TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Edvard Paas 179153IACB

Võrguliikluse seire ja sissetungi tuvastuse süsteemi juurutamine ja analüüs S4A baasil

Bakalaureusetöö

Juhendaja: Avo Ots
Tehnikateaduste magister

Kaasjuhendaja: Dmitri Ivanov
Tehnikateaduste magister

Tallinn 2021

Autorideklaratsioon

Kinnitan, et olen koostanud antud lõputöö iseseisvalt ning seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on töös viidatud.

Autor: Edvard Paas

21.05.2021

Annotatsioon

Töös käsitletakse võrgu seire ning sissetungi tuvastuse süsteemi (IDS) lahenduse juurutamist ning analüüsi ühes riigiasutuses. Töös analüüsitakse organisatsiooni küberturvalisuse vajadusi ning tehakse järeldus, et kõige kulutõhusam viis hetkeolukorra parandamiseks on sissetungi tuvastuse süsteemi kasutuselevõtmine. Parima sissetungi tuvastuse süsteemi leidmiseks võrreldakse kolme peamist avatud lähtekoodiga IDS tarkvara: Zeek, Snort ning Suricata. Võrdluse tulemusel tehakse järeldus, et Suricata on kõige sobivam IDS arvestades töös kirjeldatud organisatsiooni vajadusi. Suricata on eelistatud mitmete tänapäevaste NSM/IDS/IPS lahenduste poolt, mis kombineerivad selle muu tarkvaraga Suricata seadistuse, häirete ning teavituste haldamiseks. Erinevate IDS tarkvara seas osutus asutuses juurutatava IDS lahendusena valituks Suricata for All (S4A), kuna S4A on hallatud CERT-EE poolt ning ta on mõeldud riigiasutustele kasutamiseks. Lõputöös kirjeldatakse S4A töövoogu, arhitektuuri ning sensori paigutust asutuse võrgus. Töös valideeritakse juurutatud lahenduse funktsionaalsust ning antakse hinnang S4A juurutamise tulemusele.

Lõputöö on kirjutatud eesti keeles ning sisaldab teksti 38 leheküljel, 5 peatükki, 11 joonist, 1 tabelit.

Abstract

Deployment and Analysis of a Network Traffic Monitoring and Intrusion Detection System Based on S4A

This thesis deals with deployment and analysis of a solution that includes network monitoring and intrusion detection capabilities in a state institution. The thesis examines the cybersecurity needs of the organization and concludes that the most cost-effective method of improving the current situation would be to use an open-source intrusion detection system. In order to determine the most appropriate solution, this thesis compares features of three primary open-source IDS software: Zeek, Snort, and Suricata. As a result of this comparison, Suricata is determined to be the solution that meets the needs of the organization the most. Suricata is often included in modern NSM/IDS/IPS solutions that combine Suricata with other software, which provides better management of the IDS configuration and the analysis of the alerts and notifications generated by the IDS. Among other options, this thesis determined that Suricata for All (S4A) shall be chosen as the primary solution primarily as it is managed by CERT-EE and was tailored to meet the specific needs of public institutions. This thesis describes S4A workflow, architecture, and the sensor placement within the network. The thesis also proves that the deployed solution is operational and assesses the post-deployment result.

The thesis is in Estonian and contains 38 pages of text, 5 chapters, 11 figures, 1 table.

Lühendite ja mõistete sõnastik

IDS	(*Intrusion detection system)* sissetungi tuvastuse süsteem
NSM	(*Network security monitor*) Võrguturvalisuse monitoorija
HIDS	(*Host-based intrusion detection system*) hostipõhine sissetungi tuvastuse süsteem
NIDS	(*Network-based intrusion detection system*) võrgupõhine sissetungi tuvastuse süsteem
S4A	Suricata 4 All
APT	(*Advanced persistent threat*) arenenud püsiv rünne
IPS	(*Intrusion prevention system*) sissetungi ennetuse süsteem
ISP	(*Internet service provider*) Interneti-teenuse pakkuja
SOHO	(*Small office/home office*) väike- või kodukontor
SPAN	(*Switched port analyzer*) kommuteeritud pordi analüsaator
HTTP	Hypertext Transfer Protocol
DNS	Domain Name System
SSL	Secure Sockets Layer
SMTP	Simple Mail Transfer Protocol
MIME	Multipurpose Internet Mail Extensions
JSON	JavaScript Object Notation
OISF	Open Information Security Foundation
ASCII	American Standard Code for Information Interchange

Sisukord

Jooniste loetelu

Tabelite loetelu

1 Sissejuhatus

Ühiskond on järjepidevalt liikumas digitaalmaailma suunas ning 2020. aastal alanud koroonaviiruse pandeemia on jõuliselt puudutanud kõiki majandussektoreid, aga kõige rohkem tervishoiu- ning haridusasutusi. Üleminek informatsiooni- ja kommunikatsioonitehnoloogial põhinevatele lahendustele on jätkuv arengusuund, mida kinnitavad nt järgmised ilmingud: sotsiaalmeedia olulisuse kasv ühiskonnas, riigi infosüsteemi (nt X-tee näol) täienemine uute infosüsteemidega, ning üha enam asutuste ja ettevõtete tööprotsesside osaline või täielik digitaliseerimine.

Digitaliseerimise trendi kõrval on eriti oluliseks muutunud küberturvalisuse tagamine, kuna kõrgem sõltuvus IKT süsteemidest suurendab võimalusi küberrünnakuteks. Eesti kontekstis on küberturvalisuse teema vastu tundmas aina rohkem huvi nii eraisikud, ettevõtted kui riiklikud asutused. Seda võib näha enam tihedama teema kajastamisest asutuste väljaannetes ning strateegiates. Üks oluline küberturvalisuse aspekt on organisatsiooni kohaliku võrgu ning selles olevate seadmete turvalisus. Üks vahenditest, millega on võimalik seda tõhustada, on sissetungi tuvastuse süsteemi rakendamine võrgus.

Tööalaselt olen seotud asutusega, kuhu juurutatakse sissetungi tuvastuse süsteem Suricata-for-All. Soovin tänada tehniliste nõuannete eest juhendajaid Avo Ots'a ning Dmitri Ivanov'i, ja juurutusprotsessil toetamise eest asutuse kolleege ning CERT-EE esindajaid.

1.1 Eesmärk

Lõputöö eesmärgiks on analüüsida ning juurutada ühes riigiasutuses sissetungi tuvastuse süsteem Suricata for All. Analüüsis uuritakse Suricata for All kasutuselevõtmise põhjuseid ning eeliseid. Juurutamise käigus arvestatakse sissetungi tuvastuse süsteemi riistvaraliste nõuetega, leitakse S4A sensori jaoks sobilikum asukoht võrgus ning kinnitatakse selle funktsionaalsust.

1.2 Eelnevad tööd teema kohta

Sissetungi tuvastuse ning võrgumonitooringu süsteemide kohta on kirjutatud akadeemilises kontekstis palju, kuid mitte eesti keeles. Näiteks on võrgu monitoorimist käsitletud M. Erik magistritöös „Andmeside kursuse võrguhalduse laboritöö Simple Network Management Protocol baasil“, kuid see on pigem seotud võrguhalduse ning pedagoogika valdkonnaga [1]. Käesolevas diplomitöös käsitletakse lahendusi, mis sisaldavad endas võrgumonitooringu võimalusi.

Konkreetselt sissetungi tuvastuse süsteeme käsitles S. Farooghiani bakalaureuse lõputöö „Praktiliste oskuste töötuba – avatud lähtekoodiga sissetungimise turvasüsteemid“, kus võrreldakse kolme põhilist avatud lähtekoodiga sissetungi tuvastuse süsteemi – Suricata, Snort ning Zeek [2]. Neid süsteeme käsitletakse ka käesolevas töös ning teostatakse põhjalikum võrdlus, mis võtab arvesse rohkem tegureid ning annab nendest süsteemidest laiema kirjelduse.

Suricata for All (vanasti Snort for All nime all) sissetungi tuvastuse süsteemi kohta oli tehtud magistritöö 2012. aastal, mille autoriks on Alar Kvell, ning mille eesmärgiks oli võrrelda sissetungi tuvastuse süsteemide Snort ning Suricata võrgupakettide analüüsimise jõudlust. Tänapäeval S4A kasutab pakettide analüüsimiseks Suricata tarkvara, kuna sellel on oluliselt suurem jõudlus kui tolleaegsel Snort tarkvaral. 2021. aastal tuli välja Snort 3, mis eemaldas palju puudusi, mida mainiti ka eelmainitud töös [3]. Käesolev lõputöö ei võrdle sissetungi tuvastuse süsteemide jõudlust.

1.3 Sissetungi tuvastuse süsteemid

Sissetungi tuvastuse süsteem (*intrusion detection system* ehk IDS) on tarkvaraline või riistvaraline süsteem, mis seirab kogu liiklust, mis läbib konkreetset võrgusõlme või kogu võrku. Selle eesmärgi täitmiseks peab sissetungi tuvastuse süsteemil olema kaks põhifunktsionaalsust: võrgupakettide salvestamine ning nende analüüsimine. Eristatakse kahte tüüpi sissetungi tuvastuse süsteeme: *host-based intrusion detection system* (HIDS), mis monitoorib ühe konkreetse seadme liiklust, ning *network-based intrusion detection system* (NIDS), mis seirab kogu võrgusegmenti. Kasutaja määrab IDS konfiguratsioonis, milliseid pakette (näiteks protokolli järgi) on vaja salvestada ning mida peab tuvastama IDS analüsaatori komponent. Tuvastamine toimub tavaliselt reeglipõhiselt.

Lisaks tuvastamisele võib IDS teha ohtlikust liiklusest teavituse või vajadusel seda ka blokeerida. Juhul, kui ohtliku liikluse vastu võetakse kasutusele aktiivsed meetodid, nagu liikluse blokeerimine, siis seda süsteemi võib nimetada ka sissetungi ennetamise süsteemiks (*intrusion prevention system* ehk IPS) [4].

