Kristálygömb 2022

Csinos Tamás, CISSP
country manager
Clico Hungary
tamas.csinos@clico.hu

CLICO | 30 YEARS

Security Networking Management

A CLICO Európában

- Poland: HQ Kraków, Offices: Katowice, Rzeszów, and Warsaw
- Bulgaria: Sofia
- Croatia: Zagreb
- Czech, Slovakia: Praha
- Hungary: Budapest
- Latvia: Riga
- Romania: Bucharest
- Serbia: Belgrade
- Slovenia: Ljubljana
- Strong presence in Baltics and Georgia

CLICO | 30 YEARS

Security Networking Management


Acronis
ARISTA
ARMIS
AVSYSTEM
cryptme
Cryptshare
CYBERARK
DIGI
ENTRUST
esecure
SECURE VISIO
exabeam
Fidelis Cybersecurity
Forcepoint
tufin
UCOPIA COMMUNICATIONS
FORESCOUT
GREYCORTEX
THALES
imperva
Infinera
JUNIPER driven by Mist AI
MICROSENS
mobileiron
NACVIEW
opengear A DIGI COMPANY
paloalto NETWORKS
Pulse Secure
radware
RAPID7
Recorded Future
rubrik
SailPoint
SentinelOne

Öveket bekötni: fejlődés és innováció

SIEM (+UEBA +SOAR (=SOC?)

