NUCLEON
AHEAD OF CYBER THREATS

Leveraging Big Data for Enhanced Cybersecurity Resilience

Tech talks

EP: 05

About me

I am a Data Engineer @Nucleon Security


tahanouali


taha-nouali


taha.nouali@nucleon-security.com

01 Introduction

Introduction

Data is exploding at an unprecedented rate, reshaping every industry.

Introduction

Finance

Healthcare

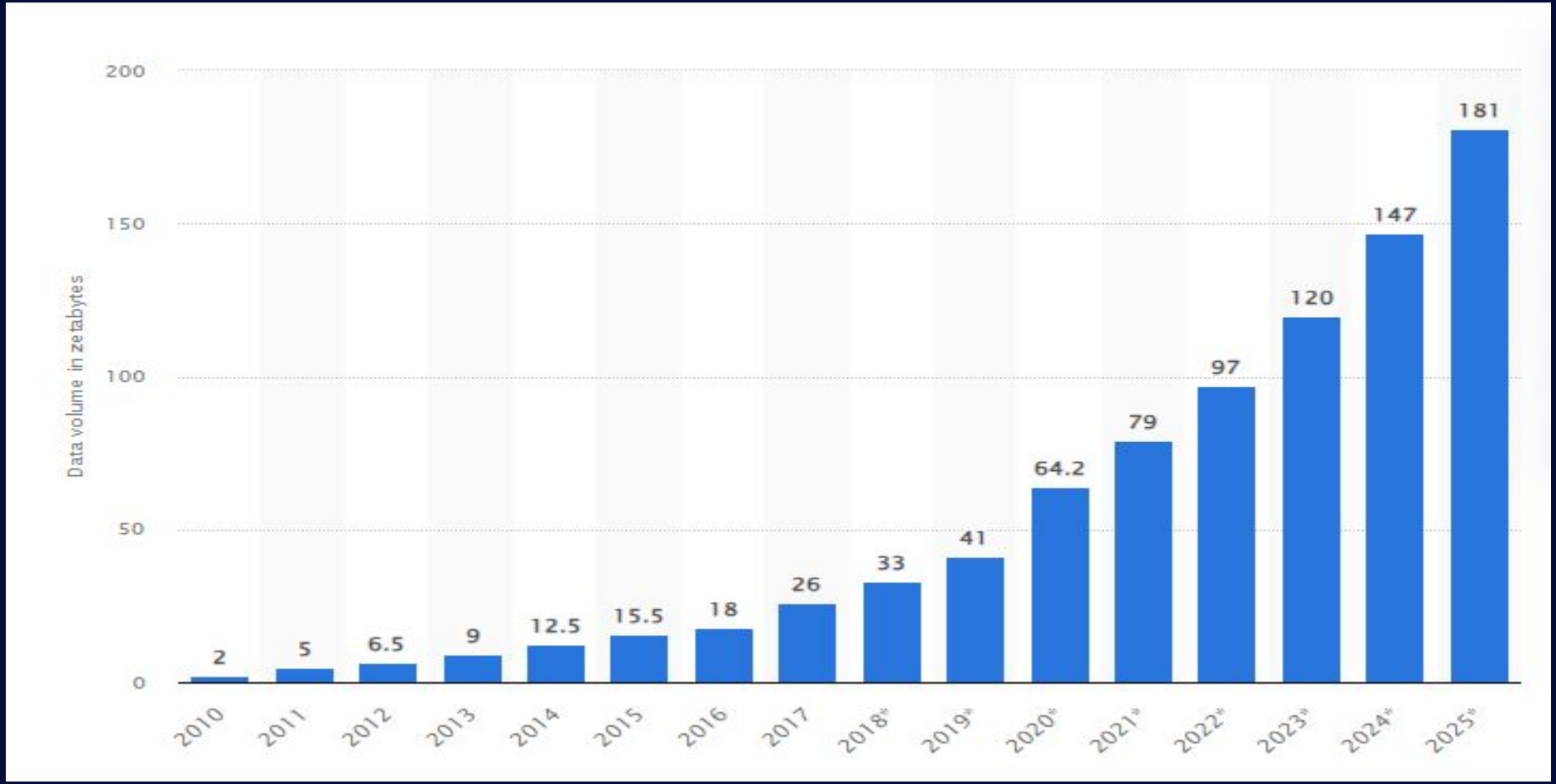
Retail

Introduction

Telecommunications

Cybersecurity

Introduction



1 ZetaB = 1 Billion TB

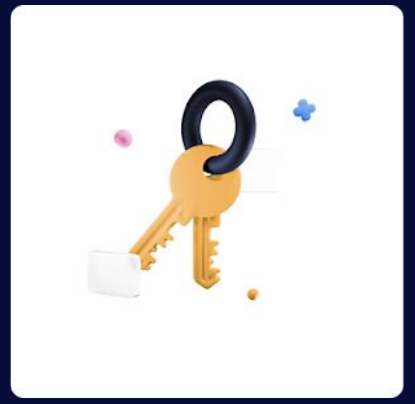
The attack surface got wider implicating more attacks





Countless cybersecurity systems generate **massive** streams of **logs every second**




This is what we call Big Data

02
Big Data Fundamentals

What is Big Data

Big Data refers to vast and complex datasets that exceed the capabilities of traditional data processing. It enables organizations to analyze large amounts of information, providing valuable insights and real-time threat detection.

