TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Karoliine Karu 186032IABB

AVATUD LÄHTEKOODIGA SOAR SÜSTEEMI THE HIVE KASUTAMINE EFEKTIIVSEMA KÜBERKAITSE OPERATSIOONIDE KESKUSE TEENUSE (SOCAAS) IMPLEMENTEERIMISEKS ETTEVÕTTE CYBERS NÄITEL

Bakalaureusetöö

Juhendaja: Jürgen Erm
Kaasjuhendaja: Dr. Gunnar Piho

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: Karoliine Karu

Annotatsioon

Käesoleva bakalaureusetöö eesmärgiks on analüüsida ettevõtte CYBERS Küberkaitse Operatsioonide Keskuse (SOC) analüütikute tööülesandeid ja muuta töötsüklid efektiivsemaks läbi Security Orchestration, Automation and Response (SOAR) süsteemi teenusesse integreerimise abil.

Küberturvalisuse vajaduse kasvades on üheks oluliseks teenuseks saanud SOC, kus tegeletakse igapäevaselt süsteemide monitoorimise, intsidentide tuvastamise ja neile reageerimisega. Töö käigus kirjeldab autor SOC analüütikute koormusega ja piiratud ajaressursiga seotud probleeme, mis mõjutavad teenuse kvaliteeti ja töötajate heaolu. Lahenduseks on välja toodud SOAR platvorm, mis võimaldab analüütikute tööd lihtsustada ja teatud ulatuses automatiseerida.

Töö käigus antakse ülevaade SOC teenustest ja analüütikute tööülesannetest ning tehnoloogiatest, mis on teenuse toimimise seisukohalt olulised. Autor analüüsib SOC analüütikute tööprotsesse ja nendega kaasnevaid kitsaskohti ning selle põhjal koostab analüütiku töötsükli graafiku. Samuti analüüsitakse The Hive platvormi funktsioone ja võimalusi valitud ettevõttes ning selle alusel luuakse ümberkavandatud töötsükli graafik.

Lõputöö on kirjutatud eesti keeles ning sisaldab teksti 39 leheküljel, 5 peatükki, 9 joonist, 0 tabelit.

Abstract

Implementing an effective Security Operations Center as a Service (SOCaaS) by the usage of open source SOAR system The Hive, case of CYBERS

The aim of this bachelor's thesis is to analyze the work of Security Operations Center (SOC) analysts in CYBERS and make their workflow more efficient through the implementation of an open source Security Orchestration, Automation and Response (SOAR) system The Hive.

As the need for cybersecurity grows, SOC has become an important service. A SOC analyst's daily work consists of real time monitoring, identifying incidents and responding to them. The main focus of this thesis is on the welfare and time resources of the analyst that affect the continuity and quality of the whole service.

The thesis first gives overview of the problem: SOC as a service, the workflow and tasks of a SOC analyst and the technologies needed to provide the service in CYBERS. The author also analyzes the shortcomings of the current workflow and, based on the analysis, compiles a workcycle model. An analysis of The Hive's functions and usage possibilities in CYBERS is also given and based on that, a redesigned workcycle model is composed.

The thesis is in estonian and contains 39 pages of text, 5 chapters, 9 figures, 0 tables.

Lühendite ja mõistete sõnastik

AQL	Ariel Query Language
Hash	Räsi
MISP	Malware Information Sharing Platform
Playbook	Analüütikute strandardiseeritud tegevuste kirjeldus
Sandbox	Isoleeritud virtuaalmasin testimiseks
SECaaS	Security as a Service
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation and Response
SOC	Security Operations Center, küberkaitse operatsioonide keskus
SOCaaS	Security Operations Center as a Service
SPOC	Single Point of Contact, kliendi kontaktisik
SQL	Structured Query Language
UTF	Unicode Transformation Format

Sisukord

Jooniste loetelu

1 Sissejuhatus

Tehnoloogia arenedes on tänapäeval olulist kõnepinda saanud küberturvalisus. Üha enam on kuulda ettevõtetest, kes langevad rünnaku ohvriks, kuid pole varasemalt teinud midagi, et oma süsteeme kaitsta. Selle tõttu on hakanud ettevõtted otsima võimalusi turvalisuse tõstmiseks ja üheks selliseks võimaluseks on Küberkaitse Operatsioonide Keskuse (SOC) teenuse kasutamine. SOC-i eesmärk on tegeleda süsteemide monitooringu, intsidentide tuvastamise ja intsidentidele reageerimisega. SOC teenuse igapäevaseid protsesse viivad läbi erinevate astmete analüütikud ja insenerid, kes töötlevad suurel hulgal informatsiooni ja vastutavad mitmete ettevõtete süsteemide turvalisuse eest.

SOC-i jõuab igapäevaselt suurel hulgal andmeid, mis tuleb analüütikutel läbi töötada. Suur andmete hulk mõjutab intsidentide tuvastamist ja nendele reageerimist, mis võib mõjutada intsidentide kulgu ja tagajärgi. Tuhandete andmete läbitöötamine nõuab mitmete analüütikute tähelepanu ja ajalise ressursi kulu, mis võib tihti lõppeda analüütiku läbipõlemisega. Nende probleemide leevendamiseks on hakatud keskenduma protsesside automatiseerimisele ja analüüsi koostamise lihtsustamisele ning üheks uusimaks arenduseks sellel alal on Security Orchestration, Automation and Response (SOAR) süsteemid.

1.1 Taust ja probleem

Aastal 2010 loodud küberturvalisusega tegelev ettevõte CYBERS on üks SOC teenusepakkujatest Eestis. Lisaks SOC teenusele pakub ettevõte erinevaid küberturvalisusega seotud teenuseid: koolitused, haavatavuse hindamine, võrguseisundi turbekontroll jt. Varasemalt tuntud kui Security Software OÜ, CYBERS on väikeettevõtte, mille eesmärk on pakkuda kliendisõbralikku ja põhjalikku teenust, mis võimaldaks ettevõtetel küberintsidente vältida või vajadusel nendele reageerida.

Ettevõttele on SOC suhteliselt uus teenus ning selle tõttu on mitmeid võimalusi teenuse võimekuse tõstmiseks. SOC analüütikutel on suur koormus, sest läbi tuleb töötada

suurel hulgal andmeid ning inimressurss väikeettevõttes on piiratud. Andmete suur kogus mõjutab ka intsidendile reageerimise aega ning seega võib oluliselt muuta intsidendi tagajärgi. Probleemi lahendamiseks on ettevõttes hakatud integreerima avatud lähtekoodiga SOAR lahendust The Hive, mille eesmärk tulevikus oleks vähendada SOC töötajate koormust ning muuta intsidendile reageerimine efektiivsemaks. Antud töös keskendutakse rohkem SOC esimese taseme analüütikute tööülesannetele ja The Hive lahendustele, mis nendele ülesannetele kehtivad.

1.2 Ülesande püstitus

Töö eesmärgiks on analüüsida SOC analüütikute tööülesandeid- ja protsesse ning leida probleemsed kohad, mida oleks võimalik The Hive kasutuselevõtuga efektiivsemaks muuta. Samuti analüüsib töö autor SOAR platvormi The Hive võimalusi ettevõttes CYBERS ja kirjeldab süsteemi põhilisi omadusi. Tehtud analüüsi põhjal koostatakse ümberkavandatud SOC esimese astme analüütiku töötsükkel, mille põhjal oleks võimalik SOC teenuse efektiivsust tõsta ja samas vähendada analüütikute koormust.

Töö ülesanneteks on:

1) Analüüsida SOC esimese astme analüütikute tööülesandeid ja -protsesse, tuua välja nende kitsaskohad ning koostada selle põhjal algne töötsükli graafik
2) Uurida ja analüüsida SOAR süsteemi The Hive integratsiooni, funktsioone ja võimalusi ettevõttes CYBERS
3) Luua ümberkavandatud SOC esimese astme analüütiku töötsükkel ja analüüsida selle võimalusi
4) Tuua välja võimalusi SOAR platvormi The Hive integratsiooniks tulevikus

1.3 Ülevaade tööst

Käesolev töö jaguneb viieks põhiosaks: sissejuhatus, töö teoreetilised alused, SOAR platvormi The Hive analüüs, CYBERS SOC teenuse tööprotsesside analüüs, SOAR platvormi The Hive integratsioon CYBERS SOC teenusesse. Samuti on töö lõpus sõnastatud kokkuvõte. Sissejuhatuses annab töö autor ülevaate probleemist ja taustast. Töö teoreetiline osa annab lühikese ülevaate ettevõttest CYBERS, kirjeldab SOAR ja SIEM süsteemide ning SOC teenuse olemust. Peatükis SOAR platvormi The Hive

analüüs kirjeldab töö autor The Hive platvormi funktsiooni ja ülesehitust ettevõttes. CYBERS SOC teenuse tööprotsesside analüüsis käsitletakse SOC esimese taseme analüütiku tööülesandeid ja nendega seonduvaid kitsaskohti. Põhiosa viimases peatükis SOAR platvormi The Hive integratsioon loob töö autor ümberkavandatud töötsükli graafiku ning hindab tööprotsessides läbiviidud muudatusi.

2 Töö teoreetilised alused

Ajastul, mil tehnoloogia areneb sekunditega ning COVID-19 on sundinud paljud ettevõtted küberruumi, on olulisele kohale tõusnud küberturve. 2021. aastal Turu-uuringute AS-i poolt läbi viidud uuringust selgub, et 55% Eesti ettevõtetest on viimase 12. kuu jooksul kokku puutunud küberturbealaste ohuolukordadega. Samast uuringust selgub ka kurb tõsiasi, et ligi 40% ettevõtetest ei tegele küberturvalisusega ükski töötaja (Telia AS, 2021). Seoses COVID-19 levikuga on suurenenud vajadus kodust töötamisega seotud võimaluste järele ning töötajate liikumine kontoritest kodudesse on suurendanud ettevõtete riski sattuda küberrünnaku ohvriks. Interpoli andmetel on küberrünnakute arv COVID-19 kriisi tõttu teinud tohutu hüppe ning kriminaalpolitseiorganisatioon ennustas veel 2020 aasta augustis küberintsidenti märgilist tõusu (Interpol, 2020). Seega saab väita, et küberturve on muutunud ettevõtte toimimise elutähtsaks osaks, mis mõjutab äri kõiki aspekte.

