Techonquer

# Security Operations Center (SOC) Course Syllabus (TCSA )

Master Cyber Defense with Cutting-Edge Skills and Tools

# Security Operations Center (SOC) Fundamentals

### Introduction

SOC importance, types, and tiers.

### Performance Monitoring

KPIs and metrics for SOC effectiveness.

# Threat Hunting and Threat Intelligence

## 1 Types of Threat Intelligence

Tactical, operational, and strategic.

## 2 MITRE ATT&CK

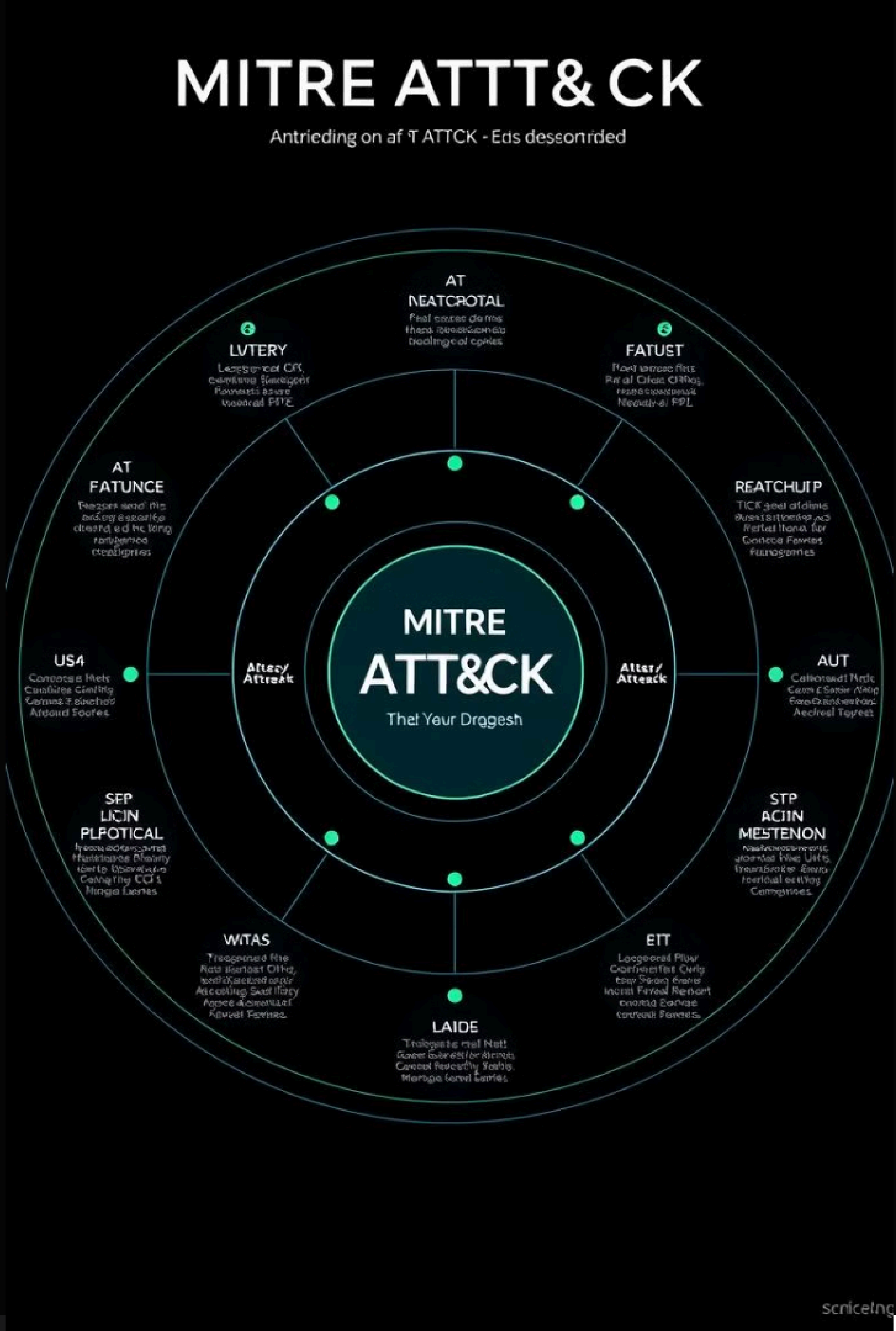
Framework for understanding attacker tactics and techniques.

## 3 Threat Hunting Techniques

Behavioral analysis and hypothesis-driven hunting.

## 4 Identifying IoCs

Hashes, domains, IPs, and URLs.



