PRILOŽNOSTI ZLIVANJA TEHNOLOGIJ SIEM, SOAR IN STROJNEGA UČENJA V PROCESIH INTELIGENCE TVEGANJ IN SAMODEJNEGA ODZIVANJA NA KIBERNETSKE INCIDENTE

Andrej Bregar, Sašo Gjergjek, Miran Novak, Damir Orlić
Informatika d.o.o., Vetrinjska ulica 2, 2000 Maribor
{andrej.bregar | saso.gjergjek | miran.novak | damir.orlic}@informatika.si

Povzetek

V sodobnih informacijskih okoljih in sistemih, ki se selijo v oblak, temeljijo na konceptih interneta stvari in podpirajo avtomatizacijo poslovanja v kontekstu industrije 4.0, imamo opravka z masovnimi podatki in obsežnim omrežnim prometom med povezanimi napravami. V takšni količini podatkov si je nemogoče zamisliti zaznavanje anomalij, varnostnih tveganj in potencialnih kibernetskih incidentov brez avtomatiziranih pristopov, ki uporabljajo tehnike strojnega učenja in umetne inteligence. Ključne so zlasti tehnologije za upravljanje varnostnih informacij in dogodkov (SIEM) ter za avtomatizacijo, orkestriranje in odzivanje na kibernetska tveganja (SOAR). V prispevku pojasnimo, kaj pridobimo z vpeljavo postopkov in tehnologij za avtomatizacijo odzivov na kibernetske incidente. Umestimo jih v širši proces obravnave in reševanja incidentov ter v kontekst življenjskega cikla in primerov uporabe na področju inteligence varnostnih groženj in tveganj. Analiziramo možnosti uvajanja in neposredne integracije gradnikov tehnologij SIEM in SOAR kakor tudi vključevanja pristopov umetne inteligence za namen avtomatiziranega zaznavanja in orkestriranja kibernetskih incidentov. Preučimo učinke zlivanja in sinergije tehnologij SIEM, SOAR in strojnega učenja, hkrati pa se dotaknemo tistih organizacijskih in tehnoloških vidikov, ki odpirajo izzive, težave ter priložnosti. Izpostavimo tudi dobre prakse in pristope, ki jih vpeljujemo v sklopu kompetenčnega centra za kibernetsko varnost.

Abstract

CONSOLIDATION OF SIEM, SOAR AND MACHINE LEARNING TECHNOLOGIES TO ENHANCE THE PROCESSES OF THREAT INTELLIGENCE AND AUTOMATED CYBER INCIDENT RESPONSE

Because contemporary information systems are moving to the cloud, utilize IoT (Internet of Things) and aim to automate business processes in the context of Industry 4.0, we have to deal with big data and heavy network traffic among interconnected devices. Such amounts of data require an automated approach to the identification of anomalies, cybersecurity risks and potential cybersecurity incidents on the basis of artificial intelligence and machine learning. In this regard, especially SIEM (Security Information and Event Management) and SOAR (Security Orchestration, Automation and Response) technologies play a key role. In the paper, we explain the benefits of procedures and technologies for the automation of responses to cybersecurity incidents. We place these processes and technologies into the broader incident response approach as well as into the context of cyber threat intelligence life cycle and use cases. We analyse the possibilities to apply, integrate and consolidate SIEM and SOAR technologies, and discuss how to use artificial intelligence and machine learning for the purpose of automated identification and orchestration of cybersecurity incidents. We review synergistic effects resulting from the integration and consolidation of SIEM, SOAR and machine learning, while we also address several organisational and technological issues, challenges and opportunities. Finally, we describe some good practices and approaches which are being introduced within the scope of our security operations center for the energy utilities domain.

Ključne besede

Kibernetska varnost, inteligenca kibernetskih groženj in tveganj, odzivanje na kibernetske incidente, avtomatizacija varnostnih postopkov, SIEM, SOAR, strojno učenje

Key words

Cybersecurity, cyber threat intelligence, incident response, cybersecurity automation, SIEM, SOAR, machine learning

UVOD

Področje zagotavljanja kibernetske varnosti v informacijskih okoljih in sistemih postaja vse bolj kompleksno. Na to vpliva več skupin dejavnikov, ki zajemajo pogostost, resnost in vpliv kibernetskih napadov, raznolikost in naprednost napadalskih tehnik, sofisticiranost vektorjev in motivov vdorov, vpetost varnosti in informatizacije v družbo ter v poslovne in upravljalske sisteme kakor tudi mnoge druge vidike. Število zaznanih kibernetskih incidentov tako iz leta v leto konstantno narašča, hkrati pa se sorazmerno povečuje obseg njihovih posledic. Glede na statistike [5, 10] je bilo zgolj v prvem četrtletju leta 2021 zaznanih okoli milijon kibernetskih napadov in blizu 20 milijonov primerov zlonamerne kode. Povprečen strošek okrevanja od kibernetskega napada znaša 5 milijonov EUR za večje organizacije oziroma 50.000 EUR za manjša podjetja. Globalna ocena stroškov posledic kibernetskega kriminala naj bi do konca leta 2025 tako na letnem nivoju narasla na kar 10,5 bilijonov EUR. Poleg tega se je v letu 2020 z ogroženimi podatki ali omrežji soočalo 54 % podjetij, z izsiljevalskim programjem pa naj bi bil vsakih 11 sekund napaden en poslovni informacijski sistem.

Napadalci svoje zlonamerne programe razvijajo, da so ti čedalje bolj škodljivi, številnejši in raznolikejši, zaradi česar jih je težko odkriti. Uporabljajo tudi najrazličnejše pristope, metode in tehnike, da pridejo v sistem, v katerem povzročijo škodo. Ti pristopi vključujejo napade DDoS (*Distributed Denial of Service*), zlorabo prijavnih podatkov, izsiljevalsko programje, socialni inženiring, napade »zero-day«, DNS (*Domain Name System*) tuneliranje, napade na naprave IoT (*Internet of Things*) in druge. V zadnjem času smo celo priča avtomatiziranim, inteligentnim in naprednim napadom, ki jih napadalci načrtujejo na podlagi strojnega učenja in umetne inteligence. Tako je poznanih nekaj sofisticiranih napadov DDoS, pri katerih je omrežje napadalskih računalnikov (*botnet*) usmerjala umetna inteligenca [7]. Čeprav si razvijalci varnostnih rešitev prizadevajo razviti boljše in kakovostnejše programske rešitve za obrambo pred kibernetskimi napadi, je varnostnim strokovnjakom, ki se trudijo zaznati in preprečiti kibernetske incidente, to zaradi vseh opisanih dejavnikov in raznolikih napadalskih pristopov zelo težko doseči. Dodatno njihovo nalogo otežuje velik obseg naprav, omrežnega prometa in varnostnih dogodkov, s katerim se soočamo v sodobnih informacijskih okoljih in sistemih, ki podpirajo avtomatizacijo celotnega poslovanja, se selijo v oblak in temeljijo na konceptih interneta stvari, zaradi česar imamo pri zagotavljanju kibernetske varnosti opravka z masovnimi podatki in obsežnim omrežnim prometom med povezanimi napravami. Da je zaznavanje kibernetskih incidentov in pravočasno odzivanje nanje zahtevna naloga, potrjujejo statistike o povprečnem času, ki preteče od incidenta do trenutka, ko varnostna skupina zazna ta incident, ter do trenutka, ko se nanj odzove. V letu 2021 je povprečni skupni izmerjeni čas 287 dni, od tega 212 dni za zaznavo incidenta in 75 dni za ukrepanje [6]. Poraja se torej ključno vprašanje, ali je količina varnostnih dogodkov in incidentov v računalniških sistemih in omrežjih obvladljiva za varnostne analitike, v kolikor nimajo le-ti na voljo ustrezne, delno ali popolno avtomatizirane tehnološke podpore.

