INSE 6210 Fall Term 2023

Total Quality Methodologies in Engineering

Optimizing the resolution process for support incidents in IT industry

Submitted By:

Vishnu Sharan T	ID – 40271136
Mulualem Assefa	ID – 40053908
Poojesh Reddy Mutra	ID – 40266279
Jashwanth Reddy Earla	ID – 40271577

Supervised By:

Prof. Zachary Patterson

Submitted On:

13th December 2023

Table of Contents

Executive Summary:

Tech Mahindra, a prominent global Information Technology company, offers a wide range of services, including cybersecurity, data analytics, infrastructure, cloud services, and network services. In today's digital era, where technology is integral to our daily lives and critical infrastructures, cybersecurity serves as the primary defense against a rising array of cyber threats. As businesses increasingly depend on digital platforms for operations and transactions, robust cybersecurity measures are crucial to uphold customer trust. Recognizing the significance of cybersecurity in the current world, incident occurrences and the time taken for incident resolution play pivotal roles in cybersecurity services. Like other cybersecurity service providers, Tech Mahindra may encounter occasional delays in incident response due to factors such as limited knowledge of specific tools and technologies or the absence of procedural documents. Reducing incident resolution time remains a top priority for any cybersecurity service provider. While Tech Mahindra has implemented measures to minimize resolution time, the growing frequency of cyber-attacks poses ongoing challenges. By consistently prioritizing incident resolution time and enhancing processes and services, Tech Mahindra is dedicated to reducing the occurrence of cyber-attacks and ensuring the security of its network and infrastructure. This project is a strategic initiative for Tech Mahindra to refine and fortify its cybersecurity incident resolution process.

Introduction:

In response to the imperative for heightened efficiency in the domain of cybersecurity incident resolution, this project employed the DMAIC (Define, Measure, Analyze, Improve, Control) methodology. This endeavor signifies a crucial advancement in strengthening Tech Mahindra's incident resolution processes, ensuring their alignment with the dynamic landscape of cybersecurity threats. Through the systematic application of DMAIC, our aim is to precisely define and measure key elements of the incident resolution workflow, analyze the root causes behind extended resolution times, institute targeted improvements, and establish robust controls for ongoing optimization. The project's diverse objectives, spanning from reducing average resolution time to refining incident prioritization, incorporating advanced training, and deploying monitoring tools, underscore our commitment to not only mitigate security risks but also position Tech Mahindra as a front-runner in delivering resilient cybersecurity solutions. This introduction sets the foundation for a DMAIC-guided expedition poised to elevate incident resolution capabilities, emphasizing our steadfast dedication to excellence amidst the ever-evolving landscape of cybersecurity challenges.

DEFINE
MEASURE
ANALYZE
IMPROVE
CONTROL
SIX
SIGMA
6σ

Project Objectives:

Enhance the efficiency of Tech Mahindra's cybersecurity incident resolution processes by employing Six Sigma methodologies. The specific goals include reducing the average resolution time for IT incidents, improving incident prioritization and classification accuracy, streamlining the overall incident handling process, conducting targeted technology training sessions, and implementing monitoring tools for performance analysis. The objective is to fortify incident resolution capabilities, minimizing security risks, preventing potential data breaches, and ensuring uninterrupted business operations. This initiative aligns with Tech Mahindra's commitment to providing cutting-edge cybersecurity solutions and staying at the forefront of the industry.

Problem Statement:

Tech Mahindra has experienced a significant delay in the security incident resolutions in the past, which can lead the threat actors to carry out a cyber-attack and cause a security breach in the client's/own network damage and can also damage the company's reputation. How can Tech Mahindra minimize the occurrence of incident resolution time and improve the safety of its services?

This problem statement succinctly outlines the challenge at hand—minimizing incident resolution time—and identifies the key stakeholders, including clients and the company. Furthermore, it articulates a precise objective for the DMAIC process: the improvement of Tech Mahindra's processes and the overall safety of its services.

