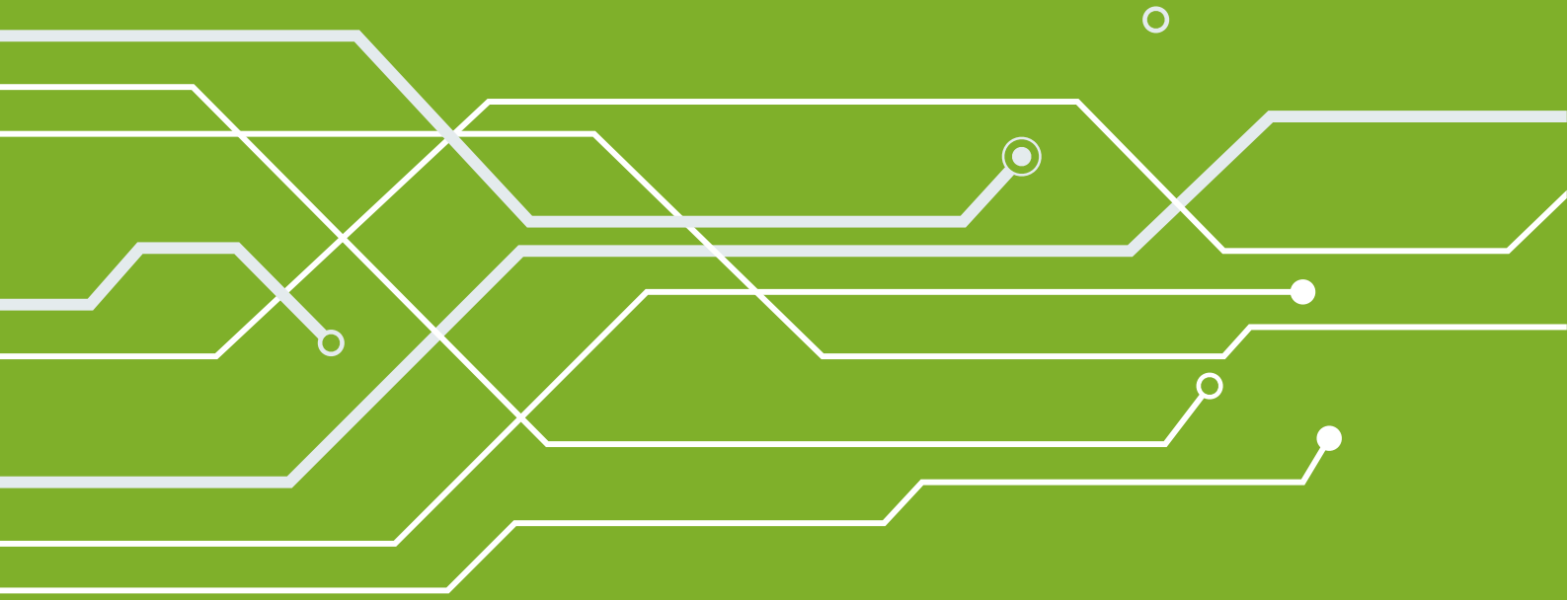
diverto

VAŠI STRUČNJACI ZA
INFORMACIJSKU SIGURNOST



Diverto pruža visoku razinu informacijske sigurnosti tvrtkama, institucijama i drugim organizacijama koje posluju u informacijski orijentiranom svijetu. Klijente štitimo od sigurnosnih prijetnji koje mogu uzrokovati povrede podataka, financijske gubitke i reputacijsku štetu.

Jedni smo od pionira i vodeći u cyber sigurnosti u ovom dijelu svijeta. Osnovani smo 2007. godine i od tada se razvijamo, kako u strateškom, tako u tehnološkom pogledu.

Kontakt: **info@diverto.hr**
Web stranica: **www.diverto.hr**

Informacijska sigurnost u vašoj organizaciji

Ako se pitate je li vašoj organizaciji potrebno ulaganje u informacijsku sigurnost, odgovor je da. Mi smo ovdje kako bismo pronašli sigurnosna rješenja koja čuvaju vaše poslovanje s ciljem unapređenja vaše sigurnosti uz najbolji omjer cijene i kvalitete.

