

# Agentic AI for Cybersecurity

## The Dawn of Self-Operating Intelligence

Dr. Parteek Kumar, Associate Professor (Career Track),  
School of EECS,  
Washington State University, Pullman, WA

# Who I Am

- Parteek Kumar, Associate Professor, School of EECS, Washington State University, Pullman, WA, USA,
- Author | Educator | Researcher | Faculty Coach
- Former Professor in the Department of Computer Science and Engineering and Former Associate Dean of Student Affairs at Thapar Institute of Engineering and Technology, Patiala (2004-2020).
- Former Visiting Professor at LAMBDA Lab, Tel Aviv University, Israel (2020-2022).
- Former Visiting Professor at the Department of Computer Science, Whitman College, Walla Walla, Washington State, USA (2022-2024).
- Former Assistant Professor DAV College, Amritsar (1998-2004)

# My Recent work

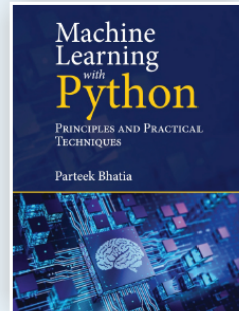
CAMBRIDGE

## Machine Learning *with Python*

Principles and Practical Techniques

**Parteek Bhatia**

Machine learning has become a dominant problem-solving technique in the modern world, with applications ranging from search engines and social media to self-driving cars and artificial intelligence. This lucid textbook presents the theoretical foundations of machine learning algorithms, and then illustrates each concept with its detailed implementation in Python to allow beginners to effectively implement the principles in real-world applications. All major techniques, such as regression, classification, clustering, deep learning, and association mining, have been illustrated using step-by-step coding instructions to help inculcate a 'learning by doing' approach. The book has no prerequisites, and covers the subject from the ground up, including a detailed introductory chapter on the Python language. As such, it is going to be a valuable resource not only for students of computer science, but also for anyone looking for a foundation in the subject, as well as professionals looking for a ready reckoner.



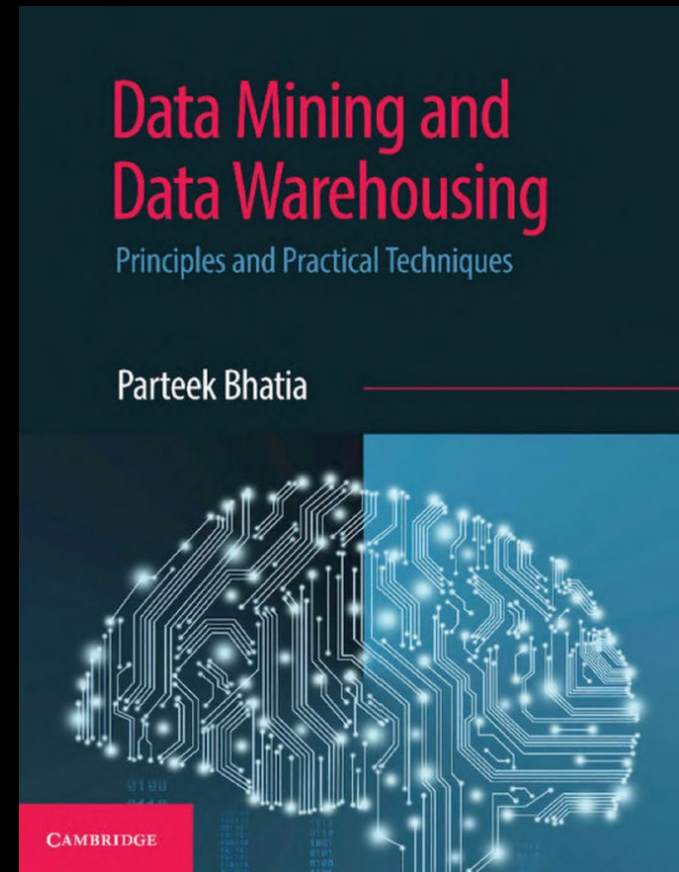
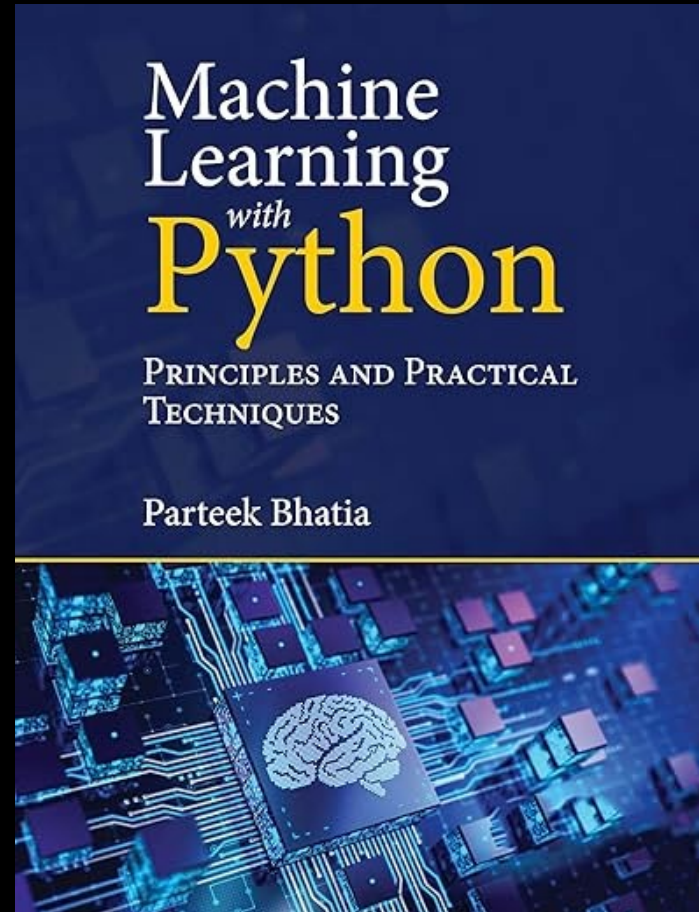
Parteek Bhatia is an Associate Professor in the School of Electrical Engineering & Computer Science, Washington State University, Pullman, WA, USA. He was previously a Professor in the Department of Computer Science and Engineering at Thapar Institute of Engineering and Technology, Patiala, India, and has also served as a Visiting Professor at Whitman College, Walla Walla, WA, USA, and at the LAMBDA Lab, Tel Aviv University, Israel. His research interests include ML, natural language processing, and explainable AI. He has authored several textbooks in the field of databases, including Data Mining and Data Warehousing: Principles and Practical Techniques, published by Cambridge University Press in 2019.

