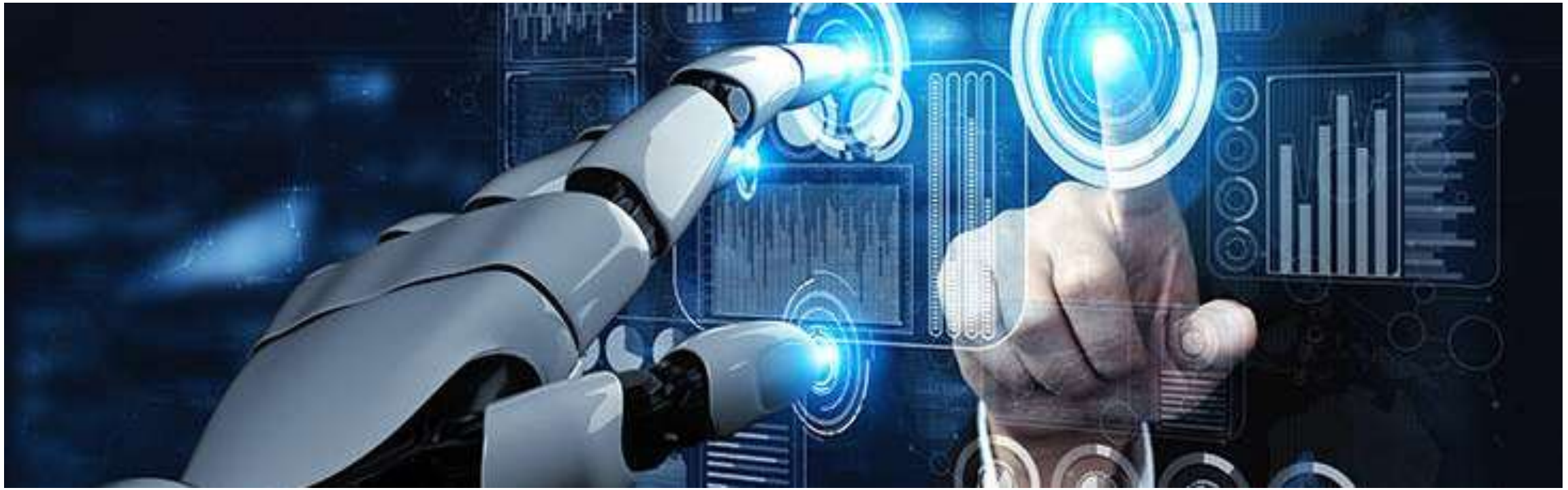
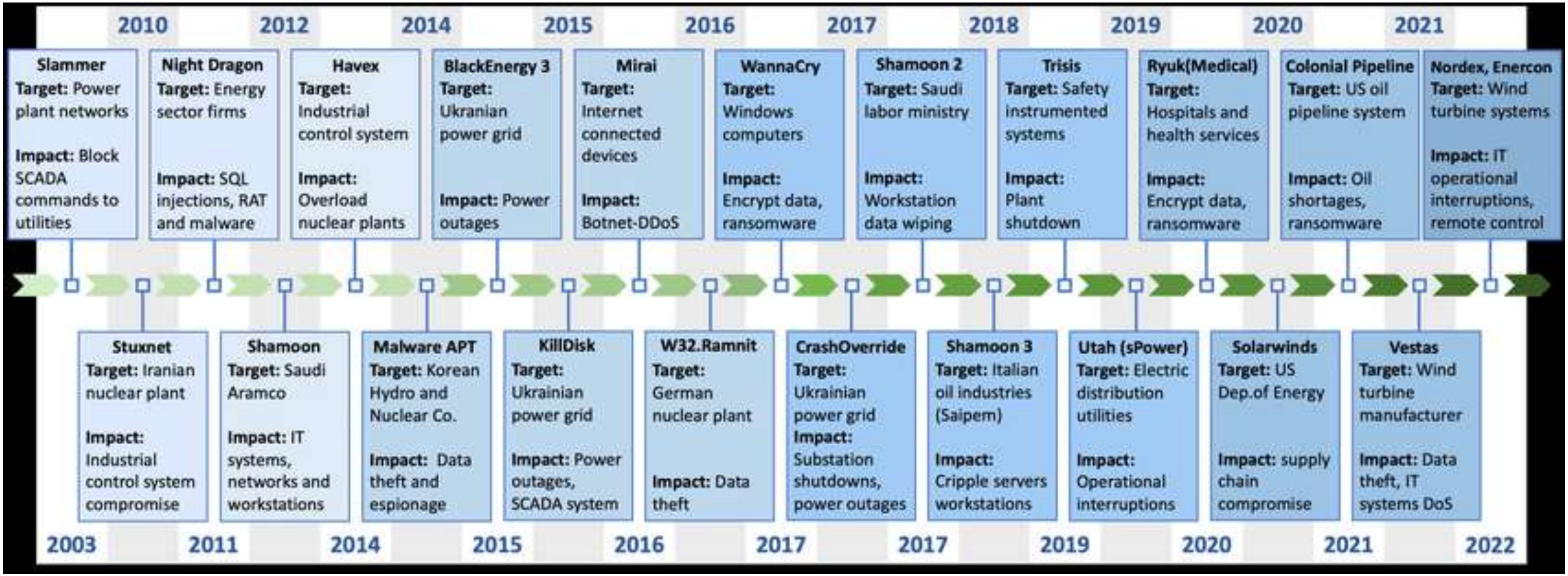
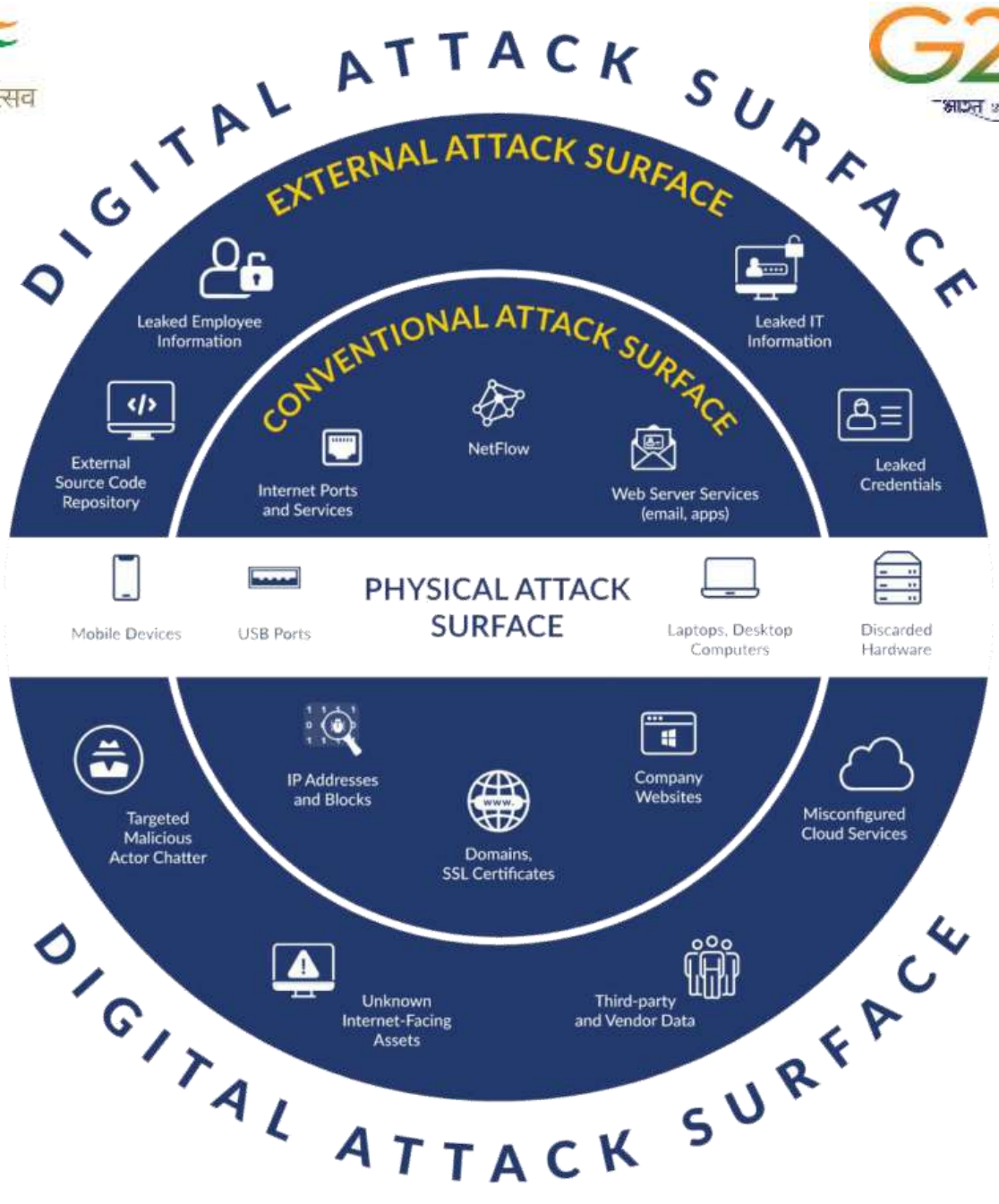
# Cyber Risk Assessment and Control using Artificial Intelligence for IT & OT



