Evaluacija rješenja za zaštitu krajnjih uređaja od kibernetičkih ugroza u poslovnom okruženju

Đurić, Matko

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Matko Đurić

EVALUACIJA RJEŠENJA ZA ZAŠTITU KRAJNJIH UREĐAJA OD KIBERNETIČKIH UGROZA U POSLOVNOM OKRUŽENJU

DIPLOMSKI RAD

Zagreb, 2024.

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

DIPLOMSKI RAD

EVALUACIJA RJEŠENJA ZA ZAŠTITU KRAJNJIH UREĐAJA OD KIBERNETIČKIH UGROZA U POSLOVNOM OKRUŽENJU

EVALUATION OF ENDPOINT PROTECTION SYSTEMS FROM CYBER THREATS IN ENTERPRISE ENVIRONMENT

Mentor: doc. dr.sc. Ivan Cvitić

Student: Matko Đurić

JMBAG: 0135250024

Zagreb, 2024.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
POVJERENSTVO ZA DIPLOMSKI ISPIT

Zagreb, 4. svibnja 2022.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Sigurnost i zaštita informacijsko komunikacijskog sustava**

DIPLOMSKI ZADATAK br. 6839

Pristupnik: **Matko Đurić (0135250024)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Evaluacija rješenja za zaštitu krajnjih uređaja od kibernetičkih ugroza u poslovnom okruženju**

Opis zadatka:

Diplomskim radom potrebno je provesti evaluaciju rješenja za zaštitu krajnjih korisnika od kibernetičkih ugroza u poslovnom okruženju. Potrebno je analizirati dosadašnju znanstvenu i stručnu literaturu i identificirati relevantnost i važnost predmetnog istraživanja. U okviru istraživanja potrebno je simulirati kibernetičke napade korištenjem MITRE ATT&CK radnog okvira uz primjenu dostupnih sigurnosnih rješenja te analizirati i interpretirati rezultate simulacije te evaluirati korištena sigurnosna rješenja.

Mentor:

dr. sc. Ivan Cvitić

Predsjednik povjerenstva za diplomski ispit:

EVALUACIJA RJEŠENJA ZA ZAŠTITU KRAJNJIH UREĐAJA OD KIBERNETIČKIH UGROZA U POSLOVNOM OKRUŽENJU

SAŽETAK

Unatoč napretku u razvoju sigurnosnih rješenja, kibernetičke prijetnje usmjerene na krajnje uređaje i dalje predstavljaju ozbiljan izazov za organizacije. Ovaj diplomski rad bavi se evaluacijom rješenja za zaštitu krajnjih uređaja, s naglaskom na sustave za detekciju i odgovor na prijetnje. Korištenjem MITRE ATT&CK okvira, simuliran je napad napredne ustrajne prijetnje grupe *Turla*, primjenom jedanaest različitih taktika. Provedene simulacije omogućile su procjenu učinkovitosti sigurnosnih sustava u detekciji i odgovoru na sofisticirane napade. Dobiveni rezultati ukazuju na snage i slabosti postojećih sigurnosnih sustava te naglašavaju potrebu za njihovim kontinuiranim razvojem. Zaključci rada ističu važnost integracije naprednih metoda analize ponašanja i strojnog učenja u sustave za kibernetičku sigurnost.

KLJUČNE RIJEČI: Kibernetička sigurnost; Simulacija napada; sustavi za detekciju i odgovor na prijetnje; MITRE ATT&CK; Poslovno okruženje

SUMMARY

Despite advancements in security solutions, cyber threats targeting endpoints continue to pose a significant challenge for organizations. This thesis focuses on the evaluation of endpoint protection solutions, with an emphasis on Endpoint Detection and Response systems. Using the MITRE ATT&CK framework, an attack by the Advanced Persistent Threat group Turla was simulated, utilizing twelve different tactics. The simulations provided insights into the effectiveness of security systems in detecting and responding to sophisticated attacks. The results highlight the strengths and weaknesses of current security solutions and underscore the need for their continuous development. The conclusions emphasize the importance of integrating advanced behavioural analysis methods and machine learning into cybersecurity systems.

KEY WORDS: Cybersecurity, Attack simulation, Endpoint Detection and Response; MITRE ATT&CK; Enterprise environment

Sadržaj

1. Uvod

Rast digitalnih tehnologija i sve veća upotreba pametnih uređaja u svakodnevnom i poslovnom okruženju omogućili su bržu komunikaciju, obradu podataka te digitalizaciju poslovanja. Iako razvoj tehnologije znatno poboljšava efikasnost organizacija, ono također otvora put novim vrstama prijetnji kao što su kibernetički napadi. S obzirom na sve veću ovisnost o informacijsko-komunikacijskim sustavima, organizacije se suočavaju sa rastućim brojem složenih napada koji ciljaju njihovu infrastrukturu.

Napadi na krajnje uređaje poput računala, pametnih telefona i poslužitelja postaju sve napredniji. Zlonamjerni akteri pronalaze nove načine za krađu podataka, narušavanje sigurnosti ili blokiranje pristupa važnim poslovnim sustavima. Tradicionalni sigurnosni sustavi, koji ugroze prepoznaju prema njihovom potpisu sve teže omogućuju davati adekvatan odgovor na novonastale prijetnje. Stoga je primjena naprednih sigurnosnih rješenja koja evoluiraju i prate trend stalno rastućih kibernetičkih ugroza ključna za očuvanje integriteta poslovnih okruženja.

Cilj ovog rada je evaluirati neka od trenutno dostupnih rješenja za zaštitu krajnjih uređaja u poslovnom okruženju, s naglaskom na detekciju i odgovor na prijetnje. Analizirati će se mogućnosti zaštite i detekcije od sofisticiranih kibernetičkih napada. Za potrebe analize korišteni su podaci dobiveni simulacijom kibernetičkih napada u kontroliranom okruženju, uz korištenje alata i platformi za simulaciju ugroza i metodologija kao što je MITRE ATT&CK okvir.

Ovaj diplomski rad podijeljen je u šest cjelina:

1. Uvod
2. Pregled dosadašnjih istraživanja
3. Kibernetičke prijetnje u poslovnom okruženju
4. Simulacija kibernetičkih prijetnji
5. Sinteza rezultata i evaluacija ispitanih rješenja
6. Zaključak

Drugo poglavlje rada donosi pregled dosadašnjih istraživanja vezanih uz primjenu i mogućnosti tehnologija zaštite krajnjih uređaja. Navedena istraživanja obrađuju metode detekcije prijetnji te evaluaciju učinkovitosti sustava kod prepoznavanja kibernetičkih ugroza. Također analiziraju razlike između tradicionalnih sustava temeljenih na detekciji potpisa te naprednih rješenja koja koriste analizu ponašanja i strojno učenje za identifikaciju prijetnji.

Istraživanja su pokazala slabosti tradicionalnih sigurnosnih rješenja, naročito kod napada koji iskorištavaju zero-day ranjivosti ili koriste napredne tehnike malicioznih programa. S druge strane, moderni sustavi usmjereni na prepoznavanje anomalija i primjenu heurističkih modela pokazali su se znatno učinkovitijima prilikom detekcije sofisticiranih napada.

Trećim poglavljem rada objašnjena su i detaljno opisana obilježja kibernetičkih prijetnji usmjerenih na krajnje uređaje u poslovnom okruženju. Analizirana je klasifikacija prijetnji s fokusom na izvore prijetnji, ranjivosti sustava i metode napada. Prijetnje su podijeljene na one uzrokovane tehničkim ranjivostima, ljudskim pogreškama te automatiziranim napadima provodanih od strane zlonamjernih korisnika.

Poglavlje obuhvaća klasifikaciju različitih metoda napada, uključujući zlonamjerne programe, socijalni inženjering, napade uskraćivanja usluge te napade korištenjem zero-day ranjivosti. Također, detaljno su opisane tehnike naprednih napada poput Man-in-the-Middle i napada korištenjem rječnika. Kroz ovu analizu prikazana je kompleksnost suvremenih prijetnji te su istaknute ključne ranjivosti koje napadači iskorištavaju s ciljem kompromitacije sustava.

Četvrtim poglavljem rada prikazana je simulacija kibernetičkog napada temeljenog na svojstvima *Turla* napredne ustrajne prijetnje. Ova simulacija obuhvatila je korištenje jedanaest taktika napada s ciljem evaluacije učinkovitosti sustava za detekciju i odgovor na prijetnje. MITRE ATT&CK okvir korišten je u svrhu vjerne replikacije stvarno korištenih taktika i tehnika zlonamjernih aktera.

Napad je proveden pomoću alata za simulaciju prijetnji, pri čemu su simulirane taktike uključivale tehnike kao što su eskalacija privilegija, lateralno kretanje unutar mreže te eksfiltracija podataka. Korištene tehnike osmišljene su s ciljem testiranja sposobnosti sigurnosnih sustava da prepoznaju i odgovore na različite faze napada naprednih ustrajnih prijetnji.

Peto poglavlje rada donosi sintezu rezultata simuliranih napada, provedenih kroz jedanaest različitih taktika. Kroz ovu evaluaciju dobiveni su vrijedni uvidi u djelotvornost sustava za zaštitu krajnjih uređaja i njihovu sposobnost detekcije naprednih prijetnji.

Na kraju rada, u šestom poglavlju, iznesen je jedinstven zaključak temeljen na provedenom istraživanju i simulaciji.

2. Pregled dosadašnjih istraživanja

Prema javno dostupnim statistikama i stručnim izvještajima vidljiv je porast kibernetičkih prijetnji koje iskorištavaju i zaobilaze platforme za zaštitu krajnjih uređaja. Interpretacijom tih izvora zaključuje se kako postoji potreba za adresiranjem sve češćih ranjivosti koje se pojavljuju u samim izvršnim aplikacijama takvih sustava te istraživanjem i definiranjem novih metoda zaštite informacijsko-komunikacijskih sustava u poslovnim okruženjima.

U radu iz 2021. godine [1], autori istražuju aktualne kibernetičke prijetnje koje sve češće ciljaju moderne organizacije. Kroz analizu se ukazuje na sve veći broj napada koji zaobilaze standardne sigurnosne sustave, narušavaju rad ključnih infrastruktura i ugrožavaju povjerljive podatke. Autori zaključuju da tradicionalni sigurnosni mehanizmi, poput platformi za zaštitu krajnjih uređaja (engl. *Endpoint Protection Platform*, EPP), više nisu dovoljni za obranu od sofisticiranih napada. Kroz detaljnu analizu dolaze do zaključka da je potrebno uvesti napredne sigurnosne mjere koje bi nadopunile postojeće sustave, s naglaskom na ograničenja trenutno korištenih metoda detekcije prijetnji bazirane na potpisima.

Istraživanjem je pružen detaljan pregled rješenja za detekciju i odgovor na prijetnje krajnjim uređajima (engl. *Endpoint Detection and Response*, EDR). Prikazan je njihov razvoj i evolucija do naprednih platformi za detekciju i reagiranje na ugroze koje se danas koriste u poslovnim okruženjima. Također, autori kroz ovaj znanstveni rad pružaju uvid u arhitektonske komponente EDR sustava, koje uključuju agente za prikupljanje podataka, platformu za centraliziranu analizu te integrirane mehanizme za odgovor na incidente. Uz analizu sustava i njegove arhitekture, dodatno se objašnjava i istražuje mogućnost iskorištavanja EDR sustava u ekosustavu kibernetičke sigurnosti, u vidu integracije s drugim sigurnosnim alatima i stvaranja jedinstvenog sigurnosnog sustava.

Prilikom usporedbe EPP i EDR rješenja, autori evaluiraju metode korištene za identifikaciju i mitigaciju prijetnji. Provedenom evaluacijom autori iznose opažanja koja ukazuju na nedostatke rješenja detekcije baziranih na potpisima kod tradicionalnih EPP sustava te podupiru prednosti sustava baziranih na analizi ponašanja sustava i metodama strojnog učenja kod današnjih EDR sustava. Evaluaciju autori obrađuju kroz dubinsku analizu različitih zlonamjernih programa te pojašnjavaju načine na koje EDR rješenja koriste napredne tehnike, kao što su pronalazak anomalija, heurističke analize i integracija s javnim izvorima podataka o prijetnjama (engl. *Threat Intelligence*, TI) s ciljem detekcije i odgovora na prijetnje u realnom vremenu. Kao zaključak istraživanja, autori prikazuju efikasnost rješenja kroz prezentiranje

studija slučaja i empirijskih podataka, čime pružaju temelje za razumijevanje mogućnosti EDR sustava u borbi protiv modernih kibernetičkih prijetnji.

Studijom [2] je prezentirana metodična evaluacija održivosti besplatnog EDR rješenja otvorenog koda. Osnovni cilj ovog istraživanja je utvrditi mogu li alati otvorenog koda pružiti zadovoljavajuću razinu preglednosti na krajnjim uređajima, kao i mogućnosti detekcije prijetnji u usporedbi s komercijalnim alatima za zaštitu krajnjih uređaja. Autor kao razlog provođenja ove studije navodi sve češću pojavu složenih kibernetičkih prijetnji koje dovode tradicionalne alate za zaštitu krajnjih uređaja do njihovih granica. Istraživanjem je potkrijepljena teza da zastarjela EPP rješenja kao primarnu tehnologiju prepoznavanja prijetnji koriste metode bazirane na potpisu, koje u suvremenoj informacijsko komunikacijskog infrastrukturi organizacije ne uspijevaju prepoznati sofisticirane napade. Autor kao komplementarnu zamjenu za tradicionalne alate za zaštitu predlaže korištenje naprednih EDR rješenja, a fokusiranjem studije na alate otvorenog koda prikazuje mogućnost korištenja naprednih alata čak i u okruženjima s ograničenim financijskim sredstvima.

S obzirom na to da je svrha ovog rada prikazati mogućnosti alata otvorenog koda, potrebno je definirati parametre prema kojima će se provoditi evaluacija. Autor u empirijskoj studiji provedenoj u kontroliranom sigurnosnom okruženju koristi priznati radni okvir Atomic Red Team, kojim simulira različite scenarije kibernetičkih napada. Korišteni scenariji temelje se na MITRE ATT&CK (engl. *MITRE Adversarial Tactics, Techniques, and Common Knowledge*) radnom okviru za anatomiju kibernetičkih prijetnji te pokrivaju četrnaest taktika zlonamjernih korisnika kojima se opisuju faze samog napada. Scenariji su definirani tako da sadrže točno propisane tehnike pomoću kojih se omogućuje praćenje i ocjenjivanje sposobnosti alata da detektira prijetnje.

Provedenim testiranjima dobiveni su rezultati koji jasno prikazuju sposobnosti alata da pruži sveobuhvatan uvid u stanje sustava krajnjeg uređaja i detekciju sofisticiranih prijetnji. Također, autor pomoću dobivenih rezultata pokazuje ograničenja korištenog rješenja. Osim provedenog istraživanja, ovom studijom želi se potaknuti diskusija i razvoj sustava koji omogućuju analizu podataka generiranih od strane alata kako bi se unaprijedio proces integracije sa sustavima centraliziranog prikupljanja zapisa. Zaključkom provedenog empirijskog istraživanja dokazana je relevantnost i primjenjivost studije, a također je ponovno potvrđeno da je korištenje naprednih sustava za obranu od sofisticiranih kibernetičkih prijetnji dostupno širokom spektru organizacija.

Autori u radu [3] pružaju iscrpnu studiju evaluacije performansi EDR sustava otvorenog koda, temeljenog na platformama *Google Rapid Response* i *Osquery*. Provedenim istraživanjem ukazuje se na potrebu izrade i korištenja detekcijskih tehnologija baziranih na praćenju obrazaca ponašanja. Također se iznosi mišljenje o nedostacima i ograničenjima postojećih sustava, osobito sigurnosnih rješenja zatvorenog koda, koja su teško prilagodljiva specifičnim okruženjima pojedinih organizacija.

Znanstveni rad temelji se na *Google Rapid Response* platformi, koja predstavlja radni okvir za provođenje digitalne forenzike u stvarnom vremenu udaljenim pristupom. Spomenuta platforma integrirana je s Osquery instrumentacijskim okvirom za operativne sustave, koji pruža informacije o sustavu putem tablica strukturiranog upitnog jezika (engl. *Structured Query Language,* SQL). Sinergija dviju platformi tvori osnovu predloženog EDR sustava. Provedenim istraživanjem pružene su metodične informacije o načinima integracije navedenih sustava te je prikazana skalabilnost i fleksibilnost kreiranja i konfiguriranja sustava.

Kako bi dokazali funkcionalnosti otkrivanja i odgovora na prijetnje predloženog rješenja, autori sustav podvrgavaju nizu testova koji simuliraju ponašanje naprednih ustrajnih prijetnji. Korišteni eksperimentalni scenariji temelje se na MITRE ATT&CK radnom okviru pomoću kojeg su prikazani različite faze napada. Nakon provedenih testiranja i dobivenih rezultata, utvrđeno je da predloženo rješenje pruža djelotvornu zaštitu u većini scenarija kibernetičkih napada, no isto tako prikazana je fluktuacija u pokrivenosti prepoznavanja prijetnji kroz različite segmente napada. Autori kroz istraživanje prikazuju područja u kojima predloženo rješenje ima slabiju sposobnost otkrivanja prijetnji, a to je najviše vidljivo u fazama napada inicijalnog pristupa i bočnog kretanja kroz mrežu. Kao mogućnost unaprjeđenja sustava, dana je preporuka izrade specifičnih pravila prilagođenih pojedinim korisničkim okruženjima.

Studijom [4] je pružena analiza strategija zaštite krajnjih uređaja s naglaskom na njihovu mogućnost odgovora na napade prouzročene unutarnjim prijetnjama. Istraživanjem autori adresiraju jaz u sigurnosnim rješenjima koja ne uspijevaju pružiti adekvatnu zaštitu od prijetnji koje nastaju unutar poslovnog okruženja. Kao okosnica ovog istraživanja korištena je usporedba dviju ključnih sigurnosnih komponenti. EPP rješenja predstavljena su kao sustavi zastarjelog pristupa, koji za otkrivanje prijetnji koriste mehanizme bazirane na potpisu. Takvi mehanizmi oslanjaju se na ažuriranu bazu potpisa zlonamjernih programa kojom otkrivaju prijetnje u sustavu te poduzimaju aktivnosti u cilju neutralizacije kibernetičkog napada. Studija također identificira značajna ograničenja takvih sustava, osobito nemogućnost prilagodbe ubrzano rastućoj prirodi malicioznih programa. Osim već spomenutih ograničenja, autori

navode kako su EPP rješenja ranjiva na *zero-day* ranjivosti i zlonamjerne programe koji se u potpunosti izvršavaju u memoriji računala (engl. *Fileless malware*). Dodatno, efektivnost ovih rješenja umanjena je i zbog nemogućnosti adekvatnog odgovora na prijetnje koje potječu iz mreže same organizacije.

Autori drugu ključnu sigurnosnu komponentu, EDR rješenja predstavljaju kao napredne sustave koji se temelje na dinamičkoj analizi krajnjih uređaja. Takvi sustavi zamišljeni da kontinuirano prate stanje krajnjih uređaja upotrebom analize obrazaca ponašanja, indikatora kompromitacije i strojnog učenja u svrhu otkrivanja anomalija koje upućuju na postojanje kibernetičke ugroze unutar poslovnog okruženja. Pomoću takvog proaktivnog načina rada, EDR sustavi imaju mogućnost otkrivanja prijetnji u realnom vremenu, što predstavlja dodatnu vrijednost u borbi protiv sofisticiranih unutarnjih prijetnji i kibernetičkih napada koji ne koriste uobičajene obrasce zlonamjernih programa.

Kako bi istraživanje pružilo kvantificirane podatke, autori definiraju model pomoću kojeg evaluiraju EPP i EDR rješenja u odnosu na različite parametre, uključujući preciznost prepoznavanja prijetnje, potrošnju resursa te opće opterećenje sustava. Navedenim modelom prikazana je detaljna analiza funkcionalnosti koja jasno razdvaja EDR i EPP rješenja. Dobivenim podacima autori pokazuju kako EPP rješenja još uvijek imaju značajnu ulogu u sustavima s dobro poznatim prijetnjama, dok se EDR rješenja moraju dodatno usavršavati zbog kompleksnijeg načina rada i integracije u postojeće sustave, kao i zbog mogućnosti pojave visoke stope lažno pozitivnih detekcija koje mogu dovesti do previda ugroze.

Radom [5] je obrađena tema istraživanja mogućnosti i ograničenja modernih EDR sustava u detekciji i odgovoru na napade naprednih ustrajnih prijetnji. Autori su provedenim istraživanjima identificirali kritične točke trenutnog stanja kibernetičke sigurnosti, pri čemu, unatoč napretku u razvoju tehnologija za zaštitu krajnjih uređaja, većina organizacija i dalje ostaje ranjiva na napade ustrajnih prijetnji. Kako bi pružili preporuke za daljnji razvoj sigurnosnih alata i procedura, autori provode empirijsku evaluaciju kojom se dobiva uvid u to koliko moderni EDR alati uspijevaju zaštititi organizacije od sve sofisticiranijih prijetnji, dok se istodobno transparentno ukazuje na slabosti i ograničenja samih sustava.

Evaluacija EDR rješenja provedena je simulacijama različitih vektora napada kojima se, osim testiranja mogućnosti sustava, prikazuje složenost aktualnih napada naprednih ustrajnih prijetnji. Iako postoji mnoštvo vektora napada, autori su se odlučili koristiti četiri najčešća: napade temeljene na datotekama upravljačke ploče (engl. *Control Panel Applet* - CPL), HTML

aplikacijama (engl. *HTML application* - HTA), bočnom učitavanju DLL datoteka (engl. *Dynamic-Link Library side-loading*) te izvršnim datotekama koje iskorištavaju injektiranje procesa (engl. *Process injection executables*).