Sissetungi tuvastuse süsteemi kriitilised funktsioonid võtab kokku J. R. Vacca käsiraamat *Computer and Information Security Handbook* [4]:

1. Võrguturvalisuse infrastruktuuri paindlikkuse suurendamine.
2. Võrgus olevate marsruuterite, tulemüüride, võtmeserverite ning kriitiliste kommutaatorite funktsionaalsuse seiramine.
3. Turvaauditite läbiviimine.
4. Kasutajate tegevuse jälgimine võrgu algpunktist lõpp-punktini.
5. Edastatud failide terviklikkuse kontrollimine.
6. Sensori konfiguratsiooni terviklikkuse valideerimine.
7. Potentsiaalsete rünnete tuvastamine ning nendest teavitamine.
8. Võrgu turvalisuse haldamine mittespetsialistide poolt.

2 Sissetungi tuvastuse süsteemide analüüs

Analüüsi eesmärgiks on paika panna raamid, mille kontekstis põhjendatakse süsteemi jaoks vajaliku infrastruktuuri hankimist ning anda alus konkreetse IDS valikule. Lõputöös esitatud analüüsis vaadeldakse küberturvalisuse aspekte Eesti Vabariigi riigiasutuse vaatenurgast. Analüüs võib olla asjakohane ka suurema tähtsusega ettevõtetele ning kriitilise infrastruktuuri pakkujatele.

Käesolevas analüüsis käsitletakse küberturvalisuse olukorda üldiselt Eestis ja konkreetsemaid juhtumeid, mis võivad tõenäolistelt puudutada Eesti Vabariigi riigiasutusi. Lisaks vaadeldakse soovitud olukorda , kus juurutatakse võrgumonitooringu süsteem ning milliseid probleeme on võimalik sellega lahendada. Analüüsis kirjeldatakse neid avatud lähtekoodiga (*open source*) kättesaadavaid võrgumonitooringu süsteemide (NSM) lahendusi, mis on lõputöö vaatest asjakohased.

Analüüsis esitatakse infotehnoloogilisest vaatenurgast lühikirjeldus ühest Eesti riigiasutusest, kus selle lõputöö raames juurutati S4A. Lisaks sellele tehakse ka asutuse küberturvalisuse hetkeolukorra ülevaate. Selles puudutatakse küberturvalisuse vajadused ning riskid, mis ajendasid S4A süsteemi kasutuselevõttu.

Peatüki lõpus tehakse metoodiline valikuotsus selle järgi, milline süsteem pakub kõige sobivamaid võimalusi ning millist süsteemi on organisatsioonis kõige lihtsam juurutada.

2.1 Eesti küberturvalisuse hetkeolukorra ülevaade

Küberturvalisuse hetkeolukorra kirjeldamiseks selles analüüsis kasutatakse kolme allikat: Riigi Infosüsteemi Ameti andmeid, mis annavad üldisema ülevaate, Kaitsepolitseiameti väljaandeid küberjulgeoleku hetkeolukorra kirjeldamiseks ning kõige viimast Majandus- ja Kommunikatsiooniministeeriumi küberturvalisuse strateegiat aastateks 2019 – 2022. Selles alaosas piirdutakse riiklike allikatega, kuna analüüsi fookuses on riiklik asutus.

Riigi Infosüsteemi Ameti andmetel on perioodil 2018 – 2020 intsidentide arvu osakaalu poolest domineerinud robotvõrgustikega, õngitsustega, pahavaraga ning

teenusetõkestusrünnetega seotud intsidendid. Nendel aastatel on olulist kasvu teinud õngitsustega seotud intsidentide arv, mis on kasvanud kolme aastaga 9 protsendilt 26 protsendini [5] [6]. Aastal 2020 on toimunud kolm märkimisväärset muutust võrreldes eelmisega: teenusekatkestust põhjustanud intsidentide hulk on kasvanud poole võrra, õngitsuste arv on kahekordistunud ning toimus kolm samalaadse mustriga küberrünnakut Eesti riigi IT-taristu vastu. Viimased olid suunatud kolme ministeeriumi vastu ning tulemusena saadi kätte mitusada gigabaiti andmeid ning COVID-19 pandeemiaga seotud isikuandmeid [7].

Küberjulgeoleku kontekstis viimastel aastatel on järjepidevalt olnud probleemiks välisriikide eriteenistuste poolt pandud APT (*advanced persistent threat*) küberrünnete tuvastamine ning tõrjumine. APT rünnakute sihtmärkideks on tavaliselt riigiasutuste töötajad ning nende IT-taristu. Nende küberrünnete lõppeesmärk on saada huvipakkuvat informatsiooni välisriikide luureasutuste jaoks. Rünnetes tihti kasutatakse pahavara sisaldavaid õngitsuskirju ning üritatakse meelitada riigiasutuse töötajaid andma oma kasutajanimesid, paroole jms ründajate võltsitud lehekülgedel [8] [9] [10].

Majandus-ja Kommunikatsiooniministeeriumi küberturvalisuse strateegia 2019 – 2022 toob selle koostamist mõjutanud arengusuundumustena näiteks järgmisi tegureid [11]:

- laienev tehnoloogiakasutus, suurenev digitaalne sõltuvus, robotiseerimine, jm, mis loob aluse uute võimalike küberrünnete jaoks ehk selle arengusuundumuse tulemusena kasvab ründevektor;
- küberkuritegevuse kasv ehk üha rohkem süütegusid pannakse toime kasutades küberruumi võimalusi, nt teenusetõkestusründed või lunavara levitamine;
- globaalne ning regionaalne keerukas julgeolekukord, mille tõttu võivad Eestis tegutsevad ettevõtted ning riigiasutused sattuda välisriikide küberoperatsioonide sihtmärkideks;
- piiratud tehnoloogiline autonoomia, mille tõttu Eesti on paljuski sõltuv välisriikide tehnoloogilistest lahendusest.

Sama strateegiadokument toob välja ka prioriteetsemad probleemid (väljatoodud esimest neli) ning väljakutsed, kusjuures Eesti olukord ei ole oluliselt erinev muudest riikidest [11]:

1. ekspertide kogukonna piiratud spetsialiseerumisvõime ja ebapiisav tippspetsialistide reserv, samal ajal kui infosüsteemid muutuvad aina keerulisemaks;

2. puudulik tervikjuhtimine strateegilisel tasemel, mille tõttu puudub vajalik küberturvalisuse koordinatsioon riigiasutuste vahel;

3. asutused ei analüüsi oma IT taristu arendamisel piisavalt, kuidas nt uued infosüsteemid mõjutavad teisi riigivõrguga seotud infosüsteeme;

4. vähene teadlikkus era- ning avaliku sektori juhtide hulgas, mille tõttu suunatakse infoturbe valdkonda vähem vahendeid.

Kokkuvõttes võivad küberturvalisusega seotud ohud võtta nii kuritegelikke (nt pettused, lunavara levitamine) kui julgeolekuga seotud (nt välisriikide eriteenistuste küberoperatsioonid) dimensioone. Intsidentide koguarv üldiselt on olnud stabiilne, kuid teatud tüüpi intsidentide arv võib oluliselt muutuda ning eeldatavasti infotehnoloogia kiire arenguga see trend jätkub. Riiklikul tasemel on vaja jätkata küberturvalisuse valdkonnas teadlikkuse tõstmisega ning leida asutuste ülene ning ühtsem lahendus küberturvalisuse tagamiseks.

2.2 Asutuse küberturvalisuse hetkeolukord

Selles osas kirjeldatakse küberturvalisuse hetkeolukorda avaliku sektori asutuses (edaspisi asutus), kuhu paigaldatakse ning juurutatakse S4A . Asutuse üks funktsioonidest on seotud rahvusvahelise suhtlusega, mis tähendab, et edukas küberrünnak asutuse vastu võib lisaks tavalistele tagajärgedele ka tõsiselt kahjustada Eesti rahvusvahelist mainet, eelkõige seetõttu, et Eesti on rahvusvaheliselt sidunud ennast e-riigi kontseptsiooniga.

Asutuse üldist infotehnoloogilist profiili iseloomustavad küllaltki konservatiivne areng viimase kahe aastakümne jooksul, infotehnoloogia osakonna vähene komplekteeritus ning IT arengute jaoks taotletud eelarvete ebapiisav rahastus valitsuse poolt. See-eest on viimastel aastatel olukord paranenud: vahetati välja aegunud töövahendid ja baastaristu

(võrguseadmed, serverid, arvutid, printerid), tegeletakse olemasolevate infosüsteemide suuremahuliste uuendamisega ning võimalike süsteemide analüüsimisega, mis tõhustaksid asutuste äriprotsesse ning vähendaksid kulusid ja riske.

Hoolimata sellest, et seisukord on suhteliselt parem kui eelmistel aastatel, on asutusel siiski piirangud eelarves, IT infrastruktuuris ning isikkoosseisu suuruses. Infrastruktuur oli suures osas vananenud ning loobuti sõltumatute baasteenuste pakkumisest, mida nüüd tellitakse teistest riigiasutusest. Oluline on märkida, et käesolevast asutusest sõltuvad avaliku sektori asutustel esinevad samuti eelmainitud probleemid, mis laiendab potentsiaalset ründevektorit ning võimendab olemasolevaid ohtusid.

Tuleb märkida, et kõikidele asutustele kehtivad üldiselt samad nõuded infoturbele sõltumata asutuse eelarvest või suurusest. 2020. aastal riigi IT-taristu vastu tehtud edukad rünnakud näitavad, et keegi pole täielikult kaitstud. Rünnaku suurim mõju oli Majandus- ja Kommunikatsiooniministeeriumi (MKM) valitsemisalas, kus veebiserveri ründamise järel õnnestus ründajatel pääseda edasi MKM-i haldusala serveriteni, kust lekkis suures ulatuses andmeid, mille tagajärjel said kurjategijad kätte ka isikuandmeid.

On alust arvata, et lisaturvameetmete rakendamine, sh juurutatud kaasaegne automatiseeritud seirelahendus, oleks neid rünnakuid ära hoidnud.

2.3 Sissetungi tuvastuse süsteemi kasutuselevõtmise eelised

Sissetungi tuvastuse süsteemi kasutuselevõtmine aitab täita puudujääke, mida eelnevalt kirjeldati, ning selle abil on võimalik tõhustada küberturvalisuse tagamist asutuses. Võttes aluseks asjakohaseid küberturbe spetsialisti kompetentse [12], saab hinnata IDS-i mõju spetsialisti tööprotsessidele:

1. IDS võimaldab tuvastada, et on toimunud küberintsident, mille järgi saab ette võtta meetmeid, et see lahendada või leevendada selle tagajärgi. Juhul, kui tarkvaral on olemas ka sissetungi ennetuse võimalused (IPS), siis ka blokeerida pahaloomuline võrguliiklus.

