Primjena Microsoft sigurnosnih rješenja u digitalnoj forenzičkoj analizi

Oštrić, David Ivan

Master's thesis / Diplomski rad

2022

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Transport and Traffic Sciences / Sveučilište u Zagrebu, Fakultet prometnih znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:119:681699

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-28**



Repository / Repozitorij:

Faculty of Transport and Traffic Sciences - Institutional Repository







SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

David Ivan Oštrić

PRIMJENA MICROSOFT SIGURNOSNIH RJEŠENJA U DIGITALNOJ FORENZIČKOJ ANALIZI

DIPLOMSKI RAD

Zagreb, 2022.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
POVJERENSTVO ZA DIPLOMSKI ISPIT

Zagreb, 4. svibnja 2022.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Forenzička analiza informacijsko komunikacijskog sustava**

DIPLOMSKI ZADATAK br. 6767

Pristupnik: **David Ivan Oštrić (0135223955)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Primjena Microsoft sigurnosnih rješenja u digitalnoj forenzičkoj analizi**

Opis zadatka:

Prikazati značajke forenzičke analize sustava u oblaku. Pojasniti regulatorne aspekte prikupljanja podataka iz sustava u oblaku. Identificirati karakteristike Microsoft XDR i SIEM sigurnosnih rješenja. Objasniti mogućnosti primjene Microsoft XDR i SIEM rješenja u digitalnoj forenzici. Opisati provedbu digitalne forenzičke analize.

Mentor:

doc. dr. sc. Siniša Husnjak

Predsjednik povjerenstva za diplomski ispit:

Sveučilište u Zagrebu
Fakultet prometnih znanosti

DIPLOMSKI RAD

Primjena Microsoft sigurnosnih rješenja u digitalnoj forenzičkoj analizi

Application of Microsoft Security Solutions in Digital Forensic Analysis

Mentor: doc. dr. sc. Siniša Husnjak

Student: David Ivan Oštrić
JMBAG: 0135223955

Zagreb, kolovoz, 2022.

ZAHVALA

Ovim putem iznimno se zahvaljujem na prilici i susretljivosti, uloženom vremenu i usmjeravanju te svim stručnim savjetima od strane mentora doc. dr. sc Siniše Husnjaka uz čiju je podršku izrađen ovaj diplomski rad.

Zahvalu upućujem i Zavodu za informacijsko komunikacijski promet te svim njenim djelatnicima čija je misija, vizija i način prenošenja znanja oblikovala moj pogled na svijet i pružila mi sve potrebno za daljnji profesionalni razvoj.

Na kraju, od srca zahvaljujem svojoj obitelji, djevojci i prijateljima čija je podrška i motivacija uvijek bila prisutna neovisno koliko je u pojedinim trenutcima bilo teško.

SAŽETAK

Ovaj diplomski rad prikazuje značajke digitalne forenzičke analize sustava u oblaku. Razvoj usluga u oblaku doprinio je stalnoj dostupnosti informacija, pristup s raznih uređaja i s bilo koje lokacije. Unatoč prednostima koje usluge u oblaku donose, pojavili su se i mnogobrojni sigurnosni rizici. Digitalna forenzička analiza razvijena je za specifične potrebe otkrivanja digitalnih elektroničkih dokaza i konstruiranja događaja. U kontekstu oblaka, dizajnirana je zasebna grana koja se njime bavi, a uzevši u obzir kontinuirani napredak i ekspanziju usluga u oblaku, postojeće metodologije i način pristupa provođenju forenzičke analize neprestano se usavršava. Ipak, forenzika usluga u oblaku svakodnevno se susreće s raznim izazovima. Jedan od ključnih izazova manifestira se kroz dinamičan smještaj i transfer podataka diljem različitih mreža i pravnih nadležnosti. Takva rasprostranjenost podataka značajno otežava prikupljanje digitalnih dokaza. Kako bi se otklonili spomenuti izazovi, razvijeni su moderni, unificirani programski alati koji omogućuju napredan pristup i provođenje digitalne forenzičke analize.

Ključne riječi: digitalna forenzika; forenzičke istrage; ekstrakcija podataka; oblak; istraga oblaka; forenzički alat; Microsoft; XDR; SIEM

SUMMARY

This master's thesis shows the features of digital forensic analysis of cloud systems. The development of cloud services has contributed to the constant availability of information, and access from various devices and any location. Many security risks have been recognized despite the benefits of cloud services. Digital forensic analysis has been developed for the specific purpose of detecting digital electronic evidence and construction of events. In the context of the cloud, a separate branch of digital forensics has been designed to deal with challenges of cloud services, existing methodologies, and the approach to forensic analysis. Nevertheless, the forensics of cloud services faces various challenges every day. One of the key challenges is recognized through dynamic storage and data transfer across different networks and legal jurisdictions. Such a prevalence of data significantly makes it difficult to collect digital evidence. To overcome the challenges, modern and unified software tools have been developed that enable advanced access and conducting of digital forensic analysis.

Keywords: digital forensics; forensic investigations; data extraction; cloud; cloud investigation; forensic tool; Microsoft; XDR; SIEM

Sadržaj

1. UVOD 1
2. ZNAČAJKE FORENZIČKE ANALIZE SUSTAVA U OBLAKU 3
   2.1. Vrste i modeli sustava u oblaku 4
   2.2. Primarni fokus forenzičke analize sustava u oblaku 6
   2.3. Modeli forenzičke istrage oblaka 8
   2.4. Proširivanje funkcionalnosti postojećih forenzičkih alata u oblak 10
3. REGULATORNI ASPEKTI PRIKUPLJANJA PODATAKA IZ SUSTAVA U OBLAKU 12
   3.1. Pružatelji usluga u oblaku 12
   3.2. Izazovi forenzike u oblaku 14
   3.3. Dokazni materijali prikupljeni iz oblaka 17
4. KARAKTERISTIKE MICROSOFT XDR I SIEM SIGURNOSNIH RJEŠENJA 20
   4.1. XDR 21
      4.1.1. Svrha XDR rješenja 21
      4.1.2. Ključne značajke 22
   4.2. SIEM 24
      4.2.1. Svrha SIEM rješenja 24
      4.2.2. Ključne značajke 25
      4.2.3. Napredne značajke 26
   4.3. Unificiranost zaštite u oblaku 29
5. MOGUĆNOSTI PRIMJENE MICROSOFT XDR I SIEM RJEŠENJA U DIGITALNOJ FORENZICI 31
   5.1. Područja 32
      5.1.1. Računalna forenzika 33
      5.1.2. Mrežna forenzika 34
      5.1.3. Forenzika mobilnih uređaja 37
      5.1.4. Email forenzika 39
      5.1.5. Forenzika dokumenata 42
   5.2. Lanac posjeda dokaza u oblaku 44
   5.3. Pretraga podataka u oblaku 46
6. PROVEDBA DIGITALNE FORENZIČKE ANALIZE 48
   6.1. Očuvanje 49
   6.2. Identifikacija 50
   6.3. Prikupljanje 51

6.4. Analiza 53
6.5. Prezentiranje 57
6.6. Verifikacija 58
7. ZAKLJUČAK 59
Literatura 60
Popis kratica i akronima 65
Popis grafičkih prikaza 67
Popis slika 67
Popis tablica 68

1. UVOD

Digitalizacija radnih procesa dovela je do digitalizacije svijeta. U tom sveprožimajućem procesu transformacije, ključnu je ulogu odigrao revolucionarni koncept, popularno nazvan „oblak." Zbog lakoće usvajanja tehnologije, znatno nižih troškova održavanja i veće učinkovitosti rada, računarstvo u oblaku zamijenilo je tradicionalni način poslovanja i korištenja IT sustava. Brojne organizacije, tvrtke i privatni subjekti preorijentirali su svoj dotadašnji način pohrane, arhiviranja i upravljanja podacima u lokalnoj infrastrukturi. Također, počinju koristiti i dijeliti usluge koje omogućuju pružatelji usluga u oblaku. Paralelno s razvojem oblaka, korisnicima postaju dostupne i sve infrastrukturne komponente IT sustava. No one korisnicima više nisu fizički dohvatljive, već se nalaze u podatkovnim centrima disperziranim diljem svijeta. Prednosti korištenja oblaka u poslovanju su neosporive, no neosporivi su i statistički podaci koji ukazuju na povećanje kibernetičkih napada sustava u oblaku. Ti napadi rezultiraju nezanemarivim financijskim gubitcima, krađom podataka i identiteta, korporativnim špijunažama i drugim kriminalnim aktivnostima. U tim se okolnostima javlja povećana potražnja za digitalnim forenzičarima, no tradicionalna digitalna forenzika te njezini alati i metodologije u slučaju istraga u oblaku nisu pokazale zadovoljavajuću učinkovitost. Na pomolu se pojavljuju brojni izazovi pravne, tehničke i organizacijske prirode, problemi vezani isključivo uz okruženja oblaka. Započinje tako strelovit uspon poddiscipline digitalne forenzike, nazvane digitalna forenzika u oblaku. Posljednje desetljeće iscrpno se radi na formiranju novih metodologija istrage, prilagođenih sustavu oblaka sa svim njegovim jedinstvenostima poput fizičke dislociranosti, skalabilnosti, dijeljenja resursa, ali i dijeljenja odgovornosti između krajnjih korisnika i pružatelja usluga u oblaku. Digitalni forenzički istražitelji u praksi su se tako susreli s nizom novih izazova, nepoznatih tradicionalnoj digitalnoj forenzici, a koji su zahtijevali urgentno pronalaženje odgovarajućih rješenja.

U ovom će se radu zato prikazati svi aspekti digitalne forenzike u oblaku, počevši od detektiranja razlika između modernog i tradicionalnog pristupa digitalne forenzičke istrage, pa sve do primjene progresivnih XDR i SIEM rješenja na primjeru studije slučaja.

Rad se sastoji od osam poglavlja:

1. Uvod
2. Značajke forenzičke analize sustava u oblaku
3. Regulatorni aspekti prikupljanja podataka iz sustava u oblaku
4. Karakteristike Microsoft XDR i SIEM sigurnosnih rješenja
5. Mogućnosti primjene Microsoft XDR i SIEM rješenja u digitalnoj forenzici
6. Provedba digitalne forenzičke analize
7. Zaključak

Drugo je poglavlje posvećeno pregledu postojećih vrsta i modela sustava u oblaku te njihovih karakterističnosti, ali i razjašnjavanju fokusa forenzičkih analiza u oblaku. U trećem se poglavlju raspravlja o pružateljima usluga u oblaku i njihovom odnosu s krajnjim korisnicima. Riječ je o tzv. modelu dijeljene odgovornosti (engl. *Shared Responsibility Model*) koji bitno utječe na sam proces forenzičke istrage. Istaknuti će se odgovornosti jedne i druge strane, ali i to zašto je kooperacija ključ uspješne istrage. U tom će se poglavlju još podrobno predstaviti i nezaobilazni izazovi pravne, tehničke i organizacijske prirode s kojim se susreću svi digitalni forenzičari, ali i kako i pod kojih uvjetima podaci prikupljeni istragom postaju sudski dokazni materijali. Četvrto se poglavlje bavi eksplikacijom ukupne svrhe XDR i SIEM sigurnosnih rješenja. Također, opisat će se njihove karakteristike i nabrojati pripadajući im alati različitih funkcionalnosti. Sljedeće poglavlje nudi pregled primjenjivosti Microsoft XDR i SIEM rješenja u različitim područjima djelovanja digitalne forenzike. Govorit će se o djelotvornosti navedenih u računalnoj i mrežnoj forenzici, forenzici mobilnih uređaja, e-mail forenzici i forenzici dokumenata. Posljednje poglavlje svojevrsna je studija slučaja tijekom koje će se ispitivati učinkovitost rješenja kroz simulirani napad na IT sustav u oblaku. Također, ispitati će se mogućnosti, benefiti i dosezi programskih alata u oblaku. Krajnji je cilj ovog istraživanja prikazati kompleksnost okoline u oblaku i eksplicirati regulatorne aspekte akvizicije podataka u provođenju forenzičke analize sustava. Predočiti na koji način moderni forenzički alati identificiraju, prikupljaju i analiziraju podatke te kako utječu na razvoj postojećih metodologija i načine provođenja forenzičke analize sustava u oblaku.

2. ZNAČAJKE FORENZIČKE ANALIZE SUSTAVA U OBLAKU

Usluge u oblaku promijenile su dosadašnje načine korištenja IT usluga, komunikacije, pohrane digitalnih informacija i omogućile rad na daljinu. U tim novonastalim okolnostima, lokalna pohrana vrijednih informacija i podataka počinje se smanjivati u korist trenda pohrane sadržaja na oblak. Zahvaćena tom globalnom digitalnom transformacijom, digitalna forenzika kao disciplina forenzičkih znanosti, bila je primorana proširiti sferu svog djelovanja. Unatoč svim pokušajima unaprjeđenja nekadašnjih standardiziranih postupaka, metoda i načina provođenja forenzičkih analiza, usluge u oblaku nepovratno su promijenile fokus forenzičkih istražitelja. U tim okolnostima do izražaja dolazi nekad zanemarena poddisciplina digitalne forenzike, digitalna forenzika oblaka. Digitalna forenzika oblaka temelji se na uporabi forenzičkih postupaka koji se sada primjenjuju na informacije pohranjene u oblak. No priroda sustava u oblaku nije statična, već se oblak neprestano usavršava i modificira prema sve većim zahtjevima korisnika. To posljedično vodi potrebi za kontinuiranim razvojem, adaptacijom i kreiranjem novih metodologija forenzike oblaka koja se suočava sa sve brojnijim izazovima.

U suvremenom dobu, okruženi smo digitalnim dokazima koji imaju ključnu ulogu u forenzičkim istragama. Za provođenje forenzičkih analiza u oblaku, neophodno je poznavanje i razumijevanje vrsta te modela sustava koji se nalaze u oblaku, a o kojima će biti više riječi u sljedećim poglavljima. Također, unatoč postojećem standardu i normiranim smjernicama za provedbu istrage, bitno je istaknuti kako se primarni fokus forenzičkih analiza promijenio. Tadašnji modeli provedbe forenzičkih istraga počinju gubiti na važnosti, a rastuće mogućnosti oblaka trajno mijenjaju tradicionalne protokole istrage. Primjetni su i iznimni napori povezani s produženim vremenskim trajanjem analiza velikih količina podataka sa starim, danas granično adekvatnim forenzičkim alatima.

2.1. Vrste i modeli sustava u oblaku

Konceptualno, oblak je zamišljen kao proširenje postojećih fizičkih IT sustava dizajniran za potrebe privatnih i javnih korisnika. Sukladno potrebama tržišta, razvijene su različite vrste računarstva u oblaku. To su privatni, javni, hibridni i višestruki oblak. Svi oni razlikuju se po svojoj strukturi, namjeni i uslugama koje pružaju krajnjim korisnicima. Privatni oblak je izolirana okolina u vlasništvu tvrtke koja ju koristi ili ustupa samo pojedinoj skupini korisnika. Okolina se nalazi zaštićena iza vatrozida. Privatne okoline u oblaku više ne moraju biti isključivo *on-premise*[1] odnosno unutar same tvrtke. Danas one mogu biti locirane i izvan tvrtke u podatkovnim centrima ili na drugim udaljenim lokacijama. Privatni oblak također se dijeli na dvije vrste, a to su: a) upravljani privatni oblaci – unaprijed raspoređeni, konfigurirani i upravljani od strane trećeg vlasnika i b) namjenski oblaci – oblak unutar oblaka, poput namjenskog privatnog oblaka smještenog unutar javnog. Za razliku od privatnih oblaka, javni oblaci u vlasništvu su velikih organizacija poput Google cloud, IBM cloud, Microsoft Azure, Amazon web services, itd. Temeljna razlika između privatnih i javnih oblaka očituje se u vlasništvu, strukturi, dostupnim funkcionalnostima i dostupnosti.

Kako bi se nadomjestili nedostatci privatnih i javnih oblaka, osmišljen je hibridni. Privatni oblaci karakterizirani su visokom razinom sigurnosti, fleksibilnosti i prilagodljivosti, no nedostaju im skalabilnost, iskoristivost, neograničenost pohrane i smanjeni troškovi ulaganja koje su karakteristične za javni oblak. Hibridni oblak ima osobine oba prethodno opisana sustava i smatra se kompleksnom okolinom. Njegova kompleksnost leži u mogućnosti povezivanja različitih sustava u oblaku. To može biti povezivanje jednog privatnog oblaka i jednog javnog oblaka, dva ili više privatna oblaka, dva ili više javna oblaka ili tzv. „bare-metal."[2] Čak ni hibridni oblaci ne omogućavaju sve usluge nužne poslovanju pojedinih organizacija. Osmišljeni su zato višestruki oblaci koji ujedinjavaju više od jednog oblaka, neovisno bili oni javni ili privatni ili kombinacija jednih i drugih. Bitno je istaknuti kako su hibridni oblaci sami po sebi višestruki oblaci jer spajaju privatne i javne, no višestruki oblaci ne moraju biti hibridni zbog niza različitih mogućnosti integracija, [1].

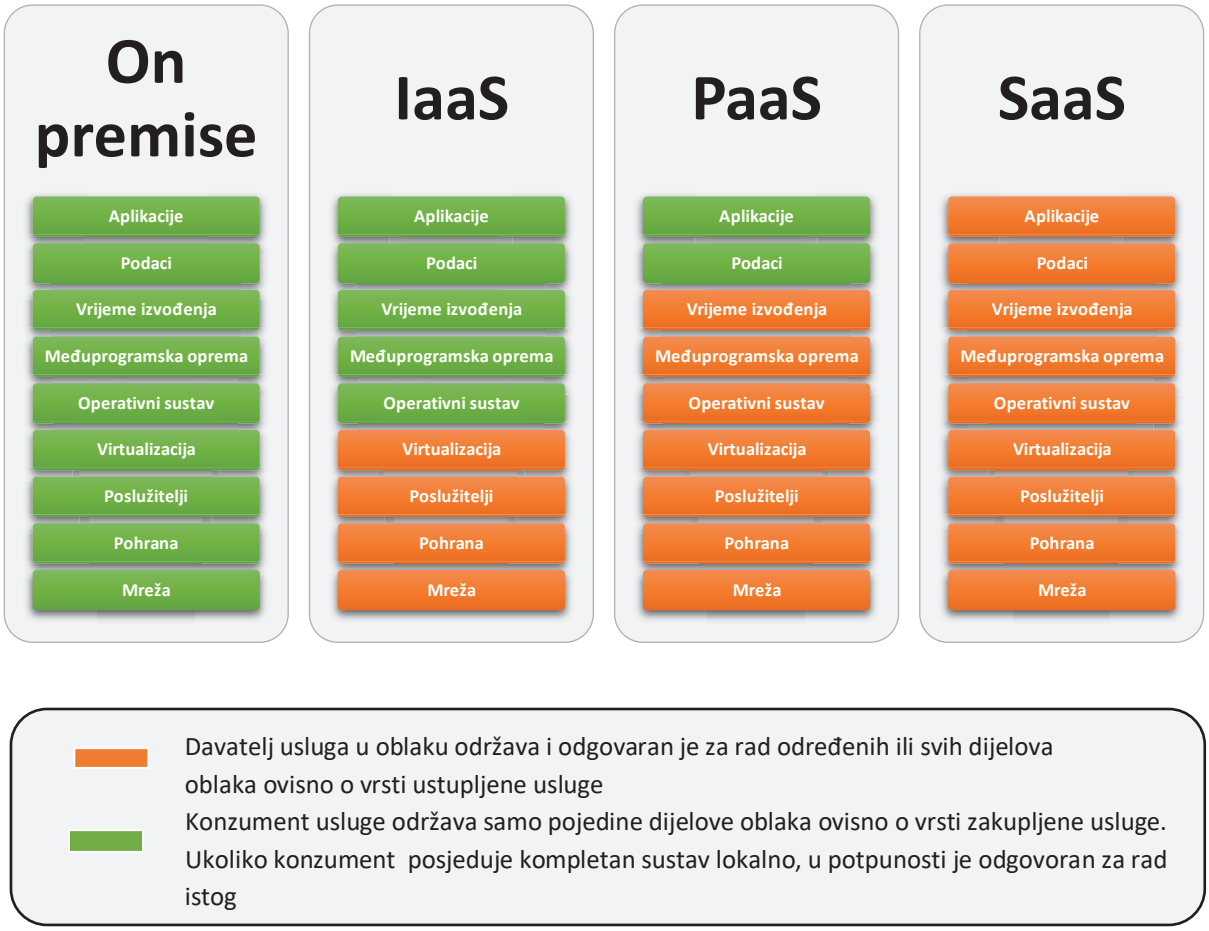
Pod pojam okoline u oblaku podrazumijevamo jedan od tri standardna modela unutar kojih su sadržani definirani setovi usluga. Prvi model, *infrastruktura kao usluga* ili kratko IaaS (engl. *Infrastructure as a Service*), odnosi se na resurse nižih razina koje je neophodno posjedovati za potrebe IT sustava. Pod pojmom resursi, primarno se misli na korištenje virtualizacijskih tehnologija koje omogućuju virtualna računala i poslužitelje. Ostali infrastrukturni resursi podrazumijevaju pohranu, mrežu i konačno platformu za upravljanje i nadzor. Drugi model karakteriziraju mogućnosti na višoj razini te uključuje cijeli infrastrukturni dio, operativni sustav, ali i servise potrebne za razvoj aplikacija ili hosting-a. Naziva se

[1] On premise – engl. pojam koji označava određenu informatičku opremu odnosno resurse sustava koji se fizički nalaze na određenoj lokaciji te su u vlasništvu pojedinca ili tvrtke

[2] Bare-metal – engl. pojam koji označava virtualnu okolinu povezanu s barem jednim javnim ili privatnim oblakom

platforma kao usluga ili kratko PaaS (engl. *Platform as a Service*). Posljednji model bazira se isključivo na korištenju određenog programskog rješenja od kojeg potječe i sam naziv, *softver kao usluga* ili kratko SaaS (*engl*. *Software as a Service*), [2].

Svaki od tri moguća modela ima i različito definiran stupanj odgovornosti (engl. *Shared Responsibility Model*). Odgovornost se dijeli između davatelja usluge ili kratko CSP-a (engl. *Cloud Service Provider*) te krajnjeg korisnika. Stupanj odgovornosti unaprijed je definiran ugovorom kojeg klijentu predlaže davatelj usluge, a pod njime se podrazumijevaju sve radnje koje je potrebno poduzeti kako bi bila podržana i omogućena određena usluga u oblaku. Na Slika 1. u nastavku, vizualno je prikazana komparacija triju standardnih modela sustava u oblaku te posjedovanja kompletnog sustava *on-premise* tj. lokalno. Odgovornost između davatelja usluga i klijenata predstavljena je kroz devet razina koji opisuju sustave u oblaku, [3].



Slika 1. Komparacija modela usluga u oblaku i privatnog oblaka
Izvor: [4]

2.2. Primarni fokus forenzičke analize sustava u oblaku

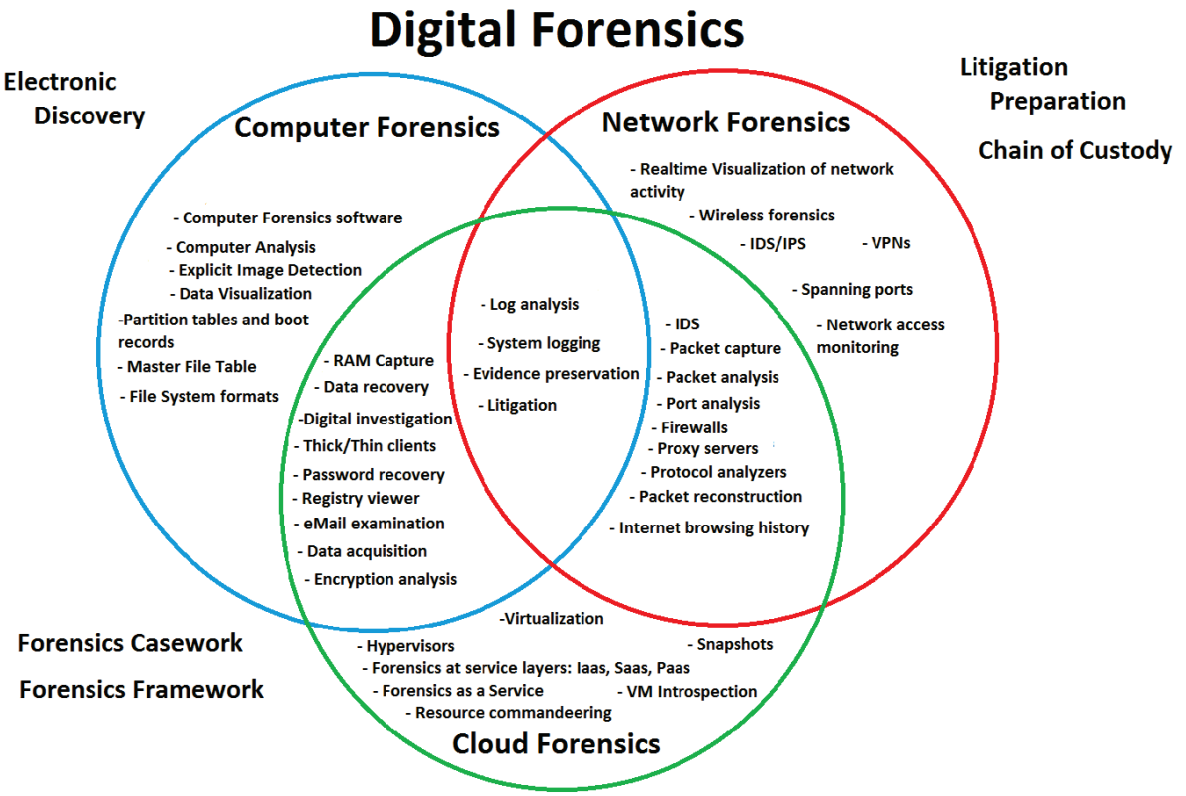
Kako bi se definirala forenzika sustava u oblaku, neophodno je poznavati temelje tradicionalne digitalne forenzike i njenu podjelu. Digitalna forenzika je primjena znanstvenog pristupa usmjerenog identifikaciji, prikupljanju, ispitivanju i analizi podataka čuvajući integritet podataka i održavajući lanac posjeda dokaza, [5]. Konvencionalni forenzički alati i pristupi prilikom provođenja forenzičke istrage temelje se na prikupljanju digitalnih dokaza iz uobičajenih komponenti informacijski sustava. Ono ovisi o disciplini digitalne forenzike, prema čemu razlikujemo četiri osnovne:

1) Računalnu forenziku čiji je fokus na prikupljanju podataka iz komponenti računala kao što su diskovi, radne memorije, USB memorije, vanjski diskovi, SD kartice, itd.
2) Mrežnu forenziku čiji je fokus na prikupljanju podataka iz mrežnog prometa, odnosno podataka unutar lokalne mreže
3) Forenziku mobilnih uređaja čiji je fokus na fizičkoj ekstrakciji podataka iz mobilnih uređaja
4) Forenziku baza podataka koja se temelji na ekstrakciji i analizi kompletne baze iz pojedinog poslužiteljskog računala

Navedeni čine osnovnu podjelu, no digitalna se forenzika grana i u niz poddisciplina. To su: forenzika oblaka, email forenzika, forenzika podataka, dokumenata, društvenih mreža, IoT uređaja, itd. Neovisno o disciplini digitalne forenzike, sve forenzičke istrage podrazumijevaju provedbu četiri temeljne faze, odnosno, prikupljanje, ispitivanje, analizu podataka i izvještavanje. Proces digitalne forenzike oblaka u svojim se osnovnim fazama bitno ne razlikuje od tradicionalne forenzike, ali značajno odudara u pristupu i načinu provođenja tih procesa. Digitalna forenzika u oblaku u kontinuiranom je razvoju te nastoji pratiti razvoj usluga u oblaku koji se svakodnevno mijenja i prilagođava potrebama tržišta. Oblak kao virtualno okruženje značajno je smanjio potrebu za fizičkim ekstrahiranjem podataka s podatkovnih diskova, radnih memorija i potrebu za analizom lokalne mreže. Sve esencijalne komponente nad kojima se nekada provodilo prikupljanje podataka, danas mogu biti virtualizirane, dijeljene te dostupne raznim korisnicima na različitim geopolitičkim lokacijama, [6].

