wipro holmes

wipro

Reimaging Cyber Defense Process

Empower analysts for faster investigation of security incident

Intro

Today's Cybersecurity Analysts are able to identify False Positive triggers from SIEM *(security information and event management)* system only after investigating the offense. Hence, unable to focus actual threats on daily basis. Also majority of the offenses are False Positive, therefore more time is spent in investigating the false threats and the system enhancement becomes difficult for the domain experts.

To identify the false positive and true positive alerts raised from SIEM (Q-Radar system) to improve the cyber defense process with Advance AI capabilities with greater accuracy is the objective of our solution.

The Solution

Wipro Holmes Reimagining Cyber-defense process is a AI solution to identify the root cause for False Positive alerts and provides AI guided insights to cyber security analysts to reduce time & effort to focus on actual alerts and reduce the associated risk of missing threat due to pipeline issues. Also, enabling the team with inferences to significantly reduce manual efforts & human errors thus regaining associated benefits of time for more productive activities.

Microsoft Workloads are used such as:

Azure Blob storage – for storing the data from SIEM tools (QRadar) and IP reputation data.
Azure Active Directory – user validation
Azure ML Studio – ML pipelines for build, deploy & monitor the AI models (the complete MLOps to automate & accelerate the machine learning lifecycle).

- ML Flow – for model tracking, registering & serving
- Github – artefact repository
- **Azure AutoML** for automating ML model development
- **Azure docker Container** – for model packaging
- **Azure Kubernetes Service** – for application deployment & management across clusters

Azure Compute – container/cluster instance - For model training, Azure inference for real time inference.

Key takeaways

- Solution provides real-time event assessment to identify pipeline issues.
- Detect data issues in pre-emptive stage of events occurred.
- Evaluate the improvement/deterioration of the existing system
- Modular and scalable solution to any new use-cases.

Key features

Identifies false alerts due to data inconsistency with greater accuracy

Empowers Cyber-Security Analysts with **Inferences** to close the incidents or offenses

Reduces associated risk by correctly identifying the alerts which the existing tool misses out

Standalone System – **Easily pluggable** to existing device as well as on any new devices

Benefits

- Provide inferences on root cause of false positive.
- Incorporate dynamicity of data and use-case.
- More rapidly offense investigation.
- Significantly reduces the time and effort in investigation.

Wipro Limited
Doddakannelli, Sarjapur Road,
Bangalore-560035,
India

Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
wipro.com

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading global information technology, consulting and business process services company. We harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help our clients adapt to the digital world and make them successful. A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, we have over 175,000 dedicated employees serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.

For more information,
please write to us at
info@wipro.com