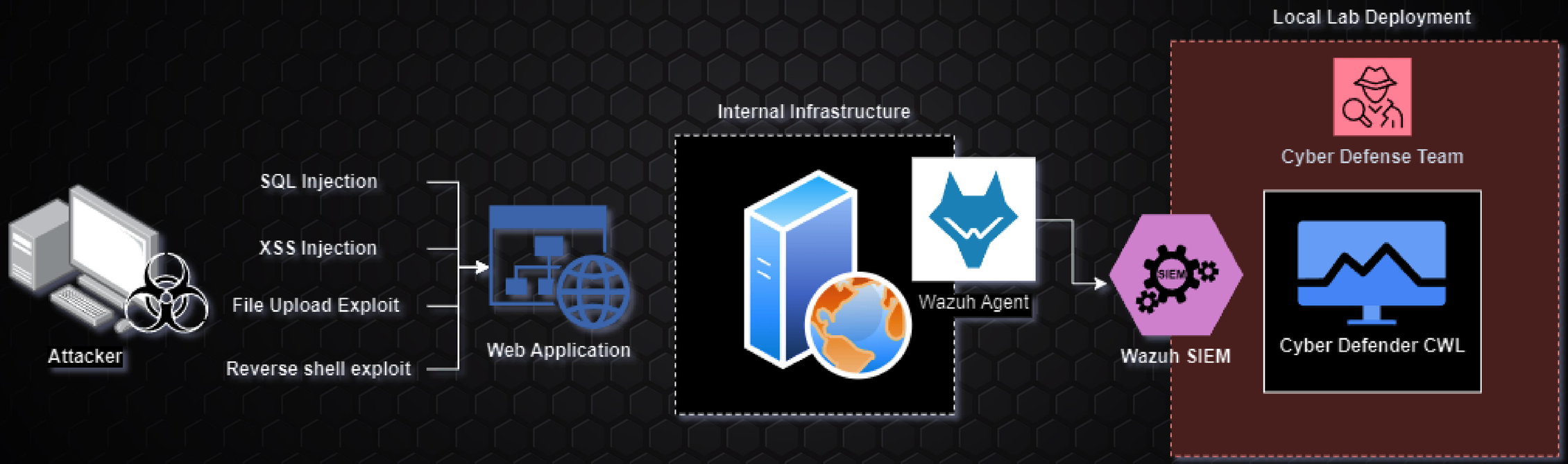
CWL
CyberWarFare Labs

Blue Team Fundamentals [BTF]

@CyberWarFare Labs

Blue Team Fundamentals [BTF] Architecture



CWL
CyberWarFare Labs

I. INTRODUCTION

II. INTRODUCTION TO CYBER OPERATIONS

2.1 General overview of SOC

2.2 Working behavior of SOC

2.3 Dedicated vs Virtual SOC

2.4 Tool & Technology

2.5 Incident Management & handling

2.6 First line of investigation

III. FOUNDATIONS OF CYBER THREAT ANALYSIS AND INTELLIGENCE

3.1 General overview of CTI

3.2 Cyber Threat Landscape

3.3 Common sources of CTI

3.4 Introduction to Threat Intel Portal | TIP

3.5 IOC Vs IOA

3.6 Pain Of Pyramid

IV. PROACTIVE CYBER THREAT HUNTING

4.1 General overview of CTH

4.2 Roles & Working of CTH

4.3 Proactive & Reactive approach

4.4 Foundational overview about MITRE ATT&CK framework

4.5 Cyber Kill Chain

V. INCIDENT RESPONSE STRATEGIES AND TECHNIQUES

5.1 General overview of IR

5.2 Key component of IR

5.3 Working of IR

5.4 IR Lifecycle

VI. UNVEILING THE SECRETS OF DIGITAL INVESTIGATIONS

6.1 General overview of digital forensics

6.2 Post incident analysis

6.3 Working of digital forensics

6.4 Evidence collection methodology

VII. Lab Exercise

7.1 Lab Set-up

7.2 Web based attack investigation

7.3 Network based attack investigation

7.4 Memory Forensics

CWL
CyberWarFare Labs

Thank You

Cyberwarfare.live