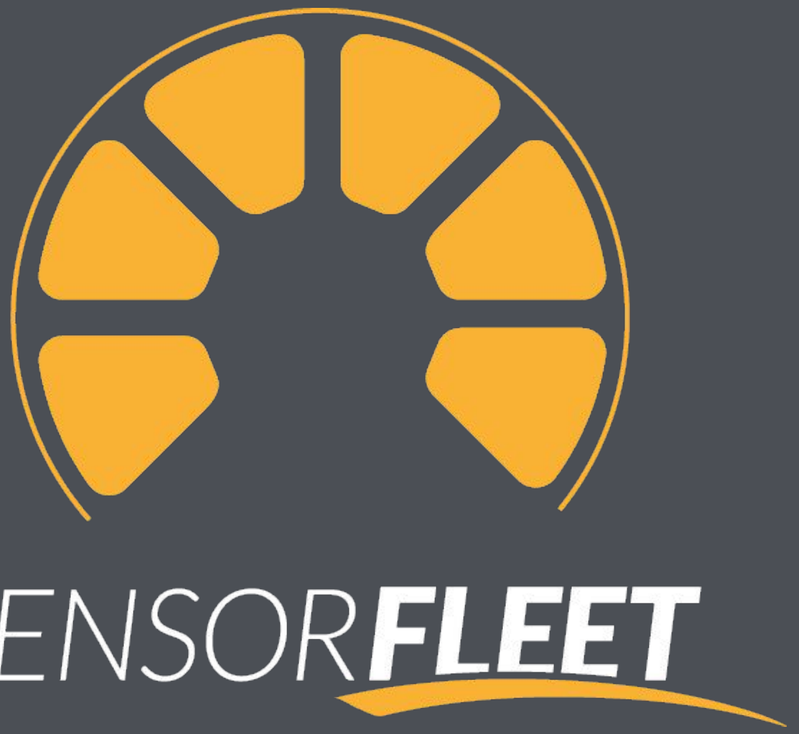


OPEN ARCHITECTURE FOR NETWORK SECURITY

NETWORK SECURITY IN 2023

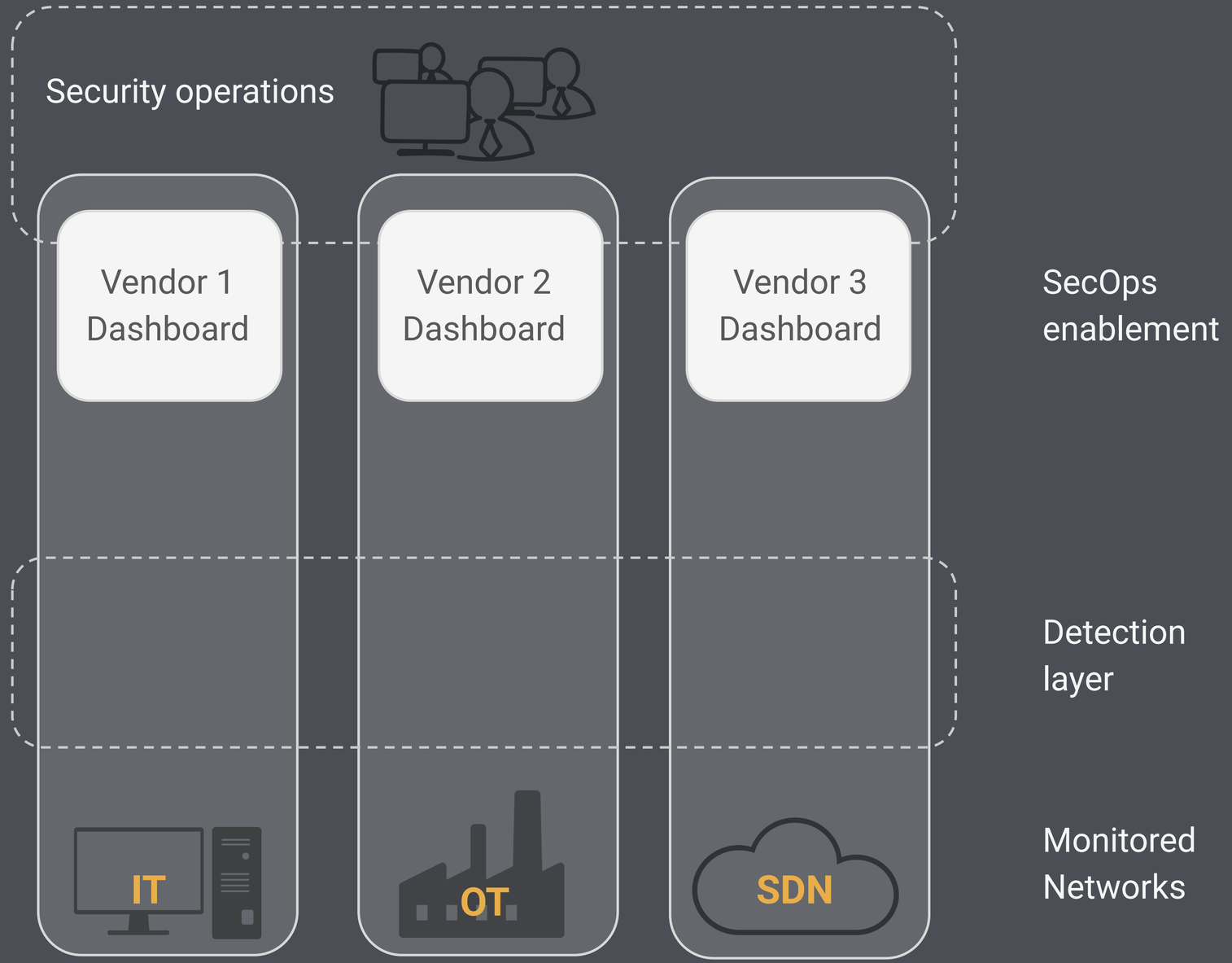
- The peak of Gartner hype cycle concentrates on other topics, but
  - Central technical requirement in ISO27001 and IEC62443

- Cloud and applications as service change the role in IT
  - Still remains relevant to inhouse datacenters and SDN

- Connected OT/IoT increases the need
  - IT - OT convergence opens up new attack vectors

