Azure Honeypot Threat Intelligence Lab — Technical Documentation

Author: Ritvik Indupuri
Date: August 2025

---

1. Project Overview

This project involved deploying a honeypot in Microsoft Azure and utilizing **pre-configured Suricata IDS dashboards in Kibana** to analyze real-world attack telemetry. The goal was to simulate a Security Operations Center (SOC) workflow by interpreting threat data, attacker behaviors, and detection patterns without manual Suricata setup.

---

2. Architecture & Deployment

2.1 Platform & Services

- **Cloud Provider:** Microsoft Azure
- **Components Used:**
    - T-Pot Honeypot Suite (Cowrie, Honeytrap, Heralding, Dionaea)
    - Suricata IDS (pre-configured in T-Pot)
    - Azure Virtual Machine (Ubuntu 24.04)
    - Azure Network Security Group (NSG)
    - Kibana Dashboards (pre-built with T-Pot)

2.2 Deployment Topology

- **Region:** East US (Zone 2)
- **VM Specs:** Standard_D2s_v3 (2 vCPUs, 8 GiB RAM)
- **IP Configuration:** Public IP for external exposure, Private IP for internal segmentation
- **NSG Rules:** Custom inbound rules exposing ports 22, 80, 443, 445, 8080 to attract attack traffic

Figure 1: Azure HoneypotVM Network Interface & NSG Configuration

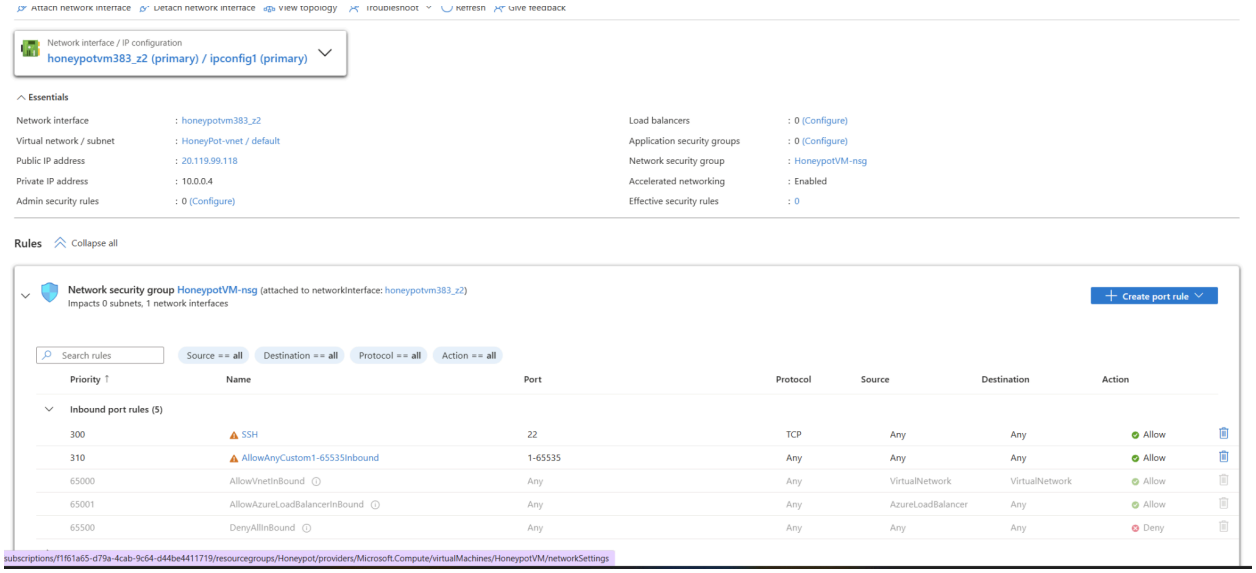
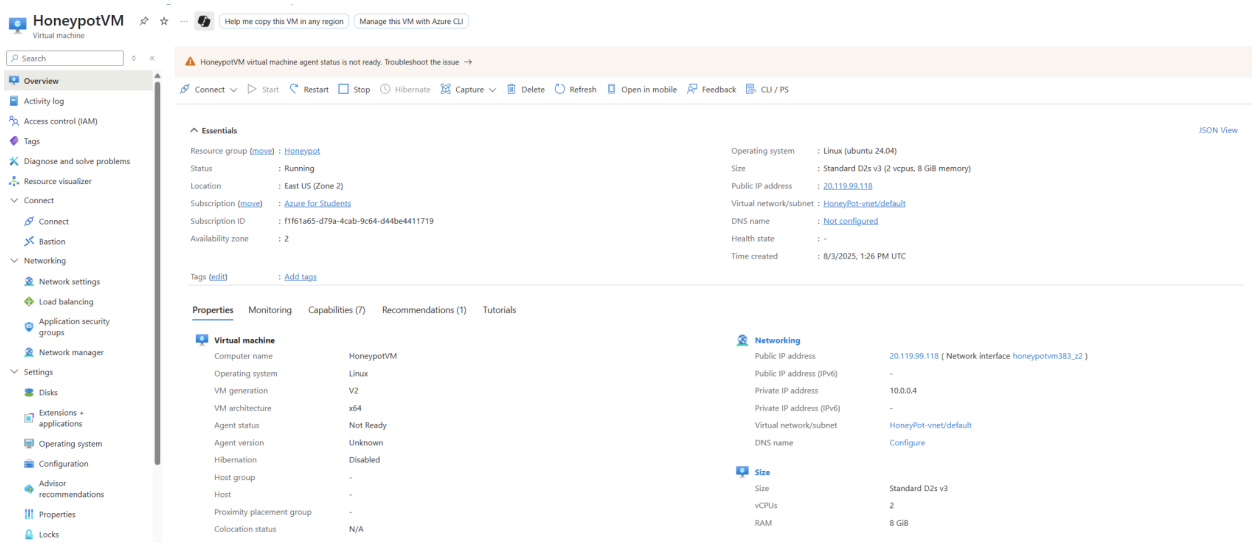


