
black hat
ARSENAL
AUGUST 7-8, 2024
MANDALAY BAY/LAS VEGAS


# ICSGoat

## A Damn Vulnerable ICS Infrastructure

# About Us

## Shantanu Kale

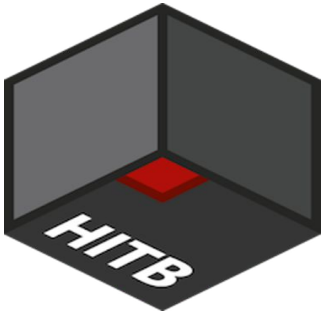
- Infrastructure Lead @ INE
- Published Research at Black Hat US/Asia Arsenal and DEFCON 30 Demo Labs
- Co-trainer in training at Seasides Goa, Rootcon 16 & 17
- Core Contributor to AWSGoat
- Strong roots in cloud and network penetration testing, vulnerability scanning, and Open Source Intelligence Techniques

# About Us

## Divya Nain

- Software Engineer @ INE
- Published Research at Black Hat Asia Arsenal
- Core contributor to AzureGoat and GCPGoat
- Co-trainer in training at Seasides Goa
- Strong roots in cloud and network security


OWASP
NEW ZEALAND DAY
2019


HITB


black hat

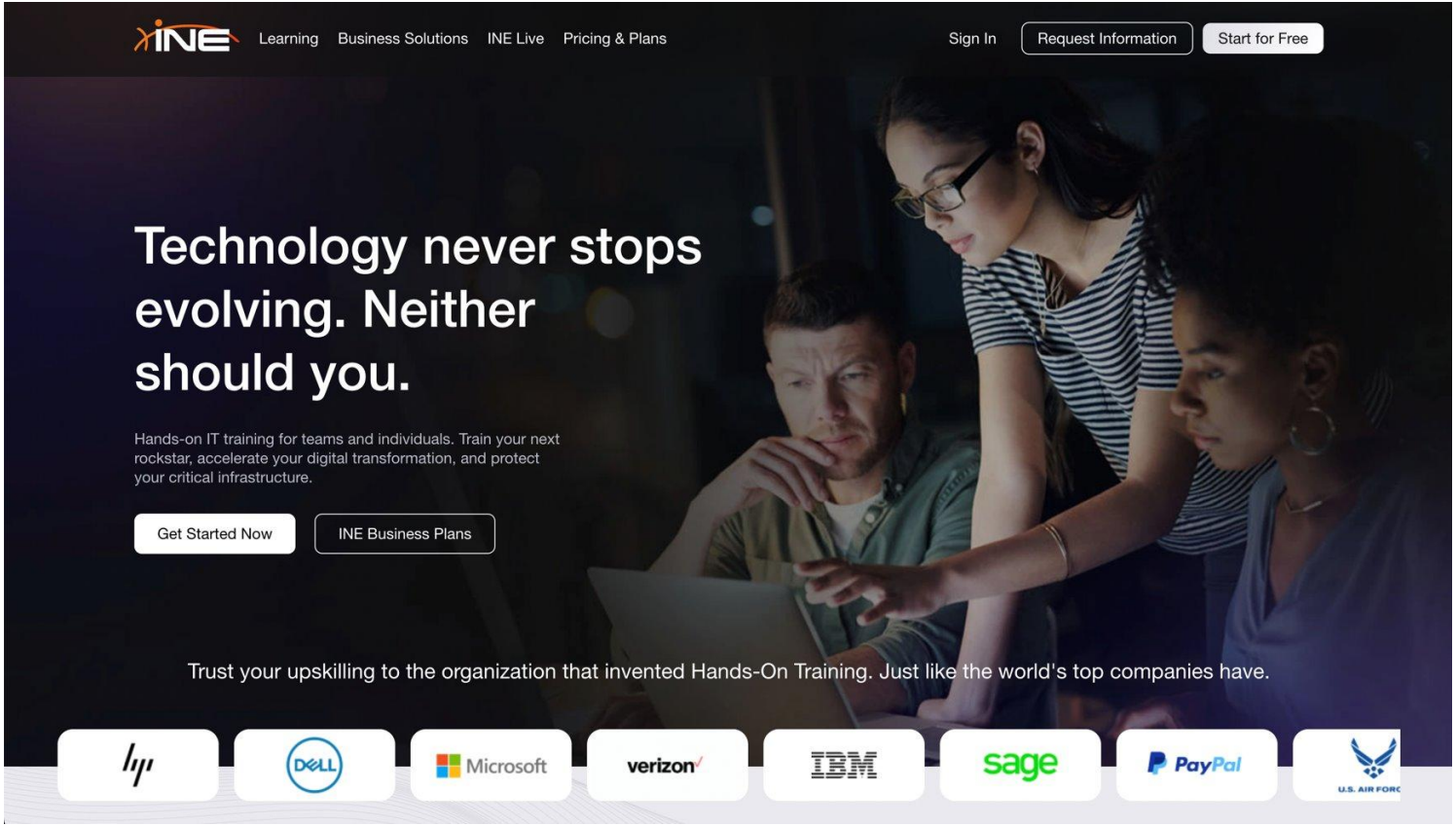

WIRELESS
VILLAGE


百度安全
DEF CON
CHINA 1.0

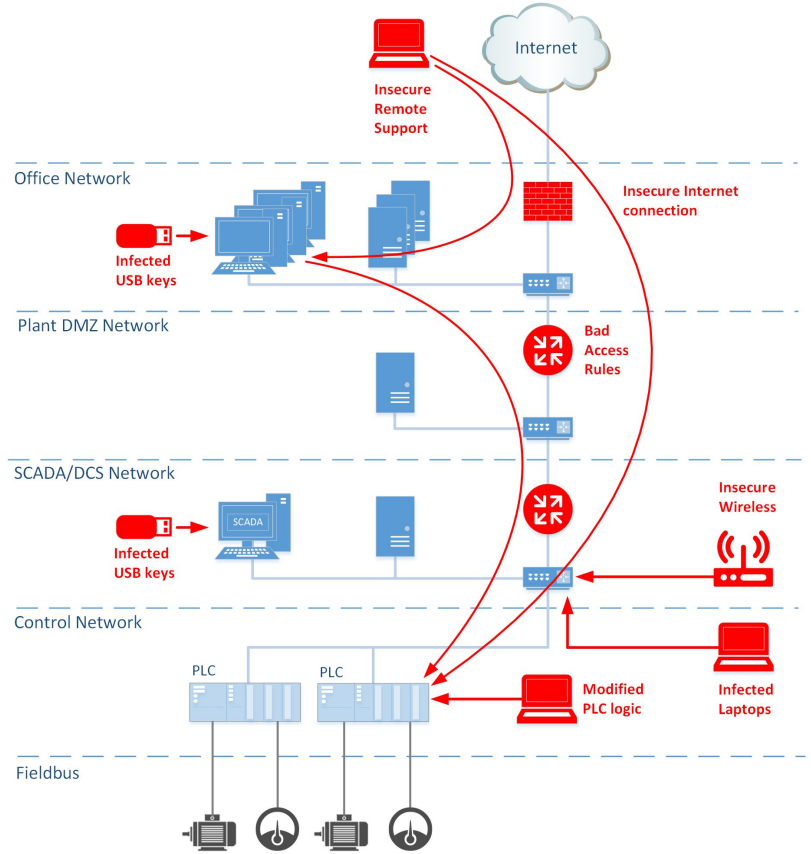

WALL OF SHEEP


DEFCON


ROOTCON
Hacker Conference


INE
Learning
Business Solutions
INE Live
Pricing & Plans
Sign In
Request Information
Start for Free
Technology never stops evolving. Neither should you.
Hands-on IT training for teams and individuals. Train your next rockstar, accelerate your digital transformation, and protect your critical infrastructure.
Get Started Now
INE Business Plans
Trust your upskilling to the organization that invented Hands-On Training. Just like the world's top companies have.
Microsoft
verizon
IBM
sage
PayPal

# Threatscape




Reference:
https://ics-cert.kaspersky.com/publications/reports/2017/03/28/threat-landscape-for-industrial-automation-systems-in-the-second-half-of-2016/

# The Motivation

- Training Needs
  - Basics and Fundamentals
  - Understanding ICS Protocols
  - Exploiting network misconfigurations
  - Exploiting popular ICS protocols like modbus, dnp3, mqtt, etc
  - What Next?
- Lack of expansive and realistic ICS Pentesting Environment
- Contribution from the open source community and security professionals

