EUROPEAN UNION AGENCY
FOR CYBERSECURITY

KAKO IMPLEMENTIRATI SOC IN KAJ ZAHTEVATI OD PONUDNIKOV STORITEV.

30 06 2021

VSEBINA

NAMEN IN CILJI SEMINARJA

Razumeti, zakaj je SOC pomemben za kibernetsko varnost.

Ugotoviti kako mednarodni standardi in vodila vključujejo SOC.

Spoznati ključne gradnike in funkcije SOC in kako ga prilagoditi določeni organizaciji.

Seznaniti se z različnimi modeli vzpostavitve in obratovanja SOC.

Spoznati, kako SOC prispeva k zagotavljanju skladnosti z ZinfV-1.

Spoznati stroškovne vidike vzpostavitve in obratovanja SOC.

Spoznati kako pripraviti povpraševanje za SOC storitve.

ČASOVNICA SEMINARJA

09:00 - 11:00 - Kaj je SOC in zakaj je pomemben
- Vzpostavitev SOC

11:00 - 11:20 - Odmor

11:20 - 13:00 - Upravljanje in prispevek SOC k skladnosti ZinfV-1
- Stroškovni modeli SOC
- Zahteve za ponudnike SOC

KAJ JE SOC IN ZAKAJ JE POMEMBEN

STANJE KIBERNETSKIH GROŽENJ

Kibernetske grožnje se razvijajo hitreje, kot se jim organizacije uspejo prilagajati.

Beleži se rast tako števila kot sofisticiranosti in raznolikosti kibernetskih napadov.

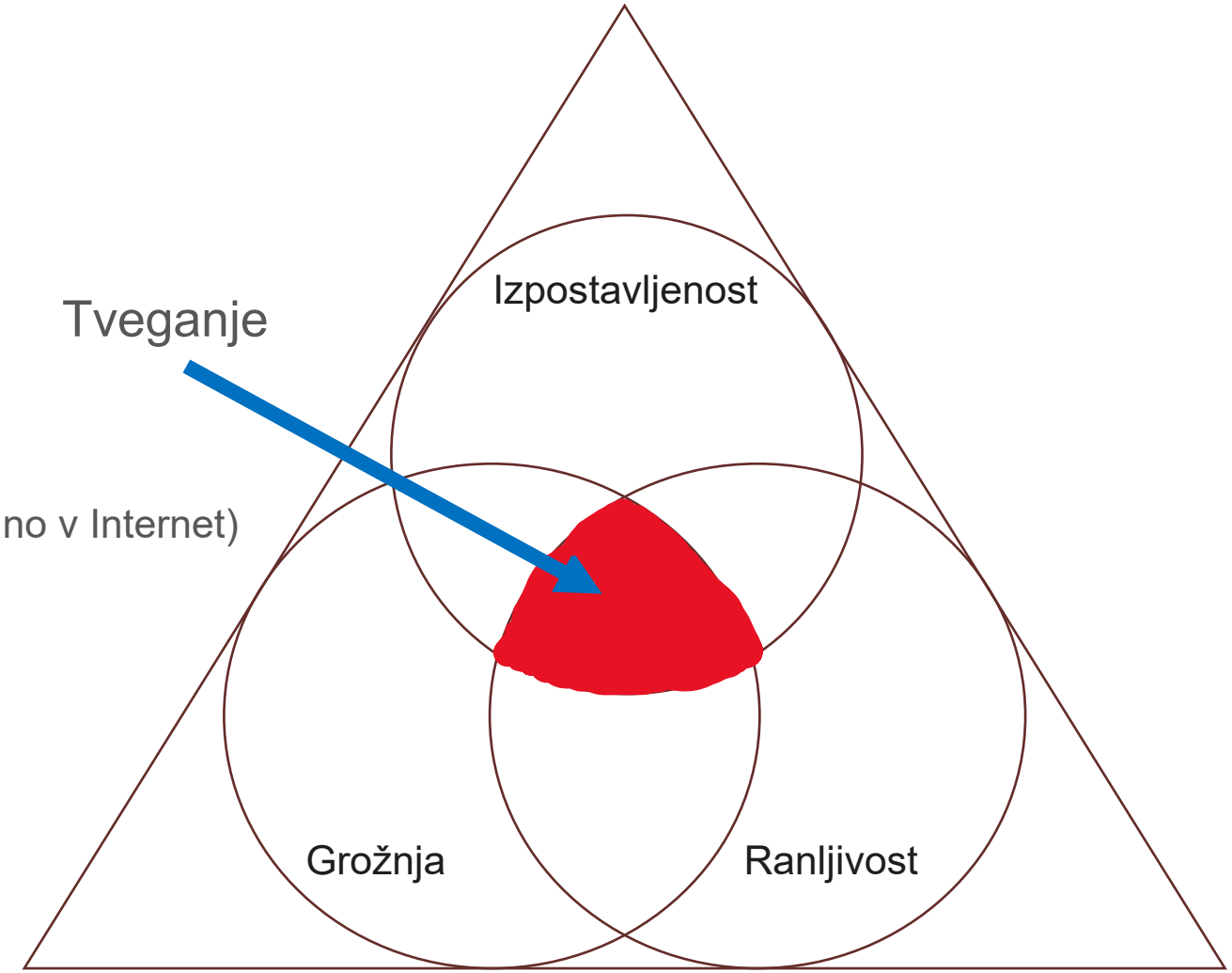
- **Ransomware** ostaja najpogostejša grožnja, razvijajo se nove tehnike napadov in večkratno izsiljevanje.
- **Phishing** ostaja eden najpogostejših vektorjev, napadalci vse pogosteje uporabljajo umetno inteligenco za zelo realistično lažno sporočilo in globoke ponaredke (*deep fake*). Phishing napad ima za posledico krajo prijavnih podatkov, sledi prijava v sisteme in dvig privilegijev s katerimi napadalec nadaljuje soje početje.
- **Napadi na storitve v oblaku**, v povezavi s phishing napadi za pridobitev dostopov, se povečujejo skladno z vse večjo uporabo oblačnih storite.
- **Izkoriščanje ranljivosti** IKT sistemov za pridobitev dostopov so stalnica.
- **Uporaba/zloraba umetne inteligence** za pripravo in izvedbo napadov je postala trend, ki se hitro razvija.
- **Napredni in državni akterji** ciljajo kritično infrastrukturo, državne organizacije in dobavne verige, predvsem, da si zagotovijo prisotnost in dostop do informacij.

KIBERNETSKE GROŽNJE IN TVEGANJA

Velika ranljivost (CVSS)

Lahko izkoriščanje (exploit)

Velika izpostavljenost (npr. neposredno v Internet)



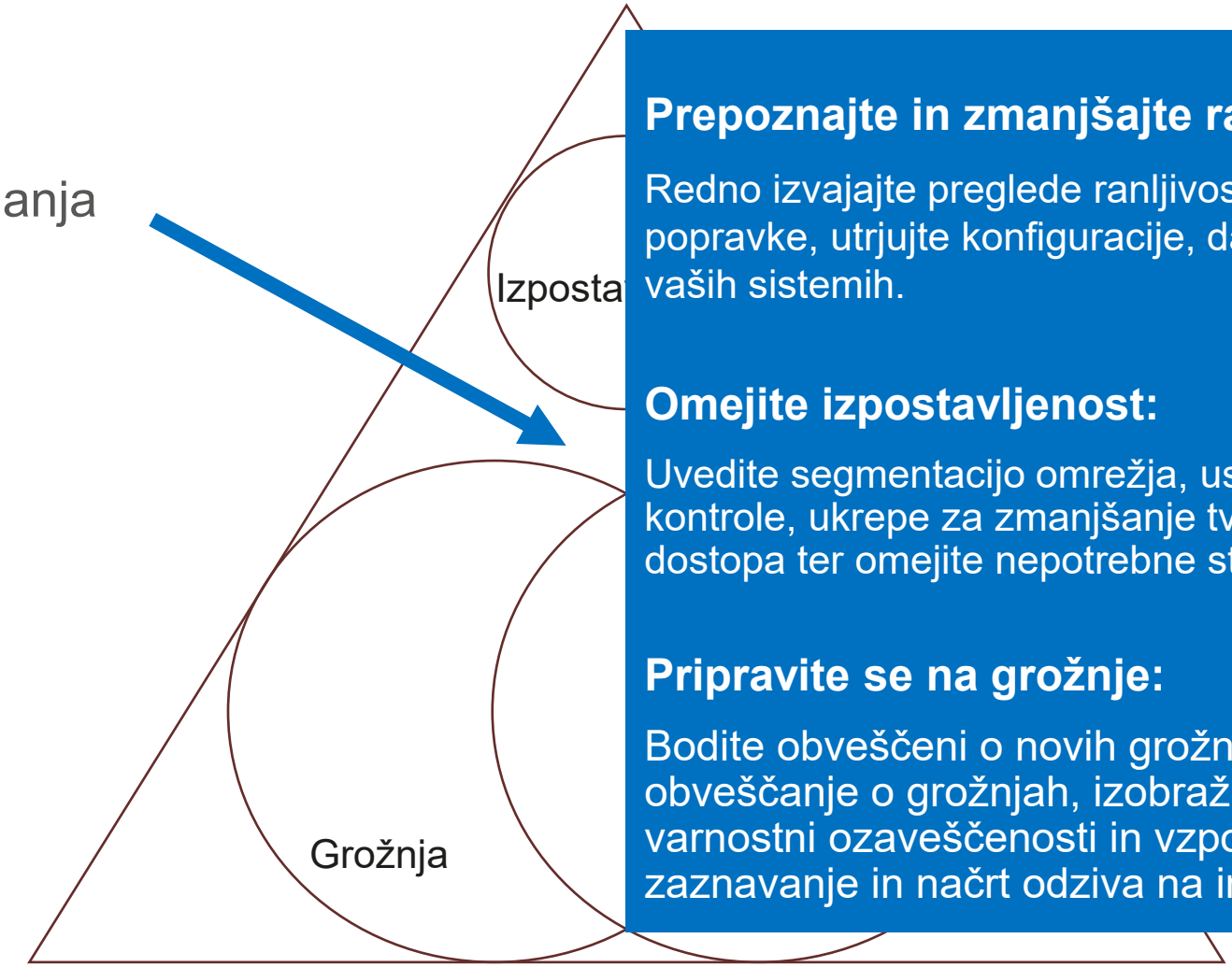
KIBERNETSKE GROŽNJE IN TVEGANJA

Ni tveganja

Velika ranljivost (CVSS)

Lahko izkoriščanje (exploit)

Ni izpostavljenosti (zaprto omrežje)



Prepoznajte in zmanjšajte ranljivosti:

Redno izvajajte preglede ranljivosti, nameščajte popravke, utrjujte konfiguracije, da zmanjšate šibkosti v vaših sistemih.

Omejite izpostavljenost:

Uvedite segmentacijo omrežja, ustrezne varnostne kontrole, ukrepe za zmanjšanje tveganj, nadzor dostopa ter omejite nepotrebne storitve in promet.

Pripravite se na grožnje:

Bodite obveščeni o novih grožnjah prek storitev za obveščanje o grožnjah, izobražujte zaposlene o varnostni ozaveščenosti in vzpostavite učinkovito zaznavanje in načrt odziva na incidente.

KIBERNETSKA VARNOST IN IT

Kibernetska varnost je specifična glede na druga IT področja.

Čeprav se kibernetska varnost povečini ukvarja z IKT, se zelo razlikuje glede na druga IT področja. Ima drugačne cilje, način delovanja, dinamiko in odgovornosti.

Za razumevanje specifik kibernetske varnosti, so pomembne sledeče značilnosti:

- Največja razlika je, da v kibernetski varnosti obstaja **inteligentni nasprotnik**. V IKT rešujemo tehnične probleme, v kibernetski varnosti pa se borimo proti ljudem, ki aktivno prilagajajo taktike, obidejo kontrole, izkoriščajo ranljivosti, uporabnike in šibke točke, so vztrajni in se vračajo na druga vrata, ko jim ene zapremo.
- **Napake** pri kibernetski varnosti lahko povzročijo velike, celo katastrofalne posledice, medtem ko so v IT napake sicer nezaželene vendar dokaj pogoste, ne tako pogubne in deterministično rešljive.
- Kibernetska varnost mora biti **multidisciplinarna** in pokrivati celoten IKT ne le enega področja, poleg tega pa še forenziko, tveganja, regulativo, obveščanje itd.

KIBERNETSKA VARNOST IN IT

Kibernetska varnost je specifična glede na druga IT področja.

