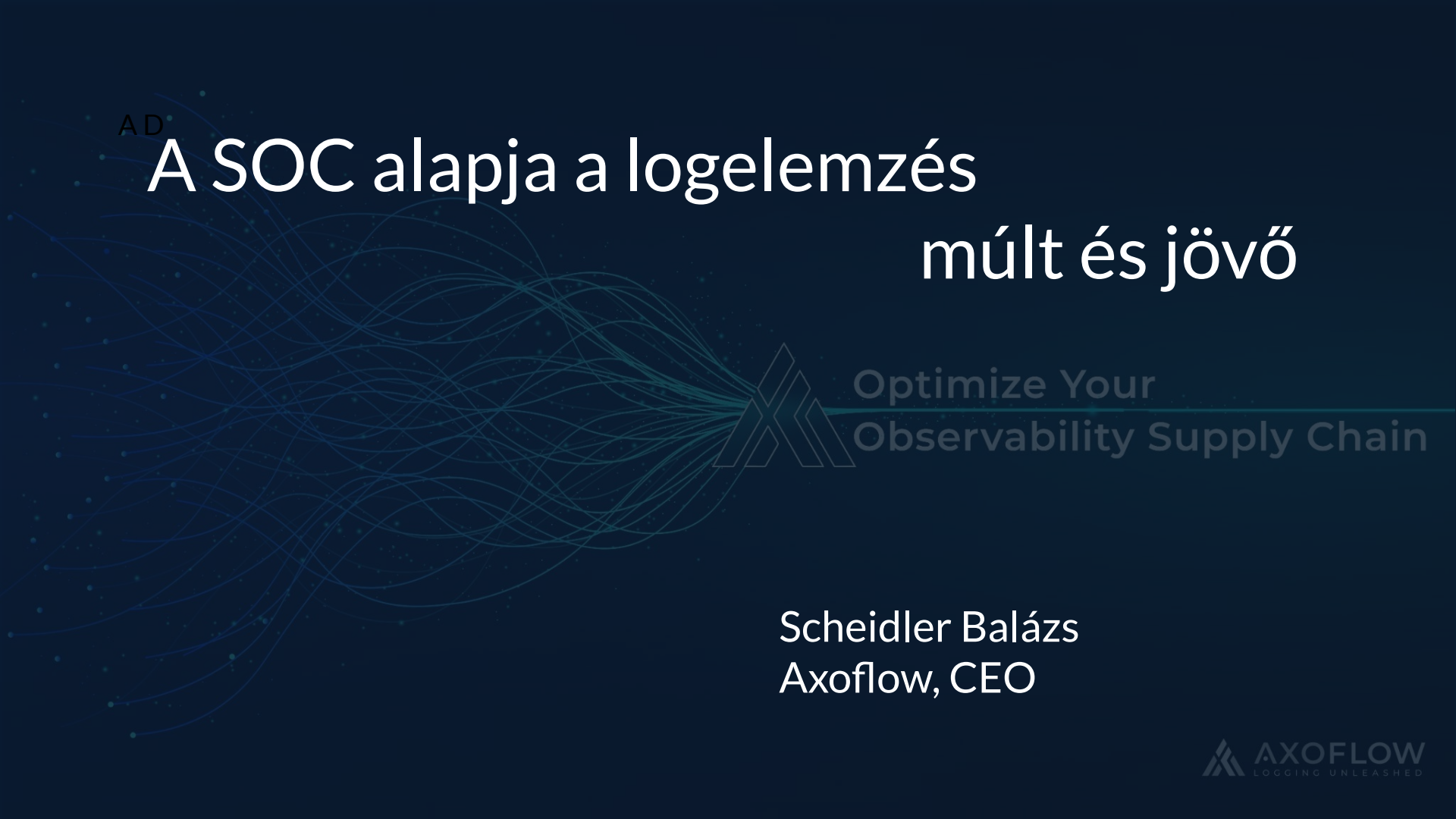
AD

# A SOC alapja a logelemzés múlt és jövő




Scheidler Balázs
Axoflow, CEO

AXOFLOW
LOGGING UNLEASHED

# Business Data vs. Machine Data

Business Data: a vállalat értékteremtéséhez közvetlenül kapcsolódó adatok

Machine Data: az infrastruktúra által generált adatok

- Triviálisan nem köthetők az üzleti adathoz
- Az infrastruktúra/alkalmazások belső eseményeit  írják le, példák