Ettevõtetel on võimalik küberturbe taset tõsta rakendades mitmeid meetodeid ja nõudeid. Oluline on tuvastada turvanõrkused ning kehtestada ettevõtte nõuetele vastavad reeglid. Intsidentide tuvastamist lihtsustab süsteemide pidev monitoorimine ja logide kogumine. Uuringutest selgub, et 95% küberintsidentidest on põhjustanud inimeste tehtud vead (e-zu Solutions, 2020). Selle tõttu on kasulik koolitada töötajaid ning teavitada neid ohtudest, mis võivad vastasel juhul intsidentideks realiseeruda. Paljudel ettevõtetel pole aga valmidust ega ressurssi, et teostada erinevaid küberturvalisusega seotud protsesse ettevõttesiseselt, ning selle tõttu ostetakse vajaminevaid teenuseid välistelt teenusepakkujatelt. Üheks selliseks teenusepakkujaks on Eestis ettevõte CYBERS (juriidiline nimi Security Software OÜ), mille põhjal on antud töö ka koostatud. Üks teenustest, mida valitud ettevõtte pakub, ja millele antud töös keskendutakse, on Security Operations Center (SOC). SOC meeskonna eesmärgiks on tegeleda süsteemide monitoorimise, intsidentide ennetamise, tuvastamise ja analüüsiga ning toimunud intsidentidele reageerimisega.

SOC meeskonna töö lihtsustamiseks ning inimeste tehtud vigade elimineerimiseks on viimastel aastatel hakatud intensiivsemalt tegelema teenuste automatiseerimisega.

Kindlate protsesside automatiseerimise tagajärjel saavad SOC töötajad keskenduda keerukamatele ülesannetele ning see säästab tohutult ajalist ressurssi ja töötajate poolt tehtavat manuaalset tööd. Uusim arendus automatsiooni maastikul on erinevad Security Orchestration, Automation and Response (SOAR) süsteemid ja platvormid, mis võimaldavad ettevõttel koguda andmeid ning reageerida vähem prioriteetsetele intsidentidele ilma, et see nõuaks töötaja sekkumist või analüüsi. SOAR platvormid on võimelised teostama ka esimesi reageerimiseks paika pandud tegevusi, et töötajad saaksid aega raiskamata hakata tegutsema intsidendi analüüsimisega, mitte süsteemide karantiinimise või tegevuste blokeerimisega (Mulder, 2020).

Käesolev töö on ajendatud eelkõige ettevõtte vajadusest SOAR süsteemi SOC teenusesse implementeerimise ja selle kasutamise võimalikult efektiivseks muutmise järele. Organisatsioon on alustanud avatud lähtekoodiga SOAR platvormi The Hive integreerimist SOC teenusesse ning töö autori eesmärk on analüüsida, kuidas muuta ettevõtte SOC lahendus efektiivsemaks kasutades valitud platvormi. Samuti standardiseeritakse ettevõttes pidevalt uusi protsesse, mille eesmärk on tulevikus tõsta ettevõtte SOC teenuse küpsusastet. Käesolev töö aitaks seega kaasa ka selle eesmärgi täitmisele. Töö autor töötab ettevõttes SOC analüütikuna ning SOAR süsteemi kasutusele võtmine lihtsustaks mitmeid autori tööülesandeid. Lisaks pole varasemalt antud teemat põhjalikult uuritud ning töö autor leiab, et SOAR süsteemidel võiks olla oluline koht tuleviku SOC lahendustes.

2.1 CYBERS

CYBERS on 2010. aastal asutatud ettevõte, mis pakub erinevaid küberturbealaseid teenuseid (Inforegister). Ettevõtte poolt pakutavate teenuste hulka kuuluvad näiteks: haavatavuse hindamine, võrguseisundi turbekontroll, Microsoft 365 turvalisus, konsultatsioonid, SOC as a Service (SOCaaS) ja Security as a Service (SECaaS) (CYBERS). Selle töö raames uuritakse eelkõige SOCaaS teenuse toimimist ja vajadusi.

2.2 Küberkaitse operatsioonide keskus ehk SOC

Küberkaitse operatsioonide keskus ehk SOC on nii öelda esimene kaitseliin igasuguste küberintsidentidega tegelemisel. SOC tiim koosneb töötajatest, kelle eesmärgiks on

tegeleda süsteemide monitoorimisega ja küberintsidendi toimumisel pakutakse kliendile otsest abi. SOC töötajad peavad seega mõistma nii klientide ettevõtete ärivajadusi kui ka turvanõudeid, mis nendest vajadustest tulenevad (Murdoch, 2018). SOC spetsialistid on tööülesannete põhjal jaotatud nelja erineva taseme vahel. Järgnevas alapunktis on ülevaatlikult kirjeldatud iga taseme tööprotsesse.

2.2.1 SOC spetsialistide jaotumine tasanditesse

SOC esimese taseme (Level 1) spetsialistide igapäevatöö hõlmab eelkõige reaalajalist monitoorimist. Level 1 spetsialistil on esimene kokkupuude kõigi intsidentidega ning selle tõttu on tema ülesanne kindlaks teha ka valepositiivseid sündmuseid ehk sündmuseid, mille puhul pole tegu ohu või intsidendiga. Sündmuse laekumisel on spetsialisti ülesanne teostada uuring ja algne analüüs. Vajadusel edastatakse sündmused SOC teise taseme spetsialistidele (Level 2), kuid Level 1 ülesanne on teostada esimesed tegevused intsidendi leevendamiseks või peatamiseks ning ka kliente teavitada. Antud töös keskendub töö autor just SOC esimese taseme spetsialistide tööülesannetega seotud protsessidele.

SOC Level 2 spetsialisti ülesanne on teostada põhjalikum uuring Level 1 poolt edastatud sündmustele. Samuti on Level 2 spetsialisti ülesanne intsidentidele reageerida, kui Level 1 töötajal pole selleks vajalikke vahendeid, teadmisi või võimalusi. Ettevõttes CYBERS puudub hetkel eraldi Level 2 töötaja ehk hetkel viib Level 2 tööülesandeid läbi Level 1 analüütik.

SOC kolmanda taseme (Level 3) ülesanneteks on süsteemide haavatavuste analüüsimine ja sissetungirünnete testide koostamine ehk koostada simuleeritud küberrünnakuid, mille eesmärk on süsteemi turvalisust veelgi enam analüüsida (Cloudflare). Level 3 töötajad tegelevad ohtude otsimise ja süsteemide nõrkuste eemaldamisega. Samuti kaasatakse Level 3 töötajad Level 2 töötajatega intsidentide lahendamisesse (Exabeam).

Kõrgeimal SOC tasemel (Level 4) töötab SOC juht. Juhi ülesandeks on hallata tervet SOC meeskonda - teostada järelevalvet, pakkuda tehnilist abi, organiseerida finantsressursse, palgata ja treenida töötajaid (Cassetto, 2019).

SOC analüütikute tööprotsessid on oluliselt seotud erinevate platvormidega, mis võimaldavad klientide süsteeme monitoorida ning logisid hoiustada. Ettevõttes

CYBERS on SOC analüütikute põhilisteks tööriistadeks SIEM platvorm QRadar ja piletisüsteem Jira. Jira on piletisüsteem, mis võimaldab SOC analüütikutel hallata tekkinud intsidente ja sündmuseid ning neid lahendada ja sulgeda. Töö autor leiab, et antud töö seisukohalt pole Jira tööpõhimõtte selgitamine niivõrd oluline. QRadari tööpõhimõtet tutvustab töö autor alapunktis 2.3 Security Information and Event Management ehk SIEM. Järgnevalt on välja toodud mõningad olulisemad CYBERS SOC esimese taseme spetsialistide poolt läbiviidavad protsessid, mis on eelkõige olulised antud töö teema raames.

2.2.2 SOC esimese taseme (Level 1) spetsialistide põhilised tööülesanded ja funktsioonid ettevõttes CYBERS

SOC Level 1 töötaja üheks põhiliseks eesmärgiks, peale süsteemide üldise montooringu, on klientide süsteemides intsidentide tuvastamine ja nende algne käsitlemine. SIEM platvormilt QRadar reeglite põhjal tuvastatud intsidendid saabuvad Jira keskkonda, kus SOC Level 1 analüütik neid esimesena näeb. Süsteemist kogutud info põhjal koostab SOC töötaja intsidendist analüüsi ning teostab esimesed vajalikud tegevused, et intsidenti vältida või leevendada.

Töötaja ülesanne on tuvastada ka valepositiivseid sündmuseid. Level 1 töötaja ülesanne on samuti teavitada kliente, kui on tekkinud intsidendid või sündmused, mis on kliendi seisukohalt väärtuslikud.

Vajaduse tekkimisel peab SOC Level 1 töötaja tegema muudatusi ka klientide süsteemides. Näiteks liikluse keelamine tulemüüris või programmide blokeerimine.

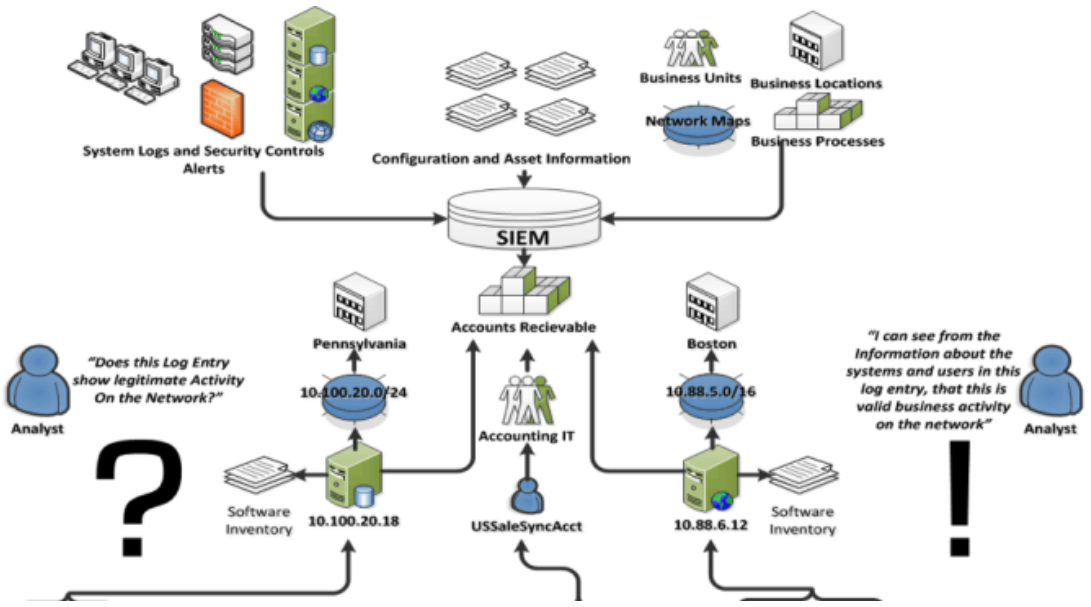
Level 1 analüütiku sekundaarne tööülesanne on ka erinevate raportite koostamine, mille analüüsimine annab klientidele parema ülevaate oma süsteemide turvanõrkustest ja ka töötajate käitumismustritest.