A B SENGUPTA, ALT-CISO GRID-INDIA

# Cyber attack on critical infrastructure






## Changing Threat Landscape

Defense is maturing, but as technology evolves — and weaknesses remain — attackers are thriving

## Sovereign Threats

Cyberwar may now be an integrated part of nation-state conflict

## Increasing Disclosure

Regulatory bodies and investors are expanding disclosure demands around cybersecurity and cyber incidents

## Third-Party Cybersecurity Risks

Increased reliance on third-party vendors increases systemic risks

## Cyber Insurance

The role of insurance in risk mitigation is undergoing significant change

## Cybersecurity and Risk Management

Cybersecurity must become an embedded part of an entity's risk management

# DO THESE THREATS PERTINENT TO INDIAN POWER SYSTEM TOO

# Information & Data Exchange – typical Control Centre

## IT SYSTEM

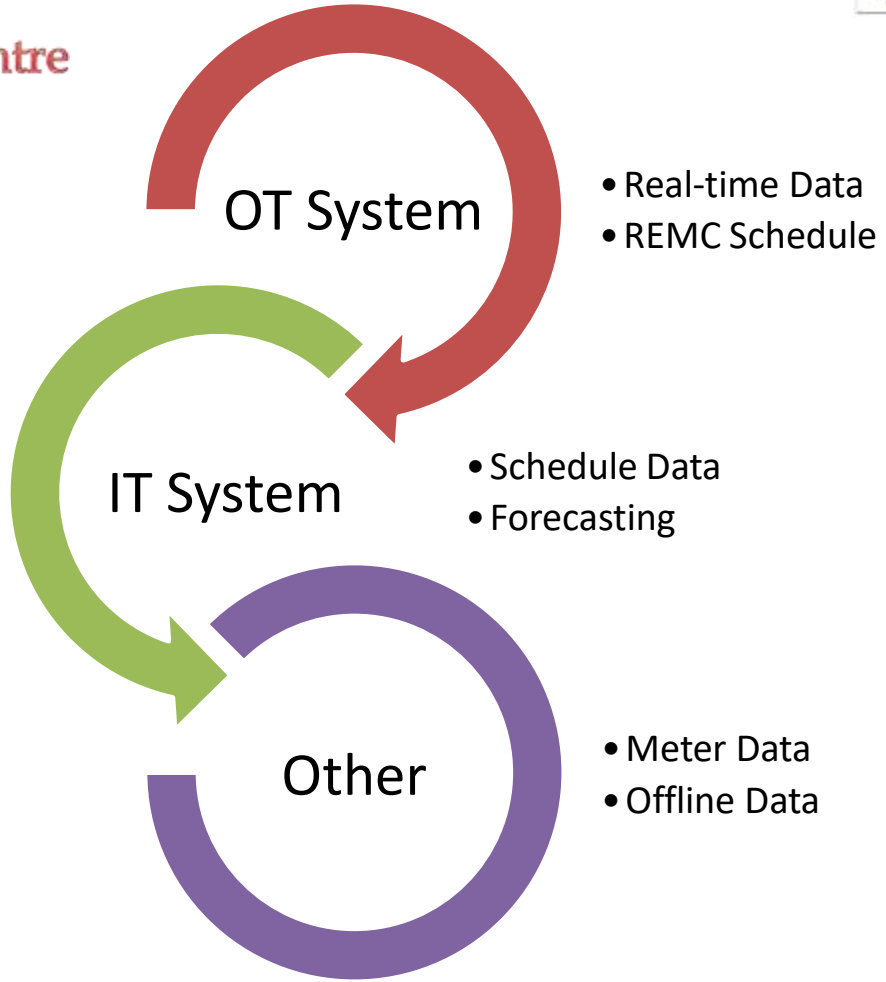
- Web based Energy Scheduling
- REC Mechanism
- Websites
- Reporting & Control Room