Moderna digitalna forenzika u oblaku, prema NIST-u, definira se kao „[...] primjena znanstvenih načela, tehnoloških praksi i dokazanih metoda za obradu prošlih događaja unutar sustava u oblaku, koristeći se pritom identifikacijom, prikupljanjem, čuvanjem, ispitivanjem i izvješćivanjem o digitalnim podacima u svrhu olakšavanja rekonstrukcija tih događaja.“

Na Slika 2. prikazanoj u nastavku, ilustrirana je povezanost računalne i mrežne forenzike kao osnovnih disciplina s forenzikom u oblaku koja danas obuhvaća većinu komponenti modernog IT sustava, [7].



Slika 2. Komplementarnost forenzike u oblaku s mrežnom i računalom forenzikom, [8]

Prilikom provođenja digitalne forenzičke istrage oblaka, neovisno o njegovoj vrsti, potrebno se držati osnovnih forenzičkih zadataka:

1) Određivanje svrhe istrage oblaka
2) Određivanje vrste usluge u oblaku (SaaS, IaaS, PasS..)
3) Određivanje vrsta tehnologija koje se koriste u oblaku
   (3 dodatne podjele – klijentska strana, serverska strana, programerska strana)
4) Provođenje istrage, [6]

U skladu sa složenim zahtjevima koje je oblak postavio pred digitalne forenzičare, bilo je potrebno osmisliti nove modele koji usmjeravaju tijek forenzičke istrage tijekom svih faza provedbe, o čemu će više riječi biti u nadolazećem poglavlju.

2.3. Modeli forenzičke istrage oblaka

Digitalna forenzika, od svojih se začetaka temelji na specifično oblikovanim modelima i smjernicama koje usmjeravaju tijek digitalne forenzičke istrage od njenog početka do samoga kraja. Nastajanje prvih, danas već tradicionalnih modela provođenja digitalne forenzičke istrage, seže u 90.-te godine dvadesetog stoljeća. U nastavku su nabrojani široko prepoznati i učestalo korišteni modeli digitalne forenzike od strane digitalnih forenzičara. To su:

- CFIP (engl. *Computer Forensic Investigative Process*)
- DFRWS (engl. *Digital Forensics Research Workshop*)
- ADFM (engl. *Abstract Digital Forensics Model*)
- IDIP (engl. *Integrated Digital Investigation Process*)
- EIDIP (engl. *Enhanced Integrated Digital Investigation Process*)
- CFFTPM (engl. *Computer Forensic Field Triage Process Model*)
- FDFI (engl. *Framework for a Digital Forensic Investigation*)
- DFMMIP (engl. *Digital Forensic Model based on Malaysian Investigation Process*)
- SRDFIM (engl. *Systematic Digital Forensic Investigation Model*)
- IDFPM (engl. *Integrated Digital Forensic Process*)
- ACSPM (engl. *Analytical Crime Scene Procedure Model*)
- ADAM (engl. *Advanced Data Acquisition Model*)

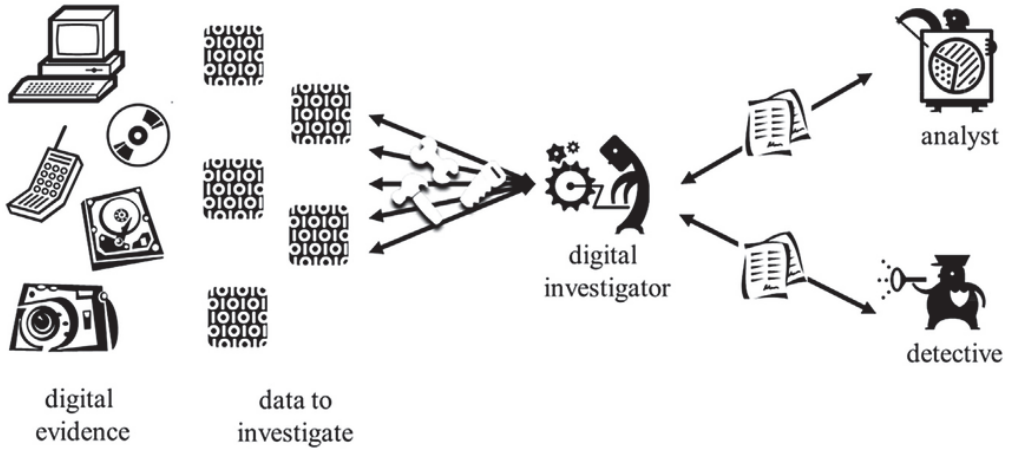
Noviji modeli, prilagođeni sustavima u oblaku razvijaju se od 2010.-te pa sve do danas. Prepoznati su:

- ICDFFCC (engl. *Integrated Conceptual Digital Forensic Framework for Cloud Computing*)
- OCFM (engl. *Open Cloud Forensics Model*)
- CFCMM (engl. *Cloud Forensics Capability Maturity Model)*
- DFaaS (engl. *Digital Forensics as a Service*), [9]

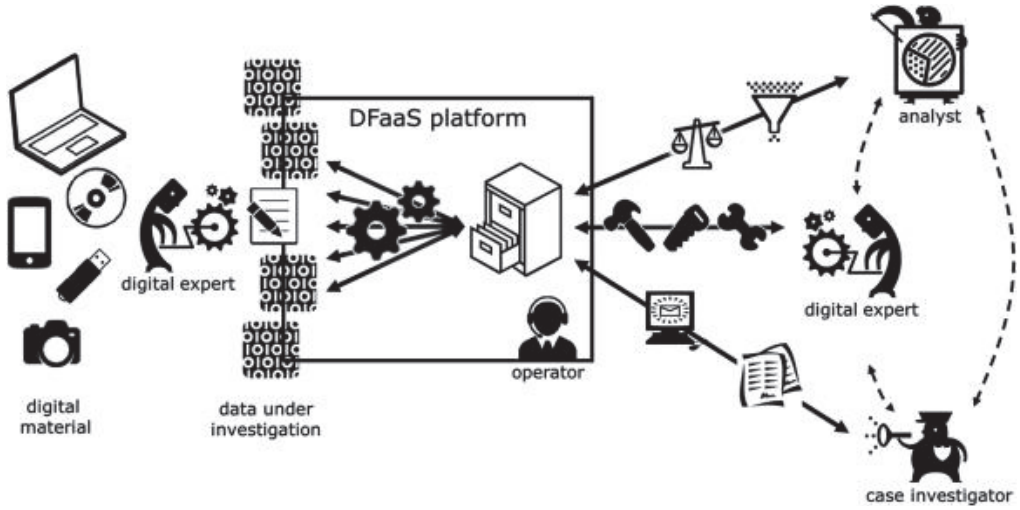
Fokus ovog rada je usmjeren na prikaz aktualnih modela digitalnih forenzičkih istraga oblaka, od kojih je dodano vrijedno istaknuti model DFaaS koji se permanentno razvija. Koncept same metode predložen je prije desetak godina od strane nekolicine studenata i profesora Odjela za računalne znanosti na Sveučilištu u Houstonu. Izdvaja ga postojanje specifično prilagodljive okoline u oblaku kojoj je osnovna svrha obrada velikih količina podataka s ciljem olakšavanja i ubrzavanja faze analize. Također, predložen je kao otvoreni sustav koji bi pružio razne alate, upute i vještine drugim forenzičkim istražiteljima. Osim toga, posjeduje povijest obrađenih podataka te iste stoga više nije potrebno duplicirati na samom oblaku. Model se smatra vizionarskim projektom, no unatoč tome, još nije uspio prevladati određene izazove. Primjer jednog od ključnih izazova je limitiranost brzine izvoza podatka s fizičkih diskova u DFaaS okolinu u oblaku. Pored brzine diskova, neophodno je spomenuti i

regulatorni aspekt prikupljanja podataka i sve sudionike koji potencijalno mogu uskratiti dio podataka za izvoz iz postojeće okoline u oblaku, [10].

Na Slika 3. i Slika 4. prikazana je komparacija tradicionalnog pristupa digitalnoj forenzici i stari model digitalne forenzičke istrage u odnosu na novi DFaaS model.



Slika 3. Grafički prikaz tradicionalnog modela digitalne forenzičke istrage, [11]



Slika 4. Grafički prikaz modernog DFaaS modela digitalne forenzičke istrage, [10]

Na temelju konceptualnog modela DFaaS-a, skupina digitalnih forenzičara i članova Instituta za forenziku u Nizozemskoj patentirala je otvorenu digitalnu forenzičku DFaaS uslugu u oblaku zvanu *Hansken*. Prema članku „Digital forensics as a service: Stepping up the game“ autora van Beeka et al., od inicijalnog razvoja pa do polovice 2020.-te godine pomoću Hansken platforme napravljeno je preko 1000 digitalnih istraga, s preko 100 TB neobrađenih podataka i 100 milijuna identificiranih tragova. Daljnji razvoj DFaaS modela postaje neupitan. Novi model za cilj ima kombinaciju iskustava, zajedničkih istraga, uključivanje svih sudionika u faze istrage, proširenje postojećih i dijeljenje znanja te poticanje na suradnju neovisno o udaljenosti, [12].

2.4. Proširivanje funkcionalnosti postojećih forenzičkih alata u oblak

Svaki oblik hardvera i softvera koji omogućuje provođenje forenzičke istrage naziva se forenzički alat. Potrebno je istaknuti kako se tradicionalna digitalna forenzika oslanjala na pojedine uređaje, komponente, mreže, baze unutar određenog informacijskog sustava. Rastućim razvojem interneta kao jedinstvene javne mreže i razvojem računalstva u oblaku, dosadašnji *on-premise* resursi, neophodni za rad informacijskog sustava razvijaju se i pružaju na korištenje u obliku usluga u oblaku. Navedeno je dovelo do drastičnih promjena u percepciji pribavljanja potrebnih resursa, ali i njihova korištenja, te naposljetku i u provođenju digitalne forenzičke istrage. Zbog naravni računarstva u oblaku, odnosno distribuiranosti, zajedničkog korištenja, skalabilnosti, povezanosti s postojećom *on-premise* opremom i općenito dostupnošću, postojeće tradicionalne metode i alati za provođenje forenzičke istrage postali su zastarjeli i nedovoljno učinkoviti. Kako bi se nadišle nastale razlike i u skladu s time nadogradili postojeći alati, tradicionalna digitalna forenzika bila je primorana pratiti moderne trendove i korištenje računarstva u oblaku te integrirati forenziku oblaka kao jednu od primarnih disciplina, [13].

Iako razvoj alata za provedbu digitalne forenzike u oblaku nastoji biti u korak s vremenom, poddisciplina se susrela s brojnim svojevrsnim izazovima. Prema Nacionalnom institutu za standarde i tehnologiju, glavni izazovi forenzike u oblaku kategorizirani su u devet glavnih skupina. Prva skupina podrazumijeva arhitekturu, odnosno njenu raznolikost, složenost, podrijetlo, višenamjensku djelatnost i segregaciju podataka. Druga skupina odnosi se na prikupljanje podataka što uključuje integritet podataka, oporavak podataka, lokaciju podataka i snimanje. Analiza podrazumijeva uočavanje korelacija, rekonstrukciju, sinkronizaciju vremena, zapisnike, metapodatke i vremenske crte. Poseban problem čine anti-forenzičari koji za cilj imaju prikrivanje, skrivanje podataka i upotrebu zlonamjernog softvera. U petu skupinu ubrajaju se nadležna tijela i osobe koje su prve odgovorile na sigurnosni incident. Upravljanje ulogama definira vlasnike podataka, odgovorne osobe za upravljanje incidentima, korisnike i kontrolu pristupa uslugama u oblaku. S pravnog aspekta izazovi se pojavljuju kroz nadležnost, zakone, ugovore o razini usluge ili kratko SLA (engl. *Service Level Agreement*), sudske pozive i međunarodnu suradnju. Od preostalih izazova pojavljuju se nestandardiziranost i nedostatak obuke forenzičkih istražitelja te povezanih sudionika, [7].

Na temelju evidentiranih izazova, oblikovan je moderni pristup digitalnoj forenzici u oblaku. U Tablica 1. prikazanoj u nastavku, kroz četiri glavne faze istrage uspoređuje se tradicionalni pristup digitalne forenzike i moderni pristup.

Tablica 1. Komparacija tradicionalnog i modernog pristupa digitalnoj forenzičkoj istrazi prema fazama
Izvor: [14]

	Tradicionalni pristup	**Moderni pristup**
Identifikacija	- Identificiranje sustava - pohrane podataka i lokacije na kojoj se nalaze resursi - Podrazumijevaju se tvrdi diskovi, eksterni diskovi, USB memorija, podatkovne kartice, optički diskovi, radna i privremena memorija, mrežni resursi	- Određivanje na kojem djelu svijeta, državi, poslužiteljima se nalaze digitalni dokazi - koja vrsta usluge u oblaku se koristi - tko je ustupio usluge u oblaku - tko je sve imao pristup - koje su sve tehnologije korištene - putem kojih uređaja se pristupalo uslugama
Prikupljanje	- Prikupljanje svih fizičkih dokaznih materijala odnosno hardvera i operativnih sustava te aplikacija koji se nalaze na njima - očuvanje lanca dokaza	- Prikupljanje svih virtualnih dokaznih materijala iz oblaka - Očuvanje lanca dokaza u oblaku
Analiza	- Korištenjem forenzičkih hardverskih i softverskih alata provodi se analiza digitalnih dokaza	- Korištenje modernih modela i alata ustupljenih kroz usluge u oblaku
Prezentacija	- Izrada i priprema krajnjeg izvještaja te prezentiranje identificiranih i analiziranih dokaznih materijala državnim tijelima	- Izrada i priprema krajnjeg izvještaja te prezentiranje identificiranih i analiziranih dokaznih materijala državnim tijelima

Iako se moderni pristup razlikuje od tradicionalnog, pojedini su se postojeći forenzički alati pokazali učinkovitima i za istragu u oblaku. Primjeri nekih od takvih alata su: Frost, UFED Cloud Analyzer, EnCase FOrensics & EnCase Endpoint Investigator on Azure, Access Data Enterprise. Vrijedno je istaknuti primjer poznatog UFED alata koji je evoluirao i prilagodio se novim zahtjevima forenzičkih istraga u oblaku.

3. REGULATORNI ASPEKTI PRIKUPLJANJA PODATAKA IZ SUSTAVA U OBLAKU

Zakup ili pretplata na usluge u oblaku od samih je početaka za neke bila revolucionarna dok je od strane drugih dočekana s nepovjerenjem i dozom skepticizma. Kao primjer može se navesti SaaS usluga u oblaku zvana Microsoft 365, plasirana na tržište 2011. godine. Brojne pravne ustanove, agencije i specijalisti u područjima digitalne sigurnosti i forenzike izrazili su zabrinutost oko upravljanja i pohrane podataka u oblaku od strane Microsoft-a. Nedostajalo je povjerenja da će podaci, ako oni budu potraživani od nadležnih državnih tijela biti predani Europskim agencijama i ostalima sudionicima u pravnim procesima. Iz tog razloga, posljednje desetljeće obilježeno je raspravama i formiranjem zakona koji bi razriješio problem vlasništva nad podacima, međunarodne suradnje i zaštite krajnjih korisnika

Ovo poglavlje ima za cilj pobrojati i definirati uloge novih sudionika u provođenju digitalnih forenzičkih istraga, onih koji u tradicionalnoj forenzici nisu bili od značajnije važnosti. Prikazat će se i pojasniti aktualni izazovi i prepreke koje usporavaju proces prikupljanja podataka iz oblaka prilikom provođenja digitalne forenzičke istrage. Opisat će se i razmjer važnosti dokaznih materijala i način na koji se oni prenose ako se radi o preklapanju različitih pravnih okvira i nadležnosti.

3.1. Pružatelji usluga u oblaku

Tradicionalni pružatelji IT usluga upravljaju hardverom, softverom, mrežama i pohranom za svoje klijente. Ukratko cijelim IT sustavom. Korisnik usluge dužan je platiti licenciranje softvera, dok pružatelj IT usluge upravlja cjelokupnim okruženjem koje se prije u vidu fizičkih uređaja nalazilo u prostorima samih korisnika. Za razliku od tradicionalnog pružatelja IT usluga, u modelu oblaka, pružatelj usluga i dalje može upravljati infrastrukturom u svojim vlastitim objektima, osim u slučaju privatnog oblaka. Međutim, infrastruktura je češće virtualizirana diljem svijeta. Računarstvo u oblaku tako postaje dominantni poslovni i ekonomski model koji zbog niza tehničkih i ekonomskih prednosti, agilnosti i brzine dostupnosti usluga sve češće zamjenjuje tradicionalni podatkovni centar.

Za uspješno funkcioniranje sustava oblaka, ključni su sljedeći sudionici. To su:

a) pružatelji usluga u oblaku (engl. *Cloud Service Provider*)
b) pružatelji infrastrukture u oblaku (engl. *Cloud Infrastructure Provider*)
c) pružatelji usluga interneta (engl. *Internet Service Provider*)

Sve veći interes za korištenjem usluga pohrane podataka u oblaku doveo je do sve relevantnijeg pitanja kako osigurati sigurnosti i privatnost. Oblak nudi iznimnu priliku za kompromitiranje mnoštva usluga pažljivo usmjerenim napadom na jednog poslužitelja, a brojni primjeri svjedoče da je upravo poslovanje u oblaku otvorilo vrata organiziranim kibernetičkim kriminalcima. Također, dostupnost strogih mehanizama šifriranja i anonimnih komunikacijskih kanala koje nudi usluga u oblaku, kontradiktorno, služi i kao paravan kibernetičkom kriminalu. Veliko oslanjanje na virtualizaciju omogućilo je poduzimanje kriminalnih aktivnosti od strane napadača koji se sada također koriste oblakom, [15].
Posljedično, eksponencijalno raste potražnja za digitalnim forenzičarima sustava u oblaku kako bi se otkrili podaci od forenzičke vrijednosti. Pored samih digitalnih forenzičkih istražitelja koji predvode takve istrage, od temeljnog su značaja i drugi sudionici istrage čiji je utjecaj često presudan za uspješno detektiranje prijetnja i provođenje istrage. Ti akteri su sljedeći:

1. Korisnici oblaka (engl. *Cloud Costumers*) - kupac i konzument usluge koji od nje ima krajnju korist
2. Pouzdana treća strana (engl. *Trusted Third Party*) - pomaže u identifikaciji i razvrstavanju sigurnosnih prijetnji uz pomoć kibernetičkih stručnjaka za sigurnost
3. Pružatelj usluge u oblaku (engl. *Cloud Service Provider*)- registrirani pružatelj usluga koji ima propisanu obveznu infrastrukturu potrebnu za pružanje usluga u oblaku
4. Forenzički istraživački tim za istrage oblaka (engl. *Cloud Forensics Investigation Team*) - koristi forenzičke istraživačke timove oblaka za rukovanje sumnjivim aktivnostima koje se događaju u oblaku klijenata

Dok tradicionalne forenzičke istrage ne zahtijevaju mnogo suradnje s drugim stranama, ono je u forenzičkoj istrazi oblaka ključno. Uspješnost forenzičkih istraga u oblaku tako ovisi o kooperaciji različitih aktera, uspješnosti prevladanih tehničkih, organizacijskih i pravnih problema, ali ovisi i o ugovorenim obvezama između pružatelja usluge i korisnika usluga oblaka koji dijele odgovornost za pojedine aspekte usluga. Pružatelji usluga u oblaku nisu uvijek dužni niti obvezni ponuditi svoje podatke na uvid digitalnim forenzičkim istražiteljima oblaka. Pružatelji usluga mogu se pozvati na zakon ili na ugovor s klijentima, o kojem se raspravljalo u uvodu, a koji ih ponekad djelomično, a ponekad u potpunosti oslobađa odgovornosti od nastale štete za njihova korisnika uzrokovane kibernetičkim napadom, [16]. Suradnja svih sudionika i stvaranje unificiranog zakona o provođenju istrage koji obvezuje sudionike procesa istrage na pomoć tijekom forenzičkih istraga poduzetih u sustavima u oblaku i dalje se smatra izazovom koji nije u potpunosti riješen.

3.2. Izazovi forenzike u oblaku

Izazovi povezani s provođenjem istrage u različitim modelima implementacije sustava u oblaku često prelaze zemljopisne i pravne granice, što je ujedno i glavni razlog prolongiranog trajanja same istrage i u konačnici rješavanja slučaja. Pojavljuju se poteškoće povezane s replikacijom i kriptiranjem podataka, transparentnošću lokacije na kojima se nalaze podatkovni centri, problemom višestrukog zakupa te mnogi drugi koji se manifestiraju tijekom procesa forenzičke istrage. Osim toga, oblak je karakteristično okruženje koje se postavlja savladavanje mnoštva tehničkih, organizacijskih i pravih izazova, [17] koji će u ovom poglavlju biti predstavljeni.

Tehnička dimenzija digitalne forenzičke istrage oblaka uključuje prikupljanje podataka, „živu“ forenziku, determiniranje dokaza, virtualizirano okruženja i proaktivne mjere. Prikupljanje podataka je proces identifikacije, označavanje, bilježenje i stjecanja forenzički značajnih podataka. Proces prikupljanja trebao bi očuvati integritet podataka s jasno definiranim podjelama odgovornosti između pružatelja usluga u oblaku i klijenta. Također, istraga ne smije kršiti zakone ili propise zemlje u kojima se podaci prikupljaju, ali niti ugrožavati povjerljivost drugih korisnika koji dijele resurse, [18]. Rješenjima ovih problema bavili su se A. Pichan i suradnici [14], čije su ideje za suočavanje s navedenim problemima predstavljene na Slika 5. u nastavku.

No.	Challenges	Recommended solutions	Comments
1	Unknown physical location	Resource tagging (Hay et al., 2011)	Adversely affects CSPs ability to ensure flexibility, service availability and manageability.
		Robust SLA with CSPs (Alhamad et al., 2010; Birk and Wegener, 2011). SLA in support of cloud forensics ((Ruan et al., 2012)	Most of the SLA guidelines are mainly focused on security requirements and less on forensic requirements.
		System level Logs	System level logs can contain prime information regarding the access, creation and deletion of system level objects
2	Decentralized data	Log frame work (Marty, 2011; Sang, 2013)	Logs including the hypervisor level logs would help the forensic process and time lining of events
3	Data duplication	Resource tagging (Hay et al., 2011)	Can adversely affect the system performance.
4	Jurisdiction	SLA, specifying where the data can be stored or migrated (Alhamad et al., 2010; Jansen and Grance, 2011; Ruan et al., 2012)	Can adversely affect CSPs ability to ensure service availability flexibility and cost benefits to consumers.
		Reverse look up for networked devices conduct a reverse look up of network topology (CSA, 2013a).	This is a very time critical action due to dynamic nature of cloud computing
5	Dependency Chain	None	Lack of solutions in the form of software tools, standard process etc. not available
6	Encryption	Key management system within cloud (CSA, 2013a) and legal authority	Policy guidelines, governance, and process doesn't exist now for key management in cloud
7	Dependence on CSP	SLA specifying the specific forensic services (Alhamad et al., 2010; Kandukuri et al., 2009; Ruan et al., 2012).	Good SLA ensures service availability and compliance (Pichan et al., 2014)

Slika 5. Izazovi prikupljanja podataka u prvoj fazi digitalne forenzičke istrage u oblaku, [14]

Organizacijska dimenzija digitalne forenzičke istrage oblaka zahtijeva suradnju niza aktera. To su revizori, posrednici u oblaku, klijenti i pružatelje usluga u oblaku te drugi suradnici čija je zadaća suradnja i osiguravanje pristupa forenzički vrijednim podacima. Organizacijske politike i sporazumi o razini usluge u oblaku (engl. *Cloud Service Level Agreement*) svojim odrednicama također mogu podržati aktivnost forenzičke istrage. Da

bi se istraga u oblaku mogla provesti na adekvatan način, neophodna je uspostava suradnje između svakog od sudionika, odnosno davatelja usluge, korisnika usluge i prema potrebi vanjskih suradnika. Istražitelji su odgovorni za ispitivanje i hipotetsko rekreiranje događaja te utvrđivanje potencijalnih povreda dužnosti, ali i rad s vanjskim agencijama za provedbu zakona. Da bi bili kompetentni za suradnju s drugim sudionicima uključenima u istragu, potrebna im je stručna osposobljenost.

Vanjske suradnike tako često čine administratori sustava, mrežni i sigurnosni administratori, etički hakeri, arhitekti sigurnosti u oblaku, tehničko osoblje i osoblje za podršku. Oni pružaju svoje stručno znanje kao potporu istragama. Rukovatelji incidentima odgovaraju na sigurnosne incidente kao što su neovlašteni pristupi podacima, „curenje“ i gubitak podataka, povreda povjerljivosti korisnika, neprikladno korištenje sustava, kompromitiranje sustava zlonamjernim kodom, unutarnje napade i slično. Da bi prikupljeni forenzički podaci bili validni, ali da i da se istraga provede prema odgovarajućem modelu i smjernicama, bitnu ulogu odigravaju pravni savjetnici. Oni osiguravaju da forenzičke aktivnosti ne krše zakone i propise te održavaju povjerljivost drugih korisnika koji dijele resurse. Intencija je da interni pravni savjetnici budu uključeni u izradu nacrta razine pružene usluge u oblaku, a koji bi neovisno o zemlji i pravnom sustavu, univerzalistički bili valjani za sva područja u kojima posluju pružatelji usluga u oblaku. Interni pravni savjetnici također su odgovorni za komunikaciju i suradnju s vanjskim agencijama za provedbu zakona tijekom forenzičkih istraga, [6].

Pravna dimenzija forenzike u oblaku zahtijeva razvoj propisa i sporazuma kako bi se osiguralo da forenzičke aktivnosti ne krše zakone i propise u nadležnosti u kojima se podaci nalaze. Takozvano „zaostaje u zakonu“ jedan je od glavnih problema s kojima se temporalna digitalna forenzika suočava. Razvoj i dopune zakona kasne za razvojem tehnologije, a ovaj problem produbljuje i dugotrajan proces stvaranja novih zakona. Odsustvo međunarodne suradnje, protekcija privatnosti i potraživanje naloga za pretragu u slučaju pokretanja istrage, samo su neki od primjera koji usporavaju razvoj, ali i provedbu digitalnih forenzičkih istraga oblaka. Ruan i suradnici proveli su anketu među 257 međunarodnih digitalnih forenzičara oblaka. Prema rezultatima, više od 80 posto ispitanih stručnjaka za forenzičke istrage istaknulo je četiri sljedeća izazova. Čak 90 posto ispitanih kao najveći problem istraga navelo je nadležnost, njih 85 posto tvrdilo je da je najveći problem istrage oblaka nedostatak međunarodne suradnje i zakonodavnih mehanizama u međunarodnoj razmjeni podataka. Na trećem mjestu nalazi se nedostatak zakona i educiranih savjetnika, te na kraju problem istrage vanjskog lanca ovisnosti pružatelja usluga u oblaku, [18].

