THREAT THIS FALL

INTELLIGENT THREAT
DETECTION WITH HONEYPOT

THREAT THIS FALL

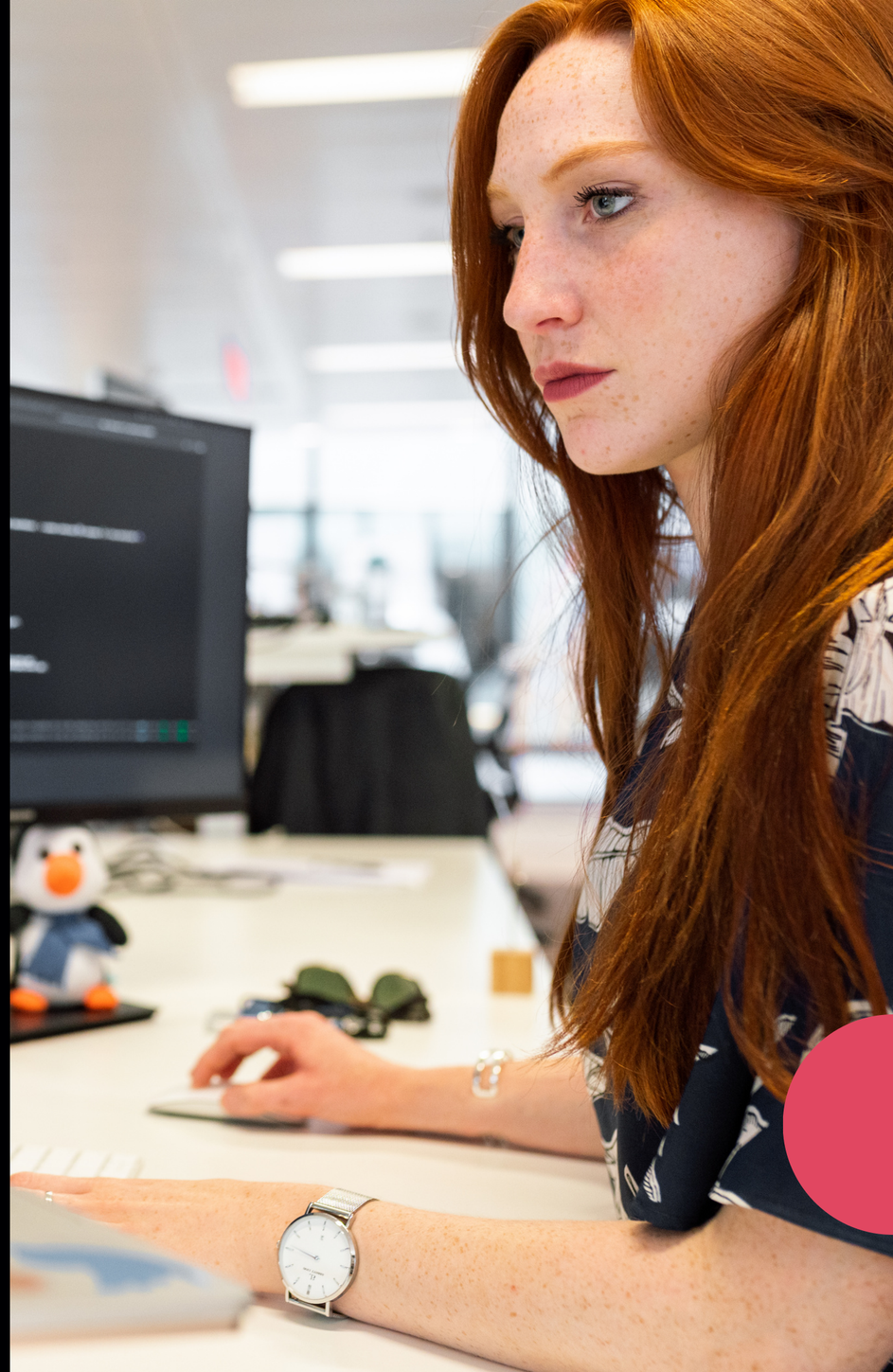
OUR PROJECT

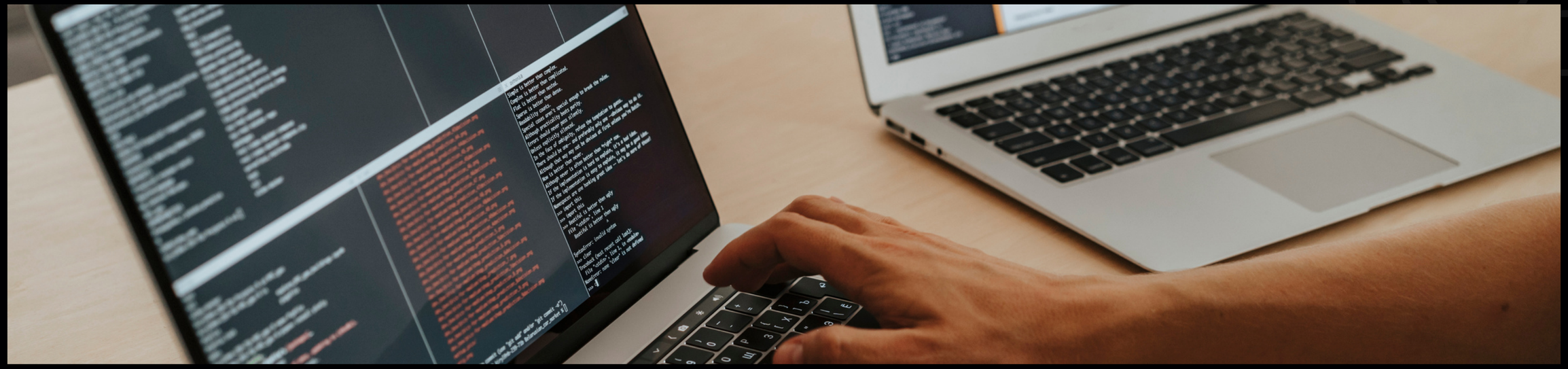
- ThreatThisFall is a cutting-edge system that integrates with Blue Wireless, Twilio and StoryBlok to provide real-time threat intelligence detection of cyber attacks.

- Our system employs the use of honeypots, both internal and external, to effectively detect and respond to potential threats.

- The internal components of the system include the ESP Node 32, which acts as a honeypot to lure in potential attackers.

- The external components include a virtual machine honeypot that provides an added layer of defense.





WHAT DO OUR PROJECT DO?

- When a hacker attacks the system, the first point of contact will be the honeypot.
- This will trigger an alert that informs the system's owner via SMS or WhatsApp message, providing them with valuable information about the attack and allowing them to take proactive measures to prevent further damage.

THREAT THIS FALL

VISION & MISSION

Vision

- Our vision is to create a secure and connected world by providing real-time threat intelligence through our cutting-edge honeypot system, HoneyNet.

- By seamlessly integrating with Blue Wireless, Twilio and StoryBlok, we aim to empower individuals and organizations to proactively defend against cyber threats and safeguard their valuable assets.

THREAT THIS FALL

VISION & MISSION

Mission

- Our vision is to create a secure and connected world by providing real-time threat intelligence through our cutting-edge honeypot system, ThreatThisFall.

