



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.

3 Threat Hunting Techniques

Behavioral analysis and hypothesis-driven hunting.

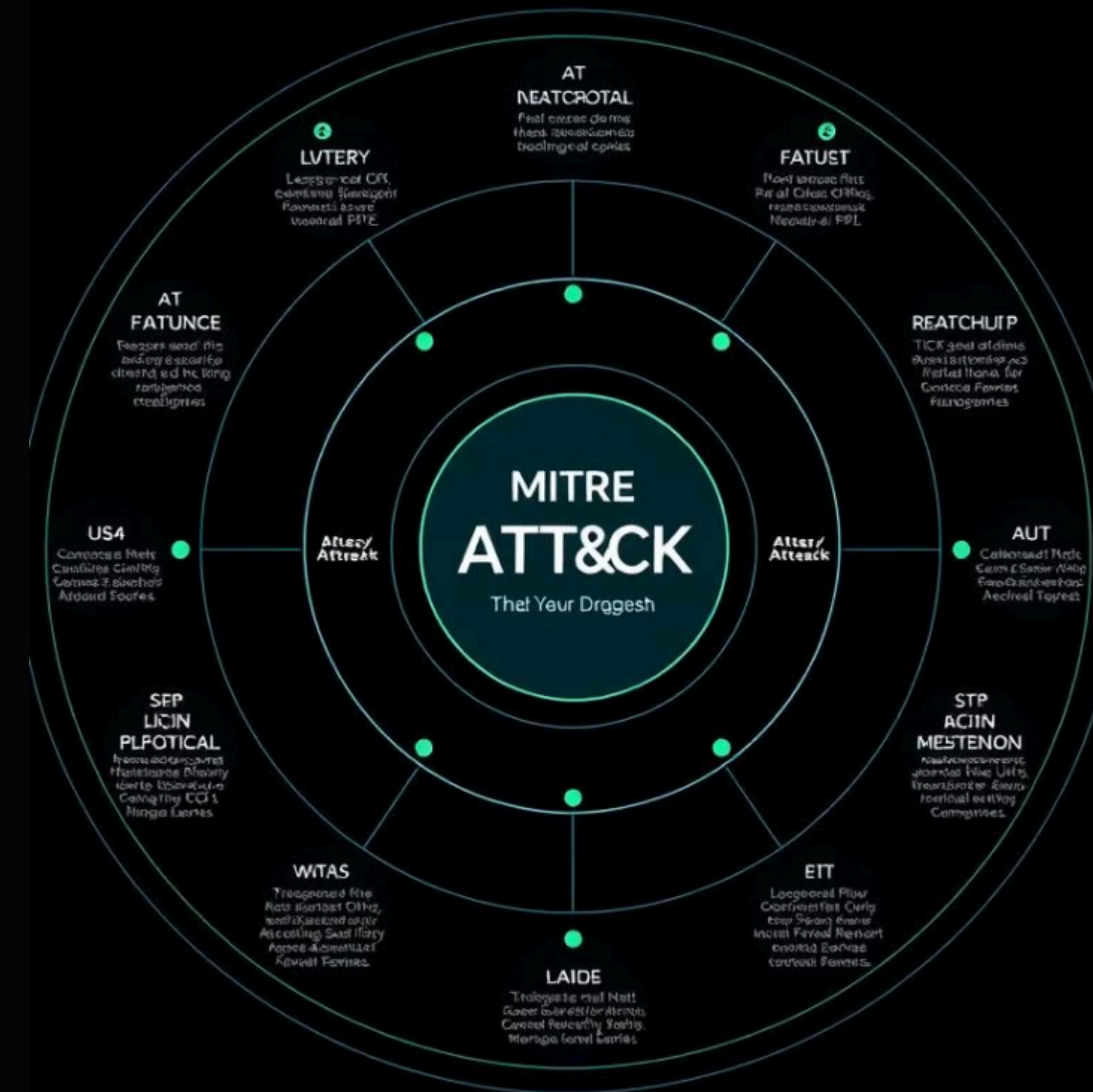
2 MITRE ATT&CK Framework for understanding attacker tactics and techniques.

