Uvođenje sigurnosnog operacijskog centra za zaštitu poslovanja srednje velike tvrtke

Hitrec, Igor

SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA
POSLIJEDIPLOMSKI SPECIJALISTIČKI STUDIJ INFORMACIJSKA SIGURNOST

ZAVRŠNI SPECIJALISTIČKI RAD

UVOĐENJE SIGURNOSNOG OPERACIJSKOG CENTRA ZA ZAŠTITU POSLOVANJA SREDNJE VELIKE TVRTKE

Igor Hitrec

Zagreb, svibanj 2021

Mentor: Doc.dr.sc. Stjepan Groš, ZEMRIS
Rad ima 40 stranica
Završni rad br.:

Povjerenstvo za ocjenu u sastavu:

1. Izv. prof. dr. sc. Miljenko Mikuc - predsjednik
2. Doc. dr. sc. Stjepan Groš - mentor
3. Izv. prof. dr. sc. Renata Mekovec, Sveučilište u Zagrebu Fakultet organizacije i informatike – članica.

Povjerenstvo za obranu u sastavu:

1. Izv. prof. dr. sc. Miljenko Mikuc - predsjednik
2. Doc. dr. sc. Stjepan Groš - mentor
3. Izv. prof. dr. sc. Renata Mekovec, Sveučilište u Zagrebu Fakultet organizacije i informatike – članica.

Datum obrane: 20. prosinca 2021.

Sadržaj

1. Uvod

Današnji načini poslovanja i isporuke usluga i roba u potpunosti koriste prednosti interneta u komunikaciji sa kupcima, dobavljačima marketinških i pravnih usluga, usluga transporta, globalno dostupne udaljene radne snage i računalnih resursa u oblaku. Ovakva dostupnost i povezanost uz stalno povećanje koristi i konkurentnosti sa sobom nosi i stalno povećavanje prijetnji koje traže odgovarajuću zaštitu. Države prepoznaju ovakve rizike i pojačanim regulatornim zahtjevima potiču da se kibernetičkoj sigurnosti pristupa na odgovarajući način.

Odgovoriti na rizike kibernetičke sigurnosti unutar kompleksnih proizvodnih i poslovnih IT sustava moguće je uspostavom centraliziranog nadzora svih njihovih dijelova. Zbog složenosti i povezanosti različitih poslovnih i upravljačkih sustava centralizirani sigurnosni nadzor olakšat će i ubrzati postupke odgovora na incidente i postupke oporavka. Također, centralizirano praćenje sigurnosnih događaja svih nadziranih sustava i primijenjenih sigurnosnih kontrola omogućuje bolje razumijevanje sigurnosnog incidenta uz brži i efikasniji odgovor, stoga se zadaća nadzora i odgovora na incidente obično organizira uvođenjem sigurnosno operacijskog centra.

Rad je strukturiran na način da će prvo opisati što je to sigurnosno operacijski centar, kako na odgovarao na sigurnosne zahtjeve nekad i danas. Potom će se opisati postupak uvođenja sigurnosno operacijskog centra (SOC) na primjeru jedne srednje velike tvrtke koja želi uspostavom SOC-a nadzirati i štititi svoju proizvodnu i poslovnu imovinu, te osigurati pravodoban odgovor na sve incidente iz domene informacijske sigurnosti. Opisat će se postupak određivanja zadaća SOC-a sukladno poslovnim zahtjevima tvrtke, prepoznatim rizicima i zahtjevima informacijske sigurnosti. Potom će se opisati postupak određivanja operativnog modela i arhitekture, potrebnih ljudskih resursa, tehnoloških rješenja i procesa SOC-a. Na kraju će se opisati način mjerenja učinkovitosti, sa ciljem stalnog unaprijeđena njegovih funkcija.

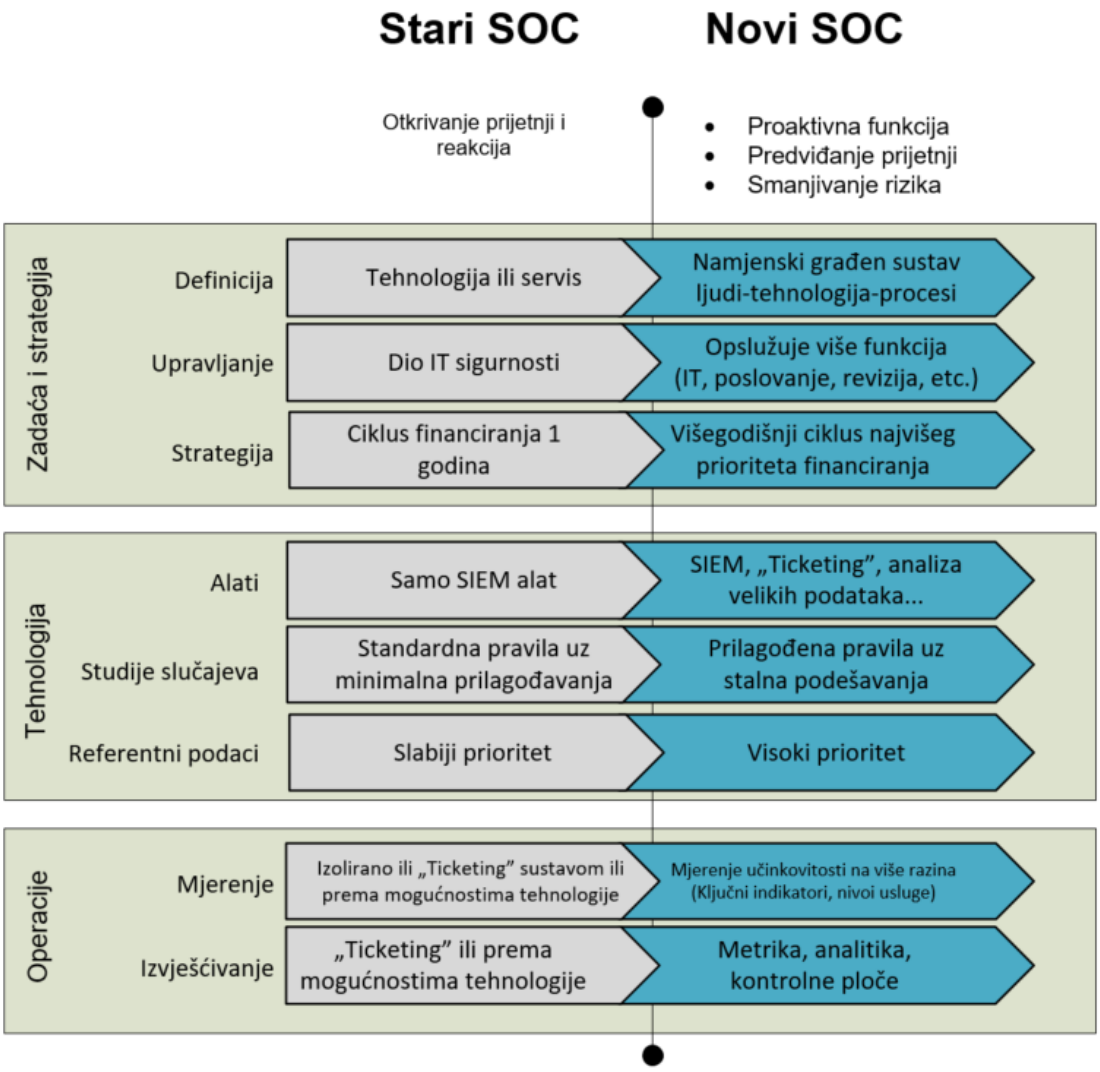
2. O Sigurnosno operacijskom centru

Sigurnosni operacijski centar (*engl. Security operation centre, SOC*) tim je vrhunski osposobljenih ljudi koji primjenom odgovarajućih tehnologija i razvijenih procesa [1] štite kritične podatke i kritičnu informacijsku imovinu, pripremaju i provode odgovore na incidente iz domene kibernetičke sigurnosti, pomažu kod osiguranja kontinuiteta poslovanja i oporavka nakon incidenta i dodatno utvrđuju zaštitu poslovne informacijske infrastrukture. Sa tom svrhom SOC provodi zadaće nadzora, analize, korelacije i eskalacija sigurnosnih događaja, razvija odgovarajuće postupke odgovora na sigurnosne događaje (zaštita, detekcija, odgovor), upravlja procesima odgovora na incidente i forenzičke istrage, surađuje sa ostalim vanjskim dionicima iz domene informacijske sigurnosti. SOC pomaže u kriznim situacijama, prati stanja sigurnosti u stvarnom vremenu, upravljanja informacijama vanjskih dojava o prijetnjama i njihovom mogućem utjecaju na organizaciju koja se štiti.

Slika 2.1 opisuje „Stari SOC“ kao početak centraliziranog nadzora i odgovora na incidente iz područja IT sigurnosti, korištenjem prvih inačica sustava za nadzor sigurnosnih informacija i događaja (*engl. Security Information and Event Management, SIEM*). SIEM bi se financirao zajedno sa svim ostalim IT alatima, rijetko bi imao na raspolaganju osoblje zaduženo isključivo za njegovu administraciju, a podešavanja i prilagođavanja ugrađenih postavki bila bi svedena na najmanju moguću mjeru. Podaci, sistemski zapisi nadziranih sustava za SIEM isporučivali bi se prema slabijem prioritetu i nerijetko bi bili nedostupni. Mjerenje učinkovitosti ovakvih sustava svodilo bi se samo na korištenje već ugrađenih SIEM izvješća. Ovako koncipiran SOC mogao je služiti otkrivanju prijetnji i intervenciji u slučaju incidenta.

Razvoj novih poslovnih modela i tehnologija, mobilni uređaji, servisi u oblaku, integracije sa servisima trećih korisnika, potreba zaštite osobnih podataka, povećanje internetskih prijetnji i stroži regulatorni zahtjevi postavljaju veće izazove pred ovakav SOC koji, zbog obima poslova, mora imati višestruku funkciju, što zahtijeva više vremena i financijskih sredstava.

Današnji novi SOC uz SIEM koristi još cijeli niz drugih alata, jer se mora prikupljati i analizirati velika količina podataka. Potom, studije slučajeva detekcije i borbe protiv prijetnji puno su složenije i zahtijevaju kvalitetna mjerenja učinkovitosti.



Slika 2.1 SOC nekad i danas [2]

Upravljanje informacijskom sigurnošću pred moderan SOC postavlja zahtjeve za ljudima, tehnologijom i procesima. MITRE dokument „*Ten Strategies of a World-Class Cybersecurity Operations Center*" [3] opisuje deset smjernica dobre strategije uvođenja SOC-a:

1) Konsolidirati i centralizirati upravljanje računalnom i mrežnom sigurnošću. Konsolidacija i centralizacija omogućuje da sa jednoga mjesta organiziramo:
   - nadzor i trijažu u realnom vremenu, analizu incidenta i koordinirani odgovor na incidente;
   - prikupljanje i analizu podataka o dojavama na prijetnje;
   - upravljanje senzorima, njihovo podešavanje i integraciju sa SOC infrastrukturom.

2) Postići ravnotežu između količine nadziranih sustava i brzine obrade, jer ćemo tako:
   - znati odabrati organizacijski model SOC-a;
   - odrediti uloge SOC-a, način upravljanja i zapovjednu strukturu;
   - znati odrediti lokaciju SOC-a i način kako koordinirati njegovu aktivnost.
3) Ovlastiti SOC da uspješno izvršava svoju zadaću, na način da SOC odgovara Voditelju IT službe ili Voditelju informacijske sigurnosti. U prvom slučaju SOC može imati dobru komunikaciju sa IT odjelom i od početka osigurati kvalitetnu integraciju i dobru vidljivost. Mogući problem u ovom slučaju jeste zajednički budžet u kojem SOC nije dovoljno zastupljen. U drugom slučaju, SOC može lakše računati na kvalitetniju podršku upravljačkih struktura i bolji budžet, ali i rizik od negativnog shvaćanja sigurnosti i sukladnosti kao opterećenja u poslovanju.

4) Izvršavati manje zadataka, ali na kvalitetan način, jer SOC, ovisno o definiranim zadaćama i svojim kapacitetima, može, ali i ne mora, u potpunosti brinuti o alatima za procjenu ranjivosti sustava, održavanju senzora na krajnjim točkama, penetracijskim testiranjima ili samoj primjeni protumjera na sustavima za aktivnu obranu (vatrozidovi, sustavi zaštite krajnje točke itd.).

5) Promicati kompetencije umjesto većeg boja uposlenih, jer za SOC treba odabrati stručnjake koji, uz znanja, imaju i odgovarajuću sposobnost kritičkog razmišljanja. Ovakve stručnjake je potrebno pronaći, zaposliti u odgovarajućem broju i truditi se zadržati ih.

6) Maksimalno iskoristiti tehnologiju koja je na raspolaganju i svakako primijeniti: alate za provjeru ranjivosti i praćenje imovine na računalnoj mreži, mrežne sustave za detekciju i prevenciju upada, alate za kontrolu toka mrežnog prometa, snimanje i analizu mrežnog prometa, sustava za detekciju i prevenciju upada na krajnjim točkama, anti-malver rješenja i nadzor promjena u konfiguraciji sustava. Također, središnje mjesto prikupljanja ovih informacija mora biti sustav za nadzor sigurnosnih informacija i događaja (SIEM) i prikupljanje i analizu svih sistemskih zapisa.

7) Procijeniti koji su podaci potrebni SOC-u i osigurati maksimalno moguću vidljivost nadzirane infrastrukture. Za dio gdje je vidljivost teže postići potrebno je planirati i primjenjivati dodatna rješenja sukladno analizi rizika. Osim vidljivosti, problem SOC-a jest i prijem nedovoljno kvalitetnih i nepotpunih podataka. Oba slučaja zahtijevaju stalnu brigu i poboljšanja. Naglasak treba staviti na zaštitu informacija sukladno njihovoj vrijednosti, dakle klasifikaciji, što će postaviti prioritete u zadaćama SOC-a.

8) Štititi podatke o sposobnostima SOC-a jer protivnik ne smije znati na koji način funkcionira nadzor i zaštita sustava kojeg želi napasti. Stoga se tehničke i operativne sposobnosti SOC-a moraju tretirati kao povjerljive informacije. Gdje god je to moguće, potrebno je osigurati čim manju vidljivost senzora nadzora, strogu izolaciju i nadzor SOC okruženja.

9) Koristiti i sudjelovati u procesu dojava o prijetnjama i graditi unutarnje kapacitete za detekciju naprednih upornih prijetnji pomoću modeliranja prijetnji i lova na prijetnje. Idealno, zreli SOC kvalitetno rješava regularne incidente automatizacijom ili uz minimalan angažman ljudskih resursa, dok su isti koncentrirani na pretrage ranjivosti i provjeru mogućih scenarija vezanih za moguće prijetnje. Važno je razviti vlastiti sustav za dojavu o mogućim prijetnjama i, po mogućnosti, to znanje dijeliti sa ostalim čimbenicima izvan tvrtke, dok istovremeno treba koristiti razne izvore dojave o sigurnosnim prijetnjama.