## OT System

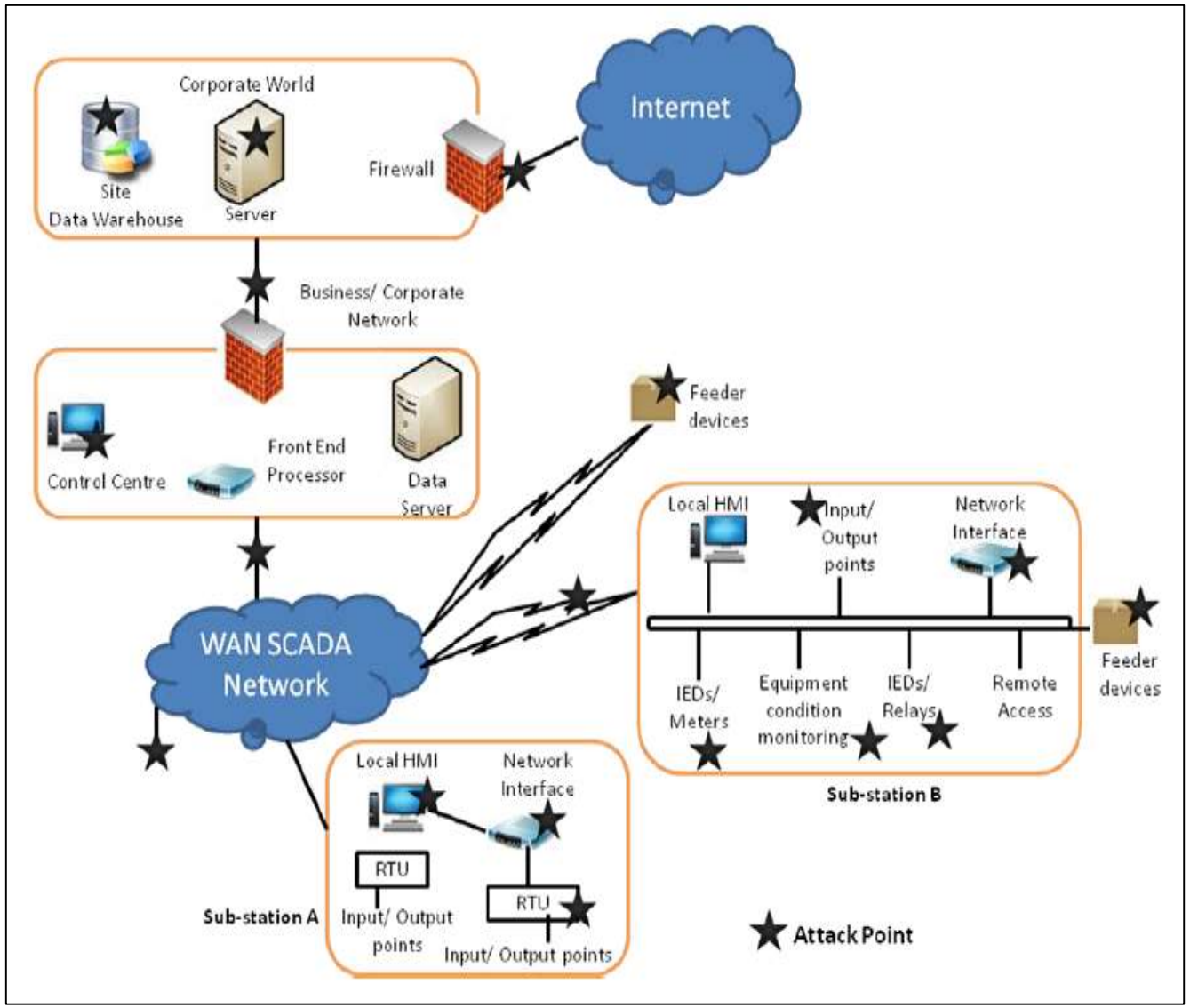
- SCADA System
- URTDSM System
- REMC System

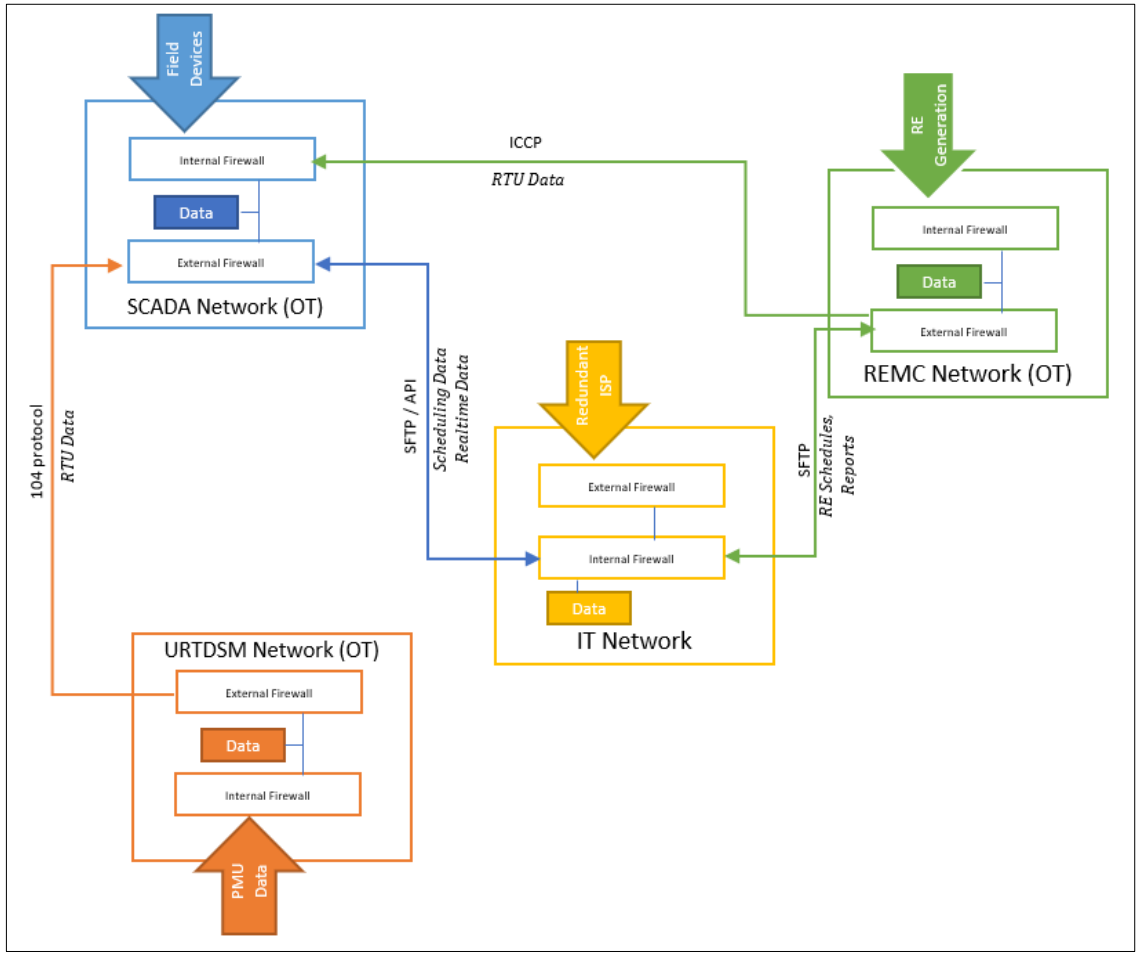
## Other Connectivity

- AMR System
- Inter RLDC Data Exchange
- PX Data




**SCADA - Supervisory Control And Data Acquisition**
**REMC – Renewable Energy Management Centre**
**URTDSM - Unified Real Time Dynamic State Measurement**
**REC – Renewable Energy Certificate**
**AMR – Automated Meter Reading**
**PX – Power Exchange**