Format: PB | ISBN: 9781009170246

Price: ₹1395

[www.cambridge.org](http://www.cambridge.org)

 CAMBRIDGE  
UNIVERSITY PRESS



# The Need for AI in Cybersecurity

- Cybersecurity alerts are growing exponentially
- Security Operations Center (SOC) analysts face alert fatigue
- Traditional security workflows are slow and expensive
- AI is transforming modern security operations
- Future SOC systems will be collaborative and autonomous

# The Real Cybersecurity Problem

## Modern Cyber Security Challenges

- Attackers are leveraging AI to automate cyberattacks
- Millions of logs generated daily
- False positives overwhelm analysts
- Slow response increases damage
- Security teams are understaffed
- Human analysis does not scale

# Traditional SOC Workflow

## Traditional Pipeline

- Logs → Security Platform → Human Analyst → Manual Decision

## Limitations

- Reactive workflows
- Limited scalability
- Slow incident handling
- Human bottlenecks

# How AI Changes Cybersecurity

## AI-Powered Security Operations

- AI reads logs automatically
- AI identifies attack patterns
- AI classifies threats
- AI prioritizes incidents
- AI security agents work autonomously to identify risks, take actions, and secure systems
- AI agents collaborate like security teams

# What is Agentic AI?

Agentic AI systems contain:

- Multiple specialized AI agents
- Role-based collaboration
- Shared reasoning
- Autonomous decisions
- Goal-oriented execution

# Agentic AI : From Prompt to Purpose

- Artificial Intelligence is evolving beyond static, one-off responses into systems that can think, act, and adapt on their own. This new wave, known as **Agentic AI**, marks a shift from reactive automation to proactive autonomy.
- Instead of just generating answers, these systems **plan, reason, execute actions**, and even **reflect** on outcomes.
- Its like an assistant that manages your project end-to-end.

# What is Agentic AI?

- **Agentic AI** refers to AI systems designed to act as *autonomous agents*, entities capable of perceiving their environment, reasoning about goals, and taking actions through connected tools or APIs.
- Unlike traditional AI models that wait for instructions, Agentic systems continuously monitor triggers, learn from context, and choose their next steps dynamically.

# What is Agentic AI?

## Core Characteristics:

- **Autonomy:** Executes actions with minimal human supervision.
- **Tool Use:** Connects to APIs, services, and devices to get real work done.
- **Memory:** Maintains context and history for long-term reasoning.
- **Reflection:** Evaluates past actions to improve future decisions.

# Agentic AI

## The AI Evolution

- From **Rule-Based Systems** → **Machine Learning** → **Generative AI**  
→ **Agentic AI**

# Evolution of Intelligent AI Systems

From Chatbots → RAG → Tool-Based RAG → Agentic AI

## Traditional AI Chatbots (Pre-2023)

- **Core Idea:** Rule-based or intent-classification chat systems.
- **Technology:** NLP + dialog trees + static responses.
- **Limitations:** No context retention, no external data, no reasoning.
- **Example:** FAQ bots, customer-support flows.

# Evolution of Intelligent AI Systems

From Chatbots → RAG → Tool-Based RAG → Agentic AI

## Retrieval-Augmented Generation (RAG)

- **Core Idea:** Combine LLM + knowledge retrieval.
- **Pipeline:**
  - User query
  - Retrieve relevant documents (vector DB)
  - Generate answer using context
- **Benefits:** Up-to-date, domain-specific, explainable.
- **Example:** Enterprise document assistants, research QA bots.

# Evolution of Intelligent AI Systems

From Chatbots → RAG → Tool-Based RAG → Agentic AI

## Tool-Based RAG / Function-Calling Systems


- **Core Idea:** LLMs use external **tools & APIs** for reasoning and actions.
- **Capabilities:**
  - Call Python code, SQL, search APIs.
  - Integrate retrieval + computation.
- **Example:** Data-analysis bots, multi-source assistants (e.g., ChatGPT + browser).