Big Data 3 Vs

Defining properties or dimensions of big data

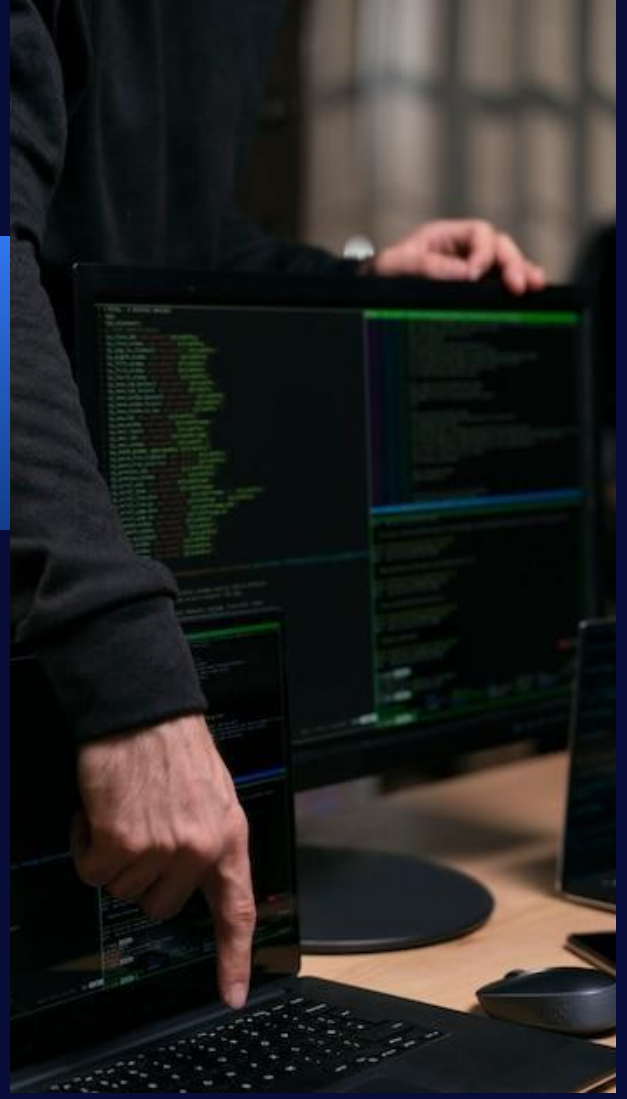
01 Volume

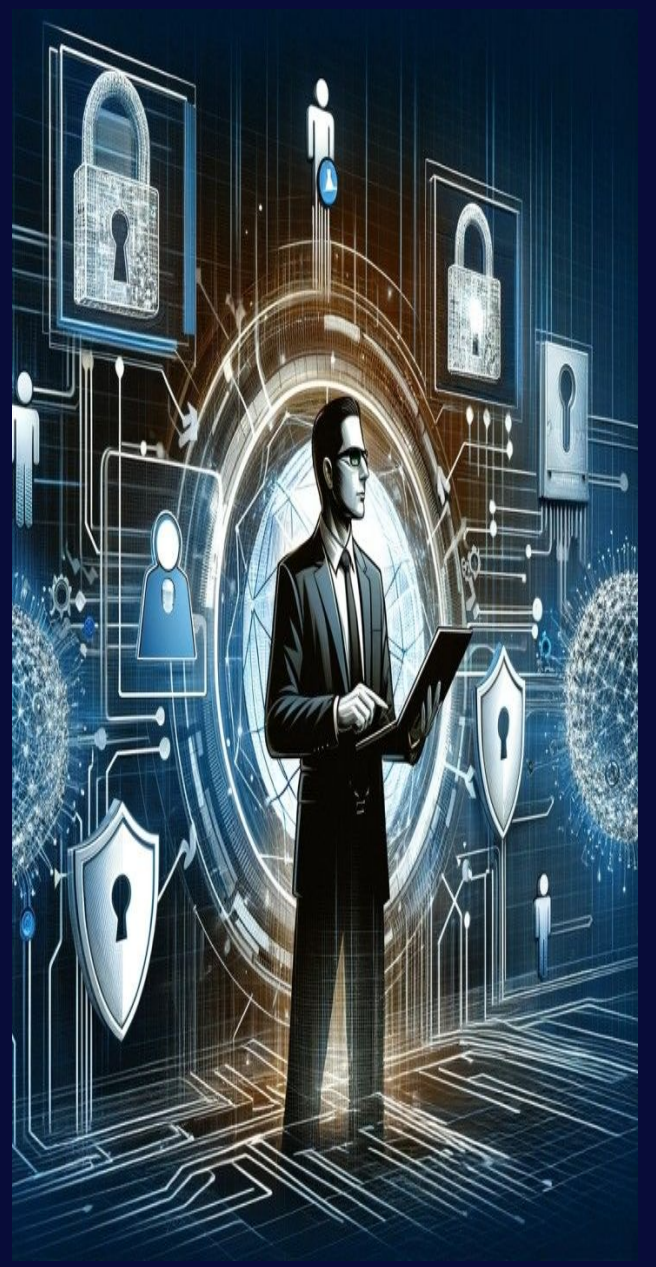
02 Velocity

03 Variety

Volume

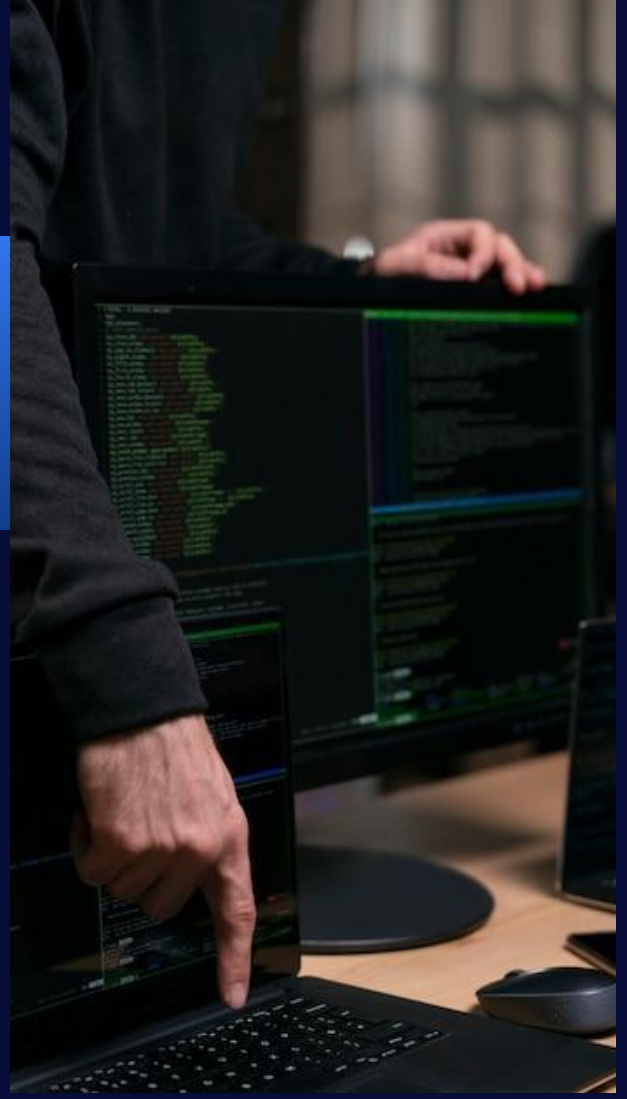
- **Exponential Data Growth:** From megabytes (10^6) a decade ago to exabytes **(10^{18})** and zettabytes **(10^{21})** today.
- **Global Data Projection:** By 2025, global data is expected to reach **181 zettabytes.**
- **Social Media:** Facebook generates **4 petabytes** of data **each day**.

