elektro gorenjska

Elektro Gorenjska,
podjetje za distribucijo
električne energije, d. d.

Sedež družbe: Kranj
Poslovni naslov:
Ulica Mirka Vadnova 3a
4000 Kranj

Klicni center: 080 30 19
Klici iz tujine: +386 4 2083 333
Faks: 04 2083 600
E-pošta: info@elektro-gorenjska.si
www. elektro-gorenjska.si

POSTAJNI IDS SISTEM

POC – potrditev koncepta

Kranj, 24.10.2025

Elektro Gorenjska,
podjetje za distribucijo
električne energije, d. d.

Sedež družbe: Kranj
Poslovni naslov:
Ulica Mirka Vadnova 3a
4000 Kranj

Klicni center: 080 30 19
Klici iz tujine: +386 4 2083 333
Faks: 04 2083 600
E-pošta: info@elektro-gorenjska.si
www. elektro-gorenjska.si

Vsebina

1. Splošno

Ta dokument opisuje najsodobnejše specifikacije za sisteme za zaznavanje vdorov (IDS) v procesnih OT omrežjih.

V prvem sklopu Osnovne funkcionalne zahteve so navedene osnovne zahteve sistema za zaznavanje vdorov.

Drugi sklop predstavlja koncepte in vedenje, ki se pričakujejo od sodobnih sistemov za zaznavanje vdorov (IDS), ter podrobno razlaga njihove funkcije. Namen tega poglavja je zagotoviti jasno razumevanje delovanja IDS. V nadaljevanju so opisane tehnične specifikacije, ki se neposredno nanašajo na funkcije, opisane v prvem delu. Te tehnične specifikacije določajo zahteve za IDS, ter za pripadajoče storitve. Tehnične specifikacije so zaradi preglednosti priložene v ločenem Excel dokumentu.

Tretji sklop opisuje nefunkcionalne lastnosti IDS sistema. Te zahteve so bolj splošne, vendar naročniku podajajo dodatne informacije, ki omogočajo optimalno izbiro IDS rešitve.

2. Okvir projekta

Projekt je zastavljen kot potrditev tehnike in postopkov za obvladovanje kibernetskih groženj in obratovalnih stanj (POC – Proof Of Concept). Rezultati in ugotovitve bodo uporabljene za razvoj in implementacijo sistemov za obvladovanje kibernetskih , tehničnih in obratovalnih anomalij v RTP postajah.

3. Osnovne funkcionalne zahteve

Sistemi za zaznavanje vdorov morajo podpirati vsaj naslednje osnovne funkcije, da lahko učinkovito zaščitijo OT omrežja pred grožnjami:

- Rešitev mora zaznavati vdore in grožnje v OT omrežjih.
- Rešitev mora zaznavati kibernetske napade na OT sisteme, na podlagi motenj in težav v procesnem omrežju.
- Rešitev naj omogoča preglednost in hitro zaznavanje kibernetskih groženj ter procesnih tveganj, pri čemer mora delovati popolnoma pasivno, brez posegov v OT naprave.
- Rešitev mora podpirati funkcionalnost popolnega pregleda paketov (full packet inspection) za IEC 60870-5-104, zaznavati kršitve protokola in pregledovati signale, prenesene v sporočilih.
- Rešitev mora podpirati funkcionalnost popolnega pregleda paketov za IEC 61850 Manufacturing Message Specification (MMS) in Generic Object Oriented Substation Events (GOOSE), zaznavati kršitve protokola in pregledovati logična vozlišča LN (Logical Nodes), prenesena v sporočilih.

- Ponudnik rešitve mora potrditi, da IDS lahko uporablja datoteke Substation Configuration Language (SCL).
- Rešitev mora podpirati centralizirano upravljanje in integracijo v centralizirano platformo za upravljanje.
- Rešitev naj zagotavlja celovit in ažuren popis (seznam) vseh sredstev v procesnem omrežju, vključno z neaktivnimi napravami.
- Rešitev mora podpirati vzdrževalni način (maintenance mode), da se preprečijo lažni alarmi med vzdrževanjem in rednim testiranjem.
- Rešitev mora samodejno prepoznati ranljivosti OT sredstev.
- Rešitev naj zaradi kibernetskih groženj in sprememb konfiguracije redno spremlja stanje procesnih naprav.
- Rešitev naj nadaljuje z zaznavanjem vdorov in forenzičnim beleženjem tudi v primeru začasne prekinitve povezave s centralnim sistemom upravljanja.
- Rešitev naj omogoča lokalni dostop do senzorja v primeru, da je prekinjena povezava s centralnim sistemom upravljanja.

4. Funkcionalne zahteve in koncepti

IDS je ključno orodje za zagotavljanje varnosti in odpornosti omrežja, ki aktivno spremlja omrežni promet in naprave, da bi prepoznal zlonamerne aktivnosti, sumljivo vedenje in kršitve varnostnih politik. IDS izvaja temeljito analizo vse komunikacije, z namenom zaznave kibernetskih groženj, prepovedanih dejavnosti in morebitnih napak.

Učinkovit IDS vključuje poglobljeno razumevanje celotnega sistema, kar mu omogoča, da se prilagaja in razvija skupaj z omrežjem. Takšno zavedanje sistema omogoča zaznavanje napak, prepovedanih dejavnosti in stalno spremljanje funkcij procesnega okolja, s čimer se izboljša splošna varnostna odpornost sistema.

Z uvedbo standarda IEC 61850 v avtomatizacijo transformatorskih postaj ter uporabo komunikacije prek Ethernet/IP v stikalnih napravah, nadzornih centrih se je pojavila potreba po spremljanju in zaščiti teh komunikacijskih omrežij. Cilj je analizirati vse podatkovne povezave v procesnem omrežju, da se hitro odkrijejo morebitni napadi, zlonamerno vedenje ali napake v delovanju, in da se pravočasno sprožijo ustrezni protiukrepi. To je še posebej pomembno za vzdrževalce in operaterje elektroenergetskih omrežij in sistemov, ki so opredeljeni kot del kritične infrastrukture.

