës së Sjelljes së Përdoruesve (User and Entity Behavior Analytics - UEBA). Kjo zgjidhje fokusohet në atë cfarë përdoruesit kryejnë duke vëne në dukje sjellje që ngjasojnë me ato të përdoruesve keqbërës. Kjo zgjidhje do lejojë grupin e sigurisë të fokusohet në identitetin dixhital të përdoruesve dhe sjelljes së tyre aktuale, pa humbur fokusin e infrastrukturës në tërësi.

Një tjetër pjesë e rëndësishme e këtij projekti është edhe integrimi i SOAR me SIEM. SOAR ndihmon në përmirësimin e efektivitetit të sistemeve SIEM duke orkestruar dhe automatizuar proceset e sigurisë. Ndërkohë që SIEM mbledh dhe analizon të dhënat e sigurisë nga burime të ndryshme, SOAR përdor këto të dhëna për të ndihmuar në reagimin e shpejtë ndaj incidenteve. SOAR lejon automatizimin e përgjigjeve ndaj kërcënimeve, duke reduktuar nevojën për ndërhyrje manuale dhe duke përshpejtuar procesin e reagimit. Kjo zgjidhje do të përfshijë ekzekutimin e skenarëve të paracaktuar për menaxhimin e incidenteve dhe kryerjen e hetimeve të automatizuara.

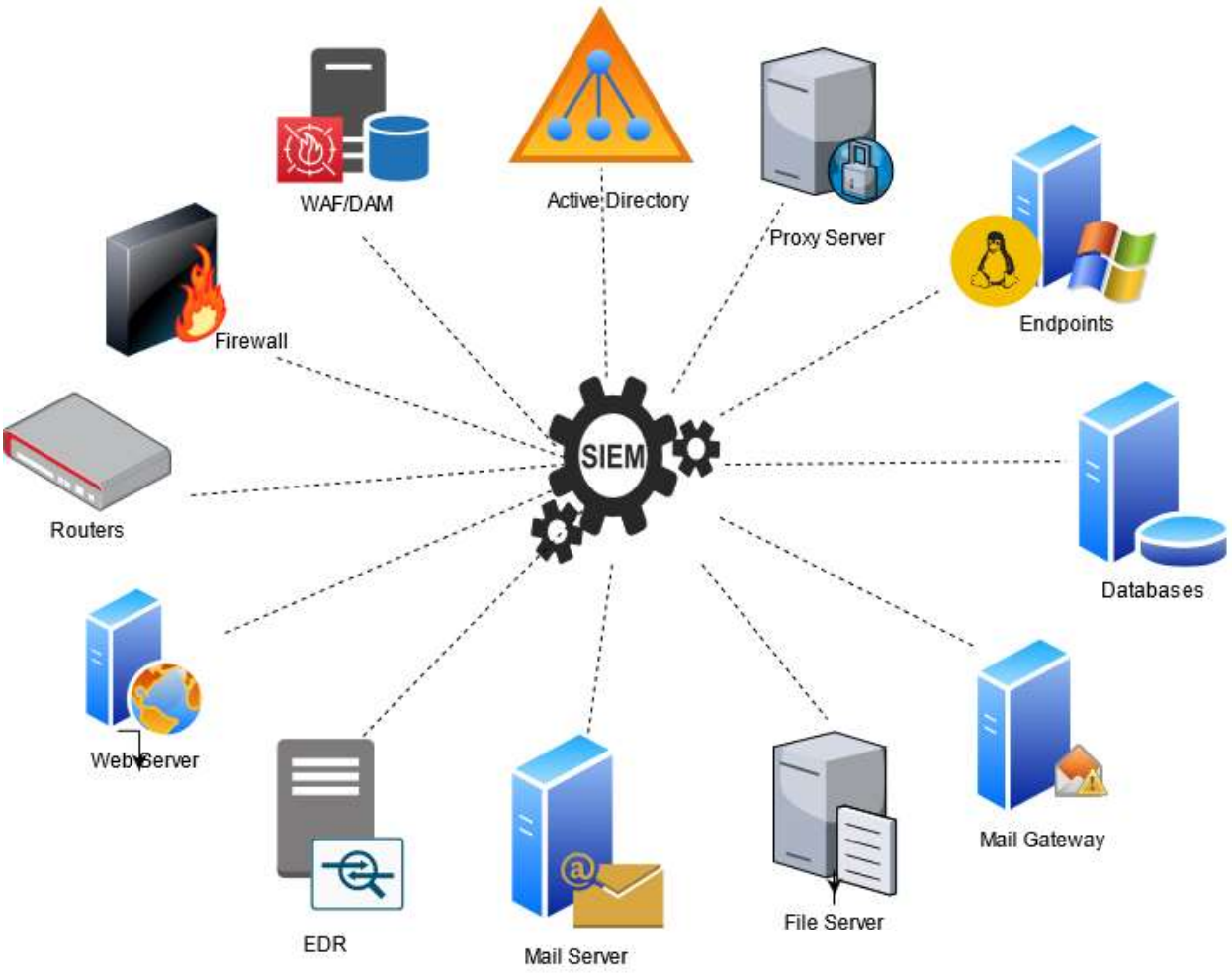

Figure 2-SIEM

Mbrojtjet tradicionale antivirus dhe antispam tashme quhen te vjeteruara nga mënyra që ato ofrojnë mbrojtjen nga sulmet kibernetike në botën moderne. Sulmet kibernetike moderne përdorin vektorë dhe teknika të shumta të sulmit që përtej mbrojtjes tradicionale të paketës antivirus/antispam që funksiononin në të shkuarën. Sulmet moderne kanë të bëjnë me shfrytëzimin e Mbrojtjes së Kërcënimit të Avancuar (ATP). Përfitimi kryesor i ofruar nga zgjidhjet e përparuara të mbrojtjes së kërcënimeve është aftësia për të parandaluar, zbuluar dhe reaguar ndaj sulmeve të reja dhe të sofistikuara që janë krijuar për të shmangur zgjidhjet tradicionale të sigurisë të tilla si antivirus, antispam, firewalls dhe IPS / IDS. Sulmet vazhdojnë të bëhen gjithnjë e më të shënjestruara dhe persistente, dhe zgjidhjet ATP marrin një qasje proaktive ndaj sigurisë duke identifikuar dhe eleminuar kërcënimet e përparuara përpara se të dhënat të kompromentohen.

Gjithashtu pjesë e projektit do të jetë implementimi i VSCAN, i cili është një mjet skanimi për të zbuluar dobësitë në sistemet kompjuterike. VSCAN kryen skanime të rrjetit dhe hosteve për të identifikuar dobësitë e sigurisë që mund të shfrytëzohen nga sulmuesit. Disa nga funksionet kryesore jane:

- **Skanimi i Dobësive:** Identifikon dobësitë në sisteme operative, aplikacione dhe pajisje rrjeti.

- **Auditimi i Konfigurimeve:** Kontrollon konfigurimet për të siguruar që ato janë në përputhje me politikat e sigurisë.

- **Zbulimi i Malware:** Skanon për prezencën e malware dhe softuerëve të dëmshëm.

- **Raportimi dhe Analiza:** Gjeneron raporte të detajuara për dobësitë e zbuluara dhe rekomandon masa për korrigjimin e tyre.

- **Skanimi i gjithanshem dhe Autentik:** Kryen skanime nga distanca dhe përmes autentikimit për të marrë informacione më të hollësishme.

Specifikimet Teknike:

1. F.V Sistemi Software i menaxhimit te logeve dhe eventeve te sigurise (SIEM + UEBA + SOAR)

Për të arritur konsistencë të aplikimit të politikës së sigurisë së APD në të gjithë kompaninë është e rëndesishme centralizimi i logeve që janë produkt i të gjithë asseteve të APD qofshin ato lokale dhe remote. Zgjidhja duhet të ofrojë mbledhjen dhe procesimin e logeve pothuajse në kohë reale nga burime të ndryshme, si sistemet operative, firewall, paisjet e sigurisë, ne varesi te messages per second (MPS) . Ky modul shërben në aplikimin e të gjithë fazave pjesë e menaxhimit proaktiv të Sigurisë Kibernetike. Përmes qendërzimit të logeve nga të gjitha asetet e interesit, kjo zgjidhje ofron mbrojtje përmes alerteve në kohë reale, hulumtim përmes përshkrimit në kohë të eventeve, si dhe zbulim përmes kërkimit të parametrave me interes.