Corporate World
Site
Data Warehouse
Server
Firewall
Internet
Business/ Corporate Network
Control Centre
Front End Processor
Data Server
Feeder devices
WAN SCADA Network
Local HMI
Input/ Output points
Network Interface
IEDs/ Meters
Equipment condition monitoring
IEDs/ Relays
Remote Access
Feeder devices
Sub-station B
Local HMI
Network Interface
RTU
RTU
Input/ Output points
Input/ Output points
Sub-station A
Attack Point


Field Devices
Internal Firewall
Data
External Firewall
SCADA Network (OT)
ICCP
RTU Data
RE Generation
Internal Firewall
Data
External Firewall
REMC Network (OT)
104 protocol
RTU Data
SFTP / API
Scheduling Data
Realtime Data
Redundant ISP
External Firewall
Internal Firewall
Data
IT Network
SFTP
RE Schedules, Reports
URTDSM Network (OT)
External Firewall
Data
Internal Firewall
PMU Data

# HOW TO MITIGATE THE CHALLENGE

# Cyber Security Infrastructure & Administration

STRICT CONTROL IMPLEMENTATION


PROACTIVE MONTORING

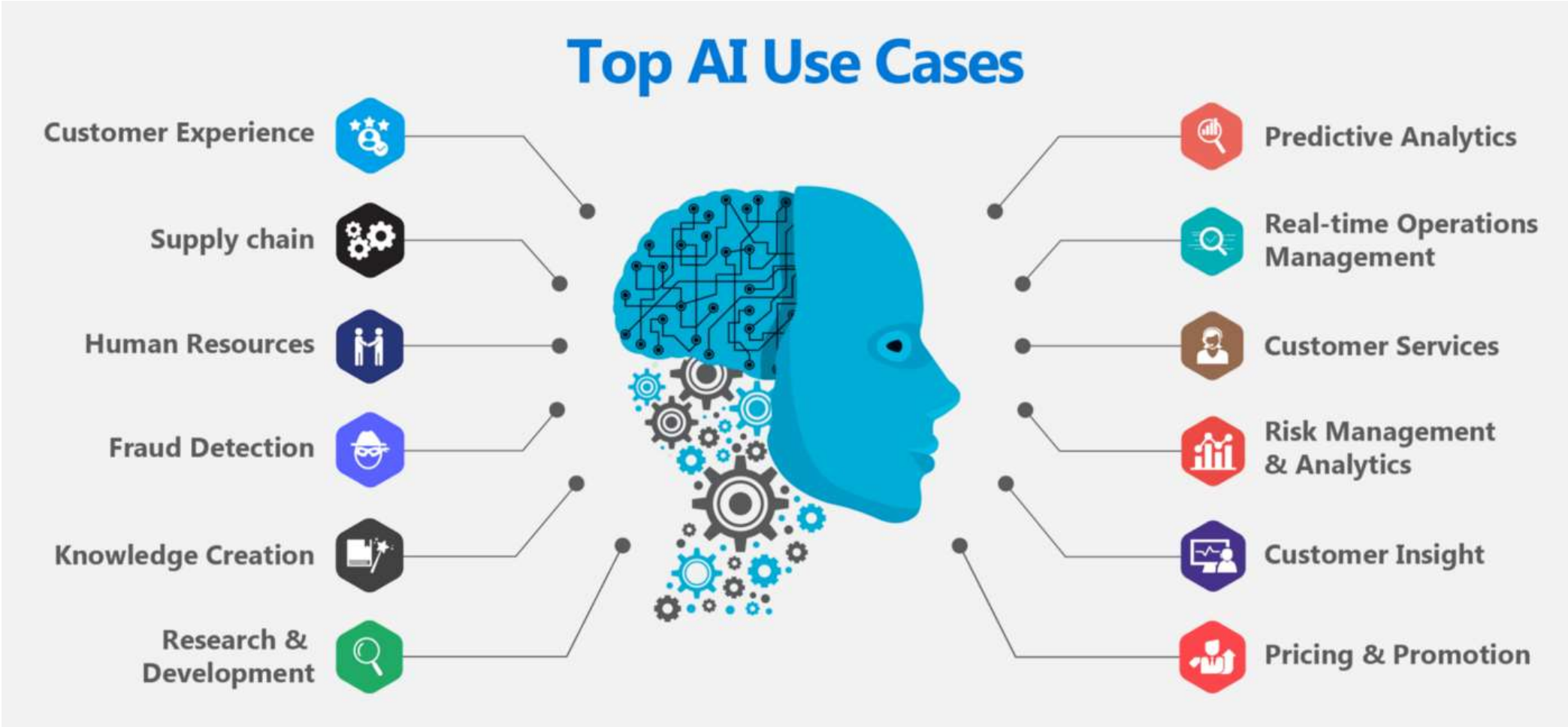

COMPLIANCE TO GUIDELINES


ADOPTION OF NEW TECHNOLOGIES

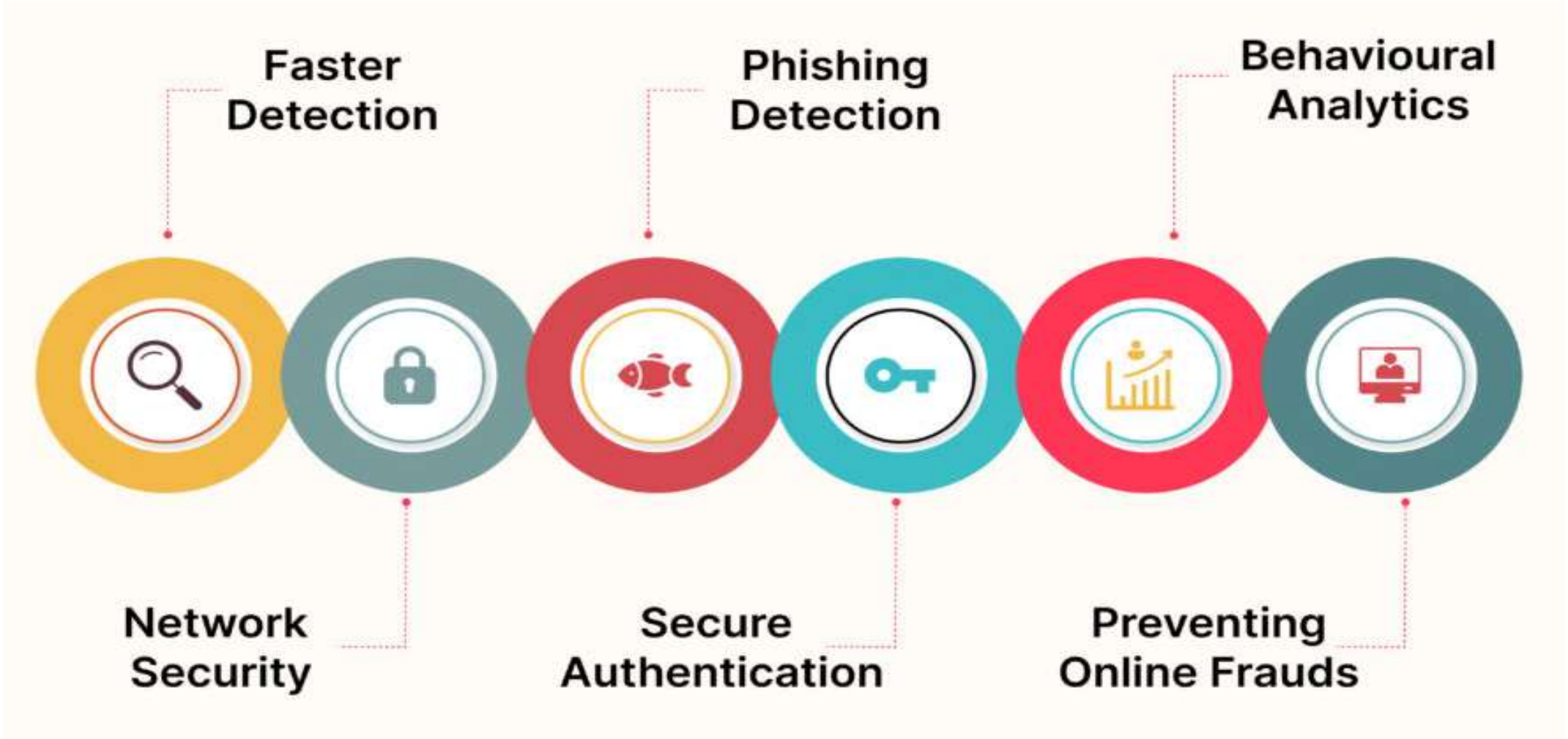

BALANCED IN-HOUSE AND OUTSOURCED RESOURCES

- INTRUSION PREVENTION SYSTEM AT GATEWAY
- LAYERED NETWORK ARCHITECTURE
- ANTIVIRUS AND ANTI-MALWARE PROTECTION
