SMART INDIA HACKATHON 2023

SIH

Basic Details of the Team and Problem Statement

Ministry/Organization Name/Student Innovation: Ministry Of Home Affairs

PS Code: SIH1408

Problem Statement Title: IT System log analyzer

Team Name: Enigma Hunters

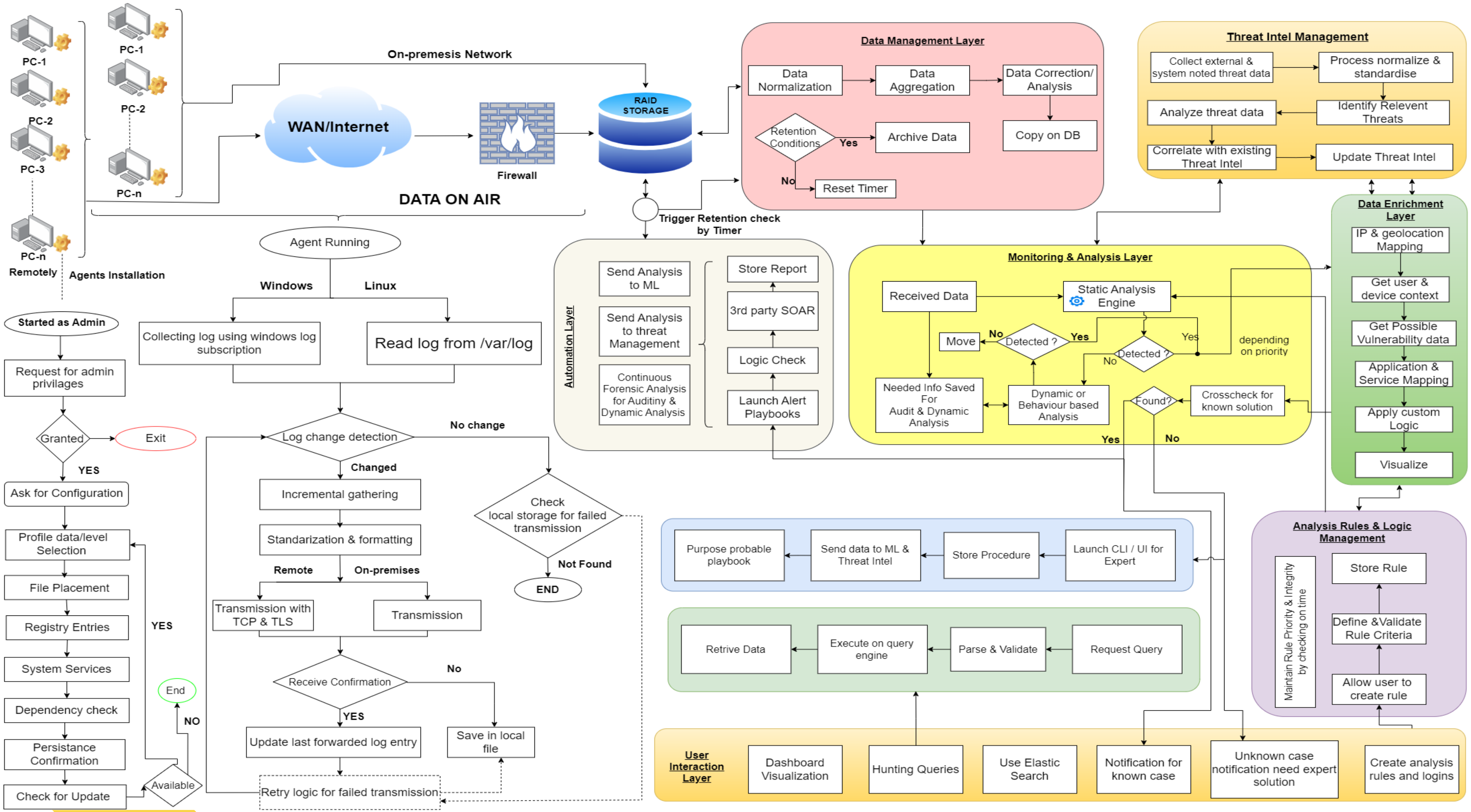
Team Leader Name: Durjoy Majumdar

Institute Code (AISHE): U-0020

Institute Name: Koneru Lakshmaiah Education Foundation

Theme Name: Blockchain And Cybersecurity

Idea/Approach Details



PC-1, PC-2, PC-3, PC-n
Remotely
Agents Installation
PC-1, PC-2, PC-n
On-premesis Network
WAN/Internet
Firewall
RAID STORAGE
DATA ON AIR

Started as Admin
Request for admin privilages
Granted
Exit
YES
Ask for Configuration
Profile data/level Selection
File Placement
Registry Entries
System Services
Dependency check
Persistance Confirmation
Check for Update
YES
Available
NO
End