# Evolution of Intelligent AI Systems

From Chatbots → RAG → Tool-Based RAG → Agentic AI

## Agentic AI (2024 → Now)

- **Core Idea:** Autonomous, goal-oriented systems using **memory**, **planning**, and **multi-agent collaboration**.
- **Features:**
  - Task decomposition and self-reflection.
  - Dynamic tool use and feedback loops.
  - Long-term state and multi-modal capabilities.
- **Example:** AI research agents, AI tutors, workflow executors

**HR Assistant** 

How many vacation days do we get per year?

You get 20 vacation days per year.

What is the policy on sick leave?

You get 10 paid sick days per year. A doctor's note is needed if you're out for more than 2 days.

Type your message here...

Send

## HR Assistant

How many vacation days do we get per year?

You get 20 vacation days per year.

What is the policy on sick leave?

You get 10 paid sick days per year. A doctor's note is needed if you're out for more than 2 days.

Type your message here...

Send

## RAG Chatbot

LLM



## RAG Chatbot

Question

LLM

Answer



## HR Assistant

How many leaves do I have left this year?

You have 7 leave days remaining this year

Apply for 2 days of casual leave on May 5 and 6

Your 2-day casual leave for May 5 and 6 has been successfully applied.

Type your message here...

Send

## HR Assistant 🧑

How many leaves do I have left this year?

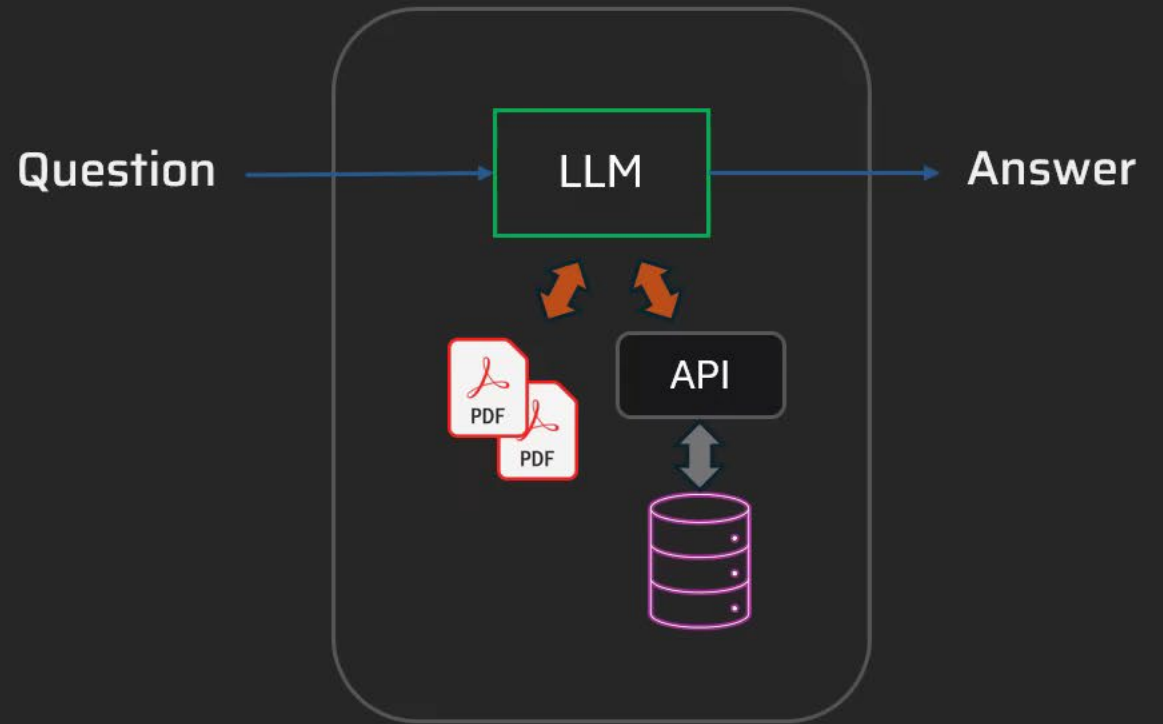
You have 7 leave days remaining this year

Apply for 2 days of casual leave on May 5 and 6

Your 2-day casual leave for May 5 and 6 has been successfully applied.

Type your message here...

Send



## HR Assistant

How many leaves do I have left this year?

You have 7 leave days remaining this year

Apply for 2 days of casual leave on May 5 and 6

Your 2-day casual leave for May 5 and 6 has been successfully applied.

Type your message here...

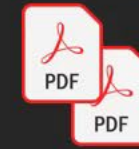
Send

## Tool Augmented Chatbot

Question

LLM

Answer



API



## HR Assistant

Prepare for Sarah's maternity leave.

I've reviewed Sarah's due date and workload. A transition plan has been drafted, backup resources identified, and a handover meeting scheduled for next Monday.

d the new intern joining next Monday,

Send

## HR Assistant

I've reviewed Sarah's due date and workload. A transition plan has been drafted, backup resources identified, and a handover meeting scheduled for next Monday.

Onboard the new intern joining next Monday.

I've prepared the onboarding checklist, scheduled a welcome meeting, and sent access requests to IT. The intern's welcome kit has also been ordered.

Type your message here...