- LEAST PRIVILEGE USER ACCESS
- ANTI-APT & VA-PT
- HARDENED IT / OT INTEGRATION
- PHYSICAL SECURITY
- DC-DR ARCHITECTURE

AI is a collection of techniques like machine learning, deep learning, speech and visual recognition, natural language processing and understanding.



# AI USE CASES FOR CYBER SECURITY IMPLEMENTATION



**Risk management** is the process of discovering, evaluating, and managing threats to an organization's profitability. The most popular threats arise from the following sources:

Financial uncertainties

Legal responsibilities

Accidents

Strategic management failures

Natural disasters

1. **Uncertainty detection**
   Get state of affairs
2. **Risk identification**
   Define risks
3. **Risk analysis**
   Calculate odds and effect
4. **Risk assessment and evaluation**
   Decide on risks' acceptability
5. **Risk mitigation**
   Device a strategy to fight risks
6. **Risk monitoring**
   Monitor new and current risks

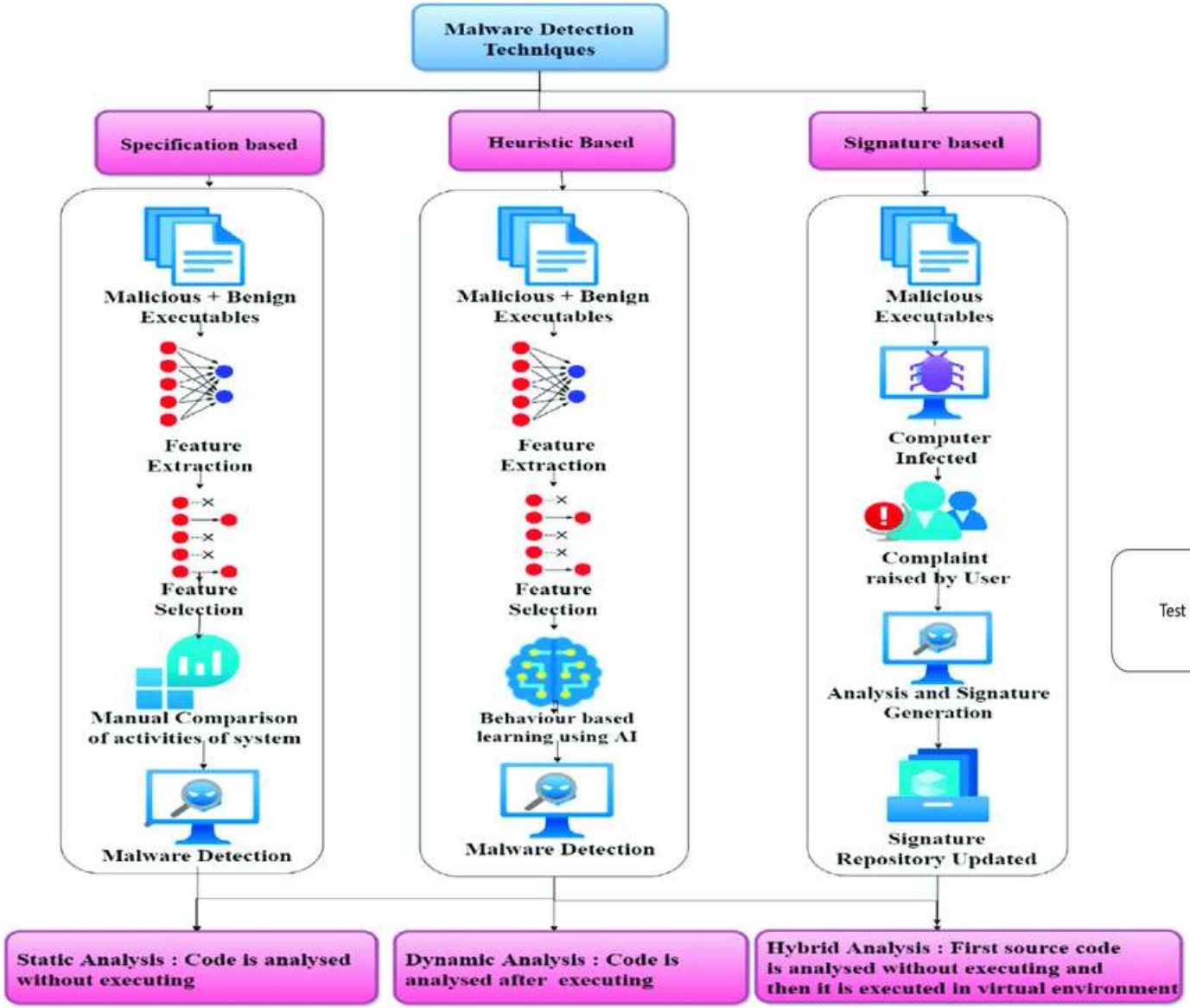
## AI Based Threat Detection & Response


- **Threat detection:** Detect cyber threats more quickly and accurately than traditional methods. This is done by using machine learning to analyze large amounts of data and identify patterns that may indicate a potential attack.