Istraživanjem su otkrivene značajne razlike u performansama ispitivanih EDR rješenja. Neka su uspjela prepoznati i blokirati specifične vektore napada, dok su druga pokazala slabosti, posebno kod detekcije složenijih prijetnji. Primijećeno je da određeni sustavi nisu detektirali napade koji se izvršavaju u memoriji, kao ni tehnike injektiranja procesa koje zaobilaze standardne sigurnosne mjere. Osim toga, poteškoće su se pojavile kod telemetrije i sustava za alarmiranje. U nekim okolnostima napadi nisu bili zabilježeni, što dovodi do izostanka reakcije na ugrozu. Istraživanje naglašava potrebu za poboljšanjem telemetrijskih mehanizama i jačom integracijom s ostalim sigurnosnim sustavima.

3. Kibernetičke prijetnje u poslovnom okruženju

Kibernetičke prijetnje u poslovnom okruženju predstavljaju ozbiljan izazov za suvremene organizacije koje se sve više oslanjaju na digitalne tehnologije u svom svakodnevnom poslovanju. Kibernetička sigurnost, kao područje koje objedinjuje tehnologije, procese i prakse s ciljem zaštite informacijskih sustava i osjetljivih podataka, usmjerena je na sprječavanje prijetnji koje bi mogle ugroziti povjerljivost, cjelovitost i dostupnost informacija. U poslovnom kontekstu, učinkovitost kibernetičke sigurnosti ovisi o sposobnosti organizacije da prepozna, analizira i odgovori na prijetnje koje dolaze iz različitih izvora, [6].

Za postizanje učinkovite kibernetičke sigurnosti potreban je sveobuhvatan pristup koji uključuje ne samo tehnička rješenja, već i kontinuiranu edukaciju zaposlenika, izradu sigurnosnih politika te implementaciju kontrola i procedura koje smanjuju rizik od incidenata. Uz to, organizacije trebaju uspostaviti mehanizme za pravovremeno otkrivanje i odgovor na sigurnosne incidente, kao i planove za oporavak kako bi osigurale kontinuitet poslovanja u slučaju ozbiljnog sigurnosnog događaja. Razumijevanje prirode i izvora prijetnji ključno je za izgradnju otpornog sigurnosnog okruženja koje može učinkovito zaštititi poslovne interese, [7].

3.1. Izvori prijetnji

Izvori prijetnji u kibernetičkom okruženju poslovanja raznoliki su i obuhvaćaju ljudske, prirodne čimbenike te tehnološke slabosti. Prijetnja, u kontekstu informacijske sigurnosti, označava potencijalnu opasnost koja može narušiti povjerljivost, cjelovitost ili dostupnost informacija i informacijskih sustava. Takve prijetnje ne djeluju u vakuumu; one su obično rezultat djelovanja specifičnih uzročnika (engl. *Threat agents*), koji mogu biti namjerni ili nenamjerni, unutarnji ili vanjski, [8].

U poslovnom okruženju prijetnje mogu proizaći iz različitih izvora, uključujući zaposlenike, hakere, zlonamjerni softver, fizičke nesreće ili prirodne katastrofe. Ljudske prijetnje često se dijele na nenamjerne, koje proizlaze iz ljudske pogreške ili nepažnje, i namjerne, koje uključuju zlonamjerne radnje usmjerene na nanošenje štete. Prirodne prijetnje, iako izvan kontrole organizacije, mogu imati ozbiljan utjecaj na poslovanje, osobito ako se ne uzmu u obzir pri planiranju kontinuiteta poslovanja. Također, tehnološke ranjivosti, koje proizlaze iz slabosti u dizajnu softvera, hardvera ili mrežne infrastrukture, često se iskorištavaju za provođenje napada, [9].

Razumijevanje različitih izvora prijetnji ključno je za razvoj učinkovitih strategija zaštite koje kombiniraju tehnička rješenja, proceduralne mjere i edukaciju zaposlenika. Takav sveobuhvatan pristup omogućava organizacijama da proaktivno upravljaju rizicima i minimiziraju potencijalne štete od kibernetičkih napada.

3.1.1. Ljudske prijetnje s atribucijom nenamjernosti

Razvoj informacijsko-komunikacijskih tehnologija, osim svojih benefita za pojedince i organizacije, donosi i negativne aspekte u vidu povećane ranjivosti korisnika sustava na kibernetičke prijetnje. Iako svaka tehnologija ima određene mehanizme zaštite od iskorištavanja potencijalnih ranjivosti, ključnu ulogu u sigurnosti korištenog sustava ima krajnji korisnik, odnosno njegovo ponašanje prilikom korištenja tehnologije, [10].

Ljudski faktor, odnosno greška korisnika u kontekstu kibernetičke sigurnosti odnosi se na nenamjerne radnje, nemar i previd prilikom donošenja odluka u radu. Iskorištavanjem tih ranjivosti krajnjeg korisnika, napadači mogu izvršiti kibernetičke napade koji mogu rezultirati curenjem povjerljivih informacija i kompromitacijom samog sustava, [11].

3.1.2. Ljudske prijetnje s atribucijom namjernosti

Prema javno dostupnim statistikama, većina kibernetičkih napada na poslovna okruženja provedena su od strane malicioznih aktera. Kako bi se definirale skupine zlonamjernih aktera, potrebno je objasniti pojam atribucije u području informacijske sigurnosti. Atribucija predstavlja skup tehničkih metoda čiji je cilj identifikacija počinitelja kibernetičkog napada. Također cilj atribucije je pružiti informacije o motivima i ciljevima koje pojedine skupine aktera nastoje postići, [12],[13].

U nastavku ovog rada, ljudske prijetnje s atribucijom namjernosti, odnosno maliciozni akteri, bit će podijeljeni na: interne napadače, poslovne partnere, nacionalne vlade, kriminalne organizacije, haktiviste te *script kiddies*, [14].

3.1.2.1. *Interni napadači*

Interni napadači, odnosno unutarnje prijetnje predstavljaju složeni rizik za sve sektore kritične infrastrukture. Prema agenciji za kibernetičku sigurnost i sigurnost američke infrastrukture (engl. Cybersecurity and Infrastructure Security Agency, CISA) interni napadači definiraju se kao insajderi koji koriste dobivenu razinu pristupa kako bi proveli maliciozne aktivnosti unutar infrastrukture organizacije, [15].

Unutarnje prijetnje kao i većina ostalih skupina napadača ovisi o razini pristupa kojeg ostvaruju u sustavu, ali u odnosu na njih svoje prednosti povlače iz dubinskog poznavanja sustava i

poslovnih procesa. Poznavanjem poslovnih procesa i infrastrukturne hijerarhije organizacije, interni napadači lakoćom definiraju svoje napade, odnosno maliciozne radnje koje žele izvršiti. Samo izvršavanje tih aktivnosti često prolazi neopaženo zbog toga što se ponašanje malicioznog zaposlenika teško može razlikovati od uobičajenih poslovnih zadataka. Motivacija iza ove vrste napada, odnosno napadača može biti raznolika, od financijske dobiti i pružanja otpora provođenoj politici do prisile i suradnje s zlonamjernim skupinama, [16].

3.1.2.2. Državno sponzorirani napadači

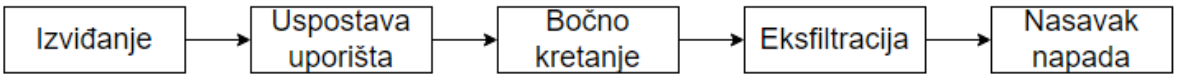
Državno sponzorirani napadači kao izvor prijetnje infrastrukturi organizacije predstavljaju skupinu visoko obučenih pojedinaca koji izravno ili neizravno rade za druge države kojima je cilj destabilizacija, narušavanje rada i uništavanje kritičnih sustava. Promatranjem ponašanja ovih aktera zaključuje se kako im je glavni cilj ostvarivanje postojanosti unutar kompromitiranog sustava. Ostvarivanjem perzistentnosti napadači ostaju neprimijećeni te koristeći dostupnu tehnologiju provode eksfiltraciju informacija i pozicioniraju se za provođenje strateških napada. Kako bi ostali neopaženi od strane sigurnosnih kontrola organizacije, državno sponzorirani akteri kreiraju suptilne digitalne otiske u svrhu skrivanja pravog izvora prijetnje, [17], [18].

U odnosu na ostale kibernetičke prijetnje, držano poduprtim akterima glavna svrha je prikupiti osjetljive informacije kritičnih infrastruktura pomoću kojih stvaraju bolju poziciju u pregovorima s drugim državama, odnosno te informacije koriste kako bi oslabili protivnike u slučaju ratnog stanja. Također ovaj tip kibernetičke prijetnje se razlikuje od ostalih vrsta prema tome što se infrastrukture koje se napadaju pomno biraju i u najvećoj mjeri su samo dio šire slike napada koji određena država provodi, [19].

3.1.2.3. Napredne ustrajne prijetnje

Napredne ustrajne prijetnje (engl. Advanced Persistent Threats, APT) predstavljaju ekspertnu skupinu napadača koja ima visokotehnološka rješenja pomoću kojih provode zamišljene aktivnosti različitim vektorima napada. APT skupine uglavnom za cilj imaju uspostavljanje uporišta unutar infrastrukture informacijsko-komunikacijskog sustava organizacije s ciljem eksfiltracije podataka, ometanja rada kritičnih sustava te pozicioniranja za izvođenje budućih napada, [20].

Za postizanje zadanih ciljeva, skupine svoje napade provode u etapama koje su često različitih oblika, a model kojim se njihovi napadi opisuju vidljiv je na idućoj slici.



Slika 1: Model APT napada

Prva faza napada APT skupina je provođenje izviđačkih aktivnosti, kojima je svrha prikupljanje svih dostupnih informacija s dubinskog razumijevanja ponašanja ciljane infrastrukture. Uspješnim izviđanjem i prikupljanjem kritičnih informacija, akteri provode iduću etapu napada kojom ostvaruju inicijalni pristup sustavu u svrhu kreiranja uporišta putem kojih će provoditi daljnje napadačke aktivnosti. Kreiranjem uporišta unutar targetirane infrastrukture stvorena je podloga koja se koristi za bočno kretanje, odnosno iduću fazu samog napada. Bočnim kretanjem APT skupine prvenstveno otkrivaju sustave unutar mreže te mapiraju moguće ranjivosti i slabosti tih sustava kako bi ih iskoristili u nastavku zamišljenih malicioznih aktivnosti. Nakon uspješnog otkrivanja svih napadačima bitnih resursa, započinje idući korak napada kojim se prikupljeni podaci neovlašteno iznose van kompromitirane infrastrukture. Završetkom eksfiltracije podataka APT skupine zaključuju inicijalni napad, te dobiveni pristup i stečeno znanje kompromitirane infrastrukture koriste na način da nastavljaju pratiti životni ciklus same organizacije i izvlačiti novootkrivene informacije od interesa [21], [22], [23].

3.1.2.4. Haktivisti

Haktivisti su pojedinci ili grupe koje koriste svoje znanje o informacijsko komunikacijskim sustavima kako bi promovirali svoje ideje. Nekada su njihovi postupci i akcije potpuno legalne, kao što je organiziranje online prosvjeda, dok ponekad provode napade, pokušavajući skrenuti pažnju na svoja politička ili društvena pitanja. Njihovi napadi nisu uvijek usmjereni na stvaranje štete, već na isticanje svojih stavova. Ipak, te aktivnosti mogu uzrokovati ozbiljne probleme unutar poslovnih okruženja, jer su rezultati njihovog djelovanja često nepredvidivi, [24].

3.1.2.5. Kibernetički kriminalci

Kibernetički kriminalci kao izvor prijetnje poslovnom okruženju definiraju se kao pojedinci ili skupine aktera koji koriste svoje znanje i tehnologiju kao alat za provođenje malicioznih aktivnosti u svrhu krađe povjerljivih ili osobnih podataka te financijske dobiti. Njihova glavna karakteristika je uporaba prikrivene mreže (engl. *darknet*) s ciljem skrivanja tragova i trgovine podacima i uslugama drugih zloćudnih dionika. U odnosu na prijašnje tipove malicioznih aktera razlikuju se u namjerama prilikom provođenja napada, to jest kibernetički kriminalci ne biraju

specifične ciljeve, već svoje maliciozne kampanje provode nad velikim brojem korisnika informacijskih sustava, [25].

3.1.3. Automatizirane probe

Automatizirane probe kao izvor prijetnji poslovnoj infrastrukturi mogu se podijeliti u dvije skupine. Prva skupina obuhvaća skenere, dok drugu skupinu čine maliciozni kodovi poznati pod nazivom crvi. Općenito, automatizirane probe mogu se definirati kao skup specijaliziranih alata koji pretražuju ranjivosti na dostupnim mrežama i Internetu općenito.

Skeneri su često prva skupina automatiziranih alata koji ispituju mrežnu infrastrukturu, no obično ne predstavljaju izravnu prijetnju. Umjesto toga, mogu se smatrati konstantnom smetnjom u radu sustava. Glavna svrha skenera je analizirati mreže i aplikacije kako bi otkrili slabosti koje napadači mogu iskorištavati. Iako skeneri koji pretražuju Internet svaki dan nisu opasni, oni mogu pomoći napadačima da prikupe informacije o ciljanom sustavu. Dvije glavne vrste skenera koji se najčešće koriste u svijetu informacijske sigurnosti su oni za mrežno mapiranje i oni za otkrivanje ranjivosti.

Vanjski skeneri za mapiranje mreža sustavno istražuju i prikupljaju informacije iz ciljanih mreža. Gledano iz perspektive prijetnji informacijskom sustavu organizacije, ova vrsta skenera napadačima može pružiti informacije o rasponu korištenih mrežnih adresa, aktivnim uređajima na mreži, otvorenim mrežnim portovima i korištenim servisima.

Skeneri za otkrivanje ranjivosti, kada ih koriste vanjski napadači, predstavljaju ozbiljnu prijetnju infrastrukturi ciljane organizacije. Ova vrsta skenera napadačima služi kao izvor informacija o mogućim ranjivostima koje se mogu iskoristiti u maliciozne svrhe, [26].

Računalni crvi također se smatraju vrstom automatiziranih probi iz perspektive kibernetičke sigurnosti zbog svoje sposobnosti replikacije bez potrebe za interakcijom korisnika. Računalni crvi šire se mrežom neovisno, s ciljem pretraživanja infrastruktura kako bi pronašli i iskoristili ranjive sustave. Početni korak kibernetičkih napada, odnosno izviđanje, provodi se mapiranjem mrežne arhitekture i identifikacijom potencijalnih meta unutar infrastrukture. Autonomna replikacija crva omogućuje im brzo i lako širenje mrežom, s ciljem inficiranja što većeg broja krajnjih uređaja. Kao automatizirane probe, računalni crvi malicioznim akterima omogućuju jednostavno prikupljanje informacija poput točaka ulaska i slabosti ciljane infrastrukture.

3.1.4. Prirodne prijetnje

Vremenske nepogode, poput oluja ili poplava, mogu ozbiljno narušiti rad informacijskih sustava. Iako nisu namjerne, ove prirodne pojave mogu uzrokovati oštećenja na opremi, gubitak važnih podataka ili prekid mrežnih veza. Takvi problemi često vode do dodatnih troškova i gubitaka.

Iako prirodne nepogode nemaju namjeru narušiti integritet poslovnog okruženja, njihova pojava omogućuje zlonamjernim korisnicima njihovo iskorištavanje. Najčešće provođeni napadi u takvim okolnostima uključuju socijalni inženjering i napade na pogođene infrastrukture zlonamjernim kodom.

3.1.5. Nezgode

Nezgode kao izvor prijetnji informacijsko-komunikacijskim sustavima odnose se na nenamjerne incidente koji mogu izazvati poremećaje u radu sustava ili gubitak podataka. Ovi događaji, iako često neizbježni u složenim tehnološkim okruženjima, mogu imati ozbiljne posljedice za sigurnost i funkcionalnost poslovnih procesa.

Najčešće vrste nezgoda uključuju ljudske pogreške, kao što su nenamjerno brisanje podataka ili pogrešna konfiguracija sustava, te tehničke kvarove koji mogu dovesti do nedostupnosti ključnih komponenti ili gubitka pristupa resursima. Iako su ove nezgode nenamjerne, njihov utjecaj na sigurnost sustava može biti značajan, posebno ako se ne prepoznaju i pravovremeno ne uklone.

3.2. Ranjivosti

Ranjivost (engl. *Vulnerability*) odnosi se na specifičnu slabost u sustavu, procesu, dizajnu, implementaciji ili upravljanju informacijskim sustavom koja može biti iskorištena dovodeći do narušavanja integriteta, povjerljivosti ili dostupnosti podataka. Ranjivosti su inherentni dio kompleksnih informacijskih sustava, a njihova prisutnost omogućuje eksploataciju koja često rezultira gubitkom podataka, prekidom usluga ili kompromitacijom poslovne infrastrukture, [14].

Ranjivosti se klasificiraju prema različitim kriterijima, a najčešće se grupiraju prema komponentama ili domenama na koje se odnose. Detaljna klasifikacija omogućuje precizniju analizu i implementaciju politika za smanjenje rizika, [9].

Fizičke i infrastrukturne ranjivosti odnose se na fizičke aspekte zaštite informacijskih sustava i infrastrukture. Najčešće ranjivosti koje se povezuju s poslovnim okruženjima su: neadekvatna

fizička zaštita prostora, neadekvatna kontrola pristupa te nestabilnost energentske mreže. Iskorištavanjem ovih ranjivosti zlonamjerni pojedinci izravno utiču na fizičke komponente informacijsko-komunikacijskih ustava organizacije, te uzrokuju smetnje i totalni prekid poslovnih procesa.

Hardverske ranjivosti odnose se na elektroničke komponente informacijskih sustava. Većinski se ove ranjivosti odnose na same karakteristike pojedinih elektroničkih komponenti, a najčešće se manifestiraju kroz nisku toleranciju na varijabilne okolišne uvjete i zamor materijala.

Softverske ranjivosti predstavljaju slabosti unutar koda aplikacija ili operativnih sustava koje mogu biti iskorištene za neovlašteni pristup, eskalaciju prava ili druge zlonamjerne radnje. Najčešće ranjivosti ovog tipa uključuju: neadekvatna validacija ulaznih podataka, nedostatak ažurnih verzija programa te jednostavna i neadekvatna autentifikacija. Iskorištavanjem navedenih ranjivosti napadači s lakoćom dobivaju pristup osjetljivim podacima i intelektualnom vlasništvu organizacije.

Komunikacijske ranjivosti odnose se na sami proces prijenosa podataka. Korištenjem nezaštićenih komunikacijskih kanala, organizacije ostavljaju svoje podatke dostupne svima te ih napadači lako presreću i modificiraju. Također upotreba starijih ili ranjivih komunikacijskih protokola onemogućuje inherentnu enkripciju, odnosno zaštitu integriteta čime se pospješuje napredak kibernetičkog napada usmjerenog na infrastrukturu organizacije.

Ljudske ranjivosti u kontekstu sigurnosti informacijskih sustava organizacija predstavlja jednu od najkritičnijih točki ulaska. Ranjivosti u ljudskoj prirodi se najčešće eksploatiraju manipulacijom, odnosno tehnikama socijalnog inženjeringa. Također kako se tehnike socijalnog inženjeringa svakodnevno poboljšavaju, zaposlenici postaju sve češća meta kibernetičkih napada, a velika stopa uspješnosti tih napada govori da osim sofisticiranih napada postoji veliki jaz između obuke i svijesti o sigurnosti i organizacijskih politika.

3.3. Metode kibernetičkih napada

Kibernetički napadi predstavljaju ozbiljan izazov za suvremene informacijske sustave, s obzirom na sve veću ovisnost o digitalnoj tehnologiji i Internetu. Razvoj sofisticiranih tehnika omogućava napadačima pristup osjetljivim podacima, narušavanje integriteta sustava i ometanje poslovnih procesa. Metode kibernetičkih napada su raznolike i neprestano se razvijaju, uključujući širok spektar zlonamjernih aktivnosti usmjerenih na kompromitaciju sigurnosti informacijskih sustava. Kibernetički mogu biti motivirani financijskom dobiti,

industrijskom špijunažom, političkim ciljevima ili jednostavnom željom za ometanjem rada sustava. Kroz detaljnu analizu metoda kao što su zlonamjerni programi, socijalni inženjering, napadi uskraćivanja usluge, napadi korištenjem rječnika i Man-in-the-Middle napadi, ovaj će rad istražiti temeljne principe, taktike i tehnike koje napadači koriste. Razumijevanje ovih metoda ključno je za razvoj učinkovitih strategija obrane i zaštite informacijskih sustava, osiguravajući kontinuitet poslovanja i zaštitu podataka od neovlaštenog pristupa.

3.1.1. Zlonamjerni programi

Zlonamjerni programi predstavljaju računalne alate dizajnirane u svrhu ostvarivanja neovlaštenog pristupa, kompromitacije i narušavanja funkcionalnosti poslovnih sustava. Programi malicioznog koda u poslovnom okruženju postaju učestala pojava, a njihova nekontrolirana evolucija klasificira ih kao jednu od kritičnih stavki protiv koje se sigurnosni sustavi i stručnjaci suočavaju svakodnevno. Obuhvaćaju viruse, trojanske konje, ucjenjivačke zlonamjerne programe, crve i špijunske programe, gdje svaka od kategorija cilja specifične segmente sustava kako bi ostvarila svoje zlonamjerne ciljeve.

Zlonamjerni programi distribuiraju se putem različitih vektora napada, uključujući zaražene privitke elektroničke pošte, zlonamjerne web stranice, nesigurna preuzimanja te iskorištavanje ranjivosti unutar aplikacija i operativnih sustava. Uspješnim inficiranjem krajnjih uređaja programi malicioznog koda pokreću aktivnosti poput eksfiltracije podataka, enkripcije datoteka radi iznude, praćenje korisničke aktivnosti te uspostave stražnjih vrata (engl. *Backdoor*), [27].

3.1.1.1. Trojanski konj

Trojanski konj predstavlja zlonamjerni program koji je naizgled bezopasan i legitiman s ciljem prevare krajnjih korisnika u njegovo preuzimanje i egzekuciju unutar poslovnog okruženja. Preuzimanjem i pokretanjem takvog programa malicioznog koda, korisnik nesvjesno kompromitira infrastrukturu u kojoj se nalazi, te zlonamjerni program izvršava svoju svrhu, odnosno uzrokuje štetu za koju je kreiran. Iako postoji veliki broj inačica ove vrste zlonamjernog programa, većina ih se može definirati kao maliciozni kod čiji je cilj preuzimanje kontrole nad sustavom, krađa podataka te špijunaža krajnjeg korisnika, tj. kompromitirane infrastrukture, [28].