# Mastering SIEM Tools

## SIEM Architecture

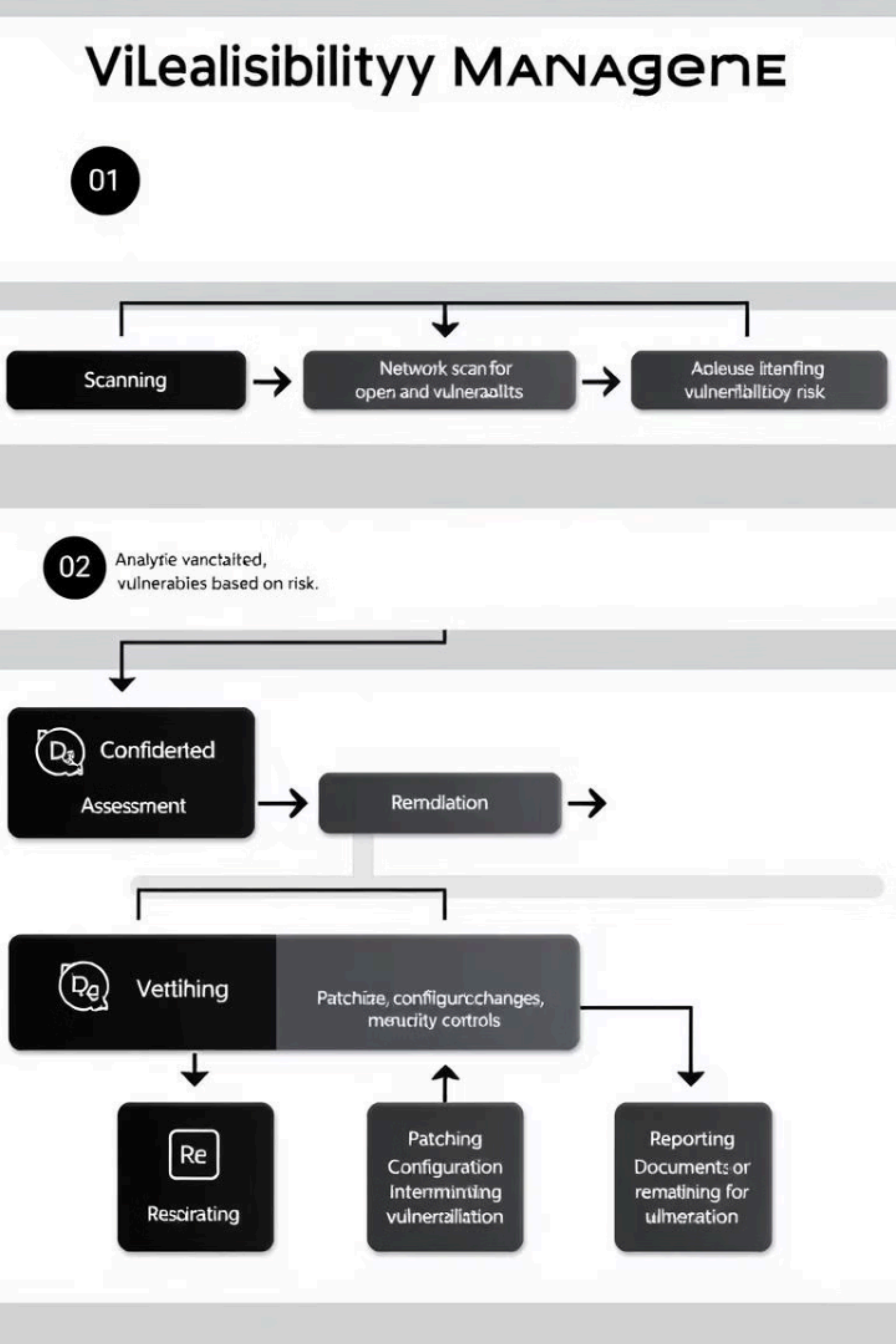
Log sources, correlation techniques, and use cases.

## Rule Creation

Fine-tuning and alert management.

## Hands-on

IBM QRadar and Splunk.


ViLealisibilityy MANAgeme
01
Scanning
Network scan for open and vulneraalits
Aoleuse litenfing vulnerilbilltioy risk
02
Analyfie vanctaited, vulnerabies based on risk.
Confiderted Assessment
Remdlation
Vettihing
Patchize, configurcchanges, meucity controls
Re
Resciating
Patching Configuration Interminting vulnerallation
Reporting Documents or remating for ulmeration

# Proactive Vulnerability Management

## Network Scans

Identify vulnerabilities in network devices.

