Mandiant Commercial services for Cybersecurity Services for Canadian federal, provincial, local and municipal entities

When the Whole World is Watching: The Tested Approach to Election Security

Defending against cyber threats targeting elections requires active defenses informed by intelligence. Those who support elections demand strategic security program capabilities and specific technical solutions to harden and enhance their security posture prior to an event and to support operations during the event. Delivering resilient cyber capabilities in a compressed time frame under intense public attention and scrutiny is a major challenge that requires focus and investment to properly plan and implement.

Mandiant Election Infrastructure Protection

Mandiant's unique combination of expertise across threat intelligence, services, and solutions empower organizations to continually evolve to defend themselves against election threats like: data integrity and destruction, ransomware, insider threats, and information operations (IO).

Take the first step in securing your election infrastructure and follow the QR code to the Election Security checklist.

Prepare and protect your election infrastructure with these paid offerings today by visiting https://www.mandiant.com/.

Google Threat Intelligence (Google TI)

Google Threat Intelligence offers unparalleled visibility into the threat landscape, enabling organizations to proactively defend against cyber attacks. By leveraging insights from defending billions of users and analyzing millions of phishing attacks, Google Threat Intelligence empowers security teams to understand threat actors and their tactics, techniques, and procedures (TTPs).

Learn more by visiting — https://www.mandiant.com/advantage/threat-intelligence.

Google Digital Risk Protection

Google Digital Risk Protection encompasses products and services that safeguard critical assets and data from external threats by providing visibility across the open, deep, and dark web. This enables organizations to identify malicious targeting, high-risk attack vectors, and attack campaigns while gaining insights into relevant threat actors and their tactics, techniques, and procedures (TTPs). Google offers digital risk protection through self-managed SaaS products or comprehensive services, empowering organizations to proactively enhance their cybersecurity posture.

Learn more by visiting — https://www.mandiant.com/solutions/digital-risk-protection.

Before the Election: Repeatedly Prepare, Harden, and Exercise

Cyber Incident Response Service

Cyber Incident Response Service through Mandiant offers comprehensive cyber incident response services, including investigation, containment, and recovery, backed by industry-leading threat intelligence to understand attacker tactics and motivations.

With 24/7 response coverage through Mandiant Managed Defense, organizations gain continuous protection and peace of mind throughout the incident lifecycle. Learn more by following the QR code.

Mandiant Threat Hunt

Mandiant Threat Hunt combines our extensive experience responding to intrusions carried out by advanced threat actors, industry-leading threat intelligence, to proactively uncover advanced threats missed by your existing security tools and controls. Identifies ongoing or past intrusions within your organization. Assesses risk by identifying weaknesses in security architecture, vulnerabilities, improper usage or policy violations, and system security misconfigurations. And, assess if your organization has the visibility to answer these questions.

Increases your organization's ability to respond effectively to future incidents. Follow the QR code to learn more.

Exercising and "re"exercising

Exercising and "re"exercising identifies opportunities for improvement and confidence in processes, capabilities, and capacity to detect and respond quickly to cybersecurity challenges and threats which may impact citizen voting experiences and confidence.

Beyond retaining leading incident response capabilities and capacity, Mandiant offers review, alignment, and exercising of Election incident response playbooks, to include cyber crisis communications with all stakeholders.

During the Election: Continually Test, Monitor, and Defend

Red and Purple team exercises

Red and Purple team exercises can effectively test your security capabilities and technical readiness to find flaws before attackers can. Test your controls against the latest attack scenarios, aligned with industry-standard ethical red-teaming frameworks and driven by real-world threat intelligence.

Exercises range from red team assessments, penetration testing, purple team and embedded device assessments, and more. Follow the QR code to learn more.

Mandiant Managed Defense

Mandiant Managed Defense provides 24/7 threat detection, investigation, and response (TDIR) with access to frontline experts who monitor your security technology to help find and investigate threats, proactively hunt for ongoing or past breaches, and respond before attacks impact your business.

The Managed Defense team works seamlessly with your security team and the AI-infused capabilities of Google Security Operations to quickly and effectively monitor, detect, triage, investigate, and respond to incidents. Follow the QR code to learn more.

Mandiant Situation Room

Mandiant Situation Room provides executive experience and expertise to bring together intelligence, events, and capability to respond, contain, and remediate critical security incidents with speed, scale and efficiency. This means using intelligence to establish resilience in a real-world threat environment.

Effective incident and breach response extends beyond technical investigation, containment and recovery and includes executive communication and crisis management. The criticality of resolving incidents quickly and providing continuity is paramount. Doing this requires taking into account a potential adversary's view of the situation where de-escalation plans are often more important than escalation plans.

Following the major event, an after-action report should detail successes, challenges and recommendations. This phase provides three outcomes for active cyber defense: response, recovery and continuity.

Prepare and protect your election infrastructure with these paid offerings today by visiting https://www.mandiant.com/.

Google