Kako odabrati pravog partnera za informacijsku sigurnost?

Informacijska sigurnost je kontinuirani proces usmjeren na zaštitu i osiguranje vašeg nesmetanog poslovanja. Kako biste bili sigurni da radite u skladu s najboljim praksama, poželjno je osigurati podršku strateškog partnera.

Prepoznajte partnera na čiju se pouzdanost, povjerljivost i stručnost možete osloniti te koji ima široko iskustvo u ovom području rada. Partnera koji prepoznaje stvarne prijetnje vašem poslovanju i koji je posvećen njihovom uklanjanju.
Osim što treba biti iskusan i sposoban, vaš partner u informacijskoj sigurnosti treba kontinuirano pratiti sva dostignuća, trendove i nove prijetnje u području informacijske sigurnosti.

VODITELJ INFORMACIJSKE SIGURNOSTI CISO

Mnoge organizacije funkciju voditelja informacijske sigurnosti (Chief Information Security Officer - CISO) povjeravaju vanjskom suradniku, prvenstveno zbog smanjenja troškova, naprednih tehnologija i vještina koje treća strana može ponuditi, te uvijek dostupne podrške i fleksibilnosti.

Koristimo provjerene mehanizme rada te načine prikupljanja znanja i informacija. Imamo najaktualnije informacije s tržišta te pristup iskustvima iz radne okoline, što je jedan od temelja za uspješno upravljanje sigurnošću. Ta znanja i informacije donosimo kao posebnu vrijednost za vaše poslovanje.

Trebam li informacijskoj sigurnosti pristupiti strateški ili je to operativna uloga IT-a?

Prvi korak do informacijske sigurnosti jest shvaćanje da ona nije tek dodatak vašem poslovanju, već njegova nužnost. S porastom cyber kriminala, ključno je znati kako točno stojite kada je riječ o informacijskoj sigurnosti vaše organizacije. Ako sigurnosti pristupate kao samo jednom od IT operativnih zadataka, nikada nećete postići više od osnovne razine informacijske sigurnosti.

STRATEŠKO PLANIRANJE

Pomoći ćemo vam u razvoju i provedbi strateških i operativnih planova vaše organizacije.
Naš je pristup osmišljen kako bi vam osigurao da na temelju stvarnih rizika odredite prioritetne zadatke te razvijete strategiju za rješavanje prijetnji i napada u području informacijske sigurnosti.

Uz naše dokazano poznavanje industrije informacijske sigurnosti, možemo vam pomoći u usklađivanju strategije informacijske sigurnosti s glavnim pokretačima vašeg poslovanja te definirati prihvatljivu vrijednost ulaganja u aktivnosti koje pripadaju području informacijske sigurnosti.

Našu pomoć baziramo na dobrim praksama i pomažemo vam pri:

- Poravnanju pristupa informacijskoj sigurnosti sa strateškim smjerom organizacije
- Uspostavi sustava upravljanja informacijskom sigurnosti
- Provedbi analize rizika i procjene usklađenost
- Uspostavi poslovnih procesa i standardnih postupaka
- Procjeni trećih strana
- Razvoju i implementaciji tehničkih i operativnih mjera (fizička i okolišna sigurnost, operativna sigurnost, sigurnost komunikacija)
- Uspostavi planova oporavka poslovanja i izgradnji mogućnosti oporavka

45%	59%	73%
rukovoditelja tvrdi da njihova uprava aktivno sudjeluje u određivanju budžeta za sigurnost	zaposlenika otuđuje korporativne podatke kada daju otkaz ili su otpušteni	CISO-a očekuje da će doživjeti veliku povredu sigurnosti u roku od godinu dana

Kako uskladiti informacijsku sigurnost s relevantnim propisima i normama?

