# L’importanza dei Big Data nella cybersecurity

come monitorare la propria infrastruttura con sistemi intelligentii

# DATA BEERS ROMA #01

**DATA:** WPP CAMPUS

**LUOGO:** VENERDÌ 17 FEBBRAIO

ROMA DATA BEERS

Sponsor Ufficiali

+WUNDERMAN THOMPSON

ESTRELLA DAMM BARCELONA 1876

# WHO I AM

- Mario Cuomo
- cloud solution architect
- 25 years old
- waiting for Master degree in Computer Science – Roma Tre University
- enthusiast for algorithms, crittography

# AGENDA

# AGENDA

- BIG DATA OVERVIEW

# AGENDA

- BIG DATA OVERVIEW
- MAIN TREND IN CYBERATTACK

# AGENDA

- BIG DATA OVERVIEW
- MAIN TREND IN CYBERATTACK
- SENTINEL

# AGENDA

- BIG DATA OVERVIEW
- MAIN TREND IN CYBERATTACK
- SENTINEL
  - AS SIEM

# AGENDA

- BIG DATA OVERVIEW
- MAIN TREND IN CYBERATTACK
- SENTINEL
  - AS SIEM
  - AS SOAR

# BIG DATA OVERVIEW

# BIG DATA OVERVIEW

- VOLUME

# BIG DATA OVERVIEW

- VOLUME
  - huge amount of data, sometimes with big size

# BIG DATA OVERVIEW

- VOLUME
  - huge amount of data, sometimes with big size
- VELOCITY

# BIG DATA OVERVIEW

- VOLUME
  - huge amount of data, sometimes with big size
- VELOCITY
  - several frequency: batch, near and real time

# BIG DATA OVERVIEW

- VOLUME
  - huge amount of data, sometimes with big size
- VELOCITY
  - several frequency: batch, near and real time
- VARIETY

# BIG DATA OVERVIEW

- VOLUME
  - huge amount of data, sometimes with big size
- VELOCITY
  - several frequency: batch, near and real time
- VARIETY
  - structured and unstructured

# BIG DATA OVERVIEW

- VOLUME
  - huge amount of data, sometimes with big size
- VELOCITY
  - several frequency: batch, near and real time
- VARIETY
  - structured and unstructured
- VERACITY

# BIG DATA OVERVIEW

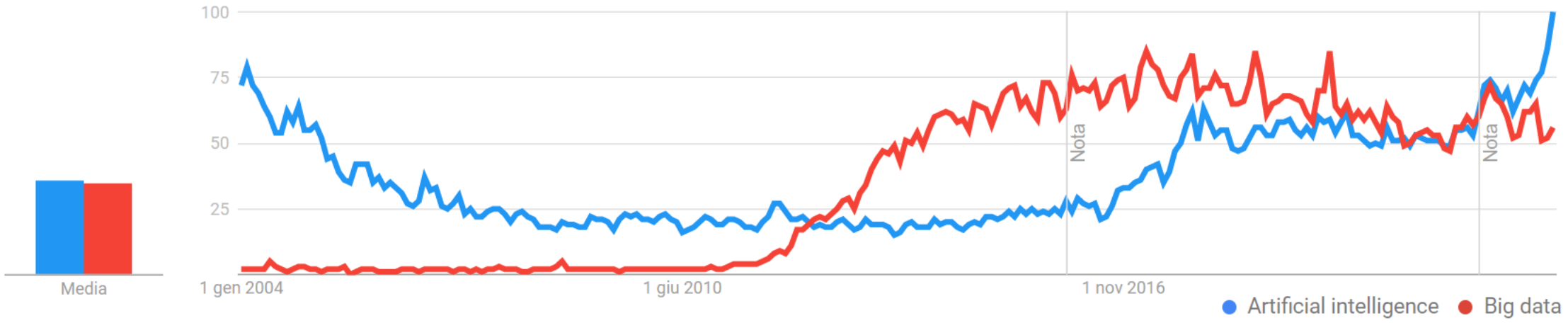
- VOLUME
  - huge amount of data, sometimes with big size
- VELOCITY
  - several frequency: batch, near and real time
- VARIETY
  - structured and unstructured
- VERACITY
  - unprocessed data, maybe with no accuracy

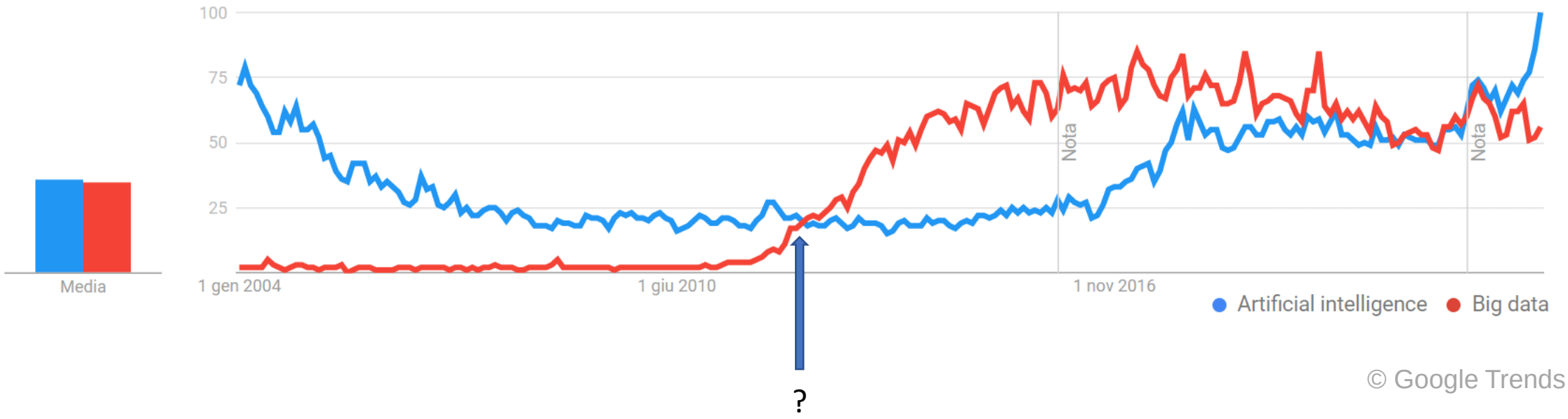
# BIG DATA OVERVIEW

- VOLUME
  - huge amount of data, sometimes with big size
- VELOCITY
  - several frequency: batch, near and real time
- VARIETY
  - structured and unstructured
- VERACITY
  - unprocessed data, maybe with no accuracy
- VALUE