2.3 Security Information and Event Management ehk SIEM

SIEM ehk Security Information and Event Management platvormi eesmärk on koguda andmeid ning võimaldada nende andmete põhjal koostada raporteid ning viia läbi põhjalikku analüüsi. SIEM võimaldab lisaks logide kogumisele neid ka hallata ja hoiustada. Antud vajalikke andmeid hoiustatakse loogiliselt nii, et vajaduse tekkimisel

saaks need võimalikult kiiresti kätte (Johansen, 2020). Joonisel 1 on välja toodud SIEM süsteemi tööpõhimõte. SIEM platvorm kogub informatsiooni sündmuste, võrkude, süsteemide konfiguratsiooni ja muu osas ning selle põhjal suudab platvorm andmeid töödelda. Reeglid, mille põhjal platvorm sündmuseid liigitab, luuakse ettevõtte SIEM inseneride poolt. SIEM platvormile saavad omakorda ligi ettevõtte analüütikud erinevatest füüsilistest asukohtadest ning SIEM platvormilt saadava informatsiooni analüüsimise põhjal on võimalik tuvastada intsidente ja ka valepositiivseid sündmuseid. Lisaks on joonisel välja toodud ka raamatupidamisosakonna ligipääs, mis võimaldab koostada klientidele arveid ja teostada muid tegevusi.

SIEM lahendusi kasutades on võimalik tuvastada palju erinevaid intsidente. Kasutusjuhtudeks on näiteks: autentimiste tuvastamine, sessioonide jälgimine, administratiivsete kasutajate tegevuste jälgimine ja erinevate rünnakute mustrite tuvastamine (Balaji, 2021). Ettevõttes CYBERS-s on kasutusel IBM poolt loodud SIEM platvorm QRadar.



Joonis 1. SIEM süsteemi tööpõhimõte

Allikas: https://gbhackers.com/security-information-and-event-management-siem-a-detailed-explanation/

2.3 Security Orchestration, Automation and Response ehk SOAR

SOC lahendused on tihti hädas erinevate ressursside puuduse tõttu. Informatsiooni pealevool on lõputu, sest võrgus olevad erinevad süsteemid koguvad pidevalt uut andmestikku ning SOC spetsialistid peavad saabuvat teavet jooksvalt analüüsima.

Security Orchestration, Automation and Response ehk SOAR süsteemid on loodud selleks, et lihtsustada SOC töötajate tööprotsesse ning intsidentidele reageerimist ja nende haldamist. SOAR süsteemid loovad võimaluse ühendada endas andmestiku kogumise ja grupeerimise, intsidentide analüüsimise ning protsesside standardiseerimise ja lihtsamate tegevuste automatiseerimise (Kirtley, 2020). SOAR platvormid on ühenduses erinevate turbevahenditega, mis võrgus eksisteerivad ning läbi selle on võimalik kõigi teiste platvormide andmed koguda ühte süsteemi (Walker, 2020). Kogutud andmestiku põhjal suudab platvorm tuvastada mustreid sündmustes ja läbi selle tuvastada intsidente või valepositiivseid sündmuseid. Erinevatelt süsteemidelt kogutud andmed annavad sündmustele rohkem konteksti ning võimaldavad SOC analüütikutel kiiremini intsidentidele reageerida. Samuti võimaldab kogutud informatsioon analüütikul läbi viia põhjalikuma analüüsi intsidendist. Üheks oluliseks eeliseks on ka *playbook*'ide ehk standardiseeritud tegevuste automatiseerimine. See tähendab, et SOAR platvorm suudab ise läbi viia tegevusi, mis on kindlatele intsidentidele defineeritud (Muniz ja Lakhani, 2021). Näiteks, ühe seadme nakatumisel pahavaraga, karantiinib SOAR selle seadme ja takistab viiruse levikut teistesse võrgu seadmetesse. Seega SOAR süsteemi teiste tehnoloogiatega integreerimine aitab vähendada SOC spetsialistide koormust, võimaldab efektiivsemalt tuvastada valepositiivseid sündmuseid ja intsidentidele kiiremini reageerida (Bedell, 2019). CYBERS-s on kasutusel The Hive platvorm, mida töö autor analüüsib peatükis 3 SOAR platvorm The Hive analüüs.

2.4 SIEM ja SOAR lahenduste integratsioon

SIEM on süsteemide kogu võrgus, mis sarnaselt SOAR tehnoloogiatele, koguvad ja hoiustavad andmeid, haldavad logiallikaid ning võimaldavad andmete baasil raporteid koostada. SIEM süsteemide ülesanne on tuvastada erinevate sündmuste vahel mustreid ning nende alusel SOC spetsialiste teavitada (Chakrabarty et al., 2020). Paljud juba

arendatud SOAR süsteemid on loodud SIEM lahenduste põhjal. SOAR lahenduste loomist motiveerisid just SIEM lahenduste puudujäägid (Muniz ja Lakhani, 2021). Seega on SOAR osati SIEM platvormide edasiarendus, kuid ettevõtetes kasutatakse tehnoloogiaid tihti paralleelselt.

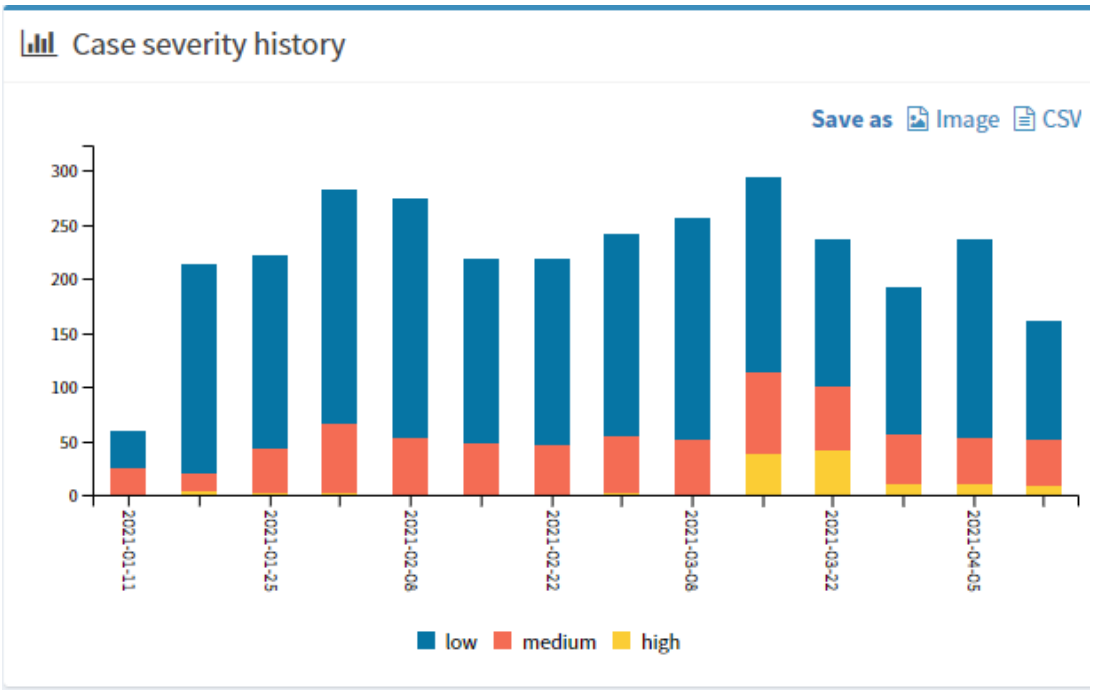
Erinevalt SIEM platvormidele, suudab SOAR automatiseerida ka tegevusi, mida vastasel juhul peaks läbi viima SOC spetsialist. SIEM puhul tuleb intsidentidele reageerida manuaalselt. Mõned SOAR süsteemid aga ei hoiusta ise andmestikku ning nad vajavad selleks SIEM platvormi. Selle tõttu lisab SOC-ile väärtust just mõlema süsteemi kasutamine. SIEM süsteemi põhiülesanne oleks seega andmestiku kogumine ja hoiustamine ning SOAR süsteem võimaldaks kogutud andmestikku grupeerida, interpreteerida, tuvastada mustreid ja automatiseerida lihtsamaid tegevusi intsidentide lahendamiseks.

3 SOAR platvormi The Hive analüüs

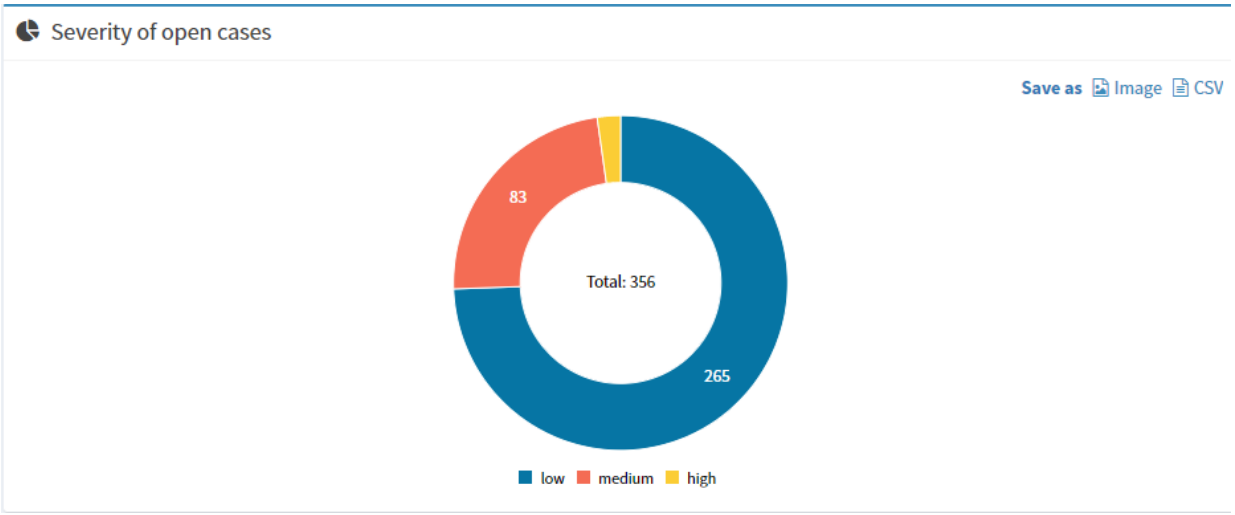
The Hive on avatud lähtekoodiga tasuta SOAR platvorm, mis võimaldab SIEM alertide parema grupeerimise ja analüüsimise. The Hive platvormi eesmärgiks on tagada intsidentide põhjalikum analüüs ja nendele kiirem reageerimine.

Platvormi üheks eeliseks on kollaboratsiooni võimaldamine. See tähendab, et ühte intsidenti on võimalik käsitleda mitmel analüütikul korraga. Läbi selle on analüütikutel parem ülevaade süsteemides toimuvast ning kergem omavahel ülesandeid delegeerida. The Hive pakub analüütikutele võimalust salvestada oma töökäiku, lisada intsidentide lahendustesse tõendeid või avastusi ning jälgida ka teiste analüütikute poolt tehtud tööd. The Hive platvormil on samuti väga kerge koostada ja jälgida intsidentide statistikat, mis annab analüütikutele ja klientidele parema ülevaate kogutud sündmustest ja intsidentidest (The Hive). Joonistel 2 ja 3 on välja toodud sündmuste raskusastme statistika. Joonisel 2 on näidatud kõikide sündmuste raskusastmete ajalugu. Joonis 3 näitab lahendamata juhtumite raskusastmete jagunemist.

