Team 1 Consulting

The Cost of a Breach: Prioritizing Cybersecurity

Guiding MissaTech in data protection & safety

Meet Our Team

Benjamin Tran

Chelsey Luc

Elijah Chan

Jonathan Dang

Agenda

1. Overview
Objective and why it matters

2. Visualizations
Exploring the breach impact

3. Dashboard
Centralized information showcase

4. Recommendations
Future-proofing MissaTech's future

Overview

Why Should MissaTech **prioritize** Cybersecurity?

Customer Trust & Reputation

Strong cybersecurity protects customer data, building lasting confidence in the MissaTech's reliability

Financial & Legal Protection

Prevents costly breaches, regulatory fines, and lawsuits that could harm MissaTech's future

Growth & Innovation

Secure systems allows for MissaTech to grow safely and potentially expand into other markets

About the Data

4.35 million records exposed

$73.6 million USD lost

100 total incidents

5 Systems: HR, Billing, CRM, Support, Analytics

3 Attack Types: Misconfiguration, External Hacker, Insiders

Problem Statement

MissaTech must prioritize their focus on **implementing cybersecurity measures** in order to have long-term success.

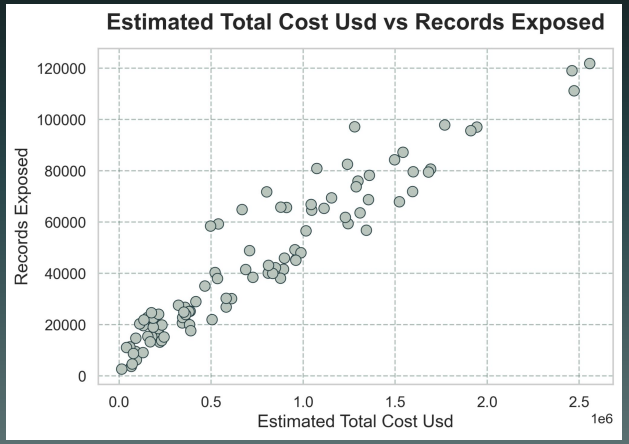
Visualizations

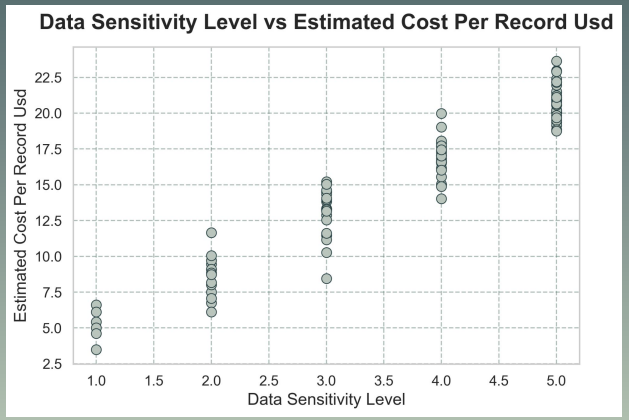
Correlations

2 columns have an extremely high correlation (>.9):

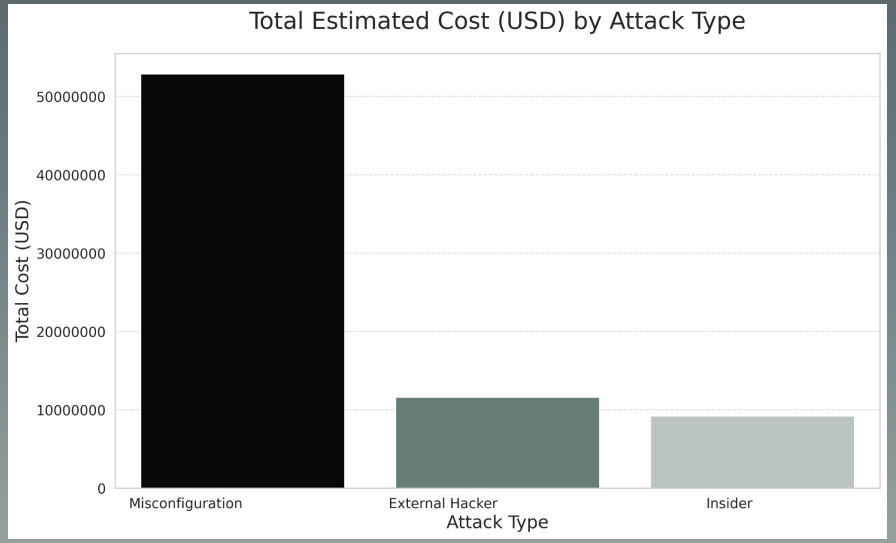
- ➢ Estimated total cost & records exposed
- ➢ Data sensitivity level & estimated cost per record

