SOC Threat Intelligence Report: Cloud-Native Honeypot Analysis

Incident ID: TI-Honeypot-2025-10-26

Project Title: Cloud-Native Threat Detection Lab (TPOT Honeypot)

Status: Observation Complete / Findings Documented

Field	Detail
Observation Period	[Date and Time Range of Honeypot Activity]
Reporting Analyst	SOC Analyst [Your Name]
Technology	**TPOT (The Honeypot Project)**, Elastic Stack (Kibana)
Environment	DigitalOcean Droplet (Ubuntu 24.04 LTS)
Severity	**Informational** (High volume of internet-wide scanning activity observed)

---

1. Executive Summary and Objective Achieved 🎯

The primary objective of establishing a cloud-native **TPOT Honeypot** on DigitalOcean was successfully met. Within the observation period, the honeypot collected a high volume of real-time, undirected attack telemetry. The deployment process emphasized **Linux security hardening** (non-root users, package updates, non-standard SSH port), and the subsequent analysis leveraged **Kibana** (Elastic SIEM) for visualization. Key findings confirm that automated scanners heavily target default services, predominantly **SSH**, and leverage major cloud/hosting providers to mask their origin. This lab serves as a high-fidelity source of threat intelligence for future security policy construction.

2. Infrastructure Deployment and Security Hardening ⚙️

The foundation of the lab involved deploying a secure server environment, demonstrating essential cloud administration skills:

Action (Ref)	Technical Detail	Security Rationale
Droplet Provisioning (Ref 1)	Ubuntu 24.04 LTS server (`tzmnc-web-server1`) provisioned on DigitalOcean.	Established a stable, external-facing platform for the honeypot services.
System Hardening (Ref 3, 4, 5)	Performed `apt-get upgrade` and created a non-root administrative user (`martin`) with `sudo` privileges.	Ensures the base OS is secure and minimizes the attack surface by avoiding daily root usage.
TPOT Installation (Ref 7, 8, 9)	Cloned the `tpotce` repository and selected the **HIVE** installation type.	Deployed a multi-honeypot system and the centralized **Elastic SIEM** stack (Kibana/Elasticsearch).
SSH Port Change (Ref 10, 12)	The installation automatically migrated the administrative SSH port from default **22** to **64295**.	Critical defense against automated SSH brute-force bots, which often target port 22 exclusively.

3. Threat Intelligence Analysis (Kibana Findings) 📈

Analysis of the log data ingested by the Elastic Stack provided clear, actionable insights into attacker TTPs:

A. Attack Distribution and Targets (Ref 15, 17)

- **Total Attacks: 38** incidents were recorded within the initial period.

- **Most Targeted Service: Cowrie** (the SSH honeypot) recorded **34** attacks, confirming that automated brute-force attempts on SSH remain the most prevalent threat against exposed internet services.
- **Geographic Origin:** The **Global Attack Map (Ref 17)** highlighted that while threats were diverse, the **United States** was a top source location, along with other countries frequently associated with large scanning botnets (e.g., China, Russia).

B. Attacker Infrastructure and Alert Details (Ref 16)

The detailed analysis of the attacker's source and IDS logs provides crucial context for blocking strategies:

Finding Category	Details from Kibana	Security Implication
Attacker ASN	Top source Autonomous System Numbers (ASNs) include **GOOGLE-CLOUD-PLATFORM** and **Alibaba US Technology**.	Attackers are relying on large, legitimate cloud/hosting providers to host their scanning infrastructure, making simple geo-blocking ineffective.
Suricata Alerts	Common alerts included "STREAM Packet with broken ack" and "TLS invalid record type."	Indicates the use of aggressive, poorly formed network scanning tools that trigger signatures in the Intrusion Detection System (Suricata), signifying malicious intent.

---

4. Conclusion and Recommended Mitigation Actions 💡

The Cloud-Native Honeypot lab successfully demonstrated the entire **Detect and Analyze** lifecycle. The immediate observation of high-volume scanning traffic validates the need for a robust defense strategy.

Key Learnings and Actionable Recommendations:

1. **Non-Standard Ports are Essential:** The immediate post-installation SSH port change to **64295** was confirmed as a vital defense, as it instantly eliminated access from the vast

majority of port 22-targeting bots (Ref 10). This practice should be mirrored across all production environments.
2. **Cloud-Source Blocking:** Due to the high volume of traffic originating from major cloud providers (Ref 16), organizations must implement dynamic reputation feeds and more intelligent behavioral blocking rules, as blanket blocking of these ASN ranges is impractical.
3. **SIEM Utility:** The **Elastic Stack** proved its value by transforming thousands of raw log entries into clear, visual, and actionable threat intelligence, such as the top targeted services and geographical sources (Ref 15).

The collected IOCs (Attacker IPs, Usernames used in Cowrie) will be fed into organizational **Threat Intelligence Platforms (TIPs)** to enhance perimeter defenses and refine SIEM detection rules.