Zbog potrebe za pojačanim korištenjem vlastitih resursa i vremena, provođenje sigurnosnih zahtjeva i usklađivanje s novim propisima predstavlja izazov za svaku organizaciju. Isto se odnosi i na područje usklađivanja s različitim normama koje, iako su dobrovoljnog karaktera, predstavljaju skup prepoznatih dobrih praksi koje organizaciji pomažu pri upravljanju, ali i usklađenju s regulativom.

USKLAĐIVANJE

Naši stručnjaci vam mogu pomoći pri odabiru najbolje metodologije i prilagodbi procesa kako biste vašu organizaciju uskladili s propisima i normama koji se odnose na vaše poslovanje ili su relevantni za njega. Da bismo razumjeli kako zakonske i regulatorne obveze utječu na vašu organizaciju te jesu li vaše trenutne sigurnosne kontrole prikladne za postizanje usklađenosti, prvo obavljamo temeljitu procjenu usklađenosti.

Usklađenost se bazira na upravljanju rizicima, stoga primjenjujemo pristup temeljen na procjeni rizika koji rezultira modelom usklađenosti poslovanja i cjelovitim planom za usklađivanje poslovnih funkcija, procesa i kontrola.

Dok radimo na tome, savjetovat ćemo vas kako da poboljšate cjelokupno poslovanje, uštedite vrijeme i novac te učinite vašu tvrtku konkurentnijom.
Ukratko, pomažemo vam razumjeti koji su zahtjevi za usklađenost relevantni za vas, kako se oni odnose na vaše poslovne potrebe i kako ih ispuniti.

Područja usklađivanja s regulativom i propisima:

Kako mogu znati je li moja organizacija sigurna?

Budući da je svaka organizacija jedinstvena, vaš put do informacijske sigurnosti trebao bi početi procjenom sigurnosnog stanja vaše organizacije. Kao treća strana, možemo vam dati neovisnu sliku trenutnog stanja informacijske sigurnosti i sposobnosti u usporedbi s najboljim praksama.

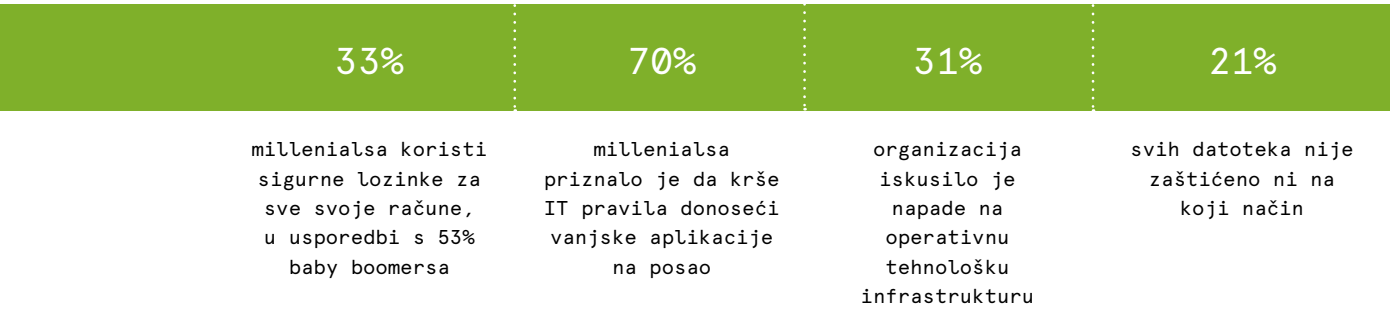
Kao rezultat, imat ćete pregled prepoznatih područja informacijske sigurnosti i preporuke temeljene na najboljim praksama i standardima.

PROCJENE INFORMACIJSKE SIGURNOSTI

Provodimo prilagođene intervjue s ključnim zaposlenicima kako bismo utvrdili zahtjeve zaštite informacija, pregledali trenutne prakse upravljanja rizicima i prikupili druge relevantne podatke uz koje ćemo razumjeti trenutne sigurnosne procese implementirane u vašoj organizaciji. Možete biti sigurni da ćemo biti uz vas tijekom procesa prikupljanja informacija.

Rezultat je detaljno izvješće s prioritetnim preporukama o tome kako poboljšati cjelokupnu informacijsku sigurnost organizacije.

