CENTAR ZA BEZBJEDNOSNE OPERACIJE (SOC)

SAJBER BEZBJEDNOST PRILAGOĐENA VAŠIM JEDINSTVENIM POTREBAMA

ČIKOM | Dalmatinska 78, Podgorica

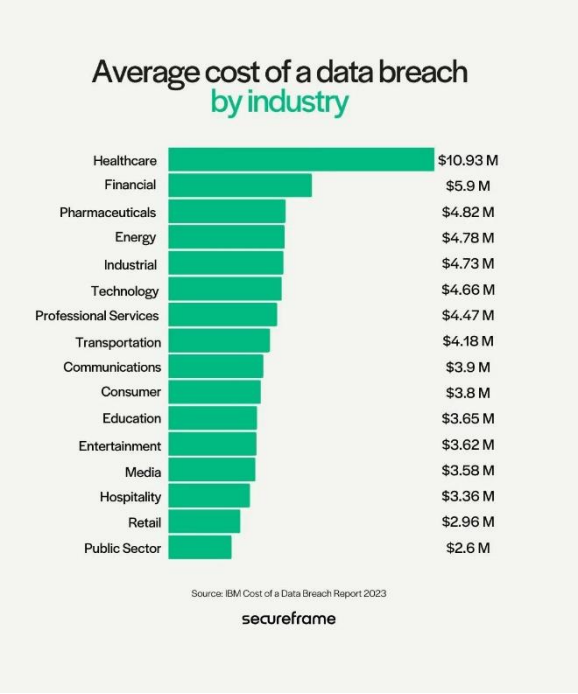
ČIKOM
informatički inženjering

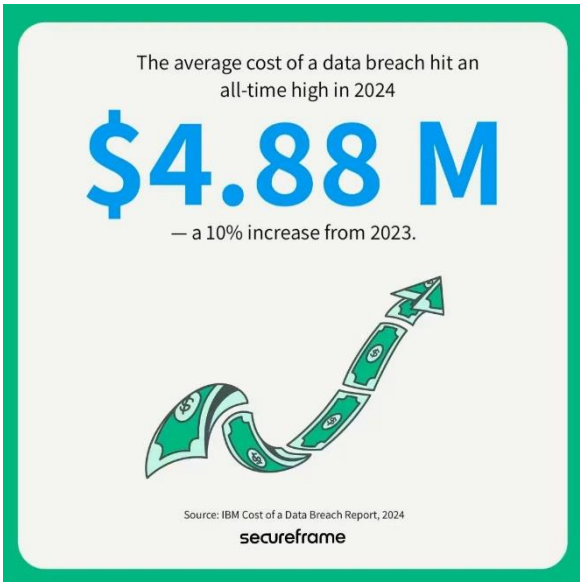
IZAZOV

Učestalost i sofisticiranost sajber napada eskaliraju, a sajber kriminalci koriste napredne tehnike za probijanje sistema zaštite. To uključuje ransomware, phishing i napade putem socijalnog inženjeringa. Gubici podataka postaju sve češći, izlažući osjetljive informacije i uzrokujući značajnu finansijsku i reputacijsku štetu.

Pitanje danas nije da li će moja kompanija biti meta sajber napada, već kada i da li sam spreman za to?

U 2024. godini, prosječno vrijeme za kompanije da identifikuju napad i gubitak podataka bilo je 194 dana[1]. Ovo vrijeme, koje je bilo potrebno da se uoči incident, naglašava stalni izazov sa kojim se organizacije suočavaju u otkrivanju zlonamjernih aktivnosti u realnom vremenu. Smanjenje ovog vremena je od ključnog značaja za minimiziranje uticaja incidenta i zaštitu osjetljivih informacija.





[1] Vrijeme je da se identifikuju i sadrže povrede podataka globalno 2024 | Statista

Zaštita podataka

U vrijeme kada tehnologija neprestano napreduje i mijenja način na koji poslujemo i komuniciramo, zaštita ličnih podataka nikada nije bila važnija nego danas. Podaci podstiču poslovni uspjeh. Ako su podaci sigurni, organizovani i ljudi će imati više povjerenja u vašu organizaciju. Daleko od zaustavljanja načina na koji monetizujete podatke ili gradite digitalne strategije oko njihove vrijednosti, zaštita vaših podataka može vam pomoći da postanete konkurentniji i produktivniji. Efikasna sigurnost podataka zahtijeva od vas da slijedite šire digitalne mogućnosti.

