AI BASED INTRUDER PREVENTION SYSTEM WITH INCORPORATING AN IMPROVED KNN

By
Vishnu Mohan Edala Dhanraj
Shivang Rangoonwala

Introduction

- Security and Privacy
- Multilayers of protection
- Threats - Recognise and avoid them
- Cyber safety & Security : making smart cyber defence choices.

Problem Statement

- Any Network of an organisation faces threats or cyber attacks.
- Cisco states that 31% of their organisations faced threat and attacks in their operations part.
- Data Breach
- Malware Attack & Hacking
- Single factor passwords
- Insecure Application User Interface (API)

Solution

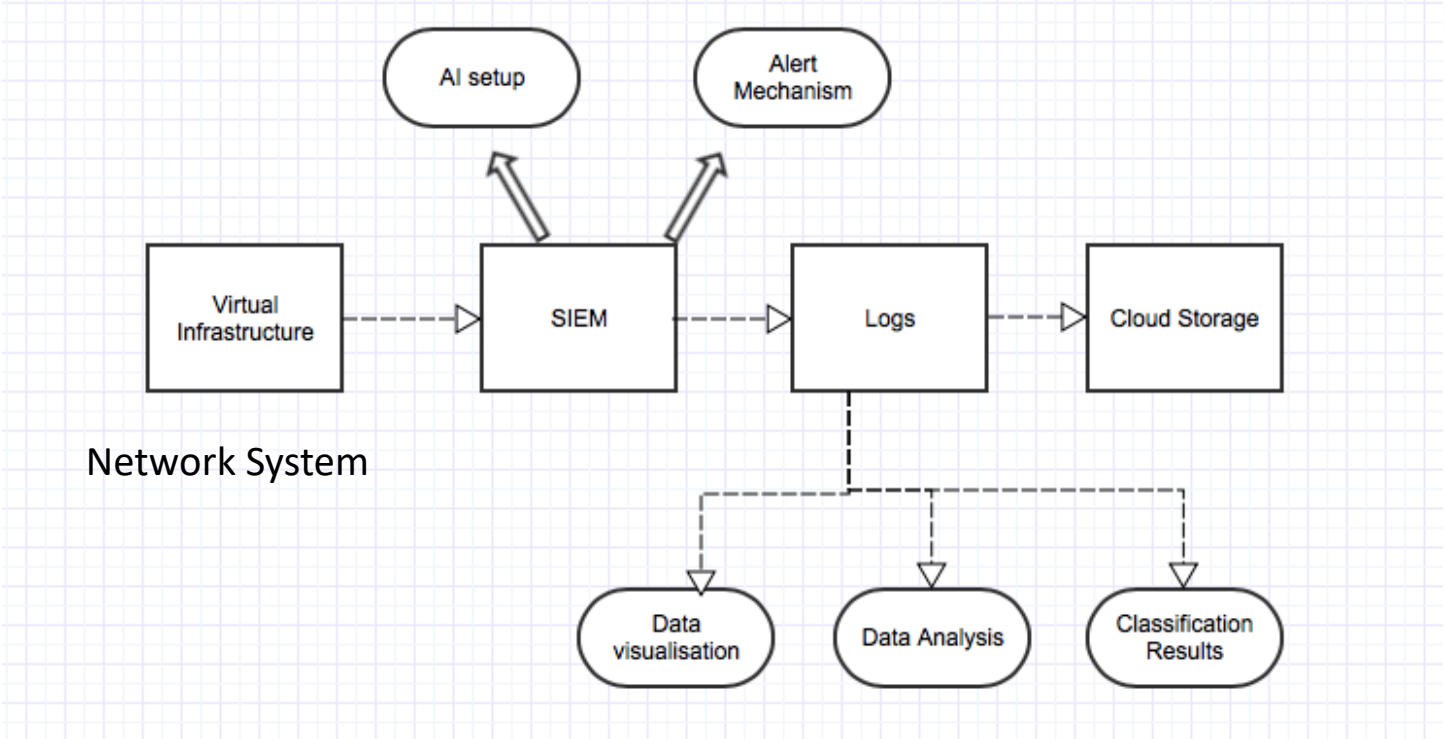
- Intelligent systems powered by data-centric algorithms and machine learning.
- more proactive prevent threats in real-time.

- Detects Behaviour patterns, typical signals and triggers and the potential deviations and the vulnerabilities.
- proactively destroy a threat in its nascent stage or Safe Guards.

