MISY 650: Security and Control

IT Risk Assessment Report

ABC Information Security Inc.

Group 3:

Rishabh Jagtap

Shailendra Rathore

Henry Chan

Contents **Page Number**

About "ABC Information Security Inc."

"ABC Information Security Inc." is based in San Francisco, CA. The company provides a leading cloud-native email security platform that leverages AI-based behavioral data science to stop socially engineered and never-seen-before email attacks that evade traditional secure email gateways. "ABC Information Security Inc." delivers a fundamentally different approach that precisely detects and protects against the widest range of attacks including business email compromise, phishing, malware, ransomware, social engineering, spam and graymail, supply chain compromise, and internal account compromise.

The "ABC Information Security Inc." platform delivers inbound email security, internal and external account takeover protection, and full automation. ABC Information Security Inc.'s API-based approach enables customers to get started in minutes and be used standalone to enhance native cloud email security protection with Microsoft 365 and Google Workspace.

Executive Summary

We are a team from the University of Delaware, MISY 650 "Security & Control" graduate students. We performed a comprehensive IT risk assessment for the company "ABC Information Security Inc.". The company is a leading cybersecurity firm specializing in email security. The company has been engaged by "University of Delaware" to detect and prevent a range of email-based threats, including phishing and business email compromise.

Reference: https://www.upguard.com/security-report/abnormal-security

Our team evaluated the assets and threats associated with ABC Information Security Inc.'s email security platform to gain a thorough understanding of potential risks and vulnerabilities. The likelihood of each identified vulnerability was multiplied by its potential impact to calculate a risk score, providing a quantitative basis for the assessment.

This risk assessment serves as a foundation for informed decision-making and strategic planning to enhance the resilience of company ABC Information Security Inc.'s email security platform.

By implementing the proposed controls, ABC Information Security Inc. can strengthen its defenses, reduce the likelihood of successful email attacks, and optimize its cybersecurity investment.

The team identified the highest risks and suggested countermeasures and recommendations for the management of ABC Information Security Inc.

Introduction

Purpose

In the rapidly evolving landscape of cybersecurity, the company ABC Information Security Inc. stands at the forefront with a singular focus on email security. Through its innovative platform, ABC Information Security Inc. addresses the escalating threats posed by email attacks, including but not limited to phishing, business email compromise, and various other email-based threats. This risk assessment centers around ABC Information Security Inc.'s cutting-edge solution, which not only detects and prevents these attacks but also empowers security teams with organized insights through its Threat Log functionality. Through this risk assessment, we aim to deliver full documentation to the management regarding our analysis and evaluation of the technological risks arising in the email security system that could potentially hamper the company’s daily business functions. We addressed the organizational vulnerabilities and assigned risks accordingly using the risk calculation matrix to demonstrate the severity of each risk to the management and guide them into taking the necessary action plans. Our consultant team was also able to provide recommendations to the management to protect against potential future threats.

Scope

Recognizing the criticality of the email security landscape and the potentially severe impact of email attacks, the risk assessment covers both the email security platform itself and the broader processes involved. The assessment aims to ensure a comprehensive understanding of potential threats and vulnerabilities associated with Company ABC Information Security Inc.'s innovative solution.

Risk Assessment Approach

The risk assessment was carried out by a team of three consultants.

Name	Title
Henry Chan	Technology Risk Assessment Consultant
Rishabh Jagtap	Technology Risk Assessment Consultant
Shailendra Rathore	Technology Risk Assessment Consultant

Initial Assessment:

The information-gathering process was conducted via a review of the documentation available on the website of ABC Information Security Inc. that provided clear descriptions of the existing systems, user interactions, system integrity, network diagrams, and operational manuals related to email security systems. While looking at the documentation, we had the questions recommended by the National Institute of Standards and Technology as a reference in mind to help us extract the right information. Supporting diagrams and system architectures were part of the documentation and have been used in conducting the risk assessment.

Data Collection and Documentation:

The data collection and documentation were tailored for business specifics, capturing insights related to current procedures, controls, user access processes, system integrity, database administration, and audit. Supporting documentation and flowcharts were foundational for the risk assessment.

