Postavitev varnostno-operativnega centra

Z naraščajočim številom incidentov v kibernetskem prostoru so organizacije spoznale, da je treba vzpostaviti obrambno ravnotežje. Varnostnim sistemom, kot jih poznamo danes, se tako dnevi počasi iztekajo. Potrebujemo nove prakse, ki temeljijo na razumevanju razvojnih stopenj napada, nenehnem spremljanju in hitrem odkrivanju groženj.

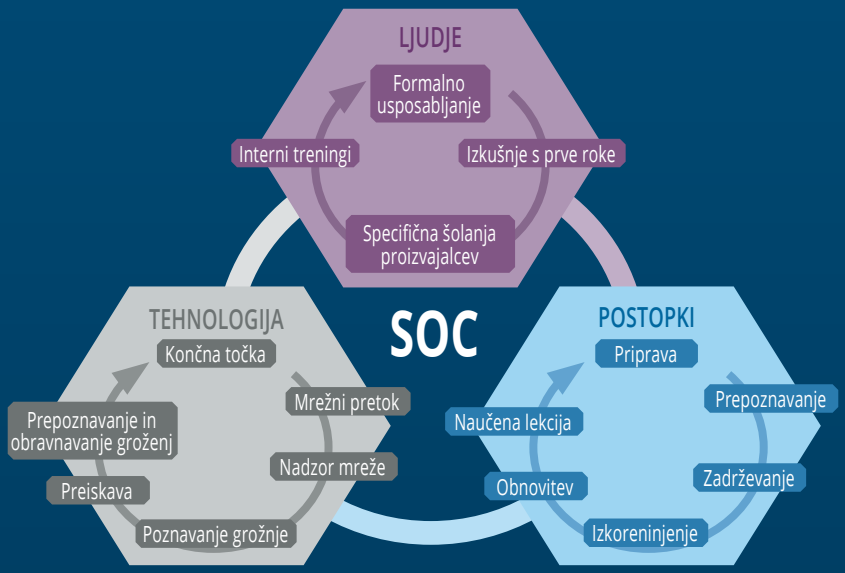
Zakaj je SOC najboljša izbira preprečevanja varnostnih incidentov?

Najučinkovitejši odziv za omejevanje in prihodnje preprečevanje kibernetskih napadov je vzpostavitev okolja, katerega ključni cilje je spremljanje, prepoznavanje in pravočasno odzivanje na vse tipe varnostnih incidentov.

Vzpostavitev **varnostno-operativnega centra** (Security Operation Center – SOC) je pravi odgovor za sodobni čas, ko je digitalna infrastruktura s povečano dostopnostjo vse pogosteje tarča kibernetskih napadov.

S&T Slovenija, Informacijske rešitve in storitve d.d., Leskoškova cesta 6, 1000 Ljubljana, tel.: (0)1 5855 200, www.snt.si, info@snt.si

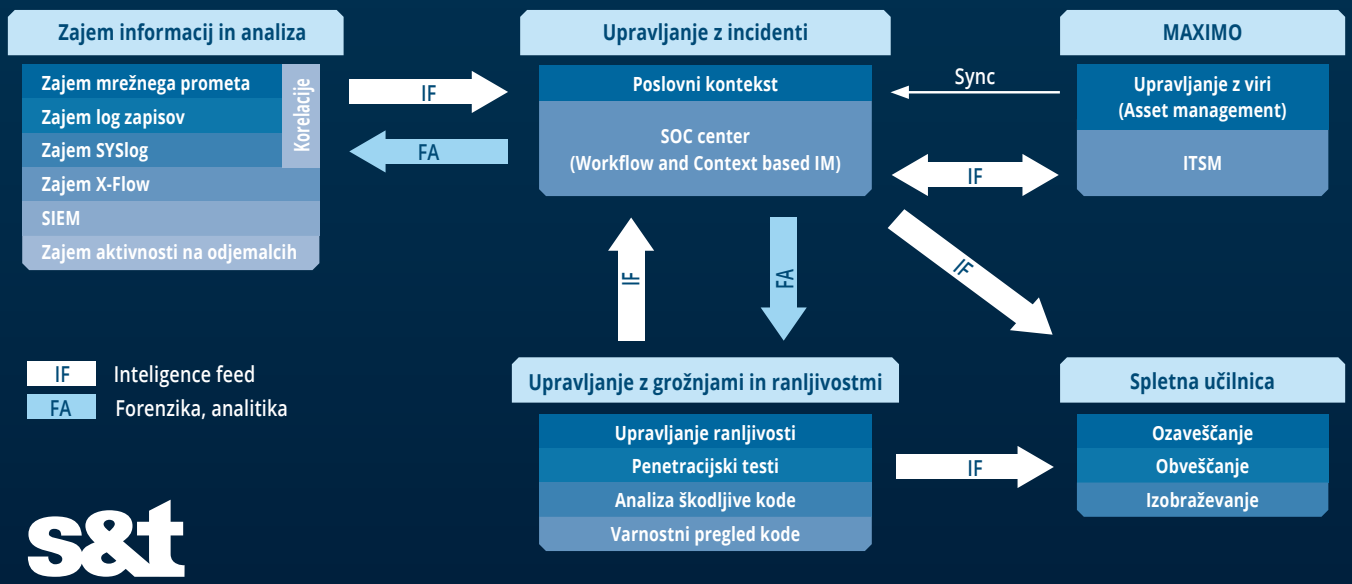
Ključni gradniki varnostno-operativnega centra



Vir: SANS: Building a world-Class Security Operations Center: a Roadmap, Maj 2015

Storitve varnostno-operativnega centra

Konceptualna shema storitev SOC



S&T Slovenija, Informacijske rešitve in storitve d.d., Leskoškova cesta 6, 1000 Ljubljana, tel.: (0)1 5855 200, www.snt.si, info@snt.si