Eden ključnih dejavnikov za obseg, posledice in zapletenost kibernetskih napadov v sodobnih informacijskih okoljih in sistemih je velika odvisnost ljudi, družbe, držav in poslovnih okolij od informacijske tehnologije. To odvisnost narekuje vpetost v koncepte in tehnologije, kot so svetovni splet, oblačne storitve in tehnologije, internet stvari, industrija 4.0, informatizacija in avtomatizacija poslovnih procesov, elektronsko poslovanje, neprekinjeno poslovanje, storitve 24/7, oddaljeno delo in delo od doma, socialna omrežja, vrednost in zaupnost elektronskih osebnih in poslovnih podatkov, kritična infrastruktura idr. To pomeni, da pridobivajo uspešno izvedeni kibernetski napadi za napadalce vse večjo (škodljivo) vrednost. Posledica je porast kibernetskega kriminala, ki prinaša številna kibernetska tveganja in ranljivosti, ki obsegajo finančne izgube, zmanjšano konkurenčnost, zmanjšan tržni delež, sistemske izpade, osebno škodo posameznikov ter v hujših primerih celo širše negativne in neželene socialne, politične in ekonomske učinke. Iz teh razlogov je obravnava kibernetskih groženj, tveganj in vdorov še toliko bolj kompleksna, saj so potencialni napadi vpeti v vsa področja družbe. In sicer se je na različnih nivojih potrebno soočiti z:

- napadi na kritično infrastrukturo in geopolitično motiviranimi napadi, ki so strateškega in političnega pomena ter so bili v preteklosti izvedeni na elektroenergetska omrežja (Ukrajina, ZDA), jedrske elektrarne (Iran, Indija), plinovode, zdravstvene ustanove in drugo infrastrukturo;
- napadi na podjetja in poslovne sisteme, ki predstavljajo gospodarski kriminal in so bili v preteklosti ciljani na številna podjetja, na primer na nemškega proizvajalca koles Canyon, ki posluje na osnovi spletno naravnanega poslovnega modela, zaradi česar je vdor povzročil zamude pri proizvodnji in dobavi ter nedostopnost sistema [2];
- napadi na posameznike.

Preostanek prispevka sestoji iz petih poglavij. V drugem poglavju analiziramo in predstavimo zmožnosti, koncepte, pomen in pridobitve avtomatizacije zaznavanja kibernetskih incidentov in odzivanja nanje. Izpostavimo tudi izzive, težave, omejitve in priložnosti avtomatizacije. V tretjem poglavju opišemo tehnologije SIEM, SOAR in strojnega učenja v povezavi s postopki avtomatizacije zaznavanja in obravnave kibernetskih incidentov. Nato preučimo možnosti zlivanja, integracije in medsebojnega dopolnjevanja teh tehnologij. Četrto poglavje umesti tehnologije in postopke avtomatizacije v kontekst dveh pomembnih samostojnih področij – odzivanja na incidente (*incident response*) ter inteligence kibernetskih groženj in tveganj (*threat intelligence*). Pokazano je, kako lahko avtomatizacija izboljša učinkovitost postopkov v okviru teh dveh področij. V petem poglavju povzamemo, kako se področja avtomatizacije zaznavanja kibernetskih incidentov lotevamo v kompetenčnem centru za kibernetsko varnost za domeno energetike. Prispevek zaključuje šesto, sklepno poglavje.

AVTOMATIZACIJA ODZIVANJA NA KIBERNETSKE INCIDENTE

Zaradi dejstev, omejitev, težav in izzivov, opredeljenih v uvodnem poglavju prispevka, si je nemogoče zamisliti zaznavanje anomalij, varnostnih tveganj in potencialnih kibernetskih incidentov brez pomoči avtomatiziranih pristopov. Ključno vlogo tako dobivajo koncepti in postopki samodejnega zaznavanja kibernetskih incidentov in odzivanja nanje. V zadnjih letih zato stremimo k temu, da bi se odzivanje na kibernetske incidente avtomatiziralo na osnovi algoritmov, strojnega učenja in umetne inteligence, saj tudi napadalci pogosto uporabljajo avtomatizirana orodja za napade, kakršni so na primer napadi DDoS in napadi socialnega inženiringa.

Avtomatizirano odzivanje na kibernetske incidente pomeni, da organizacija dvigne nivo varnosti na podlagi boljših, močnejših in hitrejših ukrepov – algoritmov, strojnega učenja in umetne inteligence – v primeru kibernetskega napada ali druge kršitve varnosti in tako omeji učinek na poslovanje organizacije. Storitve avtomatiziranega odzivanja na incidente postajajo primarne in so bistvene za delovanje organizacij. S pomočjo teh storitev in postopkov lahko razbremenimo varnostno skupino, saj omogočajo samodejno zaznavanje kibernetskih groženj in incidentov ter odziv nanje. Poudariti pa je potrebno, da se kljub avtomatiziranemu procesu kaže zavedati, da je interakcija varnostih strokovnjakov še vedno potrebna.

Glavni namen vpeljave postopkov in tehnologij avtomatiziranega odzivanja na kibernetske incidente je razbremenitev varnostne skupine v organizaciji, kajti praktično nemogoče je spremljati in obdelati tako veliko število podatkov ter sprožiti najustreznejši odziv na vsako grožnjo. S pomočjo umetne inteligence ter zapisanih pravil in procesov, ki se izvajajo v realnem času, sistem zazna incident in nanj nato ustrezno reagira, zaradi česar je interakcija varnostnih strokovnjakov nujna le deloma oziroma v omejenem obsegu. Na podlagi tega se polni baza znanja sistema za nadaljnje ukrepanje ter odpravljanje varnostnih lukenj, s čimer se dvigne nivo varnosti. Tako tudi zmanjšujemo število lažno pozitivnih in lažno negativnih primerov. Ustrezna vpeljava učinkovitih postopkov in tehnologij za samodejno odzivanje na kibernetske incidente lahko doprinese k znižanju stroškov organizacije, čeprav je začetna investicija za avtomatizacijo nekaj večja. Če postopki in tehnologije niso pravilno vpeljani, pa lahko to povzroči škodo organizaciji, bodisi z vidika financ ali varnosti.