10) „Stani. Razmisli. Odgovori... Mirno“ je najbolji i provjereni način odgovora na sigurnosni incident koji zahtjeva da SOC tim, osim tehničkog i analitičkog znanja, ima razvijene i komunikacijske sposobnosti. Izuzetno je važno da SOC također ima pripremljene protokole za obradu raznih vrsta incidenata, te opisan i izvježban proces komuniciranja sa svim zainteresiranim stranama. Kod postupka rješavanja incidenata nema mjesta panici, preranim zaključcima i optužbama bez pokrića. Svaki ozbiljan incident mora biti temeljito istražen, objašnjen zainteresiranim stranama na jednostavan i razumljiv način uz informaciju o mogućim rizicima, počinjenoj šteti i načinima oporavka.

Isti MITRE-ov dokument (stranica 51.) opisuje pet različitih predložaka veličine SOC-a, opisanih u Tablici 2.1 i podijeljenih obzirom na veličinu nadzirne infrastrukture, postavljene zadaće postavljene pred SOC i dostignute vidljivosti nadzirane infrastrukture.

Tablica 2.1 Pet različitih predložaka veličine SOC-a

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

Gartnerov dokument „The Five Models of Security Operation Centers“ [4] opisuje pet operativnih modela SOC-a, opisanih u Tablici 2.2. Gartnerova podjela naglašava razlike u zadaćama SOCa obzirom na zahtjeve radnog vremena i namjenski angažiranog osoblja. I MITREov i Gartnerov model će se razmatrati pri određivanju ACME SOC operativnog modela sukladno zahtjevima informacijske sigurnosti.

Tablica 2.2 Operativni modeli SOC-a prema Gartneru

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

Ove su smjernice korisne u izradi operativnog modela SOC-a za pojedinu organizaciju.

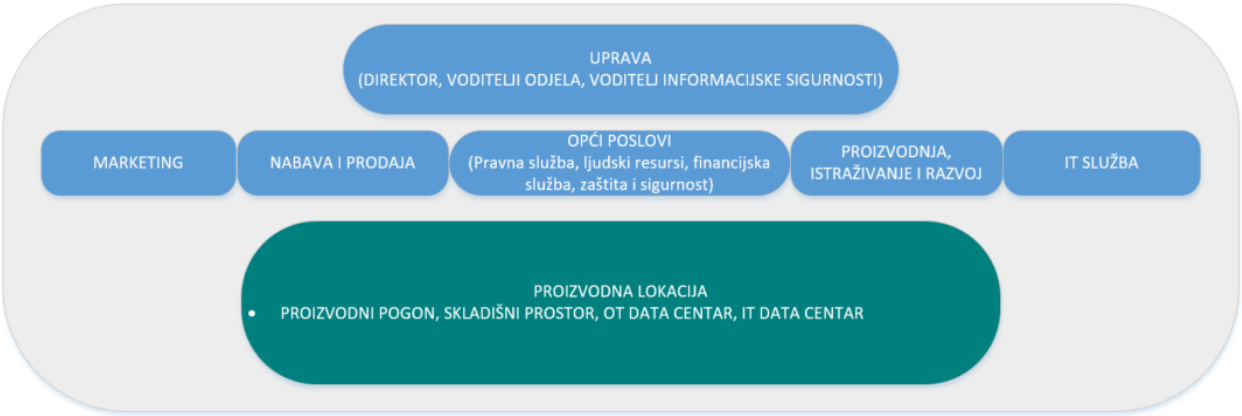
3. Uvođenje sigurnosnog operacijskog centra

Postupak uvođenja sigurnosnog operacijskog centra prikazat ćemo na primjeru tvrtke ACME (Slika 3.1). ACME proizvodi raznovrsne zaštitne premaze, boje i lakove za industrijsku primjenu u energetici, infrastrukturnim projektima, građevini i brodogradnji. Svoje proizvode plasira na tržište zemalja Europske Unije.

3.1 Tvrtka ACME

ACME posjeduje proizvodni pogon i poslovnu zgradu unutar zajedničkog poslovnog kompleksa. Poslovni dio tvrtke sastoji se od odjela marketinga, nabave sirovina i prodaje gotovih proizvoda, općih poslova (pravne službe, upravljanja ljudskim resursima, financija, zaštite i sigurnosti), odjel istraživanja i razvoja te odjela IT podrške. Ukupno jedna četvrtina djelatnika tvrtke radi na poslovima proizvodnje, dok je ostali dio djelatnika zaposlen u poslovnom dijelu tvrtke. Proizvodni proces podržan je modernom proizvodnom tehnologijom i upravljačkim sustavom (*engl. Operations technology, OT*). Uz proizvodni pogon nalazi se odgovarajući skladišni prostor za proizvodne sirovine, gotove proizvode te potrebna infrastruktura za utovar i istovar kamionskim prijevozom.

Organizacijska shema prikazana je u Slici 3.1.



Slika 3.1 Organizacijska shema tvrtke ACME

I proizvodni i poslovni dio tvrtke u potpunosti su digitalizirani, a udio ne-digitalizirane informacijske imovine vrlo je nizak. Stalna poboljšanja izvode se na dijelu IT sustava podrške narudžbi sirovina i prodaje gotovih proizvoda, financija, odjela istraživanja i IT podrške. IT oprema poslovnih sustava redovito se obnavlja i nadograđuje.

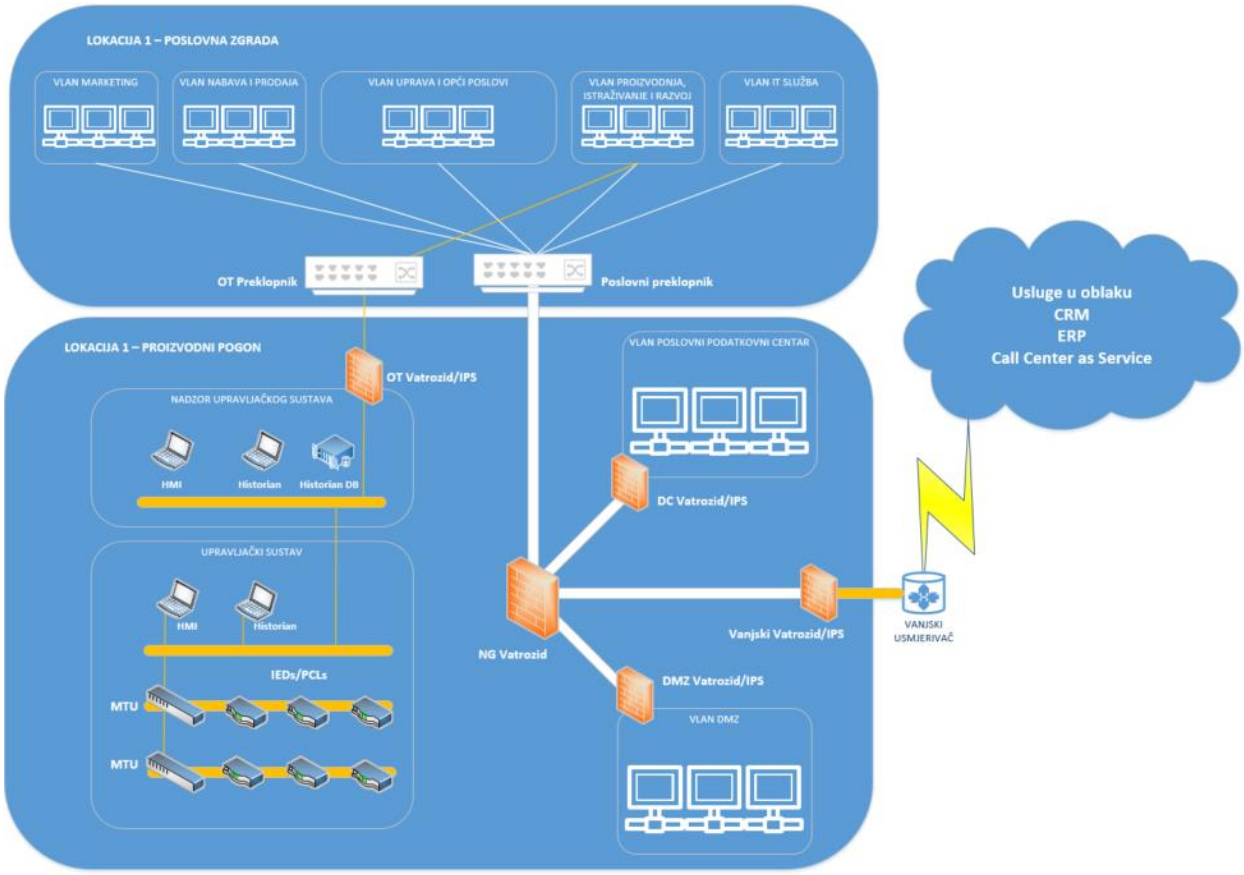
Odjeli poslovnog dijela tvrtke, prema Slici 3.2, odijeljeni su posebnim virtualnim mrežama i preko preklopnika i glavnog vatrozida (NG Vatrozid) koriste servise poslovnog podatkovnog centra. Poslovni podatkovni centar udomljava poslužitelje unutarnjih servisa podrške poslovanju, elektroničku poštu i sustave zaštite elektroničke pošte, podatkovno skladište nestrukturiranih podataka i poslužitelje sa bazama podataka. Podatkovni centar štiti DC vatrozid i integrirani sustav detekcije i prevencije upada.

DMZ virtualna mreža udomljuje servise posredničkog sustava za pristup javnom web sadržaju (*engl. web proxy*), virtualne radne okoline za udaljeni rad (*engl. virtual desktop*) i web servise tvrtke koji moraju biti dostupni preko interneta. DMZ je zaštićen DMZ vatrozidom i integriranim sustavom detekcije i prevencije upada. Direktni mrežni promet između tvrtke i interneta

provjerava se pomoću NG vatrozida, vanjskog vatrozida i integriranog sustava detekcije i prevencije upada.

Upravljački sustav proizvodnje i njegov nadzorni dio u potpunosti je izoliran od poslovnog dijela tvrtke OT vatrozidom. Ograničeni pristup dozvoljen je jedino Odijelu proizvodnje, istraživanja i razvoja.

Tvrtka koristi servise usluga trećih strana u oblaku: sustav za odnose sa kupcima i dobavljačima (*engl. Customer Relationship Management, CRM*), sustava za upravljanje resursima tvrtke (*engl. Enterprise Resouce Planning, ERP*), te sustav za podršku kontaktnom centru (*engl. Contact Center as a Service, CCaaS*). Hardverska infrastruktura upravljačkog sustava zasebna je za svaku lokaciju i odgovarajuće udomljena unutar proizvodnih pogona.



Slika 3.2 Funkcionalna shema IT i OT infrastrukture ACME tvrtke

Tvrtka dobro posluje i želi proširiti svoje proizvodne i poslovne kapacitete kako bi odgovorila zahtjevima tržišta. Glavne proizvodne sirovine osjetljivi su kemijski spojevi za koji imaju stroge procesne i proizvodne zahtjeve i kod čijeg rukovanja je potrebno strogo poštivati pravila zaštite zdravlja i zaštite od požara. Stoga je provedena analiza rizika postojeće informacijske imovine kako bi se, uz ostalo, utvrdile potrebe nadogradnje postojeće infrastrukture i osigurala primjena svih zaštitnih kontrola propisanih zakonom.

Uskladištenje i transport također moraju biti sukladni ovim zahtjevima. Uz fizičku zaštitu, zaštitu od požara i zaštitu na radu utvrđeni su rizici i proizvodnje i poslovanja povezani sa povjerljivošću, cjelovitošću i dostupnosti poslovnih i proizvodnih informacija. Utvrđeno je da dosadašnji nadzor upravljačkog sustava kojeg je provodio Odjel za proizvodnju, razvoj, istraživanje i razvoj nije sukladan očekivanim poslovnim zahtjevima. Problemi u proizvodnji moraju biti brže otkriveni i brže riješeni. Planirano proširenje proizvodnje zahtijevat će uvođenje novih elemenata

upravljačkog sustava čiji nadzor i zaštita neće biti moguća postojećom organizacijom poslovnih procesa.

IT služba upravlja i održava cjelokupnu IT imovinu tvrtke i mora odgovoriti izazovima zaštite IT imovine. Prepoznati su rizici sustava u računalnom oblaku, rizici korištenja mobilnih uređaja (mobilni telefoni, prijenosna računala) i rizici za cijelu informacijsku imovinu, a zbog nedostatka kontrola zaštite upravljačkog sustava od malicioznog računalnog koda . Odlučeno je stoga da se u tvrtki organizira sigurnosno operacijski centar (*engl. Security operations centre, SOC*) koji će na jednom mjestu objediniti zadaću nadzora informacijske imovine upravljačkog i poslovnog sustava.

3.2. Odabir operativnog modela

Uprava tvrtke odredila je zadaće koje SOC mora ispunjavati:
- odgovarati na prijetnje i rizike koje ugrožavaju povjerljivost, cjelovitost i dostupnost informacija,
- osigurati Upravi upravljanje i kontrolu informacija,
- osigurati i prikazati sukladnost sa regulativama propisanim zaštitnim standardima i zakonima,
- zaštititi intelektualno vlasništvo i privatnost osobnih podataka kojima tvrtka upravlja,
- efikasno upravljati sigurnosnim operacijama,
- osigurati stalan uvid u sigurnosno stanje tvrtke,
- pratiti sigurnosne dojave, procjenjivati mogući učinak novih prijetnji i pro aktivno štititi tvrtku,
- omogućiti tvrtki vidljivost i transparentnost korištenja informacijske imovine kako se u svakom trenutku može utvrditi tko je što radio, i kada, i za to osigurati odgovarajuće dokaze.

Dakle, potrebno je procijeniti operacijski model SOC koji će odgovarati potrebama ACME tvrtke. Da bi se sve gore navedeno postiglo, ACME SOC-u potrebni su odgovarajući ljudi, razvijeni procesi i kvalitetna tehnologija organizirana unutar prostora koji odgovara sigurnosnim zahtjevima fizičke zaštite kontrole pristupa zbog zaštite zdravlja i zaštite od požara.

Potrebno je procjeniti koje funkcije unutar tvrtke moraju biti pokrivene nadzorom iz SOC-a.
Učinkovit SOC znači imati učinkovit tim analitičara koji mora odgovoriti zadatku nadzora i odgovora na incidente u uvjetima IT/OT okruženja ovisno o broju korisnika i uređaja od kojih se sastoje. Za tvrtku ACME napravili smo predložak malog SOC-a i prilagodili zahtjevima informacijske sigurnosti, kako je prikazano u Tablici 3.1.