4 Identifying IoCs

Hashes, domains, IPs, and URLs.

MITRE ATTT&CK

Antrieding on af T ATTCK - Eds dessonridd



Mastering SIEM Tools

SIEM Architecture

Log sources, correlation techniques, and use cases.

Rule Creation

Fine-tuning and alert management.

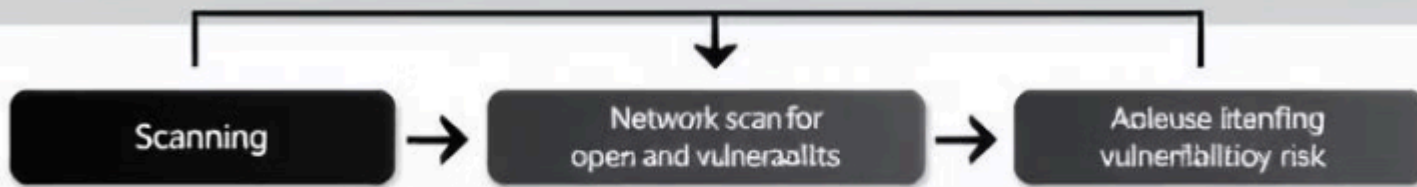
Hands-on

IBM QRadar and Splunk.



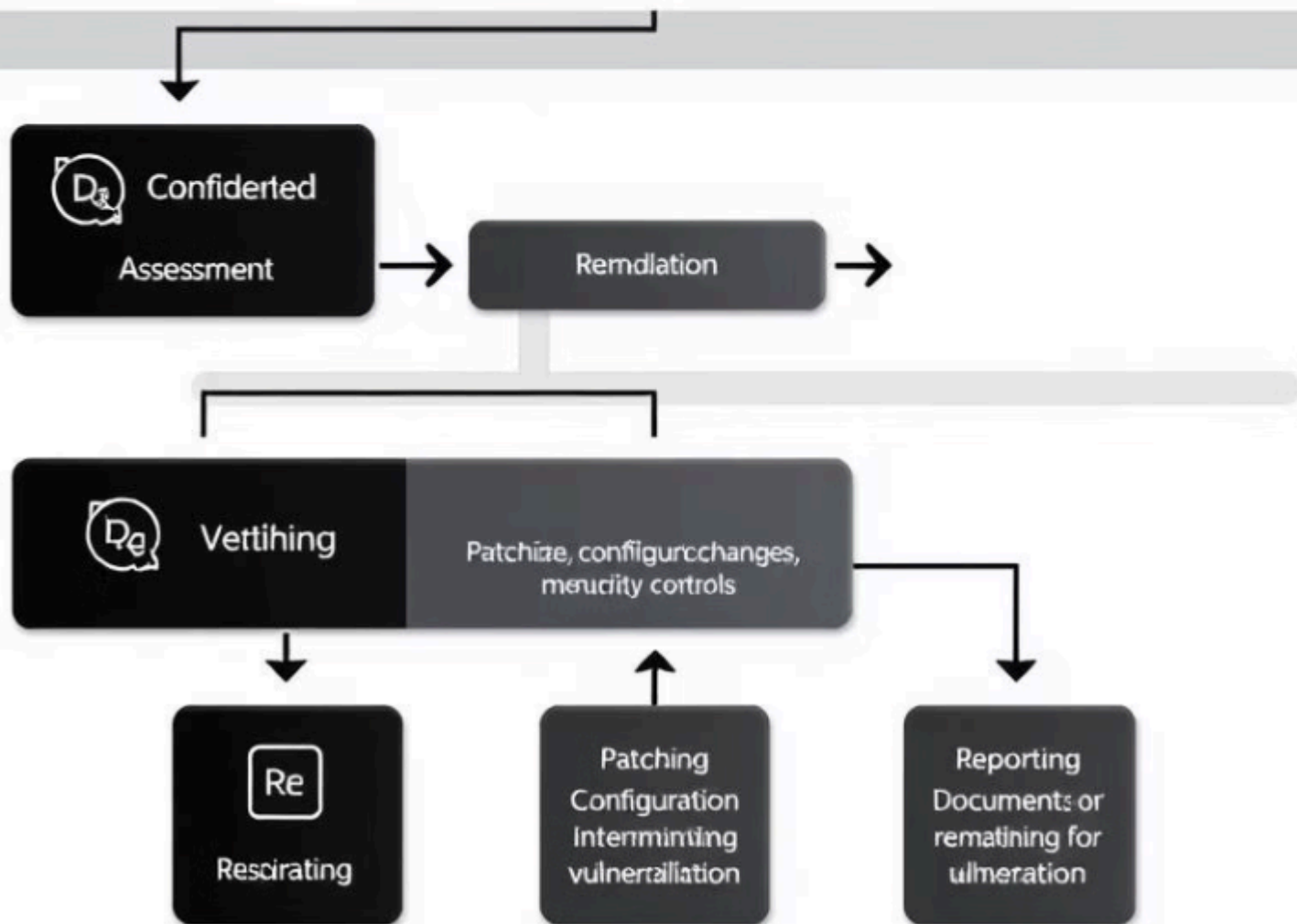
ViLealisibilityy MANAgene

01



02

Analyse validated, vulnerabilities based on risk.



Proactive Vulnerability Management



Network Scans

Identify vulnerabilities in network devices.



Web Scans

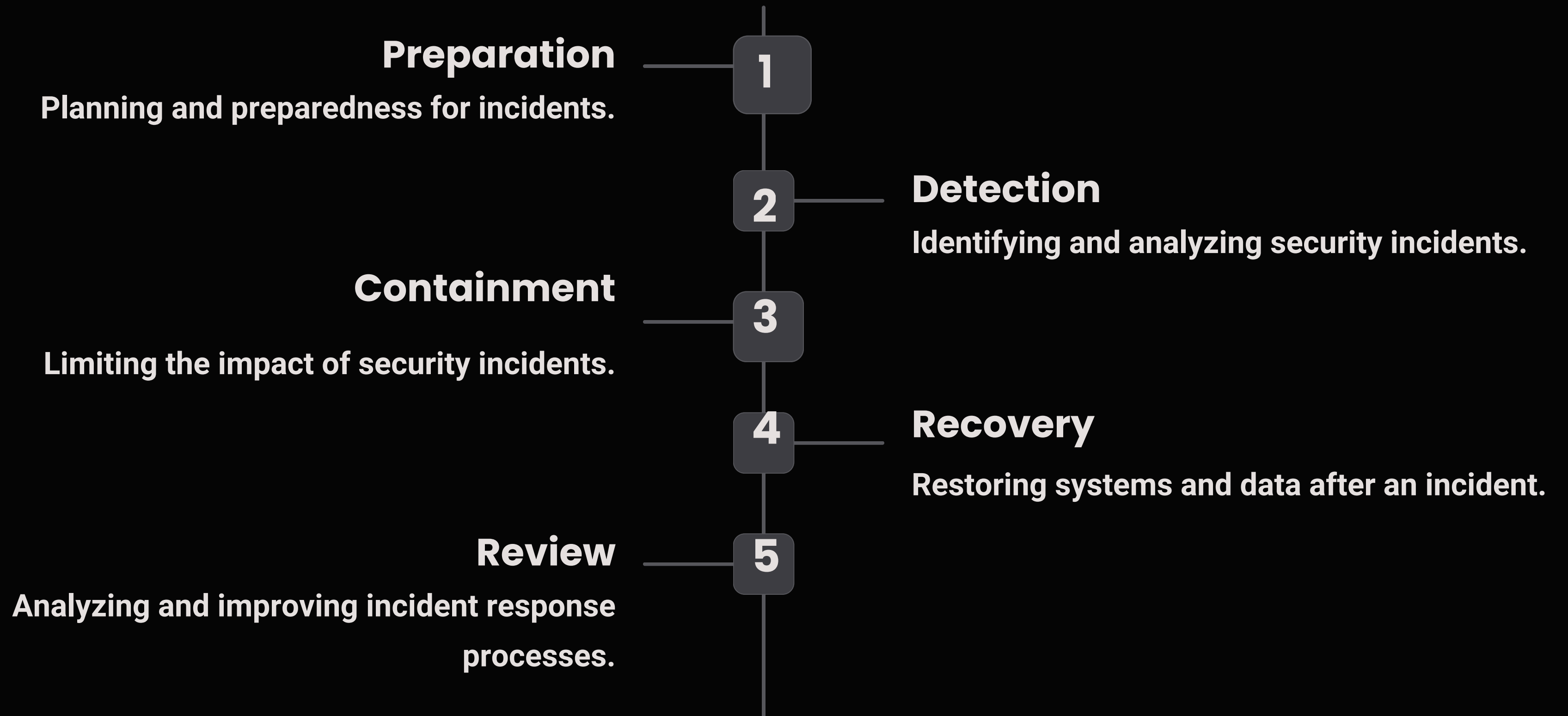
Assess vulnerabilities in web applications.