- Stvari morajo istočasno delovati in biti varne. IT želi omogočati storitve, varnost želi omejiti, ne da bi pri tem preveč vplivala na uporabnost storitev. To povzroča naravno trenje med IT in varnostjo. Stališče IT je “naj deluje takoj in hitro”, stališče varnosti je “naj deluje varno, tudi za ceno okrnjenih funkcionalnosti”. Naloga varnosti je tudi **iskanje ravnotežja med tema dvema poloma**.
- Grožnje niso samo tehnične ampak so **organizacijske, psihološke in tudi regulatorne**. Napadalci izkoriščajo vse mogoče načine za dosego svojega cilja, tudi regulatorno odgovornost izkoriščajo za izsiljevanje. Tega v klasičnem IT svetu ni.
- Varnost je odvisna **od najšibkejšega člena**. V IT lahko zgradiš sistem, ki je 95 % stabilen, in je vse v redu. Pri varnosti varen sistem pomeni 0 napak, kompromitacijo pa lahko povzroči le ena napaka. Razlika je drastična. Varnost je asimetrična, napadalec mora najti eno ranljivost, branilec mora zapreti vse.

KIBERNETSKA VARNOST IN IT

Kibernetska varnost je specifična glede na druga IT področja.

- Večina IT področij je stabilnih in kontroliranih, verzije, procesi itd., dinamika kibernetske varnosti pa se **spreminja dnevno in nepredvidljivo**:
  - novi CVE-ji , nove 0-day ranljivosti,
  - nove kampanje ransomware-a vsak teden,
  - nove TTP tehnike hekerskih skupin,
- V IT je relevantno nekaj kar je: uptime, razpoložljivost, hitrost, poraba sredstev, pri varnosti je treba **dokazovati, da nečesa ni**, da se nekaj ni zgodilo, da ni bilo kompromitacije, da ni več prisotnosti napadalcev (persistance), vodstvo želi metrike za »odsotnost kompromitacije«
- Kibernetska varnost je bliže **forenziki in obveščevalni dejavnosti** kot IT-ju:
  - SOC analitiki, threat hunterji in IR ekipe pregledujejo loge ,rekonstruirajo dejanja napadalca, sledijo njihovim taktikam (MITRE ATT&CK), analizirajo motive, zbirajo indikatorje kot kriminalisti,
  - To ni monitoring delovanja IT okolja, ampak preiskovanje napadov in napadalcev.

VODILA V KIBERNETSKI VARNOSTI

Vodila (*framework*) in standardi so za kibernetsko varnost ključni, ker:

- zagotavljajo strukturiran in sistematičen pristop k kibernetski varnosti z upoštevanjem vseh vidikov,
- omogočajo skupen pojmovnik in jezik med vsemi deležniki, vodstvom, IT, varnostjo in regulatorji,
- pomagajo prevajati zakonske in strateške zahteve v konkretne procese in kontrole,
- podpirajo odločanje na podlagi tveganj in z določanjem prioritet,
- omogočajo merjenje zrelosti, zmogljivosti in spremljanje napredka skozi čas,
- olajšajo doseganje skladnosti z regulativo (npr. ZinfV-1, DORA),
- zmanjšujejo odvisnost od posameznikov in sistemsko povečujejo organizacijsko odpornost.

Vodila in standardi določajo kaj mora organizacija zagotoviti na področju kibernetske varnosti, SOC pa je eden ključnih operativnih mehanizmov, s katerim organizacija te zahteve izvaja v praksi.

VODILO NIST CSF

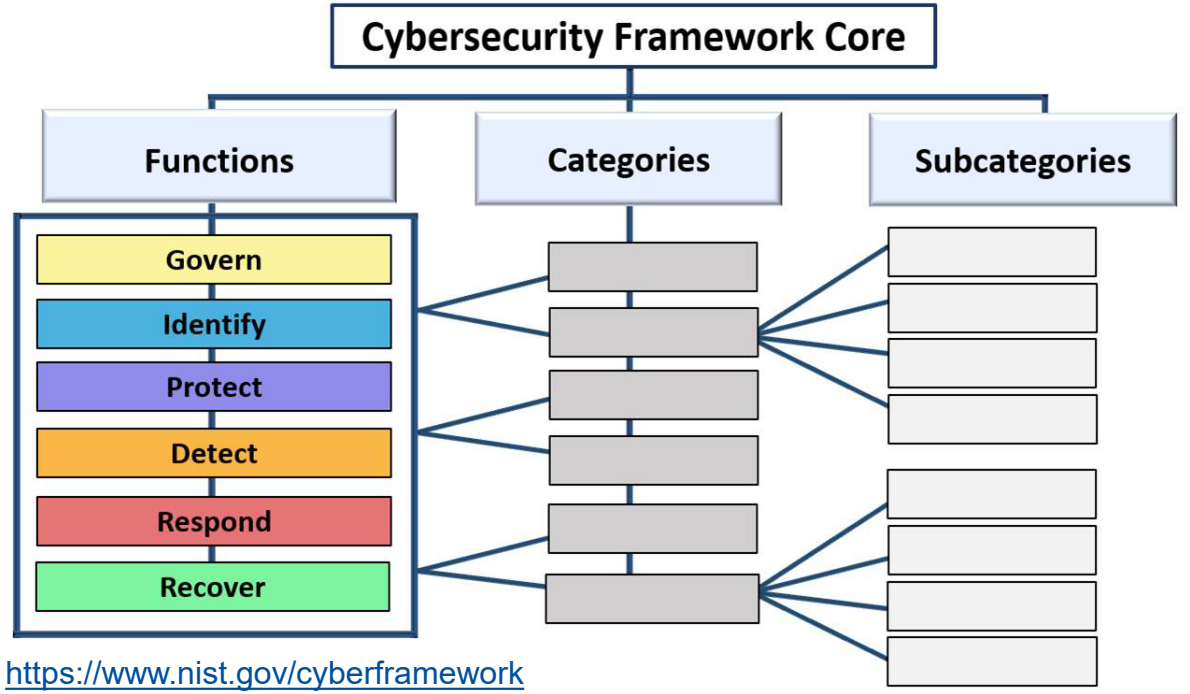
NIST CSF (Cyber Security Framework) je med najpogosteje uporabljenimi vodili

Zadnja različica CSF2.0 je izdaja februarja 2024.

NIST CSF je enostavno razumljivo strateško vodilo, ki vključuje vse potrebne elemente za kibernetsko odpornost.

NIST CSF ima 6 področij, 22 kategorij in 106 podkategorij:

- Upravljanje (*Govern*),
- Identifikacija (*Identify*),
- Zaščita (*Protect*),
- Zaznavanje (*Detect*),
- Odzivanje (*Respond*),
- Obnova (*Recover*).



https://www.nist.gov/cyberframework

VODILO NIST CSF IN SOC

Primeri, kako SOC prispeva k sledenju NIST CSF vodilom.

NIST CSF funkcija	Namen	Prispevek SOC
Identify (Prepoznava)	Razumevanje sredstev, tveganj in okolja	– Popis sistemov preko zbiranja logov in skeniranja
		– Spremljanje konfiguracij (CMDB, baseline monitoring)
		– Podpora analizi tveganj s podatki o sistemih
		– Identifikacija ključnih sredstev za monitoring
Protect (Zaščita)	Vzpostavitev zaščitnih ukrepov	– Upravljanje ranljivosti (Vulnerability scanning)
		– Implementacija EDR/AV politik
		– Spremljanje dostopov in privilegijev
		– Nadzor varnostnih konfiguracij in skladnosti
Detect (Zaznava)	Hitro odkrivanje anomalij in incidentov	– Stalno spremljanje dogodkov preko SIEM, korelacija dogodkov
		– UEBA analiza vedenja
		– NDR/ADS zaznavanje omrežnih anomalij
		– Threat hunting
Respond (Odziv)	Obvladovanje in zajezitev incidentov	– Proces odziva na incident
		– Aktivna izolacija končnih točk, blokade IP, domen, ukinitev računov…
		– Komunikacija z deležniki in poročanje
		– Forenzična preiskava
Recover (Obnovitev)	Povrnitev delovanja ter izboljšave	– Preverjanje uspešnosti obnove po incidentih
		– Analiza vzrokov (root-cause analysis)
		– Priprava “lessons learned” poročil, priporočila za izboljšave varnostne drže
		– Posodobitev IR postopkov in politik

STANDARD ISO/IEC27001

ISO/IEC 27001 je najbolj uporabljen standard informacijske varnosti

Zadnja različica ISO/IEC 27001:2022 je izdana oktobra 2022.

Obvezne zahteve za skladnost s tem standardom so:

4. Kontekst organizacije, razumevanje notranjega in zunanjega konteksta, zainteresiranih strani, obsega ISMS.

5. Voditeljstvo, zavezanost vodstva, politika informacijske varnosti, vloge in odgovornosti.

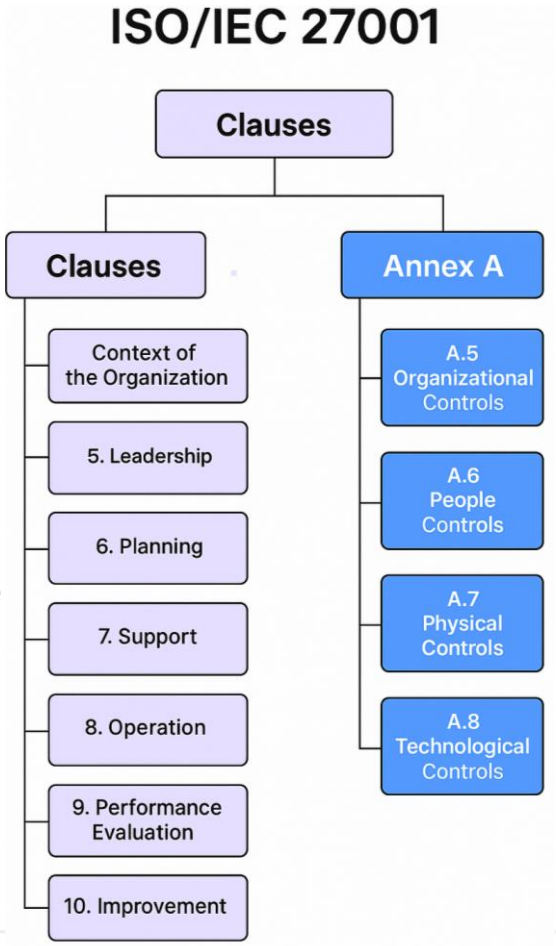
6. Načrtovanje, ocena tveganj, obravnava tveganj, cilji informacijske varnosti.

7. Podpora, viri, kompetence, ozaveščanje, komunikacija, dokumentirane informacije

8. Operacije, izvajanje ukrepov za obvladovanje tveganj, upravljanje sprememb.

9. Vrednotenje uspešnosti, spremljanje, merjenje, analiza, notranje presoje, vodstveni pregled.

10. Izboljševanje, nenehno izboljševanje ISMS, obravnava neskladnosti.



STANDARD ISO/IEC27001, KONTROLE

ISO/IEC 27001 je najbolj uporabljen standard informacijske varnosti

Kontrole standarda (93) so razdeljene v 4 kategorije:

5. Organizacijske kontrole (37), obravnavajo politike, procese in upravljanje tveganj, ki zagotavljajo okvir za informacijsko varnost v organizaciji.

6. Kontrole oseb (8), osredotočajo se na ozaveščanje, usposabljanje in odgovornosti zaposlenih ter zmanjšanje človeških napak.

7. Fizične kontrole (14), zagotavljajo zaščito fizičnih prostorov, opreme in infrastrukture pred nepooblaščenim dostopom ali poškodbami.

8. Tehnološke kontrole (34), vključujejo tehnične ukrepe, kot so nadzor dostopa, zaznavanje groženj, zaščita omrežij in sistemov ter upravljanje ranljivosti.

Skladnost z ISO/IEC 27001 organizaciji bistveno olajša izpolnjevanje zahtev ZInfV-1, saj zagotavlja sistematično upravljanje informacijske varnosti, dokazljivo obvladovanje tveganj ter zagotovljeno zaznavanje in obravnavo incidentov.

ISO/IEC27001 IN SOC

Primeri, kako SOC prispeva k skladnosti z ISO/IEC 27001.