Tablica 3.1 Opis odabranog rješenja za ACME SOC

Zahtjevi tvrtke ACME	odgovaraju MITRE predlošku [1]	kod opisa	i u detaljima MITRE predloška
ACME preferira strogo centralizirani SOC za podršku i poslovnog i upravljačkog sustava	**Veliki SOC**	organizacijskog modela	Interno centraliziran SOC sa elementima distribuiranog SOC-a
ACME koristi 3,000 IP adresa unutar tvrtke	**Mali SOC**	veličine	do 10,000 korisnika/IP adresa
ACME traži sveobuhvatnu vidljivost, najveću moguću automatizaciju kod poslovnog sustava a kod upravljačkog sustava automatizacija mora biti u skladu sa procjenom rizika	**Veliki SOC**	zahtjeva vidljivosti	Sveobuhvatna vidljivost, automatizacija provedena kod većine uređaja i za veći dio entiteta koje nadzire
ACME SOC imat će u potpunosti reaktivnu ulogu za poslovni dio, pro aktivna uloga za poslovni dio dijeliti će se sa IT službom. Za upravljački dio, ACME SOC dijeliti će reaktivnu i pro aktivnu ulogu a Odjelom proizvodnje. ACME SOC će preporučati preventivne i za poslovni sustav i za upravljački sustav.	**Veliki SOC**	zadaća	Reaktivna uloga u potpunosti pripada SOC-u, pro aktivnu ulogu dijeli obično sa IT operacijama osim u slučaju taktičkog odgovora na incident. SOC preporučuje preventivne kontrole.
ACME SOC mora razviti kompetencije podrške sigurnosti upravljačkom sustavu	**Veliki SOC**	bilješki	Ovakav SOC je dovoljno velik da pruža napredne servise sa jedne centralizirane lokacije i dovoljno kompaktan da provodi direktan nadzor i odgovor na incidente. U heterogenim okruženjima različitih geografskih lokacija ovakav SOC se može naslanjati na lokalno osoblje za dio funkcije nadzora i odgovora.

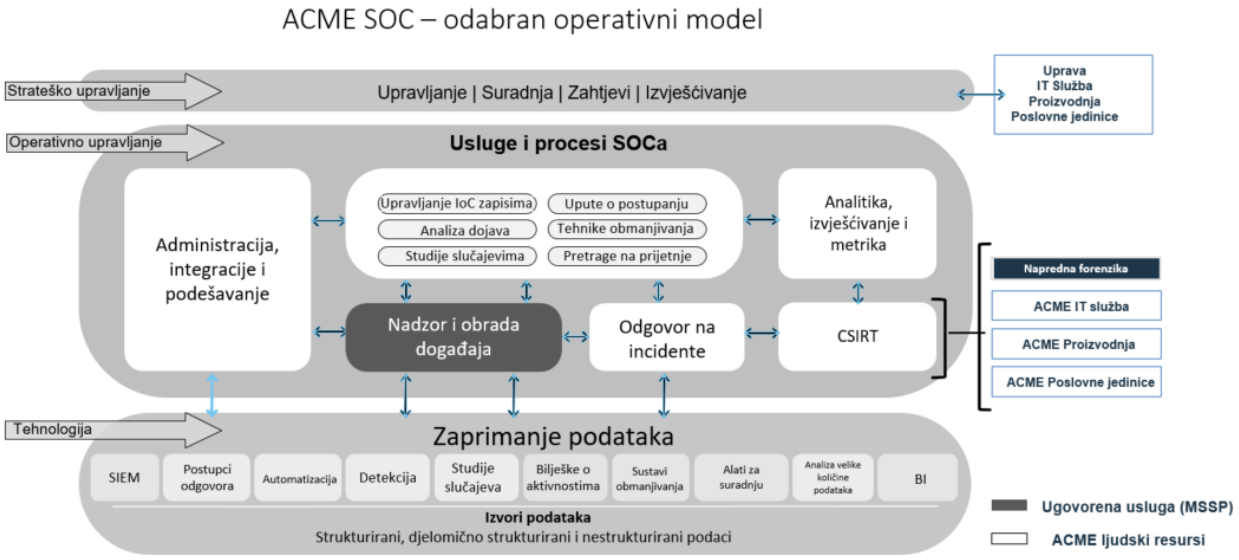
Bitna odluka koju treba donijeti je koje funkcije SOC-a ćemo razviti unutar tvrtke, a koje ćemo ugovoriti sa vanjskim dobavljačima usluga.

Iz GARTNERovog dokumenta [4] preuzeli smo karakteristike koje bi odgovarale zahtjevima ACME SOC-u i opisali u Tablici 3.2.

Tablica 3.2 Odabrani model ACME SOC-a

Zahtjevi tvrtke ACME	Operativni modeli SOC-a	Svojstva	Primjena
Djelomično namjensko osoblje za pokrivanje važnijih incidenta sa naglaskom na upravljačke sustave proizvodnje 24/7, a za poslovne sustave 5x8	**Distribucijski/Co- managed SOC**	• Namjensko ili djelomično namjensko osoblje • Uglavnom pokriva 5 radnih dana po 8 sati • Koristi usluge vanjske tvrtke (*engl. MSSP – Managed security service provider*)	Velike i srednje tvrtke

Nakon odabira distribucijskog modela, čije značajke veličinom i potrebama odgovaraju tvrtki jer ona može osigurati namjensko osoblje i koristiti usluge vanjske kompanije (MSSP), definirali smo operativni model opisan Slikom 3.3.

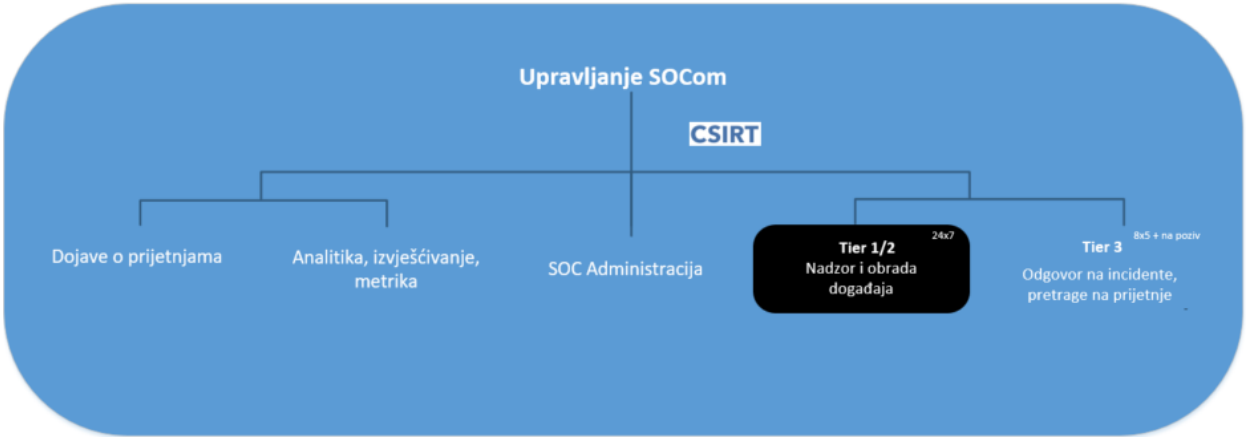


Slika 3.3 ACME SOC odabran operativni model

Strateško upravljanje zahtijevat će funkciju Voditelja SOC-a koji će brinuti o svim funkcijama SOC-a, uslugama i procesima. Nadzor i obrada događaja, kao i napredna forenzika, u početku zahtijevaju angažiranje većeg broja zaposlenika, odnosno posebne kompetencije, koje tvrtka ne posjeduje. Stoga će se ove usluge ugovoriti sa vanjskim dobavljačem. Za ostale funkcije operativnog upravljanja SOC-om koristiti će se postojeći resursi tvrtke. Za sam odgovor na incidente, uposliti će se novi ljudi zbog potreba zaštite upravljačkog sustava koji se planira dodatno širiti.

3.3. Ljudi, tehnologija i procesi

Slijedeći korak jeste utvrditi potreban broj zaposlenika odgovarajućih kompetencija obzirom na procjenu radnog opterećenja, učinak vremena potrebnog za upoznavanje sa tehnologijom i zahtijevano vrijeme rješavanja incidenta. Faktor zrelosti i iskustva, uz automatizaciju, ubrzava rješavanje incidenta i eventualno prebacivanje ljudi na druge ili odgovornije funkcije.
Stoga ljudski resursi moraju pokrivati nekoliko osnovnih funkcija opisanih na Slici 3.4.



Slika 3.4. ACME SOC osnovne funkcije

Upravljanje SOC-om podrazumijeva nadzor rada i stalno poboljšavanje kvalitete usluge, brigu o zaposlenicima i njihovom stalnom usavršavanju. Voditelj SOC-a mora biti u stalnoj i kvalitetnoj komunikaciji sa svim zainteresiranim stranama ACME tvrtke i prenositi uposlenicima SOC-a sve relevantne poslovne zahtjeve.

Odgovorna osoba za upravljanje SOC-om i procesom za slučaj težeg incidenta (*engl. Computer Security Incident Response Team, CSIRT*) koordinira slijedeće aktivnosti koje SOC mora pokrivati:

- Funkciju dojava o prijetnjama (*engl. Threat Intelligence*) - prikuplja podatke o uočenim vanjskim i unutarnjim prijetnjama temeljem kojih se razvijaju studije slučajeva za detekciju i njihovo zaustavljanje, te razvijaju interni procesi i postupci. Ova funkcija pruža uvid u trenutno i prognozirano sigurnosno stanje u kontekstu regije, države, industrijske branše i korištene tehnologije. Također, ovi prikupljeni podaci važni su za konačnu analitiku i izvješćivanje SOC-a prema poslovnim procesima koje štiti.

- Analitika, izvješćivanje i metrika - pruža uvid u sigurnosno stanje vanjskog konteksta i mjerljive rezultate rada SOC-a. Ova funkcija će se brinuti o dizajnu mjernih podataka, prezentaciji rezultata i praćenju ključnih pokazatelja uspješnosti (KPI). Funkcija također pokriva zadatke pisanja, uređivanja i revizije sigurnosnih izvješća.

- SOC Administracija - uvodi, implementira i stalno podešava uvezivanje sigurnosnih rješenja sa SOC-ovim nadzornim alatima (SIEM), te brine o stalnom podešavanju i obogaćivanju kontekstualnih podataka. Ova funkcija brine o svim procesima implementacije, integracije i održavanja svih tehnoloških rješenja korištenima u SOC-u.

- Nadzor i obrada događaja (T1/T2) – funkcija nadzora događaja (T1) podrazumijeva nadzor sigurnosnih događaja i reakciju u skladu sa dokumentiranim postupcima i najboljom industrijskom praksom.

  T1 predstavlja prvu liniju obrane u zaštiti informacijskih sustava od unutarnjih i vanjskih prijetnji. Ona uključuje analizu upozorenja na prijetnje, eskalaciju sigurnosnih upozorenja, procjenu lažno pozitivnih dojava, prikupljanje kontekstualnih podataka, klasifikaciju prijetnji, početnu trijažu i određivanje prioriteta. T1 može predložiti postupak odgovora. T1 funkcija ili zatvara ili eskalira sigurnosni događaj na T2. T1 funkcija aktivno prati i doprinosi svojim prijedlozima poboljšavanju studija slučajeva na SIEM alatu, postupaka odgovora i finom podešavanju automatizacije odgovora.

  T2 funkcija za obradu incidenata odgovorna je za upravljanje sigurnosnim upozorenjima koje zaprimi eskalacijom od T1, potom provodi analizu temeljnog uzroka sigurnosnog incidenta. Može prikupljati dodatne kontekstualne informacije za tehničku analizu sa ciljem utvrđivanja osnovnog uzroka sigurnosnog upozorenja. T2 može sigurnosno upozorenje klasificirati kao sigurnosni incident, i po potrebi utvrditi metode napada, identificirati napadača, cilj napada i svrhu napada. T2 može ažurirati klasifikaciju događaja, važnost, pomoći T3 pri forenzičkoj analizi i određivanju sljedećih koraka (npr. zaključivanje upozorenja, zaključivanje incidenta) i, po potrebi, eskalirati upozorenja na nivo incidenta.

  Odgovor na incidente (T3) - Funkcija odgovora na prijetnju zaprima eskalirane sigurnosne incidente i analizira njihov utjecaj na poslovanje. T3 može dodavati kontekstualne informacije, provoditi dodatnu analizu i na temelju poslovnog učinka preporučiti odgovore i druge razine eskalacije. T3 može zatvoriti, zadržati, vratiti ili eskalirati sigurnosne incidente. Ova funkcija također provodi akciju odgovora na incident, uključujući eskalaciju sigurnosnog incidenta na CSIRT (tim za odgovor na računalne sigurnosne incidente). T3 također može obavljati ulogu pretrage na prijetnje (*engl. Threat Hunt*) i dodatno provjeravati učinkovitost sigurnosnih kontrola i moguće tragove kompromitacije štićenog sustava.

  CSIRT funkcija koordinira posebne postupke za ublažavanje posljedica incidenta, minimiziranje kratkoročnog rizika i štete i povratak na radnu funkciju. Ova funkcija koordinira potrebne aktivnosti između unutarnjih čimbenika kao što su IT služba, proizvodnja, pravna služba, upravljanja ljudskim resursima kao koordinacije sa vanjskim čimbenika – vanjski dobavljači ili kupci, državna tijela uprave, Policija itd.

Za procjenu broja potrebnog ljudskog resursa u obzir moramo uzeti čimbenik vremena potrebnog da:

- SOC završi integraciju SIEM-a, svih sigurnosnih kontrola i krajnjih točaka sa kojih se prikupljaju podaci,
- dodatnim podešavanjem, unaprjeđivanjem i obogaćivanjem podataka postignemo bolju vidljivost,
- poboljšava i optimizira interne postupke odgovora,
- osoblje SOC-a ovlada cjelokupnom tehnologijom SOC-a, upozna unutarnju kulturu tvrtke i sve njene proizvodne i poslovne procese.

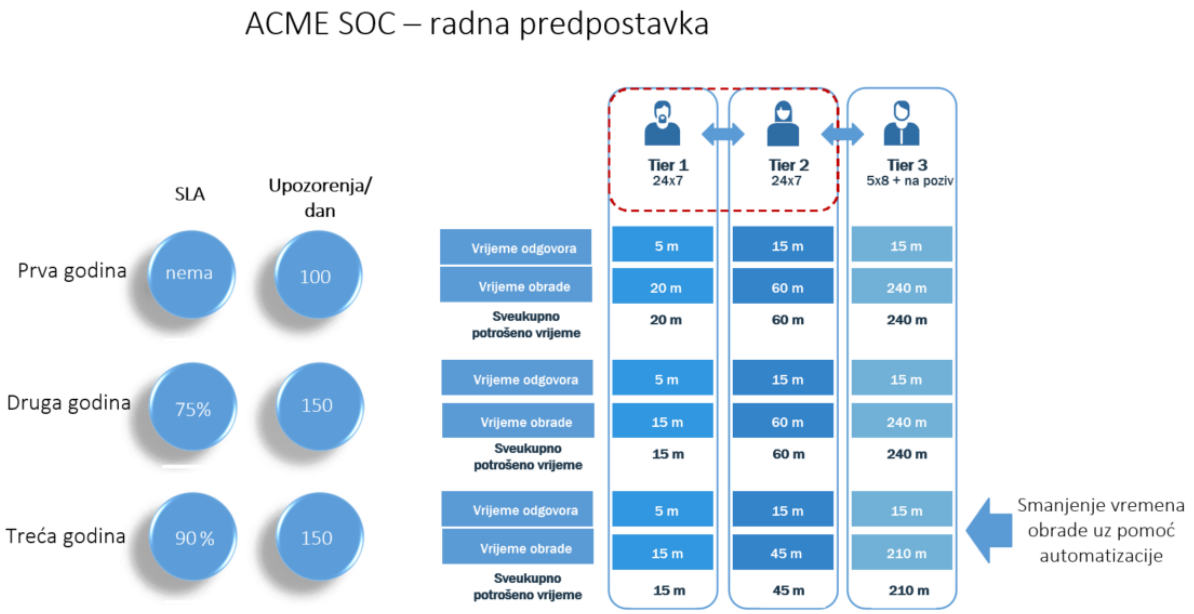
Pretpostavka je da će zrelost SOC-a biti postignuta nakon 3 godine.