The Hive on hetkel suhteliselt noor SOAR, mis tähendab, et platvormil pole lõpuni välja arendatud osasid SOAR süsteemile iseloomulikke funktsioone. The Hive kasutamise võimekus oleneb seega suuresti organisatsiooni eesmärkidest ja võimekusest erinevaid tööriistu The Hive-ga integreerida. Mõned populaarsemad tööriistad on näiteks MISP, Cortex, Synapse, ElasticSearch, VirusTotal, Google Safe Browsing, Cuckoo Sandbox ja Joe Sandbox. Lisatud tööriistade eesmärk on abistada SOC Level 1 analüütiku tööd ja lisada olulist informatsiooni koostatud intsidentide raportitesse.



Joonis 2. Sündmuste raskusastmete ajaloo graafik

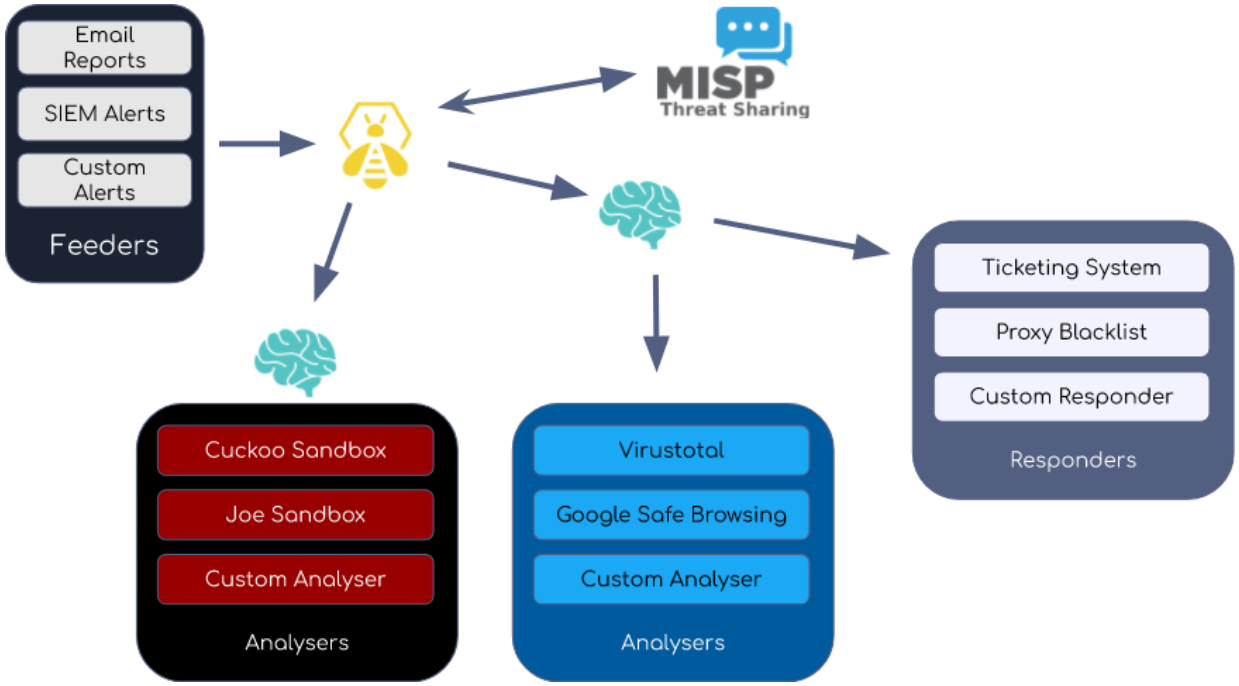


Joonis 3. Lahendamata sündmuste raskusastme graafik

3.1 The Hive tööpõhimõte

SOAR platvormi The Hive tööpõhimõte sarnaneb suuresti SIEM platvormi tööpõhimõttele. Joonisel 4 on näha lihtsustatud The Hive tööpõhimõtte plaan. Platvorm kogub informatsiooni erinevate logide põhjal, mis jõuavad The Hive süsteemi SIEM platvormilt, emailide või muude kanalite kaudu. CYBERS-is on The Hive platvormiga integreeritud ka Malware Information Sharing Platform (MISP). MISP eesmärk on

jagada toimunud intsidentide informatsiooni oma kolleegide ja partneritega ning ehitada andmebaas, mille põhjal lihtsustada pahavaraliste üksuste tuvastamist (MISP project). MISP kõrval on CYBERS-is The Hive-ga integreeritud ka Cortex. Cortex on The Hive-ga paralleelselt loodud tööriist, mis võimaldab koostada päringuid intsidendiga seotud üksuste kohta ühel platvormil. Näiteks, IP aadressi analüüs (The Hive Project: Cortex). MISP-i ja Cortexi kõrval on samuti kasutusel Synapse ja ElasticSearch. Synapse on samuti The Hive Projecti toode, mille ülesanne on genereerida sündmuseid meili ja SIEM alertide põhjal (The Hive Project: Synapse). Elasticsearchi töö on toetada The Hive ja Cortex teenuseid The Hive klastrite jooksutamisega. Automaatse analüüsi koostamiseks kasutab The Hive erinevaid vabavaralisi tööriistu: Cuckoo Sandbox, Joe Sandbox, VirusTotal, Google Safebrowsing jt. Automaatse analüüsi tulemused on abiks analüütikutele lõpliku raporti koostamisel. Analüüsitud ja kogutud informatsioon jõuab analüütikuni valitud piletisüsteemis (CYBERS-is kasutusel Jira).



Joonis 4. SOAR platvormi The Hive tööpõhimõte

Allikas: https://skilledfield.com.au/what-we-do/

4 CYBERS SOC teenuse tööprotsesside analüüs

Nagu eelnevalt mainitud, viivad SOC analüütikud ja insenerid läbi erinevaid protsesse, mis aitavad tagada teenuse eduka toimimise. Nendeks protsessideks on näiteks: süsteemide monitoorimine, intsidentide ja valepositiivsete sündmuste tuvastamine ja intsidentidele reageerimine.

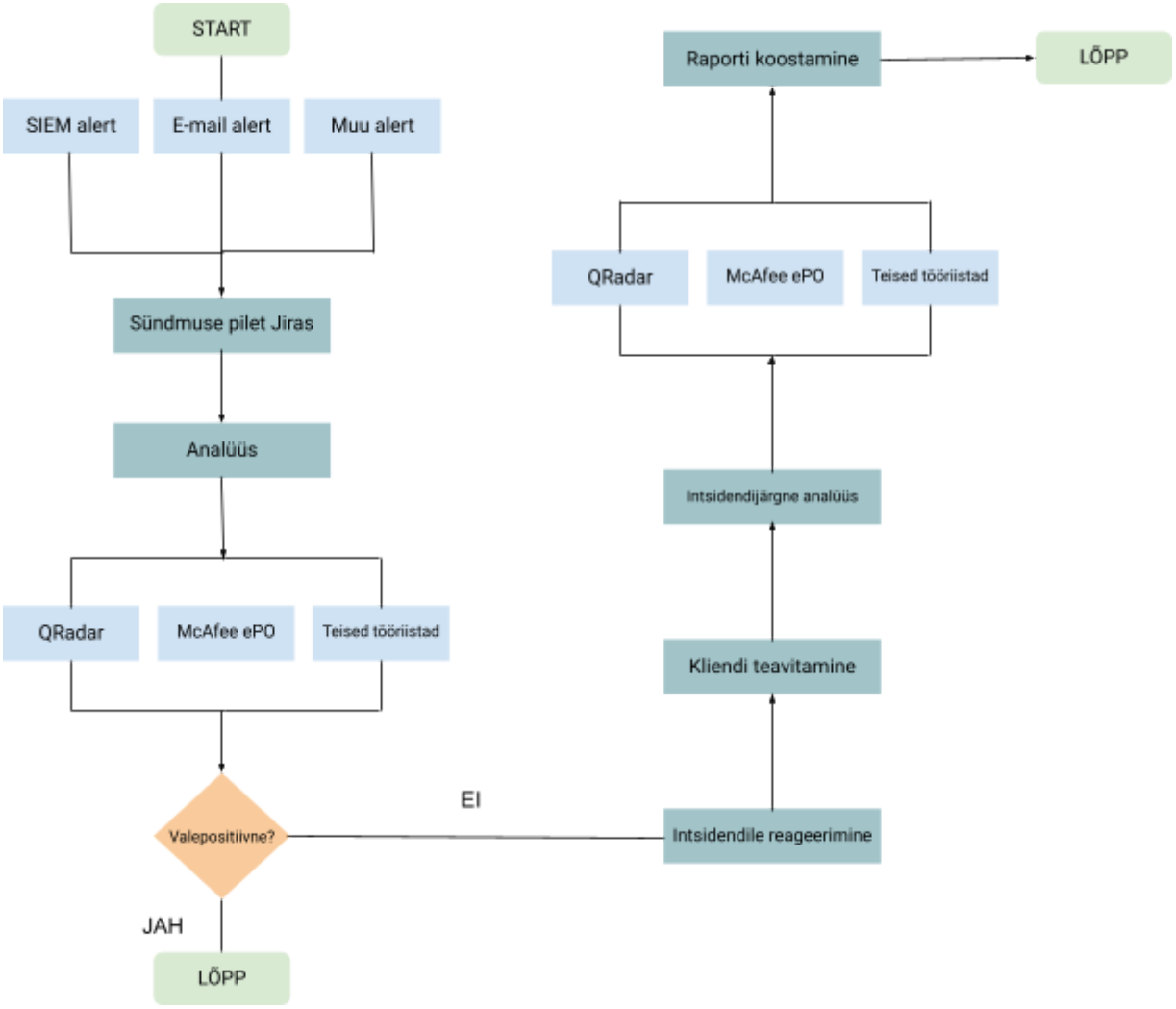
Antud peatükis analüüsib töö autor põhilisi SOC teenuse tööprotsesse ettevõttes CYBERS. Analüüsi käigus käsitletakse protsesside olemust ja olemasolevaid nõrkuseid, mida aitaks leevendada või eemaldada SOAR platvormi integratsioon SOC teenusesse.

4.1 SOC Level 1 analüütiku töötsükkel

SOC Level 1 analüütiku tööprotsess koosneb mitmetest erinevatest tegevustest. Joonisel 5 on välja toodud lihtsustatud töötsükkel, mille protsesse töö autor käesoleva töö raames analüüsib. Nendeks protsessideks on süsteemide monitooring, intsidentide ja valepositiivsete sündmuste tuvastamine ja analüüs, intsidendile reageerimine, klientide teavitamine, intsidentide lahendamises osalemine ja intsidendijärgne analüüs. Antud joonis on lihtsustatud versioon analüütiku tööülesannetest, et anda töö lugejale visuaalne ülevaade protsesside järjekorrast. Tegelikes olukordades hõlmab analüütiku töötsükkel veel tegevusi, kuid töö autor leiab, et antud töö raames pole need niivõrd olulised.