1.1 Karakteristika te pergjithshme

- Zgjidhja duhet të lejojë regjistrim të pakufizuar logesh, ku licenca ne asnje menyre nuk duhet te nderpresi mbledhjen e logeve edhe ne rast tejkalimi te saj.
- Licensimi i paisjes duhet te kryhet me pajtim 1 vjecar duke përfshirë suport nga prodhuesi.
- Modeli i licensimit të zgjidhjes duhet të sigurojë strukturë të parashikueshme të kostos, pavarësisht nga rritja e vëllimit të të dhënave në infrastrukturë.
- Zgjidhja duhet te jete e zhvilluar dhe e integruar plotesisht “on premise”, ne premisat e autoritetit kontraktor.
- Zgjidhja duhet të jetë e aftë të mbledhë loge nga burime të ndryshme, të tilla si sistemet operative, firewall, pajisjet e sigurisë dhe shumë sistemeve apo aplikacioneve të tjera si: Authentication dhe Access Management, Infrastruktura e levrimit te Aplikimeve, Database Activity Monitoring, Web Application Firewalling, Email Security dhe Management, Endpoint Security (EPP/EDR), Information Technology dhe Service Management (ITSM), IT Management dhe Monitoring, Privileged Access Management, VSCAN systems, Utilites/Others: Web Security dhe Monitoring.

- Zgjidhja duhet të lejojë regjistrim të pakufizuar logesh, ku licenca ne asnje menyre nuk duhet te nderpresi mbledhjen e logeve edhe ne rast tejkalimi te saj.
- Zgjidhja duhet te suportoje paisjet e fundit si dhe paisje legacy, duke ofruar te njeten cilesi sherbimesh.
- Zgjidhja duhet të mundësojë kërkim të plotë të tekstit me përformancë të lartë në të gjithë loget e mbledhura.
- Zgjidhja duhet të përpunojë të gjitha të dhënat pothuajse në kohë reale.
- Zgjidhja duhet te jete plotësisht e integruar në të gjitha shtresat, përfshirë mbledhjen e të dhënave, përpunimin, analitikën, indeksimin dhe automatizimin dhe orkestrimin e sigurisë.
- Zgjidhja duhet te ofroje UEBA dhe te perdore autentikim e userave dhe loget e akseseve ne te dhena, duke pasuruar (enrich) me loge te mbledhura nga endpoint dhe te dhena rrjeti, per te suportuar identifikimin, vertetimin dhe prioritizimin e alarmeve.
- Zgjidhja UEBA duhet te ofroje shikueshmëri të thellë në aktivitetin e përdoruesit, duke ndihmuar në zbulimin e kërcënimeve të brendshme, llogarive të komprometuara, abuzim të privilegjuar të llogarisë dhe kërcënime të tjera të bazuara në përdorues.
- Zgjidhja duhet te përdore informacionin e menaxhimit të identitetit dhe aksesit, kontekstin e brendshëm dhe të jashtëm dhe të dhënat e makinerisë të mbledhura nga e gjithë kompania.
- Zgjidhja duhet te ofroje aftesi SOAR (Security Orchestartion Automation and Response) te integruar, qe ti ofroje analisteve te APD mundesi te hetojne dhe neutralizojne kercenimet.
- Zgjidhja duhet te aplikoje tekniken e machine-lerning per te detektuar anomali pa njohuri te meparshme te sulmeve, tekniken bazuar ne skenare per te detektuar modele te njohura aktivitetetesh kercenuese, si dhe kombinimin e ketyre dy teknikave.
- Zgjidhja duhet te jete e zhvilluar si nje zgjidhje e integruar plotesisht “on premise”, ne premisat e autoritetit kontraktor.
- Zgjidhja SIEM duhet te jete e disponueshme si një pajisje ose si softuer për vendosjen në infrastrukturen tone ose në të gjithë hipervizitorët kryesorë.

- Zgjidhja duhet te ofroje mbledhjen e te dhenave lokale, agent-based ose remote, si dhe pa agjente.
- Zgjidhja duhet ne monitoroje ne menyre te pavarur aktivitetin qe ndodh ne host ku agjenti eshte i instaluar, duke gjeneruar te dhena ne kohe reale. Keto aktivitete perfshijne modifikimin e fileve, applikacionet active dhe komunikime ne rrjet.
- Zgjidhja duhet te ofroje ndarje te pergjegjesive administrative granulare.
- Zgjdhja duhet te suportoje burime te dhenash komerciale, protokollet standarte, API te paleve te treta etj.
- Zgjidhja duhet te suportoje zgjerimin horizontal dhe vertikal.
- Zgjidhja duhet te suportoje marrjen e logeve nga Windows 7/8/8.1/10/11, Server 2008/2008 R2/2012/2012 R2/2016/2019/2022, AIX 7.1, Debian 7/8, Oracle Linux 5.10/6.4/7, Solaris x86 10/11, Solaris Sparc sun4v 9/10/11, Red Hat 5/6/7, CentOS 5/6/7/8/9, SUSE 11/12/13, Ubuntu 12/14/16/18/18.04 LTS.
- Zgjidhja duhet të lejojë integrimin me Active Directory duke përfshire dhe pasurimin e te dhenave dhe grupimet e roleve.
- Integrimi me Active Directory duhet te ofroje kerkimin, raportimin, alarmet si dhe trendet ne sjellje bazuar ne grupet e AD.
- Zgjidhja duhet te supportoje SSL (secure sockets layer) per transportin e te dhenave.
- Integrimi me AD duhet te suportoje marrjen e te dhenave sa i perket validimit te kredencialeve locale dhe remote, autentifikimin interaktiv dhe te automatizuar, modifikimin e permissions te userit, hosteve dhe grupeve, si dhe ndryshimin e anetaresise ne grupe, per te suportuar funksionalitet UEBA.
- Zgjidhja duhet te ofroje një pamje të shpejtë të gjendjes së sistemit te tij duke përfshirë detaje të tilla si statusi i hostit, performanca e hostit, përdorimi i bazës së të dhënave, metrikat e përpunuesit të të dhënave dhe statistikat per volumin e logeve.
- Zgjidhja duhet te perfshije raporte te thjeshtezuara bazuar ne compliance si: SOX, SOX-COSO, PCI-DSS, NRC, NIST 800-53, NERC CIP, NEI, ISO-27001, HIPAA, Healthcare Security Compliance, GPG-13, FISMA, DoDI 8500.2, GDPR, MAS-TRMG, NIST Cyber Security Framework, BSI: IT-Grundschutz, 201 CMR 17.
- Zgjidhja duhet ofroje analitik sigurie te automatizuar per të detektuar threats te avancuar.

APD për implementimin e zgjidhjes SIEM + UEBA + SOAR do ofrojë kapacitetet e meposhtme virtuale per procesim (computing) dhe ruajte informacioni (Storage), .

Specifikimet Teknike te Virtual Appliance:

- Vcpu: 24 threads
- Memory: 128 GB
- Storage:
  - 3 TB hapësirë storage SSD
  - 30 TB hapësirë storage HDD

SHENIM:

Në rast se zgjidhjes së ofruar nga Operatori Ekonomik i nevojiten më shumë resurse ato duhen të merren përsipër nga vetë Operatori Ekonomik gjatë implementimit të zgjidhjes.

1.2 Licensimi

- Zgjidhja të jetë e licensuar minimualisht për 300 perdorues (users).
- Ne rast të tejkalimit të perdorimit mbi numrin e përdoruresve (users) të licensuar zgjidhja duhet të vazhdojë të funksionojë.
- Licensimi të jetë i pajtueshëm për një periudhe një (1) vjecare duke përfshirë suport nga prodhuesi.

1.3 Suporti dhe implementimi

- Ne zgjidhje të përfshihet suport për update të software për 1 vit me nivel kontrate sherbimi 24x7 në cdo dite të vitit nga Operator Ekonomik.
- Instalimi, konfigurimi dhe testimi duhet të bëhet nga ofertuesi, zgjidhja duhet të dorëzohet e plotë (Turnkey Solution).
- Zgjidhja të ofroje mundësi për komunikim me chat, web, telefon dhe email me qendrën, suportin e autorizuar të vet prodhuesit të pajisjes.

