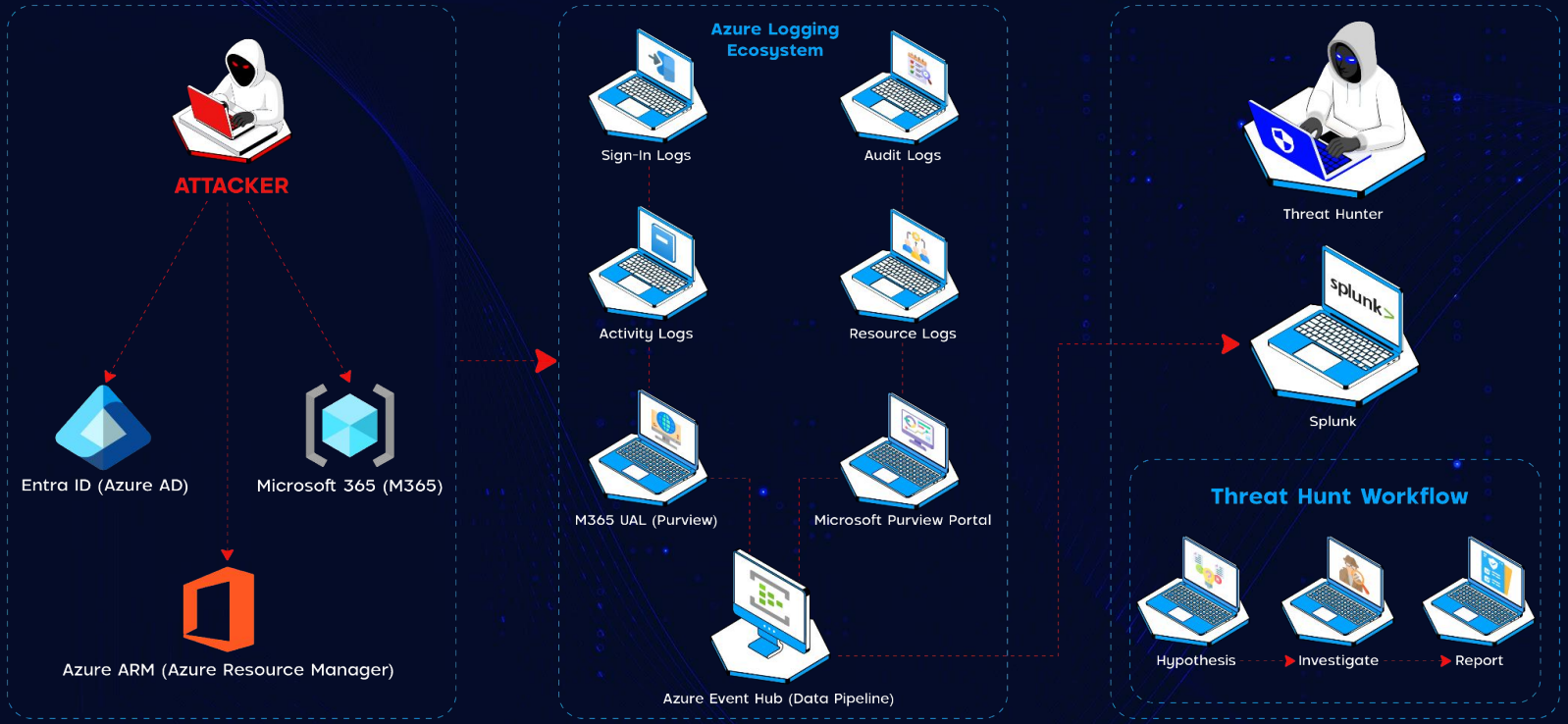
CWL
CyberWarFare Labs

Certified Azure Threat Hunter

CAz-TH

Certified Azure Threat Hunter - CAz-TH Lab Architecture



I. Fundamentals of Threat Hunting

1.1 What is Threat Hunting?

1.2 Where Threat Hunting Stands in the Organization

1.3 The Pyramid of Pain

1.4 Types of Threat Hunting

1.5 MITRE ATT&CK Framework and Navigator

1.6 Threat Hunting Maturity Model

1.7 How to Plan a Threat Hunt

II. Azure Cloud Fundamentals for Blue Teamers

2.1 Azure Cloud Architecture Overview
2.2 Microsoft Entra ID (Azure AD) Fundamentals
2.3 Fundamentals of Azure Resource Manager (ARM)
2.4 365 Fundamentals
2.5 Azure Logging Ecosystem:
    2.5.1 Sign-in Logs
    2.5.2 Audit Logs
    2.5.3 Activity Logs
    2.5.4 Resource Logs
    2.5.5 M365 Logging
2.6 Unified Audit Log (UAL)
2.7 Inbuilt Security Services in Azure Cloud

III. Environment Setup & Tooling

3.1 Deploying and Configuring Splunk (SIEM) for Azure

3.2 Data Integration: Routing Azure Logs to Splunk

IV. Azure Attack Investigations

4.1 Entra ID Attack Investigation [Attack Path 1]

4.2 Entra ID Attack Investigation [Attack Path 2]

4.3 ARM Attack Investigation

4.4 Office 365 Attack Investigation

V. Operationalizing Threat Hunting & Incident Response

5.1 Containment Strategies for Azure Resources

5.2 Identity Remediation and Token Revocation

5.3 Threat Eradication and Persistence Removal

5.4 Introduction to SOAR and Playbook Automation

CWL
CyberWarFare Labs

THANK YOU