Bezpečnostný dohľadový systém

V uplynulých mesiacoch sa na nás valilo množstvo informácií ohľadom plnenia legislatívnych požiadaviek známych pod skratkou GDPR. Jednou z oblastí tejto regulácie je aj evidovanie a nahlasovanie bezpečnostných incidentov, a to najmä takých, kedy môže dôjsť k úniku spracúvaných osobných údajov. Na tieto požiadavky sú spoločnosti pomerne slabo pripravené a to z technického aj personálneho hľadiska. Vlastný bezpečnostný tím je samozrejmosťou skôr vo veľkých spoločnostiach ako napríklad banky, ale v prípade menších firiem alebo verejných organizácií je luxusom často aj jeden človek, ktorý je zodpovedný za bezpečnosť IT prostredia.

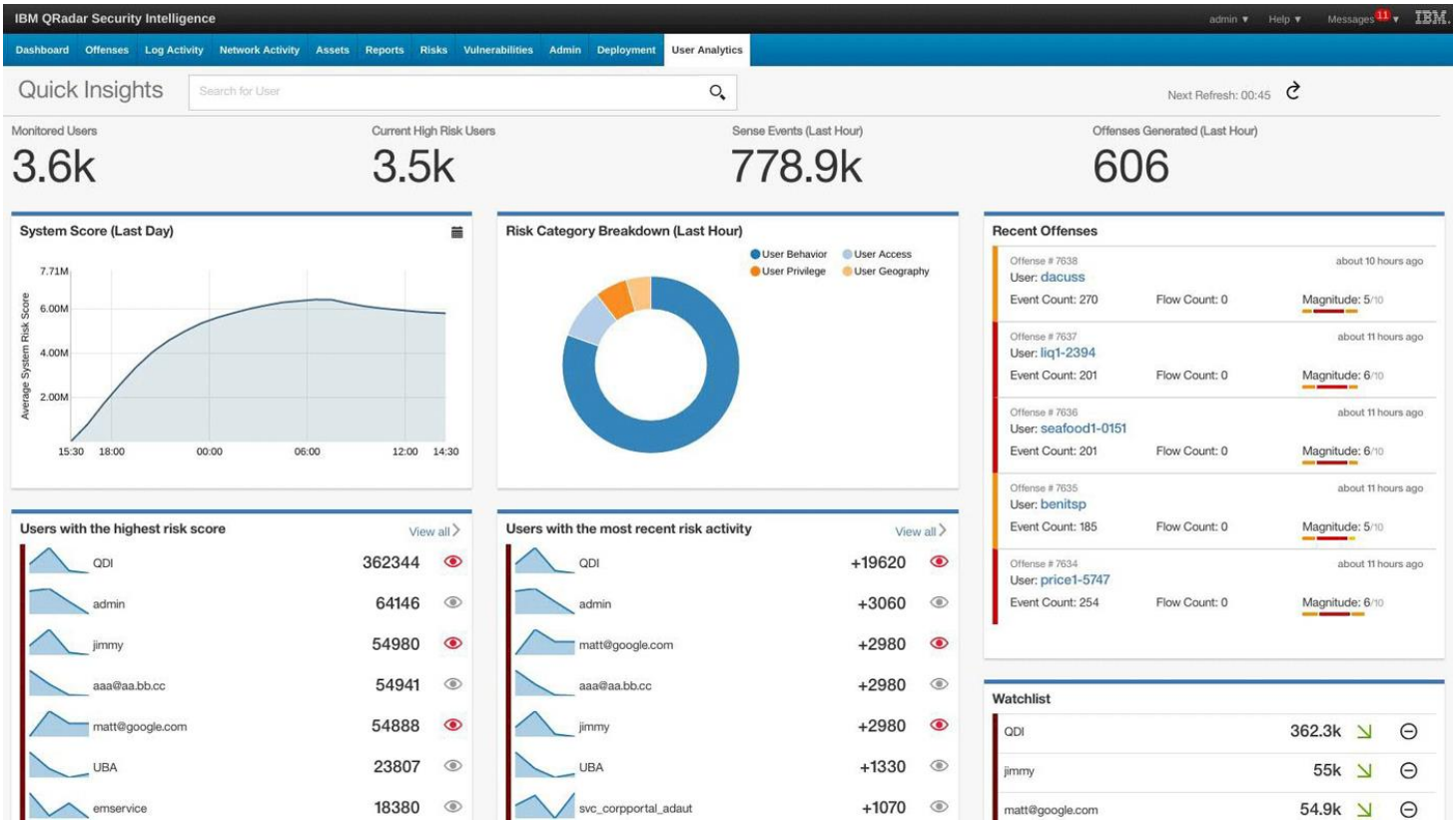
Technicky je možné túto požiadavku splniť nasadením riešenia zo skupiny produktov **Security information and event management (SIEM)**. Netreba ale zabudnúť ani na zabezpečenie prevádzky, pretože len nasadenie takéhoto systému bez dostatočného personálneho zabezpečenia má často slabý efekt. Naša spoločnosť poskytuje služby nasadenie bezpečnostného riešenia a následne komplexnú službu bezpečnostného dohľadu prostredníctvom **Security Operations Center (SOC)**. Súčasťou tímu SOC sú vyškolení špecialisti, ktorí sa venujú vzniknuvším bezpečnostným incidentom, následne ich vyšetrujú a vyhodnocujú. Ich úlohou je aj koordinácia s produktovou podporou výrobcu, vedenie dokumentácie, manažment zmien, proaktívny monitoring, identifikácia a odstraňovanie chýb v závislosti od dohodnutej úrovne služby.

