Pratiques exemplaires sur la mise en place d'un centre des opérations de sécurité (COS)

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Mai 2023 | ITSAP.00.500

Un centre des opérations de sécurité (COS) combine des personnes, des processus et des technologies en vue d'améliorer la résilience de votre organisation contre les cybermenaces. Un COS est géré à partir d'un emplacement central par une équipe de spécialistes de la sécurité de l'information, y compris des ingénieures et ingénieurs en sécurité qui peuvent travailler en étroite collaboration avec votre équipe de développement, des analystes de sécurité et des analystes en menaces informatiques. Tandis que les cybermenaces deviennent plus complexes et que les acteurs de la menace deviennent plus sophistiqués, de nombreux COS sont mis en place au niveau régional comme première ligne de défense contre les cyberattaques, en particulier dans le secteur des soins de santé et dans le milieu universitaire. Parmi les autres raisons pour lesquelles les COS sont de plus en plus communs, citons l'augmentation du nombre de systèmes de contrôle industriels (SCI) et de technologies opérationnelles (TO), ainsi que l'adoption de technologies mobiles et infonuagiques. Ce document fourni des conseils aux organisations de toutes tailles sur les pratiques exemplaires à adopter lors de la mise sur pied et de l'exploitation d'un COS. De plus, le présent document propose des conseils aux organisations souhaitant s'abonner à un COS en tant que service (COSS) auprès d'un fournisseur de tierce partie.

En quoi consistent les activités d'un COS?

Un COS est principalement responsable de la détection des cyberincidents et des cybermenaces et de l'intervention nécessaire. Les COS peuvent aussi effectuer des évaluations des vulnérabilités, des tests de pénétration, des analyses des menaces et des audits de conformité aux règles. Les COS effectuent les activités suivantes:

Surveillance

Recueillir en continu des données sur la sécurité et les événements en temps réel à partir de l'ensemble de l'infrastructure des TI de votre organisation. Cela comprend des données des appareils sur place, du nuage, des SCI et TO, des systèmes à distance et des appareils mobiles.

Détecter

Définir les tendances anormales, les écarts ou autres indicateurs de compromission (IC) dans les volumes de données recueillies. Les menaces potentielles sont classées par gravité et évaluées pour déterminer s'il s'agit de menaces réelles dont votre organisation devrait se préoccuper. Des outils automatisés de détection peuvent aussi servir à isoler les menaces réelles.

Intervenir

Prendre des mesures immédiates pour résoudre les incidents et mettre en œuvre des mesures d'atténuation appropriées contre les menaces. Après un incident, un COS s'occupera de remettre à leur état de base votre réseau et vos systèmes et de récupérer toute donnée perdue ou compromise.

Analyse

Mener une enquête sur la source de l'incident à l'aide des données du journal et d'autres informations afin d'aider à éviter que des incidents semblables se reproduisent à l'avenir.

COS en tant que service (COSS)

Si votre organisation dispose de ressources limitées, il peut être difficile de mettre sur pied et d'exploiter un COS. Dans ce cas, votre organisation devrait considérer un COS en tant que service (COSS) comme solution de rechange. Une option consiste à adopter une approche hybride en matière de sécurité. Dans cette approche, des activités du COS comme la surveillance et l'intervention en cas d'incident peuvent être effectuées à l'interne, mais des activités plus spécialisées, comme des tests de pénétration ou des analyses de maliciels, peuvent être effectuées à l'externe. Tenez compte des éléments suivants avant de choisir un fournisseur de COSS:

- Quels services de COS sont offerts?
- Peut-on accroître ou réduire l'ampleur des équipes et des services pour les adapter aux besoins organisationnels ou en réponse à des événements précis?
- Quels outils et technologies sont utilisés pour recueillir les données?
- Les services peuvent-ils être adaptés à l'environnement et à l'industrie de votre organisation?
- Comment les données seront-elles saisies?
- Comment les données seront-elles utilisées?
- Où les données sont-elles stockées?
- Comment protège-t-on les données sensibles?
- Qu'est-ce qui est inclus dans l'accord sur les niveaux de service (ANS)?
- Comment mesure-t-on ou évalue-t-on l'ANS?
- À quelles normes et pratiques de sécurité se conforme-t-on pour s'assurer d'atténuer les vulnérabilités de la chaîne d'approvisionnement?