Za učinkovito spremljanje teh okolij mora biti IDS prilagojen za razumevanje OT protokolov, kot sta IEC 60870-5-104, IEC 61850 in podobni. Prav tako mora biti sposoben prepoznati funkcije posameznih sredstev znotraj sistemov SCADA (Supervisory Control and Data Acquisition), nadzornih centrov. Takšna prilagoditev zagotavlja, da je IDS natančno usklajen z zahtevami teh kritičnih okolij in omogoča zanesljivo zaznavanje groženj.

4.1 IDS platforma

Procesi korelacije, agregacije in alarmiranja v IDS morajo delovati samostojno, brez potrebe po povezavi z višje-nivojskim strežnikom znotraj Purdue modela. Te funkcije morajo delovati neposredno na gostiteljski platformi, kjer se zbira celoten omrežni promet. Tak pristop zagotavlja, da IDS ostane učinkovit pri zaznavanju groženj ne glede na stanje višjih omrežnih ravni.

V primeru prekinitve povezave med IDS platformo in nadzornimi strežniki mora IDS ohraniti sposobnost samostojnega spremljanja vseh dogodkov ter jih zapisovati v dnevnike, s čimer se zagotovi neprekinjeno zaznavanje groženj in beleženje dogodkov.

4.1.1 *Strojna platforma*

Strojne platforme IDS so zasnovane za uporabo v zahtevnih industrijskih okoljih in morajo strogo upoštevati industrijske standarde, kot sta IEC/EN 61850-3 in IEEE 1613. Izpolnjevanje teh standardov je ključno za zagotavljanje zanesljivega in robustnega delovanja v industrijskih pogojih.

Poleg tega mora biti strojna platforma zasnovana tako, da omogoča enostavno namestitev v 19 inčni strežniški okvir ali na DIN letev, kar zagotavlja prilagodljivost pri montaži in združljivost z različnimi konfiguracijami industrijske infrastrukture. Tako se omogoča brezhibna integracija IDS strojne opreme v različna industrijska okolja ob hkratnem zagotavljanju skladnosti z bistvenimi standardi za operativno zanesljivost in zmogljivost.

Za večjo prilagodljivost v različnih delih omrežja naj IDS vključuje možnost mobilne platformo, ki omogoča enostavno začasno uporabo.

Strojna platforma IDS mora imeti binarne I/O kontakte za spremljanje delovanja nadzornega mehanizma (watchdog) opreme ter za obveščanje zunanjih sistemov v primeru sproženih alarmov.

Za učinkovito spremljanje omrežja mora imeti platforma najmanj osem namensko dodeljenih vmesnikov za spremljanje prometa (Switched Port Analyzer-SPAN). To zagotavlja popolno pokritost in omogoča poglobljeno analizo omrežnega prometa za namene diagnostike in odpravljanja napak.

Vsak vmesnik mora podpirati povezave RJ45 ali FOB. IDS platforma mora imeti tudi namenski krmilni vhod za upravljanje IDS aplikacije.

Vsaj ena različica strojne platforme mora imeti redundantno napajanje z možnostjo uporabe DC ali AC napetosti. Poleg tega morajo biti izpolnjene naslednje zahteve:

4.1.1.1 *Skladnost*

Izjava o skladnosti (EU)

4.1.1.2 *Splošni standardi*

IEC/EN 1850-3
IEEE 1613

4.1.1.3 *Elektromagnetne motnje (EMI)*

Evropa: EN 61326, EN 60255-26; EN 61000-6-4; EN 55032, razred A

Mednarodno: IEC 61326-1; IEC 60255-26; IEC 61000-6-4; CISPR 32, razred A

4.1.1.4 *Elektromagnetna odpornost (EMS) / raven imunosti*

Evropa: EN 61326-1; EN 60255-26; EN 61000-6-2; EN 61000-6-5

Mednarodno: IEC 61326-1; IEC 60255-26; IEC 61000-6-2; IEC 61000-6-5

4.1.2 *Virtualna platforma*

V nekaterih konfiguracijah omrežja je mogoče IDS virtualizirati, da se zagotovi združljivost in učinkovita uvedba v različnih okoljih. Virtualizacija omogoča tudi hitro obnovitev sistema z uporabo posnetkov stanja (snapshots).

4.1.3 *Licence / Programska oprema*

Rešitev mora biti podprta s pogodbo o vzdrževanju, ki zagotavlja 24/7 tehnično podporo. Garancija naprave mora veljati ves čas trajanja servisne pogodbe. V primeru napak v garancijskem obdobju morajo biti te odpravljene v okviru garancijskega zahtevka.

Ponudnik se zavezuje, da bo zagotovil najmanj dve uradni posodobitvi programske opreme na leto, s čimer se izboljšuje delovanje celotne rešitve in odpravlja morebitne napake.

Ponudnik naj redno posreduje informacije o varnostnih posodobitvah (security patches), ki takoj odpravljajo ranljivosti in povečujejo odpornost sistema IDS proti morebitnim grožnjam.

4.2 Konfiguracija

4.2.1 *Vizualizacija*

Alarmi, ki jih sproži varnostni sistem, morajo procesnemu inženirju pomagati pri odkrivanju težav in ne povzročati dodatne zmede. Zato se alarmi IDS ne smejo prikazovati samo kot seznam dogodkov, temveč morajo biti grafično prikazani tudi v preglednih diagramih. Dogodki v elektroenergetskem sistemu, ki povzročijo omrežni promet, morajo biti prepoznani in prikazani z jasno in razumljivo terminologijo.

4.2.1.1 *Uporaba SCD datotek*

Datoteke SCD (Substation Configuration Description), po standardu IEC61850 vsebujejo procesne informacije o postaji, kot na primer enopolno shemo postaje in pripadajoče krmilno zaščitne komponentame (IED ipd.). IDS mora imeti možnost uporabe SCD datotek.

Ta funkcionalnost deluje kot vizualizacija postaje ter omogoča jasen pregled nad medsebojnimi povezavami različnih delov omrežja. Zaradi tega imajo procesni inženirji razumljiv in boljši vpogled v delovanje sistema in ga lažje upravljajo.