  - valaki bejelentkezett (login),
  - az endpoint securty eszköz talált egy malware-t,
  - a tűzfal elutasított egy kapcsolatot,
  - Stb

A Machine Data tipikus megjelenése a log

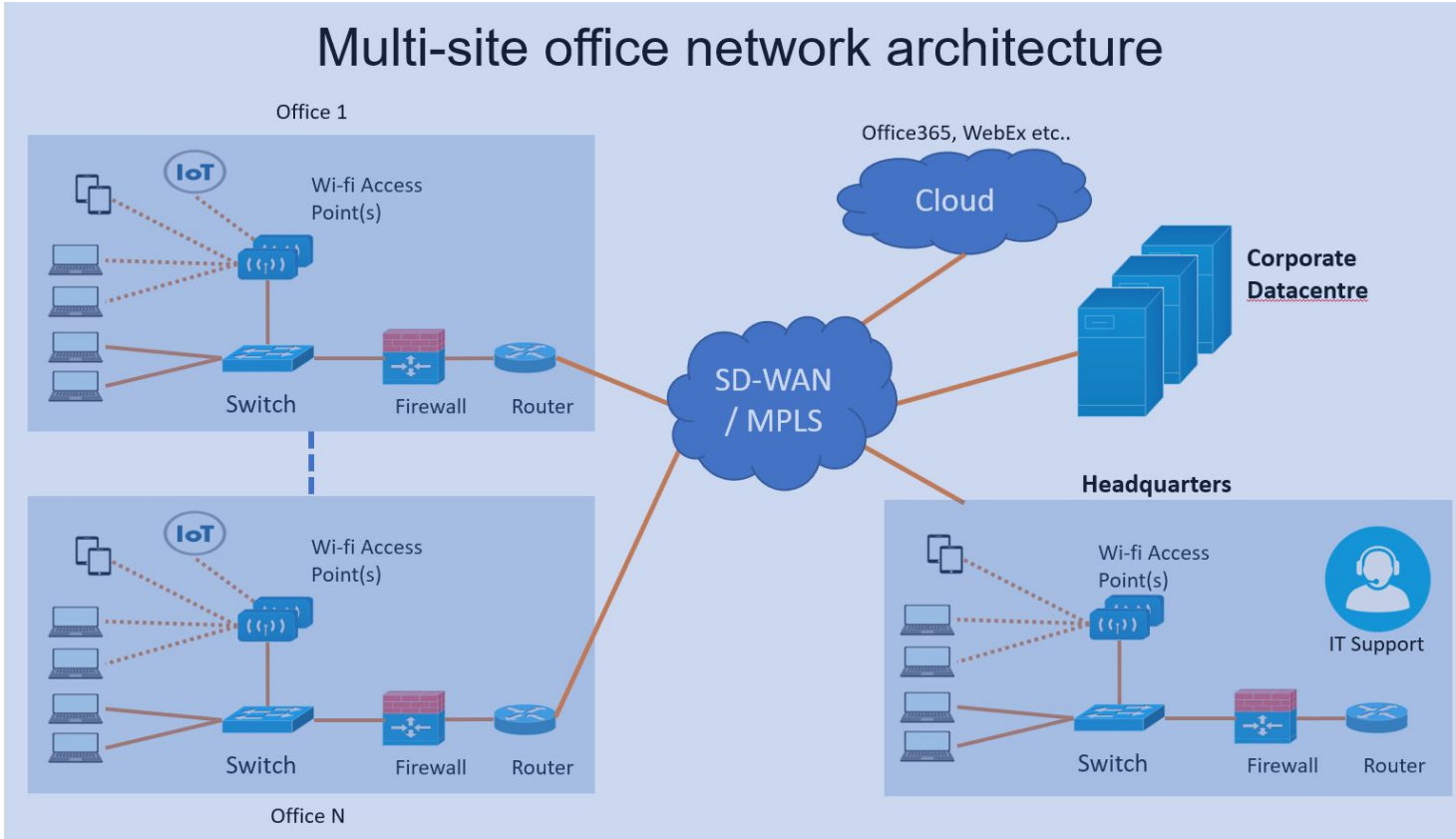
- Időpecsét + az esemény leírása,
- Az esemény általában egy emberi fogyasztásra szánt szöveg.
- Előfordulnak struktúráltabb események is, de ezek sémája alkalmazás/gyártó és verzió függő.