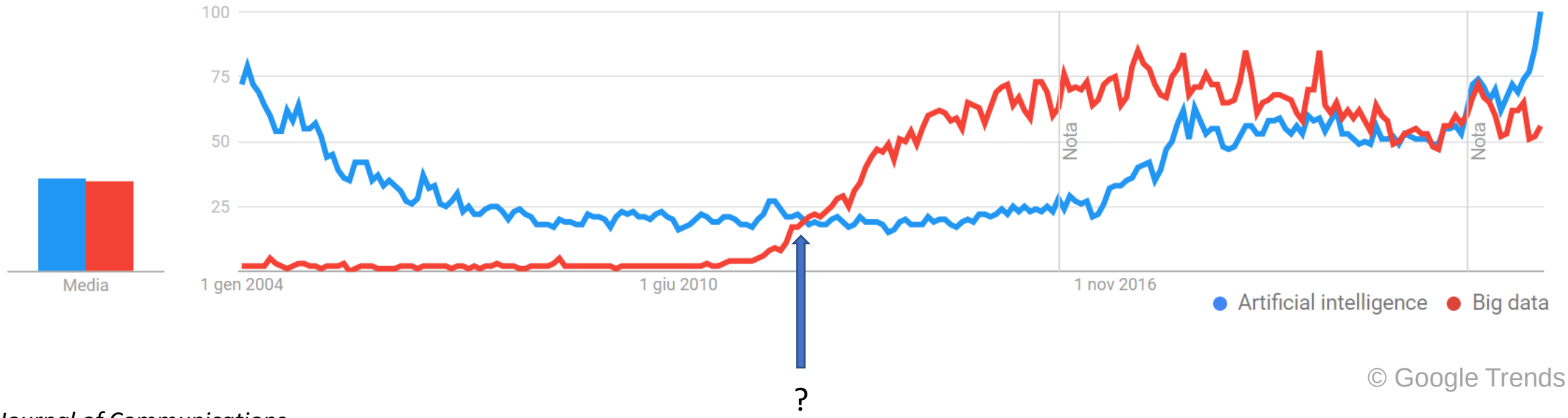
# BIG DATA OVERVIEW

- VOLUME
  - huge amount of data, sometimes with big size
- VELOCITY
  - several frequency: batch, near and real time
- VARIETY
  - structured and unstructured
- VERACITY
  - unprocessed data, maybe with no accuracy
- VALUE
  - insights gained




100
75
50
25
Media
1 gen 2004
1 giu 2010
1 nov 2016
Nota
Nota
Artificial intelligence
Big data
© Google Trends

?




?

- *Journal of Communications*
  *"approaching a thousand minutes of mediated content available for every minute available for consumption". (April 2012)*

- *Critical Questions for Big Data (Danah Boyd e Kate Crawford)*
  *"a cultural, technological, and scholarly phenomenon that rests on the interplay of: technology, analysis and mythology. (May 2012)*

- *Big Data Research and Development Initiative (March 2013)*

# MAIN TREND IN CYBERATTACK

# MAIN TREND IN CYBERATTACK

© IBM report data breach 2022

# MAIN TREND IN CYBERATTACK

© IBM report data breach 2022

- HEALTHCARE GETS HIT HARD

# MAIN TREND IN CYBERATTACK

© IBM report data breach 2022

- HEALTHCARE GETS HIT HARD
  - up 42% since 2020

# MAIN TREND IN CYBERATTACK

© IBM report data breach 2022

- HEALTHCARE GETS HIT HARD
  - up 42% since 2020
  - $ 10.10M

# MAIN TREND IN CYBERATTACK

© IBM report data breach 2022

- HEALTHCARE GETS HIT HARD
  - up 42% since 2020
  - $ 10.10M
- STOLEN OR COMPROMISED CREDENTIALS

# MAIN TREND IN CYBERATTACK

© IBM report data breach 2022

- HEALTHCARE GETS HIT HARD
  - up 42% since 2020
  - $ 10.10M
- STOLEN OR COMPROMISED CREDENTIALS
  - phishing $ 4.91M

# MAIN TREND IN CYBERATTACK

© IBM report data breach 2022

- HEALTHCARE GETS HIT HARD
  - up 42% since 2020
  - $ 10.10M
- STOLEN OR COMPROMISED CREDENTIALS
  - phishing $ 4.91M
  - business email compromised $ 4.89M

# MAIN TREND IN CYBERATTACK

© IBM report data breach 2022

- HEALTHCARE GETS HIT HARD
  - up 42% since 2020
  - $ 10.10M
- STOLEN OR COMPROMISED CREDENTIALS
  - phishing $ 4.91M
  - business email compromised $ 4.89M
  - vulnerability in third-party software $ 4.55M

# MAIN TREND IN CYBERATTACK

© IBM report data breach 2022

- HEALTHCARE GETS HIT HARD
  - up 42% since 2020
  - $ 10.10M
- STOLEN OR COMPROMISED CREDENTIALS
  - phishing $ 4.91M
  - business email compromised $ 4.89M
  - vulnerability in third-party software $ 4.55M
- LIFECYCLE

# MAIN TREND IN CYBERATTACK

© IBM report data breach 2022

- HEALTHCARE GETS HIT HARD
  - up 42% since 2020
  - $ 10.10M
- STOLEN OR COMPROMISED CREDENTIALS
  - phishing $ 4.91M
  - business email compromised $ 4.89M
  - vulnerability in third-party software $ 4.55M
- LIFECYCLE
  - it took an average of 277 days—about 9 months—to identify a breach!!

