Security Incident & Event Management (SIEM)

Sistem SIEM zagotavlja nenehno izboljševanje varnosti informacijskega sistema. Zakaj?

1. Sistem za upravljanje varnostnih informacij in dogodkov (SIEM) zbira podatke z različnih naprav v informacijskem sistemu, ustvarja povezave med podatki, ki jih dobi s teh naprav, in na podlagi dobljenih rezultatov obvešča o varnostnih incidentih v informacijski strukturi.
2. Sistem SIEM je tudi primarni gradnik varnostno-operativnega centra (SOC).
3. Sistem SIEM povezuje varnost, skladnost in obratovanje IT informacijskega sistema v centralno točko.

Prednosti vpeljave sistema SIEM:

- centralizirano zbiranje dnevniških zapisov, podatkov o podatkovnih pretokih, zajem prometa glede na vključene module v SIEM-rešitvi,
- spremljanje velike količine dnevniških zapisov v realnem času,
- povezovanje podatkov, ki omogoča večje možnosti zaznave incidentov,
- skladnost z zakonodajo in predpisi,
- izboljšano obvladovanje tveganj in višja stopnja varnostne politike,
- avtomatizirano poročanje.

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

Vhodni podatki sistema SIEM

Sistem SIEM sprejema/zajema dnevniška sporočila z različnih naprav, npr. varnostnih naprav, mrežnih naprav, strežnikov, aplikacij itd. Sporočila so največkrat povezana z dogodki, kot so prijave, spremembe na sistemu, varnostni dogodki itd.

Poleg dnevniških sporočil so za SIEM pomembni tudi podatki o podatkovnih pretokih, ki dajejo podatke o izvornih/ponornih napravah, tipu aplikacije ter količini prenesenih podatkov.

Za zaznavanje sodobnih varnostnih incidentov v sistemu SIEM tudi spremljajo celoten promet in iščejo anomalije.

Obdelava podatkov

Sistem SIEM poleg normalizacije in agregacije tudi filtrira log sporočila ter jih razčlenjuje v obliko, ki je primerna za prikaz v grafih ali tabelah. Vmesniki za pregledovanje in analizo omogočajo rudarjenje po zbranih podatkih prek različnih nadzornih plošč. Zelo učinkovito se lahko izvaja forenzika, saj je mogoče hitro ugotoviti, na katerih napravah se je pojavil problem in kateri dogodki so se še zgodili ob pojavu problema.

Korelacija podatkov

Poleg osnovnih korelacij sodobni sistemi SIEM omogočajo tudi povezovanje z zunanjimi izvori, npr. reputacijo IP-naslovov, spletnih strani ..., ki jih povežejo s podatki ali prometom nadzorovane infrastrukture. Korelacija je pomembna tudi za zaznavanje napadov na informacijsko infrastrukturo, npr. APT.

Poročanje

Sistemi SIEM omogočajo izdelavo poročil glede na različna priporočila oz. standarde, kot so npr.: **ISO27002**, **NERC**, **BASEL II**, **PCI DSS**, **Sarbanes-Oxley** in **HIPAA**.

Shranjevanje log sporočil

Sistemi SIEM omogočajo tudi dolgoročno shranjevanje glede na pomembnost log sporočil. Shranjenih sporočil tudi ni mogoče spreminjati, zato jih je mogoče uporabiti za dokazovanje.

SIEM ni produkt, ampak rešitev

Sistem SIEM je orodje, ki brez virov dogodkov ne more izvajati svoje funkcije. Za uspešno implementacijo je zato treba določiti vse vire, možnost filtriranja (s tem se lahko zmanjša potrebne performanse sistema SIEM), prilagojeno razčlenjevanje dogodkov, primerne točke za zajem prometa, smiselne korelacije, poročila, alarme ...

Glede na ugotovitve analize vam pripravimo predlog rešitve z opremo, ki je glede na ceno in zmogljivost najprimernejša.

SIEM-rešitve izvajamo z opremo proizvajalcev RSA in McAfee.

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