Cloud-Based Honeypot-as-a-Service

QABAS AHMAD & MALAK ALSHAWISH

Problem Statement

•Rise of malicious cyber-activity.

•Need for insight into attacker behavior beyond traditional firewalls and intrusion detection systems.

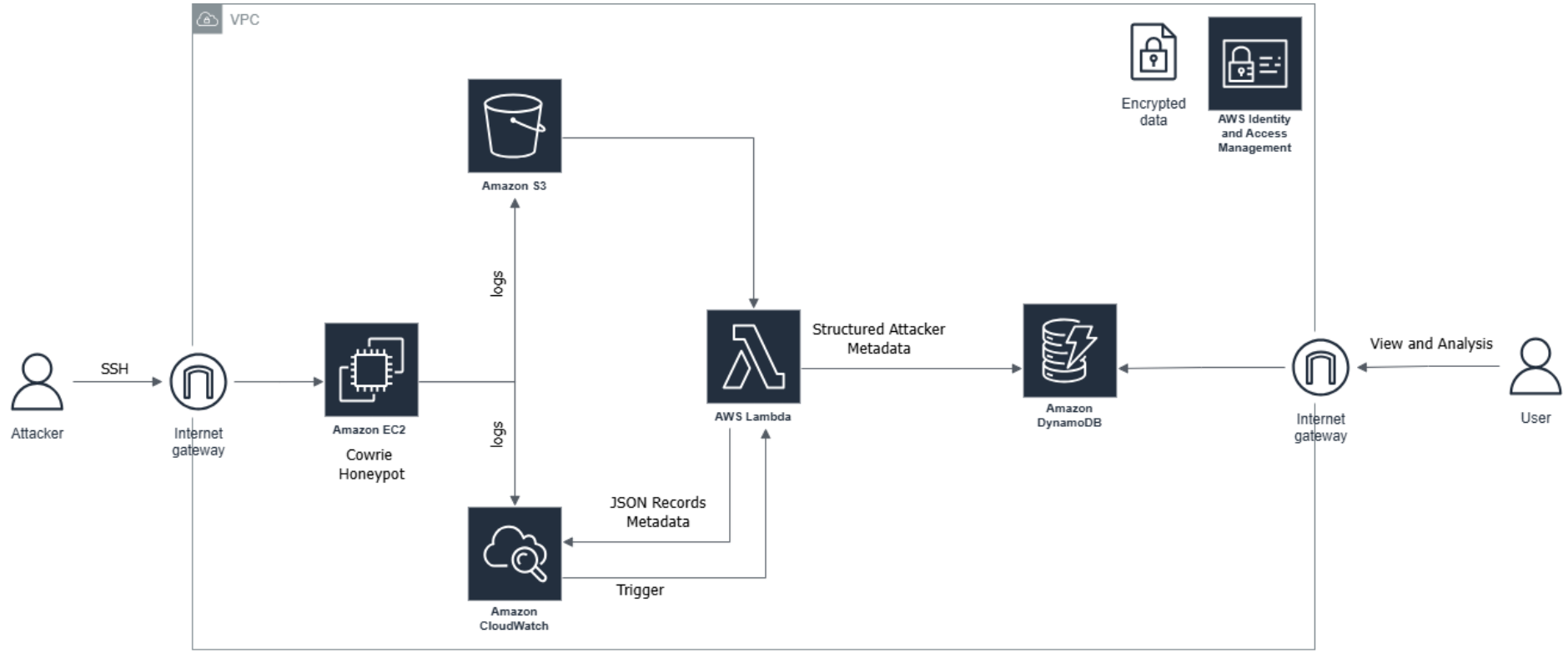
Objectives

- Track and analyze attacker behavior in real time.
- Demonstrate cloud-based proactive security measures (IAM, network isolation).
- Learn attack patterns using attacker metadata.

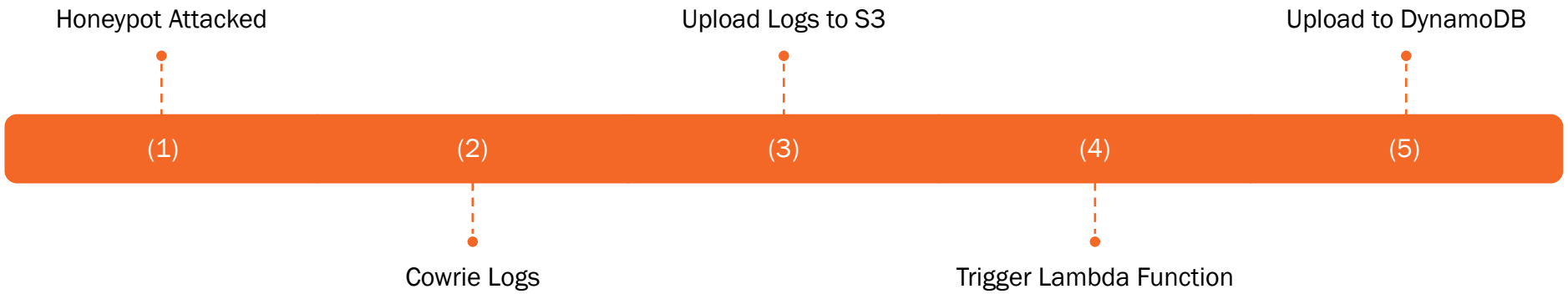
Honeypot Overview

- A security mechanism to detect, deflect, or counteract unauthorized system use.
- Simulates legitimate targets for attackers.
- Types:
  - Physical: Real machines, costly.
  - Virtual: Simulated environments, more scalable.
  - Project uses Cowrie (SSH/Telnet honeypot).

Architecture Diagram



Events Overview



Testing & Evaluation

•Functional Testing:
SSH attempts captured by Cowrie & Commands recorded.

•Benign Hydra Simulation:
Python script for brute-force attempts.

•Performance Testing:
PowerShell TCP Flood & Python Async Flood (5000 connections).
Cowrie remained stable (CPU peaked at 69%).

Challenges Faced

- Ensuring secure isolation of honeypot.
- Managing AWS resource costs.
- Balancing logging volume with performance.
- Ethical concerns in handling real attack data.

Conclusion

- Project showcases scalable, secure honeypot design.
- Valuable for threat intelligence and proactive security.
- Future potential for deeper analytics and multi-tenant support.