Vrijedi se osvrnuti na nekoliko primjera u kojima zakoni zemlje sputavaju provedbu istrage oblaka. Jedan od njih je potraživanje naloga za pretragu. Nalog za pretragu odnosno prikupljanje potencijalnih dokaza sudski je nalog koji službenike ovlašćuje za pretragu osoba ili lokacija u potrazi za kriminalnim dokazima. Iako se nalozi među zemljama razlikuju, oni moraju sadržavati popis onoga što se traži i dokaza koje je potrebno zaplijeniti. Nalog za digitalnu forenzičku istragu oblaka mora sadržavati opis informacija koje je potrebno zaplijeniti, ali i lokaciju mjesta gdje se nalaze podaci treba. To je velik izazov za digitalne forenzičare oblaka, budući da se podaci mogu replicirati na više poslužitelja i često u različitim podatkovnim centrima čije lokacije prelaze granice nadležnosti zemlje koja je izdala nalog. Taj je problem savladiv ako se za potrebe digitalne forenzike oblaka formira zakon koji u slučaju potraživanja naloga ne zahtijeva navođenje fizičke lokaciju predmeta, već ovlašćuje istražitelje da provedu istragu nad cjelokupnim sustavom poslužitelja usluge u oblaku, neovisno o dislociranosti njegovih podatkovnih centara. Digitalni forenzički istražitelji oblaka često ovise o pomoći davatelja usluga u oblaku koji može ponuditi suradnju, jednako kako je i odbiti pravdajući se ugovorom o podijeljenoj odgovornosti. Ako druga strana i pristane na suradnju, istražitelji se moraju osloniti na stručnost i pouzdanost osoblja pružatelja usluge u oblaku. Taj postupak može otežati prihvatljivost tih dokaza na sudu. Karakteristike okruženja u oblaku su *multi-tenancy*[3] i dijeljenje resursa. Prvo se odnosi na korištenje jednog sustava od strane više korisnika, a drugo na dijeljenje softverskih i hardverskih resursa između korisnika. To dovodi u pitanje kršenje privatnosti drugih korisnika, što je samo još jedan u nizu problema koji prate digitalnu forenzičku istragu oblaka, [19]. Predstavljeni su ovdje samo neki od izazova i problema tijekom faze prikupljanja podataka, dok će u sljedećem poglavlju biti riječ o zakonima, prikupljenim dokaznim materijalima iz oblaka te nedosljednim i kompleksnim međunarodnim pravnim procesima koji usporavaju donošenje presude osumnjičenicima za kibernetički kriminal.

[3] Multi-tenancy – engl. pojam koji označava jednu platformu koja je ustupljena na korištenje većem broju korisnika.

3.3. Dokazni materijali prikupljeni iz oblaka

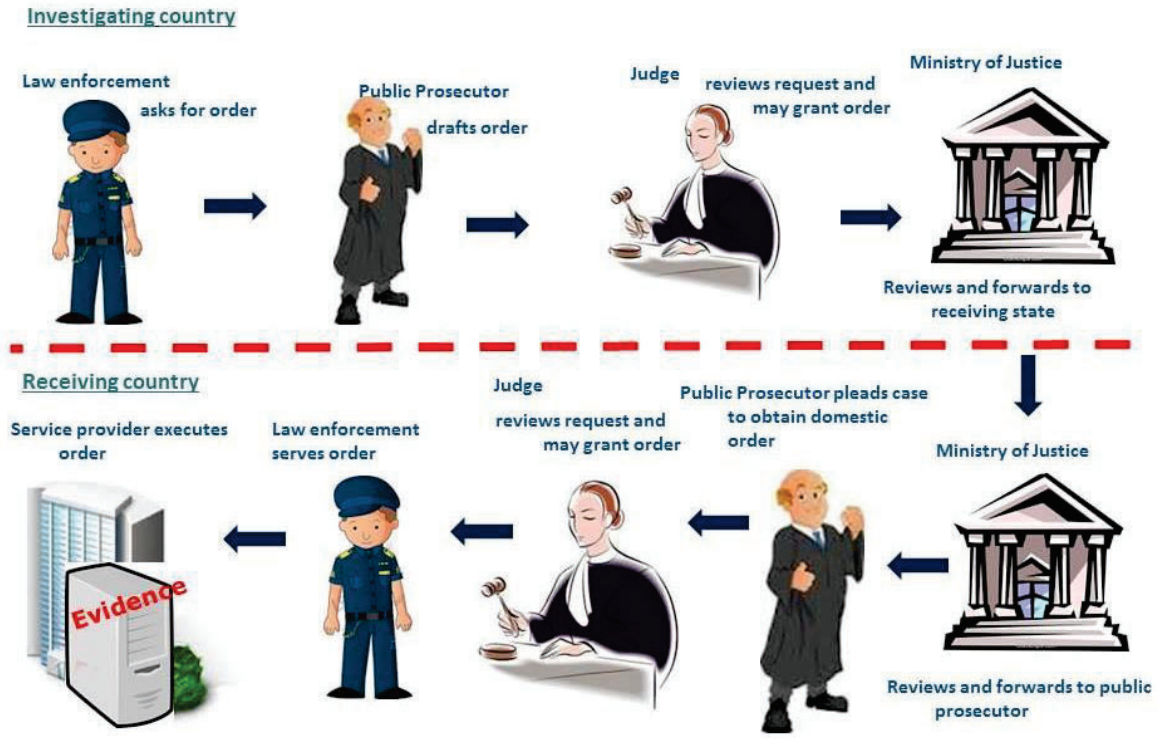
Rukovanje digitalnim dokazima složen je i višestruk proces jer oni mogu pružiti ključne dokazne informacije na neupitan i nepobitan način. Kada se digitalni dokazi nalaze u okruženju za pohranu u oblaku, kaznena istraga suočava se sa zamršenim suvremenim pravnim izazovima. Recentne studije identificiraju tri glavna pravna izazova koja proizlaze iz trenutne konstitucije sustava u oblaka a to su:

- teritorijalnost (gubitak lokacije)
- posjedovanje (vlasništvo nad sadržajem u oblaku)
- postupak oduzimanja i zaplijene dokaznog materijala (pitanja autentifikacije korisnika/čuvanja podataka)

Važno je naglasiti da se detektirani izazovi pojavljuju na globalnoj razini, ali i da se postojeći američki, europski i međunarodni pravni okviri razlikuju u pristupu digitalnim dokaznima materijalima, [20]. Svaki značajan elektronički podatak u kaznenom postupku smatra se dokazom s kojim je potrebno postupati uz određene znanstvene postupke kako bi zadržao svoju dokaznu vrijednost. Sve dok je svaki evidentni predmet prihvatljiv, autentičan, pouzdan i potpun, sudac ga može sigurno procijeniti kako bi donio svoj konačni zaključak i sudsku odluku. Iz tog je razloga od najveće važnosti za digitalnu forenzičku istragu da svi prikupljeni elektronički dokazi zadovoljavaju definirane standarde, prikladno nazvane "Zakonima o dokazima". Spomenuti zakon skup je proceduralnih pravila i pravnih načela koja uređuju korištenje dokaza u pravnim postupcima. Ova pravila utvrđuju metode kojima se mogu prezentirati dokazni materijali i određuju koje dokaze sudac ili porota moraju ili ne smiju uzeti u obzir pri donošenju svoje odluke. Međutim, kada se podaci presele u okruženje za pohranu u oblaku, gore spomenute forenzičke procedure, više nisu relevantne i pojavljuju se novi pravni izazovi [20].

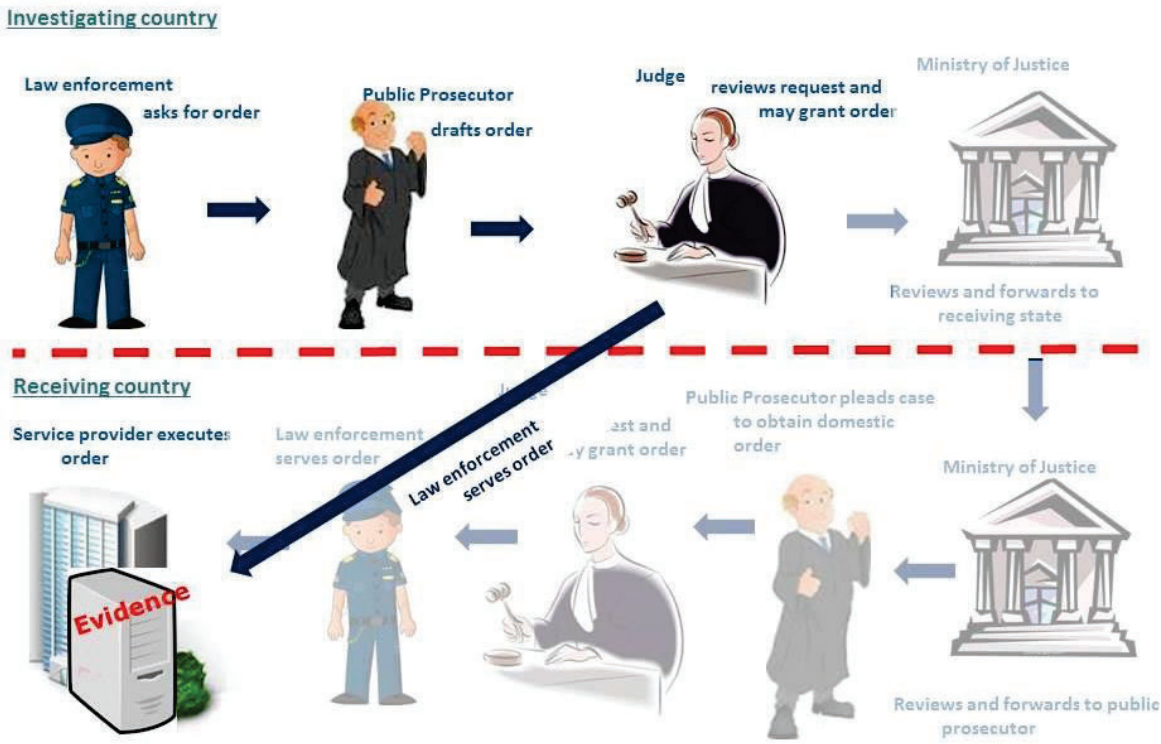
Digitalni forenzički stručnjaci i državna pravna tijela različitih država sve se češće suočavaju s pitanjem što znači osigurati točnost, autentičnost, potpunost i uvjerljivost digitalnih dokaza. Pitanja uzajamne pravne pomoći i prihvatljivosti javljaju se kada vrhovni sud neke zemlje traži od drugog pravosudnog tijela da prikupi digitalne dokaze u ime druge zemlje. Kao temeljni problem pojavljuje se nepostojanje univerzalnih smjernica, standarda i odgovarajućeg pristupa prilikom pristupanja forenzičkoj istrazi oblaka. Metode kojima su prikupljeni digitalni podaci u nekoj zemlji tako ponekad metodološki ne zadovoljavaju standarde druge zemlje. Tako prikupljeni digitalni dokazi mogu biti odbačeni kao nepravovaljani. Za pokretanje, provedbu i prikupljanje digitalnih dokaza zadužena je Agencija za provedbu zakona (engl. *Law Enforcement Agency*). Mnoge dosad poduzete akcije LEA-e u cilju prikupljanja podataka iz oblaka dobro ilustriraju problematičnost rada u tom okruženju u kojem se često istodobno primjenjuje više zakona. Ti zakoni razlikuju se na materijalnoj i proceduralnoj razini i mogu dovesti do međudržavnih razmirica. Iako su poduzete inicijative za usklađivanje zakona, kao što je Konvencija o kibernetičkom kriminalnu, rad agencija i dalje

remete značajne zakonske razlike, poglavito one koje se tiču privatnosti u čemu prednjače Europa i SAD. Primjerice, zakonodavstvo koje dodjeljuje ovlasti za pokretanje istrage pretpostavlja da je ono ograničeno na teritorijalnu nadležnost domaće države. Budući da podaci u sustavima oblaka često dislocirani i smješteni u prostoru drugih država, svako postupanje LEA koje prekoračuje te granice (ako su podaci duplicirani i premješteni u podatkovne centre neke druge države), smatra se nezakonitim ili prijetećim. Komisija je izvijestila da je taj slučaj prisutan u dvije trećine aktualnih slučajeva kibernetičkog kriminala, što je potaknulo zemlje da rade na formiranju međunarodnog zakona i sporazuma koji bi olakšali i ubrzali provođenje istraga. Ugovor o uzajamnoj pravnoj pomoći obvezuje dvije ili više zemalja na međusobno pomoć i razmjenu ključnih podataka, informacija i dokaza u slučaju prekograničnog kibernetičkog kriminala, [21]. Prema ugovoru definirani su koraci koje je potrebno slijediti prilikom istrage, a prikazani su na Slika 6. u nastavku.



Slika 6. Prikaz sudionika i međusobne suradnje tijekom postupka uzajamne pravne pomoći u forenzičkim istragama, [21]

U praksi, sporazum se pokazao neproduktivnim dok je proces koji on pretpostavlja dugotrajan i opterećen nizom postupaka, a njegov hijerarhijski slijed onemogućuje brzu obradu zahtjeva. „Vrijeme“ je bit prekograničnih zločina, a kašnjenje u provedbi daje prednost osumnjičeniku za kibernetički kriminal. Također, u vremenu ishođena ovlasti, ključni podaci mogu biti uništeni ili modificirani, [22]. Predložen je zato drugi protokol ishođenja ovlasti koji bi ubrzao proces digitalne forenzičke istrage, koji je prikazan na Slika 7. na sljedećoj stranici.



Slika 7. Prikaz direktne suradnje bez posredovanja pojedinih sudionika, [21]

Godine 2018. Sjedinjene Američke Države donesen je Zakon o oblacima (engl. *Cloud Act*) Tim zakonom željelo se doskočiti problemu podataka izvan teritorija države. Njime je definirano kako je svaki terećeni subjekt dužan dostaviti podatke koje posjeduje, čuva ili kontrolira, bez obzira na to jesu li oni pohranjeni u Sjedinjenim Državama ili inozemstvu. Ta se odredba odnosi ne samo na subjekte obveznike, već i na pružatelje usluga u oblaku, [22]. Zakon je definirao okvir za pregovore o bilateralnim međunarodnim sporazumima između Sjedinjenih Država i inozemnih partnera koji bi utvrdili, između ostalog, načela za izdavanje i izvršenje naloga za prikupljanjem digitalnih forenzičkih dokaza. Kao rezultat toga, Zakon o oblacima stvara okvir za prekogranični model prijenosa osobnih podataka, u kojem vodeću ulogu imaju norme nacionalnog prava, dopunjene bilateralnim međunarodnim ugovorima. Europska unija u to je vrijeme radila na prijedlogu mjera za očuvanje i postupanje s e-dokazima, prijedlogu koji bi olakšao razmjene elektroničkih dokaza između Europske Unije i SAD-a za potrebe kaznenog postupka. Konačni oblik paketa e-dokaza još se pregovara među članicama unije. Očekuje se da će pregovori Europske Unije i SAD-a koji se odnose na Zakon o oblaku biti prihvaćeni, ali uz preinake koje će biti usklađene s paketom e-dokaza. Tako bi EU osigurala dosljednost između oba pravna mehanizma. Ako se sporazum realizira, on neće eliminirati odredbe uzajamne pomoći, već će biti njegova svojevrsna nadopuna. Sporazum uzajamne pomoći ostaje opcija za dobivanje forenzički značajnih podataka, no novi protokoli mogli bi značajno olakšati proces digitalnih forenzičkih istraga i sudskih procesa [23].

4. KARAKTERISTIKE MICROSOFT XDR I SIEM SIGURNOSNIH RJEŠENJA

Neosporiva činjenica je da količina kibernetičkih napada u kontinuiranom porastu. Drastičan, eksponencijalni rast zabilježen je 2020. godine kao nusprodukt nagle digitalne transformacije i potrebe rada s udaljenih lokacija uzrokovan globalnom pandemijom. Organizacije diljem svijeta susrele su se s dosad najvećim izazovima po pitanju ne samo strukture i mogućnosti IT sustava već i njegove zaštite. Pored brojnih komponenti sustava koje je potrebno štiti na različite načine, očekivan je razvoj sigurnosnih rješenja dostupnih na tržištu od strane raznih proizvođača. Dosadašnja percepcija bila je oblikovana uvjerenjem da je svako računalo potrebno zaštiti antivirusnim rješenjem, segregirati internu mrežu i zaštiti ju od zlonamjernih napada s javne mreže vatrozidom. Osim toga, paziti na komunikaciju između poslužitelja i vanjskih servisa i uređaja, kontrolirati na kojoj se lokaciji nalaze krajnji uređaji, odnosno inventar organizacije.

Sve navedeno navelo je organizacije na implementaciju mnogobrojnih sigurnosnih rješenja od različitih proizvođača, odnosno uzimanje najbolje za svaku komponentu sustava budući da je uska specijalizacija proizvođača ulijevala sigurnost i pouzdanje u njihov proizvod. Krajnji rezultat doveo je do preopterećenja odgovorih osoba informacijama i obavijestima iz raznih konzola, otežanog snalaženja i općenito kontrole sigurnosti što bi za ishod imalo određenu stopu izloženosti i ranjivosti samog sustava. Uzimajući to u obzir, proizvođači poput Microsoft-a, IBM-a i ostalih, svoje su napore usmjerili u unificiranje svojih proizvoda i omogućavanje komplementarnosti sa sličnim rješenjima. Iz inicijalnog EDR (engl. *Endpoint Detection and Response*) sustava čija je namjena proaktivno nadziranje i zaštita svih krajnjih uređaja, razvijen je XDR (engl. *Extended Detection and Response*) sustav koji pruža zaštitu kroz višestruke slojeve IT sustava. Osim osnovnih funkcionalnosti koje je imao nekadašnji EDR, XDR se odlikuje automatskim prikupljanjem podataka i njihovom analizom iz svih izvora s kojima je povezan, što podrazumijeva krajnje uređaje, email sustav, poslužitelje, mreže i aplikacije neovisno o njihovoj infrastrukturi, neovisno nalazila se ona fizički u organizaciji ili u oblaku. Kako bi se proširio doseg i omogućila dodatna vidljivost događaja u sustavu nerijetko se proaktivni XDR povezuje s reaktivnim SIEM sustavom namijenjenim za bilježenje i nadziranje događaja. Ranije spomenuti Microsoft, krajem 2020. godine svojim korisnicima ustupa povezano rješenje Microsoft Defender XDR s Microsoft Sentinel SIEM sustavom. U daljnjim poglavljima opisat će se i razjasniti svrha i ključne značajke oba sustava kao uvod u njihovu mogućnost primjene prilikom provođenja digitalnih forenzičkih istraga.

4.1. XDR

Sigurnosni alati sadržani u EDR rješenjima fokusirani su isključivo na krajnje uređaje, njihov rad, mogućnost nadzora i otkrivanja potencijalnih zlonamjernih aktivnosti te pružanje adekvatnog odgovara. XDR kao inovativna skupina raznih sigurnosnih alata karakterizirana je holističkim pristupom ne djeluje samo na jednu instancu, već na sustav u cjelini. Takav pristup podrazumijeva djelovanje, ali i razumijevanje podataka koji prolaze kroz višestruk broj OSI slojeva pojedinog sustava.

XDR je sastavljen od tri ključne komponente koje su dio njegovog akronima. Znak X označava proširenje koje se odnosi na mogućnost dosega i široku primjenjivost XDR-a unutar postojećeg IT sustava. Pojam detekcije podrazumijeva mogućnost provođenja automatizirane analize nad prikupljenim podacima koja je od značaja za detektiranje nepravilnost u radu sustava, identificiranje sigurnosnih incidenata i stvaranje izvještaja. Zadnja komponenta odnosi se na odaziv odnosno reakciju XDR sustava. Ona sadrži sve potrebne alate koji imaju mogućnost brzog odgovor na napad, neovisno radi li se o metodi izolacije krajnjih uređaja, dodatnog segmentaciji mreže ili drugim proaktivnim metodama, [24]. Microsoft Defender XDR sustav dizajniran je kao *nativni*[4] XDR sustav u oblaku, prvotno namijenjen isključivo povezivanju s rješenjima proizvedenim od strane Microsoft-a. Zbog potreba krajnjih korisnika, ali i konkurentnosti na tržištu, Microsoft je stvorio hibridni XDR sustav s mogućnošću povezivanja s partnerskim sustavima.

4.1.1. Svrha XDR rješenja

Kontinuirana digitalna transformacija i novi trendovi koji su omogućili udaljeni rad postojećim sigurnosnim sustava dodali su novu razinu kompleksnosti i ujedno izložili sustave javnoj mreži. XDR rješenja osmišljena su i dizajnirana kako bi adresirala nove izazove stvorene od strane krajnjih korisnika, ali i ponudila adekvatnu zaštitu te odgovor na postojeće i nove potencijalne i stvarne prijetnje. XDR unificiranim pristupom podrazumijeva zaštitu mreže i krajnjih uređaja, krajnjih uređaja unutar i izvan mreže te zaštitu usluga u oblaku. Osim osnovne namjene, XDR sustav predstavlja jedinstvenost u smislu objedinjenja brojnih funkcionalnosti, manje lažno pozitivnih obavijesti, transparentnost i vidljivost napada prema sustavu, mogućnost dodatne istrage i uvida u stanje sustava, brže djelovanje i smanjivanje štetnog utjecaja unutar sustava.

[4] Nativno - Inicijalno dizajnirano s određenim ciljem

4.1.2. Ključne značajke

Svaki XDR sustav kategorizira se prema njegovim funkcionalnostima koje su objedinjene kroz tri kategorije. U prvu kategoriju spadaju *front-end*[5] funkcionalnosti poput telemetrije, primjene sigurnosnih politika i odgovora na prijetnje. Takozvana *back-end*[6] kategorija sadrži pozadinsko prikupljanje i korelaciju podataka iz agenata[7] ili API-a[8] (engl. *Application Programming Interface*), detekciju prijetnji, automatizirane obavijesti, istrage incidenata i automatski odgovor na prepoznate prijetnje sustavu. Treća kategorija podrazumijeva prvenstveno prikupljanje sadržaja kroz API, *parsiranje*[9] podataka, prepoznavanje pravila i modela, usmjeravanje istrage i izvještaje. Na temelju kategorizacije, razlikujemo tzv. *nativni* i otvoreni XDR sustav. *Nativni* sustav prilagođen je povezivanju i implementaciji proizvoda od istog proizvođača, dok je otvoreni prilagođen za upotrebu sa svim sustavima, neovisno o proizvođaču, [25].

Agenti na krajnjim uređajima i API-i povezani s različitim dijelovima IT sustava kontinuirano prikupljaju i prosljeđuju podatke povezanim sustavima u oblaku. Strojno učenje u oblaku omogućuje obradu, segregiranje i klasifikaciju podataka nakon čega se isti prosljeđuju sustavima umjetne inteligencije koji provode bihevioralnu analiza i određuju način rada i ponašanja sustava u različitim stanjima. Prepoznavanje anomalija i potencijalnih opasnosti glavna je odlika XDR rješenja koja je omogućena kroz uvid u višestruke slojeve informacijskog sustava. Microsoft XDR sustava pod nazivom Microsoft 365 Defender objedinjuje sljedeće podsustave, [26]:

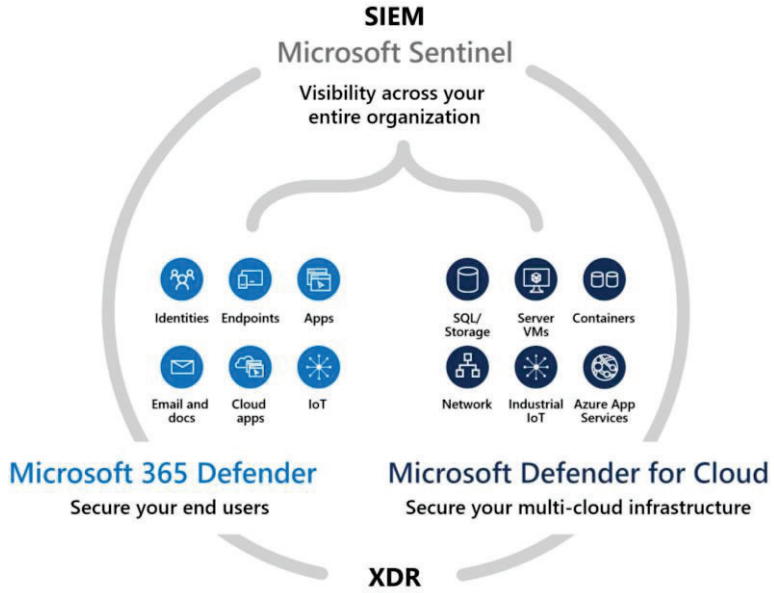
- *Microsoft Defender for Endpoint* za zaštitu svih krajnjih uređaja
- *Microsoft Defender for Office 365* za zaštitu poznate Microsoft SaaS platforme
- *Microsoft Defender for Identity* za zaštitu korisničkih identiteta
- *Microsoft Defender for Cloud Apps* za nadgledanje i zaštitu aplikaciju u oblaku
- *Exchange Online Protection* kao esencijalna zaštita Exchange mail sustava
- *Azure AD Identity Protection* za prepoznavanje sigurnosnih rizika povezanih s korisničkim računima

Svaki od navedenih podsustava međusobno je povezan s ostalim podsustavima kako bi se omogućila unificiranost i pokrivenost cijelog *on-premise*, ali i dijela sustava koji se nalazi u oblaku. Uzevši u obzir da su moderne digitalne tvrtke u postupku migracije postojeće infrastrukture u oblaku ili im se sustav temelji isključivo na infrastrukturi i uslugama u oblaku, razvijeni je novi XDR sustav nazvan *Microsoft Defender for Cloud* namijenjeni zaštiti Microsoft infrastrukture u oblaku, odnosno Azure-a.

[5] Front-end – dio sustava vidljiv krajnjem korisniku
[6] Back-end – pozadinski dio sustav zadužen za pohranu i logiku
[7] Agent - je softver namijenjen prikupljanju i prosljeđivanju podataka s jednog ili više krajnjih uređaja unutar informacijskog sustava prema centralnom mjestu
[8] API - aplikacijsko programsko sučelje
[9] Postupak provođenja sintaksne analize

Microsoft Defender for Cloud rješenje u suštini je nativno aplikativno rješenje u oblaku za zaštitu platforme ili kratko CNAPP (engl. *Cloud-Native Application Protection Platform*). Budući da je sama zaštita oblaka širok pojam, u nastavku je kratko navedeno od kojih podsustava je sačinjen CNAPP. Upravljanje stanjem sigurnosti sustava je prva komponenta poznata još pod nazivom CSPM (engl. *Cloud Security Posture Management*), namijenjena identifikaciji manjkavosti konfiguracija te rizicima po pitanju nedostatka usklađenosti. Drugi podsustav upravljanja opterećenjem sustava u oblaku ili kratko CWPP (engl. *Cloud Workload Protection Platform*) zadužen je za optimalan rad i korištenje infrastrukturnih resursa poput virtualnih računala, poslužitelja, kontejnera i ostalih, [27].

Na Slika 8. Prikazani su podsustavi *Microsoft Defender* i *Microsoft Defender for Cloud* XDR sustava te njihova povezanost sa SIEM sustavom.



Slika 8. Objedinjeno Microsoft rješenje XDR i SIEM sustava i podsustavi, [28]

Prema Gartner-u, CNNAP sustavi su: „integrirani set mogućnosti sigurnosti i usklađenosti dizajnirani s ciljem sigurnost i zaštite *nativnih* aplikacija u oblaku tijekom razvijanja i po puštanju u produkciju. CNNAP osim što konsolidiraju velik broj mogućnosti uključuju skeniranje artefakata tijekom razvoja aplikacije, sigurnosno upravljanje oblakom, skeniranje koda, upravljanjem ovlaštenjima unutar oblaka, zaštitu opterećenja same platforme u oblaku, [29].„ Prednosti koji donosi implementacija XDR rješenja u pojedini sustav su:

- Cjelovita zaštita sustava
- Poboljšano i ubrzano prepoznavanje
- Brzo reagiranje i poduzimanje akcija te blokiranje zlonamjernih aktivnosti
- Efektivnost u provođenju kibernetičke zaštite sustava

4.2. SIEM

Akronim SIEM (engl. *Security Information and Event Management*) sadržan je od dvije discipline koje svojim nastankom datiraju s razvojem interneta. Disciplina upravljanja sigurnošću informacija ili kratko SIM (engl. *Security Information Protection*) označava mogućnost prikupljanja podataka iz raznih izvora kao što su mrežni vatrozidi, poslužitelji, antivirusni softveri i razni drugi fizički, ali i virtualni uređaji i sustavi. Disciplina upravljanja sigurnosnim događajima ili kratko SEM (engl. *Security Event Management*) označava mogućnost praćenja i analiziranja događaja koji se odvijaju na svim OSI slojevima unutar informacijskog sustava.

