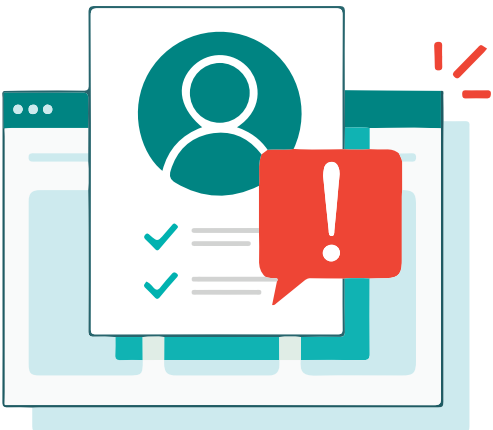# liferaft

CASE STUDY

How a Renowned Biotechnology Company Used Liferaft to Safeguard Their Executives

A biotech company faced a potential threat to one of its Executives.

An alarming Tweet raised concerns about the Executive's safety, but swift removal hindered efforts to gather crucial information, leaving the team with an incomplete profile of the individual involved.

The company was alerted by Liferaft and was able to retrieve an image of the original Tweet before its deletion. This enabled their team to obtain the full name of the threat actor, the content of the Tweet, and its timestamp. With the acquired information the team member used Liferaft's identity resolution tool, People Search, and was able to assemble a basic profile of the individual, including factors such as age, location, and any previous mentions of their company on their social media accounts.

Through careful analysis, the company determined that the person of interest did not reside locally. However, it was discovered that the original post originated from a location in close proximity to where the Executive was currently residing.

Acting promptly, the team shared this crucial intelligence with both the Executive Protection team and the Physical Security team. The breadth of information allowed the team to make an informed decision as to whether or not to implement a heightened level of security.

The companys proactive approach and utilization of Liferaft's capabilities, enabled them to assess the threat level and take the appropriate action to ensure the overall safety and security of the organization and Executives.

> "We went back to our Queries and found Liferaft had an image of the Tweet, so it was collected before the person had the opportunity to delete it... If Liferaft hadn't captured it, we would not have been able to do anything. That was a big win for us!"

Threats to Executives

- Stalking, harassment, threats to physical safety, and reputational damage

- Risk of doxxing and identity theft to executive and their families and close relatives

- Geographic-based risks including political unrest, civil freedoms, health & medical, weather, and others

How Liferaft Can Help

- Monitor for threats using keywords or geolocation and be alerted to high-risk posts in real-time

- Manage threat actor intelligence as it relates to brand and executive protection

- Follow and tag accounts to be notified of online activity

Using Open Source Intelligence for Executive Protection

Keyword Queries
Watch out for mentions of executives, team members, and their families and close contacts alongside threatening terms.

Deep & Dark Web
Threats can emerge from a growing list of alt-tech social networks and the Dark Web.

Location Monitoring
Set up a geofence to monitor social media posts published from specific locations.

Keep Records
Posts can get deleted — record all relevant content for future reference.

Set Up Alerts
Set up a process to quickly alert if a violent threat is spotted online.