Analüütiku töö algab süsteemide logide põhjal moodustatud alertide jõudmisel piletisüsteemi Jira. Seejärel teostab analüütik algse analüüsi, mille põhjal otsustab analüütik, kas tegu on intsidendiga või mitte. Joonisel on välja toodud tööriistad QRadar ja McAfee ePO, mis on põhilised platvormid, millelt infot kogutakse. Teiste tööriistade alla kuuluvad näiteks VirusTotal, Sophos ja Sharepoint. Valepositiivse sündmuse esinemisel lõppeb intsidendi käsitlemine, kuid analüütik peab siiski valepositiivsest sündmusest teavitama SIEM tiimi, kelle ülesanne on kohandada reegleid nii, et valepositiivseid sündmuseid ei genereeritaks nii suures mahus. Intsidendi puhul on järgmiseks sammuks intsidendile reageerimine, mille käigus teeb analüütik vajalikke samme, et intsidenti peatada või leevendada. Samuti tuleb intsidendist teavitada kliente ning vajadusel kaasata nad intsidendile reageerimise etapis. Peale intsidendi

lahendamist tuleb analüütikul koostada intsidendijärgne analüüs, mille läbiviimiseks tuleb analüütikul taaskord kasutada joonisel kirjeldatud vahendeid. Lõpliku analüüsi põhjal koostab analüütik raporti, mis vajadusel klientidele edastatakse. Raporti koostamisega lõppeb SOC Level 1 analüütiku töötsükkel ettevõttes CYBERS.

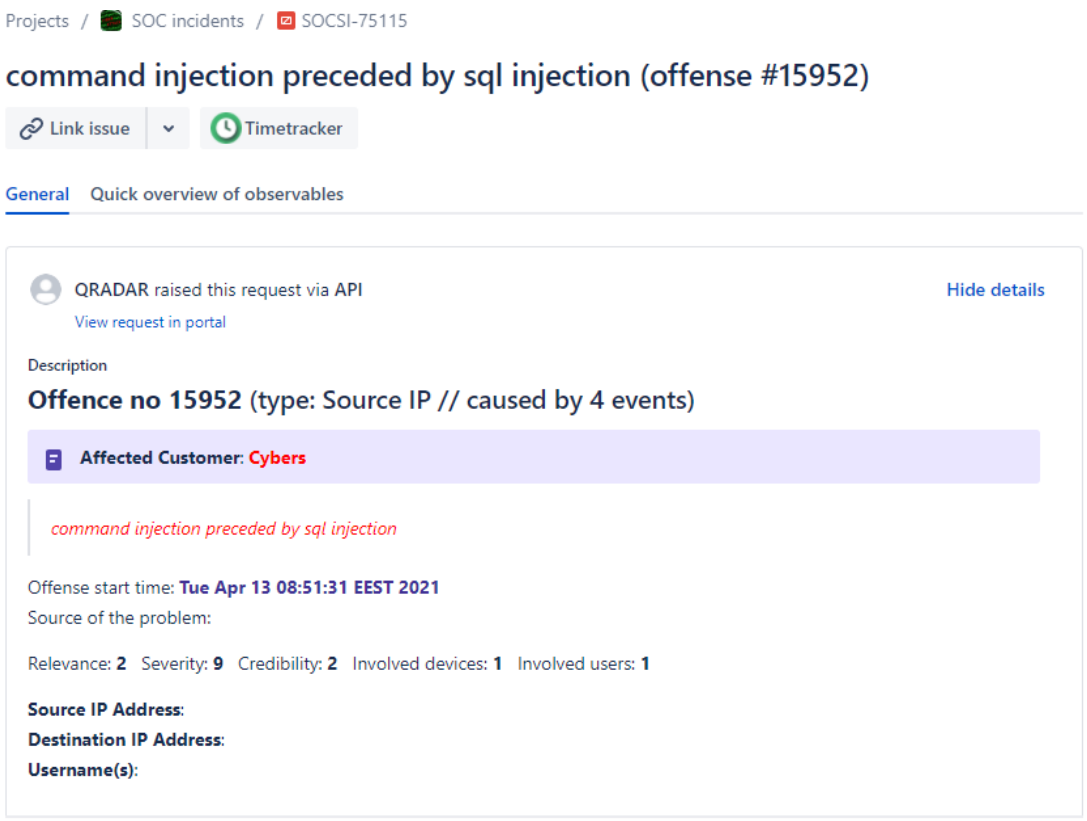


Joonis 5. SOC Level 1 analüütiku töötsükkel

4.1.1 Reaalajaline monitooring

Süsteemide monitoorimine on üks põhilistest SOC teenuse protsessidest, mis paneb aluse nii intsidentide tuvastamisele kui ka nendele reageerimisele. Monitooringu eesmärgiks on jälgida süsteemide keskkonda, platvormide seisundit ja tuvastada alarme. Võimalikke turbesündmuseid grupeeritakse QRadari platvormil koostatud reeglite põhjal ning seejärel edastatakse juba Level 1 analüütikule läbi piletisüsteemi. Piletisüsteemis Jira näeb analüütik piiratud informatsiooni, mis kuvatakse Jirasse kindla

vormi põhjal. Joonisel 6 on välja toodud SQL süstimisründe intsident. Joonisel on näha väärtuseid, mis Jiras analüütikule kuvatakse: intsidendi identifikaator ehk *Offence no*, intsidendi algusaeg ehk *Offense start time*, lähtesüsteemi IP aadress ehk *Source IP Address*, lõppsüsteemi IP aadress ehk *Destination IP Address*, intsidendiga seotud kasutajad ehk *Username* ja erinevad intsidendiga seotud mõõdikud (*Relevance, Severity, Credibility, Involved Devices* ja *Involved Users*). Sensitiivse informatsiooni turvalisusega seoses on jooniselt eemaldatud mõned väärtused.



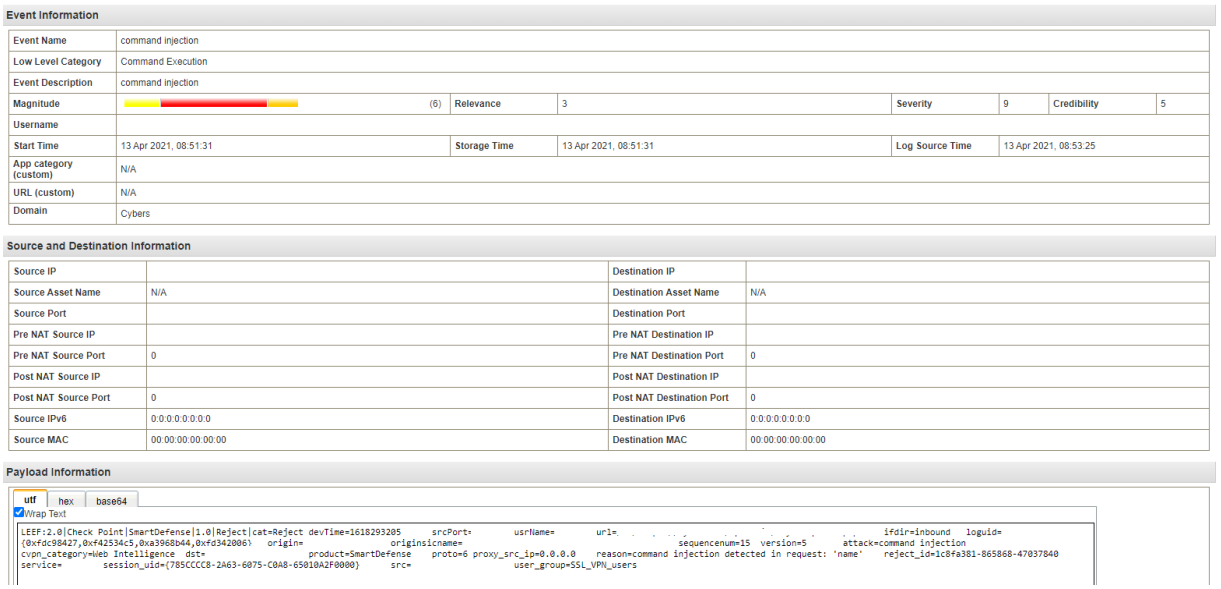
Joonis 6. Sündmuse vorm piletisüsteemis Jira

4.1.2 Intsidentide ja valepositiivsete sündmuste analüüs ning tuvastamine

SOC Level 1 analüütiku üheks põhiliseks tööülesandeks on tuvastada intsidente ja valepositiivseid sündmuseid. Kõik kogutud sündmused saabuvad piletisüsteemi platvormile Jira ning analüütiku ülesandeks on läbi viia analüüs, mille käigus tuleb tal välja selgitada, kas tegu on reaalse intsidendiga või valepositiivse sündmusega.

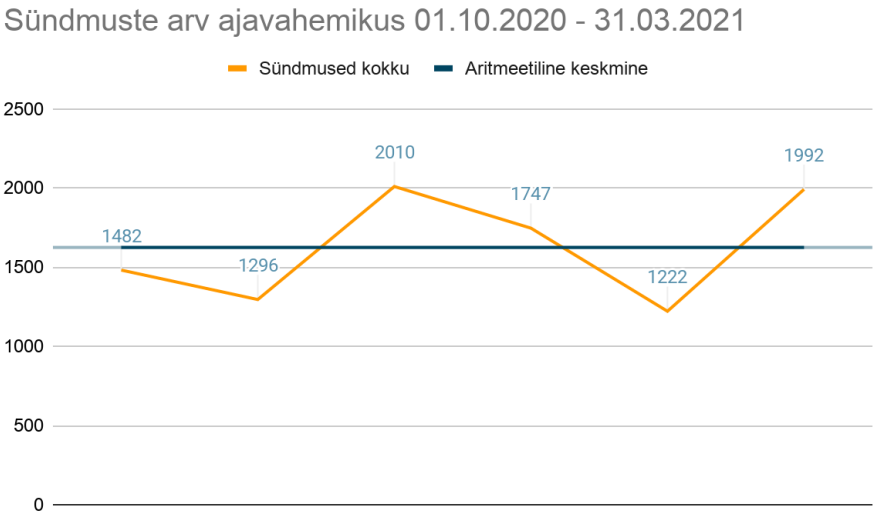
Jiras saadaval olev informatsioon pole tihti piisav, et analüütik saaks läbi viia põhjaliku uuringu ning selle tõttu peab analüütik pöörduma SIEM platvormile QRadar, mis pakub sündmuse kohta rohkem informatsiooni. Joonisel 6 on näha eelnevas alapunktis välja

toodud intsidendi raportit QRadar platvormil. Lisaks Jiras olemasolevatele väljadele, on lisandunud uued väljad ja ka sündmuse *raw log* ehk töötlemata logi UTF formaadis. QRadaris kuvatakse ka reeglid, mille põhjal on sündmuse tuvastamine tehtud ning see annab analüütikule aimduse sündmuse võimalikest põhjustest. Kuvatud informatsiooni põhjal teostab Level 1 analüütik sündmuse analüüsi. Sensitiivse informatsiooni turvalisusega seoses on jooniselt eemaldatud mõned väärtused.



