

# 30SEC

## Security Operations Center

30SEC je Combisov Security Operations Center (SOC) koji je nastao kao odgovor na povećano izlaganje informacijskih sustava svakodnevnim sofisticiranim prijetnjama i napadima.

Rizik da budete hakirani veći je nego ikad prije. Tko želi na ovaj način uništiti reputaciju tvrtke? Tko želi da njegovi povjerljivi podaci završe na webu i budu dostupni svima pa tako i konkurenciji? Ovdje nastupamo mi - tim stručnjaka koji pokriva široki spektar rješenja iz informacijske i kibernetičke sigurnosti (tzv. vendor independent security). Combis je kao Managed Security Services Provider (MSSP) vaš pouzdan partner koji pruža cjelokupni izbor objedinjenih sigurnosnih usluga koje će zadovoljiti sve vaše potrebe.

### 30SEC Security Operation Center

Posvetite se svome poslovanju - informacijsku sigurnost prepustite **Combisu!**

Combis kao članica HT Grupe na tržištu prosperira gotovo trideset godina. Na raspolaganju imamo potrebno iskustvo, najnovija znanja, certificirane stručnjake i najnaprednije tehnologije što nas čini pouzdanim partnerom koji svojim korisnicima pruža vrhunski izbor objedinjenih sigurnosnih usluga.



## Tko koristi naše usluge?



Tvrtke koje se suočavaju s manjkom internih resursa za određena područja informacijske sigurnosti



Korisnici koji imaju potrebu za kontinuiranim nadzorom



Poslovni subjekti koji ne žele ulagati sredstva uskupi softeri i opremu (rackovi, serveri, vatrozidi, licence...)

## Koje su prednosti 30SEC rješenja?



Korisnik plaća samo uslugu, mi smo zaduženi za opremu.



Uska suradnja s tehničkim timovima proizvođača opreme (IBM, Palo Alto Networks, TrendMicro, Sophos, FireEye, Cisco).



Trošak usluge je fiksni i plaća se na mjesečnoj bazi.



Dijeljenje znanja - u slučaju hakerskih napada u Hrvatskoj i/ili regiji korisnik će biti promptno obaviješten o eventualnim ugrozama.



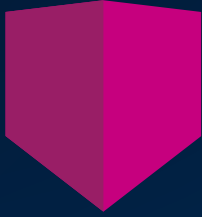
Naši stručnjaci su vam neprestano na raspolaganju.



Uz navedeno, korisnik za čitavo vrijeme trajanja ugovora dobiva i kontinuirano unaprjeđenje informacijske sigurnosti. Naši stručnjaci će s vama podijeliti informacije o aktualnim ugrozama s kojima su se susreli na drugim, sličnim cjelinama.



Modularno rješenje - svaki korisnik bira točno one usluge koje su mu potrebne.



# 30SEC

Security Operations Center



## Security Information and Event Management (SIEM)

- Centralizirani sustav koji u stvarnom vremenu prikuplja i automatski analizira zapise s različitih uređaja s vaše mreže, servera, baza podataka, klijentske opreme... te po potrebi od njih generira upozorenja (alerte) i izvještaje.
- Dobiveni podaci se analiziraju te se iz njih daju savjeti za poboljšanja čitavog sustava informacijske sigurnosti pojedine kompanije.
- Nadzire i provodi korporativne politike te usklađuje propise.
- Rezultati dobiveni iz SIEM-a vam olakšavaju put ka zadovoljavanju zahtjeva raznih regulatora (npr. PCI-DSS) i/ili certificiranja po nekoj od security normi (npr. ISO:27001).

## Security Orchestration Automation & Response (SOAR)

- Zahvaljujući podacima prikupljenima u SIEM-u, generira se veliki broj upozorenja (eng. alert) koje je, koliko god SIEM bio dobro podešen, potrebno ručno recenzirati. Ipak, ukoliko na raspolaganju imate SOAR, taj "rudarski" dio posla odrađuje ovaj alat.
- Štedi dragocjeno vrijeme security stručnjacima.



## EPP & EDR

- Endpoint Protection Platform i Endpoint Detection and Response rješenja brinu o malware, antivirusnoj i antispyware zaštiti koja osim vanjskih ugroza, krajnje uređaje štiti i od internih prijetnji.



## Next-Generation Firewall (NG-FW)

- U potpunosti automatizirani vatrozid koji provodi dosljednu zaštitu na čitavoj mreži (SSL dekripcija, ograničavanja dijeljenja podataka, izrada URL filtering politika...).



## DNS Security

- Omogućuje provjeru izvornosti DNS podataka.
- Sprečavanje DDoS i amplifikacijskih napada.
- 91% malwarea koristi DNS za komunikaciju i krađu podataka.
- Rješenja za zaštitu DNS prometa sprečavaju neželjeni DNS i IP promet.



## E-mail Security

- Zaštita elektroničke pošte nove generacije.
- Značajno smanjuje količinu neželjenih e-mailova (Spam blocking, Graymail detection, Outbreak filters...).



## Web Security

- Nadzor i inspekcija web prometa.
- Kao najizloženije dijelove vašeg informacijskog sustava, vaše web stranice, web aplikacije i web servisi trebaju posebnu zaštitu.
- Enkriptiranje, autentikacija, "krpanje" otkrivenih slabih točaka, sprečavanje krađe podataka...



## Analiza mrežnog prometa

- Zahvaljujući naprednom Cisco Smartwatch rješenju ima uvid u mrežni promet (NTA) i brzinu odaziva vaše mreže (NDR) bez obzira jesu li vaši resursi on-premise ili u Cloudu.

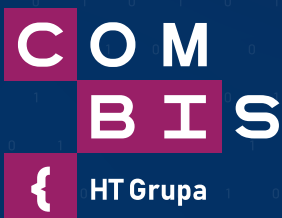
## Zašto COMBIS?

Raspolažemo s velikim brojem stručnjaka koji brinu o informacijskoj sigurnosti najzahtjevnijih korisnika.

Uz dugogodišnje iskustvo u radu na polju informacijske sigurnosti tim posjeduje certifikate stečene na najrelevantnijim institutima i trening centrima poput SANS, EC-Council, ISC2, CompTIA, Offensive Security i sl.. Dodatno, ekspertizu tima potvrđuju i certifikati renomiranih proizvođača gdje se ističu Palo Alto, IBM, Fireeye, TrendMicro i drugi.

Naš cilj je vaša vrhunska zaštita - neprekidno pratimo potencijalne opasnosti i negativne trendove te na njih pravovremeno reagiramo.

# S NAMA JE VAŠE POSLOVANJE SIGURNO!



Kreirajte vaše poslovanje s  
Combisovim poslovnim rješenjima!

e: [sales@combis.hr](mailto:sales@combis.hr), w: [combis.hr](http://combis.hr)