Goal Statement:

Minimize the time taken to resolve incidents by deploying a comprehensive incident response plan and consistently monitoring and enhancing service capabilities.

This goal statement specifies the target that Tech Mahindra is aiming to achieve (a maximum reduction in incident resolution time). It also identifies the key actions that will be taken to achieve the goal (implementing incident response procedures and other changes in the organization).

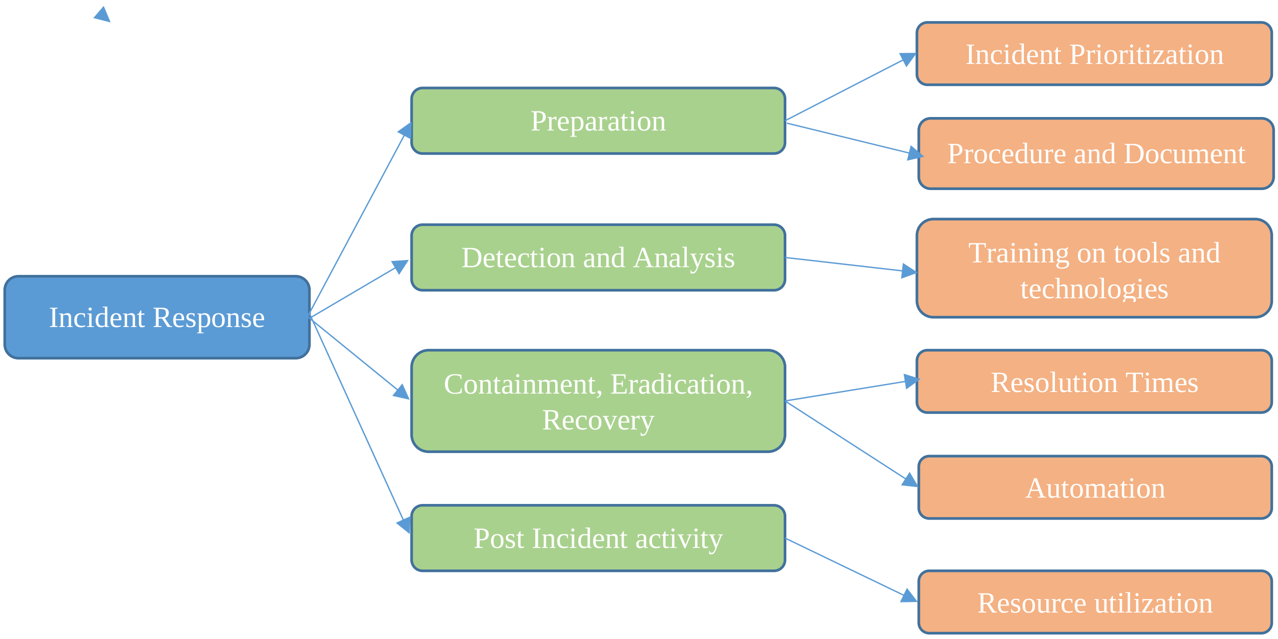
By setting a clear goal, Tech Mahindra can focus its efforts on achieving a specific, tangible result and track its progress towards that goal over time. Ultimately, this initiative seeks to strengthen Tech Mahindra's position as a leader in cybersecurity, providing cutting-edge solutions and ensuring the uninterrupted flow of business operations in the face of evolving cyber threats.