Send

Onboard the new intern joining next Monday. *z good*

Schedule welcome meeting



LLM

Onboard the new intern joining next Monday. *Good*

Schedule welcome meeting



LLM

Create intern's profile in HR Management System



LLM

IT Helpdesk (Wi-Fi credentials, Email, Slack access)



LLM

Onboard the new intern joining next Monday. *Good*

Schedule welcome meeting



LLM

Create intern's profile in HR Management System



LLM

IT Helpdesk (Wi-Fi credentials, Email, Slack access)



LLM

Order Laptop, ID Card



LLM

Onboard the new intern joining next Monday. *Goal*

Goal Oriented  
Planning

Schedule welcome meeting



LLM

Create intern's profile in HR Management System



LLM

IT Helpdesk (Wi-Fi credentials, Email, Slack access)



LLM

Order Laptop, ID Card



LLM

Onboard the new intern joining next Monday. *Goal*

Schedule welcome meeting



LLM

Create intern's profile in HR Management System



LLM

IT Helpdesk (Wi-Fi credentials, Email, Slack access)



LLM

Order Laptop, ID Card



LLM

Goal Oriented  
Planning

Multi-step  
Reasoning

Onboard the new intern joining next Monday. *Goal*

Schedule welcome meeting



LLM

Create intern's profile in HR Management System



LLM

IT Helpdesk (Wi-Fi credentials, Email, Slack access)



LLM

Order Laptop, ID Card



LLM

Goal Oriented  
Planning

Multi-step  
Reasoning

Autonomous  
Decision Making

Onboard the new intern joining next Monday. *Goal*

Schedule welcome meeting



LLM

Create intern's profile in HR Management System



LLM

IT Helpdesk (Wi-Fi credentials, Email, Slack access)



LLM

Order Laptop, ID Card



LLM

Goal Oriented  
Planning

Multi-step  
Reasoning

Autonomous  
Decision Making

Tool, Knowledge,  
Memory

## HR Assistant 🧑

I've reviewed Sarah's due date and workload. A transition plan has been drafted, backup resources identified, and a handover meeting scheduled for next Monday.

Onboard the new intern joining next Monday.

I've prepared the onboarding checklist, scheduled a welcome meeting, and sent access requests to IT. The intern's welcome kit has also been ordered.

Type your message here...

Send

## Agentic Chatbot

Question

LLM

Answer

API

Calendar

One Drive





Expedia



Book me the cheapest  
Emirates flight from New  
York to Delhi tomorrow?



1. Searches Flights



Expedia



Book me the cheapest  
Emirates flight from New  
York to Delhi tomorrow?



1. Searches Flights

2. Decides the cheapest one



Expedia



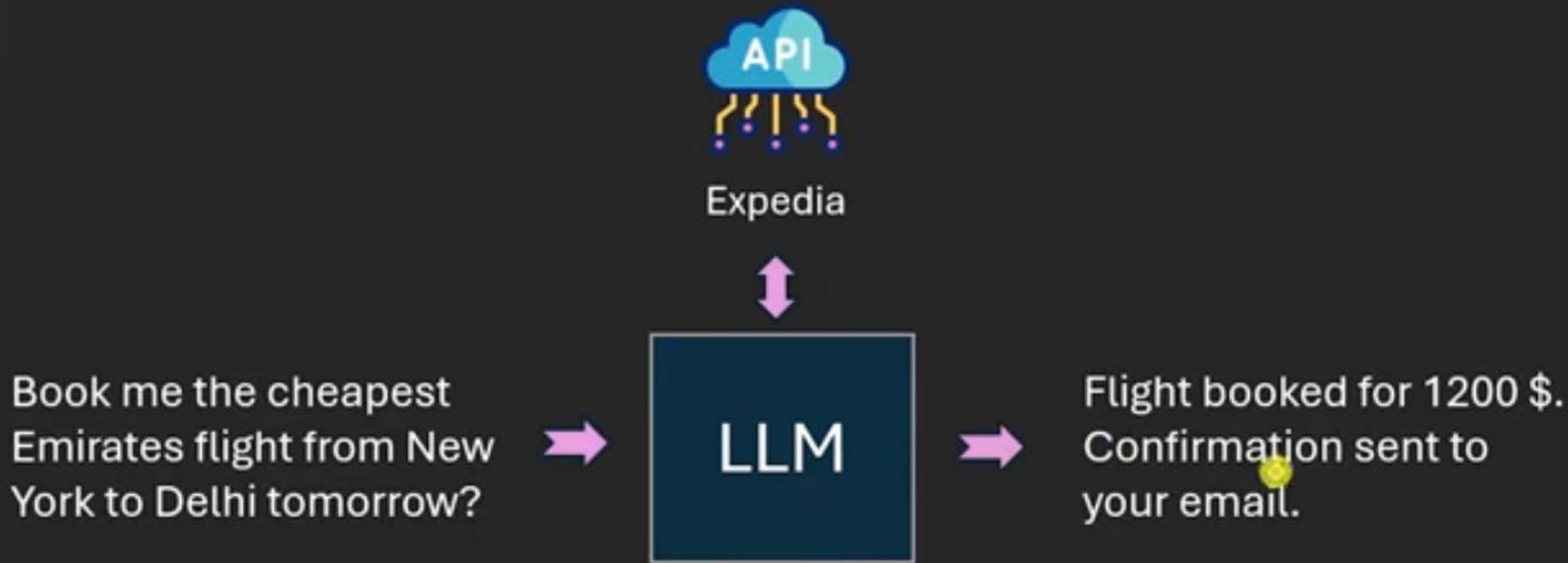
Book me the cheapest  
Emirates flight from New  
York to Delhi tomorrow?