2. Isegi juhul, kui intsidendi toimumine tuvastati mitte IDS-i poolt, kuid see tehti piisavalt kiiresti, et intsidenti puudutav võrguliiklus on veel salvestatud (mis on vajalik, et IDS saaks seda analüüsida), on ikkagi võimalik saada intsidendi kohta

lisaandmeid ning luua reegel, mis sellist liiklust kirjeldaks ning edaspidi seda tüüpi intsidenti tuvastada.

3. Kuna oluline osa IDS funktsionaalsusest on võrguliikluse seire ning vajadusel selle põhjal teavituste edastamine, siis kaob vajadus võrgu turvalisuse eest vastutaval isikul aktiivselt kontrollida liikluse sisu või andmeid selle kohta ning selle tõttu saab suunata tähelepanu teistele kohustustele.

4. IDS annab parema ülevaate sellest, mis toimub võrgus, ning seetõttu suurendab vastutava isiku arusaama asutuse küberruumist. See on abiks ka võrgu administreerimisel ning tehnilise toe pakkumisel.

Nagu näha, siis IDS-i rakendamine toob kaasa lisaks küberrünnete tuvastamisele või ennetamisele ka mitmeid eeliseid küberturvalisuse tagamisele. Piisava keerulisusega IDS saaks automatiseerida mitmeid tööülesandeid, mis puudutavad nt logiandmete analüüsi ja küberintsidentide uurimist. Samas on ka selge, et iseenesest IDS-i juurutamine ei saa asendada asutuse võrgu eest vastutavat isikut, ning on pigem üks paljudest meetmetest, mis aitavad tagada asutuses küberjulgeoleku.

2.4 Avatud lähtekoodiga sissetungi tuvastuse süsteemide lahendused

Sissetungi tuvastuse süsteeme, mis põhinevad vaba lähtekoodiga tarkvaral ning millega arvestatakse selles lõputöös, on kolm: Zeek, Snort, Suricata. Analüüsi käigus tehakse ülevaade mainitud IDS-ide võimalustest ning võetakse arvesse ka kättesaadavad lahendused, mis sisaldavad endas mõnda IDS-i koos teise tarkvaraga, et pakkuda nt graafilist liidest või muid lisavõimalusi.

2.4.1 Zeek

Zeek on passiivne võrguliikluse seire- ning sündmuspõhine analüüsimise tarkvara, mida on võimalik rakendada sissetungi tuvastuse süsteemina. Arhitektuurselt jaguneb Zeek kaheks osaks: sündmuste mootor (*event engine* ehk *core*) ning skripti interpretatoor (*policy script interpreter)*. Kasutades Zeek'i skriptimiskeelt on võimalik valida sündmus (nt HTTP päring), mille puhul täidetakse kasutaja poolt programmeeritud tegevused. Tavaliselt kasutatakse Zeek'i detailsete logiandmete saamiseks ning need suunatakse

töötlemiseks või esitlemiseks teise programmi. Zeek võimaldab logida nii madal- kui ka kõrgtaseme protokollide tegevust [13].

Zeek'i dokumentatsiooni järgi Lisa 2 Joonis 6 kirjeldab soovitatud võrgu topoloogiat SOHO tingimustes. Asukohad on märgitud tähtedega A – G ning need tähistavad kohti, kus sensor saab võrku jälgida. Parim asukoht selles näites on D, juhul kui kasutaja kommutaatoril (*Customer switch*) on võimalus SPAN (*mirror*) pordi kasutamiseks, et peegeldada võrgusõlme läbivat võrguliiklust seadmesse, mis vastutab selle töötlemise ja analüüsimise eest [14].

Zeek'i abil saab teostada analüüsi, mis toimub kasutaja kirjutatud skriptide kaudu. Näiteks saab HTTP liiklusest saada faile, analüüsida võrgus kasutatud veebitarkvara, jpm. Zeek'i puudusena võib välja tuua, et ta vajab liidestamist tarkvaraga, mis töötleksid Zeek'i peamist väljundit ehk võrguliikluse logisid (nt HTTP, DNS, SSL sertifikaadid, SMTP sisu, MIME tüübid jpm), mida ta väljastab *tab-separated* või JSON formaadis. Erinevalt Suricata’st või Snort'ist, Zeek ei ole optimeeritud konkreetsete signatuuride tuvastamiseks (*byte-matching*) vaid see on pigem töövahend pahaloomulise liikluse analüüsiks [13].

Oluliseks puuduseks on Zeek'i ühelõimelisus ning selle tõttu soovitatakse luua klastri Zeek'i kasutatavatest süsteemidest, mille soovituslik arhitektuur on dokumentatsiooni kirjeldatud Lisa 2 Joonisel 7.

2.4.2 Snort

Snort on Cisco poolt arendatud avatud lähtekoodiga võrgupõhine IDS/IPS. Snort kasutab ohtude tuvastamiseks reegleid, mis on üldiselt ühilduvad ka Suricata reeglitega (v.a keeruliste reeglite puhul, mis sõltuvad rohkem konkreetse IDS-i funktsionaalsusest [15]). 2021. aasta jaanuaris tuli välja Snort 3, mille üheks oluliseks võimaluseks on rohkem kui ühe lõime kasutamine pakettide analüüsimiseks. Snort’i eelmiste versioonide ühelõimelisus oli suureks puuduseks võrreldes Suricata’ga, mis on olnud algselt tehtud mitmelõimelisena. Samuti on sarnaselt Suricata’ga toetatud LuaJIT mootorit skriptide ning plugin’ide arenduseks [16].

Snort’il on dokumentatsiooni järgi kolm erinevat töörežiimi [17]:

1. *Sniffer Mode* – loeb võrguliiklusest pakette ning esitab neid ekraanil.

2. *Packet Logger mode* – logib pakette kettale.

3. *Network Intrusion Detection System (NIDS) mode* – Snort teostab võrguliiklusele tuvastust ning analüüsi. See on režiimidest kõige keerulisem ning seadistatavam.

Snort'i jaoks on kättesaadav tasuta reeglite kogumik (*Community Ruleset*), mida sertifitseerib võrguturbe ekspertide grupp Talos. Samuti on võimalik tasuta saada *Registered* reeglistiku, kuid see ei ole kättesaadav süsteemides, mis integreerivad Snort'i tarkvara (*Snort Integrator*). Tasulistel Snort'i kasutajatel on võimalik saada reeglistiku uuendusi reaalajas ning Talose pakutud kasutajatuge [18].

Kuna Snort 3 oli avalikult lansseeritud 19. jaanuaril 2021.a [19] ning Snort 2 puuduste tõttu on viimaste aastate jooksul mitmed IDS lahendused üle läinud Suricata peale, siis eeldatavasti pole veel avatud lähtekoodiga täismahulisi integreeritud süsteeme, kus oleks kasutatud Snort 3.

2.4.3 Suricata

Suricata on suure jõudlusega võrgu mitmelõimeline IDS, IPS ning võrguturbe monitoorimise tarkvara, millega on võimalik salvestada võrguliiklust ning teostada PCAP failidel analüüsi. Suricata on avatud lähtekoodiga ning selle eest vastutab mittetulundusühing Open Information Security Foundation (OISF) [20]. Suricata'l on vaikimisi palju võimalusi, nt failide saamine võrguliiklusest, LuaJIT mootori integratsioon keerukamate võrguliikluse analüüside teostamiseks, koormuse jagamine GPU-ga (*hardware acceleration*), rakenduskihi protokollide logimine ning analüüs, k.a TLS/SSL sertifikaadid, HTTP päringud, DNS päringud, jpm [21].

Üle pika aja oli Suricata suureks eeliseks Snort 2 ees mitmelõimeline arhitektuur ning selle tõttu on mitmed tuntumad avatud lähtekoodiga IDS lahendused nagu S4A [22], Security Onion [23] ja RockNMS [24] Suricata'le üle läinud.

2.5 Sissetungi tuvastuse süsteemi valimine

Eelnevates alapeatükkides kirjeldatu põhjal esitan käsitletud kolme sissetungi tuvastuse süsteemide võrdleva tabeli Tabel 1. Tabel võrdleb erinevate IDS-ide sisse ehitatud võimalusi ning koheselt kättesaadavaid komponente.

Komponent / funktsionaalsus	Zeek	Snort 3	Suricata
IDS	Jah	Jah	Jah
IPS	Ei	Jah	Jah
Mitmelõimeline	Ei. Klastritepõhine arhitektuur. [25]	Jah. Pole dokumenteeritud.	Jah.
PCAP analüüs	Jah	Jah	Jah
TCP/IP analüüsimootor	Jah	Jah	Jah
Rakenduskihi analüüsimootor	Jah	Jah.	Jah
Analüüsi loogika laiendamine	Zeek Script	LuaJIT	LuaJIT
Pistikprogrammide lisamine	Jah	Jah	Puudulik.
Kasutatavus, paigaldus	Keeruline	Lihtne	Lihtne
Litsents	BSD litsents [26]	GPLv2	GPLv2
Integreeritud lahendused	Security Onion [23], RockNMS [24]	Puuduvad	S4A, SELKS, RockNMS, Security Onion

Tabel 1. Sissetungi tuvastuse süsteemide võrdlus

Tabeli põhjal saab järeldada, et Suricata on jätkuvalt kõige sobivam variant IDS-i jaoks. Snort 3 on alles lansseerimise algfaasis ning seetõttu pole turul veel IDS lahendusi, mis seda sisaldaksid. Kuna käesoleva töö raames on tegemist sellise lahenduse leidmisega, mille kasutuselevõtmiseks on vajalik minimaalne arv ressursse, siis peab välja jääma

Zeek, kuna tal puudub kogu vajalik funktsionaalsus, nt IPS komponent, mis laseks teatud tingimuste põhjal blokeerida võrguliiklust. Snort 3 ei ole samuti sobilik, sest hetkeseisuga peab süsteemiadministraator ise looma vajaliku NSM *stack*-i, et saada täismahuline IDS lahendus. Selline mõttekäik jätab alles ainult Suricata, mis sisaldab endas vajaliku funktsionaalsuse ning selles lõputöös arvestatud IDS lahenduste seas on see kasutuse poolest eelistatuim.