Za sve gore navedene funkcije potrebno je osigurati odgovarajuće ljudske resurse u skladu sa dnevnom procjenom broja sigurnosnih upozorenja. Procjenu radnog opterećenja T1, T2 i T3 napraviti ćemo pod pretpostavkom da:

- prve godine rada SOC dnevno bilježi 100 sigurnosnih upozorenja, ostale godine 150,
- sve sigurnosne kontrole i sve nadzirane krajnje točke integrirane su sa SIEM sustavom,
- SIEM sustav, sigurnosne kontrole i krajnje točke su tek inicijalno podešene,
- T1 i T2 funkcije rade u 3 radne smjene od po 8 radnih sati, 7 dana u tjednu,
- T3 funkcija radi u jednoj smjeni, 5 dana u tjednu, a ostalo vrijeme dežura po pozivu.

Početna ugovorna razina usluge (*engl. Service Level Agreement, SLA*) preferira završetak kompletne obrade upozorenja i incidenta do maksimalno 4 sata. Prvu godinu SOC ne mora slijediti ugovornu razinu usluge, a drugu godinu 75% upozorenja i incidenata mora biti riješeno sukladno SLA, dok treću godinu SLA zahtijeva 90% pokrivenosti. Slika 3.5 prikazuje početnu procjenu vremena odziva T1, T2 i T3 funkcije gdje u prvoj godini zahtjev SLA nije obaveza i gdje je broj upozorenja i incidenata u prvoj godini rada po danu procijenjen na 100.

Prve godine rada SOC-a pretpostavljamo da T1, za svako dobiveno upozorenje, mora početi sa trijažom unutar 5 minuta po dojavi i za 20 minuta završiti sa obradom incidenta ili, po potrebi, eskalirati slučaj na T2 funkciju. T2 zaprima slučajeve eskalirane od T1 unutar 15 minuta po dojavi, i za 60 minuta završi sa obradom srednjih incidenta ili, po potrebi, eskalira slučaj na T3 funkciju. T3 zaprima slučajeve eskalirane od T unutar 15 minuta po dojavi, i za 240 minuta završi sa obradom većih incidenta ili, po potrebi, eskalira slučaj na CERT funkciju.



Slika 3.5 ACME SOC - radna pretpostavka operativnog opterećenja SOC osoblja

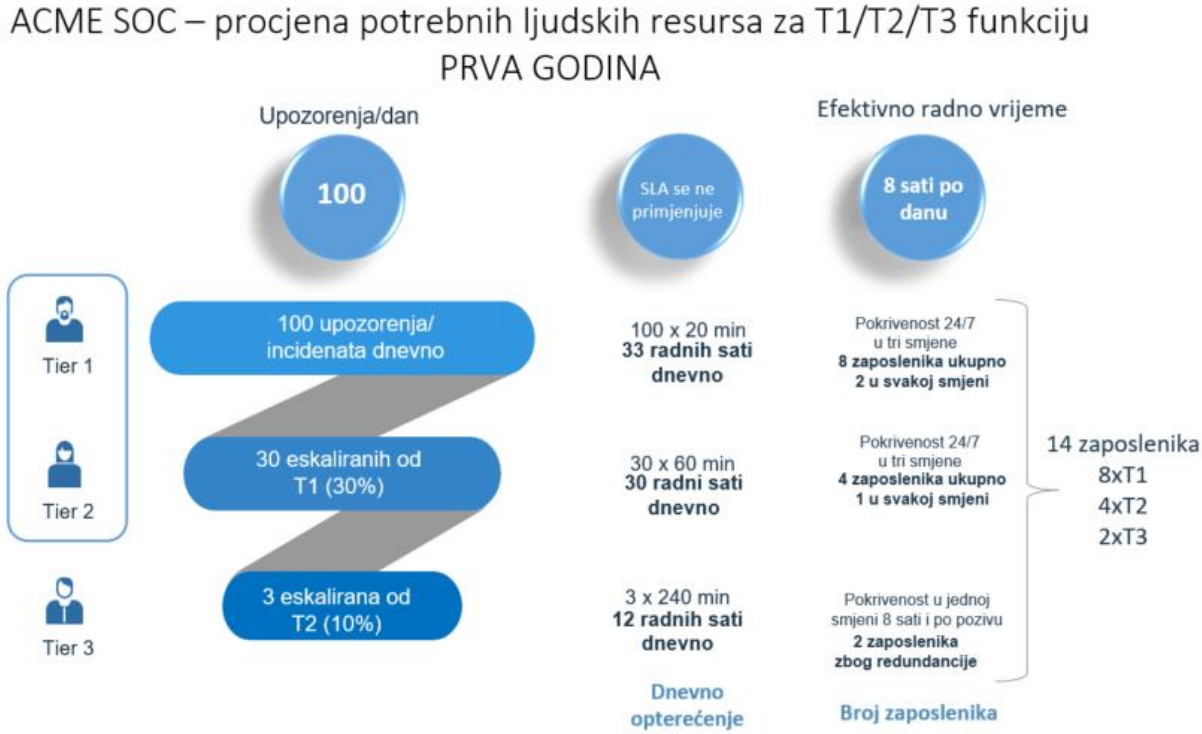
Tokom prve godine rada završena je i dodatno poboljšana integracija SIEM-a sa svim kontrolama i krajnjim točkama. SOC administracija stalno radi na poboljšanju prikaza i vidljivosti dobivenih podataka, interni postupci su bolje optimizirani, a osoblje SOC-a već dobro poznaje radnu kulturu tvrtke.

Stoga, u drugoj godini rada, SLA zahtjeve treba poštovati za 75% upozorenja i incidenata. Istovremeno, podižemo očekivani kapacitet obrade upozorenja sa prijašnjih 100 na 150 po

danu. Ovo povećanje postavljamo zbog očekivane kvalitetnije integracije i povećanja ukupne vidljivosti događaja iz SOC-a. U drugoj godini T1 za svako dobiveno upozorenje mora početi sa trijažom unutar 5 minuta po dojavi, i za 15 minuta završiti sa obradom incidenta ili, po potrebi, eskalirati slučaj na T2 funkciju. T2 zaprima slučajeve eskalirane od T1 unutar 15 minuta po dojavi, i za 60 minuta završi sa obradom srednjih incidenta ili, po potrebi, eskalira slučaj na T3 funkciju. T3 zaprima slučajeve eskalirane od T unutar 15 minuta po dojavi, i za 240 minuta završi sa obradom većih incidenta ili, po potrebi, eskalira slučaj na CERT funkciju.

U trećoj godini pretpostavljamo da su SOC sustavi i procesi zreliji, ljudi iskusniji i da je već dostignut određeni nivo automatizacije odgovara na upozorenja i incidente. Ovdje očekujemo da SLA vrijedi za 90% slučajeva i procijenjenog broja od 150 upozorenja dnevno. T1 ostaje na istom utrošenom vremenu, dok T2 i T3 smanjuju vrijeme obrade sa 60 minuta na 45 minuta, odnosno sa 240 minuta na 210 minuta.

Sada je potrebno procijeniti koliki broj ljudi nam je potreban za T1/T2/T3 funkciju kako bi dnevno obradili 100 sigurnosnih upozorenja. Pretpostavka je da 70% upozorenja (70) predstavljaju lažno pozitivni nalazi koje će T1 istražiti, preporučiti dodatno podešavanje kontrole ukoliko je moguće i zatvoriti slučaj. Pretpostavka je da će 30% upozorenja (30) biti proslijeđeno T2 koji nastavlja obrađivati incident do njegovog rješavanja i zatvaranja. Od 30% eskaliranih incidenata 10% (3) bit će eskalirano T3 kao sumnja na ozbiljan sigurnosni problem.



Slika 3.6 Procjena potrebnih ljudskih resursa za prvu godinu ACME SOC-a

Prema Slici 3.6, 70% upozorenja riješit će dvoje T1 u svojoj radnoj smjeni koja traje 8 sati. 24/7 zahtjev bit će pokriven sa ukupno osam zaposlenika od kojih su na dužnosti šest, a dvoje su na odmoru. 30% eskaliranih upozorenja za T2 rješavat će jedan T2 u svojoj radnoj smjeni od 8 sati. 24/7 zahtjev pokrivat će ukupno četiri zaposlenika od kojih je na dužnosti troje, a jedan je na odmoru.

I na kraju tri potencijalno najopasnija incidenta rješavat će jedan T3 u svojoj redovitoj smjeni

ili, zbog eskalacije izvan radnih sati, po pozivu. Potrebno je dvoje T3 zaposlenika zbog redundantne dužnosti po pozivu, a dodatni T3 može biti korišten i za ostale poslove SOC-a.

U drugoj godini, prema Slici 3.7, procjenjujemo veći dnevni broj sigurnosnih upozorenja (150) i primjenu SLA odredbi za 75% obrađenih upozorenja.

Slika 3.7 Procjena potrebnih ljudskih resursa za drugu godinu ACME SOC-a

Iako procjenjujemo da će broj upozorenja porasti za 50% (150) očekujemo da će vrijeme obrade, zbog iskustva, uigranosti tima i automatizacije biti smanjeno na 15 minuta. Zato broj T1 i T2 resursa nećemo povećavati. Očekujemo također više posla za T3, pa procjenjujemo da treba u drugoj godini povećati broj ovog resursa na ukupno tri. Uz T3 ulogu, isti ljudski resursi se mogu koristiti kao potpora SOC administraciji i poslovima dojava o prijetnjama.

U trećoj godini očekujemo isti broj dnevnih upozorenja, ali uz stroži SLA koji zahtjeva da 90% upozorenja T2 i T3 rješavaju brže – T2 sa 60 minuta na 45 minuta, a T3 sa 240 minuta na 210 minuta, kao što je opisano na Slici 3.8.

Slika 3.8 Procjena potrebnih ljudskih resursa za treću godinu ACME SOC-a

Dakle, pretpostavka je da unutar trogodišnjeg perioda, uz porast broja dnevnih upozorenja sa 100 na 150 i postupnu primjenu strožih SLA odredbi (0 - 75% - 90%) sveukupno 15 zaposlenika može kvalitetno pokrivati ACME SOC u režimu 24/7. To će biti moguće uz postepenu primjenu automatizacije trijažnog postupka koji će smanjiti vrijeme trijaže. Također, vidljivo je da najkvalitetniji potencijal T3 analitičara ima dovoljno prostora da bude iskorišten za zadatke dojava o prijetnjama, analitiku i izvješćivanje i CSIRT. T3 analitičari također mogu biti dodatno angažirani na poslovima SOC administracije na kojima se mogu osloniti na pomoć IT službe i Odjela proizvodnje, istraživanja i razvoja.

Obzirom da ACME SOC mora štititi i poslovni i proizvodni upravljački sustav, poželjno je da T2 i T3 analitičari imaju prethodno iskustvo u radu na upravljačkim sustavima ili završen tečaj o poznavanju i razumijevanju upravljačkog sustava kojeg štite. Sve zaposlenike SOC-a treba upoznati sa rezultatima procjene rizika, cjelokupnom imovinom upravljačkog sustava i poslovnim procesima koji njime upravljaju. Usvojena znanja o upravljačkom sustavu po potrebi treba periodički obnavljati. Uz temeljna znanja o upravljačkim sustavima, dobri kandidati za rad u SOC-u mogu biti i iskusniji inženjeri iz ACME IT Službe koji poznaju oba sustava. Potrebna su još dodatna znanja zaposlenika iz područja informacijske sigurnosti, sigurnosti računalnih mreža i operacijskih sustava, znanja o upravljanju sigurnosnim incidentima i mrežnoj i računalnoj forenzici.

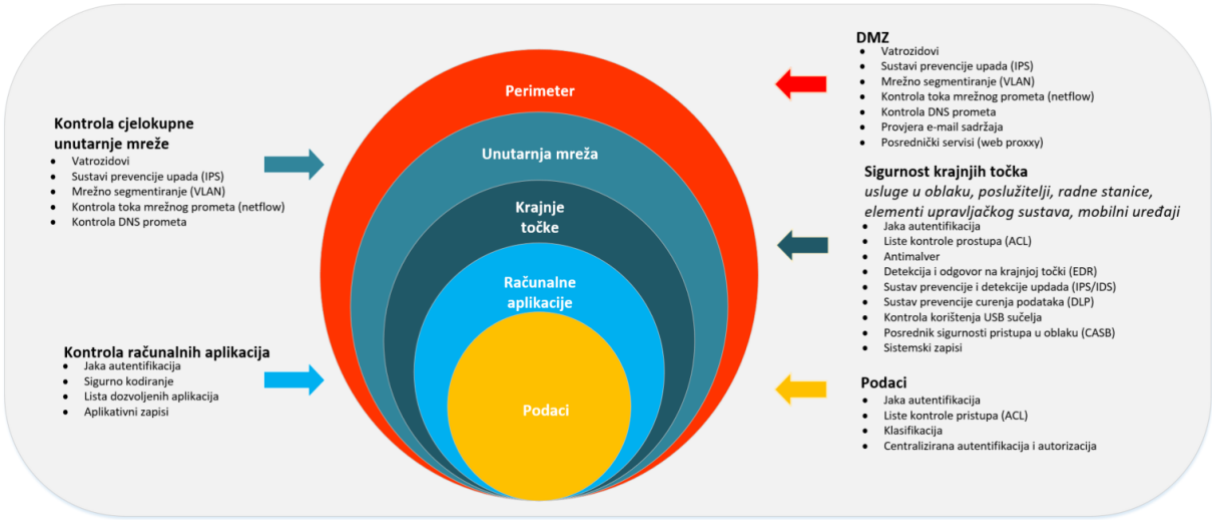
Tržište danas nudi nekoliko kvalitetnih programa za obuku i certifikaciju iz navedenih područja, a na raspolaganju su i službena Microsoft i Cisco obuka i postupci certifikacije znanja, certifikacija za Linux operacijske sustave i za područje upravljanja sigurnosnim incidentima. Tablica 3.3 navodi tečajeve i certificiranje znanja koja su poželjna u SOC koji štiti upravljačke sustave.