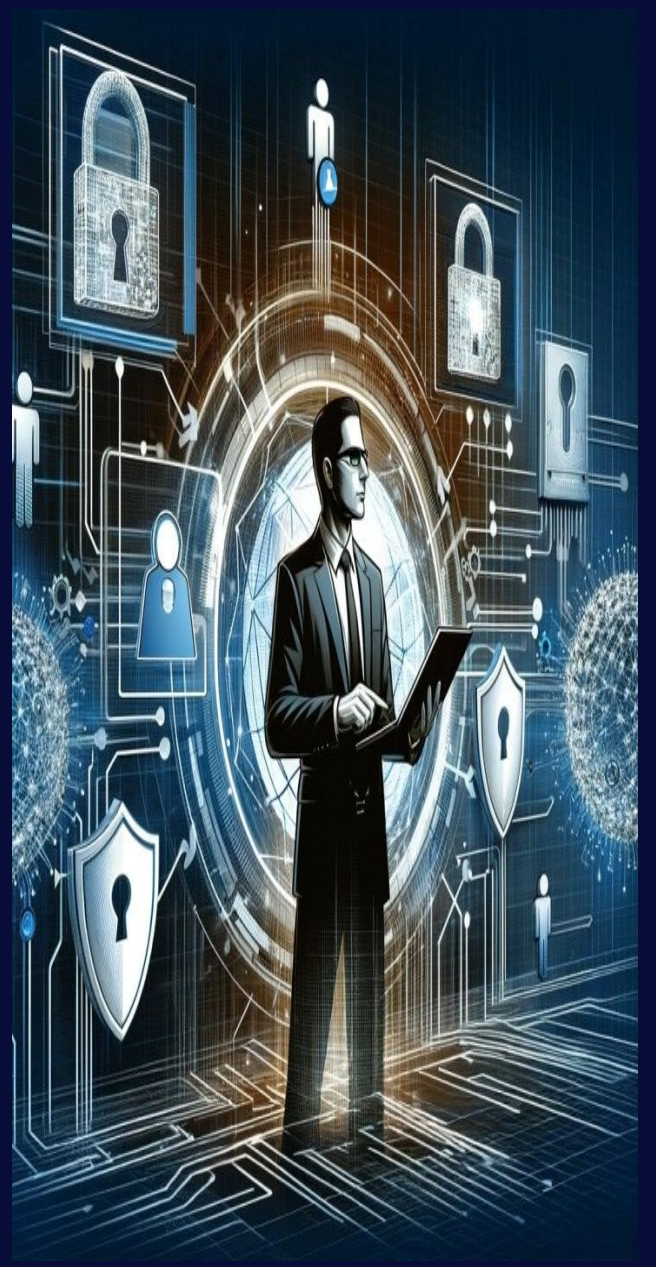




Velocity

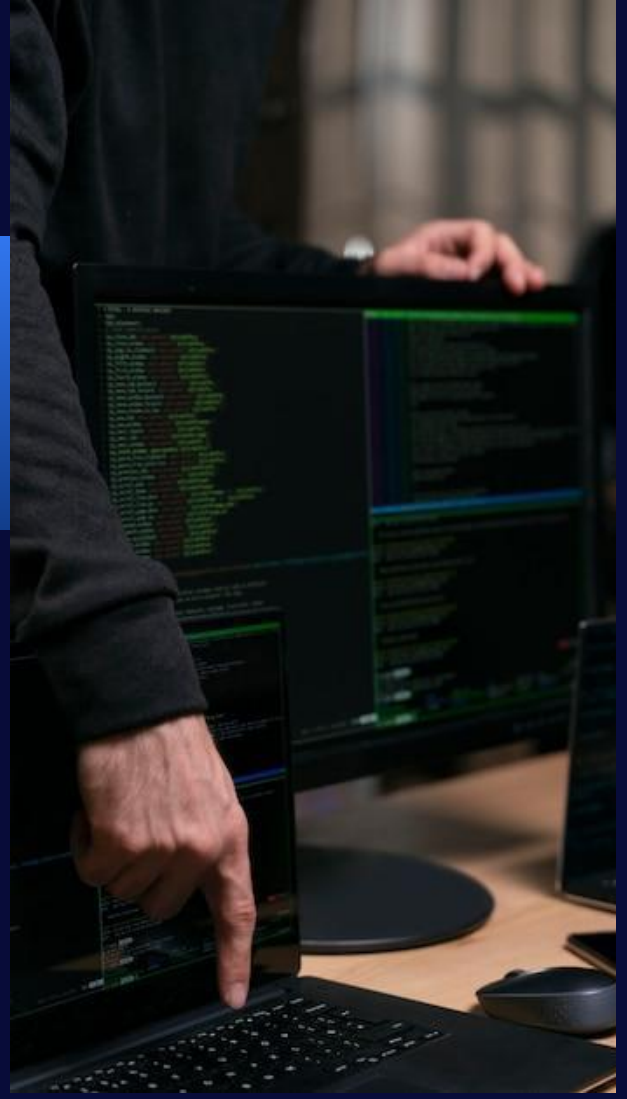
- **Speed of Data Ingestion:** Data arrives rapidly, often requiring systems to store **terabytes** of data per **day**.
- **Speed of Data Processing:** The rapid influx of data also requires fast processing.
- **Real-Time Data Streaming:** Plethora of sources requires continuous processing

