National College of Ireland

Configuration Manual

MSc Internship
Cyber Security

Pradeep Raj Mohanur Jagadeesan
Student ID: X18165672

School of Computing
National College of Ireland

Supervisor: Muhammad Iqbal

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Pradeep Raj Mohanur Jagadeesan
Student ID:	X18165672
Programme:	MSc in CyberSecurity **Year:** 2019
Module:	Internship
Lecturer:	Muhammad Iqbal
Submission Due Date:	8th January 2020
Project Title:	A Framework Design to Improve and Evaluate the Performance of Security Operation Center (SOC)
Word Count:	347 **Page Count:** 2

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.
I agree to an electronic copy of my thesis being made publicly available on NORMA the National College of Ireland's Institutional Repository for consultation.

Signature: .....

Date: .....

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Pradeep Raj Mohanur Jagadeesan
Student ID: x18165672

1 SIEM Tool Interface:

The below image shows in the console interface of the SIEM tool IBM Qradar which can be accessed by an analyst.

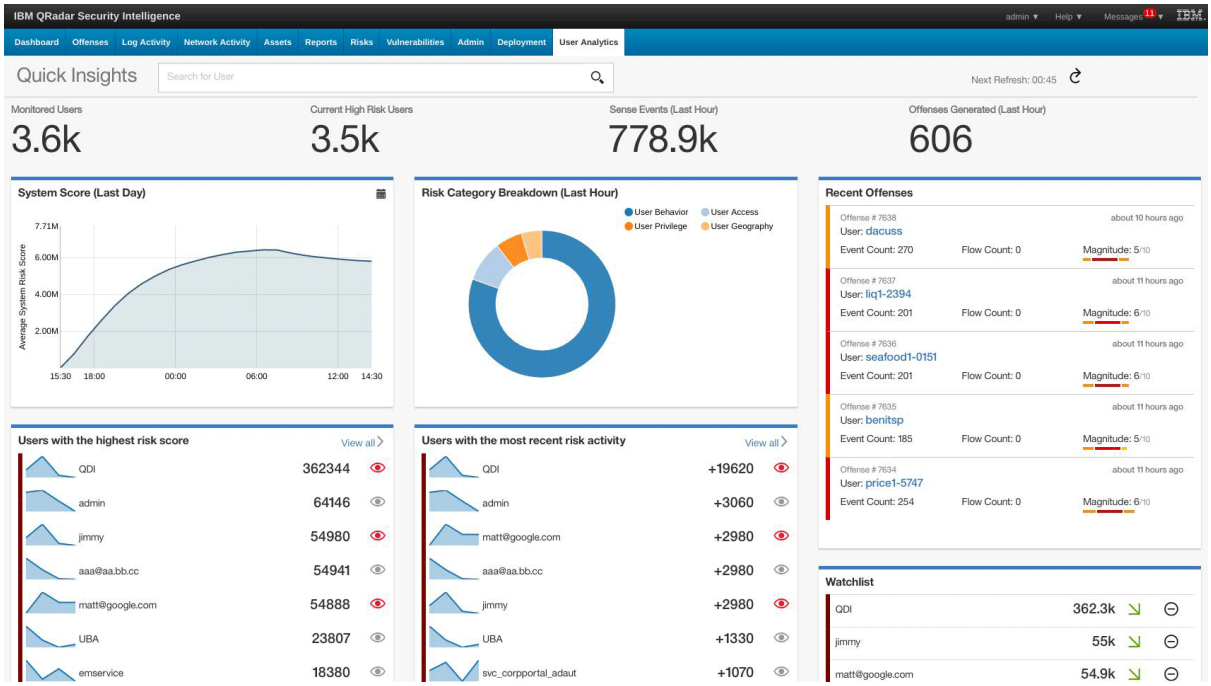

Figure 1 Qradar Interface[1]

2 Internship activity:

Company: Ward Solutions Month Commencing: September 2019

- Learnt the basic functioning of SOC.
- Performed threat hunting.
- Learned to handle the incident.
- Performed penetration testing.
- Developed python tools to reduce the time for daily tasks.
- Learned the configuration of SOC.

[1] https://www.ibm.com/security/security-intelligence/qradar

3 Internship Feedback:

Company: Ward Solutions Month Commencing: September 2019

WardSolutions www.ward.ie | www.wardinfosec.co.uk

To whom it may concern, November 29th 2019

Internship Feedback Form

Pradeep Raj Mohanur Jagadeesan attended an internship in ward Solutions for three months between the dates 2nd September 2019 and 29th of November 2019.

During this time, Pradeep was embedded into the Ward Solution SOC (Security Operations Centre) team under my supervision. During the course of the internship, Pradeep worked in the following areas:

- SIEM Management
- Incident Response
  - Alert investigations
  - Threat hunting
- SOC improvement
  - Development of API solutions
- Network Traffic analysis
- SOC Management
- Web App Penetration Testing

By gaining experience in the above areas, Pradeep was able to gain an understanding of SOC operations and management including the following areas

- SOC operations Best practice
- SOC solution development
- SOC team management
- SOC performance measurement and Management

Pradeep has used this knowledge to develop a research project titled (Working title) "**Building a SOC framework to enhance the performance of the SOC**"

I found Pradeep to be an excellent intern and he was a valuable addition to the team, his dedication, innovation and enthusiasm made him a pleasure to work with and I would happily recommend him to future employers, he is a credit to both NCI and to the School of Computing.

If you have any questions please do not hesitate to contact me

Kind Regards

Kenneth Murphy

SOC Manager Ward Solutions

Kenneth.Murphy@ward.ie

Unit 2054 Castle Drive
Citywest Business Campus
Dublin 24
Ph +353 1 6420100
Fax +353 1 6420161
Email info@ward.ie

25 Talbot Street
Cathedral Quarter
Belfast BT1 2LD
Ph: +44 28 90-823688
Fax: +44 28 90-823601
Email info@wardinfosec.co.uk

50 O'Connell Street
Ennis
Co Clare
Ph +353 1 6420100
Fax +353 1 6420161
Email: sales@ward.ie

Registered in Ireland no 316165
Vat no IE6336165K
Registered office: unit 2054
Castle Drive, Citywest Business Campus
Dublin 24, Ireland
Directors: Pat Larkin, Patricia Larkin, Paul Hogan