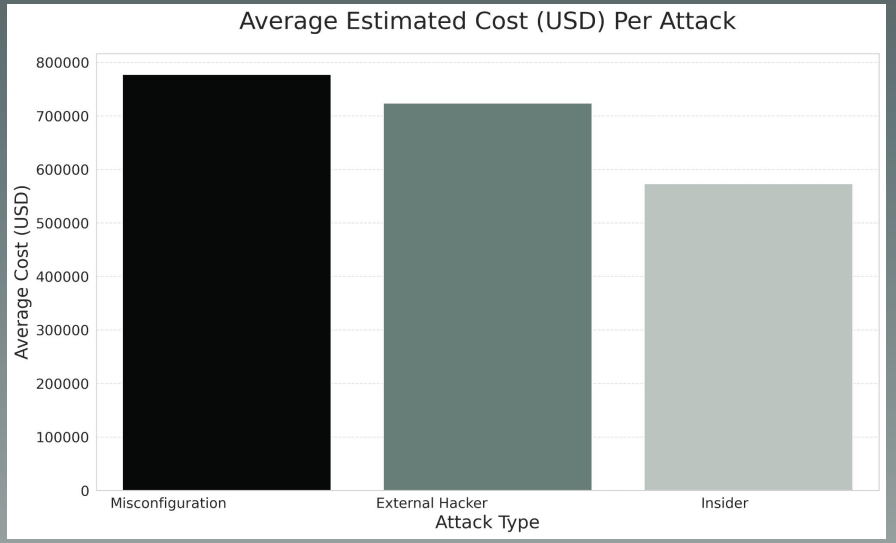
The former is expected, but the latter tells us that sensitive information is worth more.





