Analiza efikasnosti sigurnosnih operativnih centara u detekciji i reakciji na kibernetičke prijetnje

Sviličić, Fran

Undergraduate thesis / Završni rad

2024

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Organization and Informatics / Sveučilište u Zagrebu, Fakultet organizacije i informatike**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:211:849480

Rights / Prava: Attribution 3.0 Unported/Imenovanje 3.0

Download date / Datum preuzimanja: **2024-11-28**

SVEUČILIŠTE U ZAGREBU
FAKULTET ORGANIZACIJE I INFORMATIKE
VARAŽDIN

Repository / Repozitorij:

Faculty of Organization and Informatics - Digital Repository

zir.nsk.hr

DIGITALNI AKADEMSKI ARHIVI I REPOZITORIJI

SVEUČILIŠTE U ZAGREBU
FAKULTET ORGANIZACIJE I INFORMATIKE
V A R A Ž D I N

Fran Sviličić

Analiza efikasnosti sigurnosnih operativnih centara u detekciji i reakciji na kibernetičke prijetnje

ZAVRŠNI RAD

Varaždin, 2024.

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Fran Sviličić

Matični broj: 0016147268

Studij: Informacijski sustavi

Analiza efikasnosti sigurnosnih operativnih centara u detekciji i reakciji na kibernetičke prijetnje

ZAVRŠNI RAD

Mentor/Mentorica:

Doc. dr. sc. Igor Tomičić

Varaždin, lipanj 2024.

Fran Sviličić

Izjava o izvornosti

Izjavljujem da je moj završni/diplomski rad izvorni rezultat mojeg rada te da se u izradi istoga nisam koristio drugim izvorima osim onima koji su u njemu navedeni. Za izradu rada su korištene etički prikladne i prihvatljive metode i tehnike rada.

Autor/Autorica potvrdio/potvrdila prihvaćanjem odredbi u sustavu FOI-radovi

Sažetak

Ovaj rad se bavi analizom efikasnosti sigurnosnih operativnih centara (SOC) u detekciji i odgovoru na kibernetičke prijetnje, s naglaskom na usporedbu različitih alata i tehnologija koji se koriste u industriji.

Rad pruža pregled trenutnih procesa unutar SOC-a, identificira njihove slabosti i predlaže moguća unapređenja s ciljem povećanja efikasnosti. Metodološki pristup obuhvatio je teorijsku analizu SOC sustava, studije slučaja stvarnih cyber napada te evaluaciju alata poput QRadar-a, Splunk-a, CrowdStrike Falcon-a i Vectra AI-a.

Kroz empirijsku analizu performansi SOC sustava, rad je pokazao značaj automatizacije i korištenja napredne analitike u smanjenju vremena reakcije i povećanju učinkovitosti u zaštiti organizacija. Zaključci ukazuju na potrebu kontinuiranog razvoja i prilagodbe sigurnosnih tehnologija kako bi SOC sustavi mogli pravovremeno i učinkovito odgovoriti na sve sofisticiranije prijetnje.

Ključne riječi: sigurnosni operativni centar; SOC; kibernetičke prijetnje; automatizacija; upravljanje prijetnjama; SOAR; detekcija prijetnji; analiza performansi

Sadržaj

1. Uvod

U suvremenom digitalnom okruženju, kibernetičke prijetnje postaju sve učestalije i sofisticiranije. Sigurnosni operativni centri (SOC) igraju ključnu ulogu u zaštiti organizacija od tih prijetnji, pružajući kontinuirani nadzor, detekciju i odgovor na incidente. Kako bi se organizacije učinkovito zaštitile, potrebno je razumjeti kako SOC djeluje i njegove prednosti i nedostatke. Iako je SOC samo jedan dio šireg spektra kibernetičke sigurnosti, on je vrlo bitan dio. Uspostava centraliziranog nadzora svih dijelova sustava olakšava i ubrzava reakciju na incidente i postupke oporavka. Zadaću nadzora i odgovora na incidente obavljamo uvođenjem sigurnosnog operativnog centra. [1]

Motivacija za odabir ove teme proizašla je iz rastuće prijetnje koju cyber napadi predstavljaju za organizacije svih veličina te mog osobnog interesa za područje kibernetičke sigurnosti. kroz rad istražiti ćemo različite vrste kibernetičkih prijetnji i njihovu važnost za suvremene organizacije. Zatim će se opisati uloga sigurnosnih operativnih centara, njihove osnovne komponente, procesi i arhitektura. Sljedeće obrađujemo konkretne primjere cyber napada, uključujući detekciju i propuste u detekciji tih napada te klasifikaciju alarma. Sljedeće prolazimo kroz pregled trenutnih metoda i tehnologija za detekciju prijetnji, uz razmatranje prednosti i ograničenja različitih pristupa. Fokusirat ćemo se na analizu suvremenih alata i tehnika koje se koriste u SOC-ovima. Na kraju opisat ćemo trenutne procese unutar SOC-a.

.

2. Metode i tehnike rada

Glavna istraživačka metoda ovog rada je kvalitativna analiza. Kvalitativna analiza nam omogućuje detaljno ispitivanje specifičnih aspekata sigurnosnih operativnih centara (SOC), njihovih procesa, alata i učinkovitosti u detekciji i reakciji na kibernetičke prijetnje.

Istraživačke aktivnosti uključivale su analizu stručne literature, studija slučaja, te upotrebu specifičnih programskih alata i aplikacija. Stručna literatura i istraživački radovi pružili su temeljno razumijevanje teorijskih aspekata SOC-a i kibernetičkih prijetnji, dok su studije slučaja omogućile praktičan uvid u stvarne incidente i odgovore SOC-ova na njih. Osim toga, stekao sam praktično iskustvo u cybersecurity sektoru tijekom stručne prakse, što je dodatno obogatilo moje razumijevanje sigurnosnih operativnih centara i njihovih procesa. Tijekom stručne prakse imao sam priliku vidjeti kako svaki alat funkcionira, pa sam ih uključio u završni rad.

Programski alati korišteni u ovom istraživanju uključuju:

1. QRadar: IBM-ov alat za sigurnosne informacije i upravljanje događajima (SIEM), korišten za analizu sigurnosnih podataka i identifikaciju prijetnji.
2. SOAR (Security Orchestration, Automation, and Response): Alat koji pomaže u automatizaciji odgovora na incidente i koordinaciji među različitim sigurnosnim alatima.
3. CrowdStrike: Napredna platforma za zaštitu krajnjih točaka koja koristi umjetnu inteligenciju za detekciju i odgovor na prijetnje.
4. Akamai: Rješenje za zaštitu web aplikacija i mrežnih resursa od napada, posebno DDoS napada.

Kombinacija ovih alata omogućava sveobuhvatnu analizu sigurnosnih događaja, brz i učinkovit odgovor na incidente, te stalno praćenje i zaštitu od novih prijetnji.

Ove metode i alati pružili su potrebne podatke i uvide za temeljitu analizu efikasnosti sigurnosnih operativnih centara u detekciji i reakciji na kibernetičke prijetnje.

3. Analiza cyber prijetnji

cyber prijetnje predstavljaju kontinuiranu opasnost za organizacije diljem svijeta, predstavljajući različite vrste napada i rizika za sigurnost informacija. U ovom poglavlju, istražit ćemo definiciju cyber prijetnji i njihove različite vrste, također opisat ćemo koje još prijetnje uključujemo u cyber prijetnje, kao i važnost sigurnosnih operativnih centara (SOC) u suvremenom poslovnom okruženju.

3.1. Cyber prijetnje

Cyber prijetnja ili prijetnja kibernetičke sigurnosti je potencijalna opasnost koja ima za cilj oštetiti podatke, ukrasti podatke ili poremetiti digitalni život općenito. Cyber prijetnje uključuju računalne viruse, povrede podataka, napade uskraćivanja usluge (DoS) i druge vektore napada. Također, cyber prijetnje odnose se na mogućnost uspješnog kibernetičkog napada koji ima za cilj neovlašteni pristup, oštećenje, poremećaj ili krađu informacijske tehnologije, računalne mreže, intelektualnog vlasništva ili bilo koje druge vrste osjetljivih podataka. Cyber prijetnje mogu dolaziti unutar organizacije od povjerenih korisnika ili iz udaljenih lokacija od nepoznatih strana. [2], [3]

Kibernetičke prijetnje dolaze od brojnih prijetnji, u njih uključujemo i [2], [3], [4]:

1. Neprijateljske državne aktere: Nacionalni kibernetički ratni programi predstavljaju rastuće kibernetičke prijetnje koje se kreću od propagande, narušavanja web stranica, špijunaže i ometanja ključne infrastrukture do gubitka života. Državno potpomognuti programi postaju sve sofisticiraniji i predstavljaju napredne prijetnje u usporedbi s drugim prijetnjama. Njihove razvijene sposobnosti mogle bi prouzročiti široka i dugoročna oštećenja nacionalnoj sigurnosti mnogih zemalja. Neprijateljske države predstavljaju najveći rizik zbog njihove sposobnosti učinkovite upotrebe tehnologije i alata protiv najtežih ciljeva poput klasificiranih mreža i kritične infrastrukture poput elektroenergetskih mreža i ventila za kontrolu plina.
2. Terorističke grupe: Terorističke grupe sve više koriste cyber napade kako bi oštetile nacionalne interese. Manje su razvijene u cyber napadima i imaju manju sklonost korištenju cyber sredstava od država. Vjerojatno je da će terorističke grupe predstavljati značajne kibernetičke prijetnje kako se u njihove redove pridružuje tehnički kompetentnije generacije što znači da potreba za kibernetičkom sigurnošću svakog dana sve više raste.

3. Korporativni špijuni i organizirane kriminalne organizacije: Korporativni špijuni i organizirane kriminalne organizacije predstavljaju rizik zbog svoje sposobnosti provođenja industrijske špijunaže radi krađe poslovnih tajni ili masovne krađe novca. Općenito, ove stranke zainteresirane su za profitne aktivnosti, bilo ostvarivanje profita ili ometanje sposobnosti poslovanja tako što napadaju ključnu infrastrukturu konkurenata, kradući poslovne tajne ili dobivajući pristup i materijale za ucjenu.
4. Haktivisti: Aktivnosti haktivista kreću se u okviru političkih ideala i pitanja. Većina haktivističkih grupa zabrinuta je zbog širenja propagande umjesto oštećivanja infrastrukture ili ometanja usluga. Njihov je cilj podržati svoj politički program umjesto prouzročiti maksimalnu štetu organizaciji.
5. Nezadovoljni insajderi: Nezadovoljni insajderi čest su izvor cyber kriminala. Insajderi često ne trebaju visok stupanj računalnog znanja za izlaganje osjetljivih podataka jer im može biti odobren pristup tim podacima. Prijetnje insajdera uključuju i dobavljače treće strane i zaposlenike koji mogu slučajno unijeti zlonamjerne programe u sustave, što dovodi do povrede podataka.
6. Hakeri: Zlonamjerni napadači mogu iskoristiti “zero day” ranjivost kako bi neovlašteno pristupili podacima. U prošlosti je to zahtijevalo visoku razinu vještine. Danas se napredni napadi mogu izvesti pomoću automatskih napadačkih skripti i protokola koje je moguće preuzeti s interneta, što čini sofisticirane napade jednostavnima.
7. Prirodne katastrofe: Prirodne katastrofe predstavljaju kibernetičku prijetnju jer mogu poremetiti ključnu infrastrukturu baš kao što bi to mogao cyber napad.
8. Slučajni postupci ovlaštenih korisnika: Neke od najvećih povreda podataka izazvane su lošom konfiguracijom umjesto hakerima.

3.2. Vrste cyber prijetnji

Ima mnogo vrsta cyber prijetnji tako da ću se držati najrelevantnijih i onih koji mogu najviše i najlakše oštetiti sustav [2], [3], [4], [5]:

1. Malware Napadi
    - Virusi – zlonamjerni kod koji se pričvršćuje na host aplikaciju. Glavna aplikacija mora se izvršiti da bi se pokrenula, a zlonamjerni kod izvršava se kada se izvrši glavna aplikacija.
    - Crvi (Worms) – zlonamjerni softver koji se sam umnožava i putuje kroz mrežu bez pomoći glavne aplikacije ili interakcije s korisnikom.
    - Trojanci – u početku trojanac se čini kao nešto korisno, ali uključuje zlonamjerne komponente, kao što je instaliranje backdoor-a na korisnikov sustav. Mnogi se trojanci isporučuju putem “drive-by” preuzimanja. Oni

također mogu zaraziti sustave iz lažnog antivirusnog softvera, piratskog softvera, igara ili zaraženih USB ključeva.
    - Ransomware – Posebna vrsta trojanaca. Napadači šifriraju korisničke podatke ili preuzimaju kontrolu nad računalom i kako bi zaključali korisnika. Zatim, zahtijevaju da korisnik plati otkupninu kako bi ponovno dobio pristup podacima ili Računalu.
    - Cryptojacking – Koristi resurse korisnikovog uređaja za rudarenje kriptovaluta bez njihovog znanja.
    - Spyware – Prikuplja podatke korisnika, poput lozinki i detalja o plaćanju.
    - Adware – Prati aktivnost pregledavanja radi prikazivanja ciljanih reklama.
    - Fileless malware – Ne instalira softver na sustav, već koristi postojeće datoteke za zlonamjerne funkcije.
    - Rootkiti – Rootkit je grupa programa koja skriva činjenicu da je sustav zaražen ili ugrožen zlonamjernim kodom.
    - Wyper attack - osmišljen je za trajno brisanje ili oštećenje podataka na ciljanim sustavima. Često se promatraju u geopolitičkim sukobima i u kontekstu haktivizma.
2. Social engineering napadi

   To je praksa korištenja društvenih taktika za dobivanje informacija. Često nije potrebna neka vrsta visoke tehnologije da bi se koristila ta metoda, potiče pojedince da rade nešto što inače ne bi učinili ili ih natjerati da otkriju neku informaciju, kao što su korisnički pristupni podaci. Često se korsite sljedeće tehnike:

    - Baiting – Mami korisnike da otkriju osjetljive informacije obećavajući nešto atraktivno.
    - Pretexting – Napadač se predstavlja kao autoritet kako bi iznudio informacije.
    - Phishing – slanje e-pošte sa svrhom da prijevarom navede korisnika da otkrije osobne podatke ili klikne na link.
    - Vishing (Voice phishing) – telefonskim pozivom navode korisnika kako bi im dao privatne i financijske podatke.
    - Smishing (SMS phishing) – Korištenje SMS poruka za prijevaru korisnika.
    - Tailgating – Neautorizirana osoba slijedi autoriziranog korisnika u zaštićeni prostor.
3. Napadi na Lanac Opskrbe
    - Kompromitiranje alata za izgradnju ili razvojnih kanala.
    - Kompromitiranje postupaka potpisivanja koda ili računa programera.

- Slanje zlonamjernog koda kao automatiziranih ažuriranja hardverskih ili firmverskih komponenti.
- Unaprijed instaliran zlonamjerni kod na fizičkim uređajima.

4. Man-in-the-Middle Napad (MitM)
    - Napad koji koristi aktivno presretanje ili prisluškivanje. Koristi treće računalo za dohvatačanje prometa koji se šalje između dva druga sustava
    - Wi-Fi prisluškivanje, Email otmica, DNS spoofing, IP spoofing, HTTPS spoofing.
5. Denial-of-Service (DoS) Napad
    - Preopterećuje ciljani sustav velikim volumenom prometa, ometajući njegovo normalno funkcioniranje.
    - Tehnike uključuju: HTTP flood DDoS, SYN flood DDoS, UDP flood DDoS, ICMP flood, NTP amplifikacija.
6. Napadi Injekcije
    - SQL injekcija – Umetanje SQL naredbi u korisnički unos.
    - Injekcija koda – Umetanje zlonamjernog koda u aplikaciju.
    - Data poisoning – vrsta napada u kojem protivnik namjerno kompromitira skup podataka za obuku koju koristi model umjetne inteligencije ili strojnog učenja kako bi manipulirao radom tog modela.
    - LDAP injekcija – Manipulacija LDAP upitima.
    - XML eXternal Entities (XXE) injekcija – Iskorištavanje ranjivosti XML parsiranja.
    - Cross-Site Scripting (XSS) – Umetanje zlonamjernog JavaScript koda.

4. Funkcije i značajke sigurnosnih operativnih centara

Sigurnosni operativni centar (SOC) predstavlja centralizirani tim unutar organizacije koji je odgovoran za praćenje, prevenciju, detekciju i reakciju na cyber prijetnje. SOC koristi napredne tehnologije i stručnjake kako bi osigurao sigurnost informacija i kontinuitet poslovanja. Ovo poglavlje će se fokusirati na važnost SOC-a u suvremenom poslovnom okruženju, detaljno će objasniti njegovu ulogu u detekciji, analizi i odgovoru na prijetnje, te će prikazati osnovne komponente i procese unutar SOC-a, kao i arhitekturu koja omogućava učinkovito funkcioniranje SOC-a.[1]

4.1. Važnost sigurnosnih operativnih centara (SOC) u suvremenom poslovnom okruženju

Sigurnosni operativni centar je važno imati zbog sve većih prijetnji kibernetičke sigurnosti.

4.1.1. Razlozi za uspostavu SOC-a

Kako bi organizacija postala sigurnija SOC omogućuje sljdeće ključne potrebe za svaku organizaciju [6], [7], [8]:

- Detekcija i prevencija prijetnji: Cyber prijetnje se kontinuirano razvijaju. Primarna uloga SOC-a je praćenje i detekcija prijetnji u stvarnom vremenu, što omogućuje organizacijama da brzo reagiraju i spriječe potencijalne proboje ili gubitak podataka.
- Odziv na incidente: U slučaju sigurnosnog incidenta, SOC može brzo reagirati kako bi ublažio štetu, ograničio prijetnju i smanjio utjecaj na organizaciju. To smanjuje vrijeme neaktivnosti i financijske gubitke.
- Sustav ranog upozoravanja: SOC djeluje kao sustav ranog upozoravanja koji može pomoći organizacijama da proaktivno riješe ranjivosti i prijetnje prije nego što eskaliraju u veće sigurnosne incidente.
- Usklađenost: Mnoge industrije imaju stroge regulatorne zahtjeve za zaštitu i sigurnost podataka. SOC pomaže organizacijama da ispune ove standarde usklađenosti putem praćenja i izvještavanja o sigurnosnim događajima.
- Zaštita podataka: Uloga SOC-a uključuje zaštitu osjetljivih podataka, što je ključno za održavanje povjerenja korisnika i izbjegavanje pravnih posljedica.
- Upravljanje ranjivostima: SOC se često bavi kontinuiranim procjenama ranjivosti i pomaže organizacijama da identificiraju i zakrpaju sigurnosne slabosti prije nego što ih napadači iskoriste.
- Detekcija prijetnji iznutra: SOC može pomoći u identificiranju i ublažavanju prijetnji iznutra, koje predstavljaju sigurnosne rizike od strane zaposlenika ili drugih osoba s unutarnjim pristupom sustavima organizacije.
- Forenzika i analiza: Kada se incidenti dogode, SOC provodi detaljnu analizu nakon incidenta kako bi razumio kako je došlo do proboja, njegov opseg i korištene taktike.
- Obavještavanje o prijetnjama: SOC timovi ostaju informirani o najnovijim prijetnjama i ranjivostima koristeći izvore obavještajnih podataka o prijetnjama, omogućujući im da proaktivno brane protiv novih rizika.
- Povećana sigurnosna svijest: Prisutnost SOC-a povećava svijest o sigurnosnim pitanjima unutar organizacije.