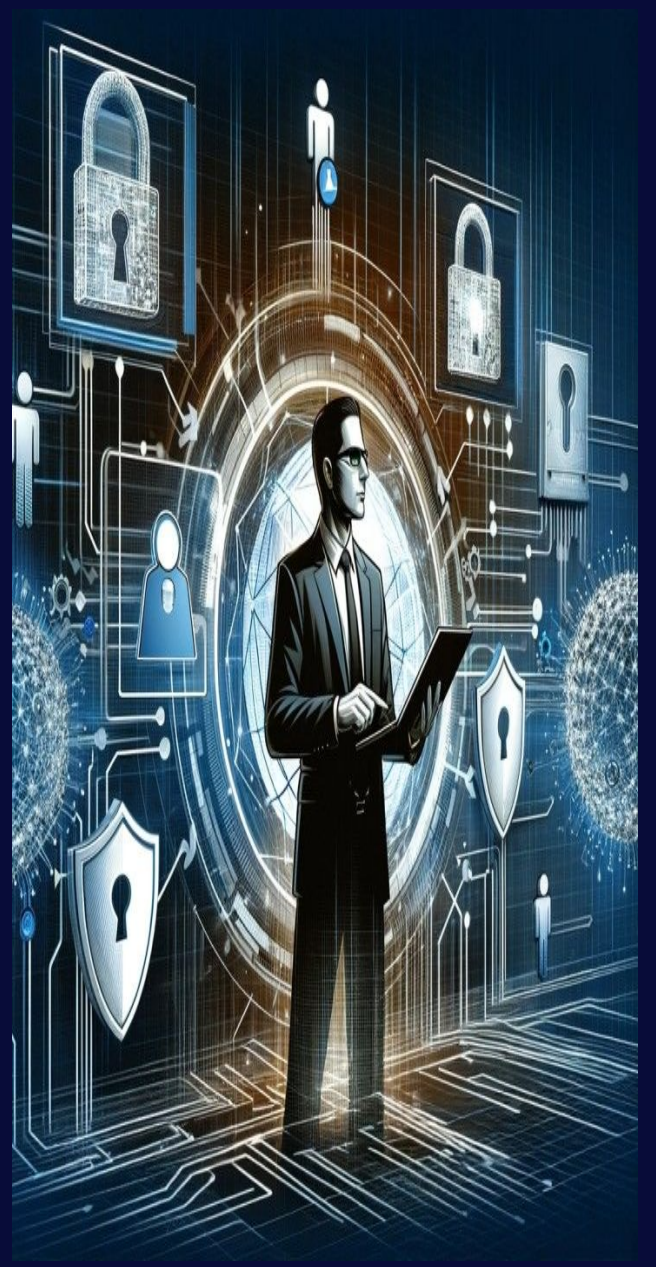




Variety

- **Diverse Data Types:** Includes structured, semi-structured, and unstructured data.
- **Multiple Sources:** Generated from social media, IoT devices, logs, and transactional systems.
- **Integration Challenges:** Requires advanced tools for seamless processing and analysis.





