ENIGMA
HUNTERES

SIH 2023

ENIGMA HUNTERS

PRESENTING

LOGALYZER

IT LOG ANALYZER

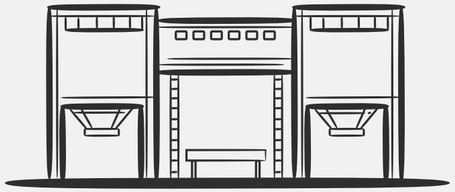
PS - 1408

IDEATION

PROBLEMS ENCOUNTERED

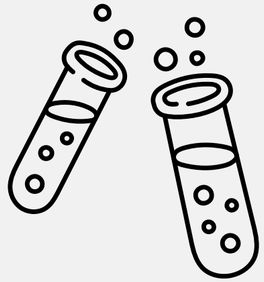
TRANSPORT

Secure
Real-time
Incremental
Reliable
Remote Data Aggregation



STORAGE

Centralized
Scalable
Reliable
Encrypted
Redundant



ANALYSIS

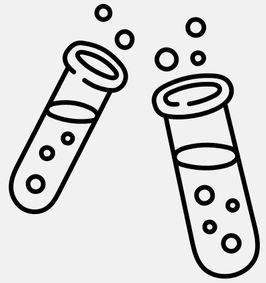
Real-time
Signature Based
Behaviour Based
Anomaly Based
Threat remediation system

PS - 1408

IDEATION

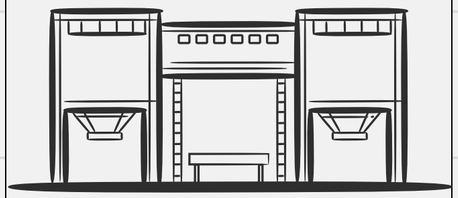
TRANSPORT

+



ANALYSIS

+



STORAGE

=

LOGALYZER

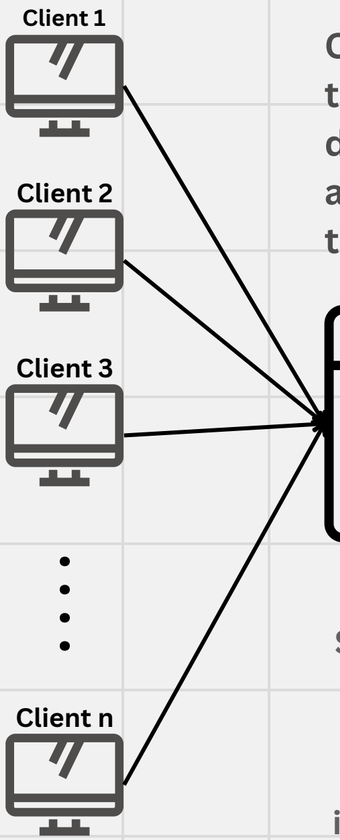
HOW OUR SOLUTION STAND OUT?

1. Log collection from geographically isolated devices.
2. End-to-End data integrity.
3. Centralized analysis dashboard.
4. Anywhere accessibility.
5. Granular access control.
6. Scalability & Flexibility.
7. Huge and Up-to-Date Threat Intelligence.
8. Logical, behavioral, anomaly and signature based detections.
9. Compliance with security standards.

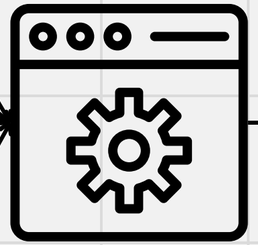
NO OTHER EXISTING SOLUTIONS DEALS ALL THESE 3 ASPECTS!

FLOW DIAGRAM - APPROACH

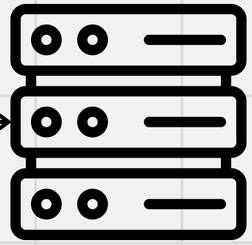
REGISTER UNITS & DEVICES → AGENT IS SHIPPED WITH ACCESS KEY → COMMUNICATION OF AGENT WITH CENTRAL SERVER



Centralized system that enables experts to monitor and analyze system logs to detect and respond to security threats and breaches in real-time or near real-time.