Joonis 7. Intsidendi informatsioon QRadaris

Hetkel toimub valepositiivsete ja intsidentide tuvastamine analüüsi ajal. See tähendab, et analüütik kulutab aega, et sündmuseid uurida, ja selle käigus saab aru, kas tegu on intsidendiga või mitte. Keerukamate sündmuste analüüs võib ka vajada palju aega ja teiste töötajate kaasamist. Kui süsteemid genereerivad suurel hulgal sündmuseid, peavad analüütikud kõik sündmused käsitsi läbi töötama ja analüüsima, mis kurnab nii inim- kui ka ajalist ressurssi. Joonisel 7 on näha kuus genereeritud sündmuste arvu ajavahemikus 01.10.2020 - 31.03.2021. Valitud ajavahemikus genereeriti kuus keskmiselt 1625 sündmust. Sündmused sisaldavad nii intsidente kui ka valepositiivseid sündmuseid ehk Level 1 analüütik pidi selles ajavahemikus kuus keskmiselt analüüsima 1625 sündmust. Lisaks võib oluliselt pikeneda intsidentidele reageerimise aeg, mis võib mõndadel juhtudel intsidendi tagajärgi oluliselt mõjutada. Selle tõttu on oluline, et süsteemid tekitaksid võimalikult vähe valepositiivseid sündmuseid ja pakuksid analüütikule võimalikult olulist informatsiooni.



Joonis 8. Sündmuste arv ajavahemikus 01.10.2020 - 31.03.2021

4.1.3 Intsidendi analüüs

Intsidendi toimumisel on SOC töötaja ülesandeks koostada intsidendi analüüs, mis edastatakse ka kliendile teavitust tehes. Analüüsi koostamiseks kasutatakse erinevaid platvorme ja allikaid: Jira, QRadar, McAfee ePO, McAfee Trustedsource, VirusTotal jne.

Nagu eelpool mainitud, toimub hetkel intsidendi analüüs mitme erineva platvormi pealt saadava informatsiooni kombineerimisel. Informatsiooni kogumine, otsimine ja analüüsimine kulutab aega ning pikendab võimalikule intsidendile reageerimise aega. Suureks probleemiks võib kerkida ka analüütiku tähelepanu hajumine. Mitme erineva platvormiga töötamine ja informatsiooni rohkus võib olla töötajale koormav ning töökvaliteet võib selle tõttu langeda. Lisaks tähendab platvormide rohkus seda, et analüütik vajab igale platvormile eraldi ligipääsu, mis võib omakorda suurendada turvariske.

4.1.4 Intsidendile reageerimine

Kui analüütik on tuvastanud intsidendi, on tema ülesanne sellele reageerida ja protsessi alusel teavitada vajalikke kontaktisikuid. Intsidendile reageerimise protsess oleneb intsidendi olemusest ning vastavad tegevused on dokumenteeritud SOC *playbook*'is. Protsessi läbiviimiseks peab SOC analüütik avama antud dokumentatsiooni ning jälgima seal kirjeldatud samme. Näiteks saab tuua kliendi süsteemist pahavara

avastamise. Esimese sammuna peab analüütik tuvastama pahavaralise faili ning seda analüüsima. Analüüsi saab teostada kasutades faili *hash*-i ehk räsi väärtust, võrreldes seda juba varasemalt tuvastatud pahavaraliste failide räsidega. Samuti saab faili proovi analüüsida erinevatel *sandbox* platvormidel. Oluline on tuvastada, kui kaua fail süsteemis oli ja, kuidas see sinna sai. Selle abil on võimalik teada saada, kas fail võib olla ka teistes süsteemides või on tegemist üksikjuhtumiga. Kui avastatud pahavaralist faili pole viirustõrjetarkvara juba puhastanud või kustutanud, tuleb nakatunud süsteem võrgust eemaldada ja karantiinida. Seejärel tuleb süsteem puhastada ja kinnitada, et pahavaraline fail sai süsteemist kustutatud. Igal juhul tuleb teavitada klienti pahavaralise faili tuvastamisest süsteemis. Kliendi ülesanne on teavitada süsteemi omanikku või kasutajat.

4.1.5 Klientide teavitamine

Üheks SOC töötaja ülesandeks on klientide teavitamine intsidendi tuvastamise korral. Samuti on vaja kliente intsidentide lahendamisesse kaasata, kui SOC töötajatel pole klientide süsteemidele piisavat ligipääsu. Kliendi teavitamise protsess on kirjas iga kliendiga sõlmitud intsidendi halduse protsessis. Protsessi tutvustab ja lepib kliendiga kokku vastav SPOC. Kliente teavitatakse meili ja/või Microsoft Teamsi või Skype teel. Iga kliendi teavitamise protsess on dokumenteeritud ning kliendi teavitamiseks peab analüütik seda tegema dokumentatsiooni alusel. Mõndade klientide teavitamiseks on loodud meilivormid, mille analüütik peab saatmisel täitma. See sisaldab vajalikku informatsiooni intsidendi kohta: toimumise aeg, intsidendi detailid ja edasised tegevused.

Seni toimub klientide teavitamine paika pandud dokumentatsiooni alusel. See tähendab, et analüütik peab teavitamiseks dokumentatsioonist ligi saama meilivormidele ja kontaktidele, keda teavitada tuleb. Samas pole mõndade klientide teavitamise protsessi lõpuni paika pandud, sest protsesside loomine sõltub suuresti lepingu sõlmimise staatusest ja kliendi hõivatusest. Sellisel juhul peab analüütik lähtuma isiklikust hinnangust. Selline protsessi puudumine loob olukorra, kus teavitused võivad suuresti erineda ning kliendil võib olla raske intsidenti süveneda, kui teavituste vormistus analüütikuti erineb. Ühtse protsessi loomine kõigile klientidele aitab tagada vajaliku informatsiooni jõudmise klientideni ning samuti tõstab teavituste professionaalsuse taset.

4.1.6 Intsidendijärgne analüüs

Intsidendile reageerimisele järgneb intsidendijärgne analüüs, mille käigus koostab SOC töötaja põhjaliku ülevaate intsidendist ja tegevustest, mida tehti. Analüüsi saab kaasata erinevaid aspekte, mida mõjutab suuresti intsidendi olemus. Uurida saab näiteks: miks intsident juhtus, kas intsidenti oleks saanud ära hoida, kuidas intsidenti tulevikus ära hoida ja tuvastada, kas ilmnes mingeid mustreid või trende. Lisaks tuleb analüüsi lisada kõik tegevused, mida tiimi poolt tehti, et intsidendiga tegeleda. Saab välja tuua asju, mida võiks tulevikus teisiti teha ja ettepanekuid järgmiste intsidentidega tegelemiseks (Roberts ja Brown, 2017). Intsidendijärgse analüüsi eesmärk on tagada ülevaatlik kokkuvõtte protsessidest, reageerimisajast reaalses situatsioonis ning võimalikest nõrkustest. Analüüsi on võimalik kasutada sarnastes situatsioonides ning võimaldab oluliselt parandada intsidentide lahendusi ja protsesse (Herrera, 2010).

Nagu eelnevalt mainitud, toimub pidev analüüs mitmel platvormil korraga ning see tähendab, et analüüsi läbiviimiseks kurnatakse rohkem ressursse ja aega. Analüüsi koondamine vähematele platvormidele aitaks kiirendada intsidendijärgse analüüsi valmimist.

5 SOAR platvormi The Hive integratsioon CYBERS SOC teenusesse

Peatükis 4 kirjeldas töö autor SOC Level 1 analüütiku põhilisi tööülesandeid ning nendega seotud nõrkuseid. SOAR platvormi integreerimine SOC-i pakub võimalust leevendada või lahendada osasid probleeme ning samas aitab luua uusi funktsioone, mis veelgi enam SOC teenust arendavad. Antud analüüsi on töö autor koostanud tuginedes enda tööülesannetele ja kogemustele. Samuti on tulemuste efektiivsust kinnitanud ettevõtte insenerid ja SOC haldur Jürgen Erm.

5.1 Kollaboratsioon

The Hive integreerimise üheks eeliseks praeguse süsteemi ees on kollaboratsiooni võimaldamine SOC analüütikute vahel. Piletisüsteemi Jira litsentsid on üsna kallid ning platvormil töötamiseks tuleb igale analüütikule soetada eraldi kasutajalitsents. Seni on CYBERS-i SOC tiim noor ning töötajate arv on väike ning selle tõttu pole ka Jiraga seotud väljaminekud eriti kulukad. Tiimi kasvades võib tekkida olukord, kus tuleb investeerida uutesse litsentsidesse või organiseerida töökorraldust nii, et analüütikutel oleks võimalik jagada ühist litsentsi. Selline lahendus võib osutuda liialt kulukaks või keerukas ning pole pikas perspektiivis efektiivne. Samuti on probleemiks analüütiku tuvastamine jagatud litsentsiga töö tegemisel. Ühe litsentsi all töötavatel analüütikutel tuleks intsidendi lahendusse lisada oma andmed, et lihtsustada töötaja tuvastamist tulevikus. Juhul, kui analüütik unustab seda teha, muutub töötaja tuvastamine keerukaks ning võib olulistes olukordades pikendada tööprotsesse ja intsidentide lahendamist.

The Hive võimaldab ettevõtetele piiramatu arvu töötajate lisamise keskkonda. Kasutaja lisamine on tasuta ning ei nõua ettevõttelt väljaminekuid. Igale SOC töötajale tuleb luua kasutaja, mis annab talle võimaluse platvormile ligi pääseda. Personaalsete kasutajate loomine annab analüütikutele ka võimaluse koostööks. Keerukamate intsidentide lahendamisel on tihti vaja mitme töötaja kaasamist ning personaalsete kasutajate puhul on võimalik igal töötajal probleemile eraldi ligi saada. Personaalsete kasutajatega töötamine likvideerib ka probleemid analüütiku tuvastamisel, mis tekivad ühise kasutaja jagamisel.