Figure 2: Azure HoneypotVM Instance Overview



3. Workflow Execution

Step 1: Honeypot Deployment

- Deployed HoneypotVM in Azure.
- Configured NSG to expose key service ports for reconnaissance and exploit attempts.
- T-Pot suite (including Suricata IDS) was pre-installed, streamlining setup.

Step 2: Attack Telemetry Capture

- Real-world attackers targeted the honeypot, triggering pre-configured sensors.
- Logs were automatically ingested into Kibana dashboards provided by T-Pot.

Step 3: Telemetry Analysis in Kibana

Focus areas:

- Honeypot-Level Engagement Metrics
- Suricata Alerts & Signature IDs
- Source ASN & IP breakdowns
- Service-specific attack patterns (SSH, FTP, DNS, HTTP)
- Geolocation mapping of attack sources
- Protocol distribution & JA3/JA4 fingerprinting

---

4. Honeypot Attack Telemetry & Suricata IDS Analysis

4.1 Honeypot-Level Alerts & Attack Map

The T-Pot honeypot sensors (Cowrie, Honeytrap, Dionaea) captured raw connection attempts across exposed services. Key insights include:

- Service-specific hit counts (SSH, FTP, HTTP)
- IP-level engagement metrics
- Real-time global attack heatmap

Figure 3: Honeypot Attack Counts & Service Hit Distribution

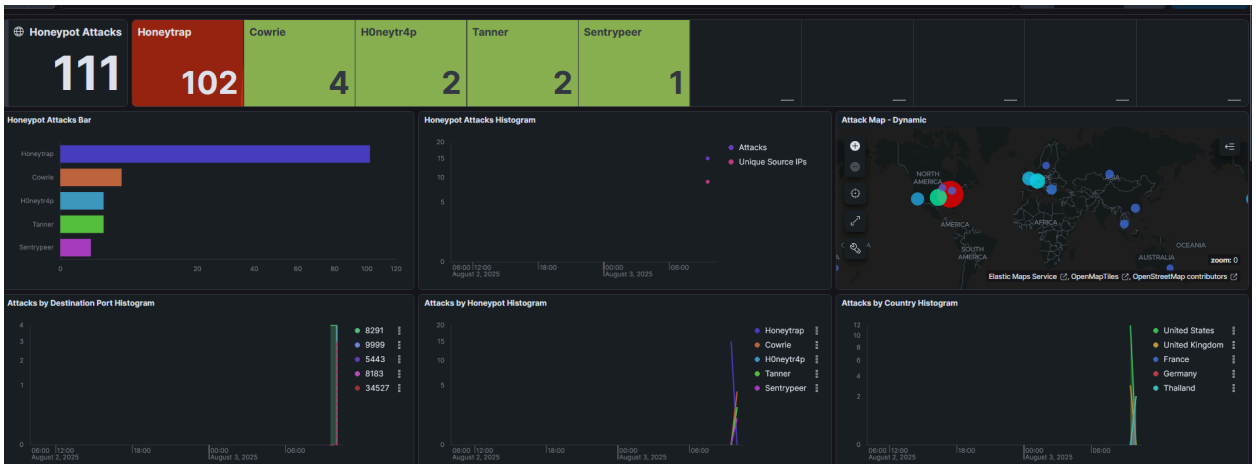
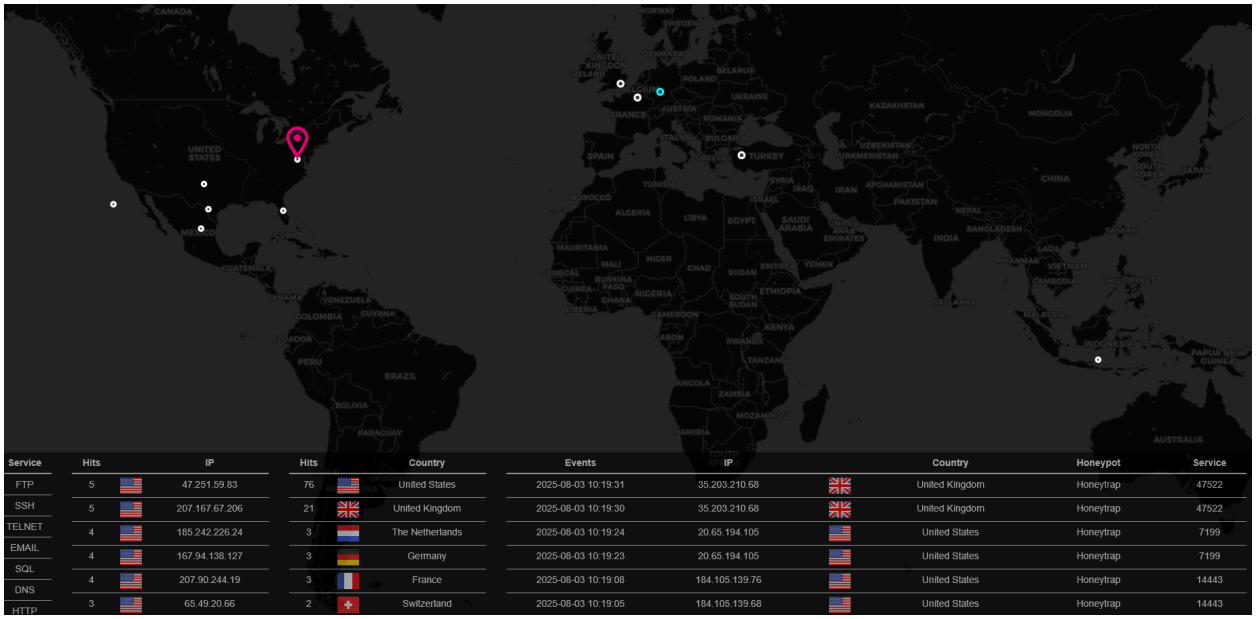