- Automatizacija i orkestracija sigurnosti: Mnogi SOC-ovi koriste alate za automatizaciju i orkestraciju kako bi optimizirali sigurnosne operacije.
- Isplativa sigurnost: Iako postavljanje i održavanje SOC-a može biti skupo, potencijalne uštede su značajne u usporedbi s financijskim gubicima i štetom za ugled koje mogu proizaći iz sigurnosnih incidenata.
- 24/7 nadzor: Cyber prijetnje mogu se dogoditi u bilo kojem trenutku. SOC pruža 24/7 nadzor, osiguravajući da se prijetnje otkriju i da se na njih reagira bez obzira na doba dana.
- Prilagođena sigurnost: SOC-ovi mogu prilagoditi svoje procese praćenja i odgovora na sigurnosne incidente specifičnim potrebama organizacije, uzimajući u obzir industriju i veličinu prijetnji
- Mir i sigurnost: Posjedovanje SOC-a pruža mir vodstvu organizacije, zaposlenicima i korisnicima, znajući da postoji posvećeni tim koji prati i brani od sigurnosnih prijetnji.

4.1.2. Prednosti koje SOC donosi poslovanju

Jedna od ključnih prednosti koje SOC donosi je zaštita imovine, pri čemu proaktivno praćenje i brza reakcija SOC-a pomažu u sprječavanju neovlaštenog pristupa i minimiziranju rizika od proboja podataka. To osigurava sigurnost kritičnih sustava, osjetljivih podataka i intelektualnog vlasništva od sigurnosnih povreda i krađe. SOC također doprinosi kontinuitetu poslovanja smanjujući sigurnosne incidente i njihov utjecaj, čime se osigurava nesmetano poslovanje, održava produktivnost, prihodi i zadovoljstvo korisnika. [8]

Uz to SOC pomaže organizacijama u ispunjavanju regulatornih zahtjeva i industrijskih standarda za kibernetičku sigurnost tako da implementira učinkovite sigurnosne mjere i održava detaljne zapise o incidentima i odgovorima. Ova proaktivna sigurnosna rješenja mogu rezultirati značajnim uštedama sprječavanjem skupih proboja podataka i cyber napada. Ulaganje u SOC često je znatno manje od financijskih gubitaka i ugrožavanja ugleda koje mogu prouzročiti sigurnosni incidenti. Ako se SOC usluge outsourceaju, organizacije mogu izbjeći troškove zapošljavanja i obuke internih sigurnosnih stručnjaka. [7], [8]

Demonstriranje predanosti kibernetičkoj sigurnosti kroz rad SOC-a povećava povjerenje i sigurnost među korisnicima i dionicima. Brza reakcija SOC-a smanjuje vrijeme zastoja i financijske gubitke brzim suzbijanjem prijetnji i brzom obnovom normalnih operacija kako bi se minimizirale smetnje. Analizom sigurnosnih događaja i trendova, SOC timovi mogu identificirati potencijalne ranjivosti organizacije i poduzeti proaktivne mjere za njihovo ublažavanje prije nego što ih napadači iskoriste. Kontinuiranim praćenjem mreža i sustava,

SOC-ovi mogu brže identificirati i ublažiti sigurnosne prijetnje, čime se minimizira potencijalna šteta i proboji podataka te organizacijama omogućava da budu korak ispred u sve složenijem pejzažu prijetnji. [8]

4.2. Uloga SOC-a u detekciji, analizi i reakciji na cyber prijetnje

Sigurnosni operativni centar (SOC) ima ključnu ulogu u osiguravanju IT infrastrukture organizacije kroz tri glavne kategorije aktivnosti: priprema, planiranje i prevencija; nadzor, detekcija i reakcija; te oporavak, poboljšanje i usklađenost. SOC je odgovoran za kontinuirano praćenje, detekciju prijetnji i brzu reakciju na sigurnosne incidente, omogućujući organizacijama da zaštite svoje kritične sustave i podatke.[8]

4.2.1. Procesi detekcije prijetnji

SOC neprekidno nadzire cijelu IT infrastrukturu organizacije, uključujući aplikacije, servere, mreže i uređaje, kako bi prepoznao znakove poznatih napada i sumnjivih aktivnosti. Glavne tehnologije za nadzor i detekciju u SOC-u su sustavi za upravljanje sigurnosnim informacijama i događajima (SIEM) te proširena detekcija i odgovor (XDR). SIEM prikuplja i analizira podatke u stvarnom vremenu, dok XDR pruža detaljniju telemetriju i automatizaciju. Upravljanje logovima, odnosno prikupljanje i analiza log podataka generiranih svakim mrežnim događajem. XDR je ključan za prepoznavanje anomalija koje mogu ukazivati na sigurnosne prijetnje. SOC tim također razvrstava stvarne prijetnje od lažnih alarma, koristeći umjetnu inteligenciju za automatizaciju procesa i poboljšanje točnosti detekcije.[9]

4.2.2. Analiza prijetnji i procjena rizika

SOC tim redovito provodi procjene ranjivosti kako bi identificirao potencijalne ili nove prijetnje i procijenio njihove troškove. Osim toga, SOC provodi penetracijske testove, odnosno simulacije napada na sustave, kako bi testirao sigurnosne mjere i identificirao slabosti koje je potrebno ispraviti. SOC također stalno prati najnovija sigurnosna rješenja i tehnologije te prikuplja najnovije informacije o prijetnjama, kako bi uvijek bio korak ispred potencijalnih napadača. U slučaju incidenta, SOC provodi forenzičku analizu kako bi detaljno istražio kako je došlo do proboja, procijenio njegov opseg i identificirao taktike korištene u napadu.

4.2.3. Odgovor na incident i oporavak sustava

U slučaju prijetnje ili incidenta, SOC brzo reagira kako bi ograničio štetu. To uključuje istraživanje uzroka, isključivanje ugroženih uređaja, izolaciju kompromitiranih područja mreže, zaustavljanje kompromitiranih aplikacija, brisanje zaraženih datoteka i pokretanje antivirusnih programa. Nakon što je prijetnja eliminirana, SOC vraća pogođene resurse u stanje prije incidenta, što može uključivati ponovno povezivanje diskova i uređaja, obnavljanje mrežnog prometa i ponovni rad aplikacija. SOC koristi nova saznanja iz incidenta za unapređenje sigurnosnih mjera, ažuriranje procesa i politika te izbor novih alata. Također osigurava da su svi sustavi u skladu s propisima o zaštiti podataka te obavještava nadležne institucije prema zakonskim zahtjevima. SOC ima ključnu ulogu u zaštiti organizacije od cyber prijetnji, pružajući stalno praćenje, brzu reakciju i stalno poboljšanje sigurnosnih mjera, čime osigurava kontinuitet poslovanja i usklađenost s propisima.

4.3. Pregled osnovnih komponenti i procesa unutar SOC-a

Ključne komponente sigurnosnog operativnog centra obuhvaćaju ljude, procese i tehnologiju. Ljudi su temelj SOC-a, obuhvaćajući stručnjake za sigurnost, analitičare, forenzičare i druge članove tima koji su ključni za nadzor, analizu i reakciju na cyber prijetnje. Procesi SOC-a uključuju razvoj incidentnih planova, analizu sigurnosnih događaja i reakciju na incidente, što osigurava organizirani pristup u slučaju prijetnji. Tehnologija, kao središnja komponenta SOC-a, pruža alate za brzo identificiranje i reagiranje na cyber prijetnje ti alati su sustavi za upravljanje sigurnosnim informacijama i događajima (SIEM), te sustavi za proširenu detekciju i odgovor (XDR).

4.3.1 Članovi SOC tima i njihove uloge

Kao i u svakoj drugoj organizacijskoj jedinici, unutar SOC-a (Sigurnosnog Operativnog Centra) postoji nekoliko različitih uloga i odgovornosti. Ovisno o opsegu i veličini organizacije, potrebni su različiti timovi u različitim brojevima. Tipične osnovne uloge u SOC-u su različite razine analitičara te posvećeni menadžeri. Razlikujemo tri uloge s odgovarajućim odgovornostima [7], [8], [9], [10], [11], [12], [13]:

- Tier 1 (Triage Specialist): Analitičari Tier 1 su uglavnom odgovorni za prikupljanje sirovih podataka, te pregledavanje alarma i upozorenja. Njihov zadatak je potvrditi, odrediti ili prilagoditi kritičnost upozorenja. Za svako upozorenje, specijalist za trijažu mora utvrditi je li opravdano ili lažno pozitivno. Dodatna odgovornost na ovoj razini je identifikacija drugih visokorizičnih događaja i potencijalnih incidenata. Ako se

problemi ne mogu riješiti na ovoj razini, prosljeđuju se analitičarima Tier 2. Također, specijalisti za trijažu često upravljaju i konfiguriraju alate za praćenje.

- Tier 2 (Incident Responder): Na razini Tier 2, analitičari pregledavaju kritičnije sigurnosne incidente koje su eskalirali specijalisti za trijažu i rade detaljniju procjenu koristeći obavještajne podatke o prijetnjama. Oni moraju razumjeti opseg napada i biti svjesni pogođenih sustava. Sirovi podaci o napadu prikupljeni na razini Tier 1 pretvaraju se u korisne obavještajne podatke na ovoj razini. Incident responderi odgovorni su za osmišljavanje i implementaciju strategija za ograničavanje i oporavak od incidenta. Ako analitičar Tier 2 naiđe na veće probleme u identifikaciji ili ublažavanju napada, konzultiraju se dodatni analitičari Tier 2 ili se incident eskalira na Tier 3.
- Tier 3 (Threat Hunter): Analitičari Tier 3 su najiskusniji unutar SOC-a. Oni rješavaju velike incidente koje su im proslijedili incident responderi. Također provode ili barem nadziru procjene ranjivosti i penetracijske testove kako bi identificirali moguće napadne vektore. Njihova najvažnija odgovornost je proaktivno identificiranje mogućih prijetnji, sigurnosnih rupa i ranjivosti koje mogu biti nepoznate. Kako stječu razumne informacije o mogućoj prijetnji sustavima, također trebaju preporučiti načine za optimizaciju implementiranih alata za sigurnosno praćenje.
- SOC Manager: SOC menadžeri nadziru tim za sigurnosne operacije. Oni pružaju tehničke smjernice po potrebi, ali najvažnije, odgovorni su za adekvatno upravljanje timom. To uključuje zapošljavanje, obuku i procjenu članova tima, stvaranje procesa, procjenu izvješća o incidentima te razvoj i implementaciju potrebnih planova krizne komunikacije. Također nadziru financijske aspekte SOC-a, podržavaju sigurnosne revizije i izvještavaju glavnog službenika za informacijske sigurnosti (CISO) ili odgovarajuću poziciju na najvišoj razini upravljanja.

Svaka od ovih osnovnih uloga zahtijeva specifičan skup vještina. Te osnovne uloge nalaze se u SOC-ovima neovisno o njihovoj veličini. Međutim, u manjem SOC-u odgovornosti svake uloge su šire, dok se u većem SOC-u uloge mogu specijalizirati. Na primjer, u malom SOC-u s nekoliko analitičara, svi trebaju biti upoznati s više vještina jer nekoliko zaposlenika mora pokriti sve zadatke koji se pojavljuju. U većem SOC-u, uloge mogu biti specifičnije jer se neki analitičari mogu fokusirati na praćenje mreže dok su drugi stručnjaci za specifičnosti Windowsa ili Linuxa. To donosi mnoge prednosti, poput bržeg odgovora na prijetnje ili bolje raspodjele zadataka.[7], [8], [9], [10], [11], [12], [13]

Pored četiri već opisane osnovne uloge, postoje i dodatne uloge koje su barem donekle uključene u svakodnevni rad SOC-a. Te dodatne uloge trebaju voditi, surađivati ili raditi

zajedno s prethodno opisanim osnovnim ulogama, koje su također uključene u sliku. Međutim, može postojati značajno preklapanje između uloga i dodatnih uloga koje mogu biti uključene u vođenje određenog SOC-a. Zbog toga sam grupirao uloge u pet glavnih skupina [7], [8], [9], [10], [11], [12], [13]:

- Upravljačke uloge: U kontekstu SOC-a identificiramo tri ključne upravljačke uloge. Prvo, glavni službenik za informacijsku sigurnost definira strategije, ciljeve i ciljeve ukupnih sigurnosnih operacija organizacije. SOC menadžer vodi sam SOC. Unutar SOC-a, postoji još jedna upravljačka uloga na visokoj razini, a to je koordinator odgovora na incidente, koji koordinira sve aktivnosti povezane s odgovorom na incidente.
- Tehničke uloge: Postoji širok raspon dodatnih sigurnosnih stručnjaka koji trebaju surađivati s analitičarima SOC-a kako bi omogućili učinkovite i efikasne SOC operacije. Analitičari zlonamjernog softvera pomažu u odgovoru na sofisticirane prijetnje obavljajući reverzno inženjerstvo zlonamjernog softvera i stvarajući ključne rezultate za aktivnosti odgovora na incidente. Da bi bili svjesni mogućih napada, lovci na prijetnje aktivno traže prijetnje unutar organizacije, primjerice pregledavanjem logova ili izvan organizacije analizirajući dostupne TI podatke. Ove TI podatke također eksplicitno analiziraju analitičari ili istraživači obavještajnih podataka o prijetnjama. Ako su dijelovi napada uspjeli, forenzički stručnjaci provode detaljne istrage o njima. Oni prikupljaju i analiziraju forenzičke dokaze. Crveni timovi i plavi timovi aktivno pokušavaju napasti ili obrambeno djelovati na sustave organizacije kako bi identificirali ranjivosti te testirali i povećali učinkovitost i otpornost sigurnosnih mehanizama, dalje stručnjaci za procjenu ranjivosti provode istraživanja kako bi identificirali nove, prethodno nepoznate ranjivosti i upravljaju poznatim ranjivostima s obzirom na poslovni rizik. Ti stručnjaci izrađuju detaljna tehnička izvješća sa svojim nalazima i podržavaju analitičare SOC-a ili timove za odgovor na incidente u određenim otkrićima ranjivosti. Još jedna vitalna uloga ove skupine je sigurnosni inženjer (SE). SE razvija, integrira i održava SOC alate. Sigurnosni inženjeri također definiraju zahtjeve za nove alate. Oni osiguravaju odgovarajući pristup alatima i sustavima. Dodatni zadaci su konfiguracija i instalacija vatrozida i sustava za otkrivanje/prevenciju upada. Također, pomažu u pisanju i ažuriranju pravila za otkrivanje za SIEM sustave.
- Savjetodavne uloge: Dvije najvažnije uloge ove skupine su sigurnosni arhitekt (SA) i sigurnosni savjetnik. SA planira, istražuje i dizajnira sigurnosnu infrastrukturu unutar tvrtke. SA provodi redovite sustavne testove i testove ranjivosti, te implementira ili nadzire implementaciju poboljšanja. Također su zaduženi za uspostavljanje

postupaka oporavka. Sigurnosni savjetnici često istražuju sigurnosne standarde. Oni mogu pružiti pregled industrije za organizaciju i usporediti trenutne sposobnosti SOC-a s konkurentima. Mogu pomoći u planiranju, istraživanju i dizajniranju sigurnosnih arhitektura.

- Vanjsko osoblje: Vanjsko osoblje može biti uključeno u bilo koju SOC operaciju, te se stoga, ovisno o arhitekturi i modelu rada SOC-a, više ili manje vanjskog osoblja uključuje u različite SOC uloge i skupine.

4.3.2 Procesi unutar SOC-a

U operacijama SOC-a odvijaju se različiti, vrlo specifični procesi. Budući da je cilj SOC-a odgovoriti na incidente ili se pripremiti za njih, jedan način strukturiranja osnovnih procesa je kroz životni ciklus odgovora na incidente (Incident Response Lifecycle) ili slične okvire. Životni ciklus odgovora na incidente obuhvaća četiri koraka: "priprema", "detekcija i analiza", "ograničavanje, uklanjanje i oporavak" i "aktivnosti nakon incidenta".[9], [13], [14], [15]

1. Priprema

Procesni koraci unutar pripreme su normalizacija s vremenskom sinkronizacijom, filtriranje, redukcija, agregacija i prioritizacija ili procjena rizika. Redoslijed procesnih koraka nije jedinstven, jer može varirati ovisno o korištenoj aplikaciji., [14]

- Normalizacija: Važno je prevesti heterogene formate podataka u jedinstvenu reprezentaciju za daljnju obradu. Također je bitno promijeniti sve vremenske podatke u jednu standardnu vremensku zonu i format. Sinkronizacija pomaže izbjeći zabunu u vremenskoj liniji sigurnosnih događaja i smanjuje vjerojatnost donošenja pogrešnih zaključaka o nedosljedno mjerenoj mrežnoj aktivnosti. , [15], [16]
- Filtriranje: Budući da sustavi obično generiraju ogromne količine podataka, bitno je filtrirati podatke koji su vjerojatno važni s aspekta sigurnosti. , [15], [16]
- Redukcija: Redukcija je slična filtriranju, s razlikom da se pojedinačni, nevažni podaci sortiraju kako bi se smanjila količina podataka., [15], [16]
- Agregacija: Slični događaji se kombiniraju u jedan jedini podatkovni element. Na primjer, tri zapisa logova koji ukazuju na pokušaj prijave na host mogu se agregirati u jedan jedini log koji navodi vrstu i broj pokušaja prijave. , [15], [16]

- Prioritizacija: Svaki podatak u logu treba klasificirati prema važnosti kako bi se olakšala daljnja obrada. Na primjer, da bi se odlučilo kako reagirati na događaje ili koliko dugo treba čuvati logove, korisno je prioritizirati dolazne podatke. , [15], [16]

Specifično za SOC-ove, postoje samo dva značajna rada. Analitičari žele šire, manje ručno prikupljanje podataka, ali samo s pravim alatima za razumijevanje i rad s podacima, to čemo obraditi u posebnom poglavlju. Predložena je arhitektura zapisivanja za SOC-ove koja sadrži generatore logova, poslužitelj za prikupljanje, poslužitelj za pohranu i bazu podataka logova. Ključne funkcionalnosti uključuju normalizaciju, filtriranje, redukciju, rotaciju, vremensku sinkronizaciju, agregaciju i provjeru integriteta. , [15], [16]

2. Detekcija i Analiza

Ogromna količina podataka prikupljena u prethodnim koracima može biti preplavljujuća. Pretvaranje tih podataka u korisne informacije vrši se kroz analizu podataka i suštinski je način da se razumije što je prikupljeno. Identificirani procesni koraci uključuju Detekciju, Analizu i Prioritizaciju upozorenja/trijažu. [13], [17], [18] :

- Detekcija: Incidenti se detektiraju uz pomoć ljudi ili automatskim procedurama. Potrebno je odlučiti pokazuje li prikupljeni podaci na sigurnosni incident.
- Analiza: Tehnike korištene za analizu uključuju korelaciju izvora i ciljeva, strukturnu analizu, funkcionalnu analizu i analizu ponašanja. Svrha korelacije je omogućiti analizu složenih sekvenci proizvodnjom jednostavnih, sintetiziranih i točnih događaja.
- Prioritizacija upozorenja/Trijaža: Prioritizacija upozorenja, također poznata kao trijaža, može se smatrati vezom prema ograničavanju, uklanjanju i oporavku. Njena dva primarna cilja su osigurati da se najteži incidenti tretiraju s prioritetom i da se incidenti distribuiraju za daljnju obradu prema dostupnim resursima.