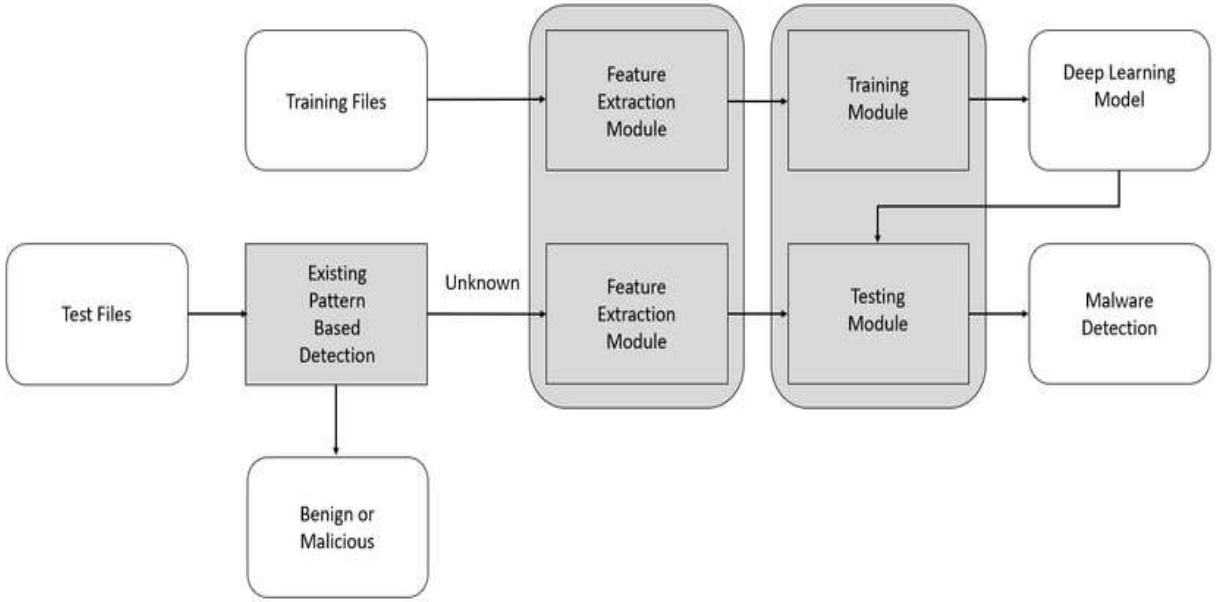
- **Threat analysis:** Analyze cyber threats in order to understand their nature and impact. This information can then be used to develop effective mitigation strategies.

- **Threat response:** Respond to cyber threats more quickly and effectively. This is done by using machine learning to identify and block malicious traffic, as well as to automate the process of incident response.

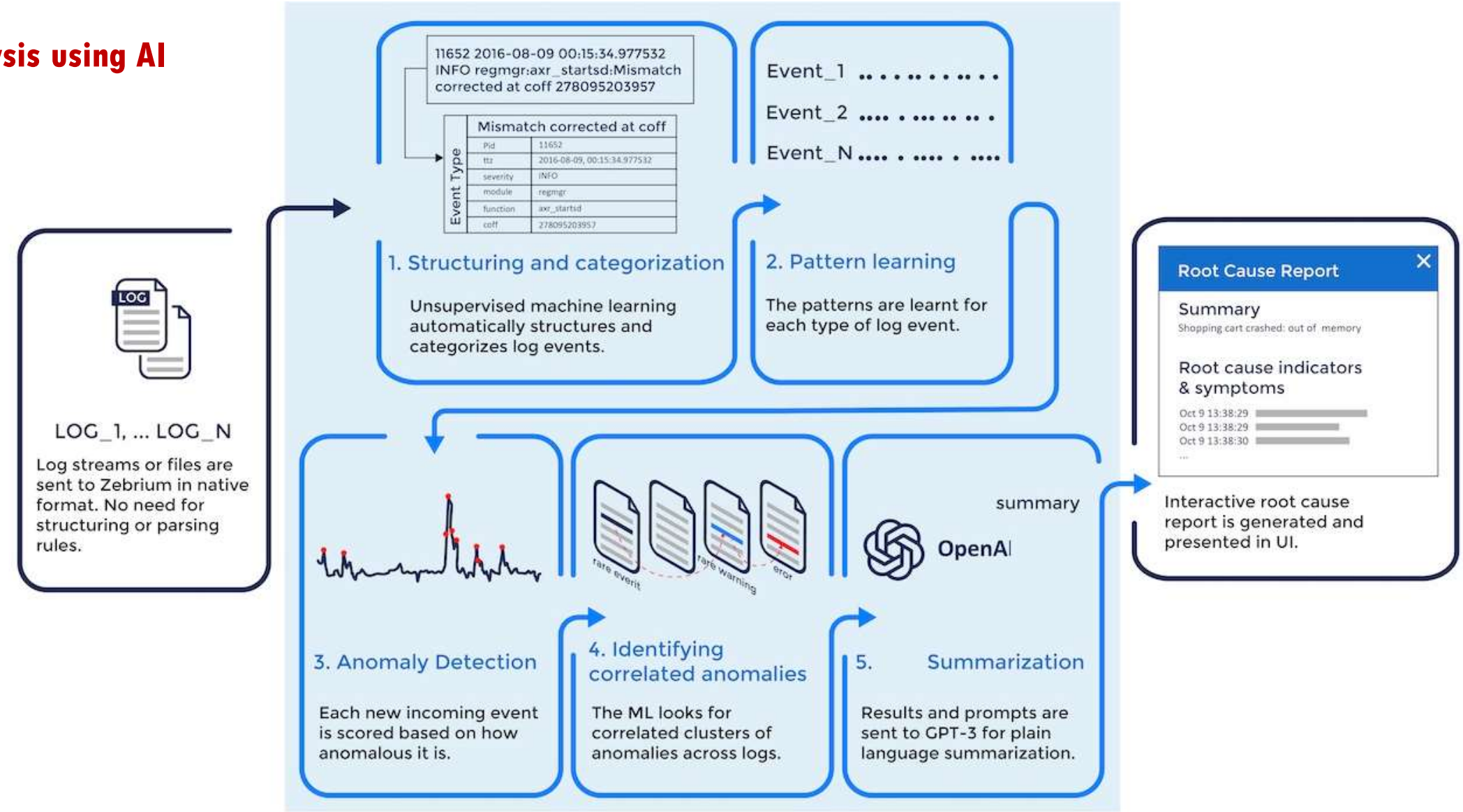
- **Network Traffic Analysis:** AI identifies malicious activities hidden in legitimate network traffic.