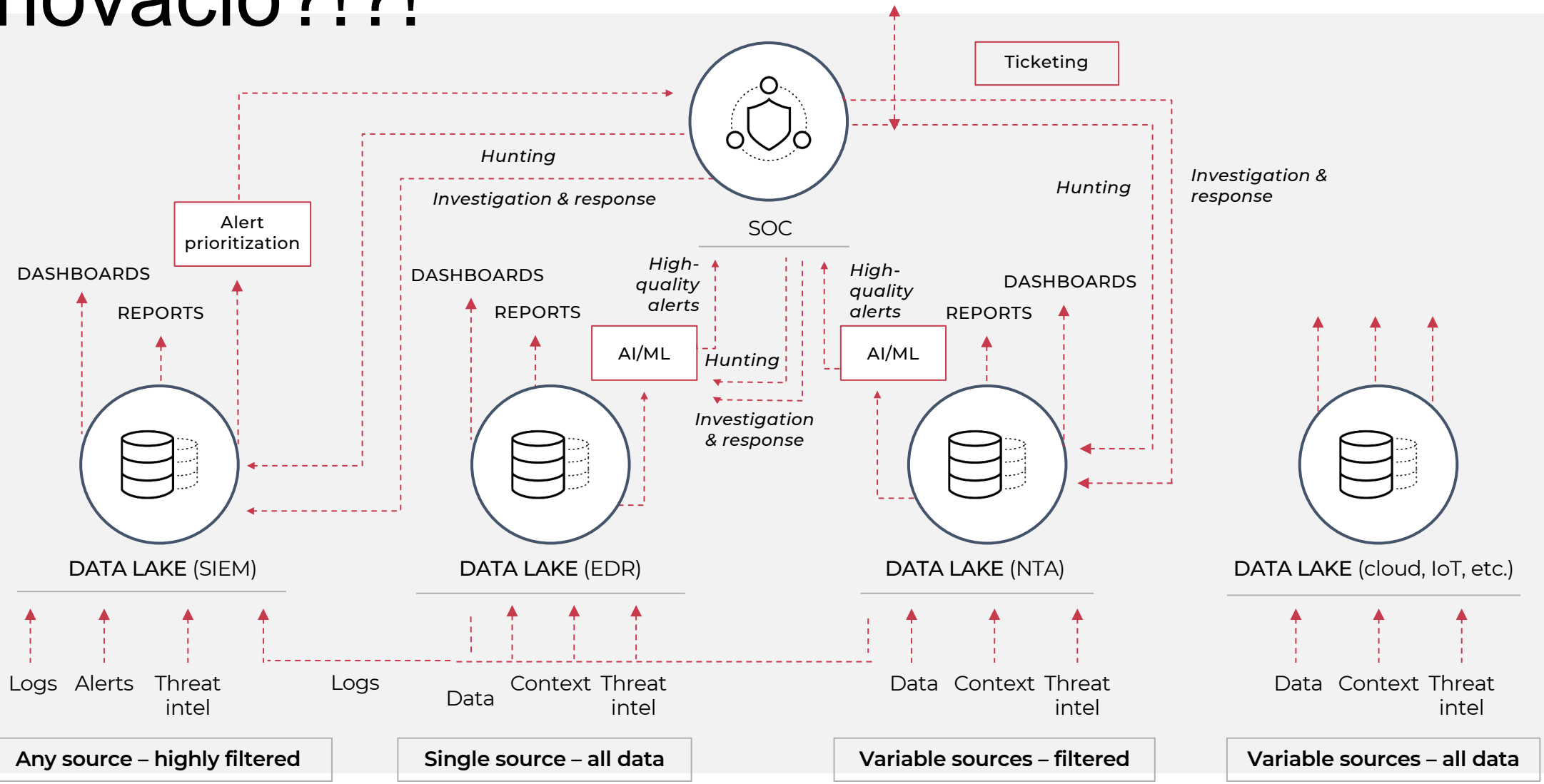
NTA->NDR + végponti telemetria

EPP->EDR + hálózati telemetria

