Deloitte.

Digital Forensic Insider Threat (DFIT)

An innovative and proactive approach to help combat insider threats

Insider threat emanating from an organisation's employees, suppliers or vendors continues to be one of the largest unsolved issues in the fight against fraud. According to a study by Ponemon Institute, the average global cost of insider threats in 2022 is expected to rise to $15.38 million — a 44 percent jump from 2018[1].

While organisations are certainly aware of the issue, they rarely dedicate the resources or attention required to solve it till it is too late. Most prevention programmes fall short either by focusing exclusively on monitoring behaviour or by failing to consider cultural and privacy norms.

At Deloitte, we can capture digital evidence before it's lost and help you make intelligence-led decisions to prevent possible crises.

Have you faced a similar situation?

Monitor access to sensitive customer data
Due to remote working, an employee has been granted full access to company data, including data that he/she may not normally have access to. – DFIT can help investigate and help you take necessary action to prevent fraud that may result from copying, transferring or anomalous access to information by monitoring user behaviour proactively.

Respond to regulatory requests or conduct a covert investigation
A whistle blower allegation on supplier fraud has been received. – DFIT can help conduct localised surveillance of the procurement team, focus on suspicious activity and collect vital evidence before it gets potentially destroyed.

Monitor the systems of at-risk employees
A disgruntled employee has recently put down his papers. While his last day is a month away, you need help to actively monitor his online activities across your company network. – DFIT can help identify 'at-risk' employee groups and develop risk profiles for each along with tailored customised alerts. The tool can also help you develop procedures to detect, respond and investigate, if necessary.

Manage risk during sensitive transactions (including handling of Unpublished Price Sensitive Information (UPSI))
Your organisation is part of a merger, acquisition, or other type of price-sensitive transaction where privileged information is available and/or circulated by a subset of employees, such as a merger project team or specific members of the finance teams. – DFIT can help you understand general user habits. Comprehensive logging can provide context around alerts to distinguish suspicious behaviour from routine activity.

Identify data misuse
An employee crops a signature from a confidential financial document and shares it over skype/ other IM chats. – DFIT can help you understand the user's habits and investigate the files accessed by the user. It can check the screenshots taken and provide a trail of who the files were shared with.

Investigate and isolate the systems
Your IT team has observed alerts where systems seem to have been compromised, volume shadow copies have been deleted and similar other unusual behaviour on the endpoints. – DFIT can help investigate the alerts and isolate the system from the network, to stop the ransomware from spreading. Further analysis for the root cause can be conducted by investigating all the events on the system.

1) 2022 Ponemon Cost of Insider Threats Global report

Employee pre-departure. Regulatory response. Internal compliance. Investigations. Litigation. M&A – These are just some of the scenarios where DFIT can prove to be a valuable asset.

Keeping your organisation secure and protecting your assets from threats can be challenging. Combining total visibility with flexible automated detection, DFIT can help:

Anticipate events and incidents to determine the rules required to capture vital evidence.

Monitor systems for keyboard, application and file activity in order to identify events to alert.

Respond in real-time by preserving evidence covertly and forensically; as well as isolating devices and automating investigative tasks.

Provide vital information to the management, and help you take strategic informed decisions.

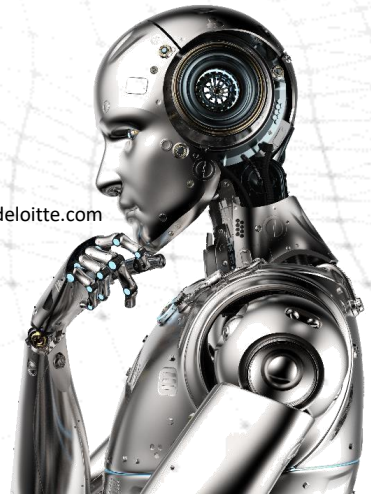
A pre-emptive approach can enable organisations to make decisions strategically and be better placed to defend themselves from any legal actions. Ultimately, finding issues pre-emptively can help reduce the risk of a serious data compromise or compliance violation. It can also help investigation teams to be in a better position to protect the organisation, while meeting regulatory obligations.

To understand how this technology can transform your organisation, reach out to:

Nikhil Bedi
Partner and Leader – Forensic
Financial Advisory
Deloitte India
Email: nikhilbedi@deloitte.com

Jayant Saran
Partner – Forensic
Financial Advisory
Deloitte India
Email: jsaran@deloitte.com

Sachin Yadav
Director – Forensic
Financial Advisory
Deloitte India
Email: sachyadav@deloitte.com



Learn more about Deloitte Forensic services.
Visit our website: https://www2.deloitte.com/in/en/pages/finance/topics/forensic.html