Pour tre prt faire face aux cyber-incidents invitables, il ne suffit pas de se prparer simplement ragir pour neutraliser une attaque isole. Cela ncessite la capacit dintervenir efficacement et de manire rptitive pour planifier pro-activement, dfendre nergiquement vos systmes et vos actifs informationnels vitaux, devancer lvolution des menaces, et assurer une reprise complte des activits aprs les attaques. Dans un contexte o les cyber-attaques grvent de plus en plus les rsultats financiers et ternissent la rputation des grandes socits, la mise sur pied dune solide capacit dintervention en cas de cyber-incident (ICC) devient imprieuse pour les entreprises qui tiennent sauvegarder leur scurit, leur vigilance et leur rsilience. Une solide capacit dintervention en cas de cyberincident peut aider votre entreprise faire ce qui suit : Comprendre rapidement la nature dune attaque pour mieux faire face aux questions quoi, o, comment et combien, et y rpondre Rduire le plus possible les cots en temps, en ressources et en perte de confiance des clients associs la perte de donnes Instaurer un niveau accru de gestion et de contrle pour renforcer les TI et les processus oprationnels et, ainsi, pouvoir vous concentrer sur vos activits de base gnratrices de valeur

Orchestration

CyberDefenseMatrix dutta2019cyber

Cyberrange

les grandes fragilits des infrastructures

La rsilience est dpendante de composantes itemize

S ur l'identit : Les annuaires : (AD ...)

S ur l'infrastructure de routage (DNS, AS ..)