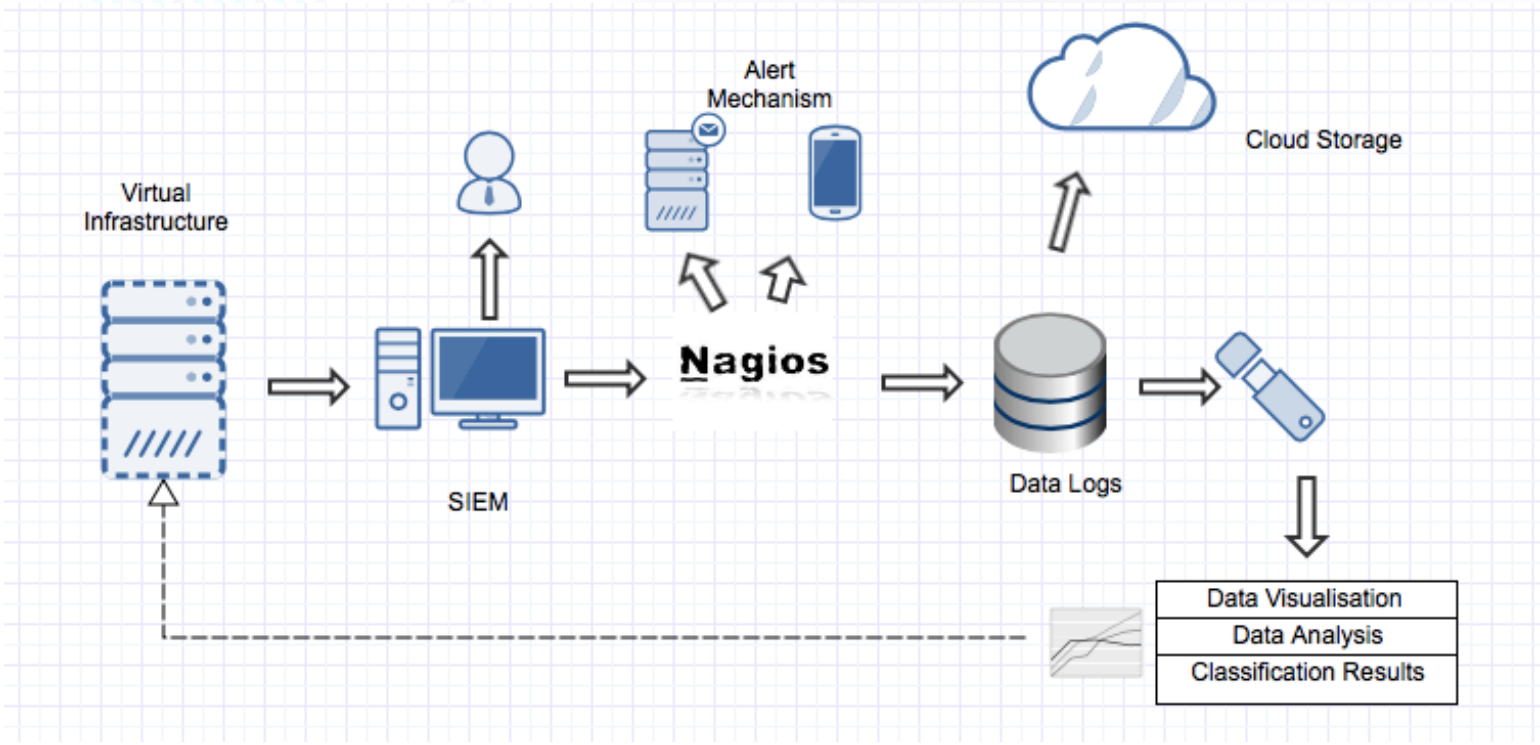
AI BASED INTRUDER PREVENTION SYSTEM WITH INCORPORATING AN IMPROVED KNN

- Machine Learning Algorithms
- Predictive Analysis
- Notify Intruder actions
- Proactive and prevent Threats