Prema Gartneru, vodećoj konzultantskoj organizaciji koja je ujedinila iznad navedene discipline u jednu; SIEM je tehnologija koja upravlja sigurnosnim i informacijskim događajima u stvarnom vremenu te za cilj ima rano otkrivanje ciljanih napada, detektiranje neovlaštenog pristupa podacima. Također uloga SIEM-a je prikupljanje, pohranjivanje, provođenje istraga i kreiranje izvještaja za potrebe odgovora na prijetnje, forenzičkih istraga i usklađenosti s propisima, [30]. SIEM sustav dizajniran je kao digitalna centralizirana platforma povezana s gotovo svim komponentama modernog informacijskog sustava pomoću svojih alata. Navedena povezanost omogućena je kroz sljedeće alate:

- *agent* odnosno softver prilagođen za određenu programsku okolinu koji za cilj ima provođenje specifičnih radnji i komunikaciju s vanjskim softverom koji se nalazi u istoj okolini
- aplikacijsko programsko sučelje ili kratko API, koje se učestalo razvija od strane brojnih proizvođača softvera kako bi se na aplikativnoj razini povezala razna programska rješenja i proširile postojeće funkcionalnosti

Više o samoj svrsi i značajkama SIEM rješenja i alata objašnjeno je u sljedećem poglavlju.

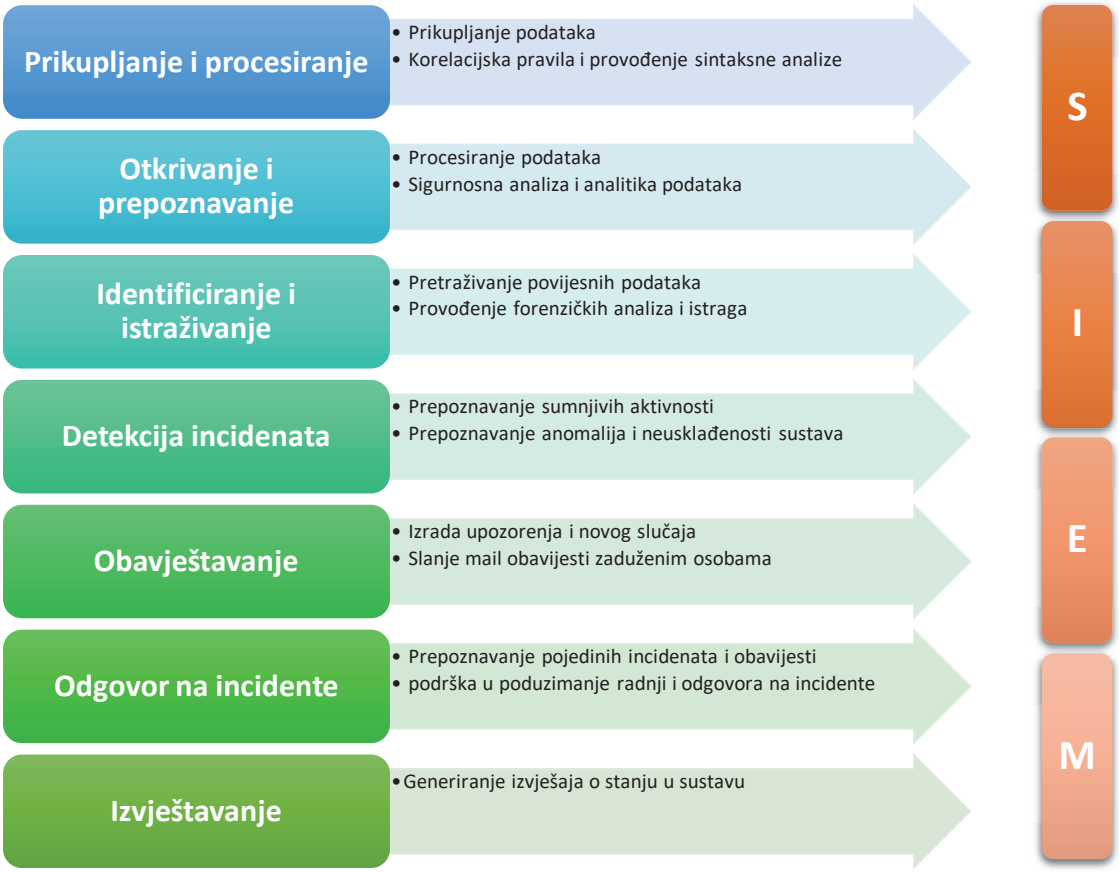
4.2.1. Svrha SIEM rješenja

Visoka razina kompleksnosti, kontinuirani razvoj i brojne mogućnosti integracija s drugim softverima i sustavima pridonijele su nepotpunoj dokumentiranosti tradicionalnih SIEM sustava što uvelike utječe na razumijevanje, ali i poimanje svih mogućnosti i primjene samog alata. Kako bi se adresirali spomenuti nedostatci neophodno je razumijevanje svrhe same SIEM platforme. Inicijalno, SIEM sustavi dizajnirani su kako bi nadzirali i prikupljali podatke iz svakog dijela mreže i krajnjeg uređaja u informacijskom sustavu. Na temelju obrade prikupljenih podataka SIEM bi iznosio relevantne povratne informacije o stanju sustava i obavještavao o potencijalnim ili aktualnim prijetnjama. Brojni proizvođači modernih tehnologija, platformi, softvera i uređaja prepoznaju važnost nadziranja, kontinuiranog obavještavanja i načinu rada te istim funkcionalnostima nadograđuju vlastite proizvode.

Zahvaljujući XDR-u, SIEM sustav je naizgled rasterećen direktnog prikupljanja podataka iz brojnih izvora, ali težnja za centraliziranim upravljanjem, shvaćanjem informacija i događaja u sustavu je i dalje ostala prisutna. Uzevši u obzir navedeno, ali i sukladno modernim trendovima, moderni SIEM sustavi baziraju se na uslugama u oblaku i prezentirani su na tržištu kao SaaS usluga. Prelazak u oblak rezultirao je brojnim poboljšanjima u odnosu na postojeće sustave koji su nekoć egzistirali isključivo na *on-premise* poslužiteljskoj opremi. Ključna poboljšanja i prednosti podrazumijevaju povezivanje s postojećim *on-premise* sustavima i uslugama u oblaku, dok su ostala navedena u nadolazećem poglavlju.

4.2.2. Ključne značajke

Razvoj značajki SIEM sustava nametnuo je podjelu istih na primarne, osnovne i napredne značajke koje variraju ovisno o proizvođaču SIEM sustava, njihovim mogućnostima i ekspertizi. Tako razlikujemo osnovne ili jednostavne te moderne, odnosno SIEM sustave nove generacije. Na Slika 9. prikazane su i kratko opisane ključne značajke koje podrazumijeva svaki SIEM sustav:



Slika 9. Ključne značajke SIEM sustava prema fazama

Osim navedenih ključnih značajki, SIEM sustavi okarakterizirani su širokim spektrom integracije s raznim sustavima i uređajima brojnim proizvođača kako bi detektirali što je moguće veću količinu podataka koja se generira u informacijskim sustavima. Neophodno je za napomenuti kako su SIEM sustavi kompleksna tehnologija kojoj je osnovna namjena detaljan uvid u stanje u sustavu i podrška za optimizaciju istog. Moderni SIEM sustavi nove generacije prvenstveno se odnose na *nativno* podržane u oblaku odnosno SIEM sustave koji se ustupaju krajnjim korisnicima kao SaaS usluga. Prema istraživanju Gartner-a, do 2024. godine, 80% od ukupnog broja proizvođača ustupit će SIEM rješenja kao uslugu u oblaku, [31].

4.2.3. Napredne značajke

Mnoštvo sigurnosnih procedura unutar brojnih informacijskih sustava karakterizira njihova anakronost. Takvi sustavi i njihovi sigurnosni alati ne mogu prepoznati niti nositi se s modernim prijetnjama. Način rada krajnjih korisnika je nepoznat i gotovo je nemoguće prepoznati kad će netko od zaposlenika nesvjesno ili svjesno izložiti informacijski sustava kompromitaciji. Kako bi se spomenutoj problematici adekvatno pristupilo i minimizirala zastarjelost i ustaljenost sigurnosnih procedura, u novu generaciju SIEM sustava uključuju se dodatni pozadinski sustavi poput umjetne inteligencije i strojnog učenja. Neosporivu promjenu u načinu rada SIEM sustava donijela je analiza ponašanja korisnika i entiteta, kratko UEBA (engl. *User and Entity Behavior Analytics)* ili EUBA (engl. *End User Behaviour Analysis*).

Prema Fortinet-u, „UEBA je rješenje kibernetičke sigurnosti koje koristi algoritme i strojno učenje kako bi detektiralo anomalije u ponašanju ne samo krajnjih korisnika već i korporativnih mreža, poslužitelja i ostalih krajnjih uređaja u mreži, [32].„

Na Slika 10., prikazan je pojednostavljeni tok procesa biheviоralne analize potpomognut strojnim učenjem koji se sastoji od pet glavnih faza.



Slika 10. Proces provođenja biheviоralne analize

Prema simplificiranom prikazu procesa bihevioralne analize koju provodi UEBA, vidljivo je kako je korak analiziranja prožet strojnim učenjem. Ono u pozadini primjenjuje razne matematičke, statističke modele i pravila kako bi se analizirali podaci o korisničkom identitetu, uređajima i mreži, odnosno, kako bi se ustvrdilo ponašanje na temelju prikupljenih uzoraka.

Nakon inicijalne implementacije UEBA-e, strojno učenje izrađuje inicijalne profile kako za korisnike sustava tako i za sve prisutne uređaje. Također, kontinuirano utvrđuje karakteristično ponašanje i bilježi odstupanja od istog. Zahvaljujući ovakvom pristupu, UEBA sustav je u mogućnosti, [33]:

- detektirati anomalije i prijetnje u stvarnom vremenu
- vizualno prezentirati rezultate analize
- klasificirati i rangirati anomalije i prijetnje na temelju dokaza
- pomoći odgovornim osobama pravovremeno reagirati

Na temelju sjedinjenja SIM i SEM sustava iz kojeg je proizašao SIEM sustav, dolazi do ispreplitanja i s drugim sigurnosnim rješenjima kako bi se postojeće funkcionalnosti dodatno proširile te ujedno odgovorilo na potrebe tržišta, ali i na potencijalne prijetnje. Zahtjevi koji se postavljaju pred proizvođače naprednih sigurnosnih sustava podrazumijevaju:

- Proaktivnost i kontinuirano praćenje svih dijelova sustava
- Analizu ponašanja krajnjih uređaja i njihovih korisnika te predviđanje budućih događaja
- Preventivno automatizirano djelovanje na neusklađenost i anomalije
- Kontinuirano minimiziranje rizika unutar informacijskog sustava

Primjer je sustav automatizirane sigurnosne konfiguracije i odgovora na događaje ili kratko SOAR (engl. *Security Orchestration and Automation Response*). Prema Gartner-u, koji je prvi oformio naziv SOAR još 2017. godine, definicija glasi, [34]:

„SOAR je rješenje koja kombinira odgovor na incidente, orkestraciju[10] i automatizaciju, upravljanje inteligencijom o prijetnjama. SOAR alate moguće je primijeniti za široki spektar zadataka, što uključuje dokumentiranje i implementaciju procesa, podršku u upravljanju sigurnosnim incidentima, primjenu strojnog učenja u podršci u radu sigurnosnih analitičara i operatera, poboljšano korištenje inteligencije o prijetnjama u operativnom radu.“

[10] Orkestracija - u području informacijskih tehnologija odnosi se na automatizaciju konfiguracije pojedinih dijelova sustava, koordinaciju i upravljanje računalnim sustavima i programima.

SOAR sustavi su dizajnirani kako bi bili komplementarni, odnosno namijenjeni integraciji s drugim sigurnosnim sustavim i alatima. Primarna integracija odnosi se na SIEM sustave s kojima se međusobno nadopunjavaju.

Microsoft SOAR komponenta omogućuje stvaranje automatizacijskih pravila koja na temelju okidača koji može biti u statusu kad je incident stvoren ili kad je incident ažuriran, automatski pokreće određene radnje. Na temelju stvorenog automatizacijskog pravila definira se određena kolekcija radnih zadataka odnosno radnji temeljnih na Azure logičkim aplikacijama koje će sustav napraviti samostalno, bez posredovanja ljudskog faktora.

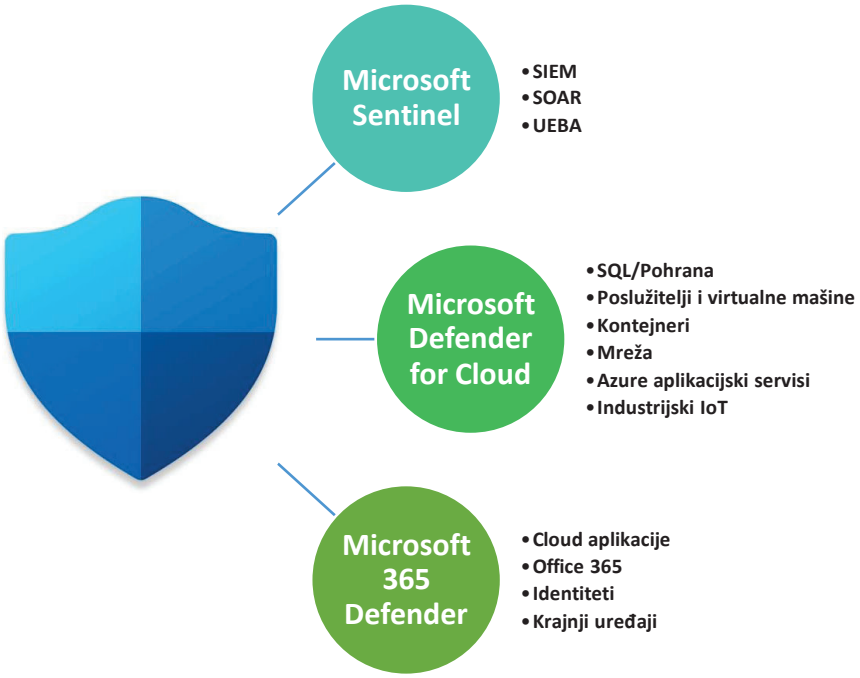
Ključne značajke koje doprinosi integracija SOAR-a i SIEM-a u Microsoft Sentinel su sljedeće, [35]:

- Jednostavna automatizacija predvidivih radnih zadataka vezanih uz odgovor na ponavljajuće sigurnosne incidente i potencijalne prijetnje
- Automatizacija pojedinih dijelova istrage i upravljanja incidentima
- Doprinos smanjenju resursa za potrebe nadgledanja SIEM sustava i omogućavanje povećanja fokusa prema istragama i provjeri potencijalnih prijetnji

4.3. Unificiranost zaštite u oblaku

Tijek razvoja strojnog učenja tijekom zadnjeg desetljeća ukazao je na primjenjivost u širokom spektru informacijske sigurnosti. Postojeći sigurnosni sustavi i alati nastoje povećati učinkovitost, analizirati veće količine podataka i adekvatno s istima upravljati te automatizirati ponavljajuće procese. Strojno učenje i umjetna inteligencija vidno transformiraju postojeće sigurnosne sustave, doprinose razvoju novih alata i općenito ih dovode ih na novu razinu prilagođenu radu u oblaku. U bliskoj budućnosti, očekuje se primjena umjetne inteligencije i strojnog učenja u gotovo svim područjima kibernetičke sigurnosti, ali i digitalne forenzike. Primjer takozvanog unificiranja tj. stapanja postojećih alata i strojnog učenja, potpomognutim umjetnom inteligencijom je Microsoft Defender i Microsoft Sentinel sustav. Postojeće, osnovne funkcionalnosti koje su bile ograničene isključivo na postojeće proizvode istog proizvođača, sada su značajno proširene i nadograđene. Nekadašnji Microsoft EDR sustav pokrivao je isključivo računala s operativnim sustavom Windows, dok je danas Microsoft Defender XDR sustav moguće povezati s bilo kojim operativnim sustavom renomiranog proizvođača. Osim po pitanju krajnjih uređaja, povezanost se odnosi na poslužiteljska računala neovisno radilo se o Linux ili Windows distribuciji. Također, integracija s oblakom omogućila je i djelovanje i kroz druge sustave u oblaku poput Google Cloud-a i AWS-a, [36].

Spomenuti sustavi u prethodnim poglavljima čine ključan dio zaštite informacijskog sustava pojedine tvrtke ili korporacije kojima u praksi najčešće upravlja sigurnosno operativni centar ili kratko SOC (engl. *Security Operations Center*). Ključni međusobno povezani sustavi u oblaku prikazani su na Slika 11. a odnose se na XDR, CASB, SIEM, SOAR i UEBA-u.



Slika 11. Unificiranost Microsoft 365 Defender, Microsoft Defender for Cloud i Microsoft Sentinel sustava

Microsoft Sentinel, sam po sebi nije isključivo sadržan od SIEM sustava, već je inicijalno dizajniran kako bi bio komplementaran s UEBA i SOAR sustavima. Sva tri sustava naknadno su povezana, potpomognuta i dodatno povezani s XDR sigurnosnim rješenjima. Nude jedinstven pogled na cijeli informacijski sustav pojedine tvrtke ili povezanih organizacija. Unificiranost sigurnosnih rješenja u oblaku, ali i sveobuhvatan pogled na sustav nije maksimizirao razinu sigurnosti i ponudio apsolutnu zaštitu, već detaljan uvid u sustav i mogućnosti pravovremenog reagiranja u slučaju potrebe.

Glavne karakteristike, a ujedno i prednosti koje je doprinijela unificiranost sustava prepoznate su i od strane Gartner-a, koji je u svojem izvještaju „Magic Quadrant for Security Information and Event Management 2021, [30].“

- *Nativno* podržan SIEM sustav koji se odlikuje elastičnosti prema potrebi krajnjih korisnika. Model pretplate je jednostavan koji omogućuje unaprijed rezervaciju određenog kapaciteta ili plaćanje prema potrošnji
- Širina i opseg SIEM sustava pružaju širok spektar integracija s postojećim sigurnosnim rješenjima unutar istog sustava Microsoft oblaka što rezultira korištenjem i pregledom sustava s centraliziranog mjesta
- Integracijske sposobnosti s rješenjima drugih proizvođača omogućene su na temelju kompaktnog API sučelja koji je pružio povezanost s drugim sustavim u oblaku, vatrozidima i raznim aplikacijama u oblaku

Daljnji trendovi razvoja XDR, SIEM i povezanih alata idu u smjeru otvorenosti i integraciji svemu onoga što je moguće povezati putem API konektora ili agenata. Cilj je postići široku pokrivenost i dati detaljni uvid u sustave. Rezultat šire pokrivenosti doprinijet će većoj količini prikupljenih podataka što će u konačnici uz pomoć strojnog učenja i umjetne inteligencije voditi poboljšanom detektiranju potencijalnih prijetnji i kvalitetnijem razumijevanju cijelog sustava.

5. MOGUĆNOSTI PRIMJENE MICROSOFT XDR I SIEM RJEŠENJA U DIGITALNOJ FORENZICI

Prva polazišna točka svake računalne forenzičke istrage počiva upravo na samom krajnjem uređaju, najčešće računalu. Dugi je niz godina prevladavalo mišljenje da se na fizičkom računalu odvija sav posao, ali ujedno i manifestiraju poteškoće prouzročene raznim kibernetičkim prijetnjama. Sve donedavno, računalo se poimalo materijalne, opipljiva stvar.

Moderno doba usluga u oblaku i neizbježna potreba za udaljenim radom promijenila je iznad spomenuto poimanje računala. Nove tehnologije omogućile su rad na daljinu. Osim rada na vlastitom računalu u privatnom ili poslovnom vlasništvu, postao je dostupan i rad na dislociranim, odnosno virtualiziranim računalima. Kao što je spomenuto u poglavlju 2.1. osim računala, usluge u oblaku omogućile su virtualizaciju svih dijelova IT sustava, ovisno o odabiru vrste modela oblaka odnosno usluge. Rezultat navedene virtualizacije, dostupnosti cijele IT infrastrukture u oblaku, mogućnost administracije, fleksibilnosti, skalabilnosti i brojni drugi faktori učinili su IT sustave kompleksnijim nego li su ikada bili. Uz niz prednosti, pojavila se i ona negativna strana. Ona se manifestirala u obliku novih prijetnji i kibernetičkih napada, ali se postavilo i pitanje financijske isplativosti. Svi ovi faktori utjecali su na neizbježne promjene perspektive digitalnih forenzičara, pa tako i na njihov pristup forenzičkim istragama.

Neposredno nakon pojave globalne pandemije koja je uslijedila 2020. godine, Microsoft je predstavio moderno unificirano XDR i SIEM rješenje. U samom početku, alati unutar spomenutih rješenja bili su manjkavi po pitanju integracije s rješenjima drugih proizvođača i orijentirani isključivo na oblak te nisu zadovoljavali potrebe organizacija. Nedostaci su još bili zabilježeni po pitanju održavanja lanca dokaza, modelu dijeljene odgovornosti i općenito otežanom provođenju forenzičkih istraga. Dvije godine kasnije, XDR, SIEM, CASB i ostali popratni sustavi izmijenjeni su i nadograđeni brojnim funkcionalnostima i integracijama putem API-a.

U poglavljima koje slijede u nastavku objasnit će se primjenjivost Microsoft sustava i alata u provođenju forenzičkih istraga i analiza prema pojedinim područjima digitalne forenzike. Dodatno će se raspraviti o važnosti lanca posjeda dokaza u oblaku i načinima prikupljanja podataka iz oblaka.

5.1. Područja

U doba općeg prihvaćanja i rasta usluga u oblaku, pokazalo se nedovoljnim nadzirati samo jedan dio IT sustava. Javila se potreba za nadziranje svih komponenata sustava i svakog povezanog krajnjeg uređaja. Takva vrsta pogleda na IT sustav naziva se *Full Stack Monitoring*[11]. Microsoft Defender, Microsoft Defender for Cloud Apps i Sentinel svojim funkcionalnostima *nativno* štite gotovo sve proizvode Microsoft-a neovisno o tome nalaze li se oni na fizičkoj infrastrukturi ili u oblaku. Imajući na umu opseg i kompetitivnost tržišta, razvijena su i brojna prilagođena rješenja koja omogućuju povezivanje Microsoft Sentinela sa sustavima drugih proizvođača.

Količina podataka, distribuiranost širom svijeta, inovativni načini napada i kompromitiranja IT sustava postavili su pred digitalne forenzičare nove izazove. Kako bi uspješnost forenzičke istrage i analize bila zadovoljavajuća, neophodnom se pokazala asistencija sustava u oblaku. Sustavi u oblaku moraju omogućiti identifikaciju, uvid u sustav te njegovu strukturu, otkriti radnje krajnjih korisnika i njihovu interakciju s podacima u oblaku te olakšati pristup podacima uz podršku lancu posjeda dokaza.

U daljnjim poglavljima objasnit će se pojedina područja digitalne forenzike, ukazati na važnost održavanja lanca posjeda dokaza i mogućnost prikupljanja podataka iz oblaka uz podršku modernih sigurnosnih alata proizvedenih od strane Microsoft-a, namijenih zaštiti, ali i asistenciji prilikom provođenja digitalnih forenzičkih istraga.

[11] Full Stack Monitoring – engl. pojam za nadziranje i praćenje svih komponenti IT sustava

5.1.1. Računalna forenzika

Računalna forenzika podrazumijeva prikupljanje i analizu podatka s krajnjeg uređaja odnosno računala neovisno o njegovoj vrsti, proizvođaču, operativnom sustavu ili korisniku. Ti podaci moraju moći odgovori na šest osnovnih pitanja o digitalnim dokazima – tko, što, gdje, kada, zašto i kako? Prema tradicionalnoj forenzičkog praksi, istraga je započinjala fizičkim pristupom računalu i njegovom izolacijom iz postojeće okoline. Tek kad su sigurnosni uvjeti ispunjeni, počinjalo se s ekstrakcijom podataka koji su se potom podvrgavali analizi. Moderni pristup značajno se razlikuje od tradicionalnog, prvenstveno jer je fizički pristup računalu najčešće onemogućen. Dodatnoj razlici doprinijela je i virtualizacija, odnosno korištenje virtualne radne površine ili kratko VDI (engl. *Virtual Desktop Infrastructure*), koja je putem javne ili privatne mreže konstantno dostupna krajnjim korisnicima. Zahvaljujući tome, moguće je kontinuirano nadzirati i pratiti svaki krajnji uređaj neovisno o njegovoj lokaciji.

Microsoft Defender for Endpoint (*u daljnjem tekstu skraćeno - MDE*) XDR rješenje je koje omogućuje instalaciju tzv. agenta i skripti za sve komercijalne operativne sustave koji se nalaze na računalima, ali i na pametnim mobilnim uređajima poput Windows-a, macOS-a, Linux-a, iOS-a i Android-a. Izuzev krajnjih uređaja, MDE agente moguće je rasporediti i na Windows Server i Linux Server poslužitelje te na VDI računala. Jednom kad su svi uređaji unutar IT sustava povezani i dostupni na administrativnim konzolama u oblaku, moguće je konfigurirati brojne funkcionalnosti od kojih se ističu, [37]:

- EDR (engl. *Endpoint Detection & Response*)
- TVM (engl. *Threat & Vulnerability Management)*
- NGP (engl. *Next Generation Protection*)
- ARS (engl. *Attack Surface Reduction*)
- AIR (engl. *Auto Investigation & Remediation*)
- MTE (engl. *Microsoft Threat Experts*)

Svaki od navedenih podsustava svojim funkcionalnostima može značajno doprinijeti forenzičkoj istrazi računala:

- pregled upozorenja unutar sustava, kompletan uvid u pokušaj ili uspješan proboj u sustav kroz krajnje uređaje, poduzimanje adekvatnih radnji za daljnje sprječavanje
- prepoznavanje prijetnji i odgovor na iste u stvarnom vremenu te mogućnost praćenja ranjivosti uređaja, iskorištavanja ranjivosti i pristupa pojedinim dijelovima sustava
- napredna *anti-malware*[12] zaštita u stvarnom vremenu
- Automatizirane istrage bazirane na matematičkim algoritmima, korelacijama i predefiniranim procesima nedvojbeno ubrzavaju i olakšavaju postupak istrage digitalnim forenzičarima smanjujući količinu podataka koju je nekoć bilo potrebno pregledavati

[12] Malware – zlonamjeran softver

Uz prednosti, važno je istaknuti funkcionalnost udaljenog pristupa u stvarnom vremenu putem *shell*-a[13]. Ključni dio svake istrage je pravovremena reakcija i prikupljanje podataka prije njihove izmjene ili brisanja. Udaljeni pristup putem *shell*-a omogućuje trenutno povezivanje na računalo ili poslužitelj koji je pod sumnjom ili potvrđeno kompromitiran. Pored samog udaljenog povezivanja omogućuje i manualno prikupljanje i preuzimanje podataka na udaljeni prostor za pohranu bez znanja krajnjeg korisnika. Po potrebi, dopušta i izvršavanje skupnih naredbi u obliku skripti, [38].

5.1.2. Mrežna forenzika

Potreba za nadziranjem mrežnog prometa i aktivnosti te analizom unutar IT sustava prepoznata je već od ranijih dana postojanja javne mreže. Svrha je zato mrežne forenzike pravovremeno prikupljanje podataka, dokaznih materijala i prepoznavanje neovlaštenog upada tj. pristupa mreži. Ključna i danas aktualna metodologija zvana „OSCAR" prema akronimu „Obtain information, Strategize, Collect evidence, Analyze, Report" sastoji se od pet ključnih faza ili koraka koje je neophodno proći kako bi se provela mrežna forenzička analiza. Uzevši u obzir da je metodologija razvijena početkom 2010. godine može se zaključiti kako nije u potpunosti prilagođena novim mrežnim tehnologijama i protokolima u oblaku.