Tablica 3.3 Znanja, tečajevi i industrijski certifikati za djelatnike ACME SOC-a

Radno mjesto SOC-a	Djelatnost SOC-a	Opis poslova	Tečajevi i certificiranje
T1 Analitičar T2 Analitičar T3 Analitičar	Praćenje prijetnji	Praćenje događaja, otkrivanje incidenata, osnovna klasifikacija i određivanje prioriteta rješavanja, istraga	GIAC Security Essentials (GSEC) EC-COUNCIL Certified incident handler GIAC Certifiified Incident Handler (GCIH) $(ISC)^2$ CISSP Certified Information Systems Security Professional
T2 Analitičar T3 Analitičar Upravitelj SOC-a	Upravljanje incidentima	Upravljanje incidentom do njegovo zaključivanja	ISO/IEC 27035 Lead Incident Manager
Upravitelj SOC-a	CSIRT	Koordinacija sa timom za upravljanje sigurnosnim incidentima	ISO/IEC 27035 Lead Incident Manager, ISACA CISM Certified Information Security Manager, $(ISC)^2$ CISSP Certified Information Systems Security Professional
T2 Analitičar T3 Analitičar	Hitne intervencije	Odgovor na kibernetičke prijetnje, koordinacija pri izvođenju digitalne forenzike	GIAC Cyber Threat Intelligence (GCTI), EC-COUNCIL Certified Ethical Hacker
SOC Administrator T2 Analitičar T3 Analitičar	Izrada studija slučaja	Izrada studija slučaja prijetnji, izrada uputa i procedura odgovora na prijetnje Modeliranje prijetnji	EC-COUNCIL Certified Ethical Hacker, SANS FOR578: Cyber Threat Intelligence, GIAC Cyber Threat Intelligence (GCTI) GIAC Response and Industrial Defense (GRID)
T3 Analitičar	Analiza sigurnosnog stanja	Analiza sigurnosnog stanja temeljem vanjskih i unutarnjih izvora informacija	SANS FOR578: Cyber Threat Intelligence, GIAC Cyber Threat Intelligence (GCTI)
T3 Analitičar	Pretraga na kompromitirane sustave	Analiza i praćenje unutarnjeg stanja u cilju otkrivanja aktivnosti koje ukazuju na kompromitiranost sustava	SANS FOR508: Advanced Incident Response, Threat Hunting and Digital Forensics, GIAC Certified Forensic Analyst (GCFA) GIAC Response and Industrial Defense (GRID)
T3 Analitičar	Izvješćivanje	Izvješćivanje o stanju praćenog sustava, količini zadataka i broju incidenata prema klasifikaciji važnosti	Osnovni treninzi proizvođača korištenih SOC rješenja
T3 Analitičar	Analitika	Pretraga na specifične podatke, otkrivanje anomalija i praćenje trendova i pojava	GIAC Certified Forensic Analyst (GCFA) ARCITURA Big Data Science Certified Professional (BDSCP)
SOC Administrator T3 Analitičar	Administracija svih SOC alata	Poslovi upravljanja i održavanja SOC alata	Osnovni treninzi proizvođača korištenih SOC rješenja
SOC Administrator T3 Analitičar	Upravljanje sigurnosnim zapisima i kontekstualnim podacima	Poslovi zaprimanja i održavanja sigurnosnih zapisa	Microsoft MTA, Microsoft MCSE, LPI Linux Enterprise Professional – Security GIAC Global Industrial Cyber Security Professional (GICSP)
SOC Administrator T3 Analitičar	Uvođenje i integracija SOC tehnologija	Izrada, testiranje i uvođenje tehničkih rješenja u SOC-u za upravljačke sustave	Osnovni treninzi proizvođača korištenih SOC rješenja

Obzirom da je ova procjena rađena temeljem pretpostavke o broju upozorenja odnosno incidenata i zahtjeva razine usluge, tek početnom primjenom sigurnosnih kontrola i njihovom integracijom sa SIEM-om, uz ostale izvore informacija, imat ćemo stvarnu početnu sliku o općem sigurnosnom stanju u tvrtki.

ACME SOC će objedinjavati nadzor i odgovor na incidente temeljem informacija dobivenih od sigurnosnih kontrola i sistemskih zapisa računala i uređaja sa poslovnog i upravljačkog sustava, te korištenih poslovnih sustava u oblaku. Izuzetno je važno da SOC preko ovih podataka ima čim kvalitetniju vidljivost, pravilo "više je bolje" za SOC uvijek vrijedi. Slika 3.9 opisuje primjer "dubinske obrane" korištenja različitih sigurnosnih kontrola.

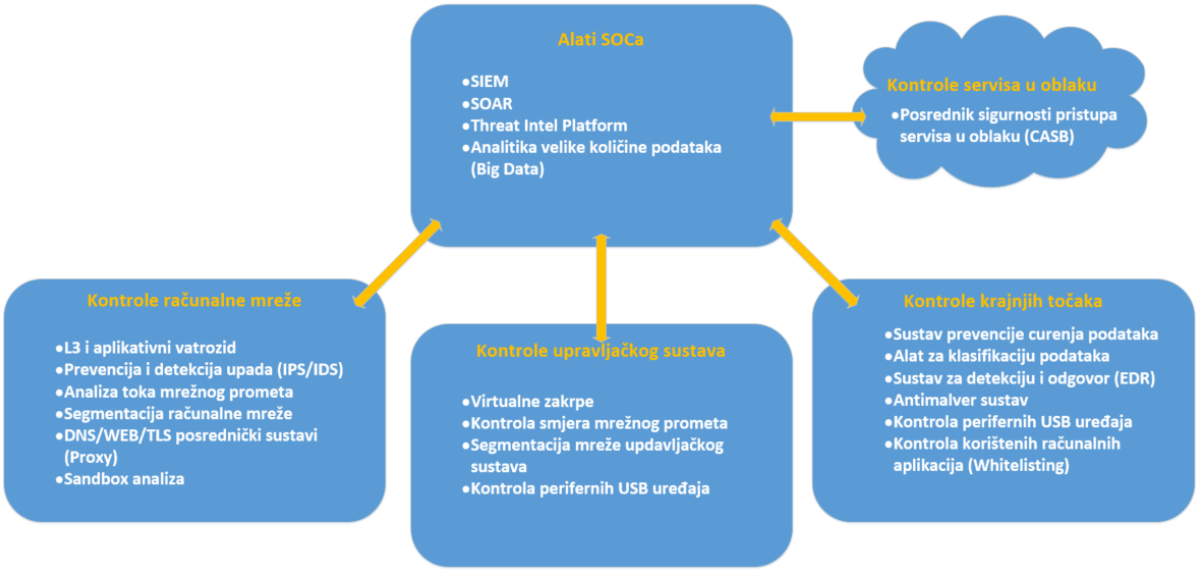


Slika 3.9 "Dubinska obrana" korištenjem sigurnosnih kontrola

Važni poslovni podaci se moraju klasificirati i nositi odgovarajuću oznaku klasifikacije koja omogućuje nadzor i kontrolu, obično pomoću sustava za prevenciju curenja i gubitka podataka (*engl. Data Leakage Prevention, DLP*).

Pristup važnim podacima kontrolira se mehanizmima jake autentikacije gdje god je to moguće, te autorizacije čije procese također SOC mora nadzirati. Računalne aplikacije moraju poznavati mehanizme jake autentikacije i njihove aktivnosti moraju biti bilježene u odgovarajuće aplikativne sistemske zapise. Dobro je imati mogućnost održavanja liste dozvoljenih računalnih aplikacija uz mogućnost sprječavanja korištenja računalnih aplikacija koje nemaju poslovnu funkciju. Na krajnjim točkama obrade podataka, računalima poslužiteljima, radnim stanicama i mobilnim uređajima potrebno je primijeniti kontrole jake autentikacije, sustave detekcije malvera, prevencije i detekcije upada (*engl. Intrusion Prevention/Detection Systems, IPS/IDS* –), curenja podataka, kontrolu USB sučelja i osigurati odgovarajuće sistemske zapise svih kontrola i samog operacijskog sustava (Slika 3.10).

Unutarnja mreža mora biti optimalno segmentirana, štićena vatrozidom, IPS/IDSom i kontrolom toka mrežnog prometa (*engl. netflow*). Poželjno je dodatno kontrolirati internu uporabu DNS protokola. Isto vrijedi i za vanjsku mrežu (DMZ) koja se štiti vatrozidom, IPS/IDSom, kontrolom toka cjelokupnog mrežnog prometa, kontrolom DNS prometa i unutar koje se udomaćuju sigurnosni servisi koji se koriste za pristup internetu. Naravno, svi ovi servisi moraju SOC-u slati odgovarajuće informacije.



Slika 3.10 Integracija alata SOC-a i sigurnosnih kontrola

Na samom upravljačkom sustavu trebamo osigurati prihvat svih sistemskih zapisa sa OT elemenata gdje god je to moguće. Treba razmatrati primjene virtualnih sistemskih ispravaka, ovdje se radi o aplikativnom klijentu koji dodaje dodatni sloj zaštite na potencijalno ranjive servise OT elemenata. Stroga segmentacija mrežnog okruženja i njezina kontrola također je obavezna u OT okruženju zajedno sa kontrolom smjera prometa.

Za nadzor sigurnosti korištenja servisa u oblaku potrebno je primijeniti neko od rješenja posrednika sigurnosti pristupa u oblaku (*engl. Cloud Access Security Broker, CASB*). To je softversko rješenje koje se udomljuje ili unutar tvrtke ili kao dodatni servis u oblaku, a omogućuje primjenu politike dodatnog nadzora korištenja usluga u oblaku i integraciju sa ostalim kontrolama koje postoje unutar tvrtke.

Zbog specifičnosti servisa u oblaku, davatelji ovih usluga obično preporučuju zaobilaženje standardnih sigurnosnih kontrola kao što su korištenje web posrednika (*engl. web proxy*), dubinsku analizu sadržaja mrežnog prometa i izuzimanje provjere antimalver kontrole za klijente servisa u oblaku (MS Teams na primjer). Ovisno o proizvođaču, CASB omogućuje integraciju sa postojećim sigurnosnim kontrolama (EDR, DLP, klasifikacija, provjere na malver) i svakako je potrebno temeljito procijeniti primjenu ove kontrole.

Alati za obmanjivanje (*engl. Deception tool*) jedna je od prvih sigurnosnih kontrola koje treba primijeniti u početcima uspostave SOC-a i ona mora odgovoriti na pitanje dali je IT/OT okruženje (*engl. Information technology and Operation technology, IT/OT)* tvrtke već kompromitirano. Ovi alati primjenjuju tehnike zavaravanja napadača nudeći mu unaprijed pripremljene interesantne informacije i podatke (mamci). Uvođenje u IT/OT okruženje planira se i priprema vrlo pažljivo i informacije o ovim pripremama se dijele između uskog broja povjerljivih ljudi. Neki od boljih sustava omogućuju konfiguraciju bez potrebnog mrežnog priključka, onemogućujući tako već prisutnom napadaču uvid u ove aktivnosti. Alat pritom ima mogućnost praćenja mamaca i prikrivenog izvješćivanja o njihovom korištenju. Uporabom ovog alata imat ćemo jasniju početnu situaciju prije primjene ostalih sigurnosnih kontrola i pokretanja SOC-a.

Nadzor svih kontrola centralizira se pomoću SIEM sustava. SIEM osigurava kvalitetnu

vidljivost svih događaja prikupljanjem sistemskih zapisa i njihovu korelaciju prema vremenu nastajanja. Većina SIEM rješenja sadrži bogatu bazu podataka već definiranih sigurnosnih događaja i njihove korelacije, sa podrškom za veliki broj poznatih modela različite sigurnosne opreme gotovo svih renomiranih proizvođača. To olakšava izradu studija slučajeva sigurnosnih incidenata. Svejedno je potrebno pratiti i stalno podešavati prikaze zaprimljenih sistemskih zapisa sa svih sigurnosnih kontrola (vatrozida, antivirusnih rješenja, sustava za detekciju i prevenciju upada (IPS/IDS) i ostalih), aktivne mrežne opreme (preklopnici i usmjerivači), svih osobnih računala, računala poslužitelja i aktivnih elemenata upravljačkog sustava. I ovdje treba slijediti pravilo „Čim više - tim bolje“ - veća količina prikupljenih kvalitetnih informacija jamči bolju vidljivost unutar SOC-a, bolje razumijevanje konteksta poslovanja, a na kraju i izradu boljih studija slučajeva sigurnosnih incidenata. SIEM zahtjeva stalnu brigu o kvaliteti podataka koje prima i dodatna podešavanja podatkovnih prikaza. Popis obaveznih sigurnosnih kontrola naveden je u Tablici 3.4.

Tablica 3.4 Obavezne sigurnosne kontrole [5]

Osnovne tehnološke kontrole	• Antivirus/antimalware na svih računalima I poslužiteljima • Sustavi za rano otkrivanje i odgovor (Endpoint Detection and Response EDR) • Sustav detekcije i prevencije upada na računalnoj mreži (IPS/IDS) • Mehanizmi jake autentifikacije (2FA, MFA) • Redovito penetracijsko testiranje
Napredne tehnološke kontrole	• Automatska provjera ranjivosti sustava i virtualne zakrpe • Sustavi sprečavanja “curenja” podataka (DLP) • “Data diode” između upravljačkog sustava i korporativne računalne mreže • Sustav nadzora promjena na bazama podataka • “Honeypot” i sustavi za obmanjivanje napadača • “Sandobox” kontrola • Lista dozvoljenih računalnih aplikacija • Provjera integriteta datoteka • Vatrozid na višim OSI slojevima • Provjera SSL i TLS mrežnog prometa
Posebne kontrole za upravljačke sustave	• “Data diode” između upravljačkog sustava i korporativne računalne mreže • Primjena sustava virtualnih zakrpi • Kontrola segmentacije upravljačke mreže • Kontrola smjera prometa na upravljačkoj mreži • Kontrolni popisi sigurnih mrežnih uređaja

Podrška za upravljačke sustave obično se ne isporučuje redovito sa svakim SIEM rješenjem nego se dodatno naplaćuje. Iskusan SOC tim može pripremiti svoje specifične studije slučajeva za svoj upravljački sustav na primjer:

1. Nadzor korisničkih računa upravljačkih sustava: kriva lozinka, krivo korisničko ime, višestruka neispravna autentikacija;
2. Nadzor količine i vrste prometa iz upravljačke mreže prema računalnim sustavima i aplikacijama u poslovnoj mreži: profiliranje prometa prema vrsti protokola i vremenu nastajanja prometa, nadzor i uzbunjivanje u slučaju devijacija, uzbunjivanje u slučaju da je primijećen promet iz upravljačke mreže prema internetu ili nekom netipičnom dijelu korporativne mreže;
3. Mrežna nedostupnost većeg broj elemenata upravljačkog sustava: istovremeni privremeni gubitak mrežne veze mora biti temeljito istražen jer se od uglavnom prilikom nadogradnje firmwarea uređaja;
4. Detekcija većeg broja pokušaja skeniranja sistemskih portova: ovakvi sigurnosni incidenti moraju biti istraženi jer bude sumnju na kompromitiranost nekih od internih sustava i mogu ukazivati na aktivnost napadača da uz pomoć skeniranja prikupi čim više informacija o elementima računalne mreže;
5. Povećana količina ICMP prometa: povećanje ove vrste mrežnog prometa također budi sumnju na kompromitiranost sustava;

6. Značajne promjene u kapacitetu za pohranu podataka: ova vrsta alarma može značiti da neka od malicioznih aktivnosti rezultira naglim povećanjem količine sistemskih podataka na kompromitiranom sustavu ili ukazuje na moguću krađu podataka;
7. Promjene integriteta datoteka osjetljivih aplikacija: nenajavljene promjene na nadziranim sustavima moguće je otkriti sustavom detekcije promjena integriteta datoteka što također ukazuje na potencijalni sigurnosni incident.

