CASE STUDY

LARGE FINANCIAL INSTITUTION

reva™

THE CHALLENGE

Hackers could access our client and collecrt information to:

- Blackmail
- Access accounts
- Phish/scam the CEO/CFO
- Identity theft of key people

These threats cannot be detected using traditional approaches such as:

- **Penetration testing**
- **Security Operations Center**
- **IT infrastructure assessments**

In order to become preventive, organizations must monitor external activities that target them, not only to detect threats but to predict and counter any future possibility of violations.

THE SOLUTION: REVA

REVA provided a real time platform that:

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

THE RESULTS

TAKEDOWNS

600 pages of Facebook imitators, Instagram impostors and Twitter

REPORTS

Weekly and monthly reports, with quantitative cyber threat and risk assessment

PRE-ATTACK SECURE

Improved their security posture and blocked malicious intruders in pre-attack phases

REMEDIATION

Remediation plans and operational assistance to eliminate these threats in the future

CONCLUSION

- Millions of dollars saved on potential lawsuits from leaked credentials and data

- 600 imposter pages takren down

f in

www.shelt.com