Današnji mrežni vatrozidi nazvani su vatrozidima nove generacije ili kratko NGFW (engl. *Next Generation Firewall)* te su dizajnirani u skladu s fazama OSCAR metodologije. Nastoje kontinuirano nadirati mrežni promet, pregledavati i analizirati mrežne pakete i izvještavati o statusu mreže. Kako bi uspješno provodili navedene zadatke, potpomognuti su suvremenim rješenjima, odnosno, brojnim algoritmima, strojnim učenjem i umjetnom inteligencijom. Budući da su ključni u provođenju mrežnih forenzičkih analiza, ostatak poglavlja 5.1.2 Mrežna forenzika bit će usmjeren na vatrozide nove generacije, Microsoft Firewall i Sentinel.

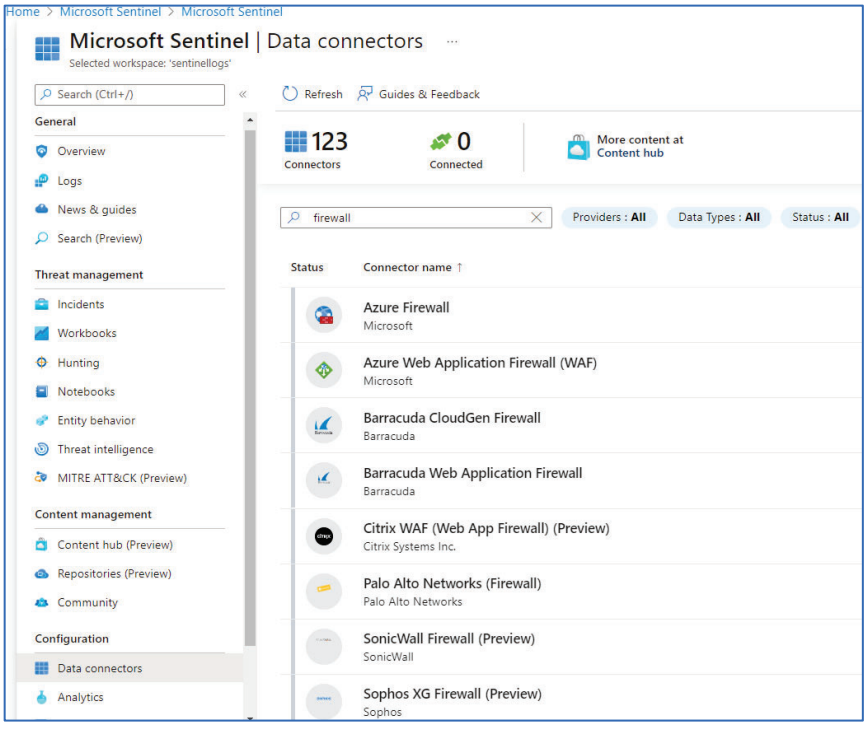
NGFW vatrozidi nadišli su one tradicionalne, obuhvaćajući sada i sloj sesije, prezentacijski sloj i aplikacijski sloj OSI[14] modela, a imaju i mogućnosti prikupljanja gotovo svih ključnih dokaznih materijala koje čine cjeloviti sadržaj, podaci o sesijama, upozorenjima i statistički podaci. Prema VMware-u, NGFW vatrozidi su karakterizirani sljedećim funkcionalnostima, [39]:

- Sustav za prevenciju upada - IPS (engl. *Intrusion Prevention System*)
- Sustav za detekciju upada - IDS (engl. *Intrusion Detection System*)
- Dubinska analiza mrežnog prometa - DPI (engl. *Deep Packet Inspection*)
- Filtriranje prometa aplikacija
- Osviještenost o vanjskim prijetnjama

[13] Remote shell – engl. naziv za softverski alat namijenjen izvršavanju naredbi na udaljenom računalu
[14] OSI – Open Systems Interconnection je prezentacijski model svih slojeva IT sustava

Uzimajući u obzir tržišno natjecanje, tijek razvoja i primjene naprednih vatrozida nove generacije Microsoft je razvio Azure Firewall kao potpuno sigurnosno rješenje vatrozida u oblaku. Prema Gartner-ovom čarobnom kvadrantu za mreže vatrozide za 2021. godinu, [40] Microsoft je svrstan u kategoriju izazivača sa svojim vatrozidom zvanim Azure Firewall. Svojim djelovanjem zahvaća ranije spomenute slojeve OSI modela po uzoru na vatrozide nove generacije, no u kombinaciji sa servisom NSG (engl. *Network Security Group*) i Sentinel sustavom pruža sustav koji svojim djelovanjem može iznimno pridonijeti mrežnoj forenzici.

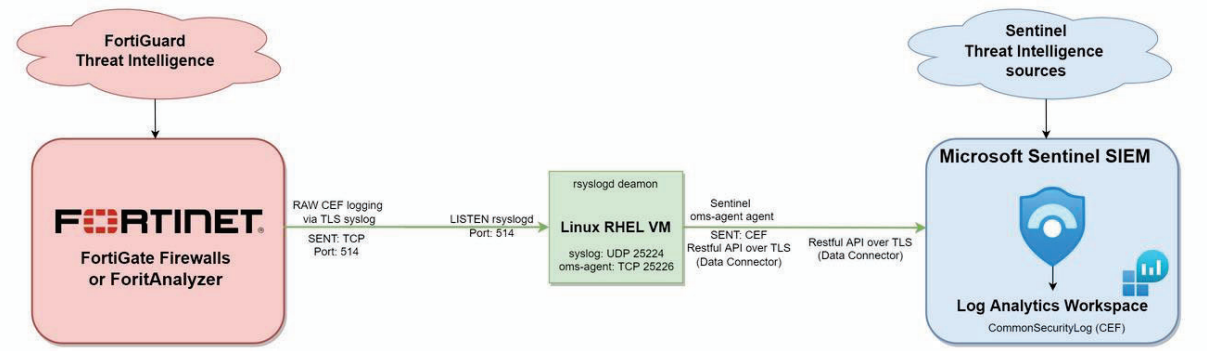
Brojne renomirane organizacije već dugi niz godina koriste vatrozide vodećih proizvođača poput Palo Alto, Fortinet, CheckPoint, Cisco i drugih. Kako bi se doskočilo primjenjivosti Microsoft Sentinel SIEM rješenja, kroz partnerstva između proizvođača dizajnirani su i stvoreni brojni softveri namijenjeni povezivanju dvaju različitih sustava. Poveznici su poznatiji pod nazivom API, spomenuti ranije u poglavlju 4.2. Poveznici omogućuju propuštanje svih informacija iz fizičkih i softverskih mrežnih vatrozida brojnih proizvođača prema Microsoft Sentinel SIEM rješenju, koje iste priprema, analizira i prezentira. Na Slika 12. u nastavku, prikazani su aktualni poveznici koji omogućuju komplementarno djelovanju vatrozida i Sentinel-a.



Slika 12. Snimka zaslona s prikazom sučelja Microsoft Sentinel i poveznici za vatrozid rješenja drugih partnerskih proizvođač

Izuzev prikazanih poveznika za vatrozid rješenja renomiranih proizvođača, potrebno je istaknuti kako su dizajnirani i ustupljeni poveznici i za proizvođače bežičnih mreža i sustava poput Unifi-a. Putem API-a, Unifi kontroler bežičnih mreža može isporučiti sve relevantne informacije o stanju bežičnih mreža.

Za konkretan primjer primjene Microsoft Sentinel i konektora moguće je uzeti Fortinet-ov vatrozid poznat još pod nazivom FortiGate. Jedna od funkcionalnosti kojom se ističe je pohrana logova na udaljenu sigurnu lokaciju u oblaku. Nad njima se provodi analiza od strane rješenja u oblaku potpomognuta strojnim učenjem i umjetnom inteligencijom, zvanom FortiAnalyzer. Prema arhitekturi Sentinel API konektora, na Slika 13. prikazan je način razmjene informacija odnosno komunikacija između FortiAnalyzer-a i Sentinel-a. Svi obrađeni podaci prosljeđuju se direktno prema Sentinelu koji iste pohranjuje na mjesto za čuvanje logova te provodi dodatnu analizu i prikazuje sve u centraliziranoj konzoli.



Slika 13. Prikaz komunikacije između vatrozida i SIEM sustava pomoću API poveznika, [41]

Samo neke od radnji koje su podržane od strane poveznika su navedene u nastavku, [41]:

- Prepoznavanje maliciozne IP adrese
- Prepoznavanje malicioznog DNS naziva
- Prepoznavanje malicioznog mrežnog prometa između lokalne i širokopojasne mreže
- Prepoznavanje neželjenih i zlonamjernih aplikacija
- Prepoznavanje IP adrese i komunikacije između kompromitiranih računala

Razvijena rješenja pružaju značajnu podršku prilikom provođenja mrežnih forenzičkih istraga. Dodatnu prednost donijela je komplementarnost različitih sustava, pohrana zapisa na udaljenim lokacijama u oblaku dok je revoluciju označila automatizacija nekad ručnih procesa odnosno analize, povezivanja i prezentacije.

5.1.3. Forenzika mobilnih uređaja

Razvoj nove bežične komunikacijske mreže 5G dodatno je proširio postojeće funkcionalnosti i potaknuo kontinuirani rast korištenja pametnih mobilnih uređaja. Prema predviđanjima Ericsson-ovog izvještaja mobilnosti iz 2022. godine, [42], broj mobilnih pretplata povezanih s 5G mrežom prijeći će 4,4 milijarde do kraja 2027. godine. Također, prosječna potrošnja mobilnog prometa prijeći će 15 GB krajem 2022. godine. Rapidan rast označava i povećanje korištenja pametnih mobilnih uređaja (u daljnjem tekstu PMU) u poslovne svrhe. Brojne renomirane organizacije i dalje uz iznimne napore nastoje zaštiti inventar PMU, ali i izolirati IT sustav od već godinama poznatog izazova zvanog BYOD. Putem PMU, organizacije se izlažu brojnim napadima od koji su najčešći, [43]:

- Socijalni inženjering - Phishing
- Curenju podataka putem malicioznih aplikacija
- Povezivanje na nesigurne mreže
- Krađa uređaja
- Ne ažurirani operativni sustav
- Pretjerana dopuštenja aplikacijama

Prema autoriziranim predavanjima kolegija forenzička analiza informacijsko komunikacijskog sustava, [44], digitalna forenzika mobilnih uređaja provodi se ako incident ukazuje da je proboj u sustav nastao kao posljedica kompromitiranja mobilnog uređaja. Recentna metodologija CPEEP (engl. *Cellular Phone Evidence Extraction Process*) dizajnirana od strane SANS-a definira 9. slijednih koraka kako bi se provela forenzička analiza. Koraci su: uvođenje, identifikacija, priprema, izolacija, procesiranje, verifikacija, dokumentiranje, prezentacija, arhiviranje.

Zbog širokog spektra uređaja, specifičnosti softvera i općenito kompleksnosti provođenja forenzičke analize mobilnih uređaja, razni sustavi zaštite i nadziranja inventara PMU ne mogu u potpunosti provesti analizu, ali svojim djelovanjem mogu potpomoći provođenju iste. Jedno od takvih XDR rješenja je MDE koje kao i kod računala omogućuje nadzor, sigurnost i kontrolu. Podržana su dva opće prihvaćena operativna sustava Android i iOS koja se s centralnim sustavom povezuju putem aplikacije Microsoft Defender kao krajnje točke zadužene za komunikaciju i nadzor. Brojnost digitalnih dokaza koji se nalaze na PMU proizlazi iz navika samih korisnika. Svakom uporabom i iteracijom prilikom korištenja uređaja, korisnici nesvjesno ostavljaju brojne digitalne tragove.

U nastavku na Tablica 2. prikazane su funkcionalnosti kojima MDE XDR potpomaže u provođenju istrage, prema fazi identifikacije i pripreme recentne metodologije CPEEP, kategorizirani su u tablici u nastavku:

Tablica 2. Prikaz vrsta informacija koje je moguće prikupiti od strane MDE XDR sustava s pametnih mobilnih uređaja Izvor: [45], [46]

Faze:	**Prikupljeni/generirani podaci od strane XDR sustava**
Identifikacija	Vrsta i verzija operativnog sustava Informacije o procesoru, radnoj memoriji i pohrani MAC adresa WiFi adaptera ICCID SIM kartice Serijski broj, IMEI AndrodID, GUID AAD ID, Azure User ID Azure Tenant ID Organizacijski ID
Priprema	Korištenost aplikacija, procesora i mrežnog prometa Stanje uređaja iz perspektive aplikacija, dodijeljena prava pristupa, status ažuriranosti aplikacija Konfigurirane sigurnosne funkcionalnosti od strane XDR sustava Osnovne informacije o web preglednicima Informacije o korištenim protokolima Lista aplikacija, putanje na kojoj su instalirane aplikacije, verzija i naziv proizvođača Detaljni popis interakcije s korporativnim dokumentima na oblaku

Korak izolacije označava specifičan postupak fizičke izolacije uređaja iz okoline, odnosno onemogućavanja bilo koje vrste komunikacije. No ne omogućuju ga XDR rješenja, već digitalni forenzičari specijalizirani za provođenje mobilne forenzičke istrage. U daljnjim koracima tijekom faze analize, verifikacije i dokumentiranja, kombinacija rješenja MDE, MDCA i Microsoft Sentinel svoj funkcionalnostima mogu doprinijeti na sljedeći način:

- Grafički i tekstualni uvid u tijek događaja
- Izvještaji o zlonamjernom softveru, pokušajima napada phishing-om, ranjivosti operativnog sustava, procjene ranjivosti aplikacija, mrežne zaštite
- Prijedlozi konfiguracije i daljnjih koraka kako bi se minimizirao utjecaj na sustav i pospješila sigurnost mobilnih uređaja, [47]

5.1.4. Email forenzika

Usluga slanja digitalne pošte (u nastavku „e-mail[15]“) uz sve promjene posljednjih desetljeća i dalje je ostala standard i osnovni vid poslovne komunikacije. Kibernetička sigurnost značajno je napredovala, dok e-mail sustavi i komunikacijom e-mail-om ostaju bazirani na starim nepromijenjenim protokolima dizajniranim prije više od tri desetljeća. Računajući na taj nedostatak, svakodnevno se dizajniraju novi napadi temeljeni na iskorištavanju zastarjele e-mail arhitekture, ali i lakovjernosti krajnjih korisnika i općenito nedostatka zaštitnih mehanizama e-mail komunikacije. Prema izvješću Proofpoint 2022 State of Phishing Report, [48], 83% ispitanika potvrdilo je kako je njihova organizacija uspješno zaprimila najmanje jedan „Phishing[16] mail“ u 2021 godini. Također, zabilježeno je povećanje od 214.345 jedinstvenih Phishing web stranica, što označava povećanje za 50% u odnosu na 2020.-tu godinu. Otprilike 30% pristiglih Phishing mailova je otvoreno od strane krajnjih korisnika, dok je od toga 42% korisnika pokušalo otvoriti sumnjivu poveznicu ili privitak. Spomenuto izvješće jasno prikazuje kako se uspješnost kompromitiranja pojedinih IT sustava i dalje temelji na iskorištavanju najranjivije točke odnosno ljudskog faktora. U trenutku kad jedan od krajnjih korisnika nesvjesno podlegne napadu, a tzv. „treća strana“ uspije pristupiti sustavu, otvaraju se mogućnost za kompromitiranje i drugih korisničkih računa, ali i za manipulaciju u komunikaciji između organizacije i vanjskih partnera i/ili klijenata.

E-mail forenzika posebna je disciplina digitalne forenzike čiji je primarni zadatak istražiti i analizirati izvor i sadržaj mail-ova koji su ranije prikupljeni kao digitalni dokaz. Prema literaturi Cyber Security and Digital Forensics, [49], tehnike koje se provode unutar email forenzike podrazumijevaju:

- Analizu zaglavlja
- Analiza poveznica i privitaka
- Istragu servera
- Istragu mrežnih uređaja
- Istraga prikrivanja otisaka

[15] E-mail – engl. pojam koja označava digitalnu poštu
[16] Phishing – metoda kibernetičkog napada temeljena na obmanjujućem e-mail sadržaju

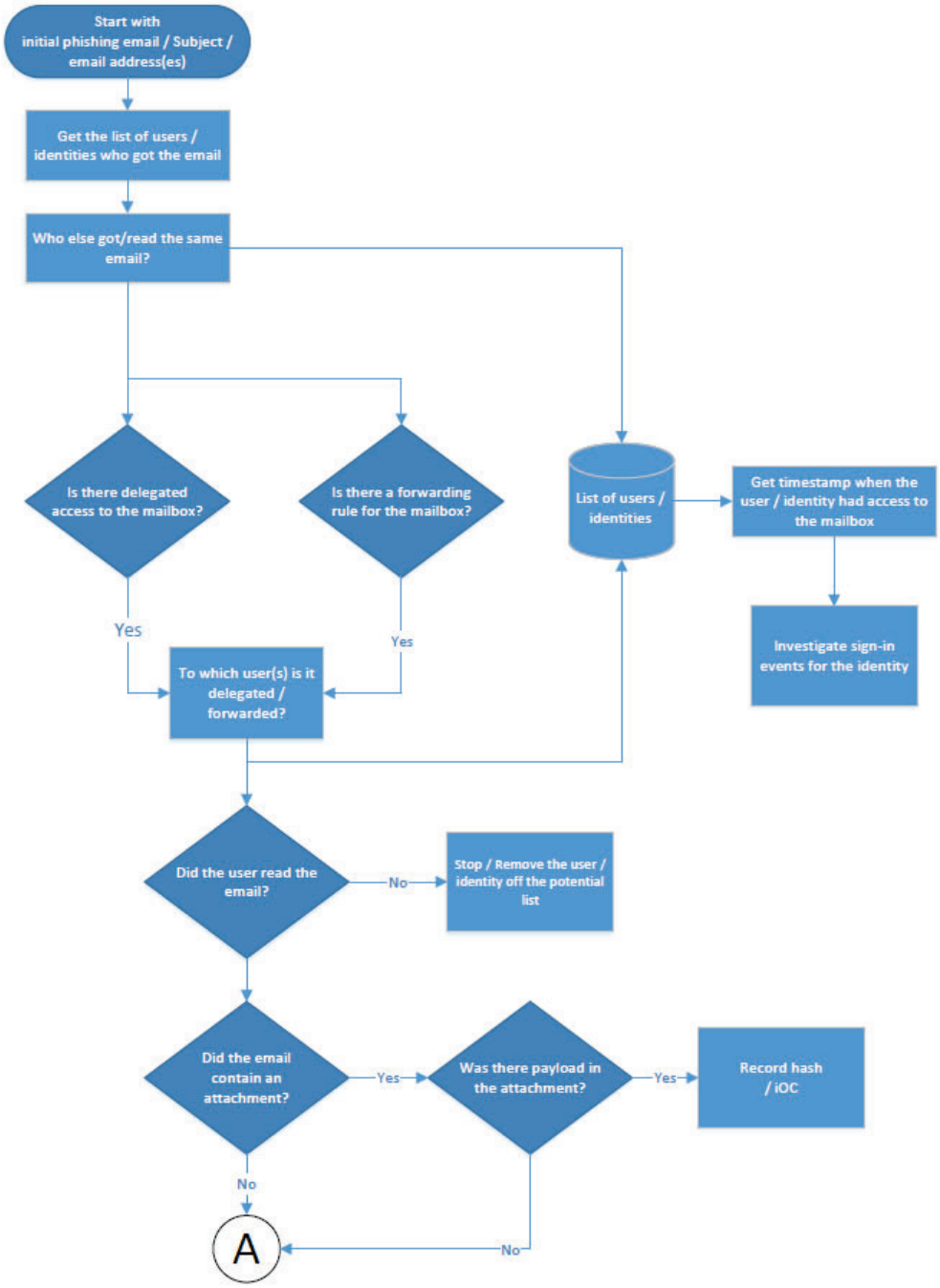
Pristup tradicionalne forenzike prema email analizi bio je orijentiran na samo mjesto gdje je mail pohranjen. U slučaju POP konfiguracije unutar mail klijenta, pristigli i poslani mailovi bili bi pohranjeni direktno na krajnji uređaj u mail bazu. Ekstrakcijom mail baze, analizom specifičnih mailova i njihovih zaglavlja, dolazilo bi se do određenih informacija koje bi poslužile kao temeljni digitalni dokaz u istrazi. Moderni pristup e-mail forenzike nalaže udaljeni pristup, odnosno istragu direktno na samom serveru kroz centraliziranu web konzolu. Ono ne ovisi o fizičkoj udaljenosti uređaja na kojoj je mail pohranjen.

Microsoft Defender for Office 365 (u daljnjem tekstu skraćeno MDO) je moderno rješenje namijenjeno primarno nadziranju i zaštiti Microsoft mail rješenja, odnosno Exchange Online servisa koji omogućava sinkronizaciju maila s mail klijentom Outlook. Izuzev same zaštite, omogućuje široki spektar integriranih alata koji omogućuju detaljnu analizu poslanih i zaprimljenih mail poruka. U Tablica 3. prikazani su alati MDO koji svojim funkcionalnostima mogu prikupiti informacije koje su od forenzičke vrijednosti.

Tablica 3. Popis funkcionalnosti i produkta od forenzičke vrijednosti

Otkrivanje
• grupni prikaz odnosno kontrolna ploča s listom primljenih i poslanih mailova •prikaz URL-ova unutar mailova, prikaz mail adresa koje su podložne zlonamjernim mailovima •filtriranja po raznim kategorijama, eDiscovery
Istrage
•istraživanje podrijetla mail-ova, pregled primjenjenih sigurnosnih politika i mehanizama •pregled i analiza zaglavlja mail-a •pregled i filtriranje mail-ova prema vremenskoj crti
Pregled
•Uvid u obavještajni centar i generirane obavijest od strane sustave o zlonamjernim mailovima •Uvid u karantenu unutar koje se nalaze sumnjive i privremeno zadržane mail poruke •Uvid u blokirane interne mail adrese za koje se smatra da su kompromitirane
Kampanje
•Prepoznavanje i istraga prepoznatih Phishing i spam kampanja usmjerenih prema organizaciji

Pored spomenutih alata i vrijednosti koje mogu generirati za forenzičku istragu, neophodno je spomenuti funkcionalnost vođene istrage. Kao primjer, na Slika 14. prikazan je blok dijagram toka istrage Phishing mail napada.



Slika 14. Primjer toka vođene istrage u email forenzici koristeći se Microsoft Defender for Office 365 alatima, [50]

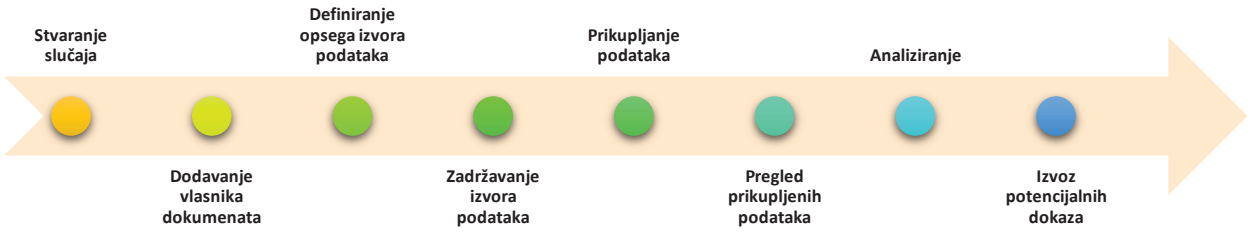
Primjenjivost novih funkcionalnosti MDO baziranih u oblaku važne su za forenzičke istrage email usluge zbog direktnog uvida u mail sustav samog poslužitelja. Alati za istragu koji se nalaze na platformi dostupni su unatoč udaljenosti, a moguće im je pristupiti s bilo kojeg računala, a vođenje je istrage također moguće prilagoditi potrebama i mogućnostima.

5.1.5. Forenzika dokumenata

U svakoj forenzičkoj istrazi neovisno bila ona fizička ili digitalna, manualno ili digitalno pisani dokumenti učestalo sadržavaju informacije od vrijednosti za forenzičku istragu. Poznavajući radne procese raznih organizacija, lako je zaključiti kako se povjerljive informacije nalaze zapisane unutar digitalnih dokumenata.

U odnosu na nekadašnju pohranu fizičkih dokumenata, digitalnih dokumenti mogu lako biti umnožavani i disperzirani na širok spektar uređaja za pohranu. Dodatni izazov predstavljen je s pohranom dokumenata u oblaku. Pored izazova lokacije pohrane, u interakciji s oblakom pojavljuje se metoda takozvane sinkronizacije. Dokumenti pohranjeni na internoj memoriji računala ili prijenosnog mobilnog uređaja sinkroniziraju se pomoću agenta odnosno aplikacije putem javne mreže na oblak. Takva funkcionalnost omogućila je interaktivno uređivanja dokumenata na više lokacije, ali i uređivanje dokumenata od strane više sudionika u stvarnom vremenu čime se dodatno otežalo prikupljanje i analiza.

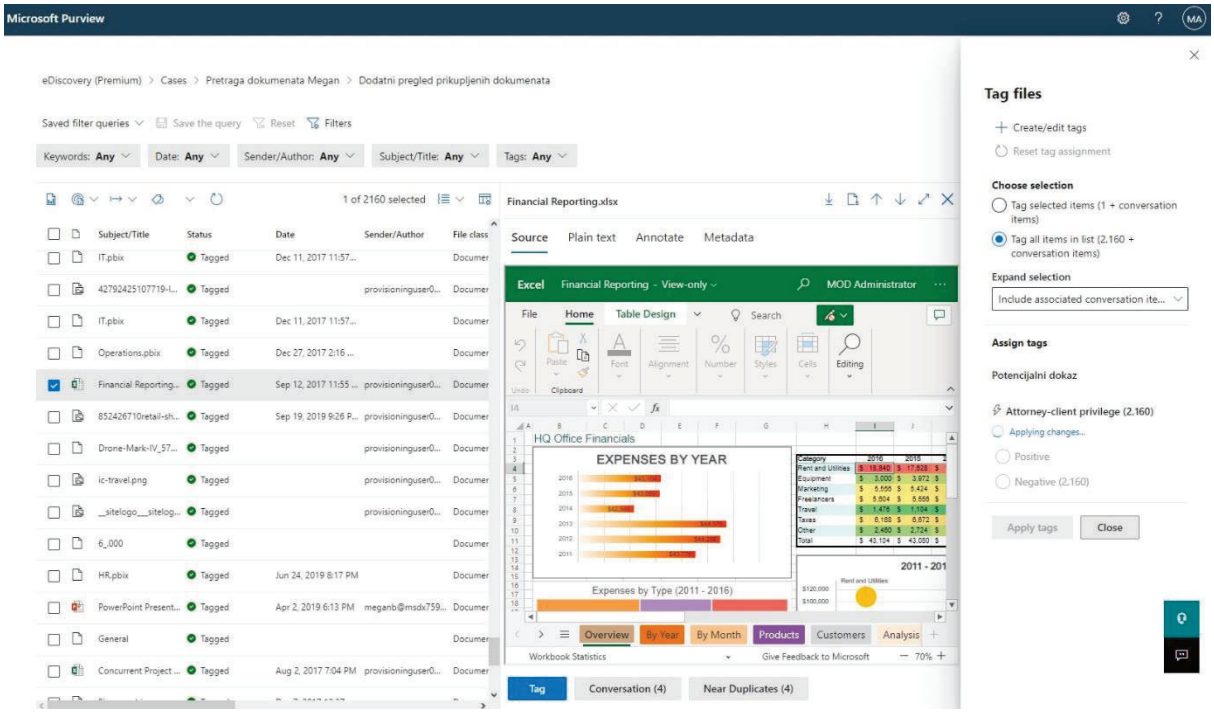
Kako bi se adekvatno adresirali izazovi pohrane u oblaku i sinkronizacije, stvoreni su alati za pretragu i analizu digitalno temeljenih dokaza pohranjenih u oblaku. Primjer takvog alata je Microsoft eDiscovery Premium. Temeljen i dizajniran na preporučenim digitalnim forenzičkim procesima i recentnom modelu elektroničkog otkrivanja ili kratko EDRM-u (engl. *Electronic Discovery Reference Model*) stvorenom od strane EDRM globalnog savjetodavnog vijeća, [51]. Tijek prikupljanja podataka i analize pomoću eDiscovery Premium alata prikazan je u nastavku na Slika 15.