C 27001 kontrola	Ime kontrole	Prispevek SOC
A.5.7	Obveščanje o grožnjah	SOC uporablja TI feed-e, IOC-je in korelacijo za zaznavo aktualnih groženj
A.5.24	Načrtovanje in priprava vodenja informacijskih varnostnih incidentov	SOC ima definirane postopke, playbooke, eskalacije
A.5.25	Ocenjevanje informacijskih varnostnih dogodkov in odločanje o njih	SOC izvaja triažo dogodkov in razvrščanje incidentov
A.5.26	Odziv na informacijske varnostne incidente	SOC izvaja ali koordinira tehnični odziv (blokade, izolacije)
A.5.27	Učenje iz informacijskih varnostnih incidentov	Analize incidentov, izboljšave pravil, lessons learned
A.5.28	Zbiranje dokazov	Centralizirano zbiranje in zaščita logov
A.6.8	Poročanje o informacijskem varnostnem dogodku	SOC deluje kot centralna točka za prijavo dogodkov
A.8.1	Končne naprave uporabnika	Spremljanje varnostnih dogodkov na končnih napravah
A.8.7	Zaščita pred zlonamerno programsko opremo	SOC zaznava in koordinira odziv na malware
A.8.9	Upravljanje konfiguracij	SOC zazna odklone konfiguracij (posredno)
A.8.15	Beleženje	SOC zagotavlja centralno zbiranje in korelacijo logov
A.8.16	Aktivnosti spremljanja	24/7 nadzor, zaznava anomalij in incidentov
A.8.20	Varnost omrežij	Nadzor omrežnega prometa, IDS/IPS, C2 zaznave
A.8.23	Filtriranje spleta	Spremljanje zlonamernih URL-jev in spletnega prometa
A.8.24	Uporaba kriptografije	Zaznava anomalij pri šifriranem prometu

PRIMERJAVA VODILA, STANDARDA IN ZAKONA

Področje	NIST CSF	ISO/IEC 27001	ZinfV-1
Narava	Okvir oziroma vodila najboljših praks. Prostovoljen.	Mednarodni standard, preverljivost. Prostovoljen.	Zavezujoča EU in nacionalna zakonodaja. Obvezno za zavezance.
Namen	Upravljanje kibernetskih tveganj in izboljšanje varnosti.	Vzpostavitev, upravljanje in izboljševanje Sistema upravljanja varovanja informacij (ISMS).	Povečanje kibernetske odpornosti bistvenih storitev. Določitev minimalnih varnostnih zahtev in skladnosti.
Usmerjenost	Upravljanje tveganj. Operativna in taktična	Upravljavska, procesna, sistemska.	Regulatorna skladnost, nadzor, poročanje incidentov.
Struktura	5 funkcij (ID, PR, DE, RS, RC), 106 podkategorij	Zahteve standarda in Priloga A z 93 varnostnimi kontrolami.	Upravljanje in obvladovanje tveganj, tehnični in organizacijski ukrepi, poročanje, dobavna veriga, odgovornost vodstva, kazni.
Stopnja fleksibilnosti	Zelo fleksibilen, prilagodljiv	Srednje fleksibilen – zahteva skladnost, vendar omogoča prilagoditev organizaciji	Manj fleksibilen, eksplicitne minimalne obvezne zahteve.
Poročanje incidentov	Ne zahteva poročanja, priporoča deljenje informacij.	Zahteva notranje postopke ki vključujejo poročanje.	Strogo: 24h prva prijava, 72h podrobnosti, končno poročilo.
Vodstvena odgovornost	Ni pravne odgovornosti	Vodstvo odgovorno v okviru ISMS, ni pravno odgovorno.	Vodstvo pravno odgovorno.
Dobavna veriga	Vsebuje priporočila.	Zahteve za nadzor dobaviteljev (A.15 iz stare verzije / A.5.23 v novi)	Obvezno upravljanje tveganj dobaviteljev.
Kazni	Ni kazni	Ni kazni, razen izgube certifikata.	Lahko visoke kazni, inšpekcijski pregledi.
Uporaba	Globalno, prostovoljno	Globalno, prostovoljno, pogosto zahtevano v poslovnem okolju.	EU/Slovenija, organizacije in upravljalci bistvenih storitev, ki jih zakon določa.
Dokazovanje skladnosti	Samoocenjevanje.	Certifikacijski pregledi, notranji in zunanji.	Formalno dokazovanje skladnosti pristojnim organom, inšpekcije.
Tehnični ukrepi	Priporočila	Standardne kontrole, varnostno testiranje, nadzor dostopov, kriptografija, operativna varnost ipd.	Zahtevani dokaj specifični tehnični ukrepi do nivoja njihovih ključnih funkcij.
Ciljni rezultat	Izboljšana varnostna drža in upravljanje varnosti.	Sistematičen, ponovljiv in dokumentiran ISMS z možnostjo certificiranja.	Doseganje minimalne zahtevane varnostne ravni.

SOC (SECURITY OPERATIONS CENTER)

Kaj je SOC (VOC)?

SOC je organizacijska enota, ki vključuje strokovnjake različnih profilov in kompetenc, uporablja nabor tehnologij, orodij in postopkov za neprekinjeno zaznavanje in obravnavo varnostnih dogodkov ter odziv na incidente.

Glavne naloge SOC

Osnovna naloga SOC je, da izvaja stalni nadzor kibernetskih varnostnih dogodkov, zaznava grožnje v organizaciji in izven nje in se učinkovito odziva na incidente. Zagotavlja čim krajši čas od pojave do zaznave in odziva, preprečuje in zmanjšuje vpliv napadov ter zagotavlja delovanje storitev.

Širša vloga SOC

SOC ima lahko tudi širšo vlogo, lahko analizira ranljivosti, izvaja varnostne preglede in teste, spremlja nove grožnje in skrbi za stalne izboljšave varnostnih mehanizmov, ozaveščа zaposlene itd. Aktivnost SOC so lahko zelo raznolike, odvisno od organiziranosti.

KAJ NE SPADA MED NALOGE SOC

To niso naloge SOC čeprav so v kontekstu kibernetske varnosti:

- Določanje strategije varnosti, razvoj varnostnih politik, odločanje o tveganjih, proračun za varnost - to je naloga vodstva informacijske varnosti, CISO, upravljanja tveganj
- Upravljanje IKT infrastrukture in odpravljanje ranljivosti - to je naloga IT oddelka, infrastrukture in programskih rešitev
- Fizična varnost in nadzor objektov - to je naloga oddelka fizične varnosti, zaželeno je da oddelka operativno tesno sodelujeta
- Upravljanje skladnosti in revizije - to je naloga oddelka za skladnost, ima pa skladnost velik vpliv na delo SOC.

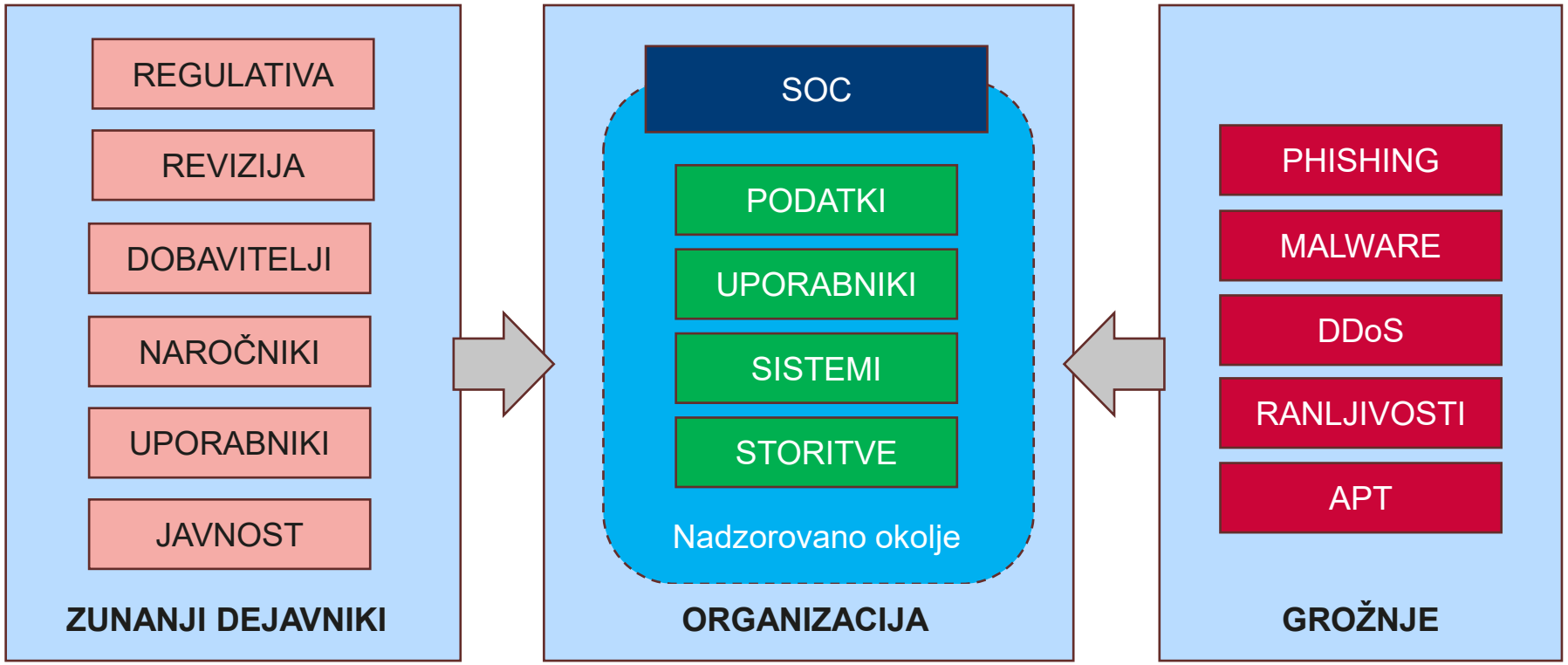
POSLANSTVO SOC

SOC je namenjen temu, da podpira neprekinjeno delovanje organizacije, zato se SOC vzpostavi in se njegove naloge organizira v skladu s tem.

Na vzpostavitev SOC vplivajo **zunanji dejavniki**, pozitivni, regularni, med katerimi je tudi regulativa (ZinfV-1, DORA,…)

ter

negativni, neregularni, ki predstavljajo namerno povzročene grožnje.



ZRELOST SOC IN OBSEG NALOG

Nabor nalog SOC lahko zajema od osnovnih nalog do širokega nabora naprednih aktivnosti. Zrelost SOC razvrstimo v 4. nivoje (po NIST, Gartner, SANS, Microsoft.)

Osnovni SOC (Basic/ Reactive) je neformalni, izvaja le najnujnejši nadzor, deluje reaktivno

- Zbiranje omejenih logov, ročno spremljanje brez korelacij, osnovna obravnava dogodkov, ni 24/7.
- Primerno za manjše organizacije v zgodnji fazi vzpostavljanja SOC, minimalna ali delna skladnost z ZinfV-1.

Operativni SOC (Structured / Managed) je formalno urejen, ima izdelane operativne postopke

- Implementiran SIEM s korelacijo, EDR, osnovni CTI, nadzor identitet, določeni postopki odzivanja.
- Primerno za srednje organizacije z zmerno izpostavljenostjo, srednjo zrelostjo, skladnost z ZinfV-1.

Napredni SOC (Defined / Integrated) izvaja napredno analitiko in je proaktiven

- Napredni sistemi detekcije, SIEM, EDR, NDR/ADS, korelacija in avtomatizacija nadzor identitet, oblaka, CTI, ločene analitične funkcije in nivoji, ISO 27001, ZinfV-1
- Primerno za kritično infrastrukturo, zavezance ZinfV-1.

Celovit SOC (Optimized / Inteligent),

- Napredni sistemi detekcije XDR, visoka stopnja avtomatizacije, poglobljen in lastni CTI, celovit IR, forenzika, malware analiza, strateška funkcija v organizaciji ali ekosistemu.
- Primerno za najzahtevnejše in izpostavljene organizacije, nacionalne ali panožne SOC centre.

VZPOSTAVITEV SOC

NAČELA PRI VZPOSTAVITVI SOC

Osredotočenost na bistvene storitve

Bistvene storitve so prioriteta.

Tarča je lahko katerikoli del IT sistema, vključno z dobavitelji.

Napad se lahko širi.

Izhajanje iz tveganj

Dejavnosti SOC naj temeljijo na osnovi ocene tveganj.

Prioritetna obravnava groženj s potencialno visokim vplivom na storitve.

Začetne zmogljivosti

Najprej funkcije za zaznavanje incidentov in odziv nanje. Ostale dodajamo postopoma.

Nekatere funkcije vzpostavimo v organizaciji, druge najemamo.

Odgovornosti in pristojnosti

Podeljene s strani vodstva.

Jasno določeno kdo izvaja, sodeluje, načini eskalacije, poročanja.

Koordiniran odziv na incidente

Po zaznavi incidenta mora steči vnaprej pripravljen postopek reševanja.