Quels sont les avantages d'un COS?

L'un des principaux avantages d'un COS est qu'il combine les efforts pour soutenir l'intervention en cas d'incident, y compris l'identification, le confinement, l'éradication des menaces, la reprise des activités et la production de rapports. Ces efforts combinés aideront votre organisation à améliorer sa posture de cybersécurité, qu'il s'agisse d'une grande entreprise ou d'une infrastructure essentielle. Voici d'autres avantages liés aux COS:

- **Chasse aux cybermenaces proactive.** En combinant les données antérieures et le renseignement sur les menaces, les COS peuvent aider à déceler des preuves précoces d'attaques qui, autrement, auraient pu passer inaperçues. Les COS peuvent utiliser la technologie d'intelligence artificielle (IA) pour rechercher des modèles dans les données recueillies et signaler le trafic suspect à des fins de suivi. À l'aide de divers outils, les COS peuvent établir une base de référence du trafic habituel de votre organisation, afin de faciliter la recherche d'activités malveillantes.
- **Détection des incidents et interventions plus efficaces**. En fonction de la taille du COS et du niveau d'expertise, on peut y détecter rapidement les signes d'une attaque, mener une enquête initiale et commencer à remédier à la menace. Cette réponse accrue peut limiter l'étendue des dommages causés à votre organisation et aider à empêcher les pirates d'accéder à vos précieux actifs et à vos informations sensibles.
- **Réduire les dépenses.** Les COS peuvent optimiser votre environnement de TI et réduire le nombre d'outils et d'appareils nécessaires pour protéger adéquatement votre environnement, réduisant ainsi votre budget lié aux TI.
- **Visibilité accrue de la sécurité et gestion centralisée des incidents**. En utilisant des outils et des tableaux de bord pour fournir une connaissance de la situation en temps réel de la posture de sécurité de votre organisation, les COS vous aideront à mieux coordonner les ressources nécessaires pour corriger et contenir les menaces.
- **Audit régulier des systèmes**. En veillant à ce que les réglementations de l'industrie et du gouvernement soient respectées, les COS peuvent aider à protéger votre organisation contre les atteintes à la réputation, les violations administratives ou matérielles de la vie privée et la responsabilité légale en cas de violation.

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

Pratiques exemplaires sur la mise en place d'un centre des opérations de sécurité (COS)

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Mai 2023 | ITSAP.00.500

Éléments à considérer lors de la mise sur pied de votre COS

Les cyberattaques sont de plus en plus fréquentes et complexes et il vaut mieux se préparer à toute éventualité. Voilà quelque chose dont votre organisation doit tenir compte. Un COS peut aider à accroître la résilience de votre organisation contre les cybermenaces et à minimiser l'impact en cas de compromission. Voici des pratiques exemplaires à garder en tête lorsque vous mettez sur pied et exploitez un COS:

1. Élaborez une stratégie pour votre COS dont la portée est appropriée.

- ☐ Identifiez les actifs organisationnels, comme les systèmes et les données, qui sont très précieux ou sensibles et doivent être surveillés et protégés.
- ☐ Effectuez une évaluation des risques de cybersécurité pour comprendre les menaces qui ciblent votre organisation. Il peut aussi être utile de comprendre le niveau de sophistication des autrices et auteurs de menace qui ciblent votre organisation. Les ministères du gouvernement du Canada peuvent consulter une description des agents de menace dans le tableau 5, de l'annexe A de l'ITSG-33. Les organisations qui ne font pas partie du GC peuvent consulter une description des niveaux de compétences des autrices et auteurs de menace dans le document "Structured threat information expression (STIX) v2.1 framework" (en anglais seulement).
- ☐ Efforcez-vous de comprendre les exigences légales, réglementaires et de conformité en vertu desquelles votre organisation opère pour savoir ce que le COS est tenu de faire ou de protéger .