# Enter ICSGoat!

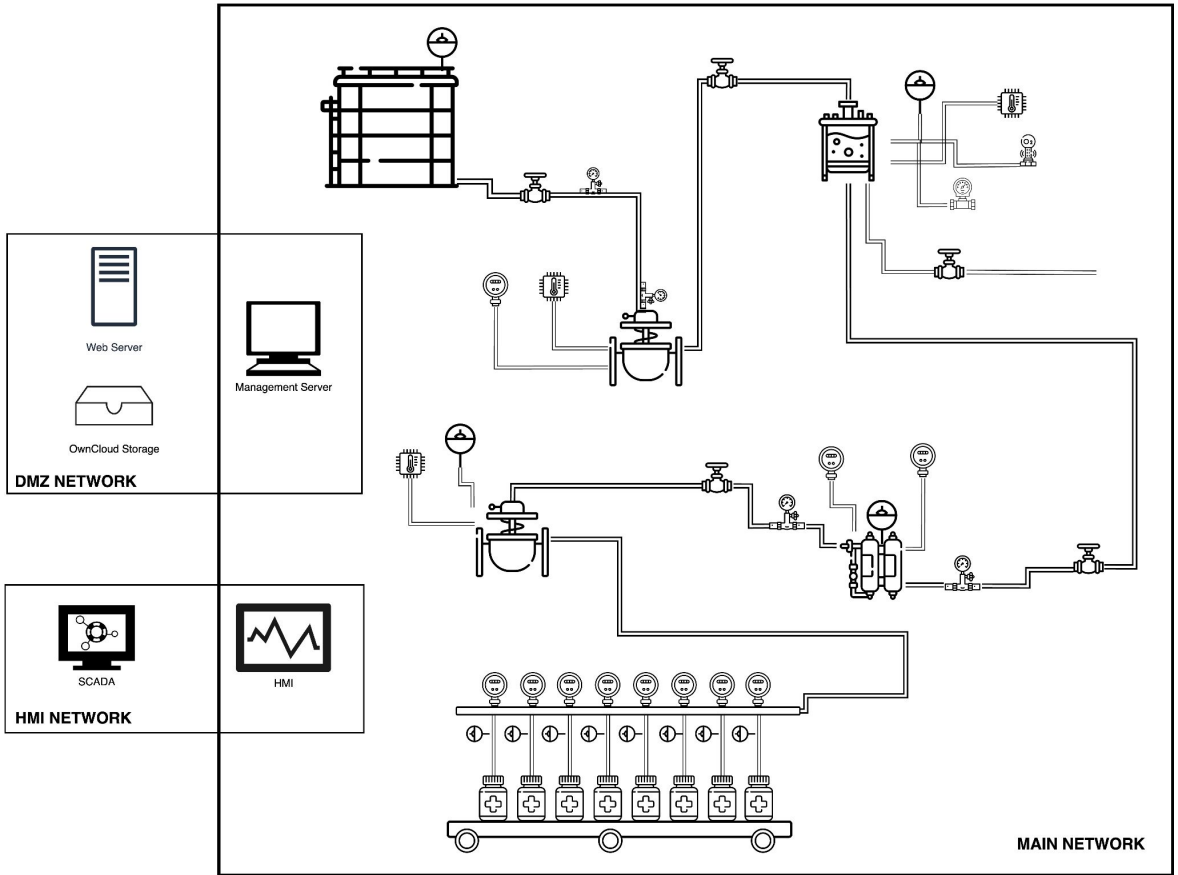
# ICSGoat: A Damn Vulnerable ICS Infrastructure

- Mimics real-world ICS infrastructure but with added vulnerabilities
- Multiple popularly used protocols are simulated
- Focused on a black box approach
- Understand possible threats to critical ICS infrastructure

# ICSGoat Protocols

- MODBUS
- DNP3
- OPCUA
- MQTT

# ICSGoat Infra Diagram



# Building Realistic ICS Scenario: Challenges

- Unavailability of publicly available resources
- Required modifications to protocol libraries
- Containerizing protocol simulations
- Incorporating multiple protocols in a single scenario
- Required custom made SCADA and HMI system