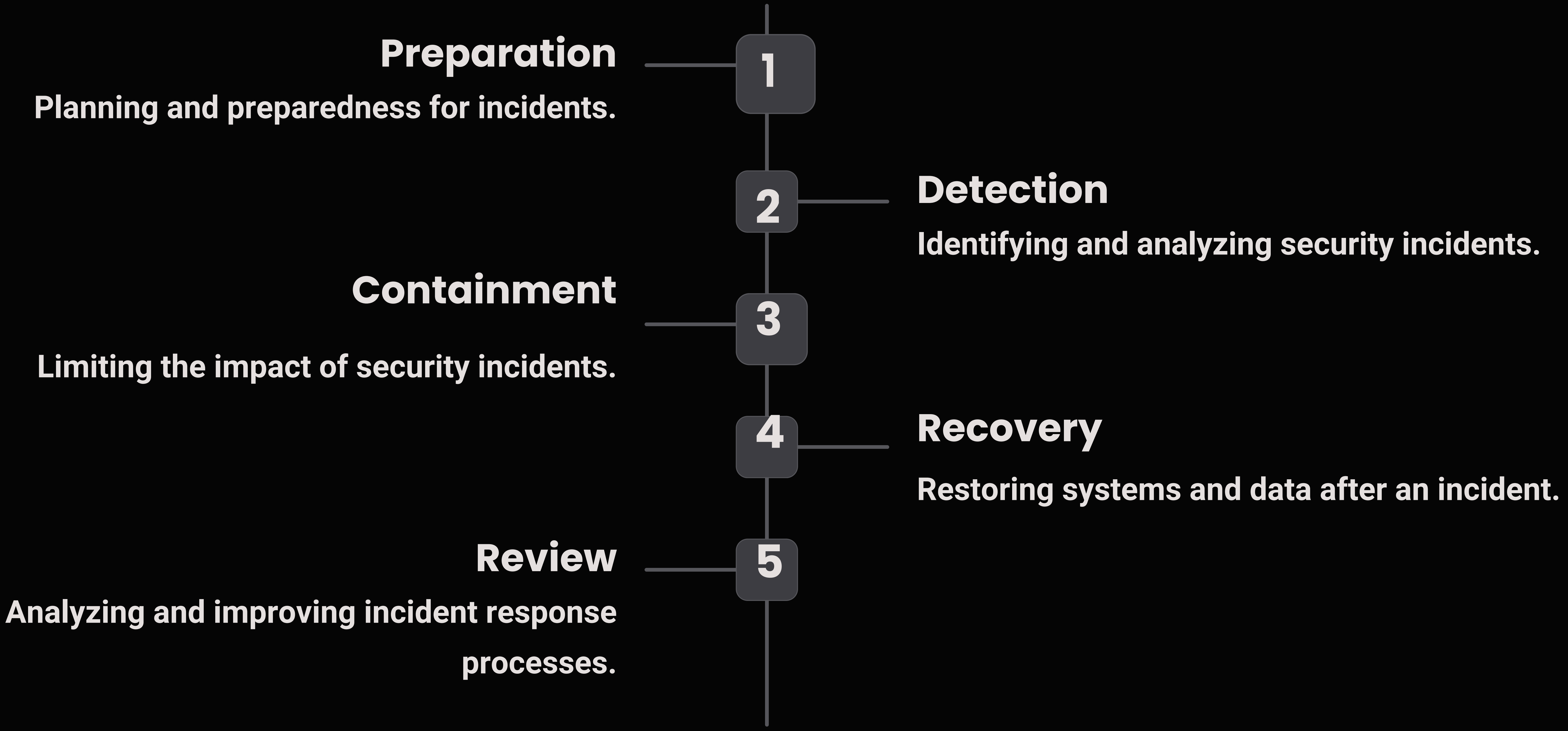
## Web Scans

Assess vulnerabilities in web applications.

## Cloud Scans

Identify vulnerabilities in cloud infrastructure.

# Incident Response and EDR



### Preparation

Planning and preparedness for incidents.

### Detection

Identifying and analyzing security incidents.

### Containment

Limiting the impact of security incidents.