Risk Matrix Development and Assessment: Following a detailed review of documentation, the team structured risk metrics based on potential threats and vulnerabilities associated with ABC Information Security Inc.'s email security system and process. All assets interacting with the ABC Information Security Inc. network, such as servers, terminals, controllers, software, and personnel were identified. Each asset impacted had identified threats and vulnerabilities, and a risk score was assigned based on the severity and probability (likelihood) of occurrence. Subsequently, the team compiled findings and constructed a matrix to document and rate the potential severity of each identified threat.

Risk Scoring System: The team employed a Risk-Level Metrics system to generate risk ratings. Assets were assigned potential threats and vulnerabilities, with each vulnerability given an impact rating of low, medium, or high, and a likelihood rating of low, medium, or high. Each identified vulnerability was assigned a risk score based on the severity level of the impact and the likelihood of occurrence. Likelihood was categorized as "High" (1.0), "Medium" (0.5), and "Low" (0.1), while impact was graded as "High" (100), "Medium" (50), and "Low" (10). The risk score for each vulnerability was calculated as the product of the impact value and the likelihood value.

Risk Score = Impact x Likelihood (e.g., 100 X 0.5 = 50).

Risk-level Metrics and Classification: A Risk-Level Metrics system was employed to generate risk ratings, categorizing them as Low (1 to 10), Medium (>10 to 50), and High (>50 to 100)

- **Low Risk:** Scores from 1 to 10. The company can decide whether to develop an action plan or accept the risk.
- **Medium Risk:** Scores between 10 and 50. While the system can continue operating, an action plan is required within a reasonable timeframe. Medium-risk issues are closely monitored as they can escalate.
- **High Risk:** A score higher than 50, necessitating immediate action. While the system can continue operating, an action plan must be developed and executed promptly.

This risk assessment approach equips Company ABC Information Security Inc. to make informed decisions and implement necessary actions to fortify its email security platform against potential threats.

Scale:

	Impact	Threat Likelihood
Low	**10**	**0.1**
Medium	**50**	**0.5**
High	**100**	**1.0**

Risk classification:

Score	Rating
1 to 10	Low
10 to 50	Medium
50 to 100	High

Metrics table:

Risk Score = Impact x Likelihood

Threat Likelihood	Impact		
	Low (10)	Medium (50)	High (100)
Low (0.1)	Low 10 x 0.1 = 1	Low 50 x 0.1 = 5	Low 10 x 0.1 = 10
Medium (0.5)	Low 10 x 0.5 = 5	Medium 50 x 0.5 = 25	Medium 100 x 0.5 = 50
High (1.0)	Low 10 x 1.0 = 10	Medium 50 x 1.0 = 50	High 100 x 1.0 = 100

Recommendation to ABC Information Security Inc. follow-up actions

Risk	Scores	Follow up Action Required
Low	**1 to 10**	The company can decide whether to develop an action plan o r accept the risk.
Medium	**10 to 50**	While the system can continue operating, an action plan is required within a reasonable timeframe. Medium-risk issues are closely monitored as they can escalate
High	**> 50**	A score higher than 50, necessitating immediate action. While the system can continue operating, an action plan must be developed and executed promptly.

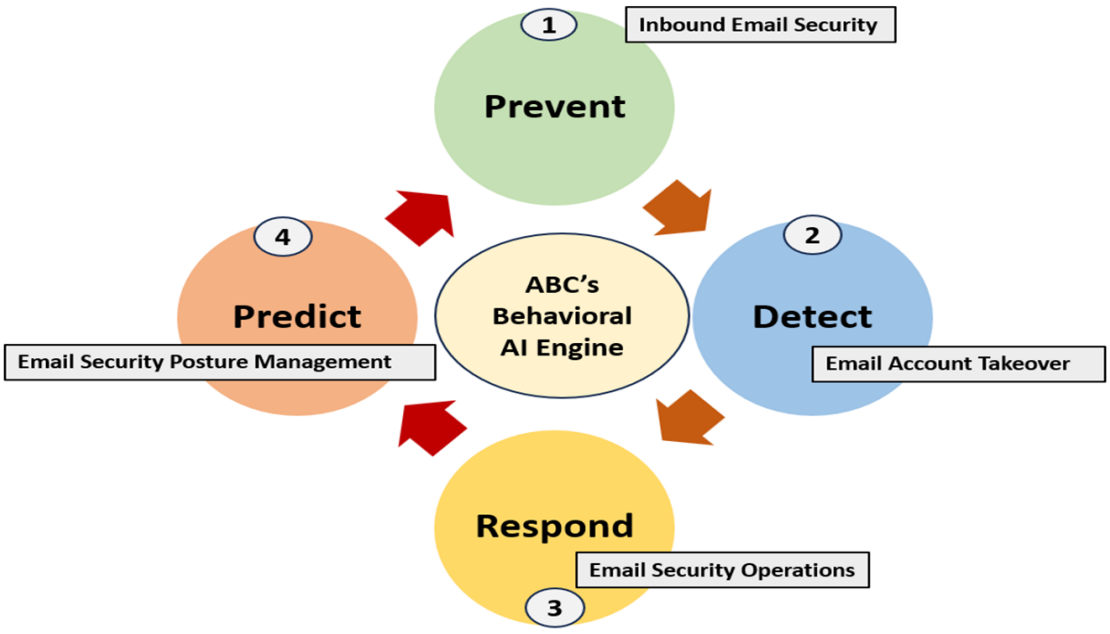
System Characterization:

The system of ABC Information Security Inc. is to have an engine that cycles through each email. These are the four main functions:

- **Prevent Inbound Email Security**: Blocks targeted inbound email attacks such as credential phishing, business email compromise, vendor invoice fraud, and more.
- **Detect email Account Takeover:** Stops account takeovers, attacks via third-party applications, and other platform threats.
- **Respond Email Security Operations:** Fully automates triage and remediation of user-reported emails.
- **Predict Email Security Posture Management:** Alerts on high-risk configuration changes to users, apps, and mail tenants.

Here is the diagram for ABC's Behavioral Engine.

ABC Information Security Inc.'s Behavioral Engine



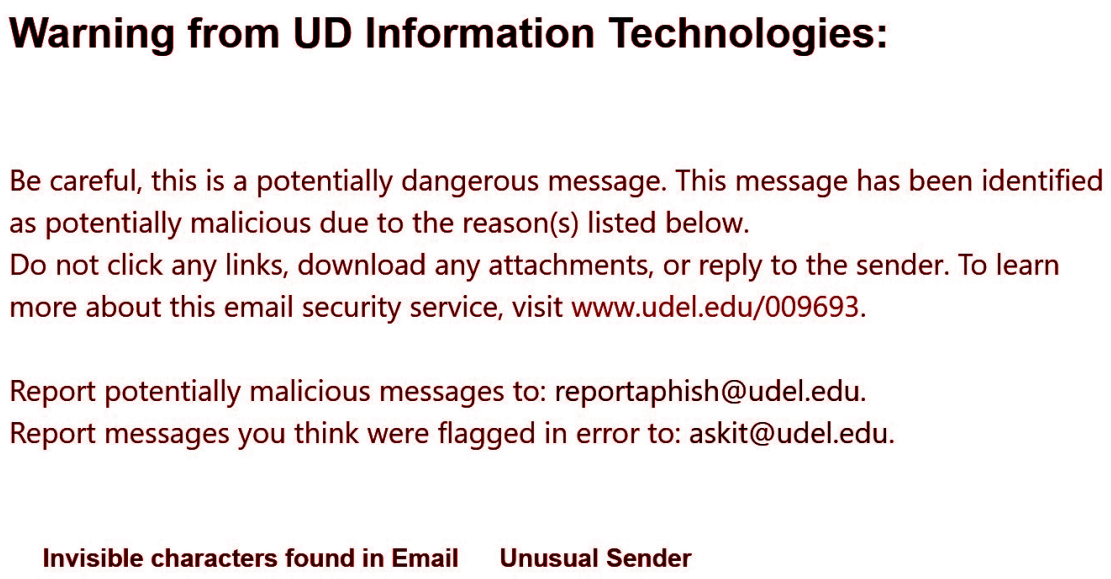
With this engine, it is a revolutionary approach to email security as it uses AI and machine learning to detect anomaly emails in comparison to traditional email where it only detects the most common red flags in typical phishing emails.