Potrebno je stalno razvijati vlastite studije slučajeva koje uzimaju u obzir specifičnosti poslovnog i upravljačkog sustava, pojedinih poslovnih procesa, usvojene navike svih korisnika sustava i uvođenje novih tehnologija. Postojeće studije slučajeva se stalno dodatno podešavaju dnevnim postupkom administriranja sustava i povećanja vidljivosti postojećih sigurnosnih događaja.

Nove studije slučajeva uvode se postupkom modeliranja prijetnji (*engl. Threat modeling*) i sastavni su dio poslovnih procesa SOC-a. MITRE ATT@CK okvir [6] opisuje poznate taktike, tehnike i procedure korištene u napadima na računalne sustave i olakšava razumijevanje i obradu incidenta. Opisuje ukupno četrnaest taktika i uz svaku od moguće korištene tehnike i procedura. Svi vodeći proizvođači SIEM rješenja omogućuju podršku studijama slučajeva i tumačenja MITRE ATT@CK okvira. Najveći dio posla ostaje na T2, T3 analitičarima i SOC administratoru koji svaku od studija slučajeva mora podesiti da bude primjenjiva u ACME okruženju i penetracijskim testiranjem potvrditi da je kontrola učinkovita.

Dodatno je moguće iskoristiti SYSMON MODULAR ekstenzije [7] poznatog Microsoftovog alata SYSMON koji pomaže razumijevanju sistemskih zapisa MS Windows operacijskog sustava i lakšu trijažu.

Na internetu postoji nekoliko korisnih zbirki skripti [8] [9] za dodatnu provjeru podešenosti sigurnosnih kontrola u otkrivanju malicioznih aktivnosti. ACME SOC tim može pokrenuti ova ispitivanja u koordinaciji sa IT službom, poštujući naravno dobru praksu obavezne zaštite kod izvođenja penetracijskog testiranja. I ove skripte koriste MITRE ATT@CK okvir.

Kao primjer, slijedeći SYSMON sistemski zapis sa MS Windows radne stanice proširen SYSMON MODULAR ekstenzijom donosi dodatne informacije koje ukazuju na moguću MITRE ATT@CK tehniku (id-T1036, maskiranje i fazu izbjegavanja obrane):

Sistemski zapis
„Apr 04 10:01:33 FINANCE01.corp.ACME.local AgentDevice=WindowsLog AgentLogFile=Microsoft-Windows-Sysmon/Operational PluginVersion=7.2.9.105 Source=Microsoft-Windows-Sysmon"
donosi zabilježeno vrijeme događaja, domensko ime računala i inačicu korištenog SYSMON alata.

Potom slijedi informacija o korisničkom računu unutar kojega je pokrenut sumnjivi proces
„Computer= FINANCE01.corp.ACME.local OriginatingComputer=10.33.22.222 User=SYSTEM Domain=NT AUTHORITY EventID=1 EventIDCode=1 EventType=4 EventCategory=1 RecordNumber=22770376 TimeGenerated=1617519615 TimeWritten=1617519615 Level=Informational Keywords=0x8000000000000000"
i ovdje se radi o sistemskom korisničkom računu koji ima visoke privilegije na sustavu.

SYSMON MODULAR ovdje unutar sistemskog zapisa donosi dodatnu informaciju:
„Task=SysmonTask-SYSMON_CREATE_PROCESS Opcode=Info Message=Process Create: RuleName:
technique_id=T1036,technique_name=Masquerading,phase_name=Defense

Evasion UtcTime: 2021-04-04 07:00:15.647 ProcessGuid: {F1143456-63FF-6069-C9CE-000000001802} ProcessId: 20464"
o mogućem korištenju tehnike maskiranja kada napadač pokušava manipulirati svojim alatima koje je uspješno postavio unutar napadnutog sustava i da bi izbjegao otkrivanje maskira ih dajući im imena legitimnih datoteka ili servisa.

Lokacija i ime sumnjive datoteke opisana je u ovom sistemskom zapisu
„Image: C:\Users\ACME.user\AppData\Local\SomeApp\SomeApp\current\suspicious.exe FileVersion: 1.4.00.7174 Description: Some App Product: Some App INC. Company: Some App INC OriginalFileName: suspicious.exe"
i nalazi se unutar standardnog korisničkog profila.

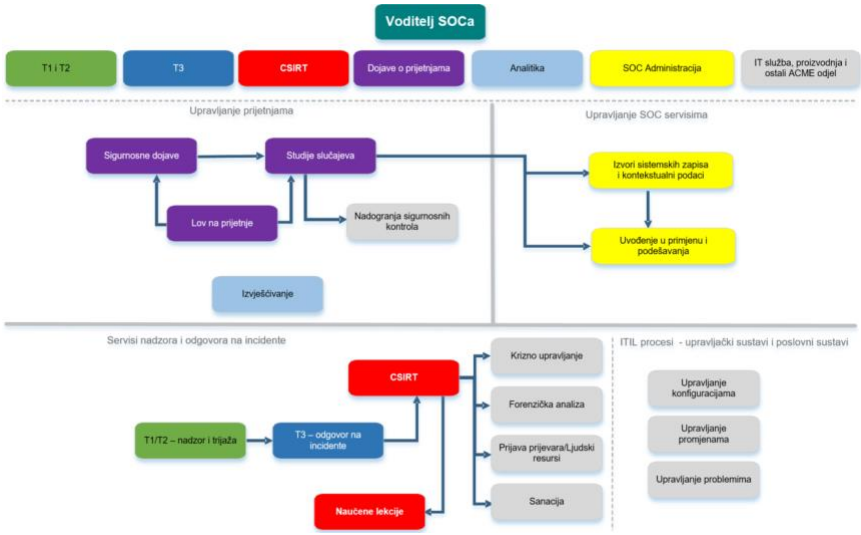
SOAR (*engl. Security Orchestration, Automation and Response*) je glavni alat SOC tima koji omogućuje ručno ili automatizirano otvaranje sigurnosnog incidenta, automatsko ili ručno prikupljanje kontekstualnih informacija iz SIEM-a i ostalih kontrola. Sa SOAR-om se uvezuje sustav dojave o prijetnjama i dodatna programska podrška za automatizaciju odgovora na prijetnje. Kroz SOAR se izgradi podrška procesima za odgovor na pojedine vrste incidenta koja pomaže analitičaru u svim koracima obrade incidenta, eskalaciju sa T1 na T2, T3 ili CSIRT. Potom, ovisno o razvijenoj podršci, automatizirani ili ručno pokrenut odgovor može zadržati i blokirati incident promjenama postavki vatrozida, sigurnosnim sustavima krajnje točke i sandboxing alatima. Razvijen SOAR s vremenom dodatnim podešavanjima u potpunosti automatizira neke postupke sigurnosnih incidenta i tako rasterećuje T1 i T2 analitičare.

Platforma za upravljanje informacijama o sigurnosnim dojavama koristi se za centralizirani prihvat vanjskih informacija, njihovo vrednovanje prema primjenjivosti i riziku za štićenu infrastrukturu i konačnoj izradi prilagođenog izvješća o sigurnosnim dojavama za interne potrebe tvrtke ACME. Ovako prikupljene informacije sadrže podatke o tzv. indikatorima kompromitacije (*engl. Indicator of compromise, IoC*) - sažetak maliciozne datoteke, IP ili URL adresa korištenog u malicioznom napadu) i korištenim taktikama, tehnikama i procedurama. One se potom integriraju sa ostalim sigurnosnim alatima, SIEM-om i SOAR-om i omogućuju bolje kontekstualno razumijevanje sigurnosnih događaja u SOC-u. Također, ukoliko analitičari uoče neke nove IoC-ijeve, mogu ih opisati, vrednovati i potom pomoću ove platforme omogućiti svim sustavima SOC-a detekciju i zaustavljanje prijetnje. Novo uočeni IoC-ijevi mogu se izmjenjivati sa vanjskim izvorima informacija kao što su komercijalni servisi i državni CSIRT izvori informacija o prijetnjama.

Procese ACME SOC-a koje treba razviti i primijeniti možemo podijeliti na četiri osnovne grupe, kao što prikazuje Slika 3.11. Prva grupa procesa su servisi nadzora i odgovora na incidente, druga su upravljanje prijetnjama i treća upravljanje ACME SOC servisima. Četvrta grupa su procesi koji reguliraju suradnju ACME SOC-a sa ostalim čimbenicima unutar i izvan ACME tvrtke.

Svaki proces opisuje se dokumentiranom procedurom koja u opisu ima određene osnovne elemente:

- podatke o periodičnom pregledu i izmjenama zbog poboljšanja,
- opisanu svrhu, ulazne informacije potrebne za proceduru i izlazne informacije kao rezultat izvođenja procedure,
- matricu dodjele odgovornosti za pojedine zadatke unutar procedure,
- opisane ključne pokazatelje performansi (KPI) za mjerenje učinkovitosti procedure.



Slika 3.11 ACME SOC dijagram procesa

Grupa procesa „Upravljanje prijetnjama“

Obrada sigurnosnih dojava – Ova procedura provodi se po primitku rezultata iz procesa naučenih lekcija nakon sigurnosnog incidenta, rezultata istraživanja lova na prijetnje, prema zahtjevima dobivenih drugim vanjskih i unutarnjim kanalima kao nestrukturirane informacije (pretplate na obavijesti o prijetnjama, voditelj informacijske sigurnosti, istrage, sumnje na prijevare, ljudski resursi itd.) i kao strukturirani (npr. STIX/TAXII) izvori sigurnosnih podataka (pretplate na obavijesti o prijetnjama). Rezultat rada ove procedure jest izrada nove ili ažuriranje postojeće sigurnosne kontrole ili studije slučajeva. Analitičar dojava o prijetnjama može izraditi odgovarajuću obavijest o otkrivenoj prijetnji i ažurirati internu bazu znanja. Pri tome su mu na raspolaganju svi alati koje SOC koristi i svi dostupni izvori informacija. U poslu surađuje sa T1/T2 analitičarima, SOC Administratorom, dobavljačima usluga i partnerima i IT Službom. O rezultatima izvješćuje također Voditelja SOC-a i Voditelja informacijske sigurnosti.

Lov na prijetnje – Ovu proceduru provodimo unaprijed određenom planu aktivnosti lova na prijetnje, po naputku obrada sigurnosnih dojava ili po naputku dobivenom iz studija slučajeva situacijske svijesti o sigurnosti. Rezultati provođenja ove procedure mogu biti eskalacija T3 analitičarima za ublažavanje rizika i odgovor na prijetnje, zahtjev za dodatnim podešavanjem studija slučajeva ili izradom novih i izrada izvješća o rezultatima pretrage. Ovom procesu na raspolaganju moraju biti svi alati SOC-a i IT službe i u procesu se po potrebi konzultiraju svi ljudski resursi koji su na raspolaganju tvrtki kao i pružatelji usluga ili izvori informacija. O rezultatima se izvješćuju Voditelj SOC-a i Voditelj informacijske sigurnosti.
Studije slučajeva – da bi ACME CSOC bio učinkovit, mora definirati i stalno ažurirati postojeće i raditi nove studije slučajeva temeljene na stalnim promjenama vrsta prijetnji u okruženju i usklađene sa strategijom upravljanja rizikom tvrtke. Ova procedura mora osigurati ponovljivost prikupljanja informacija i prilagodbe studije slučajeva na promjenu vrsta prijetnji. Potrebno je propisati stalan rad na poboljšanju vidljivosti i učinkovitosti ACME SOC procesa, strogo definirati način prikupljanja podataka. Potrebno je također propisati stalan rad na smanjenju lažno pozitivnih i lažno negativnih upozorenja, i poboljšavati kvalitetu informacija dobivenih dojavama o prijetnjama i novim nositeljima prijetnji. Procedura upravljanja studija slučajeva može započeti:

- kao rezultat periodične analize incidenata za koje je utvrđeno da su lažno pozitivni i da studija slučajeva zahtjeva podešavanje ili poboljšanje,
- sigurnosnom dojavom koja zahtjeva izradu nove ili podešavanje postojeće studije slučajeva,
- kao rezultat lova na prijetnje koji također zahtjeva podešavanje, poboljšanje ili izradu nove studije slučajeva,
- kao rezultat naučene lekcije nakon sigurnosnog incidenta koji je pokazao da postojeće kontrole nisu dovoljno učinkovite,
- uvođenjem nove kontrole u sustav nadzora.

Očekivani rezultati ove procedure mogu biti:
- zahtjev za ažuriranje postojeće ili izradu nove studije slučajeva koje će implementirati SOC Administrator,
- zahtjev za definiranje novih izvora sistemskih podataka ili promjenu prikaza postojećih sistemskih podataka,
- ažurirana promjena pravila rada T1/T2/T3 analitičara koji će postupak rješavanja incidenta izvoditi na primijenjen i efikasniji način,
- dodatna automatizacija odgovora na incident pomoću alata za orkestraciju,
- novi plan odgovora na incidente unutar produkcijskog okruženja.

Izvješćivanje - ono mora biti točno, relevantno i razumljivo za onog komu je namijenjeno. Izvješća koja se koriste unutar ACME SOC-a obično će sadržavati tehničke informacije razumljive ACME SOC timu a posebna izvješća za Upravu tvrtke i ostale korisnike SOC usluga moraju biti unaprijed dogovorene i prikazane korištenjem odgovarajućeg predloška. Procedura mora dobro opisati načine obrade i tumačenja prikupljenih podataka. Aktivnosti izvješćivanja obuhvaćene ovom procedurom trebale bi pomoći donositeljima odluka pružajući informacije o nadzoru praćenja operativnog i financijskog učinka ACME SOC-a, općoj sigurnosnoj vidljivosti, statusu pokazatelja ranog upozorenja na prijetnje i jasno opisati što ACME SOC radi kako bi se poboljšao i dodatno optimizirano njegov rad. Izvješćivanje je obično izvodi tehnički svim postojećim alata SOC-a prikazom nadzornih ploča (*Dashboards*) ili automatiziranim slanjem izvješća elektroničkom poštom.

Nadogradnja sigurnosnih kontrola - u ACME tvrtki, sigurnosne kontrole poslovnog informacijskog sustava održava IT služba a sigurnosne kontrole upravljačkog sustava pod upravljanjem su Odjela za proizvodnju. Stoga ova procedura mora točno opisati pod kojim uvjetima i na koji način se izvode nadogradnje sigurnosnih kontrola i o tome svakako ACME SOC mora biti obavješten unaprijed. Ovakvi zahvati često zahtijevaju dodatna podešavanja studija slučajeva pa je stoga preporučeno da se prije nadogradnje obave testiranja. IT Odjel slijedi preporuke ITIL prakse a Odjel proizvodnje mora poštovati preporuke dobavljača elemenata upravljačkog sustava.