Najčešće inačice trojanskih konja u poslovnom okruženju su *backdoor, exploit, rootkit, downloader* i *dropper*. *Backdoor trojan* stvara stražnja vrata na inficiranom krajnjem uređaju s ciljem omogućavanja udaljenog pristupa i kontrole sustava malicioznim akterima. *Exploit* se definiraju kao aplikacije koje sadrže programski kod koji iskorištava ranjivost unutar servisa i

programa koji se pokreću na kompromitiranom sustavu. *Rootkit* je inačica trojanskog konja koja se većinom dizajnira s ciljem skrivanja određenih entiteta i aktivnosti u zaraženom sustavu u svrhu produživanja vijeka rada zloćudnih programa. *Downloader* i *dropper* trojanci koriste se za preuzimanje i instalaciju dodatnih programa malicioznog koda s ciljem daljnje kompromitacije i sprječavanja otkrivanja malicioznih aktivnosti na inficiranom krajnjem uređaju, [29].

3.1.1.2. Aplikacije neželjenog koda

Potencijalno neželjeni programi (engl. *Potentially unwanted programs*, PUP) su dio programskog paketa koji izravno nije zlonamjeran, ali može prouzročiti neželjene učinke na informacijske sustave. Njihova distribucija se u većini slučajeva odvija korištenjem tehnika upakiravanja, gdje se PUP isprepliće s drugim legitimnim aplikacijama koje zaposlenik koristi. Neželjeni programi identificiraju se kao napredne alatne trake, dodaci za preglednike, *adware* i kao programi za praćenje, [30].

3.1.1.3. Ucjenjivački programi

Ucjenjivački program (engl. *Ransomware*) predstavlja vrstu zlonamjernog programa čija je svrha zaključavanje i kriptiranje podataka informacijskih sustava s ciljem iznuđivanja financijskih sredstava od pogođene organizacije. Ova vrsta programa malicioznog koda u sinergiji s tehnikama i napadima socijalnog inženjeringa predstavlja glavnu prijetnju poslovnim i procesnim sustavima organizacije. Iako je cilj napadača ostvariti financijsku dobit, ovisno o korištenoj vrsti ucjenjivačkog programa napadači mogu uzrokovati ispade poslovnih procesa i onemogućavanje pristupa kritičnoj infrastrukturi , [31].

Kao i kod većine ostalih malicioznih programa, *ransomware* kao ulaznu točku u sustav iskorištava interakciju s neopreznim korisnicima sustava, na način da svoj maliciozni kod ugrade u zaražene privitke i datoteke elektroničke pošte, odnosno kompromitiranih javno dostupnih Internet servisa. Jednom kada je program ostvario inicijalni pristup infrastrukturi on započinje svoje izvršavanje, te ovisno o njegovoj vrsti vrši enkripciju datoteka i sustava, [32].

Ucjenjivački programi najčešće korišteni u napadima na pravne osobe dijele se na: ransomware programe koji šifriraju podatke (engl. *Crypto ransomware*) ali ne onemogućuju pristup sustavu, ransomware programe koji zaključavaju sustav (engl. *Locker ransomware*) te *doxware* ucjenjivački program kojim napadači iznudu provode prijetnjom objave klasificiranih informacija, [33].

3.1.1.4. Crvi

Računalni crvi predstavljaju vrstu zlonamjernih programa koja se samostalno replicira unutar informacijsko-komunikacijskog sustava te iskorištava ranjivosti u mrežnim protokolima i aplikacijama kako bi se propagirali mrežom. Kako bi izvršili svoju malicioznu zadaću, crvi koriste napredne tehnike automatizirane replikacije gdje pomoću pronađenih ranjivosti i slabosti u mreži targetiraju nove krajnje uređaje. Uspješnom infiltracijom na više mrežnih lokacija računalni crvi započinju s drugom fazom svog životnog ciklusa, odnosno izvršavaju definirane maliciozne zadatke, poput ubacivanja novih malicioznih programa, uspostavljanja stražnjih vrata i eksfiltracije podataka, [34].

Gledano iz perspektive sigurnosti poslovnih organizacija, najčešće inačice računalnih crva koje pogađaju poslovne sustave su e-mail crvi, Internet crvi i *botnet* crvi. E-mail crvi funkcioniraju na način da se prilikom otvaranja zaraženog privitka ili elektroničke poruke, crvu omogućuje replikacija na način da zaraženi privitak pošalje svim kontaktima inicijalno zareženog korisničkog pretinca. Internet crvi u odnosu na e-mail crve traže ranjivosti u mrežnim uslugama i protokolima s ciljem propagacije mrežom bez potrebe za interakcijom s korisnicima sustava. Najčešće rade na način da provode skeniranja IP adresa te identifikacijom ranjivih adresa, automatizmom pokušavaju kompromitirati sustave. *Botnet* crvi služe kao jedan od inicijalnih vektora napada sofisticiranih napadača. Korištenjem ove vrste računalnih crva napadači pokušavaju stvoriti zombi mrežu zaraženih uređaja, koje kontroliraju udaljenim pristupom te ih koriste u budućim napadima na kritične infrastrukture targetiranih organizacija, [35].

3.1.2. Socijalni inženjering

Socijalni inženjering definira se kao napad koji koristi ljudsku psihologiju u svrhu stvaranja utjecaja nad ciljanim korisnikom ili skupinom korisnika informacijsko-komunikacijskog sustava. Cilj svakog napada korištenjem tehnika socijalnog inženjeringa je otkrivanje povjerljivih informacija i provođenje zlćudnih aktivnosti bez izravnog pristupa poslovnom sustavu. Kako bi uspješno proveli napade socijalnim inženjeringom, napadači svoje aktivnosti provode u nekoliko faza, od prikupljanja informacija i kreiranja scenarija do provođenja napada i kompromitiranja targetirane infrastrukture, [36].

Provođenje kibernetičkih napada korištenjem tehnika socijalnog inženjeringa započinje prikupljanjem informacija iz javno dostupnih izvora (engl. *Open Source* Intellignece, OSINT). Upotreba OSINT tehnika napadačima omogućuje prikupljanje podataka o ciljevima, poput pojedinaca i organizacija te kreiranja svojih scenarija kojima je cilj stvaranje iluzije legitimnosti. Uspješnom identifikacijom ciljeva i kreiranjem zlćudnog sadržaja, napadači

započinju s fazom napada kojom napravljeni sadržaj distribuiraju označenim kontaktima. Način distribucije malicioznog sadržaja najčešće se provodi tehnikama: *phishing*, *spear phishing*, *smishing*, *vishing*, *pretexting* i *baiting*, [37].

Phishing je jedna od najraširenijih tehnika socijalnog inženjeringa koja uključuje slanje lažnih elektroničkih poruka širokom spektru mogućih žrtvi. Cilj ovih napada je navođenje korisnika na izvršavanje malicioznih radnji i otkrivanje osjetljivih podataka koji u poslovnom okruženju često uključuju zaporke i brojeve kreditnih kartica, [36].

Spear phishing predstavlja sofisticiraniji oblik *phishing* napada koji je usmjeren na specifične pojedince ili organizacije. Ova vrsta napada koristi personalizirane informacije pomoću kojih napadači kreiraju naizgled legitimne elektroničke poruke. Ovi napadi provode se s ciljem kompromitacije organizacije, na način da se iskorištavaju ljudske ranjivosti kod zaposlenika visokog menadžmenta ili visoko privilegiranih administratora informacijskih sustava, [37].

Smishing je inačica *phishing* napada koja se provodi putem SMS poruka. Ova tehnika napada uključuje slanje tekstualnih poruka koje se čine autentičnima, a cilj im je navesti primatelje da otvore poveznice koje vode na lažne web stranice ili da nazovu brojeve telefona koji su povezani s napadačima.

Vishing tehnika odnosi se na korištenje telefonskih poziva za provođenje socijalnog inženjeringa. U ovim napadima napadači se predstavljaju lažnim identitetima s ciljem uvjeravanja žrtve da otkrije povjerljive informacije ili provede aktivnosti kojima napadači ostvaruju svoje ciljeve.

Baiting je tehnika socijalnog inženjeringa koja uključuje korištenje mamaca u svrhu privlačenja osoba na interakciju sa zlonamjernim sadržajem. Mamci mogu biti fizički u obliku zaraženih vanjskih medija za pohranu podataka ili digitalni poput lažnih oglasa koji nude besplatna preuzimanja datoteka. Cilj *baitinga* je navesti korisnike na preuzimanje zlonamjernog sadržaja pomoću kojeg napadači ostvaruju inicijalni pristup poslovnom sustavu te provode daljnje korake svojih napada.

3.1.3. Napadi uskraćivanja usluge

Napadi uskraćivanja usluge predstavljaju značajni sigurnosni izazov u poslovnim okruženjima. Ovi napadi za cilj imaju onemogućiti pristup legitimnim korisnicima određenim uslugama ili mrežnim resursima preopterećivanjem mrežne infrastrukture. Napadi uskraćivanja usluge koriste se kao strateški alati za ometanje rada informacijskih sustava, aplikacija ili usluga, [38].

Napadi uskraćivanja usluge dijele se na napade koji su generirani iz jednog izvora (*Denial of Service*, DoS) te na napade koji su generirani iz više izvora (engl. *Distrubuted Denial of Service*, DDoS). Funkcionalnosti ovih napada najčešće se manifestiraju kroz volumetrijske, protokolarne i aplikacijske napade, dok se mehanizmi rada temelje na preplavljivanju prometa, iscrpljivanju resursa i eksploataciji ranjivosti, [39].

3.1.4. Napadi korištenjem rječnika

Napadi korištenjem rječnika (engl. *Dictionary Attacks*) predstavljaju metodu kibernetičkih napada koji za cilj imaju ostvarivanje pristupa u ciljani sustav korištenjem sistematičnog testiranja riječi i fraza koje se nalaze na definiranoj listi zaporki. Lista zaporki ovisno o geografskoj lokaciji i ciljanoj infrastrukturi sadrži često koriste kao lozinke i frazeme tog područja. Sami napadi i njihova efikasnost ovise o sigurnosnim politikama organizacije, odnosno o podešenim mehanizmima za suzbijanje ovakve vrste napada, uključujući primjenjivanje kompleksnih zaporki i zaključavanje sustava nakon određenog broja neuspješnih prijava. [40].

3.1.5. Napadi čovjeka u sredini

Napadi čovjeka u sredini (engl. *Man-in-the-Middle*, MitM) sofisticirana su vrsta kibernetičkih napada u kojima napadači neovlašteno prisluškuju, izmjenjuju ili manipuliraju informacijama između dvije strane koje vjeruju da izravno komuniciraju jedna s drugom. MitM napadi presreću informacije u raznim komunikacijskim kanalima, kao što su mrežne i telefonske komunikacije, elektronička pošta i fizički uređaji. Napadači koriste različite tehnike za postavljanje svojih tehnologija kao posrednika između komunikacijskih strana, čime ostvaruju mogućnost neprimjetnog pristupa osjetljivim informacijama, [14].

3.1.6. Zero day ranjivosti

Zero-day ranjivosti odnose se na proizvođaču nepoznate sigurnosne propuste u programskim rješenjima. Takvi sigurnosni propusti omogućuju malicioznim akterima da ih iskoriste i provedu *zero-day* napade u vremenskom periodu dok još većina korisnika informacijsko-komunikacijskog sustava nije svjesna postojanja samog sigurnosnog propusta. Iskorištavanjem ovih ranjivosti napadači ostvaruju infiltraciju u inače teško dostupne poslovne infrastrukture, te samim time stvaraju uporišta za provođenje budućih napada, [41].

4. Simulacija kibernetičkih napada

U suvremenom digitalnom okruženju, kibernetička sigurnost postala je ključna komponenta u zaštiti poslovnih informacijsko-komunikacijskih sustava. S obzirom na sve veći broj prijetnji koje se pojavljuju organizacije su prisiljene implementirati napredne metode zaštite kako bi povećale sigurnost svojih digitalnih resursa. Jedna od najvažnijih metoda u ovom kontekstu je simulacija kibernetičkih napada, koja omogućuje organizacijama da procijene otpornost svojih sustava protiv potencijalnih ugroza.

Simulacija kibernetičkih napada uključuje korištenje specijaliziranih tehnika i alata pomoću kojih se identificiraju ranjivosti u informacijskim sustavima, što omogućava korištenje realističnih scenarija koji sadrže metode i tehnike korištene u stvarnim kibernetičkim napadima. Simulacijom napada organizacija se fokusira na procjenu sigurnosnih mjera iz perspektive napadača čime se omogućuje identificiranje slabih točaka koje mogu biti iskorištene, [42].

Važnost simulacije kibernetičkih napada ogleda se u sposobnosti organizacije da unaprijed identificira i adresira sigurnosne propuste prije nego što budu iskorišteni u stvarnim napadima. Provođenjem simulacije omogućuje se poboljšanje sigurnosnih kontrola na temelju stvarnih prijetnji i rizika, umjesto provođenja reaktivnih aktivnosti nakon što se sigurnosni incident dogodi. Simulacije napada također igraju ključnu ulogu u razvoju i testiranju strategija odgovora na sigurnosne incidente, jer kroz simulaciju stvarnih prijetnji organizacije mogu testirati svoje protokole i procedure odgovora na incidente, što omogućuje identifikaciju slijepih točaka, njihovo popravljanje te pripremanje sigurnosnih timova za stvarne događaje, [43], [44].

Također simulacije kibernetičkih napada omogućuju organizacijama da zadovolje sve strože regulatorne zahtjeve za kibernetičku sigurnost. Identificiranje i ispravljanje ranjivosti kroz simulacije pomaže organizacijama da osiguraju usklađenost s važećim propisima i standardima, što je ključno za izbjegavanje pravnih sankcija i drugih regulatornih posljedica. Važno je naglasiti da uspješne simulacije kibernetičkih napada zahtijevaju suradnju različitih odjela unutar organizacije, uključujući odjele sistemskog inženjerstva, menadžmenta, pravne timove i odjele za upravljanje rizicima.

4.1. Radni okviri modeliranja kibernetičkih ugroza

Radni okviri za modeliranje kibernetičkih prijetnji predstavljaju strukturirani skup smjernica, metoda i alata koji pomažu u identificiranju, analizi i upravljanju ugrozama unutar poslovnih informacijskih sustava. Organizacijama omogućuju sistematičan pristup kod prepoznavanja potencijalnih prijetnji i ranjivosti te stvaranju strategija obrane i odgovora na sigurnosne incidente. Osnovna zadaća radnih okvira je pružiti standardizirani načina razumijevanja i interpretacije različitih segmenata kibernetičke sigurnosti, što je ključno za koordiniranu i učinkovitu reakciju na prijetnje. Najkorišteniji radni okviri u poslovnim okruženjima su MITRE ATT&CK i *Cyber Kill Chain*, koji nude strukturirane metode za analizu taktika, tehnika i procedura koje napadači koriste. Navedeni okviri pomažu stručnjacima za sigurnost u razumijevanju ponašanja napadača što omogućuje provođenje proaktivnih mjera zaštite te brži odgovor na kibernetičke napade, [45], [46] .

Pomoću radnih okvira, organizacije sustavno analiziraju i dokumentiraju sigurnosne incidente s ciljem donošenja odluka o resursima za kibernetičku sigurnost, raspodjeli prioriteta i razvoju novih sigurnosnih politika. Kroz primjenu MITRE ATT&CK okvira, sigurnosni stručnjaci organizacije analiziraju prethodne napade, identificiraju korištene tehnike i uspoređuju ih s postojećim sigurnosnim mjerama kako bi identificirali slijepe točke u svojoj sigurnosnoj infrastrukturi. S druge strane, *Cyber Kill Chain* omogućuje organizacijama razumijevanje svih faza napada te da definiraju točke u kojima se napad može prekinuti u svrhu učinkovitijeg odgovora i suzbijanja širenja napadača, [47].

4.1.1. MITRE ATT&CK

MITRE ATT&CK je sveobuhvatan javno dostupan okvir osmišljen za modeliranje ponašanja napadača kroz strukturirani skup taktika, tehnika i procedura koje koriste napadači tijekom životnog ciklusa kibernetičkog napada. Osnovni cilj ovog okvira je pružanje standardiziranog jezika i strukture koja omogućuje dijeljenje informacija o ugrozama i razvoju obrambenih mehanizama unutar poslovnih okruženja, odnosno njihovih sigurnosnih timova. MITRE ATT&CK dizajniran je tako da pokriva cijeli spektar napada, od inicijalnog pristupa do eksfiltracije podataka, te time omogućava detaljnu analizu i mapiranje aktivnosti napadača.

Struktura MITRE ATT&CK okvira bazira se na tri glavne komponente: taktike, tehnike i pod-tehnike. Ove komponente su temelj za razumijevanje ponašanja napadača i omogućavanje analitičarima da mapiraju napade i identificiraju kritične točke za obranu. Tehnike predstavljaju specifične metode kojima napadači ostvaruju svoje ciljeve, dok pod-tehnike opisuju njihove

varijacije koje precizno definiraju aktivnosti napadača. Popis taktika i njihovog osnovnog opisa prikazan je idućom tablicom.

Tablica 1: Prikaz taktika MITRE ATT&CK okvira, [48]

Naziv taktike	Opis
Izviđanje (eng. Reconnaissance)	Prikupljanje informacija o potencijalnim metama
Razvoj resursa (eng. Resource Development)	Prikupljanje potrebnih resursa i alata za provođenje napada
Inicijalni pristup (eng. Initial access)	Uspostava početne točke kompromitacije
Izvršenje (eng. Execution)	Pokretanje zlonamjernih programa
Perzistentnost (eng. Persistence)	Osiguravanja kontinuiranog pristupa sustavu
Eskalacija privilegija (eng. Privilege Escalation)	Stjecanje viših razina pristupa unutar sustava
Izbjegavanje obrane (eng. Defense evasion)	Izbjegavanje otkrivanja od strane sigurnosnih sustava
Prikupljanje vjerodajnica (eng. Credential Access)	Preuzimanje korisničkih vjerodajnica za pristup sustavima
Otkrivanje (eng. Discovery)	Dubinsko prikupljanje informacija o sustavu
Bočno kretanje (eng. Lateral Movement)	Kretanje kroz sustave s istim pravima
Prikupljanje (eng. Collection)	Prikupljanje informacija i podataka od interesa
Zapovijedanje i upravljanje (eng. Command and Control)	Održavanje komunikacije s kompromitiranim sustavima
Eksfiltracija (eng. Exfiltration)	Prijenos ukradenih podataka izvan mreže
Utjecaj (eng. Impact)	Manipulacija, ometanje, uništavanje sustava

MITRE ATT&CK okvir koristi se u različitim scenarijima kako bi pomogao organizacijama u borbi protiv kibernetičkih prijetnji. Neki od ključnih načina primjene uključuju, [5]:

- Mapiranje napada: Analitičari informacijske sigurnosti koriste okvir za mapiranje napada kako bi identificirali taktike i tehnike korištene u kibernetičkom napadu. Mapiranje omogućava bolje razumijevanje ponašanja napadača i prepoznavanje obrazaca koji se koriste za detekciju sličnih napada u budućnosti.
- Razvoj detekcijskih pravila: Na temelju identificiranih tehnika i taktika, organizacije mogu razviti specifična pravila za detekciju koja su usmjerena na prepoznavanje specifičnih aktivnosti napadača.
- Analiza prijetnji: ATT&CK omogućava sigurnosnim stručnjacima da kategoriziraju i analiziraju prijetnje prema poznatim taktikama, tehnikama i procedurama napadača. Na

taj način procjenjuju rizik i integriraju sigurnosne mjere koje su usmjerene na specifične prijetnje.

MITRE ATT&CK okvir proširen je na različite specijalizirane verzije prilagođene specifičnim područjima rada s ciljem obuhvaćanja raznolikih ugroza s kojima se organizacije suočavaju. Okvir pruža dubinsko razumijevanje ugroza koje ciljaju tradicionalne informacijske sustave, mobilne uređaje i industrijske kontrolne sustave (engl. *Industrial Control Systems,* ICS).

MITRE ATT&CK *for Mobile* predstavlja specijaliziranu verziju okvira koja je usmjerena na prijetnje koje ciljaju mobilne uređaje, koji postaju sve češća meta napada zbog sveprisutnosti u modernim poslovnim okruženjima, te zbog činjenice da često sadrže osjetljive podatke. Ova inačica okvira pokriva različite taktike i tehnike koje napadači koriste u svrhu iskorištavanja mobilnih uređaja, kao što su zlonamjerne aplikacije, iskorištavanje ranjivosti operacijskog sustava i uporaba zlonamjernih profila. Cilj MITRE ATT&CK *for Mobile* je pomaganje organizacijama i pojedincima da adekvatno zaštite mobilne uređaje kroz bolje razumijevanje prijetnji specifičnih za mobilne platforme.

MITRE ATT&CK *for ICS* usmjeren je na prijetnje ICS sustavima koji upravljaju kritičnom infrastrukturom kao što su energetski sektor, proizvodnja, transport i druge industrije. ICS sustavi često su povezani s fizičkim procesima te su posebno osjetljivi na napade koji mogu izazvati fizičku štetu ili prekid u radu. Ovaj okvir pokriva specifične taktike i tehnike koje napadači koriste za kompromitiranje ICS sustava, kao što su manipulacija programibilnim logičkim kontrolerima (engl. *Programmable Logic Controllers,* PLC), iskorištavanje ICS specifičnih protokola i sabotiranje fizičkih kontrola. Cilj MITRE ATT&CK *for* ICS je pomoći operaterima kritične infrastrukture u identifikaciji i mitigaciji prijetnji koje ciljaju njihove specifične sustave.