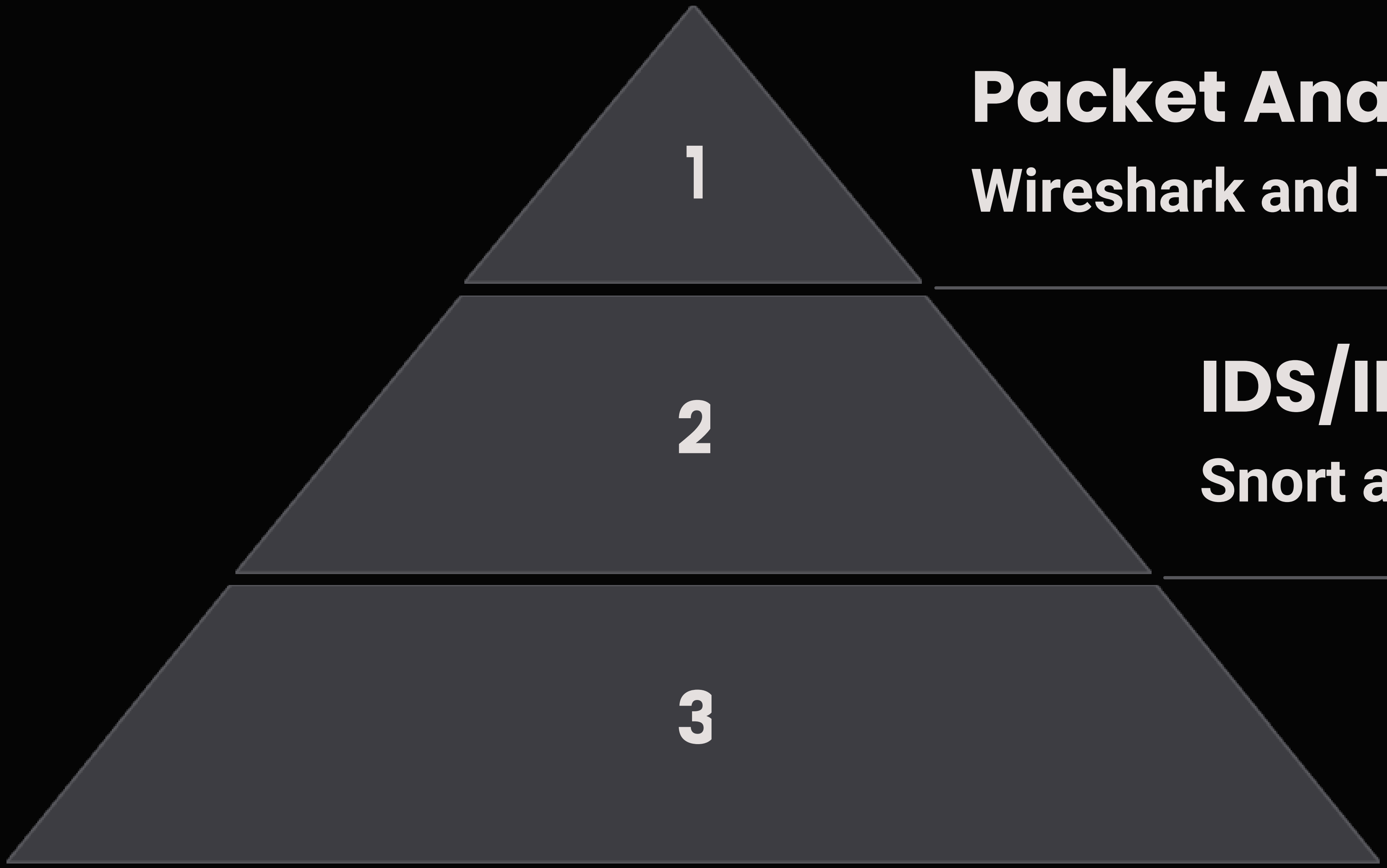
### Recovery

Restoring systems and data after an incident.

### Review

Analyzing and improving incident response processes.

# Network Security Monitoring and Automation



### Packet Analysis

Wireshark and Tcpdump.

### IDS/IPS

Snort and Suricata.

### SOAR

Automating alert triaging and playbook creation.

# Securing Cloud Environments

1

## Shared Responsibility

Understanding cloud security responsibilities.

2

## Common Threats

Identifying security risks in cloud environments.

3

## Tools

Scout Suite, Prowler, and Pacu.

4

## Logging

AWS CloudTrail and Azure Monitor.

# SOC Tools Mastery

### SIEM

IBM QRadar, Splunk.

### Vulnerability Scanning

Nessus, OpenVAS, Scout Suite.

### Threat Hunting

MITRE ATT&CK Navigator, MISP.

### EDR

Wazuh, Sophos

# Get in Touch

### Email
team@techonquer.org

### Phone
+91 6367098233

### Website
www.techonquer.org

### Location
Techonquer Pvt Ltd,
Bengaluru, Jaipur, India