1. Searches Flights

2. Decides the cheapest one

3. Books it



1. Searches Flights

2. Decides the cheapest one

3. Books it



Expedia



Book me the cheapest  
Emirates flight from New  
York to Delhi tomorrow?



Flight booked for 1200 \$.  
Confirmation sent to  
your email.

AI Agent

1. Searches Flights

2. Decides the cheapest one

3. Books it

**Agentic AI** is an AI system that can make decisions and take actions on its own to achieve a goal without being told exactly what to do at every step.



# AI Coding

Create a react native app similar to todoist

focus-today-tasks

Create a react native app similar to todoist

Lovable 06:55 on Apr 09, 2025

I'm excited to help you build a beautiful to-do app inspired by Todoist! Let's create a clean, focused task management application with a modern design.

For this app, I'll draw inspiration from Todoist's minimal and functional interface, with a color palette that uses calming blues and neutrals for focus, complemented by accent colors for priorities and categories.

**Features for our first version:**

- Task creation, editing, and deletion
- Task priority levels (high, medium, low)
- Task categories/projects
- Due dates for tasks

Ask Lovable...

Attach Edit Chat

Focus Tasks

New Task

Projects +

All Tasks

All Tasks

Personal

Work

Shopping

All Tasks

0 tasks

No tasks here yet  
Add a new task to get started

# Agentic AI System Example



Travel  
Assistant

Book a 7 day trip to London in May when the weather is sunny for at least 4 days. Book the flights with minimum flight duration. Budget < 1000\$

# Agentic AI System Example



## Travel Assistant

Book a 7 day trip to London in May when the weather is sunny for at least 4 days. Book the flights with minimum flight duration. Budget < 1000\$

Create a plan.

1. I need to first check weather to find a week that has 4 sunny days
2. Find out person's current location
3. From current location to London find flights with less than 1000\$ budget
4. Sort them by flight duration and suggest flight with min duration



Call accuweather api: location=London, month=may



May 10 to 17

Call Expedia api. Departure: JFK, Arrival: LHR, Date: 2024-05-10 to 2024-05-17



...

# Workshop Roadmap

## We Will Build

### Demo 1

- AI SOC Log Analyst using n8n

### Demo 2

- AI Phishing Email Detector

### Demo 3

- AI Driven Security Alert Prioritization

### Demo 4

- CrewAI Multi-Agent Security System

### Demo-5

- CrewAI Multi-Agent Security System

# What is a SOC?

## Security Operations Center

A SOC is responsible for:

- Monitoring security events
- Detecting cyber attacks
- Investigating incidents
- Coordinating responses
- Protecting organizational infrastructure

# Common Cyber Attacks

## Examples

### Brute Force

- Repeated login attempts

### Phishing

- Fake credential theft emails

### Malware

- Malicious code execution

### Insider Threats

- Unauthorized internal actions

### Data Exfiltration

- Sensitive data leakage

# Demo 1 Overview

## AI SOC Log Analyst

- **Workflow**
- Logs → OpenAI → Risk Decision → Alert

## Technologies

- n8n
- OpenAI
- Gmail alerts
- Conditional logic

Manual Trigger

↓

Security Logs

↓

OpenAI Analysis

↓

Risk Decision

↓

Alert System

# Why n8n?

## n8n Advantages

- Visual workflow automation
- Easy AI integration
- Real-time orchestration
- Low-code architecture
- Fast prototyping for SOC systems

# Resources and NoteBooks

- <https://tinyurl.com/AgenticAICyber>

# Transition to Phishing Detection

## Next Challenge

- Email-based attacks remain the #1 attack vector worldwide.

## AI Phishing Email Detector

### Workflow

- Email → OpenAI → Classification → Alert

# Demo 3: SOC Triage Simulator

## Concept

- Multiple events → AI prioritization → operational decisions

## Security Event Batch

- Failed login attempts
- PowerShell execution
- Large external upload
- Normal VPN login
- Password resets
- Ping sweep activity

# Demo 3: SOC Triage Simulator

## AI Risk Prioritization

### AI Tasks

- Classify events
- Assign risk score
- Rank incidents
- Recommend escalation

Event	Risk
PowerShell attack	10/10
Data exfiltration	9/10
Ping sweep	6/10
VPN login	1/10

# Transition to Multi-Agent AI

## Real SOC Teams Have Specialists

- Security operations require multiple expert roles.
- So should AI systems.

