2023 IT Priorities : Infographie Cybersécurité

Découvrez dans cette nouvelle infographie issue de l'étude priorités IT 2023, les plans d'investissement courants en cybersécurité pour 2023, axés sur la gestion des identités, la sécurité des données liée au cloud, la sécurité des applications et la gestion des vulnérabilités DevSecOps et CSPM. Des tactiques sont présentées pour améliorer la position en matière de cybersécurité en 2023, selon les besoins de chaque entreprise.

Top des plans d'investissement dans la cybersécurité

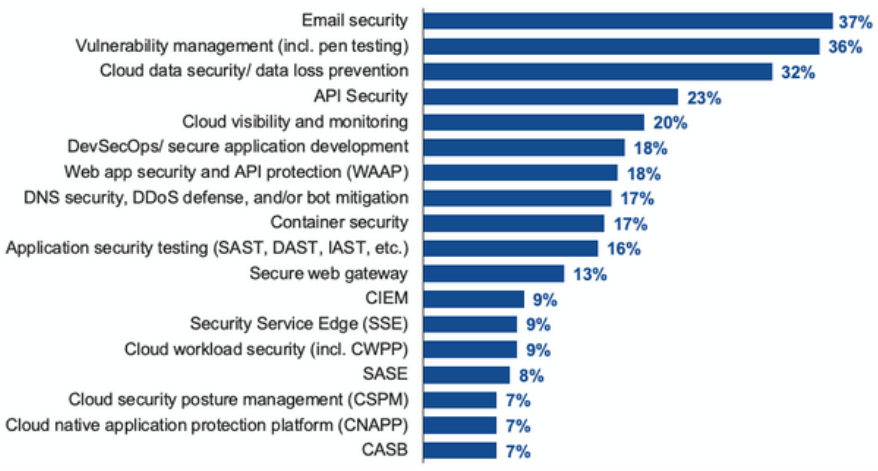
1	Expand training efforts for corporate employees	7	Email security
2	Improve security visibility/observability/monitoring	8	Vulnerability management (incl. pen testing)
3	Improve cyber risk assessment, quantification& visibility	8	Improve collaboration and communication across business units/cross-functional teams
4	Expand training efforts for corporate employees (security awareness training)	10	Reduce risk exposure from third parties (vendors/supply chain/M&A)
5	Multifactor authentication	10	Further our zero-trust strategy/vision
6	Improve our speed and ability to restore assets and systems affected by cyber-attacks	10	Single sign-on (SSO)

Observations

- Les technologies de gestion des identités et des accès sont à la tête des plans d'investissement en cybersécurité - les organisations réalisent que l'identité est un élément fondamental de leur architecture de cybersécurité, depuis les applications jusqu'au travail à distance.
- La sécurité des données fait son retour - mais elle est liée au cloud ou aux technologies liées au cloud.

Plans d'investissement dans la cybersécurité, le cloud et/ou les applications

Parmi ces initiatives liées à la sécurité du cloud et/ou des applications, lesquelles votre entreprise prévoit-elle de déployer au cours des 12 prochains mois (choisissez toutes les réponses qui s'appliquent) ?



Observations

- Parmi ceux qui sont impliqués dans les technologies de sécurité des clouds et/ou des applications, 87% prévoient des investissements.
- Les entreprises s'intéressent à la sécurité des données, qu'elle soit autonome ou qu'elle fasse partie d'une autre plateforme technologique.
- La sécurité des applications, y compris le développement d'applications sécurisées, continue d'être une priorité absolue cette année
- En croissance cette année par rapport à 2022
- Gestion des vulnérabilités
- DevSecOps
- CSPM

Activités et tactiques de cybersécurité prévues pour 2023 pour soutenir la technologie, le personnel, la culture et les processus

Parmi les activités/tactiques suivantes, lesquelles prévoyez-vous de mettre en œuvre pour améliorer la position de votre entreprise en matière de cybersécurité en 2023 ? (Choisissez toutes les réponses qui s'appliquent)

Technology-related	People-related	Culture-related	Process-related
1. Adopt more advanced cybersecurity tools to support our increased cloud usage	1. Expand training efforts for corporate employees (security awareness training)	1. Improve cyber risk assessment, quantification & visibility	1. Improve security visibility/observability
2. Prioritize cloud-based deployment for our security solutions	2. Leverage managed services to combat staffing/skills shortage (Incl. SOC, ethical hackers, MDR)	2. Expand training efforts for corporate employees (security awareness training)	2. Improve our speed and ability to restore assets and systems affected by cyber-attacks
3. Move towards solutions with greater integration capabilities (vendor agnostic)	3. Increase/ devote more budget for training security staff	3. Improve collaboration and communications across business units/ cross-functional teams	3. Reduce rick exposure from third parties (vendors/supply chain/M&A)

L'enquête sur les priorités informatiques 2023 a été menée en ligne de novembre 2022 à février 2023 afin de recueillir des informations sur le marché concernant les projets technologiques pour 2023 et les perspectives de dépenses technologiques pour les 12 mois à venir.