MITRE ATT&CK *for Enterprise* je najpoznatija i najkorištenija verzija MITRE ATT&CK radnog okvira, posebno je prilagođena informacijskim sustavima koje koriste korporacije, vladine agencije i druge velike organizacije. Ovaj okvir pokriva široki spektar napadačkih scenarija, obuhvaćajući specifične tehnike koje ciljaju operativne sustave Windows, Linux i macOS kao i različite računalne programe i mrežne protokole. Njegova glavna svrha je asistencija kod prepoznavanja, detektiranja i odgovora na prijetnje koje ciljaju informacijsko-komunikacijsku infrastrukturu.

Jedna od ključnih prednosti MITRE ATT&CK *for Enterprise* okvira je njegova sposobnost poboljšanja vidljivosti unutar mreža i sustava. Okvir omogućava postavljanje detekcijskih

točaka na ključne mrežne lokacije koje napadačima često služe za provođenje početnih faza napada kao što su bočno kretanje ili prikupljanje vjerodajnica. Postavljanjem ovih točaka organizacije značajno poboljšavaju svoju sposobnost ranog otkrivanja prijetnji i brze reakcije u svrhu eradikacije napadača i suzbijanja daljnje kompromitacije sustava.

Dodatno, ovaj okvir omogućava integraciju s različitim TI izvorima o prijetnjama s ciljem obogaćivanja organizacijskih sigurnosnih sustava relevantnim informacijama o napadačima. Korištenjem obavještajnih podataka, sigurnosni timovi prepoznaju maliciozne kampanje, identificiraju taktike i tehnike specifične za određene prijetnje, te prilagođavaju svoje sigurnosne sustave za kvalitetniju zaštitu poslovnog okruženja. Na taj način ATT&CK *for Enterprise* poboljšava operativnu sigurnost i omogućava proaktivno planiranje i prilagodbu sigurnosnih strategija prema aktivnim ugrozama.

4.1.2. Cyber Kill Chain okvir

Cyber Kill Chain radni okvir razvila je organizacija Lockheed Martin te je predstavljen kao metodologija za razumijevanje kibernetičkih napada i poboljšanje sigurnosnih strategija. Okvir pruža strukturirani pristup analizi napada, raščlanjujući napad na sedam jasno definiranih faza. Svaka faza predstavlja specifičan korak u životnom ciklusu napada, od početnog istraživanja do konačnog postizanja cilja. Svrha *Cyber Kill Chain* okvira je omogućiti organizacijama prepoznavanje i razumijevanje faza napada s ciljem efikasnije identifikacije i onemogućavanja napada u ranim fazama.

Cyber Kill Chain služi kao vodič za integraciju proaktivnih sigurnosnih mjera i politika. Omogućuje sigurnosnim timovima da razviju strategije obrane koje ciljaju specifične faze napada radi lakšeg otkrivanja napadača i sprječavanja njihovog napredovanja kroz sustav. Uporaba ovog okvira organizacijama pomaže da bolje razumiju ponašanje napadača te da optimiziraju svoje sigurnosne sustave za zaštitu ključnih resursa.

Kako je spomenuto, okvir se sastoji od sedam faza kibernetičkog napada: izviđanje, naoružavanje, dostava, izvršenje, eksploatacija, instalacija, zapovijedanje i upravljanje te djelovanje prema ciljevima. Izviđanje je faza kibernetičkog napada kojom se prikupljaju informacije o mogućim ciljevima. Faza naoružavanja opisuje kreiranje zlonamjernih programa koji iskorištavaju ranjivosti targetiranih sustava. Dostava predstavlja segment napada gdje se kreirana maliciozna datoteka ili kod distribuira kritičnim točkama organizacije. Izvršavanje zlonamjernog koda je idući korak u životnom ciklusu napada, nakon kojeg slijedi faza eksploatacije gdje se pomoću dostavljenih zloćudnih entiteta iskorištavaju ranjivosti

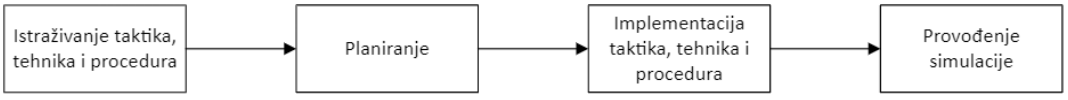
informacijsko-komunikacijskog sustava. Fazom instalacije opisuju se dodatne aktivnosti ubacivanja novih programa malicioznog koda s ciljem ostvarivanja postojanosti u sustavu. Zapovijedanje i kontrola segment je napada kod kojeg se uspostavlja komunikacija kompromitiranog sustava i samih napadača u svrhu njegove kontrole i izvršavanja definiranih malicioznih aktivnosti, te kao zadnja faza životnog ciklusa prema ovome okviru ističe se faza djelovanja prema ciljevima, odnosno provođenje aktivnosti u svrhu ostvarivanja zadanih ciljeva u kompromitiranoj infrastrukturi, [45].

Organizacije koriste ovaj okvir za evaluaciju svojih trenutnih sigurnosnih mjera i identifikaciju slabosti koje mogu biti iskorištene. Svaka faza okvira služi kao prilika za postavljanje detekcijskih točaka, primjenu sigurnosnih mjera i razvoj odgovarajućih procedura za odgovor na incidente. *Cyber Kill Chain* također pomaže organizacijama u obuci sigurnosnih timova, omogućavajući im bolje razumijevanje ponašanja napadača i potencijalnih ranjivosti unutar njihovog informacijskog sustava. Korištenje okvira kao dijela redovnih sigurnosnih vježbi pomaže organizacijama kod testiranja sposobnosti sigurnosnih sustava i poboljšaju svoje reakcije na stvarne ugroze.

4.2. Modeliranje napada

Modeliranje kibernetičkih napada jedna je od ključnih aktivnosti u provođenju modernih politika kibernetičke sigurnosti. Modeliranjem se stvaraju scenariji kibernetičkih napada koji vjerno oponašaju stvarne taktike, tehnike i procedure napadača. Korištenje ove tehnike organizacijama omogućuje proaktivno predviđanje potencijalnih napada, te im daje mogućnost pripreme za poduzimanje pravovremene reakcije i zaštite korporativnih informacijskih sustava, [42], [43].

Izrada modela napada uključuje detaljno istraživanje i analizu prijetnji, kroz koje se identificiraju relevantne taktike, tehnike i procedure. Životni ciklus modeliranja i simulacije kibernetičkih ugroza prikazan je idućom slikom. Stvaranjem realističnih scenarija napada, organizacije testiraju otpornost svojih sigurnosnih sustava i provjeravaju postojanost procedura odgovora na incidente. Provođenjem tako kreiranih testova u poslovnim okruženjima cilj je prepoznavanje i minimiziranje ranjivosti koje mogu biti iskorištene u stvarnim napadima.



Slika 2: Životni ciklus simuliranja kibernetičkih napada, [49]

Važnost modeliranja napada ogleda se u njegovoj sposobnosti poboljšavanja svih aspekata sigurnosti organizacije. Bolje razumijevanje prijetnji i identifikacija specifičnih ranjivosti omogućuju promptno korigiranje tih slabosti, smanjujući rizik od uspješnih napada. Redovitim simulacijama sigurnosni timovi stječu iskustvo i vještine potrebne za brzo prepoznavanje i odgovaranje na ugroze, što je važna karika kod minimiziranja štete i osiguravanja brzog oporavka od sigurnosnog incidenata.

4.2.1. Istraživanje taktika, tehnika i procedura

Istraživanje taktika, tehnika i procedura predstavlja ključnu fazu u procesu modeliranja kibernetičkih napada je organizacijama omogućuju bolje razumijevanje prijetnji s kojima se suočavaju. Ova faza modeliranja napada bitna je zbog toga što organizacije svrsishodno prepoznaju i analiziraju kibernetičke prijetnje koje su specifično vezane uz njihov djelokrug djelovanja. Cilj istraživanja taktika, tehnika i procedura je fokusiranje organizacije na prijetnje koje su najrelevantnije za poslovanje, industriju i tehnološku infrastrukturu u kojoj se nalaze. Takvim pristupom omogućuje se učinkovito usmjeravanje resursa u zaštitu od napadača koji predstavljaju najveću ugrozu poslovnoj infrastrukturi, [50].

Kako bi istraživanje bilo učinkovito, ono mora pratiti ciljeve organizacije i njezinu specifičnu sigurnosnu arhitekturu. Svrsishodno istraživanje zahtijeva opsežno poznavanje relevantnih kibernetičkih prijetnji, ali i usklađivanje s operativnim potrebama i strategijama organizacije. Organizacije moraju razumjeti koji su najvjerojatniji napadači koji ciljaju njihove poslovne procese te koje taktike mogli primijeniti. Ova faza nije samo tehnička analiza prijetnji, već uključuje i strateško razmatranje mogućih napadača i njihove metode napada, [51].

Za kvalitetnu istragu i identifikaciju relevantnih tehnika, ključno je prikupiti interne i eksterne informacije. Interne informacije uključuju podatke o prijašnjim sigurnosnim incidentima, ranjivostima u sustavu i zabrinutostima specifičnim za organizaciju. Ove informacije pomažu u razumijevanju gdje se organizacija nalazi na spektru sigurnosnog rizika i koje slabosti se najčešće mogu iskoristiti u budućim napadima. Eksterne informacije, poput obavještajnih izvještaja predstavljaju jednako važne izvore informacija, one uključuju izvještaje analitičara iz industrije, javno dostupne izvore te vijesti o nedavnim napadima. Ovi izvori pružaju detaljne uvide u taktike i metode koje su napadači nedavno koristili s ciljem pružanja mogućnosti organizacijama da anticipiraju buduće prijetnje, [52].

4.2.2. Odabir malicioznog aktera i taktika, tehnika i procedura

Odabir malicioznog aktera i odgovarajućih taktika, tehnika i procedura predstavlja važnu fazu u procesu modeliranja kibernetičkih prijetnji. Ova faza temelji se na nekoliko ključnih načela koja osiguravaju relevantnost, realističnost i izvedivost simulacije. Prilikom odabira malicioznih aktera i njihovih karakteristika, organizacije moraju pratiti principe relevantnosti, dostupnosti obavještajnih podataka, kompleksnosti tehnika i dostupnosti resursa.

Prvo načelo koje se primjenjuje u procesu odabira je relevantnost. Odabir malicioznog aktera mora biti u skladu s ciljevima organizacije i industrijom u kojoj se nalazi. Na primjer, organizacije u financijskom sektoru možda će biti više izložene napadima ciljanima na krađu financijskih podataka ili pristup poslovnim aplikacijama, dok će tehnološke tvrtke biti osjetljive na napade s ciljem krađe intelektualnog vlasništva. Odabir malicioznih aktera koji su već poznati po napadima na slične organizacije omogućuje simulaciju stvarnih prijetnji i testiranje otpornosti na relevantne scenarije, [51].

Drugo važno načelo je dostupnost obavještajnih podataka o malicioznim akterima. Postojanost analitičkih izvještaja, relevantnih povijesnih podataka organizacijama daje uvid u načine provođenja napada i općenito ponašanje određenih napadačkih skupina. Korištenje relevantnih izvora informacija u kontekstu modeliranja kibernetičkih napada svim dionicima simulacije omogućuje kreiranje pouzdanih imitacija stvarnih tehnika napadača.

Kompleksnost taktika, tehnika i procedura od velikog je značaja u procesu odabira malicioznog aktera čiji će se napadi simulirati. Neki napadači koriste dobro poznate alate crvenih timova, poput *Metasploit* ili *Cobalt Strike* platformi, dok složeniji napadi mogu zahtijevati razvoj prilagođenih alata koji repliciraju specifične tehnike napadača. Kod taktika koje zahtijevaju nestandardne alate, organizacija mora procijeniti isplativost njihove implementacije. Kompleksnost također utječe na vremenski okvir simulacije, gdje složeniji napadi zahtijevaju više vremena za pripremu i izvedbu što otežava njihovu realizaciju u kratkim vremenskim rokovima koji su sve češća pojava u svijetu kibernetičke sigurnosti, [44].

4.2.3. Kreiranje nacrta tehnika, taktika i procedura

Kreiranje nacrta tehnika, taktika i procedura predstavlja korak koji uključuje izradu dokumentacije koja detaljno definira sve entitete koji će biti simulirani, zajedno s referencama na relevantne izvore obavještajnih podataka o prijetnjama. Svaka tehnika mora biti jasno opisana s preciznim referencama iz obavještajnih ili industrijskih izvještaja u svrhu osiguravanja realističnosti simulacije i vjerodostojnosti korištenih podataka.

Dokumentacija služi kao operativni vodič za implementaciju odabranih taktika. Njezina svrha je omogućiti sigurnosnim timovima detaljan uvid u sve segmente simulacije, uključujući tehničke specifikacije korištenih tehnika te potrebne alate i postupke za njihovo izvođenje. Izrađenom dokumentacijom osigurava se dosljednost tijekom simulacije, omogućujući timovima da prate unaprijed definirane korake i time izbjegnu odstupanja od plana. Također, dokumentacija sadrži pravila angažmana koja definiraju ograničenja i smjernice za provođenje simulacije. Pravila angažmana osiguravaju da se simulacija odvija u kontroliranim uvjetima bez prekoračenja dogovorenih granica ili ugrožavanja operativnih sustava organizacije. Ova pravila uključuju: opseg simulacije, vremenski okvir te dozvole za provođenje napada unutar organizacije.

4.2.4. Planiranje simulacije

Planiranje simulacije kibernetičkih napada ključno je kako bi se osigurala jasna i uspješna provedba simulacije. Ova faza uključuje definiranje ključnih komponenti simulacije, kao što su ciljevi, opseg simulacije, vremenski okvir, pravila angažmana, potrebna odobrenja te komunikacijski plan. Svrha ove faze je uspostaviti detaljan plan koji omogućuje sigurno i kontrolirano provođenje simulacije, uz jasno definirane granice i ciljeve.

Ciljevi simulacije definiraju specifične ishode koje organizacija želi postići kroz simulaciju, uključujući testiranje određenih sigurnosnih sustava, identifikaciju ranjivosti ili poboljšanje procesa odgovora na incidente. Opseg simulacije određuje koji dijelovi infrastrukture će biti uključeni u simulaciju, kao i koji će sustavi biti izvan opsega. Na ovaj način osigurava se da simulacija ne utječe na kritične poslovne procese koji nisu dio scenarija napada. Opseg simulacije treba precizno definirati kako bi svi sudionici razumjeli kontekst simulacije i infrastrukturne elemente koji su uključeni.

Vremenski okvir simulacije mora biti unaprijed određen kako bi se simulacija mogla jasno razlikovati od stvarnih poslovnih aktivnosti. Definiranje vremena za provođenje simulacije ključno je kako bi se izbjegli operativni problemi ili neplanirani prekidi u radu kritičnih sustava. Također je potrebno odrediti razdoblja kada je simulacija zabranjena s ciljem minimiziranja mogućih smetnji.

Pravila testiranja definiraju koje će se tehnike, taktike i procedure koristiti tijekom simulacije te koje su ovlasti i ograničenja timova uključenih u simulaciju. Također, pravila testiranja moraju uključivati mjere oporavka za rizične taktike kako bi se izbjegli potencijalni incidenti ili neplanirane posljedice simulacije. To uključuje jasno definirane korake za upravljanje

rizicima koji proizlaze iz simuliranih napada, kao i ograničenja za korištenje određenih tehnika koje bi destruktivno djelovale na poslovne sustave.

Odobrenja za rad predstavljaju eksplicitno pisano odobrenje za provođenje simulacije i davanje ovlasti timovima uključenim u testiranje. Pisano odobrenje ključno je za pravnu i operativnu odgovornost s ciljem osiguravanja da svi sudionici i menadžment organizacije razumiju rizike i svrhu simulacije, te da su sve strane suglasne s njezinim provođenjem.

Komunikacijska matrica definira način komunikacije tijekom provođenja simulacije. Uključuje informacije kao što su: učestalost razmjene informacija, definiranje sudionika koji je zadužen za kolaboraciju između različitih timova, te procedure odgovora na incidente koji se pojavljuju tijekom simulacije. Cilj je osigurati jasne kanale komunikacije kako bi se omogućila učinkovitija koordinacija i brži odgovor na sve neočekivane događaje tijekom provođenja simulacije.

4.2.5. Implementacija taktika, tehnika i procedura

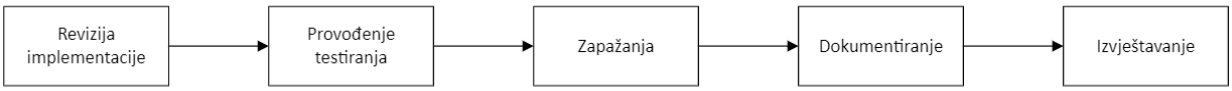
Implementacija se može definirati kao procedura za izvršenje jedne ili više tehnika i taktika koje su prethodno odabrane tijekom faze planiranja. Ona uključuje sve potrebne tehničke i resursne segmente za uspješnu realizaciju napada. To podrazumijeva korištenje odgovarajućih alata, skripti, binarnih datoteka i drugih resursa koji su potrebni za implementaciju.

Implementacija taktika također uključuje odabir i korištenje specifičnih alata i tehnika koje omogućuju simulaciju napada. Ovisno o vrsti napada koji se simulira, mogu se koristiti komercijalni ili alati otvorenog koda za penetracijsko testiranje, skriptiranje i upravljanje napadačkim kampanjama. Platforme poput *Metasploit* i *Cobalt Strike* često se koriste za simulaciju složenijih napada, dok se manje sofisticirani napadi mogu simulirati jednostavnim skriptama ili korištenjem predefiniranih binarnih datoteka. Svaki alat i tehnika trebaju biti pažljivo odabrani kako bi se osigurala realističnost napada, te s ciljem maksimiziranja relevantnosti rezultata simulacije.

Implementacijska faza predstavlja operativnu proceduru koja opisuje kako se napad provodi pomoću specifičnih alata i tehnika. Tijekom ove faze sigurnosni timovi pažljivo prate izvedbu svake taktike, procjenjujući učinkovitost sigurnosnih sustava i identificirajući slabosti u sustavima. Kroz dosljednu implementaciju organizacije utvrđuju kako njihovi sustavi reagiraju na stvarne prijetnje te daju prijedloge za poboljšanje sigurnosnih mehanizma na temelju rezultata simulacije.

4.2.6. Provođenje simulacije

Provođenje simulacije kibernetičkih napada složen je proces koji uključuje metodično i profesionalno izvršavanje unaprijed definiranih taktika, tehnika i procedura kako bi se testirala otpornost sigurnosnih sustava organizacije. Ovaj proces zahtijeva pažljivu pripremu i temeljito praćenje svih aktivnosti kako bi se osigurala uspješna provedba simulacije i postigli ciljevi definirani u fazi planiranja.



Slika 3: Proces provođenja simulacije

Proces provođenja simulacije podijeljen je u pet ključnih faza prikazanih gornjom slikom:

- Revizija implementacije: Ova faza uključuje reviziju i provjeru svih relevantnih stavki iz kreiranog plana simulacije, što obuhvaća pregled zaduženja dionika, tehničku pripremu alata i taktika te evaluaciju potencijalnog utjecaja na sustav. Prije samog pokretanja testiranja, tim mora biti siguran da su svi resursi i sustavi spremni za testiranje, a svi dionici obaviješteni o svojim zaduženjima i ulogama.
- Provođenje testiranja: Podrazumijeva izvođenje odabranih taktika, ali s dodatnom pažnjom na poštivanje opsega simulacije i pravila angažmana. Timovi u ovoj fazi provjeravaju je li su sve aktivnosti unutar definiranih granica te da simulacija ne narušava stvarne poslovne aktivnosti ili kritične sustave.
- Zapažanja: Tijekom simulacije važno je zabilježiti zapažanja o tome kako sustavi reagiraju na simulirane napade, bilješke uključuju informacije o tome je li određeni test bio uspješan ili blokiran, je li detektiran od strane sigurnosnih sustava ili je izvršen neprimijećeno. Također bilježe se moguće greške sustava, korisničke pogreške ili preventivne mjere koje su uspješno zaustavile napad. Faza zapažanja ključna je za procjenu učinkovitosti sigurnosnih mjera organizacije.
- Dokumentiranje: Dokumentacija pruža empirijske dokaze o tome kako su sustavi reagirali na simulirane napade i koliko su učinkovite postojeće sigurnosne mjere. Ovaj proces uključuje prikupljanje podataka o svakom provedenom testu, uz bilježenje rezultata i svih dodatnih informacija koje mogu biti važne za naknadnu analizu i evaluaciju.
- Izvještavanje: Nakon provođenja simulacije, tim zadužen za simulaciju napada obavještava dionike o provedenim akcijama i zapažanjima. Ova faza uključuje izradu

sažetog izvještaja koji detaljno opisuje sve segmente simulacije, provedene testove, zapažanja tijekom simulacije te rezultate testiranja. Cilj izvještavanja je pružiti dionicima jasne informacije koje im omogućuju donošenje informiranih odluka o poboljšanju sigurnosnih mjera i procedura organizacije.

4.3. Pregled alata za simuliranje kibernetičkih napada

Platforme za simulaciju napada imaju ključnu ulogu u definiranju sigurnosnih politika organizacije, osobito kada je riječ o testiranju i evaluaciji sigurnosnih rješenja kao što su EDR sustavi. Svrha ovih platformi je omogućiti organizacijama da u kontroliranim uvjetima simuliraju stvarne kibernetičke napade korištenjem poznatih napadačkih taktika, tehnika i procedura. Korištenje platformi postalo je neophodno zbog sve sofisticiranijih prijetnji s kojima se organizacije suočavaju. Sigurnosni timovi kroz simulaciju testiraju stvarne prijetnje, čime dobivaju uvid u brzinu i učinkovitost korištenih EDR rješenja kod prepoznavanja i neutraliziranja napada.

