TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Kuldar Teinmann 175920IDAR

Ohujahtimise platvormi lahenduse valik ja rakendamine

Diplomitöö

Juhendaja: Siim Vene
MSc

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: Kuldar Teinmann

29.04.2021

Annotatsioon

Käesolevas lõputöös analüüsitakse võimalikke tarkvaralahendusi ohujahtimise läbiviimiseks sobiva lahenduse leidmiseks.

Asutuste ja ettevõtete küberturvalisuse tagamine on muutumas järjest keerulisemaks, sest ründed on muutumas tehniliselt keerulisemateks ning tihti finantsiliste eesmärkide tõttu konkreetsemalt suunatuteks. Ründajad muudavad pidevalt enda taktikatid ja tehnikaid tuvastuse vältimiseks, mistõttu on neid klassikalise turvateabe ja -sündmuste haldamise lahendustega keerulisem tuvastada. Ohujahtimise eesmärk on lähtuvast ohust sõltuvalt teostada proaktiivseid tegevusi eeldatava ründaja tegevuse tuvastamiseks asutuse võrgus. Ohujahtimise teostamiseks on vajalik lõppseadmetest logide kogumine ja talletamine ning vahendid logide analüüsimiseks.

Lõputöös leitakse võimalikud tarkvaralised lahendused, mida võrreldakse töös kirjeldatud nõuetest lähtuvalt. Võrdluse tulemusena valitakse sobivaim lahendus, mille põhjal teostatakse praktiline lahendus.

Lõputöö on kirjutatud eesti keeles ning sisaldab teksti 33 leheküljel, 7 peatükki, 12 joonist, 1 tabel.

Abstract

Threat Hunting system implementation

In this thesis, author focuses on analyzing different software platforms and solutions in order to identify the best threat hunting solution accordance to the set requirements.

The importance of cyber security is becoming more and more valuable to businesses and institutions due to cyber attacks becoming increasingly sophisticated and highly targeted. The threat actors landscape is ever increasing and their TTP-s are constantly evolving to avoid detection. This makes it challenging for the defenders to protect their assets and detect malicious activity with the traditional mainstream security information and event management solutions.
The goal of threat hunting is to take a proactive approach in handling threats. This requires collecting and storing the data and logs from endpoint devices in order to have them meaningfully analyzed.

With this thesis the possible threat hunting software platforms are identified in accordance of the set requirements. After comparison and analysis of the solutions the best option is selected and on the basis of which a practical solution is implemented.

The thesis is in estonian and contains 33 pages of text, 7 chapters, 12 figures, 1 table.

Lühendite ja mõistete sõnastik

AAPI	*Application Program Interface*, programmiliides
AWS	*Amazon Web Services,* Amazoni pilveandmetöötluse platvorm
GPO	*Group Policy Object*, Microsoft operatsioonisüsteemide grupipoliitika
JSON	*JavaScript Object Notation*, lihtsustatud andmevahetusvorming
SaaS	Software as a Service, tarkvara teenusena
SCCM	System Center Configuration Manager
PGP	Pretty Good Privacy
TLS	Transport Layer Security, transpordikihi turbeprotokoll
TTP	Tactics, techniques and procedures, Taktikad, tehnikad ja protseduurid
UEBA	User Entity Behaviour Analytics, kasutajakäitumise analüüs Pretty

Sisukord

Sissejuhatus 9
1 Ülesande püstitus 10
2 Lõputöö lähtekohad 11
2.1 Nõuete kirjeldus 11
2.2 Metoodika kirjeldus 12
3 Ohujahtimine 12
3.1.1 Ohujahtimise tsükkel 13
4 Lahenduste valik 14
4.1 Esmane valik 15
4.2 Põhivalik 17
4.2.1 Elastic Stack 17
4.2.2 Splunk Enterprise 19
4.2.3 IBM Qradar 21
4.3 Valiku tegemine 23
5 Valitud lahenduse kirjeldus 25
5.1 Lahenduse ülesehitus 25
5.2 Juurutusplaan 27
6 Paigaldamine ja seadistamine 28
6.1 Elastic 28
6.2 MISP integratsioon 29
7 Tuvastustestide läbiviimine 30
7.1 Pahaloomuline e-maili manus 30
7.2 Indikaatoripõhine tuvastus 31
Kokkuvõte 33
Kasutatud kirjandus 34
Lisa 1 – Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks 36

Jooniste loetelu

Joonis 1. Gartner Magic Quadrant for SIEM [6] 15
Joonis 2. Elasticsearch loogiline disain [25] 18
Joonis 3. Splunk loogiline disain [8] 20
Joonis 4. QRadar loogiline disain [14] 21
Joonis 5. Valitud lahenduse ülevaade 25
Joonis 6. MISP tarkvarast sünkroniseeritud indikaator 29
Joonis 7. winword.exe poolt käivitatud powershelli protsess 30
Joonis 8. Pahaloomuline dokument 31
Joonis 9. Allalaetud võimalik pahaloomuline fail 31
Joonis 10. Registreeritud häire 31
Joonis 11. Indikaatori väljade sidumine 32
Joonis 12. Indikaatori tuvastamise häire 32

Tabelite loetelu

Tabel 1. Põhivalikute võrdlus 24

Sissejuhatus

Olukord kübermaastikul on muutumas järjest karmimaks – küberründed muutuvad nii tehniliselt kui iseloomult aina keerulisemaks ning tekitatud kahjud suuremaks. Tehniliselt keerukate rünnakute tõttu on asutustele ning ettevõtetele suureks ohuks eelkõige kinnisründed ning lunavarakampaaniad. Viimaste tuvastamine klassikaliste võrguturbe vahenditega on tihti väga raske. Küberturbefirma FireEye 2021 aasta raporti kohaselt saab ründaja tegutseda keskmiselt 24 päeva enne, kui tema kohalolek arvutivõrgus tuvastatakse [1]. Kõnekaim näide on 2020 aastal toimunud SolarWinds'i kampaania, mille puhul asutuste võrkudes tegutseti mitmeid kuid enne, kui välise info abil ründed tuvastati.

Lõputöös käsitletav asutus on otsustanud luua võimekuse, mille abil kogutavatest logidest otsida pahaloomulisi indikaatoreid ning tegevusi, mis on automaattuvastusest mööda pääsenud. Loodava lahenduse eesmärk on aidata tuvastada ründaja tegevused asutuse võrgus võimalikult kiiresti, hoides sellega ära potentsiaalselt suurema kahju tekitamise.

Järgnev lõputöö on jagatud nelja etappi, millest esimesed kolm on teoreetilised ning neljas praktiline.

Töö esimeses osas kirjeldatakse ülesande püstitus ning asutuse nõuded loodavale lahendusele.

Töö teises osas leitakse ning valitakse välja võimalikud lahendusvariandid ning teostatakse võrdlev analüüs sobiva tarkvara leidmiseks.

Kolmandas osas kirjeldatakse väljavalitud lahenduse planeeritavat ülesehitust.

Neljandas osas teostatakse praktiline lahendus ning viiakse läbi tuvastustestid.

1 Ülesande püstitus

Lõputöös käsitletava asutuse IT-üksus pakub IT taristu, infosüsteemide ja turbeteenuseid asutuse siseselt. Tulenevalt tõusvatest riskidest kübermaastikul, viidi asutuse juhtkonna tellimusel välise teenusepakkuja poolt läbi riskianalüüs. Analüüsi tulemusel hinnati muuhulgas peamisteks ründeohtudeks lunavarakampaaniad (sh. võimalik kaasnev andmeleke) ning asutuse töövaldkonnast tulenevalt kinnisründe ohud. Arvestades mõlema ründeohu tehnilist keerukust ning võimekusi, otsustas asutus rakendada täiendavaid turbemeetmeid võimaliku ründaja tuvastamiseks.