Međutim, ako želite samo procijeniti koliko su određena rješenja, aplikacije ili poslovni modeli u skladu sa sigurnosnim standardima, i tu smo za vas. Naša metodologija temelji se na okvirima koji su općeprihvaćeni u industriji.



Kako mogu odrediti koji je dio našeg poslovanja izložen potencijalnom incidentu?

Sigurnosni incident u vašoj organizaciji može uzrokovati ozbiljne posljedice koje mogu naštetiti njezinom poslovanju.
Gubitak vrijednih informacija ili intelektualnog vlasništva može dovesti do narušavanja reputacije, velikih financijskih gubitaka i novčanih kazni. Kako bi se incident spriječio, važno je temeljito testirati te identificirati ranjive točke u svim dijelovima vašeg poslovanja.

PROCJENA RANJIVOSTI I PENETRACIJSKO TESTIRANJE

Kako bismo shvatili potencijalne slabosti i ranjivosti u vašoj organizaciji, najbolje je provesti testiranje. Većina organizacija je ograničenog pogleda i svoju razinu informacijske sigurnosti procjenjuje samo s obrambenog stajališta. Naš stav je da se takva procjena treba raditi kroz perspektivu napadača koji će iskoristiti slabe točke kojih organizacija nije ni svjesna. Usvajanjem napadačke uloge testiramo i ispitujemo unutarnje i vanjske pristupe sustavima vaše organizacije kako bismo pronašli njezine slabosti.

600%	56%	65%	24.000
više napada na IoT uređaje u prošloj godini	više mobilnih zlonamjernih programa u prošloj godini	stručnjaka identificiralo je phishing i socijalni inženjering kao najveću sigurnosnu prijetnju njihovoj organizaciji	zlonamjernih mobilnih aplikacija blokira se svaki dan

Provodimo ciljane testove kako bismo procijenili razinu vaše informacijske sigurnosti, otkrili ranjivosti tehnologija koje koristite i utvrdili razinu opreza vaših zaposlenika.

Primjeri usluga koje pružamo:

Testovi socijalnog inženjeringa

Unutarnje i vanjsko testiranje ranjivosti

Unutarnje i vanjsko penetracijsko testiranje

Testiranje industrijskih kontrolnih sustava

Penetracijsko testiranje aplikacija

Penetracijsko testiranje proizvoda

Trebam li educirati svoje zaposlenike o važnosti informacijske sigurnosti?

Iskustvo nam govori kako možemo koristiti najpouzdanije uređaje i primijeniti najbolje procese, no ukoliko naši zaposlenici nisu educirani ni svjesni svoje uloge i važnosti informacijske sigurnosti, ostaju najslabija karika. Samo jedan uvjerljiv telefonski poziv pozivnom centru vaše organizacije može dovesti do financijskog gubitka i naštetiti reputaciji vaše organizacije. Budući da su ljudi najosjetljiviji na prijevaru, vaši zaposlenici će lakše prepoznati i izbjeći potencijalne prijetnje ako osvjeste svoju ulogu u sigurnosti vaše organizacije te upoznaju metode napadača.

30%	91%	95%	92%
phishing e-mailova se otvori	cyber napada u 2017. započelo je s phishing porukom	povreda cyber sigurnosti uzrokovano je ljudskom pogreškom	više novih inačica za preuzimanje zlonamjernih programa kreirano je u 2017. godini

TEČAJEVI I RADIONICE

Naši stručnjaci za informacijsku sigurnost tu su da podijele svoje znanje i iskustvo s vama i vašim timom. Nudimo edukacijske tečajeve i radionice — od generalnog osvješćivanja o važnosti sigurnosti prilagođenog pojedinim odjelima i ulogama zaposlenika, do specijaliziranih treninga namijenjenih educiranju onih koji administriraju IT sustave ili razvijaju aplikacije.

Temeljem vašeg područja poslovanja prilagođavamo metodologiju edukacije kako bi se postigla potrebna razina svijesti zaposlenika koji su obuhvaćeni edukacijom. Također, redovno prikupljamo povratne informacije s naših edukacija koje po njima stalno dorađujemo i prilagođavamo vašim potrebama.