- Zgjidhja të përfshije akses direkt në qendrën e autorizuar për hapje dhe ndjekje te case, informacion në forume, njoftime të reja rreth zgjidhjes, dokumenta online.
    - ***Faza 1: Planifikimi Fillestar***
        - Planifikimi i rrjetit dhe infastrukturës për integrimin e zgjidhjes
    - ***Faza 2: Instalimi i zgjidhjes***
        - Përgatitja e fizike e zgjidhjes duke përfshire kërkesat e sistemit (IP, Sistem Operimi etj.)
    - ***Instalimi/Inicializimi i zgjidhjes***
        - Licensimi i zgjidhjes
        - Testimi i rrjedhjës së trafikut dhe ndërlidhjes me infrastrukturën në tërësi
    - ***Faza 3: Konfigurimi i zgjidhjes***
        - Konfigurimi i sistemit sipas kërkesave fillestare të zgjidhjes
        - Konfigurimi i skenareve të testimit
        - Konfigurimi i target-eve (endpoint ose server sipas nevojës)
        - Inicializimi i zgjidhjes dhe marrja e logs te gjeneruara nga sistemet e instaluara.
    - ***Faza 4: Raportimi i dobësive***
        - Paraqitja e veprimtarive dhe gjetjeve të kryera
        - Përgatitje e politikave të sigurisë dhe aplikimi i tyre
        - Gjenerimi i personalizuar i raportit të dobësive të zbuluara
    - ***Faza 5: Trajnimi i personelit të departamentit të sigurise***
        - Operatori Ekonomik duhet të demonstroj, trajnoj dhe të instruktoj stafin e departamentit te Sigurisë te APD mbi perdorimin e sistemit SIEM + UEBA+ SOAR, si dhe tu demonstroj atyre skenare te ndryshme investigimi.
        - Gjenerimi dhe dorëzimi i raportit te implentimit të zgjidhjes

2. F.V Sistemi Software i detekimit dhe mitigimit te sulmeve kibernetike te avancuara ne endpoint (EDR)

Përpos infrastrukturës, perdoruesit jane nyja kyce e sistemevete informacionit të APD. Të qënit proaktiv me sigurinë kibernetike, është kritike monitorimi i rrjetit dhe përdoruesve 24/7. Ky modul software fokusohet në zbulimin dhe reagimin e menjëhershem ndaj risqeve në cdo endpoint të kompanisë, qofshin ata lokale ose remote. Zgjidhja e propozuar duhet të ekspozojë sulmet avancuara përfshirë dhe kërcenimet më inteligjencë globale, duke minimizuar njoftimet positive të rreme dhe të ndihmojë në sigurimin e niveleve të larta të produktivitetit për ekipin tonë të sigurisë. Zgjidhja në fjalë duhet të ofrojë reagim në kohë reale, të identifikojë dhe kontrollojë të gjithë endpointet e ndikuara nga një sulm i mundshëm , ndërkohë që përshkruan metodat e sulmit bazuar në taktikat dhe teknikat standarde. Eshtë e rëndesishme që software të ofroje vizibilitet të gjendjes së sistemit në tërësi, përfshire gjendjen specifike për secilen paisje fundore (endpoint) ne infrastrukturë.

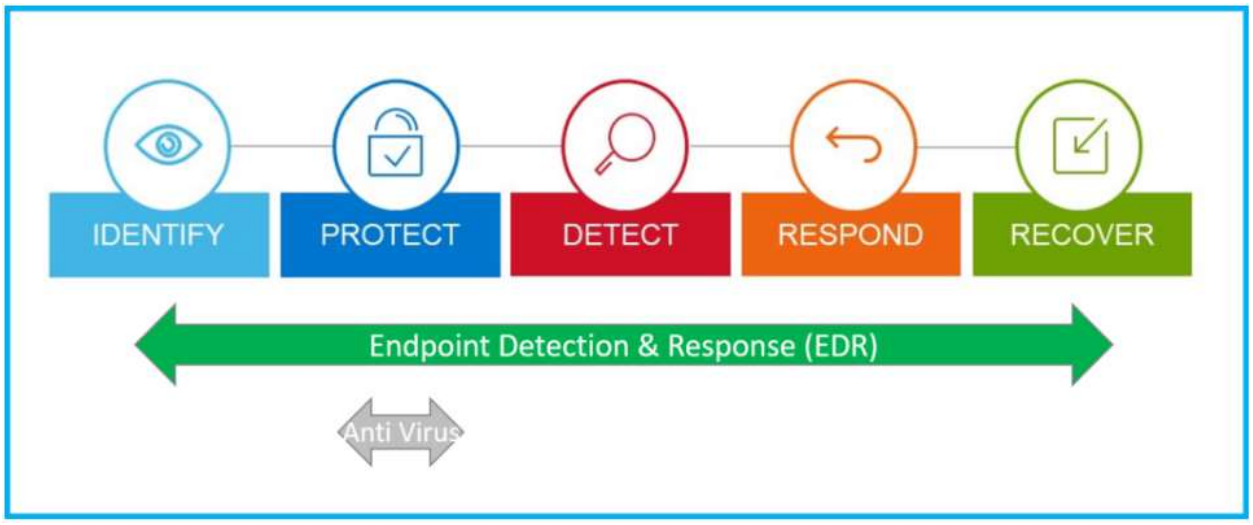

Figure 3-Endpoint Detection & Response (EDR)

2.1 Të përgjithshme

- Zgjidhja duhet të ofrojë mundësinë e përdorimit të sistemit për të paktën 300 përdorues për një periudhë një vjeçare.
- Zgjidhja duhet te jete e zhvilluar si nje zgjidhje e integruar plotesisht “on premise”, ne premisat e autoritetit kontraktor.

- Të gjitha modulet duhet të ofrohen nga i njëjti prodhues në mënyrë që të vërtetohet që janë të pajtueshëm dhe të funksionojnë siç duhet.
- Parandalimi i kërcënimeve të njohura dhe të panjohura.
- Zgjidhja duhet të dedektoje dhe zbuloje sulmet të cilat nuk përmbajnë file por operojnë vetëm në memorie.
- Zgjidhja duhet të skanoje file script ne sistemet e operimit Windows\Linux\Mac.
- Zgjidhja duhet të jete ne gjendje të analizoje dhe bllokoje ndërhyrjet që bazohen ne framework .NET së bashku me kontentet e shkarkuara nga scriptet pjese e aktivitetit dashakeqes.
- Zgjidhja duhet të zbuloje dhe bllokoje malware e njohura/panjohura, bazuar ne modelet e machine learning, inteligjences artificiale dhe analizën e mënyrës se sjelljes se sulmuesit.
- Zgjidhja duhet të ketë një shkallë të ulët false-pozitive - një rezultat të ulët ose shumë të ulët në testet krahasuese AV.
- Zgjidhja duhet të ofroje mekanizma parandaluese për bllokimin e aktivitetit dashakeqes përpara ekzekutimit të tij, si dhe ndërprerjen e këtij aktivitetit gjate ekzekutimit.
- Zgjidhja duhet të ketë funksionalitet machine learning për sistemet Windows/Linux.
- Zgjidhja të jete ne gjendje të skanoje periodikisht skedaret ne qëndrim.
- Zgjidhja të jete ne gjendje të skanoje file të pa ekzekutueshme si: dokumente, skedare të gjeneruar ne Windows/Linux/Mac.
- Zgjidhja duhet të ofroje mbrojtje ndaj shfrytëzimeve të memories përfshirë 0-day exploits, Mandatory ASLR, Bottom-Up ASLR, SEHOP, EAF, DEP.
- Zgjidhja duhet të siguroje mbrojtje bazuar ne të dhënat telemetrike mbledhura nga stacioneve fundore.
- Zgjidhja duhet të vlerësojë sjelljet individuale dhe të beje korrelacione, krahasime midis stacioneve të ndryshme.
- Te gjitha korrelacionet kërcënuese të zbuluara nga stacione të ndryshme duhet ti paraqite tek konsola e menaxhimit.
- Zgjidhja duhet të mbroj nga ndërhyrjet infektuese gjatë shkarkimit ne internet.
- Zgjidhja duhet të zbulojë fazën e lëvizjeve anësore të sulmit si: Pass-the-hash attacks, remote creation of a scheduled task, etj.

