

SIEM Cloud

QRadar je opće potreban vrhunski poslovni servis, što je potvrdio i Gartnerov 'Magični kvadrant' za SIEM proizvode za 2017.

Piše: Smart tim

Cloud usluge su postale sveprisutna stvarnost današnjih IT i poslovnih sustava. Trenutna aktivacija usluge, prilagodljivost, jednostavnost korištenja, brza implementacija sve su to karakteristike cloud usluga koje je teško postići klasičnim pristupom poslovnim IT rješenjima.

SIEM cloud

Megatrend poslovna rješenja, unutar postojećeg skupa cloud usluga, i temeljem svojeg gotovo tri desetljeća dugog iskustva nudi korisnicima SIEM cloud rješenje. QRadar je opće potreban vrhunski poslovni servis, što je potvrdio i Gartnerov 'Magični kvadrant' za SIEM proizvode za 2017. QRadar u Megatrend cloudu je cloud usluga potpunog nadzora svih segmenata bilo kojeg IT sustava. Osim nadzora usluga, pruža i mogućnost automatskog otklanjanja internetskih prijetnji, obavijesti o neautoriziranom pristupu poda-

cima, status svih resursa i planiranje performansi. U korisničko IT okruženje se instalira virtualno računalo (tzv. Log collector) koje sve prikupljene nadzorne podatke šalje u Megatrend Data Centar (centralni dio SIEM rješenja). SIEM sustav daje kompletnu sliku svih događaja na vrlo jasan i pregledan način. Svi se događaji „koreliraju“, tj. prati se svaki događaj od početka do kraja po svim uređajima – ekspertni sustav (koristi Watson podršku odlučivanju) povezuje sve tehničke detalje i daje jasnu i preglednu

sliku događaja bez nepotrebnih tehnološki akronima. Naravno, u bilo kojem trenutku moguće je pogledati bilo koji tehnički detalj. SIEM sustav je povezan sa svjetskim X-Force „Threat Intelligence“ sustavom gdje se automatski obrađuju i sprečavaju svi internet napadi.

Rješavanje problema

QRadar u Megatrend cloudu adresira niz poslovnih problema – s povećanjem automatizacije procesa i prisutnosti e-pošte, broj potencijalnih sigurnosnih slabih

točaka znatno se povećava. Zbog obveza GDPR-a klijenti preferiraju pohranjivanje podataka i rješenja unutar nacionalnih granica ili regije. Kupci nemaju dovoljno kvalificiranih stručnjaka za sigurnost, usmjereni su i ulažu u osnovnu djelatnost i obrazovanje zaposlenika za razvoj temeljnog poslovanja. Kupci imaju korporativne aplikacije (aplikacije interne transakcije) koje zahtijevaju nadzor nad sigurnošću, nerado ulažu u poslovni prostor za svoju IT infrastrukturu te žele biti "mobilni" u vezi s IT infrastrukturom.



Biznis

Prednosti rješenja

Korisnik ima svoje SIEM sučelje i može izravno upravljati rješenjem, no nije nužno da korisnik ima dedikiranu osobu za IT sigurnost. Nadzor mreže, nabava, upgrade rješenja, DR i backup te sigurnosni nadzor korporativnih aplikacija je u segmentu aktivnosti pružatelja usluga, konkretno Megatrenda u ovom slučaju. Korisnici imaju mogućnost geografskog lociranja njihova outsourced rješenja i fizičke provjere lokacije njihovih podataka. Megatrend poslovna rješenja raspolažu s ISO 20000 i ISO 27001 certifikatima na koje se korisnik može referirati te nema potrebe s korisničke strane za osiguranjem ovih certifikata u području IT sigurnosti. Uslugu je moguće besplatno testirati na linku <http://qradar.megatrend.com>.