Ovo su neki od najtraženijih treninga:

- Osvješćivanje o informacijskoj sigurnosti
- Metode socijalnog inženjeringa
- Sigurnost sustava iz ofenzivne perspektive
- Aplikativna sigurnost
- Sigurnost Linux/Unix sustava za sistem administratore
- Sigurnost sustava za administratore mreže

Što ako se sigurnosni incident već dogodio?

Nažalost, ponekad se treba dogoditi incident kako bi organizacije shvatile da njihovi sustavi nisu u skladu sa standardima i iskustvima iz najbolje prakse u informacijskoj sigurnosti. U tom slučaju je važno odmah potražiti pomoć, jer brza reakcija može spriječiti daljnje gubitke.

UPRAVLJANJE INCIDENTIMA I FORENZIKOM

Naši stručnjaci koordiniraju i obavljaju složene forenzičke usluge, pomažu vam u očuvanju informacija i upravljanju posljedicama sigurnosnih napada.

Izvodimo analize sigurnosnih incidenata u rasponu od kompromitiranih stolnih računala, mobilnih uređaja i IoT uređaja do problema na razini cijelog sustava, kao što su industrijski kontrolni sustavi, te pomažemo u povratku izgubljenih ili kompromitiranih podataka. Naši stručnjaci imaju iskustva u rješavanju posljedica povreda sigurnosti ili napada te će napraviti smjernice za sve — od pripreme dokaza za potencijalne sudske postupke do načina priopćavanja incidenta javnosti.

Pružamo usluge u svakom od šest koraka procesa odgovora na incidente:

Kako se obraniti od hakerskog napada?

Sa stajališta informacijske sigurnosti, cyber napadi dio su alarmantnog trenda.
Njihovi su ciljevi uglavnom ukrasti, razotkriti, izmijeniti ili uništiti informacije te onemogućiti funkcioniranje organizacije – što može dovesti do katastrofalnih gubitaka, pa i prestanka poslovanja. Zato je zaštita vaše organizacije od prijetnji kontinuirani proces koji počinje promjenom stava.

USLUGE OJAČANJA OBRANE

Razmišljati poput napadača često je najbolja obrana, zato vjerujemo u ravnotežu obrambenog i napadačkog pristupa. Identificirajući ciljeve napadača, potencijalne mete i načine na koje mogu izvršiti napad, pomažemo vam u podizanju ljestvice za potencijalne napadače. Nakon što smo identificirali ciljeve i slabe točke u vašoj obrani, pomažemo vam učvrstiti vašu obranu, čineći vašu mrežu otpornijom na napade, a incidente vidljivijima.

39s	43%	48%	€18,642
Svakih 39 sekundi dogodi se hakerski napad	cyber napada targetira manje tvrtke	proboja sigurnosti uzrokovano je malwerom	Prosječan proboj sigurnosti tvrtku košta €18,642 po danu

Kako mogu na vrijeme prepoznati potencijalni incident?

Svaka organizacija ima nešto što treba zaštititi — bilo da je riječ o intelektualnom vlasništvu ili informacijama o zaposlenicima, financijskim ili drugim povjerljivim podacima.
Bez obzira na to treba li vaša organizacija uskladiti poslovanje s određenim zakonima i propisima iz domene informacijske sigurnosti ili želi djelovati proaktivno u svrhu zaštite svog poslovanja, najbolji način vođenja sigurnosnih operacija s maksimalnim učinkom je centraliziranje svih vaših sigurnosnih napora.

Međutim, izgradnja Sigurnosnog operativnog centra (SOC) predstavlja veliki izazov za većinu organizacija, budući da iziskuje značajno vrijeme, stručnost i financijsko ulaganje.
Zato smo razvili naše SOC rješenje, koje je financijski optimalno i prilagodljivo postojećoj infrastrukturi svake organizacije, bez obzira na njezinu veličinu i složenost.