3. Ograničavanje, Uklanjanje i Oporavak

Cilj ovog koraka je odlučiti je li incident bezopasan događaj (npr. tijekom penetracijskog testiranja) ili štetan događaj. U slučaju štetnog incidenta, prosljeđuje se odgovarajućim dionicima za daljnje korake. Sigurnosna orkestracija, automatizacija i odgovor (SOAR) su od velike važnosti i mogu se identificirati kao vrlo aktivno istraživačko područje. Ključna svrha SOAR-a je automatizacija procesa kroz orkestraciju. SOAR integrira dostupne informacije o sigurnosnim incidentima kako bi automatski poduzeo odgovarajuće mjere za što brže ograničavanje štete.[9], [13], [19], [20]

Jednostavan okvir za rješavanje incidenata je OODA petlja (Observe, Orient, Decide, Act), dobro poznat analitički okvir za donošenje odluka koji se može primijeniti na upravljanje incidentima u kontekstu SOC-a. Proces upravljanja upozorenjima i incidentima uključuje korake identificirane dvama primarnim standardima za upravljanje informacijskom sigurnosnim incidentima.[9], [13], [19], [20], [21]

4.4. Arhitektura SOC-a

4.4.1 Opća arhitektura

SOC-ovi mogu biti strukturirani kao centralizirani, distribuirani ili decentralizirani entiteti na visokoj i apstraktnoj razini. U slučaju SOC-ova, centralizirana arhitektura opisuje pristup gdje se svi podaci šalju s različitih lokacija ili podružnica u jedan centralni SOC za daljnju obradu.[13], [22], [23]:

- Centralizirani SOC: Centralizirana arhitektura SOC-a podrazumijeva slanje svih podataka s različitih lokacija u jedan centralni SOC radi daljnje obrade. Prednosti ovog pristupa uključuju bolju koordinaciju i centralizirano upravljanje, ali postoji rizik od točke kvara (single point of failure).
- Distribuirani SOC: Distribuirani SOC, s druge strane, je jedan jedinstveni sustav koji djeluje kroz nekoliko podružnica. Korisnicima se čini kao da rade s jednim entitetom. Distribuirani sustav omogućuje svim entitetima dohvaćanje, obradu, kombiniranje i pružanje sigurnosnih informacija i usluga drugim entitetima . Omogućuje ravnomjerno raspoređivanje opterećenja i podataka.
- Decentralizirani SOC: Treći opći arhitektonski dizajn za SOC-ove je decentralizirani sustav, kombinacija dvaju sustava dizajniranih gore. Decentralizirani SOC sastoji se od nekoliko SOC-ova s mogućim ograničenim sposobnostima koji izvještavaju jednom ili više centralnih SOC-ova. Pomak od jednog centralnog SOC-a prema decentraliziranoj arhitekturi primijećen je pri usporedbi ranijih istraživanja s novijim publikacijama. Glavni razlog za to čini izbjegavanje jedne točke kvara.

4.4.2 Tehnološka arhitektura

SOC je organizacijska jedinica koja obuhvaća različite funkcionalnosti i ne samo jedan sustav. Jedan od prvih modela arhitekture za SOC-ove je SOCBox. SOCBox definira SOC kao sastavljen od pet glavnih modula: generatora događaja, sakupljača događaja, baza podataka poruka, analizačkih motora i softvera za upravljanje reakcijama.[13], [24]

Iako je SOCBox arhitektura još uvijek bitna u pogledu svojih glavnih komponenti, ima određena ograničenja jer je predložena prije gotovo 15 godina, a tehnologija je značajno napredovala. SOCBox se prvenstveno fokusira na prikupljanje podataka i upravljanje incidentima, ali ne uključuje digitalnu forenziku i reaktivne sposobnosti za sprječavanje napada. Predložena arhitektura opisuje centralizirani sustav s brojnim točkama kvara. Zbog složenosti modernih IT okruženja i tehnološkog razvoja, distribuirane arhitekture često se smatraju prikladnijima. Stoga je SOCBox arhitektura prošla kroz nekoliko iteracija i poboljšana tijekom godina. Njegov izravni nasljednik je distribuirani SOC (DSOC). [9], [13], [22]

DSOC arhitektura postavlja temelje za distribuiranu Grid SOC (GSOC) arhitekturu za kritičnu infrastrukturu, koju su ponovno razvili istraživački timovi koji su započeli rad na originalnom SOCBoxu. Ove tri arhitekture ističu pomak od centraliziranog prema distribuiranom SOC postavu tijekom vremena. SOC arhitektura sastoji se od sloja generacije, sloja akvizicije, sloja manipulacije podacima i izlaznog ili prezentacijskog sloja. [13], [25]

SOC čine slični arhitektonski blokovi: blok koji sažima izvore podataka, zatim blok dizajniran za prikupljanje podataka iz izvora i predaju trećem bloku odgovornom za analizu podataka. Posljednji blok opisuje prezentaciju rezultata analize podataka. Nijedan od ovih blokova ne pretpostavlja je li analiza izvedena ručno ili automatski.[13]

Također postoje i dodatni prijedlozi SOC arhitektura koji se fokusiraju na SOC-ove za specifične upotrebe. Settani et al. opisuje implementaciju SOC arhitekture za pružatelje kritične infrastrukture. Tafazzoli i Grakani predlažu arhitekturu za obradu događaja u OpenStack okruženju za detekciju napada u oblaku na vrlo površnoj razini. Postoji širok raspon drugih, vrlo specifičnih domena prilagođenih SOC arhitektura.[13], [26]

4.4.3 Modeli SOC-a

Postoji pet različitih operativnih modela SOC-a prema Gartneru koji su prikazani u sljedećoj tablici. Gartnerova klasifikacija ističe razlike u zadacima SOC-a u vezi s radnim vremenom i specifično angažiranim osobljem.

Predložak	Opis	Detalji
Virtualni SOC	Organizacijski model	Interni distribuiran SOC
	Veličina	Otprilike 1,000 korisnika/IP adresa
	Vidljivost	Ograničena na "post mortem" pregled sistemskih zapisa
	Zadaća	Bez mandata za reaktivnu i pro aktivnu postupke u slučaju incidenta
	Primjer	SOC malih entiteta
	Bilješka	U okruženjima koja ne zahtijevaju stalan nadzor
Mali SOC	Organizacijski model	Interno centraliziran SOC
	Veličina	Do 10,000 korisnika/IP adresa
	Vidljivost	Ograničena do dobra, provedena automatizacija zaštite za neke od ključnih točaka i uređaja
	Zadaća	Zajednički mandat, obično sa IT operacijama, pro aktivnog i reaktivnog odgovora na prijetnje. SOC sudjeluje u donošenju odluka o akcijama.
	Primjer	SOC srednje velikih tvrtki, sveučilišta ili vladinih tijela
	Bilješka	Ovdje su resursi IT operacijske sigurnosti konsolidirani unutar jedne organizacijske jedinice. Budžet ovakvog SOC-a je limitiran veličinom entiteta kojeg štiti. Ukoliko je ovakav SOC dio veće organizacije može odgovarati Tiered SOC-u ili Nacionalnom SOC-u.
Veliki SOC	Organizacijski model	Interno centraliziran SOC sa elementima distribuiranog SOC-a
	Veličina	Otprilike 50,000 korisnika/IP adresa
	Vidljivost	Sveobuhvatna vidljivost, automatizacija provedena kod većine uređaja i za veći dio entiteta koje nadzire
	Zadaća	Reaktivna uloga u potpunosti pripada SOC-u, proaktivnu ulogu dijeli obično sa IT operacijama osim u slučaju taktičkog odgovora na incident. SOC preporučuje preventivne kontrole.
	Primjer	SOC-ovi koji opslužuju najveće kompanije (Fortune 500, Global 2000) i velike vladine agencije
	Bilješka	Ovakav SOC je dovoljno velik da pruža napredne servise sa jedne centralizirane lokacije i dovoljno kompaktan da provodi direktan nadzor i odgovor na incidente. U heterogenim okruženjima različitih geografskih lokacija ovakav SOC se može naslanjati na lokalno osoblje za dio funkcije nadzora i odgovora.
Višerazinski SOC	Organizacijski model	Kombinacija interno distribuiranog, centraliziranog i koordinirajućeg SOC-a
	Veličina	Otprilike 50,000 korisnika/IP adresa
	Vidljivost	Vidljivost unutar koordinirajućeg SOC-a je različita jer podaci poslani sa krajnjih točaka moraju prvo proći kroz podređeni SOC.
	Zadaća	U potpunosti reaktivna i zajednička pro aktivna; koordinirajući SOC može pokrenuti taktički odgovor koji može uticati na podređene SOC-ove. SOC preporučuje preventivne kontrole.
	Primjer	Ovakav SOC obično služi konglomerate tvrtki ili veću grupu velikih vladinih tijela.
	Bilješka	Glavni koordinirajući SOC direktno nadzire svoju imovinu i lokacije i prima podatke iz podređenih SOC-ova. Podređeni SOC-ovi sinkroniziraju svoje operativne postupke sa glavnim SOC-om.
Nacionalni SOC	Organizacijski model	Koordinirajući SOC
	Veličina	Otprilike 50,000.000 korisnika/IP adresa
	Vidljivost	Vidljivost je ograničena ali prisutna u svim entitetima koje nadzire; ograničeni pristup neobrađenim podacima; u potpunosti se oslanja na prijave o incidentima podređenih SOC-ova.
	Zadaća	Bez reaktivne i bez pro aktivne uloge, praktično samo sa savjetodavnom ulogom
	Primjer	SOC u službi vlade ili države
	Bilješka	Omogućuje cjelokupni nadzor vladama i državama

Tablica 1 Pet predložaka veličine SOC-a[1]

Svaki model SOC-a ima specifične karakteristike koje odgovaraju različitim potrebama organizacija. Gartnerova klasifikacija pruža temelj za razumijevanje različitih razina i sposobnosti SOC-a, što omogućuje organizacijama da odaberu odgovarajući model prema svojim potrebama i resursima. U kontekstu ACME SOC-a, ovi modeli će pomoći u definiranju optimalne strategije za sigurnosne operacije.

Sljedeća tablica 2 prikazuje kako različiti modeli SOC-a odgovaraju specifičnim potrebama i veličinama organizacija. Od virtualnih SOC-a za male tvrtke, preko više funkcijskih i distribucijskih modela za srednje tvrtke, do namjenskih i upravljačkih SOC-ova za velike korporacije i vladine agencije. Ovom kategorizacijom omogućujemo da organizacije lakše odaberu odgovarajući model SOC-a koji će im pružiti optimalnu sigurnost i zaštitu prema njihovim specifičnim potrebama i resursima.

Operativni modeli SOC-a	Svojstva	Primjena
Virtualni SOC	• Bez namjenskih prostorija • Bez stalno raspoloživih namjenskih ljudskih resursa • Reaktivna uloga, aktivira se kod sumnje na incident • Početni model do trenutka korištenja iznajmljenog SOC servisa	Male tvrtke i mala okruženja
Vise funkcijski SOC/ NOC	• Namjenske prostorije, stalno raspoloživi ljudski resursi koji uz sigurnosne zadaće, u cilju smanjenja troškova, obavljaju još druge različite kritične operacije iz domene nadzora mrežne i računalne infrastrukture u cilju smanjenja troškova	Male i srednje tvrtke ili velike tvrtke malog rizika unutar kojih već postoji zrela IT i mrežna podrška koja rješava i sigurnosne i operativne zadatke
Distribucijski/Co- managed SOC	• Namjensko ili djelomično namjensko osoblje • Uglavnom pokriva 5 radnih dana po 8 sati • Koristi usluge vanjske tvrtke (*engl. MSSP Managed security service provider*)	Velike i srednje tvrtke
Namjenski SOC	• Namjenske prostorije i oprema • Namjenski tim uposlenika • Isključivo vođen unutar tvrtke • Operativan 24 sata kroz 7 dana u tjednu	Velike tvrtke, pružatelji važnih usluga, organizacije sa velikim rizikom
Upravljački SOC	• Upravlja podređenim SOC-ovima • Pruža uslugu dojave o sigurnosnim prijetnjama, situacijsku svijest i dodatne kompetencije za rješavanje sigurnosnih incidenata	Vrlo velike tvrtke i davatelji usluga, vlade, vojska i obavještajne organizacije

Tablica 2 Operativni modeli SOC-a[1]

5. Primjeri cyber napada

U ovom dijelu završnog rada fokusirat ćemo se na konkretne primjere cyber napada, istražit čemo kako su ti napadi izvedeni, tehnike koje su korištene i kako su detektirani ili u nekim slučajevima, propušteni. Cilj je razumjeti različite oblike cyber prijetnji, od njihovih osnovnih karakteristika do složenih strategija napadača. Pokušat ćemo istaknuti važnost proaktivnog pristupa sigurnosti informacija te identificirati ključne korake u sprječavanju i detekciji cyber napada.

5.1. Primjeri cyber napada

1. Napad na Colonial Pipeline [9], [27]

Colonial Pipeline, ključni naftovod u Sjedinjenim Američkim Državama, postao je meta najvećeg javno objavljenog cyber napada na kritičnu infrastrukturu u zemlji u svibnju 2021. Napad je izvela grupa poznata kao DarkSide, koristeći ransomware koji je inficirao digitalne sustave naftovoda, što je uzrokovalo njegovo zatvaranje na nekoliko dana. Ovaj događaj

označen je kao nacionalna sigurnosna prijetnja, budući da naftovod prenosi gorivo od rafinerija do industrijskih tržišta.

Napad je uključivao krađu podataka, nakon čega su napadači inficirali mrežu Colonial Pipelinea ransomwareom, to je uzrokovalo poteškoće u funkcioniranju sustava naplate i računovodstva. U cilju sprječavanja daljnjeg širenja ransomwarea, naftovod je privremeno zatvoren, a tvrtka je morala platiti otkupninu od 75 bitcoina (4,4 milijuna dolara) kako bi povratila kontrolu nad svojim sustavima.

Root uzrok ovog napada je u izloženoj lozinki za VPN račun, koja je omogućila napadačima ulazak u mrežu Colonial Pipelinea. Mnoge organizacije koriste VPN za siguran pristup svojim mrežama, no u ovom slučaju, zaposlenik tvrtke vjerojatno je koristio istu lozinku za VPN na drugom mjestu, što je dovelo do kompromitiranja lozinke. Ova pojava ponovne upotrebe lozinki postala je uobičajen problem. Nakon incidenta, provedene su brze reakcije kako bi se otklonile posljedice napada i spriječili slični incidenti u budućnosti. Vlada SAD-a izdala je izvršnu naredbu koja je usmjerena na jačanje sigurnosnih praksi, uključujući upotrebu računa računarskih programa (SBOMs) kako bi se otkrile i uklonile sigurnosne ranjivosti u softverskim komponentama.

2. Napad na log4j [28]

Ranjivost Log4j, poznata i kao Log4Shell, otkrivena je u studenom 2021. u Apache Log4j biblioteci za zapisivanje logova. Ova ranjivost omogućava hakerima potpunu kontrolu nad uređajima koji koriste nepatchane verzije Log4j. Zlonamjerni akteri mogu koristiti ranjivost Log4Shell kako bi pokrenuli gotovo bilo koji kod na osjetljivim sustavima.

Istraživači smatraju Log4Shell "katastrofalnom" sigurnosnom ranjivošću jer je toliko raširena. Log4j je jedan od najrasprostranjenijih programa otvorenog koda na svijetu i jednostavna je za upotrebu. Log4Shell je potaknuo porast cyber napada u prosincu 2021. IBM-ov X-Force Threat Intelligence Index bilježi 34% porast iskorištavanja ranjivosti između 2020. i 2021., uglavnom povezan s Log4Shellom.

Ranjivost Log4Shell je zakrpana brzo nakon otkrića, ali će predstavljati rizik godinama jer je Log4j duboko ukorijenjen u softverskom lancu opskrbe. Američko Ministarstvo domovinske sigurnosti procjenjuje da treba najmanje desetljeće da se otkriju i poprave sve ranjive instance.

Log4j je biblioteka otvorenog koda koji programeri mogu slobodno koristiti. Umjesto da pišu vlastite zapisnike, programeri mogu ugraditi biblioteku Log4j u svoje aplikacije. Ta praktičnost

je razlog zašto je Log4j tako rasprostranjen, ugrađen u proizvode velikih organizacija poput Microsofta i Amazona. Log4Shell proizlazi iz načina na koji starije verzije Log4j 2 rukuju Java Naming and Directory Interface (JNDI) pretragama. JNDI je programski interface aplikacija (API) koji Java aplikacije koriste za pristup resursima na vanjskim serverima. Pretraga JNDI je naredba koja govori aplikaciji da ode na server i preuzme određeni objekt, poput podataka ili skripte. Starije verzije Log4j 2 automatski pokreću bilo koji kod preuzet na ovaj način.

Korisnici mogu poslati JNDI pretrage ranjivim verzijama Log4j uključujući ih u log poruke. Na primjer, u starijim verzijama Minecraft Java Editiona, koje koriste Log4j za zapisivanje korisničkih poruka, korisnik može upisati JNDI pretragu u javni chat prozor.

Hakeri mogu koristiti ovu JNDI funkcionalnost kako bi daljinski pokrenuli zlonamjeran kod. Prvo, haker postavlja server koji koristi uobičajeni protokol, poput Lightweight Directory Access Protocol (LDAP), kako bi izbjegao privlačenje pažnje. Zatim pohranjuju zlonamjerni payload na tom serveru, poput zlonamjerne datoteke. Konačno, šalju JNDI pretragu programu, govoreći mu da ode na hakerov LDAP server, preuzme payload i pokrene kod. Log4Shell je bio nulta-dan ranjivost, što znači da patching nije bio dostupan kada je otkrivena.

3. Lapsus$ napadi [29]

23. veljače 2022. počele su kružiti glasine da je proizvođač računalnog hardvera NVIDIA pretrpio provalu podataka. Nekoliko dana kasnije, 26. veljače, LAPSUS$ se javio i preuzeo odgovornost za napad, a zatim procurio 20 GB podataka tvrtke, uključujući intelektualno vlasništvo (IP) i preko 70.000 hashiranih vjerodovnica zaposlenika.

Dan nakon objavljivanja izjave FBI-a, LAPSUS$ je procurio podatke o korisnicima tvrtke Okta, velikog pružatelja usluga upravljanja identitetom i pristupom. Međutim, nakon objave podataka i tvrđenja o provali, ispostavilo se da LAPSUS$ nije direktno provalio u Oktu, već je uspješno provalio u Oktinog partnera. Od tamo, LAPSUS$ je pokušao, ali nije uspio kompromitirati Oktu. Provalom u Oktinog partnera, LAPSUS$ je dobio pristup maloj količini podataka o Okta klijentima, što je podržalo njihovo tvrđenje o provali tvrtke. Okta je potom morala poduzeti značajne korake kako bi umirila klijente i investitore. Tokom istog tjedna,, LAPSUS$ je počeo objavljivati snimke izvornog koda koji su dokazali da su dobili pristup Microsoftu i to su učinili dok su još bili unutar mreže. U roku od nekoliko sati, Microsoft je objavio blog o LAPSUS$. Microsoft je potvrdio provalu, naznačujući da su izjave LAPSUS$ omogućile njihovom timu za sigurnost da intervenira i zaustavi izvlačenje podataka dok se to događalo. Microsoft blog je otkrio i veliki dio načina na koji LAPSUS$ djeluje. U suštini, LAPSUS$ je bio izložen kao grupa za kiberkriminal koja je koristila opsežne tehnike.

Metode koje su koristili su:

Društveni inženjering: Istraživanje ciljeva, prilagođavanje napada i korištenje različitih metoda poput phishinga i spear phishinga.

Potkupljivanje zaposlenika: Nudili su novac zaposlenicima u zamjenu za pristupne podatke ili pomoć u napadima.

Zamjena SIM kartica: Preusmjeravanje SMS kodova za MFA na napadačeve telefone.

Kompromitirane vjerodovnice: Korištenje ukradenih osobnih ili poslovnih računa za dobivanje pristupa drugim sustavima.

Umor MFA: bombardiranje žrtava MFA zahtjevima za odobrenje pristupa tako da ih iscrpe i dovedu do toga da odobre nelegitimne zahtjeve.