Features: ABC's system uses a read-only API to detect and analyze email frameworks. This is to prevent opening any malicious URLs or documents within the emails. This API works great for Microsoft 365 Office and Google Email as it does not interfere with email overflow. The best part of a fully integrated API is that you can integrate with many platforms, such as cloud email platforms, EDR and IAM tools, and other SaaS apps. For example, it can protect collaboration apps like Slack, Google, and Microsoft. This will allow you to be flexible on the platforms that you are using to help secure your email. It also offers visibility to internal and external traffic so that you can find the relationship and patterns between each user.

With the integration of third-party applications, it can scan any third party that has been integrated into the cloud email environment, revealing an entry point for ABC security, and can tell the user on how many privileges the third-party applications have for the system. Not only that, but it can actively detect threats from collaboration apps like Gmail or Zoom, which enable ABC Information Security Inc. companies to take action using the method downstream.

ABC's anomaly detection builds a model for each user and uses their behavioral data to determine which is "good" behavior and "bad" behavior. This is a distinguishing feature of the system that determined its ability to detect and stop sophisticated social engineering attacks with the help of machine learning and behavioral AI. By training the AI to recognize "good" behavior, it may be able to detect anomalies within suspicious emails, URLs, or attachments that accompany them. This AI contains over 45,000+ unique signals, enabling it to form a comprehensive picture to determine if the emails are malicious or not.

After the system detects a malicious email, it will notify the user. Here is an image to see what it looks like:



Threat Statement:

Even though ABC is an email security company, it also has the potential to be jeopardized in a security breach. Although many threats could endanger ABC, here is the list of threats that we believe are the threats to ABC:

- External hackers
- Insider Threats
- Employee Negligence
- State-Sponsored Actors
- Competitors
- Disgruntled Employees
- External Vendors
- Misleading Feeds

To briefly explain why we think these are threats:

- External hackers: they can be granted unauthorized access to the system of ABC.
- Insider Threats: they can gain information from working from ABC and can pass on information to malicious outsiders.
- Employee Negligence: it can happen when an employee is unmonitored.
- State-Sponsored Actors: The most dangerous threat. They have the backing of a nation-state. They may have an interest in taking down the ABC security system for political reasons.
- Competitors: Other companies may try to undermine ABC for business reasons.
- Disgruntled Employees: if an employee wants to get revenge on ABC for any reason, they may work with malicious actors.
- External Vendors: they may be compromised by external threats, which in turn may have access to ABC themselves, depending on how much access they have to ABC's information.
- Misleading Feeds: False Negative. It may be a faulty system that enables attackers to bypass the security.

By reconstructing the threat statement, we can conduct the possibility of likelihood and the impact it causes on the system of ABC company.

Risk Assessment Results:

Using the Risk Assessment approach, we individually examine all the assets, threats, and vulnerabilities in addition to evaluating the likelihood and impact of each asset of ABC. We calculate the risk score of each asset that is a threat to the ABC.

Based on the information provided in Appendix B, it concludes that the Email Server and AI attacks have the highest risk score out of all the assets in ABC. It is a

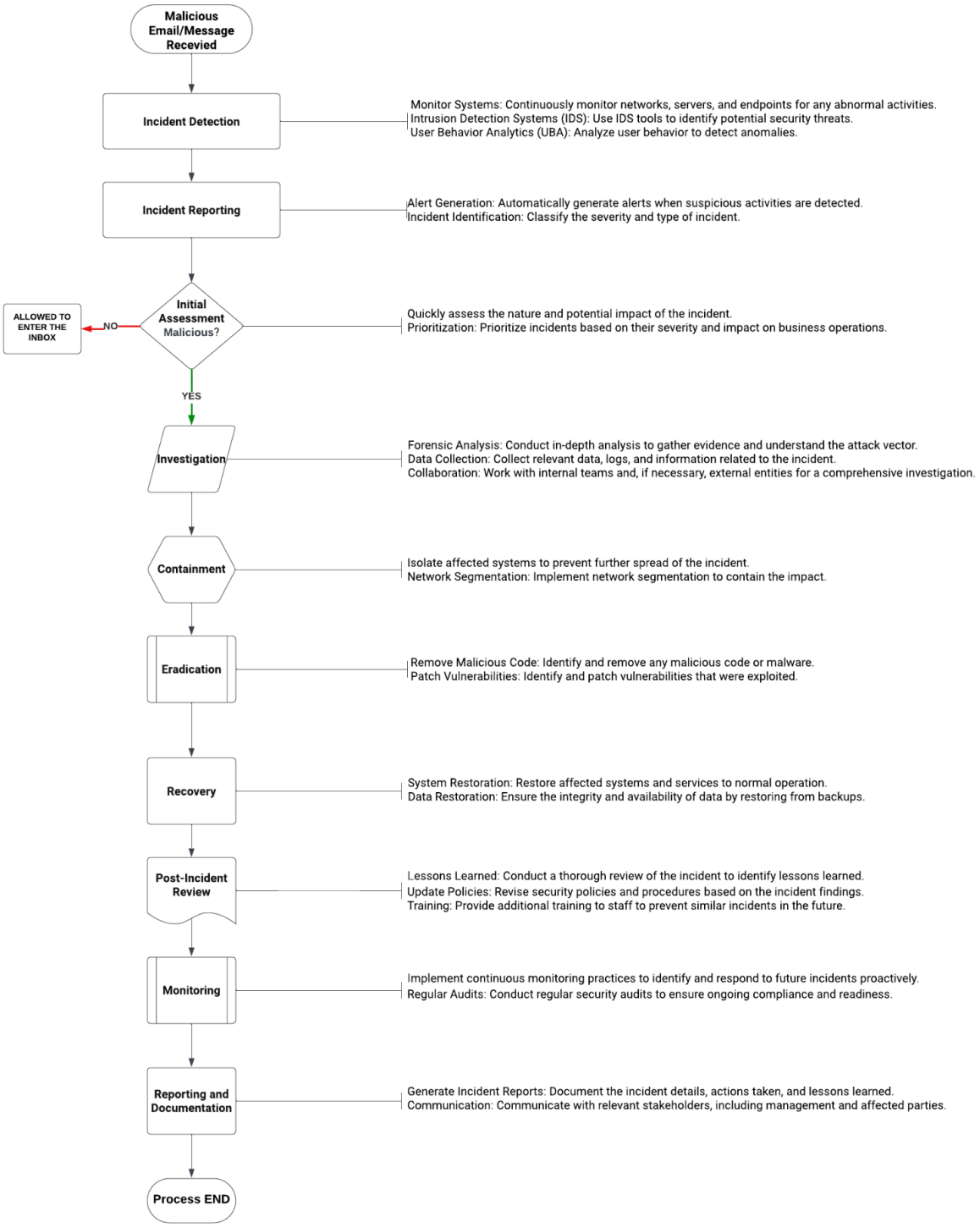
natural conclusion, accounting that the state-sponsored actors have access to resources and information from the state to carry out their activities. With that same note, AI was just as likely to be targeted as Email Servers. If the AI were to be compromised, it would be used for malicious purposes, allowing malicious emails to be able to bypass security parameters. The other assets at risk score greater than 50 also need immediate attention but with less focus on them than the most critical risks: Email Servers and AI.

Those within the risk score of 10 to 50 may not need immediate action, but an action plan is still required. A reasonable timeframe is in place for those in the medium risk score. This is important because if it isn't solved, it can be escalated to a serious problem, which may or may not be tapped into other assets that could be affected in ABC. For the low-risk score of 1 to 10, it is up to ABC if they want to implement an action plan or not, acknowledging the possible risk they are willing to take.

You may look at Appendix B for full details on the risk statement for each asset in ABC.

Appendix A

Process Flow Chart



Appendix B

Risk table

Information Asset	Vulnerability	Threat Source	Threat Action	Impact	Threat Likelihood	Tentative Risk Score
Email Server	Lack of Regular Patching	State-sponsored Actors	Exploitation of Unpatched Systems	High	1.0	100
AI Protection	Limited Self-Learning	Cyber Threats	Adversarial Attacks on AI Systems	High	1.0	100
Anomaly Detection	Limited Data Sources	External Threat Actors	Evasion of Anomaly Detection	High	0.6	60
SIEM (Security Information and Event Management)	Inadequate Log Analysis	External Threat Actors	Evasion of Detection through Clever Log Manipulation	High	0.6	60
Customer Email Data	Insufficient Encryption	External Hackers	Unauthorized Access	High	0.5	50

Threat Intelligence	Inadequate Monitoring	Disgruntled Employees	Unauthorized Access to Threat Data	High	0.5	50
VPN	Weak Authentication	Cybercriminals	Unauthorized Access through VPN	High	0.5	50
Attachment and URL Analysis	Limited File Type Analysis	Malware Distributors	Successful Malware Distribution	High	0.5	50
Phishing Vulnerability	Lack of Anti-Phishing Measures	Cybercriminals	Successful Phishing Attempts	High	0.5	50
Encryption and DLP	Misconfigured Encryption	Malicious Insiders	Data Leakage	High	0.4	40
Firewall and IPS	Outdated Rules	Hacktivists	Bypassing Firewall Rules	High	0.4	40
Security Policies	Lack of Employee Training	Competitors	Social Engineering Attacks	Medium	0.5	25
User Interface (UI)	Weak Authentication	Phishing Attacks	Compromised User Credentials	Medium	0.4	20

Collaboration Tools	Unauthorized Access	Former Employees	Unauthorized Sharing of Sensitive Data	Medium	0.4	20
Security Awareness Training	Low Employee Participation	State-sponsored Actors	Targeted Social Engineering Attacks	Medium	0.4	20
Agent-Based Protection	Delayed Agent Updates	Insider Threats	Exploitation of Unpatched Agents	Medium	0.4	20
Incident Management System	Lack of Automation	Insiders	Delayed Incident Response	Medium	0.3	15
Alerting System	Delayed Alerting	Insider Threats	Failure to Timely Respond to Security Alerts	Medium	0.3	15
Behavioral Analytics	Inadequate Training	Unintentional Insiders	Misinterpretation of Behavioral Data	Medium	0.3	15
Threat Intelligence Feeds	Lack of Validation	Misleading Feeds	Misinformed Security Decisions	Medium	0.3	15

Threat Log	Incomplete Logging	Internal Threat Actors	Concealing Malicious Activities	Medium	0.3	15
Reporting Module	Inaccurate Reporting	External Vendors	Manipulation of Report Data	Low	0.2	10

Recommendations to protect the above Information Asset

Email Server:
Implement regular patching and proactive monitoring to enhance server security.

AI Protection:
Continuously update AI algorithms, collaborate for resilience, and prioritize R&D for evolving threats.

Anomaly Detection:
Enhance anomaly detection by incorporating diverse data sources and refining algorithms.

SIEM (Security Information and Event Management):
Optimize SIEM configurations for improved event correlation and faster incident response.

Customer Email Data:
Strengthen encryption protocols to safeguard customer data integrity.

Threat Intelligence:
Improve threat intelligence capabilities through enhanced monitoring and analysis.

VPN:
Strengthen VPN authentication mechanisms to prevent unauthorized access.

Attachment and URL Analysis:
Enhance file type analysis to prevent successful malware distribution.

Phishing Vulnerability:
Implement anti-phishing measures to thwart phishing attempts.

Encryption and DLP:
Regularly audit and update encryption configurations to prevent data leakage.

Firewall and IPS:
Regularly update firewall rules to prevent rule bypassing.

Security Policies:
Conduct regular employee training on security policies and social engineering awareness.

User Interface (UI):
Strengthen authentication mechanisms to prevent unauthorized access.

Collaboration Tools:
Monitor and control access to prevent unauthorized sharing of sensitive data.

Security Awareness Training:
Increase employee participation in security awareness training.

Agent-Based Protection:
Ensure prompt updates to agents to prevent exploitation of unpatched vulnerabilities.

Incident Management System:
Integrate automation for swift incident response.

Alerting System:
Ensure real-time alerting to minimize response delays.

Behavioral Analytics:
Provide comprehensive training to interpret behavioral data accurately.

Threat Intelligence Feeds:
Validate and verify incoming threat intelligence feeds for accuracy.

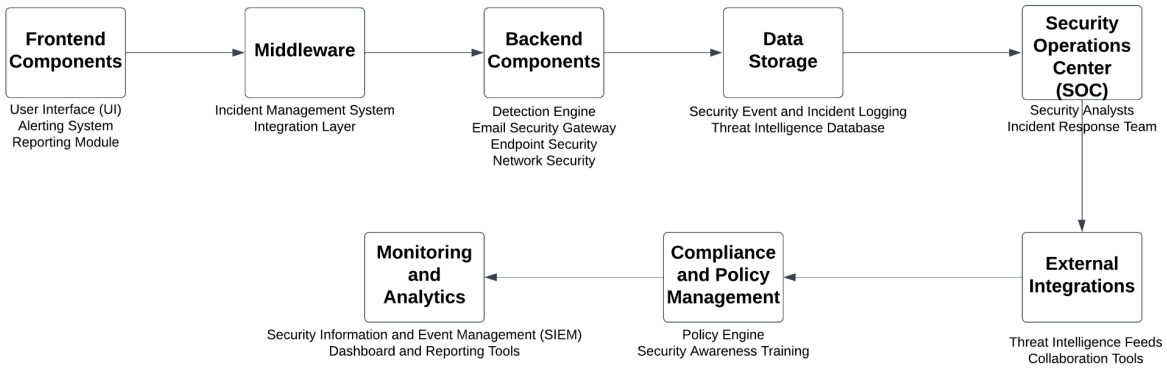
Threat Log:
Implement complete logging for transparent monitoring and detection.

Reporting Module:
Implement validation checks to maintain report data integrity.

These recommendations aim to address specific vulnerabilities and enhance the overall security posture of the ABC Information Security Inc. Information security company.

Appendix C

Basic System Architecture



Explanation

The basic system architecture for ABC Information Security Inc. an email security company involves a combination of hardware, software, networks, and processes designed to detect, prevent, and respond to security threats. Here's a simplified representation:

1. Frontend Components:

- User Interface (UI): Provides a dashboard for security analysts and administrators to monitor and manage security alerts.
- Alerting System: Sends real-time alerts to security personnel in case of detected anomalies or security incidents.
- Reporting Module: Generates detailed reports on security incidents, trends, and performance.

2. Middleware:

- Incident Management System: Orchestrates the workflow for handling security incidents, from detection to resolution.
- Integration Layer: Connects with external systems and tools for threat intelligence, log analysis, and incident response.

3. Back-end Components:

- Detection Engine: Anomaly Detection: Utilizes machine learning algorithms to identify abnormal patterns in email and network traffic.
- Behavioral Analytics: Analyzes user behavior to detect deviations from normal activities.
- Threat Intelligence Integration: Incorporates threat feeds to enhance detection capabilities.
- Email Security Gateway: -Spam and Anti-Phishing: Filters incoming emails to block spam and phishing attempts.
- Attachment and URL Analysis: Scans email attachments and URLs for malicious content.
- Encryption and Data Loss Prevention (DLP): Ensures secure transmission and prevents accidental data leakage.
- Endpoint Security: Agent-Based Protection: Deploys security agents on endpoints to detect and mitigate threats.
- Patch Management: Ensures that software and systems are up-to-date to prevent vulnerabilities.
- Network Security: Firewall and Intrusion Prevention System (IPS): Monitors and filters network traffic to prevent unauthorized access and attacks.
- Virtual Private Network (VPN): Ensures secure communication for remote access.

4. Data Storage:

- Security Event and Incident Logging: Stores logs and events for auditing, analysis, and forensic purposes.
- Threat Intelligence Database: Maintains a repository of known threats and indicators of compromise.

5. Security Operations Center (SOC):

- Security Analysts: Monitor alerts, conduct investigations, and respond to security incidents.
- Incident Response Team: Coordinates the response to security incidents, including containment, eradication, and recovery.

6. External Integrations:

- Threat Intelligence Feeds: Integrates with external sources to receive real-time threat intelligence.
- Collaboration Tools: Connects with communication platforms for team collaboration during incident response.

7. Compliance and Policy Management:

- Policy Engine: Enforces security policies and ensures compliance with industry regulations.
- Security Awareness Training: Provides training modules to educate employees about security best practices.

8. Monitoring and Analytics:

- Security Information and Event Management (SIEM): Collects, analyzes, and correlates security events from various sources.
- Dashboard and Reporting Tools: Provides visualizations and reports for security performance and incidents.

Conclusion

In conclusion, ABC Information Security Inc. is well-equipped, but continuous improvement is vital for staying ahead in digital security. Implementing the outlined recommendations ensures a proactive and resilient approach, emphasizing regular assessments, training, and collaboration to maintain top-tier email security standards.