AI in Modern Cyber Security

Krishita Haresh Ravat
BTech9 – 39
22UF17301CM046

CONTENTS

01 Opening

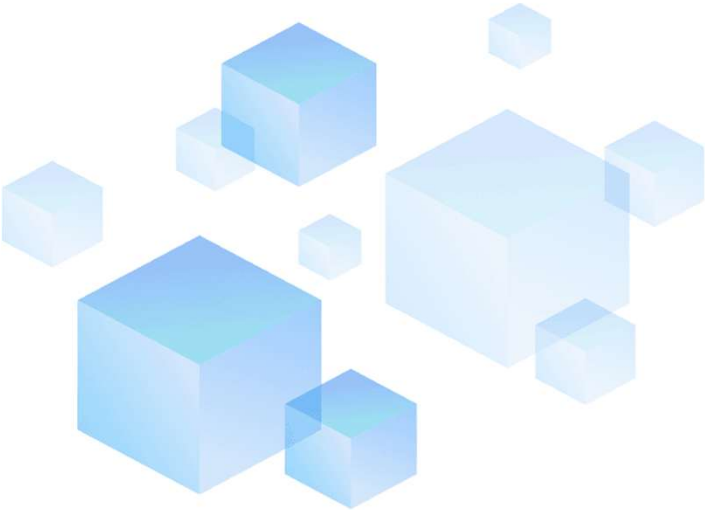
02 The Challenge

03 The AI Shift

04 AI Applications

05 Conclusion

06 Thanks



01

Opening

The New Frontier:

Applications of AI in Modern Cyber Security

Enhancing Digital Forensics & Enterprise Defense

02

The Challenge

The Challenge: Traditional Defenses are Reactive

Legacy tools are ill-equipped for modern, dynamic threats.

Signature-Based Detection

Can only identify **known threats**, leaving systems vulnerable to new attacks.

Slow, Manual Processes

Human analysis is time-consuming, creating **delays in threat response**.

Vulnerable to Advanced Threats

Ineffective against **zero-days** and **polymorphic attacks**.

03

The AI Shift

The AI Shift: Proactive & Intelligent Defense

AI transforms security from a reactive posture to a proactive, predictive, and automated discipline.

Big Data Processing

Analyzes massive datasets to uncover hidden threat patterns.

Pattern Recognition & Prediction

Learns normal behavior to identify anomalies and predict attacks.

Real-time Decision Making

Automates responses to threats at machine speed.