Društveni inženjering je i dalje rizik s kojim se tvrtke i zaposlenici moraju suočiti. Potrebno je da budu svjesni opasnosti phishinga, spear phishinga i drugih tehnika društvenog inženjeringa. Treba obratiti pažnju na lanac dobavljača i osigurati da partneri imaju snažne sigurnosne mjere, te da im se ne dodjeljujte više pristupa informacijama nego što je potrebno. Treba koristiti sigurnije MFA metode poput autentifikatora aplikacija ili hardverskih tokena jer nisu sve MFA metode jednake. To su neke od ključnih koje su tvrtke naučile da treba obratiti pažnju zbog ovog napada.

4. HTTP/2 “Rapid reset” napad[30]

U listopadu 2023. godine, Cloudflare je pomogao u otkrivanju zero-day ranjivosti u HTTP/2 protokolu koja omogućava velike količine DDoS napada na HTTP resurse poput web poslužitelja i web aplikacija. U roku od nekoliko tjedana nakon otkrića, napadači su iskoristili ovu ranjivost za pokretanje stotina napada rekordnih razmjera. Ovaj događaj predstavlja značajan pomak u otkrivanju novih prijetnji i zahtijeva brzu prilagodbu sigurnosnih praksi.

Tijekom 2010-ih, mnogi najveći DDoS napadi iskorištavali su 3. i 4. slojeve OSI modela. Poznati primjeri takvih napada su napadi na SpamHaus (2013), Dyn (2016) i Wikimedia (2019). Organizacije su se s vremenom prilagodile ovim napadima, povečano je korištenje cloud-a i ulaganje u specijaliziranu tehnologiju za ublažavanje najvećih mrežnih DDoS napada.

Kako se povijest ponavlja, napadači su promijenili svoje taktike. U novije vrijeme, zabilježeni su brojni DDoS napadi koji iskorištavaju 7. sloj OSI modela, što ukazuje na novi trend. Ovi napadi su vrlo velikog volumenai, fokusirani na volumen prometa i koriste složenije taktike, uključujući zero-day ranjivosti.

Ranjivost HTTP/2 ili "Rapid Reset", iskorištava funkciju otkazivanja streamova u HTTP/2 protokolu. Napadači generiraju velike količine zlonamjernih zahtjeva za otkazivanjem streamova koji zaobilaze uobičajene ograničenja brzine poslužitelja. U kolovozu 2023., Cloudflare je promatrao napadače koji koriste ovu metodu za snažne napade, od kojih su neki premašili prethodne rekorde po broju zlonamjernih zahtjeva po sekundi.

Ono što ovu ranjivost čini posebno zabrinjavajućom je infrastruktura napadača. Rekordni napad koristio je botnet od 20,000 računala, što je relativno skromno u usporedbi s modernim botnetima koji se sastoje od stotina tisuća pa čak i milijuna računala. HTTP/2 protokol koristi se za oko 62% internetskog prometa, što znači da su mnoge web aplikacije i poslužitelji neposredno ranjivi.

Za zaštitu od ovih napada, trebalo bi prioritizirati nekoliko ključnih koraka:

- Premjestiti mitigaciju sloja 7 DDoS napada izvan podatkovnih centara.
- Razmotriti sekundarni cloud-based Layer 7 DDoS provajder za otpornost.
- Osigurati primjenu relevantnih patchova za web poslužitelje i operacijske sustave. Također, osigurati da su svi automatizirani alati potpuno patchani kako starije verzije ne bi slučajno bile puštene u proizvodnju.

5.2. Detalji o detekciji ili propustima detekcije u slučajevima napada

5.2.1 Specifični primjeri detekcije

1. IDS/IPS sustavi [5], [9], [31]

Intrusion Detection Systems (IDS) i Intrusion Prevention Systems (IPS) su ključni alati za otkrivanje i prevenciju cyber napada. Ovi sustavi analiziraju mrežni promet i prepoznaju zlonamjerne aktivnosti pomoću unaprijed definiranih pravila. IDS i IPS su izvorno razvijeni kako bi odgovorili na nedostatke koji su prisutni u većini vatrozida. IDS sustavi se koriste za otkrivanje prijetnji ili upada u mrežni segment, dok je IPS usmjeren na identifikaciju tih prijetnji ili upada kako bi ih blokirao ili zaustavio njihove aktivnosti. IDS i IPS dijele niz sličnih

funkcija kao što su inspekcija paketa, analiza stanja, ponovno sastavljanje TCP segmenata, dubinska inspekcija paketa, validacija protokola i uspoređivanje potpisa.

Najbolji primjer sigurnosnog mehanizma u smislu razlike između IDS-a i IPS-a može se usporediti s patrolnim automobilom i sigurnosnim stražarom. IDS djeluje kao patrolni automobil unutar granice koji nadzire aktivnosti i traži situacije koje nisu u skladu s definiranim pravilima. S druge strane, IPS djeluje kao sigurnosni stražar na ulazu koji dopušta i odbija pristup na temelju vjerodajnica i unaprijed definiranog skupa pravila ili politika. Bez obzira na to koliko je sigurnost na ulazu jaka, patrole nastavljaju djelovati u sustavu koji osigurava vlastite provjere.

IDS može biti softver ili uređaj koji detektira prijetnje, neovlašteni ili zlonamjerni mrežni promet. IDS ima unaprijed definirane skupove pravila pomoću kojih može pregledati konfiguraciju krajnjih točaka kako bi utvrdio jesu li one podložne napadu (poznato kao IDS temeljen na domaćinu), te može bilježiti aktivnosti unutar mreže i uspoređivati ih s poznatim napadima ili uzorcima napada (poznato kao mrežno-baziran IDS). Svrha otkrivanja upada je pružiti nadzor, reviziju, forenziku i izvještavanje o zlonamjernim mrežnim aktivnostima.

IPS ne samo da otkriva zlonamjerne pakete uzrokovane zlonamjernim kodovima, botnetima, virusima i ciljanih napada, već može poduzeti i mjere kako bi spriječio te mrežne aktivnosti od nanošenja štete mreži. Glavni motiv napadača je dobivanje osjetljivih podataka ili intelektualnog vlasništva, uključujući podatke o zaposlenicima, financijske zapise i druge podatke o korisnicima. IPS je specifično dizajniran za zaštitu imovine, resursa, podataka i mreža.

Napad putem malwarea koji se širi mrežom može biti otkriven pomoću IDS-a koji prepoznaje neobične uzorke u mrežnom prometu. Jedan konkretan primjer je otkrivanje WannaCry ransomware napada. IDS sustavi su prepoznali neobične pokušaje komunikacije i blokirali ih prije nego što je malware mogao nanijeti veću štetu.[32]

2. SIEM sustavi [5], [9], [33]

Security Information and Event Management (SIEM) sustavi predstavljaju ključni alat za modernu informatičku sigurnost, omogućuju organizacijama prikupljanje, analizu i korelaciju sigurnosnih podataka iz različitih izvora. SIEM sustavi integriraju podatke iz mrežnih uređaja, servera, aplikacija, sigurnosnih alata, i drugih izvora unutar organizacije. Prikupljeni podaci se normaliziraju kako bi se osigurala konzistentnost i omogućila usporedba iz različitih izvora, dok napredni algoritmi korelacije događaja prepoznaju obrasce koji ukazuju na potencijalne prijetnje.

Na primjer, niz neuspješnih prijava na sustav, praćen uspješnom prijavom, može ukazivati na brute force napad. Analiza i izvještavanje unutar SIEM sustava omogućuju identifikaciju sigurnosnih incidenata, dok integrirani sustavi za odgovor na incidente omogućuju automatiziranu reakciju, poput blokiranja sumnjivih IP adresa ili izolacije zaraženih uređaja. SIEM sustavi pružaju centraliziranu vidljivost nad sigurnosnim događajima u cijeloj organizaciji time omogućujui timovima za sigurnost da bolje razumiju stanje sigurnosti u realnom vremenu.

Jedan od najpoznatijih primjera korištenja SIEM sustava je napad na Target 2013. godine, gdje su hakeri iskoristili zlonamjerni softver za prikupljanje podataka o kreditnim karticama. SIEM sustav je detektirao neobične aktivnosti kroz korelaciju različitih događaja, poput višestrukih neuspješnih pokušaja prijave s različitih IP adresa, uspješne prijave iz istog raspona IP adresa nakon niza neuspjelih pokušaja, i neobično visoke aktivnosti skeniranja mreže. Kombinacija ovih naizgled nepovezanih događaja omogućila je SIEM sustavu da podigne alarm za mogući brute force napad, što je omogućilo sigurnosnim timovima da brzo reagiraju i spriječe daljnju štetu.

SIEM sustavi također pomažu organizacijama da se usklade s različitim propisima i standardima sigurnosti, mogu pružiti detaljne izvještaje i audit trailove. Prikupljeni podaci i izvještaji omogućuju detaljnu forenzičku analizu nakon sigurnosnih incidenata. SIEM sustavi su stoga ključni alat u modernom pristupu informatičkoj sigurnosti.

3. Prikupljanje i analiza logova [9]

Prikupljanje i analiza logova su ključni elementi učinkovite informatičke sigurnosti, jer omogućuju praćenje i razumijevanje aktivnosti unutar IT infrastrukture. Zahvaljujući logovima, organizacije mogu otkriti sigurnosne prijetnje. Logovi sadrže detaljne informacije o aktivnostima koje se odvijaju na sustavima i uređajima u mreži, što omogućuje SOC analitičarima da prepoznaju sumnjive aktivnosti koje mogu ukazivati na napad ili kompromitaciju. Također logovi mogu pomoći u pronalaženju i rješavanju problema s IT sustavima. Na primjer, analiza logova može otkriti poteškoće s performansama, greške u konfiguraciji ili probleme s konektivnošću. Mnoge industrije zahtijevaju da organizacije prikupljaju i čuvaju log datoteke kako bi se dokazalo usklađivanje s propisima o sigurnosti podataka.

Neke od najčešćih vrsta logova su:

1. Logovi aplikacija:

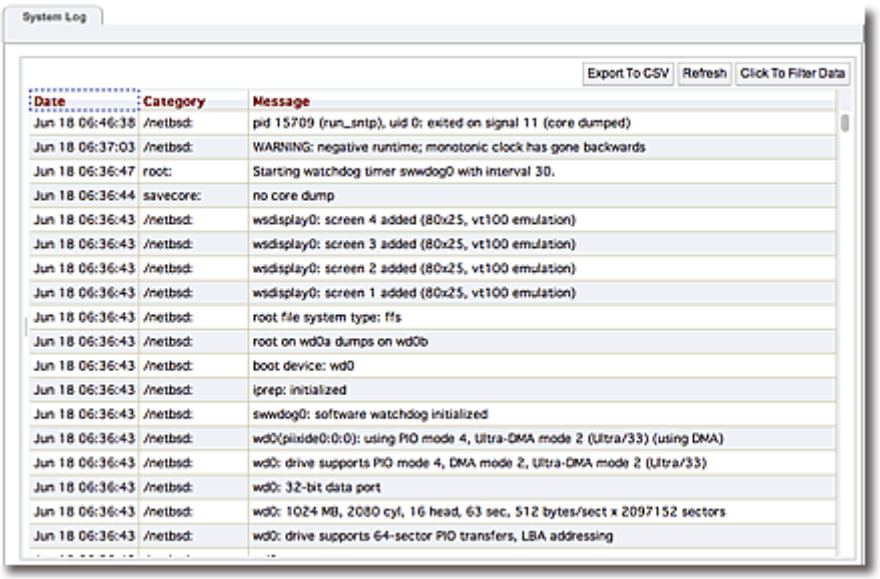
Ove dnevnike generiraju same aplikacije i sadrže detaljne informacije o svim radnjama koje se unutar njih događaju. To uključuje prijave korisnika, zahtjeve za resursima, promjene konfiguracije i eventualne greške. Analiza logova aplikacija pomaže u otkrivanju sumnjive aktivnosti, dijagnosticiranju problema s performansama i praćenju korištenja aplikacija.


```
{"timestamp":"2020-04-12T23:26:32.013Z","level":"INFO","message":"Ap
plication started","meta":{"tag":"MyExampleApp"}}
{"timestamp":"2020-04-12T23:26:32.013Z","level":"DEBUG","message":"L
oading fonts...","meta":{"tag":"MyExampleApp"}}
{"timestamp":"2020-04-12T23:26:32.013Z","level":"DEBUG","message":"L
oading user details...","meta":{"tag":"MyExampleApp"}}
{"timestamp":"2020-04-12T23:26:32.014Z","level":"INFO","message":"Us
er found:","payload":{"username":"testuser","firstname":"John","last
name":"Smith"},"meta":{"tag":"MyExampleApp"}}
{"timestamp":"2020-04-12T23:26:32.014Z","level":"DEBUG","message":"P
reparing environment...","meta":{"tag":"MyExampleApp"}}
{"timestamp":"2020-04-12T23:26:32.014Z","level":"INFO","message":"We
lcome Screen","meta":{"tag":"MyExampleApp"}}
{"timestamp":"2020-04-12T23:26:32.014Z","level":"INFO","message":"Ap
plication closed","meta":{"tag":"MyExampleApp"}}
```


Slika 1: Primjer logova aplikacije[34]

2. Logovi sustava:

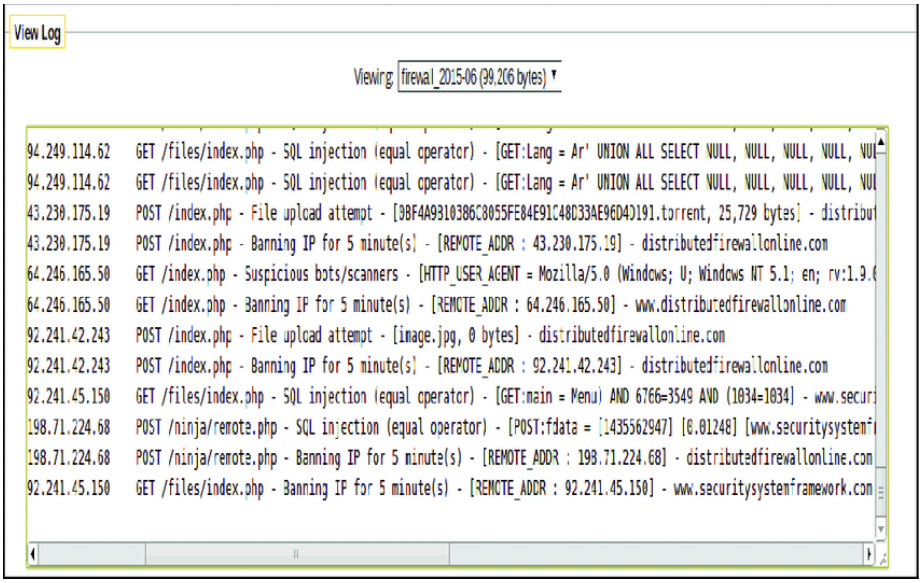
Operativni sustavi generiraju ove log datoteke. Oni bilježe događaje poput pokretanja i zaustavljanja procesa, korištenja CPU-a i RAM-a, te eventualne pogreške i upozorenja. Analiza logova sustava pomaže u otkrivanju neovlaštenih pristupa, loše konfiguracije i problema s stabilnošću sustava.



Slika 2: Primjer logova sustava[35]

3. Logovi sigurnosnih uređaja:

Sigurnosni uređaji, kao što su firewalli, IDS/IPS sustavi i antivirusi, generiraju ove logove koji bilježe sve relevantne sigurnosne događaje. To uključuje pokušaje prijave, blokiran promet, zlonamjerne aktivnosti, detektirane viruse i druge potencijalne prijetnje. Analiza logova sigurnosnih uređaja pomaže u otkrivanju napada, prati trendove sigurnosti i poboljšava opću sigurnosnu pozu.



Slika 3: Primjer firewall logova[36]

4. Logovi mreže:

Mrežni uređaji, poput usmjerivača i prekidača, koriste ove log datoteke koje sadrže detalje o mrežnom prometu. To uključuje IP adrese, portove, protokole, veličinu paketa i smjer prometa. Analiza logova mreže pomaže u otkrivanju neovlaštenog pristupa, anomalija u prometu i potencijalnih napada na mrežu.

Efektiivna analiza sigurnosti počinje prikupljanjem logova iz raznovrsnih IT komponenata poput mrežnih uređaja, servera, aplikacija i sigurnosnih uređaja. Međutim, prije analize, ovi logovi koji stižu u različitim formatima moraju se pretvoriti u jedinstveni, standardizirani format. To omogućava usporedbu i korelaciju podataka iz različitih izvora. Centralizirano spremanje ovih normaliziranih logova, obično u sustavu za upravljanje logovima (log management system) ili SIEM (Security Information and Event Management) rješenju, omogućava temeljitu analizu. Sam proces analize podrazumijeva pretraživanje i povezivanje podataka kako bi se identificirali obrasci i anomalije koji mogu ukazivati na sigurnosne prijetnje. Automatizirani alati mogu olakšati ovaj proces, a nakon detekcije sumnjivih

aktivnosti, sistemi automatski generiraju izvješća i alarme za sigurnosne timove kako bi se na vrijeme reagiralo na potencijalne incidente.

5.2.2 Analiza propusta

Ovdje razmatramo najčešće uzroke neuspjeha u detekciji i nudimo konkretne primjere kako bi se ilustrirali učinci tih propusta. Fokusirat ćemo se na tri glavna uzroka: nedostatak ažuriranja, ljudske greške i nedostatak vidljivosti.

1. Nedostatak ažuriranja

Jedan od najčešćih razloga za neuspjeh sustava detekcije je nedostatak redovitih ažuriranja. Sustavi koji nisu redovito ažurirani postaju ranjivi na nove prijetnje koje nisu prepoznate starijim verzijama softvera. Ažuriranja su ključna za implementaciju najnovijih sigurnosnih patcheva i otkrivanje novih oblika napada.

Dobar primjer bio bi napad na Equifax 2017. godine rezultirao je kompromitacijom osobnih podataka milijuna korisnika. Uzrok napada bio je neuspjeh u primjeni zakrpe za poznatu ranjivost u Apache Struts okviru, koja je bila dostupna nekoliko mjeseci prije napada. Neprimjenjivanje zakrpe omogućilo je napadačima da iskoriste ovu ranjivost i pristupe osjetljivim podacima.[37]

2. Ljudske greške

Ljudske greške, poput nepravilnog konfiguriranja sustava ili ignoriranja sigurnosnih upozorenja, također mogu dovesti do propusta u detekciji prijetnji. Unatoč sofisticiranim alatima i tehnologijama, ljudski faktor ostaje ključna komponenta u sigurnosnom ekosustavu. Greške koje proizlaze iz neadekvatne obuke, nepažnje ili pogrešne procjene mogu imati ozbiljne posljedice.

U slučaju Target napada, sigurnosni tim je zanemario više upozorenja sustava koji su mogli spriječiti napad. Prekomjeran broj lažnih pozitivnih alarma također je doprinjeo ignoriranju stvarnih prijetnji, što je omogućilo napadačima da neometano djeluju unutar mreže.

3. Nedostatak vidljivosti

Nedovoljna vidljivost mrežnog prometa i aktivnosti unutar organizacije može spriječiti učinkovitu detekciju napada. Bez sveobuhvatnog pregleda i praćenja, sigurnosni timovi možda neće biti svjesni prijetnji koje se odvijaju unutar njihovih sustava.