Architecture



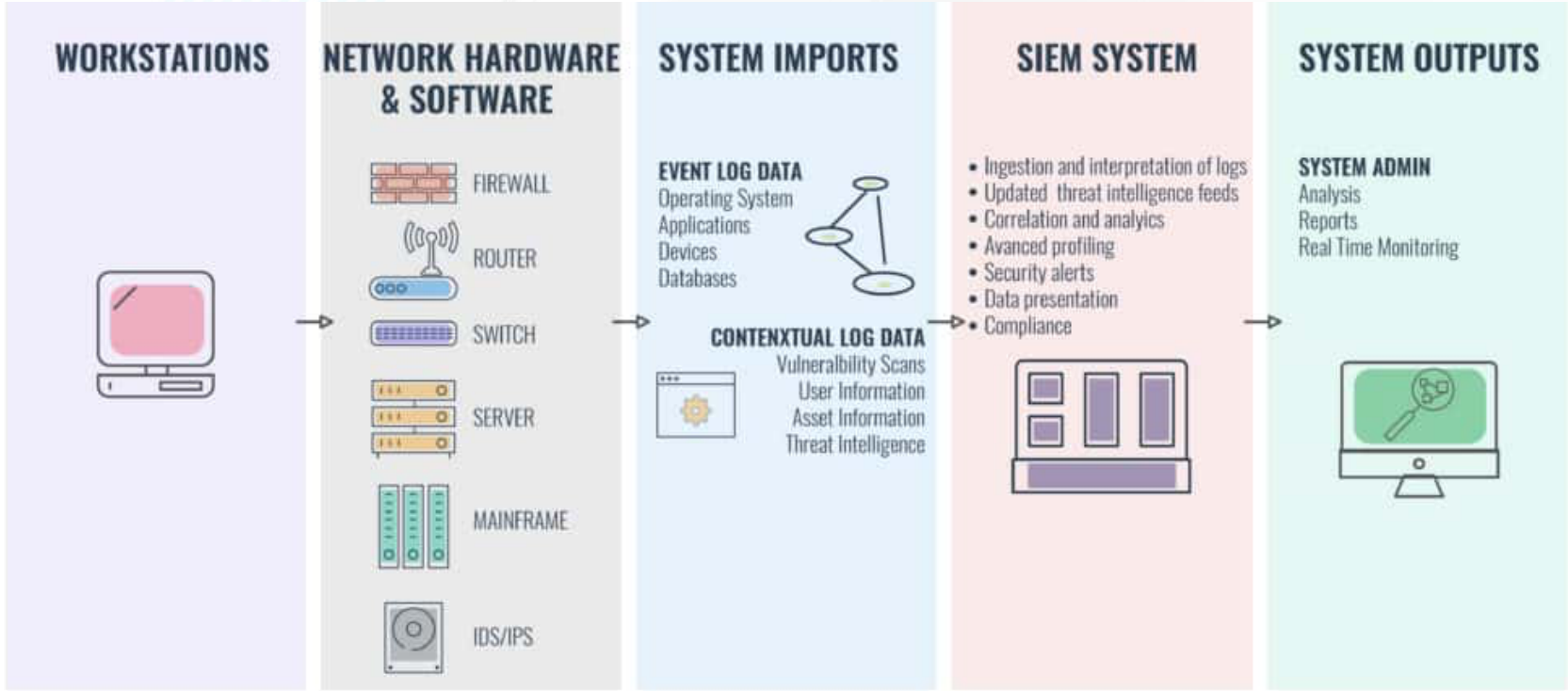
Proof of Concept



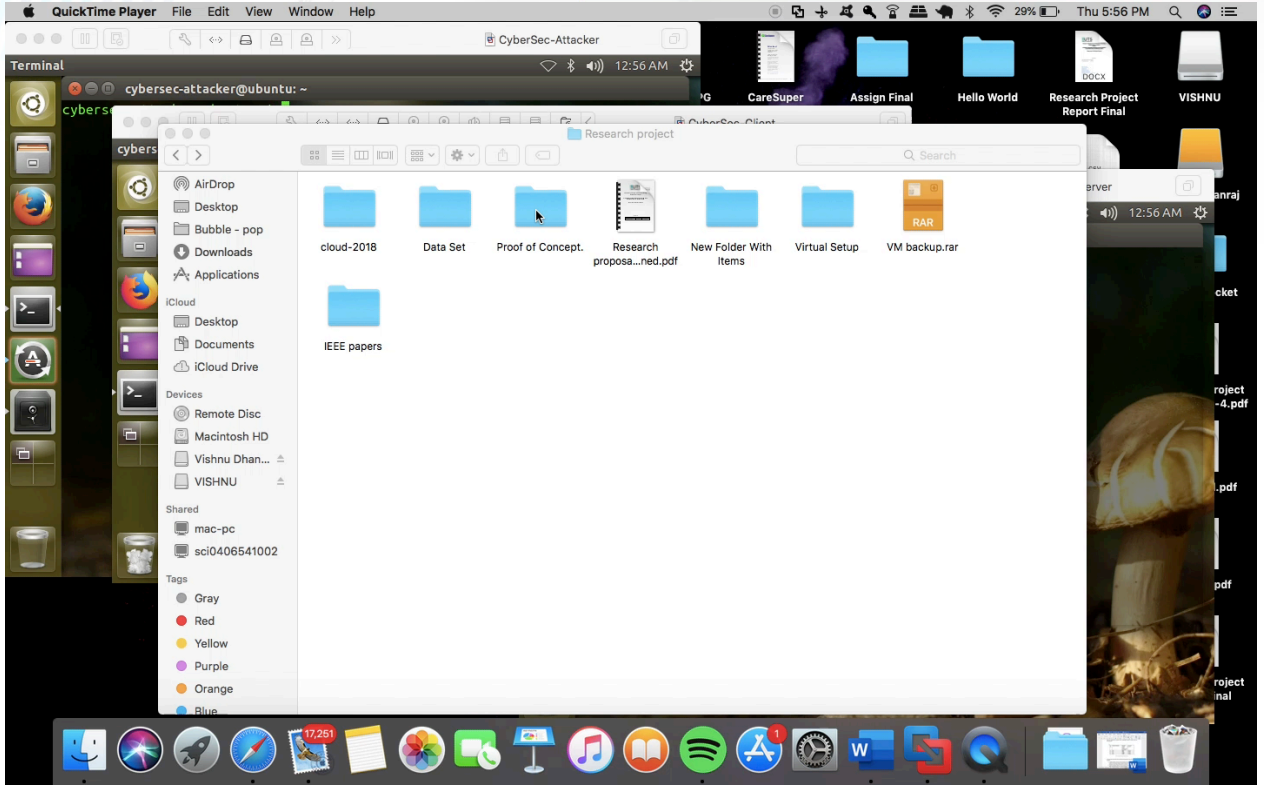
Software System

- Network - Virtual - ubuntu 14.04
- Netwox/Netwag
- Wireshark Tool
- Nagios
- Exploratory
- Knime (Machine Learning Algorithms)
- Python