Agent or Software that runs in the client side to push log files incrementally



- Store
- Analyse
- Alert
- Dashboard

COMMUNICATION OF AGENT WITH CENTRAL SERVER → THREATS DETECTED, ALERTS RAISED AND EXPERTS GET NOTIFIED → AUTOMATED REMEDIATION. SUGGESTION AND PLAYBOOKS

TECHNICAL ASPECTS

PS - 1408

STACK

- Django
- ReactJS
- Postgreql
- Redis Queue

TECHNOLOGIES

- Microservices
- Regex Engine
- Websockets
- Telemetry (ANALYTICS)

DEVELOPMENT

- GitHub Actions
- Bulkgate (SMS)
- Django Mail
- LeafLet (Map)

PROS

- Vast threat intelligence Database and telemetry.
- Compute, Storage and Bandwidth optimized.
- No involvement of 3rd party services except libraries.

TIERED: PROJECT REQUIREMENTS

Assume: handling traffic from 50+ units, each with an average of 5 devices, in a geographic landscape like India

COMPUTE & STORAGE	BANDWIDTH	CLIENT	MISCENALEOUS	COST (C&S)	RECOMMENDED TIERS
INTEL XEON SCALABLE, 128GB RAM, 64 TB RAID-5 SSDS	1 GBPS	I9, RAM 32 GB	ADVANCED	15784$	PRODUCTION
INTEL XEON PLATINUM, 64GB RAM 16 TB RAID-5 SSDS	500 MBPS	I7, RAM 16 GB	REGULAR	10871$	PRE-PRODUCTION
INTEL XEON MAX, 32 GB RAM, 128 GB RAID-5 SSDS	100 MBPS	I5 - RAM 8 GB	OCATIONAL	6110$	DEVELOPMENT
INTEL XEON W, 16 GB RAM, 128GB RAID-5 SSDS	50 MBPS	I3 - RAM 4 GB	MINIMAL	2238$	TESTING

OUR THREAT INTEL STATISTICS

Our default shipment threat intelligence system provides a robust foundation for safeguarding against cyber threats. Here's a detailed breakdown of the threat intelligence data:

PS - 1408

DEFAULT SHIPMENT THREAT INTEL

- THREAT SIGNATURES: 14 LAKHS+
- MALWARE HASHES: 80 LAKHS+
- MALICIOUS IPS: 20K+
- MALICIOUS URLS: 11 LAKHS+

ACCOMADATABLE THREAT INTEL (+)

- TIER 1: BILLION RECORDS
- TIER 2: BILLION RECORDS
- TIER 3: 100 BILLION RECORDS
- TIER 4: 10 TRILLION RECORDS

TIMELINE: 2023

DAWN: SEPTEMBER

Research on existing solutions, brainstorming and ideation

OCTOBER

Examining, setting realistic goals and start of development life-cycle.

NOVEMBER

Collection of threat signatures, samples for testing and intel to inventory assets

DEC, HACKATHON

Making of the MVP or with the more features collected as feedback to build a high fidelity prototype

TIMELINE

Research > Ideation > Threat Intel Aggregation > Prototyping

PS - 1408

HACKATHON TIMELINE

ROUND 1

Finalize development planning depending on research output and mentoring session 1 feedback.

ROUND 2

Developing the prototype and make improvement as per suggestions recieved from 2nd mentoring session

ROUND 3

Improve the product as per feedback. Finalize it with Threat Intel Database.
Demonstrate fully functional prototype.

PS - 1408

CONTRIBUTION TO PROJECT

DEVELOPMENT

ARJUN S

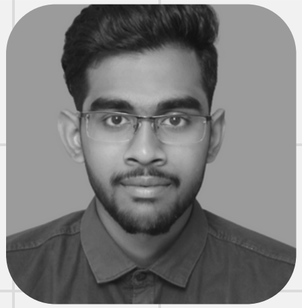
Frontend Integrations

VENKATA SAI RAM

DB Design (Relation + Schema + API)

PRANAVI BOVINA

CRPF Client Software Development



V NIVAS CH.

API Integrations

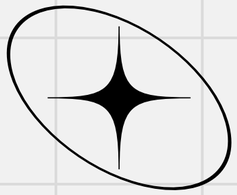
TECHNICAL

DURJOY M.

- Research on PS and finding out best possible solution.
- Threat Data Collection.

SRI SAI PRIYA R.

- Regex Based Signature Development.
- Threat Intel Collection.



THANK YOU

PS - 1408

0012 7482901 2744103 0592346 8774510 7255