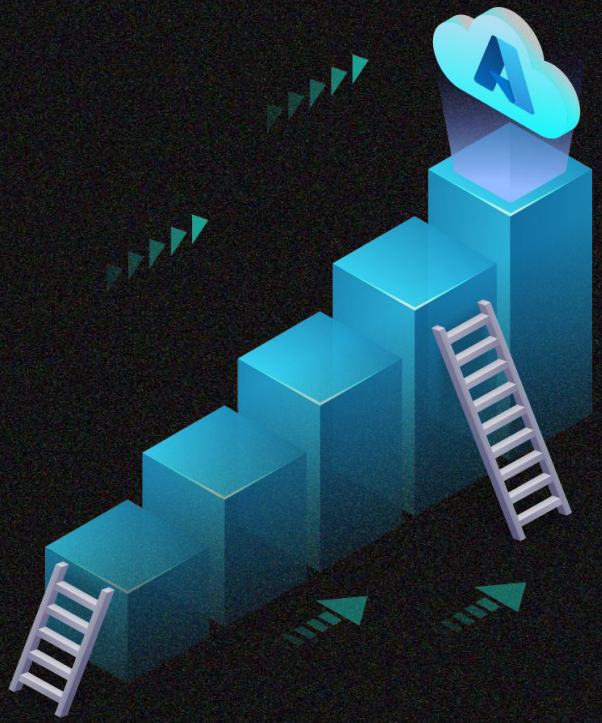


Zero to Azure Threat Hunter

What the Work Actually Looks Like

About CW Labs :

CW Labs is a renowned UK based Ed-tech company specializing in cybersecurity cyber range labs. They provide on-demand educational services and recognize the need for continuous adaptation to evolving threats and client requirements. The company has these primary divisions:

1. Cyber Range Labs
2. Up-Skilling Platform
3. Infinity Learning Platform

CWL provides customized on-site training for organizations and accepts bulk orders for corporate upskilling. For inquiries or more details, feel free to reach out at **support@cyberwarfare.live.**

About Speaker

Rahul Chakraborty

Blue Team Security Engineer@CWL

Blue Team Security Engineer at CyberWarfare Labs. Interested in Cloud and On-Premise Defense Operations

Why Azure Threat Hunting Matters

Organizations are moving to:

- Microsoft Azure
- Microsoft 365
- Entra ID
- Azure DevOps
- SaaS Applications

Attackers are targeting:

- Identities
- OAuth Applications
- Service Principals
- Cloud Resources
- Mailboxes

Key Message

Attackers don't need malware anymore. Stolen identities and cloud permissions are often enough.

What Does an Azure Threat Hunter Actually Do?

Traditional SOC Analyst

- Reviews alerts
- Waits for detections
- Investigates incidents

Threat Hunter

- Assumes compromise
- Searches for hidden attackers
- Finds activity before alerts trigger

Daily Activities

- Hunting suspicious logins
- Investigating OAuth abuse
- Tracking privilege escalation
- Detecting persistence mechanisms
- Correlating Azure & M365 logs

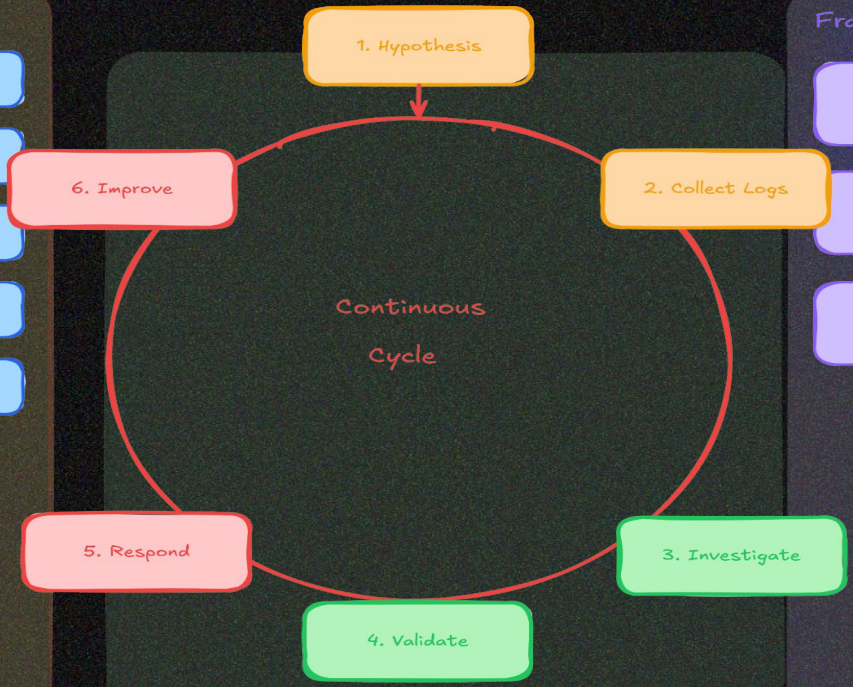
Understanding the Azure Attack Surface

Threat Hunting: The Foundation

Proactive Security Investigation Lifecycle

How Hunters Think

- Question Everything
- Look for Patterns
- Assume Compromise
- Follow the Data
- Continuous Learning