Project Charter:

<table>
<tr><td><b>Project name</b></td><td>Optimizing the resolution process for support incidents in IT industry</td></tr>
<tr><td><b>Start date</b></td><td>18-October-2023</td></tr>
<tr><td><b>Target completion date</b></td><td>15-December-2023</td></tr>
<tr><td><b>Goal</b></td><td>Optimize cybersecurity incident resolution processes to reduce average resolution time, enhance incident prioritization, streamline handling procedures, provide technology training, and implement performance monitoring tools for Tech Mahindra's cyber security team, ensuring heightened security, decreased risks, and uninterrupted business operations.</td></tr>
<tr><td><b>Objective</b></td><td>Improve cybersecurity incident resolution efficiency through Six Sigma methodologies, targeting reduced resolution times, enhanced prioritization, streamlined processes, technology training, and performance monitoring for Tech Mahindra's cyber security team.</td></tr>
<tr><td><b>Business case</b></td><td>Enhancing cybersecurity incident resolution processes will mitigate security risks, decrease potential data breaches, and optimize operational efficiency, reinforcing Tech Mahindra's industry leadership and ensuring client confidence.</td></tr>
<tr><td><b>Project scope</b></td><td><b>In Scope</b> - Optimizing the resolution time, incident prioritization, and handling processes within Tech Mahindra's cyber security department.
<b>Out of Scope –</b> Implementation of organizational-wide IT infrastructure changes unrelated to the immediate incident resolution objectives.</td></tr>
<tr><td><b>Team members</b></td><td>
<table>
<tr><th>Name</th><th>Role</th><th>Student ID</th></tr>
<tr><td>Vishnu Sharan</td><td>Data Analyst</td><td>40271136</td></tr>
<tr><td>Poojesh Reddy Mutra</td><td>Project Manager</td><td>40266279</td></tr>
<tr><td>Jashwanth Reddy Earla</td><td>Data Analyst</td><td>40271577</td></tr>
<tr><td>Mulualem Assefa</td><td>Quality Assurance</td><td>40053908</td></tr>
</table>
</td></tr>
<tr><td><b>Schedule</b></td><td>
<table>
<tr><th>Phase</th><th>Start Date</th><th>End Date</th><th>Duration</th></tr>
<tr><td>Define</td><td>18-oct-2023</td><td>29-Oct-2023</td><td>12</td></tr>
<tr><td>Measure</td><td>30-Oct-2023</td><td>15-Nov-2023</td><td>17</td></tr>
<tr><td>Analyze</td><td>16-Nov-2023</td><td>30-Nov-2023</td><td>15</td></tr>
<tr><td>Improvement</td><td>01-Dec-2023</td><td>15-Dec-2023</td><td>15</td></tr>
<tr><td>Control</td><td>16-Dec-2023</td><td>25-Dec-2023</td><td>10</td></tr>
</table>
</td></tr>
<tr><td><b>Support Required</b></td><td></td></tr>
<tr><td><b>Project sponsor</b></td><td>Prof. Dr. Zachary Patterson</td></tr>
</table>

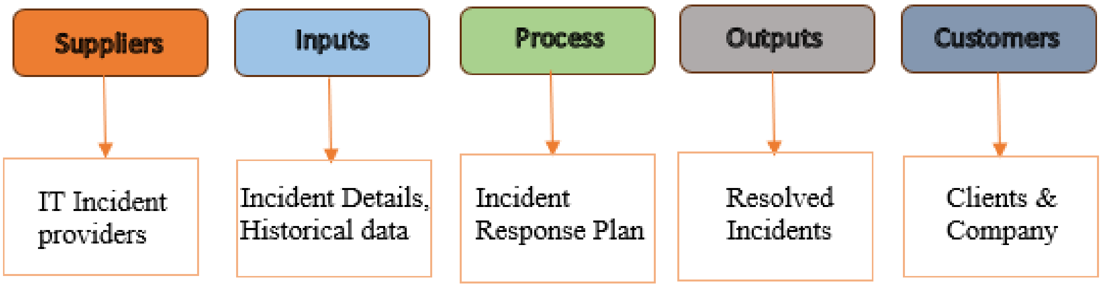
Define:

In the context of our cybersecurity incident resolution optimization project, the "Define" phase serves as the bedrock, providing a comprehensive understanding of the project's purpose and scope. During this phase, we delineate the critical issue at hand: prolonged resolution times for IT incidents in the cybersecurity domain. We articulate specific project objectives, including the reduction of average resolution times, improvement of incident prioritization and classification, and the streamlining of the overall incident handling process. Key stakeholders are identified, and their expectations are documented, ensuring alignment with organizational goals. This phase establishes the roles and responsibilities of the project team members, sets clear success criteria, and defines the project timeline. By distinctly defining the parameters and goals, we lay the groundwork for a focused, strategic, and outcome-driven cybersecurity incident resolution enhancement initiative.