5.1.1 Töövoog ja tööülesannete jagamine

Analüütikute töö efektiivsemaks muutmiseks tuleks samuti kasutusele võtta tööülesannete jagamine ja töövoo haldamine. Sündmuse jõudmisel The Hive platvormile peab esimesena reageeriv analüütik selle lisama enda tööülesannete alla. See võimaldab efektiivselt intsidente jagada ning vältida olukorda, kus mitu analüütikut töötavad korraga sama intsidendiga. Tööülesannete jagamine aitab samuti vähendada analüütikute koormust ning jagada seda töötajate seas võrdsemalt. The Hive portaalist on võimalik näha ühe analüütiku alla koondatud tööülesandeid ja vajadusel on neid võimalik teisele töötajale edasi delegeerida. Tööülesannete jagamine annab samuti võimaluse tulevikus kergemini tuvastada intsidendiga töötanud analüütikut. See on eriti oluline, kui esinevad sarnased intsidendid või intsidendi lahenduse osas on tekkinud küsimusi.

5.2 Reaalajaline monitooring, intsidentide ja valepositiivsete sündmuste tuvastamine

SOAR süsteemi paralleelne kasutamine SIEM ja teiste platvormidega hõlpsustab süsteemide monitoorimist, logide kogumist ja nende põhjal intsidentide tuvastamist. The Hive-i eesmärk pole andmestikku kogumine, vaid teiste platvormide kogutud logide grupeerimine ja tuvastamine. Valepositiivsete sündmuste tuvastamiseks tuleks The Hive-ga siduda erinevad turbetööriistad, nt. MISP, VirusTotal, Joe Sandbox jt. Need võimaldavad platvormile koguda informatsiooni sündmuses esinenud väärtuste kohta (IP aadressid, domeenid, kasutajanimed) ning selle tulemusena on analüütikul kergem valepositiivseid sündmuseid tuvastada.

Erinevate turbetööriistade integreerimine ühe platvormiga kiirendab intsidentide tuvastamist ja grupeerimist. MISP ja teiste sarnaste andmebaaside lisamine võimaldab hinnata intsidenti varem esinenud sarnaste sündmuste ja väärtuste põhjal. Varem toimunud intsidentide kuvamine on abiks intsidendi kriitilisuse hindamisel ja võimaldab töötajal sündmuseid prioritiseerida. Sarnaste intsidentide hindamine aitab analüütikul ka võimalikke reageerimiseks vajalikke tegevusi plaanida. Valepositiivsete sündmuste tuvastamise lihtsustamine säästab Level 1 analüütiku aega ning võimaldab töötajal keskenduda reaalsetele intsidentidele. Tänu sellele vähendatakse intsidendile

reageerimise ja analüüsi koostamise aega. Kriitilistes olukordades mängib selline funktsioon suurt rolli ning võib aidata vältida võimalikke tagajärgi.

5.2.1 Automatiseerimine algse analüüsi tasemel

Tegevuste automatiseerimine on platvormil seni piiratud ning nõuab ettevõtte initsiatiivi ja ressursse. Automatsioon on siiski võimalik, kuid suurem osa tööst tuleks läbi viia CYBERS inseneride poolt. Platvormipoolne automatsioon seisneb eelkõige informatsiooni kogumises ja väärtuste analüüsimises erinevate turbetööriistadega. Nagu eelnevalt mainitud, saab The Hive-ga siduda erinevaid turbetööriistu. Tööriistade poolt tehtav analüüs on võimalik automatiseerida ning sündmuse avamisel platvormil kuvatakse ka juba automaatselt käivitatud analüüs.

5.3 Intsidendi analüüs

The Hive platvormi kasutusele võtmine muudaks intsidendi analüüsimist oluliselt. Nagu varasemalt mainitud, koondab The Hive mitmete erinevate platvormide logid ühte süsteemi ning elimineerib vajaduse töötada korraga üle mitme aplikatsiooni. The Hive konsooli kuvatakse sündmusega seotud UTF formaadis logid, seotud intsidendid ja varasemalt esinenud väärtused (nt. korduvad IP aadressid, kasutajanimed). The Hive sidumisel erinevate tööriistadega (Cortex, Synapse, Elasticsearch, Joe Sandbox, VirusTotal jt.) suurendatakse SOC võimekust veelgi.

Informatsiooni koondamine ühele platvormile muudab SOC analüütiku tööd efektiivsemaks mitmes aspektis. Olulisim muutus esineb eelkõige ajalises ressursis, mida analüütik kulutab, et koostada intsidendi analüüsi. The Hive kasutamine võimaldab SOC Level 1 töötajal suure osa raportist koostada ainult ühelt platvormilt saadava informatsiooni põhjal. Varasem lahendus on nõudnud analüütiku töötamist üle mitme erineva süsteemi ning läbi selle kulutab Level 1 oluliselt rohkem aega, et intsidendi lahendamiseni jõuda. Ühel platvormil töötamine aitab ka koondada analüütiku tähelepanu. Kogu informatsioon on ühes kohas ning ei nõua analüütikult pidevat uue andmestiku läbi töötlemist erinevatel platvormidel.

5.4 Klientide teavitamine ja raportite esitamine

The Hive-i on sisse ehitatud funktsioon, mille abil on mugav luua erinevaid visuaalseid materjale. Visuaalsete kujutiste kaudu on eelkõige kasulik klientidele saata statistilisi andmeid või tulemuste raporteid. Tulemuste toetamine visualiseeritud andmetega muudab nende töötlemise kergemaks ning samuti loob kliendile suurema pildi kogutud informatsioonist. Varasemalt on visuaalseid materjale loodud käsitsi ja raportite loomiseks kasutatud skripte või AQL päringuid. The Hive võimaldab raportite automatiseerimise ja andmete põhjal graafikute koostamist ühel platvormil. Visuaalsete graafikute kasutamine lisab väärtust ka Level 1 analüütikute koormuse jagamisel. Graafikutelt on näha, kui palju on iga analüütik intsidente lahendanud ja intsidente, mille lahendamisega tegeletakse.

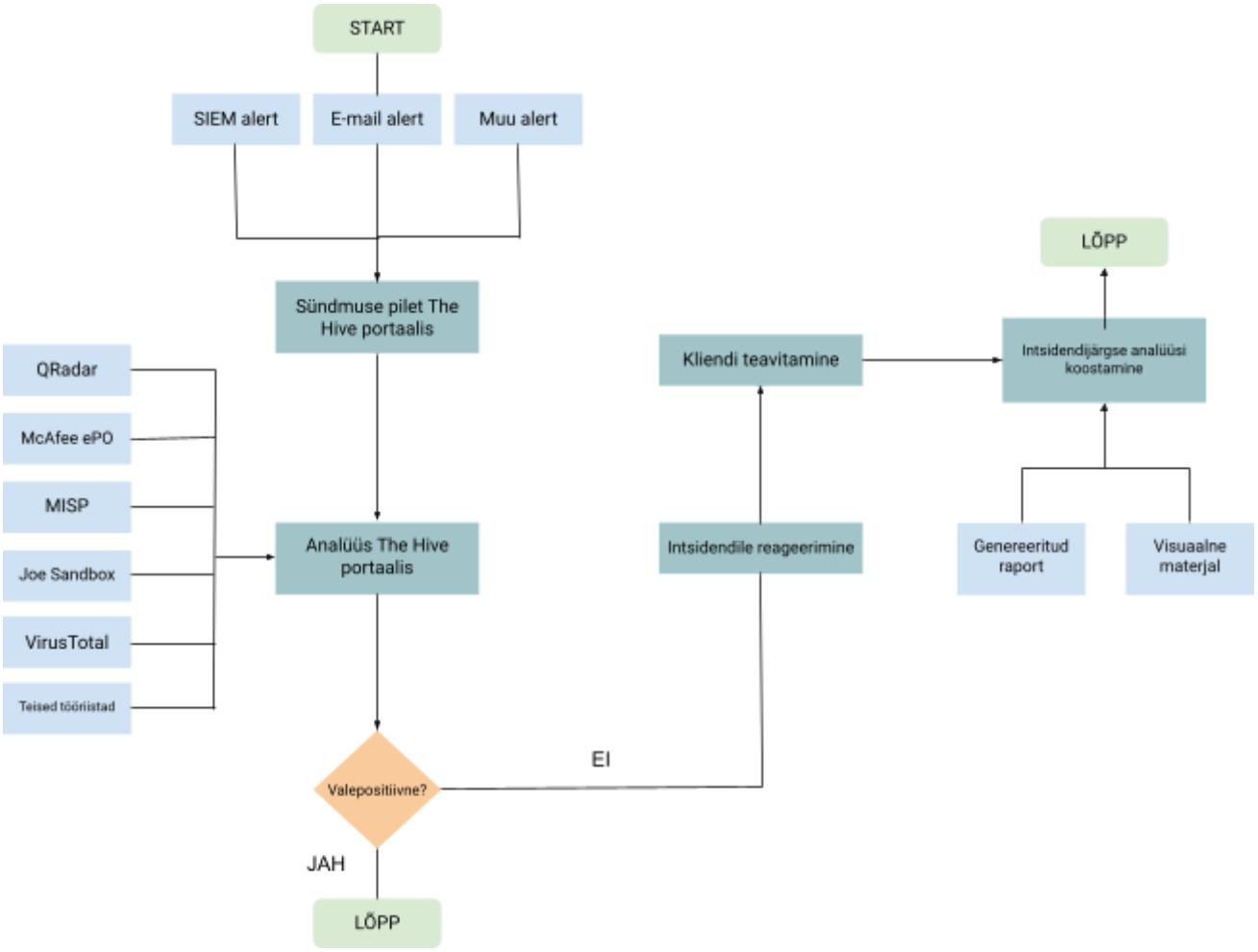
Raportite ja visuaalsete materjalide automatiseeritud genereerimine on SOC Level 1 analüütikule abiks mitmes aspektis. Esiteks, säästab automaatne genereerimine analüütikule aega ja manuaalse töö tegemist. Teiseks, loob The Hive atraktiivseid ja loogilisi graafikuid, mille koostamiseks ei pruugi igal analüütikul piisavat pädevust olla. Kolmandaks, jälgivad koostatud graafikud ja raportid ühtset vormistust ja ülesehitust ehk kliendile saadetakse alati sarnaseid materjale, mille läbi töötlemine on selle tõttu lihtsam.

5.5 Ümberkavandatud SOC Level 1 analüütiku töötsükkel

Efektiivsema SOC teenuse implementeerimiseks tuleb teha muudatusi Level 1 analüütiku töötsüklis arvestades The Hive integreerimisel tekkivaid võimalusi ja funktsioone. Võimalikult efektiivse teenuse loomiseks peab kindlaks tegema, et kõik SOC analüütikud on teadlikud ja võimelised kõiki platvormi funktsioone kasutama ning suudavad töötsükli osasid täita. Selleks peaks iga töötaja läbima The Hive koolituse, mis tuleb organiseerida ettevõtte CYBERS poolt.

