Building Automation

This module introduces automation concepts and shows how AI-assisted scripting can support cybersecurity, audit, and IT operations.

Balaji Dinakaran
Corporate Trainer | Artificial Intelligence | Applied Machine Learning, LLMs & Agent Workflows

Module 1: Introduction to Automation

- What is automation?
- Types: No-code, low-code, and scripting-based
- Importance of automation in cybersecurity, audit, & IT ops
- Introduction to Copilot / AI-assisted automation

1. What is Automation?

- Automation means using technology to perform tasks with minimal human effort.
- Examples:
  - Auto-generating audit reports
  - Sending security alerts automatically
  - Automating server patching

2. Types of Automation

Type	Description	Examples
No-code	Drag-and-drop automation	Power Automate workflows
Low-code	Minimal scripting required	ServiceNow automation rules
Scripting-based	Full control using code	PowerShell, Python scripts

3. Importance in Cybersecurity, Audit & IT Ops

- Automation helps in:
  - Faster incident response
  - Continuous compliance checks
  - Reduced manual errors
  - Efficient SOC operations

4. Introduction to Copilot / AI-Assisted Automation

- AI tools like Microsoft Copilot can help:
  - Generate scripts quickly
  - Explain errors
  - Suggest improvements
  - Speed up workflow creation

Module 2: Foundations of Workflow Automation

Identifying Automatable Tasks

Workflow Basics

1. Identifying Automatable Tasks

- Good candidates:
  - Repetitive tasks
  - Rule-based actions
  - Data extraction/reporting
  - Alert notifications
- Examples:
  - Daily log review
  - Compliance evidence collection

2. Workflow Basics

Key components:

- **Trigger** → Event starts automation
- **Action** → Task performed automatically
- **Condition** → Logic (if/else)

Example:

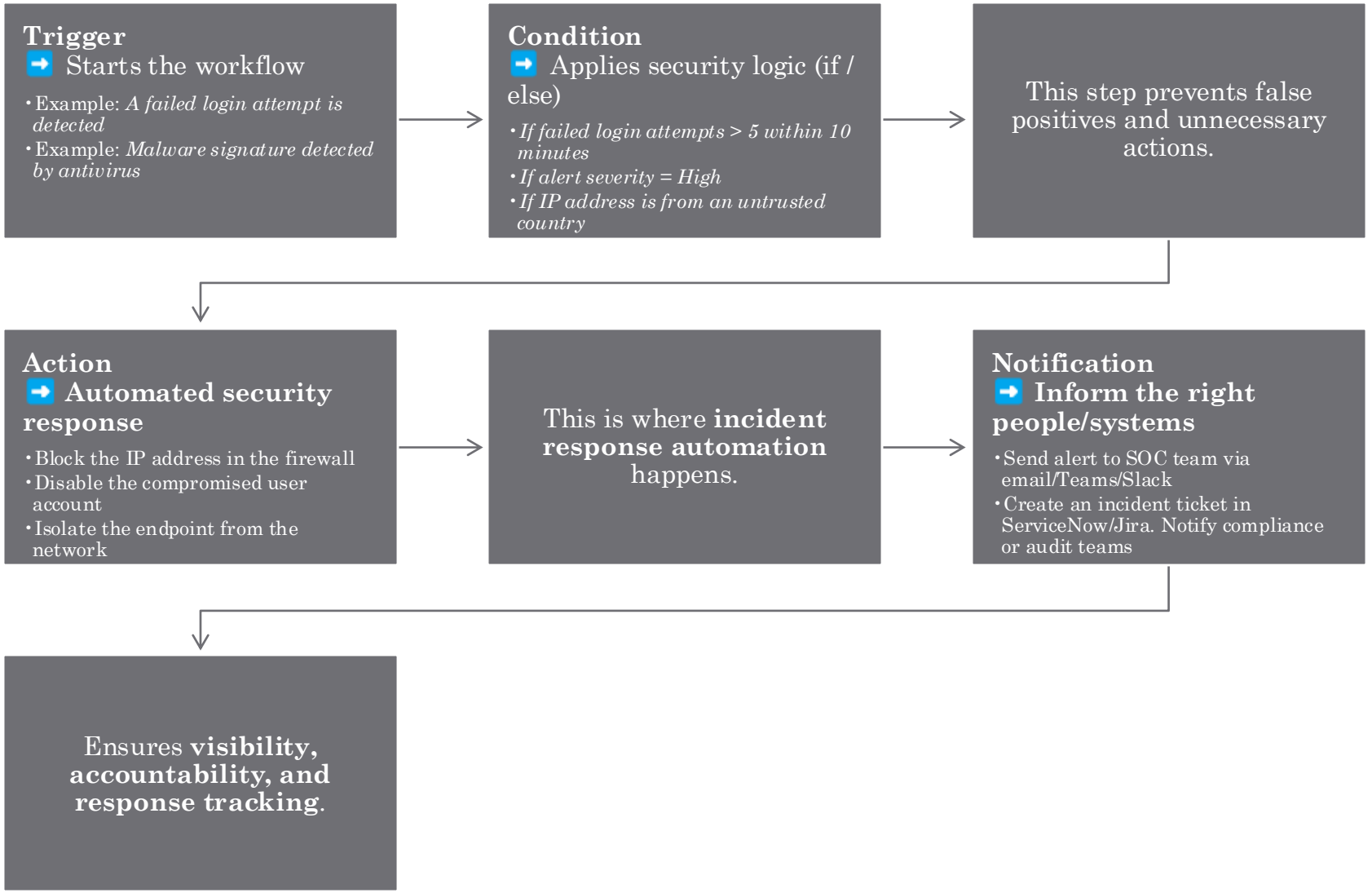
- Trigger: New phishing email detected
  Action: Notify SOC team + create ticket

- Note: A SOC is a centralized function or team responsible for improving an organization's cybersecurity posture and preventing, detecting, and responding to threats.