4.2.1.2 *Grafično urejen omrežni diagram*

Diagram IDS mora biti dovolj prilagodljiv, da ustreza potrebam uporabnikov. Uporabnikom mora omogočati ustvarjanje Purdue modela v diagramu ter razvrščanje naprav v posamezne ravni ali skupine.

4.2.2 *Profili sredstev in pravila*

4.2.2.1 *Vnaprej določeni in prilagodljivi profili za OT naprave*

Vsako zaznano sredstvo mora biti označeno s posebnim profilom, ki predstavlja funkcijo tega sredstva. Dodeljeni profili morajo biti prilagodljivi, kar pomeni, da jih je mogoče definirati kot uporabniško določene profile naprav.

IDS mora biti sposoben analizirati vedenjske vzorce vsakega aktivnega sredstva v omrežju. Poleg preprostega imenskega prepoznavanja mora sistem znati predlagati najprimernejši profil za posamezno sredstvo glede na njegovo zaznano vedenje.

4.2.2.2 *Vnaprej določena in prilagodljiva pravila*

Za poenostavitev postopka konfiguracijo in zagotavljanja prepoznavanja uveljavljenih komunikacijskih vzorcev za določena sredstva, mora imeti vsak profil znotraj IDS vnaprej določen nabor dovoljenj in pravil za tipične naprave v elektroenergetskem omrežju.

IDS mora imeti predefinirane profile z naborom dovoljenj, hkrati pa mora uporabnikom omogočati, da jih po potrebi prilagodijo. Tako se doseže ravnovesje med učinkovitostjo (vnaprej določene nastavitve) in prilagodljivostjo (uporabniške spremembe).

Vse spremembe profilov in dovoljenj morajo biti zabeležene v dnevniku.

4.2.2.3 *Prenos komunikacijskih profilov med senzorji*

Sistem mora omogočati možnost kopiranja komunikacijskih profilov določenega tipa sredstva na druge senzorje, da se prepreči ponavljanje istih lažnih alarmov v več objektih. Zato mora IDS uporabnikom omogočati migracijo prilagojenih pravil na drug senzor.

4.2.3 *Varnostno kopiranje*

Senzor IDS mora shraniti celotno konfiguracijo, vključno s profili, pravili, zaznanimi sredstvi, vpisi v dnevnik, Purdue modelom in strojno konfiguracijo. Uporabniki morajo imeti po potrebi možnost obnovitve teh konfiguracij na kateremkoli senzorju.

4.2.4 *Vzdrževanje*

Vzdrževalne aktivnosti v procesnih OT okoljih, kot so vzpostavljanje povezav s sredstvi, spreminjanje konfiguracij, prenos datotek ali odpravljanje napak, se lahko izvajajo redno ali občasno. Vendar pa lahko takšna dejanja sprožijo lažne pozitivne alarme, saj odstopajo od običajnega operativnega prometa in vedenja.

Da bi se to preprečilo, mora IDS imeti možnost obvladovanja (izločanja, blokiranja) v vnaprej določenih vzdrževalnih obdobjih, s čimer se zmanjša verjetnost lažnih alarmov.

4.2.5 *Namestitev in posodabljanje programske opreme*

Programska oprema IDS mora omogočati namestitev v okolju brez internetne povezave (offline). Datoteke za posodobitev mora biti mogoče ročno naložiti (t. i. offline update). Posodobitve ne smejo zahtevati internetne povezave.

Posodobitve programske opreme (firmware) morajo biti podpisane s certifikatom in šifrirane z vsaj SHA-512 ali primerljivim algoritmom.

4.2.6 *Sinhronizacija časa*

Programska oprema mora podpirati sinhronizacijo s časovnim strežnikom z uporabo Network Time Protocol (NTP), da se zagotovi natančno časovno označevanje dogodkov (timestamping).

4.3 Zaznavanje

4.3.1 *Zaznavanje in nadzor vdorov*

Avtomatizacija elektroenergetskih sistemov in SCADA sistemi so deterministični, kar pomeni, da je njihovo vedenje jasno določeno tudi v izjemnih situacijah, npr. med dogodki, ki jih sprožijo zaščitne funkcije. Te lastnosti je potrebno uporabiti pri pristopu zaznavanja kibernetskih napadov, ki temelji na poznavanju narave delovanja sistemov v postaji.

Ker IDS mora poznati funkcijo vsake naprave, mora biti izdelan seznam dovoljenih dejanj (allow list ali whitelist), kjer so opisane vse dovoljene aktivnosti, medtem ko vsako odstopanje od tega sproži alarm.

IDS mora biti sposoben prepoznati aplikacije in storitve, ki jih uporablja uporabnik, da lahko analizira zajeti promet.

4.3.1.1 *Zaznavanje s podpisom (Signature detection)*

IDS naj bo med drugim zasnovan za zaznavanje in sprožanje alarmov pri znanih kibernetskih napadih, a ne omejeno na: port scanning, ARP spoofing, SYN flooding.

V IDS naj bo možno konfigurirati indikatorje kompromitiranosti (Indicator of Compromise-IoC) za prepoznavanje zlonamernih dejavnosti. Ponudnik naj predstavi rešitev za uporabo in zaznavanje IoC.

4.3.1.2 *Zaznavanje anomalij (Anomaly detection)*

IDS mora prepoznavati nepravilnosti, vključno z odkrivanjem tipičnih dejavnosti, kot so:

- zlorabe računalnikov,
- IED (Intelligent Electronic Devices),
- stikal (switches),
- RTU (Remote Terminal Units),
- HMI (Human-Machine Interfaces).

Spremljanje odstopanj od običajnega vedenja teh ključnih komponent je bistvenega pomena za zagotovitev celovitega zaznavanja groženj.

4.3.1.3 *Neobičajno kodiranje protokolov*

IDS mora ne le zaznavati uporabljene protokole, temveč tudi preverjati njihovo celovitost in veljavnost. Tak pristop omogoča temeljit pregled vseh identificiranih protokolov ter potrjuje, da izpolnjujejo pričakovane standarde in ne kažejo znakov kompromitiranja ali manipulacije.