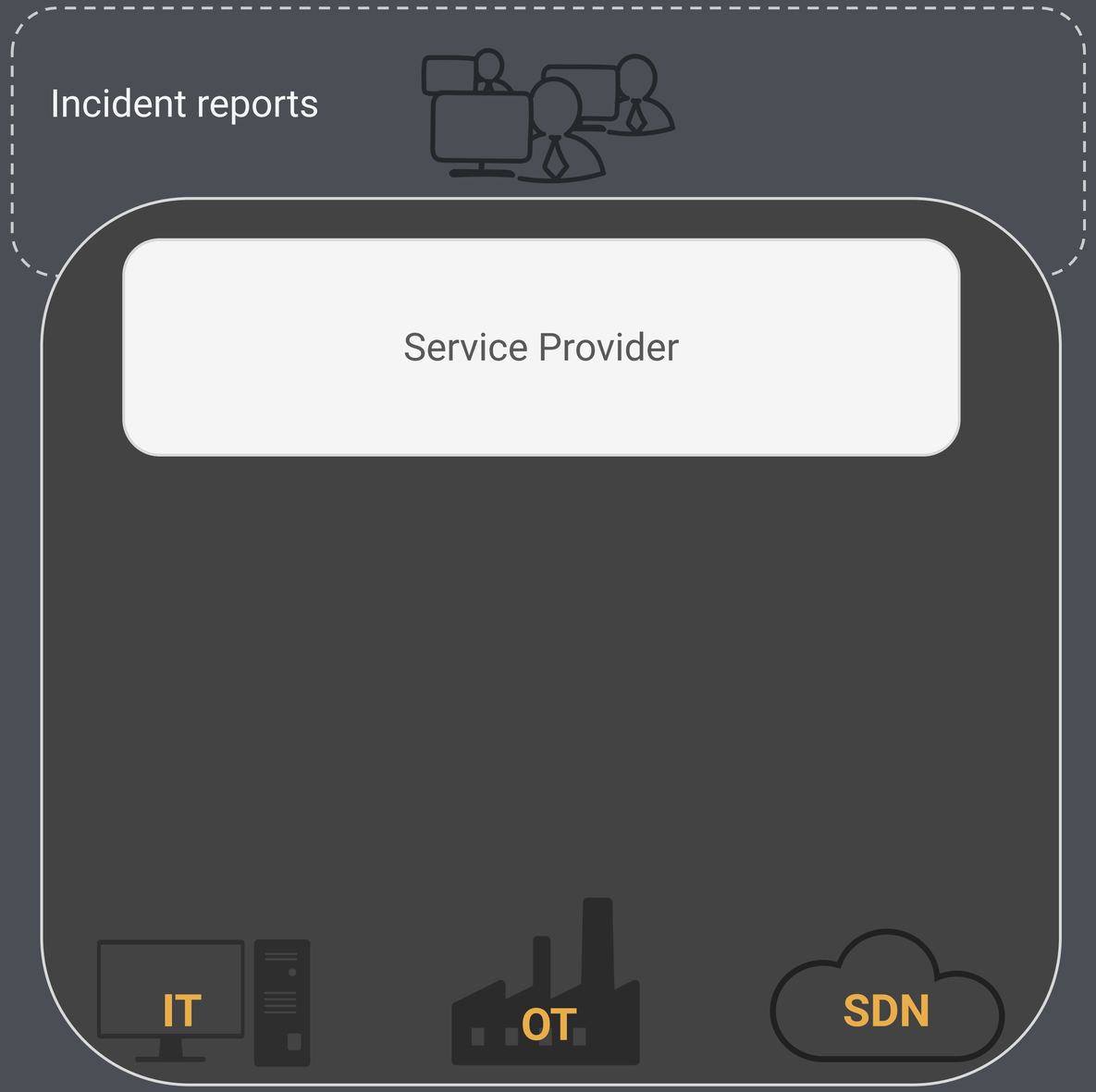
WHAT WE HAVE TODAY - INHOUSE SECURITY OPERATIONS

- **Collection of vendor specific silos**
  - End-user has full control and visibility
  - Undefined relationship between vendor solutions
  - Changes are costly



WHAT WE HAVE TODAY - SECURITY AS A SERVICE

- **Turnkey service**
  - Operationally easy and cost effective
  - Detection coverage controlled by service provider - often log based
  - Change of a service provider can be a major project