Joonisel 9 kujutatud ümberkavandatud töötsükkel saab alguse samuti teavitustega, mis jõuavad nüüd The Hive portaali. Esimesena reageerinud töötaja peab selle sündmuse märkima enda tööülesannete alla ja seejärel hakkama koostama algset analüüsi. Platvormil on juba läbi viidud automatiseeritud analüüs sündmuses esinenud väärtuste kohta. Automaatse analüüsi koostavad The Hive-ga integreeritud erinevad tööriistad:

MISP, Joe Sandbox, VirusTotal jt. Samuti kuvatakse platvormil kõigist logiallikatest saadud informatsioon ehk analüütik ei pea logiallikaid eraldi läbi käima. Algse analüüsi põhjal selgitab analüütik, kas tegu on valepositiivse sündmusega või reaalse intsidendiga. Valepositiivse sündmuse puhul lõppeb analüütiku töötsükkel ning ta teavitab sellest SIEM tiimi. Intsidendi toimumisel on SOC Level 1 analüütiku tööülesandeks sellele reageerida ehk läbi viia erinevaid tegevusi, mis aitavad intsidenti peatada või tagajärgi leevendada. Sellele järgneb kliendi teavitamine ja intsidendijärgse analüüsi koostamise, mis vajadusel esitatakse ka kliendile. Intsidendijärgse analüüsi koostamisel saab analüütik kasutada erinevaid juba platvormil genereeritud raporteid ja visuaalseid materjale, mis analüüsi täiustavad. Peale analüüsi koostamist lõppeb SOC Level 1 analüütiku töötsükkel.



Joonis 9. Ümberkavandatud SOC Level 1 analüütiku töötsükkel

Ümberkavandatud SOC Level 1 analüütiku töötsükli eesmärk on muuta ülesannete läbiviimine efektiivsemaks ning läbi selle parendada SOC teenuse toimimist ettevõttes

CYBERS. The Hive kasutuselevõtuga on võimalik oluliselt vähendada intsidendi analüüsimiseks kuluvat aega ning selle tõttu intsidentidele kiiremini reageerida. Kriitilistes olukordades tähendab kiirem reageerimisaeg väiksema mõjuga tagajärgi või vahest ka intsidendi peatamist. Uus töötsükkel ja platvorm aitab vähendada analüütikute stressi ja koormust, mis tulenevad mitmel aplikatsioonil korraga töötamisest. Informatsiooni koondamine muudab info kergemini läbi töödeldavaks ning ei nõua, et töötaja analüüsib igal platvormil andmeid uuesti. Töötaja tähelepanu suunamine ainult ühele aplikatsioonile vähendab ka tõenäosust, et analüütik midagi ei märka. Rohkema informatsiooni nägemine annab parema ülevaate toimuvast ning aitab luua sisukamaid analüüse. Ühtselt vormistatud raportite ja graafikute loomine muudab nende lugemise klientidele loogilisemaks ning jätab ka teenusest professionaalsema mulje.

5.6 The Hive võimalused tulevikus

The Hive on suhteliselt noor SOAR platvorm, mis tähendab, et paljud funktsioonid on alles realiseerimisel. Klassikaliste SOAR süsteemide üheks lahutamatuks osaks on *playbook*'ide põhjal tegevuste automatiseerimine, mille eesmärgiks on vähendada analüütikute poolt tehtavaid rutiinseid tegevusi. Hetkel on automatsioon mingi tasemeni võimalik, kuid nõuab olulisel määral inseneride kaasamist. The Hive arenedes tuleks kindlasti antud funktsioon kasutusele võtta ja SOC teenusega integreerida. Hetkel pole platvormil ka iseseisvat funktsiooni, mis tegeleks valepositiivsete sündmuste tuvastamisega. Siiski toetatakse analüüsi teiste tööriistadega, mis peaks kiirendama valepositiivsete sündmuste tuvastamist. Tulevikus lisatakse kindlasti erinevate tööriistade integreerimise võimalusi juurde ja läbi selle suurendatakse platvormi analüüsivõimekust veelgi.

Tulevikus võiks ettevõte CYBERS uurida automatsiooni võimalusi ning keskenduda valepositiivsete sündmuste efektiivsemale tuvastamisele. Nende eesmärkide täitmiseks on oluline saada suurem ligipääs klientide süsteemidele ja kooskõlastada nende kasutamine. Automatsiooni kasutamiseks tuleks lõplikult üle vaadata ja paika panna *playbook*'id ning arutada platvormi võimalusi vastavate inseneridega.

Kokkuvõte

Käesoleva töö eesmärgiks oli Küberturbe Operatsioonide Keskuse (SOC) analüütikute töö efektiivsemaks muutmine SOAR süsteemi The Hive ettevõtte CYBERS SOC teenusesse integreerimise abil. SOAR süsteemid on suhteliselt uus arendus küberturbe valdkonnas ning nende kasutusele võtmine aitaks oluliselt parendada teenuse toimimist ja vähendada SOC analüütikute koormust.

Esiteks andis töö autor ülevaate tehnoloogiatest ja teenustest, mis antud töö raames olulised on: SOC, SOAR ja SIEM. Samuti kirjeldati ettevõtte CYBERS tausta ja SOC analüütikute tööülesandeid. Seejärel analüüsis töö autor põhjalikumalt SOAR platvormi The Hive funktsioone ja ülesehitust valitud ettevõttes. Toodi välja ka võimalused ja platvormi eesmärgid. Põhjalikum analüüs koostati ka SOC esimese taseme analüütiku tööülesannetest ja protsessidest ning toodi välja põhilised kitsaskohad. Selle analüüsi tulemusena koostas töö autor esmase SOC esimese taseme analüütiku töötsükli graafiku. Töö viimases põhiosas kirjeldas töö autor The Hive platvormi integratsiooni SOC teenusesse ning tõi välja süsteemi integreerimise eelised. Samuti koostas ja kirjeldas töö autor ümberkavandatud SOC esimese taseme analüütiku töötsükli graafiku.

Antud töö raames keskenduti ainult SOC esimese taseme analüütiku tööülesannetele, sest töö valmimise hetkel vastutab esimese taseme analüütik ka teise taseme analüütiku tööülesannete eest ja kaasatakse ka kolmanda taseme analüütiku tööprotsessidesse. Töö lahendused pakuti välja vastavalt praegu olemasolevatele The Hive funktsioonidele ja võimalustele. Tulevikus võiks ettevõte uurida intsidentide lahenduste automatiseerimist ja valepositiivsete sündmuste tuvastamise parendamist läbi automatsiooni. Siiski on käesolev töö ja selles välja pakutud lahendid hea koht alustamiseks ning kirjeldatud protsessid oleks võimalik implementeerida SOC töötsüklites juba täna.

Kasutatud kirjandus

Bedell, Crystal. Definitive Guide to SOAR. Annapolis, Ameerika Ühendriigid, CyberEdge Group, LLC, 2019.

Cassetto, Orion. "Security Operations Center Roles and Responsibilities." Exabeam, 2019, https://www.exabeam.com/security-operations-center/security-operations-center-roles-and-responsibilities/#:~:text=SOC%20manager%E2%80%94manages%20the%20security,%2C%20training%2C%20and%20assessing%20staff. 29.03.2021.

Chakrabarty, Boudhayan, et al. Securing Data on Threat Detection Using IBM Spectrum Scale and IBM QRadar: An Enhanced Cyber Resiliency Solution. Ameerika Ühendriigid, IBM Redbooks, 2020.

Cloudflare. "What Is Penetration Testing? What Is Pen Testing?" https://www.cloudflare.com/learning/security/glossary/what-is-penetration-testing/. 29.03.2021.

Exabeam. "The Modern Security Operations Center, SecOps and SIEM: How They Work Together." https://www.exabeam.com/siem-guide/the-soc-secops-and-siem/. 29.03.2021.

e-zu Solutions. "95% of Cyber Security Breaches are due to Human Error." e-zu, https://www.e-zu.co.uk/2020/06/16/95-of-cyber-security-breaches-are-due-to-human-error/. 21.04.2021.

Herrera, Michael. "Post Incident Analysis (PIA) – A Method to Analyze Your Actions During a BCP Event." MHA Consulting, 2010, https://www.mha-it.com/2010/08/02/post-incident-analysis-pia-a-method-to-analyze-your-actions-during-a-bcp-event/#:~:text=There%20are%20a%20number%20of,response%20areas%20under%20actual%20conditions. 21.04.2021.

The Hive. "The Hive." https://github.com/TheHive-Project/TheHive. 15.04.2021.

The Hive Project. “Cortex.” Github, https://github.com/TheHive-Project/Cortex. 06.05.2021.

The Hive Project. “Synapse.” Github, https://github.com/TheHive-Project/Synapse. 06.05.2021

Inforegister. “Security Software OÜ.” https://www.inforegister.ee/en/11924368-SECURITY-SOFTWARE-OU. 03.03.2021. 29.03.2021

Interpol. COVID-19 Cybercrime Analysis Report- August 2020. 2020.

Johansen, Gerald. Digital Forensics and Incident Response - Second Edition. Birmingham, Inglismaa, Packt Publishing, 2020.

Kirtley, Ellyn. “What is SIEM? What is SOAR? How are they different?” Swimlane, 2020, https://swimlane.com/blog/siem-soar/. 29.03.2021.

MISP project. “MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing.” MISP, https://www.misp-project.org/features.html. 06.05.2021

Mulder, Jeroen. Multi-Cloud Architecture and Governance. Brimingham, Packt Publishing, 2020.

Muniz, Joseph, and Aamir Lakhani. The Modern Security Operations Center. Addison-Wesley Professional, 2021.

Murdoch, Don. Blue Team Handbook: SOC, SIEM, and Threat Hunting Use Cases. Middletown, 2018.

N, Balaji. “Security Information and Event Management (SIEM) – A Detailed Explanation.” GBHackers on Security, 2021, https://gbhackers.com/security-information-and-event-management-siem-a-detailed-explanation/. 29.03.2021.

Roberts, Scott J., and Rebekah Brown. Intelligence Driven Incident Response. O'Reilly Media, 2017.

Security Software OÜ. “Services.” CYBERS, https://cybers.eu/services/. 03.03.2021.

Telia AS. “Uuring: Ligi 40% ettevõtetes ei tegele küberturbe teemaga otseselt keegi.” 2021, https://www.telia.ee/uudised/uuring-ligi-40-ettevotetes-ei-tegele-kuberturbe-teemaga-otseselt-keegi. 02.03.2021.

Walker, Aaron. “The Case for SOAR Solutions: The Future of Cybersecurity.” Research Hub, 2020, https://research.g2.com/insights/the-case-for-soar-solutions-future-of-cybersecurity. 04.03.2021.

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

Mina, Karoliine Karu

1. Annan Tallinna Tehnikaülikoolile tasuta loa (lihtlitsentsi) enda loodud teose "Avatud lähtekoodiga SOAR süsteemi The Hive kasutamine efektiivsema Küberkaitse Operatsioonide Keskuse teenuse (SOCaaS) implementeerimiseks ettevõtte CYBERS näitel" , mille juhendaja on Jürgen Erm ja kaasjuhendaja Dr. Gunnar Piho
   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.

18.05.2021

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.