4.3.1.4 *Predkonfiguracija IDS*

Konfiguracija IDS mora biti pripravljena vnaprej glede na funkcije sredstev, uporabljenih protokolov in konfiguracijskih datotek, kot so IEC 61850 SCL in CSV.

Datoteke SCD (Substation Configuration Description) v skladu s standardom IEC 61850 vsebujejo podatke o konfiguraciji in komunikaciji v procesnih omrežjih. IDS mora te SCD datoteke uporabiti za samodejno ustvarjanje celotnega seznama dovoljenih dejavnosti (allow list) za vse naprave, opisane v SCD.

SCD datoteke se ne smejo uporabljati zgolj za identifikacijo sredstev, temveč tudi za ustvarjanje seznama dovoljenih komunikacij. Ta proces mora biti zasnovan tako, da zmanjša pojav lažnih alarmov, saj so v datotekah SCD že opisana vsa dovoljena vedenja naprav.

Podprti morajo biti naslednji formati: IEC 61850-6 ed.1, ed.2 in ed.2.1, vključno z datotekami: *.SCD, *.IID, *.ICD.

4.3.1.5 *Pregled aktivnega omrežja (Live network overview)*

IDS mora omogočati vizualizacijo aktivnih komunikacij v ločenem prikazu omrežja, da se prikažejo vsi aktivni udeleženci in uporabljeni protokoli.

Kdo komunicira s kom:

- naprave so predstavljene kot vozlišča (nodes),
- komunikacijski tokovi so prikazani kot povezave (lines),
- sistem mora omogočati vizualizacijo vseh vozlišč in protokolov, ki sodelujejo v komunikaciji z izbranim vozliščem.

Kaj se komunicira:

- prikazati mora seznam protokolov, ki se uporabljajo v omrežju (npr. HTTP),
- zaznati mora aktivne komunikacije,
- omogočati mora pregled stanja omrežja za določen čas v preteklosti (npr. pred nekaj urami).

Situacijsko zavedanje (Situational Awareness):

- nadzorna plošča v realnem času (real-time dashboard) mora prikazovati ne le, kaj se je zgodilo, temveč tudi kje, kdaj in kako,
- omogočiti mora prioritizacijo alarmov glede na resnost vpliva na omrežje

4.3.2 *Zaznavanje napak in konfiguracijskih nepravilnosti*

IDS mora biti sposoben zaznati kibernetske grožnje in prepovedana dejanja v sistemih za avtomatizacijo elektroenergetskih omrežij in v SCADA omrežjih. Poleg tega mora imeti zmožnost obveščanja o kritičnih dogodkih in okvarah, kot so:

- odpovedi IED naprav,
- napake v konfiguraciji,
- težave s sinhronizacijo časa,
- omrežne napake.

Sistem mora te dogodke beležiti (logirati) za kasnejšo analizo. Poleg tega morajo biti vsi prenosi datotek zabeleženi z imenom datoteke, na primer pri prenosu oscilografij (disturbance records).

Ključno je, da IDS pozna in spremlja spremembe v GOOSE sporočilih, da lahko pravočasno zazna morebitne funkcionalne težave. Ker so GOOSE sporočila vedno prisotna v omrežju, jih je mogoče uporabiti tudi za diagnostične in funkcionalne nadzorne namene.

4.3.2.1 *Spremljanje GOOSE komunikacije*

4.3.2.1.1 Zaznavanje podvojenih telegramov in napak v zaporedju

Protokol GOOSE v vsakem telegramu vključuje statusno oznako in sekvenčno številko. V primeru nepravilnega prenosa GOOSE mora sistem omogočati zaznavo napak v zaporedju telegramov. Poleg tega mora nujno spremljati izvorni MAC naslov vsakega telegrama.

4.3.2.1.2 Zaznavanje manjkajočih GOOSE paketov

Če pride do izpada ponavljajočih se telegramov, mora sistem sprožiti alarm. To lahko pomeni, da je omrežje preobremenjeno. Manjkajoči telegrami, ki bi morali vsebovati spremembo statusa, se morajo obravnavati kot resna težava.

4.3.2.1.3 Zaznavanje napak sinhronizacije časa prek GOOSE

GOOSE telegrami vsebujejo časovni žig (timestamp), ki označuje zadnjo spremembo statusa. Če ima pošiljajoči IED naprava okvarjeno sinhronizacijo časa, mora sistem to prepoznati in ustrezno ukrepati — pod pogojem, da je sam sistem pravilno časovno sinhroniziran (glej točko 4.3.2.1.4).

4.3.2.1.4 Zaznavanje časovnega izpada GOOSE (GOOSE timeout detection)

Če IED naprava preneha komunicirati, se to mora odraziti kot izpad (timeout) GOOSE signala iz te naprave. To mora povzročiti sprožitev kritičnega alarma.

4.3.2.1.5 Zaznavanje simuliranih GOOSE sporočil (simulated GOOSE packets)

IDS mora zaznati GOOSE sporočila, ki imajo značko simulirano.

4.3.2.2 *Spremljanje komunikacije vzorčenih vrednosti (Sampled Values - SV)*

4.3.2.2.1 Zaznavanje osirotelih SV paketov

IDS mora omogočati zaznavo neznanih/osirotelih SV paketov, ki niso konfigurirani v SCL.

4.3.2.2.2 Zaznavanje manjkajočih SV paketov

IDS mora omogočati zaznavo manjkajočih SV, ki so konfigurirani v SCL.

4.3.2.2.1 Zaznavanje zavrženih SV paketov

IDS mora omogočati zaznavo zavrženih SV, to so SV, ki so bili prisotni vendar so izginili iz različnih razlogov, težave z omrežjem, odstranjena oprema.

4.3.2.2.1 Zaznavanje simuliranih SV paketov

IDS mora zaznati SV sporočila, ki imajo značko simulirano.

