

Original Article

Strengthening Insider Threat Monitoring Post Covid-19: Strategies and Tools

Sabeeruddin Shaik

Independent Researcher, Alpharetta, Georgia, USA.

Received Date: 30 August 2023

Revised Date: 23 September 2023

Accepted Date: 30 September 2023

Abstract: *The pandemic has made companies adopt remote work policies and convert to cloud-based technologies. This adoption has helped the companies to continue the business without disruption, but this has also increased the risks for the companies. One of the critical risks among them is Insider Threats. Due to the Remote work option, employees can access the data without any surveillance monitoring. This privilege might lead to stealing or misuse of the data. This Paper will provide the Risks associated with the adoption of the Remote work Policy and Insider Threats. This Paper also provides a solution to mitigate these Insider threats by utilizing Robust Insider Threat monitoring tools to protect sensitive data and improve the Organization's security posture in this Hybrid work Model.*

Keywords: *Insider Threats, Remote Work, Cybersecurity, Post-Covid-19, Threat Monitoring, Behavioural Analytics, Zero Trust, Data Loss Prevention.*

I. INTRODUCTION

The transition of the work model from On-site premises to remote during the pandemic has allowed companies to continue their business operations, saving them from financial losses and making available resources. However, it has also increased risks like insider threats; traditional cyber security strategies and tools cannot mitigate these latest risks. Insider Threats refer to the potential risks that an organization may face, including the impact of insiders, including employees and contractors who have access to the company's assets and data. Intentionally or accidentally, companies might face Insider Threats.

Here are a few Risks for example:

- Excess availability of data without any surveillance
- Since Employees work remotely, it has become hard to track what they are doing
- Employees or contractors steal the data or unintentionally expose the Sensitive data by not following the security standards and security controls.
- Since employees use their personal devices, they might not be configured with security measures, which leads to vulnerability for the attackers to gain the data.

This research analyses these Risks and provides solutions and Mitigation measures regarding monitoring frameworks that can Mitigate these potential risks.

II. MAIN BODY

A. Problem Statement

The transition to Remote and Hybrid work models has increased the Risks and difficulties to manage and mitigate the Insider Threats, including:

- Decentralized Data Control—It has become difficult to monitor and manage employees' privileges to access sensitive data because employees work from different locations, and it is difficult to log their accountability.
- Increase in False positives—It has become difficult to Differentiate between Legitimate and Malicious activities because of diverse work patterns.
- Data mishandling—Intentionally or accidentally due to work stress or Personal issues. There are also risks based on the employee's mood to lose the data due to carelessness or dissatisfaction.
- Lack of Monitoring and Endpoint Security Tools—Without Monitoring and Endpoint Security Tools, it has become difficult to log employees' User Activities and protect data in Transit, which leaves gaps in protecting sensitive data.

Insider Threats don't need to be malicious activity done by attackers. Insider Threats may also be possible by Employees. It might not be Intentional, but accidentally, they could transfer the data on an insecure channel. Due to a lack of security awareness, they might provide sensitive information to the social engineering attackers. Due to the Increase in dependencies on Third party vendors and adapting to the Hybrid Work environments. Companies might possess risk from the contractors or vendors. Lack of proper security controls and setting up Application setup rules. Due to improper



knowledge, employees might visit a malicious website and download applications, which will further help attackers to exploit vulnerabilities. Increase in phishing and social engineering attacks

B. Solution

To mitigate Insider Threats, Organizations should implement the following Strategies:

- Zero Trust Architecture—Implement Zero Trust Architecture (ZTA). Strict Access controls should be applied. No employee should have access to any resources without authentication. Authorization is provided to employees based on their job roles and duties.
- Analysing Behaviour Patterns-Machine learning algorithms can be used to analyse the Behaviour patterns of employees. These patterns track the employees' normal work hours and job duties, and if something suspicious happens to their behaviour, it will trigger an alert.
- Implementing Data Loss Prevention (DLP) tools—Implementing DLP Tools limits access to share, download, and transfer folders or data, which prevents unauthorized access and loss of sensitive data.
- User and Entity Behaviour Analytics (UEBA) monitors user Behaviour anomalies and alerts if someone tries to access the account during unusual hours or from unusual locations.
- Insider Threat security awareness—It is crucial to educate the employees about the Insider Threat and to have them report any suspicious activities to management. Also, employees must be trained about phishing and social engineering.
- Real-time monitoring—Use the SIEM and SOAR tools to continuously monitor and log activities. These Robust Monitoring and detection tools continuously monitor and triage alerts if something is malicious.
- Integration into Advanced Threat Intelligence Platforms- Integrating the systems with the Advanced Threat Intelligence Platforms will help the organizations to detect and mitigate the threats by continuously monitoring and detecting emerging threats and implementing preventative measures. This Intelligence integration will also be helpful in detecting the external attacks and also Internal.
- Endpoint Detection Response Tools - Deploy EDR Tools to provide end-to-end security for the data. EDR tools help to detect any suspicious activities on the systems. Deploy AI tools for Behavior Analysis- Deploy Artificial Intelligence and Automated tools to monitor the network continuously and trigger alerts if something is malicious through analyzing the Behavior patterns.
- Utilization of Blockchain for Integrity- To ensure the Integrity of the critical data Block, blockchain technology can be used. This will provide security for data from tampering. This will provide Robust evidence in the event of Insider threats.

Flow chart and Graphs:

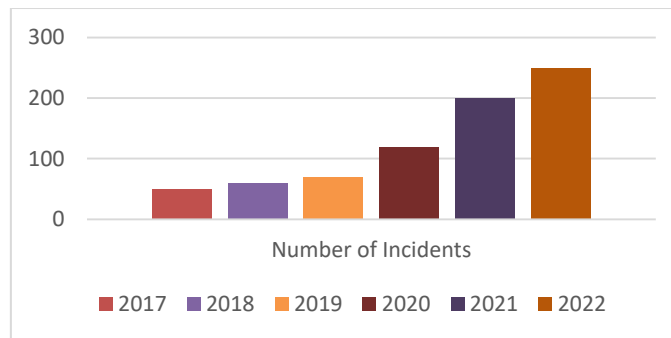


Figure 1: Graph showing the trend in insider threat incidents before and after COVID-19

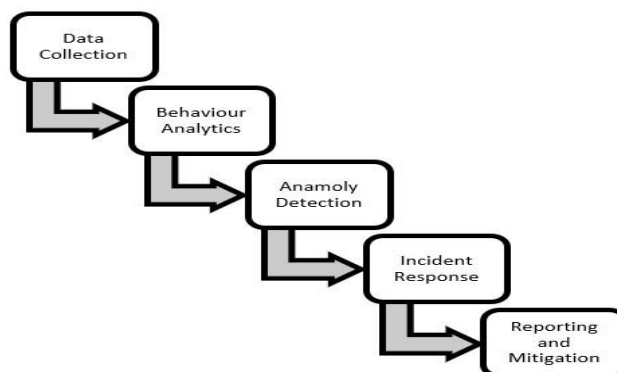


Figure 2: Flowchart Explaining the workflow for Insider threat detection

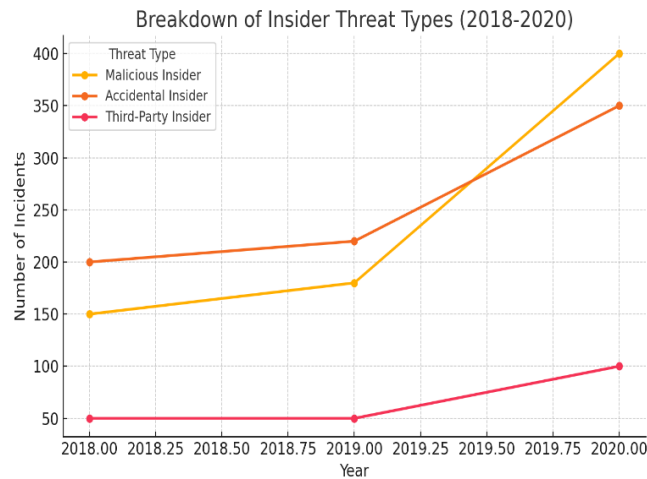


Figure 3: Breakdown of Insider Threat Types from 2018-2020

III. USES

Objectives on Implementing Insider Threat Monitoring Tools:

- **Data Protection:** Improved security Measures to protect organizations' sensitive data and secure companies from Data Breaches.
- **Regulatory Compliance:** By Implementing Insider Threat mitigation measures, companies can satisfy the compliance requirements for industries with strict measures, such as healthcare and finance.
- **Reduced Risk:** If the Data gets breached, the companies will be fined, which impacts financial loss and reputational damage. But with the Insider threat mitigation strategies, we could mitigate these risks and reduce the likelihood of financial losses and reputational damage.
- **Proactive Analysis:** Potential Threats can be predicted through Data Analysis techniques, and risks can be mitigated by implementing preventive measures before they impact.
- **Security Awareness:** Makes employees Accountable and act responsible for reporting the risks. Deploying Robust security tools helps in detecting Insider threat incidents, which helps in reducing recovery time and limiting the damage. Since the recovery time is reduced and the resources are available without any downtime, Data loss is being prevented. This helps in minimizing the financial losses. Regular monitoring and tracking of the work details and actions will make employees accountable for their actions. Deployment of EDR Tools and following ZTA Principles helps in minimizing Data loss and continuously monitoring the activities on the network. Monitoring tools also help in tracking the actions and events of vendors and contractors, thus keeping the organizations in a secure place.

IV. IMPACT

The implementation of Insider Threat Mitigation strategies has positive impacts such as:

- Improved Defense Mechanisms of the companies by improving the ability to detect and analyse the Risks
- The improved security measures will build the trust among the stakeholders and build confidence about the data security
- By following these measures, the security posture of the organizations can be improved
- By Implementing tools like DLP, the data exfiltration has been reduced. This helped in preventing the Sensitive Data loss.

Providing Greater compliance with regulatory requirements. Even though adopting Remote and Hybrid work environments due to having clear monitoring and tracking capabilities it has become safe for the organizations.

V. SCOPE

Insider Threat Management Strategies are critical for Industries like Healthcare in safeguarding Patients data from insider threats by limiting access to authorized personnel, In the Finance sector, the loss of data of Credit cards and other PII data has been minimized. Advanced AI and automation tools can detect any suspicious transactions or data transfers. In Government sectors, Classified information requires strict protocols to mitigate espionage and unauthorized disclosures. Insider threat programs in this sector must combine technical monitoring with rigorous vetting and psychological assessments. Since the data involved in these sectors are very sensitive and Top secret, these strategies could also be implemented in all other industries. In the future, with the help of Artificial Intelligence, it is also possible to develop strategies and automate security to enhance security controls, which can act as precatave measures in safeguarding Sensitive Data.

VI. CONCLUSION

The Covid-19 pandemic has changed the world. This pandemic greatly impacted the world of technology in both positive and Negative ways. So, Industries should understand this change and act responsibly to prevent the Negative Impacts. It's high time to implement Robust Security Monitoring, Endpoint security tools, and DLP tools to Prevent and safeguard the Data from Insider Threats. It is also crucial to provide security awareness to employees about these threats and educate them to mitigate these risks and act responsibly. These measures will not only impact the short term but will help to reach the long-term security goals and Ensure safety against evolving threats.

VII. REFERENCES

- [1] J. D. M. B. C. Probst, Insider Threats in Cybersecurity, springer, 2010.
- [2] S. K. a. J.Lee, Managing Insider Threats: An Integrative approach, Information systems Research, 2013.
- [3] e. al, A comprehensive survey of data mining based fraud detection research, Artificial Intelligence Review, 2010.
- [4] a. R. P.Cappelli, The CERT guide to Insider Threats, Addison Wilsey, 2012.
- [5] e. al, Common sense guide to mitigating Insider Threats, Software Engineering Insitute, Carnegie Mellon University, 2013.
- [6] E.Cole, Insider Threat: Protecting your organization from the Human point of failure, Syngress, 2014.
- [7] J. a. T.Allen, Integrating Behaviour Analytics in Insider Threat Programs, IEEE Transactions on Security, 2016.
- [8] R.K.Skopil, Finding the Blance:Data Privacy and Insider Threat, IEEE Security and Privacy, 2018.
- [9] J. a. R.D.Flaherty, The EvolvingLandscape of Insider Threats, Computers and Security, 2019.
- [10] L. a. S.Becker, Cultivating CybersecurityAwarness Among Employees, Information systems Journal, 2019.