Najčešće korišteni alati za simuliranje kibernetičkih prijetnji su: MITRE *Caldera, Cobalt Strike, Atomic Red Team, Metasploit, Core Impact, AttackIQ.*

4.3.1. MITRE Caldera

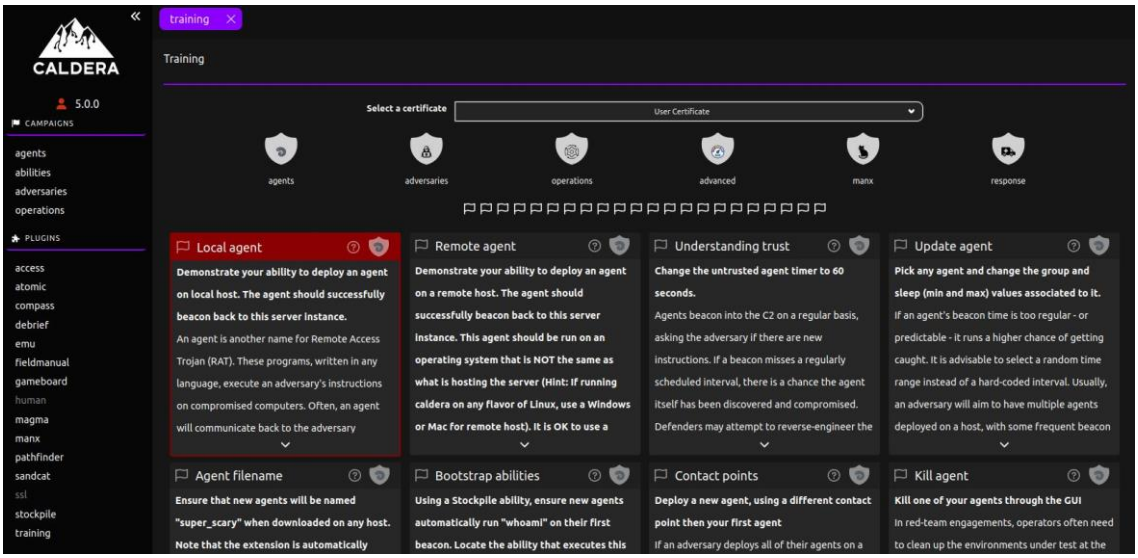
MITRE *Caldera* je napredan alat za simulaciju napadača koji se koristi u domeni informacijske sigurnosti, s posebnim fokusom na aktivnosti crvenog tima, testiranje otpornosti sustava i automatizaciju sigurnosnih ugroza. Razvijen od strane istraživačkog instituta MITRE, *Caldera* omogućuje timovima za sigurnost da automatiziraju napade koji simuliraju stvarne tehnike napadača kako bi procijenili sigurnost sustava.

MITRE *Caldera* koristi programske dodatke, odnosno proširenja koja omogućuju prilagođavanje i širenje funkcionalnosti prema specifičnim potrebama plana simulacije. Alat koristi arhitekturu temeljenu na agentima koja omogućuje izvođenje napada na udaljene sustave, svaki agent postavljen u ciljanom sustavu može izvršavati skripte koje oponašaju napadačke tehnike koje su mu instruirane kroz komunikaciju s centralnim poslužiteljem, [53].

Osnovne komponente MITRE *Caldera* sustava uključuju, [53]:

- Centralni poslužitelj: Koordinira napade i upravlja agentima. Također služi za definiranje kampanja, strategija napada, te za praćenje rezultata simulacija.

- Agenti: Programski kod koji se instalira na ciljne radne stanice kako bi simulirao napadačke tehnike. Agenti mogu izvršavati naredbe te pružati povratne informacije o uspjehu ili neuspjehu napada.
- GUI i API: Grafičko korisničko sučelje koje olakšava korisnicima upravljanje operacijama, kao i API za integraciju s drugim sigurnosnim alatima. Izgled grafičkog sučelja prikazan je idućom slikom.



Slika 4: Izgled grafičkog sučelja i prikaz funkcionalnosti MITRE Cladera platforme

Jedna od ključnih funkcionalnosti platforme je mogućnost pokretanja unaprijed definiranih ili prilagođenih scenarija napada. Upotrebom umjetne inteligencije omogućuje se automatizacija provođenja napada, na način da sustav prepoznaje i odabire različite napadačke metode i dinamiku napada u ovisnosti o rezultatima izvršavanja prijašnjih koraka napada. Ovakvim načinom rada, platforma organizacijama omogućava provođenje složenih napada bez potrebe za interakcijom s krajnjim korisnikom.

MITRE *Caldera* je često korišteni alat u korporativnom okruženju zbog svoje dostupnosti, odnosno zbog toga što se radi o alatu otvorenog koda s velikom zajednicom razvojnih programera i korisnika koji pružaju podršku i razvijaju nove funkcionalnosti. Također alat svoje prednosti manifestira kroz jednostavnu i sigurnu automatizaciju procesa, modularnu arhitekturu te integraciju s MITRE ATT&CK radnim okvirom. S druge strane, nedostaci *Caldera* platforme su zahtjevno korištenje naprednih mogućnosti zbog ograničene tehničke dokumentacije, te limitiranost agenata, koji su većinom izrađeni s podrškom za Windows poslovna okruženja.

4.3.2. Cobalt Strike

Cobalt Strike je komercijalni alat razvijen za crvene timove, simulaciju napada i procjenu sigurnosti informacijskih sustava. Korišten je od strane sigurnosnih stručnjaka, a sve češće postaje alat zlonamjernih aktera zbog svoje mogućnosti preciznog oponašanja tehnika stvarnih napadača.

Glavna svrha alata je pružanje platforme za izvođenje operacija s punom integracijom faza napada, od inicijalnog pristupa u mrežu do održavanja prisutnosti i eksfiltracije podataka. Najčešća upotreba je u vježbama crvenog tima gdje napadačke tehnike postaju ključni alat za razumijevanje stvarnih aktivnosti napadača i kako se zaštititi od njih, [54].

Cobalt Strike nudi širok spektar funkcionalnosti kroz nekoliko ključnih komponenti:

- *Beacon*: Najvažnija funkcionalnost koja se definira kao programski kod koji napadač ugrađuje u ciljanu mrežu ili sustav. *Beacon* omogućuje zlonamjernim akterima ili sigurnosnim stručnjacima da neometano komuniciraju s kompromitiranim sustavima, izvršavajući naredbe, eskalirajući privilegije i prikupljajući podatke. Agent podržava različite načine komunikacije, uključujući HTTP, HTTPS, DNS i SMB protokole, što mu omogućava izbjegavanje detekcije od strane sigurnosnih alata.
- Napredne tehnike eskalacije privilegija i bočno kretanje: *Cobalt Strike* nudi podršku za izvođenje bočnog kretanja unutar mreže, što omogućuje napadačima širenje pristupa s jednog sustava na druge unutar mreže.
- Alati socijalnog inženjeringa: Alat također uključuje module za socijalni inženjering, koji omogućuju kreiranje prilagođenih kampanja, iskorištavanje lažnih web stranica i manipulaciju korisnicima kako bi otkrili osjetljive podatke ili omogućili pristup sustavima.
- Alati za omogućavanje perzistentnosti: Nakon što je sustav kompromitiran, *Cobalt Strike* omogućuje niz aktivnosti koje uključuju skrivanje prisutnosti unutar sustava, prikupljanje osjetljivih podataka te umetanje stražnjih vrata kako bi napadači mogli ponovno pristupiti sustavu u kasnijim fazama napada.

Cobalt Strike koristi arhitekturu temeljenu na agentima, s *Beacon* agentom kao glavnim komunikacijskim alatom. Komunikacija između *Beacon* agenata i napadača modulira se s ciljem smanjenja mogućnosti detekcije napada. Alat također nudi mogućnost stvaranja prilagođenih modula za proširenje funkcionalnosti, što ga čini vrlo fleksibilnim alatom za

simulacije. Korištenjem skriptnih jezika napredni korisnici mogu automatizirati operacije i prilagoditi alat prema specifičnim scenarijima napada.

4.3.3. Atomic Red Team

Atomic Red Team (*ART*) je sigurnosna platforma otvorenog koda koja omogućava sigurnosnim timovima testiranje sigurnosnih kontrola svojih sustava simuliranjem stvarnih napadačkih tehnika. Alat je razvijen od strane tvrtke *Red Canary* i temelji se na MITRE ATT&CK okviru, dajući organizacijama strukturiran i lako prilagodljiv pristup za evaluaciju obrambenih sposobnosti kroz predefinirane testove za pojedinačne napadačke tehnike.

ART je dizajniran kako bi omogućio brzo i jednostavno provođenje testova sigurnosnih kontrola bez potrebe za kompleksnom konfiguracijom ili dubokim tehničkim znanjem. Primarni cilj ove platforme je omogućiti sigurnosnim timovima provođenje testiranja sigurnosnih mjera protiv širokog spektra stvarnih prijetnji. *Atomic Red Team* korisnicima pruža testove koji repliciraju napadačke tehnike, što omogućuje procjenu kako postojeći sigurnosni sustavi i alati reagiraju na specifične napade.

Ključne značajke *Atomic Red Team*-a uključuju, [55]:

- Brza implementacija testova: ART testovi jednostavnog su dizajna te su spremni za laku i brzu primjenu.
- Lakoća korištenja: *Atomic Red Team* koristi jednostavne skripte i alate koji su kompatibilni s različitim operacijskim sustavima.
- Modularnost i prilagodljivost: Svaki ART test može se prilagoditi specifičnim potrebama organizacije, a korisnici mogu kombinirati različite testove kako bi stvorili složenije scenarije.
- Integracija s MITRE ATT&CK okvirom: Svaki test je mapiran prema ATT&CK tehnikama, omogućujući korisnicima da precizno testiraju određene napadačke metode i identificiraju slabosti u svojim sigurnosnim mjerama.

Svaki ART test sastoji se od testnih skripti, unaprijed definiranih parametara i dokumentacije. Testne skripte sadrže naredbe pomoću kojih se simuliraju određene napadačke tehnike, pomoću unaprijed definiranih parametara omogućuje se provođenje napada uz minimalne dodatne konfiguracije sustava, dok dostupna dokumentacija korisnicima opisuje na koji način provesti simulaciju, [56].

4.3.4. Metasploit

Metasploit predstavlja sveobuhvatnu platformu za penetracijsko testiranje, osmišljenu za identifikaciju i eksploataciju ranjivosti u informacijskim sustavima. Primarno se koristi za simulaciju stvarnih napada s ciljem evaluacije sigurnosnih kontrola i procjene otpornosti sustava. Alat omogućuje korisnicima reproduciranje cijelog napadačkog ciklusa, od inicijalne identifikacije ranjivosti, preko iskorištavanja tih slabosti, do post eksploatacijskih aktivnosti unutar kompromitiranog sustava.

Metasploit se temelji na modularnoj arhitekturi, što omogućuje njegovu prilagodbu različitim scenarijima i vrstama napada. Ova platforma nudi širok raspon funkcionalnosti, uključujući eksploataciju poznatih ranjivosti, post eksploatacijske operacije, analizu mreže i prilagodbu napadačkih modula, čime se omogućuje detaljna i ciljana procjena sigurnosne infrastrukture.

Neke od ključnih funkcionalnosti *Metasploit* platforme su, [44]:

- Eksploatacija ranjivosti: Korištenjem unaprijed definiranih modula, *Metasploit* omogućuje korisnicima iskorištavanje specifičnih ranjivosti na ciljanom sustavu.
- Modularna arhitektura: *Metasploit* se temelji na modularnom sustavu koji korisnicima omogućuje jednostavno kombiniranje različitih modula za prilagodbu specifičnim scenarijima napada.
- Post eksploatacija: Nakon uspješnog iskorištavanja slabosti, platforma nudi niz post eksploatacijskih modula koji omogućuju daljnje aktivnosti na kompromitiranom sustavu.
- Integracija s drugim alatima: *Metasploit* se može integrirati s alatima kao što su *Nmap* i *Nessus*, omogućujući automatizirano otkrivanje i iskorištavanje ranjivosti.

Metasploit je razvijen s modularnom arhitekturom, što znači da se sastoji od različitih modula koji obuhvaćaju sve faze napada. Ti moduli omogućuju visok stupanj prilagodljivosti i fleksibilnosti, a među ključnim modulima su, [57]:

- Moduli ranjivosti: Moduli za iskorištavanje ranjivosti omogućuju korisnicima iskorištavanje poznatih ranjivosti u ciljnim sustavima. Kreirane ranjivosti mogu biti usmjerene na slabosti u operacijskim sustavima, aplikacijama ili mrežnim protokolima.
- Moduli malicioznog tereta: Teret je komponenta koja se izvršava nakon uspješne eksploatacije i omogućuje daljnje djelovanje unutar kompromitiranog sustava.

- Pomoćni moduli: Ovi moduli se koriste za podršku tijekom faza otkrivanja i prikupljanja informacija. Pomoćni moduli mogu se koristiti za skeniranje portova, napade rječnikom na autentifikacijske mehanizme ili otkrivanje ranjivih servisa.
- Kriptografski moduli: Enkripcijski moduli omogućuju šifriranje malicioznog tereta s ciljem izbjegavanja detekcije od strane sustava za zaštitu.
- Post eksploatacijski moduli: Nakon što je sustav kompromitiran, ovi moduli omogućuju napredne aktivnosti poput prikupljanja zaporki, eskalacije privilegija i analize mreže.

4.3.5. Core Impact

Core Impact je komercijalna platforma za penetracijsko testiranje koja omogućava stručnjacima za sigurnost provođenje sveobuhvatnih procjena ranjivosti i simulacija stvarnih napada. Cilj alata je pomoći organizacijama u procjeni otpornosti infrastrukture na različite vrste prijetnji, od napada na mreže i aplikacije do testiranja krajnjih točaka. Primjenom ove platforme omogućuje se precizna procjena učinkovitosti sigurnosnih kontrola i pomaže se u identificiranju kritičnih ranjivosti koje bi mogle biti iskorištene u stvarnim napadima.

Core Impact ističe se mogućnošću integriranja različitih faza napada u jednu cjelovitu platformu, od otkrivanja ranjivosti do post eksploatacijskih aktivnosti. Njegova modularna struktura omogućuje korisnicima prilagodbu testova specifičnim potrebama, a automatizirane funkcionalnosti čine ga pristupačnim čak i za timove s ograničenim resursima.

Ključne funkcionalnosti *Core Impact* platforme uključuju, [58]:

- Iskorištavanje ranjivosti: Platforma nudi brojne module za eksploataciju poznatih ranjivosti u operacijskim sustavima, aplikacijama i mrežama.
- Post eksploatacijske aktivnosti: Nakon uspješne kompromitacije, *Core Impact* omogućuje daljnje aktivnosti kao što su eskalacija prava, bočno kretanje unutar mreže i prikupljanje podataka.
- Testiranje aplikacija i krajnjih točaka: Platforma daje mogućnost ciljanih testova usmjerenih na web aplikacije, mobilne aplikacije i krajnje točke, omogućujući time detaljnu procjenu sigurnosnih mehanizama.

Core Impact je izgrađen na modularnoj arhitekturi, s jasno definiranim fazama napada. Svaka faza omogućuje korištenje specifičnih modula za otkrivanje i iskorištavanje ranjivosti, prilagodljivih potrebama organizacije. Osim eksploatacije, alat nudi širok raspon post

eksploatacijskih mogućnosti, kao i značajke koje omogućuju eskalaciju napada kroz lateralno kretanje u mreži.

4.3.6. AttackIQ

AttackIQ je platforma za procjenu kibernetičke otpornosti koja omogućuje organizacijama simulaciju stvarnih napada i testiranje učinkovitosti njihovih sigurnosnih kontrola. Ovaj alat koristi se za kontinuirano testiranje i validaciju sigurnosnih mjera kako bi se identificirale ranjivosti te poboljšao odgovor na ugroze. *AttackIQ* se temelji na konceptu kontinuiranog simuliranja naprednih kibernetičkih prijetnji (engl. *Breach and Attack Simulation*, BAS), koji omogućuje sigurnosnim timovima da u kontroliranim uvjetima provode simulacije napada i procjenjuju kako bi postojeći obrambeni mehanizmi reagirali u stvarnim scenarijima, [59].

AttackIQ platforma pruža širok raspon funkcionalnosti koje olakšavaju simulaciju napada kroz korištenje unaprijed definiranih napadačkih tehnika i taktika utemeljenih na MITRE ATT&CK okviru. Alat je dizajniran kako bi organizacijama omogućio stvaranje realnih simulacija napada te kontinuirano testiranje sigurnosnih mjera, čime se smanjuje rizik od kompromitacije sustava.

Ključne funkcionalnosti *AttackIQ* platforme uključuju, [60]:

- Simulacija napada: Platforma omogućuje oponašanje stvarnih napadačkih tehnika kroz korištenje unaprijed definiranih scenarija koji pokrivaju različite faze napada, uključujući inicijalni upad, eskalaciju privilegija i eksfiltraciju podataka.
- Kontinuirano testiranje: *AttackIQ* omogućuje sigurnosnim timovima da redovito provode simulacije napada i testiraju učinkovitost sigurnosnih kontrola u stvarnom vremenu, čime se osigurava stalna provjera sustava.
- Usklađenost s MITRE ATT&CK okvirom: *AttackIQ* koristi standardizirane napadačke tehnike iz MITRE ATT&CK okvira, omogućujući ciljana testiranja specifičnih ugroza koje odgovaraju stvarnim scenarijima napada.
- Automatizacija napada: Automatizirane značajke platforme olakšavaju planiranje i provođenje testova bez potrebe za ručnim upravljanjem svakom fazom napada.

AttackIQ je izgrađen na modularnoj arhitekturi, omogućujući korisnicima da biraju i prilagođavaju scenarije napada prema svojim specifičnim potrebama. Platforma koristi različite agente koji omogućuju simulaciju napada na više slojeva mreže, uključujući krajnje točke, mrežnu infrastrukturu i aplikacije. Svaki agent prikuplja podatke o učinku napada, čime omogućuje detaljnu analizu sigurnosnih sustav.

4.4. Provođenje simulacije kibernetičkih napada

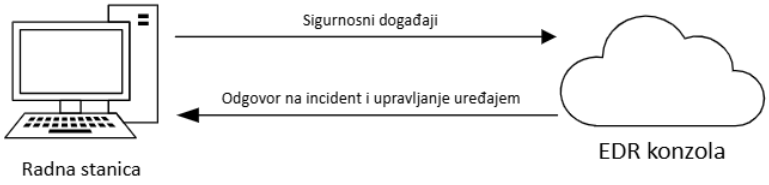
Kao dio praktičnog dijela ovog rada, simulacija kibernetičkih napada provedena je u svrhu evaluacije učinkovitosti različitih EDR sustava u detekciji i odgovoru na specifične tehnike poznatog APT malicioznog aktera *Turla*. Odabrani APT poznat je po provođenju sofisticiranih napada usmjerenih na kretanje kroz mreže, prikupljanje osjetljivih informacija i eksfiltraciju podataka. Za potrebe ove simulacije, korišten je pristup modeliranja napada temeljen na tehnikama, taktikama i procedurama MITRE ATT&CK okvira, koji pruža strukturiran uvid u metode napada koje su karakteristične za ovu grupu.

Cilj simulacije je reproducirati što vjernije scenarije napada koje APT koristi u stvarnim uvjetima. Korištenjem alata *Atomic Red Team* odabrano je jedanaest predefiniranih testova koji reflektiraju najčešće korištene tehnike, ali ne repliciraju najvjernije stvarno korištene taktike, zbog ograničenja same platforme.

4.4.1. Infrastrukturna okolina simuliranih napada

Simulacija kibernetičkih napada provedena je u izoliranom okruženju koji se sastojao od jedne Windows 10 radne stanice ,jednog EDR rješenja u svakom testnom ciklusu te preinstaliranih *Atomic Red Team* testova. Ciljni sustav bio je Windows 10 Pro, verzija 22H2 (OS Build 19045.4780) koji je služio kao glavna platforma za simulaciju napada i evaluaciju učinkovitosti pojedinih EDR rješenja.

Svaka simulacija provedena je na način da se na Windows 10 radnoj stanici nalazio instalirani EDR agent jednog od testiranih proizvođača, dok se nadzor, administracija i analitika odvijala kroz konzolu u oblaku EDR rješenja. Konzole u oblaku omogućile su praćenje naprednih detekcija, analizu incidenata i odgovore na sigurnosne prijetnje u stvarnom vremenu, uključujući korelaciju događaja i izvještavanje o aktivnostima napada. Idućom slikom prikazana je arhitektura simulacijskog okruženja te način komunikacije između EDR agenta instaliranog na radnoj stanici i EDR konzole.

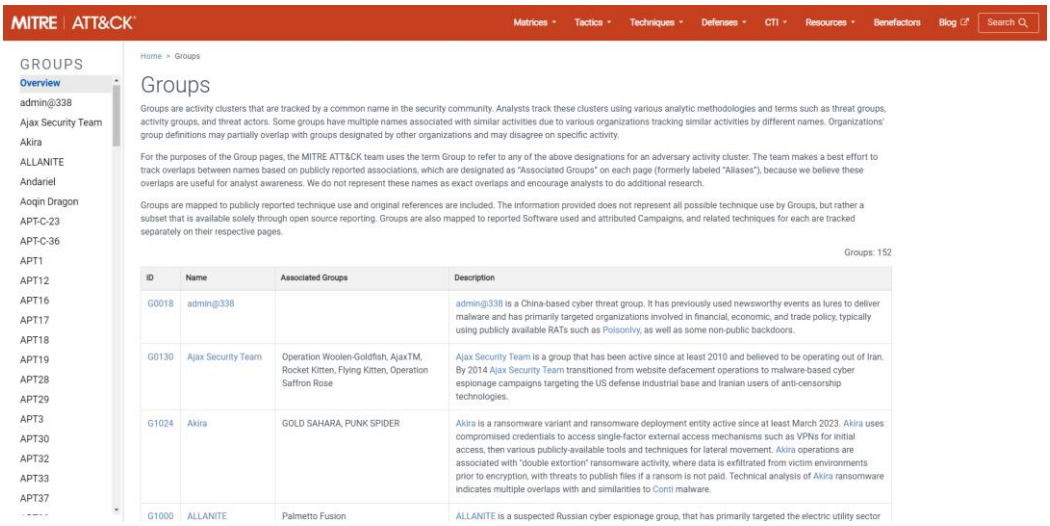


Slika 5: Arhitektura simulacijskog okruženja

Ovim radom evaluirati će se iduća EDR rješenja: Palo Alto Networks Cortex XDR, Microsoft Defender for Endpoint, Bitdefender GravityZone, Trend Micro Apex One, WithSecure Elements EDR.