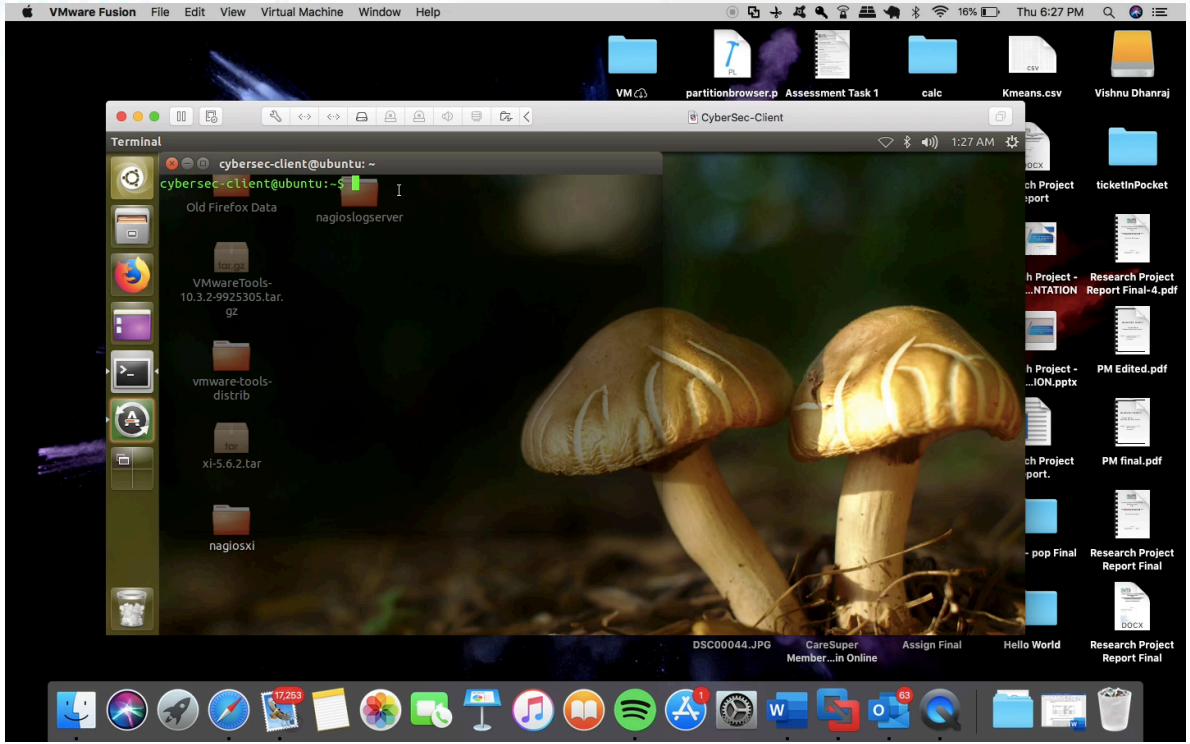
PROTOTYPE


WORKSTATIONS
NETWORK HARDWARE & SOFTWARE
FIREWALL
ROUTER
SWITCH
SERVER
MAINFRAME
IDS/IPS
SYSTEM IMPORTS
EVENT LOG DATA
Operating System
Applications
Devices
Databases
CONTENXTUAL LOG DATA
Vulneralbility Scans
User Information
Asset Information
Threat Intelligence
SIEM SYSTEM
• Ingestion and interpretation of logs
• Updated threat intelligence feeds
• Correlation and analyics
• Avanced profiling
• Security alerts
• Data presentation
• Compliance
SYSTEM OUTPUTS
SYSTEM ADMIN
Analysis
Reports
Real Time Monitoring