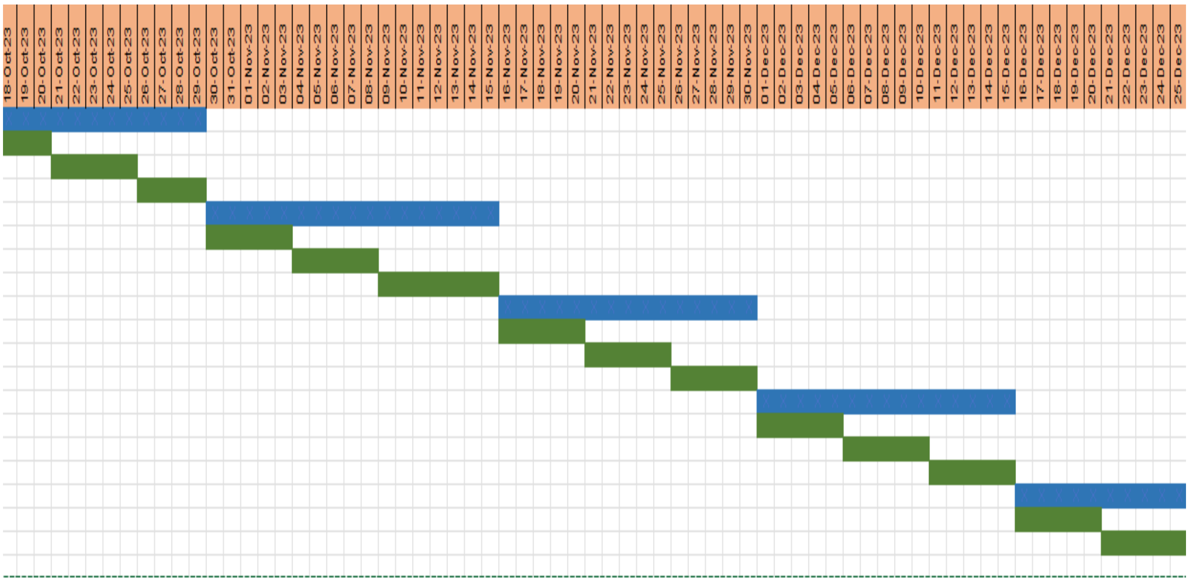
SIPOC:

SIPOC (Suppliers, Inputs, Process, Outputs, and Customers) is a graphical tool used in process improvement to help define and understand the relationships between the various components of a process. It provides us with a high-level overview of the process and helps us to identify areas for improvement by mapping out the inputs, outputs, and steps involved in the process. Here is the SIPOC diagram for our process.



Project Plan:

Phase	Start Date	End Date	Duration (days)
Design	18-Oct-23	29-Oct-23	12
Project Kick-off	18-Oct-23	20-Oct-23	3
Requirements Gathering	21-Oct-23	25-Oct-23	5
Scope Definition	26-Oct-23	29-Oct-23	4
Measure	30-Oct-23	15-Nov-23	17
Data Collection	30-Oct-23	03-Nov-23	5
Metric Identification	04-Nov-23	08-Nov-23	5
Baseline Measurement	09-Nov-23	15-Nov-23	7
Analyze	16-Nov-23	30-Nov-23	15
Data Analysis	16-Nov-23	20-Nov-23	5
Root Cause Analysis	21-Nov-23	25-Nov-23	5
Recommendations	26-Nov-23	30-Nov-23	5
Improvement	01-Dec-23	15-Dec-23	15
Implementation Planning	01-Dec-23	05-Dec-23	5
Execution	06-Dec-23	10-Dec-23	5
Verification	11-Dec-23	15-Dec-23	5
Control	16-Dec-23	25-Dec-23	10
Monitoring	16-Dec-23	20-Dec-23	5
Documentation	21-Dec-23	25-Dec-23	5