- Zgjidhja duhet të lejoje përdoruesin e sistemit të ofroje IOCs të jashtme si: hashet e skedareve, adresat IP, domainet, si edhe rregullat që shpjegojne TTPs e sulmuesve (tools, teknikat, procedurat).
- Zgjidhja duhet të jete ne gjendje të zbuloje tekninat evazive të malware bazuar ne memorje, si: kodet lundruese, proceset spoofing, perdorimi i algoritmit DGA.
- Zgjidhja duhet të analizoje të dhenat telemetrike të stacioneve fundore pa asnje filtrim të tyre nga ana e stacionit fundor. Sistemi nuk duhet të limitoje numrin e ngjarjeve të caktuara si: limitimi i numrit të DNS queries etj.
- Zgjidhja duhet të zbuloje faqe apo aplikacionet që ndajne informacione të ndjeshme të pa kriptuara, fjalkalime, detaje mbi kartat e kreditit etj.

2.2 Mbrojtja Ransomware

- Zgjidhja duhet të parandaloj përpjekjet për të kopjuar ose ekzekutuar ransomware.
- Zgjidhja duhet të jetë në gjendje të parandaloj në mënyrë sjellje ransomware per lloje të panjohura ransomware.
- Zgjidhja duhet të monitoroj operacionet përkatëse të skedarëve dhe të kryejë krahasime për të përcaktuar nëse skedarët janë modifikuar rregullisht ose jane me të vërtetë të koduar.
- Zgjidhja duhet të zbuloje çaktivizimin e Volume Shadow Copy Service si dhe fshirjen e kopjeve rezerve VSS ne sistemet operative windows.
- Zgjidhja duhet të zbuloj sulmet ransomware të cilat demtojne regjistrat master boot MBR të stacioneve.
- Zgjidhja duhet të ketë funksionalitet që të lejojne rivendosjen e skedareve ne formatin origjinal nëse sulmuesi ka arritur të kodoj me sukses disa nga skedarët.
- Zgjidhja duhet të ofroje mbrojtje të avancuar ransomware ne modalitetin "kernel based" për të zbuluar sjelljet tipike të sulmeve ransomware.
- Zgjidhja duhet të jetë në gjendje të plotësojë mbrojtjen kundër ransomware duke përdorur të ashtuquajturat skedarë Canary. Administratori duhet të jetë në gjendje të modifikojë skemën e emërtimit të skedarëve dhe të zgjedhë vendndodhjet e sistemit ku do të vendosen.
- Mbrojtja e ransomware duhet të jete proaktive dhe nuk duhet të mbështetet në rikuperimin e imazhit para infektimit.

- Mbrojtja kundër ransomware duhet të mbuloj gjithashtu disqet e rrjetit të hartuar dhe disqet cloud.

2.3 Përmirësimi dhe reagimi

- Zgjidhja duhet të performojë veprime korrigjuese në pikat fundore si: stacioni i punës, servera, etj.
- Zgjidhja duhet të izolojë makinën nga rrjeti, duke siguruar njëkohësisht vazhdimësinë e analizave të kryera për sistemin operativ në stacionin fundor.
- Zgjidhja duhet të jetë në gjendje të konfigurojë sesionet e Remote Shell në stacionet e zgjedhura, duke i siguruar operatorit ndërfaqen PowerShell të sistemit Windows ose Linux.
- Sistemi duhet të grupoj në mënyrë sintetike operacionet që mund të kryhen në një stacion/grup stacionesh të caktuar në lidhje me një kërcënim/grup të veçantë kërcënimesh.
- Sistemi duhet të kufizoj qasjen në Remote Shell vetëm në rolet e zgjedhura të përdoruesve.
- Remote Shell duhet të lejojë ekzekutimin në modalitetin e plotë dhe të kufizuar, dhe vetëm komandat e zgjedhura janë të disponueshme për ekzekutim.
- Zgjidhja duhet të ruajë një regjistër logesh të plotë të përdorimit të funksionit Remote Shell, në të cilin do të ruhen të gjitha komandat gjatë sesionit të vendosur me stacionin fundor.
- Zgjidhja duhet të ketë një mundësi për të çuar ne karantine automatikisht skedarët që konsiderohen të rrezikshëm.
- Sistemi duhet të lejojë shënimin manual të skedarëve si dhe fshirje automatike të skedarëve që konsiderohen të rrezikshëm.
- Sistemi duhet të sigurojë automatikisht një sërë veprimesh korrigjuese që duhen kryer për një lloj të caktuar kërcënimi të zbuluar.

2.4 Dukshmëria, Gjurmimi, Investigimi

- Zgjidhja duhet të mbledhë në mënyrë automatike të gjithë telemetrinë në kohë reale (pa kërkuar ndërveprim të përdoruesit për të gjitha llojet e të dhënave).

- Zgjidhja të korrelojë ngjarjet midis stacioneve të ndryshme dhe ti ruaje ato në qendër. Në të njëjtën kohë, softueri në anën e stacionit fundor duhet të ketë një mekanizëm për ruajtjen e të dhënave në rast të mungesës së lidhjes me databazen qendrore.
- Zgjidhja duhet të lidh çdo lloj aseti me llogarinë e përdoruesit dhe aktivitetin e tij në pajisje të ndryshme.
- Zgjidhja duhet të listojë të gjitha proceset, shërbimet, nisjet automatike në të gjithë kompjuterët.
- Zgjidhja duhet të tregojë command line execution për të filluar procesin.
- Zgjidhja duhet të tregojë të gjitha lidhjet e rrjetit dhe DNS queries që bën procesi.
- Zgjidhja duhet të jetë në gjendje të kërkojë një ekzekutues sipas emrit të skedarit ose hash-it të skedarit.
- Zgjidhja duhet të jetë në gjendje të shkarkojë skedarët e specifikuar nga pika përfundimtare.
- Zgjidhja duhet të ketë vizibilitet në të gjitha DNS queries, të ndara sipas llojit dhe përgjigjes së marrë.
- Zgjidhja nuk duhet të ketë kufizime në numrin e ngjarjeve por duhet të mundësojë mbledhjen e të gjitha ngjarjeve të një lloji të caktuar nga stacioni fundor.
- Telemetria e mbledhur nga stacionet fundore duhet të përfshijë të paktën elementët e mëposhtëm:

- lidhjet e rrjetit me/nga stacionet, duke përfshirë detaje të tilla si: adresat, portat, statusi i lidhjes, sasia e të dhënave të marra/dërguara, koha e krijimit të lidhjes, protokolli i transmetimit, serverët proxy (nëse ka), domenet URL,
- DNS queries (domain-to-domain, domain-to-ip, ip-to-domain, të pazgjidhura në domain, të pazgjidhura për ip) - të dhënat duhet të përfshijnë domainin burim dhe destinacion, serverin DNS që zgjidh emrin, llojin e regjistrimit DNS , vlera TTL e queries, kodet e gabimit për queries e pazgjidhura,
- të dhënat për të gjithë drivers të instaluar në sistem,
- të dhënat e skedarit - vetitë (emri, kalimi, madhësia, lloji i skedarit, lloji i shtesës), checksum (të paktën MD5, SHA-1 dhe SHA-256), nënshkrimi dixhital nëse ekziston (MD5

dhe SHA1), koha e krijimit, koha e modifikimit të fundit, nëse skedari është shkarkuar nga Interneti - URL-ja nga e cila është shkarkuar skedari,