Lõpliku lahendusena valitakse Suricata for All, kuna seda arendati riigiasutuste teenindamiseks, mis on kõige sobilikum omadus käesoleva lõputöö organisatsiooni jaoks. Oluliseks eeliseks on ka asjaolu, et S4A on hallatud CERT-EE poolt.

3 S4A juurutamine asutuses

Peatükis kirjeldatakse Suricata for All arhitektuuri ning nõudeid riist- ja tarkvarale. Käsitletakse S4A arhitektuuri, erinevaid komponente ning nende omavahelist suhtlust. Peatükis kirjeldatakse juurutamise tulemeid, probleeme ning valideeritakse S4A funktsioneerimist.

3.1 S4A spetsifikatsioon

S4A (Suricata for All) on sisse tungimise tuvastuse süsteem, mis kasutab avatud lähtekoodiga tarkvara komponente, et monitoorida ning analüüsida võrguliiklust võimalike sissetungimiste tuvastamiseks. S4A sisaldab endas kasutajaliideseid kesksüsteemi konsooli ehk central'i jaoks ning riigiasutustesse paigutatava sensori ehk detector'i jaoks. S4A paigaldatakse kasutades SaltStack'i ning IDS reeglite ja komponentide uuendamise eest vastutab CERT-EE [22].

3.1.1 S4A komponendid

Dokumentatsiooni järgi S4A koosneb seitsmest peamisest komponendist, mis täidavad erinevaid rolle [22]:

- Suricata – IDS
    - Lisana kasutatakse Evebox'i, mis on veebipõhine teavituste ning sündmuste haldamise tarkvara, mis kasutab sisendina Suricata väljundit Eve JSON formaadis.
- Netdata – reaalaja jõudluse ning sensori hetkeseisu seiramise tarkvara.
- nfsen – nfdump väljundi visualiseerimise tarkvara.
- Arkime (varasema nimetusega Moloch) – võrgupakettide salvestamise, indekseerimise ning sisu analüüsimise tarkvara.
- OpenVPN – kaughalduse pakkumine sensorile kesksüsteemi poolt.
- ElasticSearch – teksti otsimise ning analüüsimise tarkvara.

    - Telegraf – sensori kohta mõõtmiste kogumine ning töötlemine.

- Sensor ja kesksüsteem
    - Veebiliides IDS seadistuste haldamiseks.
    - Suhtlus SaltStack'iga ning veebiliidesega toimub kasutades Loopback raamistiku, mis on ühendatud MongoDB andmebaasiga.
    - Front-end on realiseeritud kasutades Nuxt.js ning Vuetify raamistike.

3.1.2 S4A arhitektuuri ülevaade

S4A on kokku pandud avatud lähtekoodiga komponentidest, et vähendada sõltuvust spetsiaaltarkvarast ning saada võimalikult standardne lahendus. Ainult teatud osad on spetsiaalselt S4A jaoks, nt kasutajaliidesed kesksüsteemi ning sensori jaoks. S4A sensor paigaldatakse monitooringuserverile SaltStack'i abil.

Sensori ning kesksüsteemi vahel on viis suhtlevat komponenti [27]:

1. Läbi Loopback API sensor pärib kesksüsteemilt reeglite uuendust ning kesksüsteem jagab sensoriga CERT-EE reegleid ning varem mainitud avatud reeglite kogumikku Emerging Threats Rules. Sensori administraator saab määrata ka oma reegleid kasutades S4A kasutajaliidest, mida on kirjeldatud Lisa 3 Joonisel 9. Loopback API kaudu edastatakse saadud reeglid Suricata'sse (Lisa 3 Joonis 10).
2. Suricata väljund töödeldakse kasutades Evebox ning Elasticsearch tarkvara ning tulemid ja teavitused kahtlasest võrguliiklusest edastatakse kesksüsteemi edasiseks töötlemiseks.
3. Arkime (Moloch) salvestab ning indekseerib liikluses olevad võrgupaketid. Pakette saab käsitsi analüüsida kasutades Arkime'i veebiliidest.
4. OpenVPN ühendus luuakse sensori ning kesksüsteemi kaughalduse puhul.
5. Sensori Telegrafi teenus edastab erinevaid mõõtmisi kesksüsteemi.

6. Sensori Salt *minion* saab kesksüsteemilt sensori komponentide paigalduspakette ning Emerging Threats reegleid.

Kogu protsess on illustreeritud Lisa 3 Joonisel 11.

3.1.3 S4A nõuded tuvastaja seadmele

Järgmised nõuded on piisavad tavalises keskkonnas riistvarale, kus hakkab paiknema sensor. Peab arvestama, et olenevalt võrguliikluse mahust võivad nõuded muutuda [28]:

- Protsessor: 4-tuumaline Intel i7 või parem.
- Vähemalt 64 GB muutmälu.
- SSD-kettad.
- Vähemalt 2 võrguliidest.

Väljuvate võrguühenduste puhul on vaja lubada liiklus järgmistel portidel [28]:

- 5000/tcp – S4A keskserveri API liides.
- 22/tcp – S4A Github repositooriumile ligipääs
- 80/tcp – kolmandate osapoolte tarkvara repositooriumid
- 443/tcp – S4A kaughaldus (OpenVPN) ning kolmandate osapoolte tarkvara

Kettad peavad toetama järgnevaid kasutamise juhtusid [28]:

- Suricata – minimaalselt mitu gigabaiti päevas.
- Arkime
    - Võrguliiklus sagedusega 100 Mbps vajab ca 1080 GB kettaruumi päevas.
    - Muutmälu peab olema vähemalt 1 kuni 3 protsenti kogu klastri suurusest.
- PCAP salvestamine
    - ca 50 Mbps = 540 000 MB/päevas

3.2 S4A juurutamise tulemid

3.2.1 S4A sensori asukoht võrgu topoloogias

Tavaliselt tuleb sensor paigutada võrku nii, et talle oleks nähtav kogu võrguperimeetrit läbiv liiklus, nagu on illustreeritud Joonisel 11. Lõputöös käsitletava asutuse raames kahjuks sellist asukohta ei saanud asutus lubada, kuna baasteenuste pakkuja võrguliiklus oli asutusega samas võrgus. Kuna asutus ei tohiks olla võimeline seirama oma partneri võrguliiklust, siis paigaldati sensor rakendusserverite võrku, kus asuvad sh ka asutuse veebiserverid.

Selle tulemusel saab peegeldada võrguliiklus sensorisse läbi *mirror* pordi ning sensori kasutajaliidesest on tõepoolest näha peegeldatud liiklust ning selle sisu on võimalik analüüsida. Reeglite põhjal on S4A võimeline otsustama, missugust tüüpi teavitust edastada kesksüsteemile ning kohalikule administraatorile. S4A juurutamisel on nüüd asutuse võrgus IDS, mis tagab teadlikkuse võimalike ohtude kohta võrguperimeetril.

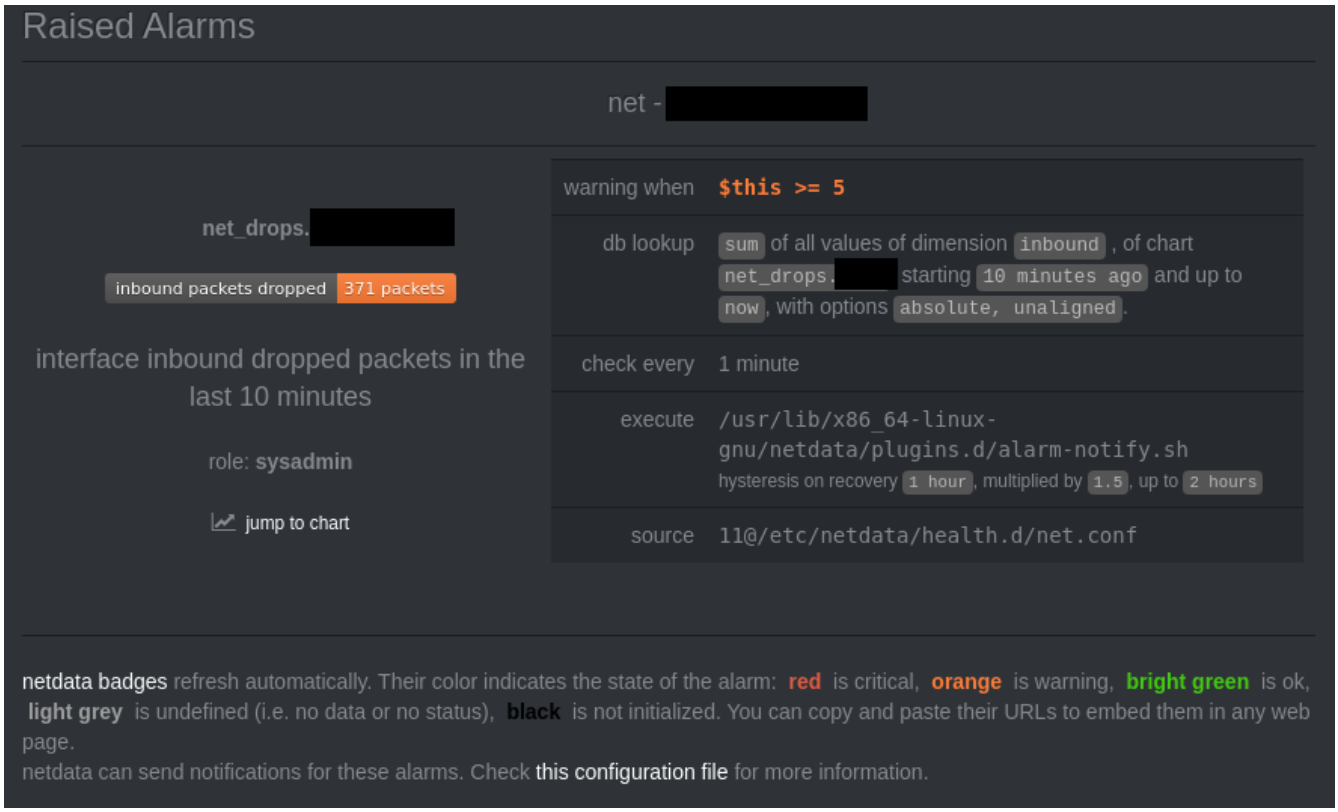
3.2.2 S4A juurutamise valideerimine

S4A juurutamise valideerimiseks on vajalik kontrollida S4A komponentide funktsionaalsust. Järgnevalt esitatakse komponentide Netdata, Arkime, Evebox ning S4A detektori töötamist. Joonistel on peidetud võrgu ning süsteemi andmed musta ristkülikuga.