Peamised asutuse poolt määratud piirangud lahenduse valikul:

- Peab olema võimalike kasvavate mahtude tõttu skaleeritav
- Tulenevalt majanduslikust olukorrast, ei tohi kaasa tuua märkimisväärseid rakendus- ja püsikulusid platvormi töös hoidmiseks

Antud töö eesmärk on leida tehnilised tarkvaralahendused ja valikud ohujahtimise läbiviimiseks ning teostada tuvastustestimised.

Ohujahtimiseks vajaliku lahenduse ja tarkvara leidmiseks on autoril planeeritud järgmised tegevused:

- Selgitada välja asutuse nõuded loodavale lahendusele
- Leida võimalikud lahendusvariandid ning teostada analüüs sobivate tarkvarade leidmiseks
- Kirjeldada väljavalitud lahenduse planeeritavat ülesehitust
- Teostada praktiline lahendus
- Teostada tuvastustestimised

Lõputöö tulemusena luuakse asutuse püstitatud nõuetele vastav ohujahtimise platvorm, kirjeldatakse edasised platvormi arengutegevused ning viiakse läbi simuleeritud ründetegevused tuvastuste testimiseks.

2 Lõputöö lähtekohad

Käesolevas peatükis kirjeldab autor asutuse poolt määratud nõuded ohujahtimise platvormile ning lõputöö tegemiseks kasutatavad metoodikad.

2.1 Nõuete kirjeldus

Asutuse nõuded loodavale lahendusele on kirjeldanud töö autor. Sisendi otsuste tegemiseks on töö autor saanud vestluse käigus turbeteenuste meeskonna ning asutuse infoturbejuhiga.

Asutuse nõuded loodavale lahendusele:

- Planeeritava lahenduse hilisem riistvaralise ressurssi lisamine ei tohi nõuda suurt lisatööd. Loodav lahendus peab olema kergesti skaleeritav.
- Kogu taristu peab asuma asutuse halduses ning olema majutatud asutuse IT taristul.
- Planeeritav lahendus peab olema tõrkekindel, et tagada kõrgkäideldavus.
- Platvorm peab olema sobilik logide pikemaajaliseks säilitamiseks (5 aastat).
- Platvorm peab võimaldama indikaatoripõhist tuvastamist ning teavitamist.
- Peab omama integratsioonivõimekust ohuteadmusbaasi tarkvaraga MISP.
- Logikirjeid peab olema võimalik analüütiku poolt määratud väljade järgi korreleerida ning töödelda.

- Modulaarne ülesehitus, mis võimaldab vajadusel uut funktsionaalsust integreerida.

2.2 Metoodika kirjeldus

Töö lahendamiseks kasutab autor kvalitatiivset analüüsi. Selle käigus leitakse esmased sobivad lahendusvariandid ning uuritakse nende funktsionaalsust ja vastavust asutuse määratud nõuetega. Uurimise tulemusi võrreldakse, mille järel valitakse välja sobivaim lahendus.

3 Ohujahtimine

Ohujahtimine on inimese poolt juhitud, proaktiivne ja korduv otsingute teostamine arvutivõrkude, tööjaamade, serverite ja teistest logiandmetest. Jahtimisel eeldatakse alati, et asutuse arvutivõrk on juba ründaja poolt kompromiteeritud.
Ohujahtimise eesmärk on otsida märke pahaloomulise tegevuse kohta asutuse arvutivõrgus, mis on automaattuvastusest mööda pääsenud ning ära hoida järgneda võiv suurem kahju [2].

Ohujahtimise saab jagada viieks tüübiks [3]:

- Andmepõhine jahtimine (*Data-driven*) – Hüpoteeside seadmine ja jahtimine olemasolevate logide alusel. Näiteks *netflow* olemasolu korral saab hakata tuvastama anomaalseid andmevahetuse mahtusid.

- Teadmuspõhine jahtimine (*Intel-driven*) – Hüpoteeside seadmine ja jahtimine ohuteadmuse alusel. Ohuteadmus võib tulla nii avalikest kui ka kommerts allikatest, koostööpartneritelt ning asutuse enda intsidendihalduse tulemustest.

- Olemipõhine jahtimine (*Entity-driven*) – Jahtimise valdkond on lai ning tööjõud alati piiratud, mistõttu ei jõuta alati katta kogu arvutivõrku. Oluline on määratleda asutuse jaoks kõrge väärtusega ja/või riskiga olemid, millele seejärel jahtimisel

saab keskenduda. Olemi, riski ja väärtuse määratlemisel tuleb olukorrapõhiselt hinnata ka potentsiaalse ründaja eesmärke.

- Ründajapõhine jahtimine (*TTP-driven*) – Ründekampaaniate tuvastamisel on oluline mõista ründaja tehnikaid, taktikaid ja protseduure (TTP), mille põhjal hüpoteesid seada ning jahtimist läbi viia.

- Hübriid (Hybrid) – Üldjuhul hõlmab jahtimine mitut tüüpi koos. Ohuteadmuse põhjal võib tulla informatsiooni käimasoleva ründekampaania kohta ning kirjeldada selle tehnikaid, taktikatid ja protseduure ning kirjeldada kampaania sihtmärgiks olevad olemid, millele jahtimisel tugineda.

Ohujahtimine on enamjaolt hüpoteesipõhine – esmalt seatakse küsimus või hüpotees potentsiaalselt toimunud pahaloomulise tegevuse kohta ning seejärel hakatakse püstitatud olukorda tuvastama. Jahtimise eesmärk on saada seatud hüpoteesile kinnitus või see ümber lükata. Seatud hüpoteesi alusel jahi läbiviimiseks peavad olemas olema kõik vajalikud sisendlogid [4].

3.1.1 Ohujahtimise tsükkel

Ohujahtimise läbiviimise juures on oluline, et see oleks planeeritud ning kogu tsükkel oleks hallatud. Endise USA küberturbe ning ohujahtimise valmisplatvormi pakkuva firma Sqrrl Data Inc. poolt on välja töötatud ohujahtimise tsükkel, mis on valdkonnas laialdast kasutus leidnud [5].

Sqrrl ohujahtimise tsüklis on neli sammu:

a) Hüpoteeside loomine – Seatud hüpoteesil peab olema alus. Selleks võib olla ohuteadmusest tulnud informatsioon või jahtija eelnevast kogemusest tulenev hinnang. Hüpotees võib tuleneda ka esinenud anomaaliast või analüütiku tähelepanekust, et leitud infokild ei tundu tema jaoks õige.

b) Jahtimise tehniline teostamine – Kasutades olemasolevaid tööriistu ja platvorme teostatakse ohujahtimine, toimub toor- ja töödeldud andmetest otsimine ning sündmuste korreleerimine. Selles sammus seatud hüpotees kinnitatakse või lükatakse ümber. Oluline on arvestada, et hüpoteesile kinnituse mitte leidmine ei tähenda automaatselt eeldatud pahaloomulise tegevuse puudumist.

c) Leitud mustrite ja TTP'de kirjeldamine – jahtimise teostamisel võib avastada uusi ründaja mustreid ning tehnikaid, taktikaid ja protseduure. Oluline on kõik leiud dokumenteerida ning vajadusel leidude põhjal uus hüpotees seada.

d) Automatiseerimine – jahtimine on korduv tegevus, mistõttu on oluline õnnestunud jahtimine dokumenteerida ning selle edasine läbiviimine automatiseerida. Nii saab kokku hoida tööjõu aega ning keskenduda järgmiste jahtimiste planeerimisele.

4 Lahenduste valik

Ohujahtimise teostamise eelduseks on vajalike logide kogumine ja talletamine. Logihalduseks kasutatakse üldjuhul turvateabe ja -sündmuste halduslahendust (SIEM), mille eesmärk on erinevatest allikatest logide kogumine ning nende normaliseerimine, korreleerimine, klassifitseerimine. SIEM abil on võimalus monitoorida ning saada teavitusi arvutivõrgus ning seadmetes toimuvast. Ohujahtimise läbiviimiseks on võimalik kasutada ka logide talletamiseks andmejärvesid. Andmejärved võimaldavad talletada erinevat tüüpi andmeid, mis tagab ohujahtimise teostamisel analüütikule laiema pildi ühes töövahendis.