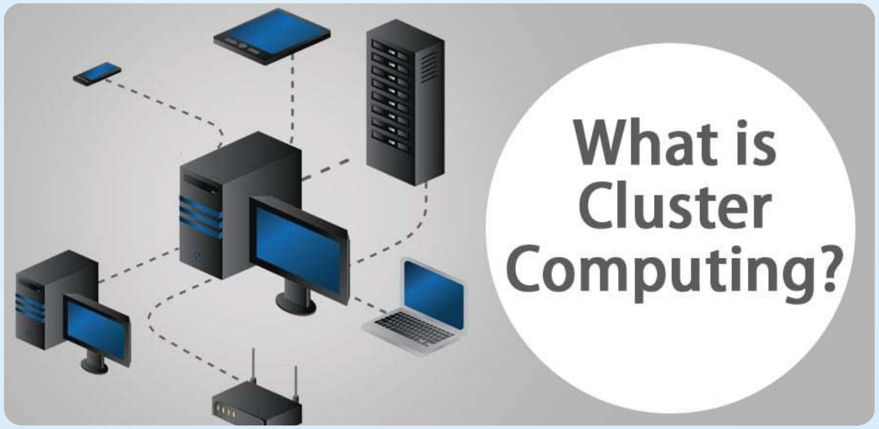
04

AI Applications

1. Superior Threat Detection: Behavioral Analysis

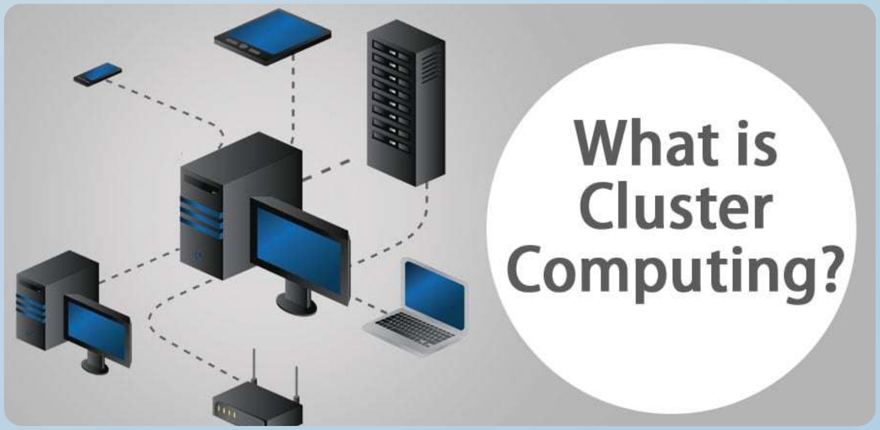
AI learns what "normal" looks like to find the abnormal .

Normal Behavior



AI establishes a baseline of regular, consistent patterns.

Anomalous Behavior



Deviations from the baseline are flagged as potential threats.

Detecting the Undetectable

Zero-Day Exploits

Identifies attacks leveraging unknown vulnerabilities before signatures exist.

Insider Threats

Spots malicious or compromised internal actors based on behavioral changes.

Reduced False Positives

Delivers focused, high-fidelity alerts, allowing analysts to concentrate on real threats.

2. Intelligent Phishing & Spam Filtering

AI moves beyond simple keyword blocking to understand context and intent .

Contextual Analysis

Understands the full context of a message.

Natural Language Processing

Analyzes language for malicious intent.

URL Scanning

Inspects links for hidden threats.

Countering Sophisticated Spear-Phishing

Seemingly Legitimate Email

An email that appears normal to the human eye.

AI Analysis Reveals Threat

AI spots subtle malicious cues invisible to users.

Sender History & Tone Analysis

Detects Typosquatting

Learns from Enterprise Reports

3. Automated Vulnerability Management

AI transforms vulnerability management from a numbers game into a risk-based strategy .

- Continuous Scanning
- Intelligent Risk Scoring
- Predictive Prioritization

Vulnerability Queue

HIGH RISK

HIGH RISK

Focus on Critical Risk, Not Just Quantity

AI helps focus resources where they matter most, maximizing efficiency and impact.

Internal Scans

Vulnerability data from your systems.

+

Threat Intelligence

Real-world exploitability data.