Netdata tarkvara peab näitama reaalajas andmeid monitooringuserveri kohta, kuhu on paigaldatud S4A sensor. Joonisel 1 on näidatud mõned parameetrid, mida esitab Netdata.

Joonis 1. Ekraanipilt Netdata pealehest

Netdata on võimeline tegema kasutajale teavituse ka kogutud andmete põhjal. Näiteks juhul, kui Netdata tuvastab, et võrguliides on teatud perioodi jooksul kaotanud määratud arvu pakette, siis esitatakse vastav informatsiooni eraldi aknal. Seda olukorda illustreerib Joonis 2.

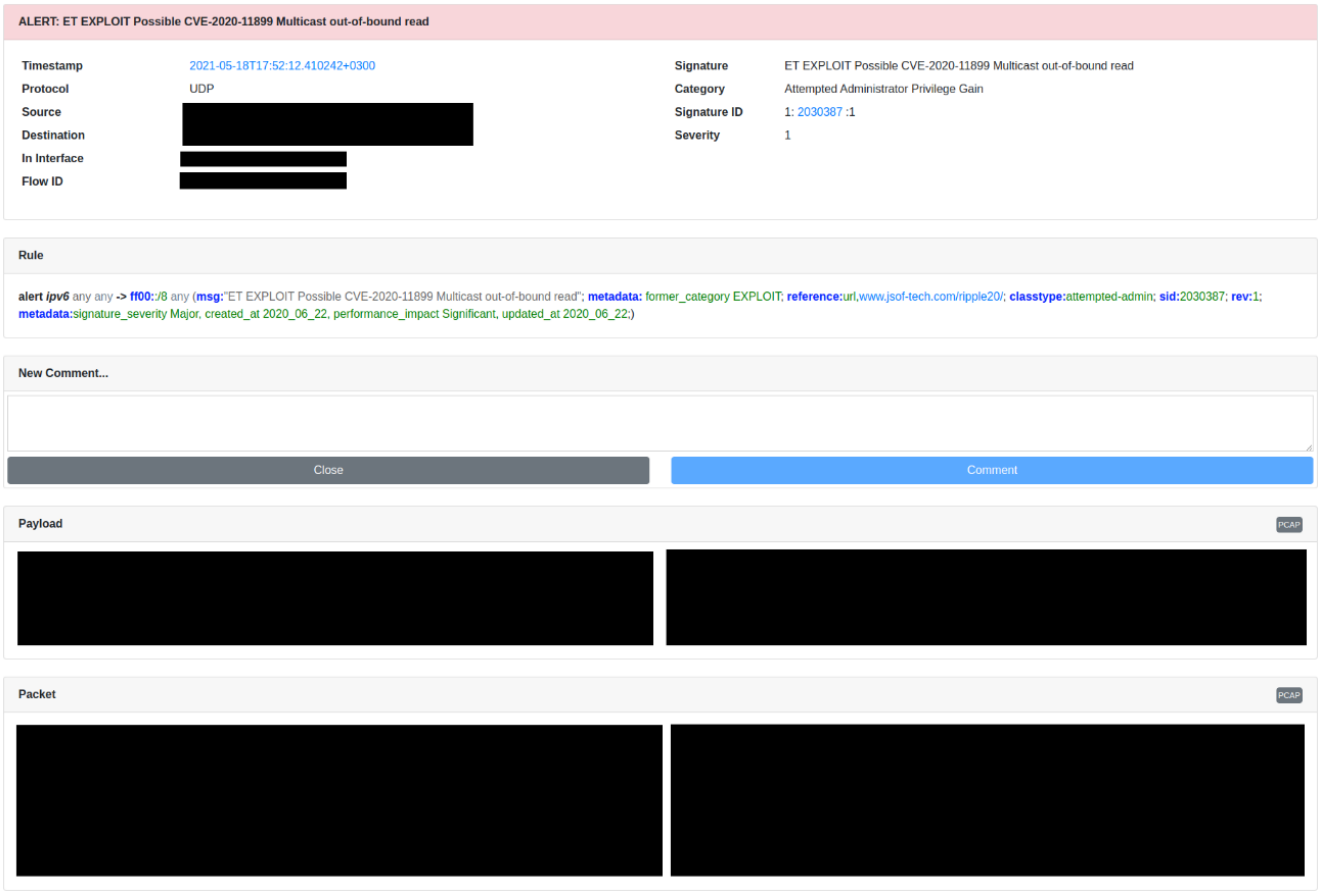


Joonis 2. Netdata teavitus

Arkime'i tarkvara veebiliidese kaudu on võimalik vaadata erinevate protokollide pakette ning uurida nende sisu. Joonisel 3 on kujutatud HTTP päringu sisu vaade.

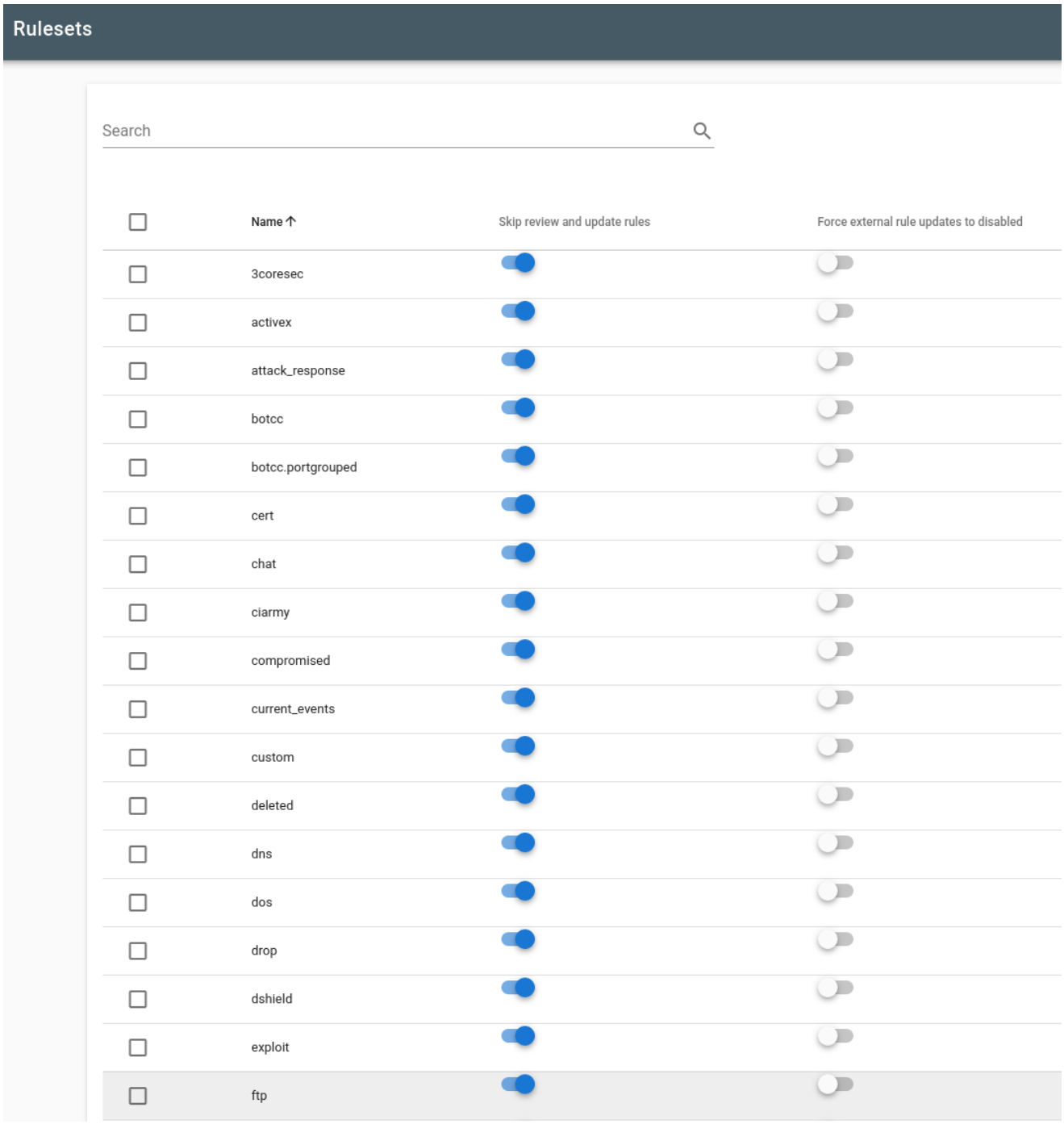
Joonis 3. Paketi sisu vaatamine Arkime's

Evebox teeb kasutajale loetavamaks Suricata Eve JSON väljundi, kus on võimalik lähemalt tutvuda häire tekitanud paketiga ning reegliga, millega see sai tuvastatud. Joonisel 4 on esitatud näide valepositiivse häirest. Paketi sisu uurimiseks on vasakul ASCII vaade ning paremal kuueteistkümnendsüsteemi vaade.



Joonis 4. Evebox'i teavitus võimaliku ründe kohta

Detektori kasutajaliidesega on võimalik näha sensori kohta üldist informatsiooni, nt kas sensor on CERT-EE poolt registreeritud, millal on viimati uuendatud reegleid, milliseid komponente on paigaldatud jne. Detektor võimaldab ka mugavalt hallata Suricata reegleid, nagu on näha Joonisel 5.