Pridobivanje in izmenjava informacij

Povezanost z zunanjimi deležniki pri pridobivanju in deljenju informacij, ki so pomembne za zaznavanje in reševanje incidentov.

Neodvisnost in povezanost SOC in IT

Neodvisnost SOC funkcije od IT.

Tesna operativna povezanost SOC in IT.

Neprestani razvoj

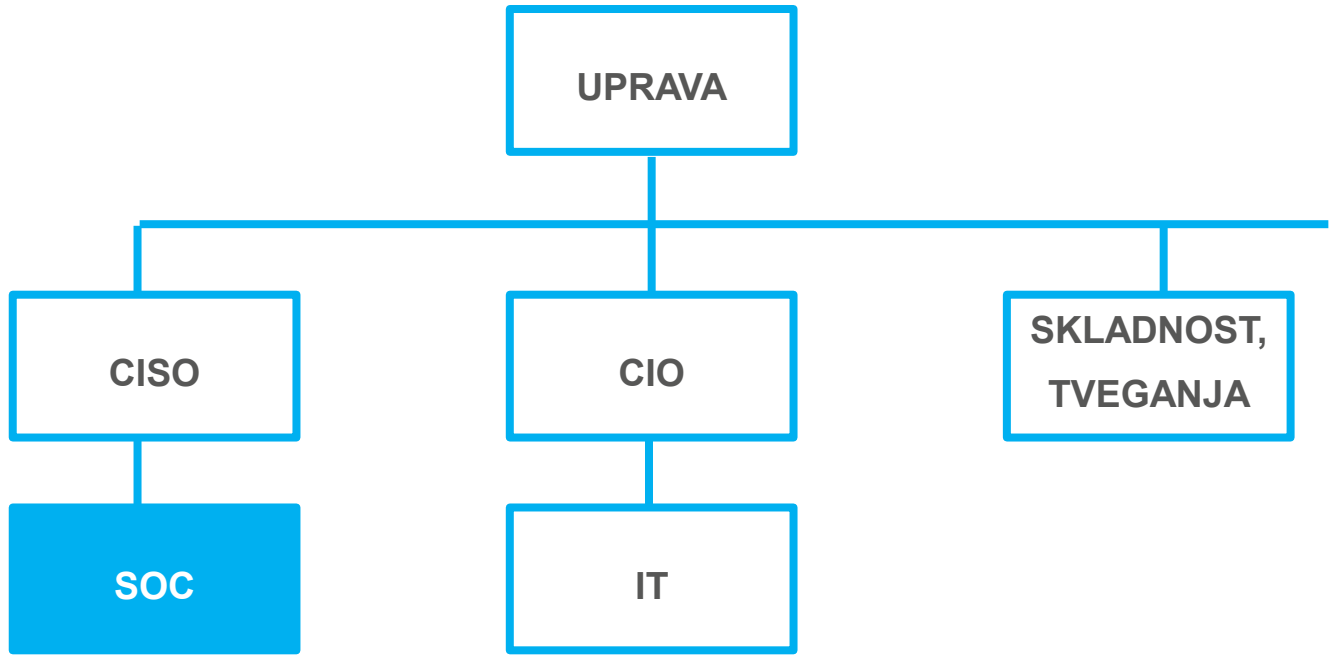
SOC ni samo projekt temveč proces.

Dodajanje funkcij v SOC, povečevanje zmogljivosti in zrelosti.

SOC V ORGANIZACIJSKI STRUKTURI

SOC je operativna varnostna funkcija zato mora biti organizacijsko umeščen tako, da ima jasno odgovornost, ustrezna pooblastila za nadzor in je ločen od izvajanja IT.

SOC običajno poroča vodji informacijske varnosti (CISO), nadzorno in usmerjevalno vlogo pa ima oddelek za tveganja, notranja revizija, skladnost.



PRISTOJNOSTI IN ODGOVORNOSTI

Pristojnosti in odgovornosti posameznih deležnikov pri zagotavljanju informacijski varnosti določa RACI matrika (ang. **R**esponsible, **A**ccountable, **C**onsulted, **I**nformed).

Zahteva ZinfV-1: organizacija mora imeti jasne postopke, odgovornosti in nadzorere.

Aktivnost / Vloga	SOC	CISO	CIO/IT	Pravna, Skladnost	Tveganja	PR	Vodstvo	SI-CERT SIGOV-CERT
24/7 monitoring kritičnih sistemov	R	A	I	–	–	–	–	–
Upravljanje SIEM/SOAR	R	A	C	–	–	–	–	–
Zaznavanje incidentov	R	A	I	–	–	–	–	I
Korelacija logov in alarmov	R	A	C	–	–	–	–	–
Skeniranje ranljivosti	R	A	C	–	–	–	–	–
Odprava ranljivosti	C	A	R	–	–	–	–	–
Penetracijski testi	R	A	C	–	–	–	–	–
Poročanje	R	I	I	–	I	–	I	–

Odziv

Primer RACI matrike za spremljanje varnostnih dogodkov in ranljivosti

PRISTOJNOSTI IN ODGOVORNOSTI

Primer RACI matrike za odziv na incidente

Aktivnost / Vloga	SOC	CISO	CIO/IT	Pravna, Skladnost	Tveganja	PR	Vodstvo	URSIV, SI-CERT
Triaža incidenta	R	A	C	I	–	–	I	–
Raziskava incidenta (L2/L3)	R	A	C	I	–	–	I	–
Odpravljanje incidenta	C	C	R	I	–	–	I	C
Odločanje o eskalaciji	R	A	C	I	–	I	C	C
Priprava obvestila SI-CERT, SIGOV-CERT	R	A	C	C	–	C	I	I
Pravni ukrepi (npr. zlorabe, atribucija)	C	C	C	R	I	–	A	–
Komuniciranje znotraj in navzven	C	A	C	C	R	R	I	–
Post-incident poročilo	R	A	C	C	I	I	I	I

ZNAČILNOSTI ORGANIZACIJ

Organizacije (zavezanci) se razlikujejo glede na dejavnosti, pomembnosti svojih storitev, velikosti, proračunu, zrelosti informacijske varnosti, kadrovskih zmogljivostih itd.

Značilnosti	Opis
Velikost organizacije	Število zaposlenih, število in lokacij in geografija,
Dejavnost	Komunalne storitve, energetika, digitalne storitve, državna in lokalna uprava, spletne storitve
Stopnja pomembnosti storitev	Bistvene ali pomembne storitve, delež na trgu, odvisnost uporabnikov in družbe
Obseg in nivo tveganj	Kritičnost poslovnih procesov, vrste podatkov, izpostavljenost
Regulatorne zahteve	ZinfV-1, ZVOP2, DORA, ISO 27001, ISO 22301, IEC 62443, drugi industrijski standardi
Sistemi in organiziranost IT	Kompleksnost IT okolja, operativni model IT/OT, zunanje izvajanje
Zrelost informacijske varnosti	Nivo vodenja IV, uvedene politike, procesi, standardi, organizacijski in tehnični ukrepi
Kadrovske zmožnosti	Razpoložljivost varnostnih analitikov, forenzikov, IR inženirjev
Režim delovanja	Non-stop 24/7, delovni čas, kampanje
Proračun	Višina sredstev, capex/opex

Organizacija svoje značilnosti upošteva pri načinu uvedbe SOC.

MODELI VZPOSTAVITVE SOC

Model SOC	Nadzor, avtonomija	Stroški	Zahtevani kadri	Hitrost vzpostavitve	Prilagod-ljivost	Prednosti	Slabosti
1. Interni SOC	Zelo visok	Zelo visoki CAPEX + OPEX	Visoka potreba po kadrih (24/7)	Počasna (6–24 mesecev)	Visoka	Popoln nadzor, specifična prilagoditev, hitri odzivi	Najdražji model, težko zagotavljanje kadrov
2. Panožni SOC	Srednji	Srednji CAPEX + OPEX	Srednja potreba po kadrih	Srednja (3–12 mesecev)	Visoka, na panogo	Izmenjava groženj, nižji stroški, panožna specializacija	Manj individualne prilagoditve
3. Zunanji SOC (MSSP)	Nizek–srednji	Nizek CAPEX višji OPEX	Minimalna interna potreba	Zelo hitra (1–3 mesece)	Srednja, odvisno od ponudnika	Cenovno ugodno, 24/7, dostop do različnih strokovnjakov	Manjši nadzor, odvisnost od izvajalca
4. Hibridni SOC (MSSP + interni)	Srednji–visok	Srednji pretežno OPEX	Srednja potreba po kadrih	Hitra (2–6 mesecev)	Srednja	Ravnotežje stroškov in kontrole, zelo prilagodljiv	Zahteva jasno RACI in upravljanje pogodbe
5. Centralizirani SOC (holding, ministrstvo + organi v sestavi)	Visok-nizek	Srednji CAPEX + OPEX	Srednja-visoka	Počasna, postopna (6–24 mesecev)	Srednja	Optimiziran strošek, enotni standardi, izmenjava groženj, sinergije	Kompleksno upravljanje, notranja birokracija

TEHNOLOŠKA ORODJA V SOC (1)

SOC za svoje delovanje potrebuje zmogljiva tehnološka orodja, ki omogočajo zaznavo širokega spektra varnostnih dogodkov, poglobljen vpogled vanje, čim hitrejšo analizo, sprejem odločitev ter izvedbo ustreznega odziva glede na naravo dogodka.

Tehnološka orodja omogočajo:

- zajemanje in obdelavo ogromne količine podatkov v realnem času, generiranje varnostnih dogodkov,
- analiziranje varnostnih dogodkov, zaznavanje groženj in generiranje alarmov-incidentov,
- zagotavljanje informacij analitikom za analizo in odločanje,
- Izvedbo odziva, aktivnosti zamejitve varnostnega incidenta.

Tehnološka orodja so bodisi nameščena v okolju organizacije ali pa se uporabljajo v oblaku, kjer je vse več rešitev povezanih z UI.

TEHNOLOŠKA ORODJA V SOC (2)

Tehnologija	Opis
SIEM Security Information and Event Management)	Centralizira zbiranje, korelacijo in analizo dnevniških zapisov iz različnih virov (strežniki, požarni zidovi, aplikacije). Omogoča zaznavanje anomalij in ustvarjanje alarmov.
EDR/XDR Endpoint/Extended Detection and Response	EDR spremlja in analizira dejavnosti na končnih točkah (računalniki, strežniki), XDR pa razširi to funkcionalnost na več virov (omrežje, e-pošta, oblak). Omogoča izolacijo okuženih naprav in forenzično analizo.
NDR Network Detection and Response	Analizira omrežni promet za zaznavanje sumljivih vzorcev, ki lahko kažejo na napade. Uporablja se za odkrivanje naprednih groženj, ki jih tradicionalni požarni zidovi ne zaznajo.
SOAR Security Orchestration, Automation and Response	Avtomatizira odzivne procese v SOC, npr. samodejno blokiranje IP naslovov, obveščanje ekip, sprožanje skript. Povezuje različna orodja in omogoča hitrejši odziv na incidente.
CTI Cyber Threat Intelligence Platforma	Zbirajo in analizirajo informacije o aktualnih grožnjah (indikatorji kompromitacije, TTP napadalcev). SOC uporablja te podatke za proaktivno zaščito in izboljšanje detekcijskih pravil.

TEHNOLOŠKA ORODJA V SOC (3)

Tehnologija	Opis
VM Upravljanje ranljivosti	Orodja za skeniranje sistemov in aplikacij z namenom odkrivanja znanih ranljivosti. Pomagajo pri prioritizaciji popravkov in zmanjševanju napadalne površine.
Zavajanje napadalcev (honeypots)	Uporabljajo se za zavajanje napadalcev – ustvarijo lažne sisteme ali podatke, ki napadalce pritegnejo in razkrijejo njihove metode.
DLP Data Loss Prevention	Preprečuje nenamerno ali zlonamerno uhajanje občutljivih podatkov iz organizacije. SOC spremlja alarme in preiskuje morebitne kršitve.
Sandboxing	Izolirano okolje za analizo sumljivih datotek (npr. priponk iz e-pošte), kjer se preveri njihovo vedenje brez tveganja za produkcijske sisteme.
Upravljanje incidentov (Ticketing)	Sistemi za beleženje, sledenje in upravljanje varnostnih incidentov. Omogočajo dokumentiranje ukrepov, komunikacijo med ekipami in poročanje.

KADRI IN ORGANIZACIJA SOC

SOC je operativna služba in kadri so zelo pomemben del operacije.

Praviloma SOC sestavlja več nivojev analitikov ter podpornih specializiranih vlog.