Z avtomatizacijo odzivov na kibernetske incidente lahko ukrepamo proti številnim težavam, ki jih prinaša kibernetska varnost v sodobnih kompleksnih informacijskih okoljih in sistemih. Če povzamemo, lahko s temi ukrepi dosežemo mnoge prednosti. Mednje sodijo:

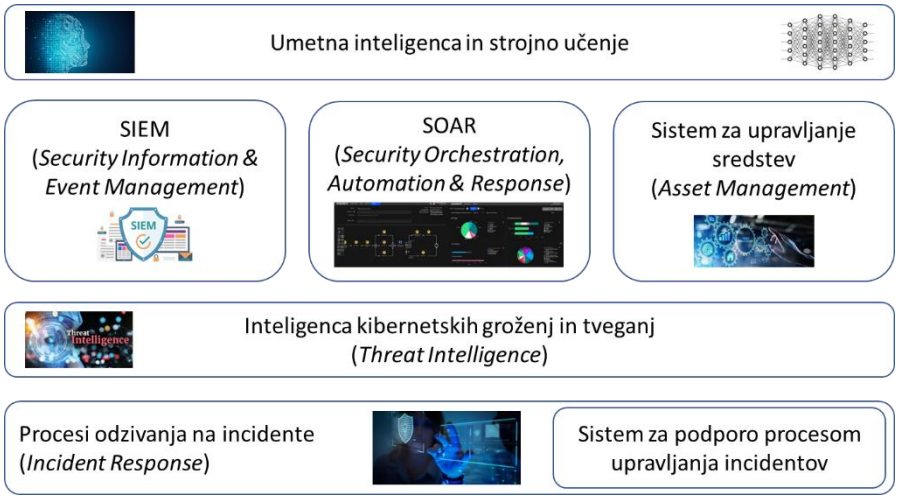
- razbremenitev varnostne skupine ter primarna osredotočenost analitikov na triažo in reševanje zahtevnejših forenzičnih primerov;
- avtomatizacija obravnave enostavnih in ponavljajočih se incidentov;
- povečanje učinkovitosti in uspešnosti procesov zaznavanja in obravnave kibernetskih groženj ter incidentov;
- standardizacija postopkov ukrepanja ob incidentih;
- zmanjšanje deleža lažno pozitivnih in lažno negativnih primerov;
- spremljanje in izboljševanje ključnih indikatorjev in kazalnikov učinkovitosti;
- gradnja in izboljševanje baze znanja o kibernetskih incidentih ter o novih vektorjih in oblikah napadov;
- zmožnost odkrivanja vzorcev v kibernetskih napadih in incidentih;
- poenotena in sistematična integracija informacijskih virov;
- obvladovanje velike množice naprav, virov in varnostnih dogodkov;
- optimizacija področja inteligence kibernetskih groženj in tveganj ter dvig udejanjanja tega področja na višji taktični nivo;
- zmožnost izkazovanja proaktivnosti, kar vključuje zavedanje širše varnostne slike v sistemu in izven njega, predvidevanje varnostnih tveganj in ranljivosti ter ukrepanje ob razpoznanih tveganjih, še preden ta preidejo v napade in incidente;

- boljša komunikacija in poročanje znotraj varnostne skupine.

Popolna avtomatizacija je v določenih primerih neizvedljiva ali neustrezna. Zato je smotrno analizirati in presoditi, kaj je smiselno avtomatizirati in na kateri stopnji. Pri tem je potrebno neodvisno obravnavati vsako fazo procesa zaznavanja kibernetskih incidentov in odzivanja nanje. Stopnjo avtomatizacije določimo za faze priprave, zaznavanja in obveščanja, triaže in analize, omejevanja in nevtralizacije ter aktivnosti po incidentu. Za določitev stopnje lahko uporabimo več metrik, kot so pričakovana korist avtomatizacije, tveganje, učinkovitost, cena ali zgodovina kazalnikov predhodnih avtomatizacij. Praviloma upoštevamo lestvico desetih stopenj avtomatizacije, ki je bila vpeljana že pred nekaj desetletji [14] ter se razteza od prve stopnje popolnega človeškega nadzora do najvišje stopnje računalniškega odločanja. Stopnjo avtomatizacije lahko opišemo tudi po obsegu in po zrelosti. Po obsegu so na najvišjem nivoju avtomatizacije natančno specificirana in zapisana pravila avtomatizacije odziva, npr. v obliki postopka (*playbook*), ki pokrije tudi primere odhoda varnostnih analitikov iz podjetja. Po zrelosti pade pri omejeni avtomatizaciji večina bremena na uporabnika, zaradi česar težimo k pametni avtomatizaciji, ki pokriva triažo in zbiranje podatkov, ali zlasti k zreli avtomatizaciji, ki vključuje avtomatizacijo preiskave, proaktivni lov na grožnje ter napredne tehnike zbiranja in izkoriščanja podatkov.

Avtomatizacija odpira nekaj težav, pasti in izzivov. Prva potencialna težava je efekt »jo-jo«, katerega podlaga je, da je zaradi nerazumevanja razporeditve virov včasih lažje vzpostaviti model kot ga vzdrževati, saj viri niso potrebni le za načrtovanje, implementacijo in testiranje, temveč tudi za kasnejše vzdrževanje. Avtomatizacija se lahko zalomi tudi pri pooblastilih, organizaciji in modelu komuniciranja, zaradi česar je bistvenega pomena podpora vodstva. Ključne pasti in izzivi pa se skrivajo v pravnih in pogodbenih vidikih. To pomeni, da je potrebno nasloviti in pravno regulirati vprašanje krivde in odgovornosti za določene postopke. Kdo je namreč kriv, če zaradi samodejnega odziva sistema pride do izpada oziroma zastoja v produkciji (ker na primer požarni zid prekine vse komunikacije)? Dodatni vidik je dinamična stopnja avtomatizacije. V tem kontekstu lahko sistem zazna stanje in če je varnostna ekipa zasedena, je sam pooblaščen za določena avtomatizirana opravila. Če so analitiki na voljo, pa posreduje sistem le-tem potencialni incident v odločanje, s čimer se stopnja avtomatizacije dinamično zmanjša.

Za avtomatizacijo odzivanja na kibernetske incidente uporabimo sklad povezanih postopkov in tehnologij, ki jih prikazuje slika 1. Osnovni nivo so tehnike umetne inteligence in strojnega učenja, ki so integrirane v tehnologiji SIEM in SOAR. Za učinkovito upravljanje varnostnih dogodokov in omrežnega prometa na povezanih napravah neposredno integriramo tudi sistem za upravljanje sredstev. Te tehnologije nudijo podporo postopkom inteligence kibernetskih groženj in tveganj ter procesom odzivanja na incidente. Vsi gradniki so podrobneje opisani v nadaljevanju prispevka.