THE NEW WAY - OPEN NETWORK SECURITY STACK

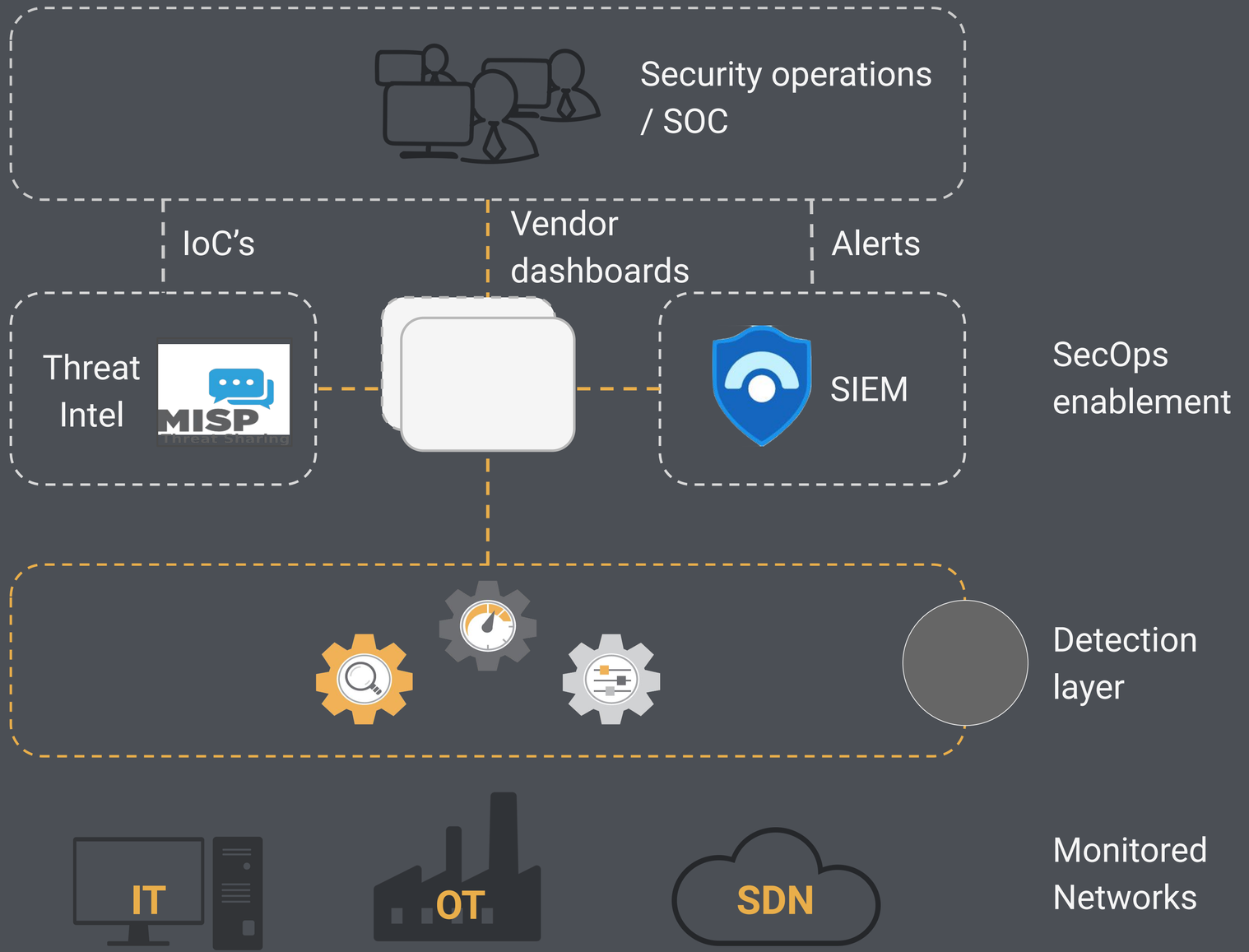
- End-user controls solutions and coverage based on their priorities and risk assessment
  - Service provider can be used for day to day monitoring
- Avoid solution fragmentation
  - Different sites can have different capabilities
  - Yet, run on organisation wide platform and orchestration
- Low cost of changes
  - Plug’n’play from operational perspective
  - Loose vendor lock

By 2024, organizations adopting a cybersecurity mesh architecture will reduce the financial impact of security incidents by an average of 90%.

Top Technology Trends for 2022: Cybersecurity Mesh, Gartner

OPEN NETWORK SECURITY STACK - EXAMPLE

- **Detection layer**
  - Unified network level detection
  - Any solution supporting virtual appliances or containers
- **SecOps enablement**
  - Industry standard solutions as primary Dashboards/workflows
  - Vendor Dashboards as supplementary tools
- **Maximum flexibility**
  - Plug’n’play any solution or service provider anytime



(MISP & Sentinel as examples only*

MAJOR DEVELOPMENT PROJECT?

- Not really
  - For example, solution for a large industrial customer with 10+ global manufacturing sites deployed and operational in less than two weeks
  - Network security solutions from 3 vendors, including SensorFleet

- OSS angle - Several powerful OSS security solutions exist
  - Scalable adoption and maintenance remains a challenge
  - Open network security architecture solves this

- Data privacy
  - End user has the control on sharing and storing of detection data

THANK YOU!

QUESTIONS?