# MAIN TREND IN CYBERATTACK

© IBM report data breach 2022

- HEALTHCARE GETS HIT HARD
  - up 42% since 2020
  - $ 10.10M
- STOLEN OR COMPROMISED CREDENTIALS
  - phishing $ 4.91M
  - business email compromised $ 4.89M
  - vulnerability in third-party software $ 4.55M
- LIFECYCLE
  - it took an average of 277 days—about 9 months—to identify a breach!!
- INCIDENT RESPONSE COST SAVING

# MAIN TREND IN CYBERATTACK

© IBM report data breach 2022

- HEALTHCARE GETS HIT HARD
  - up 42% since 2020
  - $ 10.10M
- STOLEN OR COMPROMISED CREDENTIALS
  - phishing $ 4.91M
  - business email compromised $ 4.89M
  - vulnerability in third-party software $ 4.55M
- LIFECYCLE
  - it took an average of 277 days—about 9 months—to identify a breach!!
- INCIDENT RESPONSE COST SAVING
  - $ 2.66M

# Traditional SOC Challenges

- Sophistication of threats
- High volume of noisy alerts
- IT deployment & maintenance
- Rising infrastructure costs and upfront investment
- Too many disconnected products
- Lack of automation
- Security skills in short supply

Security Operations Team

+

Artificial Intelligence

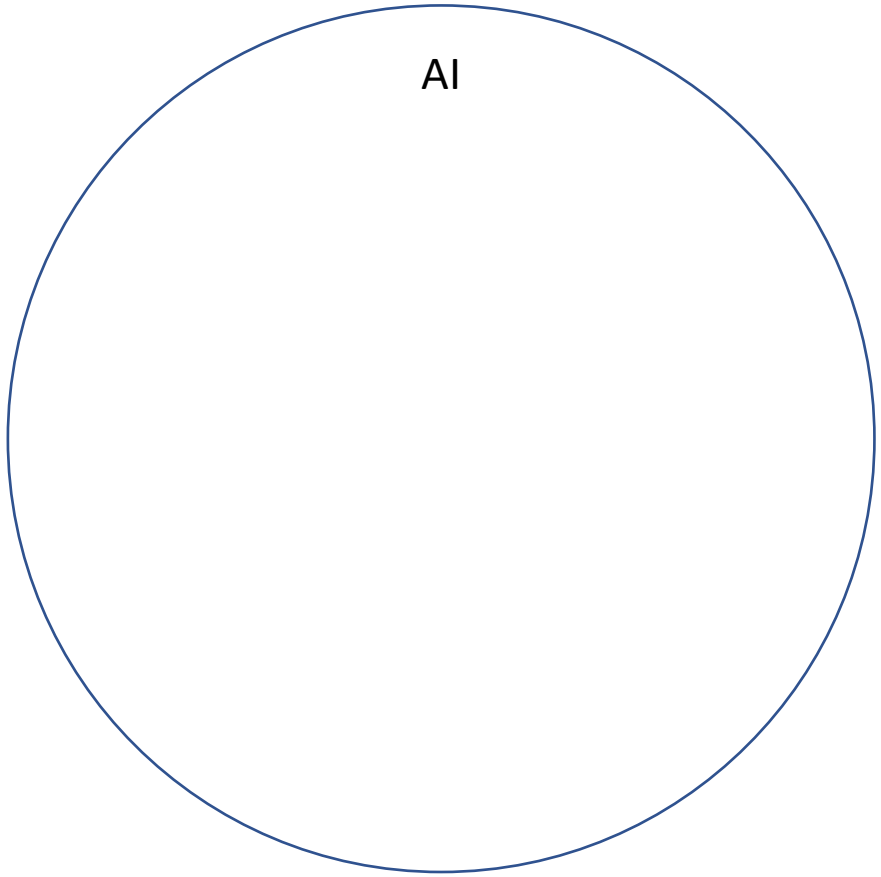
# ARTIFICIAL INTELLIGENCE

# ARTIFICIAL INTELLIGENCE

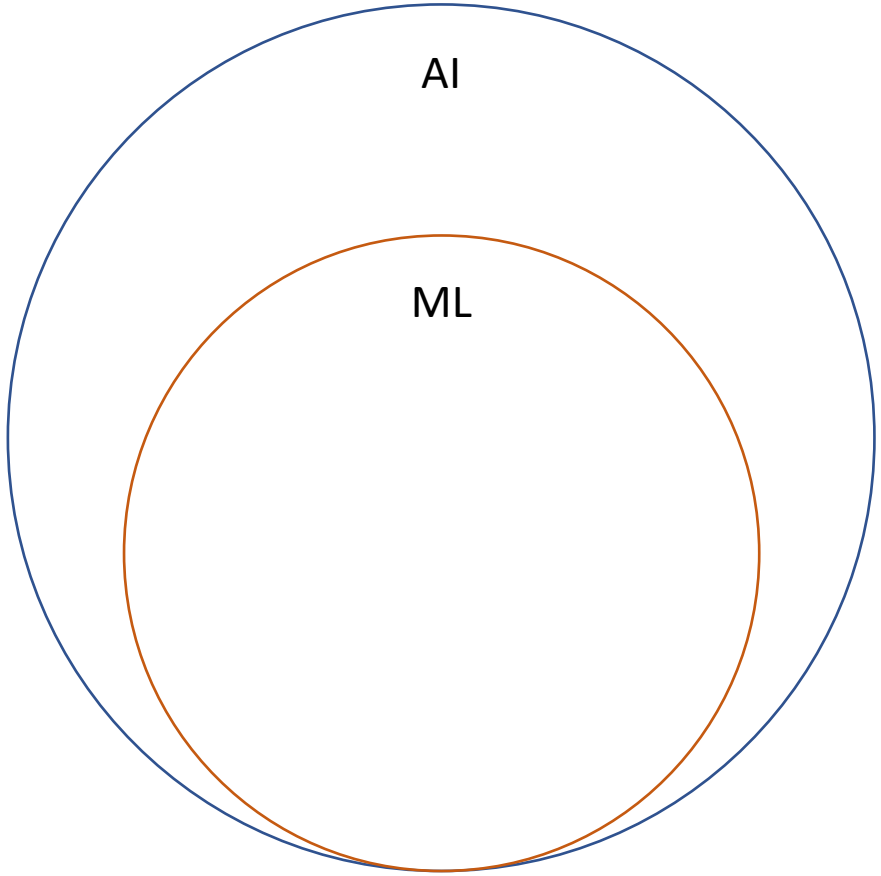
*Kurzweil e Raymond. The Age of Intelligent Machines. Cambridge 1990*

