Detectare rapidă a amenințărilor de securitate și răspuns prioritar

Integrarea datelor, analiza jurnalelor (log-urilor) și prioritizarea incidentelor accelerează remedierea amenințărilor.

Studiu de caz. Industrie: Finanțe. Tehnologie: Qradar SIEM

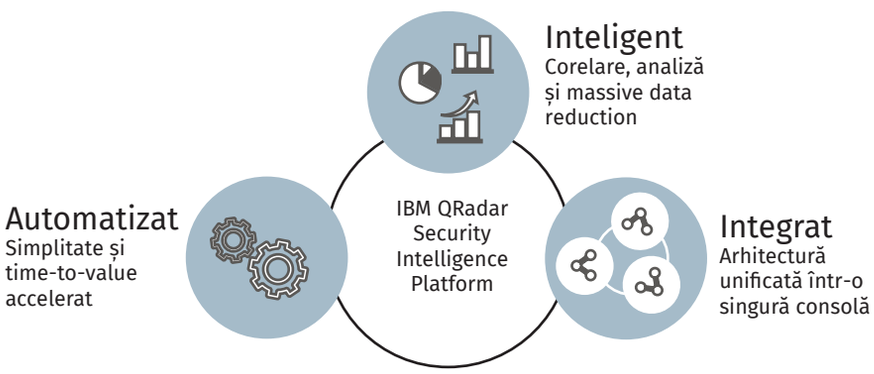
Clientul

Banca Națională a Moldovei este banca centrală a Republicii Moldova. Obiectivul fundamental al instituției este asigurarea şi menţinerea stabilităţii preţurilor. BNM promovează şi menţine un sistem financiar bazat pe principiile pieţei şi sprijină politica economică generală a statului.

Problema

BNM s-a confruntat cu necesitatea de a implementa un sistem informaţional modern, care să răspundă tuturor cerințelor de dezvoltare ale băncii, inclusiv în domeniul administrării securității IT și monitorizării conformității cu reglementările actuale. Un sistem care să răspundă la provocări generate de:

- **escaladarea atacurilor** – metode sofisticate de atac, limite de acces care dispar, accelerarea breșelor de securitate;
- **complexitatea crescândă** – infrastructură în cotinuă schimbare; prea multe produse de la prea mulți vendori care sunt costisitoare de configurat și gestionat; instrumente ineficiente și necorespunzătoare;
- **constrângeri legate de resurse** – echipe de securitate în dificultate; prea multe date în condițiile în care resursele umane sunt limitate; creșterea cerințelor de conformitate privind monitorizarea și gestionarea resurselor.



Soluție

IBM Qradar SIEM – o soluție ce permite echipelor de securitate să detecteze și să prioritizeze amenințările din instituție, oferind informații inteligente pe baza cărora echipele să poată răspunde rapid și să reducă impactul incidentelor de securitate.

Prin consolidarea datelor de tip “log event” și “network flow” de la mii de dispozitive, endpointuri și aplicații existente în rețea, QRadar corelează toate aceste informații și consolidează evenimentele în alerte unice. Astfel, analiza și remedierea incidentelor este accelerată.

Rezultat

- Integrarea datelor, analiza jurnalelor (log-urilor) și prioritizarea incidentelor – caracteristici cheie ale IBM Qradar SIEM au condus la accelerarea remedierii amenințărilor asupra sistemului informțional al BNM.

- Analiza inteligentă a contribuit la economisirea timpului, prin reducerea numărului de fals pozitive pentru investigare, ceea ce în final a condus la diminuarea semnificativă a numărului de incidente detectate.

- Prioritizarea a redus volumul de muncă al echipei prin identificarea celor mai periculoase amenințări.

IBM® QRadar® Security Information and Event Management (SIEM)

Un produs SIEM care identifică evenimentele de securitate IT și le prioritizează în funcție de importanța lor.

Magic Quadrant for Security Information and Event Management, conform Gartner 2021

Qradar SIEM - o platformă exhaustivă de analiză a datelor din infrastructura IT care elimină practic orice barieră dintre obținerea efectivă a informațiilor şi generarea unor acțiuni de răspuns pe baza acestora.

Platforma centralizează date structurate din întreaga infrastructură IT, indiferent de sursă, le interoghează și analizează, însă valoarea nu este dată de posesia datelor ci de faptul că, pe baza rezultatelor obținute, pot fi generate rapid acțiuni.

Top cazuri de utilizare SIEM în sistemul bancar :

- (Tentative de) a compromite credențialele utilizatorului.
- Escaladarea nejustificată a privilegiilor.
- Folosirea greșită a unui cont.
- Comportament neobișnuit pe conturile privilegiate.
- Trafic către domain-uri rău intenționate.
- Protecție împotriva pierderii datelor.
- Schimbări de sistem.
- Instanțe de refuzare a serviciului.

Contactați-ne

Chișinău MD-2012
Str. Alexandru cel Bun 85
Republica Moldova

Telefon: +373 22 210 208
Email: office@rsd.md
Website: www.rsd.md

Silver Business Partner