Joonis 5. Detektori reeglite kogumike vaade

Kuna Suricata for All komponendid võrgu monitoorimiseks ning sissetungi tuvastamiseks töötavad (võrgumonitooringu serveri parameetrite mõõtmine, pakettide logimine ning analüüsimine, kahtlase liikluse puhul teavituse või häire edastamine ning reeglite haldamine), siis võib järeldada, et lõputöö eesmärk on saavutatud. Praegune olukord nõuab veel teatud hulka tööd. Näiteks tuleb teha asutusesiseses võrgus Wi-Fi seadmete võrguliiklus nähtavaks sensorile, kuna liikluse peegeldamise eest vastutaval kommutaatoril puudub hetkel vajalik konfiguratsioon.

4 Kokkuvõte

Käesolevas lõputöös analüüsiti Eesti ning ühe riigiasutuse küberturvalisuse hetkeolukorda ning selle tulemusel pakuti selle parandamiseks juurutada riigiasutuses sissetungi tuvastuse võrgumonitooringu süsteem Suricata for All.

Esiteks tutvustati lühidalt küberturvalisuse olukorda Eestis, mille jaoks kasutati kolme riigisektori allikat ning vaadati hetkeolukorda viimase kolme aasta jooksul. Riigi Infosüsteemi Ameti küberturvalisuse aastaaruanded andsid teavet üldise hetkeolukorra kohta. Kaitsepolitseiameti väljaanded selgitasid küberturvalisust sisejulgeoleku vaatenurgast. Viimaks, et tuvastada peamised probleemid Eestis küberturvalisuse valdkonnas, uuriti Majandus- ja Kommunikatsiooniministeeriumi küberturvalisuse strateegiat aastateks 2019-2022.

Peale riikliku hetkeolukorra esitamist analüüsiti ühte riigiasutust ning kirjeldati selle küberturvalisuse hetkeseisu ning selle olemasolevaid ressursse. Selle põhjal tehti otsus, et avatud lähtekoodiga võrgupõhine sissetungi tuvastuse süsteem oleks kõige soodsam viis, kuidas maandada küberintsidentidega seotud riske.

Lõputöö raames kirjeldati kolme erinevat sissetungi tuvastuse süsteemi ning võrreldi neid, et leida riigiasutuse vajadustele kõige sobivam lahendus. Analüüsi käigus leiti, et Eesti riigiasutusele on kõige sobivam kasutada S4A, kuna tal on olemas suur osa vajalikust funktsionaalsusest ning on riigiasutusele kergesti kättesaadav.

Järgnevalt kirjeldati S4A arhitektuuri, tarkvara komponente ning nende omavahelist suhtlust, ning soovituslikud riistvaralised nõuded. S4A juurutamisel oli takistuseks asjaolu, et paigutades sensori maksimaalse nähtavusega asukohta, oleks asutusele nähtav ka koostööpartneri võrguliiklus. Selle tõttu tuli sensor paigutada nii, et talle poleks nähtav koostööpartneri võrguliiklus, mille tulemusel piirati monitooritavate seadmete arvu. Hetkeolukorras on asutusel potentsiaalselt võimalik näha enda võrgus paiknevate serverite ning Wi-Fi ühenduste võrguliiklust, kuid mitte statsionaarsete töökohtade võrguliiklust, kuna nende ühenduste eest vastutab baasteenuste partner.

Töö käigus kontrolliti ka S4A peamiste komponentide funktsioneerimist. Netdata komponent raporteerib andmeid riistvara kasutamise kohta, Arkime tarkvaraga on võimalik analüüsida üksikuid võrgupakette, ründe või kahtlase liikluse kohta teeb

teavituse Evebox ning IDS reegleid on võimalik hallata detektori kaudu. Kuna S4A komponendid funktsioneerivad vastavalt spetsifikatsioonile, siis võib järeldada, et S4A oli juurutatud edukalt.

5 Kasutatud kirjandus

[1] M. Erik, „Andmeside kursuse võrguhalduse laboritöö Simple Network Management Protocol baasil,“ [Võrgumaterjal]. Available: https://digikogu.taltech.ee/et/Item/1fbd9122-2ac4-440b-ba6c-7be61b0755d0. [Kasutatud 19 05 2021].

[2] S. Farooghian, „Praktiliste oskuste töötuba - avatud lähtekoodiga sissetungimise turvasüsteemid,“ [Võrgumaterjal]. Available: https://digikogu.taltech.ee/et/Item/9aaa03ee-2deb-499b-be4d-69fd0ad8e144. [Kasutatud 19 05 2021].

[3] A. Kvell, „Suure jõudlusega sissetungi tuvastuse süsteemi lahendus S4A tarkvara jaoks,“ [Võrgumaterjal]. Available: https://dspace.ut.ee/handle/10062/33047. [Kasutatud 19 05 2021].

[4] J. R. Vacca, Computer and Information Security Handbook. Third Edition., Morgan Kaufmann, 2017.

[5] Riigi Infosüsteemi Amet, „Aastakokkuvõte. Küberturvalisus 2019,“ [Võrgumaterjal]. Available: https://www.ria.ee/sites/default/files/content-editors/kuberturve/kuberturvalisus-2019.pdf. [Kasutatud 10 05 2021].

[6] Riigi Infosüsteemi Amet, „Aastakokkuvõte. Küberturvalisus 2020,“ [Võrgumaterjal]. Available: https://www.ria.ee/sites/default/files/content-editors/RIA/cyber_security_in_estonia_2020_0.pdf. [Kasutatud 10 05 2021].

[7] Riigi Infosüsteemi Amet, „Aastakokkuvõte. Küberturvalisus 2021,“ [Võrgumaterjal]. Available: https://www.ria.ee/sites/default/files/content-editors/kuberturve/kuberturvalisus-2021.pdf. [Kasutatud 10 05 2021].

[8] Kaitsepolitseiamet, „Aastaraamat 2018,“ [Võrgumaterjal]. Available: https://kapo.ee/sites/default/files/public/content_page/Aastaraamat-2018.pdf. [Kasutatud 10 05 2021].

[9] Kaitsepolitseiamet, „Aastaraamat 2019 - 2020,“ [Võrgumaterjal]. Available: https://kapo.ee/sites/default/files/public/content_page/Aastaraamat_2019_2020.pdf. [Kasutatud 10 05 2021].

[10] Kaitsepolitseiamet, „Aastaraamat 2020 - 2021,“ [Võrgumaterjal]. Available: https://kapo.ee/sites/default/files/public/content_page/Aastaraamat-2020-2021.pdf. [Kasutatud 10 05 2021].

[11] Majandus- ja Kommunikatsiooniministeerium, „Küberturvalisuse strateegia 2019-2022,“ [Võrgumaterjal]. Available: https://www.mkm.ee/sites/default/files/kuberturvalisuse_strateegia_2019-2022.pdf. [Kasutatud 10 05 2021].

[12] Poliitikauuringute Keskus Praxis, „Küberturbe valdkonna tööjõuvajaduse ja hariduse uuringu aruanne 29.03.2019,“ [Võrgumaterjal]. Available: https://www.mkm.ee/sites/default/files/kuberturbe_uuring_aruanne_23_04_2019.pdf. [Kasutatud 10 05 2021].

[13] The Zeek Project, „Zeek Documentation. About Zeek,“ [Võrgumaterjal]. Available: https://docs.zeek.org/en/current/about.html. [Kasutatud 10 05 2021].

[14] The Zeek Project, „Zeek Documentation. Monitoring With Zeek,“ [Võrgumaterjal]. Available: https://docs.zeek.org/en/current/monitoring.html. [Kasutatud 10 05 2021].

[15] Open Information Security Foundation, „6.37. Differences From Snort,“ [Võrgumaterjal]. Available: https://suricata.readthedocs.io/en/latest/rules/differences-from-snort.html. [Kasutatud 10 05 2021].

[16] The Snort Project, „Why Snort 3?,“ [Võrgumaterjal]. Available: https://snort.org/snort3. [Kasutatud 10 05 2021].

[17] The Snort Project, „Snort Overview,“ %1 *SNORT © Users Manual 2.9.16*, 2020, p. 9.

[18] The Snort Project, „Snort FAQ. What are the differences in the rule sets?,“ [Võrgumaterjal]. Available: https://www.snort.org/faq/what-are-the-differences-in-the-rule-sets. [Kasutatud 10 05 2021].

[19] The Snort Project, „Snort 3 officially released,“ [Võrgumaterjal]. Available: https://blog.snort.org/2021/01/snort-3-officially-released.html. [Kasutatud 10 05 2021].

[20] Open Information Security Foundation, „Suricata dokumentatsioon. 1. What is Suricata,“ [Võrgumaterjal]. Available: https://suricata.readthedocs.io/en/latest/what-is-suricata.html. [Kasutatud 10 05 2021].

[21] Open Information Security Foundation, „Complete list of Suricata Features,“ [Võrgumaterjal]. Available: https://suricata-ids.org/features/all-features/. [Kasutatud 20 05 2021].

[22] CERT EE, „What is Suricata for All,“ [Võrgumaterjal]. Available: https://docs.s4a.cert.ee/source/what_is_s4a.html. [Kasutatud 10 05 2021].

[23] Security Onion Solutions, „About Security Onion,“ [Võrgumaterjal]. Available: https://docs.securityonion.net/en/2.3/about.html. [Kasutatud 10 05 2021].

[24] RockNSM Foundation, „ROCK NSM - An open source Network Security Monitoring platform.,“ [Võrgumaterjal]. Available: http://rocknsm.io/. [Kasutatud 10 05 2021].

[25] The Zeek Project, „Zeek Documentation. Cluster Architecture,“ [Võrgumaterjal]. Available: https://docs.zeek.org/en/v4.0.1/cluster-setup.html#cluster-architecture. [Kasutatud 10 05 2021].

[26] The Zeek Project, „The Zeek Network Security Monitor,“ [Võrgumaterjal]. Available: https://github.com/zeek/zeek#license. [Kasutatud 10 05 2021].

[27] CERT-EE, „Install Detector,“ [Võrgumaterjal]. Available: https://docs.s4a.cert.ee/source/install.html. [Kasutatud 10 05 2021].

[28] CERT-EE, „Detector GUI user manual.,“ [Võrgumaterjal]. Available: https://docs.s4a.cert.ee/source/detector_ui.html. [Kasutatud 10 05 2021].

[29] CERT-EE, „System technical overview,“ [Võrgumaterjal]. Available: https://docs.s4a.cert.ee/source/system_overview.html. [Kasutatud 10 05 2021].