Workflow Sequence

- Trigger → Condition → Action → Notification
- Why:
  - A workflow always starts with a Trigger
  - Then (optionally) evaluates a Condition
  - Performs an Action
  - Ends with a Notification or outcome

Workflow Sequence



Hands-on Activity 1:

Automated Incident Evidence Collector (Audit + SOC)

- **Scenario**
  - A new security incident is reported. The SOC needs evidence immediately.
- **Workflow**
  - **Trigger:** Incident created (manual or form submission)
- **Actions:**
  - Collect system logs automatically
  - Export evidence into a folder
  - Notify SOC/Audit team
- **PowerShell Example Task**
  - Students build a script to:
  - Pull last 50 Security Event Logs
  - Save output as evidence file

  Workflow outcome: Evidence collection becomes automatic.

Hands-on Activity 2:

SQL-Based Suspicious Login Detection Workflow

- **Scenario**
  - SOC wants automation to detect brute-force attempts.
- Workflow Steps
  - **Trigger:** Daily scheduled run
  - **Action:** Query login database table
- SQL Example:

```
SELECT username, COUNT(*) AS failed_attempts
FROM login_logs
WHERE status = 'FAILED'
GROUP BY username
HAVING COUNT(*) > 5;
```

Then Action:

- Generate report
- Send to SOC mailbox

Hands-on Activity 3:

Automated User Access Review (IAM + Audit)

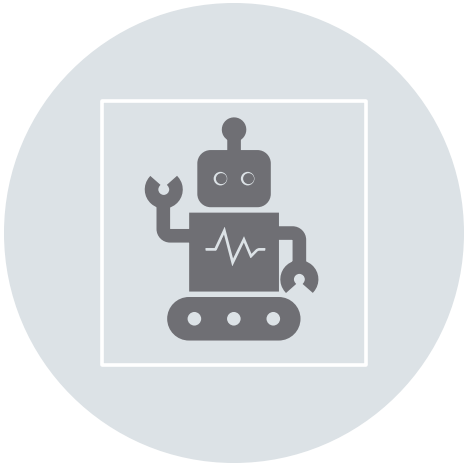
- **Scenario**
  - Audit team needs a monthly privileged access review.
  - Workflow
  - **Trigger:** Monthly schedule
- **Actions:**
  - Extract all Admin group members
  - Export to CSV
  - Send for manager review

Hands-on Activity 4:

Patch Compliance Check Automation

- Scenario
  - IT Ops needs to verify patch compliance weekly.
  - Workflow
- **Trigger:** Weekly scan
- **Action:** Check installed updates

Module 3: AI-Assisted Scripting Basics



USING AI TO GENERATE SCRIPTS (POWERSHELL, PYTHON)

DEBUGGING WITH AI

1. Using AI to Generate Scripts

1. AI can help create scripts in:
   - PowerShell
   - Python

Working with Copilot

1. Setup VS Code
2. Install Copilot extension
3. Understanding Ask, Agent, Plan

Working with Copilot - Agent and Plan

- Example prompt 1: Using Copilot Agent
  - Write a PowerShell script to extract failed login attempts from Windowslogs.
- Example prompt 2: Using Copilot plan and then agent
  - Scenario:
    An incident occurs and evidence must be collected immediately.
  - Workflow:
    Trigger:
    Incident is reported.
  - Actions:
    Collect relevant system and security logs.
    Collect a list of all installed patches/hotfixes.
    Save all collected evidence in a designated evidence folder.
    Notify the audit team that evidence has been collected and is available for review.
  - Objective:
    Ensure timely, consistent, and secure collection of digital evidence following an incident, supporting audit and investigation requirements.

2. Debugging with AI

- AI can:
  - Explain error messages
  - Fix syntax issues
  - Improve script readability

Module 4: Security & Audit Automation Use Cases

1. Automated email alerts
2. Evidence collection automation (We can use work done last module)
3. Report formatting automation
4. Compliance checks using templates

Module 5: Mini Lab + Assessment

- **Mini Lab Option : Failed Login Alert Automation (SOC Task)**
- Scenario
  - SOC wants an alert if multiple failed logins happen.
- Task 1
  - Create a PowerShell script that:
  - Get the 10 most recently installed hotfixes and export to HotFixes.csv
- Task 2
  - Create a python script:
  - Use csv module to read PSComputerName, HotFixID, Description from HotFixes.csv and print in the console for reference
  - Generate summary report HotFixesReport.txt by reading the HotFixes.csv using python
  - Review the generated output