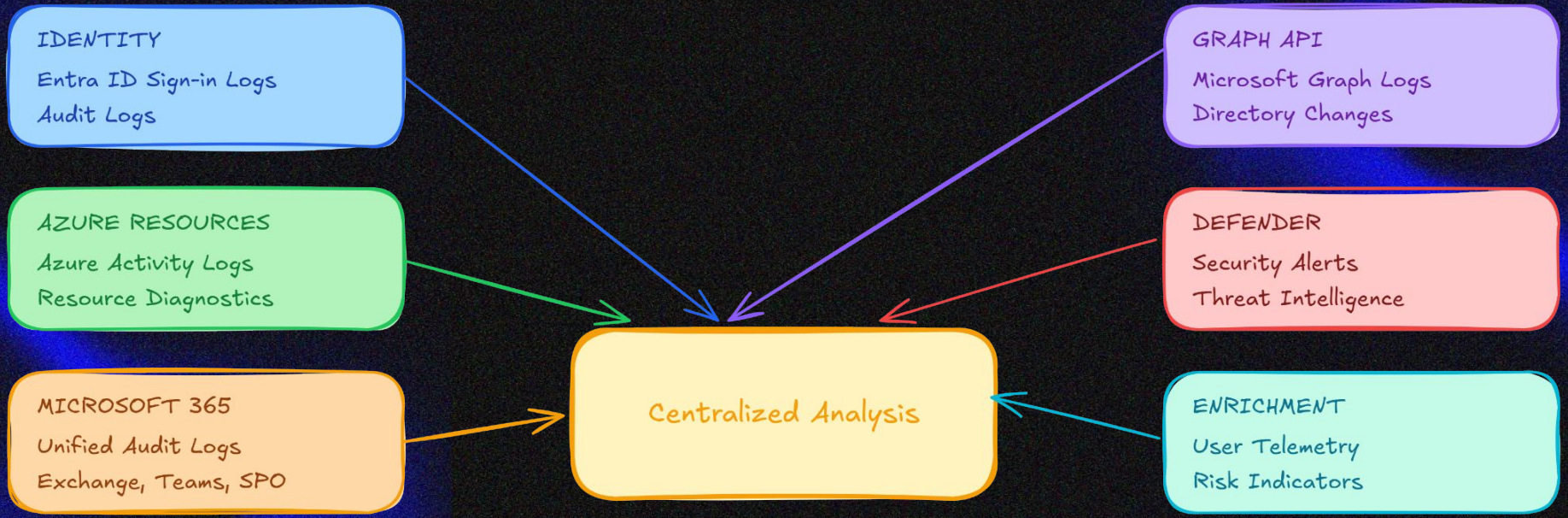
Frameworks Used

- **MITRE ATT&CK**
  Tactics & Techniques
- **Cyber Kill Chain**
  Attack Phases
- **Pyramid of Pain**
  Indicator Levels

Threat hunting bridges detection & response

The Logs That Matter

Azure & M365 Logging Ecosystem



Defense in Depth: Multiple Log Sources

Correlate logs across services to identify attacks

No single log source tells the complete story

What Skills & Tools Do You Need?

Building Your Threat Hunter Toolkit

TECHNICAL SKILLS

- Azure Fundamentals
- Entra ID Identity & Auth
- M365
- SPL
- Splunk SIEM Platform
- MITRE ATT&CK Framework
- Incident Response
- PowerShell Scripting

TOOLS & PLATFORMS

- Sentinel Azure SIEM
- Splunk Log Analysis
- Defender XDR Threat Intel
- Azure Portal Management
- Entra Admin Identity Mgmt
- Log Analytics KQL Workspace
- Incident Hub IR Platform
- GitHub Automation

Knowing vs Defending Azure

The Critical Skill Gap in Cloud Security

MOST PROFESSIONALS

Learn How to Use Azure

- Virtual Machines
- Networking
- Storage Accounts
- M365 Admin
- Entra ID Management

VS

THREAT HUNTERS

Think Differently (Defensively)

- What identities are abused?
- What behavior hides?
- What logs tell the story?
- What would I miss?
- How to validate with data?

THE SKILL GAP: What Organizations Need

- Understand Cloud Attack Techniques
  Know how attackers exploit cloud services
- Hunt Threats Proactively
  Shift from reactive to proactive threat hunting
- Analyze Cloud Telemetry
  Master cloud-specific logs and signals
- Support Incident Response
  Collaborate effectively during investigations

5. Improve Detection Coverage

Create better detections based on threat hunting findings - close the gaps before attackers exploit them

"The future of cloud security belongs to those who can see what others overlook."

This webinar is just the beginning. Stay connected with Cyber Warfare Labs for advanced Azure Threat Hunting.

Any Questions ?

Thank You

For Professional Red Team / Blue Team / Purple Team / Cloud Cyber Range labs / Trainings

Please Contact :

support@cyberwarfare.live

To know more about our offerings, please visit: **https://cyberwarfare.live**