Big Data 7Vs

01

Veracity

02

Value

03

Variability

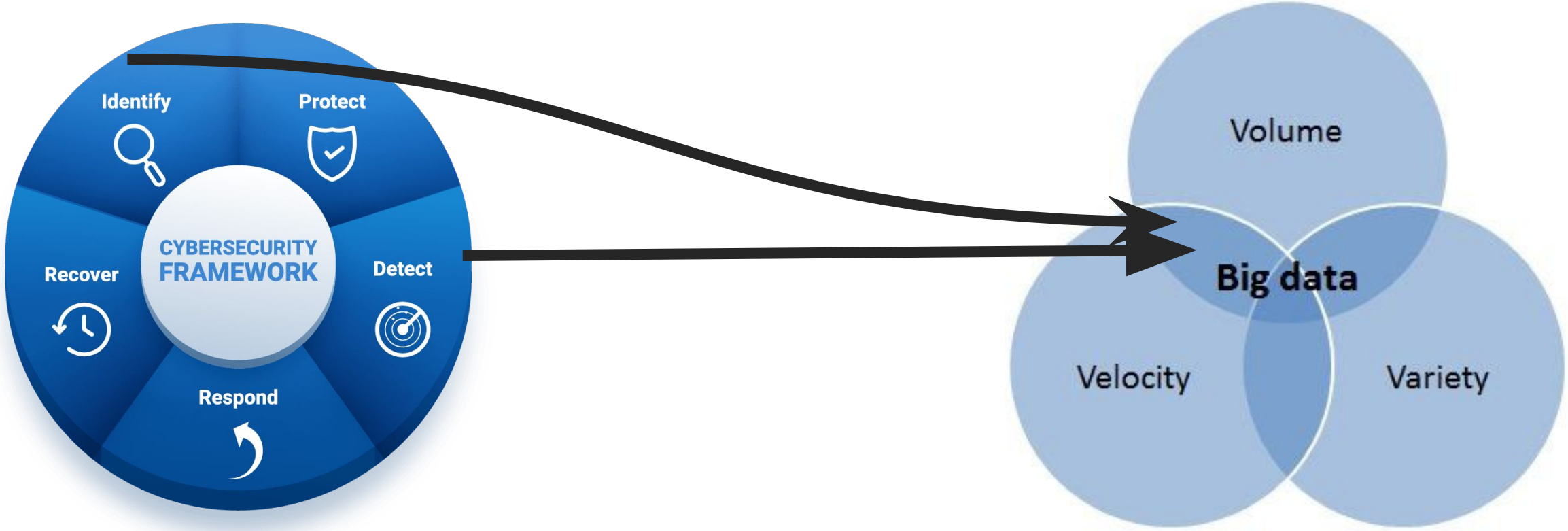
03

Visualization

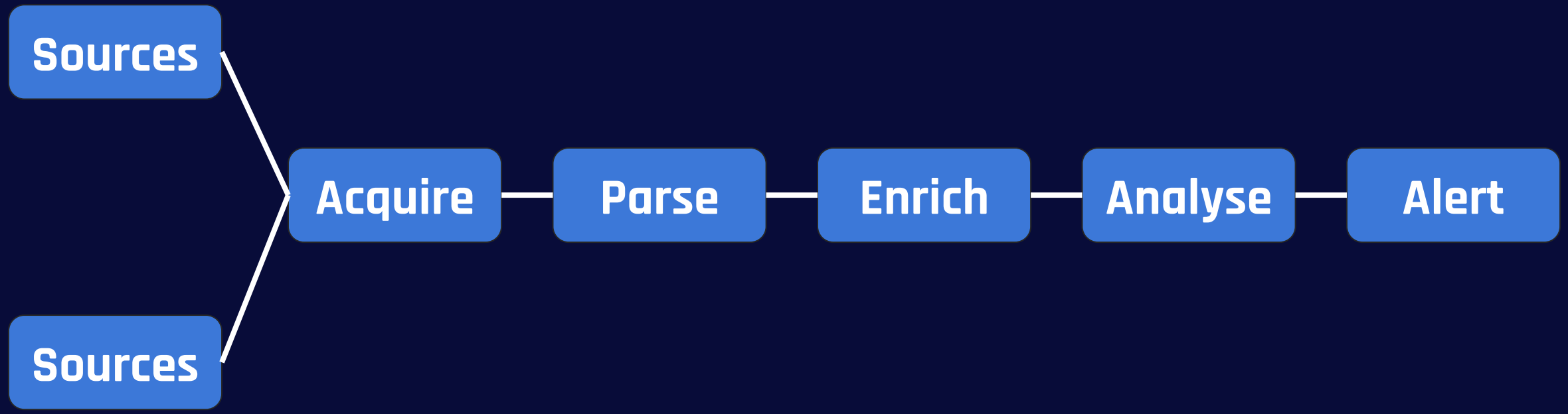
The evolution of big data solutions has fundamentally impacted the following categories

03
Big Data in Cybersecurity

Cybersecurity is a Big Data use case



Detection Data Engineering Pipeline