## CrewAI Multi-Agent SOC

### Agents

- SOC Analyst
- Threat Intelligence
- Incident Responder
- Report Generator
- Email Notification Agent

# Transition to Multi-Agent AI

Logs



SOC Analyst



Threat Intelligence



Incident Response



Executive Report



Email Notification

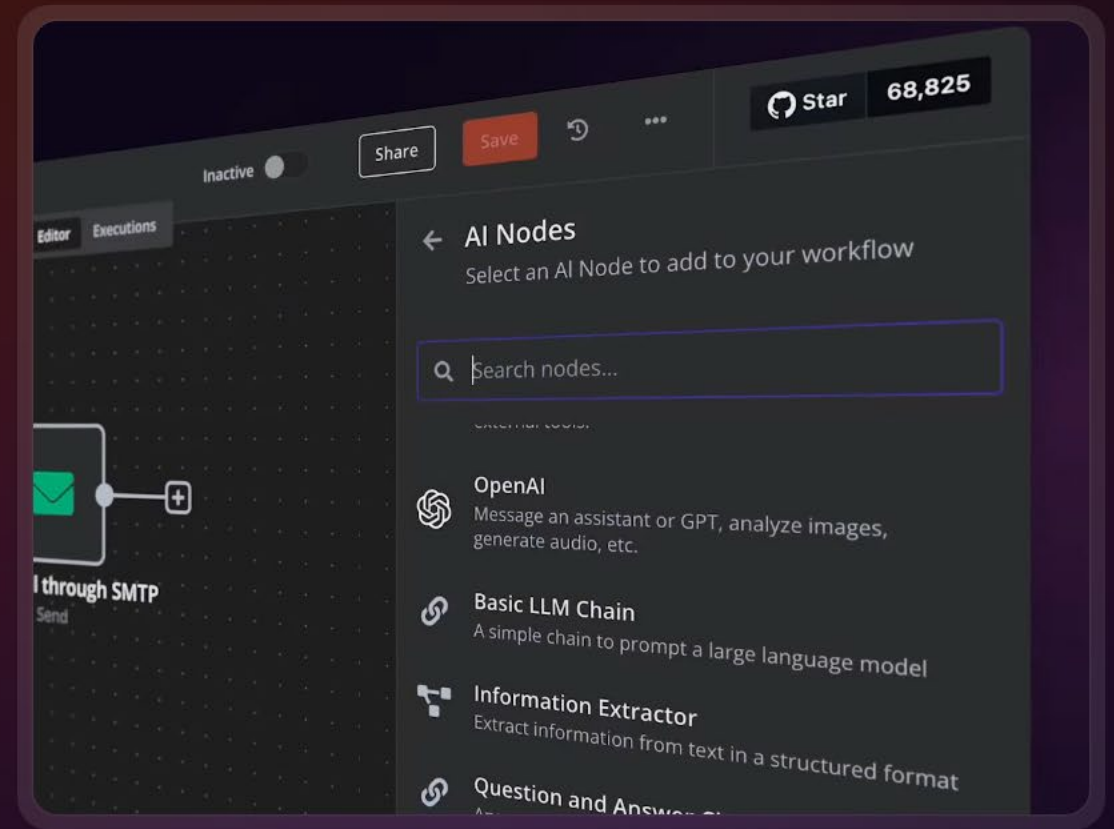
# n8n AI agent builder

## Build AI agents that work predictably in prod

Source availability, 500+ integrations, and support for code give you the flexibility to connect AI models to your business systems at scale. Human-in-the-loop guardrails and the ability to add pre-defined logic give you the confidence they won't fail.

[Start building AI agents\\*](#) [Talk to sales](#)

\*14-day free trial. No credit card needed



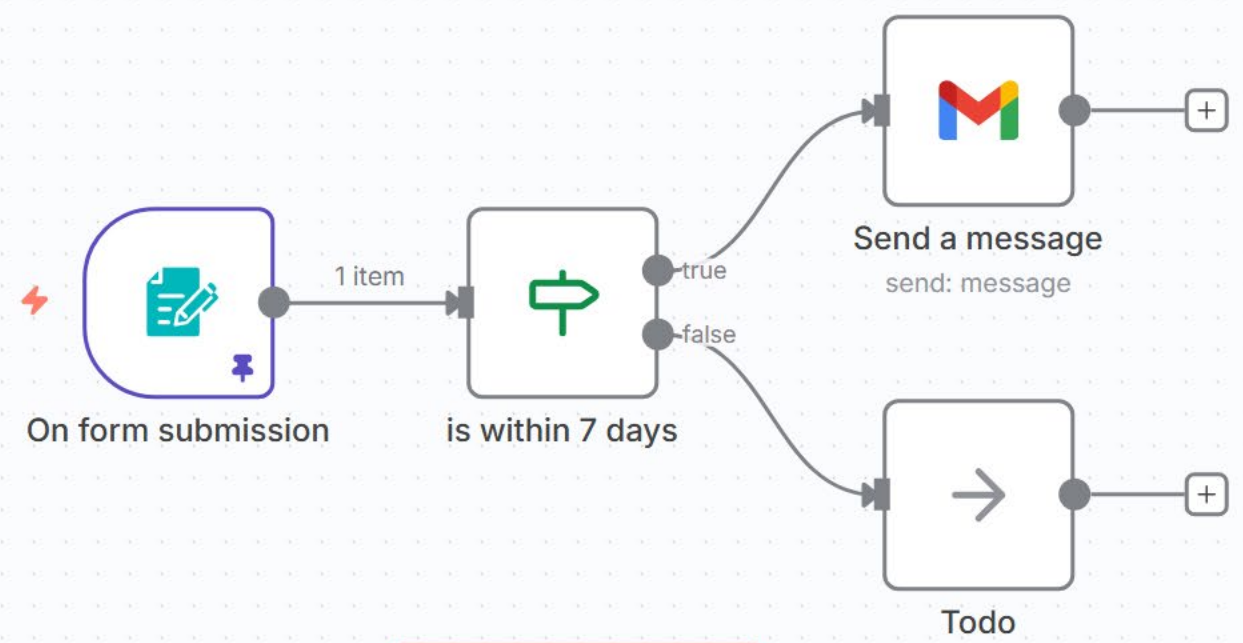
13 days left in your n8n trial | 3/1000 Executions