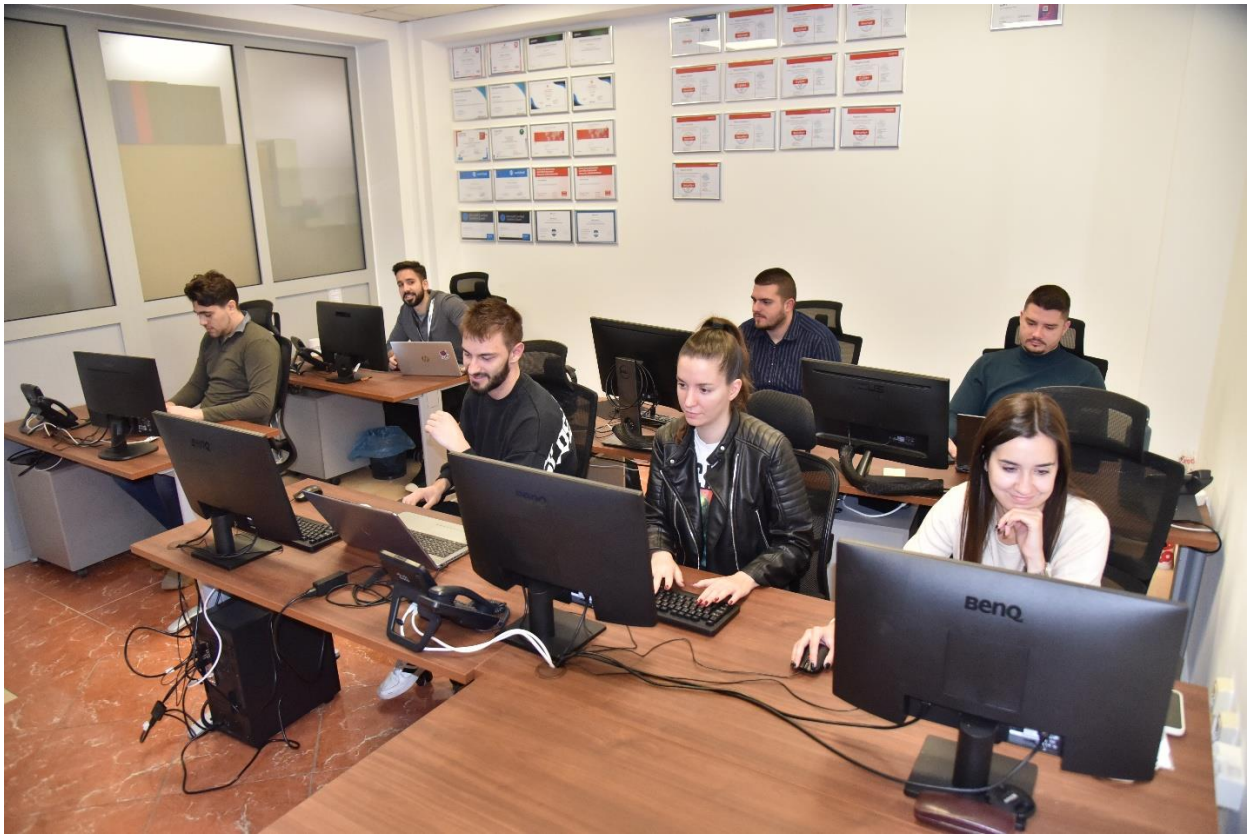
Ponuda i potražnja

Borba za iskusne inžinjere je još jedan kritičan izazov za sajber bezbjednost. Kako rastuća potražnja za stručnošću u oblasti sajber bezbjednosti daleko nadmašuje ponudu, mnogim preduzećima nedostaju interni resursi za usmjeravanje, izvršavanje i usavršavanje strategije sajber bezbjednosti. U različitim istraživačkim projektima, više od polovine (55%) anketiranih kompanija reklo je da se jaz digitalnih eksperata između potražnje i ponude širi, pri čemu su vještine sajber bezbjednosti na prvom mjestu.

SAJBER BEZBJEDNOST PRILAGOĐENA VAŠIM POTREBAMA

Svako preduzeće ima svoje jedinstvene bezbjednosne zahtjeve. Zato je uvijek polazište da pomognemo našim klijentima da razumiju i kvantifikuju svoje profile rizika, identifikuju kritične podatke i procijene njihove trenutne bezbjednosne strategije i nivoe zaštite, **Čikom konsalting**. Ovaj pristup od kraja do kraja usmjeren na kupca, omogućava nam da odredimo prioritete i upravljamo prijetnjama poslovanju. Ovim obezbjeđujemo da rješenja koja gradimo odgovaraju individualnim strateškim prioritetima i bezbjednosnim izazovima svakog klijenta, omogućavajući im da zaštitu stave tamo gde je najpotrebnija.