12%	101 dan	100%
vrtki vjeruje da je spremno u slučaju cyber napada	je prosječno vrijeme potrebno za identifikaciju zlonamjernog napada	svih incidenata u 2018. uključivalo je krađu podataka za prijavu

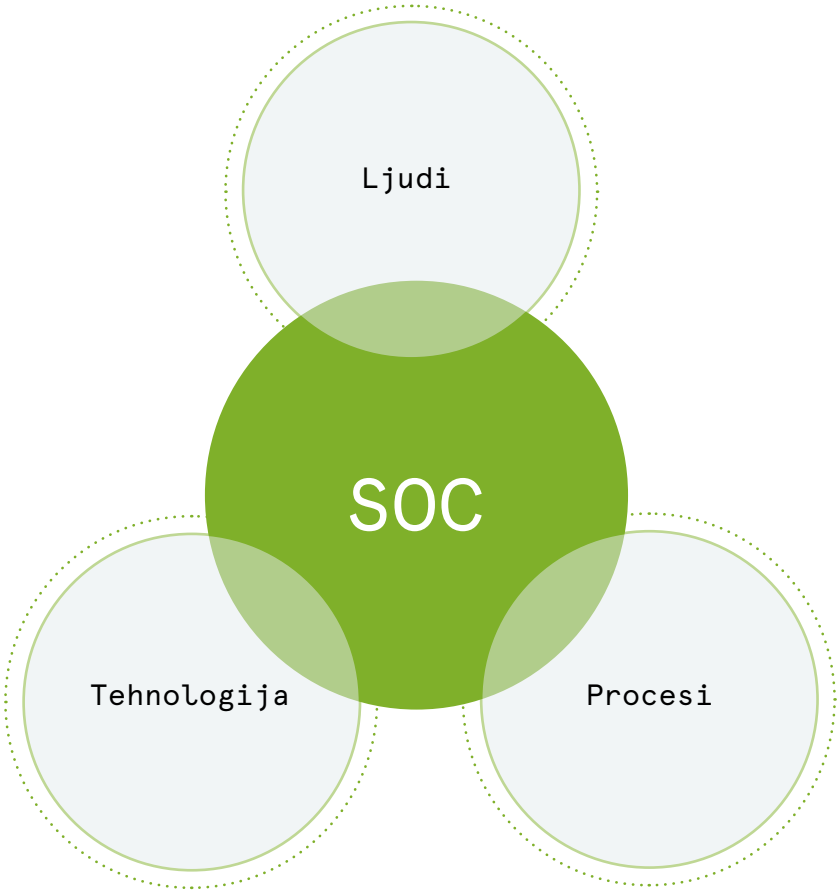
SIGURNOSNI OPERATIVNI CENTAR

SOC je centralizirano rješenje zaduženo za kontinuirano praćenje, procjenjivanje i zaštitu organizacija čuvanjem njihovih informacija, infrastrukture i poslovanja od napada. Uz SOC možete brzo reagirati i uštedjeti dragocjeno vrijeme, novac i ugled.

Naše SOC rješenje nadgleda vašu mrežu u svakom trenutku, 24/7. Pokrivamo sva tri aspekta koja trebate za cjelovitu operativnu informacijsku sigurnost vaše organizacije: implementiramo tehnologiju, razvijamo sigurnosne procese i imamo tim koji nadzire svakodnevne operacije. Time se omogućuje pravodobno otkrivanje vanjskih i unutarnjih prijetnji, poboljšano otkrivanje incidenata i odgovor na incidente, poboljšane mogućnosti forenzičkih istraživanja i cjelokupna prevencija incidenata.

Prednosti Diverto SOC-a

- Prilagodljiv svakoj organizaciji
- Fleksibilni i ekonomični modeli integracije
- Praćenje u stvarnom vremenu i otkrivanje prijetnji utemeljenih na obavještajnim podacima
- Stručnost na svim razinama SOC-a
- Brzo otkrivanje i odgovor na incident
- Proaktivan lov na prijetnje
- Usklađenost s regulatornim zahtjevima
- Napredne mogućnosti izvješćivanja


Ljudi
SOC
Tehnologija
Procesi

info@diverto.hr
www.diverto.hr