Data Storage For Long Term Threat Intelligence

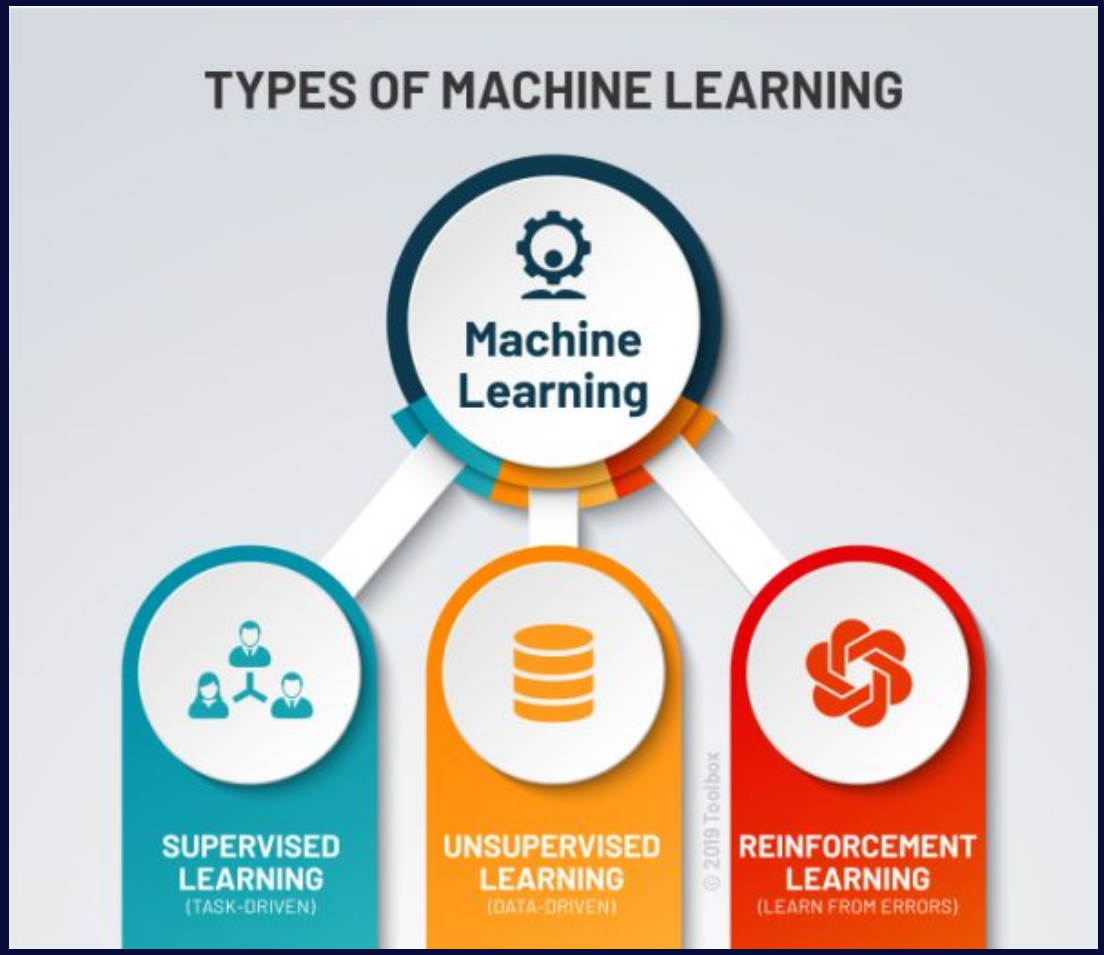
- Long-term storage allows analysis of past events to identify patterns, trends, and ongoing threats.
- Enables Advanced Persistent Threat (APT) detection, where attackers slowly infiltrate systems over long periods.
- Data lakes are optimized for handling large, diverse datasets cost-effectively.