Lekcija je jasna: sajber bezbjednost preduzeća takođe mora da se razvija. Sa uslugama prilagođenim specifičnom kontekstu i poslovnim ambicijama naših klijenata, ispunjavamo ovu potrebu. To su usluge koje su dovoljno fleksibilne da se prilagode preduzeću, a istovremeno mogu da se razvijaju sa novim prijetnjama, tako da identifikujemo, sprječavamo sofisticirane napade i usklađujemo vaše procedure sa propisima (GRC). Ovaj progresivni spektar end-to-end usluga isporučuje se kroz naš model Centra za bezbjednosne operacije (SOC). Sa našim prilagodljivim SOC servisom pružanje usluga se uskladjuje prema potrebama svakog kupca, kao što je opisano na sledećim stranicama.

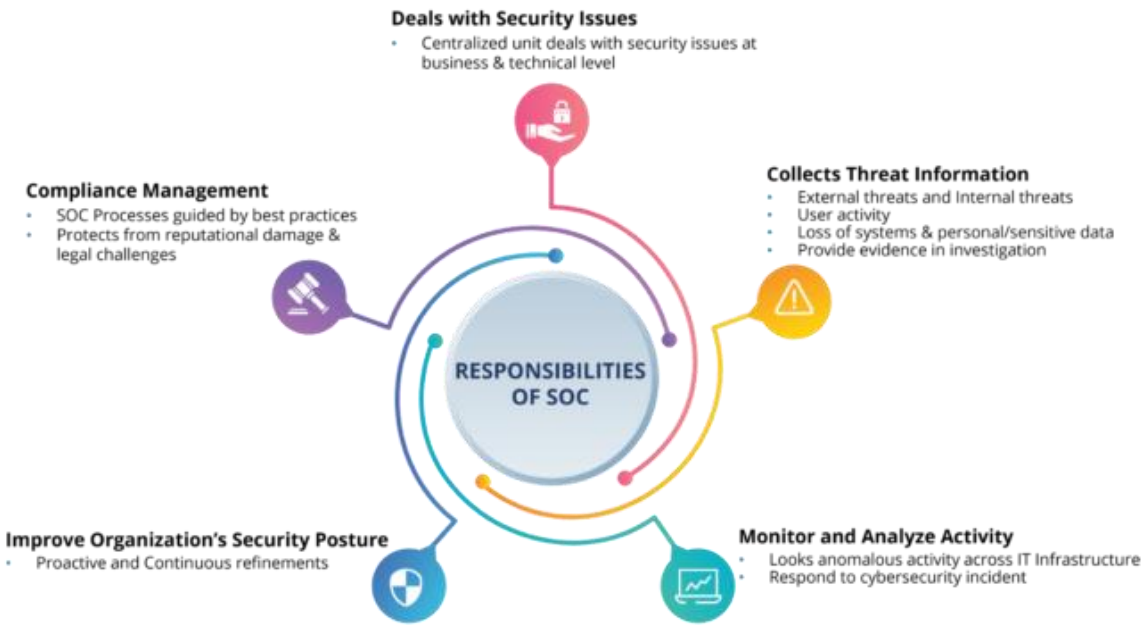


CENTAR ZA BEZBJEDNOSNE OPERACIJE

Čikomov bezbjednosni operativni centar (SOC) orkestrira višestruke uloge, procese i tehnologije potrebne da bi se omogućilo efikasno otkrivanje, analiza i reagovanje na incidente. Sastoji se od skupa procesa, tehnologija i tima pouzdanih i sertifikovanih bezbjednosnih analitičara i stručnjaka za istraživanje i razvoj. SOC pruža potpunu vidljivost IT preduzeća i njegovog sigurnosnog sistema. Obezbijeđen kao upravljana usluga, Čikom SOC će vas opremiti alatima i resursima koji su vam potrebni da: spriječite; Otkrije; i Odgovorite. (Protect-Discover-Respond)

Ključne funkcije SOC-a:

- Praćenje i otkrivanje: Kontinuirano praćenje mrežnog saobraćaja, Sistema protoka informacija. Praćenje bilo kakvih znakova sumnjive aktivnosti ili potencijalnih prijetnji.
- Odgovor na incident: Brza reakcija na bezbjednosne incidente kako bi se ublažila šteta i oporavak od napada.
- Threat Intelligence: Prikupljanje i analiza informacija o novim prijetnjama kako bi bili ispred potencijalnih rizika i proaktivno djelovali.
- Usklađenost: Obezbjeđuje se da organizacija ispunjava regulatorne i industrijske standarde za sajber bezbjednost.
- Izvještavanje: Incident, usklađenost, performanse, ranjivost, executive, ad hoc



Vaša bezbjednost - vaš izbor modela isporuke

Znamo da ne postoji jedinstveni pristup sajber bezbjednosti. Dakle, ponudili smo našu uslugu kroz dva modela isporuke:

- **Hibridni SOC**: Pružamo SOC nakon određivanja najboljeg balansa između vaših resursa i naših. Identifikujemo idealnu kombinaciju resursa i alata kako bismo pružili optimalno rješenje za vaše poslovanje. Omogućava vam da zadržite kontrolu nad određenim aspektima bezbjednosti dok se druge outsource-uju. Koristeći ovaj model, moći ćete da poboljšate svoju produktivnost, predvidljivost i odziv, istovremeno smanjujući troškove, rizike i radno opterećenje za svoje timove, posebno zbog nedostatka stručnjaka za bezbjednost.
- **Managed SOC**: Naš industrijalizovani model pružanja usluga koristi jedinstvene i standardizovane SOC procese koji se mogu brzo primijeniti. Izaberite nivo usluge koji najbolje odgovara vašim poslovnim potrebama, od standardnih usluga, do obogaćenih nivoa usluga koji kombinuju standardne usluge sa Advanced uslugama i Premium paket.

Nivoi usluga za naš 24/7 Managed SOC (SOCaaS):

Standardni

Sveobuhvatno praćenje: Temeljno otkrivanje, prevencija i istraga prijetnji.

Automatizacija: Koristi IT automatizaciju za poboljšanje sposobnosti i efikasnosti tima.

Odgovor na incident: Početni odgovor na bezbjednosne incidente, uključujući konternizaciju i mitigaciju.

Threat Intelligence: Pristup izvorima obavještavanja o prijetnjama kako biste bili u toku sa novim prijetnjama.

Izvještavanje: Redovni bezbjednosni izvještaji i analize.

Advanced

Standardni plus:

Proaktivni threat hunting: Bavi se proaktivnim threat hunting i naprednim tehnikama otkrivanja prijetnji.

Ljudska ekspertiza: Kombinuje automatizovane alate sa direktnim ljudskim učešćem za sofisticirano upravljanje prijetnjama.

Napredna analitika: Koristi naprednu analitiku i mašinsko učenje za otkrivanje prijetnji.

Incident Response and Recovery: Sveobuhvatno reagovanje na incidente, uključujući oporavak i sanaciju.

Premium

Advanced plus:

Prilagodljive Sigurnosne Politike: Kreiranje i implementacija sigurnosnih politika prilagođenih specifičnim potrebama organizacije.

Integracija sa Sigurnosnim Alatima

Forenzika

Upravljanje Usklađenošću

Redovne Sigurnosne Procjene i Auditi: Periodične procjene sigurnosnog stanja i auditi za identifikaciju područja za poboljšanje.

THREAT INTELIGANCE, ANALITIKA I FORENZIKA

Podaci su ključni element naše priče o uspjehu SOC-a. Naše napredne mogućnosti analize podataka objedinjuju SIEM, nadgledanje bezbjednosti mreže, nadgledanje računara, servera, payload analizu i offline big data analitiku po intelligence-driven principu. Takođe poboljšavamo kapacitete za otkrivanje najsofisticiranijih naprednih upornih prijetnji (advanced persistent threats) uz:

- Fokusirana pravila detekcije usklađena sa IT okruženjem klijenta i threat landscape-om.
- Duboko razumijevanje konteksta (obavještenja i informacije o prijetnjama; poznavanje aplikacija unutar perimetra napada).
- Security analitika i forenzika fokusirana na korisnika (ponašanje i spoljni napadi).
- Prediktivna analitika i otkrivanje napada putem IT ranjivosti, vulnerability management, patch preporuke kao i Honey pot mreža.

Čikom GRC

Čikom GRC, uključen u SOC, pomaže klijentima da se pridržavaju regulatornih promjena koje se odnose na bezbjednost, uključujući evropsku NIS2 i DORA direktivu, EU GDPR i ISO27001. Zajedno sa povećanjem učestalosti, obima i sofisticiranosti sajber napada, ovi propisi prisiljavaju preduzeća da prevaziđu svoju konvencionalnu mrežnu zaštitu kako bi se fokusirali na zaštitu podataka, kao i na otkrivanje i predviđanje prijetnji u svojim sistemima. Donosimo duboko razumijevanje ovog regulatornog pejzaža, povezanih poslovnih problema i mogućnosti, kao i relevantnih tehnoloških rješenja i pristupa sajber bezbjednosti.

Čikom je jedna od vodećih informatičkih kompanija u Crnoj Gori koja je od klasičnog isporučioca računarske opreme evoluirala u integratora i implementatora najsloženijih informatičkih rješenja, osposobljena da svojim korisnicima pruži najširi spektar usluga i roba u oblasti informacionih i komunikacionih tehnologija. Čikom je danas prepoznatljiv po sertifikovanom kadru osposobljenom za realizaciju visokosofisticiranih mrežnih i komunikacionih sistema, po pouzdanim i savremenim softverskim rješenjima, po razgranatoj prodajnoj i servisnoj mreži i što je najvažnije po hiljadama zadovoljnih Korisnika.