

# Network Analysis with Maltrail

---

Analyzing Network Trail Logs with Maltrail



**Rushabh Doshi**

Cloud Security Architect



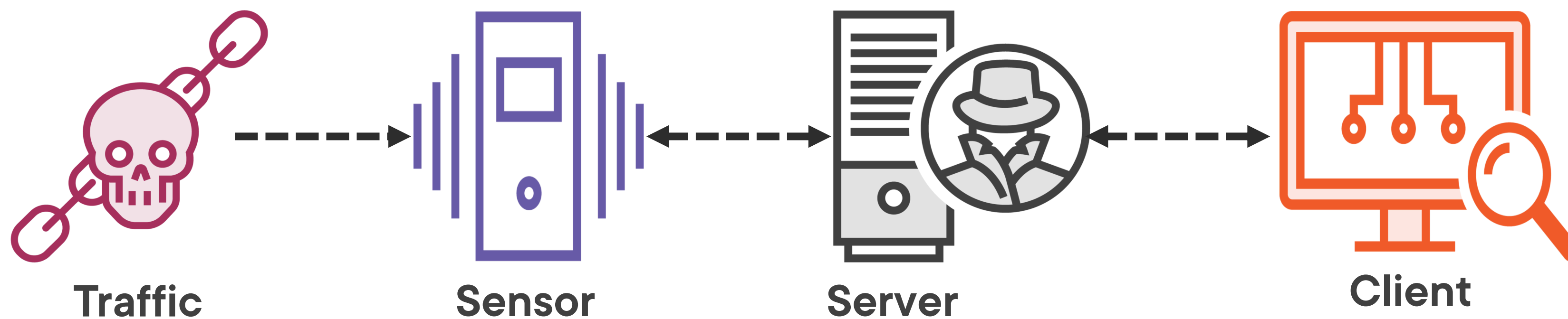
# Overview



- **Maltrail architecture**
- **Real-life cases**
- **Demo - installation of maltrail**
- **Demo - assess configuration of sensor and server**
- **Demo - monitor the threats using dashboard**



# Maltrail Architecture



# Real Life Cases

## Mass Scans

Right to scan the  
whole IP range

## Anonymous Attackers

Spot potential  
attackers behind Tor  
Anonymity Network

## Malware

Connection attempts  
from infected  
computers

## Suspicious Requests

Vulnerability scans

## Port Scanning

Too many connection  
attempts towards  
different TCP ports



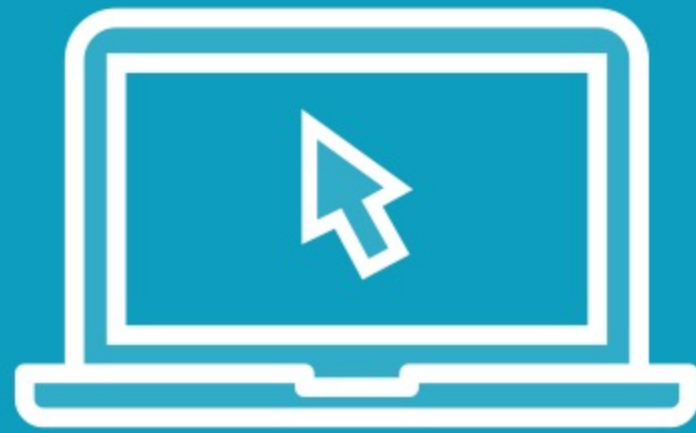
# Demo



- **Installation of Maltrail**



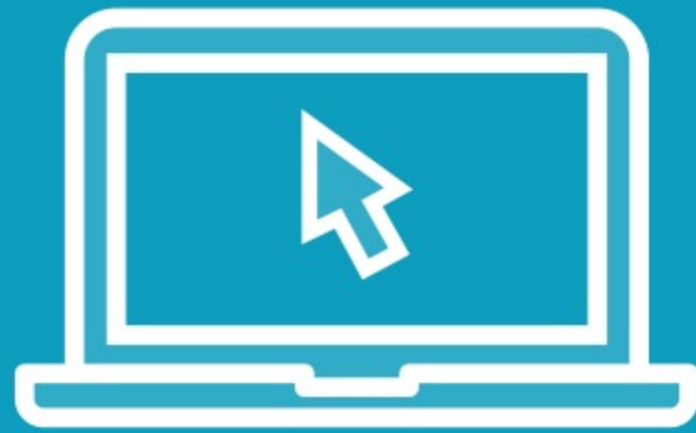
# Demo



- **Assess configuration of sensor and server**



# Demo



- **Monitor the threats using dashboard**



# Summary



- **Network intrusion detection**
- **Monitor traffic using live dashboard**