Joonis 1. Gartner Magic Quadrant for SIEM [6]

Tarkvaralahenduste valiku tegemise aluseks on „Gartner Magic Quadrant for Security Information and Event Management“ [6]. Nimekirja on lõputöö autori poolt lisatud Elastic Stack, mille puhul on tegemist ohujahtimiseks laialt kasutatava logide talletamise ja analüüsi platvormiga [7].

4.1 Esmane valik

Esmase valiku tegemiseks on autor valinud nõuded, millele peavad tarkvaralahendused vastama:

- Lahendus peab olema kergesti skaleeritav

- Tarkvara peab olema võimalik paigaldada asutuse andmekeskuses (*on-premise*) ning olema täielikult asutuse halduses

- Lahendus ei tohi olla tarkvaratootja riistvarast sõltuv

Järgnevalt on kirjeldatud esmased valikud ning nende sobivus antud lahendusega:

- **Splunk Enterprise –** Splunk Enterprise on logiandmete kogumiseks, indekseerimiseks, otsimiseks, analüüsimiseks ning visualiseerimiseks. Splunk omab laia lisarakenduste baasi, mille abil on võimalik tarkvara funktsionaalsust laiendada. Splunk Enterprise põhitarkvarale on võimalik juurde soetada mitmeid lisatarkvarasid, näiteks Enterprise Security (SIEM funktsionaalsus) või User Behavior Analytics (UBA). Kõik lisatarkvarad litsentseeritakse eraldi [8].

- **IBM QRadar** – IBM QRadar on tooteperekond, kuhu kuuluvad QRadar SIEM, QRadar User Behavior Analytics, QRadar Network Insights, QRadar Data Store ja mitmed muud turbe eesmärgilised tarkvarad. QRadar SIEM on logiandmete kogumiseks ja parsimiseks ning sündmuste korreleerimiseks ja teavituste saatmiseks. IBM QRadar omab laia integratsioonivõimekust paljude IBM ja kolmanda osapoole tarkvaradega. QRadar SIEM'i on võimalik paigaldada nii *on-premise*, kui ka pilvelahendusena.

- **Securonix –** Securonix SIEM platvorm koosneb SIEM, andmejärve, UEBA, SOAR ning mitmest muust toetavast turbekomponendist. Securonix SIEM on SaaS põhine teenus, mida pakutakse AWS keskkonnas [6].

- **Rapid7** – Rapid7 *Insight* tooteplatvormi SIEM komponendiks on InsightIDR rakendus. InsightIDR on SaaS põhine teenus, mida pakutakse AWS keskkonnas [6].

- **LogRythm** – LogRythm SIEM platvormi põhikomponent on XDR Stack, mis koosneb DetectX, AnalytiX ja RespondX toodetest. AnalytiX on logide kogumiseks ning kestseks haldamiseks, DetectX loob analüütika ja visualiseerimise osa ning RespondX on intsidendihalduse funktsionaalsus. Lisaks on võimalik liidestada tooteid UserXDR, Network XDR, SysMon ning NetMon.

LogRythm platvormi on võimalik paigaldada nii *on-premise*, kui ka pilvelahendusena. [9]

- **Elastic Stack -** Elasticsearch on hajutatud otsingu- ja analüüsimootor, mis pakub peaaegu reaalajas andmete otsimist ja analüüsimist. Elastic Stack'i kuulub Kibana, mis pakub esmast analüüsi ja visualiseerimise, samuti klastri haldamise võimekust. Elasticsearch omab stabiilset ja skaleeruvat ülesehitust ning integratsioonivõimekusi paljude turbetarkvaradega [10].

Valitud nõuetele ei vasta Rapid7 ning Securonix lahendused, sest neil puuduvad *on-premise* paigalduse võimalused. LogRythm puuduseks luges autor asjaolu, et kuigi ametliku dokumentatsiooni järgi on kolmanda osapoole riistvara kasutamine toetatud, siis väga tugevalt suunatakse LogRythm enda seadmeid (*appliance*) kasutama. Esmase valiku põhjal valis autor edasiseks võrdlemiseks Splunk Enterprise, IBM QRadar ning Elastic Stack lahendused.

4.2 Põhivalik

Ohujahtimise platvormi logide talletamise lahenduse valikul on kriteeriumid:

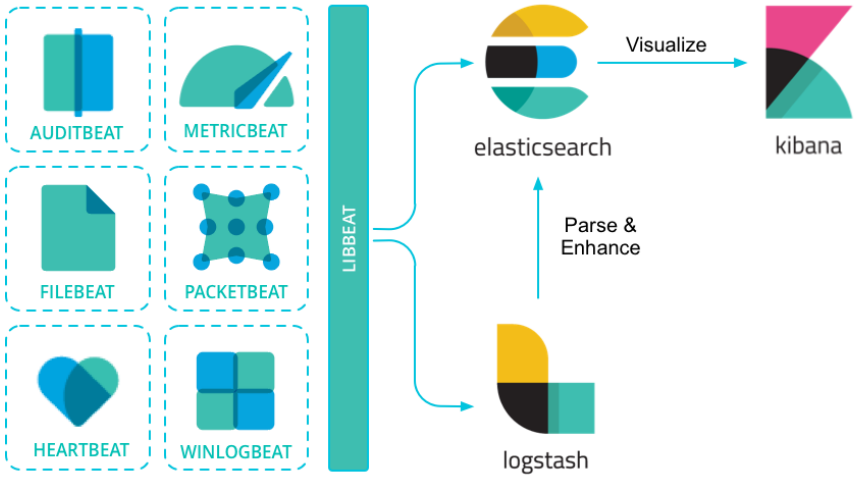
- Peab võimaldama indikaatoripõhist tuvastamist ning teavituste saatmist
- Peab omama integratsioonivõimekust ohuteadmusbaasi tarkvaraga MISP
- Peab võimaldama graafilist visualiseerimist ning kohaldatavate töölaudade (*dashboard*) loomist
- Tagatud peab olema kõrgkäideldavus
- Peab olema võimalikult väikese juurutamis- ja ülalpidamiskuluga

4.2.1 Elastic Stack

Elasticsearch on hajutatud otsingu- ja analüüsimootor, mis pakub peaaegu reaalajas andmete otsimist ja analüüsimist ning on Elastic Stacki keskmeks. Elasticsearch hoiustab andmeid JSON vormingus dokumentides. Kui kasutusel on mitme õlaga klaster, jaotatakse salvestatud dokumendid klastrisse ning neile pääseb ligi igast sõlmest. Elasticsearch kasutab andmestruktuuri, mida nimetatakse ümberpööratud indeksiks

(*inverted index*) ning mis võimaldab väga kiireid täistekstiotsinguid. Pööratud indeks loetleb kõik unikaalsed sõnad, mis ilmuvad mis tahes dokumendis ning indentifitseerib kõik dokumendid, milles need sõnad esinevad. Dokumendid koosnevad võti-väärtus paaridega väljadest, kus hoitakse salvestatud andmeid.

Süsteemi skaleeruvuse ja käideldavuse tagamiseks on indeks jagatud kildudeks (*shard*), mille puhul iga kild on tegelikult iseseisev indeks. Kilde on kahte tüüpi – põhikild ja koopiakild. Iga dokument kuulub ühte põhikildu ning ühte või mitmesse koopiakildu. Jagades dokumendid selliselt kildudesse ning põhi- ja koopiakillud klastri õlgade vahel laiali, suudab Elasticsearch tagada indeksite tõrkekindluse ning tõsta lugemispäringute kiirust [10].



Joonis 2. Elasticsearch loogiline disain [12]

Logstash on andmekogumismootor, mis suudab reaalajas erinevatest allikatest pärinevad andmed ühendada ning edastada normaliseeritult valitud sihtkohta. Enne andmete edastamist, võimaldab Logstash andmeid rikastada, filtreerida ning teisendada [11]. Kibana on veebiliides andmete vaatamiseks, analüüsimiseks, visualiseerimiseks ning Elastic Stack'i haldamiseks.

