groupsense

DATA SHEET:

CYBER THREAT PROTECTION FOR ELECTIONS

PROTECTING ELECTIONS BEGINS LONG BEFORE VOTERS CAST THEIR BALLOTS

Ensuring the security and integrity of elections has become a vital concern for democracies worldwide. Elections shape leadership, policy and governance, affecting the safety and prosperity of billions of citizens. There are countless illicitly-motivated forces that desire to influence elections. The power of the internet enables their interference and magnifies their influence.

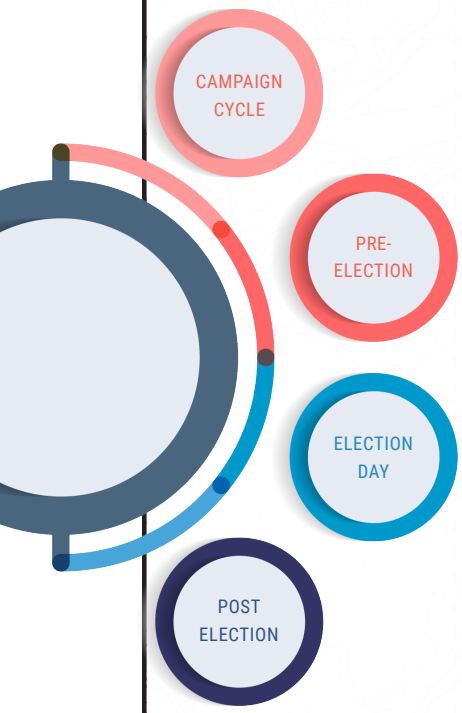
From the 2016 US presidential election to local and national elections worldwide, a flood of cyber attacks continues in many forms:

Attacks on election bodies, voting infrastructure, parties and candidates.

Disinformation campaigns that propagate false or misleading information to disrupt voting and influence public opinion.

Coordination of physical and kinetic threats to polling places and candidates.

Governments, political parties and candidates must all act now to activate cyber threat intelligence services to harden their information security and get ahead of inevitable cyber threats to the election process.



GROUPSENSE EMPLOYS A FOUR-STAGE MODEL FOR MONITORING ELECTIONS

18 Months Before Election Day

- Assess the digital threat profile of the organization and the election
- Identify threats, adversaries, vulnerabilities and high risk issues
- Advise client on security improvements
- Commence threat monitoring

30 Days Before Election Day

- Increase tracking of identified threat actors
- Identify and monitor disinformation and disruption attempts
- Assess impact and response to adverse events
- Advise on any last minute security changes

Day of Election

- Continuous monitoring before, during and after polls close
- Real-time monitoring to detect active threats
- Constant communication with the client security team

Post-Election

- Monitoring for post-election communications
- Documenting behavior of threat actors
- Debrief with client on findings and results

WHAT DOES IT TAKE TO SECURE AN ELECTION?

You need a cyber threat intelligence service provider with the skills and technology necessary to assess the risks and monitor for threats before and during elections. GroupSense has a proven track record of providing cyber threat intelligence on elections for large municipalities and state governments. We work alongside you to understand your organization's profile, structure, assets, vulnerabilities and requirements. We advise you on how to reduce your risk profile and monitor for threats throughout the election cycle.

4040 North Fairfax Drive, Arlington, VA 22203 | +1-877-469-7226 | sales@groupsense.io

groupsense

4040 North Fairfax Drive, Arlington, VA 22203 | +1-877-469-7226 | sales@groupsense.io

groupsense

DATA SHEET:

CYBER THREAT PROTECTION FOR ELECTIONS

FEATURES

Assessment

GroupSense will assess and analyze your cyber threat posture and vulnerabilities, providing guidance on technical and operational improvements.

Portal

All alerts, advisories, questions and support are conducted via a secure intelligence portal.

Support

GroupSense intelligence analysts are available to support you throughout your engagement.

Intelligence Advisories

You will receive high-fidelity, finished intelligence advisories specific to your organization, which include analysis and recommended actions.

Monitoring

Using its Tracelight cyber reconnaissance platform, GroupSense will monitor the surface, social, deep and dark web for threats and risks directed at your organization and election.

ADDITIONAL ELECTION RELATED SERVICES

- Operational Security education and training for leadership, managers and staff;
- Full time managed threat monitoring;
- Integration and coordination between Threat Intelligence and Security Operations.

SHARKS REPORT

Learn about how weaponized email addresses were used to launch a large-scale disinformation campaign that may have impacted the outcome of the 2016 US presidential election.

ABOUT GROUPSENSE

Actions are louder than words. We are changing the way cyber intelligence is delivered and put into action.

GroupSense is a leading provider of cyber intelligence services. GroupSense is not a feed, or a search engine for the dark web. GroupSense are people, empowered by proprietary technology, helping information security and intel teams realize value.

We are trusted by governments worldwide to assist in cyber intel program development, election monitoring, and anti-fraud and risk measures.

GroupSense tracks known and suspected threat actor and groups, publishing research. Our team reaches out to affected organizations regardless of customer status.

groupsense

4040 North Fairfax Drive, Arlington, VA 22203 | +1-877-469-7226 | sales@groupsense.io

groupsense

4040 North Fairfax Drive, Arlington, VA 22203 | +1-877-469-7226 | sales@groupsense.io