Slika 15. Grafički prikaz tijeka provođenja istrage pomoću alata eDiscovery Premium
Izvor: [51]

Unatoč činjenici da navedeni alat nije kategoriziran kao dio XDR i SIEM rješenja, neophodno je njegovo poznavanje zbog funkcionalnosti, ali i utjecaja koji može imati na samu istragu. Oblak kao unificirani sustav povezanih mogućnosti ipak i ovaj alat indirektno povezuje sa Sentinel rješenjem. Iz takve komplementarnosti proizlaze dodatni uvidi u samo ponašanje krajnjih korisnika što dodatno može pridonijeti digitalnim forenzičarima u definiranju slučaja.

Na Slika 16. prikazana je snimka zaslona alata eDiscovery Premium u trenutku pregleda i označavanja relevantnih dokumenata za istragu unutar prikupljenih podataka.



Slika 16. Snimka zaslona alata eDiscovery Premium u trenutku pregleda i označavanje relevantnih dokumenata za forenzičku istragu

Uzevši u obzir iznimno jednostavnu pohranu, sinkronizaciju, lako dijeljenje i zajedničko uređivanje dokumenata, logično je za zaključiti kako će pojedine organizacije i financijske institucije pažnju usmjeriti na alate koji mogu kriptirati dokumente. Izazov provođenja analize nad kriptiranim dokumentima unutar Microsoft oblaka riješen je putem eDiscovery alata, ali uz određena ograničenja. U budućnosti se očekuju dodatna poboljšanja u smislu funkcionalnosti, jednostavnosti korištenja ali prije svega i automatizacije pojedinih procesa kako bi se smanjilo vrijeme potrebno za provođenje istrage.

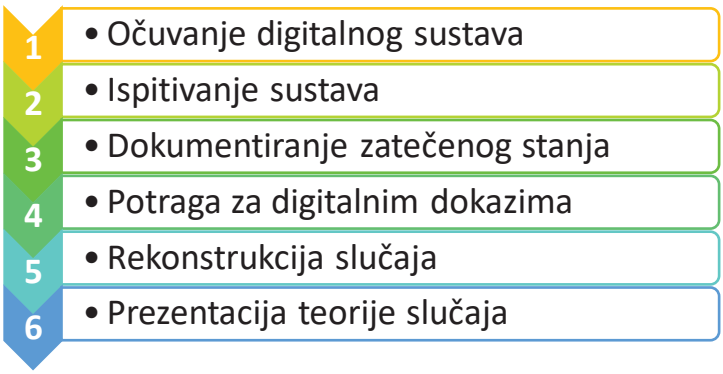
5.2. Lanac posjeda dokaza u oblaku

Lanac posjeda dokaza ili kratko CoC (engl. *Chain of Custody*) je konkretna pismena dokumentacija koja prati logičan slijed zaprimanja, pripreme, analize i prijenosa elektroničkog dokaza tijekom cijelog trajanja, odnosno provođenja digitalne forenzičke istrage. Adekvatno rukovanje dokaznim materijalima, potvrda da dokazi nisu kompromitirani, a kontinuiranim dokumentiranjem lanca posjeda dokaza osigurava se validnost svih dokaznih materijala u trenutku suđenja.

Načela svakog lanca posjeda dokaza su:

- Analiza se nikada ne smije provoditi na originalnim dokazima
- Mjesto za pohranu mora biti ili novo odnosno nikad korišteno ili formatirano tako da se ne može niti na koji način pristupiti prethodnim podacima
- Dokumentiranje svakog poduzetog osnovnog ali i dodatnog koraka
- Osiguravanje istrage i sigurnosti sustava od daljnjih promjena i zlonamjernih aktivnosti

Prema članku Digital Chain of Custody: State of The Art, [52], na Slika 17. navedeni su koraci upravljanja digitalnim dokazima tokom kojih je neophodno kontinuirano dokumentirati lanac posjeda dokaza:



Slika 17. Temeljni koraci upravljanja digitalnim dokazima
Izvor: [52]

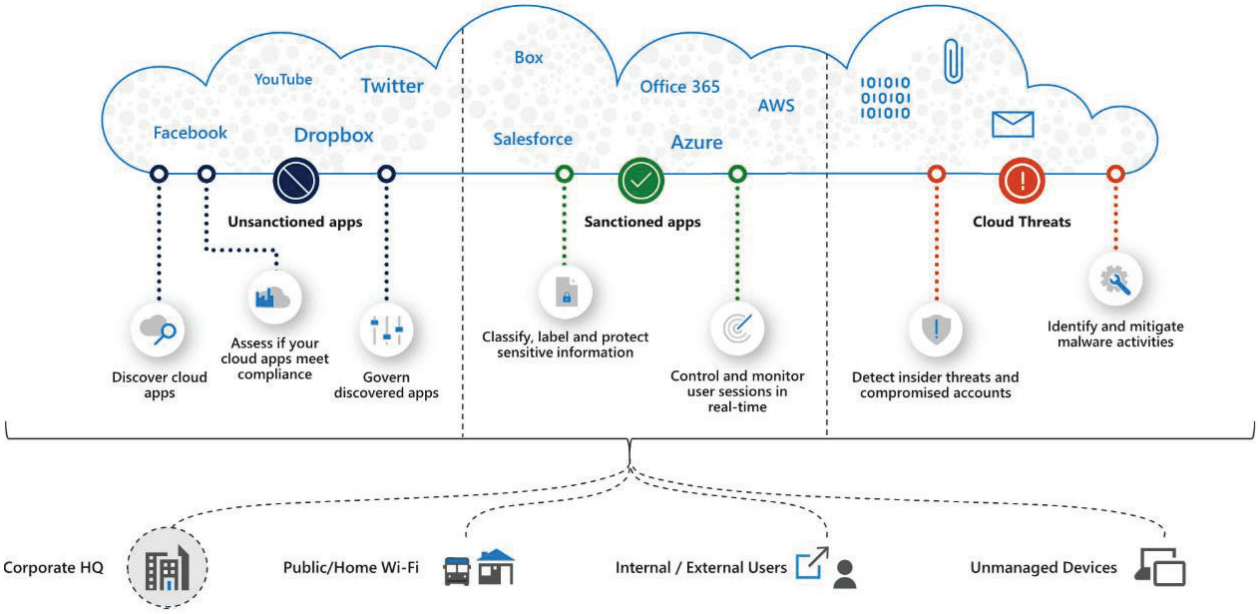
Microsoft 365 kao SaaS usluga u smislu odgovornosti nakon sigurnosnog incidenta temelji se na modelu dijeljene odgovornosti. Pojednostavljeno rečeno, proizvođači usluga u oblaku garantiraju sigurnost samog oblaka, dok su za sigurnost unutar oblaka i pohranjenih podataka odgovorne organizacije odnosno korisnici. Microsoft sigurnosna rješenja omogućena su krajnjim korisnicima odnosno odgovornim osobama kako bi upravljali sigurnošću ali i bili u mogućnost asistirati u digitalnim forenzičkim istragama s ustupljenim i adekvatno konfiguriranim alatima.

Primjer alata temeljenog na očuvanju originalnih podataka u neizbrisivom i neizmjenjivom formatu je ranije spomenuta nova verzija Microsoft eDiscovery Premium alata dizajniranog prema EDRM modelu. Ključna funkcionalnost koja podržava lanac posjeda dokaznih materijala je očuvanje odnosno zaključavanje podataka i blokiranje njihove promjene, premještanja i brisanja. Sukladno provedenim koracima, prikupljeni skup informacija validan je za daljnji pregled i predaju uz očuvanje lanca posjeda dokaza.

Neizbježan izazov s kojim se digitalni forenzičari susreću u doba sve većeg prihvaćanja usluga u oblaku je provedba digitalne forenzičke istrage nad virtualnim računalima. Dodatni izazov stvaraju kriptirana virtualna računala kojima je pristup gotovo u potpunosti onemogućen. Drugi primjer alata koji posebnu pažnju posvećuje očuvanju lanca posjeda u oblaku je sama Azure platforma. Azure oblak je svojoj arhitekturi i funkcionalnostima prilagođen kako bi cijela virtualna računala prema potrebi premjestio u zaseban virtualni kontejner unutar kojega bi sadržaj virtualnih računala bio zadržan. Kao i u fizičkoj provedbi računalne forenzičke analize, sadržaj cijelog virtualnog računala se klonira odnosno izrađuje se takozvani „snapshot“ i pohranjuje na nepromjenjiv prostor za pohranu. Prostor za nepromjenjivu pohranu (engl. *Immutable Azure Blob Storage*) namijenjen je pohrani neophodnih podataka za poslovanje koji uvjetuje jedno zapisivanje podataka i nemogućnost naknadne izmjeni istih. Izuzev pohrane moguća je isporuka ključa za dekriptiranje svake kopije kriptiranih virtualnih računala. Dodatno, kako bi se vrijeme od prepoznavanja nepoželjnog događaja do završetka provođenja digitalne forenzičke analize minimiziralo, digitalnim forenzičarima omogućen je direktan udaljeni pristup kriptiranoj kopiji virtualnog računala u VHD formatu putem Azure Storage Explorer aplikacije i specifičnog ključa za dijeljeni pristup, [53].

5.3. Pretraga podataka u oblaku

Primjer jednog od alata namijenjenom naprednom pretraživanju podataka je Microsoft Defender for Cloud Apps odnosno CASB (engl. *Cloud Access Security Broker*) sustav namijenjen nadziranju svake interakcije između oblaka i krajnjih korisnika. Kroz web sučelje moguće je na jednostavan način i u kratkom vremenu prikupiti sve potrebne podatke o interakciji korisničkog računa, odnosno krajnjeg korisnika s oblakom. Svaki izrađeni i preuzeti izvještaj označen je hash vrijednošću kojim se može potvrditi autentičnost preuzetih informacija.



Slika 18. Grafički prikaz Microsoft Defender for Cloud Apps strukture i funkcionalnosti, [54]

Prema Slici 18. prikazanoj iznad, vidljivo je kako CASB sustavi omogućuju jasnu vidljivost i povezanost različitih platformi i usluga u oblaku putem javne mreže koja se smatra ključnom u fazi identifikacije. Microsoft Defender for Cloud sustav dizajniran je kao hibridni sustav koji se povezuje s drugim aplikacijama u oblaku putem API-a, kombiniranim s ulogom obrnutog posrednika u prosljeđivanju korisničkih sesija prema oblaku. Takav dizajn omogućio je detaljan uvid u svaku interakciju korisničkih računa s aplikacijama i podacima na oblaku, primjenu raznih politika usklađenosti i sigurnosti te prepoznavanje sumnjivih aktivnosti, [55].

Relevantne funkcionalnost u procesu identifikacije i prikupljanja podataka pomoću Microsoft Defender for Cloud sustava prikazane su u Tablica 4. u nastavku:

Tablica 4. Kategorizacija funkcionalnosti Microsoft Defender for Cloud sustava

Kategorija	Funkcionalnosti
Zapis o aktivnostima	- Vrsta aktivnosti i povezane aktivnosti - Prikaz datuma, vrste uređaja i aplikacije - Prikaz IP adrese, ISP-a i lokacije - Povijest aktivnosti za pojedinog korisnika - Interaktivna karta lokacije
Datoteke	- Prikaz naziva datoteke, vlasnika i suradnika - Prikaz datuma izrade i zadnjeg uređivanja - Direktna poveznica na dokument - Prikaz strukture direktorija i dodatna pretraga - Pregled povezanih aktivnosti - Mogućnost uskraćivanja pristupa
Korisnički računi	- Prikaz korisničkog imena, mail adrese, statusa aktivnosti - Prikaz datuma i sata kad je detektirana zadnja aktivnost - Pregled povezanih aktivnosti, upozorenja, datoteka - Mogućnost označavanja kompromitiranog korisničkog računa - Mogućnost traženja ponovne prijave - Mogućnost suspendiranja korisničkog računa
Sigurnosna konfiguracija	- Prikaz preporuka za poboljšanje sigurnosnih politika i konfiguracije za povezane sustave u oblaku
Status sigurnosti identiteta	- Prikaz predloženih radnji za povećanje stupnja sigurnosti i zaštite korisničkih računa (identiteta)
OAuth aplikacije	- Pregled dozvola dodijeljenih vanjskim aplikacijama - Pregled povezanih aktivnosti koje su omogućile dodijeljene dozvole
Povezane aplikacije	- Mogućnost dodatnog povezivanja s vanjskim aplikacijama - Kontrole i uvjetovani pristup aplikacijama - Testiranje i status povezanosti s vanjskim aplikacijama

Prikazane funkcionalnosti isporučuju često tražene odgovore na pitanja o radnjama krajnjih korisnika prilikom provođenja forenzičke istrage. Značajnu asistenciju pri provođenju analize predstavlja grafički kronološki prikaz aktivnosti dostupan za svaki korisnički račun individualno za zadnjih 7 dana. Manualno je dostupno pretraživanje aktivnosti i obavijesti za period u zadnjih 180 dana, dok se otkriveni podaci o datotekama čuvaju i prikazuju za zadnjih 90 dana.

6. PROVEDBA DIGITALNE FORENZIČKE ANALIZE

U ovom poglavlju, prikazat će se provedba digitalne forenzičke istrage, simulirane okoline davatelja usluga u oblaku Microsoft 365 i Azure, uz korištenje rješenja Microsoft 365 Defender i Microsoft Sentinel.

Konkretan slučaj, temelji se na prijavi organizacije „Contoso“ o prepoznatim potencijalnim napadima na njihov sustav. Kako bi se slučaj pravovremeno provjerio, prema potrebi očistio od prijetnji i općenito održala sigurnost unutar sustav, organizacija Contoso angažirala je privatne digitalne istražitelje kako proveli digitalnu forenzičku istragu. Prve dostupne informacije koje oblikuju slučaj a ustupljene su od strane IT odjela Contoso:

- IT sustav organizacije Contoso primarno se temelji na uslugama u oblaku ustupljenim od strane raznih proizvođača
- Primarni sustav kojim se tvrtka koristi je SaaS rješenje Microsoft 365 i Azure oblakom na kojemu se nalazi nekoliko virtualiziranih računala
- Obavijest o upozorenjima i incidentima ukazuju kako postoji razlog za zabrinutog zbog napada na virtualno računalo naziva „testmachine1“
- Potencijalne opasnosti za sustav prepoznate su zahvaljujući adekvatno implementiranom rješenju Microsoft Defender for Endpoint koje je povezano sa svakim fizičkim i virtualnim računalom te prijenosnim mobilnim uređajima

Na Slika 19. u nastavku, prikazana su dodatna dva koraka u cijelom procesu neophodna u provođenju forenzičke istrage zbog same naravi sustava u oblaku.



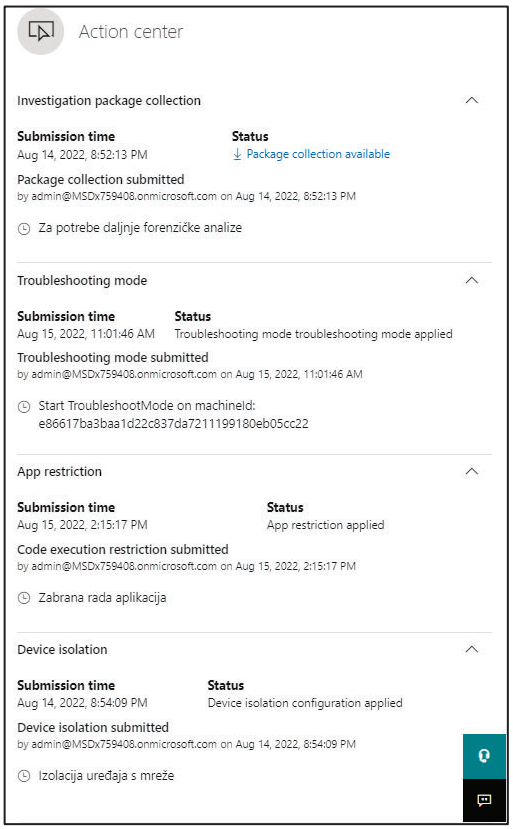
Slika 19. Faze OCFM modela

Za potrebe korištenja istrage koristit će se relevantan forenzički model OCFM (engl. *Open Cloud Forensics Model*) koji u odnosu na standardni proces koji podrazumijeva faze identifikacije, prikupljanja, analize i prezentacije dodatno sadrži i fazu očuvanja na početku i verifikacije na samome kraju.

6.1. Očuvanje

Microsoft Defender for Endpoint kao dio XDR sustav kontinuirano vrši komunikaciju sa svim povezanim krajnjim uređajima koju zatim pohranjuje unutar oblaka kako bi istu prikazao unutar web sučelja krajnjem korisniku. Podaci se fizički nalaze u više podatkovnih centara unutar Europske unije, ovisno o odabranoj lokaciji prilikom sklapanja ugovora o korištenju usluga u oblaku. Za regiju zapadne Europe, lokacija podatkovnih centara je Nizozemska. Izuzev same lokacije, potrebno je znati da je svim podacima moguće isključivo pristupiti koristeći se identitetom povezanim sa samom organizacijom, s adekvatnim pravima pristupa. Prema ugovoru o korištenju, garantirano je čuvanje svih podataka stvorenih u oblaku do 180 dana te ih je tijekom tog perioda moguće vratiti u slučaju potrebe, uključujući i podatke generirane od strane povezanih računala i uređaja s XDR sustavom. Podatke o događajima o sustavu nije moguće mijenjati niti brisati s platforme, što potvrđuje da su isti očuvani, ali je moguće upravljati trajanjem njihova čuvanja odnosno postojanja i prikaza u web platformama.

Dodatno, kako bi osigurali računalo od mogućnosti komunikacije s drugim računalima unutar mreže, ali i s uslugama u oblaku , unutar same web platforme Microsoft 365 Defender dostupna je opcija izolacije računala i zabrana izvršavanja svih aplikacija od drugih proizvođača. Na snimci zaslona prikazanoj na Slika 20. u nastavku, kroz takozvani akcijski centar, vidljive su izvršene naredbe izolacije uređaja kako bi računalo ostalo u istom, zatečenom stanju.

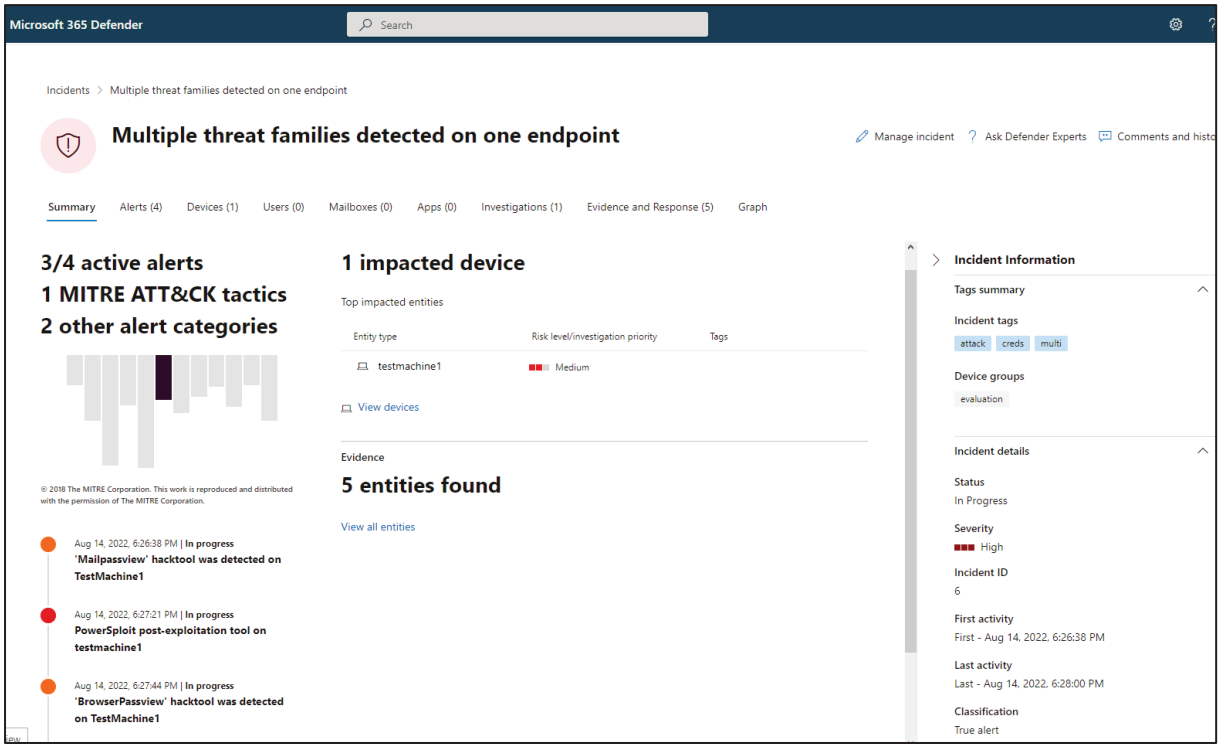


Slika 20. Snimka zaslona s prikazanim akcijskim centrom i provedenim metodama izolacije

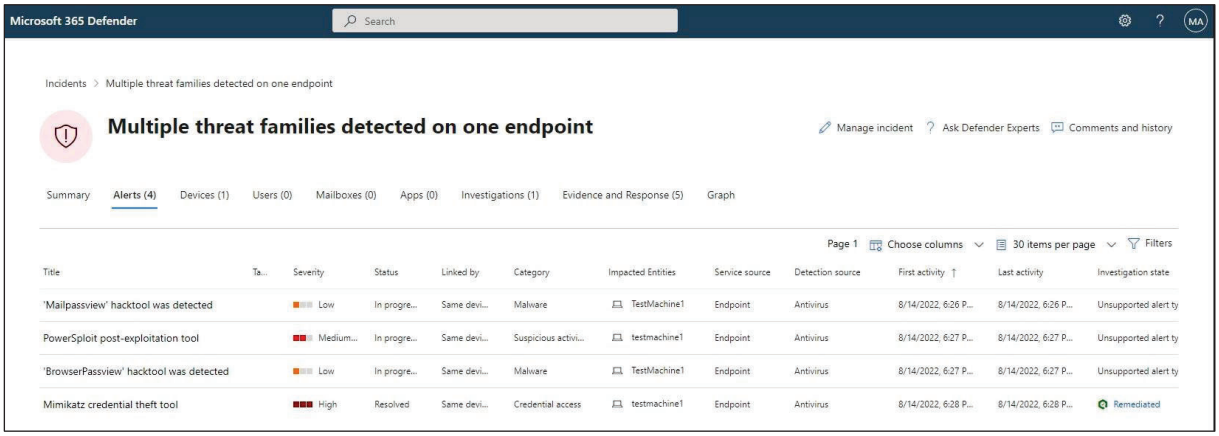
Faza očuvanja generiranih podataka već je od strane sustava autonomno napravljena, dok je za izolaciju pojedinih krajnjih uređaja, koju je moguće napraviti udaljenim putem koristeći se web portalom zadužena odgovorna osoba tj. forenzički istražitelj. Neovisno o dostupnosti podataka u web sučelju, forenzički istražitelj dužan je sve dostupne podatke ekstrahirati i osigurati od njihove namjerne ili slučajne izmjene kako bi se održano lanac posjeda dokaza, ali i uspješno provela verifikacija na kraju forenzičke istrage.

6.2. Identifikacija

Identifikacija kao faza istrage podrazumijeva pomni pregled podataka relevantnih za daljnju analizu, odnosno podataka s forenzičkom vrijednošću koji mogu biti predstavljeni kao digitalni dokaz. Kao što je spomenuto u poglavlju 4., XDR sustavi sa svojim funkcionalnostima proaktivno prikupljaju i pregledavaju podatke kako bi identificirali i prevenirali potencijalne napade unutar organizacije, obavijestili i upozorili odgovorne osobe te potpomogli daljnjoj istrazi s relevantnim podacima.



Slika 21. Snimka zaslona s prikazanim incidentom, brojem ugroženih uređaja i općim statusom

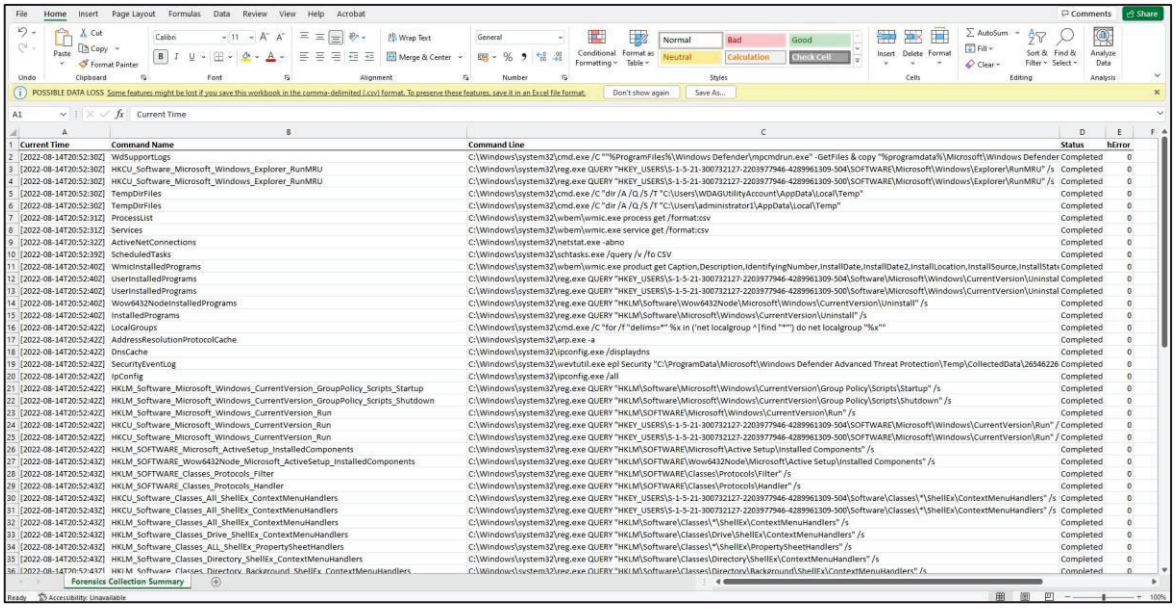


Slika 22. Snimka zaslona s prikazom obavijesti o višestrukim zlonamjernim aktivnostima

U slučaju organizacije Contoso, na iznad prikazanim snimkama zaslona Slika 21. i Slika 22. vidljivo je kako je MDE sustav zamijetio četiri slijedne radnje na računalu „testmachine1“ i u pozadini zabilježio sve interakcije sustava i aplikacija, servise, stanje i povezanosti s mrežom, korištene i spremljene dokumente, ali i brojne druge informacije.