04

AI in Cybersecurity

Machine Learning use cases In Cybersecurity

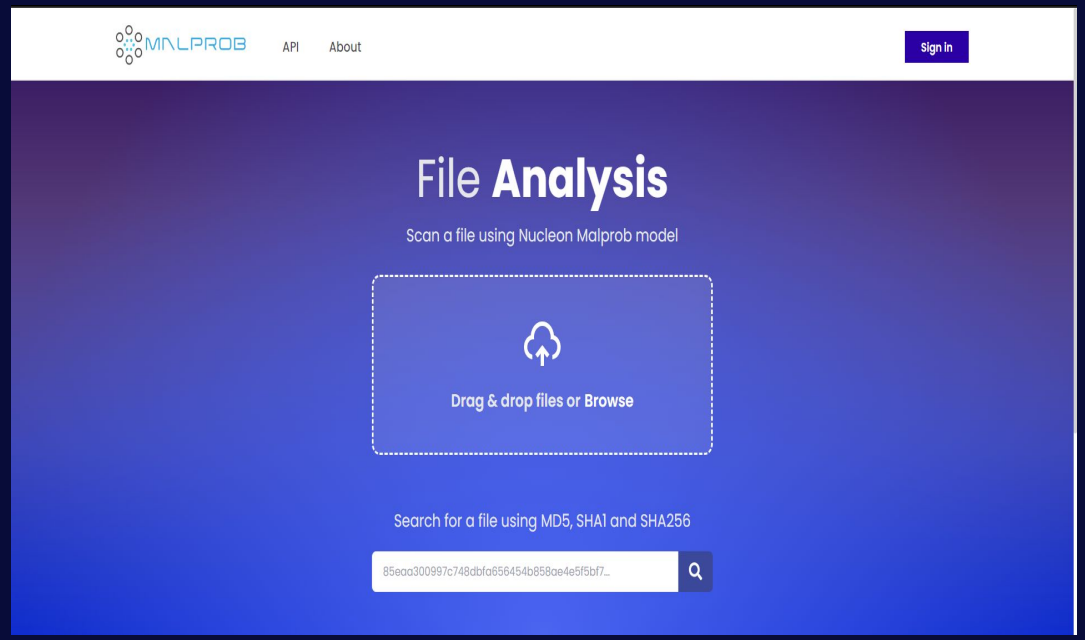
- **Threat Detection :** AI and ML can detect anomalies and threats that traditional systems might miss.
- **Automated Response:** Once a threat is detected, AI-based systems can automatically trigger responses to mitigate risks.
- **Predictive Analytics:** AI and ML help in forecasting potential future attacks by analyzing historical data.



Zero-day attacks

In a world of ever evolving cyber threats, it is getting harder and harder to stay ahead of them.

Zero-day attacks are of high risk since the traditional approaches of signatures and sandboxing often fall short. **Nucleon ecosystem** provides new solution for this modern problem such as the usage of **zero trust** and the **usage of AI** for file detection.



What is malprob

malware detection and identification service, powered by AI.

Nucleon EDR

1 Prevention
User behavior absorption and protection rules creation

2 Detection
Unknown threats detection

4 Remediation
Back to a resilient state

3 Response
Automation and coordination

Q&A

Feel free XD

Thank you !!

For further information don’t hesitate to contact me

 NucleonSec

 Nucleon Security

 team@nucleon-security.com