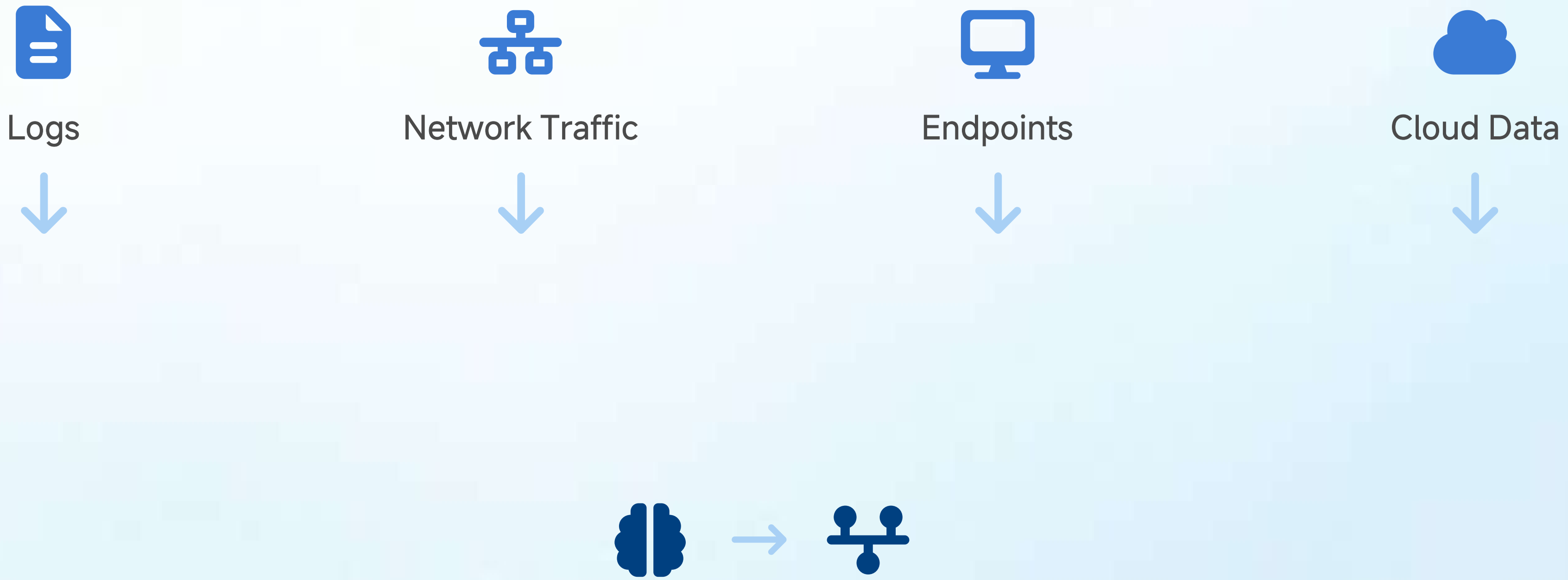
→

Prioritized Action

A focused list of high-impact vulnerabilities.

4. Accelerating Advanced Digital Forensics

AI automates the correlation of vast datasets to reconstruct attack timelines in hours, not weeks .



Logs

Network Traffic

Endpoints

Cloud Data

From Weeks to Hours: Expediting Investigations

Identify Attack Path & Entry Point

Quickly trace the attacker's steps to understand how the breach occurred.

Determine Scope of Compromise

Accurately assess which systems and data were affected.

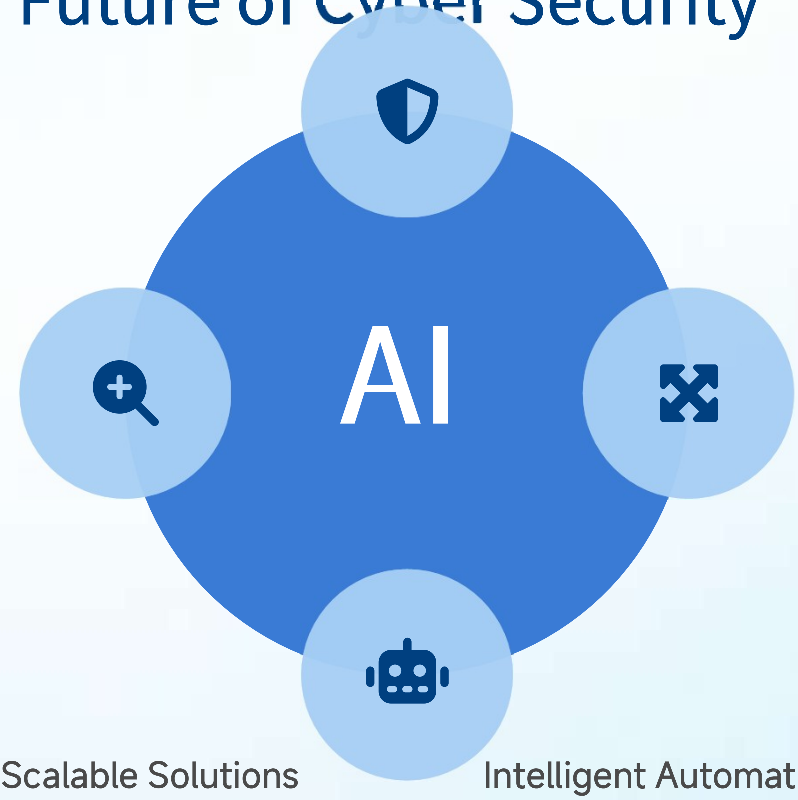
Faster Recovery & Remediation

Execute a targeted response to contain the threat and restore operations swiftly.

05

Conclusion

Conclusion: AI - The Future of Cyber Security



Proactive Defense

Scalable Solutions

Intelligent Automation

Enhanced Forensics

06

Thanks

Thank You

Questions?

For a deeper dive, please refer to the full article.

SCAN ME

Scan for Full Article