4.3.3 *Identifikacija sredstev*

Vsa aktivna sredstva, ki komunicirajo v omrežju, mora IDS identificirati in spremljati. Ti podatki morajo biti na voljo za izvoz iz IDS. Zbrani morajo biti naslednji podatki o sredstvih:

Pasivno odkrivanje (Passive Discovery) temelji na:

- IP naslov
- MAC naslov

Dodatne informacije o sredstvih je mogoče pridobiti z uporabo SCL datoteke kot konfiguracijske osnove (za naprave/sisteme IEC 61850):

- Naziv po standardu IEC 61850
- Proizvajalec naprave
- Model naprave
- Serijska številka
- Različica strojne opreme (Hardware version)
- Različica programske opreme (Software version)

Za identifikacijo sredstev z uporabo drugih inženirskih datotek, kot je CSV, mora IDS omogočati, da se manjkajoči podatki o sredstvih vnesejo ročno.

Aktivna poizvedovanja z uporabo MMS:

- Naziv po standardu IEC 61850 - IEC 61850 Name
- Proizvajalec naprave - Device manufacturer
- Model naprave - Device model

- Serijska številka - Serial number
- Različica strojne opreme - Hardware version
- Različica programske opreme - Software version

4.3.4 *Zaznavanje ranljivosti*

Za prepoznavanje morebitnih tveganj je bistveno, da sistem omogoča zaznavanje ranljivosti v procesnih okoljih. Rešitev mora prav tako omogočati stalno preverjanje ranljivosti in sredstev, da se odkrijejo potencialne grožnje v sistemski infrastrukturi.

Postopek zaznavanja mora vključevati celovito analizo možnih ranljivosti, pri čemer je treba upoštevati različne dejavnike, kot so:

- proizvajalci naprav,
- tipi naprav in družine produktov,
- različice programske opreme (firmware).

Za optimalno delovanje mora IDS omogočati integracijo varnostnih obvestil (security advisories) v obliki PDF datotek za zaznane ranljivosti. Za oceno tveganja mora biti na voljo CVSS (Common Vulnerability Scoring System) ocena.

Ko so vsi potrebni podatki zbrani, mora biti postopek zaznavanja ranljivosti popolnoma avtomatiziran. Proces mora potekati brez potrebe po ročnem posredovanju, če so podatki o sredstvih dovolj popolni. S tem se zagotovi učinkovito in pravočasno prepoznavanje ranljivosti, brez odvisnosti od ročnih postopkov.

Poleg tega mora uporabnik imeti možnost, da vsako prizadeto sredstvo upravlja individualno, tako da določi rešitve (resolutions) za posamezne zaznane ranljivosti.
Te rešitve predstavljajo ukrepe, sprejete kot odziv na ranljivosti, in določajo status odprave (remediation status), ki sledi napredku izbranega ukrepa.

Uporabnikom mora biti omogočeno tudi skupinsko izvajanje rešitev (bulk resolutions) za vsa sredstva, ki jih prizadene ista ranljivost (npr. CVE-xxxx).

4.3.5 *Podprti omrežni protokoli*

IDS mora podpirati analizo spodaj navedenih protokolov. To so minimalne zahtevane zmogljivosti zaznavanja:

Alarmi za protokole IEC 60870-5-104 in IEC 61850 MMS, GOOSE morajo biti prikazani v jasnem in poenostavljenem besedilu, enostavno berljiv procesnim inženirjem. IDS mora biti sposoben prepoznati uporabljen protokol v povezavi, neodvisno od TCP/UDP številk vrat. Še posebej pri OT protokolih, uporabljenih v elektroenergetskem omrežju, je nujno, da se to zaznavanje lahko

izvede brez ponovnega vzpostavljanja TCP povezave. Poleg tega mora IDS omogočati, da se v seznam dovoljenih aktivnosti (allow list) vključijo tudi storitve in aplikacije, ki delujejo na 7. sloju OSI modela.

OT protokoli

- IEC 61850 MMS, GOOSE
- IEC 62439-3 PRP
- IEC 62439-3 HSR with RedBox
- IEC 60870-5-104
- DNP3
- Modbus TCP
- IEC 62056 (DLMS/COSEM)
- IEEE C37.118 (synchrophasor protocol)
- IEEE 1703-2012 / ANSI C12.22 (AMI protocol)
- IEC 60870-6 (ICCP/TASE.2 – UCA 2.0)

IT protokoli

- FTP
- http
- HTTPS (brez dešifriranja, vendar z zaznavo aplikacij)
- RDP
- NTPNetBIOS (Windows file sharing) – NetBIOS (souporaba datotek v okolju Windows)
- ARP – Address Resolution Protocol
- DHCP – Dynamic Host Configuration Protocol
- MySQL – MySQL podatkovna baza
- MSSQL – Microsoft SQL Server
- PostgreSQL – PostgreSQL podatkovna baza
- SSH (without decryption but with application detection) – SSH (brez dešifriranja, vendar z zaznavo aplikacij)
- telnet – Telnet protokol
- ICMP / ICMPv6 – Internet Control Message Protocol / Internet Control Message Protocol v6
- RIPv2 – Routing Information Protocol Version 2
- SSDP – Simple Service Discovery Protocol
- MDNS – Multicast DNS

4.3.6 *Podpra PCAP datotekam*

Rešitev IDS mora vključevati funkcijo, ki omogoča predvajanje predhodno posnetega omrežnega prometa (datotek PCAP) za namene testiranja, validacije in forenzične analize. Vsako odstopanje, zaznano med predvajanjem, mora sprožiti opozorilo, ki je enako opozorilu, ki ga je sprožilo spremljanje v živo. Takšna opozorila morajo biti označena z »PCAP/Simulacija«, da se zagotovi sledljivost in loči simulirana zaznavanja od incidentov v omrežju.

4.4 Dogodki (Events)

Vsi dogodki, ki jih zazna IDS, morajo biti zabeleženi v sistemu. Uporabniku mora bit na voljo prijazni vmesnik, ki ponuja različne možnosti filtriranja.
To omogoča enostavno iskanje specifičnih dogodkov.