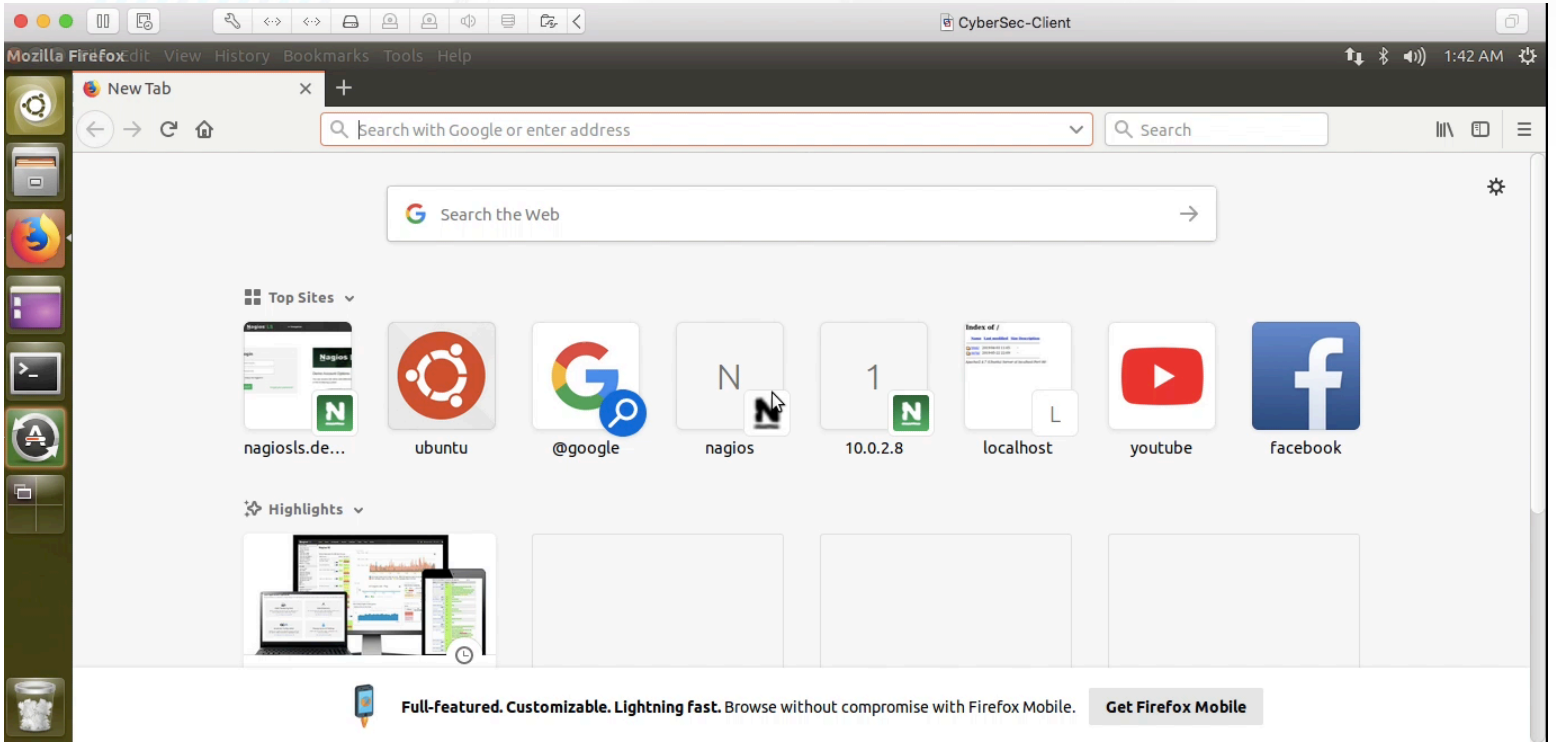
Virtual Setup



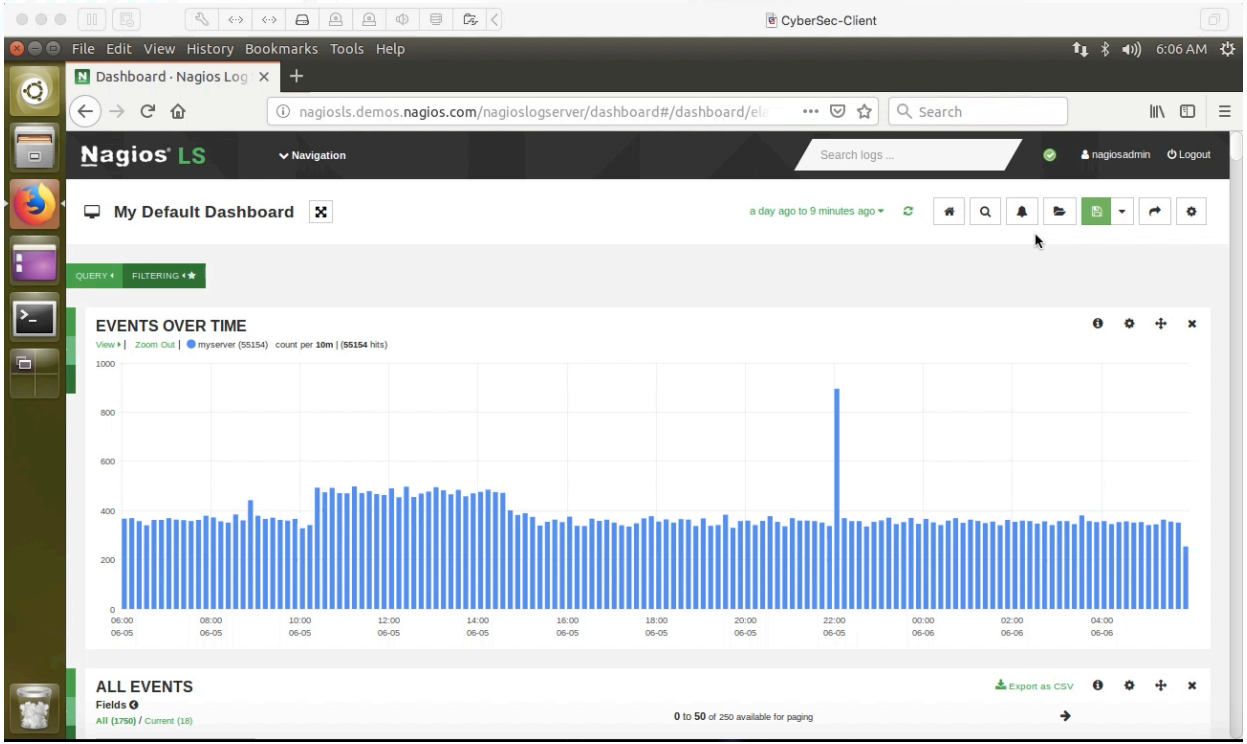
Cyber attack – Demo



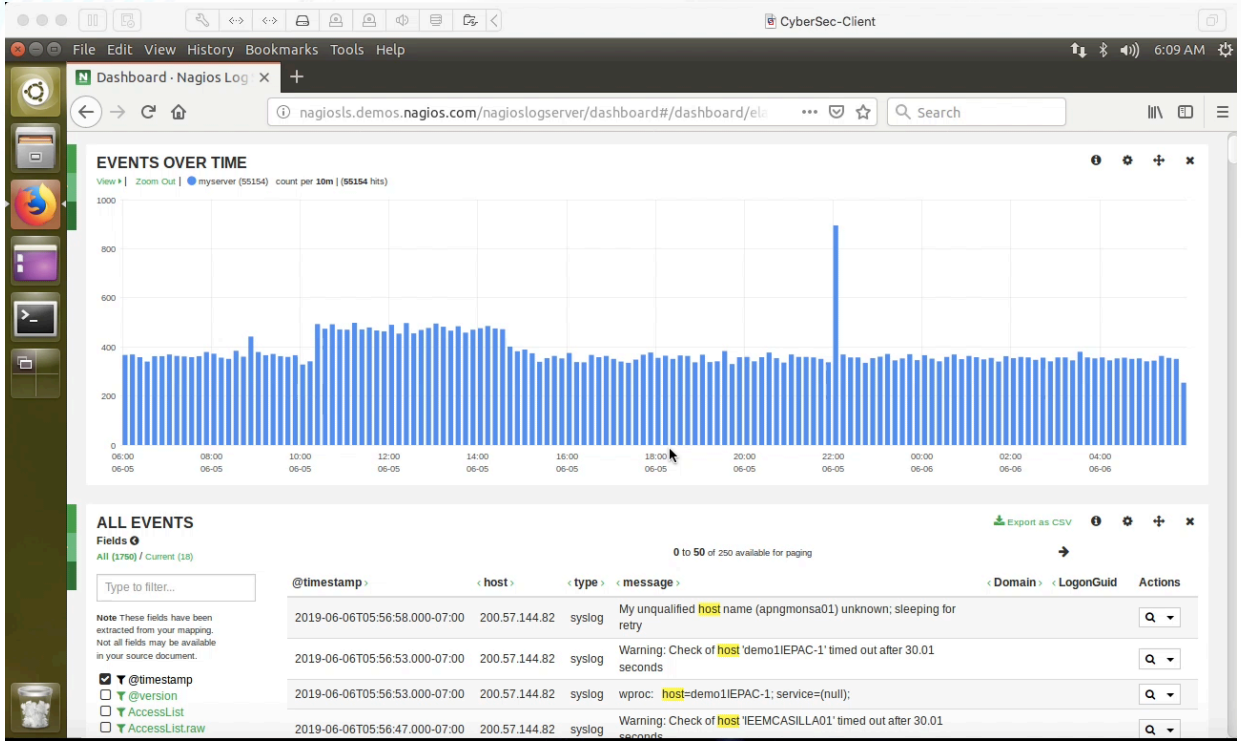
Dashboard System



Alert Monitoring System



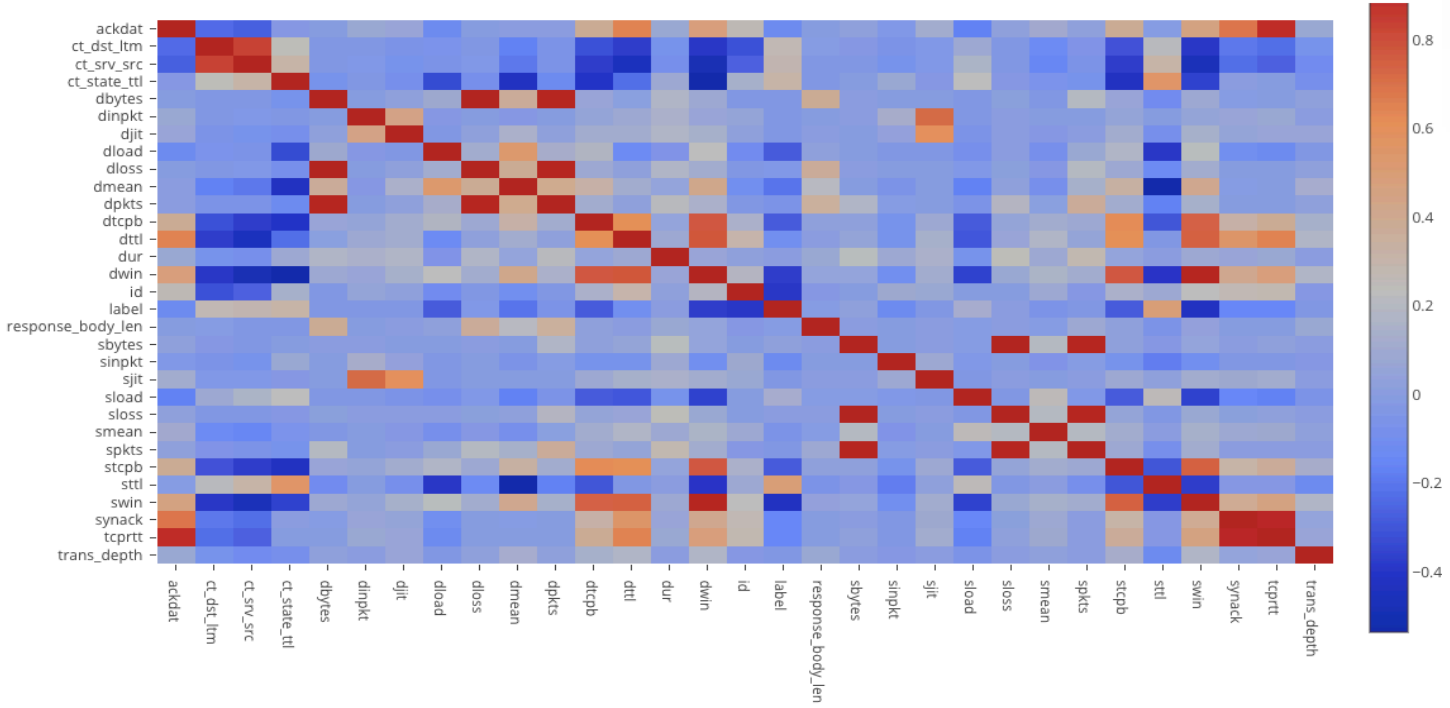