Beats'id on logide kollektorid, mis paigaldatakse tööjaamadesse ja serveritesse agentidena logide edastamiseks Logstashi või otse Elasticsearchi. Põhilised agendid on Windows operatsioonisüsteemi logide edastamiseks Winlogbeat ning Linux operatsioonisüsteemidel Filebeat. [12]

Logstash omab integratsioonivõimekust MISP andmebaasiga [13]. SIEM funktsionaalsus on koondatud Elastic Security moodulisse. Indikaatoripõhise tuvastuse ning teavituste loomise funktsionaalsus on Elastic Security moodulis saadaval. Teavituste edastamine valitud kanali kaudu on saadaval alates Gold litsentsist. Vajadusel saab tuvastuse ning häirete loomise, sealhulgas häireteavituste edastamise funktsionaalsuse täiendamiseks kasutada ElastAlert lisatarkvara [14].
Logide otsingute teostamiseks, analüüsimiseks ning visualiseerimiseks on Elastic Stacki kuuluv Kibana. Täiendavaks logide süvaanalüüsiks on võimalik Elastic Stackiga integreerida Jupyter Notebooks ja GraphFrames.

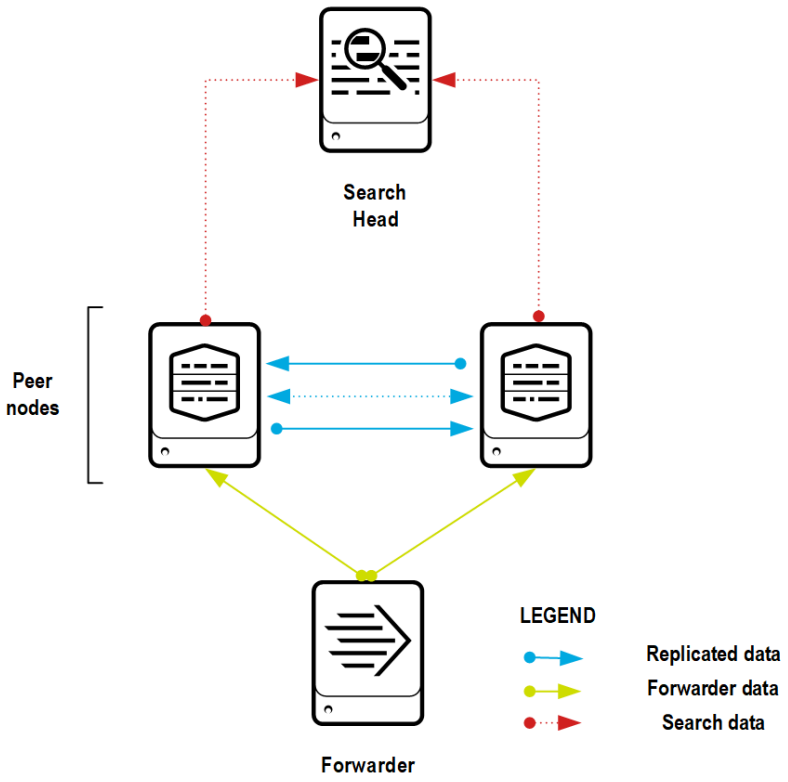
Elastic Stack on jagatud nelja versiooni – Standard, Gold, Platinum ja Enterprise. Standard versioon on tasuta, ülejäänud kolm tasulised. Antud lahenduse jaoks on sobiv versioon Standard, mistõttu tarkvara soetamiseks lisakulusid ei ole.

4.2.2 Splunk Enterprise

Splunk Enterprise on tarkvaratoode, mis võimaldab otsida, analüüsida ja visualiseerida erinevatest IT infrastruktuuri komponentidest kogutud andmeid.

Splunk Forwarder on logide kollektor, mis paigaldatakse tööjaamadesse ja serveritesse agentidena logide edastamiseks indekseerimiskomponenti (Indexer). Splunk kasutab kahte tüüpi kollektoreid - *Universal*, mille puhul edastatakse kogu logi toorel kujul ning *Heavy*, mille puhul toimub logide parsimine ja töötlemine enne saatmist kliendi masinas.

Indexer on Splunki komponent, mille eesmärk on sisendandmete indekseerimine ning salvestamine. Kui sisendandmed on töötlemata kujul (tulevad Universal Forwarderist), töötleb ja parsib Indexer need enne indekseerimist. Andmete indekseerimisel kirjutatakse need failidesse, mis omakorda on eraldatud kataloogides, mida nimetatakse ämbriteks (*buckets*). Andmete käideldavuse tõstmiseks on võimalik luua indekseerijate klaster, mille puhul andmete indekseerimisel replikeeritakse see klastri õlgade vahel. Splunk Search Head on komponent, millega juhitakse ja korraldatakse otsingute teostamist Splunki indeksitest. Otsingute teostamisel kasutatakse hajutatud otsingut, mille puhul saadetakse päringud mitmele indekseerijale korraga [8].



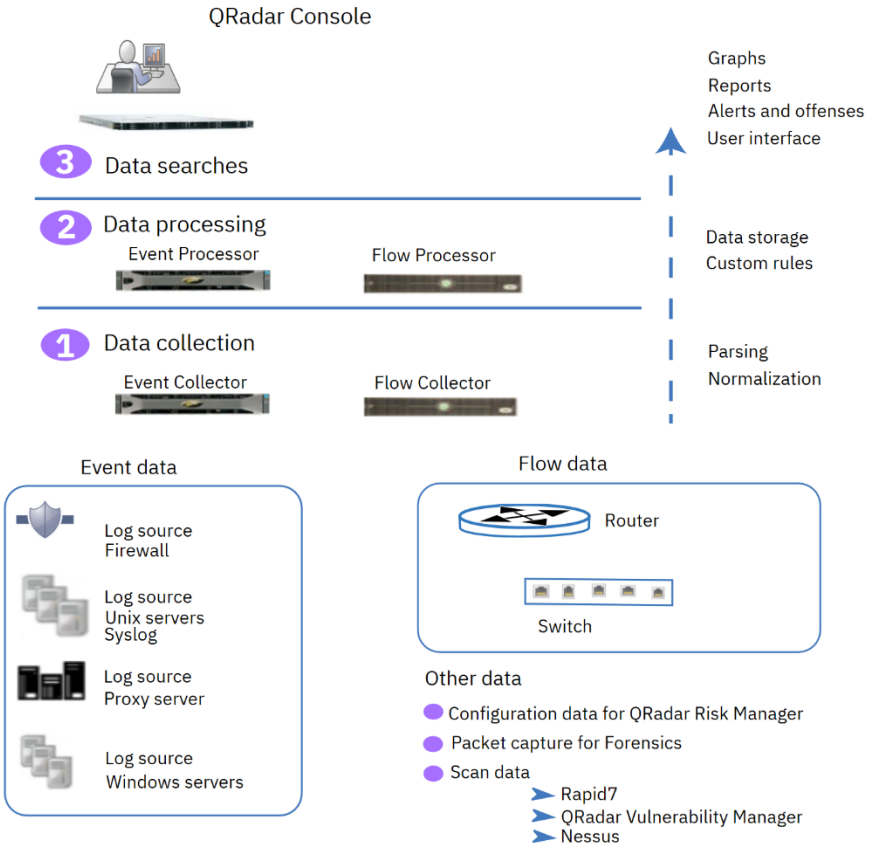
Joonis 3. Splunk loogiline disain [8]

Splunk Enterprise on baastoode, mille funktsionaalsuse laiendamiseks on võimalus juurde soetada lisatarkvarasid. Splunk Enterprise Security lisab SIEM'i funktsionaalsuse, tuues juurde näiteks indikaatoripõhise tuvastuse ja teavitamise.
Splunk tooteid litsentseeritakse indekseeritava andmemahu järgi päevas (GB/päevas). Litsentseeritakse kõik Splunk osised, Enterprise Security litsentseerimise eelduseks on Splunk Enterprise litsentseerimine. Splunk litsentsikalkulaatori näidisarvutuste järgi on 15GB/päevas andmesalvestuse puhul litsentsikulu Splunk Enterprise ligikaudu 75 000€ viie aastase perioodi peale [15].

