A USER-CENTRIC MACHINE LEARNING FRAMEWORK

FOR CYBER SECURITY OPERATIONS CENTER

**A Project Report submitted to JNTUK, Kakinada in the partial fulfillment of the requirements for the award of the degree of**

**BACHELOR OF TECHNOLOGY**

IN

**COMPUTER SCIENCE AND ENGINEERING**

SUBMITTED BY

**Nagarjuna Reddy.A – 16JE1A0538**

**Rakesh.K – 17JE5A0501**

**Linga Babu.A – 16JE1A0526**

**Suresh Babu.CH – 16JE1A0557**

**Under the Esteemed Guidance of Mr. MD John Saida M.Tech**

**Assistant Professor**

**CSE Department**



**Department Of Computer Science and Engineering**

**ESWAR COLLEGE OF ENGINEERING**

(Approved by AICTE, Affiliated to JNTU, Kakinada) NARASARAOPET-522601, ANDHRA PRADESH

**2016-2020**

**ESWAR COLLEGE OF ENGINEERING**

(Approved by AICTE &Affiliated to JNTU, Kakinada)

NARASARAOPET-522601, ANDHRA PRADESH

**2016 – 2020**

**CERTIFICATE**

This is to certify that the Project Report titled **“A USER-CENTRIC MACHINE LEARNING FRAMEWORK FOR CYBER SECURITY OPERATIONS CENTER”** is submitted by

**NAGARJUNA REDDY. A (16JE1A0538)**

**RAKESH. K (17JE1A0501)**

**LINGA BABU. A (16JE1A0526)**

**SURESH BABU. CH (16JE1A0557)**

students of **B.Tech (CSE),** in partial fulfillment of the requirements for the award of the degree of **Bachelor of Technology** in **Computer Science and Engineering** is a record of bonafide work carried out by them under my supervision. The matter embodied in this report has not been submitted to any other University or Institution for the award of any other degree.

**Internal Guide**

**MD. JOHN SAIDA**

**Assistant Professor**

**Head of the Department**

**Dr. SYED KHASIM**

**Professor**

**Submitted for Viva voce Examination held on**

**External Examiner**

**ACKNOWLEDGEMENT**

We are indebted to the **Management** for providing me an opportunity with excellent academic, infrastructural Lab facilities to carry out my U.G program successfully.

We would like to express my deepest sense of gratitude towards my Internal Guide, **MD. JOHN SAIDA , Assistant Professor** in Department of CSE for his encouragement and valuable guidance in bringing shape to this dissertation.

We are grateful to **Dr. SYED KHASIM**, HOD & VICE-PRINCIPAL Department of Computer Science & Engineering, **ESWAR COLLEGE OF ENGINEERING,** Narasaraopet affiliated **JNTUK Kakinada** Who have given for his encouragement and motivation.

We express my deep gratitude and regards to our beloved principal **Dr. G. NAGA MALLESWARA RAO,** who have given support for the project or in other aspects of our studies at **ESWAR COLLEGE OF ENGINEERING, Kesanupalli, Narasaraopet**, affiliated **JNTUK Kakinada**.

We are thankful to all the **Faculty Members** in the department for their teachings and academic support and thanks to **Technical Staff and Non-teaching staff** in the department for their support.

At last but not least we thank all my well-wishers for rendering necessary support during the execution of this work.

**DECLARATION**

We hereby declare that the Project report titled **“A USER-CENTRIC MACHINE LEARNING FRAMEWORK FOR CYBER SECURITY OPERATIONS CENTER”** is bonafide work done by us, under the guidance of **MD. JOHN SAIDA, Asst. Professor, Eswar College of Engineering.** This report is submitted in partial fulfillment of the requirements for the award of the degree **Bachelor of Technology** in **CSE*.***

We also declare that this project is a result of my own effort and that has not been copied from anyone and we have taken only citations from the sources which are mentioned in the references.

This work was not submitted earlier at any other University or Institute for the award of any degree.

**NAGARJUNA REDDY ANNAPUREDDY (16JE1A0538)**

**RAKESH KINTHALA (17JE5A0501)**

**LINGA BABU ADANKI (16JE1A0526)**

**SURESH BABU CHUNDU (16JE1A0557)**

**Place :** Kesanupalli

**Date :**

**ABSTRACT**

In order to ensure a company's Internet security, SIEM (Security Information and Event Management) system is in place to simplify the various preventive technologies and flag alerts for security events. Inspectors (SOC) investigate warnings to determine if this is true or not.

However, the number of warnings in general is wrong with the majority and is more than the ability of SOC to handle all awareness Because of this, malicious possibility. Attacks and compromised hosts may be wrong. Machine learning is a possible approach to improving the wrong positive rate and improving the productivity of SOC analysts. In this article, we create a user-centric engineer learning framework for the Internet Safety Functional Center in the real organizational context.

We discuss regular data sources in SOC, their work flow, and how to process this data and create an effective machine learning system. This article is aimed at two groups of readers. The first group is intelligent researchers who have no knowledge of data scientists or computer safety fields but who engineer should develop machine learning systems for machine safety.

The second groups of visitors are Internet security practitioners that have deep knowledge and expertise in Cyber ​​Security, but do Machine learning experiences do not exist and I'd like to create one by themselves. At the end of the paper, we use the account as an example to demonstrate full steps from data collection, label creation, feature engineering, machine learning algorithm and sample performance evaluations using the computer built in the SOC production of Seyondike .