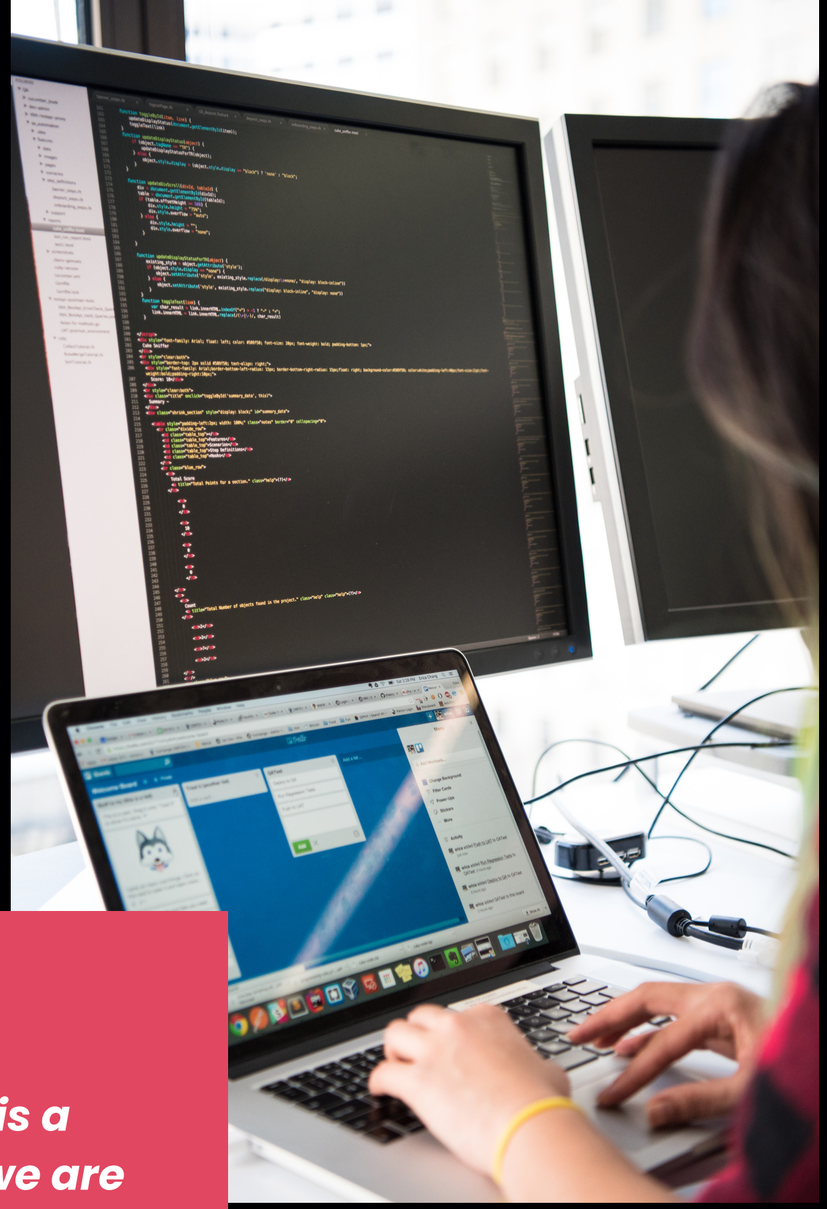
- By seamlessly integrating with Blue Wireless, Twilio and StoryBlok, we aim to empower individuals and organizations to proactively defend against cyber threats and safeguard their valuable assets.

THREAT THIS FALL

USE OF HONEYPOT

Internal Honeypot

- In the internal network, we recognize the potential for intruders to penetrate the network.
- To address this, we have implemented an internal wifi honeypot that acts as a normal access point and records IP addresses and BSS IDs.
- This allows us to identify and block unauthorized IP addresses, enhancing the overall security of the internal network and organization.



> ***Privacy is a myth but we are on a mission to break that myth***

USE OF HONEYPOT

External Honeypot

- In the external network, organizations are constantly facing cyberattacks on their network and web services.
- To identify and block these attackers, we have set up an intentionally vulnerable honeypot.
- This honeypot allows hackers to attack it and records all their IP addresses, port numbers, and the services they use.
- With this information, we can effectively block the attacker's IP address, ensuring that they cannot access the real network and compromising the security of the organization.

THREAT THIS FALL

01

Real-Time Threat Detection

It employs the use of honeypots to detect potential cyber threats in real-time, providing immediate protection for your network.

02

Instant Notification

Upon detection of an intrusion, ThreatThisFall instantly notifies the network owner via WhatsApp or SMS message, allowing for immediate response and protection.

03

Comprehensive Log Files

All functions of the system are recorded in log files for future reference and investigation, providing a thorough understanding of the threat landscape.

04

Efficient Response

By providing real-time notification and comprehensive log files, ThreatThisFall enables efficient response to potential threats, ensuring the security of your network.

05

Peace of Mind

It provides peace of mind by ensuring that your network is protected against potential threats 24/7

06

Mission to Secure the Digital World

Our mission is to secure the digital world and protect against potential cyber threats. Join us in this pursuit as we strive to provide comprehensive and efficient solutions to enhance the security of your network.

THREAT THIS FALL

SPONSERS

01 Blues Wireless

- It is used to provide wireless connectivity for the honeypot system and internal network security (ESP Node 32)

02 Twillio

- it is being used to provide connectivity for the SMS or WhatsApp notifications sent in response to an detected intrusion

03 GitHub

- It is used in the project to store and manage the source code, collaborate with others, and track changes and progress.
- It provides tools for version control, bug tracking, and project management, making it a valuable tool

THREAT THIS FALL

MEET OUR TEAM

Ashish Vishwakarma
Network Programmer

Manan Patel
Bug Hunter & Securrity Researcher

Rushi Padhiyar
Cyber Analyst & CTF Player

THREAT THIS FALL

CONTACT US

+917096635849

ashishvish4778@gmail.com

Project Link

Parul University

THANK YOU

VISIT US