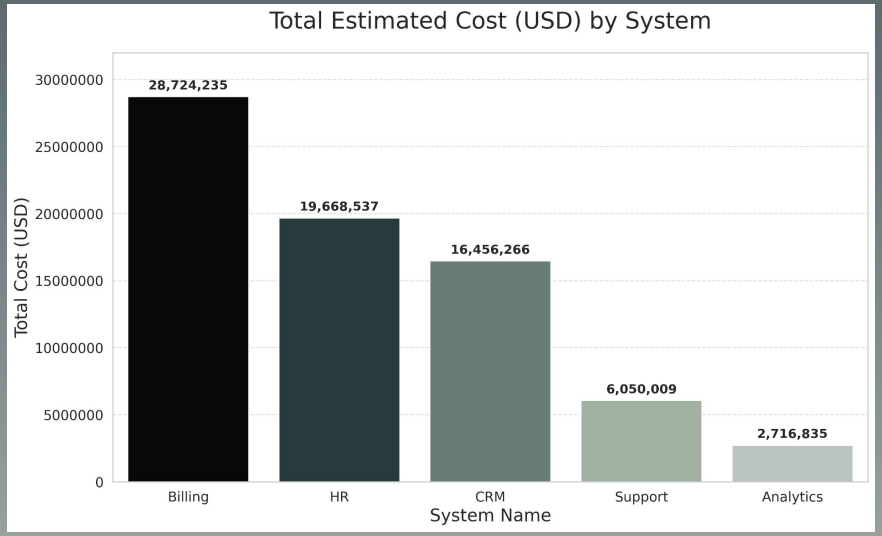
Attack Type Estimated Cost

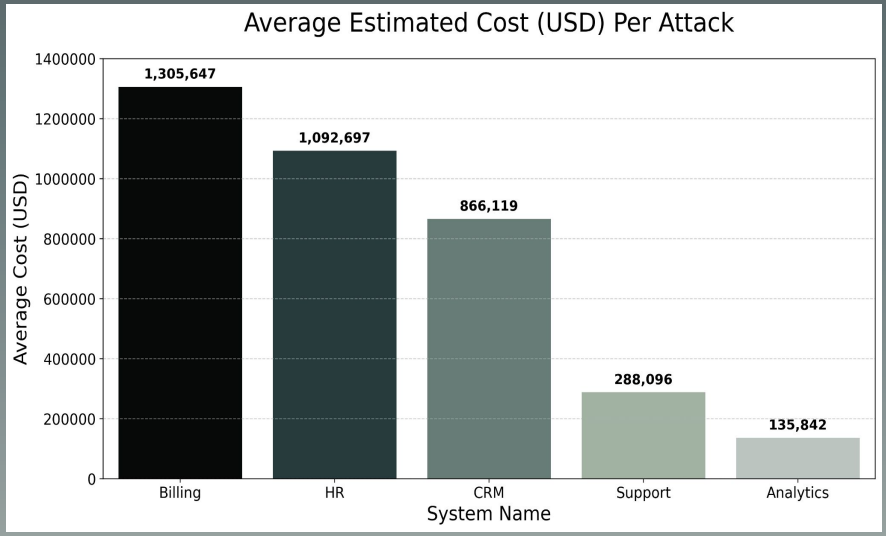




Misconfiguration **dominates** the total financial loss due to it accounting for **two-thirds** of the dataset. However, average costs are around the same. When attacks happen, each one has similar average cost, with Insider attacks falling shortly behind.

System Estimated Cost

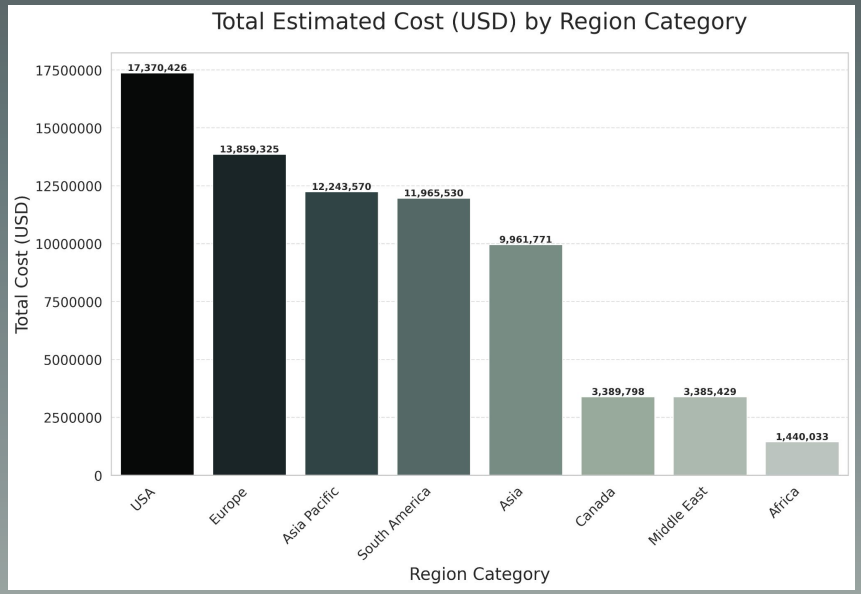


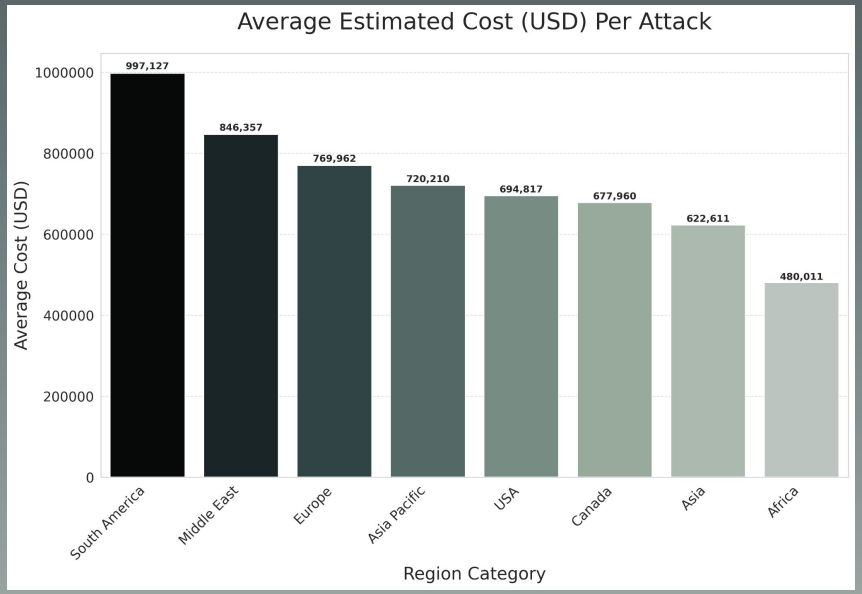


Billing, HR, and CRM were impacted the most due to the breaches.