Tehnologija	Opis
Analitik 1. ravni (L1)	Izvajajo triažo, stalno spremlja alarme, je “vratar”, ki prvi oceni pomen alarma, ga obogati s kontekstom (npr. preveri, kateri sistem je tarča, kakšna je grožnja) in odloči, ali gre za resen incident ali ne. Če problema ne more rešiti na tej ravni, ga eskalira analitikom višjega nivoja.
Analitik 2. ravni (L2)	Prevzamejo resnejše dogodke od L1, izvede poglobljeno analizo, pregleda dodatne podatke, uporabi obveščevalne podatke o grožnjah (CTI). V primeru incidenta izvede takojšnje odzivne ukrepe: npr. odklop sistema, blokiranje IP naslovov in domen. L2 vodi tehnični odziv na incident in sodeluje z drugimi IT ekipami v vseh fazah odziva. Če naleti na zelo kompleksno grožnjo (npr. napredni trajni napad APT), vključi tudi L3 ali dodatne strokovnjake.
Analitik 3. ravni (L3)	So najbolj kompetentni in izkušeni člani ekipe, ki obvladajo napredne napade. Prevzemajo eskalirane incidente velikih razsežnosti in vodijo forenzične preiskave. Poleg tega proaktivno iščejo prikrite napadalce v omrežju (t. i. threat hunting) in izvajajo varnostne preglede ter teste vdorov.
Vodja SOC	Vodi celotno SOC ekipo in skrbi za organizacijo procesov. Odgovoren je za kadrovanje in usposabljanje analitikov, za določanje pravilnikov in postopkov odziva na incidente, komunikacije ob krizi ter zagotavljanje poročanja vodstvu. Vodja SOC skrbi tudi za skladnost operacij z varnostnimi standardi in zakonodajo ter pogosto poroča neposredno CISO oz. vodstvu o stanju varnosti.
Ekspertni strokovnjaki	To so lahko reverse engineering strokovnjaki (za analizo zlonamerne kode), forenziki (za poglobljeno analiziranje vdorov in zbiranje dokazov) in inženirji varnosti (za vzdrževanje varnostne infrastrukture in razvoj novih zaščit). Velike organizacije imajo v SOC tudi ločeno ekipo za CTI , ki spremlja zunanje vire o napadalcih in opozarja SOC na nove tehnike ali specifične grožnje.

STANDARDNI OPERATIVNI POSTOPEK

STANDARDNI OPERATIVNI POSTOPEK ZA OBRAVNAVO VARONOSTNIH DOGODKOV IN INCIDENTOV

1.Namen in področje uporabe

Ta dokument določa postopke za zaznavanje, potrjevanje, obravnavo, dokumentiranje in poročanje varnostnih incidentov v informacijskih sistemih organizacije, skladno z zahtevami Zakona o informacijski varnosti (ZInfV-1).

Ta SOP velja za vse zaposlene in zunanje izvajalce, ki sodelujejo pri upravljanju, nadzoru ali uporabi informacijskih sistemov organizacije.

2. Vloge in odgovornosti

- SOC analitik: Prevzame in triažira varnostni dogodek, potrdi in kategorizira incident. Izvede začetno preiskavo in sproži odzivne ukrepe.
- Vodja SOC: Odloča o eskalaciji, potrdi resnost incidenta, koordinira aktivnosti v organizaciji in z zunanjimi deležniki.
- CISO: spremlja aktivnosti, usmerja, poroča vodstvu in regulatorju
- IT podpora: Izvede tehnične ukrepe (izolacija sistemov, ponovne namestitve, povrnitev iz varnostnih kopij).
- Pravna služba: Svetuje glede pravnih obveznosti (npr. obveščanje prizadetih oseb, sodelovanje z organi).

3.Postopek obravnave incidenta

Zaznava incidenta

- Vir: SIEM, EDR, NDR, CTI, prijava uporabnika, skrbnika, zunaniega partnerja.
- SOC analitik pregleda alarm in preveri verodostojnost.

Standardni operativni postopek

Kategorizacija in ocena resnosti

- Uporabi se definiran model za razvrščanje (npr. nizka/srednja/visoka kritičnost).
- Če incident vpliva na zaupnost, celovitost ali razpoložljivost ključnih storitev, se označi kot pomemben (ZInfV-1, 30. člen).

Ukrepanje

- Aktivacija odzivne skupine (navedeni vodja in člani, kontaktni podatki)
- Izolacija prizadetih sistemov (navedeni načini tu ali v prilogah, kdo jih izvede)
- Zbiranje dokazov (dnevniki, posnetki pomnilnika, mrežni promet).
- Obveščanje notranjih deležnikov (zaposleni, vodstvo, pravna služba, IT).

SOC IN NIST CSF

SOC proces je pretežno del NIST CSF (Cybersecurity Framework) faz Odkrivanje in Odzivanje.

Upravljanje	Priprava	Preprečevanje	Odkrivanje	Odzivanje	Obnovitev
SUVI, politike in odgovornosti	Grožnje in tveganja	Identitete, pravice	Spremljanje dogodkov	Načrtovanje odzivanja	Načrtovanje obnovitev
Skladnost	Sredstva	Osveščanje, izobraževanje	Analiza odstopanja	Odprava incidentov	Izvajanje obnovitev
Strateško odločanje	Strategija in prioritete	tehnologije	Zaznava incidentov	Analiza odzivanja	Analiza stanja

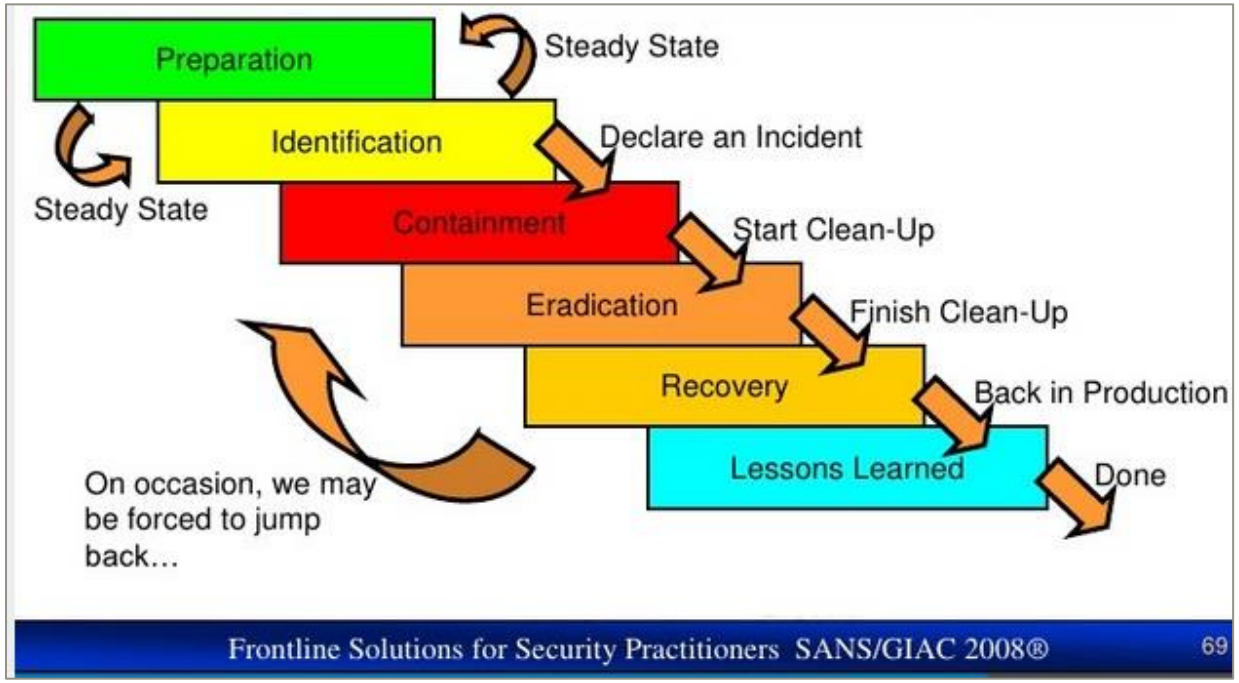
SOC

SOC IN FAZE ODZIVANJA NA INCIDENT

SOC proces je vključen v vse faze odzivanje na incident.

Načrt odzivanja vsebuje navodila za specifične tipe incidentov po fazah:

1. Priprava
2. Zaznavanje in analiza
3. Zajezitev
4. Odprava
5. Obnovitev
6. Aktivnosti po incidentu



https://www.sans.org/security-resources/glossary-of-terms/incident-response

KAKO PRIČETI Z VZPOSTAVITVIJO SOC (1)

(za zavezance ZinfV-1)

Razumevanje zakonskih zahtev ZinfV-1 in kontekst

- Bistvene storitve organizacije
- Obveznosti glede nadzora zaznavanja, poročanja in upravljanja incidentov
- Tehnični in organizacijski ukrepi

Analiza tveganj

- Identifikacija groženj za bistvene storitve
- Izpostavljenost in ranljivosti IT/OT sistemov
- Ocena vpliva na poslovanje
- Scenariji kibernetskih incidentov

Določitev obsega in nivoja SOC za zaščito bistvenih storitev

- IKT sistemi, ki omogočajo te storitve
- OT/SCADA procesni sistemi
- Zbirke podatkov
- Identitete in dostopi
- Revizijske sledi

KAKO PRIČETI Z VZPOSTAVITVIJO SOC (2)

(za zavezance ZinfV-1)

Izbira SOC modela

Kriteriji
- Obseg
- Potrebna zmogljivost, zrelost
- Razpoložljivost kadrov
- Proračun
- Režim delovanja

Model
- Interni
- Panožni
- Zuanji (MSSP)
- Hibridni
- Centralizirani

Vzpostavitev krovnega procesa, vloge, odgovornosti

- Vodenje SOC
- Odgovornosti SOC-IT-vodstvo
- Postopki izvajanja
- Postopek odziva na incidente
- RACI matrike

Vzpostavitev tehnologij

- SIEM za zbiranje revizijskih sledi, korelacijo dogodkov in alarme
- EDR za končne naprave
- NDR/IDS za spremljanje omrežja
- Zaznavanje ranljivosti
- Obveščanje o kibernetskih grožnjah
- SOAR za avtomatizacijo

KAKO PRIČETI Z VZPOSTAVITVIJO SOC (3)

(za zavezance ZinfV-1)

Določitev operativnih postopkov

- Monitoring in obravnava dogodkov
- Zaznavanje ranljivosti
- Nadzor identitet in dostopov
- Operativno poročanje
- Prijava incidentov
- Sodelovanje z organi (CERT, Policija)

Poročanje in dokazila skladnosti

- Upravljanje varnostnih dogodkov
- Upravljanje sprememb konfiguracij
- Upravljanje ranljivosti
- Postopki odzivanjan na incidente
- Poročanje o incidentih

Izboljševanje

- Usposabljanje SOC analitikov
- Izvajanje kibernetskih vaj
- Vključevanje novih sistemov v monitoring
- Izboljšave analitičnih detekcijskih pravil
- Posodabljanje postopkov

UPRAVLJANJE IN PRISPEVEK SOC K SKLADNOSTI Z ZINFV-1

UPRAVLJANJE SOC

Upravljanje SOC je zahtevna naloga, ker mora SOC obvladovati nepredvidljive dogodke.

Upravljanje SOC vključuje:

- Procesi in postopki
- Kadri
- Tehnologije in detekcije
- Incidenti
- Kakovost, KPI
- Skladnost
- Poročanje, komuniciranje

Ključni cilj upravljanja SOC je zagotoviti, da ta učinkovito zaznava, analizira, se odziva in preprečuje kibernetske grožnje na način, da podpira poslovno strategijo in skladnost z zakonodajo in standardi (ZInfV-1, DORA, ISO 27001,…).

VLOGA SOC V ORGANIZACIJI

SOC ima lahko v organizaciji določeno vlogo na vse treh ravneh: **operativni, taktični in strateški** ravni.

Ta vloga se lahko z zrelostjo SOC tudi spreminja in s časom preraste iz čisto operativne funkcije v vlogo, ki je bolj vpeta v poslovno strategijo.

SOC se vzpostavi z določenim razlogom in nameni, ki izhajajo iz tveganj in regulatornih zahtev ZinfV-1.

Potrebno je poslovno upravičiti investicijo in stroške.

ZMOGLJIVOST IN ZRELOST SOC

Zmogljivost (Capability)

Opredeljuje **kaj SOC zmore**, nabor in funkcionalno sposobnost izvajanja varnostnih aktivnosti, od osnovnega monitoringa, odzivanja, naprednega iskanja groženj, testiranja ranljivosti itd.

