Services commerciaux de Mandiant pour les services de cybersécurité destinés aux entités fédérales, provinciales et municipales canadiennes.

Sous le regard du monde entier: l'approche éprouvée de la sécurité électorale

La défense contre les cybermenaces ciblant les élections nécessite des protections actives qui s'appuient sur le renseignement. Les personnes qui soutiennent les élections exigent des programmes de capacités stratégiques de sécurité et des solutions techniques spécifiques pour renforcer et améliorer leur posture de sécurité avant un événement et pour soutenir les opérations pendant l'élection. Le déploiement de cybercapacités résilientes s'effectuant selon un échéancier serré et sous l'œil attentif du public constitue un défi majeur qui nécessite des efforts de planification et des investissements suffisants pour une mise en œuvre adéquate.

Protection de l'infrastructure électorale de Mandiant

La combinaison unique d'expertise de Mandiant tant au niveau du renseignement sur les menaces que des services et des solutions permet aux organisations d'évoluer continuellement pour se défendre contre les menaces électorales telles que: l'intégrité et la destruction des données, les logiciels de rançon, les menaces internes et les opérations d'information (IO). Faites le premier pas pour sécuriser votre infrastructure en scannant le code QR vers la liste de vérification de sécurité électorale.

Préparez et protégez votre infrastructure électorale dès aujourd'hui grâce à ces offres payantes avec Mandiant.

Le Service Renseignements sur les menaces de Google (Google Threat Intelligence)

offre une visibilité inégalée sur l'évolution des pratiques et des risques de cyberattaques, outillant ainsi les organisations pour se défendre de manière proactive. En tirant parti des informations provenant de la défense de milliards d'utilisateurs et de l'analyse de millions d'attaques d'hameçonnage, Google Threat Intelligence permet aux équipes de sécurité de comprendre les acteurs de la menace et leurs tactiques, techniques et procédures (TTP).

Consultez la page **https://www.mandiant.com/advantage/threat-intelligence** pour en savoir plus.

La Protection contre les risques numériques Google

comprend les produits et services qui protègent les biens numériques critiques contre les menaces externes en offrant une visibilité qui englobe le Web ouvert, profond et sombre. Cela permet aux organisations d'identifier le ciblage malveillant, les vecteurs d'attaque à haut risque et les campagnes d'attaque tout en obtenant des informations sur les acteurs de la menace pertinents et leurs tactiques, techniques et procédures (TTP). Google offre une protection contre les risques numériques grâce à des produits SaaS autogérés ou à des services complets, contribuant à ce que les organisations améliorent de manière proactive leur posture de cybersécurité.

Consultez la page **https://www.mandiant.com/solutions/digital-risk-protection** pour en savoir plus.

Avant L'élection: Préparation, Renforcement et Exercice à Répétition

Le Service de réponse aux cyberincidents

par Mandiant offre un éventail complet de réponses aux cyberincidents, comprenant l'enquête, le confinement et la récupération, soutenu par un service de renseignements sur les menaces à la fine pointe, pour comprendre les tactiques et les motivations des attaquants. Avec une couverture de réponse 24/7 grâce à Mandiant Managed Defense, les organisations bénéficient d'une protection continue et d'une tranquillité d'esprit tout au long du cycle de vie de l'incident.

Mandiant Threat Hunt

combine notre vaste expérience de réponse aux intrusions menées par des acteurs de menace avancés, notre service de renseignements sur les menaces à la fine pointe, afin de dévoiler de manière proactive les menaces avancées manquées par vos outils et contrôles de sécurité existants. Ce service identifie les intrusions en cours ou passées au sein de votre organisation. Il évalue les risques en identifiant les faiblesses et les vulnérabilités de l'architecture de sécurité ainsi que les mauvaises configurations, l'utilisation inappropriée ou les violations de politique dans le système. Et, il évalue si votre organisation a la visibilité nécessaire pour réagir adéquatement. Il augmente ainsi la capacité de votre organisation à répondre efficacement aux incidents futurs.

L’exercice et la répétition d’exercices

contribuent à identifier les opportunités d'amélioration et augmentent la confiance dans vos processus, vos compétences et votre capacité à détecter et répondre aux défis et menaces de cybersécurité qui peuvent avoir un impact sur les expériences de vote des citoyens et leur confiance. Au-delà d’offrir les meilleures compétences et capacités de réponse aux incidents, Mandiant propose l'examen, l'alignement et l'exercice des manuels de réponse (playbook) aux incidents électoraux, y compris les communications de crise cybernétique avec les parties prenantes.

Pendant L'élection: Test, Surveillance et Défense en Continu

Les exercices d'équipe rouge et violette

peuvent tester efficacement vos capacités de sécurité et votre préparation technique pour trouver les failles avant que les cyberattaquants ne le fassent. Testez vos contrôles contre les plus récents scénarios d'attaque, en accord avec les cadres éthiques standard de l'industrie pour l'équipe rouge et à la lumière du renseignement sur les menaces réelles. Les exercices vont des évaluations de l'équipe rouge et des tests de pénétration, aux évaluations de l'équipe violette et des dispositifs intégrés, et plus encore.

Mandiant Managed Defense

fournit une détection, une enquête et une réponse aux menaces 24/7 (TDIR) avec un accès à des spécialistes de première ligne qui surveillent votre technologie de sécurité pour aider à trouver les menaces et faire enquête, à rechercher de manière proactive les violations en cours ou passées et à réagir avant que les attaques n'aient un impact sur votre entreprise. L'équipe Managed Defense travaille main dans la main avec votre équipe de sécurité et les capacités infusées d'IA de Google Security Operations pour surveiller, détecter et trier les incidents ainsi que faire enquête à leur sujet et y réagir rapidement et efficacement.

Mandiant Situation Room

fournit une expérience et une expertise de direction pour rassembler le renseignement, les événements et la capacité nécessaire, afin de réagir aux incidents de sécurité critiques en les contenant et en les corrigeant avec rapidité, proportionnalité et efficacité. Cela signifie utiliser le renseignement pour mettre en place la résilience dans un environnement de menace réel. Une réaction efficace aux incidents et aux violations s'étend au-delà de l'enquête technique, du confinement et de la récupération pour inclure la communication de direction et la gestion de crise. Il est primordial de résoudre rapidement les incidents et d'assurer la continuité. Pour ce faire, il faut tenir compte de la vision de la situation d'un adversaire potentiel où les plans de désescalade sont souvent plus importants que les plans d'escalade.

Après l'événement majeur, un rapport d'après-action doit déterminer les réussites, les défis et les recommandations, et ce, pour chacun des trois axes clés d’une cyberdéfense active : réaction, récupération et continuité.

Préparez et protégez votre infrastructure électorale dès aujourd'hui grâce à ces offres payantes avec Mandiant.

Google