Slika 1: Postopki in tehnologije za avtomatizacijo odzivanja na kibernetske incidente

VPELJAVA TEHNOLOGIJ SIEM, SOAR IN STROJNEGA UČENJA

Umetna inteligenca in strojno učenje

Umetna inteligenca lahko olajša in pohitri delo s podatki ter pogosto najde vzorce v masovnih podatkih, ki jih sicer ne bi zasledili ali bi jih bilo možno opaziti le s težavo. Zato jo s pridom uporabljajo tako napadalci na eni strani [7] kot varnostni analitiki v varnostni skupini na drugi strani [13]. Napadalcem omogoča načrtovanje naprednih in zapletenih vektorjev napadov ter samodejno proženje kibernetskih napadov, pri čemer je zmožna:

- identificirati potencialne programske ranljivosti sistemov s skeniranjem le-teh;
- analizirati vzorce obnašanja uporabnikov in delovanja informacijskih sistemov ter v skladu z ugotovljenimi vzorci predvideti uspešne vektorje napadov, npr. prepričljive izsiljevalske napade in socialni inženiring na podlagi značilnosti uporabnikov;
- usmerjati kibernetske napade s posnemanjem poznanih ljudi ali nadrejenega kadra na osnovi generiranja govora, teksta in/ali videa;
- analizirati učinkovitost pristopov in vektorjev napadov ter jih aktivno izboljševati;
- usmerjati omrežje napadalskih računalnikov (*botnet*) v sofisticiranih napadih DDoS.

Hkrati lahko tudi varnostna skupina uporabi metode umetne inteligence in strojnega učenja za razpoznavanje vzorcev običajnega in neobičajnega obnašanja uporabnikov ter delovanja IT sistemov. Ti vzorci opišejo značilnosti kibernetskih napadov, omogočajo zaznavanje anomalij in odstopanj ter pomenijo osnovo za predvidevanje kibernetskih napadov. S tem zagotovijo mehanizme za samodejno odzivanje in ukrepanje. Tako je tudi na strani varnostne ekipe eden osnovnih scenarijev uporabe algoritmov strojnega učenja zaznavanje napadov DDoS [13].

SIEM (Security Information and Event Management)

Sistem za upravljanje varnostnih informacij in dogodkov SIEM [9, 16] zagotavlja celovit prikaz omrežnega prometa varovanega okolja. Omogoča spremljanje varnostnih dogodkov v realnem času ter pregled in analiziranje za nazaj. Analizira dnevniške podatke (*log*) iz različnih sistemov, ki so povezani z njim, na primer aplikacijskih in spletnih strežnikov, strežnikov Linux in Windows, delovnih postaj, podatkovnih baz, aktivnih imenikov, požarnih pregrad,

usmerjevalnikov, avtentikacijskih programov, programov za zaščito pred škodljivo in zlonamerno programsko opremo idr. Ko SIEM zazna potencialno grožnjo, proži opozorilo.

Sistem SIEM ima nekaj omejitev. Omejen je na razpoznavanje incidentov, ki so razvidni iz »logov«, kar pomeni, da ne zna prepoznati oziroma opisati incidentov iz drugih vrst virov (ki niso »logi«). Prav tako ni zmožen orkestrirati postopkov odziva na incidente. Predvsem pa ne povezuje, združuje in selekcionira sorodnih opozoril, zato lahko kot posledica (pre)velikega števila proženih opozoril pride do preobremenitve varnostne ekipe.

Sistem SIEM sestoji iz več gradnikov, ki so shematsko prikazani na sliki 2. Nekateri od njih (ne vsi!) v ozadju aplicirajo strojno logiko in umetno inteligenco ter jih lahko uporabimo za avtomatizirano odzivanje na kibernetske incidente. Eden relevantnejših gradnikov za namen avtomatiziranega odzivanja na kibernetske incidente je analiza vedenja uporabnikov (UBA – *User Behaviour Analytics*), ki razpoznava zlonamerne in tvegane uporabnike, nenavadne in neobičajne aktivnosti uporabnikov ter zlorabe uporabniških računov in pravic dostopa. Prav tako vključuje izračun ocen tveganosti uporabnikov na osnovi dnevniških zapisov njihovih aktivnosti. Naslednji pomembni gradniki so pravila, poizvedbe in referenčne množice, ki na podlagi evidentiranih varnostnih dogodkov in tokov izvedejo neko akcijo, denimo kreiranje opozorila ali incidenta. Dogodki in tokovi predstavljajo omrežni promet, ki ga sistem SIEM pridobiva iz različnih virov. Ker vseh dogodkov in tokov ni možno pregledati, je ključnega pomena avtomatizacija s pravili, ki omogoča samodejno zaznavanje sumljivih ali nevarnih kombinacij le-teh. Bolj ko zapolnimo bazo s pravili, poizvedbami in referenčnimi množicami, tem bolj izpopolnimo ozadje gradnikov, kar zagotavlja boljše in natančnejše delovanje. S tem zmanjšamo število lažno pozitivnih primerov. Pravilno konfigurirani gradniki sistema SIEM imajo velik vpliv na avtomatizirano odzivanje na kibernetske grožnje in incidente.

Slika 2: Gradniki sistema SIEM

SOAR (Security Orchestration, Automation and Response)

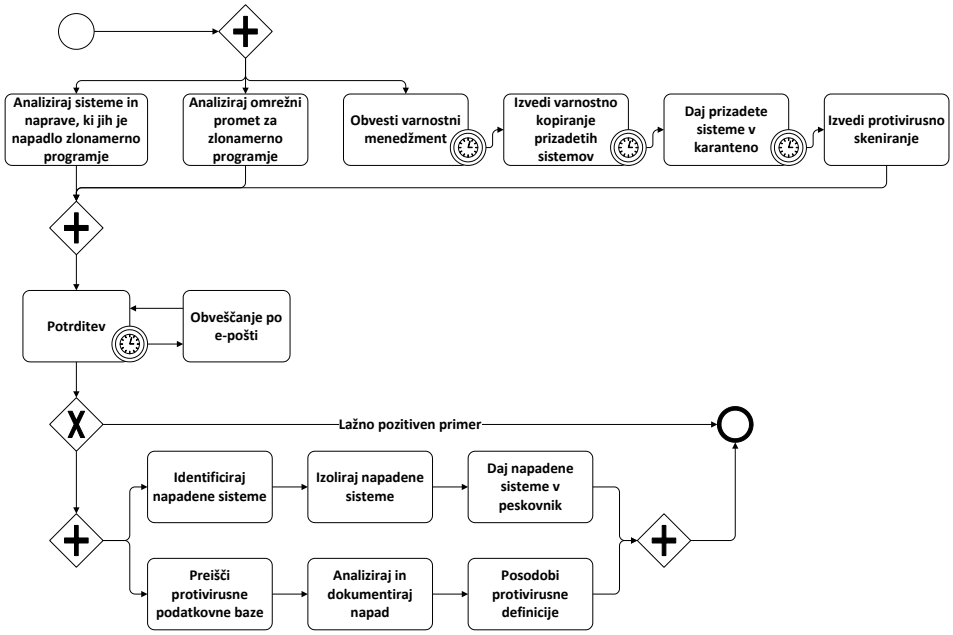
Sistem za varnostno orkestracijo, avtomatizacijo in odzivanje SOAR [4, 15] je enoten sistem oziroma platforma, ki združuje tri ključne funkcionalnosti, in sicer avtomatizacijo varnostnih operacij, odzivanje na varnostne incidente ter upravljanje groženj, tveganj in ranljivosti. Pri tem podpira štirifazni cikel zaznavanja incidentov, triaže, odzivanja in prioretizacije, v okviru katerega omogoča avtomatizacijo ponavljajočih se postopkov odzivanja na varnostne grožnje,

standardizacijo odzivov na incidente ter prihranek časa varnostnega osebja za bolj pomembna in zahtevnejša opravila triaže.