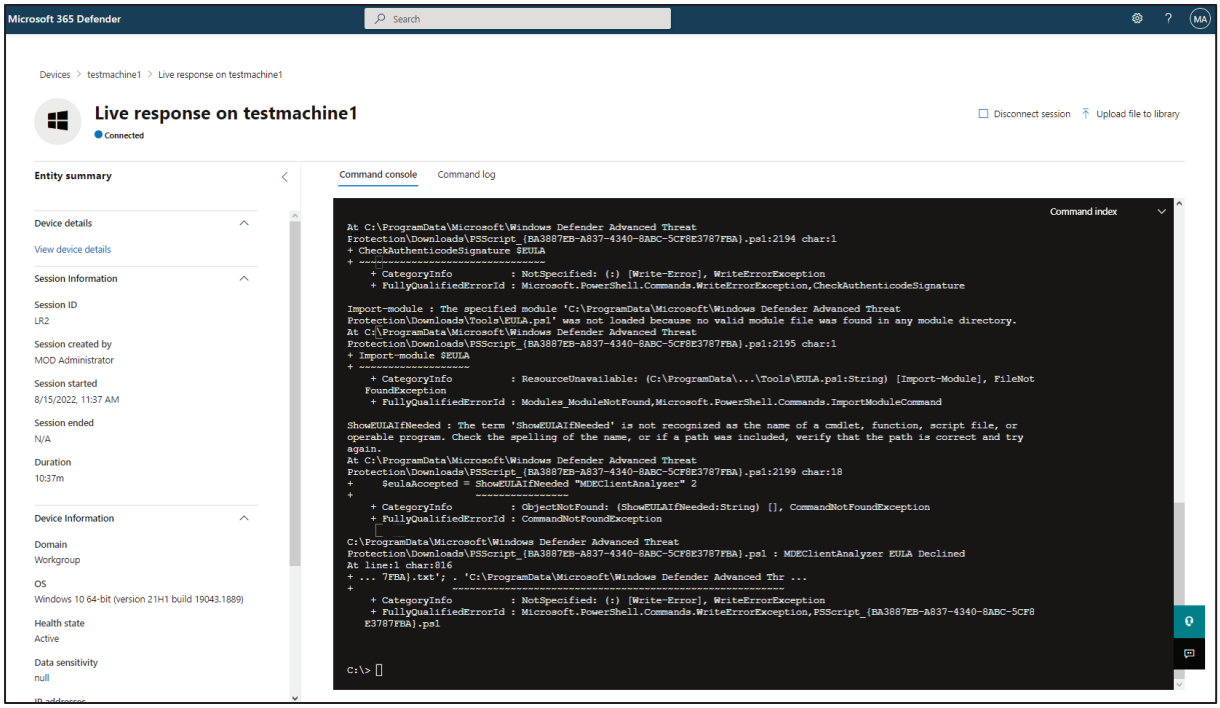
6.3. Prikupljanje

U fazi prikupljanja, pažnja se posvećuje dodatnom pregledu sustava i prikupljanju svih ranije identificiranih podataka, koju su potencijalno povezani sa sigurnosnim incidentom. MDE sustav omogućava za potencijalno kompromitiran krajnji uređaj izvoz dijagnostičkih podataka, događaja u sustavu i ostale podatke koji mogu biti od koristi u istrazi kao što je prikazano na sljedećoj snimci zaslona Slika 23.



Slika 23. Snimka zaslona tabličnog ispisa svih događaja u sustavu za pojedini krajnji uređaj

Budući da sam sustav MDE prethodno detekciji automatski provodi prikupljanje povezanih podataka, iste je potrebno detaljno pregledati i pohraniti za potrebe iduće faze, odnosno prema potrebi, provođenja manualne analize. Pored izvoza podataka iz oblaka, dostupna je i funkcionalnost takozvane žive istrage, odnosno direktnog spajanja na virtualno računalo i upravljanja konzolnim putem. Ako sustav nije samostalno prikupio dovoljnu količinu podataka, a pristup računalu nikako nije moguć, kao niti kloniranje i kopiranje svih podataka, ovakva funkcionalnost omogućava direktan pristup i ekstrakciju pojedinih podataka putem naredbi ili skripta.

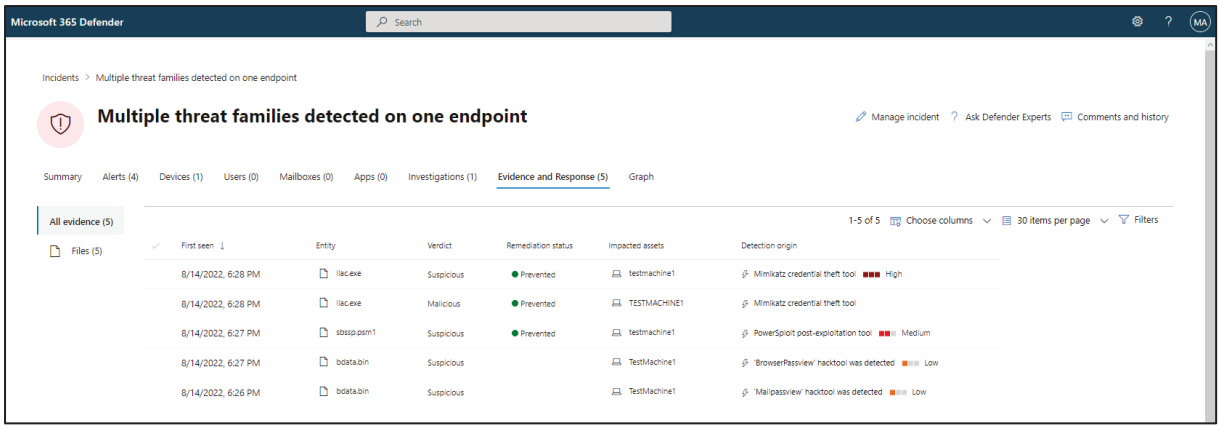


Slika 24. Snimka zaslona s prikazom provođenja "žive forenzičke istrage" nad krajnjim uređajem

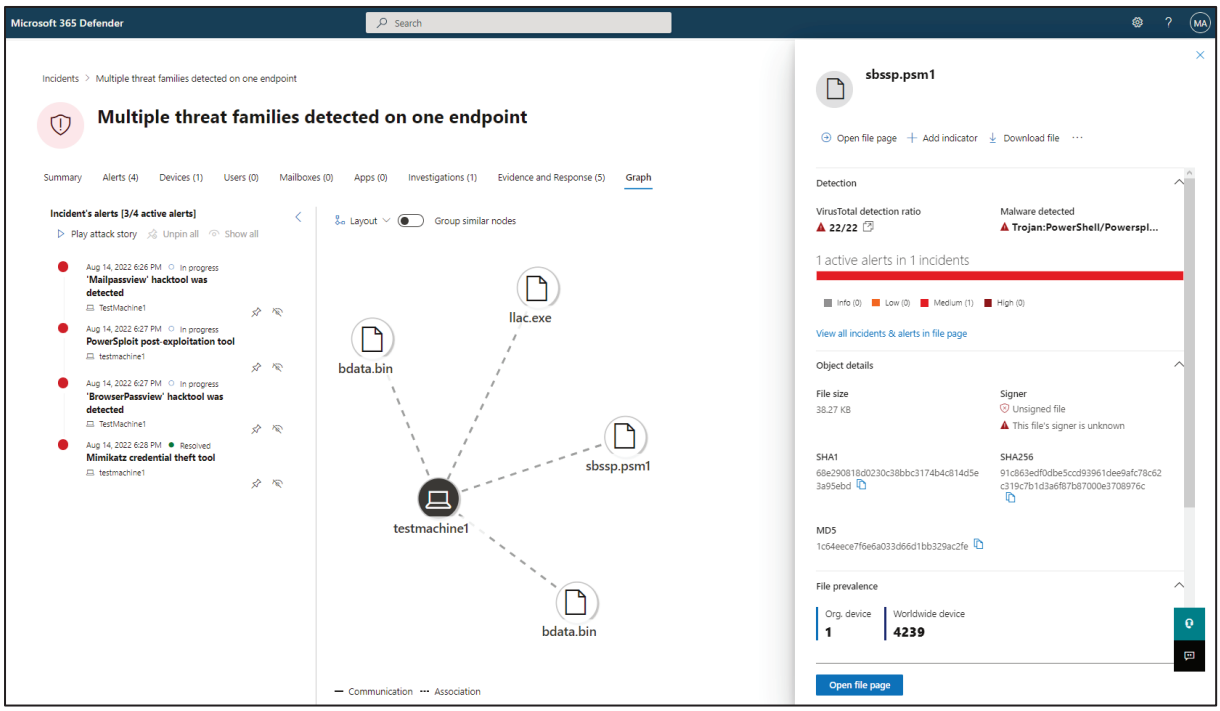
Na Slika 24. iznad, prikazana je snimka zaslona konzolnog pristupa udaljenom virtualiziranom računalu koje je predmet istrage.

6.4. Analiza

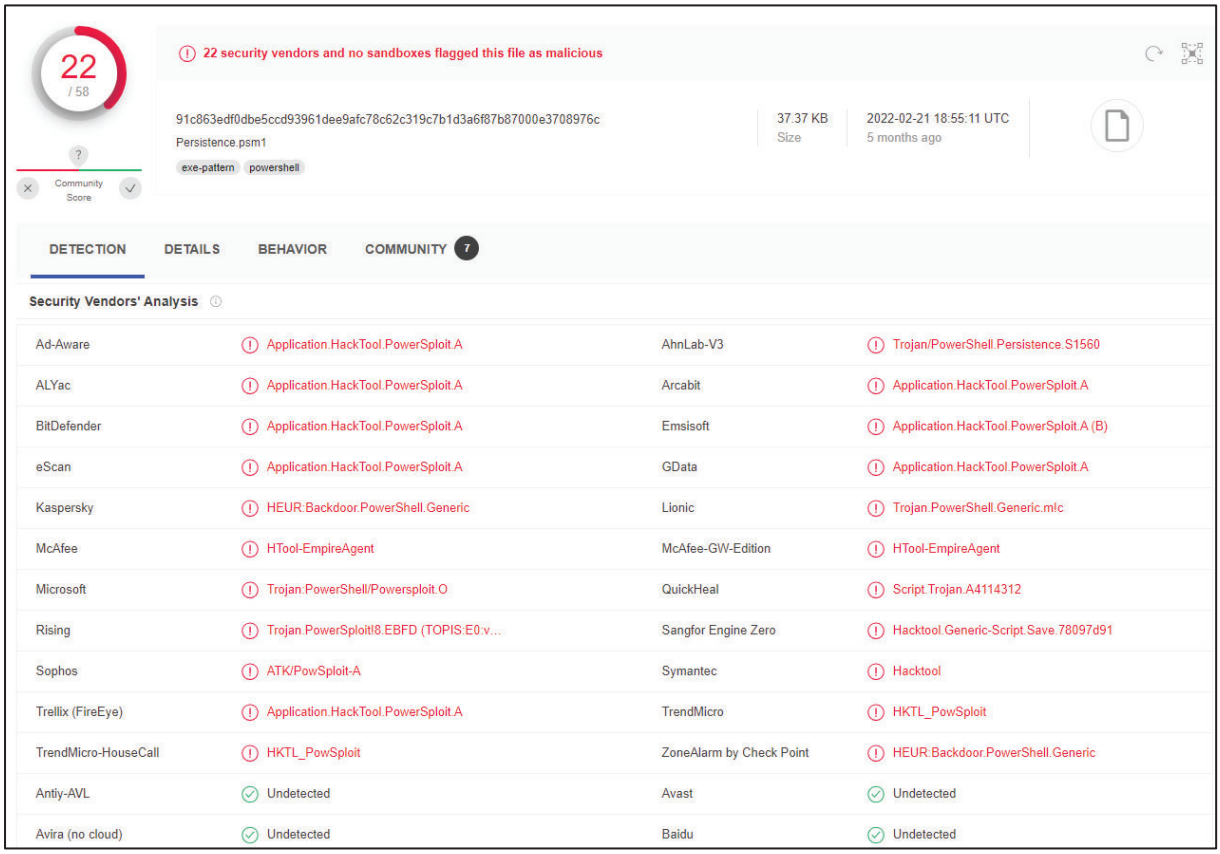
Kao što je slučaj s očuvanjem, identifikacijom i prikupljanjem, tako je i faza analize obavljena direktno od strane samog MDE sustava. Analiza je, kao što je spomenuto u ranijim poglavljima potpomognuta strojnim učenjem, umjetnom inteligencijom i povezanim sustavima partnera na temelju kojih ima lako donosi odluke o pozitivnih i lažno pozitivnim rezultatima. Primjer prepoznavanja sumnjivih i zlonamjernih aktivnosti prikazan je na sljedećim snimkama zaslona:



Slika 25. Snimka zaslona s prikazom ključnih dokaznih materijala



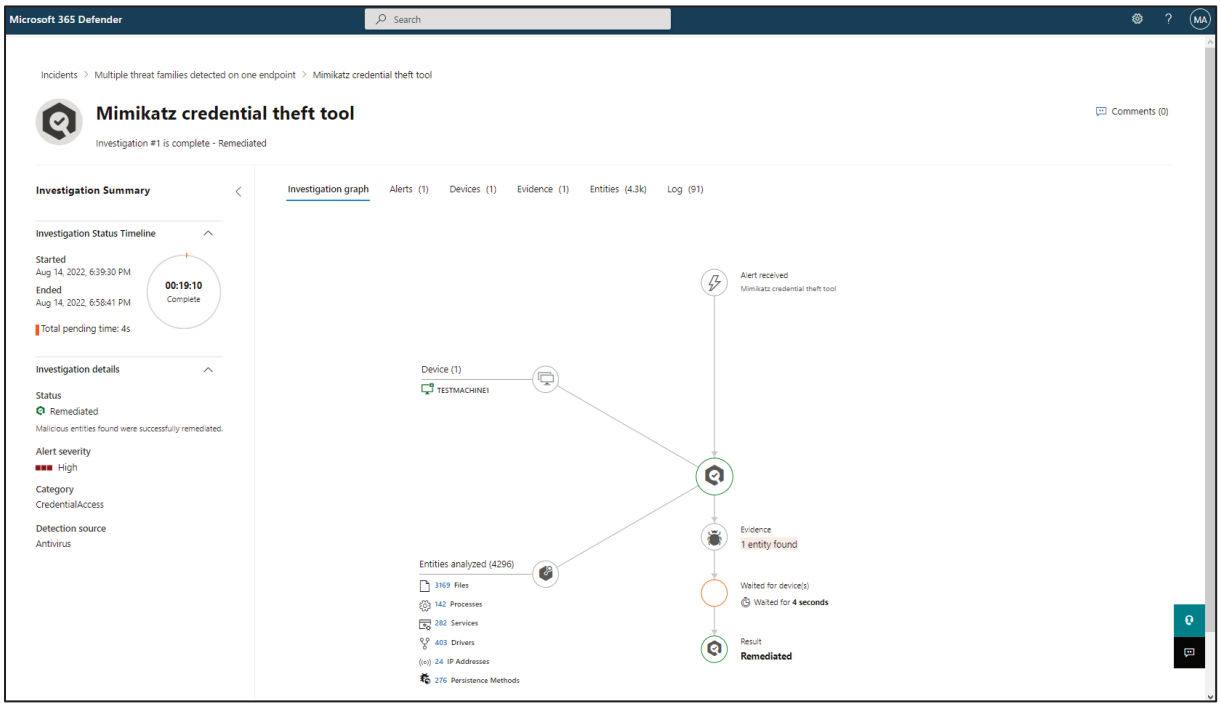
Slika 26. Snimka zaslona s grafičkim prikazom korelacija između krajnjeg uređaja i zlonamjernog softvera



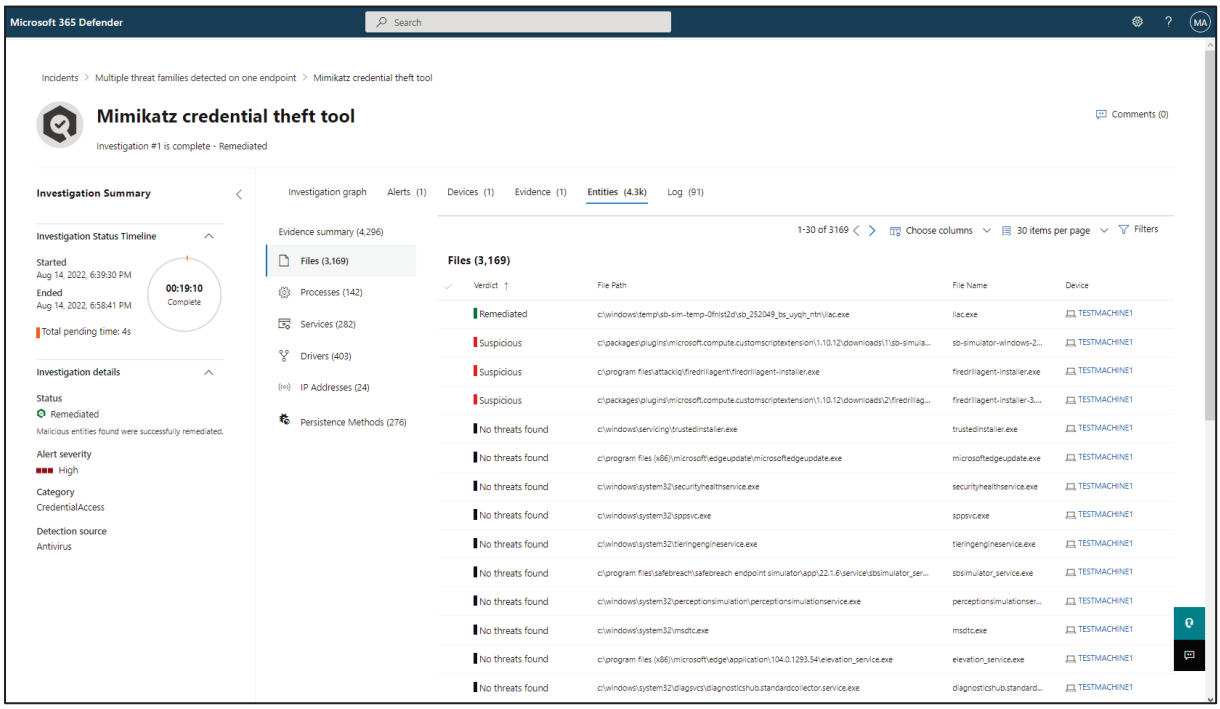
Slika 27. Snimka zaslona s prikazom analize zlonamjernog softvera od strane drugih proizvođača sigurnosnih rješenja

Za potrebe dodatne manualne analize, dostupno je napredno istraživanje svih izvršnih datoteka i pojedinih vrsta sistemskih datoteka. Za prepoznat „Mimikatz credential theft tool“ odnosno zlonamjerni softver za prikupljanje pristupnih korisničkih podataka, MDE sustav je prikupio 4.296 povezanih dokaznih materijala i 91 zapis događaja sa samog krajnjeg računala „testmachine1“. Svaki od navedenih dokaznih materijala dostupan je za detaljan pregled bez direktnog povezivanja na samo računalo. Primjer korelacije zlonamjernog softvera, računala, dokaznih materijala i obavijesti o upozorenjima grafički je prikazan te u svojim opcijama omogućuje detaljni pregled prikupljenih dokaznih materijala direktno od strane sustava.

Detaljna kategorizacija prikupljenih dokaznih materijala prema dokumentima, procesima, servisima, pokretačkim programima, IP adresama i metodama opetovanih napada značajno olakšava fokus i provođenje manualne analize kao što je prikazano na Slika 29. i Slika 30. na sljedećoj stranici.

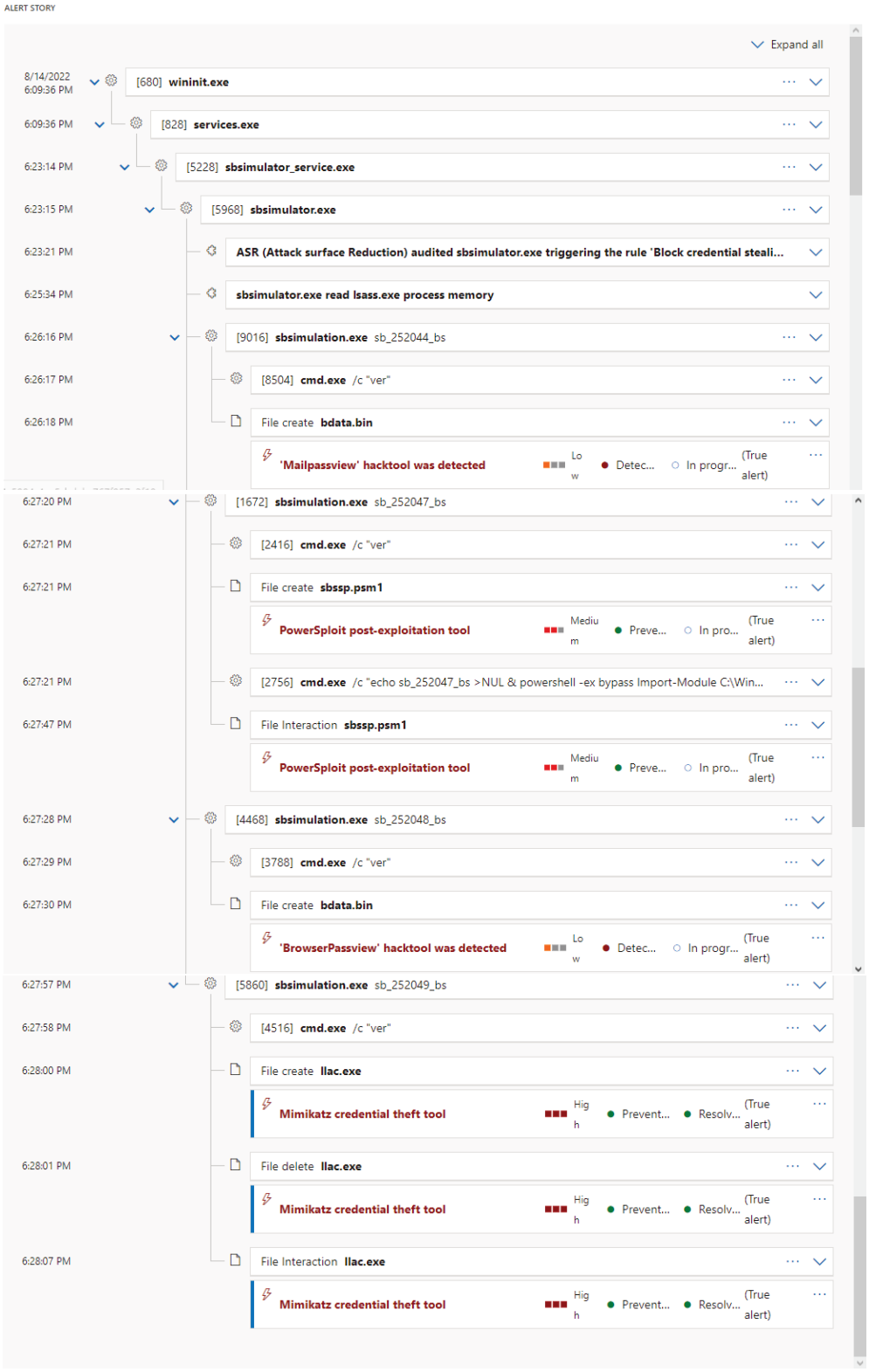


Slika 28. Snimka zaslona analize zlonamjernog softvera "Mimikatz credential theft tool"



Slika 29. Snimka zaslona s prikazom prikupljenih dokaznih materijala

Pored detaljnog uvida u zlonamjerne aplikacije i datoteke te dokazne materijale, sustav automatski, prema kronološkom slijedu događaja sortira i prikazuje napredovanje zlonamjernog softvera kroz sustav, njegovo djelovanje, stupanj rizika i poduzete radnje s ciljem sprečavanja daljnjih zlonamjernih aktivnosti, što je vidljivo u nastavku na Slika 30.



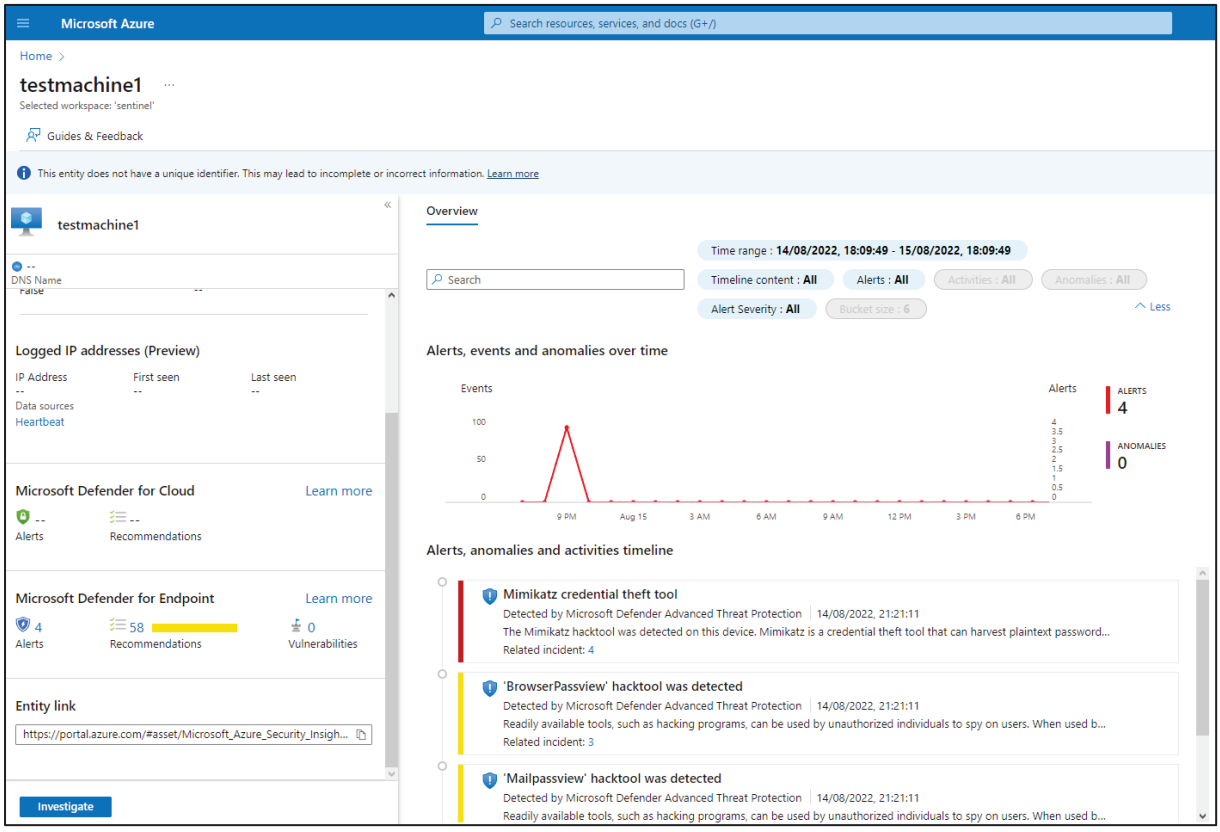
Slika 30. Snimka zaslona kronološkog prikaza napredovanja zlonamjernog softvera na krajnjem uređaju

6.5. Prezentiranje

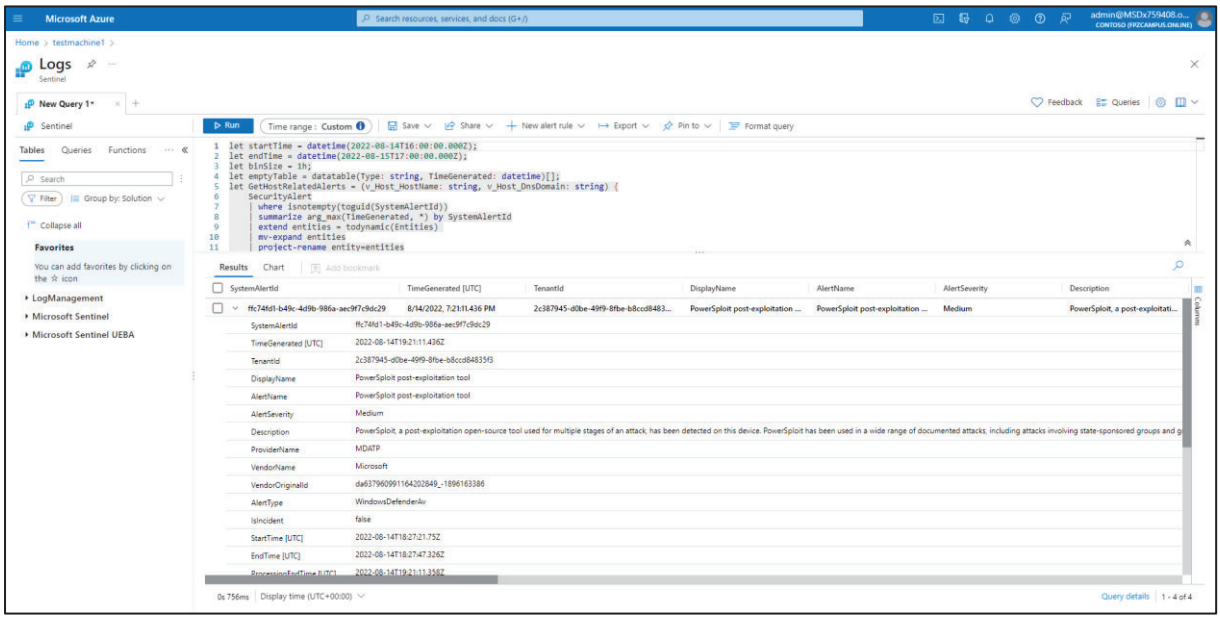
Digitalni istražitelji prilikom izrade forenzičkog izvještaja kao zadnje faze forenzičke istrage koriste standardizirane smjernice koje olakšavaju njegovu izradu. Standardni forenzički izvještaj mora sadržavati uvod i opće informacije o sustavu, kratak opis slučaja i zadatke koje je neophodno napraviti, izjavu o povjerljivosti, popis alata korištenih u istrazi, lanac posjeda dokaza, klase dokaza prema forenzičkoj vrijednosti, opis i prikaz samih dokaznih materijala, sažetak zaključaka na temelju provedene istrage, dodatna mišljenja drugih stručnjaka.