Grupa procesa „Upravljanje SOC servisima“

Izvori sistemskih podataka i kontekstualnih podataka - Proces upravljanja zapisima i kontekstualnim podacima opisuje zahtijevane korake implementacije i stalnog održavanja izvora sistemskih zapisa i SIEMa. Postupak zahtjeva interakciju SOC tima sa vlasnicima izvora sistemskih zapisa tijekom dodavanja, ažuriranja i uklanjanja uređaja iz poslovnog ili upravljačkog sustava. Postupak se pokreće:
- na zahtjev za dodavanje, ažuriranje ili uklanjanje izvora sistemskih zapisa ili kontekstualnih podataka,
- od strane T1/T2 analitičara tokom nadzora sustava,
- na zahtjev IT Službe ili Odjela proizvodnje kao zahtjev za dodavanje ili uklanjanje uređaja koji šalju podatke u SIEM,
- kao zahtjev Odbora za upravljanje promjenama na sustavu.

Rezultat ove procedure su uvijek svježi i aktualni kontekstualni podaci kojima ACME SOC raspolaže uz održavanje maksimalne vidljivosti svih nadziranih uređaja.
Uvođenje u primjenu i podešavanja - opisuje potrebu komunikacije i dogovora oko upravljanja promjenama u slučajevima kada to može utjecati na dostupnost ACME SOC servisa u nadzoru proizvodnje. Da bi se smanjio rizik procedura mora raspisati uvjete testiranja i izdavanje dozvole za uvođenje promjena u proizvodno i poslovno okruženje i osigurati zapise o eventualnim odstupanjima, uočenim rizicima i problemima uočenih kod nove imovine povezane sa ACME SOC-om. Procedura mora propisati i poduzimanje odgovarajućih korektivnim mjera kojima će se ispravljati uočeni problemi. Ova procedura se mora odnositi na sva ACME SOC rješenja, servise, točke integracije, prilagođene alate, ažuriranja stavki konfiguracije i sistemskih zapisa, u poslovnom i proizvodnom okruženju. Primjerice, ažuriranja vezana uz proizvode ACME SOC-a mogu biti glavne ili manje nadogradnje softverskih proizvoda i njihove zakrpe kao i ažuriranja primijenjena automatski – primijenjena za SIEM, orkestrator, alat za upravljanje prijetnjama i ostale alate ACME SOC-a. Također, ovom procedurom moraju biti pokrivena i ažuriranja svih konfiguracija, studija slučajeva, SIEM pravila, orkestracijskih procesa i automatizacije odgovora. Proceduru pokreće SOC Administrator ili analitičar za prijetnje a procedura mora završiti dokumentiranim postupkom uvođenja ili podešavanja promjena unutar sustava ACME SOC-a.

Grupa procesa „Servisi nadzora i odgovora na incidente“
T1/T2/T3 procedure nadzora, trijaže i odgovora na incidente - ovi procesi zahtijevaju najveći mogući stupanj automatizacije koji se primjenjuje pomoću SOAR alata i kojim se analitičari vode pri rješavanju incidenata. Svaka od ovih procedura opisuje postupke prema fazama obrade incidenta: početna faza zaprimanja incidenta, identifikacija, zadržavanja (*engl. containment*), iskorjenjivanje (*eradication*), oporavak i naučene lekcije. Zadaci unutar pojedine faze obrade incidenata razlikuju se obzirom na vrstu incidenta i oni moraju biti posebno raspisani. Odgovor na phishing napade, sumnjiva mrežna aktivnost, sumnjive aktivnosti korisničkih računa ili grupa korisničkih računa, nenajavljene promjene konfiguracije nadziranih sustava, otkrića sumnjivih računalnih aplikacija ili malvera – svaki od ovih incidenata će zahtijevati drugačije odgovore koji se moraju slijediti propisanom procedurom. Kriteriji eskalacije sa T1 na T2, sa T2 na T3 i prema CSIRTu također moraju biti opisani unutar svake od ovih procedura. SOAR omogućuje automatsko prikupljanje kontekstualnih podataka, bilježenje vremena izvođenja svakog zadatka, automatizirani odgovor ovisno o scenariju incidenta, automatsku eskalaciju i izvješćivanje putem elektroničke pošte i kontrolne ploče.
CSIRT procedura - opisuje upravljanje sigurnosnim incidentima primljenim od T3 ili izravno prijavljenim CSIRT-u. Ova procedura koordinira i voditi analizu procjene prirode incidenta i upravlja kroz faze zadržavanja, iskorjenjivanja, oporavka i zaključenja kao koordinirani rad ACME SOC-a, Voditelja informacijske sigurnosti ali i svih ostalih zainteresiranih strana u ACME tvrtki i izvan nje. Procedura sadrži i eskalacijske kriterije u slučaju ako treba kontaktirati vanjske zainteresirane strane (nacionalni CSIRT, Policiju, vanjskog davatelja usluga pravne zaštite) kako i kontakt informacije svih važnih osoba uključenih u CSIRT proces.
Naučene lekcije - prikuplja povratnim informacije naučene tokom incidenta sa ciljem ispravljanja uočenih nedostataka i boljeg odgovora na buduće incidente. I ova procedura ima zadatak da formalizira potrebu primjene naučenih lekcija, za sve T1/T2/T3 vrste incidenata i CSIRT proces. Rezultati naučenih lekcija primjenjuju se i u studijama slučajeva, poboljšavanju sigurnosnih kontrola, mjerenju učinkovitosti ACME SOC procesa, novim strateškim inicijativama i zahtjevima za dobavljače sigurnosnih rješenja.

Ostali procesi koje preporučljivo razviti unutar ACME tvrtke jesu:

- Krizno upravljanje - u slučaju većih incidenata proces opisuje način ublažavanja posljedica i kriznu komunikaciju unutar tvrtke i u slučaju potrebe komunikacije sa javnošću;
- Forenzička analiza i sumnje na kriminalnu radnju prijevare – raspisuje postupak prikupljanja podataka potrebnih za izvođenje računalne forenzike sa ciljem da prikupljeni podaci imaju vrijednost dokaznog materijala u slučaju sudskog spora.
- Sanacija nakon incidenta - raspisuje točne i testirane postupke povratka proizvodnog i poslovnog sustava na stanje prije većeg incidenta.

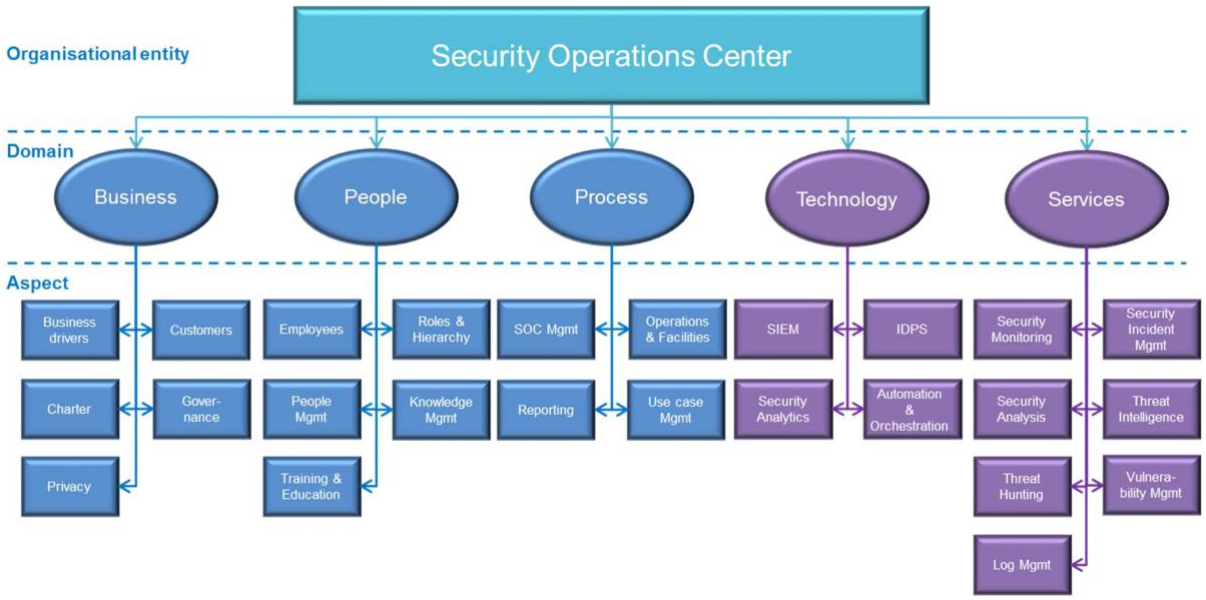
3.4. Mjerenje učinkovitosti sigurnosno operacijskog centra

Odgovornost ACME SOC-a jest da spriječi i zaustavi kibernetičke prijetnje prije nego utječu na proizvodne i poslovne procese tvrtke. Za procjenu učinkovitosti SOC-a, njegovih slabosti i snaga, mogućnosti proširenja i u konačnici ocjenu povrata investicije možemo koristiti SOC-CMM metodu [8]. Ona koristi metodu samo ocjenjivanja nivoa zrelosti i nivoa sposobnosti prema slijedećim kriterijima:

Tablica 3.5 Nivoi zrelosti i sposobnosti [10]

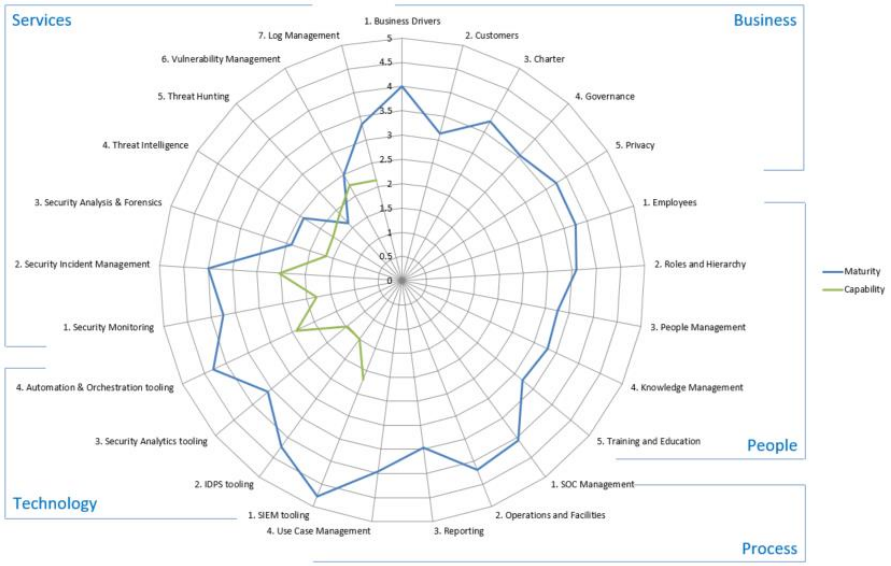
Nivo zrelosti		Opis
0.	Ne postoji	Tek započeto ili u ad-hoc fazi, ne garantira rezultate
1.	Početna	Ad-hoc faza, započet rad
2.	Upravljana	Dokumentirano stanje i rezultati dosljedni
3.	Određena	Ad-hoc upravljanje kvalitetom
4.	Kvantitativno upravljana	Stalno i sistematično mjerenje kvalitete i kvantitete rezultata
5.	Optimalna	Stalno optimiziranje i poboljšavanje učinkovitosti
Nivoi sposobnosti		**Opis**
0.	Nije započeto	Funkcija SOC-a još ne postoji i SOC nema tu mogućnost
1.	Izvodi se	SOC ima sposobnost pružanja jedino osnovnog nivoa usluge
2.	Upravljana	SOC ima sposobnost konzistentnog pružanja usluge
3.	Određena	Stalno optimizirana usluga, dobro dokumentirana i pruža dodanu vrijednost

SOC-CMM model opisan je pomoću upitnika koji pokriva odgovarajućim pitanjima sveukupno 5 područja (*engl. domains*) i 25 funkcionalnosti (*engl. aspects*), prema Slici 3.12.



Slika 3.12 SOC-CMM – Model zrelosti i sposobnosti [11]

Model opisuje ocjenjuje kvalitetu poslovnih očekivanja (Business domena) procjenom 5 funkcionalnosti, upravljanja ljudskim potencijalima SOC-a, i raspoloživom tehnologijom. Posebno dijeli procese na interne – koji upravljaju organizacijom i na servise – usluge koje SOC pruža. Plavom bojom označene su funkcionalnosti kojima se mjeri samo zrelost primjene, a ljubičastom bojom prikazane su funkcionalnosti kojima se mjeri i zrelost i sposobnost – to su SOC tehnologija i SOC servisi.
Za izvođenje samo procjene na raspolaganju je dokument [12] u obliku upitnika i nakon unesenih odgovora odgovarajućim grafičkim prikazom dobiveni su rezultati za svih 5 područja (Slika 3.13).