Napad na Marriott International, gdje su napadači ostali neotkriveni gotovo četiri godine, pokazuje koliko je bitna sveobuhvatna vidljivost i monitoring mrežnih aktivnosti. Napadači su se infiltrirali u sustav i neometano prikupljali podatke zbog nedostatka vidljivosti i odgovarajućih sigurnosnih alata. U ovom primjeru očito je da su potrebni napredni alati za praćenje i analizu mrežnog prometa kako bi se pravovremeno identificirale i spriječile sumnjive aktivnosti.[38]

6. Metode detekcije kibernetičkih prijetnji

Detekcija kibernetičkih prijetnji postaje sve složenija i zahtijeva korištenje raznih naprednih tehnologija i metoda, moramo biti spremni prepoznati prijetnje što je prije moguće kako bi se spriječila šteta i osigurala sigurnost organizacija. U ovoj temi, fokusirat ćemo se na pregled trenutnih metoda i tehnologija za detekciju prijetnji, kao i na njihove prednosti i ograničenja.

6.1. Behavioral Analysis Systems (BAS)

Sustavi za analizu ponašanja temeljeni na umjetnoj inteligenciji postaju sve potrebniji. Korištenjem umjetne inteligencije za učenje i predviđanje obrazaca neprijateljskog ponašanja, ovi sustavi nadopunjuju tradicionalne metode detekcije proaktivnom, stvarnom vremenskom detekcijom anomalija i potencijalnih prijetnji, čime pomažu smanjiti rizik od sigurnosnih proboja i jačaju cjelokupnu sigurnosnu poziciju organizacije.[9], [39], [40]

Analiza ponašanja u kibernetičkoj sigurnosti uključuje promatranje aktivnosti unutar sustava kako bi se razlikovalo normalno ponašanje od ponašanja koje nije tipično, te identificirale potencijalne prijetnje. Tradicionalne metode kibernetičke sigurnosti oslanjaju se na sustave za detekciju temeljenima na potpisima ili već propisanim pravilima. Iako ove metode mogu učinkovito identificirati poznate prijetnje, teško prepoznaju nove, prethodno neviđene kibernetičke napade, poput zero-day ranjivosti. Napadači neprestano razvijaju svoje taktike kako bi izbjegli detekciju. To je dodatno kompliciranо jer napadači koriste napade bez

malvera ili ukradene korisničke podatke za imitaciju legitimnih korisnika. Osim toga, ogromna količina podataka koju generiraju suvremeni mrežni sustavi može preplaviti tradicionalne sigurnosne tehnologije.[9], [39], [40]

CrowdStrike je bio među prvim tvrtkama koje su učinkovito izvodile analizu ponašanja i uveli indikatore napada (Indicators of Attack - IOAs) primjenom napredne analitike i inteligencije generirane od strane stručnjaka za obradu trilijuna podataka koje redovito prikuplja CrowdStrike Falcon platforma zasnovana na oblaku. IOAs su proaktivni, generalizirani indikatori neprijateljskog ponašanja koji se razlikuju od češćih reaktivnih indikatora poznatih kao indikatori kompromitacije (Indicators of Compromise - IOCs). Promatranjem sekvenci ponašanja u odnosu na napadačke obrasce i motivacije, IOAs omogućuju organizacijama identificiranje suptilnih znakova neprijateljskog ponašanja u okruženju.[9], [39], [40], [9], [39], [40]

Nedavno je CrowdStrike ubrzao svoju sposobnost klasificiranja novih IOAs uz pomoć AI-temeljenih indikatora napada. Kombiniranjem brzine i snage AI-ja zasnovanog na oblaku s visokokvalitetnim podacima CrowdStrikea, CrowdStrike je ubrzao i proširio svoju sposobnost izdavanja novih IOAs, omogućujući organizacijama zaštitu koja se brzo prilagođava sve evoluirajućem krajobrazu prijetnji.[9], [39], [40]

6.1.1. Prednosti

1. Detekcija prijetnji u stvarnom vremenu i brže vrijeme odziva
2. Dodatni sloj obrane tijekom izvođenja
3. Sposobnost obrade velikih količina podataka i skaliranja
4. Poboljšanje prediktivnih sposobnosti: Iz prošlih ponašanja i trendova, AI može predvidjeti potencijalne buduće prijetnje
5. Smanjenje lažnih pozitivnih rezultata: Kroz stalnu obuku, sustavi strojno učenja poboljšavaju svoju sposobnost razlikovanja sumnjivih aktivnosti od bezopasnih odstupanja od norme što smanjuje vrijeme i resurse utrošene na istraživanje lažnih alarma.

6.1.2. Ograničenja

1. Teška ovisnost o podacima za obuku: Performanse AI sustava izravno ovise o kvaliteti i volumenu podataka na kojima se izvodi obuka. Nedovoljni ili pristrani podaci mogu dovesti do loše detekcije prijetnji i viših stopa lažnih pozitivnih i negativnih rezultata.

2. Rizik od lažnih negativnih rezultata i pretjerane oslanjanje na AI: Unatoč naprednim sposobnostima, AI sustavi povremeno mogu propustiti prijetnje (lažni negativni), osobito sofisticirane. Pretjerano oslanjanje na AI bez ljudskog nadzora može potencijalno omogućiti da neke prijetnje ostanu neotkrivene.
3. Mogućnost da napadači ciljaju ili manipuliraju AI sustavima: Kako AI sustavi postaju ključni za obranu kibernetičke sigurnosti, i sami mogu postati meta napadača. Sofisticirani napadači mogli bi pokušati manipulirati procesom obuke AI-ja ili iskoristiti ranjivosti u sustavu.

6.2. Next generation firewalls (NGFW)

Napredni vatrozid (NGFW) je izumljen oko 2009. godine od strane Gartnera. Sličan je UTM-u (Unified Threat Management) u ranim danima, ali se od tada razvio u inovativniji i sofisticiraniji proizvod. NGFW ima sve značajke tradicionalnih vatrozida, poput filtriranja paketa, prevođenja mrežnih i port adresa (NAT), stateful inspekcije i virtualne privatne mreže (VPN). Također ima napredne značajke kao što su sustav za prevenciju upada (IPS), dubinska inspekcija paketa i identifikacija korisnika.[41], [42]

NGFW može identificirati i kontrolirati promet na razini aplikacija gledajući duboko u aplikacijski sloj, odnosno u sadržaj paketa. Dok se tradicionalni vatrozidi fokusiraju na mrežne protokole i zaglavlja paketa, NGFW koristi inteligenciju aplikacija za identificiranje aplikacija bez obzira na port i protokol, prepoznajući korisnika i povezujući identitet korisnika s paketom te prepoznajući stvarnu namjeru sadržaja paketa.[41], [42]

Koncept NGFW-a je postići sve što tradicionalni vatrozidi rade, ali s proširenim sposobnostima koje kombiniraju nove tehnologije identifikacije, visoke performanse i dodatne inovativne značajke.[41], [42]

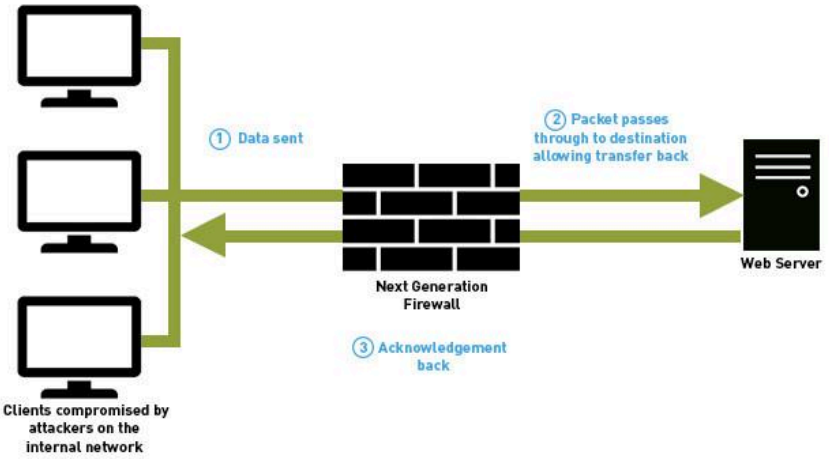
6.2.1. Prednosti

1. Integracija s drugim sigurnosnim alatima
2. Dubinska inspekcija paketa:
3. Prepoznavanje složenih napada: NGFW koristi napredne metode za prepoznavanje i blokiranje sofisticiranih prijetnji, uključujući one koje koriste tehnike zaobilaženja tradicionalnih vatrozida.

6.2.2. Ograničenja

1. Visoki troškovi implementacije i održavanja

2. Složenost konfiguracije



Slika 4: Next generation firewall pojednostavljena shema[43]

6.3. Zero trust security

Zero Trust pristup sigurnosti temelji se na pretpostavci da niti jedan korisnik ili uređaj nije pouzdan prema zadanim postavkama, čak i ako se nalazi unutar mreže organizacije. Ovaj model zahtijeva stalnu provjeru identiteta, autorizaciju i kontinuiranu validaciju sigurnosne konfiguracije i stanja prije nego što se omogući pristup aplikacijama i podacima. Zero Trust model polazi od ideje da ne postoji tradicionalna mrežna granica, mreže mogu biti lokalne, u oblaku ili hibridne, s resursima bilo gdje i radnicima na bilo kojoj lokaciji. [44]

Koristi se mikrosegmentacija mreže što zanči da se mreža “razbije” na manje, izolirane segmente kako bi se smanjio domet napadača u slučaju proboja. Time dobivamo precizniju kontrolu pristupa i minimiziranje rizika od unutarnjih i vanjskih prijetnji.[44]

Vrlo je stroga kontrola pristupa, samo ovlašteni korisnici i uređaji mogu pristupiti određenim resursima. Politike pristupa temelje se na riziku, pridržavanju pravila i specifičnim zahtjevima za pristup, a pristup se kontinuirano prati i revidira.[44]

Tradicionalni pristupi mrežnoj sigurnosti slijedili su metodu "vjeruj, ali provjeri", koja je automatski povjeravala korisnicima i uređajima unutar mrežne granice. Ovaj model je

zastario s premještajem u cloud i distribucijom radnog okruženja, posebno nakon pandemije 2020. godine.[44]

6.3.1. Prednosti

1. Poboljšana sigurnost: Zero Trust model pruža sveobuhvatniju zaštitu mreže, smanjuje rizik od unutarnjih i vanjskih prijetnji. Kontinuirano praćenje i stroga kontrola pristupa omogućuju pravovremeno otkrivanje i reakciju na sumnjive aktivnosti.
2. Veća fleksibilnost: Model omogućuje sigurnu migraciju u oblak i podržava rad na daljinu, ovime korisnici i uređaji mogu biti sigurni bez obzira na njihovu lokaciju.
3. Smanjenje rizika od napada: Zero trust model omogućuje segmentaciju mreže i minimalne privilegije, čime se ograničava domet napadača i mogućnost lateralnog kretanja unutar mreže.

6.3.2. Ograničenja

1. Složena implementacija: Implementacija zero trust modela zahtijeva sveobuhvatno razumijevanje mreža i može zahtijevati značajne promjene u postojećoj sigurnosnoj infrastrukturi, što može biti složeno i skupo.
2. Potencijal za frustraciju korisnika: Rigorozne kontrole pristupa mogu dovesti do frustracije korisnika, posebno ako ometaju učinkovitost obavljanja zadataka.
3. Povećano opterećenje resursa: Implementacija i održavanje zahtijeva puno resursa, uključujući vrijeme i troškove za kontinuirano praćenje i upravljanje mrežnim aktivnostima te potrebu za naprednim alatima i tehnologijama sigurnosti.
4. Potencijal za lažne pozitive: Stroga priroda sigurnosti zero trust modela može rezultirati lažnim pozitivima, gdje legitimne aktivnosti ili korisnici mogu biti označeni kao sumnjivi.
5. Ovisnost o tehnologiji: Sigurnost nultog povjerenja ovisi o tehnologiji, uključujući napredne alate za verifikaciju identiteta, enkripciju i segmentaciju mreže, to može organizacijom učiniti ranjivom i ovisnom o neprekidnom ažuriranju i ulaganju u nove tehnologije. [45]

6.4. Extended Detection and Response (XDR)

Extended Detection and Response (XDR) je evolucija tradicionalnih EDR (Endpoint Detection and Response) sustava, proširuje detekciju i odgovor s krajnjih točaka na cijelu IT infrastrukturu, uključujući mreže, servere, aplikacije i cloud okruženja. XDR unificira sprječavanje prijetnji, njihovu detekciju i odgovor na njih. Rješenja XDR prikupljaju podatke iz alata u sigurnosnom tehnološkom sklopu organizacije kako bi stvorila širi kontekst za timove sigurnosnog operativnog centra, te omogućila bržu detekciju, istragu i odgovor na prijetnje. XDR omogućuje sveobuhvatnu vidljivost i korelaciju događaja iz različitih izvora, te pružai bolju detekciju složenih prijetnji i ubrzava odgovor na incidente. Ključne značajke XDR uključuju detekciju sigurnosnih incidenata, automatizirane sposobnosti odgovora te integraciju podataka iz više izvora s sigurnosnom analitikom kako bi se korelirale i kontekstualizirale sigurnosne uzbune.[46], [47], [48]

Razlike između XDR, MDR i EDR također su značajne. EDR (Endpoint Detection and Response) pruža detekciju i odgovor za krajnje točke. MDR (Managed Detection and Response) pruža detekciju i odgovor kao upravljanu uslugu, dok XDR (Extended Detection and Response) pruža detekciju i odgovor preko više sigurnosnih kontrola i izvora podataka. [46], [47], [48]]

6.4.1. Prednosti

1. Detekcija naprednih prijetnji: XDR osigurava napredne sposobnosti detekcije i odgovora, nudi detekciju i odgovor na ciljanje napade, nativnu podršku za analizu ponašanja korisnika i tehnoloških sredstava.
2. Automatizacija i orkestracija: Moguća je automatizacija ponavljajućih zadataka, a integrirane opcije odgovora s potrebnim kontekstom iz svih sigurnosnih komponenti omogućuju brzo rješavanje uzbuna.
3. Smanjenje lažnih pozitivnih: Korelacija i automatska potvrda uzbuna smanjuje potrebu za praćenjem lažnih pozitivnih.
4. Centralizirana konfiguracija i očvršćivanje: Centralizirana konfiguracija pomaže u prioritetizaciji aktivnosti te pruža centralizirano sučelje za istrage i odgovore na događaje.
5. Priručnici za automatizaciju: Priručnici za automatizaciju omogućuju analitičarima uspostavljanje najboljih praksi za detekciju i odgovor na prijetnje.[46], [47], [48]

6.4.2. Ograničenja

1. Teža integracija različitih sigurnosnih rješenja

2. Dodatan pritisak na IT timove koji moraju upravljati složenim sustavima i osigurati njihovu stalnu usklađenost i funkcionalnost.
3. Ne postoji univerzalni standard XDR rješenja što može otežati interoperabilnost između ostalih rješenja

6.5. Behavioral biometrics

Iako su fizičke biometrije poput otiska prsta i prepoznavanja lica još uvijek među najčešće korištenim tehnologijama za autentifikaciju, noviji sigurnosni sustavi brzo dobivaju na značaju. Ove tehnologije autentifikacije privlače veliku pažnju zbog niskih troškova implementacije i nenametljivog okruženja u usporedbi s drugim sustavima fizičke biometrije. Najčešće korišteni sustavi bihevioralne biometrije su[49]:

1. Prepoznavanje glasa
2. Prepoznavanje hoda
3. Prepoznavanje potpisa
4. Dinamika tipkanja

koriste se u različite sigurnosne svrhe i razlikuju se po prirodi biometrijskih obilježja, okruženju korištenja te prednostima i nedostacima. Većina ovih sustava još nije ispunila 100% očekivanja aplikacija, ali su dostigli određenu razinu upotrebljivosti i implementacije zahvaljujući raznim prednostima, uključujući minimalne napore potrebne od strane korisnika za prikupljanje podataka i nepostojanje potrebe za specifičnim hardverom osim tradicionalne tipkovnice za proces autentifikacije. Razvoj aplikacija i biometrijskih obilježja je u tijeku kako bi se postigao optimalan način autentifikacije koji može učinkovito prevladati većinu sigurnosnih izazova.[49]

6.5.1. Prepoznavanje glasa

Danas je prepoznavanje glasa uvelike korišteno kao jedna od pouzdanih metoda prijave. Mnoge organizacije primijenile su prepoznavanje glasa, poput online bankarstva preko telefona, gaming sustava, telefona, televizora i računalnih sustava. Glasovna identifikacija/autentifikacija se također koristi u mnogim sigurnosnim sektorima, forenzičkoj znanosti i nadzoru. Jedini nedostatak bio bi da pouzdanost i točnost sustava za prepoznavanje glasa mogu biti loši zbog brojnim faktorima, kao što su bolesti ili infekcije grla, emocionalna stanja i starenje.[49]

6.5.2. Prepoznavanje hoda

Prepoznavanje hoda koristi se kao moderna metoda za identifikaciju/autentifikaciju identiteta pojedinaca. Zbog povećane potražnje za učinkovitom tehnologijom koja pruža visoku razinu sigurnosti, prepoznavanje hoda privuklo je pažnju istraživača sigurnosnih zajednica. Tehnologija prepoznavanja hoda pokazuje prihvatljive performanse u video nadzoru. Prepoznavanje osobe temeljem stila hodanja jedna je od tehnika bihevioralne biometrije jer se oslanja na analizu strukture tijela ili pokreta tijela.[49]

Tehnologija prepoznavanja hoda postala je preferirani način autentifikacije, posebno u područjima koja zahtijevaju pouzdane sustave kontrole pristupa. Posebne značajke su mogućnost prepoznavanja osoba s velikih udaljenosti i minimalnu ili nikakvu suradnju s tehnologijom ili promatranim objektom. Stoga je prepoznavanje hoda označeno kao nenametljiva tehnologija autentifikacije. Tradicionalne CCTV kamere mogu raditi savršeno za ovaj sustav. Može prepoznati osobe čak i s manje rezolucije snimljenih slika iz odabranih videozapisa.[49]

Neki nedostatci uključuju ako na primjer, osoba ozljedi nogu, ozljeda noge može negativno utjecati na prepoznavanje hoda, kao i nošenje različitih vrsta odjeće ili promjene u izgledu.[49]

6.5.3. Prepoznavanje potpisa

Prepoznavanje potpisa je bihevioralna biometrijska metoda za prepoznavanje pojedinaca analizom njihovih pisanih potpisa, bilo online ili offline. Ova tehnologija je korištena desetljećima kao način razlikovanja osoba. Potpis se može dobiti tradicionalnim načinom na papiru ili elektroničkim uređajima.

