



SRC SMART™

SRC BUILD

Razvoj rešitev in izvedba

SRC MANAGE

Prevzem celotne infrastrukture v upravljanje (hosting...)

SRC OPERATE

Podpora/vzdrževanje, odprava napake v predvidenem času

SRC REPAIR

Zagotavljanje in namestitev nadomestnih delov

SRC ORCHESTRATE

Avtomatizacija upravljanja IKT

SRC SOC

Spremljanje in analiza varnostnih incidentov



SRC d.o.o.
Tržaška cesta 116
1001 Ljubljana
Slovenija

E: info@src.si
T: 01 600 7000
www.src.si

www.src.si

SRC

SOC



Vrste storitve

Ranljivost informacijskih sistemov je dolgo veljala za grožnjo, ki sicer nedvomno obstaja, a je bil njen obseg pogosto podcenjen. V zadnjem obdobju je postalo očitno, kako vsakdanji so napadi na prav vsako napravo, ki je priključena v omrežje. Ne glede na to, s čim se podjetje ali posameznik ukvarja, predstavlja potencialno in dejansko tarčo. Ni več vprašanje, ali bomo napadeni, saj se napad že dogaja. Vprašanje je le, kdaj ga bomo zaznali in kako se bomo odzvali nanj.

Učinkovito, več nivojsko varovanje pred napadi je postalo nuja in ne več privilegij največjih. S tem povezani stroški za podjetje lahko predstavljajo nesprejemljivo breme. Za podjetja, ki želijo upravljanje z varnostjo v celoti zagotoviti znotraj lastne hiše, so posledice slabo varovanje, ali pa finančno breme, ki ga podjetje le stežka nosi.

Obstaja pa tudi tretja pot! V podjetju SRC smo v ta namen razvili storitev **SRC SOC** namenjeno kupcem, ki so pripravljeni vsaj del skrbi za varnost svojih informacijskih sistemov zaupati zunanjemu partnerju. Skupina naših usposobljenih strokovnjakov združuje svoje znanje in tehnologijo v napredne rešitve in procese varovanja. S številom in velikostjo varovanih informacijskih okolij se večja tudi količina podatkov o napadih.

Zato vsak dan vemo več in lahko varujemo vedno bolje!

Z uporabo storitve **SRC SOC** so naši naročniki deležni visokega nivoja varovanja, stroški pa ostanejo sprejemljivi in predvidljivi. Za svoj denar dobijo več varnosti, kot bi jo za iste stroške lahko zagotovili sami.

SRC SOC predstavlja **varnostno informacijski center**, ki deluje na strani izvajalca storitve. Predstavlja vozlišče, kamor se stekajo informacije o stanju, varnostnih grožnjah in napadih, ki pretijo informacijski infrastrukturi naših naročnikov. Informacije skupina strokovnjakov hrani, analizira ter orkestrira morebitne potrebne odzive.

Storitve, ki jih v **varnostno informacijskem centru** v okviru znamke **SRC SOC** izvajamo za svoje naročnike, se v grobem delijo na naslednje:

- + **spremljanje in zaznavanje varnostnih dogodkov**
- + **analiza varnostnih dogodkov**
- + **proženje procesa odpravljanja ali zmanjševanja posledic**
- + **priprava predlogov za posodabljanje programske opreme in nastavitve virov informacijskega sistema**
- + **priprava priporočil za izboljševanje varnostne politike kot zaščite pred varnostnimi incidenti.**

Storitev **SRC SOC** lahko do določene mere prilagodimo potrebam in zmožnostim naročnika. Če ima naročnik že vzpostavljeno zbiranje, spremljanje in koreliranje varnostnih dogodkov prek lastnega sistema SIEM, ta ostane v uporabi, hkrati pa postane tudi posrednik informacij v varnostno-informacijski sistem **SRC SOC**. Če naročnik takšnega okolja še nima, pa se lahko dogovorimo, da v naročnikovo omrežje vgradimo le priključnik, ki posreduje varnostne informacije v sistem SIEM, ki je že del našega varnostno-informacijskega sistema. V tem primeru naročnik nima neposrednega vpogleda v dogajanje v svojem informacijskem sistemu, je pa še vedno deležen vseh storitev, ki mu jih zagotavlja storitev SRC SOC. Nivo varnosti je tako tudi v tem primeru povsem primerljiv s tistim, ki ga dobijo naročniki z lastnim sistemom SIEM.