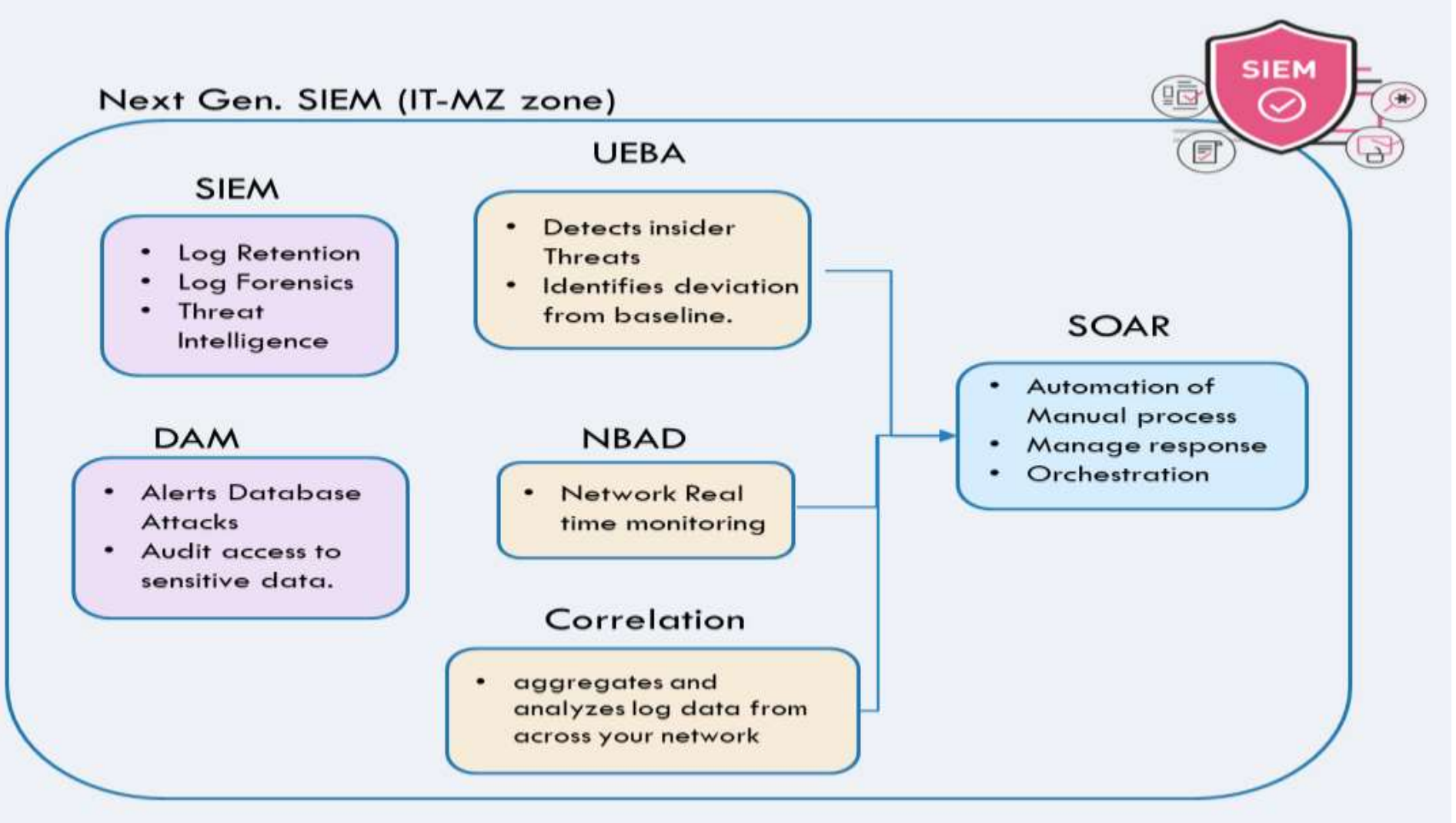

## Malware detection using AI



# Log Analysis using AI



# Components of 24 x 7 Security Operation Centre for IT / OT installations



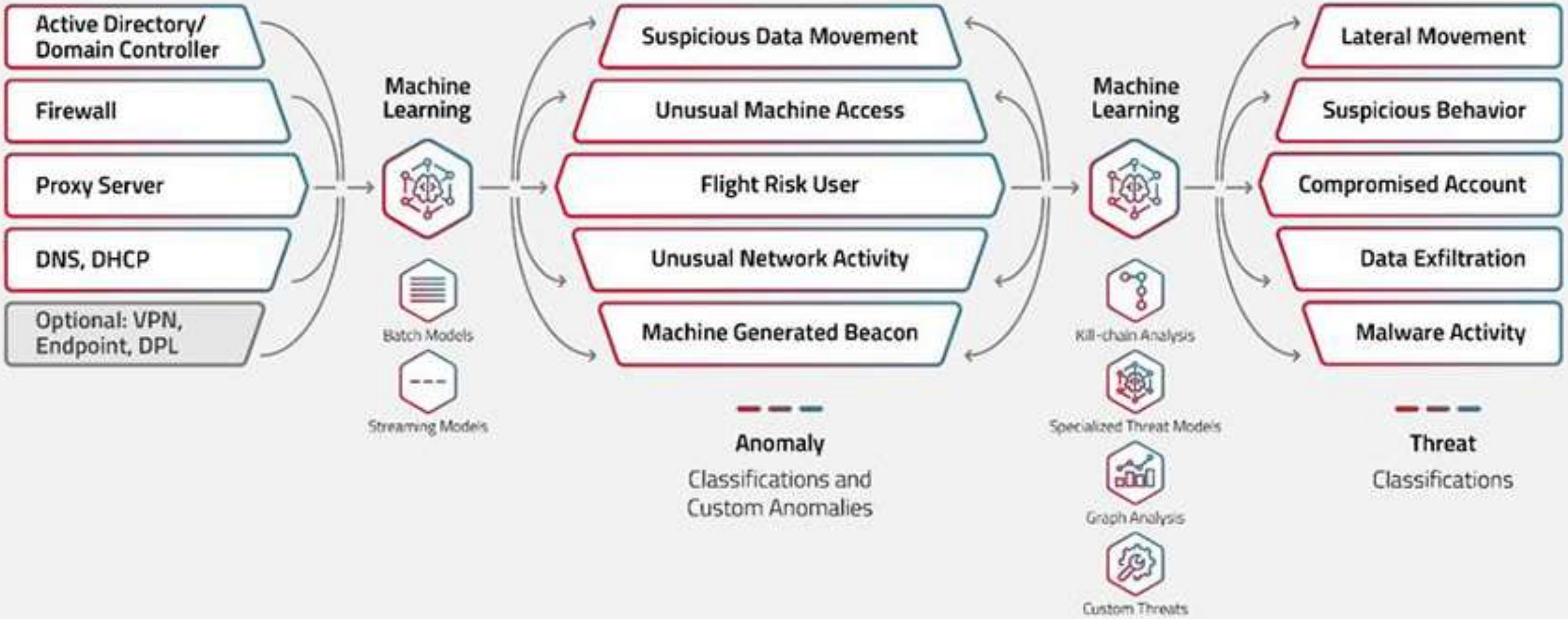

**SIEM**
Security Information and Event Management

**UEBA**
User Entity Behavior Analysis

**NBAD**
Network Behavior Anomaly Detection

**SOAR**
Security Orchestration and Automated Response

# How Does UEBA Work?



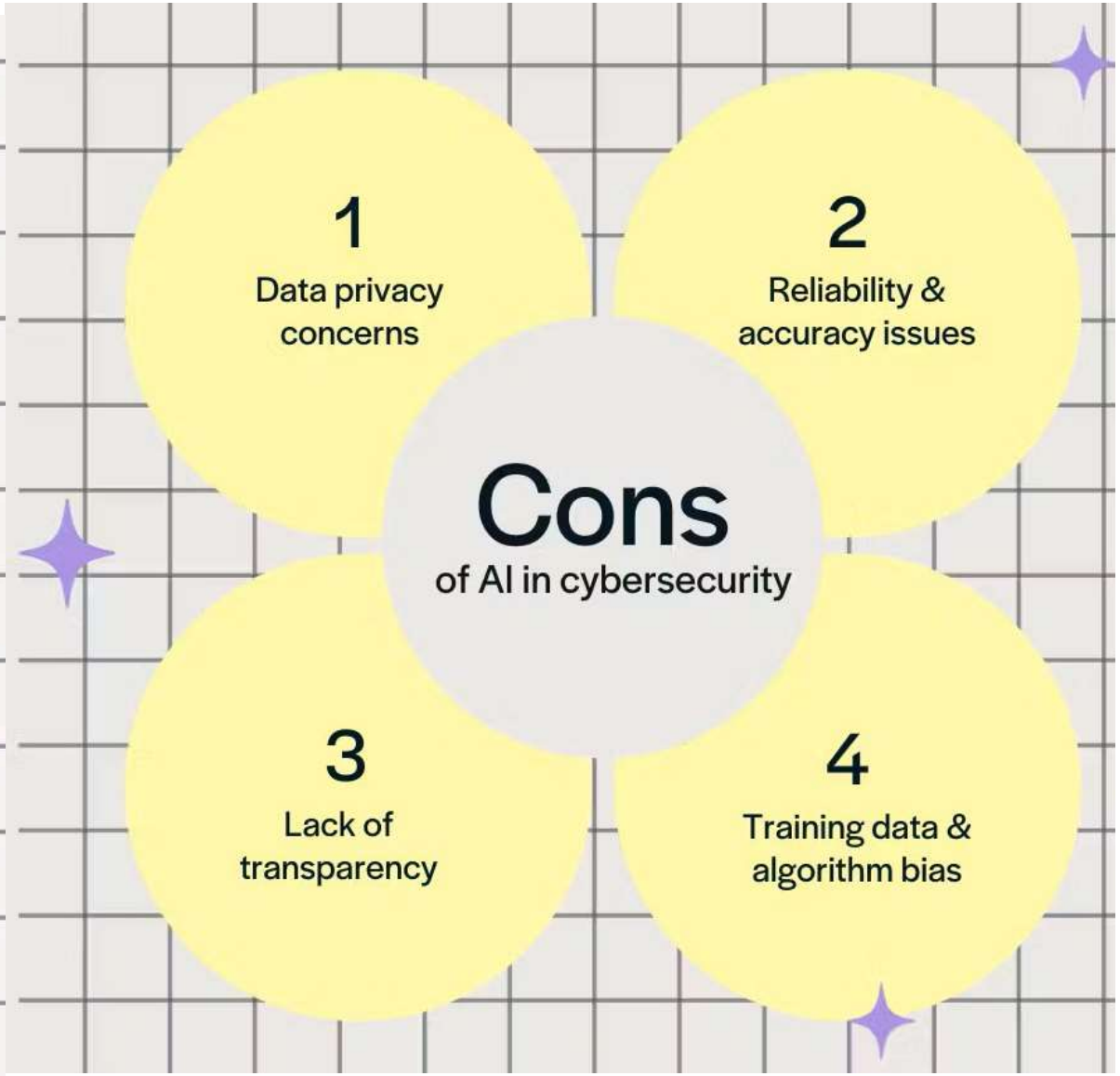
## UEBA use cases

**Detecting Suspicious User Accounts:** such as accessing sensitive data or systems without authorization, logging in from unusual locations or devices, or performing unauthorized actions.

- **Detecting Suspicious User-Like Entities:** Detect entities that mimic user behavior, such as bots, malware, or rogue applications. These entities may try to evade traditional security tools by blending in with normal user activity such as browsing the web or sending emails.
- **Monitoring User Activity:** Provide a comprehensive view of user activity across the network, such as what data or systems they access, when and how often they log in, what actions they perform, and who they interact with.
- **Detecting Suspicious Account Creation Attempts:** Provide a comprehensive view of user and entity behavior across the network, including who is accessing what resources, when, where, how, and why.
- **Speeding Up Cybersecurity Investigations:** Correlate different events and alerts across the network and provide a timeline of activities and interactions for each user and entity involved in an incident. It can also provide contextual information, such as the risk score, the motivation, and the impact of each behavior.
- **Other uses for UEBA:** These can include detecting data exfiltration, preventing fraud, enforcing policies, optimizing performance, and enhancing user experience.

# ADVANTAGES OF AI IN CYBER SECURITY


Pros
of AI in cybersecurity
1
Identifying attack precursors
2
Enhancing threat intelligence
3
Strengthening access control & password practices
4
Minimizing and prioritizing risks
5
Automating threat detection & response
6
Increasing human efficiency & effectiveness


Cons
of AI in cybersecurity
1
Data privacy concerns
2
Reliability & accuracy issues
3
Lack of transparency
4
Training data & algorithm bias

# Thank you!

anwayasen@grid-india.in