Na temelju prikazanih snimki zaslona, lako je zaključiti kako je XDR sustav isporučio značajne količine informacija, dokaznih materijala, grafičkih prikaza o incidentu, zlonamjernom softveru i neovlaštenom pokušaju krađe korisničkih pristupnih podataka. Sve navedeno značajno olakšava i ubrzava sve korake prethodne korake forenzičke istrage i na kraju, izradu prezentacije. U slučaju da svi dobiveni dokazi nisu dostatni za prezentaciju, te ih je potrebno dodatno potkrijepiti metapodacima, digitalnim istražiteljima dostupan je Microsoft Sentinel, SIEM sustav kojem se prosljeđuju sve informacije iz XDR-a na dodatnu obradu i analizu.

Snimke zaslona vidljive na Slika 31. i Slika 32. koje se nalaze u nastavku, prikazuju dodatni uvid u sam tijek događaja, okvirne, ali i detaljne informacije zapisa o događajima u sustavu.



Slika 31. Snimka zaslona Sentinel sustava i općih informacija o incidentima povezanim s računalom "testmachine1"



Slika 32. Snimka zaslona detaljnog uvida i ispitivanja zapisnika o događajima u sustavu

Kao što je prikazano na snimci zaslona iznad, Sentinel omogućuje napredno ispitivanje zapisnika o događajima te dohvaćanje informacija koje nisu nužno prikazane kroz MDE i web sučelje.

6.6. Verifikacija

U ovom koraku, od strane nadležnog tijela dokazuje se pouzdanost i integritet dokaznih materijala ustupljenih od strane forenzičkog istražitelja, ali i pouzdanost i iskrenost svih sudionika, njihovih radnji, namjera te pouzdanost alata u oblaku koji su izvršili automatizirano prikupljanje, identifikaciju i analizu u toku trajanja digitalne forenzičke istrage. Nadležno tijelo može verifikaciju provesti nad inicijalnim, takozvanim surovim podacima iz prve faze očuvanja. Digitalnih istražitelj, dužan je na određene načine ekstrahirati sve dostupne podatke bez utjecaja na predmet istrage i neovisno o zatečenom stanju i informacijama prikazanim kroz web platformu XDR i SIEM sustava. Glavni razlog tomu je ograničeno vremensko čuvanje zapisa o događajima u sustavu u sustavima u oblaku.

7. ZAKLJUČAK

Usluge u oblaku nadmašile su predviđanja i transformirale pogled na dosadašnji rad temeljen na korištenju računala i informacijskih sustava. Opća dostupnost usluga u oblaku s bilo kojeg uređaja preko javne mreže, neovisno o lokaciji u samim je počecima postavile visoke izazove za kibernetičku sigurnost. Unatoč brojnim sigurnosnim rješenjima, apsolutne sigurnosti nema što za posljedicu ima povećanje kibernetičkih napada te shodno tomu i povećanu potražnju za digitalnim istražiteljima. Forenzičke istrage provode se na temelju pripremljenih i standardiziranih smjernica koje istražitelj prema potrebi samostalno prilagođava u ovisnosti o slučaju. Eksponencijalni razvoj usluga u oblaku ostavio je jaz u odnosu s digitalnom forenzikom koja je do tada primarno bila orijentirana na tradicionalne metode provođenja istrage.

Konstrukcija samih usluga u oblaku, tradicionalni modeli forenzičke istrage oblaka i smjer daljnjeg razvitka, polazišne su točke za razumijevanje problematike provođenja forenzičkih istraga u oblaku. Kroz upoznavanje s novim sudionicima poput davatelja usluga i infrastrukture u oblaku, ali i s pravnim zakonima bitno je istaknuti potrebu za nužnim promjenama. One se primarno odnose na poboljšanje međunarodne suradnje u kontekstu prikupljanja podataka koji se nalaze unutar drugih država i pravnih nadležnosti. Daljnje analiziranje disciplina digitalne forenzike ukazuje na nedovoljno ukazivanje pažnje poddisciplini zvanoj digitalna forenzika oblaka. Iz toga je proizašla anakronost postojećih modela provođenja digitalne forenzičke istrage.

U ovome diplomskom radu prikazane su mogućnosti primjene sigurnosnih sustava nove generacije i njihov utjecaj na provođenje forenzičke analize. Za studiju slučaja, odabrani su aktualni Microsoft sigurnosni sustavi XDR i SIEM koji svojim funkcionalnostima značajno ubrzavaju proces trajanja prikupljanja i identifikacije podataka. U odnosu na tradicionalne forenzičke alate, potpomognuti strojnim učenjem, umjetnom inteligencijom i bihevioralnom analizom, spomenuti sustavi proaktivno prikupljanju, identificiraju i analiziraju podatke u pozadini. Budući da XDR i SIEM sustavi svojim djelovanje pokrivaju gotovo sve aspekte informacijskih sustava, neosporiva je njihova primjenjivost u brojnim disciplinama digitalne forenzike. Digitalni forenzičari nakon određene edukacije, uz pomoć navedenih sustava i raznolikog spektra alata mogu provoditi istrage s udaljenih lokacija, nad dislociranim i virtualiziranim resursima uz očuvanje lanca posjeda dokaza. Daljnji razvitak ovakvih sustava neće zamijeniti uloge s digitalnim istražiteljima kao visoko educiranim individualcima, već osnažiti razumijevanje i način rada usluga u oblaku, ponašanje krajnjih korisnika, učvrstiti suradnju svih sudionika istrage i dati jasan uvid u tijek događaja u samom informacijskom sustavu.

Literatura

[1] B. Briggs i E. Jassber, Enteprise Cloud Strategy, 2nd edition ur., Redmond, Washington: Microsoft Press, 2017.

[2] C. Millard, Cloud Computing Law, 2nd edition ur., C. Millard, Ur., Oxford: Oxford University Press, 2021.

[3] A. Lisdorf, Cloud Computing Basics: A Non-Technical Introduction, S. MC Dermott, L. Berendson i R. Fernando, Ur., Copenhagen, 2021.

[4] »IaaS vs PaaS vs SaaS,« 2020. [Mrežno]. Available: https://www.redhat.com/en/topics/cloud-computing/iaas-vs-paas-vs-saas. [Pokušaj pristupa 3 Lipanj 2022].

[5] »Digital Evidence,« 2020. [Mrežno]. Available: https://www.nist.gov/digital-evidence. [Pokušaj pristupa 4 Lipanj 2022].

[6] C. Jackson, R. Agrawal, J. Walker i W. Grosky, »Scenario-based design for a cloud forensics portal,« u *IEEE International Symposium on Technologies for Homeland Security (HST)*, Waltham, 2015.

[7] A. J. Marcella, »Cyber Forensics,« u *Cyber Forensics Examining Emerging and Hybrid Technologies*, A. J. Marcella, Ur., Boca Raton, Florida: CRC Press, 2022.

[8] L. Chen, H. Takabi i N.-A. Le-Khac, Security, Privacy, and Digital, L. Chen, H. Takabi i N. Le-Khac, Ur., Singapore: John Wiley & Sons, 2019.

[9] H. van Beek, J. van den Bos, A. Boztas, E. van Eijk, R. Schramp i M. Ugen, »Digital forensics as a service: Stepping up the game,« *Forensic Science International: Digital Investigation,* svez. 35, br. 301021, p. 13, December 2020.

[10] R. van Baar, H. van Beek i E. van Eijk, »Digital Forensics as a Service: A game changer,« *Digital Investigation,* svez. 11, br. 1, May 2014.

[11] Hansken, »Hansken The open digital forensic platform,« Hansken, May 2022. [Mrežno]. Available: https://www.hansken.nl/binaries/hansken/documenten/publications/2022/05/24/hansken-product-vision/202205-Hansken_product_vision.pdf. [Pokušaj pristupa 1 Srpanj 2022].

[12] S. O'shaughnessy i A. Keane, »Impact of Cloud Computing on Digital Forensic Investigations,« u *9th International Conference on Digital Forensics (DF)*, Orlando, 2013.

[13] M. Herman, M. Iorga, A. M. Salim, R. H. Jackson, M. R. Hurst, R. Leo, R. Lee, N. M. Landreville, A. K. Mishra, Y. Wang i R. Sardinas, »NIST Cloud Computing Forensic Science Challenges,« NIST, Gaithersburg, 2020.

[14] A. Pichan, M. Lazarescu i S. T. Soh, »Cloud forensics: Technical challenges, solutions and comparative analysis,« *Digital Investigation,* svez. 13, pp. 38-57, June 2015.

[15] M. Ouedraogo i H. Mouratidis, »Selecting a Cloud Service Provider in the age of cybercrime,« *Computers & Security,* svez. 38, pp. 3-13, October 2013.

[16] R. Montasari, H. Jahankhani, R. Hill i S. Parkinson, Digital Forensic Investigation of Internet of Things (IoT) Devices, A. J. Masys, Ur., Chanm: Springer, 2021.

[17] Y. Arafat, B. Mondal i S. Rani, »Technical Challenges of Cloud Forensics and Suggested Solutions,« *International Journal of Scientific & Engineering Research,* svez. 8, br. 8, pp. 1142-1149, August 2017.

[18] G. Peterson i S. Shenoi, »Advances in Digital Forensics XIV,« u *14th IFIP WG 11.9 Internation Conference*, New Delhi, 2018.

[19] E. M. Lopez, S. Y. Moon i J. H. Park, »Scenario-Based Digital Forensics Challenges in Cloud Computing,« *Symmetry in Secure Cyber World,* svez. 8, October 2016.

[20] C. Karagiannis i K. Vergidis, »Digital Evidence and Cloud Forensics: Contemporary Legal Challenges and the Power of Disposal,« *Information 2021,* svez. 12, br. 5, p. 18, May 2021.

[21] COMMISSION STAFF WORKING DOCUMENT, "Zakonodavstvo Europske unije," European Commission, 17 April 2018. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018SC0118&from=SV. [Accessed 15 Srpanj 2022].

[22] M. Tuba, S. Akashe i A. Joshi, »ICT Systems and Sustainability,« u *International Conference on ICT for Sustainable Development (ICT4SD)*, Goa, 2020.

[23] T. Christakis i F. Terpan, »EU-US negotiations on law enforcement access to data: divergences, challenges and EU law procedures and options,« *International Data Privacy Law,* svez. 11, br. 2, pp. 81-106, April 2021.

[24] A. S. George, A. S. H. George, T. Baskar i D. Pandey, »XDR: The Evolution of Endpoint Security Solutions - Superior Extensibility and Analytics to Satisfy the Organizational Needs of the Future,« *International Journal of Advanced Research in Science, Communication and Technology,* svez. 8, br. 1, pp. 493-501, August 2021.

[25] exabeam, »The Ultimate Guide to XDR,« 2021. [Mrežno]. Available: https://www.exabeam.com/wp-content/uploads/GUIDE-The-Ultimate-Guide-to-XDR.pdf. [Pokušaj pristupa 22 Srpanj 2022].

[26] »Evaluate and pilot Microsoft 365 Defender,« Microsoft, 2022. [Mrežno]. Available: https://docs.microsoft.com/en-us/microsoft-365/security/defender/eval-overview?view=o365-worldwide. [Pokušaj pristupa 24 Srpanj 2022].

[27] T. Supasatit, »What's The Difference Between CASB, CWPP, CSPM and CNAPP,« 23 March 2021. [Mrežno]. Available: https://www.uptycs.com/blog/whats-the-difference-between-casb-cwpp-cspm-and-cnapp. [Pokušaj pristupa 24 Srpanj 2022].

[28] »SIEM and XDR: Your ally against ransomware,« 2022. [Mrežno]. Available: https://www.microsoft.com/en-us/security/business/threat-protection. [Pokušaj pristupa 27 Srpanj 2022].

[29] Gartner, 2022. [Mrežno]. Available: https://www.gartner.com/reviews/market/cloud-workload-protection-platforms. [Pokušaj pristupa 27 Srpanj 2022].

[30] K. Kavanagh, T. Bussa i J. Collins, »Magic Quadrant for Security Information and Event,« Gartner, 2022.

[31] T. Bussa, K. Kavanagh i G. Sadowski, »Critical Capabilities for Security Information and Event Management,« Gartner, 2022.

[32] Fortinet, »What is UEBA,« Fortinet, 2022. [Mrežno]. Available: https://www.fortinet.com/resources/cyberglossary/what-is-ueba. [Pokušaj pristupa 30 Srpanj 2022].

[33] A. H. Zolait i M. A. Salitin, »The role of User Entity Behavior Analytics to detect network attacks in real time,« u *International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, Bahrain, 2018.

[34] Gartner, »Security Orchestration, Automation and Response (SOAR),« Gartner, 2022. [Mrežno]. Available: https://www.gartner.com/reviews/market/security-orchestration-automation-and-response-solutions. [Pokušaj pristupa 1 Kolovoz 2022].

[35] Y. Diogenes, N. DiCola i T. Turpijn, Microsoft Sentinel: Planning and implementing Microsoft's cloud-native SIEM solution, 2nd ur., L. Yates, Ur., Pearson Education, 2022.

[36] R. Lefferts, 22 September 2020. [Mrežno]. Available: https://www.microsoft.com/security/blog/2020/09/22/microsoft-unified-siem-xdr-modernize-security-operations/. [Pokušaj pristupa 4 Kolovoz 2022].

[37] Microsoft, »Onboard to the Microsoft Defender for Endpoint service,« Microsoft, 2022. [Mrežno]. Available: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/onboarding?view=o365-worldwide. [Pokušaj pristupa 4 Kolovoz 2022].

[38] Microsoft, »Investigate entities on devices using live response,« Microsoft, 2022. [Mrežno]. Available: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/live-response?view=o365-worldwide. [Pokušaj pristupa 4 Kolovoz 2022].

[39] VMware, » What is a next-generation firewall (NGFW),« VMware, 2022. [Mrežno]. Available: https://www.vmware.com/topics/glossary/content/next-generation-firewall.html. [Pokušaj pristupa 4 Kolovoz 2022].

[40] R. Kaur, J. D'Hoinne, N. Smith i A. Hils, » Magic Quadrant for Network Firewalls,« Gartner, 2021.

[41] J. Kessel, »Fortinet Firewall Threat Hunting with Sentinel,« 10 June 2022. [Mrežno]. Available: https://cryptsus.com/blog/fortinet-firewall-sentinel-siem-hunting.html. [Pokušaj pristupa 5 Kolovoz 2022].

[42] Ericsson, »Ericsson Mobility Report,« Ericsson, Sweden, 2022.

[43] IBM, »What is mobile security,« IBM, 2022. [Mrežno]. Available: https://www.ibm.com/topics/mobile-security. [Pokušaj pristupa 5 Kolovoz 2022].

[44] Fakultet prometnih znanosti, »Metodologije forenzičke analize informacijsko komunikacijskog sustava - DIO 2,« *Forenzička analiza informacijsko komunikacijskog sustava,* 2021.

[45] Microsoft, »Microsoft Defender for Endpoint on Android - Privacy information,« Microsoft, 2022. [Mrežno]. Available: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/android-privacy?view=o365-worldwide. [Pokušaj pristupa 6 Kolovoz 2022].

[46] Microsoft, »Configure Defender for Endpoint on Android features,« 2022. [Mrežno]. Available: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/android-configure?view=o365-worldwide#privacy-controls. [Pokušaj pristupa 6 Kolovoz 2022].

[47] R. Park, »Announcing general availability of vulnerability management support for Android and iOS,« Microsoft, 25 January 2022. [Mrežno]. Available: https://techcommunity.microsoft.com/t5/microsoft-defender-vulnerability/announcing-general-availability-of-vulnerability-management/ba-p/3071663. [Pokušaj pristupa 6 Kolovoz 2022].

[48] Proofpoint, »2022 State of the Phish Report,« Proofpoint, 2022.

[49] M. M. Ghonge, S. Pramanik i D.-N. Le, Cyber Security and Digital Forensics, R. Agrawal i D. G. Gopal, Ur., New York: John Wiley & Sons, Scrivener, 2022.

[50] Microsoft, »Phising investigation,« Microsoft, 2022. [Mrežno]. Available: https://docs.microsoft.com/en-us/security/compass/incident-response-playbook-phishing. [Pokušaj pristupa 9 Kolovoz 2022].

[51] Microsoft, »Overview of Microsoft Purview eDiscovery (Premium),« 2022. [Mrežno]. Available: https://docs.microsoft.com/en-us/microsoft-365/compliance/overview-ediscovery-20?view=o365-worldwide. [Pokušaj pristupa 11 Kolovoz 2022].

[52] A. Sn i Y. Prayudi, »Digital Chain of Custody: State of The Art,« *International Journal of Computer Applications,* svez. 114, br. 5, 5 March 2015.

[53] Microsoft, »Computer forensics chain of custody in Azure,« Microsoft, 2022. [Mrežno]. Available: https://docs.microsoft.com/en-us/azure/architecture/example-scenario/forensics/. [Pokušaj pristupa 11 Kolovoz 2022].

[54] J. Harding, »Microsoft Cloud App Security update: March 2021,« Microsoft, 12 March 2021. [Mrežno]. Available: https://techcommunity.microsoft.com/t5/security-compliance-and-identity/microsoft-cloud-app-security-update-march-2021/ba-p/2157650. [Pokušaj pristupa 12 Kolovoz 2022].

[55] Microsoft, »Azure Sentinel Best Practices,« Microsoft, July 2020. [Mrežno]. Available: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjixtS288r5AhW9VvEDHaMfD0YQFnoECAoQAQ&url=https%3A%2F%2Fwww.micro

soft.com%2Fsecurity%2Fblog%2Fwp-content%2Fuploads%2F2020%2F07%2FAzure-Sentinel-whitepaper.pdf&usg=AOvV. [Pokušaj pristupa 9 Kolovoz 2022].

[56] U.S. Department of Justice, »The United States Department of Justice,« 2022. [Mrežno]. Available: https://www.justice.gov/dag/page/file/1153466/download. [Pokušaj pristupa 18 Srpanj 2022].

[57] C. Winckless i N. MacDonald, »Innovation Inshight for Cloud-Native Application Protection Platforms,« 25 August 2021. [Mrežno]. Available: https://www.gartner.com/doc/reprints?id=1-27AL6QP3&ct=210826&st=sb?utm_source=marketo&utm_medium=email&utm_campaign=Global-DA-EN-7014u000001hBJYAA2-P3-Prisma-gartner-report-cloud-native-application-protection. [Pokušaj pristupa 24 Srpanj 2022].

[58] DFLabs, »SOAR Technology,« 2021. [Mrežno]. Available: https://www.acadiatech.com/wp-content/uploads/2020/11/SOAR-Technology.pdf. [Pokušaj pristupa 2 Kolovoz 2022].

[59] A. Grigorof, M. Mocanu i J. Shaw-Young, »Azure Sentinel Deployment Best Practices,« BlueVoyant, 2021. [Mrežno]. Available: https://www.bluevoyant.com/resources/azure-sentinel-deployment-best-practices. [Pokušaj pristupa 3 Kolovoz 2022].

Popis kratica i akronima

AAD	Azure Active Directory
ADAM	The Advanced Data Acquisition Model
AIR	Auto Investigation & Remediation
API	Application Programming Interface
ARS	Attack Surface Reduction
BYOD	Bring Your Own Device
CASB	Cloud Access Security Broker
CDR	Cloud Detection and Response
CFCMM	Cloud forensics Capability Maturity
CFIT	Cloud Forensics Investigation Team
CMM	Capability Maturity Model
CNAPP	Cloud-Native Application Protection Platform
CoC	Chain of Custody
CPEEP	Cellular Phone Evidence Extraction Process
CPI	Cloud Infrastructure Provider
CSA	Cloud Security Alliance
CSP	Cloud Service Provider
CSPM	Cloud Security Posture Management
CWPP	Cloud Workload Protection Platform
DFaaS	Digital Forensics as a Service
DNS	Domain Name Service
DPI	Deep Packet Inspection
EDR	Endpoint Detection and Response
EDRM	Electronic Discovery Reference Model
EU	European Union
EUBA	End User Behaviour Analysis
FaaS	Forensics as a Service
GUID	Globally Unique Identifier
IaaS	Infrastructure as a Service
ICCID	Integrated Circuit Card Identification Number
ICDFFCC	Integrated Conceptual Digital Forensic Framework for Cloud Computing
IDFPM	Integrated Digital Forensic Process Model
IDS	Intrusion Detection System
IMEI	International Mobile Equipment Identity
IP	Internet Protocol
IPS	Intrusion Prevention System
ISP	Internet Service Provider
LAN	Local Area Network
MDE	Microsoft Defender for Endpoint
MDR	Managed Detection and Response
MLA	Mutual Legal Assistance
MLAT	Mutual Legal Assistance Treaty

MTE	Microsoft Threat Experts
NDR	Network Detection and Response
NFGW	Next Generation Firewall
NGP	Next Generation Protection
NIST	National Institute of Standards and Technology
OCFM	Open Cloud Forensics Model
OSCAR	Obtain,Strategize, Collect, Analyze, Report
PaaS	Platform as a Service
PMU	Pametni Mobilni Uređaj
SaaS	Software as a Service
SEM	Security Event Management
SIEM	Security Information and Event Management
SIM	Security Information Protection
SOAR	Security Orchestration and Automation Response
SQL	Structured Query Language
TVM	Threat & Vulnerability Management
UEBA	User Entity Behavior Analytics
UFED	Universal Forensics Extraction Device
USB	Universal Serial Bus
VDI	Virtual Desktop Infrastructure
VMM	Virtual Machine Manager
VPN	Virtual Private Network
WAN	Wide Area Network
XDR	Extended Detection and Response

Popis grafičkih prikaza

Popis slika

Slika 1. Komparacija modela usluga u oblaku i privatnog oblaka Izvor: [4] 5
Slika 2. Komplementarnost forenzike u oblaku s mrežnom i računalom forenzikom, [8] 7
Slika 3. Grafički prikaz tradicionalnog modela digitalne forenzičke istrage, [11] 9
Slika 4. Grafički prikaz modernog DFaaS modela digitalne forenzičke istrage, [10] 9
Slika 5. Izazovi prikupljanja podataka u prvoj fazi digitalne forenzičke istrage u oblaku, [14] 14
Slika 6. Prikaz sudionika i međusobne suradnje tijekom postupka uzajamne pravne pomoći u forenzičkim istragama, [21] 18
Slika 7. Prikaz direktne suradnje bez posredovanja pojedinih sudionika, [21] 19
Slika 8. Objedinjeno Microsoft rješenje XDR i SIEM sustava i podsustavi, [28] 23
Slika 9. Ključne značajke SIEM sustava prema fazama 25
Slika 10. Proces provođenja bihevioralne analize 26
Slika 11. Unificiranost Microsoft 365 Defender, Microsoft Defender for Cloud i Microsoft Sentinel sustava 29
Slika 12. Snimka zaslona s prikazom sučelja Microsoft Sentinel i poveznici za vatrozid rješenja drugih partnerskih proizvođač 35
Slika 13. Prikaz komunikacije između vatrozida i SIEM sustava pomoću API poveznika, [41] 36
Slika 14. Primjer toka vođene istrage u email forenzici koristeći se Microsoft Defender for Office 365 alatima, [50] 41
Slika 15. Grafički prikaz tijeka provođenja istrage pomoću alata eDiscovery Premium Izvor: [51] 42
Slika 16. Snimka zaslona alata eDiscovery Premium u trenutku pregleda i označavanje relevantnih dokumenata za forenzičku istragu 43
Slika 17. Temeljni koraci upravljanja digitalnim dokazima Izvor: [52] 44
Slika 18. Grafički prikaz Microsoft Defender for Cloud Apps strukture i funkcionalnosti, [54] 46
Slika 19. Faze OCFM modela 48
Slika 20. Snimka zaslona s prikazanim akcijskim centrom i provedenim metodama izolacije 49
Slika 21. Snimka zaslona s prikazanim incidentom, brojem ugroženih uređaja i općim statusom 50
Slika 22. Snimka zaslona s prikazom obavijesti o višestrukim zlonamjernim aktivnostima 51
Slika 23. Snimka zaslona tabličnog ispisa svih događaja u sustavu za pojedini krajnji uređaj 51
Slika 24. Snimka zaslona s prikazom provođenja "žive forenzičke istrage" nad krajnjim uređajem 52
Slika 25. Snimka zaslona s prikazom ključnih dokaznih materijala 53
Slika 26. Snimka zaslona s grafičkim prikazom korelacija između krajnjeg uređaja i zlonamjernog softvera 53
Slika 27. Snimka zaslona s prikazom analize zlonamjernog softvera od strane drugih proizvođača sigurnosnih rješenja 54
Slika 28. Snimka zaslona analize zlonamjernog softvera "Mimikatz credential theft tool" 55
Slika 29. Snimka zaslona s prikazom prikupljenih dokaznih materijala 55
Slika 30. Snimka zaslona kronološkog prikaza napredovanja zlonamjernog softvera na krajnjem uređaju 56
Slika 31. Snimka zaslona Sentinel sustava i općih informacija o incidentima povezanim s računalom "testmachine1" 57
Slika 32. Snimka zaslona detaljnog uvida i ispitivanja zapisnika o događajima u sustavu 58

Popis tablica

Tablica 1. Komparacija tradicionalnog i modernog pristupa digitalnoj forenzičkoj istrazi prema fazama Izvor: [14] 11
Tablica 2. Prikaz vrsta informacija koje je moguće prikupiti od strane MDE XDR sustava s pametnih mobilnih uređaja Izvor: [45], [46] 38
Tablica 3. Popis funkcionalnosti i produkta od forenzičke vrijednosti..... 40
Tablica 4. Kategorizacija funkcionalnosti Microsoft Defender for Cloud sustava 47

Sveučilište u Zagrebu
Fakultet prometnih znanosti
Vukelićeva 4, 10000 Zagreb

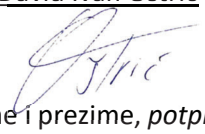
IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOSTI

Izjavljujem i svojim potpisom potvrđujem da je _____diplomski rad_____
(*vrsta rada*)
isključivo rezultat mojega vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju upotrijebljene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedopušten način, odnosno da je prepisan iz necitiranog rada te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog/diplomskog rada pod naslovom Primjena Microsoft sigurnosnih rješenja u digitalnoj forenzičkoj analizi, u Nacionalni repozitorij završnih i diplomskih radova ZIR.

Student/ica:

U Zagrebu, 29.8.2022 David Ivan Oštrić



(ime i prezime, *potpis*)