Splunk Enterprise keskkonda on võimalik laiendada platvormisiseste rakendustega, mida saab alla laadida ja paigaldada Splunkbase kataloogist. Ohuteadmusbaasi MISP integreerimiseks Splunkiga on Splunkbase kataloogis saadaval MISP42Splunk rakendus. Splunk Enterprise võimaldab salvestatud otsingute põhjal luua reaalajas või ajastatult teavitamist, kui leitakse vaste etteantud tingimusele.

4.2.3 IBM Qradar

IBM QRadar on tooteperekond, kuhu kuuluvad QRadar SIEM, QRadar User Behavior Analytics, QRadar Network Insights, QRadar Data Store ja mitmed muud turbe eesmärgilised tarkvarad. IBM QRadar omab laia integratsioonivõimekust paljude IBM ja kolmanda osapoole tarkvaradega. QRadar SIEM on logiandmete kogumiseks ja parsimiseks ning sündmuste korreleerimiseks ja teavituste loomiseks ning saatmiseks. QRadar SIEM'i töövoog on jagatud kolme etappi – logide kogumine (*Data collection*), logide töötlemine (*Data processing*) ja logide analüüs ning otsingute teostamine (*Data searches*). Logide kogumiseks, parsimiseks ning normaliseerimiseks on QRadari komponent *Event Collector*, kuhu Windowsi tööjaamade logisid saab edastada üle MSRPC protokolli või kasutades WinCollect agenti ning Linux operatsioonisüsteemide logisid üle syslog protokolli. Võrguliikluse *netflow* kogumiseks on komponent *Flow Collector*.



Joonis 4. QRadar loogiline disain [16]

Logide edasine töötlus toimub *Event/Flow Processor* komponendis, kus kõik kirjed läbivad *Custom Rules Engine (CRE)* kihi. Logikirjeid võrreldakse vastu eelnevalt defineeritud reegleid ning leiu korral käivitatakse eelseadistatud tegevused. Tegevuseks võib olla näiteks e-maili saatmine või syslogi sõnumi genereerimine. *CRE* kihi läbinud kirjed salvestatakse andmepinnale. Logidest otsimine, analüüsimine ning teavituste ja leidude uurimine toimub läbi *QRadar Console* kasutajaliidese.
QRadar SIEM'i paigalduseks on mitu viisi – *All-in-One* või eraldatud rollidega serverid. *All-in-One* paigalduse puhul on kõik kompnendid ühes serveris. Mahtude kasvades saab lahendusse servereid juurde lisada. Servereid saab jooksvalt juurde lisada rollipõhiselt. Kogumismahtude kasvu puhul tuleks paigaldusse juurde lisada *Event Collector* ning arvutusjõudluse ja andmemahu tõstmiseks *Event Processor* [16].
Kõrgkäideldavuse tagamiseks võimaldab QRadar SIEM teise serveri paigaldusega luua klastri, millega tagatakse ühe serveri tõrke korral süsteemi töö jätkamine. QRadar SIEM klaster töötab aktiivne-passiivne põhimõttel, mille puhul aktiivsest sünkroniseeritakse andmed sekundaarsesse serverisse või kasutatakse välist jagatud andmepinda. Primaarse serveri tõrke korral võtab sekundaarne server töö üle [17].

QRadar toodetele lisafunktsionaalsuse paigaldamiseks on võimalik *IBM X-Force Exchange/App Exchange* kataloogist leida ning paigaldamiseks alla laadida lisatarkvarasid. Indikaatoripõhise tuvastuse funktsionaalsuse saavutamiseks on võimalik rakenduste kataloogi abil paigaldada „IOC Manager for QRadar" [18]. Integratsioonivõimalus MISP platvormiga vaikimisi puudub, kuid kommuuni poolt arendatud skriptidega on seda siiski võimalik teha.

QRadar SIEM komponenti litsentseeritakse andmevoo (sündmuseid sekundis, event per second [EPS]) järgi. QRadar SIEM indikatiivse hinna saamiseks viis autor läbi vestluse tarkvara edasimüüja ning kahe sama toodet kasutava ettevõtte spetsialistidega. Antud lahenduse juures, võttes arvesse EPS väärtust 300, oleks litsentsihind 4 aasta peale ligikaudu 25000€. Kõrgkäideldavuse tagamiseks on vajalik paigaldada kaks serverit, kuid teine server pärib litsentsi primaarselt serverilt, mistõttu ei ole seda vaja eraldi litsentseerida.

4.3 Valiku tegemine

MISP platvormi integratsiooniks on Elastic Stacki kuulval Filebeat komponendil ThreatIntel moodul, QRadar ning Splunk puhul saab kasutada pistikprogramme või kommuuni poolt teostatud arendusi [13]. Häirete loomise funktsionaalsus on kõikidel sisseehitatud funktsionaalsusena olemas. Teavituste edastamine valitud kanali kaudu on vaikimisi olemas Splunkil ja QRadaril, Elastic Stack Standard versiooni puhul saab kasutada ElastAlert lisatarkvara. Splunk Enterprise Security ja QRadar SIEM omavad indikaatoripõhist tuvastust, Elastic Stacki puhul on võimalik kasutada selleks ettenähtud Elastic Security SIEM mooduli tuvastusreegleid. Graafilise visualiseerimises ning kohaldatavate töölaudade loomises on kõigil kolmel tarkvaral väga head võimalused. QRadar SIEM puhul ei soovita tootja üle 10 erineva töölaua luua, sest see võib kaasa tuua jõudluse probleeme [19].

Kõrgkäideldavuse tagamiseks kasutavad Splunk ja Elastic Stack indeksi koopiate hoidmist mitmes klastri õlas, tagades nii ka väga hea paindlikkuse ning skaleeruvusvõime. QRadar SIEM tagab kõrgkäideldavuse aktiivne-passiivne meetodil, mille puhul andmeid hoitakse küll sünkroniseerituna, kuid korraga töödeldakse andmeid ühes klastri serveris.

Elastic Stacki kasutuselevõtt ei tooks kaasa kulusid tarkvaralitsentsi ostmiseks, sest antud röö raames sobib kasutamiseks Standard versioon. QRadar SIEM ja Splunk suhtes teostati ligikaudne hinnastamine, mille alusel võrdlus teostati.

Hinnangud võrdlustele on autor andnud skaalal 1 – 5 (1- väga halb, 2 – halb, 3- rahuldav, 4- hea, 5 – väga hea).

Nõue	Elastic Stack	IBM QRadar SIEM	Splunk Enterprise
Kõrgkäideldavus	5	3	5
MISP integratsioon	3	3	3
Indikaatoripõhine tuvastus	4	5	5
Teavituste geneerimine ja saatmine	4	5	5
Graafiline visualiseerimine ning kohaldatavad töölauad	5	4	5
Litsentsikulud	5	4	2
Kokku	**26**	**24**	**25**