Platforma SOAR je skupek varnostnih orodij in programov za zbiranje in obdelavo podatkov o grožnjah iz množice različnih virov, pri čemer uporabi človeško znanje, umetno inteligenco in strojno učenje z namenom analize podatkov ter prioretizacije aktivnosti v okviru postopkov odzivanja na incidente. Bistvena sta koreliranje in združevanje opozoril o zaznanih incidentih ter definicija odzivov v obliki natančno opisanih postopkov (*playbook*). Primer opisa takšnega postopka odziva v notaciji BPMN je razviden na sliki 3.

Uporabo sistema SOAR lahko ponazorimo na primeru. Ko pride do poskusa vdora v sistem prek požarnega zidu iz nepooblaščenega IP-ja s prijavo po metodi »brute force«, se najprej izvrši samodejna detekcija poskusa vdora, kateri sledijo operacije obveščanja varnostne ekipe, komunikacije s požarnim zidom in nazadnje samodejno blokiranje IP-ja. Podobnih scenarijev uporabe tehnologije SOAR je še nekaj. Med njimi so:

- »Ribarjenje«: Integracija tehnologije SOAR in inteligence groženj skrajša odzivni čas pri iskanju in obdelavi škodljivih informacij, prisotnih v zlonamerni e-pošti.
- Iskanje ranljivosti: Hekerji izkoriščajo ranljivosti za vdor, zato je iskanje ranljivosti ključno za obvladovanje tveganj. SOAR lahko izboljša iskanje in poročanje ranljivosti ter omogoči varnostni ekipi, da vpelje dodatne točke nadzora.
- Zlonamerni omrežni promet: SOAR lahko omogoči samodejno triažo zlonamernega omrežnega prometa na osnovi specifičnih vzorcev in indikatorjev.
- Ponudniki varnostnih storitev: SOAR je na podlagi analiz varnostnih podatkov, metrik in indikatorjev zmožen avtomatizirati ter orkestrirati akcije za zadostitev zahtevam SLA (*Service Level Agreement*).



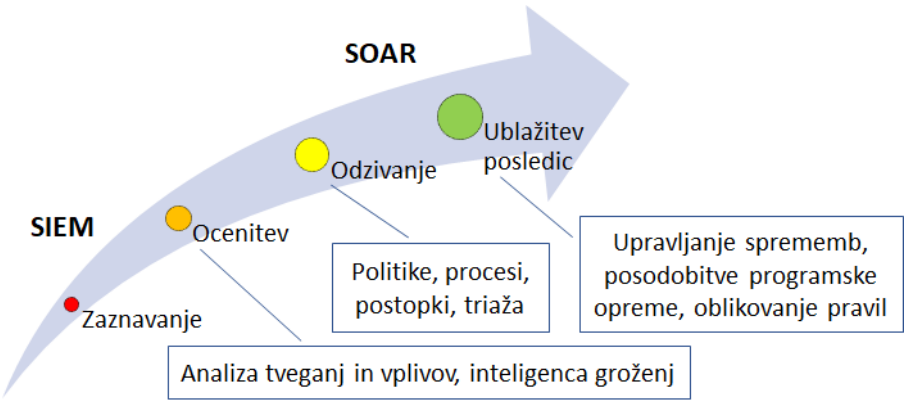
Slika 3: Primer postopka odziva (*playbook*)

Če povzamemo, so ključni koncepti tehnologije SOAR naslednji:

- orkestracija in avtomatizacija: jasno definirani postopki izvajanja varnostnih operacij na osnovi pridobljenih varnostnih podatkov;
- proučevanje groženj in upravljanje primerov: prioretizacija groženj z grupiranjem v skupne tipe/primere glede na sorodne značilnosti in medsebojne korelacije/povezave;
- okolje za varnostni operativni center: pregled opozoril, odzivanje, komunikacija in sodelovanje;
- poročanje in analiza: vpogled v varnostne trende.

Zlivanje tehnologij SIEM in SOAR

Sistem SIEM pomaga pri zaznavanju groženj in incidentov na podlagi podatkov, ki se zbirajo iz aplikacij, sistemov in infrastrukture. Lahko sproži opozorila, vendar mora varnostna ekipa sama poskrbeti za odziv. Tehnologija SOAR pomaga oceniti resnost in lastnosti opozoril na podlagi varnostnih podatkov, se je zmožna samodejno odzvati na grožnje ter sledi aktualnim varnostnim trendom na podlagi inteligentne analize masovnih podatkov. Tehnologija SOAR tako nadgrajuje tehnologijo SIEM, vendar so funkcionalnosti slednje – zbiranje, analiziranje in poročanje o varnostnih dogodkih – še vedno osnova dela varnostnih analitikov in vsakega varnostnega operativnega centra. SIEM in SOAR sta tako komplementarni tehnologiji. SIEM predstavlja osnovo, SOAR pa dvigne učinkovitost varovanja in izkoristek virov na višji nivo, in sicer na podlagi razbremenitve ljudi od varnostnih opozoril, sprostitve kadrov, neposredne integracije različnih orodij na skupni enotni točki ter dobro definiranih procesov odzivanja in ukrepanja. Slika 4 povzema dopolnjujoče se nivoje uporabe tehnologij SIEM in SOAR. V tabeli 1 pa je podana neposredna primerjava glede na osnovne dejavnike [15].



Slika 4: Nivoji uporabe tehnologij SIEM in SOAR

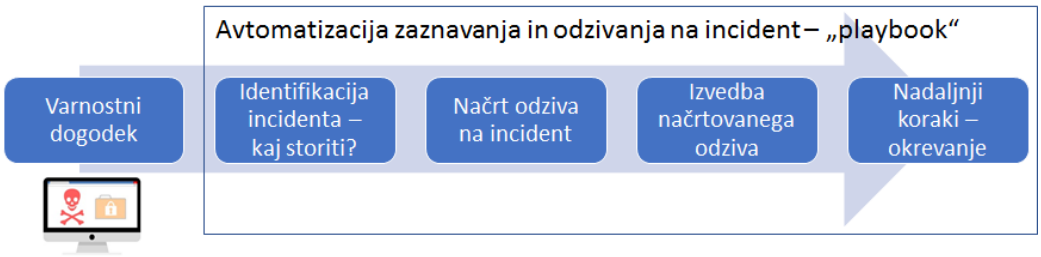
	SIEM	SOAR
Namen	Informacije na osnovi varnostnih dogodkov in dnevniških zapisov	Analiza in inteligenca groženj z uporabo raznovrstnih orodij na enotni platformi (programi za zaščito pred zlonamerno kodo, upravljanje končnih točk, SIEM …)
Zmožnosti	Realnočasovna analiza varnostnih dogodkov	Definicija tokov in postopkov za odzivanje na incidente, standardizacija aktivnosti, izboljšanje sodelovanja
Podatkovni viri	Notranji viri, opozorila	Notranji in zunanji viri, avtomatizacija odzivov na opozorila