Tetszőleges kombinációja az eddigieknek

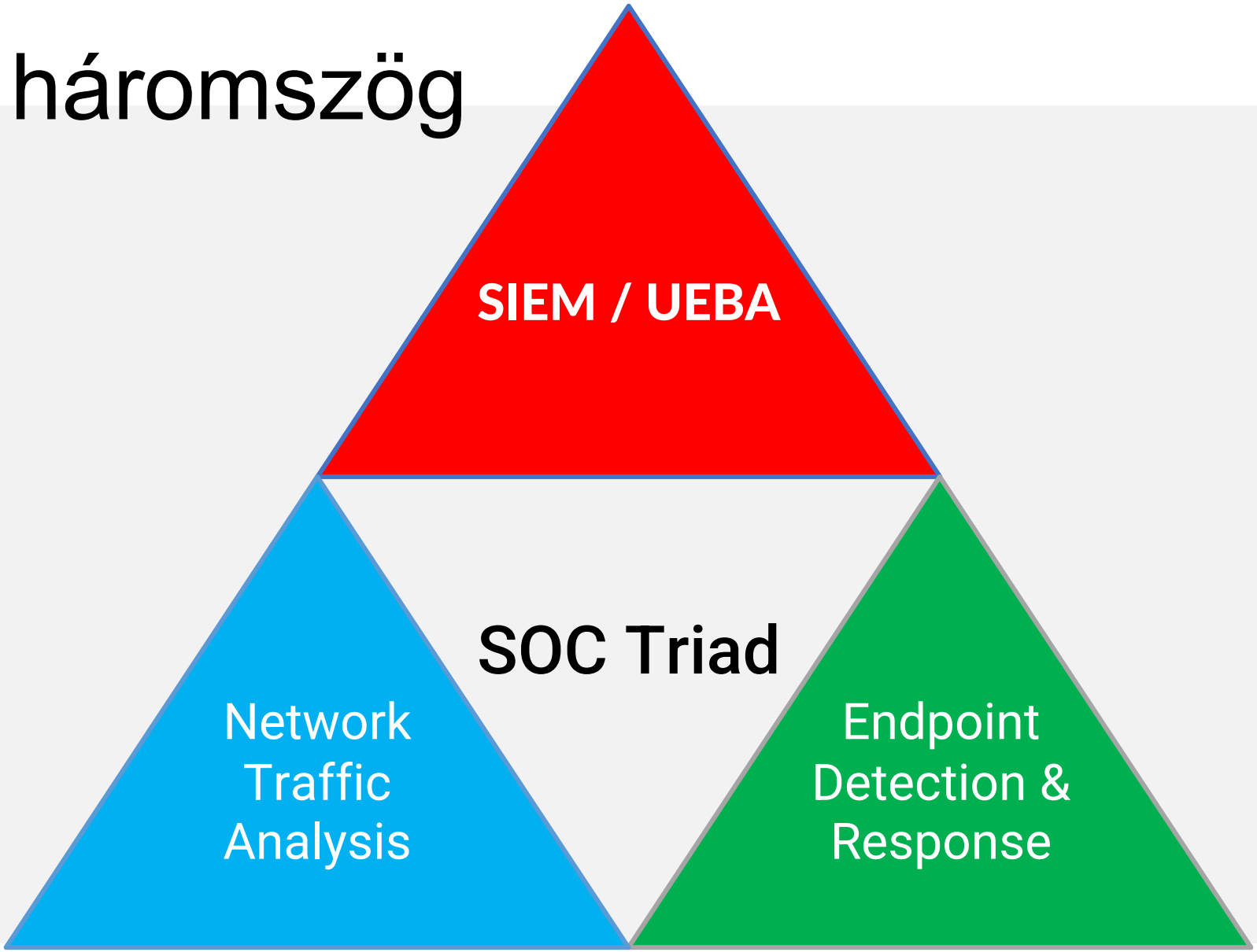
Marketing bullshit

Innováció?!?!

