


Cybersecurity in IoT – for Local Area Networks

1. Hypothesis

The difference the team thinks the project will make for it's customers. We think that ... will have the following effect ..

Airline example: "We believe that a low cost air travel product will meet customers travel needs and increase revenue for our airline".

We think that as more devices connect through IoT local networks, like WiFi, the need for better security will increase. This is because cyber threats, like hacking and attacks, are getting smarter. Our project's goal is to create stronger security measures specifically designed for these IoT networks. By doing this, we aim to protect the networks and the devices connected to them. This will help network providers, IoT solution makers, and regular users to keep their systems safe from cyber threats and improve the overall security of IoT networks.

 10min

2. Problem

What triggered the hypothesis?
Clearly list challenges, issues and root causes.

Airline example: "Many travellers are preferring train travel over plane due to costs".

End users of IoT solution seek instant notifications to stay informed about any potential threats or anomalies on their network. This need arises because IoT networks are becoming more complex, and users want to ensure the safety and reliability of their connected devices and data. They require solutions that provide real-time

7. Ideas

What could solve the customer personas' problems and meet stakeholders' requirements?

Airline example: "Refurbished airplanes with no check-in baggage and no food/drinks served".

Advanced Intrusion Detection System: Develop an advanced intrusion detection system tailored for IoT networks. This system should employ machine learning algorithms to proactively identify and respond to emerging threats in real-time.

6. Value

What is the likely user benefit and business benefit:

- expected user gains
- \$ business benefits
- technical benefits

Only list what can be measured and rank them as a team in terms of perceived customer value.

Airline example: "Air travel speed (not service) at the price of train tickets."

4. Stakeholders

Who supports this effort?
Who could potentially block this project? Who also has requirements?

Airline example: "CEO, pilots, travel agents, air regulators".

Network Service Providers (e.g., Uni4Network, Vodafone)



IoT Solution Providers (e.g., ACS - Smart Grid, uni.systems - Software



3. Customer personas



Who has this problem?
What motivates them? What are they trying to accomplish?

Airline example: "John is a university student who wants to travel during semester vacation without spending a fortune".

Internet Providers (e.g. Vodafone): They are a company that provides internet services. They want to make sure that the networks of their customers

<p>visibility and proactive alerts to address emerging cybersecurity challenges in the rapidly evolving IoT landscape.</p> <p> 10min</p>	<p>Security Analytics Dashboard: Create a comprehensive security analytics dashboard that provides network administrators with a centralized view of IoT device activity, anomalies, and potential security breaches. The dashboard should offer real-time monitoring and reporting capabilities.</p> <p>Threat Intelligence Integration: Monitor the effectiveness of threat intelligence feeds in proactively identifying and mitigating threats. Success is the timely identification of emerging threats.</p> <p> 10min</p>	<p>Network Service Providers (e.g., Uni4Network, Vodafone): These providers aim to enhance the security of their IoT networks to maintain customer trust, expand their customer base, and ensure the reliability of their services.</p> <p>IoT Solution Providers (e.g., Smart Grid – Unisystems - Software): IoT solution providers are interested in improving the security and robustness of their offerings, such as Smart Grids, to meet evolving customer demands.</p> <p>IoT Device Manufacturers (e.g., Cisco): Manufacturers seek to enhance the security protocols of their IoT devices.</p> <p>Buyers/End-Users (e.g., ACS, Public Government, Public Agent (Hospital)): End-users expect increased security and confidence in their IoT solutions to protect critical operations and sensitive data. They rely on robust security measures to mitigate risks.</p> <p> 10min</p>	<p>IoT Device Manufacturers (e.g., Cisco)</p> <p>Buyers/End-Users (e.g., ACS, Public Hospitals, Government)</p> <p> 10min</p>	<p>who use IoT (Internet of Things) devices, like Smart Grids, are safe from cyber threats.</p> <p>IoT Solution Provider (e.g. uni.systems): They create IoT solutions, such as Smart Grids. They want to enhance the security of their solutions to ensure they work reliably and securely for their customers.</p> <p>End-users (e.g. Quest Energy): They rely on these IoT solutions for various purposes. Their motivation is to have trust in the security of these systems, reduce worries about cyber threats, and ensure the uninterrupted operation of critical services.</p> <p> 10min</p>
	<p>8. Minimum viable experience</p> <p>The smallest, easiest, fastest-to-make version of your idea that can reliably prove the hypothesis.</p>		<p>5. Team</p> <p>What experience and skills are required to set up this experience for success?</p> <p><i>Airline example: "marketing manager, operations lead, finance, IT dev team"</i></p> <p>Data Analyst , Data Scientist, IT developers' team , Exploitation/Marketing</p>	

