Objectifs pdagogiques

On les nomme technologies au collge, sciences industrielles ou sciences de lingnieur au lyce et dans le suprieur. Derrire ces diffrentes appellations se cachent les mmes disciplines, utilises pour comprendre les ralisations techniques qui nous entourent et imaginer celles de demain. Il me semblait donc important d'apporter au lecteur un peu d'information autour des lments pdagogiques de corient vers les sciences et techniques de l'ingnieur cyberscurit. Vous trouverez donc dans ce chapitre quelques lments sur les comptences, les mtiers, le positionnement des activits de la cyberscurit pour protger et dfendre l'entreprise. En effet, ctente d'tre une introduction la permettant des acteurs du digital n'ayant pas ou peu de connaissances du domaine de se reprer dans ces activits large spectre de mtiers et de comptences.

Nous y abordons aussi les limites de cainsi que des recommandations pour profiter du contenu avec plus de facilit pour ceux, en particulier moins familiers du monde de l'informatique et des rseaux.

Je vous engage explorer le https://www.ssi.gouv.fr/entreprise/glossaireglossaire de l'ANSSI qui vous permettra de vous familiariser avec les terminologies de la cyberscurit.

Les comptences acqurir A l'issue de c, vous devriez tre en mesure de comprendre les mcanismes qui contribuent la mise en place d'une organisation de cyberdfense d'entreprise avec les grandes capacits ncessaires. Pour les raliser avec pleine conscience et efficacit, il est ncessaire de positionner ces activits au sein des autres fonctions digitales d'entreprise.

¡all¿ComptencesAcquisition

Les comptences acquises sont de diverses natures, mais globalement vous devriez tre en mesure un niveau de gouvernance et de pilotage :

itemize

- d 'analyser les risques numriques pesant sur l'entreprise ou l'organisation;
- d e mesurer le niveau de scurit de l'environnement;
- d 'auditer, conseiller, accompagner le changement;
- d e mettre en place une gouvernance efficace dans le domaine de la cyberscurit;
- d e dployer une politique de scurit informatique et de cyberscurit et appliquer des mthodologies efficaces de renforcement et d'aguerrissement;
- d e comprendre l'intgration des solutions de scurit suite l'analyse de risque;
- d e grer des situations d'incident pouvant aller la crise cyber.