Poleg tega mora biti vsak dogodek kategoriziran glede na stopnjo kritičnosti.

4.4.1 *Analiza*

Rešitev IDS mora uporabnikom omogočati izvoz dogodkov v formatu CSV ali PDF. Vsak alarm mora vključevati podatke v pcap formatu, ki jih je mogoče prenesti za nadaljnjo analizo.

Vsak sprožen alarm ali dogodek, ki ga zazna IDS, mora vsebovati minimalno naslednje podatke (če so konfigurirani in se uporabljajo):

- Izvorni in ciljni IP/MAC naslov
- Časovni žig (Timestamp)
- Številko vrat in transportni sloj (če se uporablja)
- Aplikacijski sloj in storitev (če se uporablja)
- VLAN ID in prioriteto (če se uporablja)
- Status povezave (če se uporablja)

Pomembno je, da se kritične aktivnosti, kot so krmilni ukazi (switching commands) ali prenosi datotek, beležijo tudi po tem, ko so bile dovoljene.

4.4.2 *Združevanje dogodkov*

Združeni alarm (aggregated alarm) je alarm, ki združuje več napak iste vrste in med istim parom izvor–cilj, ter procesnemu inženirju olajša reševanje okvare. Na primer: če se IED poveže z drugim IED, se sproži aktivni združeni TCP alarm, ki lahko vsebuje več kršitev TCP, saj lahko naprava pošlje več TCP paketov drugemu IED.

4.4.3 *Izguba komunikacije s centralnim upravljalnim sistemom*

V primeru, da senzor izgubi povezavo s centralnim sistemom za upravljanje, mora IDS sistem delovati na sledeč način:

''Alarmi morajo biti shranjeni na senzorju najmanj tri dni (priporočeno več) in se morajo samodejno prenesti v upravljalni sistem, takoj ko se povezava ponovno vzpostavi. Alarme je treba omogočiti analizirati neposredno na senzorju (senzor bere promet, omogočen mora biti lokalni dostop in konfiguracija), tudi brez povezave z upravljalnim sistemom.''

4.5 Centralno upravljanje

Celotno IDS okolje mora zagotavljati centralni sistem za upravljanje, kjer je uporabniku na voljo lista senzorjev in njihovi podatki. Ta sistem mora uporabnikom omogočati, da lahko na enem mestu upravljajo svoje procesno okolje z vidika obvladovanja kibernetskih tveganj.

V primeru, da se katerikoli del nadzornega sistema (zbiranje podatkov, prikazi,…) nahaja izven notranjega varovanega okolja je zahtevana uporaba podatkovnega prehoda med varnostnimi conami (proxy).

4.5.1 *Centralno upravljanje senzorjev*

Vsak senzor mora imeti možnost povezave s centralnim sistemom za upravljanje. Ta centralni sistem mora omogočati nadzor nad vrsto informacij o senzorju, vključno z:

- statusom povezave senzorja,
- številom alarmov,
- zaznanimi ranljivostmi,
- različico programske opreme (firmware) senzorja,
- različico strojne opreme (hardware) senzorja,
- in imenom senzorja samega.

4.5.2 *Centralni dnevnik dogodkov*

Vsi dogodki in alarmi, zbrani iz več senzorjev, morajo biti prikazani v centralnem dnevniku dogodkov. Dnevnik dogodkov mora omogočati uporabo inteligentnih in prilagodljivih nadzornih plošč (dashboards) za podrobnejšo analizo.

Poročanje prek centralnega dnevnika dogodkov mora biti omogočeno najmanj v obliki PDF poročil in po elektronski pošti (email).

4.5.3 *Centralni inventar sredstev*

Vsa sredstva, ki jih zaznajo senzorji, morajo biti zbrana na centralni lokaciji, kjer lahko uporabniki do njih dostopajo prek enotne točke. Centralni inventar sredstev mora omogočati uporabo inteligentnih in prilagodljivih nadzornih plošč, ki omogočajo dodatno analizo.

Inventar sredstev mora biti mogoče izvoziti najmanj v obliki CSV ali PDF poročil.

4.5.4 *Usklajevanje varnostnih obvestil z inventarjem sredstev*

Centralni upravljalni sistem mora združevati vsa ujemanja ranljivosti in jih vizualno prikazovati za vsako posamezno sredstvo.

Postopek zaznavanja mora vključevati celovito analizo morebitnih ranljivosti, pri čemer je treba upoštevati naslednje dejavnike:

- proizvajalce naprav,
- tipe naprav in družine produktov,
- različice programske opreme (firmware).

Za optimalno delovanje mora IDS omogočati integracijo varnostnih obvestil (security advisories) v obliki PDF datotek za zaznane ranljivosti. Za oceno tveganja mora biti na voljo CVSS (Common Vulnerability Scoring System) ocena.

4.5.5 *Baza podatkov o ranljivostih in varnostnih obvestilih*

Ker naprave in sistemi v okoljih kritične infrastrukture niso povezani v svetovni splet, mora biti baza podatkov posodobljena brez internetne povezave (offline). Tak pristop povečuje varnost sistema, saj omejuje dostop do zunanjih omrežij.

Uporabnikom mora biti omogočeno ročno iskanje ranljivosti znotraj baze podatkov.

Baza mora vključevati vsaj varnostna obvestila vodilnih proizvajalcev relejev in omrežnih stikal, kot so na primer: SIEMENS, Hitachi Energy, Cisco, ABB, Ruggedcom, Moxa, Fortinet in ostali

4.5.6 *Upravljanje z ranljivostmi in izpostavljenostjo*

Centralni sistem upravljanja IDS mora vključevati celovit modul za upravljanje z ranljivostmi in izpostavljenostjo, ki uporabnikom omogoča sledenje in upravljanje ranljivosti, ugotovljenih v vseh nadzorovanih sredstvih.