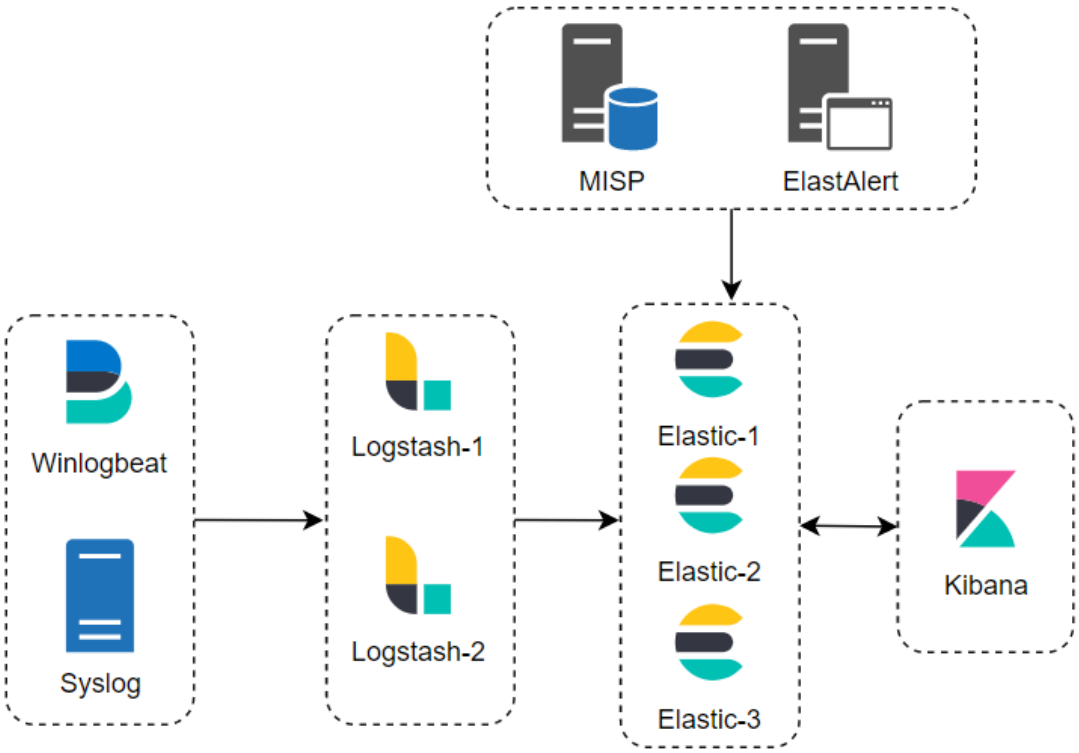
Tabel 1. Põhivalikute võrdlus

Tulenevalt teostatud võrdlusest ning tabelis 1 toodud hinnangu tulemustest, osutus antud lahenduse teostamisel valituks Elastic Stack.

5 Valitud lahenduse kirjeldus

Käesolevas peatükis kirjeldab autor valitud lahenduse arhitektuuri ning lahenduse kasutuselevõtuga kaasnevaid tegevusi.

5.1 Lahenduse ülesehitus



Joonis 5. Valitud lahenduse ülevaade

Elastic Stacki arhitektuuri planeerimisel lähtus autor Elasticsearch'i parimatest praktikatest [20]. Elasticsearch servereid paigaldatakse antud lahenduse puhul kolm ning Logstash servereid kaks. Kaks Logstash'i serverit tagavad koormuse jaotamise ning ühtlasi ühe serveri rikke korral jätkub logide vastuvõtmine, töötlemine ning edastamine. Mahtude tõstmise vajaduse korral on võimalik elasticsearchi servereid kiiresti ja lihtsasti klastrisse juurde liita. Elasticsearchi serverid paigaldatakse otse riistvarale, Logstash ning

Kibana majutatakse asutuse virtualiseerimisklastrisse. Elasticsearch *master* rollile määrab autor seadistuse *minimum_master_nodes = 2*, et vältida võimalikku *split-brain* olukorra tekkimist.

Windowsi logide edastamiseks kasutatakse Winlogbeat agenti kõikidel lõppseadmetel. Alternatiivina on võimalus kasutada Windows Event Collector teenust, kuid autori hinnangul lisab see logide edastamisele ühe lisahüppe ning potentsiaalse tõrkekoha. Winlogbeat agentide paigaldus teostatakse läbi SCCM tarkvara. Kõikidele Windows operatsioonisüsteemiga seadmetele paigaldatakse ka Sysmon teenus täiendate logide kogumiseks [21].
Linuxi serveritest logide edastamiseks võetakse kasutusele rsyslog tarkvara, mille abil edastatakse logid Logstashi kasutades syslog protokolli.

Logid salvestatakse elasticsearchi indeksitesse ühe kuulise perioodi kaupa ning lähtudes algallikast – Windowsi, Linuxi, võrguseadmete ning muud (rakendused, turbeseadmed jms) logid eraldi indeksitesse. On võimalik, et edasise töö käigus võib tekkida vajadus indekseid veel omakorda eraldada ning lähtuvalt andmeallikast muuta salvestamise perioodi pikkust.

Windowsi põhiste lõppseadmete logi edastatakse hinnanguliselt kuni 10GB päevas, mis toob kuu lõikes ligikaudu 300GB toorest andmemahtu. Elasticsearchi indeksi jagamisel kildudeks soovitatakse killu suurust hoida maksimaalselt 50GB [22]. Antud lahenduse puhul võttis autor indeksi parameetrite arvutamisel killu suuruseks 40GB ning ühte indeksisse salvestatakse ühe kuu logid. Sellest tulenevalt on andmemahu 10GB/päevas juures vajalik indeks jagada vähemalt kaheksaks killuks. Sealjuures iga kild omab kahte koopiakildu, et tagada ühe serveri rikke korral andmete käideldavus ning edasine tõrkekindlus. Andmepinda kasutatakse sellisel juhul kuu lõikes ligikaudu 900GB indeksi kohta.
Linuxi serverite ning võrguseadmete osas ei ole töö kirjutamise hetkel ülevaadet võimalike mahtude osas, mistõttu indeksi parameetrid seadistatakse lõplikult andmete kogumise käigus.

Peamiste tuvastusreeglitena võetakse kasutusele Elastic Security *Detection Rules* reeglid. Tuvastusreeglite abil automatiseeritakse ohujahtimise protsessi käigus teostatud otsingud ning reegleid kasutatakse indikaatoripõhiseks tuvastuseks. Tulenevalt asjaolust, et Elastic

Stack Standard litsentsiga puudub võimalus tuvastusreegli vaste leidmisel edastada teavitust valitud kanali kaudu, näeb antud lahenduse puhul tuvastusi ainult läbi Kibana konsooli. Olukorras, kui on vajadus mõne tuvastuse kohta saada kiireloomulist teavitust, võetakse kasutusele ElastAlert lisatarkvara.

5.2 Juurutusplaan

Valitud lahenduse rakendamine on jagatud nelja etappi:

1. Elastic Stack paigaldus ja esmane seadistamine
2. Seadmepargi logide edastamise seadistamine
3. Ohujahtimise päringute teostamise testimine
4. Lisategevused lahenduse kasutuselevõtmise teotamiseks

Esimeses etapis teostatakse Elasticsearchi andmejärve paigaldus ning seadistamine. Paigaldatakse Logstash serverid ning seadistatakse andmetorud logide vastuvõtmiseks, töötlemiseks ning edastamiseks Elasticsearchi. Paigaldatakse ning seadistatakse Kibana, luuakse ning määratakse kasutajakontode õigused.

Teises etapis teostatakse agentide paigaldus lõppseadmetesse. Seadmepargi logide edastamise seadistamine on jagatud kolme etappi:

1. Logisid edastama seadistatakse Windows operatsioonisüsteemi põhised tööjaamad ja serverid.
2. Logisid edastama seadistatakse Ubuntu/CentOS operatsioonisüsteemiga serverid. Logide edastamiseks kasutatakse rsyslog tarkvara.
3. Logisid edastama seadistatakse kõik muud seadmed kasutades syslog protokolli.

Etapipõhine seadistamine on oluline tagamaks vajadusel andmetorude seadistamine sõltuvalt andmeallikast ja -tüübist ning seadistatud logide talletamise kontrollimiseks.

Windowsi põhistesse seadmetesse paigaldatakse Sysmon teenus täiendavaks logimiseks ning Winlogbeat agent logide edastamiseks Logstashi andmetorusse. Paigaldus

teostatakse SCCM keskhalduse abil. Ubuntu/CentOS serverites teostatakse rsyslog tarkvara seadistamine autori tellimusel vastava teenuseserveri administraatori poolt.