- veprimet në skedarë - operacionet e krijimit, riemërtimit dhe fshirjes së një skedari, së bashku me informacionin se çfarë procesi ka kryer veprimin e dhënë dhe cili përdorues është regjistruar në sistem gjatë këtij operacioni,
- përmbajtjen e skedarit Hosts,
- adresimi IP i stacionit - duke përfshirë portën e paracaktuar, adresën MAC, serverët e konfiguruar DHCP dhe DNS, WiFi SSID ,
- lidhjet e koneksioneve të hapura në stacion - duke përfshirë informacionin për adresën lokale, porten, protokollin,
- Sesionet e hyrjes në Windows - duke përfshirë IP-në e sesionit, IP-në e burimit të sesionit, llojin e aplikacionit, kohën e krijimit, makinën në distancë që merr pjesë në seancë, proceset e hapura brenda një sesioni të caktuar, përdoruesi që hapi sesionin,
- detajet e stacionit fundor, si: emri, FQDN, lloji i stacionit, OS, statistikat e përdorimit të CPU-së, memoria e lirë, zënia e diskut, kontrolli për MBR, proceset që ekzekutohen në stacion, përdoruesit e regjistruar në stacion, shërbimet që funksionojnë në stacionin, pajisjet e memories të instaluara ne stacion,
- modulet që funksionojnë në stacion, duke përfshirë: emrin, madhësinë, kontrollin, adresën, madhësinë e header, skedarët e lidhur me modulin, mbrojtjen e header,
- ndërfaqet e rrjetit,
- proceset që ekzekutohen në stacion, duke përfshirë: ID, kontrollin, gjendjen, kalimin, përdorimin e CPU/RAM, statusin e procesit të fshehur, hierarkinë e procesit, kohën e krijimit dhe përfundimit, lidhjet e rrjetit të hapura nga procesi, skedarët e hapur nga procesi, command line, module të lidhura dhe të ngarkuara nga procesi, ngjarje të injektimit të procesit, aktiviteti WMI, detaje të procesit që u shkarkua nga rrjeti,
- proxy i konfiguruar në stacion, duke përfshirë: adresën e proxy, URL-në për PAC proxy, portat, modalitetit i proxy,
- shënimet e regjistrit të sistemit të lidhura me autorun, duke përfshirë çelësat dhe vleren e tyre,
- operacionet në regjistër, me mundësinë e shënimit të seksioneve shtesë që i nënshtrohen monitorimit,

- sesionet e hyrjes në distancë të sistemit, duke përfshirë: protokollin e përdorur, lidhjen e pajisjes dhe përdoruesit nga distanca, proceset e nisura gjatë sesionit në distancë,
- Thirrjet RPC, duke përfshirë: nivelin dhe llojin e shërbimit të vërtetimit të përdorur nga RPC, adresën dhe porten RPC të destinacionit, burimin RPC, RPC UUID, protokollin RPC, proceset e krijuara nga RPC,
- orari i detyrave, duke përfshirë: kush shtoi detyrën e planifikuar dhe kohën e përditësimit të fundit të detyrës, statusin e detyrës, thirrjen e detyrës së fundit, argumentet e përdorura në detyrën e krijuar, rrugën e veprimit në detyrë, skedarët e lidhur me detyrën,
- shërbimet në sistemin operativ, duke përfshirë: statusin dhe nën-statusin e shërbimit, llojin e shërbimit, hyrjen e përdorur nga shërbimi në momentin e nisjes, skedarin binar të lidhur me shërbimin, linjën e komandës së përdorur nga programi që nis shërbimi, rruga drejt skedarit të përdorur nga shërbimi, procesi që krijoi shërbimin, driver e lidhur me shërbimin,
- të gjithë përdoruesit, duke përfshirë: emrin, organizatën, domainin, nivelin e autorizimit, SID, hyrjen e fundit, kohën që nga ndryshimi i fundit i fjalëkalimit, emrat e stacioneve në të cilat një përdorues i caktuar është identifikuar, proceset e filluara nga një përdorues i caktuar,
- Aktiviteti WMI - si lokal ashtu edhe në distancë, duke përfshirë: operacionet që gjeneruan përdorimin e WMI, burimin e aktivitetit WMI, kohën e krijimit, proceset e ekzekutuara në kontekstin e WMI, objektet e vazhdueshme të krijuara si pjesë e aktivitetit WMI, pyetjet WMI.

- Kontrollet e portave të hyrjes/daljes (Kontrollet e pikës fundore):
- Zgjidhja duhet të jetë në gjendje të aktivizoj dhe çaktivizoj kontrollin e portes I/O.
- Zgjidhja duhet të jetë në gjendje të kontrolloj pajisjen duke specifikuar:
- cilat pajisje USB mund të lidhen me stacionin,
- Zgjidhja duhet të lejojë kontrollin e firewall të rrjetit lokal, me aftësinë për të shtuar rregullat Inbound dhe Outbound.
- Zgjidhja duhet të kontrollojë përdorimin e të dhënave të enkriptimit të BitLocker në disqet e përdoruesve.

2.5 Vecorite e platformës

- Zgjidhja duhet të korreloj sinjalizimet dhe ngjarjet e zbuluara si pjesë e një sulmi të zbuluar, bazuar në taktikat, teknikat, procedurat MITER (TTP), me një incident të vetëm.
- Zgjidhja duhet të sigurojë automatikisht informacion në lidhje me pajisjet dhe llogaritë e përdoruesve që janë prekur ose kanë marrë pjesë në rrjedhën e sulmit.
- Zgjidhja duhet të konsolidojë të dhënat e shkakut rrënjësor (të tregojë dyshimet dhe provat, të tregojë toplogjine e procesit, duke përfshirë Parent,Child, etj.).
- Zgjidhja duhet të siguroj mbajtjen afatgjatë të të dhënave për incidentet e konsoliduara, të paktën 12 muaj.
- Incidenti duhet të paraqesë një afat kohor grafik në të cilin do të vendosen ngjarjet dhe dyshimet kryesore, proceset e nisura, përhapja e sulmit në stacionet pasuese, së bashku me mundësinë e gjurmimit interaktiv të detajeve të këtyre ngjarjeve.
- Ndërfaqja e përdoruesit duhet të krijojë një pamje të incidentit që përmban informacione kyçe si shkaku rrënjësor, shtrirja e sulmit (makinat e lidhura dhe llogaritë e përdoruesve), fazat e ndryshme të sulmit të paraqitura në një afat kohor, fillimi dhe mbarimi, komunikimi në rrjet i vendosur gjatë sulmit.
- Zgjidhja duhet të shfaqë një pamje të plotë të topologjisë së sulmit për çdo proces me qëllim të keqdashës dhe jo keqdashës.
- Zgjidhja duhet të hartojë saktë sinjalizimet dhe të dhënat në kornizën MITER ATT&CK.
- Zgjidhja duhet të klasifikojë të dhënat e papërpunuara bazuar në përputhje me modele të ndryshme të sjelljes, sulmeve, TTP-ve, të dhënave të inteligjencës së kërcënimeve, provat, dyshimet, etj.
- Zgjidhja duhet të lejoje komentet për incidentet në mënyrë që të lehtësojë përpunimin dhe transferimin e tyre ndërmjet analistëve.
- Zgjidhja duhet të bllokojë nisjen e skedarëve të ekzekutueshëm (.exe dhe .dll) në Sistemet Windows. Lista e skedarëve që do të bllokohen të krijohet në mënyrë dinamike gjatë analizës së incidentit (mundësia e shtimit të bllokimit si pjesë e përgjigjes së incidentit), si dhe duke shtuar një listë statike.
- Zgjidhja duhet të lejojë shtimin e skedarëve bazuar në kontrollet SHA-1 dhe SHA-256.

- Shtimi i skedarit të ri në listën e bllokimit duhet të parandalojë nisjen e proceseve të reja dhe të përfundojë funksionimin e proceseve tashmë ekzistuese që janë krijuar në bazë të skedarëve të ekzekutueshëm të bllokuar.
- Zgjidhja duhet të gjenerojë një incident gjate përpjekjes për të ekzekutuar një skedar të shtuar në listën e bllokimit .
- Zgjidhja duhet të sigurojë përdorimin e një tenant në cloud dhe burime të dedikuara vetëm për klientin. Ndalohet ruajtja e të dhënave të klientit mbi burimet ose tenante të ndara me klientët e tjerë.
- Zgjidhja duhet të mundësojë caktimin e roleve të analistit dhe administratorit vetëm për një pjesë të zgjedhur të agjentëve të instaluar në stacionet e menaxhuara. Analisti dhe administratori i caktuar për agjentët e përzgjedhur mund të kenë akses vetëm në të dhënat që lidhen me këta agjentë.
- Softueri i instaluar në stacionin fundor duhet të jetë në gjendje të regjistrohet në Windows Security Center si një zgjidhje e plotë AV.
- Zgjidhja duhet të ketë një mekanizëm për zbulimin e pajisjeve të pambrojtura të regjistruara në Active Directory.
- Zgjidhja duhet të lejoj caktimin e politikave të ndryshme për grupe të ndryshme agjentësh dhe të lejoje ndryshime dinamike të politkave të caktuara.
- Zgjidhja duhet të lejoj zbulimin e agjentëve për të cilët politika aktive nuk përputhet me atë të caktuar për grupin të cilit i përket agjenti.
- Zgjidhja duhet të lejoj tejkalimin e cilësimeve individuale për agjent, pavarësisht nga cilësimet e grupit.