	<p><i>Airline example: "Serving one popular tourist destination during university vacation."</i></p> <p>Advanced Intrusion Detection Sstem (IDS) will detect unusual traffic and generate reports of possible intrusions in the IoT LAN. Also, this IDS has the ability to self-train in order to be able to detect with good possibility day-0 attacks.</p> <p> 5min</p>		<p>manager , Operation support Uni4Network</p> <p> 10min</p>	
<h2>10. End to end demo</h2> <p>Tell an end to end story from the point of view of the customer that focuses on the problems solved, the solution applied and value achieved. List key scenarios as role play, sketches or lo-fi (wireframes) that later could be worked into hi-fi (pixel perfect) mockup journeys.</p> <p>End to end previews of the user experience will give the entire team a desired end goal to work towards.</p> <p><i>Airline example: "Screen journey of booking a low cost flight; end to end experience from check-in to disembarking; complaint hotline process and experience, etc."</i></p> <p>Imagine a scenario where Uni4Network, the network service provider, deploys the enhanced security solution in a Smart Grid environment for a customer, ACS. The demo showcases the system's capabilities:</p> <p>Phase 1: Deployment Uni4Network deploys the advanced intrusion detection system and security analytics dashboard within ACS's Smart Grid infrastructure.</p>			<h2>9. Metrics</h2> <p>Define success metrics directly related to the desired values for this experience that will be used to prove or disprove the hypothesis.</p> <p>Metrics are often overlooked or not executed. Determine early when, how and by who they will be measured.</p> <p>Also, you want to have metrics not only for the ultimate value but also for milestones along the way that can provide early success or warning indicators.</p> <p><i>Airline example: "The low-cost air travel offering website will trigger at least 10,000 leads and 1,500 bookings within the first month".</i></p> <p>Detection Accuracy: Measure the system's accuracy in identifying security threats. Success is defined by a high true positive rate and a low false positive rate.</p>	

<p>Phase 2: Real-Time Monitoring The security dashboard provides real-time monitoring of all IoT devices within the Smart Grid, including sensors, controllers, and actuators.</p> <p>Phase 3: Threat Detection The system identifies a suspicious surge in traffic on a particular segment of the network, (e.g. signaling a potential DDoS attack).</p> <p>Phase 5: Reporting and Analysis Post-incident, the system generates detailed reports on the attack, including its origin, type, and impact. This information is crucial for forensic analysis.</p> <p>Phase 6: Detection Mechanism Retrain After an incident the detection mechanism can get retrained based on the results of the Reposting and Analysis phase. This will ensure that the detection mechanism stays up to date and gain more intelligence.</p> <p style="text-align: right;"> 5min</p>	<p>Response Time: Evaluate the system's response time in reacting to security incidents. Success involves rapid detection and mitigation of threats.</p> <p>Reduction in Incidents: Track the number of security incidents and breaches before and after the solution's implementation. Success is a noticeable reduction in incidents.</p> <p>User Satisfaction: Gather feedback from network administrators and end-users to assess their satisfaction with the enhanced security measures. Success involves positive feedback and increased security confidence.</p> <p>Cost Savings: Calculate the cost savings achieved through automated threat detection and response compared to manual security practices. Success involves significant cost reductions.</p> <p>Threat Intelligence Integration: Monitor the effectiveness of threat intelligence feeds in proactively identifying and mitigating threats. Success is the timely identification of emerging threats.</p> <p style="text-align: right;"> 10min</p>
---	--

Learn more: <https://www.atlassian.com/team-playbook/plays/experience-canvas>

This work, the 'Experience Canvas', is a derivative of 'The Business Model Canvas' by strategyzer.com used under [CC BY-SA 3.0](https://creativecommons.org/licenses/by-sa/3.0/). This Experience Canvas is licensed under [CC BY-SA 3.0](https://creativecommons.org/licenses/by-sa/3.0/) by Atlassian.