Kolmandas etapis testitakse näidispäringutega ohujahtimise läbiviimist ning indikaatoripõhist tuvastust.

Neljandas etapis viiakse autori poolt läbi lahenduse kasutamiseks vajalikud koolitused analüütikutele, kes hakkavad põhiliselt antud lahendust kasutama. Lõputöö autoril on planeeritud läbida koolitus *Elasticsearch Engineer*, et täiendada enda oskusi Elasticsearchi haldamisel ja edasisel arendamisel [23].
Lahenduse kasutuselevõtmisel määratakse vastutav isik ohujahtimiste teostamisel, kelle ülesandeks on automatiseerimiseks loodavate reeglite üle kontrolli pidamine ning vajadusel ülesannete jaotamine. Määratud isik vastutab, et teostatud jahtimised saaksid automatiseeritud ning need tegevused oleksid dokumenteeritud.

6 Paigaldamine ja seadistamine

Käesolevas peatükis teostab autor valitud lahenduse tehnilise paigalduse ja esmase seadistamise.

6.1 Elastic

Autor paigaldas serveritele Elastic Stacki komponendid versiooniga 7.12. Paigalduse teostamiseks kasutas autor elastic.co ametlikku repositooriumit. Elasticsearchi paigaldamiseks imporditi esmalt pakkide PGP võti ning määrati repositoorium, seejärel paigaldati Elasticsearch. Elasticsearch klastri loomisel tehti seadistused */etc/elasticsearch/elasticsearch.yml* konfiguratsioonifailis:

```
cluster.name: hunting-cluster
node.name: elastic-1
network.host: 172.16.30.101
discovery.seed_hosts: ["172.16.30.101", "172.16.30.102", "172.16.30.104"]
cluster.initial_master_nodes: ["172.16.30.101", "172.16.30.102",
"172.16.30.104"]
```

Kibana paigaldamiseks imporditi esmalt pakkide PGP võti ning määrati repositoorium,

seejärel paigaldati Kibana. Kibana paigaldamisel olulisemad väärtused */etc/kibana/kibana.yml* failis:

```
server.host: 172.16.30.105
server.name: "hunting-kibana"
elasticsearch.hosts: ["http://172.16.30.101:9200",
"http://172.16.30.102:9200", "http://172.16.30.104:9200"]
```

Logstash paigaldamiseks imporditi esmalt pakkide PGP võti ning määrati repositoorium, seejärel paigaldati Logstash. Kataloogi */etc/logstash/conf.d/* lõi autor kolm erinevat konfiguratsioonifaili: winlog.conf, linlog.conf ning syslog.conf. Nendes failides kirjeldas autor erinevatest allikatest tulevate logide andmetoru seadistused.

Peale esmast klastri ülesseadmist ja töökorra testimist seadistas lõputöö autor kõik ühendused kasutama TLS protokolli.

Tööjaamadesse ning Windowsi serveritesse paigaldas autor Winlogbeat ning Sysmon tarkvarad. Winlogbeat'i seadistas autor logisid edastama Logstashi serveritesse.

ElastAlert paigaldamiseks kasutas autor ElastAlert'i Github repositooriumis asuvat installatsiooni [24]. Peale repositooriumi kloonimist käivitas autor *setup.py* skripti, mille töö tulemusena paigaldati ElastAlert tarkvara. Käsuga *elastalert-create-index* lõi autor Elasticsearch'i uue indeksi ElastAlert informatsiooni ning metaandmete hoiustamiseks.

6.2 MISP integratsioon

MISP ohuteadmusbaasi tarkvarast indikaatorite sünkroniseerimiseks kasutab autor Filebeat agendi *ThreatIntel* moodulit [13]. Mooduli konfiguratsioonis määrati MISP serveri aadress ning autentimistõend MISP API poole pöördumiseks. Peale seadistuste tegemist ning filebeat teenuse käivitamist sünkroniseeritakse MISP'is olevad indikaatorid elasticsearchi vastavasse indeksisse.

Time	event.dataset	event.type	threatintel.misp.attribute.category	threatintel.misp.attribute.type	threatintel.indicator.file.hash.md5
Apr 19, 2021 @ 14:15:15.000	threatintel.misp	indicator	Payload delivery	md5	423d3ade2f14572c5bd5f546973eb493

Joonis 6. MISP tarkvarast sünkroniseeritud indikaator

7 Tuvastustestide läbiviimine

Käesolevas peatükis püsititab töö autor näidishüpoteesid ning testib simuleeritud ründetegevuste ja kogutud andmete põhjal loodud lahenduse otsingu- ja tuvastusmeetmeid.

7.1 Pahaloomuline e-maili manus

Hüpotees: Asutuse võrku on laetud pahavara õngitsuskirjaga saadetud pahaloomulise e-maili manuse kaudu. Asutuse turbevahendid, sh. antiviirus ei ole laetud pahavara tuvastanud.

Tuvastamine: Otsida märke Outlook ja Word rakenduse poolt käivitatud tavapäratute protsesside kohta.

Autor teostas Kibana veebirakenduses winlogbeat indeksist otsingu: *(process.parent.name: winword.exe or process.parent.name: outlook.exe) and (process.name: "powershell.exe" or process.name: "cmd.exe")* ning tuvastas winword.exe poolt käivitatud powershelli käsu.

Joonis 7. winword.exe poolt käivitatud powershelli protsess

Tuvastatud logikirje lähemal vaatamisel on näha, et powershelli protsessi käivitas Word dokumendi invoice-WR45362.docm avamine.

```
ParentImage: C:\Program Files\Microsoft Office\Office16\WINWORD.EXE
ParentCommandLine: "C:\Program Files\Microsoft Office\Office16\WINWORD.EXE" /n "C:\Users\kuldar\Downloads\invoic
e-WR45362.docm" /o ""
```

Joonis 8. Pahaloomuline dokument

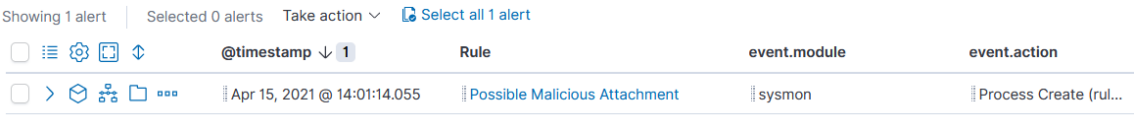
Käivitatud powershelli käsk on obfuskeeritud, mistõttu ei ole koheselt välja loetav, mis tegevusi käsu poolt teostati. Arvestades asjaoluga, et üldjuhul kasutatakse manust pahavara payloadi allalaadimiseks sihtmasinasse, teostas autor otsingu tuvastamaks antud ajaraamis powershell.exe poolt teostatud failide kirjutamisi.

Teostatud otsingu (*event.code : 11 and process.name: "powershell.exe"*) tulemustest nähtub, et mõned sekundid peale manuse avamist laeti alla dead.exe nimeline fail.

```
File created:
RuleName: Downloads
UtcTime: 2021-04-15 10:57:28.057
ProcessGuid: {62996017-1c13-6078-dd03-000000001200}
ProcessId: 5380
Image: C:\Windows\syswow64\Windowspowershell\v1.0\powershell.exe
TargetFilename: C:\Users\kuldar\Downloads\dead.exe
CreationUtcTime: 2021-04-15 10:40:35.647
```

Joonis 9. Allalaetud võimalik pahaloomuline fail

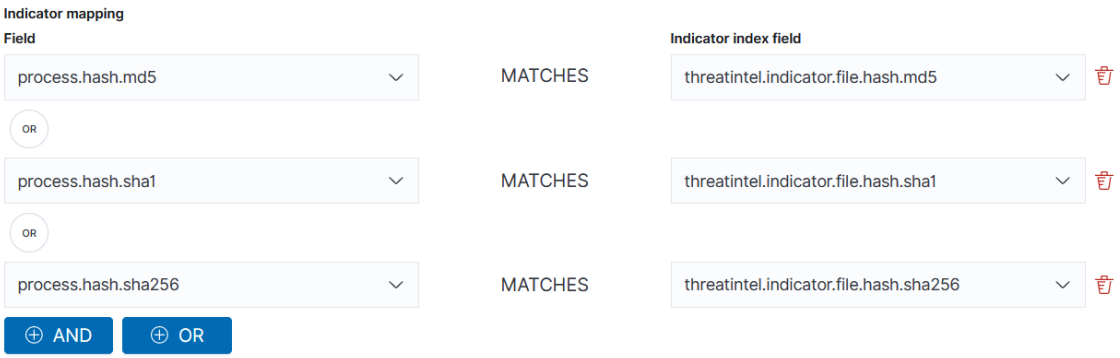
Teostatud tuvastuse automatiseerimiseks kasutas autor Elastic Security tuvastusreegleid. Uue tuvastusreegli lõi autor sama otsingufraasiga, mida kasutas käsitsi otsimise puhul. Reegli loomise järel teostati uuesti pahaloomulise faili avamine, mille peale registreeriti Elastic Security tuvastuse poolt häire.