[Upgrade now](#)

Personal / My workflow + Add tag

0 / 2 Active  Share Saved

Editor Executions Evaluations



[Execute workflow](#)

Zoom and view controls: Full screen, Zoom in, Zoom out, Erase

PK  
Logs

13 days left in your n8n trial | 3/1000 Executions

[Upgrade now](#)

Personal / My workflow 2 + Add tag

Inactive  [Share](#) [Save](#)

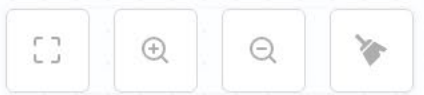
**Editor** Executions Evaluations



or

Add first step...

Build with AI



Logs

### What triggers this workflow?

A trigger is a step that starts your workflow

- On a schedule**  
Runs the flow every day, hour, or custom interval
- On webhook call**  
Runs the flow on receiving an HTTP request
- On form submission**  
Generate webforms in n8n and pass their responses to the workflow
- When executed by another workflow**  
Runs the flow when called by the Execute Workflow node from a different workflow
- On chat message**  
Runs the flow when a user sends a chat message. For use with AI nodes

← Back to canvas

13 days left in your n8n trial | 3/1000 Executions

Upgrade now

### On form submission

[Execute step](#)

**Parameters** Settings Docs

Form URLs

Test URL Production URL

<https://parteekumar.app.n8n.cloud/form-test/c33e783a-fe4e-46cb-968f-2420acc3475b>

Authentication: None

Form Title: e.g. Contact us

Form Description: e.g. We'll get back to you soon

Form Elements: Currently no items exist

Add Form Element

### OUTPUT

Execute this node to view data or **set mock data**

PK  
Logs

I wish this node would...

13 days left in your n8n trial | 3/1000 Executions

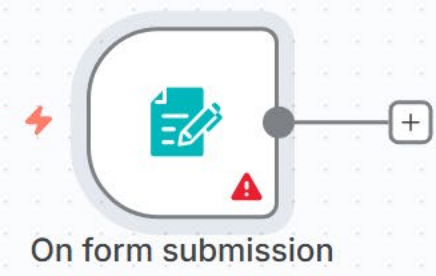
[Upgrade now](#)

Personal / My workflow 2 + Add tag

Inactive  [Share](#) [Save](#)

**Editor** Executions Evaluations

- + (Add node)
- Home icon
- Workflow icon
- + (Add node)
- > (Expand)
- Workflow icons
- PK (Profile)



- Fullscreen icon
- Zoom in icon
- Zoom out icon
- Pointer icon

[Execute workflow](#)

Logs

### What happens next?

- Action in an app**  
Do something in an app or service like Google Sheets, Telegram or Notion →
- Data transformation**  
Manipulate, filter or convert data →
- Flow**  
Branch, merge or loop the flow, etc. →
- Core**  
Run code, make HTTP requests, set webhooks, etc. →
- Human in the loop**  
Wait for approval or human input before continuing →

13 days left in your n8n trial | 3/1000 Executions

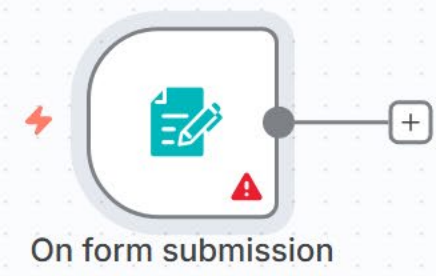
[Upgrade now](#)

Personal / My workflow 2 + Add tag

Inactive  [Share](#) [Save](#)

**Editor** Executions Evaluations

+  
Home  
Workflow  
+



[Execute workflow](#)

### Flow

Search nodes...

#### Popular

- Filter**  
Remove items matching a condition
- If**  
Route items to different branches (true/false)
- Loop Over Items (Split in Batches)**  
Split data into batches and iterate over each batch
- Merge**  
Merges data of multiple streams once data from both is available

#### Other

PK

Logs

**INPUT** Schema

On form submission

- T Email sanmeetkhatail.com
- T Install Date 2025-10-
- T submittedAt 2025-10-28T14:45:58-07:00
- T formMode test

Variables and context

### is within 7 days

**Parameters** Settings Docs

**Conditions**

fx `{{ $json['Install Date'] }}` is before or equal fx `{{ $now.plus(7, 'days') }}`

Add condition

Convert types where required

**Options**

No properties

Add option

Execute step

# Academic Contributions

## **Online Udemy Courses: 07**

- Number of Learners: 43000+
- Number of Countries: 160+
- Average Rating: 4.4

## **YouTube Channel:: Simplifying Computer Education**

- Subscribers: 27500+
- Videos: 500+
- Views: 10,35,000 +
- Watch Hours: 31000 +

**FDP and Workshops Conducted: 60+**



Courses start at ₹490 | Pick from thousands of instructors who practice what they teach. Ends March 4.  
**1 day left!**

