# 

# Student Project: Network Analytics

|  |  |
| --- | --- |
| Project Title | Network Analytics: An Intrusion Detection Alarm System |
| Team Member: | Renato Barroco & Joaquin Gianantonio |

## Project Description

**Problem definition / Problem mitigation**

|  |
| --- |
| With the expanded applications of modern-day networking, network infrastructures are at risk from cyber-attacks and intrusions, which can compromise their availability, confidentiality, and integrity. These threats are difficult to detect unaided.  These attacks affect all types of companies, from large corporations with specialized response resources but with immense number of network connections at risk to monitor, to small companies with no dedicated network specialists.  We propose developing a machine learning based network intrusion detection ***alarm system*** to provide rapid identification of intrusions, letting network administrators take corrective action to terminate these threats and mitigate its effects on users and providers. |

**Key Research Questions that the Project Answers**

|  |
| --- |
| What are the types of threats to the network flow?  What are the benefits from identifying not just an intrusion but also the type of attack?  The ability to use a multi-classification analysis provides a robust identification of the network flow giving the security team a better understanding of the type of port flow and provide a better response to the threat. |

**Project Deliverables**

|  |
| --- |
| Our multi-classification model evaluates port-level statistics and delta port statistics to provide insight into the network’s behaviour.  The intrusion detection alarm system will monitor network flow at port level, robustly identify threats with high accuracy and provide multi-class classification results, through a dashboard and/or by alerting response personnel in the organization. |