Measure:

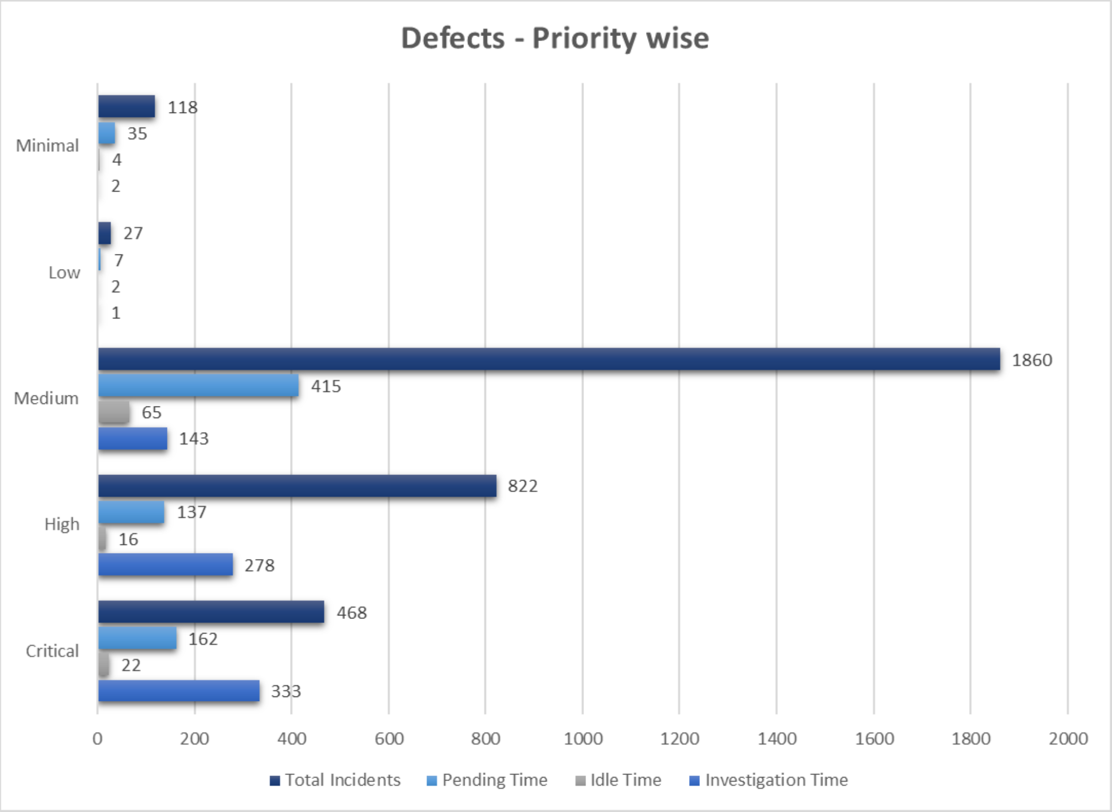
The Measure phase is the second step in the DMAIC (Define, Measure, Analyze, Improve, Control) methodology. This phase involves collecting data to gain a thorough understanding of the current process performance. We've compiled six months of historical data on security incidents at Tech Mahindra, categorized them based on priority using the NIST framework. Given the critical role incident resolution time plays in thwarting security breaches, we focused on parameters like incident resolution time, pending time, and idle time. Additionally, we examined the organization's Service Level Agreements (SLAs) for each priority, aligning them with industry standards, and reviewed the existing response plan.