# ARTIFICIAL INTELLIGENCE

*Kurzweil e Raymond. The Age of Intelligent Machines. Cambridge 1990*

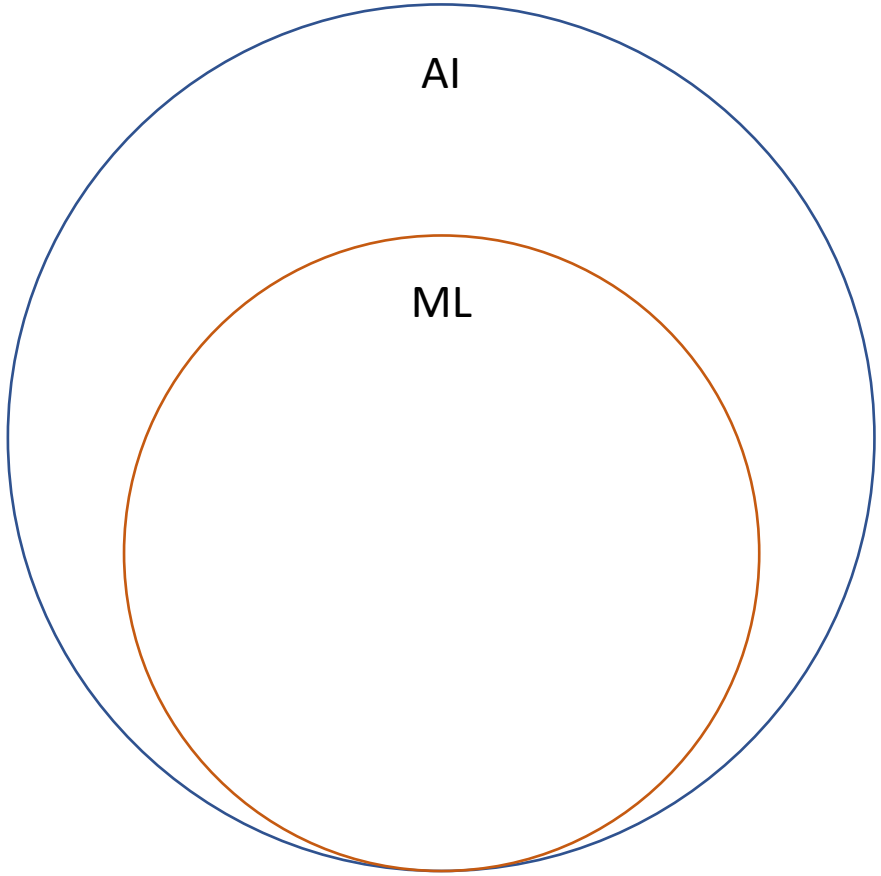


# ARTIFICIAL INTELLIGENCE



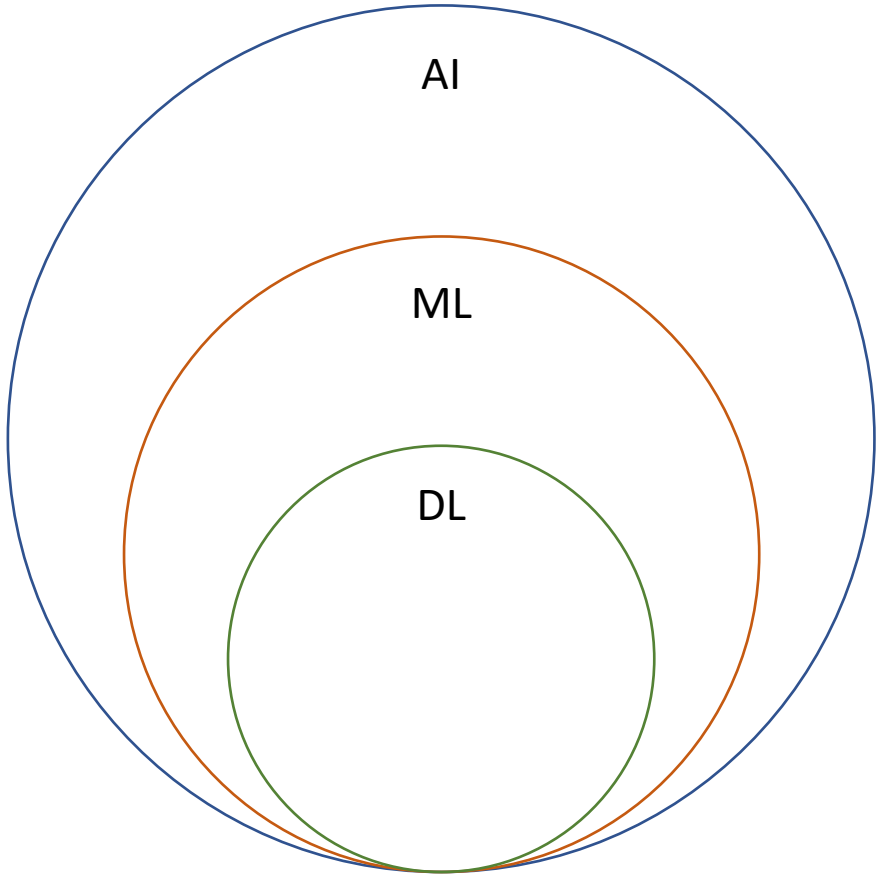
# ARTIFICIAL INTELLIGENCE

*Tom M Mitchell. Machine learning. Vol. 1. 9. McGraw-hill New York, 1997.*



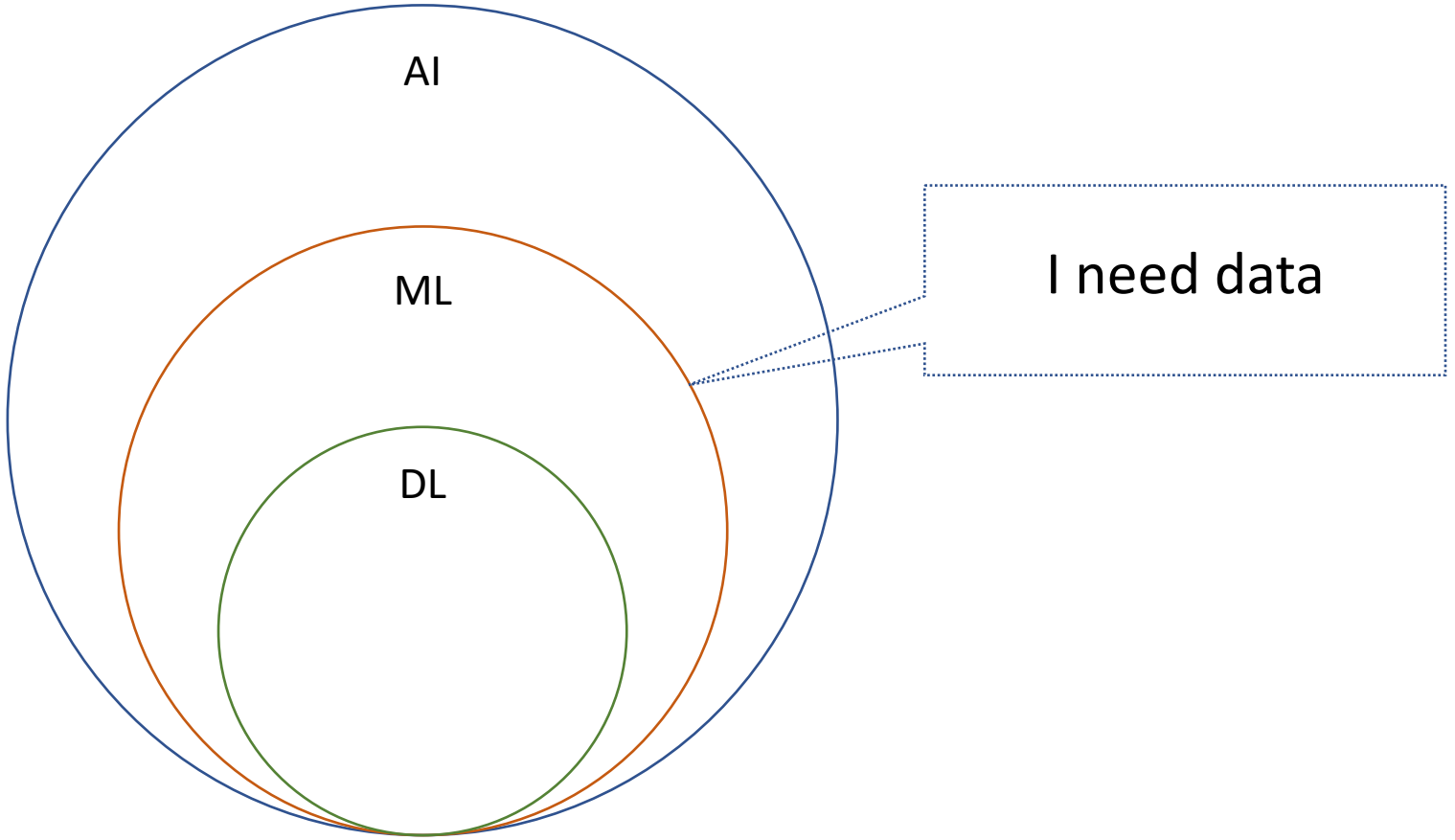
