ANDREWS IT ENGINEERING

A SOCaaS működése

24/7 észlelés, reagálás, riportálás

A Galileum SOC valós időben védi a vállalatot — a fenyegetés észlelésétől a teljes incidenskezelésig.

1

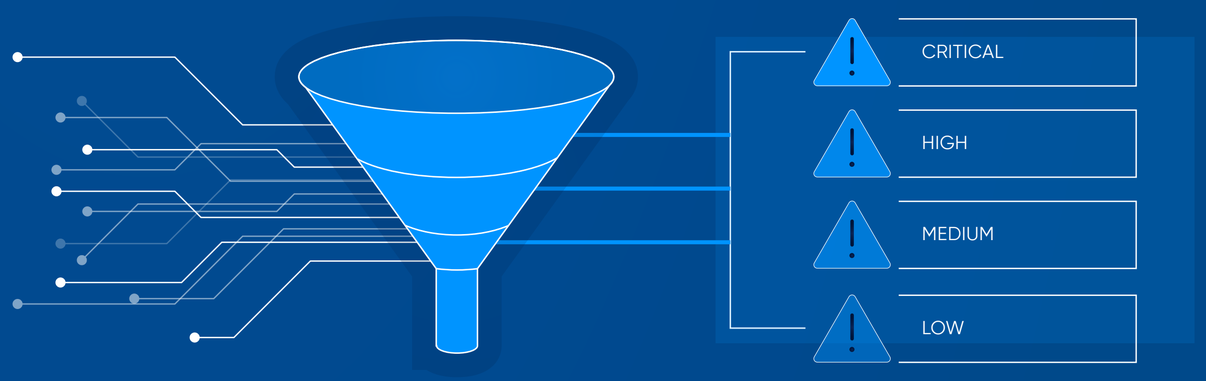
Adatgyűjtés és Észlelés

Logok és telemetria több száz forrásból → SIEM + UEBA elemzés → gyanús minták felismerése.

2

Triage és Priorizálás

A SOC kiszűri a false positive-okat, enrich-eli az adatokat, és eldönti, mely riasztás valódi fenyegetés.



3

Incidensvizsgálat

A SOC elemzők mély log-összefüggések feltárásával meghatározzák a támadás útvonalát, hatókörét és célját.

4

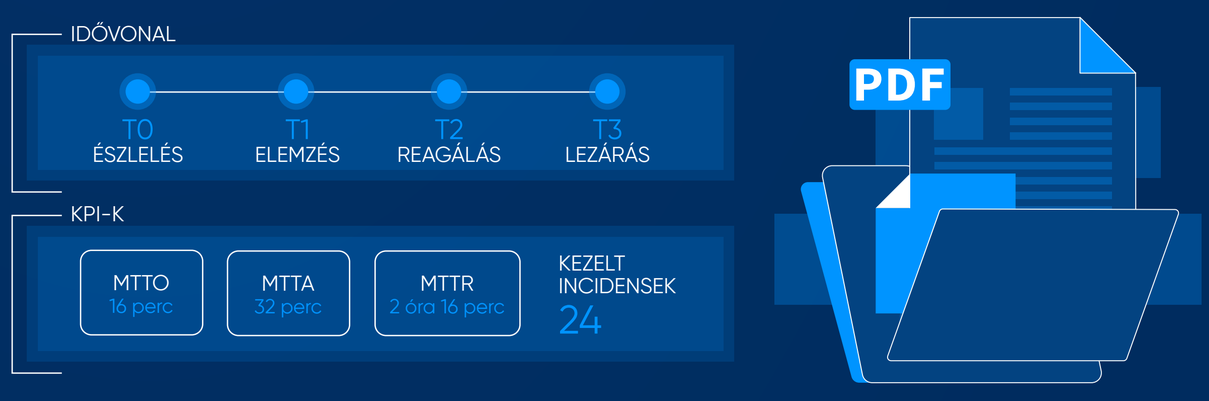
Reagálás és Elhárítás

Automatizált munkafolyamatok vagy a SOC szakértők megállítják a támadást: izolálás, blokkolás, helyreállítás.

5

Riportálás és Kommunikáció

Részletes incidensriport, idővonal, érintett rendszerek, ajánlások — átlátható, auditálható működés.

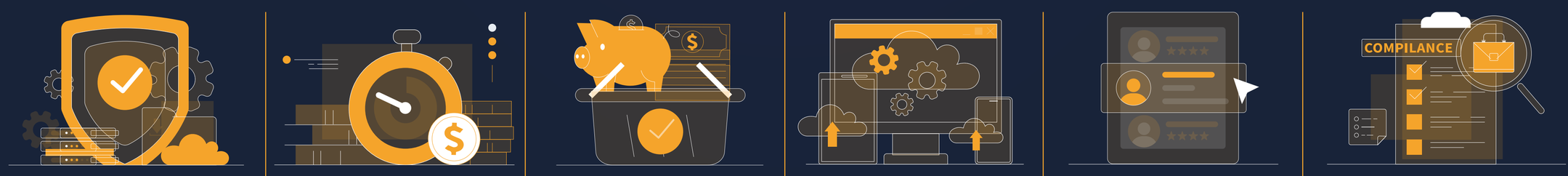


6

Folyamatos Fejlesztés

Use case és szabály finomhangolás, threat hunting — minden incidens után erősebb védelem.

Ügyfélérték



24/7 kibervédelem

Zéró beruházási költség

Kiszámítható, használat-alapú árazás

Személyre szabott szolgáltatás

Szakértői csapat

Auditálható működés