Figure 4: Global Attack Heatmap & IP Hit Breakdown



Service	Hits	IP
FTP	5	47.251.59.83
SSH	5	207.167.67.206
TELNET	4	185.242.226.24
EMAIL	4	167.94.138.127
SQL	4	207.90.244.19
DNS	3	65.49.20.66
HTTP		

Hits	Country
76	United States
21	United Kingdom
3	The Netherlands
3	Germany
3	France
2	Switzerland

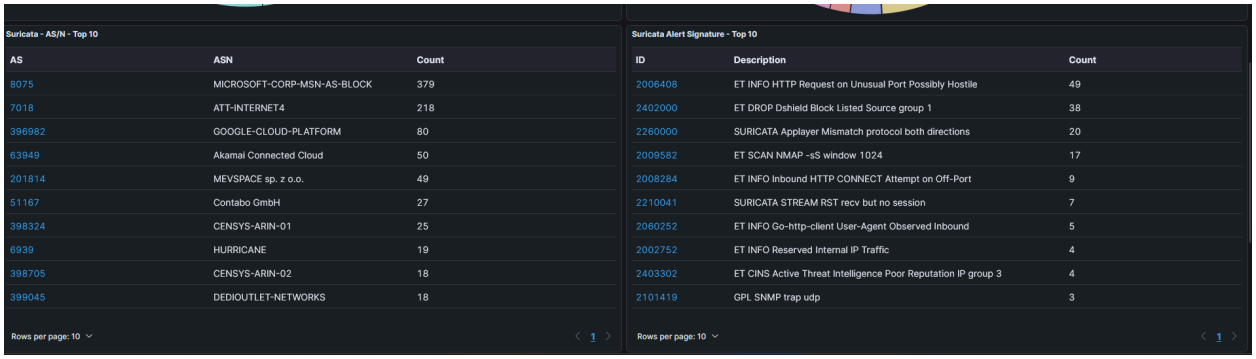
Events	IP	Country	Honeypot	Service
2025-08-03 10:19:31	35.203.210.68	United Kingdom	Honeytrap	47522
2025-08-03 10:19:30	35.203.210.68	United Kingdom	Honeytrap	47522
2025-08-03 10:19:24	20.65.194.105	United States	Honeytrap	7199
2025-08-03 10:19:23	20.65.194.105	United States	Honeytrap	7199
2025-08-03 10:19:08	184.105.139.76	United States	Honeytrap	14443
2025-08-03 10:19:05	184.105.139.68	United States	Honeytrap	14443

4.2 Suricata IDS Telemetry & Signature Breakdown

Suricata IDS categorized the incoming traffic using pre-configured detection rules. Key metrics analyzed:

- Suricata Alert Signatures (Nmap Scans, Dshield Blocklists, HTTP Anomalies)
- ASN breakdown (Microsoft, Google Cloud, Akamai)
- Protocol-specific activity (HTTP, DNS, FTP)
- JA3/JA4 SSL/HTTP Fingerprint diversity

Figure 5: Suricata Alert Signatures & ASN Intelligence



Suricata - AS/N - Top 10

AS	ASN	Count
8075	MICROSOFT-CORP-MSN-AS-BLOCK	379
7018	ATT-INTERNET4	218
396982	GOOGLE-CLOUD-PLATFORM	80
63949	Akamai Connected Cloud	50
201814	MEVSPACE sp. z o.o.	49
51167	Contabo GmbH	27
398324	CENSYS-ARIN-01	25
6939	HURRICANE	19
398705	CENSYS-ARIN-02	18
399045	DEDIOUTLET-NETWORKS	18