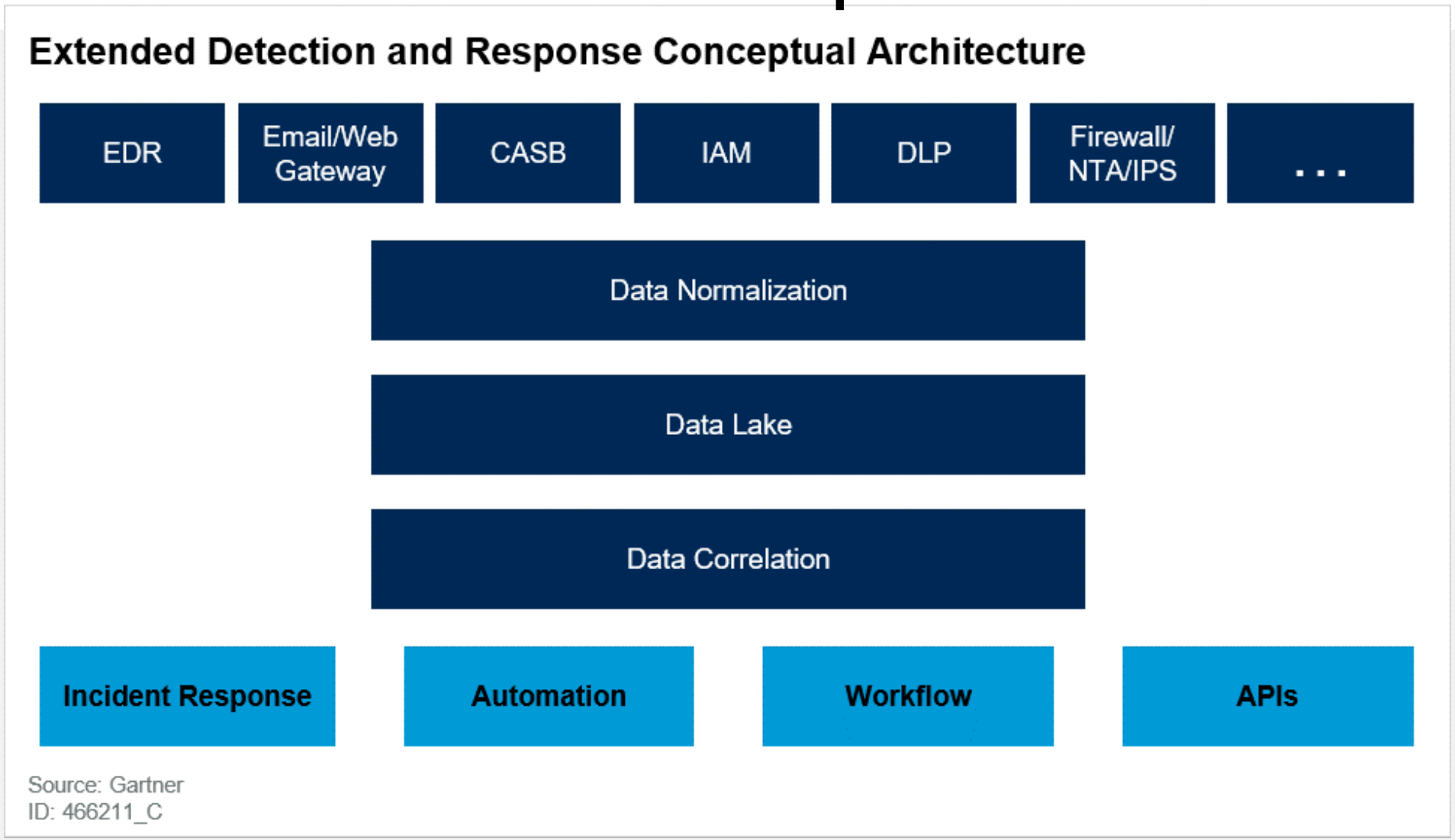


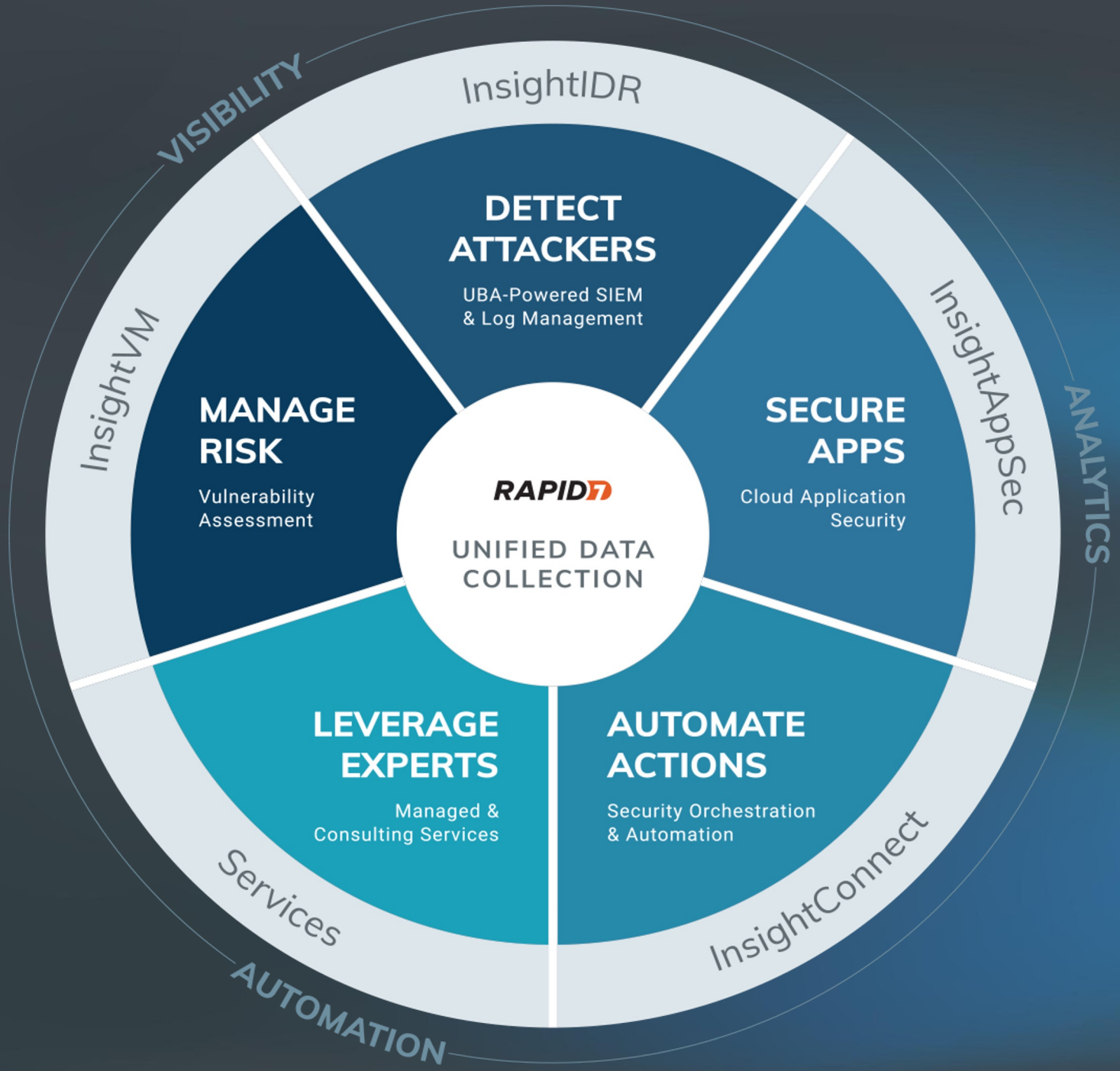
Security Networking Management

A Gartner-féle háromszög



A Gartner-féle XDR koncepció





RAPID7

RAPID7

Fidelis Elevate®

Fidelis Cybersecurity

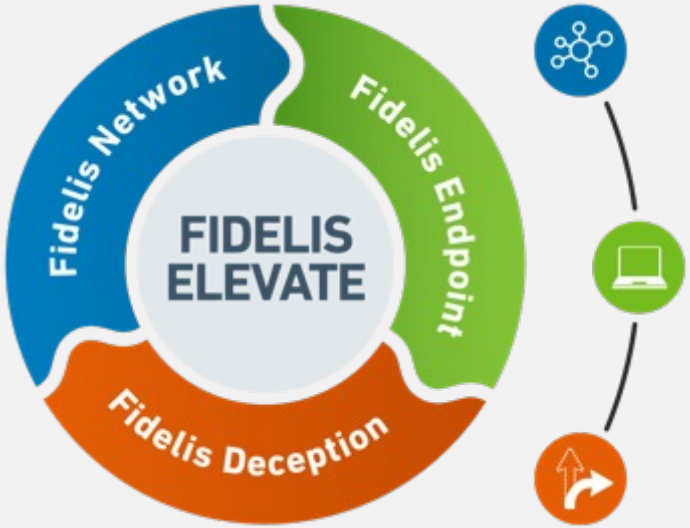
Automate Detection, Hunting, Investigation and Response

One Platform. Multiple Use Cases and Categories.

Network Detection & Response | Insider Threats | Network DLP | EDR + EPP | Asset Profiling & Classification | Deception | Incident Response | MDR

Fidelis Elevate – ADR – Automated Detection and Response :