# Goat Family

AWSGoat

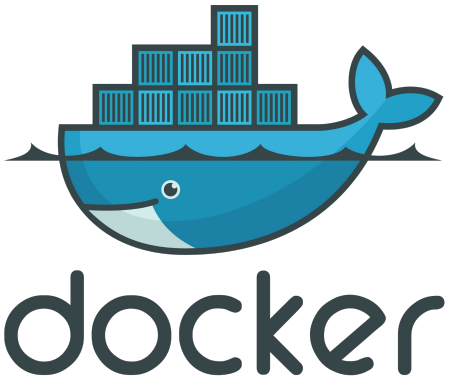
GCPGoat

AzureGoat

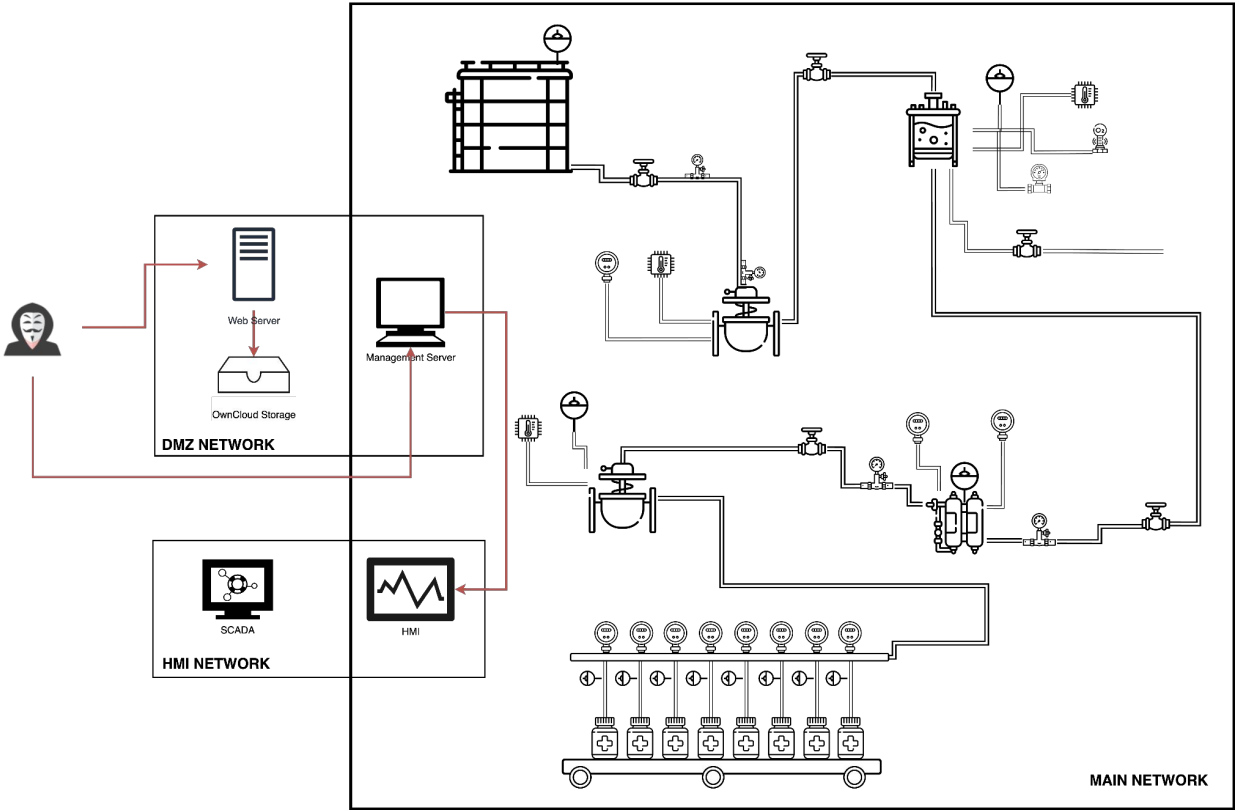
# Installation

- Repository: https://github.com/ine-labs/ICSGoat

- Manual Installation (Linux/Windows Machine)
  - Requirements
    - Docker (Docker Compose)
    - Git
  - Commands:
    - git clone https://github.com/ine-labs/ICSGoat
    - cd ICSGoat
    - docker compose up



# Initial Attack Vector



# DEMO

# Future Plans

- Work with the community to introduce more protocols to ICSGoat
- Utilize ICSGoat to create realistic scenarios with the help of industry professionals
- Co-exist with other projects

# Thanks

skale@ine.com