The averages show a very similar distribution because each system has about 20 appearances in the dataset.

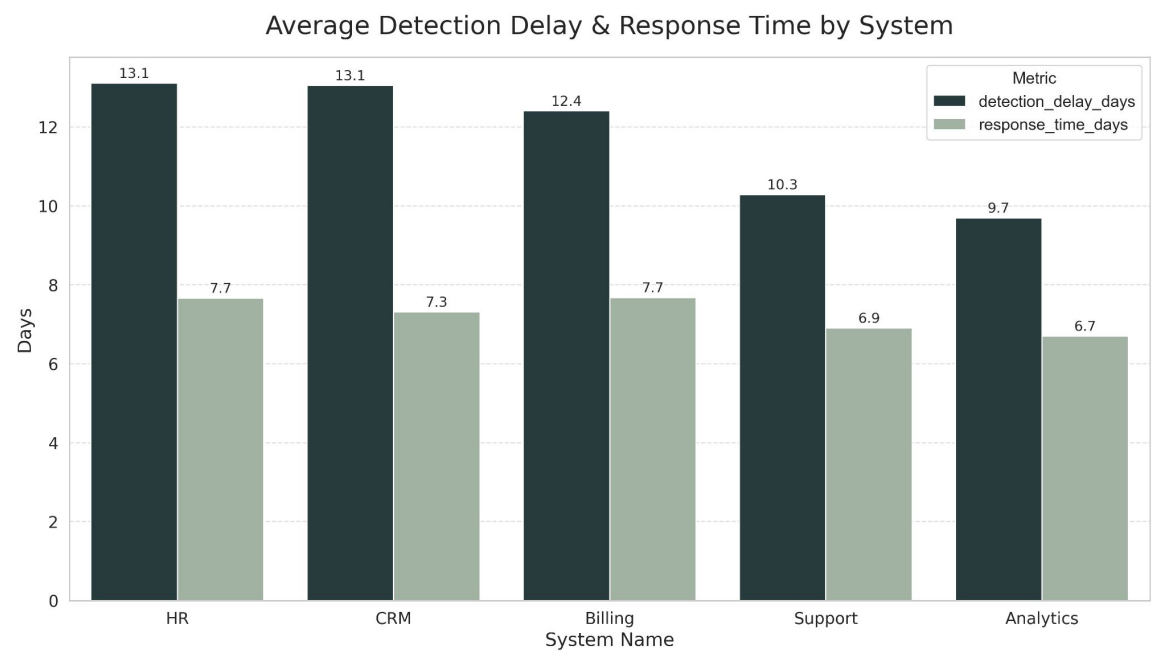
Region Estimated Cost





The United States have the greatest total due to a quarter of rows being from there. **South America** has the highest average despite having half (12) of the instances from there.

Detection & Response Times



HR and **CRM** take the longest to detect, and the response time is relatively similar across all the systems.

Costliest Incidents

System Name	Region	Attack Type	Data Sensitivity	Records Exposed	Estimated Cost per Record (USD)	Total Estimated Cost (USD)	Detection Delay (Days)	Response Time (Days)	Notification Required	Region Category
Billing	latam-north1	Misconfiguration	5	121863	20.98	2556820.26	8	10	Yes	South America
Billing	ap-northeast1	Misconfiguration	5	111309	22.2	2471140.33	12	8	Yes	Asia Pacific
Billing	ap-south1	Misconfiguration	5	119149	20.65	2460599.64	16	10	Yes	Asia