IT & Software > IT Certifications > Artificial Intelligence

# Explainable AI (XAI) with Python

Simplified Way to Learn XAI

Hot & New 4.6 ★★★★★ (25 ratings) 1,282 students

Created by [Parateek Bhatia](#)

Last updated 1/2022 English English [Auto]



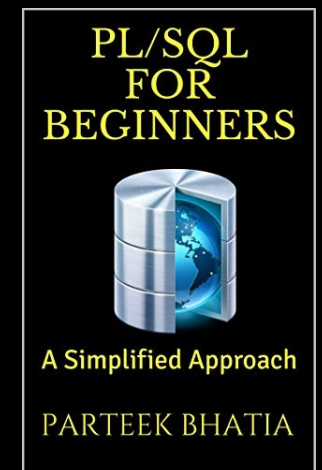
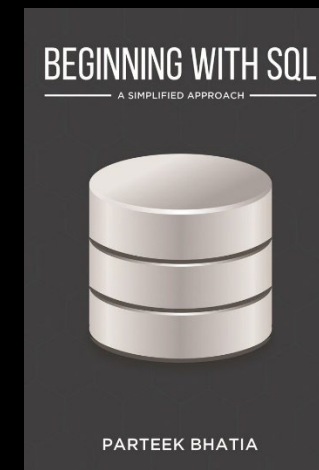
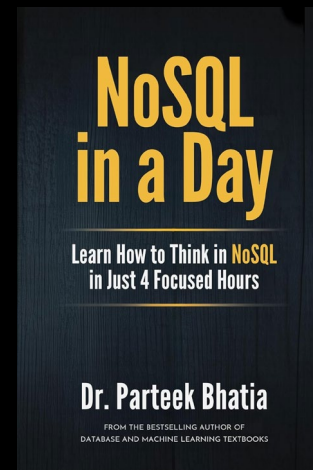
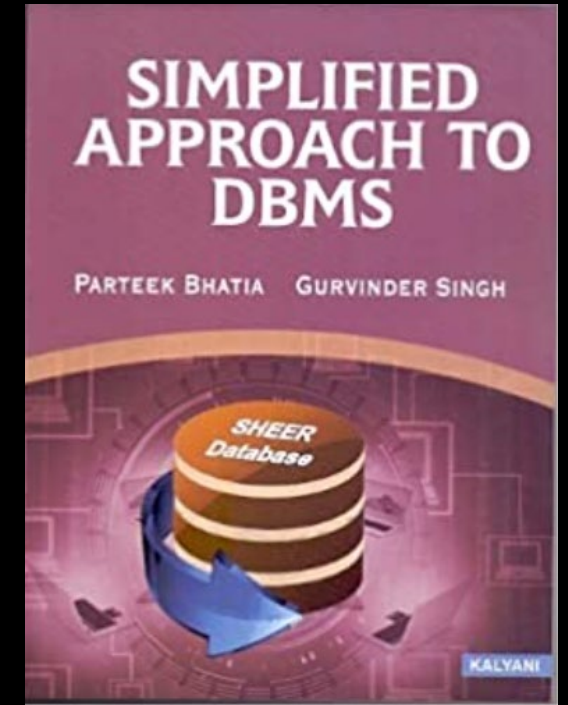
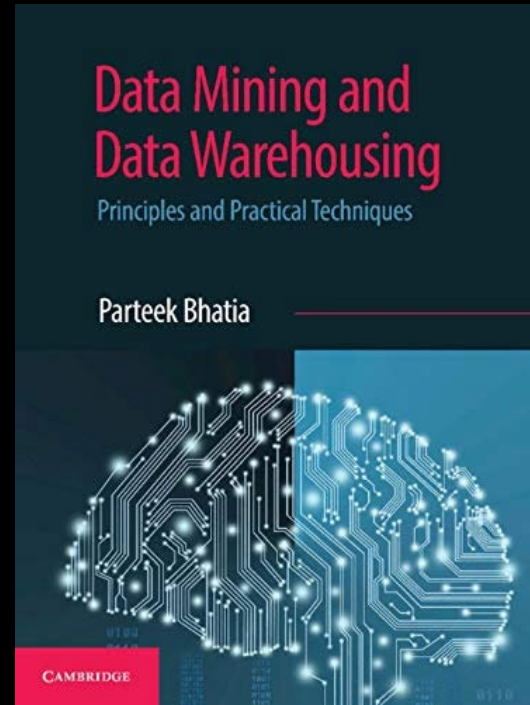
## What you'll learn

- ✓ Importance of XAI in modern world
- ✓ Categorization of XAI on the basis of their scope, agnosticity, data types and explanation techniques
- ✓ Application of InterpretML package from Microsoft to generate explanations of ML models
- ✓ Working principles and mathematical ;, SHAP,
- ✓ Differentiation of glass box, white box and black box ML models
- ✓ Trade-off between accuracy and interpretability
- ✓ Need of counterfactual and contrastive explanations
- ✓ Application of XAI techniques like LIME, SHAP, DiCE, LRP to generate explanations for

Waiting for gtm.udemy.com...

# Books

[www.parateekbhatia.com](http://www.parateekbhatia.com)





Thanks