Ručno pisani potpis dugo se smatrao najpopularnijim načinom provjere identiteta. Ova metoda ima posebnu karakteristiku među drugim soft biometrijskim metodama jer zahtijeva vrlo malo mjerenja prilikom analize potpisa. Široka upotreba ove tehnologije čini je vrlo poznatom i bliskom svakodnevnom životu. Teško je uzeti nečiji potpis kada je osoba bez svijesti, za razliku od drugih biometrijskih tehnologija kao što su otisci prstiju koji se lako mogu prikupiti čak i kada je osoba bez svijesti.[49]

Unatoč brojnim konkurentnim značajkama, prepoznavanje potpisa ima određene nedostatke. Osoba može promijeniti način potpisivanja kroz vrijeme, a bolest može utjecati na način pisanja potpisa.[49]

6.5.4. Dinamika tipkanja

Dinamika tipkanja je metoda autentifikacije u kojoj se korisnik prepoznaje na temelju ritma tipkanja. Može se podijeliti u dvije kategorije: statična dinamika tipkanja (SKD), gdje korisnik unosi unaprijed definiranu lozinku na početku sesije, i kontinuirana dinamika tipkanja (CKD), gdje se prati promjena u ponašanju korisnika tijekom cijele sesije autentifikacije.[49]

Jedna od značajnijih prednosti dinamike tipkanja je da nije potreban dodatni hardver za povezivanje sa sustavom. Jedini senzor ili uređaj za prikupljanje podataka je obična tipkovnica. Ova tehnologija pruža učinkovit dodatak trenutnim starim metodama verifikacije lozinki. Prepoznavanje osoba na temelju ritma tipkanja je ugrađena sigurnosna tehnika koja je teška za promatranje od strane vanjskih promatrača. Također, analiza dinamike tipkanja ne zahtijeva velika računalna opterećenja, ali postoje i nedostatci. Budući da se radi o zadacima tipkanja, metoda zahtijeva dobre vještine tipkanja kako bi se dobili dobri parametri za svaku osobu.[49]

6.5.5. Prednosti

1. Niski troškovi implementacije: Bihevioralne biometrijske tehnologije često ne zahtijevaju specifičan hardver. To značajno smanjuje troškove implementacije u usporedbi s fizičkim biometrijskim sustavima poput skenera otisaka prstiju ili prepoznavanja lica.
2. Nenametljivo prikupljanje podataka: Prikupljanje bihevioralnih podataka može se odvijati nenametljivo, bez potrebe za aktivnom suradnjom korisnika. Na primjer, prepoznavanje hoda može se provesti analizom video snimki iz CCTV kamera, a dinamika tipkanja prati se tijekom uobičajenog unosa teksta na tipkovnici.
3. Jedinstvenost i osobna prilagodljivost: Bihevioralne karakteristike poput glasa, hoda, potpisa i ritma tipkanja su jedinstvene za svaku osobu. Ove karakteristike se prilagođavaju pojedincu i teško ih je imitirati.
4. Povećana sigurnost: Kombinacija bihevioralnih biometrijskih metoda s drugim sigurnosnim mjerama može pružiti višu razinu sigurnosti. Na primjer, kombinacija prepoznavanja glasa s tradicionalnim lozinkama može značajno smanjiti rizik od neovlaštenog pristupa.
5. Prilagodljivost različitim okruženjima: Bihevioralne biometrijske tehnologije mogu se prilagoditi različitim aplikacijama i okruženjima. Prepoznavanje glasa se može koristiti u mobitelima, dok se dinamika tipkanja može koristiti na računalima i mobilnim uređajima.

6. Neprekidna autentifikacija: Neke bihevioralne biometrijske metode omogućuju kontinuiranu autentifikaciju, što znači da se identitet korisnika provjerava tijekom cijele sesije, a ne samo na početku.

6.5.6. Ograničenja

1. Varijabilnost bihevioralnih karakteristika: Bihevioralne karakteristike mogu varirati zbog različitih faktora. Na primjer, prepoznavanje glasa može biti nepouzdano zbog bolesti ili emocionalnog stanja korisnika, dok hod može varirati zbog ozljeda ili nošenja različite obuće.
2. Potreba za kvalitetnim podacima: Kvaliteta prikupljenih podataka može značajno utjecati na točnost bihevioralnih biometrijskih sustava. Loša kvaliteta zvuka u prepoznavanju glasa ili niska rezolucija video snimaka u prepoznavanju hoda može smanjiti učinkovitost ovih sustava.
3. Manjak standardizacije: Bihevioralne biometrijske tehnologije još uvijek nisu u potpunosti standardizirane
4. Sigurnosne ranjivosti: Bihevioralne biometrijske sustave moguće je prevariti korištenjem sofisticiranih napada. Na primjer, napadači mogu koristiti snimke glasa ili videa za prijevaru sustava prepoznavanja glasa ili hoda.
5. Privatnost i etička pitanja: Prikupljanje i pohrana bihevioralnih podataka postavlja pitanja privatnosti i zaštite podataka. Potrebno je osigurati da se ovi podaci prikupljaju i koriste u skladu s zakonima o zaštiti privatnosti i da su zaštićeni od neovlaštenog pristupa.
6. Ograničenja u točnosti: Unatoč napretku, mnoge bihevioralne biometrijske metode još uvijek ne pružaju 100% točnost.

6.6. Deception technology

U području kibernetičke sigurnosti obrambena prijevara sprječava napadače da otkriju ranjivosti, a također omogućuje braniteljima da proučavaju metode napadača. Glavne tehnike koje se koriste u obrambenoj prijevari su maskiranje, prepakiranje, zasljepljivanje, oponašanje, izmišljanje i varanje.[50]

Tehnike obrambene prijevare:

1. Maskiranje: Skriva informacije u pozadini.
2. Repakiranje: Prikazuje informacije kao nešto drugo

3. Zasljepljivanje: Prekriva stvarne informacije pretjeranim količinama nebitnih podataka.
4. Imitacija: Oponaša aspekte pravih objekata kako bi zavarala napadače.
5. Izmišljanje: Stvara nove, lažne objekte ili informacije za zavaravanje napadača.
6. Mamci: Omogućava dostupnost lažnih informacija javnosti kako bi se zavarali napadači.

Jedna od najpoznatijih tehnika obmane je honeypot, koji je istražen u kontekstu pametnih mreža. Honeynet sustavi mogu emulirati cijelu komunikacijsku mrežu pametne mreže, uključujući višestruke podstanice. Adaptivne honeynets bazirane na POMDP-u (Partially Observable Markov Decision Process) mogu se koristiti za dinamičku prilagodbu obrambenih strategija.[50]

6.6.1. Prednosti

1. Širok spektar napadačkih strategija: Tehnologija bazirana na mamcima može učinkovito upravljati raznim napadačkim strategijama kao što su skeniranje, otisci mreže, odbijanje usluge (DoS), malware, napadi na privatnost, napredne perzistentne prijetnje (APT) i lažno predstavljanje.
2. Zaštita kritičnih sustava: U kontekstu električnih podstanica, mamci se mogu koristiti za skrivanje stvarne komunikacijske mreže (VLAN) i obmanjivanje napadača na lažnu VLAN mrežu.
3. Alarmiranje i odgovor na incidente: Kada napadač stupi u interakciju s mamcem, to može pokrenuti alarm za operatera sustava i inicirati odgovor na incident.
4. Analiza napadačkih metoda: Interakcija napadača s mamcem pruža vrijedne informacije o napadačkim metodama i tehnikama.
5. Tehnologija jednostavna za implementaciju: Mnogi sustavi obmane, kao što su honeypots, već su dobro istraženi i mogu se lako implementirati u razne mrežne okoline, uključujući pametne mreže i IoT sustave.

6.6.2. Ograničenja

1. Kompleksnost upravljanja: Upravljanje velikim brojem mamaca i drugih obmanjujućih tehnika može biti kompleksno i zahtijeva značajne resurse za održavanje i nadzor.
2. Ranjivosti u implementaciji: Neispravno implementirani mamci mogu biti otkriveni od strane napadača, čime se smanjuje njihova učinkovitost.
3. Ograničenja u specifičnim scenarijima: Postojeći modeli obmane možda nisu primjenjivi u svim situacijama. Na primjer, zaštita podstanica kroz obmanu može

zahtijevati posebne modele i strategije koje uzimaju u obzir specifične zahtjeve i uvjete mreže.

4. Ograničena skalabilnost: Implementacija obmanjujućih tehnologija na velikim mrežama može biti izazovna zbog problema sa skalabilnošću i potrebom za značajnim resursima za održavanje efikasnosti sustava.

7. Pregled novih alata i tehnika u industriji

SOC-ovi koriste razne alate i tehnike za detekciju, analizu i odgovaranje na sigurnosne incidente. U nastavku su opisani neki od najznačajnijih alata koji se koriste u SOC-ovima, uključujući i alate s kojima sam se susreo tijekom studentske prakse u banci za cybersecurity

7.1 Qradar (IBM security Qradar)

IBM Security QRadar je rješenje za detekciju prijetnji i odgovore, služi kako bi ubrzalo rad sigurnosnih analitičara kroz cijeli životni ciklus incidenta. Koristi se AI i automatizacija kako bi se povećala produktivnost analitičara, omogučuje timovima sa ograničenim resursima da rade efikasnije kroz ključne tehnologije. QRadar uključuje integrirane proizvode za endpoint security (EDR, XDR, MDR), log management, SIEM i SOAR, sve unutar zajedničkog korisničkog sučelja, s dijeljenim uvidima i povezanim radnim tokovima. [51]

Ključne Komponente IBM QRadar [51]:

1. Endpoint security (EDR, XDR, MDR)
    - Endpoint Detection and Response (EDR): Pruža detaljnu vidljivost i kontrolu nad krajnjim točkama.
    - Extended Detection and Response (XDR): Integrira višestruke sigurnosne funkcije za sveobuhvatnu zaštitu.
    - Managed Detection and Response (MDR): Nudi upravljane usluge detekcije i odgovora.
2. Log management
    - Praćenje i analiza sigurnosnih događaja u realnom vremenu.
    - Omogućava napredne pretrage i izvještavanje.
3. SIEM (Security Information and Event Management)

    - Kombinira znanje o mrežnim tokovima, korelaciju sigurnosnih događaja i procjenu ranjivosti imovine.
    - Pruža podršku za usklađenost i svijest o situacijama u mreži.
4. SOAR (Security Orchestration, Automation, and Response)
    - Automatizira i orkestrira odgovore na sigurnosne incidente.
    - Povećava efikasnost sigurnosnih timova kroz automatizaciju procesa.

7.1.1 Praktično Iskustvo s QRadar-om

Tijekom moje studentske prakse u banci za cybersecurity, imao sam priliku vidjeti kako SOC analitičari rade s IBM QRadar-om. Uz IBM Qradar imao sam priliku vidjeti i alate Crowdstrike Falcon, Akamai, SOAR. Iskustvo je uključivalo sljedeće aktivnosti:

1. Monitoring log aktivnosti
    - U QRadar-u se može pratiti i prikazivati mrežne događaje u realnom vremenu ili izvršavati napredne pretrage.
    - Koristili su napredne pretrage za identifikaciju i analizu potencijalnih sigurnosnih prijetnji.
2. Istraživanje mrežnih aktivnosti
    - Istraživanje komunikacijskih sesija između dva hosta.
    - Analizirali su mrežne tokove za identifikaciju sumnjivih aktivnosti.
3. Kreiranje profila imovine
    - QRadar automatski kreira profile imovine koristeći pasivne podatke o tokovima i podatke o ranjivostima.
    - Moguća je Identifikacija ključnih servera i hostova unutar mreže.
4. Istraga prekršaja (Offenses)
    - Istraživanje prekršaja kako bi se utvrdio osnovni uzrok mrežnog problema.
    - Koriste se pravila za monitiranje događaja i tokova kako bi se detektirale prijetnje.
5. Generiranje izvještaja
    - Mogućnost kreiranja prilagođenih izvještaja ili korištenje podrazumijevanih izvještaja.
6. Prikupljanje podataka
    - QRadar prihvaća informacije u raznim formatima iz širokog spektra uređaja, uključujući sigurnosne događaje, mrežni promet i rezultate skeniranja.
7. Pravila i odgovori

- Pravila u QRadar-u izvode testove na događajima, tokovima ili prekršajima. Ako su svi uvjeti testa zadovoljeni, pravilo generira odgovor.
- Kreiranje i podešavanje pravila za preciznu detekciju prijetnji.

8. Aplikacije i dodaci
    - QRadar administratori mogu pregledati, preuzeti i instalirati aplikacije iz IBM Security App Exchange za specifične sigurnosne potrebe.

Slabosti:

QRadar se suočava s izazovima u implementaciji u složenim IT okruženjima, gdje može biti teško prilagoditi rješenje specifičnim potrebama organizacije. Također, za manje organizacije, može biti financijski zahtjevan, zbog visokih troškova licenciranja i održavanja. QRadar se oslanja na kvalitetu podataka koje prikuplja, što znači da se slabosti u izvornim podacima (npr. neodgovarajuće logove ili zastarjele informacije) mogu negativno odraziti na performanse sustava, osobito u detekciji naprednih prijetnji.

7.2 Crowdstrike falcon

CrowdStrike falcon je platforma dizajnirana za sprječavanje sigurnosnih proboja putem clouda. Današnji napadači ne koriste samo malware kako bi probili organizacije, sve više se oslanjaju na eksploite kao što su zero-day ranjivosti i metode kao što su krađa korisničkih podataka i alati koji su već dio okruženja žrtve ili operativnog sustava, kao što je PowerShell. CrowdStrike Falcon odgovara na te izazove s rješenjem koje ujedinjuje antivirus nove generacije (NGAV), endpoint detection and response (EDR), cyber threat intelligence, managed threat hunting, sve unutar senzora koji se upravlja i isporučuje putem clouda.[52]

Ključne Komponente CrowdStrike Falcon Platforme[52] :

1. Endpoint Security Solutions
    - Falcon prevent: Antivirus nove generacije (NGAV) dizajniran za sprječavanje malware napada.
    - Falcon insight: Endpoint detection and response (EDR) koji omogućava dubinsku analizu krajnjih točaka.
    - Falcon device control: Kontrola USB uređaja za sprječavanje neovlaštenih pristupa.
    - Falcon firewall management: Upravljanje host firewall-om za kontrolu mrežnog prometa.

    - Falcon for mobile: Mobile Endpoint Detection and Response za zaštitu mobilnih uređaja.
    - Falcon forensics: Analiza forenzičkih podataka za detaljno istraživanje incidenata.
2. Security & IT operations
    - Falcon overwatch: Upravljanje prijetnjama (Managed Threat Hunting) koje koristi tim stručnjaka za lov na prijetnje.
    - Falcon discover: Sigurnosna higijena koja omogućava pregled nad sigurnosnim stanjem mreže.
    - Falcon spotlight: Upravljanje ranjivostima koje omogućava identifikaciju i prioritizaciju ranjivosti.
3. Threat intelligence
    - CrowdStrike falcon intelligence: Prijetnjama inteligencija za proaktivno otkrivanje i analizu prijetnji.
    - Falcon search engine: Najbrži pretraživač malware-a za brzu analizu prijetnji.
    - Falcon sandbox: Automatizirana analiza malware-a koja omogućava sigurno testiranje sumnjivih datoteka.
4. Cloud security solutions
    - Falcon Cloud Workload Protection: Zaštita radnih opterećenja u cloud okruženjima kao što su AWS, Azure i GCP.
    - Falcon Horizon: Upravljanje sigurnosnim postavkama u cloud okruženjima (Cloud Security Posture Management - CSPM).
    - Container Security: Sigurnosna rješenja za kontejnere.
5. Identity protection solutions
    - Falcon Identity Threat Protection (ITD): Zaštita identiteta i vjerodajnica.
    - Falcon Zero Trust: Implementacija Zero Trust sigurnosnog modela.
6. Falcon Fusion SOAR
    - Falcon fusion SOAR: Integrirani set mogućnosti za orkestraciju, automatizaciju i odgovore na sigurnosne incidente. Omogućava lako implementiranje automatizacije radnih tokova za prikupljanje podataka, obogaćivanje, odgovore i obavijesti.

7.2.1 Praktično Iskustvo s Crowdstrike Falcon-om

1. Implementacija i konfiguracija falcon prevent

    - Postavljanje pravila i politike za sprječavanje malware-a i zaštitu krajnjih točaka.
2. Korištenje falcon insight za EDR
    - Detekcija sumnjivih aktivnosti i provođenje istraga uz detaljne zapise i alate za analizu.
3. Upravljanje USB uređajima putem falcon device control-a
    - Kontrola pristupa i korištenja USB uređaja u mreži.
4. Forenzička analiza s falcon forensics
    - Korištenje alata za prikupljanje i analizu forenzičkih podataka.
5. Lov na prijetnje s falcon overwatch
    - Suradnja s timom za detekciju prijetnji i brzo reagiranje na sumnjive aktivnosti.
6. Upravljanje ranjivostima s falcon spotlight
    - Korištenje alata za upravljanje ranjivostima i provedbu sigurnosnih zakrpa.
7. Analiza prijetnji s falcon intelligence
    - Praćenje najnovijih prijetnji i trendova te prilagodba sigurnosnih mjera.
8. Automatizacija odgovora s falcon fusion SOAR
    - Implementacija automatiziranih radnih tokova za brz i učinkovit odgovor na prijetnje.

Slabosti:

Osjetljivost na lažne alarme predstavlja izazov za sigurnosne timove koji moraju upravljati velikim brojem upozorenja. U praksi, platforma se učinkovito bori protiv modernih prijetnji, uključujući napade bez malvera i eksploatacije zero-day ranjivosti, no postoje poteškoće u prilagođavanju specifičnih sigurnosnih potreba organizacije. Npr. organizacija koja koristi microsoft active directory za upravljanje korisničkim računima može doći do problema u kojem napadači koriste legitimne račune za lateralne pokrete unutar mreže (tzv. living off the land napadi). CrowdStrike može imati poteškoća u razlikovanju legitimnih aktivnosti od malicioznih, jer napadači ne koriste vanjske alate, nego resurse već prisutne u sustavu.

7.3 Akamai kona site defender

Akamai kona site defender pruža zaštitu za web aplikacije i API-je, uključujući DDoS zaštitu, WAF i zaštitu API-ja. [53]

Ključne komponente akamai kona site defender-a [53]:

1. DDoS zaštita uvijek aktivna

- Kona Site Defender koristi web aplikacijski firewall (WAF) za zaštitu od DDoS napada usmjerenih na aplikacijski sloj i autentificiranje validnog prometa na mrežnom rubu. Automatske kontrole reagiraju na napade unutar sekundi, a stručnjaci za sigurnost mogu kreirati prilagođena pravila za sofisticirane napade.
- Akamai Intelligent Platform je dizajnirana kao reverse proxy i automatski odbija sve mrežne DDoS napade, s kapacitetom preko 61 Tbps za apsorbiranje najvećih napada.

2. Web application firewall (WAF)
    - WAF uključuje bogatu kolekciju unaprijed definiranih pravila za aplikacijski sloj. Akamai threat research team redovito ažurira ova pravila temeljem unutarnje inteligencije prijetnji koja dolazi iz jedinstvenog uvida u 15 do 30% svjetskog web prometa.
3. Zaštita API-ja
    - Kona Site Defender koristi pozitivne i negativne sigurnosne modele za zaštitu API-ja od zlonamjernih poziva. Korisnici mogu definirati koje vrste zahtjeva i poziva su dopuštene, a Kona Site Defender će provjeriti parametre RESTful API-ja protiv popisa očekivanih vrijednosti i provjeriti JSON tijelo i putanje za rizični sadržaj.

7.3.1 Praktično Iskustvo s Akamai kona site defender-om

1. Implementacija i konfiguracija kona site defender-a
    - Instalacija i konfiguracija WAF-a za zaštitu web aplikacija i API-ja.
2. Korištenje DDoS zaštite
    - Opis: Aktivno praćenje i mitigiranje DDoS napada usmjerenih na aplikacijski sloj.
3. Upravljanje WAF pravilima
    - Konfiguracija i prilagodba unaprijed definiranih pravila za aplikacijski sloj.
4. Zaštita API-ja
    - Definiranje i implementacija sigurnosnih modela za zaštitu API-ja od zlonamjernih poziva.
5. Analitika i izvještavanje
    - Opis: Praćenje i analiza sigurnosnih događaja te izvještavanje o sigurnosnim incidentima na razini API-ja.

Slabosti:

Jedna od glavnih slabosti je kompleksnost upravljanja WAF pravilima, gdje su početne postavke često previše opće. Organizacije bi mogle profitirati od dodatnih automatiziranih alata za optimizaciju pravila i prilagodbu zaštite prema specifičnim potrebama aplikacija, čime bi se smanjili operativni teret i ljudske pogreške.