4.4.2. Odabir APT grupe

Proces evaluacije EDR rješenja započeo je odabirom malicioznog aktera koji predstavlja značajnu prijetnju za sektore poput vladinih institucija, kritične infrastrukture i financijskih organizacija. Kako bi se identificirala najrelevantnija prijetnja, korištena je baza podataka MITRE ATT&CK koja sadrži popis poznatih APT grupa i njihovih ciljeva. Idućom slikom prikazana je navedena ATT&CK baza znanja o APT grupama.



Slika 6: Prikaz MITRE ATT&CK podataka o APT grupama, [61]

Prilikom pretraživanja baze, APT grupa *Turla* istaknula se kao relevantna grupa za provođenje analize. *Turla* je poznata po napadima na Vlade, sigurnosne agencije i ključnu infrastrukturu, s posebnim fokusom na napade u Europi i Sjevernoj Americi. S obzirom na njezin kontinuirani fokus na ove kritične sektore, *Turla* je odabrana kao maliciozni akter za procjenu EDR sustava u ovoj studiji, zbog svoje sposobnosti dugotrajnog infiltriranja u sustave te korištenja sofisticiranih tehnika za izbjegavanje detekcije i eksfiltraciju osjetljivih podataka.

4.4.3. Istraživanje i odabir relevantnih taktika

Prilikom odabira taktika, tehnika i procedura za simulaciju napada, ključno je da odabrane tehnike odgovaraju stvarnim napadačkim metodologijama koje koristi odabrani maliciozni akter. U ovom slučaju, proces odabira temelji se na analizama obavještajnih podataka i podacima iz MITRE ATT&CK baze znanja, koja pruža sveobuhvatan pregled metoda koje

koristi APT *Turla*. Cilj je pokriti cijeli lanac napada, od inicijalnog pristupa do eksfiltracije podataka, kako bi se osigurala potpuna evaluacija EDR sustava.

Za odabir taktika korištena su dva ključna kriterija:

- Relevantnost tehnika: Odabir tehnika koje su specifične za grupu *Turla*, a koje su identificirane kroz MITRE ATT&CK *Navigator*. Time se osigurava da simulacija napada bude realistična i da reflektira stvarne prijetnje.
- Dostupnost testova: Tehnike su odabrane na temelju dostupnosti testova u okviru alata Atomic Red Team.

Odabrane tehnike pružaju uvid u različite aspekte napada, poput kompromitacije računalnih sustava, lateralnog kretanja kroz mrežu, eskalacije privilegija i krađe osjetljivih informacija. Pritom, svaka tehnika odabrana je kako bi testirala određene komponente EDR sustava, kao što su detekcija malicioznih skripti, otkrivanje bočnog kretanja unutar mreže i praćenje eksfiltracije podataka. Idućom tablicom prikazane su osnovne specifikacije odabranih taktika.

Tablica 2: Prikaz odabranih taktika

Taktika	MITRE ATT&CK ID	Tehnika
Inicijalni pristup	T1566.001	Spearphishing Attachment
Izvršenje	T1059.001	Command and Scripting Interpreter: PowerShell
Perzistentnost	T1547.001	Boot or Logon Autostart Execution: Registry Run Keys
Eskalacija privilegija	T1110	Brute Force
Izbjegavanje obrane	T1562.001	Impair Defenses: Disable or Modify Tools
Prikupljanje vjerodajnica	T1555.004	Credentials from Password Stores: Windows Credential Manager
Otkrivanje	T1083	File and Directory Discovery
Bočno kretanje	T1021.002	Remote Services: SMB/Windows Admin Shares
Pripupljanje	T1005	Data from Local System
Zapovijedanje i upravljanje	T1071.001	Application Layer Protocol: Web Protocols
Eksfiltracija	T1567.002	Exfiltration Over Web Service

4.4.4. Opis i implementacija taktika

Simulacija kibernetičkih napada temelji se na preciznom opisu i implementaciji odabranih taktika, tehnika i procedura, koje reflektiraju stvarne napadačke metode. Cilj ovog segmenta rada je pružiti tehnički uvid u način na koji se odabrane taktike manifestiraju unutar stvarnih napada te kako se mogu simulirati korištenjem specifičnih alata i metoda. Implementacija

taktika ključan je korak u stvaranju realističnog okruženja za testiranje, omogućujući organizacijama procjenu učinkovitosti njihovih sigurnosnih mehanizama. Kroz korištenje Atomic Red Team alata svaka od odabranih taktika simulira specifične napadačke tehnike koje su u svojim inačicama korištene u stvarnim napadima.

Kroz daljnji tekst biti će navedene sve odabrane tehnike, te će za svaku od njih biti pružen tehnički osvrt i način implementacije u sustav.

Inicijalni pristup – kako je već ranije spomenuto inicijalni pristup predstavlja napadačku taktiku čiji je cilj pronaći ulaznu točku u ciljani sustav. U provedenoj simulaciji korištena je taktika T1566.001 kojom se simulira početna kompromitacija sustava preuzimanjem *spearphishing* privitka koji sadrži makro naredbe. Ovim ART testom želi se testirati mogućnosti EDR rješenja da prepoznaju i blokiraju maliciozne datoteke.

Izvršenje – ovom taktikom napadači izvršavaju pokretanje programa malicioznog koda na ciljanim sustavima. Odabrani ART test za ovu tehniku je T1059.001 koji se temelji na simulaciji iskorištavanja naredbene ljuske (engl. *PowerShell*) pomoću koje se pokreću zlćudne komande i skripte. Za potrebe testiranja umjesto stvarno korištenog *Empire PSInject* alata, kroz skriptu je pokrenuto dohvaćanje *Mimikatz* alata putem sumnjive poveznice, te je nakon uspješnog preuzimanja alat se kroz istu skriptu pokreće i pokušava kopirati kredencijale iz memorije kompromitiranog sustava.

Perzistentnost – tehnika perzistentnosti odnosi se na aktivnosti napadača kojima teže ostvarivanju postojanosti u sustavu nakon provedene inicijalne kompromitacije. Korišteni simulacijski scenarij za ovu tehniku je T1547.001 kojim se u sustavu kreira postojanost referenciranjem zlonamjernog programa s novokreiranim registarskim ključem (engl. *Registry Key*). Pomoću takvog referenciranja, prilikom svakog pokretanja zaraženog sustava ili prijave kompromitiranog korisnika program malicioznog koda se izvršava. Za potrebe testiranja korištena je biblioteka dinamičke veze (engl. *Dynamic-Link Library*, DLL) kreirana od strane proizvođača umjesto korištenja izvršne datoteke koja sadrži alat *Metasploit*.

Eskalacija privilegija – ovom tehnikom napadači žele ostvariti veća prava u kompromitiranom sustavu u odnosu na inicijalno ostvarena prava. Kod stvarnih napada koje provodi odabrani APT, tehniku eskalacije prava koriste na način da iskorištavaju lokalno kreirane račune koji imaju identičnu zaporku u svim segmentima kompromitirane domene. U svrhu testiranja korištena je taktika T1078.003 pomoću koje se u simuliranom okruženju kreirao novi korisnički račun koji je imao ovlasti lokalnog administratora.

Izbjegavanje obrane – korištenje ove tehnike za cilj ima onesposobiti ili zaobići ugrađene sigurnosne mehanizme operativnih sustava. U kontekstu APT *Turla*, izbjegavanje obrane je korišteno na način da napadači korištenjem *PowerShell* sesije pokušavaju modificirati logičku vrijednost povezanu s funkcionalnošću sučelja za skeniranje zlućudnih programa (engl. *Antimalware Scripting Interface*, AMSI). Uspješnim zaobilaženjem, odnosno gašenjem AMSI sučelja napadači ostvaruju pravo pokretanja malicioznih skripti koje neće biti inspektirane. U svrhu simulacije ponašanja navedene grupe korištena je taktika T1562.001 koja vjerno replicira ponašanje stvarnih napadača. Izvršavanjem navedenog testa želi se onemogućiti AMSI sučelje i testirati detekcijske sposobnosti EDR rješenja.

Prikupljanje vjerodajnica – ovom taktikom napadači unutar kompromitirane infrastrukture koriste tehnike krađe podataka kako bi kreirali uporište putem kojeg se mogu neprimijećeno kretati mrežom. Prilikom provođenja simulacije korištena je tehnika T1555.004 kojom se simulira stvarno ponašanje odabrane napadačke grupe. Taktika koristi skriptu koja poziva legitimni Windows alat *vaultcmd* pomoću kojeg vrši ispisivanje svih trenutno spremljenih vjerodajnica na zaraženoj radnoj stanici. Navedeni alat informacije o vjerodajnicama povlači iz servisa za upravljanje kredencijalima (engl. *Credential Manager*).

Otkrivanje – svrha korištenja ove taktike je prikupljanje informacija o kompromitiranom sustavu s ciljem pronalaska kritičnih točki koje se žele iskoristiti za povećanje opsega napada. ART test korišten prilikom provođenja simulacije baziran je na tehnici T1083, gledajući sa stajališta realističnosti testa može se potvrditi kako je kreirani test sličan stvarnom napadu koji prilikom svojeg izvršavanja pretražuje specifične direktorije. Provedeni test u odnosu na stvarni napad, pretražuje i ispisuje sadržaj svih direktorija koji su dostupni korisniku čiji račun se koristi za izvršavanje napada.

Bočno kretanje – ovom tehnikom napadači koriste informacije prikupljene u prijašnjim koracima u svrhu ostvarivanja konekcije na druge sustave unutar mrežnih segmenata kompromitirane infrastrukture. Za potrebe simulacije stvarnih napada korištena je tehnika T1021.002 koja vjerno replicira ponašanje *Turla* grupe. Navedenom taktikom simulira se ostvarivanje konekcije prema mrežno dijeljenim resursima korištenjem legitimnih Windows procesa.

Prikupljanje – u ovoj fazi kibernetičkog napada, napadačima je cilj pripremiti informacije od interesa za daljnju obradu i eksfiltraciju. Prema dostupnim izvorima odabrana APT grupa koristi ovu tehniku kako bi unutar kompromitirane infrastrukture kreirala mrežu računala koja

razmjenjuje informacije korištenjem RPC protokola. Cilj kreiranja takve mreže je kreacija lokalno bazirane zapovjedne infrastrukture putem koje zaraženi resursi izvršavaju dane instrukcije. Za potrebe simulacije korištena je taktika T1005, koja je također korištena od strane *Turla* grupe, ali u odnosu na stvarne napade kreirani test provodi pretraživanje datoteka od interesa te kreiranje komprimirane mape koja sadrži takve dokumente.

Zapovijedanje i upravljanje – ovom tehnikom napadači ostvaruju udaljeni pristup pomoću kojeg orkestriraju daljnje faze napada. U kontekstu simulacije stvarnih napada korištena je taktika T1071.001 kojom se simulira komunikacija zaražene infrastrukture s malicioznim zapovjednim poslužiteljem napadača. Testiranje je provedeno s predefiniranim vrijednostima koje umjesto stvarnog malicioznog poslužitelja koriste *Google* domenu, zbog toga postoji mogućnost da EDR rješenja neće prepoznati provedene aktivnosti kao maliciozne.

Eksfiltracija – završna faza većine naprednih kibernetičkih napada, kojoj je cilj krađa podataka i njihovo korištenje za nove kibernetičke napade. Gledajući dostupna izvješća o napadima grupe *Turla* vidljivo je kako grupa koristi više metoda za iznošenje ukradenih podataka, a jedna od metoda je korištenje pohrane u oblaku. Iako se prema dostupnim informacijama prikazuje kako stvarni napadi koriste servise *OneDrive* i *4shared*, za potrebe simulacije korišten je servis pohrane u oblaku *Mega*. Taktika koja je korištena za provođenje simulacije bazira se na T1567.002 i korištenju alata komandnog retka *rclone*.

4.4.5. Provođenje simulacije

Provedenim istraživanjem i pažljivim odabirom relevantnih taktika, kao i njihovom implementacijom, stvorena je solidna osnova za završnu fazu simulacije napada. Ovaj segment plana obuhvaća sve aktivnosti prikazane na slici 3, uključujući završne provjere definiranih taktika i tehničkih zahtjeva kako bi se osiguralo da simulacija bude provedena uspješno i u skladu s ciljevima. Tokom same simulacije, bilježe se ključne informacije o rezultatima testova, reakcijama EDR sustava, kao i o ponašanju ciljanog sustava. U nastavku će biti detaljno opisan cjelokupan proces simulacije koji je korišten u ovom istraživanju, uključujući analizu zapažanja i reakcija testiranih sigurnosnih mehanizama.

Završne provjere definiranih testova i zahtjeva sustava u ovom slučaju zahtijevaju dodatnu analizu dokumentacije *Atomic Red Team* platforme, odnosno dokumentacije odabranih taktika. Kako je vidljivo u niže prikazanoj tablici, za uspješno provođenje simulacije napada potrebno je na ciljanim sustavima omogućiti dodatne funkcionalnosti za taktike T1005 i T1567.

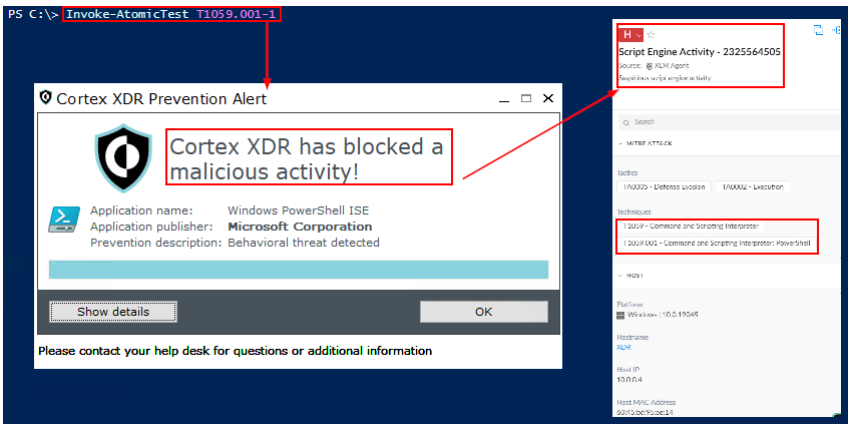
Za taktiku T1005, potrebno je provjeriti da li postoji neka od vrsti tekstualnih datoteka u sustavu, odnosno potrebno je kreirati novi tekstualni dokument proizvoljnog naziva i sadržaja.

Za taktiku T1567, potrebno je provjeriti da li postoji mapa *ExternalPayloads* unutar *C* direktorija, te da li sadrži *rclone* izvršnu datoteku. Ukoliko navedena mapa ili datoteka ne postoje, potrebno je kreirati navedenu mapu, odnosno preuzeti izvršnu datoteku s Interneta.

Tablica 3: Prikaz dodatnih zahtjeva odabranih taktika

Taktika	Oznaka testa	Dodatni zahtjevi
T1566	T1566.001 #1	Simuliranje ne zahtjeva dodatne funkcionalnosti sustava
T1059	T1059.001 #1	Simuliranje ne zahtjeva dodatne funkcionalnosti sustava
T1547	T1547.001 #2	Simuliranje ne zahtjeva dodatne funkcionalnosti sustava
T1078	T1078.003 #1	Simuliranje ne zahtjeva dodatne funkcionalnosti sustava
T1562	T1562.001 #13	Simuliranje ne zahtjeva dodatne funkcionalnosti sustava
T1555	T1555.004 #1	Simuliranje ne zahtjeva dodatne funkcionalnosti sustava
T1083	T1083 #2	Simuliranje ne zahtjeva dodatne funkcionalnosti sustava
T1021	T1021.002 #4	Simuliranje ne zahtjeva dodatne funkcionalnosti sustava
T1005	T1005 #1	Simuliranje zahtjeva postojanje jedne ili više datoteka s ekstenzijama .doc, .docx, .txt
T1071	T1071.001 #1	Simuliranje ne zahtjeva dodatne funkcionalnosti sustava
T1567	T1567.002 #1	Simuliranje zahtjeva postojanje datoteke rclone.exe unutar mape na putanji C:\ExternalPayloads

Nakon što su provedene sve završne provjere, sustav je spreman za pokretanje simulacije kibernetičkih napada. Simulacija se odvija sekvencijalno, gdje se svaka od odabranih taktika izvršava prema unaprijed definiranom redoslijedu. Tijekom izvođenja svake taktike, pažljivo se prati ponašanje sustava te reakcije aktivnog EDR rješenja unutar testne okoline. Na idućoj slici prikazano je pokretanje jedne od odabranih taktika, uz pripadajući odgovor EDR sustava na napad.



Slika 7: Simuliranje odabrane taktike i praćenje ponašanje ciljanog sustava

Kao što je već ranije navedeno, cilj praktičnog dijela ovog diplomskog rada jest simulirati kibernetičke napade koji oponašaju stvarne APT prijetnje, a sve u svrhu praćenja i evaluacije učinkovitosti odabranih EDR rješenja. Važno je napomenuti da svrha simulacije nije pružiti iscrpan uvid u sve mogućnosti EDR rješenja, budući da bi takav opsežan pristup zahtijevao znatno više vremena i resursa. Umjesto toga, simulacija ima za cilj identificirati osnovne reakcije sigurnosnih sustava i pružiti uvid u njihove mogućnosti detekcije i odgovora na tipične prijetnje, dok će se usporedba s komercijalnim evaluacijama obraditi kasnije u radu.

Zadnji segment provođenja simulacije kibernetičkih napada podrazumijeva izvještavanje o zabilježenim događajima. Kako se identična simulacija provodila pet puta u svrhu testiranja različitih EDR rješenja, izvještaj o zabilježenim događajima biti će pružen niže prikazanom tablicom, dok će se za svako EDR rješenje ukratko opisati zabilježeni događaji.

Dodano, za lakše razumijevanje priložene tablice, potrebno je opisati oznake korištene u istoj:

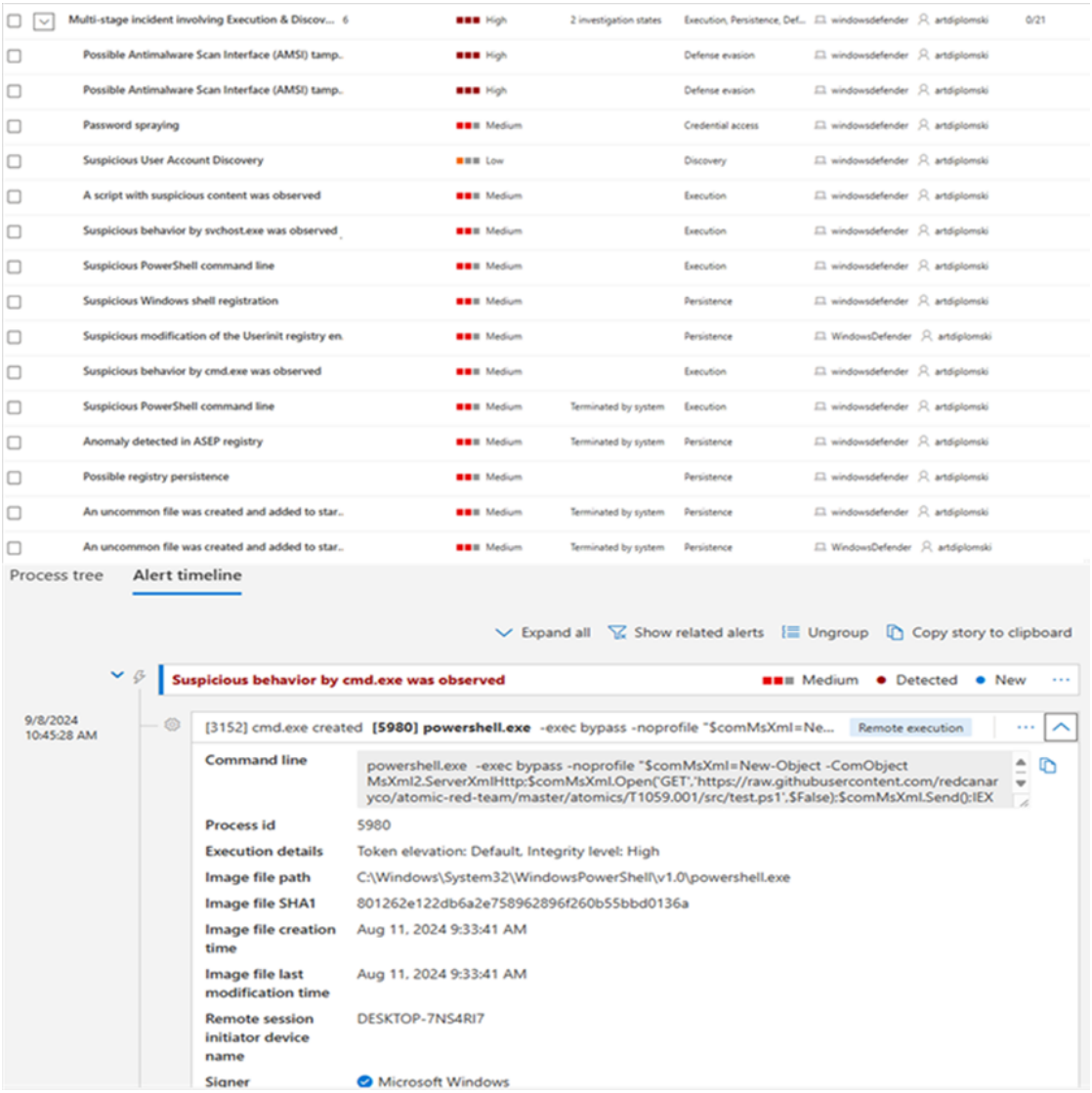
- Crveno označene ćelije: Sustav nije detektirao napad i ne postoji zapis u EDR konzoli
- Narančasto označene ćelije: EDR nije detektirao napad, ali su pronađeni zapisi u vremenskoj crti događaja
- Žuto označene ćelije: Sustav je detektirao napad, ali ga nije blokirao
- Zeleno označene ćelije: Sustav je uspješno detektirao i blokirao napad

Tablica 4: Sumarni prikaz rezultata testiranja EDR rješenja

	Microsoft Defender	Palo Alto Networks Cortex XDR	Trend Micro Apex One	Bitdefender Gravity Zone	WithSecure Elements EDR
T1566					
T1059					
T1547					
T1078					
T1562					
T1555					
T1083					
T1021					
T1005					
T1071					
T1567					

Rezultati simulacije napada na odabrana EDR rješenja pružaju pregled učinkovitosti samih rješenja u detekciji i odgovoru na sofisticirane prijetnje. Fokus ove analize je na tome kako sustav reagira na specifične tehnike napada, uključujući detekciju i blokiranje zlonamjernih aktivnosti. U svrhu ovog rada, rezultati su prikazani sažeto, bez dublje tehničke analize, s ciljem davanja jasne slike o osnovnim mogućnostima sustava. Ovaj način evaluacije omogućuje razumijevanje temeljnih funkcionalnosti testiranih EDR rješenja, pri čemu su zabilježene različite reakcije sustava, od potpune detekcije i blokiranja napada, preko djelomičnih detekcija, do slučajeva u kojima sustav nije uopće prepoznao maliciozne aktivnosti.