Lisa 1 – Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks[1]

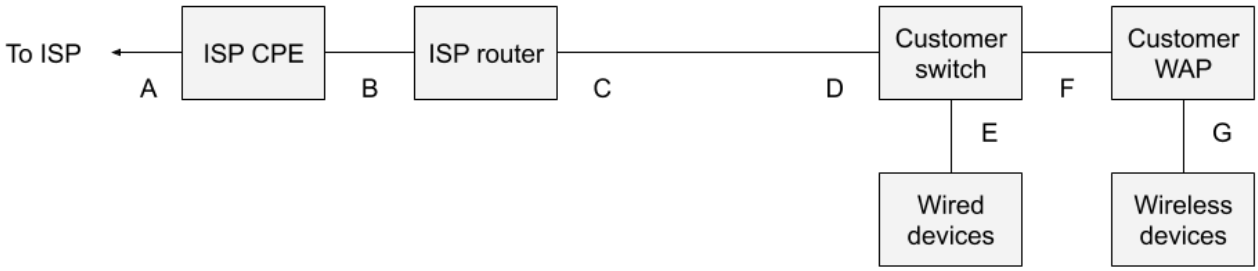
Mina, Edvard Paas

1. Annan Tallinna Tehnikaülikoolile tasuta loa (lihtlitsentsi) enda loodud teose „Võrguliikluse seire ja sissetungi tuvastuse süsteemi juurutamine ja analüüs S4A baasil“, mille juhendaja on Avo Ots
   1.1. reprodutseerimiseks lõputöö säilitamise ja elektroonse avaldamise eesmärgil, sh Tallinna Tehnikaülikooli raamatukogu digikogusse lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;
   1.2. üldsusele kättesaadavaks tegemiseks Tallinna Tehnikaülikooli veebikeskkonna kaudu, sealhulgas Tallinna Tehnikaülikooli raamatukogu digikogu kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.
2. Olen teadlik, et käesoleva lihtlitsentsi punktis 1 nimetatud õigused jäävad alles ka autorile.
3. Kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest ning muudest õigusaktidest tulenevaid õigusi.

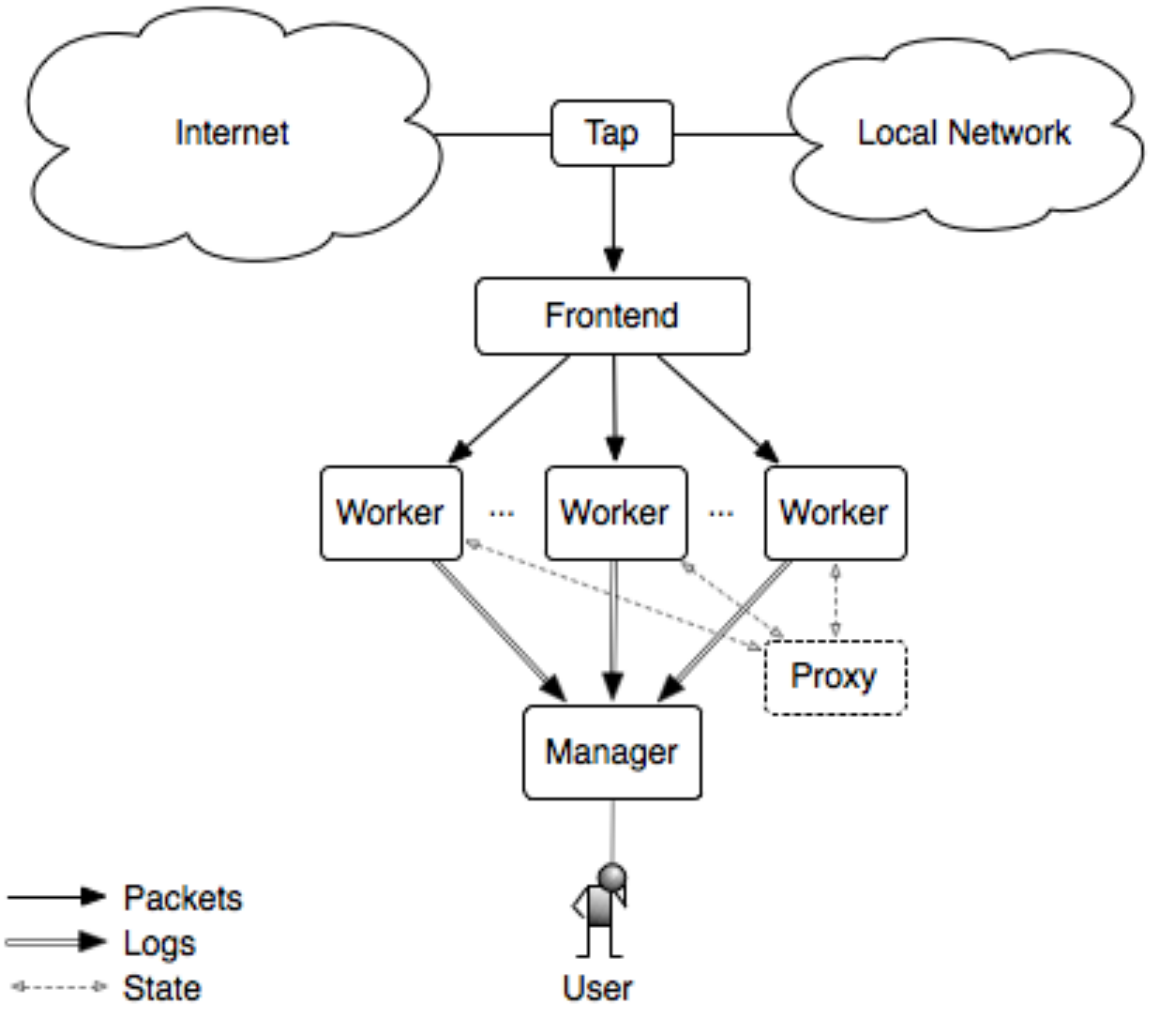
21.05.2021

1 Lihtlitsents ei kehti juurdepääsupiirangu kehtivuse ajal vastavalt üliõpilase taotlusele lõputööle juurdepääsupiirangu kehtestamiseks, mis on allkirjastatud teaduskonna dekaani poolt, välja arvatud ülikooli õigus lõputööd reprodutseerida üksnes säilitamise eesmärgil. Kui lõputöö on loonud kaks või enam isikut oma ühise loomingulise tegevusega ning lõputöö kaas- või ühisautor(id) ei ole andnud lõputööd kaitsvale üliõpilasele kindlaksmääratud tähtajaks nõusolekut lõputöö reprodutseerimiseks ja avalikustamiseks vastavalt lihtlitsentsi punktidele 1.1. ja 1.2, siis lihtlitsents nimetatud tähtaja jooksul ei kehti.

Lisa 2 – Zeek tarkvara monitoorimise lahendused

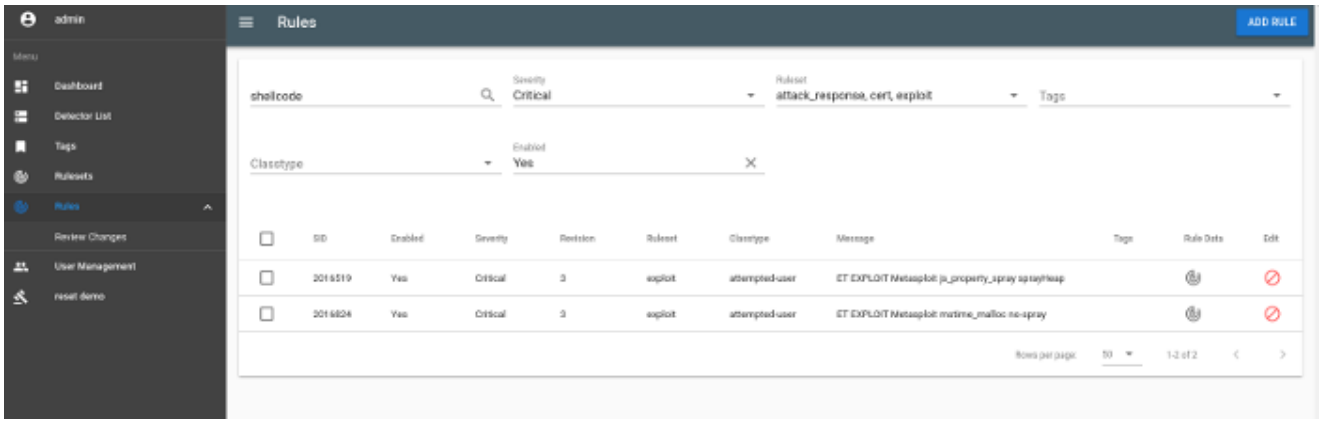


Joonis 6. Lihtsustatud võrgu topoloogia [14]