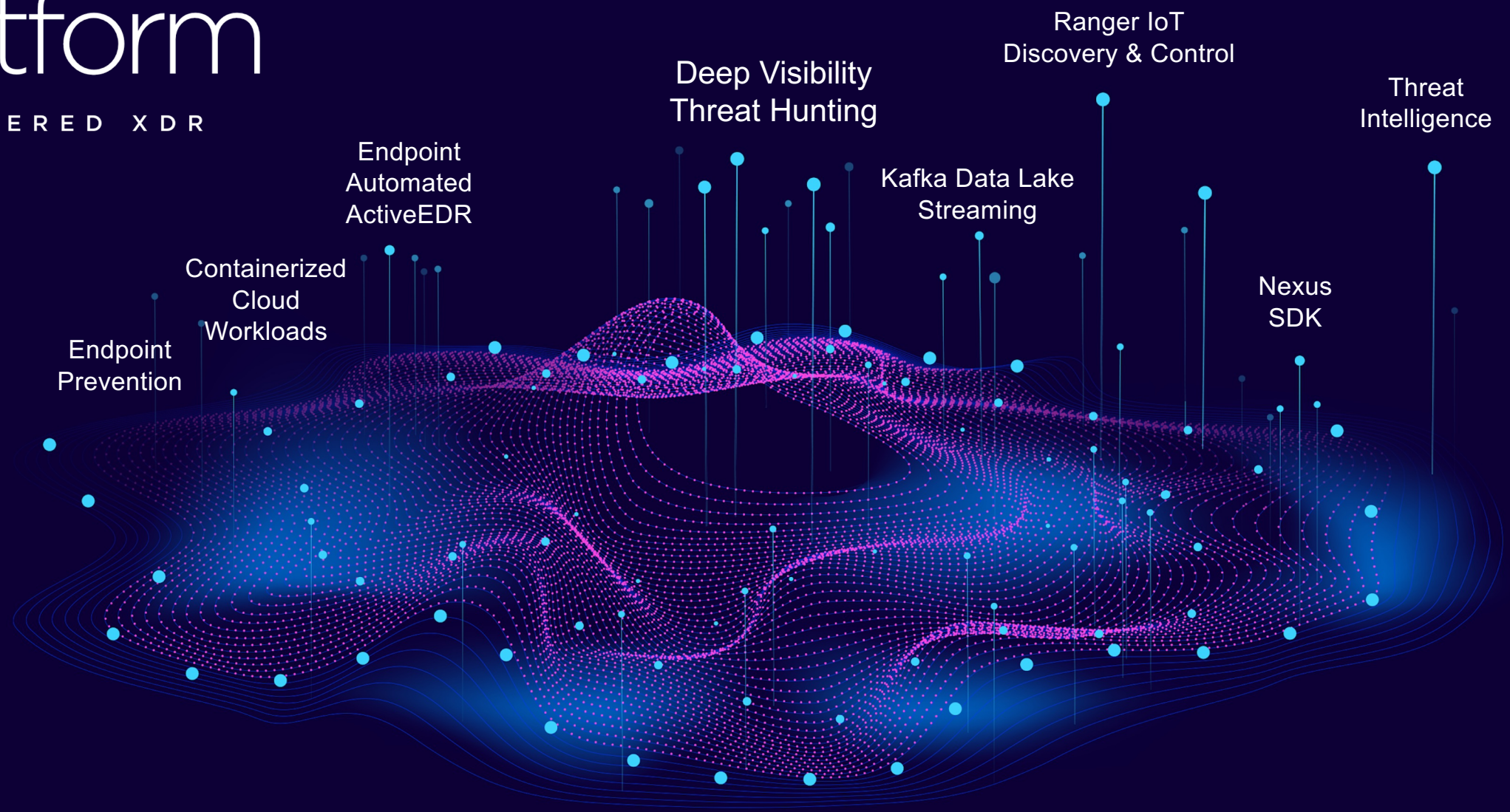
- Integrated platform for **cyber incidents prevention, detection and investigation**
- Security experts' instrument for deep **visibility on network and endpoints**
- **Unified User Interface** for 3 fully integrated modules :
  - **Fidelis Network** – detection and prevention in network
  - **Fidelis Endpoint** – EDR + EPP – complete endpoints detection (DLP soon)
  - **Fidelis Deception** – intelligent decoys – proactive detection



Singularity Platform

AI-POWERED XDR

SentinelOne™



Palo Alto Networks Cortex XDR

Prevent everything you can

CORTEX XDR BY PALO ALTO NETWORKS

Everything you can't prevent, detect and investigate fast

CORTEX XDR BY PALO ALTO NETWORKS

Automate response and get smarter with each incident

CORTEX XSOAR BY PALO ALTO NETWORKS

Cortex XDR 3.0 - **Deeper** Detection, **Broader** Investigation, **Faster** Response