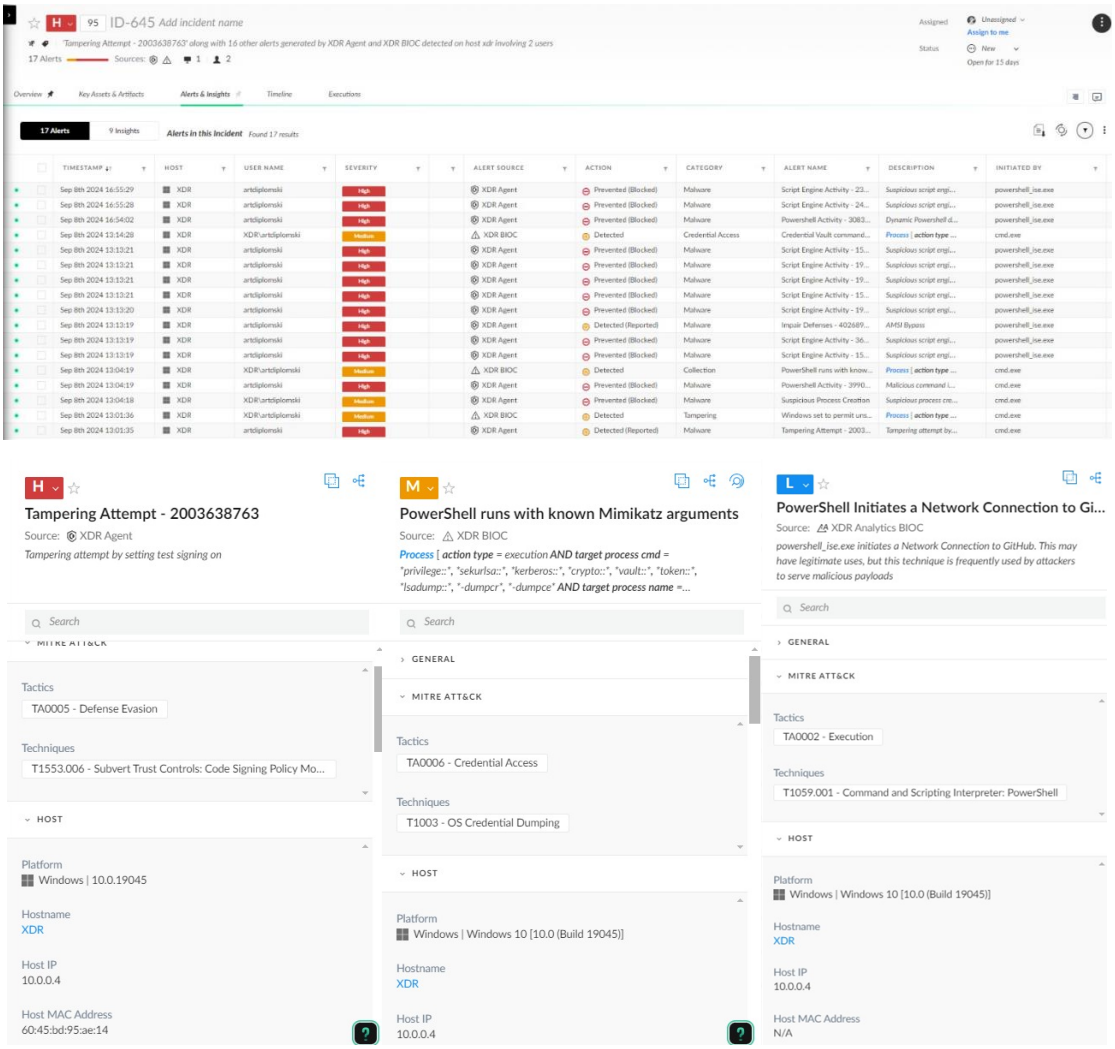
Izvođenjem testiranja EDR rješenja Microsoft Defender for Endpoint primijećeno je kako sustav funkcionira prema definiranim parametrima dostupnim u tehničkoj dokumentaciji. Izvršavanjem svakog od jedanaest definiranih testova pozorno su ispraćene reakcije sustava, te je zaključeno da su detekcijske sposobnosti sustava vrlo dobre, dok s druge strane automatizirani odgovor na prouzročene sigurnosne incidente nije bio na zavidnoj razini. Daljnjom analizom dizajna testiranog sustava potvrđeno je da je sustav bio konfiguriran u načinu rada „monitoring“ što znači da će sustav zabilježiti napad, ali ga neće blokirati, osim u slučajevima gdje se radi o poznatim malicioznim datotekama. Izgled sučelja i neke od detekcija vidljive su idućom slikom. Također prilikom praćenja rada sustava primijećeni su nedostaci u funkcionalnostima EDR konzole, odnosno nemogućnost potpunog pretraživanja vremenske crte događaja testirane radne stanice. Navedeni nedostaci proizlaze iz licenciranja koje je za vrijeme provođenja simulacije bilo u probnoj verziji. Završetkom simulacije i analizom zabilježenih događaja i ponašanja sustava može se donijeti zaključak da je Microsoft Defender for Endpoint dobar izbor za zaštitu krajnjih uređaja organizacija čije se poslovanje temelji na Windows infrastrukturi te čiji sigurnosni timovi nisu sačinjeni od visoko kvalificiranih stručnjaka iz razloga što samom instalacijom rješenja nisu potrebne velike preinake kako bi sustav zadovoljio sve potrebe organizacije.



Slika 8: Prikaz detekcija i ponašanja sustava Microsoft Defender for Endpoint

Palo Alto Networks Cortex XDR prilikom testiranja pokazao se kao funkcionalan i sveobuhvatan alat za zaštitu krajnjih uređaja. Prema dostupnoj dokumentaciji i izvještajima trećih strana, ponašanje sustava tokom simuliranih kibernetičkih napada pokazalo se kao očekivano. Kod izvršavanja pojedinih testova primijećeno je da se svaki od prepoznatih napada klasificirao prema istim taktikama koje su bile korištene u samim testovima. Kao i kod prethodno spomenutog rješenja, zabilježena je veća količina detektiranih pokušaja napada u odnosu na blokirane iz razloga što je u vrijeme simulacije bila primijenjena politika koja onemogućava automatiziranu mitigaciju ugroza. Takva politika je definirana s ciljem provjere detekcijskih sposobnosti sustava, te zbog osiguravanja izvršavanja samih testova. Ukoliko bi se koristila restriktivnija politika postojale bi velike šanse da se simulacija ne bi mogla uspješno izvršiti iz razloga što bi EDR rješenje prilikom prvog pokretanja testne skripte blokiralo daljnje izvršavanje procesa, te bi datoteke iz mape *Atomic Red Team* testova stavio u karantenu.

Provođenje simulacije, odnosno reakcija sustava na pojedine testove prikazana je idućom slikom.

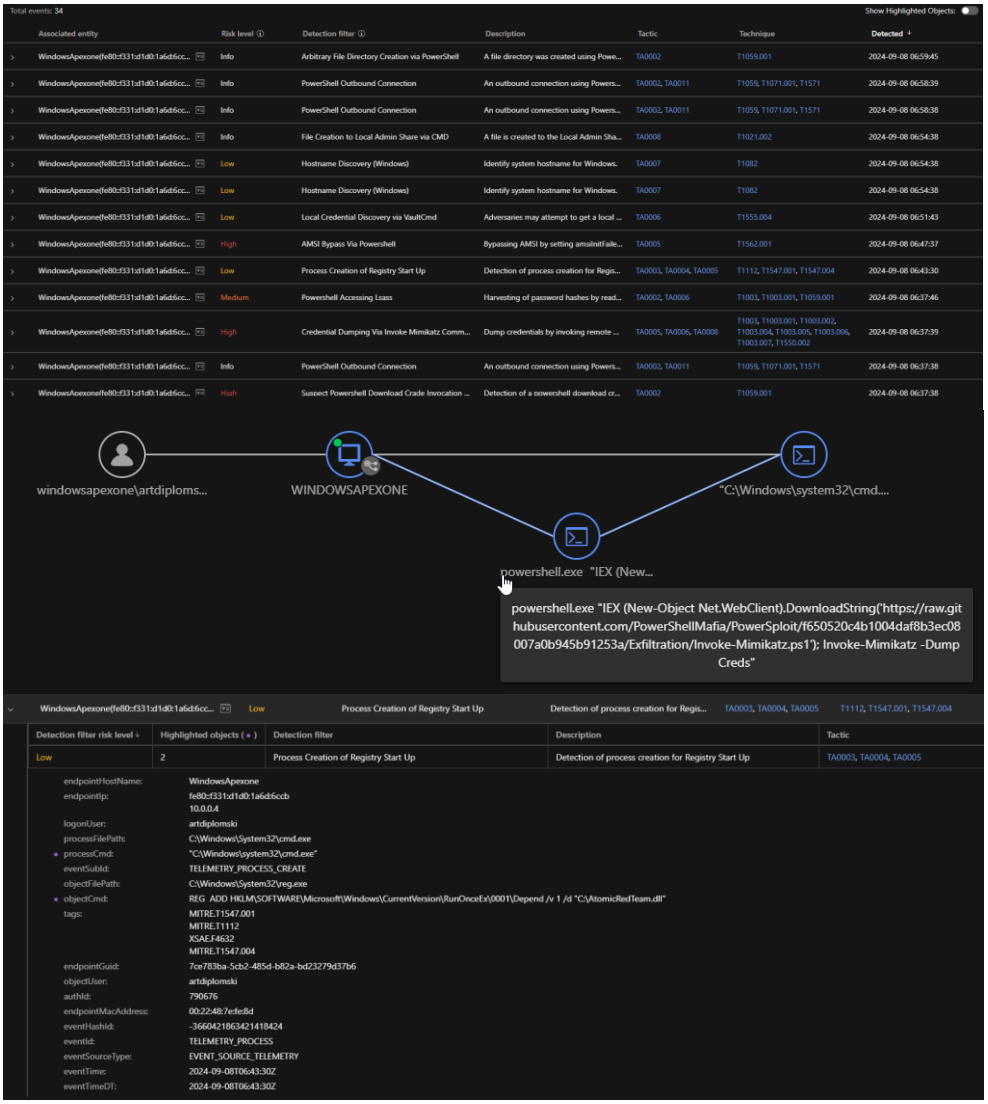


Slika 9: Prikaz detekcija i zapisa Cortex XDR rješenja

Usporednim praćenjem rada sustava i pokretanjem simulacije, nisu zabilježeni neočekivani događaji, dok se nedostaci platforme manifestiraju kroz nemogućnost izričitog pronalaska mrežnih aktivnosti, odnosno pristupa određenim poveznicama što otežava trijažu sigurnosnog incidenta. Navedeni nedostatak moguće je kompenzirati integracijom logova s drugih mrežnih sustava koji odrađuju analizu prometa. Provedenim testiranjem može se donijeti zaključak kako je Palo Alto Networks Cortex XDR jedan od najpotpunijih alata na tržištu, te je njegova implementacija pogodna za srednje i velike organizacije, neovisno o infrastrukturi operativnih sustava koje koriste.

Trend Micro Apex One rješenje za zaštitu krajnjih uređaja u poslovnim okruženjima prilikom provođenja simulacije pokazalo je varijacije u mogućnostima detekcije. Rješenje je bilo

konfigurirano na sličan način kao i ostala EDR rješenja, odnosno onemogućene su funkcionalnosti automatskog blokiranja prijetnje, ali u odnosu na druge sustava prilikom isključivanja tih funkcionalnosti, također se gube funkcionalnosti blokiranja poznatih malicioznih datoteka. Provođenjem simulacije i bilježenjem ponašanja sustava nisu uočeni veći nedostaci u detekcijskim mogućnostima. Analizom generiranih incidenata potvrđeno je očekivano ponašanje sustava, dok se istovremeno identificirao nedostatak vezan uz mogućnost pretraživanja sistemskih zapisa sa simulirane radne stanice. Također daljnjim radom sa samom konzolom zaključuje se kako konzola sadrži sve potrebne funkcionalnosti, ali iskustvo i intuitivnost korištenja se mogu opisati kao dovoljni uz dosta prostora za napredak. Idućom slikom prikazani različiti prozori putem kojih se odrađuje analiza simuliranih napada.



Slika 10: Prikaz detekcija i zapisa Trend Micro Apex One rješenja

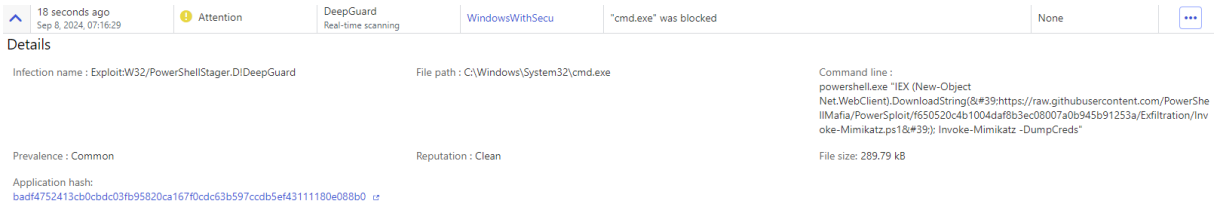
Bitdefender Gravity Zone prvo je EDR rješenje koje je pokazalo velike varijacije u detekcijskim sposobnostima simuliranih kibernetičkih napada. Od jedanaest provedenih napada, ovo rješenje

uspješno je blokiralo i detektiralo četiri napada, dok za ostale napade ne postoje vidljivi zapisi. Ovakvo ponašanje sustava može se pripisati poteškoćama s licenciranjem samog rješenje, zbog toga što se simulacija kibernetičkih napada provodila na sustavu s evaluacijskom licencom koja ne sadrži sve funkcionalnosti plaćene verzije. Prema danim mogućnostima, iskustvo korištenja i dostupnost zapisa o događajima je jako štura, za detektirane događaje moguće je korištenjem konzole vidjeti o kojim alarmima je riječ, odnosno o putanji detektiranih datoteka što je prikazano idućom slikom. U odnosu na prije testirane sustave Bitdefender Gravity Zone prema dobivenim rezultatima ne zadovoljava kriterije korištenja u poslovnom okruženju. Dodatno, zaključak je izveden prema subjektivnom osjećaju korištenja i vidljivih informacija vezanih uz simulirane prijetnje, u nastavku rada biti će prezentirani rezultati industrijskih testova pomoću kojih će se donijeti završna evaluacija ovog EDR rješenja.

Category	Details	Action taken	Endpoint name	Detected on ↑
Process	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	Allowed (1 times)	WindowsGravityZ	8 Sep 2024 11:31
Process	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	Allowed (1 times)	WindowsGravityZ	8 Sep 2024 11:30
Process	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	Allowed (1 times)	WindowsGravityZ	8 Sep 2024 11:30
Process	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	Allowed (1 times)	WindowsGravityZ	8 Sep 2024 11:30
Process	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	Allowed (1 times)	WindowsGravityZ	8 Sep 2024 11:30
File	C:\AtomicRedTeam\atomics\T1555.004\T1555.004.yaml	Deleted (1 times)	WindowsGravityZ	8 Sep 2024 11:18
Process	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	Disinfected (1 times)	WindowsGravityZ	8 Sep 2024 11:17
Process	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	Disinfected (1 times)	WindowsGravityZ	8 Sep 2024 11:13
Process	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	Disinfected (1 times)	WindowsGravityZ	8 Sep 2024 11:10
File	C:\AtomicRedTeam\atomics\T1059.001\T1059.001.yaml	Deleted (1 times)	WindowsGravityZ	8 Sep 2024 11:10
Process	C:\Windows\System32\Taskmgr.exe	Disinfected (1 times)	WindowsGravityZ	8 Sep 2024 11:02

Slika 11: Prikaz detekcija sustava Bitdefender Gravity Zone

WithSecure Elements EDR zadnji je sustav za zaštitu krajnjih uređaja koji se testirao. Kao i kod prijašnjih sustava bilo je potrebno kreirati politiku u sustavu kojom se onemogućava automatsko blokiranje prijetnji. Kreiranje i provođenje politike je bilo uspješno, te je odrađeno simuliranje kibernetičkih prijetnji. Prilikom provođenja pojedinačnih testova zabilježena je samo jedna reakcija na test povezan preuzimanjem i pokretanjem malicioznog programa *Mimikatz*, za ostale simulirane prijetnje nisu uočeni zapisi o detekciji istih. Analizom generiranog incidenta dobivene su informacije koji proces je inicirao aktivnost te koja komanda je bila korištena. Navigiranje konzolom i konfiguriranje samog rješenja je izazovno, te zahtjeva dobru tehničku pripremu za uspješno savladavanje korištenja sustava. U odnosu na ostale testirane sustave prema rezultatima testiranja koji su prikazani ranije u ovome radu, donijet je zaključak kako ovaj sustav nije pogodan za korištenje u korporativnom okruženju.



Slika 12: Prikaz detekcije WithSecure rješenja

5. Sinteza rezultata i evaluacija ispitanih rješenja

U ovom poglavlju analizira se učinkovitost odabranih EDR rješenja kroz tehničke performanse u detekciji naprednih prijetnji. Istraživanje se fokusira na usporedbu rezultata simulacija napada provedenih u okviru ovog rada s rezultatima MITRE *Engenuity 2023 Turla* industrijske evaluacije. Sintezom navedenih testiranja omogućuje se detaljan uvid u sposobnost svakog rješenja da prepozna i odgovori na specifične napadačke tehnike, pružajući tako temelj za daljnju analizu njihove učinkovitosti u informacijsko-komunikacijskim sustavima organizacija.

5.1. Analiza rezultata MITRE Engenuity 2023 evaluacije

MITRE *Engenuity* predstavlja relativno novu vrstu evaluacije EDR rješenja koja se provodi na godišnjoj razini i za cilj ima simulirati APT napade te prezentirati detekcijske i protekcijske mogućnosti pojedinih EDR rješenja. Evaluacija EDR rješenja odvija se u simuliranim okolinama gdje su kreirane inačice stvarne informacijsko-komunikacijske infrastrukture unutar kojih su ugrađena sama rješenja za koja se provodi testiranje. Ovom industrijskom evaluacijom cilj je kreirati jedan ili više napadačkih scenarija koji se temelje na MITRE ATT&CK radnom okviru i koriste alata i tehnologije stvarnih napadača.

Evaluacija EDR sustava bazira se na detekcijskim i korektivnim mogućnostima sustava za svaki korak simuliranog kibernetičkog napada. Detekcijske performanse opisuju se kroz sposobnost sustava da mapira provedene napade prema definiranim detekcijskim kategorijama s ciljem prikazivanja količine kontekstualnih informacija koje sustav pruža prilikom detekcije napada. Dok korektivne odnosno protekcijske mogućnosti prikazuju točni korak napada u kojem je isti bio zaustavljen. Detekcijske kategorije korištene u zadnjoj iteraciji evaluacija, podijeljene su na: detekciju tehnike, detekciju taktike, općenitu detekciju, detekciju pomoću telemetrije, nepostojanje detekcije i neprimjenjivo. Detekcija tehnike pokazuje da je sustav detektirao napad i uspješno identificirao tehniku izvođenja, kod detekcije taktika sustav prepoznaje obrazac ponašanja ali nije u mogućnosti definirati kako je napad izvršen. Opće detekcije ukazuju da sustav ima mogućnost prepoznavanja malicioznih aktivnosti ali ne može dati kontekst sigurnosnog događaja. Kod telemetrijske detekcije sustav je zabilježio događaj ali ga nije u mogućnosti klasificirati.

U kontekstu ovog rada i mogućnosti usporedbe rezultata dobivenih simulacijom i rezultata prikupljenih iz ove evaluacije, kroz daljnji tekst biti će ukratko opisane performanse korištenih EDR sustava, na način da će se sve detekcijske kategorije koje pokazuju uspješnu detekciju

napada klasificirati kao jedna kategorija, dok će nesposobnost detekcije ostati kao druga samostalna kategorija.

Tablica 5: Prikaz rezultata MITRE Engenuity evaluacije, [62]

EDR rješenje	Broj provedenih napada	Broj detektiranih napada	Postotak uspješnosti
Bitdefender Gravity Zone	143	131	92%
Microsoft Defender for Endpoint	143	143	100%
Palo Alto Networks Cortex XDR	143	143	100%
Trend Micro Apex One	143	126	88%
WithSecure EDR	143	96	67%

Prema prikazanoj tablici i provedenom analizom rezultata vidljivo je kako su testirani sustavi Microsoft Defender for Endpoint i Palo Alto Networks Cortex XDR pokazali znatno bolje rezultate u odnosu na ostala testirana EDR rješenja. Kako je već ranije definirano, evaluacija dobivenih rezultata se odrađuje generaliziranim pristupom kojim će pružiti manje precizni podaci, ali potreba za takvim pristupom proizlazi iz sinteze industrijskih rezultata i rezultata provedene simulacije u četvrtom poglavlju ovog rada.