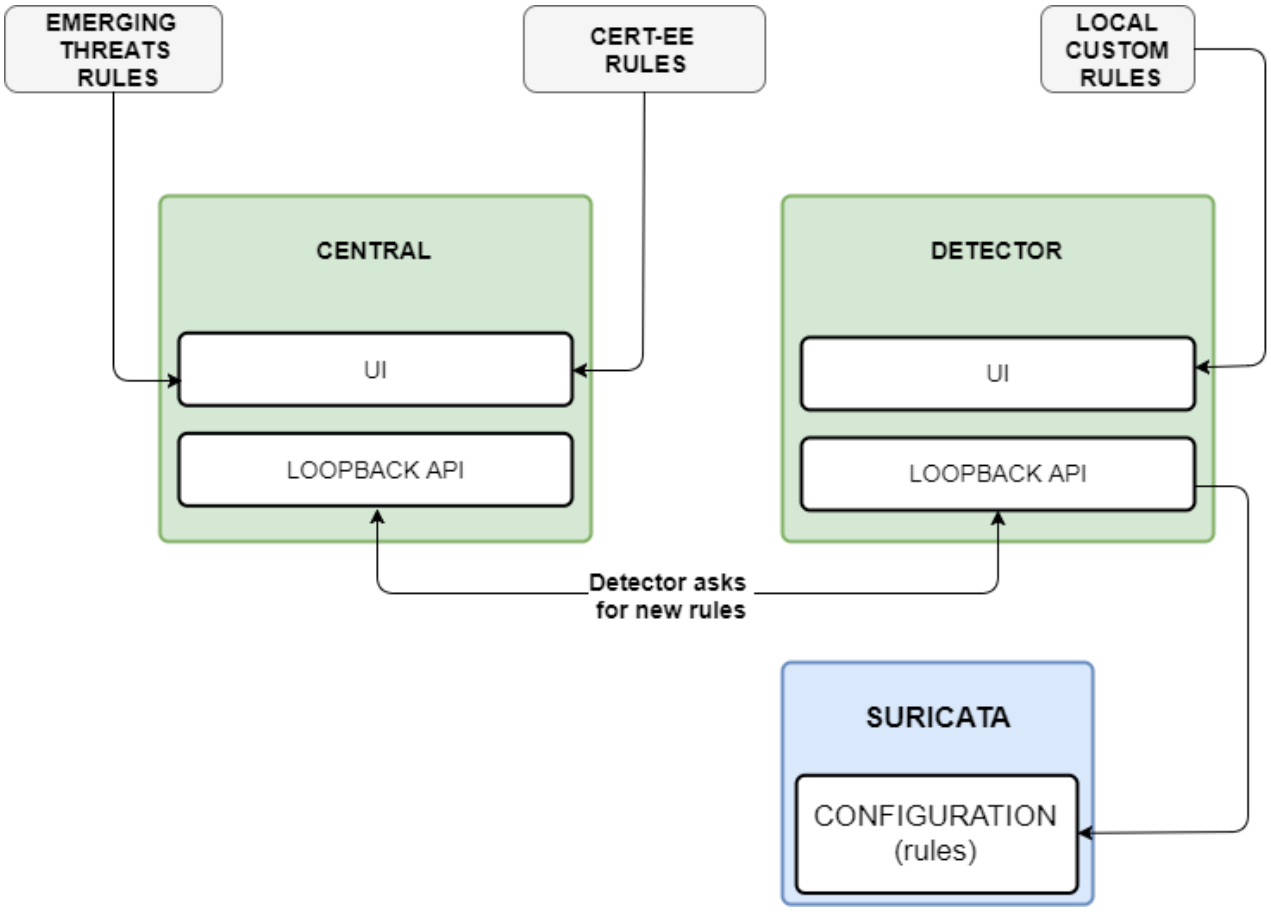


Joonis 7. Zeek'i klastri arhitektuur [25]

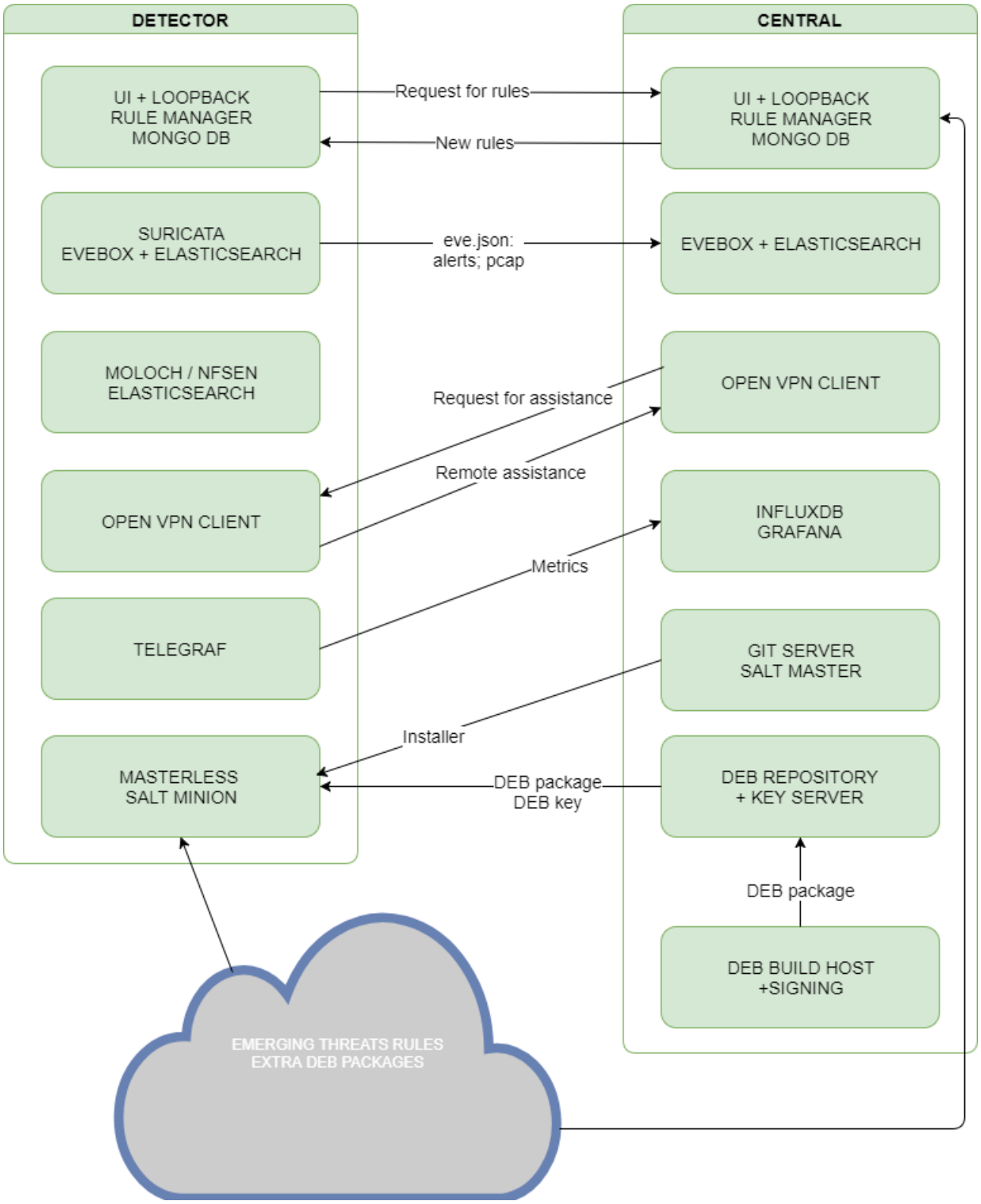
Lisa 3 – S4A tarkvara arhitektuur



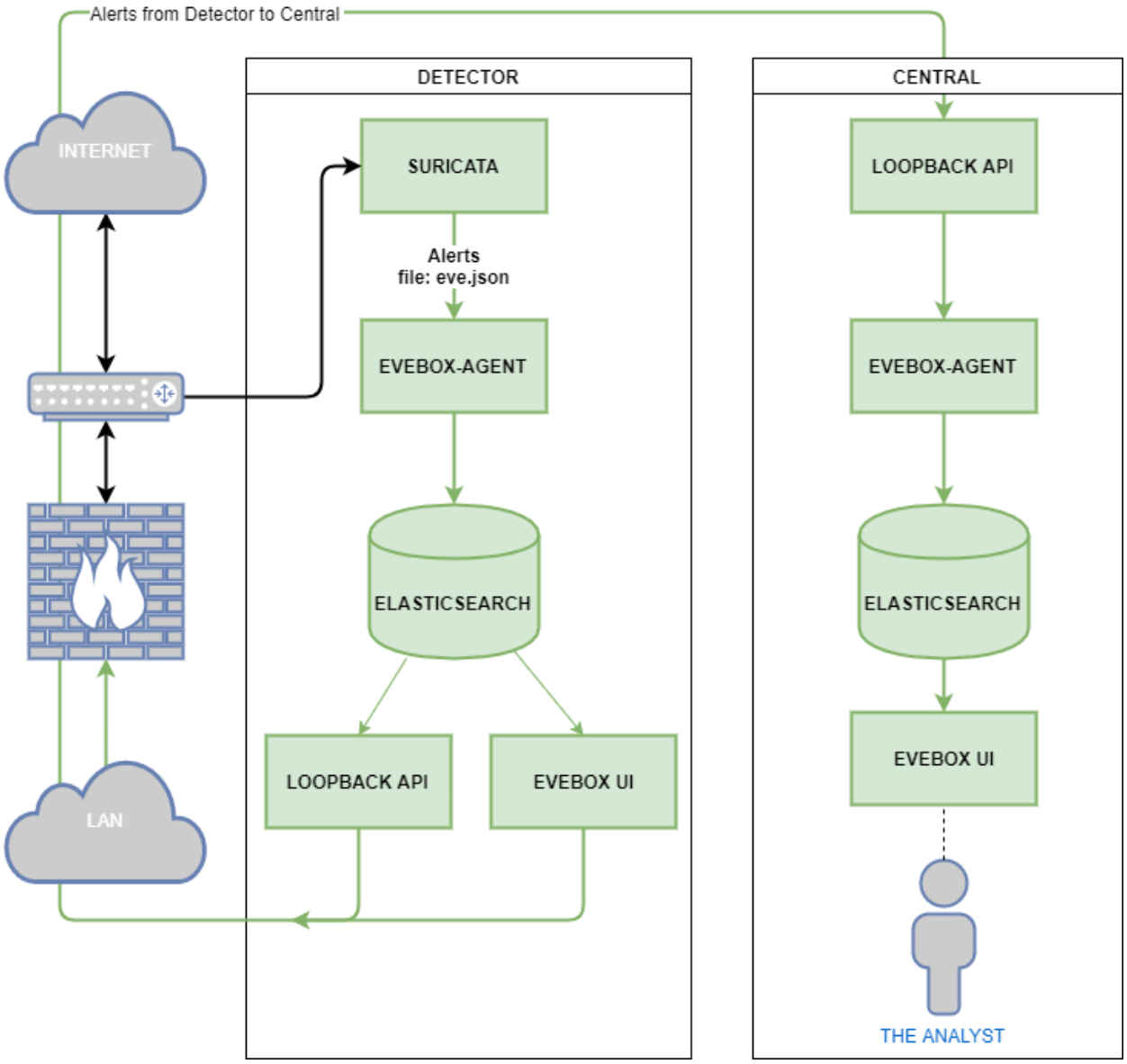
Joonis 8. IDS reeglite määramine S4A kasutajaliideses. [28]



Joonis 9. S4A reeglite haldus [29]



Joonis 10. S4A süsteemide vaheline integratsioon. [29]



Joonis 11. S4A teavituste voodiagramm [29]