7.4 Tenable.io

Tenable.io je rješenje za upravljanje ranjivostima koje pruža vidljivost i uvid u sigurnosnu sposobnost organizacije. Omogućuje prepoznavanje ranjivosti, pogrešnih konfiguracija i sigurnosnih slabosti u mrežama, sustavima i aplikacijama putem automatiziranog skeniranja.[54]

Ključne Funkcionalnosti Tenable Rješenja [54]:

1. Skeniranje Ranjivosti
    - Tenable.io i Tenable.sc (ranije SecurityCenter) pružaju automatizirano skeniranje ranjivosti kako bi identificirali ranjivosti, pogrešne konfiguracije i sigurnosne slabosti u mrežama, sustavima i aplikacijama.
2. Otkrivanje Prijetnji
    - Tenable pomaže organizacijama u otkrivanju i odgovoru na sigurnosne prijetnje pomoću alata poput Tenable.io s Nessus Network Monitor (NNM) i Tenable.ot (ranije Indegy).
3. Inventar sredstava
    - Tenable rješenja pomažu organizacijama u održavanju sveobuhvatnog inventara sredstava, nudi vidljivost uređaja, servera, aplikacija i cloud resursa.
4. Upravljanje patchevima
    - Tenable pomaže u upravljanju patchevima tako da identificira nedostajuće patcheve i prioritizira njihovo implementiranje kako bi se riješile kritične ranjivosti.
5. Procjena usklađenosti
    - Omogućava organizacijama procjenu njihove usklađenosti s različitim sigurnosnim standardima i regulativama provođenjem skeniranja usklađenosti i generiranjem izvještaja.
6. Skeniranje web aplikacija
    - Tenable može skenirati web aplikacije za ranjivosti poput SQL injekcija, cross-site scripting (XSS) i sigurnosnih pogrešnih konfiguracija.
7. Sigurnost IoT

- Tenable procjenjuje sigurnost uređaja Interneta stvari (IoT) i pomaže identificirati ranjivosti u IoT implementacijama.

8. Analiza ponašanja korisnika i entiteta (UEBA)
    - Tenable rješenja prate ponašanje korisnika i entiteta kako bi otkrili unutarnje prijetnje, kompromitirane račune i neuobičajene aktivnosti.

Slabost:

Jedno od ključnih ograničenja je kompleksnost izvještavanja i upravljanja velikim brojem ranjivosti u velikim IT okruženjima. Organizacije se ponekad suočavaju s problemima u prioritetizaciji otkrivenih ranjivosti i zbog toga dolazi do preopterećenja sigurnosnih timova.

Rješenje bi moglo uključivati poboljšane algoritma za automatsko određivanje prioriteta i više prilagodljivih izvještajnih opcija, koje bi omogućile timovima da se fokusiraju na najkritičnije prijetnje.

7.4.1 Princip rada i arhitektura

Organizacije se pretplaćuju na Tenableove cloud usluge (Tenable.io) ili implementiraju on-premises rješenja (Tenable.sc) prema svojim zahtjevima. Tenable rješenja započinju otkrivanjem i profiliranjem sredstava u okruženju organizacije, uključujući uređaje, servere, aplikacije i cloud resurse. Provode se automatizirana skeniranja kako bi se identificirale ranjivosti, pogrešne konfiguracije i potencijalne prijetnje. Tenableovo kontinuirano praćenje pruža stalnu vidljivost sigurnosne posture. Primjenjuje se analitika ponašanja i strojno učenje za identifikaciju anomalija. Kada se otkriju sigurnosni incidenti, Tenable, zajedno s procesima odgovora na incidente, pomaže organizacijama istražiti, odgovoriti i ublažiti incidente.[54]

Tenable.sc ili Tenable.io su centralne komponente Tenableove arhitekture. Tenable.sc je on-premises rješenje, dok je Tenable.io cloud-based. One služe kao glavne platforme za upravljanje ranjivostima, otkrivanje prijetnji i procjenu usklađenosti. Skeneri su odgovorni za provođenje skeniranja ranjivosti. U slučaju on-premises rješenja, organizacije implementiraju skenere unutar svoje mreže. Cloud-based rješenja mogu koristiti virtualne skenere. Tenable agenti su lagane softverske komponente koje se mogu instalirati na pojedinačnim hostovima kako bi prikupljali podatke i olakšali real-time praćenje i skeniranje. Tenable pohranjuje i analizira podatke prikupljene skeniranjem, logovima i mrežnim prometom. Tenableova rješenja dizajnirana su za integraciju s drugim sigurnosnim alatima, SIEM platformama i uslugama trećih strana kako bi stvorili sveobuhvatan sigurnosni ekosistem.[54]

7.5 Vectra.AI

Vectra AI služi kao alat za detekciju prijetnji u stvarnom vremenu, oslanja se na naprednu analitiku i umjetnu inteligenciju. [55]

Ključne funkcionalnosti [55]:

1. Vidljivost i otkrivanje prijetnji u stvarnom vremenu
2. Umjetna inteligencija (AI)
    - Koristi AI-augmented rješenja za prepoznavanje ponašanja napadača i predviđanje njihovih ciljeva, poput implementacije ransomware-a ili eksfiltracije podataka.
3. Analiza anomalija
    - AI detektira anomalije i prijetnje koje ljudi ne mogu uočiti dovoljno brzo. Sortira ove anomalije i klasificira ih prema prioritetima, omogućujući sigurnosnim timovima da budu proaktivni umjesto reaktivni.
4. Kontekstualna analiza
    - prepoznaje ponašanja i obrasce napadača u povijesnom kontekstu lokalnog okruženja, kao i u stotinama drugih cloud i mrežnih domena. Prijetnje se klasificiraju prema ozbiljnosti, te prioritizira stvarne napade.
5. Integracija s cloudom i on-premises okruženjima
    - otkriva napadače i proboje prije nego što se nanese šteta, bilo da je riječ o on-premises ili cloud okruženju. Pomaže organizacijama u upravljanju sigurnošću tijekom migracije podataka u cloud.

Slabost:
Iako nudi značajnu vidljivost mrežnih aktivnosti i prepoznavanje prijetnji postoje i određene slabosti. Na primjer, u okruženjima s vrlo visokim prometom, Vectra AI ponekad generira lažne alarme, što može preopteretiti sigurnosne timove. Također, integracija s drugim alatima je ponekad otežana, posebno u IT okruženjima gdje koji se sastoje od različitih platformi, aplikacija i uređaja. Iako je alat učinkovit u prepoznavanju prijetnji, mogao bi se poboljšati u segmentu smanjenja broja false positive rezultata te u jednostavnijoj integraciji s postojećim sustavima.

8. Procesi unutar SOC-a

Sigurnosni operativni centar predstavlja srce operacija kibernetičke sigurnosti unutar organizacije. Njegova uloga je ključna u prepoznavanju, analizi i odgovoru na sigurnosne incidente. SOC procesi su set procedura i praksi koje SOC timovi koriste za identifikaciju, prevenciju, detekciju, odgovor i oporavak od sigurnosnih prijetnji. Da bi SOC bio učinkovit, važno je kontinuirano istraživati i unapređivati procese unutar SOC-a. Ova cjelina će obraditi istraživanje trenutnih procesa unutar SOC-a, identifikaciju slabosti u postojećim procesima i prijedloge za unapređenje efikasnosti SOC-a.

8.1 Istraživanje trenutnih procesa unutar SOC-a

Istraživanje trenutnih procesa unutar SOC-a uključuje detaljno ispitivanje kako SOC operira, koje alate i tehnologije koristi, te kako se incidenti prepoznaju, analiziraju i rješavaju.

Unutar sigurnosnih operativnih centara (SOC), glavni procesi uključuju prikupljanje podataka, otkrivanje prijetnji, odgovor na incidente i stalno praćenje sigurnosne situacije. Ovi procesi su ključni za pravovremenu detekciju i mitigaciju prijetnji. Međutim, istraživanja pokazuju da mnogi SOC-ovi imaju problema s optimizacijom ovih procesa zbog nedostatka automatizacije, ograničenih resursa i složenosti modernih prijetnji. Na primjer, standardni alati poput SIEM sustava često stvaraju veliki broj false positive alarma, što dovodi do preopterećenja analitičara i usporava vrijeme reakcije.

Ključni pokazatelji uspješnosti (KPI) za SOC-ove uključuju MTTD (Mean Time to Detect), MTTR (Mean Time to Respond), stopu lažnih alarma, troškove po incidentu, i MTBF (Mean Time Between Failures). Ovi pokazatelji su kritični za procjenu učinkovitosti SOC-ova jer odražavaju sposobnost sustava da brzo otkriva, odgovara na prijetnje i održava stabilnost sustava.

Identifikacija potencijalnih sigurnosnih prijetnji[56], [57]:

- Proces uključuje praćenje mrežnog prometa, sistemskih logova i drugih izvora podataka kako bi se identificirale potencijalne sigurnosne prijetnje. To mogu biti sumnjivi pokušaji prijave, mrežne anomalije ili neovlašteni pokušaji pristupa.

Prevencija sigurnosnih prijetnji [56], [57]:

- SOC timovi koriste tehnike za prevenciju sigurnosnih prijetnji, kao što su kontrola pristupa, vatrozidi i sistemi za prevenciju upada (IPS). Također surađuju s drugim timovima unutar organizacije kako bi osigurali da se sigurnosne politike i procedure slijede.

Detekcija sigurnosnih prijetnji [56], [57]:

- Nakon što je potencijalna prijetnja identificirana, SOC timovi koriste različite alate i tehnike za detekciju i analizu prijetnje. To uključuje mrežno praćenje, obavještajne podatke o prijetnjama i alate za detekciju i odgovor na krajnjim točkama (EDR).

Odgovor na sigurnosne prijetnje [56], [57]:

- Kada se otkrije sigurnosna prijetnja, SOC timovi moraju brzo i učinkovito reagirati kako bi obuzdali prijetnju i minimizirali štetu. Mogu blokirati mrežni promet, izolirati zaražene sustave i onemogućiti kompromitirane račune.

Oporavak od sigurnosnih prijetnji [56], [57]:

- Nakon što je sigurnosni incident obuzdan i riješen, SOC timovi moraju raditi na vraćanju sustava i podataka u normalno stanje. To uključuje obnavljanje podataka, zakrpanje sustava i oporavak korisničkih računa.

8.2 Identifikacija slabosti u postojećim procesima

Identifikacija slabosti u postojećim procesima unutar sigurnosnog operativnog centra ključno je za poboljšanje učinkovitosti i otpornosti na kibernetičke prijetnje. SOC-ovi se suočavaju s brojnim izazovima, uključujući napredne prijetnje kao što su zero-day ranjivosti i napredne uporne prijetnje (APT-ovi), koje je teško otkriti i ublažiti zbog nedostatka poznatih patcheva ili rješenja. Ogromna količina sigurnosnih podataka i alarma može preplaviti analitičare i to uzrokuje zamor alarmima i povećava rizik od propuštanja stvarnih prijetnji. Složeni i dinamični IT sustavi, koji često uključuju on-premises i cloud infrastrukturu, također predstavljaju izazov za upravljanje i osiguranje.

Uz to, napadi na opskrbne lance zahtijevaju nadzor ne samo vlastite infrastrukture već i infrastrukture dobavljača i partnera, što je dodatno kompliciranо ograničenom vidljivošću u njihove sigurnosne prakse. Nedostatak kvalificiranih stručnjaka za kibernetičku sigurnost otežava SOC-ovima pronalaženje i zadržavanje iskusnih analitičara i lovaca na prijetnje, dok nedostatak integracija među različitim sigurnosnim alatima otežava učinkovitu korelaciju

informacija i odgovor na prijetnje. Osim toga, balansiranje sigurnosnih potreba s brigama o privatnosti predstavlja dodatni izazov, posebno kada organizacije prikupljaju i analiziraju više korisničkih podataka za detekciju prijetnji. Identificirane slabosti, poput preopterećenja alarmima, usmjerenosti na usklađenost sigurnosti, nedovoljno funkcionalnih sigurnosnih kontrola i stagnacije u operacijama, dodatno otežavaju učinkovitost SOC-a. Uz sve to, izazovi poput povećanog volumena sigurnosnih alarma, upravljanja brojnim sigurnosnim alatima, natjecanja za kvalificirane analitičare, ograničenih budžeta i usklađivanja s pravnim i regulatornim zahtjevima samo dodatno kompliciraju situaciju.

Jedan od glavnih izazova s kojima se SOC-ovi suočavaju je povećana složenost prijetnji koja zahtijeva napredne tehnike analize i automatizirane procese. Ograničenja tradicionalnih SIEM sustava, poput QRadar-a, uključuju njihovu ovisnost o pravilima temeljenima na prethodnim uzorcima napada, što znači da su manje učinkoviti u detekciji novih, nepoznatih prijetnji. Da bi se prevladali ovi izazovi, SOC-ovi trebaju usvojiti proaktivan i adaptivan pristup, kontinuirano poboljšavati svoje procese, ulagati u automatizaciju i napredne tehnologije te surađivati s drugim timovima i organizacijama za dijeljenje obavještajnih podataka i odgovora na incidente.[58], [59]

8.3 Empirijska analiza performansi SOC sustava

Cilj ove komparativne analize je usporediti Splunk SOC i IBM QRadar SOC u smislu njihovih performansi, učinkovitosti i sposobnosti za zaštitu informacijskih sustava od cyber prijetnji. Tablica ispod prikazuje usporedbu ključnih pokazatelja performansi (KPI) između dva popularna SOC sustava. Analiza performansi Splunk i QRadar sustava temelji se na industrijskim podacima prikupljenim iz relevantnih izvora. Ključni pokazatelji uspješnosti (KPI) analizirani su kako bi se procijenila učinkovitost ova dva sustava u različitim aspektima sigurnosnih operacija.[51], [60], [61]

KPI	**Splunk**	**QRadar**
MTTD (Mean Time to Detect)	Splunk je općenito brži zahvaljujući svojoj fleksibilnosti u kreiranju upita i vizualizaciji podataka.	QRadar može biti sporiji zbog većeg broja unaprijed definiranih pravila

MTTR (Mean Time to Respond)	Vrijeme odgovora ovisi o složenosti incidenta i dostupnosti stručnjaka. Splunk nudi dobre mogućnosti za automatizaciju i orkestraciju.	MTTR kod QRadara često se navodi kao jača strana zbog usmjerenosti na sigurnost i ugrađenih alata za istragu incidenata.
Stopa uspješnog rješavanja incidenata	Ovisi o kvaliteti pravila, tuneliranju i stručnosti analitičara. Splunk može postići visoku stopu uspješnosti.	QRadar može imati nešto veću stopu uspješnog rješavanja incidenata zbog svoje usmjerenosti na sigurnost.
Broj lažnih alarma	Splunk može imati manje lažnih alarma zbog veće fleksibilnosti u fine tuning-u pravila.	QRadar može imati više lažnih alarma zbog većeg broja unaprijed definiranih pravila.
Troškovi po incidentu	Ovise o složenosti incidenta, broju uključenih ljudi i vremenu potrebnom za rješavanje.	Kod QRadara mogu biti niži zbog automatizacije i ugrađenih alata.
TTC (Time to Contain)	Kod Splunka ovisi o brzini reagiranja i učinkovitosti mjera.	QRadar može imati kraće vrijeme sadržavanja zbog usmjerenosti na sigurnost i ugrađenih alata za blokiranje pristupa.
MTBF (Mean Time Between Failures)	MTBF kod Splunka ovisi o stabilnosti infrastrukture i kvaliteti implementacije. Općenito je stabilan.	MTBF kod QRadara može biti nešto veći zbog kompleksnosti sustava i većeg broja komponenti.

Incident Response Efficiency	Splunkova učinkovitost odgovora na incidente ovisi o automatizaciji, orkestraciji i stručnosti analitičara.	QRadar može biti učinkovitiji zbog usmjerenosti na sigurnost i ugrađenih alata.
Automation Rate	Splunk nudi visoku razinu automatizacije putem skriptiranja i API-ja, što povećava učinkovitost.	QRadar također nudi visoku razinu automatizacije, posebno u području sigurnosti.
First Time Resolution Rate	Stopa prvog rješenja ovisi o kvaliteti pravila, tuneliranju i stručnosti analitičara.	QRadar može imati nešto veću stopu prvog rješenja zbog svoje usmjerenosti na sigurnost.

Tablica 3: Kvalitativna usporedba KPI-a između dva SOC sustava

Analiza Splunka i Qradara pokazuje da oba sustava imaju svoje prednosti i slabosti, ovisno o specifičnim potrebama i prioritetima organizacije. Splunk se ističe u brzini detekcije prijetnji i fleksibilnosti, što ga čini pogodnim za organizacije koje traže visoku prilagodljivost i učinkovitost u različitim scenarijima. S druge strane, QRadar se pokazuje snažnijim u sigurnosno specifičnim funkcijama, sa stabilnijom izvedbom u sigurnosnim operacijama, što ga čini pogodnim za organizacije koje daju prednost sigurnosti i pouzdanosti.

Na temelju kvalitativnih empirijskih podataka, organizacije bi trebale odabrati SOC sustav prema svojim specifičnim potrebama. Ako je brzina detekcije i fleksibilnost ključna, Splunk bi mogao biti bolji izbor. No, ako je sigurnost i pouzdanost na prvom mjestu, QRadar nudi više specijalizirane funkcionalnosti.

8.4 Prijedlozi za unapređenje efikasnosti SOC-a

Poboljšanje učinkovitosti sigurnosnog operativnog centra (SOC) predstavlja kontinuiran izazov koji zahtijeva kombinaciju odgovarajućih alata, procesa, vještina i pažnje prema dobrobiti tima. Prvi korak prema unapređenju je identifikacija specifičnih slabosti unutar SOC-a. Nedostatak kvalificiranog osoblja, preopterećenje alarmima, složenost sustava i ograničeni proračuni često dovode do smanjene učinkovitosti. Organizacije trebaju ulagati u

prave alate i automatizaciju kako bi smanjile lažne alarme i olakšale rad analitičarima, koristeći napredne analitičke alate za filtriranje lažnih pozitivnih rezultata i automatski odgovarajući na uobičajene vrste prijetnji.[62], [63], [64]

Još jedan prijedlog bio bi poboljšanje obavještajnih podataka o prijetnjama. Organizacije bi trebale ulagati u kvalitetne izvore informacija o prijetnjama i prilagođavati ih specifičnim potrebama svoje organizacije. Integracija različitih sigurnosnih platformi i upotreba alata za automatizaciju prijetnji, upravljanje alarmima, odgovaranje na incidente i provedbu politika značajno povećavaju učinkovitost. Redovita obuka i razvoj vještina osoblja su ključni za održavanje koraka s najnovijim trendovima i tehnologijama u kibernetičkoj sigurnosti.[62], [63], [64]

Također primjena višerazinskog pristupa odgovoru na incidente bolje raspoređuje resurse i stručnosti, dok proaktivno lovljenje prijetnji poboljšava obrambene sposobnosti organizacije. Poboljšanje komunikacije i suradnje unutar tima te između različitih odjela može povećati produktivnost i osigurati sveobuhvatnu svijest o prijetnjama. Korištenje ključnih pokazatelja izvedbe (KPI) za mjerenje i poboljšanje performansi SOC-a također je važno za kontinuirano poboljšanje.[62], [63], [64]

Kako bi modernizirali SOC da postane što efikasniji moramo uskladiti sigurnosne strategije s poslovnim ciljevima, procjenu trenutne sigurnosne zrelosti, prelazak na zero-trust arhitekturu, usklađivanje s industrijskim standardima i okvirima za detekciju te pojednostavljenje odgovora na incidente. Modernizacija SOC-a ne uključuje samo ulaganje u novu tehnologiju, već i izgradnju pravog tima s odgovarajućim vještinama te razvoj odgovarajućih politika i procesa. Time se osigurava da sigurnosni program podržava poslovne ciljeve i učinkovito se nosi s promjenjivim prijetnjama.[62], [63], [64]

Kako bi se unaprijedila učinkovitost SOC-ova, potrebno je uvesti napredne sustave za detekciju i odgovor na prijetnje (EDR - Endpoint Detection and Response) koji koriste strojno učenje i analizu ponašanja za otkrivanje anomaličnih aktivnosti. Alati poput Falcon Overwatch pokazali su se izuzetno korisnima u ovim područjima, ali njihova integracija s postojećim sustavima mora biti strateška kako bi se maksimizirala njihova učinkovitost. Također, nužno je kontinuirano educirati osoblje kako bi se mogli nositi s novim alatima i prijetnjama, te implementirati redovite revizije sigurnosnih politika i procedura unutar SOC-a.