Zrelost (Maturity)

Opredeljuje **kako dobro oziroma kvalitetno SOC izvaja** svoje delo, ali je posamezen proces vzpostavljen, dokumentiran, merjen in izboljševan.

	Zmogljivost	Zrelost
Kaj meri	Kaj SOC lahko naredi	Kako dobro to SOC izvaja
Fokus	Tehnologije, storitve, kadri, procesi?	Ponovljivost, dokumentiranost, merljivost, optimizacija
Vprašanje	Ali SOC imamo to sposobnost?	Kako dobro to izvajamo?
Primer	SOC ima SIEM, izvaja IR, uporablja CTI	SOC ima definirane playbooke, meri KPIje, optimizira procese

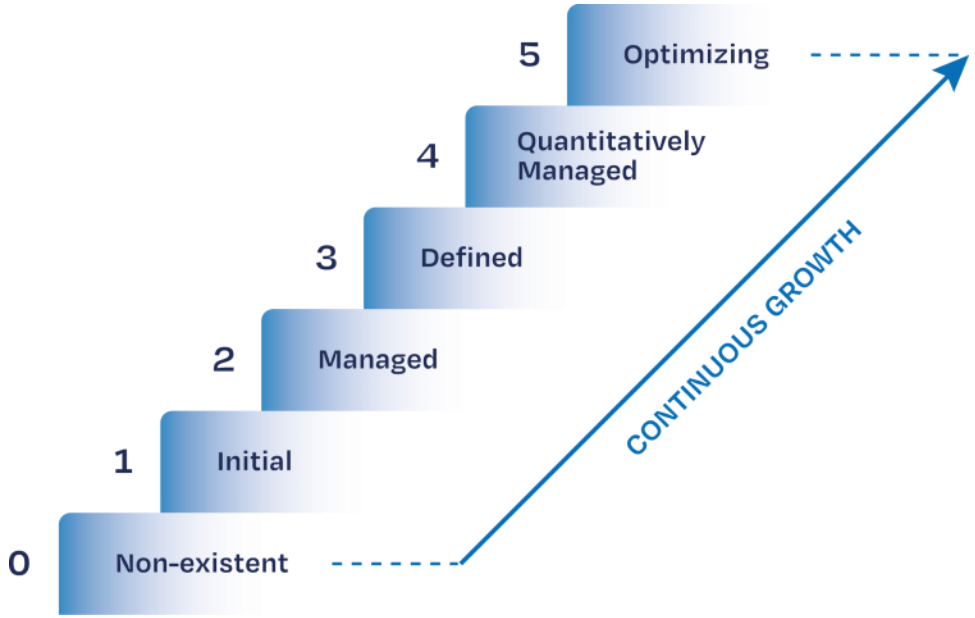
SOC-CMM MODEL ZRELOSTI IN ZMOGLJIVOSTI

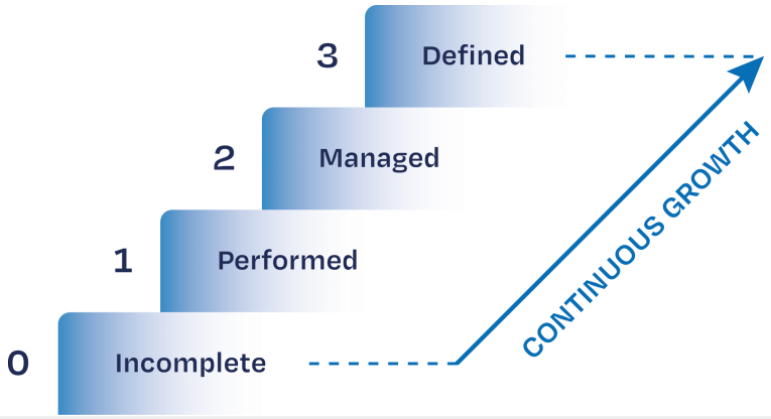
SOC-CMM (Security Operations Center – Capability Maturity Model)

Ta model je na voljo na https://www.soc-cmm.com/ in je zelo primeren za opis in oceno vseh funkcij SOC.

Odprtokodni model in excell orodje organizacijam omogoča oceno in izboljšanje zrelosti in zmogljivosti njihovega SOC.

Temelji na **šestih ravneh zrelosti** in **štirih ravneh zmogljivosti** ter pokriva vse dimenzije delovanja.





SOC-CMM KRITERIJI OCENJEVANJA

SOC-CMM kriteriji ocenjevanja zrelosti in zmogljivosti

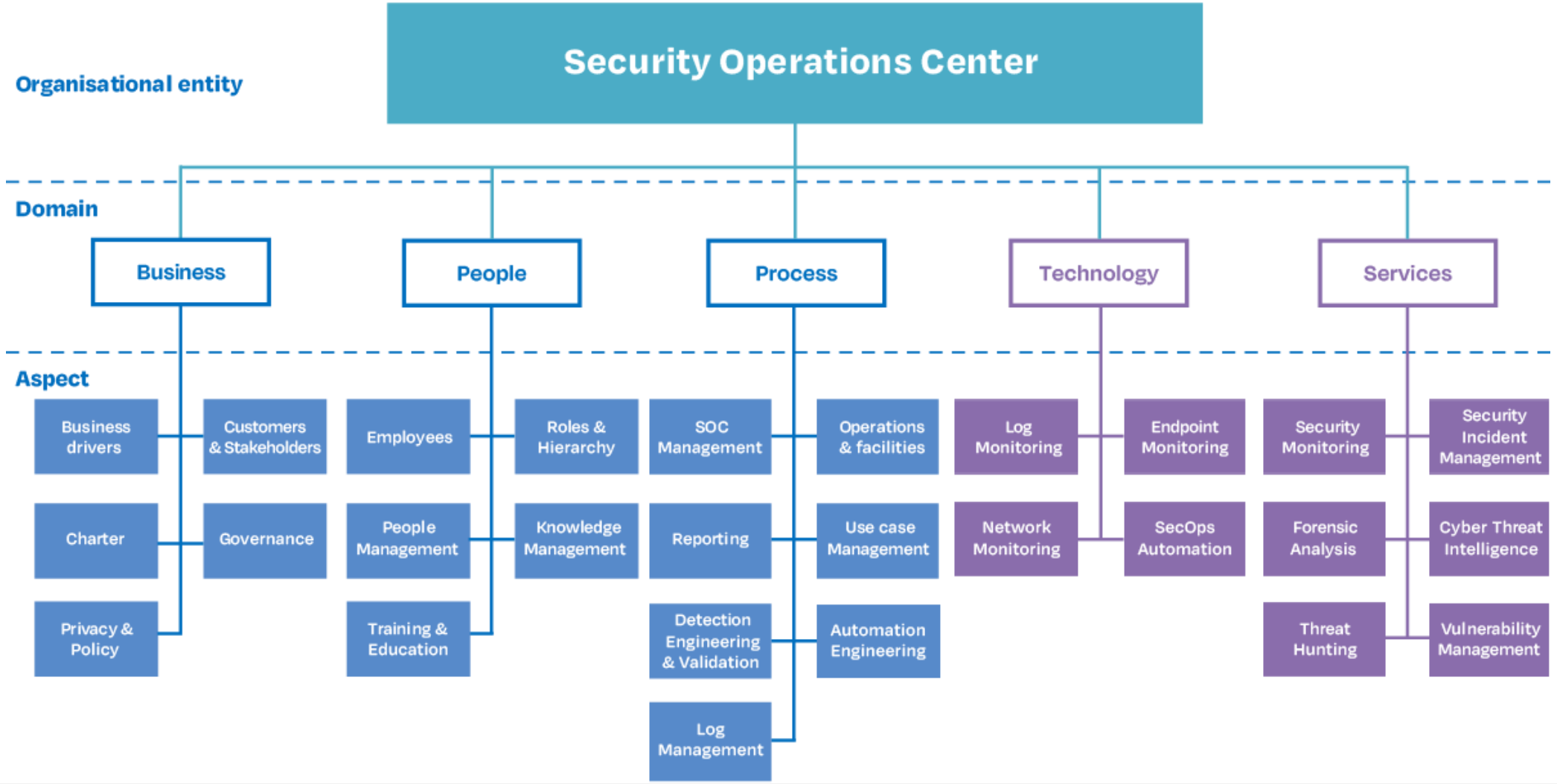
Pri zrelosti se ocenjuje vseh 27 aspektov. Uporablja se 6 ocen od 0 do 5.

Nivo zrelosti	Naziv	Opis
0	Non-existent	This element is not in place .
1	Initial	The element is performed in an ad-hoc fashion .
2	Managed	This element is somewhat structured, but not consitently
3	Defined	This element is structured and consistently performd
4	Quantitatively managed	This element is measured for effectiveness and efficiency
5	Optimizing	This element is continuously improved and optimized

Pri zmogljivosti se ocenjuje 10 aspektov v kategorijah Technology in Services. Uporablja se 4 ocene od 0 do 3.

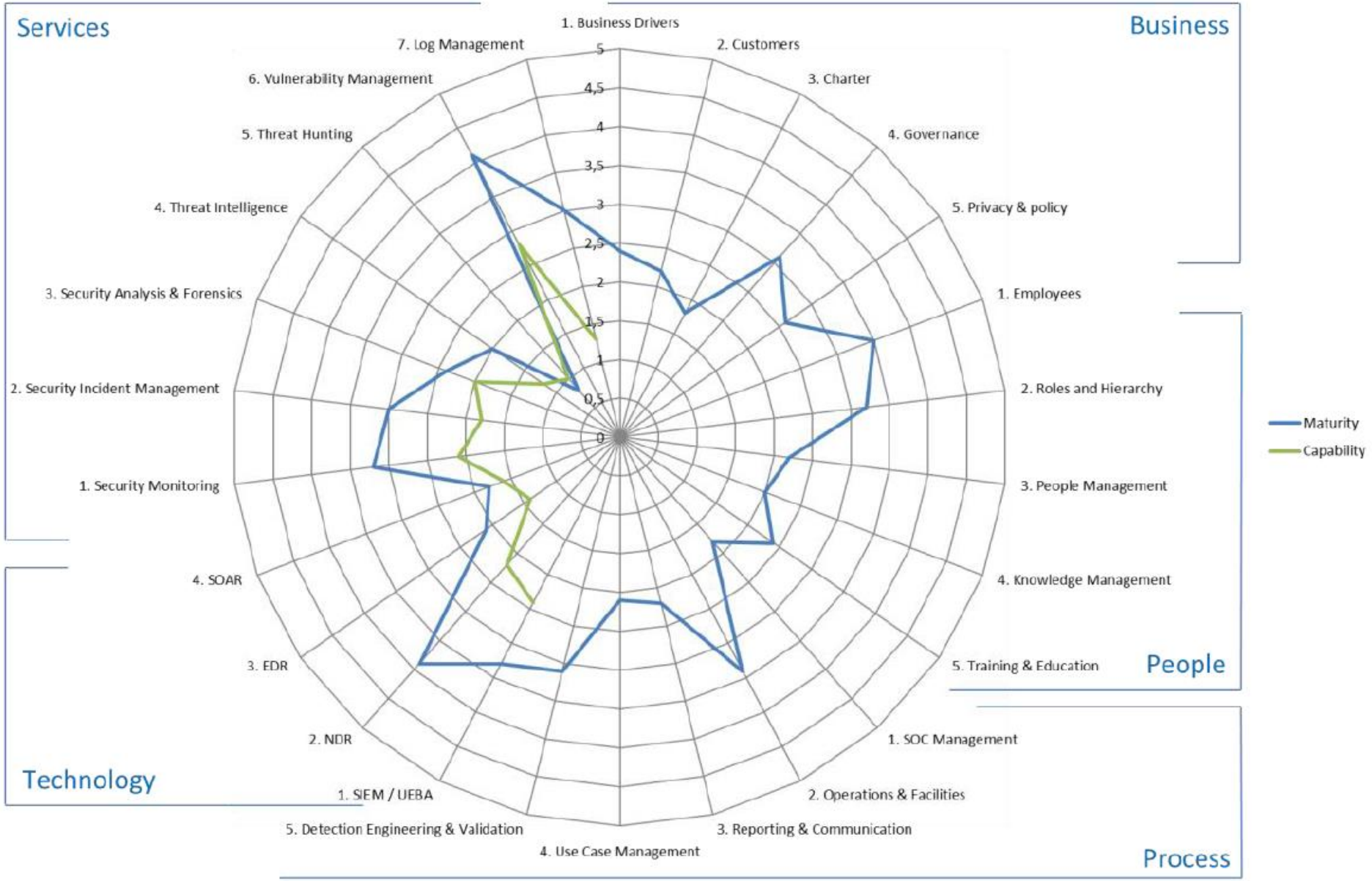
Nivo zmogljivosti	Naziv	Opis
0	Incomplete	This element is not in place .
1	Performed	The element is performed in an ad-hoc fashion
2	Managed	This element is somewhat structured, but not consitently
3	Defined	This element is structured and consistently performd

SOC-CMM DOMENE IN VIDIKI



SOC-CMM

Grafična predstavitev ocene zrelosti in zmogljivosti.