# SOC - hol kezdődött?

Központban a Machine Data elemzése

- Cél: a machine data alapján incidensek azonosítása, hogy aztán azokat vállalati szinten kezelni tudjuk.
- Machine Data gyűjtése:
  - Fő fókusz:
    - Biztonsági eszközök (identity & access management, firewalls, endpoint, IDS/IPS/NDR, stb)
    - Operációs rendszerek, hálózati eszközök
  - Másodlagos fókusz: alkalmazások saját naplói
- Tipikus eszközök:
  - Log management (pl: syslog-ng, rsyslog, graylog, fluentd, logstash, …)
  - SIEM
  - Incident workflow

# SOC helye a vállalatban



# Trendek

Volumen: +25% YoY

Cloud Service Provider (AWS, GCP, Azure):

- IaaS még integrálható (someone else's computer)
- PaaS szolgáltatások esetén a low level rendszernaplók már nem érhetők el (helyette CloudTrail pl) még akkor sem ha a CSP egyébként egy ismert komponenst használ (managed databases, managed queues, stb)

Cloud Native Engineering practices

- Mikroszervíz architektúrák, automatikusan skálázott  elasztikus workloadok
- Kubernetes, Docker
- DevOps

Software as a Service

- Külső szolgáltató által üzemeltetett alkalmazások esetén a Machine Data teljesen más jellegű, ha egyáltalán elérhető (pl: Salesforce)

Adatforgalom:

- Az adatforgalom cloud régiók között vagy on-premise/cloud között elképesztő drága!
- A legtöbb cloud előtt indult nagyvállalat hibrid módon működik és még fog is…

# SOC kihívások

A trendekre még nem született megfelelő válasz:

- A SOC a mennyiséggel küzd, inkább kidobni akarunk adatokat, mint valójában kezelni és feldolgozni azokat.
- A cloud native alkalmazások (akár publikus cloudban, akár on-premise) gyakran teljesen külön életet élnek, az itt keletkező machine data nem jut el a SOC-ig
  - Cloud native apps -> DevOps, DevSecOps által kezelve
  - Gyakran két teljesen független szervezet részeként operálnak mindenféle együttműködés nélkül.
  - Correlation-re esély sincs, valójában a DevSecOps belső működésén múlik hogy milyen incidenseket azonosítanak.
  - A kontrollok kimerülnek a szabályozások szintjén.

Ez a helyzet veszélyezteti a SOC incidens felderítési képességeit!

# Megoldási stratégiák

Vizsgáljuk felül a Machine Data gyűjtésével kapcsolatos infrastruktúrát, aminek egyformán jól kell kezelnie:

- Lehetőséget ad a költségek és mennyiségek csökkentésére azáltal hogy a megfelelő adat a megfelelő helyre kerül és csak oda.
- On-premises, cloud native (kubernetes) és cloud szolgáltatások bekapcsolása a SOC adatgyűjtésébe
- Lehetővé teszi az adatcserét és a kollaborációt a security és a DevOps csapatok között, és nem csak a szabályozás szintjén
- Képes skálázódni a vállalati szintű adat mennyiségekre


AXOFLOW
LOGGING UNLEASHED