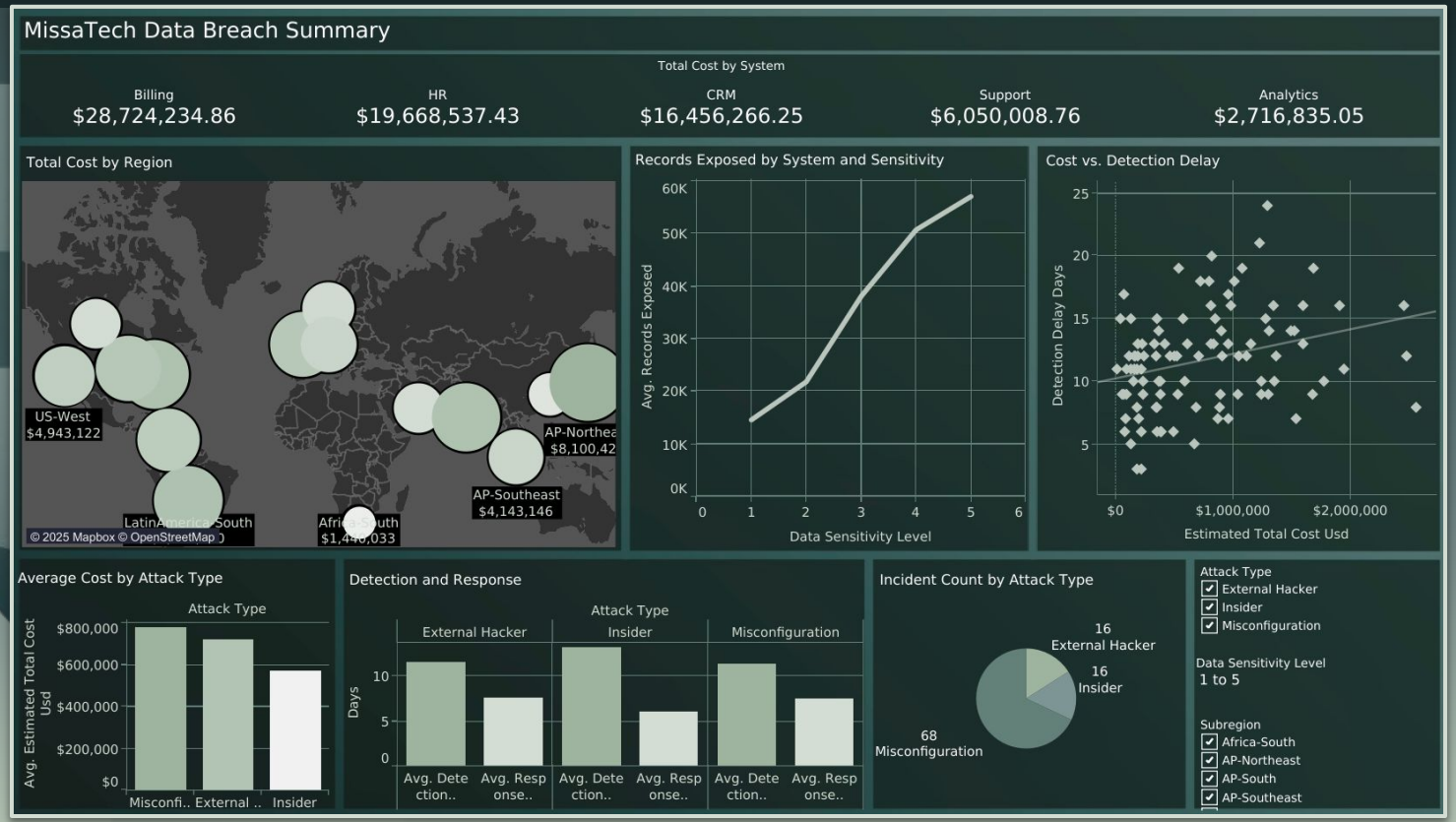
Dealing with extremely sensitive data

100k+ Records Exposed

Average Billing Detection Delay: 12.4 Days

Average Billing Response Time: 7.7 Days

Executive Dashboard



Demo

Recommendations

Implement Machine Learning

Use Cases

- Predicting high-cost incidents early
- Forecast total cost for new incidents
- Anomaly Detection

Advantages

- Faster detection → reduces cost & impact
- Predictive alerts for high cost/sensitivity breaches
- Uncover hidden relationships in security incidents

Reducing Misconfiguration Risk

Strategies

- **Strengthen** internal operational processes
- **Automated** security/configuration checks
- Conduct regular **configuration audits**
- **Standardize** data-handling practices

Benefits

- Prevents high-cost incidents (Up to **$50 million** in potential losses)
- **Safeguards** Against Human Mistakes
- Ensures **consistency** across systems
- **Minimizes** misconfiguration impact

