DETECTION & CONTAINMENT OF DATA SECURITY BREACH

The Client's Profile

The client is a prominent Industrial Automation Company with multi-city branches across India. Their company has exhaustive experience in factory automation, and integration of special machines and production lines. They are providers of engineering services and several value added services that effectively implement the automation solutions. The company partners with numerous renowned automations component manufacturers from the USA and Europe. Their installations span across sectors including heavy engineering, automotive engineering, and aerospace, among others.

Client's Requirement - Challenge Ahead of Flatworld Solutions

Illegitimate data sharing is extremely pernicious to businesses that rely majorly on data. The threat can be both: internal and external; in the former, an employee or insider may be involved in leaking data out of the office by means of portable media devices, while in the latter, hackers make way into the network due to improper security measures. Our customer, the leading Industrial Automation Company owner, was suspicious of their confidential data falling into the wrong hands. The company suspected some of its ex-employees to either have taken some crucial data during their term of service, or worse, that they still had access to the current data. The loss in business and the risk of a tarnished reputation was causing a whole lot of worries for the client. The company's management wanted to:

- Get into the roots of data theft
- Possibly identify the hackers who could have been causing the damage.

This demanded a comprehensive review of all the IT controls and the company's information security practices. The systems suspected to have been gateways to leakage were to undergo digital forensics in order to collect sufficient evidence based on which the client could take action.

Client's Major Security Concerns

- Bringing the company's IT practices in line with the standard industry practices
- Completely disabling any remote access to the company's confidential data
- Performing stringent checks on the current usage in the IT infrastructure, in order to detect any illegitimate activities
- Improving the overall position of security

Flatworld's Security and Forensics Solution

Flatworld Solutions began the security process by trying to recognize all the loopholes, by conducting a meticulous Information Security Review. We paid attention to many areas like,

- The review and implementation of information security policy and the IT policy
- Email server and configuration policy
- Active directory and proxy servers
- VPN setups
- Firewalls, policies for remote access, and for access to portable devices like USB drives, disks, and laptops
- Internet Access Policy
- In-depth scrutiny of the log files of all the above mentioned devices

The review empowered us to start forensic analysis on the systems on which we had a doubt. By capturing Hard Disk and RAM images of these machines, we extracted all the essential information that could lead us to the cause of the leakages; like emails, chat conversations, browsing history, tracing exfiltration of data through USB devices or Internet, using keyword searches for detecting any signs of confidential information being stored on the system. We accomplished all the tasks with a high level of accuracy and submitted the relevant reports based on which the client could decide the next steps of action.

If you'd like to hire our experienced software professionals for data forensic, or want to outsource software development services to us, please feel free to get in touch with our expert team.