Slika 3.13 SOC-CMM – Detalji rezultata ACME samo procjene

Prilikom ocjene zrelosti i sposobnosti implementiranog SIEM rješenja, pitanja se odnose na ugovorenu podršku za održavanje i nadogradnju sustava, načine postizanja visoke dostupnosti, sigurnosnog spremanja podataka i testiranja oporavka nakon havarije. Potom se ocjenjuju kontrole dozvola pristupa, odvojenosti produkcijskih i testnih podataka i revizija SIEM sustava. Ocjenjuje se i nivo korištenja tehničkih mogućnosti SIEM sustava kao što su prilagođavanja prikaza sistemskih zapisa, integracija sa izvorima dojava o prijetnjama, automatizirani odgovori na prijetnje, detekcija uzorka, automatizacija dojave i integracije sa ostalim sustavima (za nadzor imovine, provjeru ranjivosti, API integracije). Istim načinom se ocjenjuju sustavi za detekciju i prevenciju upada, alati za analizu, automatizaciju i orkestraciju. Upitnik traži detaljan opis stanja SOC servisa i procesa i naravno ljudskih resursa.
Za ACME SOC napravljena je samo procjena nakon prve godine izgradnje SOC-a i sa ciljnom vrijednosti 4 (*engl. Maturity Target*). Rezultati procjene opisani su Slikom 3.13 na kojoj je vidljivo da su najlošiji rezultati postignuti su za:

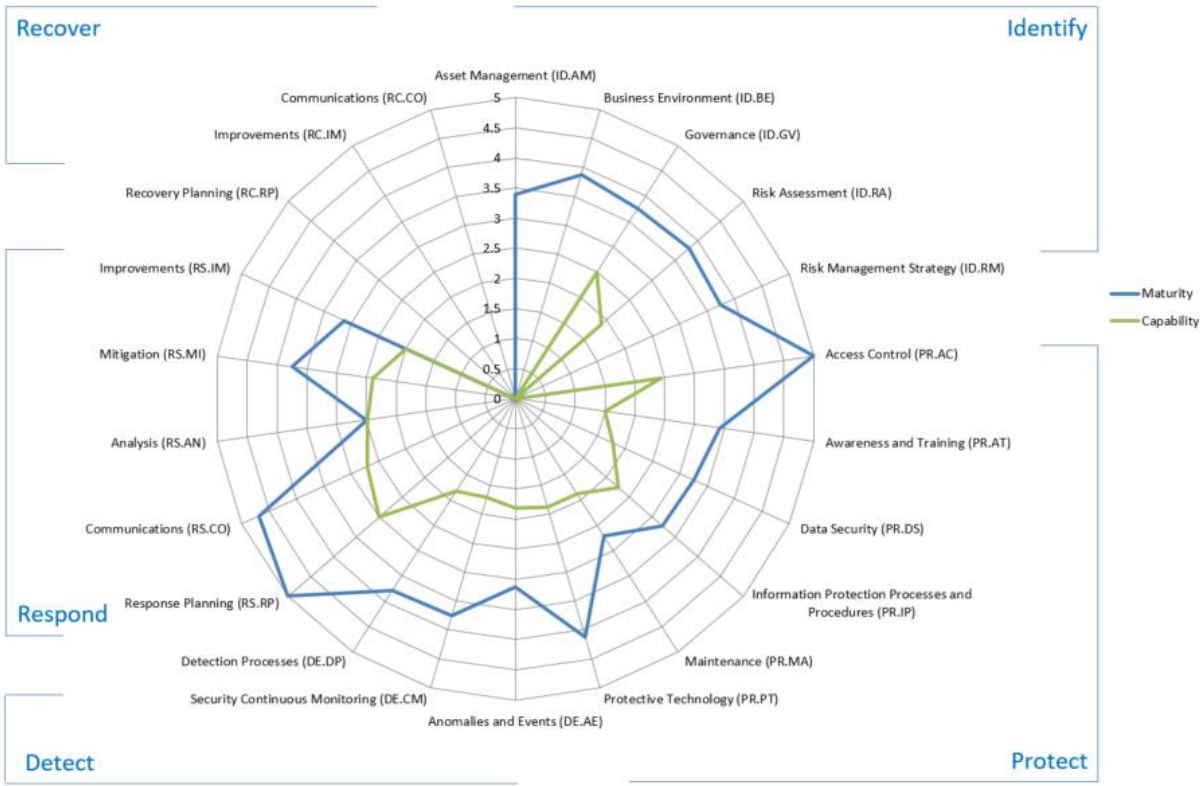
1. Lov na prijetnje (1.6) – pretpostavka uspješnosti ove funkcije jest imati odgovarajuće uvježbane ljudske resurse, razvijenu metodologiju, opisane i dokumentirane procese. Ova funkcionalnost je tek u početnoj ad hoc fazi i trebat će još vremena dok se ne razvije na odgovarajući način.
2. Dojave o prijetnjama (<2.5) – Funkcionalnost je razvijena ali odvija se bez tehničke platforme za podršku i nije integrirana sa SIEM-om i orkestratorom.
3. Analitiku i forenziku (<2.5) - Funkcionalnost je razvijena ali bez podrške za analizu mobilnih uređaja, razvijenih vlastitih studija slučajeva.
4. Upravljanje ranjivostima (2.5) – upravljanje ranjivostima ne izvodi se unutar ACME SOC-a prema odabranom ACME operativnom modelu. Ove funkcije provodi IT Služba za poslovni dio i Odjel proizvodnje za upravljačke sustave, ACME SOC koristi jedino

informacije prikupljene od ovih službi.

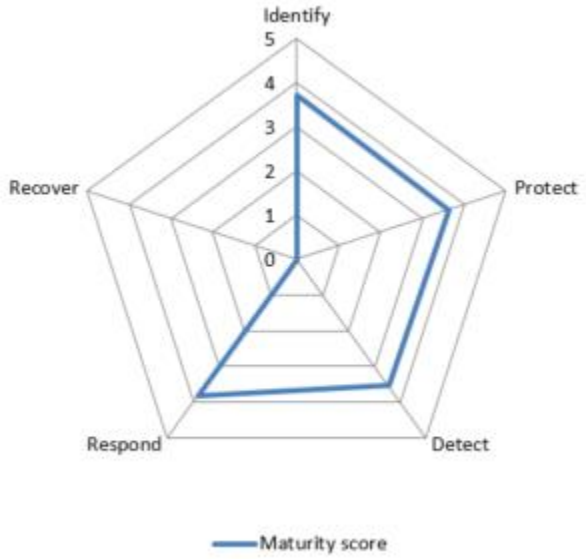
Cjelokupni uspjeh opisan je grafikonom na Slici 3.14 na kojoj se vidi da ACME SOC zadovoljava za područje tehnologije i procesa, a poboljšanja su potrebna servisima ACME SOC-a.

Slika 3.14 SOC-CMM – Ukupni rezultati ACME samo procjene

Predložak SOC-CMM okvira omogućuje i procjenu sposobnosti SOC-a na sukladnost sa NIST CSF [13] okvirom (*engl. National Institute of Standard and Technology's CyberSecurity Framework*), koji upravljanje incidentom opisuje kroz 5 faza: prepoznaj, zaštiti, odgovori, oporavi.



Slika 3.15 SOC-CMM – detalji rezultata samo procjene sukladno NIST CSF



Slika 3.16 SOC-CMM – Ukupni rezultati ACME samo procjene prema NIST CSF

Obzirom da SOC obično ima ograničenu ulogu u postupku oporavka, ova faza se ne ocjenjuje pa stoga vrijednosti na grafikonu nisu prikazane.

4. Zaključak

Kod uvođenja SOC-a svakako treba računati na čimbenik vremena potrebnog za uspostavu svih procesa, pronalaženju, zaposlenju i stalnom obrazovanju ljudskih resursa, te vremenu potrebnom da se svi alati i kontrole SOC-a integriraju na odgovarajući način. Izuzetno je važna suradnja sa vanjskim čimbenicima – u primjeru naše ACME tvrtke to je dobra suradnja sa IT Službom i Odjelom proizvodnje.

Pretpostavka ovoga rada jeste da je za uspostavu zrelog SOC-a bilo potrebno tri godine sa određenom zahtijevanom razinom usluge koja daje mogućnost razvoja unutar tog vremenskog perioda.

Ukoliko želimo ubrzati ovaj proces, vidljivo je koliki je napor, u smislu većih ljudskih resursa, potreban da bi se odgovorilo takvom zahtjevu. Najveći je napor postići zadovoljavajuću integraciju sa svim sigurnosnim kontrolama i kvalitetno uigranim procesima odgovora na sigurnosni incident – posebno kada se radi o zaštiti upravljačkih sustava.

U radu prikazano vođenje SOCa za nadzor upravljačkog i korporativnog informacijskog sustava opisane su potrebne kompetencije i objašnjen potreban broj obučenog osoblja SOCa. Opisani su potrebni SOC alati i tehničke sigurnosne kontrole koje valja međusobno integrirati, redovito održavati i fino podešavati. Opisani su procesi internog upravljanja SOC servisima, upravljanja prijetnjama te nadzora i odgovora na incidente. Učinkovitost ovih procesa valja stalno pratiti i poboljšavati da budu učinkovitiji. Na kraju je opisan i model praćenja zrelosti i sposobnosti svih komponenti SOCa koji daje smjernice za poboljšavanje.

5. Literatura

[1] Mitre Corporation Online, (2014), stranica 9, paragraf 3, "Ten Strategies of a World-Class Cybersecurity Operations Center ″, 2014. [Online] Dostupno na: https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf, [Pregledano 12. Travnja 2021]

[2] Engin Özbay, IBM Security Services, (2015), stranica 9, "Building a Security Operations Center ", [Online] Dostupno na: https://present5.com/ibm-security-services-building-a-security-operations-center/, [Pregledano 12. Travnja 2021]

[3] Gartner, (2016) The Five Models of Security Operation Centers, stranica 6, Tablica 1 [Online] Dostupno na: https://www.gartner.com/en/documents/3155618/the-five-models-of-security-operation-centers [Pregledano 12. Travnja 2021]

[4] Lacey, D. (2013). Security technology measures to mitigate APT attacks. In Advanced persistent threats how to manage the risk to your business. Rolling Meadows, IL: ISACA.

[5] MITRE ATT@CK Framework Navigator, [Online] Dostupno na:https://mitre-attack.github.io/attack-navigator/v3/enterprise/, [Pregledano 12. Travnja 2021]

[6] SYSMON MODULAR, [Online] Dostupno na: https://github.com/olafhartong/sysmon-modular, [Pregledano 10. Travnja 2021]

[7] Atomic Red Team, [Online] Dostupno na: https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1078.001/T1078.001.md, [Pregledano 10. Travnja 2021]

[8] Red Team Automation, [Online] Dostupno na: https://github.com/endgameinc/RTA, [Pregledano 10. Travnja 2021]

[9] SOC-CMM, SOC Capability Maturity Model, [Online] Dostupno na: https://www.soc-cmm.com/, [Pregledano 10. Travnja 2021]

[10] SOC-CMM, SOC -CMM Measuring Capability Maturity in Security Operations Centers, Stranica 1, [Online] Dostupno na: https://www.soc-cmm.com/downloads/soc-cmm%20whitepaper.pdf, [Pregledano 10. Travnja 2021]

[11] SOC-CMM, SOC -CMM Measuring Capability Maturity in Security Operations Centers, Stranica 2, [Online] Dostupno na: https://www.soc-cmm.com/downloads/soc-cmm%20whitepaper.pdf, [Pregledano 10. Travnja 2021]

[12] SOC-CMM, SOC -CMM Latest Version [Online] Dostupno na: https://www.soc-cmm.com/downloads/latest/soc-cmm%202.1%20-%20advanced.xlsx, [Pregledano 10. Travnja 2021]

[13] National Institute of Standard and Technology's CyberSecurity Framework, [Online] Dostupno na: https://www.nist.gov/cyberframework, [Pregledano 10. Travnja 2021]

Sažetak

Svrha ovoga rada jest opisati razloge i način uvođenja funkcije sigurnosnog operacijskog centra (SOC) kao centraliziranog načina nadzora i akcije prevencije i reakcije na sigurnosne događaje koji mogu ugroziti poslovanje tvrtke. Stoga je postupak opisan na primjeru zamišljene tvrtke ACME čiji poslovna i proizvodna funkcija isključivo ovisi o dostupnosti računalnih sustava kojima se upravlja sa ovim procesima i koja ima potrebu odgovoriti na suvremene rizike kibernetičke sigurnosti. Opisan je način odabira operacijskog modela SOC-a koji će odgovoriti ovome zadatku, način odabira potrebnih ljudskih resursa, tehnologije koja će zadovoljiti potrebe nadzora proizvodnje i poslovanja. Opisat će se procesi kojima će se osigurati da SOC ispunjava svoju funkciju i potom opisati način mjerenja učinkovitosti SOC-a koji mora pokazati njegovu učinkovitost i mogućnosti za stalna unaprijeđena u radu. Obzirom na poslovne zahtjeve i veličinu tvrtke u radu su prikazani razlozi odabira SOC-a koji za većinu svojih manje zahtjevnih funkcija koristi vanjske ljudske resurse a za važnije funkcije razvija ljudski potencijal unutar ACME tvrtke. Odabranom tehnologijom i sigurnosnim kontrolama ovaj SOC je osigurati kvalitetno pokrivanje svih ključnih proizvodnih i poslovnih procesa unutar tvrtke i onih koji se naslanjaju na računalne servise u oblaku. Primijenjena metodologija mjerenja učinkovitosti osigurat će i optimalno upravljanje i stalno poboljšavanje usluge koju ovako postavljen SOC pruža svojoj tvrtki.

Summary

This work describes the path of organizing functions of Security Operations Centre (SOC) aimed to protect business against security incidents. ACME, middle sized company been taken as example, is fully dependent of business and industrial control systems (ICS) and needs to address modern cyber security risks. Therefore, proper SOC operation model should be defined, together with capable human resources, deployed technology, and developed processes. Aim it to cover necessary SOC function and protect business. Determine and then measure maturity of such SOC will provide necessary guidance and alignment with business and risk mitigation requirements. Chosen SOC operation model uses both outsourced and in-house capabilities, focusing more on building in-house capabilities for most specialized tasks related to ICS protection. Deployed security controls should cover ACME cloud services as well. Chosen maturity metrics will assure efficient SOC management and service improvement aligned with ACME business needs.

Životopis

Igor Hitrec je rođen 1969. godine u Zagrebu, diplomirao je 1996. na Agronomskom fakultetu na smjeru Fitomedicina. Od 1994. godine stalno je bio zaposlen kao sistemski inženjer za računalne sustave, u Ministarstvu poljoprivrede i šumarstva, Agronomskom fakultetu Sveučilišta u Zagrebu i Sveučilišnom Računskom Centru (SRCE). Obavljajući sistem inženjerski posao zanima se i za računalnu i informacijsku sigurnost, a prvi posao u ovoj struci dobiva 2008. godine kao ekspert za računalnu sigurnost u tvrtki RECRO-NET. 2010. godine radi kao Voditelj Odjela za IT sigurnost u Agenciji za plaćanje u poljoprivredi, šumarstvu i ruralnom razvoju a 2013. godine seli u Ujedinjene Arapske Emirate gdje radi kao konzultant za informacijsku sigurnost u Emirates Nuclear Energy Corporation na aktivnostima izgradnje nuklearne elektrane Barakah, Abu Dhabi. 2014. godine seli u Katar gdje kao ekspert za informacijsku sigurnost radi na poslovima organizacije Svjetskog Nogometnog Prvenstva u Kataru 2022. 2018. godine prelazi u katarsku tvrtku beIN Media Group i vodi projekt izgradnje i vođenja sigurnosnog operacijskog centra sa zadaćom zaštite svih kompanija u vlasništvu Grupe koja posluje na pet kontinenata (MIRAMAX USA, Digiturk Turkey, beIN Qatar, beIN Australia, beIN Singapore, beIN France, beIN United Kingdom, beIN Miami USA, beIN Egypt).

Biography

Igor Hitrec was born in 1969 in Zagreb, he graduated in 1996 from the Faculty of Agriculture with a degree in Phytomedicine. At first, in 1994 started to work as a systems engineer for computer systems, at the Ministry of Agriculture and Forestry, the Faculty of Agriculture, University of Zagreb and the University Computing Centre (SRCE). Performing a system of engineering work, he is also interested in computer and information security. He got his first job in this profession in 2008 as a computer security expert in the company RECRO-NET. From 2010 he worked as the Head of the IT Security Department at the Paying Agency for Agriculture, Forestry and Rural Development. In 2013 he moved to the United Arab Emirates where he worked as an information security consultant at the Emirates Nuclear Energy Corporation on the construction of the Barakah nuclear power plant, Abu Dhabi. In 2014 he moved to Qatar whereas an information security expert he worked on the organization of the World Cup in Qatar 2022. In 2018 he started to work for Qatari company beIN Media Group and led the project of building and running a security operations centre with the task to protect of all companies owned by the Group who operates on five continents (MIRAMAX USA, Digiturk Turkey, beIN Qatar, beIN Australia, beIN Singapore, beIN France, beIN United Kingdom, beIN Miami USA, beIN Egypt).