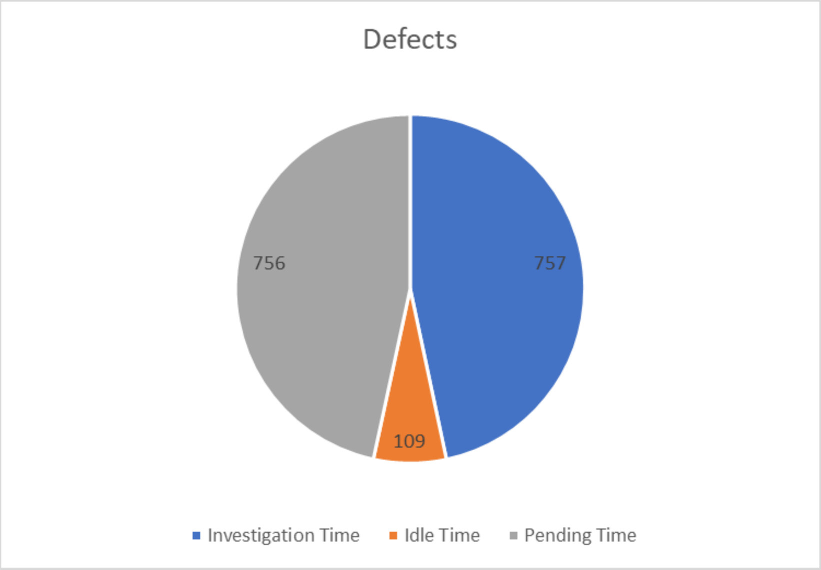
After conducting measurements, it became apparent that Incident Investigation Time, Idle Time (the period during which the incident is unaccounted for) and Pending Time (the duration for which the incident is kept in a pending state) are noticeably high and are deemed critical factors affecting quality. Also, we have calculated the Defects Per Million Opportunities (DPMO) using the available data, and the resulting metrics provide valuable insights.

$$DPMO = \frac{Total\ number\ of\ defects}{Total\ number\ of\ opportunities} * 10^6$$

	Defects			
Incidents Priority-Wise	**Investigation Time**	**Idle Time**	**Pending Time**	**Total Incidents**
Critical	333	22	162	468
High	278	16	137	822
Medium	143	65	415	1860
Low	1	2	7	27
Minimal	2	4	35	118
Total	757	109	756	3295
Fraction of defects	0.229742033	0.033080425	0.229438543	
DPMO	229742.0334	33080.42489	229438.5432	
Sigma level	2.239696674	3.337332331	2.240697152	2.477798484
DPMO considering, we have three opportunities of error (Worked time, Idle Time, Pending Time) for each incident.				164087.0005

So, after calculating the DPMO with can see that the fraction of Defects is more when we consider pending time, which is at 22.94%, while the overall on time resolution is at 77.06%, and the Process is at Sigma level of 2.24.





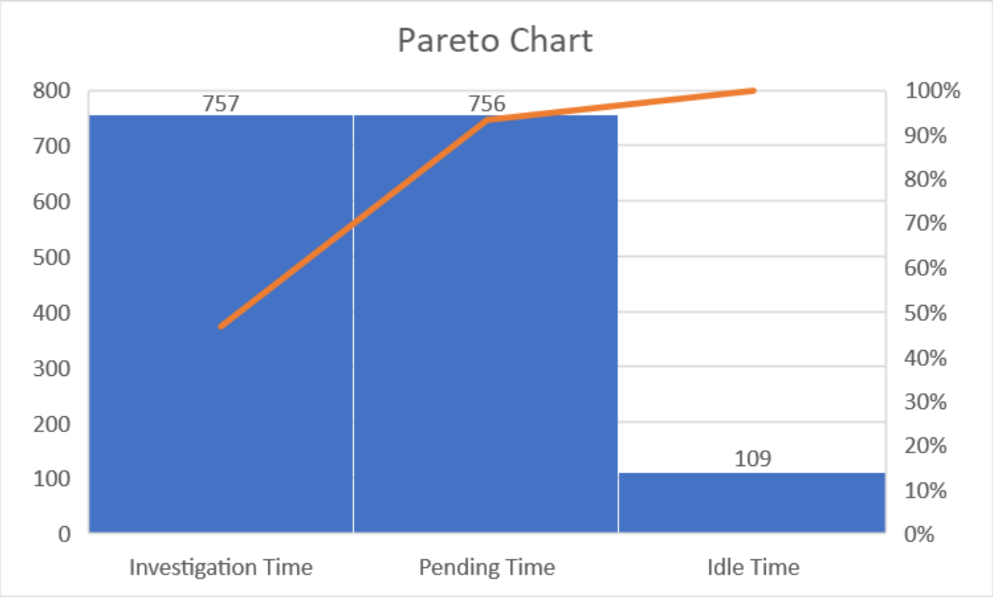
Analyze phase:

In the Analyze phase of this project, our focus is on a meticulous examination of the current cybersecurity incident resolution process. Leveraging historical incident data, insights from team managers, and feedback from former employees, we aim to identify bottlenecks, inefficiencies, and areas of improvement. Using Six Sigma methodologies, we will conduct in-depth statistical analyses to pinpoint root causes contributing to prolonged resolution times. This phase will lay the groundwork for informed decision-making by providing a comprehensive understanding of the existing challenges and opportunities for enhancement, ultimately guiding the subsequent steps in the project towards a more streamlined and effective incident resolution process.

The steps involved in the Analyze phase of the DMAIC cycle typically include:

1. Identify and validate the root causes of problems or inefficiencies in the process. This can be done using tools such as fishbone diagrams, Pareto charts, and cause and effect diagrams.
2. Analyze data and trends to understand the relationships between different process variables and identify potential causes of problems or inefficiencies.

From the 6 months historical data, we performed Pareto analysis to identify major defects causing areas. As per analysis, it has become evident that the investigation time and pending time are major areas impacting the incident response process. Upon analysis, it became evident that the analysts' time spent on each security incident is influenced by various factors. These include prolonged pending times due to limited resources during shifts, inadequate documentation of procedures, lack of proper training, and other contributing factors.



Following this we can perform root cause analysis to identify potential cause for failure or flaw. We strongly suggest performing following techniques:

- **Interviews:**

Conduct interviews with team members, stakeholders, or patients to gather insights and thoughts about the problem or inefficiency they feel about the product. After gathering data, we can use “Ishikawa diagram” and “5 why technique” to identify potential cause.

- **Integrating Ishikawa diagram and 5 why technique:**

In our endeavor to optimize cybersecurity incident resolution, the integration of the Ishikawa Diagram (also known as the Fishbone Diagram) and the 5 Whys Technique proves invaluable for comprehensive root cause analysis and solution identification. Let's explore how these methodologies synergize:

Ishikawa Diagram:

Purpose: The Ishikawa Diagram systematically categorizes potential causes of a problem to identify root causes across different dimensions.

Application: In our context, categories may include People, Processes, Technology, Policies, and External Factors influencing cybersecurity incident resolution.

5 Whys Technique:

Purpose: The 5 Whys delves deeper into the root cause by repeatedly asking "Why?" to uncover the underlying issues.

Application: For each category identified in the Ishikawa Diagram, the 5 Whys Technique is applied iteratively to drill down into specific causes within each category.