2.6 Platforma e menaxhimit

- Zgjidhja duhet të ketë sensorë lokalë EDR të instaluar në stacionet e punës dhe serverat pa pasur nevojë të rinisin kompjuterin fundor (përveç funksionit të nënshkrimit antivirus).
- Zgjidhja duhet të mundësojë funksionimin e sensorit në një mënyrë transparente për përdoruesin fundor, pa shenja vizuale në stacionin fundor dhe me opsionin për të çaktivizuar njoftimet.

- Një sensor EDR i instaluar në një stacion pune duhet të konsumojë maksimumi deri ne 5% të RAM-it.
- Sensori EDR duhet të përdorë kompresimin e të dhënave të transmetuara, pa humbje detajesh, duke mos gjeneruar më shumë se 15 MB të dhëna të dërguara në ditë (duke supozuar 10 orë aktivitet të stacionit fundor).
- Zgjidhja duhet të jetë e lehtësisht e administrueshme përmes një konsole të vetme të centralizuar, që mundëson konfigurimin dhe administrimin e politikave, si dhe punën e analistëve.
- Zgjidhja duhet të ofrojë role të ndryshme përdoruesi, duke ndarë analistët e niveleve të ndryshme (p.sh. L1, L2, L3) dhe përdoruesit me privilegje të reagimit ndaj incidentit.
- Zgjidhja nuk duhet të kërkoj një rinisje të stacionit fundor ose të serverit gjatë vendosjes të instalimit fillestar dhe përditësimit.
- Zgjidhja duhet të jetë në gjendje të konfigurojë përjashtimet e politikave të kontrollit ne stacione fundore apo sipas grupeve.

- **Sistemi operativ:**
- Zgjidhja duhet të ofroj mbështetje për Windows 7 dhe versione më të reja.
- Zgjidhja duhet të ofroj mbështetje për Windows Server 2008 dhe versione më të reja.
- Zgjidhja duhet të ofroj mbështetje për MacOs Sierra dhe versione më të reja.
- Zgjidhja duhet të ofroj mbështetje për Linux (CentOS 6, 7, 8, 9), Red Hat (6.7, 8), Oracle Linux 6, 7, 8, Ubuntu (14 LTS, 16 LTS, 18 LTS), SLES 15 and above, Debian 8, 9, 10)

- **Automatizimi:**
- Zgjidhja duhet të lejoj integrimin me sistemet SIEM, të paktën duke dërguar informacione rreth incidenteve të zbuluara nëpërmjet syslog në formatin CEF.
- Zgjidhja duhet të suportoje dërgimin e të dhënave syslog përmes një kanali të koduar.
- Zgjidhja duhet të ketë një API të hapur.
- API duhet të ofroje funksione të tilla si:
- fillimi i procesit të gjurmimit duke përfshirë: kërkimin për një skedar specifik, lidhje, procese,

- menaxhimin e agjentëve duke përfshirë: kontrollimin e versionit, mbledhjen e një liste agjentësh online/offline, kërkimin e agjentëve që i përkasin një grupi të caktuar, shkarkimin e regjistrave të agjentëve, shkarkimin e cilësimeve të agjentëve,
- fillimin e një përgjigjeje ndaj një incidenti duke përfshirë: përfundimin e procesit, vendosjen e një skedari në karantinë, fshirjen e një regjistrimi në regjistër, bllokimin e një skedari,
- shtimi i rregullave të reja të detektimit,
- përditësimin e listës së reputacionit në sistem,
- izolimin e stacionit,
- Zgjidhja duhet të suportoje orkestrimin e punëve duke përdorur SOAR, Ticketing ose platforma të tjera.

- Dixhital Forensics dhe reagimi ndaj incidenteve (vetëm sistemet operative Windows):
- Zgjidhja duhet të lejojë shfletimin e skedarëve në stacionin e përdoruesit dhe shkarkimin e skedarit të treguar.
- Zgjidhja duhet të jetë në gjendje të kërkojë stacione fundore të mbrojtura nga rregullat YARA. Operatori duhet të jetë në gjendje të tregoj shtrirjen e kërkimeve për rregullin e zgjedhur YARA, në mënyrë që të përshpejtojë të gjithë procesin.
- Zgjidhja duhet të lejojë shfletimin interaktiv të listës së skedarëve që janë në stacion me agjentin, me mundësinë e shkarkimit të skedarëve të treguar në stacionin e analistit.
- Zgjidhja duhet të kryejë një kërkim skedari dhe/ose kërkim YARA.

- Zgjidhja duhet të përditësoj vazhdimisht informacionin për të gjitha portet që dëgjojnë trafikun në stacion, gjithashtu duhet të shoqërojë informacionin për portin e hapur me procesin e dëgjimit.
- Sistemi duhet të mundësojë shpërndarjen nëpërmjet agjentit të tij të mjeteve shtesë të reagimit ndaj incidentit që analisti do të donte të përdorte gjatë trajtimit të incidentit.

- **Efektiviteti i zgjidhjes:**
- Zgjidhja sipas vlerësimit të Mitre Attack nga 2023 duhet të ketë një rezultat parandalimi prej të paktën 95%

- Zgjidhja sipas vlerësimit të Mitre Attack 2023 duhet të ketë një rezultat të mbulimit të dukshmërisë prej të paktën 95%
- Zgjidhja sipas vlerësimit të Mitre Attack nga viti 2023 duhet të ketë një mbulim analytics prej të paktën 95%

APD për implementimin e zgjidhjes EDR do ofrojë kapacitetet e meposhtme virtuale per procesim (computing) dhe ruajte informacioni (Storage), .

Specifikimet Teknike te Virtual Appliance:

- Vcpu: 24 threads
- Memory: 64 GB
- Storage:
  - 1 TB hapësirë storage SSD
  - 10 TB hapësirë storage HDD

2.7 Licensimi

- Zgjidhja të jetë e licensuar minimalisht për 300 perdorues (users).

- Licensimi të jetë i pajtueshëm për një periudhë një (1) vjecare.

2.8 Suporti dhe implementimi

- Ne zgjidhje të përfshihet suport për update të software për 1 vit me nivel kontrate sherbimi 24x7 në cdo dite të vitit nga Operator Ekonomik në bashkpunim me prodhuesin e zgjidhjes.
- Instalimi, konfigurimi dhe testimi duhet të bëhet nga ofertuesi, zgjidhja duhet të dorëzohet e plotë (Turnkey Solution).
- Zgjidhja të ofroje mundësi për komunikim me chat, web, telefon dhe email me qendrën, suportin e autorizuar të vet prodhuesit të pajisjes.
- Zgjidhja të përfshije akses direkt në qendrën e autorizuar për: hapje dhe ndjekje te case, informacion në forume, njoftime të reja rreth zgjidhjes, dokumenta online.