Deeper Analytics Detections

XDR for cloud

Cloud Detection & Response for the SOC

Analytics Detections for cloud specific threats

Prisma Cloud + XDR for cloud = Most Complete Cloud Security

Identity Analytics

Detect compromised users, entities, machines

Data integration with HR systems

Risk scoring for users plus 360° user views

Broader Investigation Scope

Third-Party Data Engine

Expanded third-party data for virtually any source

3rd party correlations to enrich XDR detections

Ad-hoc search with XQL (eXtended Query Language)

Forensics Module

Toolkit used by Unit 42 Elite Incident Responders

Deploy & collect data prior to or after compromise

Integrated into Cortex XDR Agent

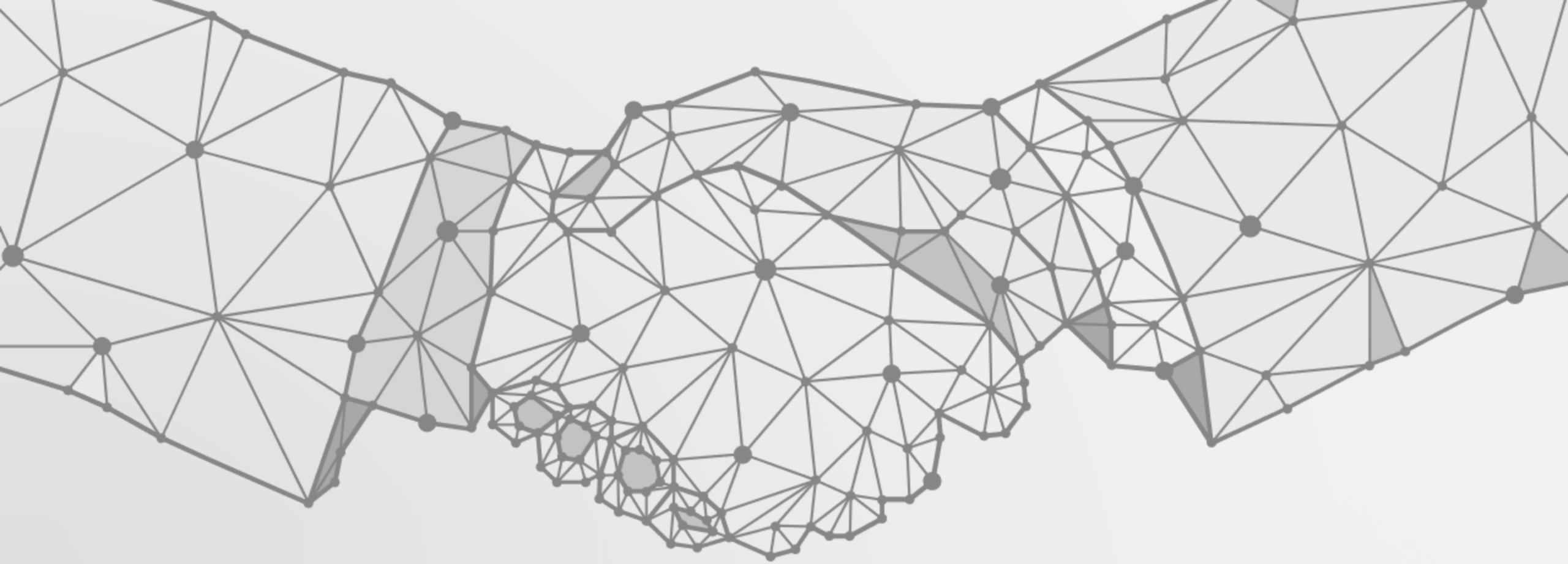
Faster Response

New Incident Management UI

MITRE ATT&CK mapping of evidence and artifacts

Inbox-style previews and contextual views

SOC manager dashboard



Köszönöm a figyelmet!