Sistem mora procesnim inženirjem odgovornim za kibernetsko varnost omogočiti, da pregledajo vsako prizadeto sredstvo posebej in določijo ustrezno rešitev za vsako ugotovljeno

ranljivost. Vsaka rešitev mora predstavljati določen odzivni ukrep (npr. popravljanje, blaženje ali sprejemanje tveganja) in določiti stanje sanacije, ki odraža trenutni napredek izbranega ukrepa.

Uporablja naj se koncept skupinskega upravljanja (bulk resolution) za sredstva, ki jih je prizadela ista ranljivost. Tako, da se poenostavi postopek sanacije.

Za podporo učinkovitemu odločanju mora rešitev zagotavljati povzetek pregleda vseh zaznanih CVE, vključno z ocenami resnosti, odkritimi ponudniki in vplivom na sredstva. Za lažjo podrobno analizo mora sistem omogočati dostop do celovite dokumentacije o ranljivostih v obliki obvestil v obliki PDF. Pri tem je potrebno upoštevati specifike izoliranih okolij (air-gapped).

Modul za upravljanje ranljivosti mora podpirati naslednja stanja rešitev:

- Nerešeno (Unresolved): Nobena rešitev ni bila opredeljena ali uporabljena. Ranljivost ostaja aktivno tveganje.
- V preiskavi (Under investigation): Ranljivost se analizira, da se določi njen vpliv in ustrezna strategija sanacije.
- Lažno pozitiven (False positive): Zaznavanje ranljivosti je bilo potrjeno kot napačno.
- Ni relevantno (Not applicable): Ranljivost se ne nanaša na konfiguracijo sredstva ali nameščeno programsko opremo.
- Ni prizadeto (Not affected): Preverjeno je, da ranljivost sredstva ne vpliva.
- Tveganje sprejeto (Risk accepted): Tveganje je priznano in sprejeto, običajno zaradi upravičenih operativnih omejitev.
- Ublažitev v teku (Mitigation pending): Ukrepi za ublažitev so bili načrtovani, vendar še niso izvedeni.
- Ublaženo (Mitigated): Vpliv ranljivosti je bil zmanjšan z ustreznimi kontrolami.
- Popravek v teku (Patch pending): Popravek prodajalca je na voljo, vendar še ni nameščen.
- Popravljeno (Patched): Ranljivost je bila v celoti odpravljena z namestitvijo popravka.
- Odloženo (Deferred): Odprava je odložena, na primer zaradi omejitev virov ali nizke izkoriščenosti.

Stanje sanacije mora biti samodejno preslikano v naslednje kategorije za poenostavljeno poročanje:

- Odprto (Open): Nerešeno, Odloženo
- V teku (Pending): V preiskavi, V teku je blažitev, V teku je popravek
- Rešeno (Resolved): Lažno pozitivno, Ni relevantno, Ni prizadeto, Tveganje sprejeto, Ublaženo, Popravljeno

Sistem mora zagotoviti podroben pregled vsakega ujemanja z ranljivostmi, vključno s korelacijo sredstev, logiko ujemanja in sklicevanjem na izvorno obvestilo. To uporabnikom omogoča razumevanje in preverjanje postopka zaznavanja.

4.5.7 *Uporabniki*

4.5.7.1 *Dostop uporabnikov*

IDS mora omogočati konfiguracijo in vzdrževanje senzorjev prek dveh vmesnikov:

- spletnega brskalnika za enostaven dostop uporabnikov,
- in odjemalske programske opreme (client software) za bolj prilagojeno in napredno uporabniško izkušnjo.

4.5.7.2 *Avtentikacija*

Centralni upravljalni sistem mora podpirati različne metode avtentikacije za prijavo in administracijo sistema, pri čemer mora biti LDAP/Active Directory osnovna zahtevana metoda preverjanja pristnosti.

Zahtevano je, da sistem podpira večfaktorsko avtentikacijo (multi-factor authentication).

4.5.7.3 *RBAC (Role-Based Access Control)*

Vsaka uporabniška povezava prek upravljalnega sistema — ne glede na to, ali je avtenticirana prek LDAP ali ne — mora biti povezana z vlogo (role), ki določa in omejuje obseg uporabniškega dostopa in nadzora.

4.5.7.4 *Upravljanje uporabnikov*

Rešitev mora omogočati ročno dodajanje, spreminjanje in odstranjevanje uporabnikov ter določanje njihovih vlog in pravic prek centralnega upravljalnega sistema.

4.5.8 *Varnostno kopiranje sistema*

Uporabnikom mora biti omogočeno ustvarjanje varnostne kopije sistema, kar omogoča povrnitev na prejšnjo konfiguracijo, če je to potrebno. Ta funkcionalnost zagotavlja zanesljiv mehanizem za obnovitev sistema v primeru napak ali izgube podatkov.

4.5.9 *Posodobitve senzorjev*

Posodobitve morajo biti možne prek centralnega upravljalnega sistema. Poleg tega mora biti omogočeno tudi daljinsko posodabljanje vdelane programske opreme (firmware).

4.6 Integracija s sistemi tretjih ponudnikov (Third-party integration)

Za izboljšanje celovitosti in integracije cyber-varnostnih sistemov mora IDS omogočati neprekinjeno integracijo s sistemi tretjih ponudnikov.

4.6.1 *Integracija s SIEM sistemi (SIEM integration)*

IDS mora omogočati pošiljanje syslog sporočil, razvrščenih po dogodkih, na SIEM strežnike. Priporočen standard za syslog sporočila je Common Event Format (CEF).

Poleg tega mora IDS zagotavljati vtičnike (plugins), prilagojene različnim SIEM rešitvam.

4.6.2 *Integracija s SCADA sistemi (SCADA Integration)*

IDS mora zagotavljati različne možnosti integracije s SCADA sistemi, pri čemer mora izpolnjevati osnovno zahtevo po oddaji binarnega izhoda prek strojne rešitve, ki omogoča takojšnje obveščanje SCADA sistema v primeru varnostnega incidenta.

Dodatna možnost integracije je tudi povezava SCADA sistemov z uporabo OT protokolov, kot je MMS.