- ***Faza 1: Planifikimi Fillestar***
  - Planifikimi i rrjetit dhe infastrukturës për integrimin e zgjidhjes
- ***Faza 2: Instalimi i zgjidhjes***
  - Përgatitja e fizike e zgjidhjes duke përfshire kërkesat e sistemit (IP, Sistem Operimi etj.)
- ***Instalimi/Inicializimi i zgjidhjes***
  - Licensimi i zgjidhjes
  - Testimi i rrjedhjës së trafikut dhe ndërlidhjes me infrastrukturën në tërësi
- ***Faza 3: Konfigurimi i zgjidhjes***
  - Konfigurimi i sistemit sipas kërkesave fillestare të zgjidhjes
  - Konfigurimi dhe shpërndarja aplikacionit te target-et (endpoint ose server sipas nevojës)
  - Inicializimi i zgjidhjes dhe monitorimi i gjetjeve
- ***Faza 4: Raportimi i dobësive***
  - Paraqitja e veprimtarive dhe gjetjeve të kryera
  - Përgatitje e politikave të sigurisë dhe aplikimi i tyre
  - Gjenerimi i perosnalizuar i raportit të dobësive të zbuluara
- ***Faza 5: Trajnimi i personelit të departamentit të sigurise***
  - Operatori Ekonomik duhet të demonstroj, trajnoj dhe të instruktoj stafin e departamentit te Sigurisë te APD mbi perdorimin e sistemit EDR, si dhe tu demonstroj atyre skenare te ndryshme investigimi.
  - Gjenerimi dhe dorëzimi i raportit te implentimit të zgjidhjes

3. Sistem Vunerability Scanner (VSCAN)

3.1 Karakteristikat e Përgjithshme

Sistemi vulnerability scanner (VSCANER) duhet te kryej skanime të thelluara për të identifikuar dobësitë në sisteme operative, aplikacione dhe pajisje rrjeti, duke ndihmuar në zbulimin e pikave të dobëta që mund të shfrytëzohen nga sulmuesit. Ai auditon konfigurimet e sistemeve për të siguruar përputhshmërinë me politikat e sigurisë dhe standardet e industrisë, duke ndihmuar në identifikimin e konfigurimeve të gabuara ose të pasigurta.

Nga VSCAN kerkohet qe te skanoj dhe detektoj për prezencën e malware dhe softuerëve të dëmshëm, duke ndihmuar në mbrojtjen kundër kërcënimeve të njohura dhe të reja. Ai duhet te përditësohet rregullisht për të përfshirë dobësitë më të fundit dhe kërcënimet emergjente, duke siguruar që referncat e mbrojtjes të jetë gjithmonë e freskët dhe relevante.

Gjenerimi i raporteve të detajuara është një tjetër veçori kyçe, qe kerkohet te ofrohet. Gjithashtu, kerkohen analiza të hollësishme mbi dobësitë e zbuluara dhe duke dhënë rekomandime për masat e korrigjimit. Ndërfaqja e përdoruesit duhet te jete sa me miqësore dhe intuitive, duke e bërë të lehtë menaxhimin e skanimeve dhe interpretimin e rezultateve.

VSCAN duhet te suportoje integrimin me mjetet e menaxhimit të sigurisë, si SIEM dhe SOAR, duke lejuar një qasje të bashkërenduar dhe efikase në menaxhimin e sigurisë. Ai gjithashtu ofron opsionet e skanimit autentik dhe joautentik, duke lejuar që skanimi të kryhet në mënyrë më të hollësishme dhe me qasje të privilegjuara kur është e nevojshme.

3.1.1. Skanimi i Dobësive

Metodat e skanimit qe duhet te ofrohen si me poshte:

- **Skanim i thelluar:** VSCAN duhet te kryeje skanime të thelluara për të identifikuar dobësitë në sistemet operative, aplikacionet, dhe pajisjet e rrjetit. Platforma duhet te jete ne gjendje per te skanuar infrastrukturen tradicionale on premise dhe ate cloud.
- **Përditësimet e cenueshmërisë në kohë reale:** Ky funksionalitet duhet te jete ”real time”.
- **Auditimi i konfigurimeve:** Platforma VSCAN duhet te kontrolloj konfigurimet për të siguruar që ato janë në përputhje me politikat e sigurisë dhe standardet e industrisë.
- **Skanimi i malware:** Platforma duhet te identifikoj malware dhe softuerë të dëmshëm nga sistemet.
- **Zbulimi i dobësive të reja:** Platforma duhet te përditësohet rregullisht për të përfshirë dobësitë më të reja dhe kërcënimet emergjente.
- **Raportim i detajuar:** Platforma duhet te gjeneroje raporte të detajuara mbi dobësitë e gjetura, duke përfshirë prioritetet dhe rekomandimet për korrigjim. Raportet duhet te jene te eksportueshem.
- **Real-Time Vulnerability Updates** – te ofrohet
- **External Attack Surface Scanning** – te ofrohet
- **Unlimited Scans** – te ofrohet
- **Number of IPs per Scanner** – pa limit
- **Web Application Scanning** – te jete I perfshire
- **Targeted Email Notifications** – te ofrohet
- **Scan Scheduling** – te ofrohet
- **Configuration Checks -** te ofrohet
- **Compliance Checks (PCI, CIS, FDCC, NIST, etc.)** – te ofrohet
- **Sensitive Data Searches** – te ofrohet
- **SCADA Plugins** – te suportohet
- **Access to the VMware Virtual Appliance** – ofrohet

3.1.2. Përdorshmëria dhe Integrimi

- **Ndërfaqe e përdoruesit miqësore:** Platforma duhet te ofroj një ndërfaqe intuitive dhe lehtësisht të përdorshme për menaxhimin e skanimeve dhe analizën e rezultateve.
- **Integrimi me mjetet ekzistuese:** Sistemi VSCAN duhet të integrohet lehtë me mjetet ekzistuese të menaxhimit të sigurisë, si SIEM dhe SOAR.
- **Skanim i autentikuar dhe joautentikuar:** Platforma duhet te mbështese skanimin autentik për të marrë informacion më të hollësishëm dhe skanimin joautentik për testime sipërfaqësore.

3.2 Licensimi dhe Suporti

Zgjidhja duhet të ofrojë mundësinë e përdorimit të sistemit për një numër të pa kufizuar IP dhe skanimi.

- Ne zgjidhje të përfshihet suport për update të software për 1 vit me nivel kontrate sherbimi 24x7 në cdo dite të vitit nga Operator Ekonomik.
- Instalimi, konfigurimi dhe testimi duhet të bëhet nga ofertuesi, zgjidhja duhet të dorëzohet e plotë (Turnkey Solution).
- Zgjidhja të ofroje mundësi për të kominikim me chat, web, telefon dhe email me qendrën, suportin e autorizuar të vet prodhuesit të pajisjes.
- Zgjidhja të përfshij akses direkt në qendrën e autorizuar për: hapje dhe ndjekje te case, informacion në forume, njoftime të reja rreth zgjidhjes, dokumenta online.

3.2.1. Modelet e Licensimit

- Zgjidhja të jetë e licensuar per 1 vit.

- Licensimi të jetë i pajtueshëm për një periudhe një (1) vjecare.

3.2.2. Suporti

- **Suport 24/7:** Te ofroj mbështetje teknike 24/7 për të zgjidhur çdo problem që mund të lind gjatë përdorimit të VSCAN.
- **Materiale trajnimi:** Te siguroj materiale të shumta trajnimi, përfshirë dokumentacionin online, videot udhëzuese, dhe kurset e trajnimit.

3.3 Implementimi

Më poshtë do të përshkruhen pikat e implementimit:

3.3.1 Planifikimi i Implementimit

- ***Faza 1: Planifikimi Fillestar***

- **Vlerësimi i kërkesave:** Identifikimi i kërkesave specifike të organizatës për skanim dhe siguri.
- **Hartimi i një plani implementimi:** Hartimi i një plani të detajuar për implementimin e VSCAN, duke përfshirë fazat dhe afatet kohore.

- ***Faza 2: Instalimi dhe konfigurimi i zgjidhjes***

3.3.2 Instalimi dhe Konfigurimi

- **Instalimi i softuerit:** Instalimi i VSCAN në sistemet target sipas udhëzimeve qe do te jepen nga autoriteti kontraktor.
- **Konfigurimi i inicial i skanimeve:** Konfigurimi i politikave të skanimit dhe planifikimi i skanimeve të rregullta.

- ***Faza 3: Testimi dhe validmi***

3.3.3 Testimi dhe Validimi

- **Testimi fillestar:** Kryerja e skanimeve testuese për të siguruar që VSCAN funksionon siç pritet dhe identifikon dobësitë me saktësi.
- **Validimi i rezultateve:** Verifikimi i rezultateve të skanimeve dhe bërja e rregullimeve të nevojshme në konfigurim.

    - ***Faza 4: Trajnimi***

3.3.4. Trajnimi i Përdoruesve

- **Trajnimi i stafit:** Ofrimi i trajnimeve për stafin e sigurisë dhe përdoruesit e tjerë të lidhur me menaxhimin e skanimeve dhe interpretimin e rezultateve.