SKLADNOST IN SOC

- Kibernetska varnostna tveganja so s širitvijo digitalizacije, z vse večjo odvisnostjo družbe od digitalnih tehnologij in storitev ter z naraščajočimi kibernetskimi grožnjami vse večja.
- Zato je področje kibernetske varnosti in odpornosti vse bolj zastopano v regulativah, ZinfV-1, ZVOP-2, ZKI DORA, PSD2, eIDAS, CRA, Data Act,… V nadaljnji obravnavi se omejimo na ZinfV-1.
- SOC ni reguliran, ne govorimo o skladnosti SOC, temveč je SOC ukrep, ki prispeva k skladnosti organizacije z ZinfV-1.
- ZInfV-1 je slovenski zakon, sprejet maja 2025, ki v nacionalno zakonodajo prenaša zahteve evropske direktive NIS2 in uvaja strožje obveznosti na področju kibernetske varnosti. Zajema bistvene in pomembne subjekte v kritični infrastrukturi in digitalnih storitvah.
- ZInfV-1 organizacijam nalaga minimalne standarde informacijske varnosti in zahteva doseganje določenih rezultatov. Organizacije imajo svobodo pri izbiri rešitev, a morajo izkazati, da izpolnjujejo predpisane obveznosti.
- V praksi se izkazuje, da vzpostavitev SOC zelo olajša izpolnjevanje velikega dela teh obveznosti.

ZAHTEVE ZINFV-1 IN SOC

SOC omogoča izpolnjevanje posameznih zahtev ZInfV-1 na področjih:

- upravljanja tveganj,
- zaznavanja in odzivanja na incidente,
- beleženja in hrambe dnevnikov,
- priglašanja incidentov,
- usposabljanja zaposlenih,
- nadzora dostopov,
- varnosti dobavne verige.

ZAHTEVE ZINFV-1 IN SOC (1)

Obvladovanje tveganj

ZInfV-1 zahteva upravljanje informacijske varnosti in neprekinjenega poslovanja ter dokumentirano upravljanje tveganj. Zahtevan je načrt varnostnih ukrepov za obvladovanje tveganj ter presoja njihove učinkovitosti in izvajanje izboljšav.

SOC k temu prispeva:

- Pomembne vhodne podatke za analizo tveganj: grožnje, incidente in ranljivosti.
- Z rednim upravljanjem ranljivosti neposredno izpolnjuje zahteve zakona (22. člen).
- Preko testov in vaj preverja učinkovitost varnostnih ukrepov in daje priporočila.
- Vodi operativne varnostne metrike (incidenti, MTTR, odprava ranljivosti), ki podpirajo vodstvene odločitve in skladnost.
- Stalno povratno zanko izboljšav: zaznave → analiza tveganj → ukrepi → preverjanje → optimizacija.

ZAHTEVE ZINFV-1 IN SOC (2)

Neprekinjeno spremljanje in zaznavanje varnostnih incidentov

ZInfV-1 zahteva stalno, zanesljivo in pravočasno zaznavanje incidentov, vključno z obveznim 24/7 poročanjem pomembnih dogodkov.

SOC k temu prispeva:

- Omogoča centraliziran nadzor nad varnostnimi dogodki prek SIEM, EDR, NDR in drugih detekcijskih tehnologij.
- Izjemno skrajšan čas zaznave incidenta (minute/ure namesto dni), kar je ključno za omejitev škode.
- Izvaja proaktivno raziskovanje in zaznavo groženj (threat hunting), zaznava napade, ki se izognejo avtomatskim zaznavam.
- Ob povišani ogroženosti na nacionalnem nivoju lahko SOC takoj preide v okrepljen režim nadzora.
- Brez SOC organizacija težko izpolnjuje zakonske obveznosti glede zaznavanja, dokazljivosti in hitrega poročanja kibernetskih incidentov.

ZAHTEVE ZINFV-1 IN SOC (3)

Odzivanje na incidente in omejevanje škode

ZInfV-1 zahteva jasno definirane postopke in odgovornosti za odzivanje na incidente ter takojšnje ukrepanje za zmanjšanje vpliva napadov.

SOC k temu prispeva:

- Ob potrditvi incidenta takoj aktivira odzivno ekipo, izolira prizadete sisteme in izvede nujne tehnične ukrepe za zajezitev škode.
- Izvaja forenzično analizo incidenta (vzrok, obseg, vstopna točka) ter pripravlja priporočila za izboljšave in odpravo ranljivosti.
- Omogoča organizaciji izpolnjevanje zakonskih obveznosti za 24h/72h poročanje CSIRT, saj zagotavlja vse ključne tehnične podatke za prijavo.
- Ob nastalih incidentih, hitro delovanje SOC močno zmanjša škodo na vseh področjih (poslovna, pravna, ugled) ter omogoča učinkovito obvladovanje kriznih situacij.

ZAHTEVE ZINFV-1 IN SOC (4)

Poročanje (priglasitev) varnostnih incidentov

ZInfV-1 zahteva fazno poročanje pomembnih incidentov na SI-CERT in SIGOV-CERT: 24 h – zgodnje obvestilo, 72 h – podrobna priglasitev, 1 mesec – končno poročilo, če traja dlje, obdobno in končno poročilo.

SOC k temu prispeva:

- Zagotavlja vse ključne tehnične informacije za prijavo: opis incidenta, obseg, prizadete sisteme, vzroke, indikatorje kompromitacije ter izvedene ukrepe.
- Ob zaznavi incidenta oceni resnost in sproži eskalacijo, skrbi da organizacija ne zamudi zakonskih rokov za prijavo.
- Podpira pravno skladnost zagotavljanja revizijskih sledi, forenzičnih podatkov
- Omogoča pripravo obvestil uporabnikom storitev, kadar incident vpliva na njih ali zahteva preventivne ukrepe.
- Centralizirano dokumentiranje incidentov v močno olajša inšpekcijske preglede, notranje revizije in dokazovanje skladnosti.

ZAHTEVE ZINFV-1 IN SOC (5)

Beleženje varnostnih dogodkov in hramba dnevniških zapisov

ZInfV-1 zahteva centralizirano beleženje vseh varnostno pomembnih dogodkov ter hrambo dnevniških zapisov min. 6 mesecev na način, ki zagotavlja avtentičnost, celovitost in zaupnost.

SOC k temu prispeva:

- Vzpostavi in upravljanje SIEM kot centralno shrambo dnevniških zapisov in revizijskih sledi, zbira zapise o prijavah in dostopih, spremembe konfiguracij, omrežne dogodke in druge ključne podatke. Zagotavlja da so logi so zaščiteni pred brisanjem ali spreminjanjem, kar omogoča zanesljivo forenziko in dokazovanj.
- SIEM izvaja korelacijo log zapisov, preverja indikatorje kompromitacij (IoC), generira varnostne dogodke in alarme.
- Centralizirani logi omogočajo učinkovito iskanje po vseh virih dnevniških zapisov in analizo incidentov za nazaj.

ZAHTEVE ZINFV-1 IN SOC (6)

Ozaveščanje in usposabljanje (kibernetska higiena)

ZInfV-1 zahteva redno usposabljanje zaposlenih in skrbnikov IKT ter krepitev kibernetske higiene.

SOC k temu prispeva:

- Realne primere napadov (phishing, vdori, incidenti) za sprotno ozaveščanje in ciljno učenje uporabnikov in skrbnikov IT sistemov.
- Poročila SOC in ugotovitve iz dejanskih dogodkov služijo kot gradivo za usposabljanje.
- Sodeluje kot vsebinski ekspert pri izobraževanjih, izvaja simulacije napadov in phishing teste, dviguje varnostno kulturo.
- Podpira usposabljanje vodstva (table-top vaje) in zboljšuje pripravljenost na krizne situacije.

ZAHTEVE ZINFV-1 IN SOC (7)

Nadzor dostopov in identitet (MFA, pravice dostopa)

ZInfV-1 zahteva zanesljivo preverjanje identitete, upravljanje pooblastil ter uporabo MFA na kritičnih točkah dostopa.

SOC k temu prispeva:

- Preko SIEM-a stalno nadzira prijave in dostope, odkriva nepravilnosti (nenavadni časi, lokacije, brute-force vzorci) in identificira poskuse zlorabe.
- Preverja učinkovitost MFA ter zaznava poskuse njegovega obvoda ali registracije nepooblaščenih naprav.
- Opozarja na nepravilnosti v pravicah (npr. prekomerne privilegije, nenadne eskalacije pravic, zlorabe računov).
- Deluje kot varnostna kontrola nad procesom upravljanja identitet in dostopov (IAM) in omogoča organizaciji dokazljivo skladnost z zahtevami glede dostopov.

ZAHTEVE ZINFV-1 IN SOC (8)

Varnost dobavne verige

ZInfV-1 zahteva, da organizacije za ključne dobavitelje določijo minimalne varnostne zahteve, ocenijo njihove ranljivosti in spremljajo njihovo varnostno prakso.

SOC k temu prispeva:

- Z uporabo CTI virov spremlja, ali so dobavitelji udeleženi v incidentih, imajo ranljivosti ali predstavljajo povečano tveganje za organizacijo.
- Lahko izvaja ali podpira varnostno ocenjevanje dobaviteljev (npr. scorecard, tehnične presoje), ter sproži ukrepe, ko varnostna drža posameznega dobavitelja pade.
- Sodelovanje in izmenjava informacij z drugimi SOC/CERT ekipami pomaga pri zgodnjem odkrivanju groženj, ki se prenašajo prek dobavne verige.
- Zagotavlja tehnična dokazila in poročila, ki organizaciji omogočajo dokazovanje skladnosti pri upravljanju dobaviteljev.

PRAKTIČNE SMERNICE (1)

Zahteva ZInfV-1 (člen)	SOC funkcionalnost za izpolnitev
Upravljanje tveganj (21. člen, 22. člen t.13) – Analiza tveganj, ocena vplivov, upravljanje ranljivosti. Preverjanje ukrepov 1× letno (21(5) člen).	SOC priskrbi vhodne podatke za oceno tveganj , poročila o grožnjah, incidentih. Izvaja skeniranje ranljivosti in spremlja njihovo odpravo. Organizira redne varnostne teste (pentesti, vaje) in predlaga izboljšave ukrepov. S tem dokazuje učinkovitost varnostnega programa.
Varnostna dokumentacija (21. člen) Sistem upravljanja varnosti z načrti: Načrt neprekinjenega poslovanja in obnovitve (točki 4,5). Načrt odzivanja na incidente (točka 6). Načrt varnostnih ukrepov (točka 7).	SOC sodeluje pri izdelavi načrtov, poda tehnične scenarije za načrt BCP/DR (kaj če te in te sisteme napade). Ima izdelane playbooke odziva na incidente (vloge, koraki), ki se vključijo v dokumentacijo. Definira tehnične varnostne ukrepe (npr. uporaba IDS, SIEM) za vse zaznane grožnje, ti postanejo del načrta ukrepov. SOC zagotavlja, da dokumentacija ni teoretična, ampak temelji na realnih zmogljivostih.
Neprekinjeno spremljanje in zaznavanje (22. člen t.14) Uvedba sredstev za zaznavanje malware, vdorov in preprečevanje incidentov. Ob visoki ogroženosti: spremljanje celotnega omrežja.	SOC vzpostavi 24/7 monitoring: SIEM, IDS/IPS, EDR, NDR ki zaznavajo napade v realnem času. Analitiki dežurajo in preverjajo alarme. Pri povišani ogroženosti SOC preide v okrepljen režim, še bolj podrobno spremlja promet, pogostejša poročila. S tem je zagotovljeno stalno opazovanje, kot ga zahteva zakon.
Odziv na incidente (21.6 člen, 22. člen t.14) Imeti definirane postopke in odgovornosti za odzivanje. Ukrepati za omejitev vpliva incidentov.	SOC ekipa ima za odziv na incidente postopkovnik , kdo kaj stori ob incidentu, kar izpolnjuje dokumentacijski vidik. Ob incidentu SOC izolira sisteme, zatre napad, povrne iz varnostnih kopij, s čimer neposredno izvede zakonsko zahtevan ukrep omejevanja škode. SOC vodi forenziko in poda ugotovitve za odpravo vzroka, kar se vključi v izboljšave.