5. Ne-funkcionalne zahteve

5.1 Kibernetska varnost izdelka

5.1.1 *Certifikacija*

Certifikat na področju kibernetske varnosti omogoča proizvajalcem, da njihove varnostne izjave o izdelku potrdi neodvisen organ.

Ponudnik IDS mora imeti veljaven kibernetski certifikat za različico programske opreme izdelka (firmware). Primer: BSI certifikat, ki velja v EU.

5.1.2 *Varni razvoj programske opreme*

Secure Software Development Life Cycle (SSDLC) opisuje strukturiran proces, ki obsega več faz z namenom zagotavljanja dosledne uporabe varnostnih ukrepov in najboljših praks pri razvoju vseh izdelkov.

Pred začetkom faze razvoja morajo biti ocenjeni vsi organizacijski vidiki, vključno s kontekstom kibernetske varnosti in kritičnostjo izdelka za poslovanje.

Med razvojem izdelka je treba izvesti modeliranje groženj (threat modeling), da se v zgodnji fazi življenjskega cikla izdelka prepoznajo potencialne kibernetske grožnje.

Varnostno testiranje (security testing) je bistvena sestavina razvoja vsakega kibernetskovarnostnega izdelka. Njegov namen je preveriti, ali so bile izpolnjene določene varnostne zahteve in ali je bil dosežen ustrezen nivo zaščite. Takšni testi se običajno načrtujejo in izvajajo s strani ekipe za zagotavljanje kakovosti (quality assurance team).

5.1.3 *Varni kriptografski procesor*

Naprava mora vsebovati ločeno integrirano vezje: Trusted Platform Module (TPM 2.0), ki je skladen s standardom ISO/IEC 11889. Ta integrirano vezje je odgovorno za varno ustvarjanje in shranjevanje varnostnih certifikatov, kot tudi za podporo varnemu zagonu sistema (secure boot).

Določeni certifikati se morajo na to integrirano vezje naložiti med varnim proizvodnim postopkom, s čimer se zagotovi visoka raven varnosti in zanesljivosti sistema.

5.1.4 *Varni zagon in nadzorovan zagon*

Vmesnik mora podpirati varni zagon (secure boot), ki predstavlja mehanizem za zagotavljanje celovitosti zagonskega procesa naprave. Varni zagon in nadzorovan zagon (measured boot) sta dva ključna mehanizma, ki omogočata preverjanje, ali so se ob zagonu naložile le zaupanja vredne in avtorizirane komponente.

5.1.5 *Šifriranje diska*

Vsi kritični podatki v sistemu IDS morajo biti šifrirani in jih lahko dešifrira samo naprava, kateri so dodeljeni (full disc encryption). Ključ, uporabljen za šifriranje podatkov, mora biti ustvarjen znotraj kriptografskega čipa v senzorju IDS.

5.1.6 *Varni dostop za podporo in servisne namene*

Vgrajena programska oprema (firmware) in strojna oprema (hardware) ne smeta vsebovati privzetih gesel ali drugih stranskih vrat (backdoors).

Dostop do senzorja za potrebe vzdrževanja ali servisiranja mora biti omogočen samo začasno. Seja se mora samodejno prekiniti po ponovnem zagonu. Poleg tega mora biti takšen dostop mogoč izključno z fizičnim posegom (na primer: s pritiskom na ustrezen gumb).

6. Reference

6.1 Reference produkta in proizvajalca

Ponudnik mora kot referenco navesti vsaj 3 projekte kjer je bila uporabljena ponujena oprema. Proizvajalec in projekti morajo ustrezati sledečim kriterijem:

- Z uporabo produkta je izveden vpogled v komunikacijska omrežja transformatorske postaje in SCADA z popisom sredstev in vizualizacijo omrežne komunikacije.
- Podrobna analiza OT protokolov, ki se uporabljajo distribucijskih omrežjih v Evropi (npr. IEC 60870-5-104, IEC 61850, IEC 60870-6, MODBUS) za potrebe odkrivanje kibernetskih vdorov in komunikacijskih anomalij.
- Uporaba SCL datoteke po standardu IEC 61850 v smislu začetne konfiguracije sistema (faza učenja) in zmanjšanju ročnega konfiguriranja in uglaševanja sistema.
- Uporaba senzorjev na osnovi strojne opreme, ki pasivno poslušajo omrežni promet, ki ga zbirajo stikala, brez aktivnega poseganja v procesna omrežja.
- Integracija senzorjev v SIEM prek Sysloga.
- Upoštevajo naj se projekti v katerih senzorji spremljajo minimalno 100–150 sredstev na RTP postajo.
- Nadzorni sistemi v projektih naj spremljajo vsaj 20 VN/SN transformatorskih postaj.
- Komunikacija med senzorji in nadrejenimi sistemi (SIEM, centralni nadzorni sistem,…) mora biti izvedena tako, da se lahko uporabi komunikacijska pot z nizko pasovno širino.
- Komunikacija med senzorji in nadrejenimi sistemi, mora potekati preko varnega komunikacijskega kanala
- Proizvajalec zagotavlja 24/7 pomoč/servisno službo in dodatno strokovno podporo med delovnim časom v angleščini.
- Proizvajalec ima vsaj 1000 zaposlenih.

Referenčni projekti ne smejo biti starejši od 1.1.2019

Ponudnik strokovno usposobljenost in referenčne projekte izkaže z lastno izjavo, v kateri na kratko opiše projekt, navede leto zaključka projekta in navede kontaktni naslov naročnika projekta.

6.2 Reference ponudnika

Ponudnik mora ustrezati naslednjim kriterijem:

- Najmanj 3 zaposleni
- Izkaže usposobljenost za delo s procesnimi sistemi, ki temeljijo na protokolu IEC61850
- Izkaže delo na projektih vodenja in avtomatizacije. Minimalno 3 projekti.

Referenčni projekti ne smejo biti starejši od 1.1.2020

Ponudnik strokovno usposobljenost in referenčne projekte izkaže z lastno izjavo, v kateri na kratko opiše projekt, navede leto zaključka projekta in navede kontaktni naslov naročnika projekta.