Security Focus

Lowering Detection Times

Assisted with ML implementation, Faster detection = Faster solutions

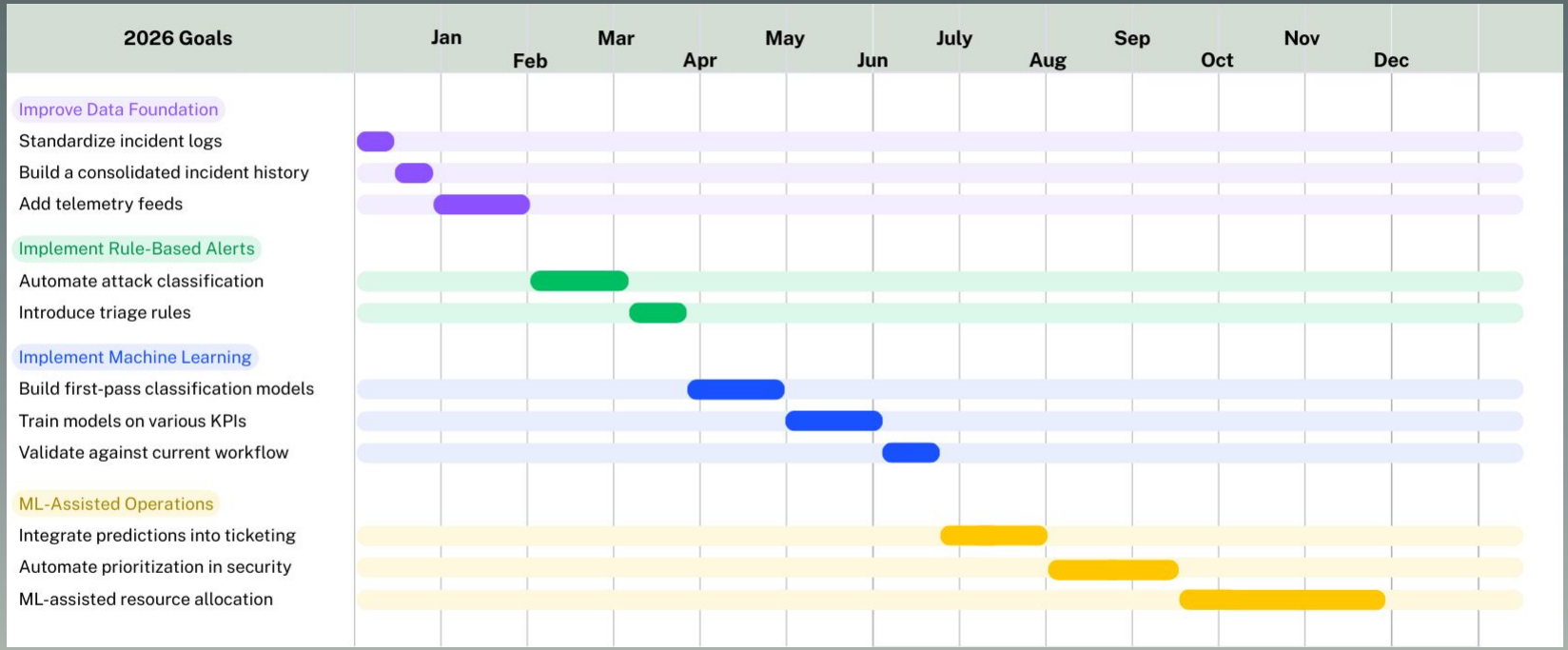
Maintain strict data protection policies

Ensure in regions like USA, South America, Canada with highly sensitive data

Prioritize high-impact systems

HR, Billing, CRM are where MissaTech should prioritize investments in data security

Roadmap


2026 Goals
Jan
Feb
Mar
Apr
May
Jun
July
Aug
Sep
Oct
Nov
Dec
Improve Data Foundation
Standardize incident logs
Build a consolidated incident history
Add telemetry feeds
Implement Rule-Based Alerts
Automate attack classification
Introduce triage rules
Implement Machine Learning
Build first-pass classification models
Train models on various KPIs
Validate against current workflow
ML-Assisted Operations
Integrate predictions into ticketing
Automate prioritization in security
ML-assisted resource allocation

Thank you!

Team 1 Consulting