Log Extraction



DATA SET

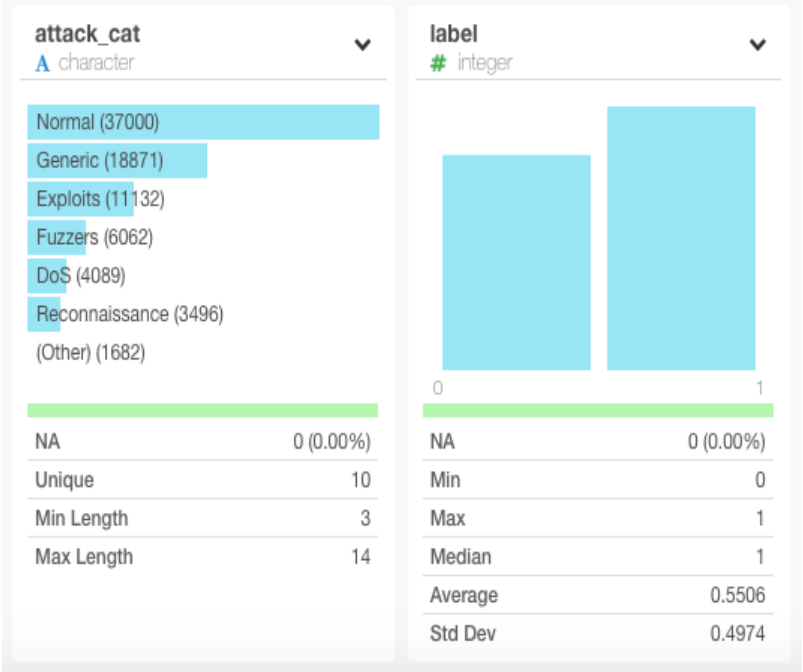
- Published by IXIA Perfect Storm tool in the Cyber Range Lab of the Australian Centre for Cyber Security (ACCS)
- Consists of 82333 rows and 45 attributes
- Nine Types of Attacks (Fuzzes, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode and Worms).

Exploratory Analysis



Categorisation

Column 1	Column 2	Correlation
dbytes	dloss	1
sbytes	sloss	1
dloss	dpkts	0.98
dbytes	dpkts	0.98
sloss	spkts	0.97
sbytes	spkts	0.97
dwin	swin	0.96
synack	tcprtt	0.94
ackdat	tcprtt	0.9
ct_dst_ltm	ct_srv_src	0.84
dttl	dwin	0.78
dwin	stcpb	0.77
dtcpb	dwin	0.77
dttl	swin	0.75
stcpb	swin	0.74
dtcpb	swin	0.74




2017/18
2016/17


2017/18
2016/17

Questions ?