# ARTIFICIAL INTELLIGENCE

*Tom M Mitchell. Machine learning. Vol. 1. 9. McGraw-hill New York, 1997.*



# ARTIFICIAL INTELLIGENCE

*Tom M Mitchell. Machine learning. Vol. 1. 9. McGraw-hill New York, 1997.*



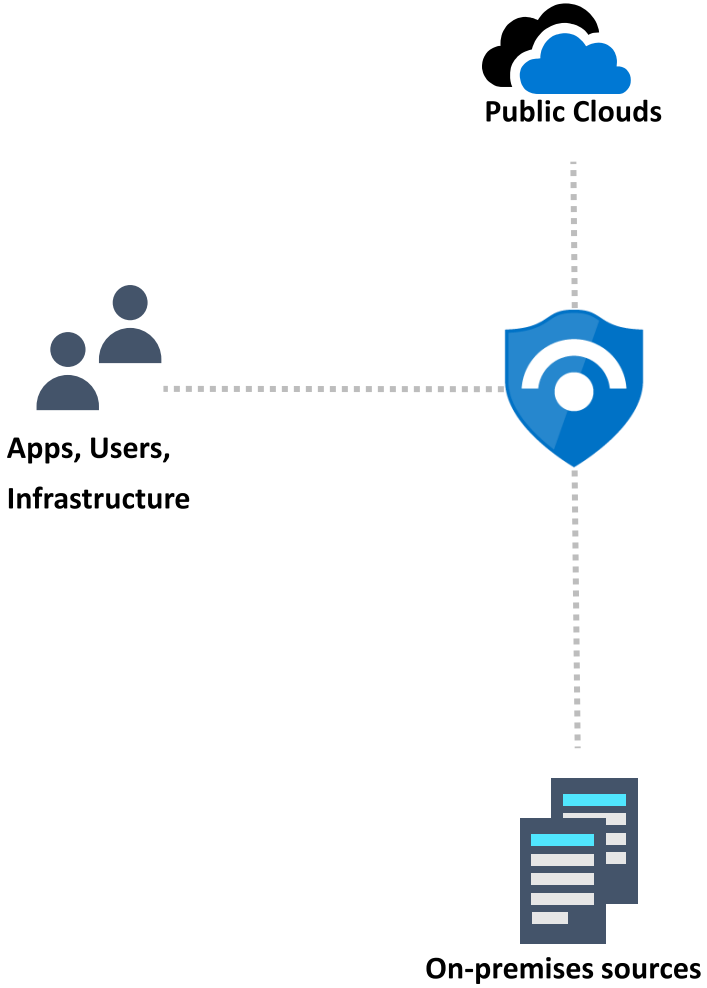
# BIG DATA AND CYBERSECURITY

# BIG DATA AND CYBERSECURITY

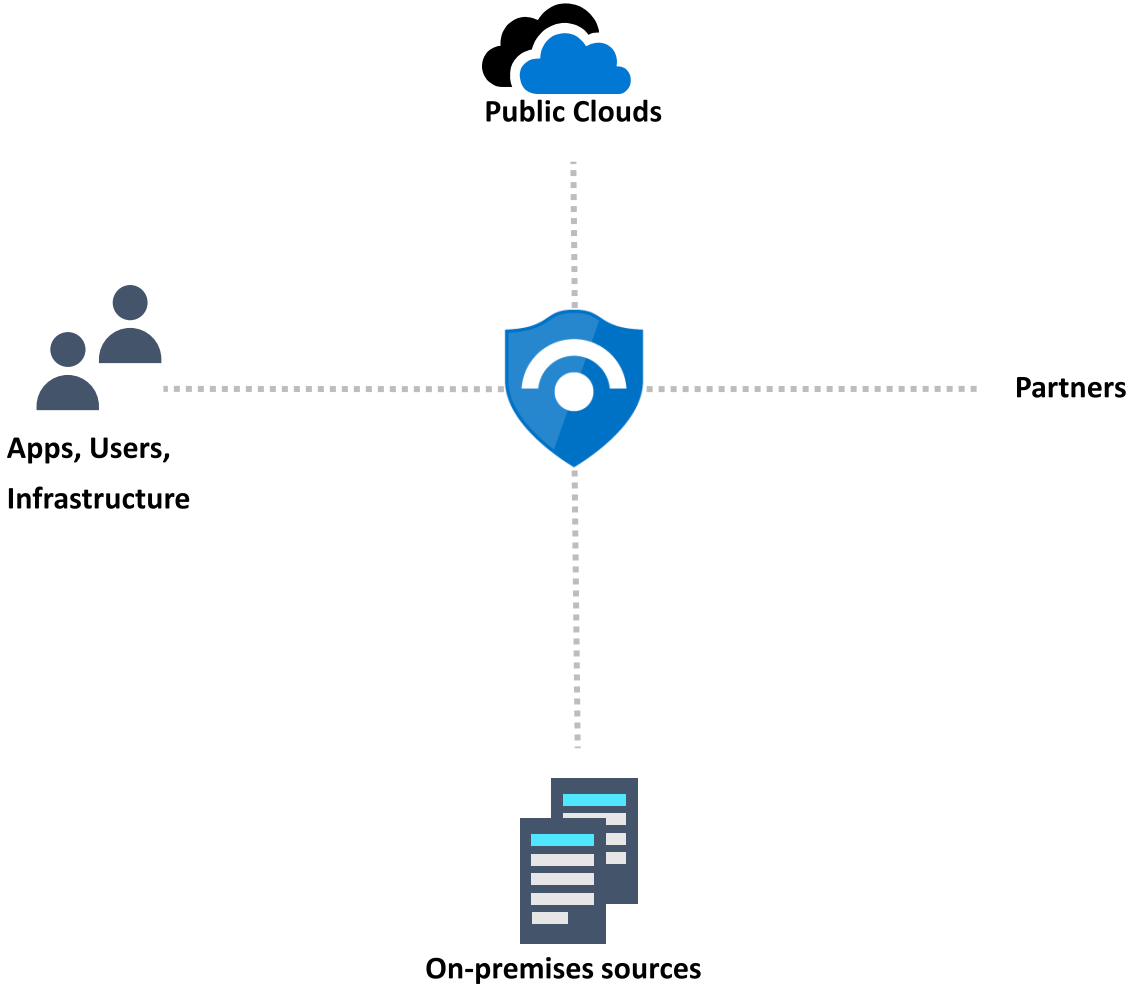