Bitdefender Gravity Zone prema dostupnim rezultatima neuspješno je detektirao neke od provedenih napada vezanih uz uspostavljanje komunikacije sa zaraženim zapovjednim poslužiteljem, izbjegavanje obrane, otkrivanje resursa, ostvarivanje postojanosti u sustavu te eskalacije privilegija. Daljnjom analizom protekcijskih mogućnosti potvrđeno je kako je sustav uspješno prevenirao napade vezane uz inicijalni pristup, izvršenje malicioznog koda, ostvarivanje postojanosti i kopiranju vjerodajnica, dok sustav nije bio u mogućnosti prevenirati napade vezane uz pogađanje korisničkih zaporki.

Microsoft Defender for Endpoint prema generaliziranim informacijama iz gornje tablice pokazao je sveobuhvatno djelovanje kod detekcije kibernetičkih napada. Detaljnijom analizom rezultata uočeno je da se kod tehnika prikupljanja, zapovijedanja i upravljanja te izbjegavanja obrane postoje testiranja koja je ovo rješenje detektiralo na osnovu telemetrijskih podataka. Osim navedenih poteškoća u detektiranju pojedinih tehnika, rješenje se pokazalo kao učinkovito i u djelu prevencije napada, gdje je svaka faza napada bila onemogućena prilikom prvog izvršavanja neke od taktika svake tehnike.

Palo Alto Cortex XDR kako je vidljivo u gornjoj tablici imao slične rezultate kao i prethodno opisano EDR rješenje. Detaljnijom analizom rezultata evaluacije vidljivo je da je sustav uspješno detektirao sve provedene napade detekcijskom kategorijom tehnika, odnosno s najvećom preciznošću. Dok je u testiranju mogućnosti prevencije napada također uspješno zaustavio simulirane napade prilikom prvog pokretanja malicioznog programa.

Trend Micro Apex One ostvario je zadovoljavajuće rezultate u provedenim industrijskim testiranjima. Poteškoće u detekcijskim mogućnostima ovog rješenja manifestirane su kroz nemogućnost prepoznavanja napada povezanih s tehnikama prikupljanja, izvršenja, zaobilaženja sigurnosnih mehanizama i zapovijedanja i upravljanja. Dok se u testiranju prevencije kibernetičkih napada rješenje pokazalo učinkovitim te je jedini nedostatak uočen kod prevencije izvršavanja malicioznih programa gdje je napad onemogućen u drugom koraku, odnosno kod korištenja metode prikrivanja malicioznog programa.

WithSecure Elements EDR prema gornjoj tablici i rezultatima provedenih industrijskih testova ovaj sustav za zaštitu krajnjih uređaja u poslovnom okruženju pokazao se kao nezadovoljavajući izbor. Sustav je ostvario solidne rezultate, ali kao najveća mana ovog rješenja ističe se nemogućnost prepoznavanja tehnika i taktika u svakoj od jedanaest testiranih faza napada, dok testiranje protekcije nije bilo provedeno.

5.2. Sinteza dobivenih rezultata

Usporedbom rezultata dobivenih provedenom simulacijom s rezultatima industrijske evaluacije MITRE Engenuity želi se provesti korelacija podataka u svrhu donošenja zaključka kojim će se svako od testiranih rješenja evaluirati. Također razmotriti će se mogućnosti zbog kojih određena testiranja nisu izvedena te će se dati prijedlog poboljšavanja za korištenje u budućim simulacijama.

5.2.1. Usporedba rezultata rješenja Microsoft Defender for Endpoint

Korelacijom rezultata provedenih simulacija jasno je vidljivo da ovo rješenje za zaštitu krajnjih uređaja pokazuje slične reakcije i ponašanje kod prepoznavanja kibernetičkih napada. Provedenom simulacijom korištenjem *ART* predefiniranih testova zabilježeno je da sustav prepoznaje napad na temelju pokretanja zlonamjernih programa i skripti, dok se klasifikacija tehnika i taktika odvija na osnovu sadržaja samih malicioznih datoteka. Analizom rezultata industrijske simulacije uočeni su isti obrasci ponašanja, što dokazuje kako se moderni EDR sustavi najčešće temelje na detekciji pokretanja programa i praćenja ponašanja sustava.

5.2.2. Usporedba rezultata rješenja Bitdefender Gravity Zero

Uspoređivanjem rezultata uočene su velike razlike u mogućnostima detekcije testiranog sustava, što proizlazi iz činjenice da su simulirani napadi bili predefinirani i služe za objašnjavanje ponašanja napadača, kao i činjenice da je testirani sustav bio licenciran kao probna verzija, koja u odnosu na verziju testiranu od strane MITRE *Enfenuity* nema uključene sve funkcionalnosti. Analiziranjem napada koji su uspješno prevenirani moguće je donijeti zaključak kako sustav kada je podvrgnut realnim kibernetičkim ugrozama pokazuje očekivano ponašanje prilikom prepoznavanja i protekcije.

5.2.3. Usporedba rezultata rješenja Trend Micro Apex One

Komparacijom rezultata simulacija može se zaključiti kako u oba scenarija provođenja simulacije odabrani sustav funkcionira na zamišljeni način. Detaljnijom korelacijom simuliranih tehnika primijećeni su slični obrasci ponašanja, kao i iste poteškoće u radu sustava. Kod testova koji nisu uspješno detektirani kroz simulaciju opisanu u četvrtom poglavlju ovog rada doneseno je mišljenje kako testovi koji su korišteni za evaluaciju EDR rješenja nisu dovoljno razrađeni kako bi sustav prepoznao njihovu malicioznu nakanu.

5.2.4. Usporedba rezultata rješenja WithSecure Elements EDR

Provedenom simulacijom korištenjem *ART* testova pokazano je kako odabrani sustav nije kompetentan pružiti zaštitu poslovnoj infrastrukturi, kada se koristi na način minimalne dodatne konfiguracije. Korelacijom dobivenih rezultata s javno dostupnim podacima MITRE *Engenuity* evaluacije moguće je uvidjeti sličnosti u radu sustava. Iako se provođenjem industrijske evaluacije rješenje pokazalo znatno bolje u odnosu na testove odrađene ranije kroz ovaj rad, i dalje su uočeni propusti u dizajnu sustava, odnosno njegovih detekcijskih mogućnosti.

5.2.5. Usporedba rezultata rješenja Palo Alto Networks Cortex XDR

Usporedbom rezultata provedenih simulacija vidljivo je identično ponašanje testiranog sustava kod detekcije kibernetičkih napada i prevencije poznatih malicioznih programa. Detaljnijom analizom rezultata potvrđeno je kako sustav bez obzira na jednostavnost korištenih tehnika, precizno detektira i klasificira ugroze.

5.2.6. Prijedlog poboljšanja provedene simulacije

Kako je već ranije definirano, a što potvrđuju rezultati odrađene simulacije, korištenje *Atomic Red Team* platforme pruža dobru inicijalnu podlogu za razumijevanje složenih kibernetičkih napada. Zbog navedenog, korištenje platforme odnosno njenih predefiniranih testova za evaluaciju EDR rješenja, predstavlja relativno nepreciznu metodu evaluacije. Kako bi navedena

platforma bila kompetentna za provođenje temeljite evaluacije EDR sustava, potrebno je njene predefinirane testove modificirati prema potrebama simulacijskog plana. To uključuje izradu i poboljšanje postojećih skripti, korištenje poznatih malicioznih programa te kreiranje automatiziranog plana izvršavanja testova.

Poboljšavanjem predefiniranih skripti i sustava omogućuje se kreiranje platforme otvorenog koda koja će pokrivati sve osnovne funkcionalnosti sustava za simulaciju, a uz to će se ostvariti neke od funkcionalnosti plaćenih rješenja za simulaciju kibernetičkih napada.

6. Zaključak

Kibernetičke prijetnje, osobito one usmjerene na krajnje uređaje, predstavljaju značajan izazov za suvremene organizacije koje se oslanjaju na digitalnu infrastrukturu. Razvoj tehnologije i globalna digitalizacija omogućili su brži pristup podacima i komunikaciju, no istodobno su stvorili novu arenu za sofisticirane napade. EDR i EPP sustavi postali su neophodni alati u obrani od ovih prijetnji, no istraživanje provedeno u ovom radu ukazuje na potrebu za njihovim daljnjim unaprjeđenjem.

Simulacija napada napredne ustrajne prijetnje *Turla,* provedena kroz jedanaest različitih taktika, pokazala je kako su suvremeni sustavi sposobni detektirati i odgovoriti na temeljne prijetnje, poput eskalacije privilegija i lateralnog kretanja unutar mreže. Međutim, složenije tehnike poput eksfiltracije podataka i napada bez datoteka pokazale su slabosti postojećih rješenja. Istraživanje je također ukazalo na važnost integracije naprednih metoda, poput strojnog učenja i analize ponašanja, kako bi se poboljšala detekcija prijetnji i smanjio broj lažno pozitivnih rezultata.

U svijetu u kojem digitalni podaci postaju najvrjednija imovina, važno je osigurati slojevitu zaštitu koja može odgovoriti na rastuće prijetnje. Simulacija napada pokazala je koliko su organizacije ranjive na napredne ustrajne prijetnje, a implementacija naprednih analitičkih metoda ključna je za zaštitu krajnjih uređaja. Osim tehničkih rješenja, istraživanje također naglašava ključnu ulogu ljudskog faktora u cjelokupnom sustavu kibernetičke sigurnosti. Iako tehnologija može pružiti obranu, ljudi ostaju najslabija karika u većini slučajeva. Zbog toga je ključno nastaviti s edukacijom korisnika, kako bi bili svjesni potencijalnih prijetnji i ranjivosti koje zlonamjerni akteri mogu iskoristiti.

Provođenjem praktičnog dijela ovog diplomskog rada, kroz simulacije napada koji oponašaju sofisticirane prijetnje poput onih koje koristi APT grupa *Turla*, provedena je detaljna evaluacija učinkovitosti odabranih EDR rješenja. Svako rješenje testirano je na temelju unaprijed definiranih taktičkih scenarija korištenjem platforme Atomic Red Team kako bi se analizirale sposobnosti detekcije i odgovora na kibernetičke prijetnje. Rezultati su ukazali na značajne razlike u detekcijskim sposobnostima, ovisno o konfiguraciji sustava i ograničenjima korištene licence. Microsoft Defender for Endpoint i Palo Alto Networks Cortex XDR pokazali su najbolje performanse, no niti jedno rješenje nije bilo potpuno imuno na sofisticirane tehnike napada.

Usporedbom i sintezom dobivenih rezultata s industrijskom evaluacijom MITRE *Engenuity* potvrđuje se da sofisticirani napadači mogu zaobići obrambene mehanizme, što naglašava potrebu za daljnjim usavršavanjem sigurnosnih sustava. Unatoč razlikama u performansama, sva testirana rješenja pruža su korisne informacije o kibernetičkim napadima. Ovaj rad potvrđuje važnost kontinuirane evaluacije i prilagodbe sigurnosnih sustava, kao i važnost korištenja predefiniranih testova kao početne točke za prilagođavanje simulacije koje preciznije oponašaju stvarne prijetnje u dinamičnom okruženju kibernetičke sigurnosti poslovnih infrastruktura.

Literatura

[1] Arfeen, A., Ahmed, S., Khan, M.A., Jafri, S.F.A., 2021. Endpoint Detection & Response: A Malware Identification Solution. 2021 International Conference on Cyber Warfare and Security (ICCWS) [Pristupljeno: Rujan 2024.] Preuzeto sa: https://ieeexplore.ieee.org/document/9703010

[2] Vrescak, C., 2021. Examining OpenEDR's Effectiveness as an EDR Solution. White paper [Pristupljeno: Rujan 2024.] Preuzeto sa: https://sansorg.egnyte.com/dl/in4L3O7eMs

[3] Park, S.-H., Yun, S.-W., Jeon, S.-E., Park, N.-E., Shim, H.-Y, Lee, Y.-R., Lee, S.-J., Park, T.-R., Shin, N.-Y., Kang, M.-J., Lee, I.-G., 2022. Performance Evaluation of Open-Source Endpoint Detection and Response Combining Google Rapid Response and Osquery for Threat Detection. IEEE Access [Pristupljeno: Rujan 2024.] Preuzeto sa: https://ieeexplore.ieee.org/document/9716119

[4] Chandel , S., Yu, S., Yitian, T., Zhili, Z., Yusheng, H., 2019. Endpoint Protection: Measuring the Effectiveness of Remediation Technologies and Methodologies for Insider Threat. 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC) [Pristupljeno: Rujan 2024.] Preuzeto sa: https://ieeexplore.ieee.org/document/8945852

[5] Karantzas, G., Patsakis, C., 2021. An Empirical Assessment of Endpoint Detection and Response Systems against Advanced Persistent Threats Attack Vectors. Journal of Cybersecurity and Privacy, 1(3), pp.387-421. [Pristupljeno: Ožujak 2022.] Preuzeto sa: https://doi.org/10.3390/jcp1030021

[6] Touhill, G.J., Touhill, C.J., Cybersecurity for executives – A Practical Guide. New Jersey: Wiley; 2014

[7] Stallings, W., Brown, L., Computer security principles and practice. New Jersey: Pearson Education, Inc; 2015

[8] Anderson, R. Security Engineering – A Guide to Building Dependable Distributed Systems. New Jersey: Wiley; 2020

[9] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf [Pristupljeno: rujan 2024.]

[10] Leukfeldt, R. Research agenda – The human factor in cybercrime and cybersecurity. Den Haag: Eleven International Publishing; 2017

[11] Cappelli, D., Moore, A., Trzeciak, R. The CERT Guide to Insider Threats How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud). New Jersey: Pearson Education, Inc; 2012

[12] https://encyclopedia.kaspersky.com/glossary/cyber-attribution [Pristupljeno: kolovoz 2024.]

[13] https://carnegieendowment.org/2022/03/28/attribution-and-characterization-of-cyber-attacks-pub-86698 [Pristupljeno: kolovoz 2024.]

[14] Peraković, D., Cvitić, I. Sigurnost i zaštita informacijsko komunikacijskog sustava. 2021

[15] Defining Insider Threats. Preuzeto sa: https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats [Pristupljeno: kolovoz 2024.]

[16] Deep learning for insider threat detection: Review, challenges and opportunities. Preuzeto sa: https://www.sciencedirect.com/science/article/abs/pii/S0167404821000456 [Pristupljeno: kolovoz 2024.]

[17] Hacker types, motivations and strategies: A comprehensive framework. Preuzeto sa: this https://www.researchgate.net/publication/357938938 [Pristupljeno: kolovoz 2024.]

[18] Nation-state Hacking – What You Need to Know. Preuzeto sa: https://heimdalsecurity.com/blog/nation-state-hacking [Pristupljeno: kolovoz 2024.]

[19] Nation-state cyber attacks aren't like your average cyber adversary https://www.verizon.com/business/resources/articles/s/nation-state-cyber-attacks-arent-like-your-average-cyber-adversary/ [Pristupljeno: kolovoz 2024.]

[20] https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-39.pdf [Pristupljeno: kolovoz 2024.]

[21] Sood, A.K., Enbody, R.J. Targeted Cyberattacks: A Superset of Advanced Persistent Threats. 2013 Michigan State University

[22] Ussath, M., Jaeger, D., Cheng, F., Meinel, C. Advanced Persistent Threats: Behind the Scenes. 2016 Annual Conference on Information Science and Systems (CISS)

[23] Ullah, F., Ramdhany, R., Edwards, M., Chitchyan, R. Data Exfiltration: A Review of External Attack Vectors and Countermeasures. Journal of Network and Computer Applications

[24] Jordan, T., Taylor, P. Hacktivism and Cyberwars. London: Routledge; 2004

[25] https://www.trendmicro.com/vinfo/us/security/definition/cybercriminals [Pristupljeno: kolovoz 2024.]

[26] Rahalkar, S. Network Vulnerability Assessment. Birmingham: Packt Publishing Ltd.; 2018

[27] Rains, T. Cybersecurity Threats, Malware Trends, and Strategies. Birmingham: Packt Publishing Ltd.; 2020

[28] Sikorski, M., Hoing, A. Practical Malware Analysis – The Hands-On Guide to Dissecting Malicious Software. San Francisco: No Starch Press, Inc.; 2012

[29] Daswani, N., Kern, C., Kesavan, A. Foundations of Security What Every Programmer Needs to Know. New York: Apress; 2007

[30] Elisan, C.C. Malware, Rootkits & Botnets A Beginner's Guide. New York: The McGraw-Hill Companies, Inc.; 2013

[31] Liska, A., Dallo, T. Ransomware. Defending Against Digital Extortion. Massachusetts: O'Reilly Media, Inc.; 2016

[32] https://www.ibm.com/topics/ransomware [Pristupljeno: kolovoz 2024.]

[33] Strah i trepet među zloglasnim softverima: Kako izgleda ransomware napad? Preuzeto sa: https://csi.hr/2024/04/25/strah-i-trepet-medu-zloglasnim-softverima-kako-izgleda-ransomware-napad/ [Pristupljeno: kolovoz 2024.]

[34] Worms as Attack Vectors: Theory, Threats, and Defenses. Preuzeto sa: https://sansorg.egnyte.com/dl/5wLpaoD9ng [Pristupljeno: kolovoz 2024.]

[35] Midhunchakkaravarthy, D., Ganapathi, P. Computer Network Worms Propagation and its Defence Mechanisms: A Survey. Journal of Network and Computer Applications Preuzeto sa: https://www.researchgate.net/publication/299468348_Computer_Network_Worms_Propagation_and_its_Defence_Mechanisms_A_Survey [Pristupljeno: kolovoz 2024.]

[36] Gray, J. Practical Social Engineering. San Francisco: No Starch Press, Inc.; 2021

[37] Hadnagy, C. Social Engineering The Science of Human Hacking. New Jersey: Wiley; 2018

[38] Bhattacharyya, D.K., Kalita, J.K. DDoS Attacks - Evolution, Detection, Prevention, Reaction, and Tolerance. New York: CRC Press; 2016

[39] https://www.checkpoint.com/cyber-hub/cyber-security/what-is-ddos/#:~:text=A%20DDoS%20attack%20is%20essentially%20the%20legitimate%20use,degraded%2C%20or%20it%20may%20be%20rendered%20completely%20inaccessible. [Pristupljeno: kolovoz 2024.]

[40] Diogenes, Y., Ozkaya, E. Cybersecurity – Attack and Defense Strategies. Birmingham: Packt Publishing Ltd.; 2018

[41] Vaisla, K.S. Analyzing of Zero Day Attack and its Identification Techniques. Preuzeto sa: https://www.researchgate.net/publication/260489192 [Pristupljeno: rujan 2024]

[42] Singer, P.W., Friedman, A. Cybersecurity And Cyberwar What everyone needs to know. New York: Oxford University Press; 2014

[43] Hoffman, B.G. Red Teaming: Transform Your Business by Thinking Like the Enemy. London: Piatkus; 2017

[44] Kennedy, D., O'Gorman, J., Kearns, D., Aharoni, M. Metasploit: The Penetration Tester's Guide. San Francisco: No Starch Press; 2011

[45] https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf [Pristupljeno: rujan 2024.]

[46] https://www.recordedfuture.com/threat-intelligence-101/tools-and-technologies/mitre-attack-framework [Pristupljeno: rujan 2024.]

[47] https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf [Pristupljeno: rujan 2024.]

[48] https://attack.mitre.org/resources/ [Pristupljeno: rujan 2024.]

[49] https://github.com/maddev-engenuity/AdversaryEmulation/tree/main/labs [Pristupljeno: rujan 2024.]

[50] Shoemaker, D:, Kognke, A., Sigler, K. The Cybersecurity Body of Knowledge. Florida: CRC Press; 2020

[51] Ajmal, A.B., Khan, S., Alam, M., Mehbodniya, A., Webber, J., Waheed, A. Toward Effective Evaluation of Cyber Defense: Threat Based Adversary Emulation Approach. Preuzeto sa: https://www.researchgate.net/publication/370516021_Towards_Effective_Evaluation_of_Cyber_Defense_Threat_Based_Adversary_Emulation_Approach [Preuzeto: rujan 2024.]

[52] Storm, B.E., Applebaum, A., Miller, D.P., Nickels, K.C., Pennington, A.G., Thomas, C.B. MITRE ATT&CK: Design and Philosophy. Preuzeto sa: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf [Pristupljeno: rujan 2024.]

[53] https://caldera.readthedocs.io/en/latest/ [Pristupljeno: rujan 2024.]

[54] https://hstechdocs.helpsystems.com/manuals/cobaltstrike/current/userguide [Pristupljeno: rujan 2024.]

[55] https://github.com/redcanaryco/atomic-red-team/wiki/_About-Atomic-Red-Team [Pristupljeno: rujan 2024.]

[56] https://github.com/redcanaryco/atomic-red-team/wiki/_Executing-Atomic-Tests [Pristupljeno: rujan 2024.]

[57] https://docs.metasploit.com/ [Pristupljeno: rujan 2024.]

[58] User Guide Core Impact 19.1. Preuzeto sa: https://s4applications.uk/wp-content/uploads/2020/08/impact-19-1-user-guide.pdf [Pristupljeno: rujan 2024.]
[59] https://www.academy.attackiq.com/learning-path/intermediate-breach-attack-simulation [Pristupljeno: rujan 2024.]
[60] https://www.attackiq.com/platform/ [Pristupljeno: rujan 2024.]
[61] https://attack.mitre.org/groups/ [Pristupljeno: rujan 2024.]
[62] https://attackevals.mitre-engenuity.org/ [Pristupljeno: rujan 2024.]

Popis slika

Popis tablica

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 Evaluacija rješenja za zaštitu krajnjih uređaja od kibernetičkih ugroza u poslovnom okruženju , u Nacionalni repozitorij završnih i diplomskih radova ZIR.

Student:

U Zagrebu, 23.9.2024.

Matko Đurić
(ime i prezime, *potpis*)