Agent Running
Windows
Linux
Collecting log using windows log subscription
Read log from /var/log
Log change detection
No change
Changed
Incremental gathering
Standardization & formatting
Remote
On-premises
Transmission with TCP & TLS
Transmission
Receive Confirmation
No
YES
Update last forwarded log entry
Save in local file
Retry logic for failed transmission
Check local storage for failed transmission
Not Found
END

Trigger Retention check by Timer

Data Management Layer
Data Normalization
Data Aggregation
Data Correction/ Analysis
Retention Conditions
Yes
Archive Data
Copy on DB
No
Reset Timer

Threat Intel Management
Collect external & system noted threat data
Process normalize & standardise
Identify Relevent Threats
Analyze threat data
Correlate with existing Threat Intel
Update Threat Intel

Automation Layer
Send Analysis to ML
Send Analysis to threat Management
Continuous Forensic Analysis for Auditing & Dynamic Analysis
Store Report
3rd party SOAR
Logic Check
Launch Alert Playbooks

Monitoring & Analysis Layer
Received Data
Static Analysis Engine
Move
No
Detected ?
Yes
Detected ?
No
Yes
depending on priority
Needed Info Saved For Audit & Dynamic Analysis
Dynamic or Behaviour based Analysis
Found?
Crosscheck for known solution
Yes
No

Data Enrichment Layer
IP & geolocation Mapping
Get user & device context
Get Possible Vulnerability data
Application & Service Mapping
Apply custom Logic
Visualize

Purpose probable playbook
Send data to ML & Threat Intel
Store Procedure
Launch CLI / UI for Expert

Retrive Data
Execute on query engine
Parse & Validate
Request Query

Analysis Rules & Logic Management
Maintain Rule Priority & Integrity by checking on time
Store Rule
Define &Validate Rule Criteria
Allow user to create rule

User Interaction Layer
Dashboard Visualization
Hunting Queries
Use Elastic Search
Notification for known case
Unknown case notification need expert solution
Create analysis rules and logins

To get a more clear view of the Flowchart kindly follow - THE LINK

Idea/Approach Details

Idea Description:

- Log files will be gathered from various CRPF units across the geography via **Agents (Uses Syslog Protocol)** installed in the local machines.
- **To Solve the challenge of gathering log from a decentralized network to a centralized server we have combined SSH and SYSLOG protocol in our agent. Which is done for the first time in computer technology.**
- The transmission occurs in a dual layer **encrypted channel** that uses SSH and TLS.
- After storing the logs in the central repository, our Monitoring & Analysis Layer (compute optimized system) kicks in for **Static Signature(s) based threat detection.**
- Upon analysis, the log data goes under data-enrichment layer which **exposes the insight** to the Analysis & Logic management layer to make the expert interaction a frictionless experience.
- Threat remedies in form of **playbooks** can be triggered via the Automation Layer and 0-Day threats needs expert interaction.
- Our ML program continues **learns from the expert interaction and 3rd party DBs** and make our threat intel a robust system.
- The Expert interaction layer allows to **write custom detection rules & logics.** It also facilitates the alerts management system.
- Our system also have data retention engine, that works **using life-cycle policy** for the backup and archival of our log files.
- The Agent Software(s) are capable of receiving **updates and patches** from the central system.

It is not possible to explain our solution here properly because of space limitation. We kindly request you to follow the link - LINK

Use Cases: Only the Expert analyst is the User here with the use case.

- **Expert Threat Analysis**: Cybersecurity experts analyze incoming log data to identify potential threats and vulnerabilities.
- **Automated Playbook Execution**: Experts develop and deploy automated playbooks to respond to known threats swiftly and effectively.
- **Manual Threat Analysis**: In cases of novel or complex threats, experts manually investigate and analyze the situation to develop tailored responses.
- **Expert Guidance**: Experts provide guidance to on-site personnel on how to respond to specific threats, ensuring a coordinated and effective response.

Technology stack:

- Django Python.
- ReactJS with ChartJS.
- Syslog, SSH, TLS.
- SQL based RDBMS.
- PowerShell & Bash.

Dependencies :

- Elastic Search
- Kibana
- MITRE ATT&CK® Navigator
- Fluentd
- Graylog
- Grafana

Team Member Details

Team Leader Name: Durjoy Majumdar

Branch : B.Tech Stream : CSE-H Year : III

Team Member 1 Name: Arjun S

Branch : B.Tech Stream : CSE-H Year : III

Team Member 2 Name: Anuj Kandel Sharma

Branch : B.Tech Stream : CSE-H Year : III

Team Member 3 Name: Sambandha Bhattarai

Branch : B.Tech Stream : CSE-H Year : III

Team Member 4 Name: Pranavi Boyina

Branch : B.Tech Stream : CSE-H Year : III

Team Member 5 Name: Sri Sai Priya Rayidi

Branch : B.Tech Stream : CSE-H Year : III

Team Mentor 1 Name: Dr. Radhika Rani Chintala

Category : Academic Expertise : Network Security Domain Experience : 17 Years

Team Mentor 2 Name: Dr. Prashant Kumar Shukla

Category : Academic Expertise : Cybersecurity & AI/ML Domain Experience : 20 Years