9. Zaključak

Ovaj završni rad se fokusirao na analizu efikasnosti sigurnosnih operativnih centara (SOC) u detekciji i reakciji na kibernetičke prijetnje. Glavni predmet rada bila je evaluacija SOC-a u kontekstu sve učestalijih i sofisticiranijih cyber napada, te identificiranje ključnih elemenata koji doprinose njihovoj učinkovitosti.

Kroz rad su korišteni različiti metodološki pristupi kako bi se dobilo sveobuhvatno razumijevanje funkcionalnosti SOC-a. Teorijska analiza pružila je temeljno razumijevanje kibernetičkih prijetnji i ključnih operacija unutar SOC-a. Studije slučajeva stvarnih cyber napada ilustrirale su konkretne prijetnje i reakcije SOC-a, dok nam je pregled različitih alata i tehnika, kao što su Falcon Overwatch, Falcon Spotlight, Falcon Intelligence i Akamai Kona Site Defender, omogućio detaljnu evaluaciju njihovih performansi. Na temelju ovog pregleda, organizacije mogu bolje razumjeti kako integrirati te alate u vlastite SOC sustave i maksimizirati njihovu učinkovitost u detekciji i odgovoru na prijetnje.

Rezultati rada pokazali su da su SOC-ovi bitni za pravovremenu detekciju i odgovor na kibernetičke prijetnje. Njihova sposobnost pružanja kontinuiranog nadzora i brzog reagiranja na incidente značajno smanjuje vrijeme oporavka i umanjuje štetu uzrokovanu napadima. Upotreba naprednih alata poput Falcon Overwatch i Akamai Kona Site Defender povećava efikasnost SOC-ova u upravljanju prijetnjama, te omogućuje i automatsku detekciju i odgovor, a samim time i smanjuje potrebu za ručnim intervencijama.

Unatoč značajnim prednostima, SOC-ovi se suočavaju s izazovima poput potrebe za kontinuiranim ažuriranjima i prilagodbama kako bi pratili razvoj novih prijetnji. Preporučeno je uvođenje dodatnih automatiziranih procesa i kontinuirana edukacija osoblja kako bi se održala visoka razina sigurnosti.

Na temelju empirijske analize, organizacije koje daju prednost brzini odgovora na incidente trebale bi razmotriti integraciju sustava sličnih QRadar-u, koji su pokazali superiorne performanse u MTTR-u. Također, ulaganje u alate za automatizaciju poput SOAR platformi koji su se pokazali učinkovitim u smanjenju lažnih alarma pomoći će organizaciji da poveća točnost detekcije, smanji opterećenje analitičara te ubrza ukupni proces odgovora na incidente.

Rad je dokazao nekoliko ključnih pretpostavki. Prvo, potvrđeno je da su SOC-ovi ključni za modernu cyber sigurnost, jer značajno doprinose smanjenju vremena detekcije i odgovora na prijetnje. Drugo, integracija naprednih alata povećava efikasnost SOC-ova, što je potvrđeno

kroz analizu njihovih performansi. Suprotno očekivanjima, ručni pristupi nisu se pokazali adekvatnima za suočavanje sa sofisticiranim prijetnjama, te je automatizacija nužna za učinkovitu obranu.

Rad je potvrdio značajnu ulogu SOC-ova u kibernetičkoj sigurnosti te istaknuo važnost kontinuiranog unapređenja i prilagodbe alata i tehnika koje koriste. Buduća istraživanja trebala bi se fokusirati na razvoj novih tehnologija i metoda koje će dodatno povećati efikasnost SOC-ova u sve kompleksnijem cyber okruženju.

Popis literature

[1] I. Hitrec, “Uvođenje sigurnosnog operacijskog centra za zaštitu poslovanja srednje velike tvrtke,” info:eu-repo/semantics/masterThesis, University of Zagreb. Faculty of Electrical Engineering and Computing. Department of Electronics, Microelectronics, Computer and Intelligent Systems, 2021. Pristupano: 22.svibanj.2024. [Online]. Dostupno: https://urn.nsk.hr/urn:nbn:hr:168:500061

[2] “What is a Cyber Threat? | UpGuard.” Pristupano: 22.svibanj.2024.. [Online]. Dostupno: https://www.upguard.com/blog/cyber-threat

[3] “Cybersecurity Threats | Types & Sources | Imperva,” Learning Center.Pristupano: 22.svibanj.2024. [Online]. Dostupno: https://www.imperva.com/learn/application-security/cyber-security-threats/

[4] “12 Most Common Types of Cyberattacks Today - CrowdStrike,” crowdstrike.com. Pristupano: 22.svibanj.2024. [Online]. Dostupno: https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/

[5] “Security+ (SY0-601) Certification Study Guide | CompTIA IT Certifications,” CompTIA. Pristupano: 22.svibanj.2024. [Online]. Dostupno: https://www.comptia.org/training/books/security-sy0-601-study-guide

[6] “Importance of Security Operations Center (SOC) | SevenMentor.” Pristupano: 27.svibanj.2024. [Online]. Dostupno: https://www.sevenmentor.com/importance-of-security-operations-center-soc

[7] “What Is a Security Operations Center (SOC)? | Trellix.” Pristupano: 22.svibanj.2024. [Online]. Dostupno: https://www.trellix.com/security-awareness/operations/what-is-soc/

[8] “What Is a Security Operations Center (SOC)? | IBM.” Pristupano: 22.svibanj.2024. [Online]. Dostupno: https://www.ibm.com/topics/security-operations-center

[9] M. Chapple and D. Seidl, *CompTIA CySA+ Study Guide: Exam CS0-003*, 3rd edition. Indianapolis: Sybex, 2023.

[10] B. P. Hámornik and C. Krasznay, “A Team-Level Perspective of Human Factors in Cyber Security: Security Operations Centers,” in *Advances in Human Factors in Cybersecurity*, D. Nicholson, Ed., Cham: Springer International Publishing, 2018, pp. 224–236. doi: 10.1007/978-3-319-60585-2_21.

[11] A. A. Mughal, “Building and Securing the Modern Security Operations Center (SOC),” *Int. J. Bus. Intell. Big Data Anal.*, vol. 5, no. 1, Art. no. 1, Jan. 2022.

[12] C. DeCusatis, R. Cannistra, A. Labouseur, and M. Johnson, “Design and Implementation of a Research and Education Cybersecurity Operations Center,” in *Cybersecurity and Secure Information Systems: Challenges and Solutions in Smart Environments*, A. E. Hassanien and M. Elhoseny, Eds., Cham: Springer International Publishing, 2019, pp. 287–310. doi: 10.1007/978-3-030-16837-7_13.

[13] M. Vielberth, F. Bohm, I. Fichtinger, and G. Pernul, “Security Operations Center: A Systematic Study and Open Challenges,” *IEEE Access*, vol. 8, pp. 227756–227779, 2020, doi: 10.1109/ACCESS.2020.3045514.

[14] “ISO/IEC 27035-1:2016(en), Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management.” Pristupano: 1.lipanj.2024. [Online]. Dostupno: https://www.iso.org/obp/ui/#iso:std:iso-iec:27035:-1:ed-1:v1:en

[15] A. Madani, S. Rezayi, and H. Gharaee, “Log management comprehensive architecture in Security Operation Center (SOC),” Oct. 2011, pp. 284–289. doi: 10.1109/CASON.2011.6085959.

[16] A. Shah, R. Ganesan, and S. Jajodia, “A methodology for ensuring fair allocation of CSOC effort for alert investigation,” *Int. J. Inf. Secur.*, vol. 18, no. 2, pp. 199–218, Apr. 2019, doi: 10.1007/s10207-018-0407-3.

[17] M. Vielberth and G. Pernul, “A Security Information and Event Management Pattern,” Nov. 2018.

[18] C. Islam, M. A. Babar, and S. Nepal, “Automated Interpretation and Integration of Security Tools Using Semantic Knowledge,” in *Advanced Information Systems Engineering*, P. Giorgini and B. Weber, Eds., Cham: Springer International Publishing, 2019, pp. 513–528. doi: 10.1007/978-3-030-21290-2_32.
[19] K. Hughes, K. McLaughlin, and S. Sezer, “Dynamic Countermeasure Knowledge for Intrusion Response Systems,” in *2020 31st Irish Signals and Systems Conference (ISSC)*, Jun. 2020, pp. 1–6. doi: 10.1109/ISSC49989.2020.9180198.
[20] C. Islam, M. A. Babar, and S. Nepal, “Architecture-Centric Support for Integrating Security Tools in a Security Orchestration Platform,” in *Software Architecture*, A. Jansen, I. Malavolta, H. Muccini, I. Ozkaya, and O. Zimmermann, Eds., Cham: Springer International Publishing, 2020, pp. 165–181. doi: 10.1007/978-3-030-58923-3_11.
[21] F. Osinga, *Science, strategy and war: the strategic theory of John Boyd*. Delft: Eburon Academic Publishers, 2005.
[22] R. Bidou, J. Bourgeois, and F. Spies, “Towards a Global Security Architecture for Intrusion Detection and Reaction Management,” in *Information Security Applications*, K.-J. Chae and M. Yung, Eds., Berlin, Heidelberg: Springer, 2004, pp. 111–123. doi: 10.1007/978-3-540-24591-9_9.
[23] J. Bourgeois, A. K. Ganame, I. Kotenko, and A. Ulanov, “Software Environment for Simulation and Evaluation of a Security Operation Center,” V. V. Popovich, M. Schrenk, and K. V. Korolenko, Eds., in Lecture Notes in Geoinformation and Cartography. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 111–127. doi: 10.1007/978-3-540-37629-3_8.
[24] “EVALUATION OF THE INTRUSION DETECTION CAPABILITIES AND PERFORMANCE OF A SECURITY OPERATION CENTER:,” in *Proceedings of the International Conference on Security and Cryptography*, Setúbal, Portugal: SciTePress - Science and and Technology Publications, 2006, pp. 48–55. doi: 10.5220/0002101900480055.
[25] S. G. Radu, “Comparative Analysis of Security Operations Centre Architectures; Proposals and Architectural Considerations for Frameworks and Operating Models,” in *Innovative Security Solutions for Information Technology and Communications*, I. Bica and R. Reyhanitabar, Eds., Cham: Springer International Publishing, 2016, pp. 248–260. doi: 10.1007/978-3-319-47238-6_18.
[26] F. Fahad and T. A. Gulliver, “SOCaaS: Security Operations Center as a Service for Cloud Computing Environments,” *Int. J. Cloud Comput. Serv. Sci. IJ-CLOSER*, vol. 3, Jun. 2014, doi: 10.11591/closer.v3i2.6236.
[27] “Colonial Pipeline hack explained: Everything you need to know,” WhatIs. Accessed: Jun. 02, 2024. [Online]. Available: https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know
[28] “What is the Log4j Vulnerability? | IBM.” Accessed: Jun. 02, 2024. [Online]. Available: https://www.ibm.com/topics/log4j
[29] “Cybersecurity lessons from the 2022 LAPSUS$ breaches.” Pristupano: 2.lipanj.2024. [Online]. Dostupno: https://fieldeffect.com/blog/cyber-security-lessons-2022-lapsus-attacks
[30] “theNET | The next era of DDoS attacks.” Pristupano: 3.lipanj.2024. [Online]. Dostupno: https://www.cloudflare.com/the-net/rapid-reset-ddos/
[31] A. S. Ashoor and S. Gore, “Intrusion Detection System (IDS) &Intrusion Prevention System (IPS): Case Study,” vol. 2, no. 7, 2011.
[32] “What is WannaCry ransomware?,” www.kaspersky.com. Pristupano: 3.lipanj.2024. [Online]. Dostupno: https://www.kaspersky.com/resource-center/threats/ransomware-wannacry
[33] S. Bhatt, P. K. Manadhata, and L. Zomlot, “The Operational Role of Security Information and Event Management Systems,” *IEEE Secur. Priv.*, vol. 12, no. 5, pp. 35–41, Sep. 2014, doi: 10.1109/MSP.2014.103.
[34] A. Rabold, “A Guide To Application Logging,” Medium. Pristupano: 8.rujan.2024. [Online].

Dostupno: https://levelup.gitconnected.com/a-guide-to-application-logging-665b4f38e1a6
[35] "System Log." Pristupano: 8.rujan.2024. [Online]. Dostupno: https://help.fortinet.com/fadc/4-2-1/html-e/Content/Logging/System_Log.htm
[36] "Figure 11.Web Firewall log attack in for the testing domain...," ResearchGate. Pristupano: 8.rujan.2024. [Online]. Dostupno: https://www.researchgate.net/figure/Web-Firewall-log-attack-in-for-the-testing-domain-http-wwwsecuritysystemframeworkcom_fig4_327546028
[37] "Equifax data breach FAQ: What happened, who was affected, what was the impact?," CSO Online. Pristupano: 4.lipanj.2024. [Online]. Dostupno: https://www.csoonline.com/article/567833/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html
[38] "Marriott data breach FAQ: How did it happen and what was the impact?," CSO Online. Pristupano: 4.lipanj.2024. [Online]. Dostupno: https://www.csoonline.com/article/567795/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html
[39] "AI-Powered Behavioral Analysis in Cybersecurity | CrowdStrike," crowdstrike.com. Pristupano: 4.lipanj.2024. [Online]. Dostupno: https://www.crowdstrike.com/cybersecurity-101/secops/ai-powered-behavioral-analysis/
[40] A. AlQadheeb, S. Bhattacharyya, and S. Perl, "Enhancing cybersecurity by generating user-specific security policy through the formal modeling of user behavior," *Array*, vol. 14, p. 100146, Jul. 2022, doi: 10.1016/j.array.2022.100146.
[41] J. Heino, A. Hakkala, and S. Virtanen, "Study of methods for endpoint aware inspection in a next generation firewall," *Cybersecurity*, vol. 5, no. 1, p. 25, Sep. 2022, doi: 10.1186/s42400-022-00127-8.
[42] Md. S. Islam, M. A. Uddin, Dr. Md. S. Ahmed, and G. Moazzam, "Analysis and Evaluation of Network and Application Security Based on Next Generation Firewall," *Int. J. Comput. Digit. Syst.*, vol. 13, no. 1, pp. 193–202, Jan. 2023, doi: 10.12785/ijcds/130116.
[43] "Next Generation Firewall and it's Vulnerability | Medium." Accessed: Sep. 08, 2024. [Online]. Available: https://abisec.medium.com/next-generation-firewall-72acf3a2c1a6
[44] "What is Zero Trust Security? Principles of the Zero Trust Model," crowdstrike.com. Pristupano: 4.lipanj.2024. [Online]. Dostupno: https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/
[45] C. Ayuya, "What Are the Benefits and Disadvantages of Zero Trust Security?," Enterprise Networking Planet. Pristupano: 4.lipanj.2024. [Online]. Dostupno: https://www.enterprisenetworkingplanet.com/security/pros-and-cons-of-zero-trust-security/
[46] A. S. George, A. S. H. George, T. Baskar, and D. Pandey, "XDR: The Evolution of Endpoint Security Solutions - Superior Extensibility and Analytics to Satisfy the Organizational Needs of the Future," *Int. J. Adv. Res. Sci. Commun. Technol.*, pp. 493–501, Aug. 2021, doi: 10.48175/IJARSCT-1888.
[47] "What Is XDR? Extended Detection and Response | Trellix." Pristupano: 4.lipanj.2024. [Online]. Dostupno: https://www.trellix.com/security-awareness/endpoint/what-is-xdr/
[48] "View of Extending Detection and Response: How MXDR Evolves Cybersecurity." Pristupano: 4.lipanj.2024. [Online]. Dostupno: https://puiij.com/index.php/research/article/view/97/69
[49] Israa Alsaadi, "Study On Most Popular Behavioral Biometrics, Advantages, Disadvantages And Recent Applications : A Review," 2021, doi: 10.13140/RG.2.2.28802.09926.
[50] D. Jay, "Deception Technology Based Intrusion Protection and Detection Mechanism for Digital Substations: A Game Theoretical Approach," *IEEE Access*, vol. 11, pp. 53301–53314, 2023, doi: 10.1109/ACCESS.2023.3279504.
[51] "IBM QRadar Security Intelligence Platform 7.4." Pristupano: 10.lipanj.2024. [Online]. Dostupno: https://www.ibm.com/docs/en/qsip/7.4?topic=qradar-getting-started-security-analysts
[52] "What is CrowdStrike? FAQ | CrowdStrike," crowdstrike.com. Accessed: Jun. 10, 2024.

[Online]. Available: https://www.crowdstrike.com/products/faq/
[53] “https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWBnqk.” Pristupano: 10.lipanj.2024. [Online]. Dostupno: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWBnqk
[54] A. K, “What is Tenable and use cases of Tenable?,” DevOpsSchool.com. Pristupano: 10.lipanj.2024. [Online]. Dostupno: https://www.devopsschool.com/blog/what-is-tenable-and-use-cases-of-tenable/
[55] “Vectra AI: The Power of AI Threat Detection - Core To Cloud,” https://www.coretocloud.co.uk/. Pristupano: 10.lipanj.2024. [Online]. Dostupno: https://www.coretocloud.co.uk/vectra-ai-the-power-of-ai-threat-detection/
[56] M. C. Ltd, “Understanding SOC Operations and Processes | Microminder Cybersecurity | Holistic Cybersecurity Services,” Microminder Cybersecurity. Pristupano: 11.lipanj.2024. [Online]. Dostupno: https://www.micromindercs.com/blog/soc-operations-and-processes
[57] “SOC Processes, Operations, Challenges, and Best Practices - Sapphire.net.” Pristupano: 11.lipanj.2024. [Online]. Dostupno: https://www.sapphire.net/insights/soc-processes/
[58] E. Sayegh, “Signs of an Inadequate Security Operations Center,” Forbes. Pristupano: 11.lipanj.2024. [Online]. Dostupno: https://www.forbes.com/sites/emilsayegh/2023/10/10/signs-of-an-inadequate-security-operations-center/
[59] “The top 5 challenges faced by Security Operations Centers,” Sumo Logic. Pristupano: 11.lipanj.2024. [Online]. Dostupno: https://www.sumologic.com/blog/the-top-5-challenges-faced-by-security-operations-centers/
[60] “Splunk Enterprise Security vs. IBM Security QRadar SIEM,” Splunk. Pristupano: 8.kolovoz.2024. [Online]. Dostupno: https://www.splunk.com/en_us/solutions/splunk-vs-ibm-qradar.html
[61] T. C. Club, “IBM Security QRadar SIEM In Depth Review,” The CTO Club. Pristupano: 8.kolovoz.2024. [Online]. Dostupno: https://thectoclub.com/tools/ibm-security-qradar-siem-review/
[62] N. Hewitt, “Ten Simple Steps to Improve SOC Efficiency • TrueFort,” TrueFort. Accessed: Jun. 11, 2024. [Online]. Available: https://truefort.com/improve-soc-efficiency/
[63] “How to Improve Your Security Operations Center.” Pristupano: 11.lipanj.2024. [Online]. Dostupno: https://www.linkedin.com/pulse/how-improve-your-security-operations-center-robert-bond-w9l3c
[64] “5 Tips for Modernizing Your Security Operations Center Strategy.” Pristupano: 11.lipanj.2024. [Online]. Dostupno: https://www.darkreading.com/vulnerabilities-threats/5-tips-for-modernizing-your-security-operations-center-strategy

Popis slika

Popis tablica