1. **Define the problem or issue:**
   Clearly define the problem or issue that needs to be addressed and ensure that all team members understand the scope and purpose of the Ishikawa diagram and the 5 why technique.
2. **Identify the categories of factors:**
   Determine the categories of factors that may be contributing to the problem, such as personnel, processes, Technology, policies, and External factors.
3. **Draw the Ishikawa diagram:**
   Draw a large arrow pointing to the right, representing the problem or issue. Draw smaller arrows branching off from the main arrow, representing the categories of factors.
4. **Identify specific factors**:
   Identify specific factors within each category that may be contributing to the problem. These are represented by boxes or rectangles on the Ishikawa diagram.
5. **Determine the relationships between factors:**
   Use lines to connect the specific factors to the main arrow, indicating the relationship between them and the problem.
6. **Identify the root cause of the problem:**
   Use the 5 why technique to ask a series of "why" questions to identify the root cause of the problem. Start with the problem at the top of the Ishikawa diagram and work your way down through the specific factors, asking "why" each factor may be contributing to the problem.
7. **Identify potential solutions:**
   Based on the root cause identified through the 5 why technique, identify potential solutions that can address the root cause of the problem.
8. **Evaluate and prioritize potential solutions:**
   Evaluate each potential solution based on its potential impact, feasibility, and cost, and prioritize them accordingly.

Improvement Proposal:

During our preliminary research of the current incident response plan, we found that there were no specific procedures or guidelines to ensure or enforce faster resolution times. Hence, for the final step we are proposing a few changes in the existing processes and some new implementations to advance the existing sigma level of 2.36 to 6 sigma level, which are as follows:

1. **Knowledge Enhancement:** Implement regular training programs for the cybersecurity team to stay updated on the latest tools, technologies, and threat landscapes. Establish a knowledge-sharing platform

to facilitate information exchange within the team.

2. **Procedural Documentation:** Develop comprehensive procedural documents outlining step-by-step incident resolution processes. Ensure the documentation is easily accessible to all team members for quick reference during incident handling process.
3. **Incident Response Automation:** Integrate automation tools such as FortiSOAR or other SIEM tools for routine and repetitive tasks within the incident resolution workflow. Automate the initial stages of incident detection and analysis to expedite the overall resolution process.
4. **Collaborative Incident Handling:** Foster a collaborative incident response culture, encouraging open communication and information sharing through daily stand-up calls. Establish open channels to enhance coordination among team members to discuss the incidents that are in doubt.
5. **Continuous Improvement Feedback Loop:** Implement a feedback mechanism to gather insights for resolved incidents from customer. Regularly review and update incident response processes based on lessons learned and emerging threats.
6. **Resource utilization:** Strengthen the cybersecurity team's capability to provide round-the-clock monitoring and support. Establish a dedicated response team for rapid intervention during critical incidents.

Implementing these improvement ideas would lead Tech Mahindra to achieve reduced Incident resolution time, enhanced client trust, improved security posture, adaptability to emerging threats, efficient resource utilization thus reducing the risk of being exposed to a cyber-attack.

Cost estimation:

Cost Component	**Estimated Cost (Rough)**
Personnel Costs	
Project Manager	$10,000
Six Sigma Specialist	$15,000
Data Analyst	$12,000
Cybersecurity Experts	$20,000
Training Specialist	$8,000
Monitoring Tools Specialist	$15,000
Technology Costs	
Monitoring Tools	$10,000
Training Resources	$5,000
Data Analysis Costs	
Data Analyst Tools	$7,000
Miscellaneous Costs	
Communication Tools	$3,000
Quality Assurance Tools	$5,000
Training and Development Costs	
Training Materials	$4,000
External Training Resources	$6,000
Travel and Accommodation	
If Required	$2,000
Contingency	
Unforeseen Expenses	$10,000
Total Project Cost (Rough)	$117,000

Conclusion:

In conclusion, the integration of Six Sigma methodologies, the Ishikawa Diagram, and the 5 Whys Technique provided a robust framework for dissecting and addressing root causes of prolonged cybersecurity incident resolution times at Tech Mahindra. The collaborative analysis among team members unearthed valuable insights, leading to targeted and sustainable solutions. Moving forward, the implementation of these solutions aims to fortify our cybersecurity capabilities and ensure a swift response to dynamic cyber threats.

References:

1. https://github.com/JashwanthReddyE/INSE-6210-Data
2. Tech Mahindra
3. https://www.gartner.com/
4. https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023
5. https://csrc.nist.gov/Projects/cybersecurity-framework/Filters#/csf/filters