PRAKTIČNE SMERNICE (2)

Zahteva ZInfV-1 (člen)	SOC funkcionalnost za izpolnitev
Priglasitev, poročanje incidentov (29. člen, 30. člen) Prijava pomembnih incidentov CSIRT v 24h (delne info) in 72h (prva ocena); mesečno končno poročilo. Obveščanje prizadetih uporabnikov.	SOC identificira incidente, ki sodijo v “pomembne” (glede na vpliv) in takoj sproži prijavo. Pripravi vsebino poročil, tehnični opis, vzrok, ukrepi in jih pravočasno posreduje oddelku skladnosti za oddajo URSIV/SI-CERT. SOC sodeluje z CSIRT. Pripravi podatke za obveščanje uporabnikov, npr. kaj naj storijo za zaščito. Vodi evidenco vseh priglašenih incidentov.
Beleženje dogodkov in hramba logov (22.6, 24. člen) Beležiti aktivnosti (prijave, dostopi, spremembe…); hraniti loge vsaj 6 mesecev, zaščititi njihovo celovitost. Sinhronizacija časov.	SOC upravlja centralni sistem za dnevnike SIEM, ki avtomatsko zbira vse relevantne dogodke. Nastavljena je hramba >= 6 mesecev (npr. 1 leto). Log strežnik ima nadzor integritete, ni možnih nepooblaščenih posegov. SOC poskrbi, da so vsi strežniki in naprave sinhronizirani s časom (NTP). SOC analitiki lahko na zahtevo najdejo in izvozijo poljubne zapise, s čimer organom dokažejo revizijsko sled).
Osnovna kibernetska higiena in usposabljanje (20. člen, 22.3) Redno usposabljanje zaposlenih in skrbnikov, izvajanje osnovnih varnostnih praks , ozaveščanje o phishingu, geslih itd.	SOC prispeva vsebino in izvedbo, posreduje primere napadov in statistike v izobraževanja, npr. “lessons learned” iz incidentov. Izvaja simulacije napadov, npr. phishing test in rezultate uporabi za ciljno ozaveščanje. SOC strokovnjaki sodelujejo kot predavatelji na treningih za zaposlene in vodstvo, npr. razložijo nove grožnje. S tem dviguje varnostno kulturo, kar izpolnjuje zahteve po rednem usposabljanju in dobrih praksah. Vodi evidenco uspešnosti npr. manj klikov na phishing.

PRAKTIČNE SMERNICE (3)

Zahteva ZInfV-1 (člen)	SOC funkcionalnost za izpolnitev
Preverjanje identitete in nadzor dostopov (22.4, 22.15) Uvesti upravljanje identitet in avtentikacije, MFA kjer je smiselno glede na tveganja. Zagotavljati, da dostopajo le pooblaščeni.	SOC nadzira vse prijave in dostope preko SIEM. Zazna neuspešne prijave v velikem številu, možni napadi ugibanja gesel, ali prijave ob neobičajnem času. Spremlja uspešne prijave skrbnikov in dostop do občutljivih podatkov. Preverja delovanje MFA, opozori, če kje ni vklopljen ali če prihaja do mnogih neuspešnih MFA, možni poskusi vdorov). Ugotavlja nepravilnosti v pravicah, npr. uporabnik z nizko vlogo izvaja admin aktivnosti kar je možna zloraba .S tem SOC hitro zazna in ustavi nepooblaščen dostop, dopolnjuje sistem IAM in zagotavlja, da zahtevani mehanizmi, MFA in upravljanje pravic dejansko funkcionirajo.
Varnost dobaviteljev, dobavna veriga (22.10, 22(4)) Varnostne zahteve za ključne dobavitelje, upoštevati specifične ranljivosti vsakega dobavitelja in spremljati njihovo varnostno prakso.	SOC spremlja varnostno stanje dobaviteljev. Uporablja obveščevalne CTI vire in orodja, npr. varnostne ocene, za spremljanje ali je kak dobavitelj kompromitiran ali ima šibke točke. Obvesti odgovorne, če se pojavi incident povezan z dobaviteljem, in svetuje ukrepe, npr. začasna blokada povezav. Pregleduje promet med organizacijam in dobavitelji (VPN, API) odkriva sumljive aktivnosti s strani dobavitelja. Sodeluje pri presoji tveganj dobaviteljev, tehnično oceni njihove varnostne certifikate, poročila, teste, npr. pregled rezultatov pentesta njihove rešitve. Če dobavitelj ne izpolnjuje dogovorjenih varnostnih zahtev, SOC to opazi in eskalira, da se ukrepa pogodbeno. Tako je zagotovljeno aktivno upravljanje varnosti v odnosu z dobavitelji, kot zakon narekuje.

STROŠKOVNI MODELI SOC

STROŠKI SOC -DEJAVNIKI

Dejavniki ki vplivajo na stroške

SOC predstavlja novo organizacijsko entiteto ali novo zunanjo storitev, ki za svoje delo potrebuje kadre, prostore, nova tehnološka orodja kar je lahko za organizacijo velik finančni zalogaj.

Dejavniki ki najbolj vplivajo na stroške:

- **Velikost organizacije in kompleksnost IT okolja**, število uporabnikov, lokacij, IT sistemov, pomeni več dogodkov, višja kompleksnost, več orodij, več analitikov
- **Panoga, pomembnost subjekta po ZinfV-1** (bistveni, pomembni),
- **Režim delovanja SOC**, polni 24/7 režim zahteva več izmen, več kadrov in stalno pripravljenost, največji strošek
- **Uporaba tehnologij** in licenčni modeli SIEM, EDR/XDR, NDR, SOAR, CTI, VM ipd., licence po GB/dan, številu dogodkov, številu naprav ali IP-jev itd.
- **Model vzpostavitve SOC**: interni, zunanji, hibridni, panožni, centraliziran

RAZRED SUBJEKTOV

Razlika med bistvenimi in pomembnimi subjekti

ZInfV-1 oba razreda (bistveni/pomembni) obravnava kot zavezance, vendar z različnimi stopnjami nadzora, zahtevnosti ukrepov in regulatornih obveznosti.Dejavniki.

- Oba razreda morata izvajati vse temeljne ukrepe ZInfV-1, npr.:
  - upravljanje tveganj, varnostna dokumentacija, tehnični in organizacijski ukrepi (22. člen), nadzor dobavne verige, beleženje logov, incident management, priglasitev pomembnih incidentov (24h / 72h / končno poročilo)

Razlike v zahtevah ZinfV-1 med bistvenimi in pomembnimi subjekti

	Bistveni subjekti	Pomembni subjekti
Nadzor	So pod strožjim, proaktivnim nadzorom.	So pod reaktivnim nadzorom, preverjanje se aktivira ob incidentih, sumih neskladnosti ali na zahtevo.
Revizije skladnosti	Obvezne redne ocene skladnosti, ,npr. intervalno preverjanje, običajno na 2 leti.	Oceno skladnosti morajo izvesti samo na zahtevo inšpektorja ali po pomembnem incidentu.
Intenzivnost ukrepov	Izvajanje ukrepov v večji globini, z višjo stopnjo formalizacije, testiranja in dokumentiranja.	Uporabi se bolj sorazmeren pristop glede na tveganja, čeprav morajo še vedno izpolniti vse zahteve 21.–25. člena.
Varnostne zahteve v praksi	Pričakovana višja stopnja operativne pripravljenosti, npr. 24/7 nadzor, hitrejša odzivnost, naprednejše rešitve.	Mogoč je manj zahteven nivo SOC/monitoringa, dokler izpolnjuje zakonske zahteve.

STRUKTURA STROŠKOV SOC

Glavne stroškovne postavke SOC

Strošek	Opis	Delež stroška
Človeški viri	SOC analitik L1: spremljanje alarmov, eskalacija SOC analitik L2: forenzika, incident response SOC inženir: integracije, tuning XDR/BDR/SIEM/SOAR SOC vodja / CISO povezava: vodenje, poročanje Tipično: 6–8 FTE za 24/7 SOC (če je interni), oz. manj pri hibridnem/zunanjem modelu.	Neposredni strošek kadrov 40-50% Posredni strošek kadrov (izobraževanja, certifikacije) 10%, OPEX
Tehnologija	SIEM licenca, obračun po EPS/GB logov na dan XDR licence, obračun po številu naprav NDR licence, obračun po številu IP SOAR (automation), EDR/XDR agenti, Strojna oprema: strežniki, storage, backup	20-30% , večinoma OPEX
Storitve zunanjih izvajalcev	Podpora, svetovanje, izvajanje MSSP/MDR CTI (Cyber Thtreat Intelligence) informacijski viri in preiskovanje Varnostni pregledi, phishing testi, penetration testi, red team vaje	10-20% , zelo odvisno, OPEX
Prostori, organizacija in procesi	Prostori Upravljanje procesov, dokumentacije Presoje skladnosti, notranje in zunanje revizije	10%, OPEX

STROŠKI SOC GLEDE NA MODEL UVEDBE

Strošek SOC pri treh glavnih modelih.

Strošek	Prednosti	Pomanjkljivosti
Interni SOC	Vse investicije gredo v lastne zmogljivosti, ni stroška zunanjega izvajanja. Pri zelo velikem obsegu npr. več tisoč naprav je lahko na enoto cenovno učinkovito, cena na dogodek ali napravo je nižja ker se fiksni stroški razporedijo na velik obseg (ekonomija obsega)	Zelo visoki začetni in tekoči stroški (ljudje, 24/7 izmene, infrastruktura, tehnologija). Zahtevno zagotavljanje kadrov in kompetenc. Slab izkoristek pri organizacijah z manjšim številom incidentov.
Zunanji SOC / MSSP	Najnižji vstopni strošek, hitra vzpostavitev. Variabilni stroški po obsegu ali napravah. Dostop do vrhunskih strokovnjakov in 24/7 pokritosti. Ekonomija obsega izvajalca znižuje stroške za naročnika.	Dolgoročno lahko dražje kot interni SOC, kumulativni OPEX. Možni skriti stroški (dodatne ure, napredne storitve). Manjša prilagodljivost organizaciji.
Hibridni SOC	Optimalno razmerje med nadzorom in stroški. Interna ekipa pokriva kritične naloge in lastni kontekst, zunanji partner skrbi za 24/7 in specialiste. Zmanjšana potreba po velikem številu internih kadrov.	Upravljanje zahteva dodatno operativno koordinacijo, potrebna jasna razmejitev odgovornosti (RACI). Če ni pravega sogovornika v organizaciji je lahko učinkovitost nizka. Delno podvojena infrastruktura (ticketing, integracije).

ZAHTEVE ZA PONUDNIKE SOC

ZAHTEVE ZA PONUDNIKE

Organizacija pred izvedbo povpraševanja naredi analizo stroška in koristi (cost-benefit) za posamezne modele uvedbe SOC in se odloči za najprimernejšega. Izvede se lahko informativna povpraševanja oziroma raziskavo trga.

Osnova

- **Namen, cilji:** npr. 24/7 nadzor, odziv na incidente, skladnost z ZInfV-1, poslovni cilji
- **Kaj se ščiti:** opis IT okolja in storitev, kritična sredstva
- **Procesi:** upravljanje dogodkov, upravljanje incidentov, eskalacije, razpoložljivost, komuniciranje, poročanje.

Interni SOC

- **Tehnološka orodja:** nakup ali najem, SIEM , EDR/XDR, NDR/ADS, skeniranje ranljivosti, forenzična orodja,…
- **Storitve:** implementacija, vzdrževanje tehnoloških orodij, svetovanje pri vzpostavitvi procesov, CTI, varnostni pregledi,…

Zunanje SOC izvajanje

- **Tehnološka orodja:** nakup oziroma pogosteje kot del storitev, SIEM , EDR/XDR, NDR/ADS,…
- **Storitve:** vzpostavitev in izvajanje SOC procesov, upravljanje tehnoloških orodij, CTI, skeniranje ranljivosti, varnostni pregledi,…

Hibridno SOC izvajanje

- **Tehnološka orodja:** nakup ali kot del storitev, SIEM , EDR/XDR, NDR/ADS,…
- **Storitve:** vzpostavitev in so-izvajanje SOC procesov, upravljanje tehnoloških orodij, CTI, skeniranje ranljivosti, varnostni pregledi,…

- Zahteve za ponudnike SOC

THANK YOU FOR YOUR ATTENTION

Agamemnonos 14, Chalandri 15231
Attiki, Greece

+111 123 456 789

info@enisa.europa.eu

www.enisa.europa.eu