

Ideation Phase


Brainstorm & Idea Prioritization Template

| | |
|--------------|--|
| Project Name | AI-Enhanced Intrusion Detection System |
|--------------|--|

Reference:

<https://app.mural.co/t/apurvalohar3763/m/apurvalohar3763/1744804799027/35201c0d64e18a558d0cb060c49276a9921b295e?sender=u5299e2e41e2aebb068029394>

Step-1: Team Gathering, Collaboration and Select the Problem Statement

| | | |
|--|---|--|
|  <h3>Brainstorm & idea prioritization</h3> <p>Use this template in your own brainstorming sessions so your team can unleash their imagination and start shaping concepts even if you're not sitting in the same room.</p> <p>🕒 10 minutes to prepare 🕒 1 hour to collaborate 👥 2-8 people recommended</p> | <h4>➔ Before you collaborate</h4> <p>A little bit of preparation goes a long way with this session. Here's what you need to do to get going.</p> <p>🕒 10 minutes</p> <div><div>+</div><div>Team gathering Online: who should participate in the session and send an invite. Share relevant information or pre-work ahead.</div></div> <div><div>+</div><div>Set the goal Think about the problem you'll be focusing on solving in the brainstorming session.</div></div> <div><div>+</div><div>Learn how to use the facilitation tools Use the Facilitation Superpowers to run a happy and productive session.</div></div> <p>Open article ➔</p> | <h4>1 Define your problem statement</h4> <p>What problem are you trying to solve? Frame your problem as a How Might We statement. This will be the focus of your brainstorm.</p> <p>🕒 5 minutes</p> <div><p>Type your paragraph...</p><p>How might I design an AI-enhanced IDS that reduces false positives and detects emerging threats in real-time?</p></div> <div><h4>2 Key rules of brainstorming</h4><p>To run a smooth and productive session</p><div><div>🕒 Stay on topic.</div><div>💡 Encourage wild ideas.</div><div>🕒 Defer judgment.</div><div>👂 Listen to others.</div><div>🗣️ Go for volume.</div><div>🎨 If possible, be visual.</div></div></div> |
|--|---|--|

Step-2: Brainstorm, Idea Listing and Grouping

2

Brainstorm

Write down any ideas that come to mind that address your problem statement.

🕒 10 minutes

TIP

You can select a sticky note and hit the pencil [switch to sketch] icon to start drawing!

Person 1

AI Modeling & Detection-
Use unsupervised learning to spot unusual patterns without labeled data. Train deep learning models on packet metadata and NetFlow data. Implement ensemble methods to combine signatures and anomaly scores.

Zero-Day Threat Handling -
Integrate threat intelligence feeds with dynamic model updates. Simulate adversarial attack scenarios to stress-test models. Use NLP to analyze dark web chatter for emerging threats.

False Positive Reduction-
Implement confidence scoring for each alert. Create an AI layer that learns from analyst feedback. Correlate multi-source logs (e.g., firewall, app, endpoint) to reduce false alarms.

Alert Prioritization-
Rank alerts by severity, asset criticality, and context. Add visual risk heatmaps for faster triage. Develop a real-time scoring dashboard with alert history.

User Experience for Analysts-
Build an explorable AI panel showing "why this was flagged". Allow feedback on false positives to refine the model. Integrate the system into existing SIEM platforms like Splunk or QRadar.

3

Group ideas

Take turns sharing your ideas while clustering similar or related notes as you go. Once all sticky notes have been grouped, give each cluster a sentence-like label. If a cluster is bigger than six sticky notes, try and see if you can break it up into smaller sub-groups.

🕒 20 minutes

TIP

Add customizable tags to sticky notes to make it easier to find, browse, organize, and categorize important ideas as themes within your mural.

Smart Alert
Management

Real-time
Detection

Analyst
Trust & UX

Zero-day
Threat
Intelligence

Step-3: Idea Prioritization

4

Prioritize

Your team should all be on the same page about what's important moving forward. Place your ideas on this grid to determine which ideas are important and which are feasible.

⌚ 20 minutes

TIP

Participants can use their cursors to point at where sticky notes should go on the grid. The facilitator can confirm the spot by using the laser pointer holding the **RT** key on the keyboard.