Jedným z riešení typu **SIEM**, ktoré naša spoločnosť podporuje aj vlastným **SOC**, je bezpečnostná platforma **IBM QRadar Security Intelligence**. Hlavnou úlohou riešenia je v reálnom čase analyzovať (agregovať, korelovať) bezpečnostné udalosti a toky generované zariadeniami a aplikáciami v sieti. Na základe vyhodnotenie potom upozorňuje na bezpečnostné incidenty, poskytuje reporting a dlhodobé úložisko záznamov.

Hlavným prvkom architektúry je centrálny **server SIEM**. Slúži pre manažment ostatných komponentov, zber udalostí a informačných tokov, identifikáciu bezpečnostných výnimiek na základe korelačných pravidiel a znalostnej databázy, automatický reporting, poskytuje garantované úložisko dát a sprístupňuje aj grafické užívateľské rozhranie. Centrálny server je potrebné navrhnúť podľa požadovaného výkonu, ktorý sa meria v jednotkách **EPS** (events per second) a **FPM** (flows per minute). Ďalším komponentom riešenia je **Event Collector**, ktorý zabezpečuje zber udalostí z jednotlivých zariadení a aplikácií v sieti. Tento komponent je typicky nasadený v režime vysokej dostupnosti, prípadne viacero komponentov podľa typu zbieraných udalostí alebo sieťovej topológie. Systém **IBM QRadar** podporuje zber udalostí z rôznych zdrojov, či už sú to sieťové zariadenia, špecializované bezpečnostné systémy, alebo bežné operačné systémy alebo rôzne aplikácie.

Hlavné charakteristiky bezpečnostného riešenia IBM QRadar Security Intelligence

- automatický nástroj na hlásenie kybernetických bezpečnostných incidentov
- monitoring, spracovanie, vyhodnocovanie a archivácia bezpečnostných udalostí
- posilnenie bezpečnosti celého prostredia ICT
- monitorovanie manipulácie s citlivými údajmi a aplikáciami
- prevencia pred únikom dát a možnosť rýchlo vypátrať konkrétneho vinníka
- normalizácia udalostí z bezpečnostných záznamov do zrozumiteľnej podoby
- jednoduché užívateľské rozhranie SIEM a on-line grafické výstupy a reporty
- služba vyšetrovania bezpečnostných incidentov v spolupráci a AC SOC


IBM QRadar Security Intelligence
admin
Help
Messages 11
IBM
Dashboard
Offenses
Log Activity
Network Activity
Assets
Reports
Risks
Vulnerabilities
Admin
Deployment
User Analytics
Quick Insights
Search for User
Next Refresh: 00:45
Monitored Users
3.6k
Current High Risk Users
3.5k
Sense Events (Last Hour)
778.9k
Offenses Generated (Last Hour)
606
System Score (Last Day)
Average System Risk Score
7.71M
6.00M
4.00M
2.00M
15:30
18:00
00:00
06:00
12:00
14:30
Risk Category Breakdown (Last Hour)
User Behavior
User Access
User Privilege
User Geography
Recent Offenses
Offense # 7638
about 10 hours ago
User: dacuss
Event Count: 270
Flow Count: 0
Magnitude: 5/10
Offense # 7637
about 11 hours ago
User: liq1-2394
Event Count: 201
Flow Count: 0
Magnitude: 6/10
Offense # 7636
about 11 hours ago
User: seafood1-0151
Event Count: 201
Flow Count: 0
Magnitude: 6/10
Offense # 7635
about 11 hours ago
User: benitsp
Event Count: 185
Flow Count: 0
Magnitude: 5/10
Offense # 7634
about 11 hours ago
User: price1-5747
Event Count: 254
Flow Count: 0
Magnitude: 6/10
Users with the highest risk score
View all
QDI 362344
admin 64146
jimmy 54980
aaa@aa.bb.cc 54941
matt@google.com 54888
UBA 23807
emservice 18380
Users with the most recent risk activity
View all
QDI +19620
admin +3060
matt@google.com +2980
aaa@aa.bb.cc +2980
jimmy +2980
UBA +1330
svc_corpportal_adaut +1070
Watchlist
QDI 362.3k
jimmy 55k
matt@google.com 54.9k