

CAPACITÉ DE MISE EN PLACE DE SOC • NATIONAL ET DÉFENSE

La plupart des SOC nationaux échouent en silence, bien avant qu'un véritable incident ne les mette à l'épreuve.

Un centre opérationnel de sécurité (SOC) national ou de défense se construit généralement de la même façon : on acquiert un SIEM, on recrute une poignée d'analystes, on coupe le ruban. Dix-huit mois plus tard, un événement survient à 2 heures du matin un samedi, et la personne de garde n'a pas l'autorité nécessaire pour l'escalader à celle qui l'a.



La véritable exposition

La convention de Malabo de l'Union africaine, ainsi que les stratégies nationales de cybersécurité élaborées depuis, ont poussé les gouvernements et les forces de défense du continent à mettre en place leur propre capacité de surveillance et de réponse aux incidents. Signer la politique est la partie facile. Faire fonctionner un SOC qui détecte réellement quelque chose à 3 heures du matin, avec un analyste qui sait exactement qui appeler, est la partie que la plupart des programmes de construction sous-estiment.

01

Un SOC, ce n'est ni la salle, ni les écrans, ——— ni la licence.

C'est un analyste reposé, une procédure testée, et une réponse claire à la question de savoir qui l'on appelle à 3 heures du matin. La plupart des programmes de construction réussissent la première partie et ne finissent jamais tout à fait la troisième.

4–5

Un poste de SOC véritablement disponible 24 heures sur 24 et 7 jours sur 7, un seul siège à couvrir en permanence, nécessite généralement **quatre à cinq analystes en rotation**, une fois pris en compte les congés, la formation et le turnover. C'est une règle empirique bien établie dans la planification des effectifs en sécurité, et elle est régulièrement absente des budgets construits autour du matériel et des licences logicielles plutôt qu'autour des personnes.

02

Les quatre phases par lesquelles nous faisons passer chaque projet de construction de SOC, dans l'ordre.

01

CONCEVOIR

02

CONSTRUIRE

03

EXPLOITER

04

MATURER

Pourquoi c'est important au salon AAD

Les forces de défense, les ports, les opérateurs de services publics et autres exploitants d'infrastructures nationales subissent une pression croissante, souvent soutenue par des financements publics ou de bailleurs, pour mettre en place leur propre capacité de surveillance et de réponse plutôt que de l'externaliser entièrement.

Nous aidons les organisations à construire correctement cette capacité dès la première fois, car un SOC qui échoue en silence est pire que l'absence de SOC : il crée une apparence de couverture sans en avoir la substance.

03

Ce que nous faisons

Nous concevons et construisons des capacités de surveillance et de réponse pour les acteurs de la défense, des administrations publiques et des infrastructures critiques, en traitant les personnes et les processus avec autant d'attention que la technologie.



Conception et construction du SOC installations, architecture de surveillance et outillage choisis en fonction de votre paysage de menaces réel et de votre budget, et non de la pile logicielle par défaut d'un fournisseur.



Cas d'usage de détection, procédures et chaînes d'escalade calqués sur votre structure de commandement, testés avant la mise en service plutôt que découverts lors du premier incident réel.



Modèles d'effectifs et conception des rotations, y compris la hiérarchisation des analystes et une véritable planification 24 heures sur 24, 7 jours sur 7, construite autour de la réalité des congés, de la formation et du turnover, et non d'un organigramme sur une diapositive.



Assurance qualité indépendante et mesure de la performance du SOC, de sorte que l'équipe qui évalue la performance du SOC ne soit pas celle qui l'a construit.

CAPACITÉ DE MISE EN PLACE DE SOC • NATIONAL ET DÉFENSE

Un centre opérationnel de sécurité n'est pas une salle pleine d'écrans. C'est un analyste reposé, une procédure testée, et une réponse claire à la question de savoir qui l'on appelle à 3 heures du matin.

DISystems – Conseil en cybersécurité et GRC en Afrique du Sud, dans la région de la SADC et à l'international, en partenariat avec **Cyberantix™**

CONTACTEZ-NOUS À L'ADRESSE :

tsepang@disystems.co.za

pour convenir d'un rendez-vous et en savoir plus.

