CASE STUDY

INSURANCE COMPANY

reva™

THE CHALLENGE

The client offers digital insurance care and consultation.

Based in the United States, the client has a large and growing database, from clients to experts and also offers an online payment gateway.

Cybersecurity measures are a main concern for the client, to secure their data. To mitigate the risk, we must first monitor external activities that may have already targetted them, not only to detect threats and leaks, but also to predict and counter any future possibility of violations.

THE SOLUTION: REVA

REVA provides a real time platform that:

- Scratches links on deep and dark webs
- Searches for information disclosed in cyberspace
- Identifies advanced threats
- Profiles data vendor
- Gathers intelligence on targeted cyber threats while removing and remediating those threats.

See the RESULTS of the DEMO.

THE RESULTS

PHISHING ATTACKS	7
OPEN PORTS	4
FAKE APPS	2
EMAIL BREACHES	11

NEXT STEPS

- Validate the list of all pages/employees and takedown profiles that might cause reputational damage

- Verify all official pages/accounts across all social media platforms

- Change the passwords of the email accounts

- Enable Multi Factor Authentication

- Disable public access to sensitive services and restrict access through VPN or IP whitelisting to authorized entities.

- Conduct Penetration Tests on needed exposed applications

- Use secure protocol versions (POP3S/ IMAPS instead of POP3/IMAP)