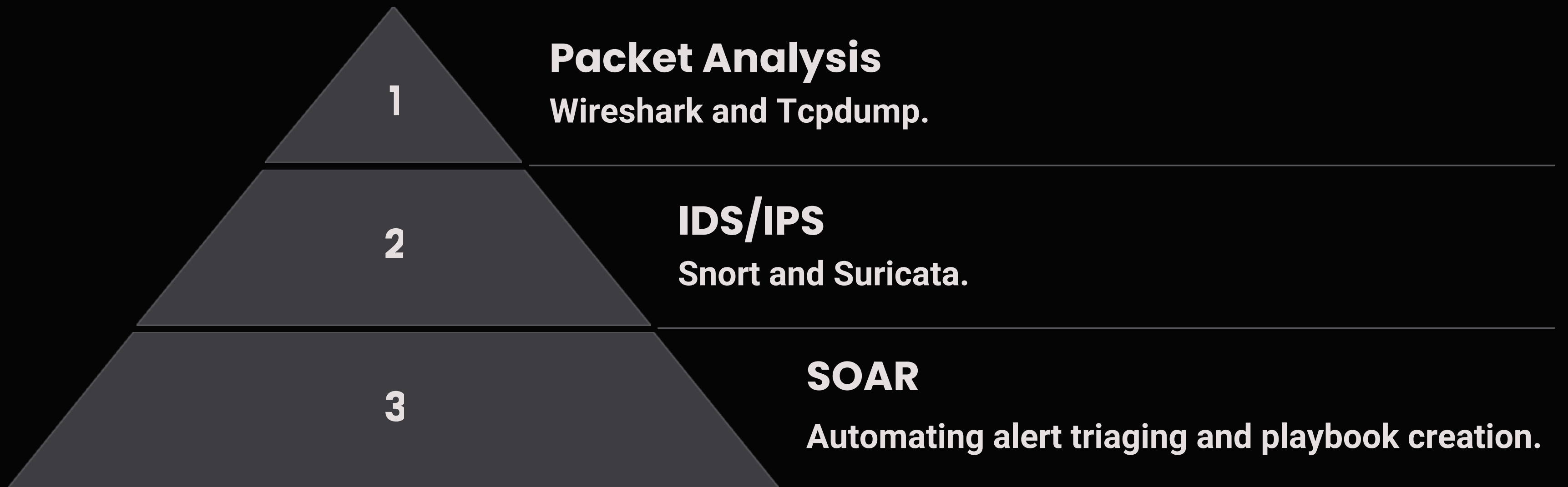
Cloud Scans

Identify vulnerabilities in cloud infrastructure.

Incident Response and EDR



Network Security Monitoring and Automation



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.

Nessus

Vulnerability Scanning

Nessus, OpenVAS, Scout Suite.

MITRE

ATT&CK

ATT&CCK
NAVIGATTOR

Threat Hunting

MITRE ATT&CK
Navigator, MISP.

wazuh

EDR

Wazuh, Sophos,
CrowdStrike.



Get in Touch



Email

team@techonquer.org



Phone

+91 6367098233



Website

www.techonquer.org



Location

Techonquer Pvt Ltd,
Bengaluru, Jaipur, India