# BIG DATA AND CYBERSECURITY

# BIG DATA AND CYBERSECURITY

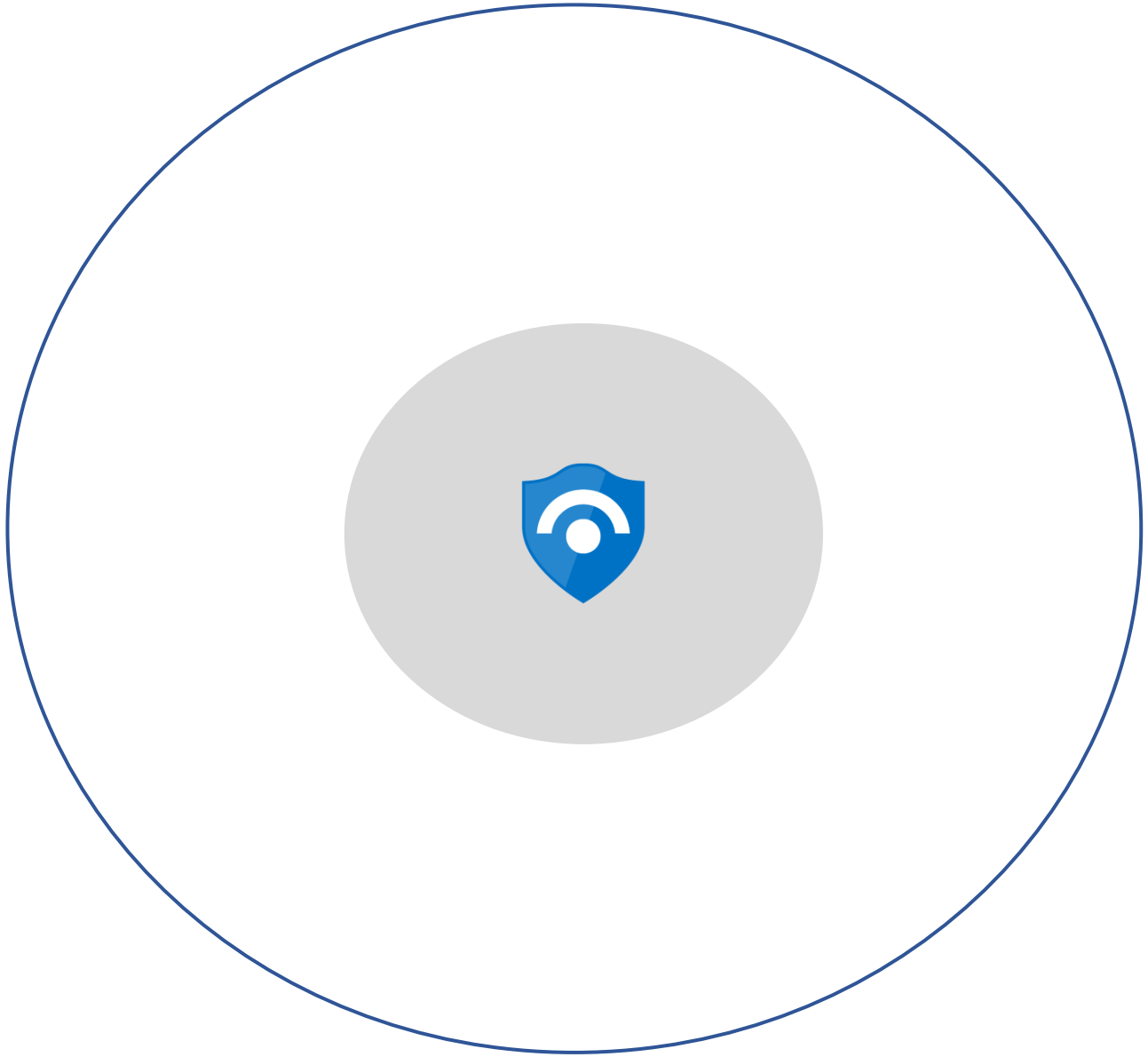
# BIG DATA AND CYBERSECURITY



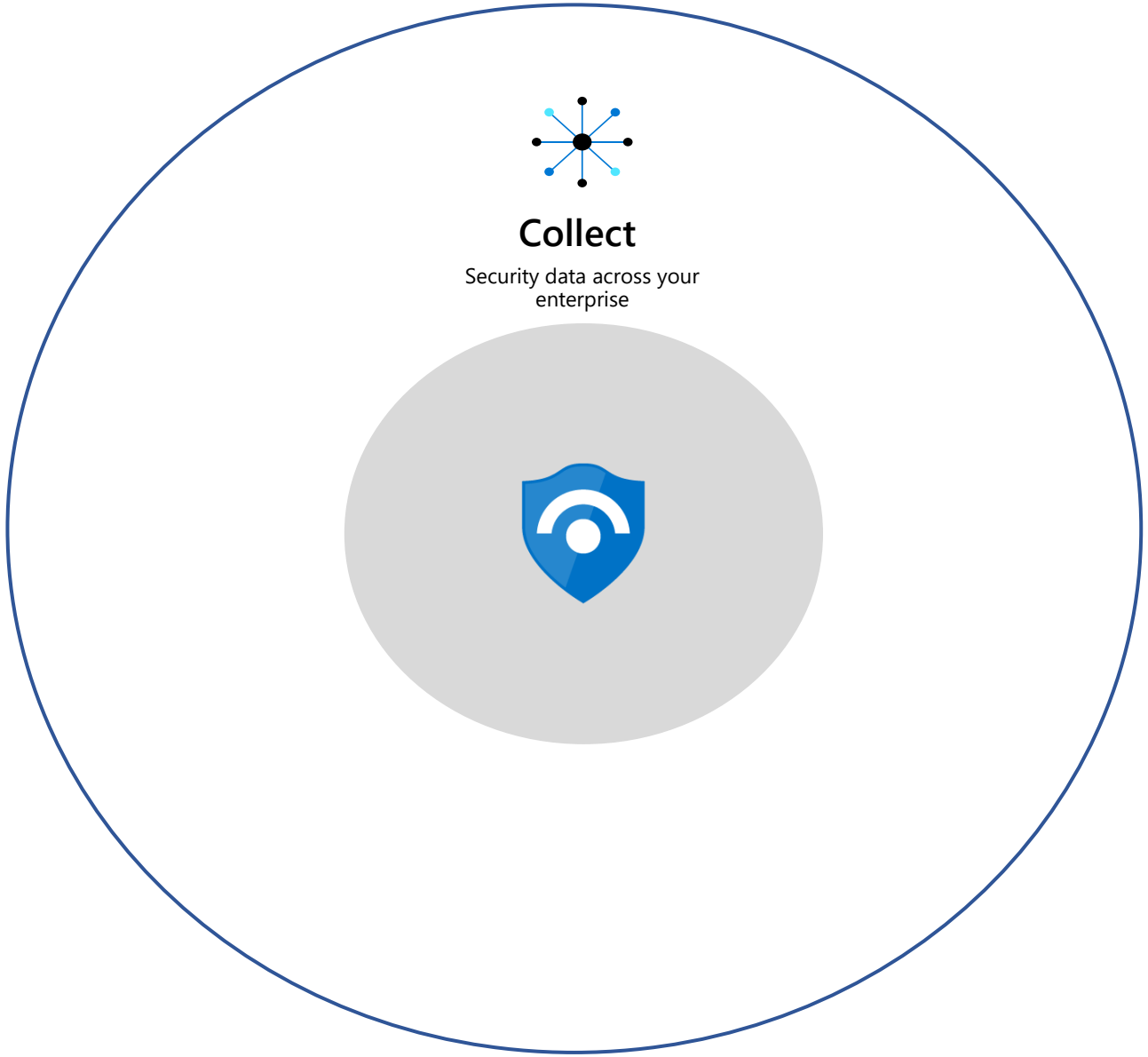
# BIG DATA AND CYBERSECURITY



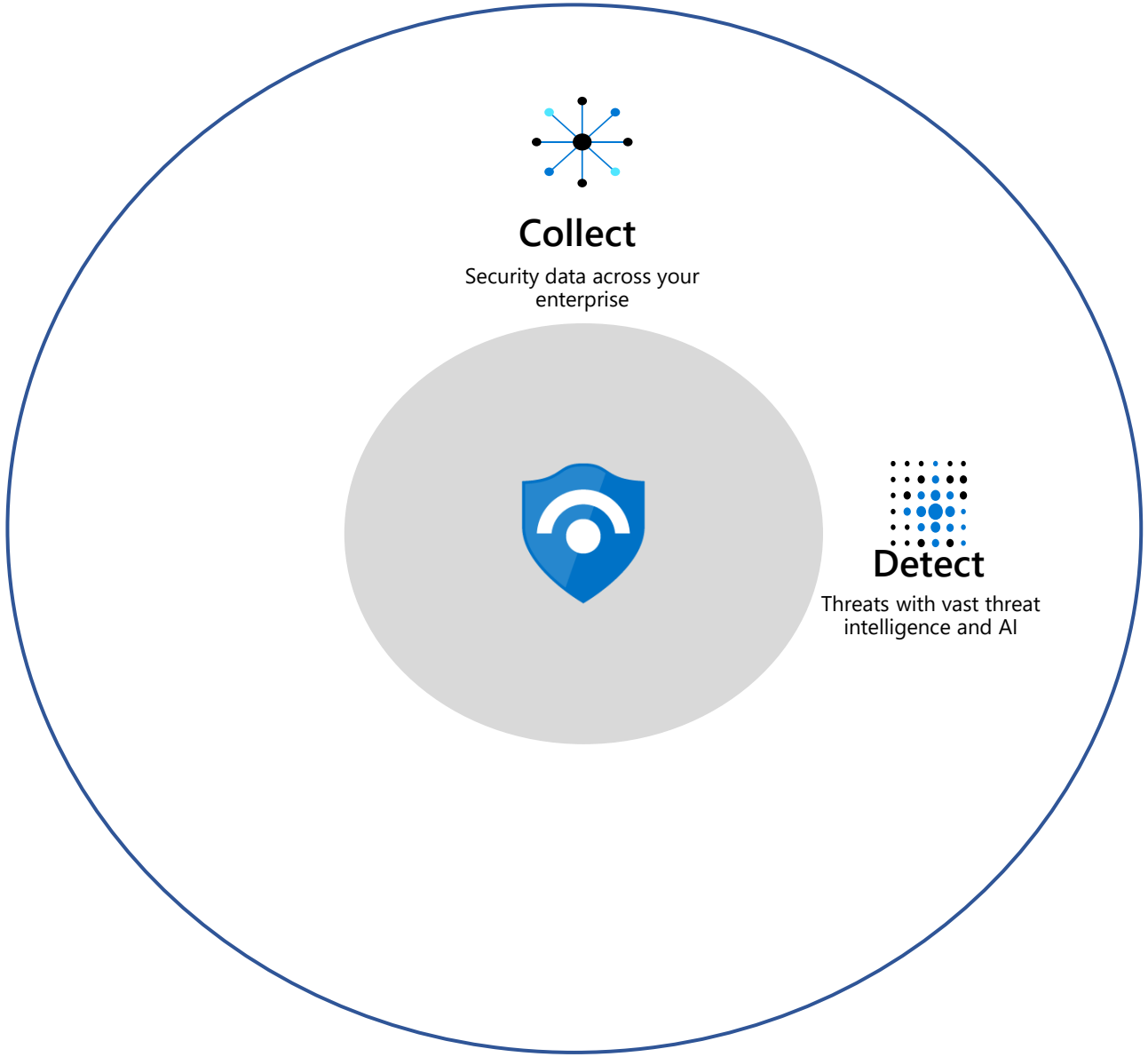
# SENTINEL



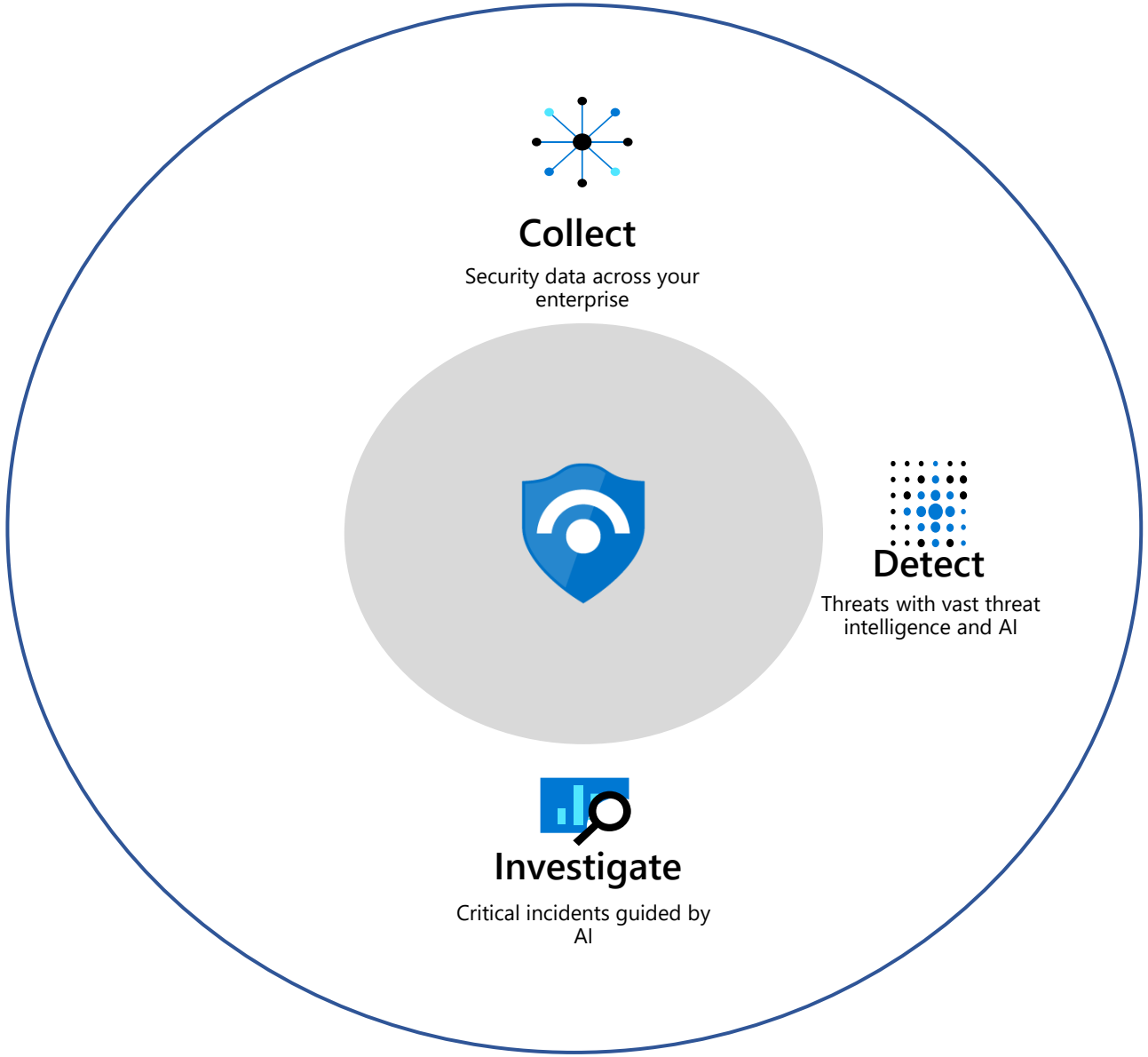
# SENTINEL



# SENTINEL


Collect
Security data across your enterprise
Detect
Threats with vast threat intelligence and AI

# SENTINEL


Collect
Security data across your enterprise
Detect
Threats with vast threat intelligence and AI
Investigate
Critical incidents guided by AI

# SENTINEL


Collect
Security data across your enterprise
Respond
Rapidly and automate protection
Detect
Threats with vast threat intelligence and AI
Investigate
Critical incidents guided by AI

# SENTINEL


SIEM - Security Information and Event Management

# SENTINEL


SOAR - Security Orchestration, Automation, and Response

SIEM - Security information and event management

# SOME EXAMPLE

- IBM Security QRadar SIEM
- McAfee Enterprise Security Manager
- Microsoft Sentinel
- SolarWinds Security Event Manager (SEM)

# QUESTIONS?

# THANK YOU!