DELL Technologies

Êtes-vous prêt à faire face à un cyberincident perturbateur ?

Les risques et les coûts associés aux cyberattaques continuent d'augmenter, les attaques par rançongiciel ayant le plus d'impact sur les opérations de la société. L'incapacité à réaliser des opérations métiers pendant une période prolongée (plusieurs semaines, voire plusieurs mois) peut être catastrophique pour la réussite à long terme de l'organisation.

La récupération est essentielle et l'effort pour revenir à un fonctionnement normal est extrêmement éprouvant. Restaurer des serveurs et d'énormes quantités de données et d'applications, mettre en ligne les applications les plus stratégiques dès que possible et atteindre les objectifs de temps de reprise (RTO) nécessitent des efforts considérables.

72 %

des sociétés rapportent avoir besoin d'une aide extérieure pour s'assurer qu'elles couvrent toutes les exigences liées à la sécurité et aux risques IT.[5]

Fournir une aide stratégique pour vous permettre de reprendre vos activités

Services de récupération et de réponse aux incidents

Notre équipe d'experts en cybersécurité certifiés travaille avec vous à chaque étape du processus. Avec l'envergure du réseau mondial de Dell Technologies, nous pouvons réagir rapidement pour éliminer la menace et restaurer les opérations métiers rapidement et avec le moins d'interruptions possible.

Les cybermenaces continuent de croître et leurs effets peuvent être catastrophiques

Toutes les 11 secondes une attaque de cyberattaque ou une attaque par rançongiciel aboutit[1]

16 jours d'interruption de service en moyenne après une attaque par rançongiciel[2]

75 % des organisations seront confrontées à une ou plusieurs attaques d'ici 2025[3]

Plus de 60 % des sociétés ont déjà fait l'expérience d'une mise en danger des données en raison d'une faille de sécurité exploitée[4]

Services de récupération et de réponse aux incidents

Chez Dell Technologies Services, nous disposons d'une expérience éprouvée en matière de restauration pour les clients ayant subi un cyberévénement

Un incident s'est produit. Quelle est la prochaine étape pour vous ?

Les opérations sont affectées et vous pouvez rencontrer les problèmes suivants :

- La messagerie électronique est en panne
- Les données sont inaccessibles
- Logiciels malveillants
- Le réseau est en panne
- Active Directory est en panne
- Les transactions ne peuvent pas être traitées
- Une rançon a été demandée

Obtenir de l'aide

Obtenir de l'aide

Notre équipe d'experts est prête à intervenir immédiatement. Il vous suffit de nous contacter à l'adresse suivante :

Incident.Recovery@dell.com

Récupération

Équipe de récupération et de réponse aux incidents (IRR)

Des experts à vos côtés à chaque étape

Faites confiance aux experts

Notre équipe dédiée d'experts en cybersécurité certifiés apporte une vaste expertise et des pratiques d'excellence pour un large éventail de talents et de domaines

Obtenez l'aide dont vous avez besoin, quelle que soit la situation

Nos services répondent à vos besoins, quelle que soit la situation que vous rencontrez ou ce qui a été affecté. D'abord, nous évaluons votre situation, puis nous engageons seulement les ressources appropriées pour vous aider à effectuer rapidement une restauration.

Ce que nous faisons

Qu'une attaque vienne de se produire ou que vous ayez déjà travaillé sur la récupération et ayez besoin d'aide pour agir plus rapidement, nos experts sont là pour :

- Évaluer quelles sont les ressources appropriées et les déployer
- Éradiquer les menaces et limiter les risques de sécurité
- Restaurer les applications métiers pour qu'elles fonctionnent de la même manière qu'avant l'incident
- Redéployer des stations de travail pour permettre aux collaborateurs de reprendre leur travail
- Fournir des services d'analyse approfondie des données proposée par des experts
- Aider à améliorer la sécurité

Obtenir de l'aide

- Fournir de l'aide par téléphone en quelques minutes/heures ainsi qu'une équipe sur site généralement en moins de 48 heures
- Faire évoluer plus de 100 ressources avec plusieurs flux de travail dans différents emplacements et langues, avec la possibilité de les adapter en fonction des besoins
- Mettre à disposition des experts en cybersécurité certifiés, avec plus de 10 ans d'expérience pour la plupart
- Fournir une expertise sur l'infrastructure et les points de terminaison Dell et non Dell
- Apporter des connaissances et de l'expérience sur la périphérie, le Cloud, l'aspect juridique, les assurances et bien plus encore.
- Portée mondiale sur plus de 170 marchés
- Exploiter des solutions de financement innovantes qui vous permettent d'aligner et d'adapter le coût des solutions IT sur la consommation technologique et le budget disponible**.

Récupération

- Éradiquer la menace
- Accélérer le retour à votre fonctionnement normal
- Augmenter le personnel IT existant en raison de l'augmentation des charges applicatives
- Reconstruire un environnement réseau renforcé
- Améliorer la posture de sécurité en développant et en mettant en œuvre une stratégie de sécurité pour éviter les cyberattaques répétées
- Former et partager les pratiques d'excellence

Pour plus d'informations, consultez **Delltechnologies.com/incident-response-and-recovery**

** Payment solutions provided to qualified commercial customers by Dell Financial Services (DFS) or through Dell Technologies group companies and/or through Dell's authorized business partners (together with DFS «Dell»). Offers may not be available or may vary by country. Offers may be changed without notice and are subject to product availability, eligibility, credit approval and execution of documentation provided by and acceptable to Dell or Dell's authorized business partners. In Spain, services are provided by Dell Bank International d.a.c branch in Spain and in remainder of the EU by Dell Bank International d.a.c, trading as Dell Financial Services which is regulated by the Central Bank of Ireland. Dell Technologies, DellEMC and Dell logos are trademarks of Dell Inc.

[1] Estimation pour 2021, Cybersecurity Ventures : https://cybersecurityventures.com
[2] Why Ransomware Costs Businesses Much More than Money, Forbes, 30 avril 2021, https://www.forbes.com/sites/forbestechcouncil/2021/04/30/why-ransomware-costs-businesses-much-more-than-money/?sh=469c541a71c6
[3] Detect, Protect, Recover: How Modern Backup Applications can protect you from ransomware, Nik Simpson, Gartner, 6 janvier 2021, https://www.gartner.com/doc/reprints?id=1-258HHK51&ct=210217&st=sb
[4] Document Forrester Consulting Thought Leadership réalisé à la demande de Dell, BIOS Security – The Next Frontier for Endpoint Protection, juin 2019
[5] Étude réalisée par Forrester Consulting à la demande de Dell Technologies, décembre 2020