Joonis 10. Registreeritud häire

7.2 Indikaatoripõhine tuvastus

Indikaatoripõhiseks tuvastuseks kasutas autor Elastic Security Detection Rules reeglit *Indicator Match*. Reegli loomisel tuleb seostada logi väljad vastavate väljadega indikaatorite indeksis, mille põhjal tuvastusi tehakse.



Joonis 11. Indikaatori väljade sidumine

Tuvastuse testimiseks käivitas autor ühes lõppseadmetest faili, mille MD5 räsi on kirjeldatud MISP ohuteadmusbaasis ning sünkroniseeritud elasticsearchi indikaatorite indeksiga. Faili käivitamise peale tuvastas Elastic Security loodud reegli põhjal vaste.

@timestamp ↓ 1	Rule	Method	event.module
Apr 23, 2021 @ 11:58:53.318	Potentially malicious hash value match detected	threat_match	sysmon

Joonis 12. Indikaatori tuvastamise häire

Kokkuvõte

Käesoleva lõputöö eesmärk oli leida asutusele ohujahtimise teostamiseks tarkvaralahendus, kuhu koguda ning talletada seadmepargi logid. Kogutud logide põhjal oli planeeritud teostada otsinguid ning tuvastusi eesmärgiga tuvastada ründaja tegevused asutuse võrgus võimalikult kiiresti.

Lõputöö teoreetilises osas kirjeldati asutuse nõuded planeeritavale lahendusele ning nendele nõuetele tuginedes teostati võrdlev analüüs sobiva lahenduse leidmiseks. Esmase analüüsi järel valiti põhivalikkusse kolm tarkvara, mida võrreldi täpsemalt. Võrdluse tulemusena valis lõputöö autor kasutatavaks platvormiks Elastic Stack'i.

Lõputöö praktilises osas kirjeldati planeeritav lahendus ning teostati lahenduse realisatsioon testkeskkonnas. Simuleeritud pahaloomulise tegevuse käigus teostati testid logidest otsingute teostamise ning indikaatoripõhise tuvastuse kohta.

Lõputöö tulemusel leiti tarkvaralahendus asutuses ohujahtimise läbiviimiseks. Lõputöö käigus teostatud analüüside tulemusel valitud lahendus võetakse kasutusele lõputöös käsitletava asutuse taristus ning ohujahtimise läbiviimisel.

Edasist tegevustena on planeeritud hinnata vajadust ning vajaduse ilmnemisel võtta kasutusele intsidendi/piletihalduse süsteem, mis on integreeritav teostatud lahendusega. Planeeritud on hinnata lisavõimaluste väärtust Jupyter Notebooks rakendusega logide täiendavaks analüüsimiseks ning ohujahtimise tegevusmallide loomiseks.

Kasutatud kirjandus

[1] „M-Trends Reports: Insights into Today's Top Cyber Trends and Attacks," FireEye, 2021. [Võrgumaterjal]. Available: https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html.

[2] Sqrrl, Hunt Evil: Your Practical Guide to Threat Hunting.

[3] „5 Types of Threat Hunting," Sqrrl, [Võrgumaterjal]. Available: https://www.cybersecurity-insiders.com/5-types-of-threat-hunting/.

[4] „SANS Institute Reading Room," 15 August 2016. [Võrgumaterjal]. Available: https://www.sans.org/reading-room/whitepapers/threats/paper/37172.

[5] „White Paper: A Framework for Cyber Threat Hunting," [Võrgumaterjal]. Available: https://www.threathunting.net/files/framework-for-threat-hunting-whitepaper.pdf.

[6] „Gartner Magic Quadrant for Security Information and Event Management," [Võrgumaterjal]. Available: https://www.gartner.com/en/documents/3981040/magic-quadrant-for-security-information-and-event-manage.

[7] „Threat Hunting. Why might you need it," [Võrgumaterjal]. Available: https://cyberpolygon.com/materials/threat-hunting-why-might-you-need-it/.

[8] „Splunk Enterprise Overview," [Võrgumaterjal]. Available: https://docs.splunk.com/Documentation/Splunk/8.1.2/Overview/AboutSplunkEnterprise.

[9] „LogRythm SIEM Solution," [Võrgumaterjal]. Available: https://logrhythm.com/solutions/security/siem/.

[10] „Elasticsearch Reference: What is Elasticsearch?," [Võrgumaterjal]. Available: https://www.elastic.co/guide/en/elasticsearch/reference/current/elasticsearch-intro.html.

[11] „Logstash Reference: Logstash Introduction," [Võrgumaterjal]. Available: https://www.elastic.co/guide/en/logstash/current/introduction.html.

[12] „Beats Platform Reference: What are Beats?," [Võrgumaterjal]. Available: https://www.elastic.co/guide/en/beats/libbeat/current/beats-reference.html.

[13] „Filebeat module ThreatIntel'," [Võrgumaterjal]. Available: https://www.elastic.co/guide/en/beats/filebeat/7.12/filebeat-module-threatintel.html.

[14] „ElastAlert - Read the Docs," [Võrgumaterjal]. Available: https://github.com/Yelp/elastalert.

[15] „Splunk Simple License Calculator," [Võrgumaterjal]. Available: https://splunkpricing.com/.

[16] „IBM QRadar Architecture and Deployment Guide," [Võrgumaterjal]. Available: Architecture and Deployment Guide.

[17] „IBM QRadar High Availability Guide,“ [Võrgumaterjal]. Available: https://www.ibm.com/docs/en/SS42VS_7.3.3/com.ibm.qradar.doc/b_qradar_ha_guide.pdf.

[18] „QRadar apps,“ [Võrgumaterjal]. Available: https://www.ibm.com/docs/en/qradar-common?topic=1-qradar-apps.

[19] „IBM QRadar SIEM Custom dashboards,“ [Võrgumaterjal]. Available: https://www.ibm.com/docs/en/qsip/7.4?topic=management-custom-dashboards.

[20] „Elasticsearch Arhitecture Best Practices,“ [Võrgumaterjal]. Available: https://www.elastic.co/webinars/elasticsearch-architecture-best-practices.

[21] „Sysmon,“ [Võrgumaterjal]. Available: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon.

[22] „How many shards should I have in my Elasticsearch cluster?,“ [Võrgumaterjal]. Available: https://www.elastic.co/blog/how-many-shards-should-i-have-in-my-elasticsearch-cluster.

[23] „Elasticsearch Engineer,“ [Võrgumaterjal]. Available: https://www.elastic.co/training/elasticsearch-engineer.

[24] „ElastAlert,“ [Võrgumaterjal]. Available: https://github.com/Yelp/elastalert.

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

Mina, Kuldar Teinmann

1. Annan Tallinna Tehnikaülikoolile tasuta loa (lihtlitsentsi) enda loodud teose „Ohujahtimise platvormi lahenduse valik ja rakendamine“, mille juhendaja on Siim Vene.
   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.

29.04.2021

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.