Tabela 1: Komplementarnost in primerjava tehnologij SIEM in SOAR

ODZIVANJE NA INCIDENTE IN INTELIGENCA GROŽENJ

Odzivanje na kibernetske incidente

Odzivanje na incidente (*incident response*) je eno temeljnih področij kibernetske varnosti, ki uvaja sistematične pristope k odpravljanju posledic napadov, incidentov in vdorov [3]. Cilj je omejiti posledice kibernetskih napadov, skrajšati čas okrevanja in zmanjšati stroške. V praksi se velikokrat uporabljajo inteligentni pristopi k odzivanju na kibernetske incidente [12]. To pomeni, da proces odzivanja ni omejen zgolj na pripravo načrta odziva in izvedbo tega odziva na osnovi vzpostavljenega načrta, temveč je potrebno v okviru procesa analizirati in celostno razumeti informacije o napadu, identificirati napadalce ter spoznati njihove motive in vzorce delovanja. Za ta namen je ključna avtomatizacija zaznavanja kibernetskih incidentov, zlasti v povezavi s tehnologijo SOAR. Kot kaže slika 5, sta avtomatizacija in tehnologija SOAR tesno vpeti v postopke in procese odzivanja na incidente, katere lahko dvigneta na višji nivo. Zelo smotrno je tudi, da ju integriramo v vse tri stebre vsakega varnostnega operativnega centra, s čimer postaneta eni od bistvenih tehnologij, ključni sestavni del večine varnostnih procesov in dejavnik podpore delu ljudi. Pri tem se morata vklopiti v življenjski cikel delovanja VOC [8].



Slika 5: Uporaba avtomatizacije in tehnologije SOAR v postopku odzivanja na incident

Inteligenca kibernetskih groženj in tveganj

Inteligenca kibernetskih groženj in tveganj (*threat intelligence*) pomeni obdelavo informacij, ki jih organizacija uporabi, da bi razumela, kaj jo ogroža, jo je ali jo bo ogrožalo [1, 11]. Na podlagi teh informacij je organizacija zmožna identificirati tveganja, se pripraviti nanje in jih preprečiti. Pridobi namreč relevantno znanje o tveganjih, vzpostavi obrambne mehanizme in premosti tveganja, ki bi lahko ogrožala vire ter škodila njenemu poslovanju in ugledu.

Rešitve za inteligenco groženj in tveganj zbirajo, filtrirajo in analizirajo podatke o napadih in napadalcih, s katerimi pridemo v stik prek različnih virov in ki ogrožajo vire. Njihovi cilji so:

- biti »na tekočem« z množico groženj in tveganj, kar vključuje tudi metode in vektorje napadov, ranjivosti, cilje napadov in identifikacijo napadalcev;
- postati proaktiven v zvezi z grožnjami in tveganji na podlagi oblikovanja priporočil in postopkov za ukrepanje proti napadom;
- informirati o nedavnih in ponavljajočih se tveganjih ter posledicah za poslovanje.

SOAR in avtomatizacija zaznavanja kibernetskih incidentov predstavljata ključno tehnologijo za inteligenco kibernetskih groženj in tveganj, saj gradita bazo znanja ter avtomatizirata odzive,

s tem pa izboljšata nivo, zmogljivost in učinkovitost inteligence in obveščanja. Na ta način je organizacija zmožna slediti cilju, da se dvigne na čim višjo raven inteligence, najbolj zaželeno na nivo strateške inteligence, ki privede do razumevanja visokonivojskih trendov in motivov napadalcev za namen vzpostavitve strateške kibernetske varnosti in odločanja. S tem se presežeta nivoja taktične inteligence, ki sloni na zajemanju atomarnih indikatorjev groženj ali kompromitiranja (IoC – *Indicators of Compromise*) v obrambnih sistemih, ter operacijska inteligenca, ki je sposobna izvajanja prednostnih in ciljnih varnostnih operacij na podlagi dobrega razumevanja infrastrukture, obrambnih zmožnosti in napadov. To lahko povezujemo z zmožnostjo in zahtevnostjo inteligence groženj, ki na najvišjem strateškem nivoju podpira aktivnosti zaznavanja in raziskovanja notranjih groženj, spremljanja napadalskih kampanij ter zavajanja napadalcev [1].

S pomočjo inteligence kibernetskih groženj okrepimo varnostno ekipo, pridobimo prednosti v zvezi z zaznavanjem groženj in incidentov, odločanjem na podlagi teh groženj in incidentov, odzivanjem ter krepitvijo politik obvladovanja tveganj. Primarno okolje uporabe tehnik in postopkov inteligence kibernetskih groženj je predvsem v varnostnem operativnem centru, kjer z integracijo v sisteme SIEM in SOAR dvignemo nivo varnosti. VOC mora spremljati in identificirati pokazatelje kompromitiranja, kakršni so IP in URL naslovi, domenska imena, registri, definicije DLL idr. Ti pokazatelji lahko razkrijejo nenavaden ali neobičajen omrežni promet, lokacijske nepravilnosti, anomalije v privilegiranih uporabniških računih, povečanje obsega prenosa podatkov iz podatkovnih baz ali prek aplikacijskih programskih vmesnikov in druga varnostna tveganja.

Inteligenca groženj je udejanjena v obliki šestfaznega življenjskega cikla, ki sestoji iz faz specifikacije zahtev, zbiranja informacij, obdelave informacij, analize, razširjanja ugotovitev in povratnih informacij. S časom se učinkovitost procesa inteligence izboljšuje, kar pomeni, da več obdelanih podatkov izboljša celoten varnostni sistem.

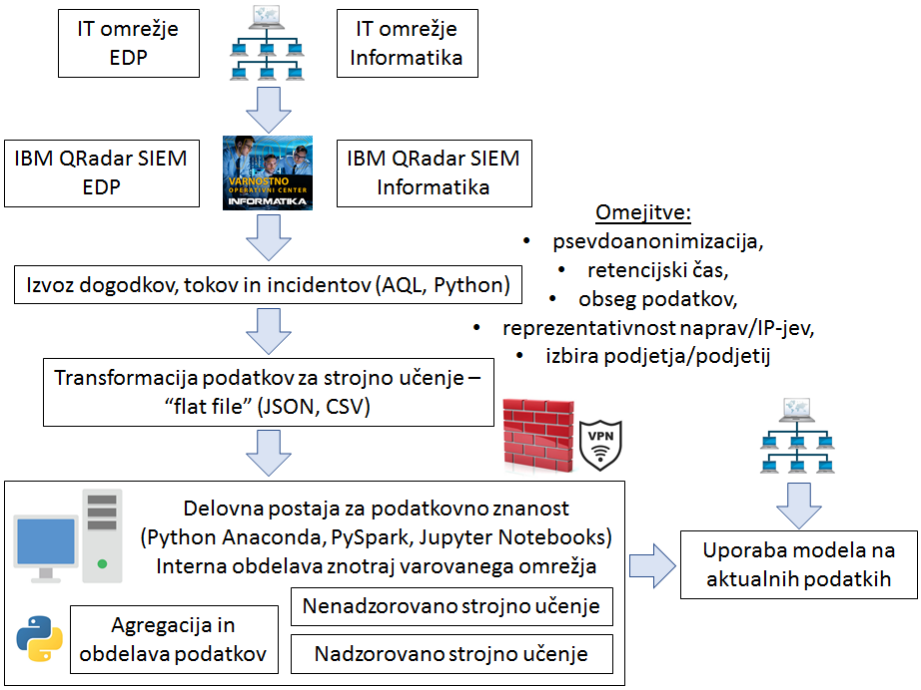
AVTOMATIZACIJA ODZIVANJA V VOC ZA ENERGETIKO