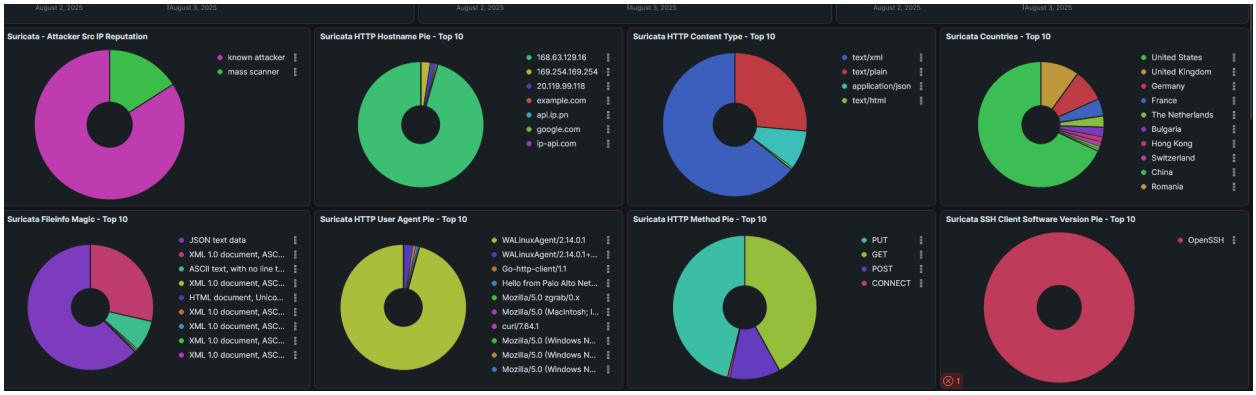
Rows per page: 10 1

Suricata Alert Signature - Top 10

ID	Description	Count
2006408	ET INFO HTTP Request on Unusual Port Possibly Hostile	49
2402000	ET DROP Dshield Block Listed Source group 1	38
2260000	SURICATA Applayer Mismatch protocol both directions	20
2009582	ET SCAN NMAP -sS window 1024	17
2008284	ET INFO Inbound HTTP CONNECT Attempt on Off-Port	9
2210041	SURICATA STREAM RST recv but no session	7
2060252	ET INFO Go-http-client User-Agent Observed Inbound	5
2002752	ET INFO Reserved Internal IP Traffic	4
2403302	ET CINS Active Threat Intelligence Poor Reputation IP group 3	4
2101419	GPL SNMP trap udp	3

Rows per page: 10 1

Figure 6: Suricata Protocol Distribution & File Metadata Analysis



Note: Figures 3 & 4 represent raw honeypot-level engagement metrics (connection attempts), whereas Figures 5 & 6 display categorized IDS detections processed by Suricata's pre-configured detection engine in Kibana.

---

5. Lessons Learned

- Differentiating between raw honeypot engagement (connection attempts) and IDS-level telemetry is crucial in operational security analysis.
- Pre-built IDS dashboards significantly accelerate SOC simulation workflows.
- ASN-level intelligence and fingerprinting provide deeper context on attack infrastructure.
- Visual telemetry enhances situational awareness for real-time monitoring.

---

6. Future Enhancements

- Integrating honeypot telemetry into Azure Sentinel for SIEM-driven alert correlation.
- Automating incident triage with SOAR playbooks connected to Kibana event triggers.
- Expanding honeypot scope into Kubernetes clusters using AKS for container-level honeypot traps.

---

7. Conclusion

While Suricata IDS and Kibana dashboards were pre-configured within T-Pot, this project emphasized hands-on threat telemetry interpretation. By deploying a honeypot in Azure and leveraging Kibana's visualization capabilities, a live SOC workflow was simulated, offering insights into attacker behaviors, detection logic, and situational analysis. The project strengthened operational skills in **network exposure management, IDS alert interpretation, and threat intelligence correlation** essential for cloud security operations.
