APPLICATION OF MACHINE LEARNING, BIG DATA AND EDGE COMPUTING FOR CYBERSECURITY ANALYTICS AT SCALE

ABDUL RAHMANSATAR

Telus Corporation

INTRODUCTION:

Signature based and rule based methods used by existing SIEM (Security Incident Event Management Tools) solutions in the market lack the ability to detect zero day attacks. In a world where IoT and M2M is the future, scalable and automated methods are needed to detect cybersecurity attacks on infrastructure which is based on IoT devices which are lightweight, resource constrained and lack proper security controls and hence are more vul- nerable to zero day exploits.

AIM

To use big data, cloud, mobile edge computing, behavior al analytics, AI and Deep Learning Methods for cybersecurity analytics at scale for critical infrastructure security.

MATERIAL ANDMETHODS

At TELUS, we have developed behavioral profiling and anomaly detection and other deep learning techniques using LSTM, CNN and Graphical Neural Networks for network intrusion detection which are used at scale for protecting enterprise networks and IoT device fleets. The techniques have been successfully benchmark edonvarious data sets and are deployed inproduction for detection of malicious net work behavior and end points including DGA Domains, Phishing domains, Bad IP Blocks, IP in flux, APT, DOS, port scan and address scans etc. Modelen semble and correlations of IOCs (indicators of compromise) isused to further improve these curity and threat detectionrate. TELUS Security Analytics Platform Architecture has to scale to billions

f data points (terabytes of data) per day and for that we employ complex feature extraction and machine learning inference on the edge and leverage Hadoop and server less architecture on the cloud. The detections from the security analytics platform integrate with off the shelf SIEM and SOAR tools so that they can be actioned through automated playbooks developed by the Incident Response teams atTELU

RESULTS

Various open source, partner and proprietary data sets were used to test the efficacy of the anomaly detection and deep learning approach we have developed for various security analytics capabilities.Were cordedan accuracy of over 85% without deep learning approaches for detecting DGA and Phishing domains and an accuracy of over80% when using anomaly detection and behavior alanalys is methods for detecting volumetric DOS, PortScan, Address Scan, R2L and U2 Rattacksetc.

CONCLUSIONS

Behavior alanalytics, Deep Learning and AI based methods perform better when it comes to detecting zero day attacks. Correlation of IOCs (indicatorsofcompromise) from various machine learning and behavior al analysis models further improves the security detection accuracy. Edge Analytics help sto improve there sponsetime and through put of the platform. Big data platforms such as Hadoopands erverless cloud architecture is needed to scale to tera bytes of data perday and perform security analytics at scale

KEYWORDS

Cybersecurity Analytics, Edge Computing, Deep Learning, AI, Machine Learning, Security Automation, IoT Security, Big Data, Server less architecture, Cloud

BIOGRAPHY

Abdul Rahman Sattar Abdul Rahman Sattaris the Lead Architect of Cy- ber security Analytics at TELUS. Inthisroleheis leading the road map for cyber security analytics using AI and Machine Learning. He was a speaker at Google NEXT 2020 and TMLS 2020 Annual Machine Learning Conference where he presented on Malware Detection using Machine Learning. Hisre-cent work around security analytics using Deep LSTM approach esto detect DGAs was accepted in multi plesecurity conferences. Heisthe steering com-mittee member at AISC (https://ai.science/), a research based machine learning community in Toronto, where he is leading the Edge Analytics, IoT and Cyber security stream