Kompleksni kibernetski sistemi, kakršni so sistemi deležnikov na slovenskem energetskem trgu, so podvrženi veliki množici komunikacijskih dogodkov med povezanimi napravami. Za te dogodke je na neavtomatiziran način ali z omejenim naborom pravil težko ali nemogoče ugotoviti, ali predstavljajo resne oziroma relevantne kibernetske grožnje, napade in incidente, katere je potrebno obravnavati z ustrezno pozornostjo. Za okolje slovenskega energetskega sektorja lahko zato prinese znatno korist izgradnja specifičnih lastnih modelov zaznavanja varnostnih anomalij na osnovi uporabe tehnik umetne inteligence in strojnega učenja. Eden ciljev vsakega modela strojnega učenja je namreč maksimizacija točnosti, kar v kontekstu kibernetske varnosti pomeni minimizacijo lažno pozitivnih in lažno negativnih zaznanih incidentov in napadov. Izkušnje kažejo, da je v ta namen potrebno vsak model pravilno prilagoditi oziroma učiti glede na dejanske podatke in problemsko domeno. Če je model pretreniran (preveč specifičen) ali podtreniran (preveč generičen), ne more zagotoviti popolne uporabnosti. Komercialni izdelki temeljijo na razmeroma splošnih tehnologijah in modelih umetne inteligence za kibernetsko varnost ter so učeni na podatkih iz drugih poslovnih domen in okolij. To pomeni, da so razmeroma generični in ne morejo enako učinkovito pokriti zaznavanja varnostnih incidentov v vseh sistemih. Ker ima slovenski elektroenergetski sektor, tako kot tudi ostali sektorji kritične infrastrukture, svoje specifike, lahko maksimalni učinek in uporabno vrednost dosežemo le z razvojem, raziskovanjem in verifikacijo specifičnih lastnih modelov umetne inteligence in strojnega učenja za kibernetsko varnost.

Podatke, ki se zbirajo v sistemu za upravljanje varnostnih informacij in dogodkov (SIEM) varnostnega operativnega centra za energetiko, uporabljamo kot učne vzorce v procesu strojnega učenja modela umetne inteligence za zaznavanje varnostnih incidentov. Podatki VOC povejo, kateri dogodki in katere kombinacije dogodkov v informacijskem omrežju so nevarne in neželene, so posledica vdorov in napadov ter predstavljajo vir kibernetskih groženj, incidentov in tveganj. Takšen model na osnovi učenja in razpoznavanja vzorcev v zgodovinskih izvoženih podatkih sistema SIEM, ki je vzpostavljen v okviru VOC, pridobi zmožnost posplošenega sklepanja, na podlagi katerega bo v prihodnosti kritične kombinacije dogodkov in tokov v omrežju samodejno in v realnem času napovedal (klasificiral, razvrstil) kot različne tipe incidentov. Postopek strojnega učenja in infrastruktura sta predstavljena na sliki 6. Podrobnejša razlaga je zaradi dolžine prispevka izpuščena. Poudariti pa je potrebno, da sta osnova za izvedbo aktivnosti izgradnje modela strojnega učenja za zaznavanje in odzivanje na kibernetske grožnje pridobljeno soglasje deležnikov na elektroenergetskem trgu za obdelavo podatkov, ki jih VOC zbira s sistemom SIEM, ter podpis ustreznega dogovora o nerazkrivanju informacij.

Modele gradimo na osnovi treh metod strojnega učenja. Te so:

- *časovna vrsta* (nenadzorovano učenje), na osnovi katere iščemo odstopanja (lokalne maksimume/minimume) v primerih incidentov;
- *segmentacija* (nenadzorovano učenje), ki sestoji iz dveh zaporednih korakov, in sicer (1.) iz segmentiranja naprav glede na značilnosti v zgodovinskih učnih podatkih ter (2.) iz segmentiranja naprav v realnem času in ugotavljanja odstopanj v segmentih glede na prvi korak, pri čemer pomeni sprememba potencialni incident;
- *klasifikacija* (nadzorovano učenje), kjer lahko dogodke in tokove klasificiramo v dva razreda (je/ni incident) ali v več razredov, ki določajo vrsto in/ali resnost incidenta.

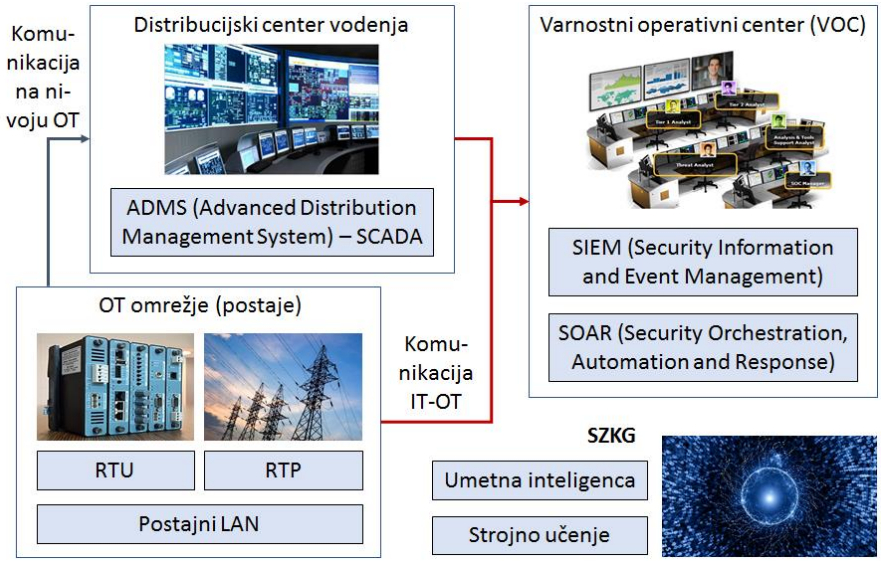


Slika 6: Postopek strojnega učenja in infrastruktura

Za uravnoteženo in učinkovito učenje potrebujemo raznolike IP-je glede na vzorce prometa, IP-je z veliko dogodki/tokovi, IP-je z visokim razmerjem med incidenti in dogodki/tokovi (če v učnih podatkih ni zadostnega deleža izstopajočih vzorcev incidentov, se model ni sposoben naučiti razpoznavanja odklonov, ki predstavljajo potencialne incidente) ter relevantne naprave oziroma IP-je glede na kontekst (podatkovni strežniki, aplikacijski strežniki, delovne postaje, DNS itd.). Pri izvozu in obdelavi podatkov upoštevamo predpisani retencijski čas in ustrezen obseg izvoza glede na metodo strojnega učenja, prostorske omejitve in zahteve posameznih deležnikov v VOC. Obdobje in obseg izvoza se tako za nadzorovano in nenadzorovano učenje razlikujeta. Podatki za strojno učenje so zajeti v treh skupinah:

- *dogodki:* domena, izvorni IP naslov vira, vrata izvora, ciljni IP naslov vira, vrata cilja, uporabnik, visokonivojska kategorija, nižjenivojska kategorija, naziv dogodka, opis dogodka, število združenih dogodkov, čas dogodka;
- *tokovi:* domena, izvorni IP naslov vira, vrata izvora, ciljni IP naslov vira, vrata cilja, vrsta toka, čas prvega paketa, čas shranjevanja posameznega paketa, število zlogov na izvoru, število prejetih zlogov na cilju, skupno število zlogov, število posredovanih paketov na izvoru, število prejetih paketov na cilju, skupno število paketov, protokol, vrsta aplikacije;
- *incidenti:* ID, domena, izvorni IP naslovi virov, ciljni IP naslovi virov, opis incidenta, vrsta incidenta, vrsta vira incidenta, začetni čas prvega dogodka/toka v incidentu, čas zadnjega dogodka/toka v incidentu.

Osnovni, trenutno podprti nivo zaznavanja kibernetskih incidentov je nivo IT omrežja, kjer deluje VOC. Kasneje bo potrebno zaznavanje in odzivanje pokriti na vseh IT-OT integriranih nivojih kritične infrastrukture, to je od najnižjega nivoja OT omrežja, prek vmesnega nivoja distribucijskega centra vodenja, do najvišjega nivoja IT omrežja. Med temi nivoji potekajo vertikalne povezave, saj lahko pride do varnostnih incidentov na kateremkoli od njih. Koncept zaznavanja in odzivanja na varnostne incidente v IT-OT integrirani kritični infrastrukturi za področje elektroenergetike je ponazorjen na sliki 7.



Slika 7: Zaznavanje varnostnih incidentov v elektroenergetski kritični infrastrukturi

SKLEP

Kot posledico vpetosti informacijskih tehnologij v vsakodnevno življenje, poslovanje podjetij in celotno družbo, velikih količin omrežnega prometa in varnostnih podatkov, velikega števila medsebojno povezanih naprav ter obsega in resnosti kibernetskih incidentov si ne moremo zamisliti zaznavanja anomalij, varnostnih tveganj in potencialnih kibernetskih incidentov brez avtomatiziranih pristopov. Ključne so zlasti tehnologije SIEM in SOAR ter tehnike strojnega učenja in umetne inteligence. Z njimi lahko povečamo učinkovitost in uspešnost zaznavanja groženj in incidentov, zmanjšamo število lažno negativnih in lažno pozitivnih primerov, gradimo znanje o novih oblikah in vektorjih napadov ter razbremenimo varnostne analitike reševanja preprostih in ponavljajočih se problemov, na podlagi česar so se analitiki zmožni prednostno posvetiti zahtevnejšemu forenzičnemu delu in triaži. Avtomatizacija zaznavanja incidentov je tudi osnova za proces samodejnega odzivanja na incidente, ki poskrbi, da celovito odpravimo vzroke in posledice incidenta, blokiramo nadaljnje napade, zagotovimo neprekinjeno delovanje sistema, upravljamo infrastrukturne vire ter spremljamo in izboljšamo ključne indikatorje učinkovitosti. Takšen pristop dodatno optimizira proces inteligence tveganj, katerega dvigne na višji taktični nivo. To pomeni, da se zavedamo širše varnostne slike v našem sistemu, na spletu ter z vidika aktualnih motivov, taktik in vektorjev vdorov napadalcev. Postanemo lahko bolj proaktivni, s čimer smo zmožni o varnostnih problemih, tveganjih in ranljivostih razmišljati vnaprej ter nismo omejeni zgolj na tiste od njih, ki se dejansko zgodijo. Ob zaznanih tveganjih na ta način pravilno in pravočasno ukrepamo, še preden preidejo v napade in incidente.

Prispevek je povezal različne dejavnike avtomatizacije zaznavanja kibernetskih incidentov in odzivanja nanje. Pojasnil je sinergijo posameznih tehnologij in pristopov. Podal je smernice in dobre prakse njihove vpeljave ter uporabe v različnih okoljih, zlasti v varnostnih operativnih centrih. Predstavil je lasten pristop k avtomatizaciji, ki ga na osnovi metod strojnega učenja vpeljujemo v sklopu razvojno-raziskovalnega projekta, ki je v teku.

VIRI IN LITERATURA

[1] BAKER, Curt: What is cyber threat intelligence?, Crowdstrike, 18. 2. 2021.

[2] BRACELY, James: Canyon targeted by cyber attack: Massive criminal cyber attack targets Canyon's online business, Cycling Weekley, 6. 1. 2020.

[3] CHAI, Wesely, BEAVER, Kevin, ROSENCRANCE, Linda: Incident response, TechTarget, 2020.

[4] FIREEYE: What is SOAR? Definition and Benefits, 2021, fireeye.com/products/helix/what-is-soar.html.

[5] FREEDMAN, Linn F.: Ransomware attacks predicted to occur every 11 seconds in 2021 with a cost of $20 billion, National Law Review, 13. 2. 2020, let. 10, št. 44.

[6] IBM Report: Cost of a data breach hits record high during pandemic, IBM Newsroom, 28. 7. 2021, newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic.

[7] JEFFERSON, Brian: The 15 most common types of cyber attacks, Lepide, Data Security & Compliance Blog, 8. 6. 2021, lepide.com/blog/the-15-most-common-types-of-cyber-attacks.

[8] KAFOL, Ciril, BREGAR, Andrej: Cyber security – building a sustainable protection, DAAAM International Scientific Book 2017, DAAAM International Vienna, str. 81–90, 2017.

[9] MILLER, David R. idr.: Security Information and Event Management (SIEM) Implementation, McGraw-Hill, 2011.

[10] MORGAN, Steve: Cybercrime to cost the world $10.5 trillion annually by 2025, Cybercrime Magazine, 13. 11. 2020.

[11] PACE, Chris: The threat intelligence handbook, CyberEdge Press, 2018.

[12] ROBERTS, Scott J.: Intelligence-driven incident response: Outwitting the adversary, O'Reilly Media, 2017.

[13] SAINI, P. S., BEHAL, S., BHATIA, S.: Detection of DDoS attacks using machine learning algorithms, 7th International Conference on Computing for Sustainable Global Development, 2020, str. 16–21.

[14] SHERIDAN, Thomas B., VERPLANK, William L.: Human and computer control of undersea teleoperators, Massachusetts Institute of Technology, 1978.

[15] SIEMPLIFY: What is SOAR – Security Orchestration & Automation, 2021, siemplify.co/resources/what-is-soar-security-orchestration-automation.

[16] THOMAS, Arun E.: Security operations center – SIEM use cases and cyber threat intelligence, 2018.