    - ***Faza 5: Monitorimi dhe mirembajtja***

3.3.5 Monitorimi dhe Mirëmbajtja

- Operatori Ekonomik duhet të demonstroj, trajnoj dhe të instruktoj stafin e departamentit te Sigurisë Kibernetike te APD mbi politikat e implementuara dhe parandalimin e kërcënimeve.
- Gjenerimi dhe dorëzimi i raportit të implentimit të zgjidhjes.

4. RAPORTIMI

4.1 Kërkesat e Raportimit

Kontraktuesi do të paraqesë raportet e mëposhtme në shqip, në origjinal dhe në 3 (tre) kopje:

- **Raporti Fillestar** duhet të prodhohet brenda 14 (katër mbëdhjetë) ditësh nga fillimi i implementimit. Në raport duhet të përshkruhen gjetjet fillestare, progresi në mbledhjen e

të dhënave, çdo vështirësi të pritura ose të hasura. Kontraktuesi duhet të vazhdojë me punën e tij / saj derisa Autoriteti Kontraktues të dërgojë komente mbi raportin fillestar.

- **Drafti i raportit përfundimtar** Ky raport duhet të dorëzohet jo më vonë se një muaj para përfundimit të periudhës së zbatimit të detyrave.
- **Raporti final** me të njëjtat specifika si drafti i raportit përfundimtar, me inkorporimin e komenteve të pranuara nga palët në draft raport. Afati i fundit për dërgimin e raportit final është 5 (pesë) ditë pas marrjes së komenteve në draft raportin përfundimtar. Raporti duhet të përmbajë një përshkrim mjaftueshëm të detajuar të opsioneve të ndryshme për të mbështetur një vendim të informuar mbi sistemin . Analizat e detajuara që i mbështesin rekomandimet do të prezantohen në anekset në raportin kryesor. Raporti përfundimtar duhet të sigurohet së bashku me faturën përkatëse.

Gjithashtu, operatori ekonomik fitues duhet te dorezoje dhe raporte, si për shembull:

1- Raport instalimi.
2- Raport i arkitekturës hardware.

4.2 Dorëzimi dhe Miratimi i Raporteve

Raporti i përmendur më sipër duhet t'i dorëzohet grupit të punës për ndjekjen e kontrates të identifikuar në kontratë. Grupi punes është përgjegjës për aprovimin e raporteve.

5. KERKESA TEKNIKE PER PAISJET HARDWARE

Më poshtë do të përshkruhen kërkesat teknike të paisjeve hardware të cilat do të shërbejnë për të monitoruar në vazhdim zgjidhjet e kërkuara.

5.1 Kompjuter Workstation sipas prodhuesit

KARAKTERISTIKA MINIMALE TEKNIKE	
Pikët Min. për Procesorin sipas: cpubenchmark.net Min Proc. Rating According to: cpubenchmark.net:	30000 Pikë
"RAM":	32 GB, min. DDR4 2666 MHz, ECC
Madhësia e Hard Diskut "HDD Size"	(1) x 500 GB SSD Sistemi Operativ dhe (2) x 1000 GB HDD
Shpejtësia e Hard Diskut "HDD Speed":	7200 RPM SATA 6.0 Gb/s
"Disk Subsystem Controler":	Serial ATA III 6.0 Gb/s, Minimum 4 Serial ATA Interface with RAID 0,1,5,10 Support. (Hard Disk të Konfiguruar në RAID 1).

Karta Grafike "Graphics":	Kartë Grafike HD e Dedikuar PCI-E x16, Minimum 4 GB Memory; Min. (2) Porta (VGA/DVI/HDMI/DP, mund të përdoret dhe adaptor). Karta të jetë e rekomanduar dhe instaluar nga prodhuesi për workstation.
"Media Device":	DVD+/-RW with Dual Layer DVD+R wri. Capacity
"Slots":	Minimum (4) PCI/PCI-E nga të cilat min. (2) PCI-E x16
KOMUNIKIMI & MENAXHIMI	
Portat e Komunikimit "Ports":	Min. (8) USB nga të cilat: a. Min. (2) USB Para; b. Min. (6) USB 3.0 (2) RJ-45, (1) Audio In/Out, (1) Mic. and (1) Headphone, (1) Portë Video (mund të përdoret dhe adaptor)
Rrjeti "Networking":	(2) 10/100/1000 LAN Gigabit Ethernet Port
"Sound":	Integrated Sound Card
"Speakers":	Internal or Built-in Monitor
Siguria "Security Management":	Embedded Security TPM 2.0
Sistemi i Operimit "Preinstalled Licensed O. S.":	OEM Windows 10 64-bit Professional për Workstation
Tastiera "Keyboard":	Standart Keyboard QWERTY
"Mouse":	Minimum 3 Button Scroll Optical
Ushqimi "Power Supply":	220 V AC, 50 Hz
Kursimi i Energjisë "Energy Efficency":	Energy Star
AKSESORËT	
Kabëll "Power Cord":	Po, European
"Recover":	Recover Partition
MONITORI	
Tipi "Type":	LCD OSE LED i të njëjtës Markë me Kompjuterin
Madhësia "Size":	≥ 32"
Rezolucioni "Native Resolution":	1920 x 1080 at 60 Hz
Raporti i Kontrastit "Constrast Ratio Static":	1000:1
"Display Port":	(1) VGA dhe të paktën (1) prej portave DP/DVI/HDMI
Koha e Rifreskimit "Response Time":	≤ 6 ms
Kursimi i Energjisë "Energy Efficency":	Energy Star
Ushqimi "Power Supply":	220 V AC, 50 Hz
GARANCIA	

Periudha e Mbulimit të Garancisë "Warranty":	3 Vjet

5.2 Televizor 75 inch

KARAKTERISTIKA MINIMALE TEKNIKE	
Madhesia e Ekranit "Screen Size":	75"
Tipi i Panelit "Panel Type":	QLED/Neo QLED
Rezolucioni "Resolution":	Ultra HD 4K (3840x2160)
Frekuenca "Refresh Rate":	min. 240 Hz MEMC
Kontrasti "Contrast":	min. 10000:1+, HDR10+, HLD, Ultimate UHD Dimming
Kendi i Shikimit "Viewing Anglet":	min 178°(H)/178°(V)
Dekoderi "TV Tuner":	DVB-T2 I integruar
Sistemi Audio "Audio System":	min 40W, 2 tweeters + 4 woofers
TV Inteligjent "Smart TV":	Po
Sistemi Operativ "Operating System":	Android 10 ose me lart
KOMUNIKIMI & MENAXHIMI	
Karte Rrjeti "Ethernet":	min. Gigabit Ethernet
Wireless "Wi-Fi":	min. Wi-Fi 6
Bluetooth TV "Bluetooth TV":	min. 5.0
USB 2.0 "USB 2.0":	min. 2 porta
USB 3.0 "USB 3.0":	min. 2 porta
Porta HDMI "HDMI Ports":	min. 4 copë
AKSESORËT	
Kabëll "Power Cord":	Po, European
Telekomanda "Remote Control":	Po, e përfshirë 360° me bluetooth
Modul Montimi ne Mur "Wall Mount":	Po, e përfshirë
Modul montimi ne tavoline "Desk Mount":	Po, e përfshirë
TE TJERA	
Kursimi i Energjisë "Energy Efficency":	Energy Star
Ushqimi "Power Supply":	220 V AC, 50 Hz
GARANCIA	
Periudha e Mbulimit të Garancisë "Warranty":	2 Vjet

6. AFATI KOHOR I IMPLEMENTIMIT TË PROJEKTIT

Nr.	Emërtimi i fazës / Periudha kohore	M1	M2	M3	M4	M5	M6
1	Faza pergatitore. Analizim i situatës ekzistuese. Verifikim i të gjitha kërkesave duke u mbështetur në specifikimet e përcaktuara	■					
2	Lëvrimi i pajisjeve software/hardware	■	■	■			
3	Faza e instalimit dhe konfigurimit i sistemeve.		■	■	■	■	
4	Faza e integrimit dhe testimit të sistemeve.			■	■	■	
5	Trajnimi i përdoruesve						■
6	Marrja në dorëzim						■