2. Concevoir une solution de COS qui répond aux besoins de votre organisation.

- ☐ Sélectionnez un modèle de COS comparable au profil de menace de votre organisation et réalisable compte tenu de vos ressources. Vos exigences et les menaces auxquelles vous faites face changeront avec le temps, votre modèle doit donc être facilement adaptable pour suivre le rythme.
- ☐ Incorporer une défense axée sur les menaces dans les opérations de sécurité de routine, y compris celles des cadres de menaces tels que MITRE ATT&CK (en anglais seulement)et l'OWASP Top 10.
- ☐ Pour les grandes organisations avec une large couverture géographique, comme les hôpitaux et les écoles, envisagez d'intégrer ou de consolider plusieurs COS pour former un COS régional. Cela permet aux COS de partager des informations, d'investir conjointement dans des outils et du personnel expert, et d'accroître la connaissance de la situation pour les organisations participantes.

3. Mettre en œuvre et exploiter efficacement la solution.

- ☐ Recueillez des données importantes à partir de capteurs et de journaux générés à partir d'applications, de systèmes d'exploitation, du réseau, du nuage et des SCI/TO.
- ☐ Utilisez des technologies automatisées dans le cadre de votre stratégie d'intervention en cas d'incident.
- ☐ Sélectionnez une solution de gestion des événements qui inclut la collecte et le traitement des journaux, le stockage, les requêtes, les alertes et la gestion des incidents. Un certain nombre de plateformes commerciales et de source ouverte de gestion des informations et des événements de sécurité (GIES) sont disponibles pour aider votre organisation à tirer parti des volumes de données d'événements recueillis jour après jour. Tenez compte des exigences de configuration, de support et de licence en cours lors du choix de la plateforme de GIES appropriée.
- ☐ Établissez un plan clair d'intervention en cas d'incident et testez-le régulièrement pour vous assurer que les fonctions critiques peuvent être restaurées et récupérées en temps opportun. Simulez l'intervention dans une zone de test isolée afin que l'environnement de production ne soit pas touché.
- ☐ Assurez-vous que le COS fonctionne conformément aux exigences légales et réglementaires qui l'encadrent. Des contrôles de sécurité appropriés doivent être en place et appliqués, comme la validation des données pour identifier les informations sensibles.
- ☐ Élaborez une documentation claire des processus et des procédures pour permettre aux membres de l'équipe du COS de travailler efficacement.
- ☐ Mettez en place une bonne équipe dans votre COS en embauchant des personnes possédant une vaste gamme de compétences techniques et d'expériences. Créez une stratégie de maintien en poste pour réduire au minimum le roulement du personnel.
- ☐ Offrir une formation continue à l'effectif et aux nouveaux membres du personnel. Cela peut améliorer leur satisfaction au travail et améliorer leurs niveaux de compétence pour suivre le rythme de l'évolution et des technologies émergentes.
- ☐ Investissez dans des ressources appropriées pour prendre soin de la santé mentale de vos employées et employés. Cela peut éviter l'épuisement professionnel, car un COS est un milieu dont le rythme opérationnel est élevé.

4. Tenir à jour et mettre à jour la solution au fil du temps, au besoin.

- ☐ Encouragez une communication et une collaboration régulières entre les membres de l'équipe du COS et les différents intervenantes et intervenants, comme les utilisatrices et utilisateurs, la direction et les propriétaires de systèmes, dans l'ensemble de l'organisation. Cela peut créer un mécanisme de rétroaction précieux pour le COS afin de fournir de meilleurs services à votre clientèle.
- ☐ Recueillez des données pour mesurer le rendement et l'efficacité du COS, ce qui vous permettra d'ajuster ses opérations en conséquence.
- ☐ Améliorez les activités de votre COS en y ajoutant la simulation et l'évaluation des attaques, la cybertromperie et la chasse aux menaces internes afin de garder une longueur d'avance sur les autrices et auteurs de menace dotés de moyens sophistiqués.

Renseignements supplémentaires

- Journalisation et surveillance de la sécurité de réseau (ITSAP.80.085)
- Élaborer un plan d'intervention en cas d'incident (ITSAP.40.003)
- Élaboration d'un plan de reprise informatique personnalisé (ITSAP.40.004)
- Publication du National Cyber Security Centre (NCSC) sur la mise sur pied d'un Centre des opérations de sécurité (COS) (en anglais seulement)
- Onze stratégies du MITRE pour un Centre des opérations de cybersécurité de calibre mondial (en anglais seulement)

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada