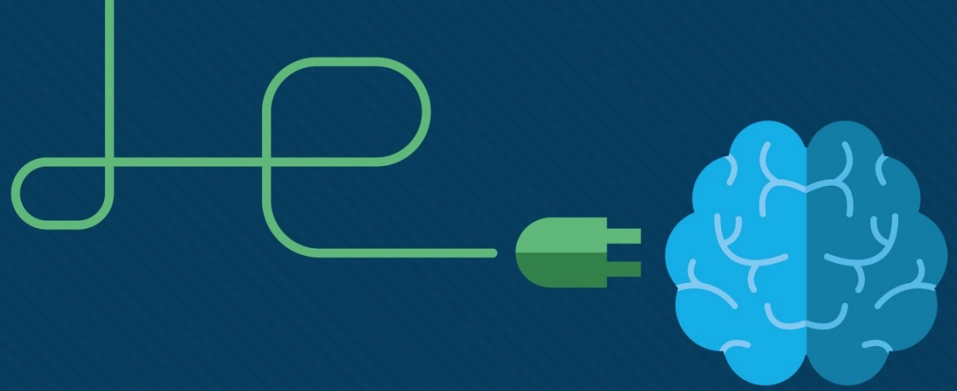


Module 2: Les combattants de la guerre contre la cybercriminalité

CyberOps Associate v1.0

Objectifs du module

Titre du Module: Les combattants de la guerre contre la cybercriminalité

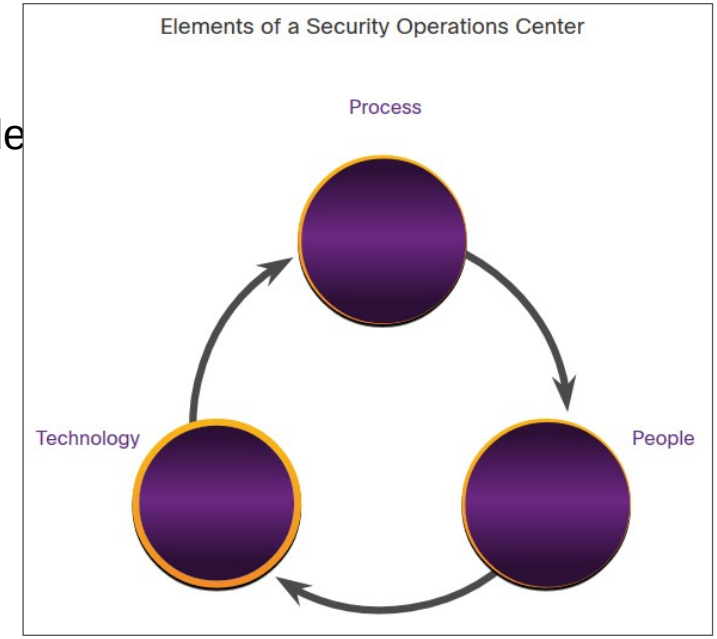
Objectif du Module: Expliquer comment se préparer à une carrière dans les opérations de cybersécurité.

Titre du Rubrique	Objectif du Rubrique
Le centre opérationnel de sécurité moderne	Expliquer la mission du centre opérationnel de sécurité (SOC).
Devenir un acteur de la protection	Décrire les ressources disponibles pour se préparer à une carrière dans les opérations de cybersécurité.

2.1 Le centre opérationnel de sécurité moderne

Composition d'un centre opérationnel de sécurité

- Pour utiliser une approche formalisée, structurée et disciplinée pour se défendre contre les cybermenaces, les organisations utilisent généralement les services de professionnels d'un Éléments d'un centre opérationnel de sécurité (SOC).
- Les centres opérationnels de sécurité fournissent une large gamme de services, depuis la surveillance et la gestion
  jusqu'à des solutions de protection complètes et des systèmes de sécurité hébergés personnalisée.
- Les SOC peuvent être installés entièrement en interne, être détenus et exploités par une entreprise, ou être confiés en partie à des fournisseurs de sécurité, tels que les services de sécurité gérée de Cisco.



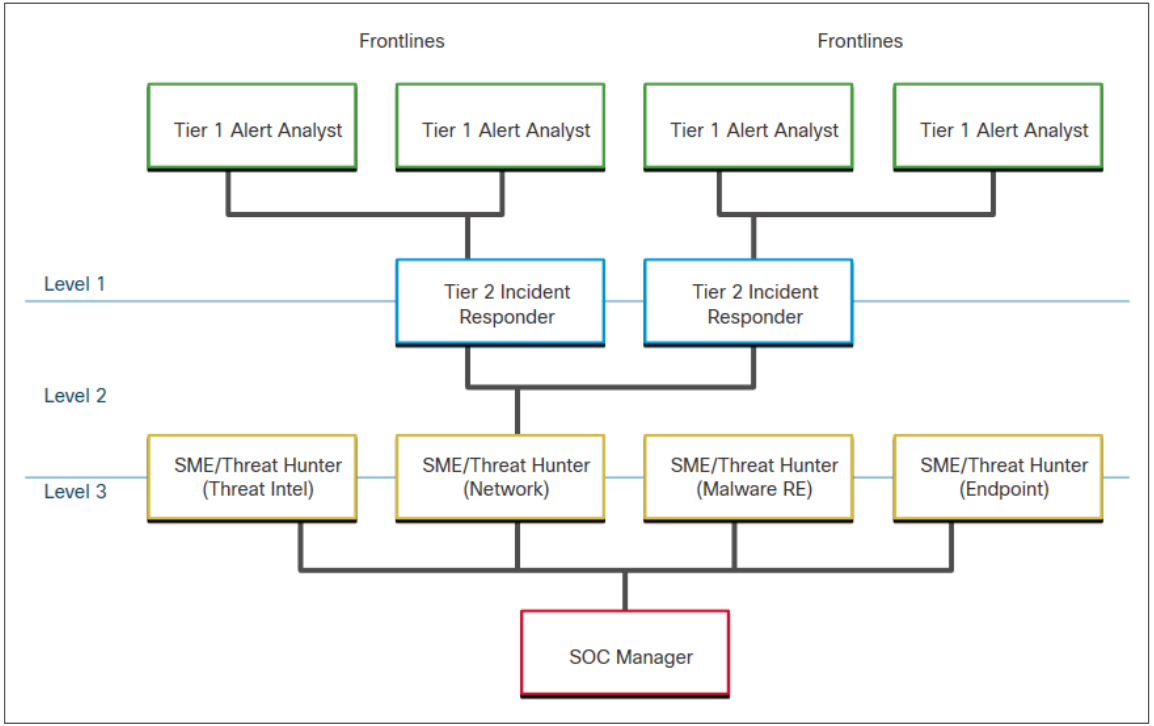
Les gens du SOC

Les SOC attribuent les rôles des postes par niveau, en fonction de l'expertise et des responsabilités requises pour chacun d'eux.

Niveaux	Responsabilités
Analyste des alertes de niveau 1	Surveillent les alertes entrantes, vérifient qu'il s'agit effectivement d'un véritable incident et transmettent des tickets au niveau 2, si nécessaire.
Gestionnaire des incidents de niveau 2	Sont chargés d'examiner en détail les incidents et de recommander des mesures ou des actions correctives à prendre.
Chasseur de menaces de niveau 3	Experts dans les domaines du réseau, du point de terminaison, du renseignement sur les menaces, de l'ingénierie inverse des logiciels malveillants et du suivi des processus du logiciel malveillant afin de déterminer son impact et comment il peut être supprimé. Ils s'impliquent également dans la chasse aux menaces potentielles et dans l'implémentation d'outils de détection des menaces. Les chasseurs de menaces recherchent les cybermenaces présentes dans le réseau mais qui n'ont pas encore été détectées.
Responsable du centre opérationnel de sécurité	Gère toutes les ressources du centre opérationnel de sécurité et sert de point de contact pour les entreprises ou clients les plus importants.

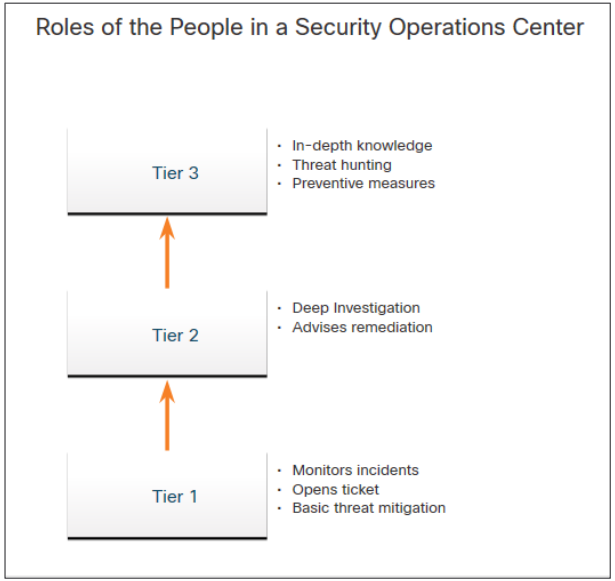
Gens du SOC (Suite)

- Les emplois de premier niveau sont plus de niveau d'entrée, tandis que les emplois de troisième niveau nécessitent une expertise approfondie.
- La figure du l'institut SANS représente graphiquement l'interaction des différents postes.



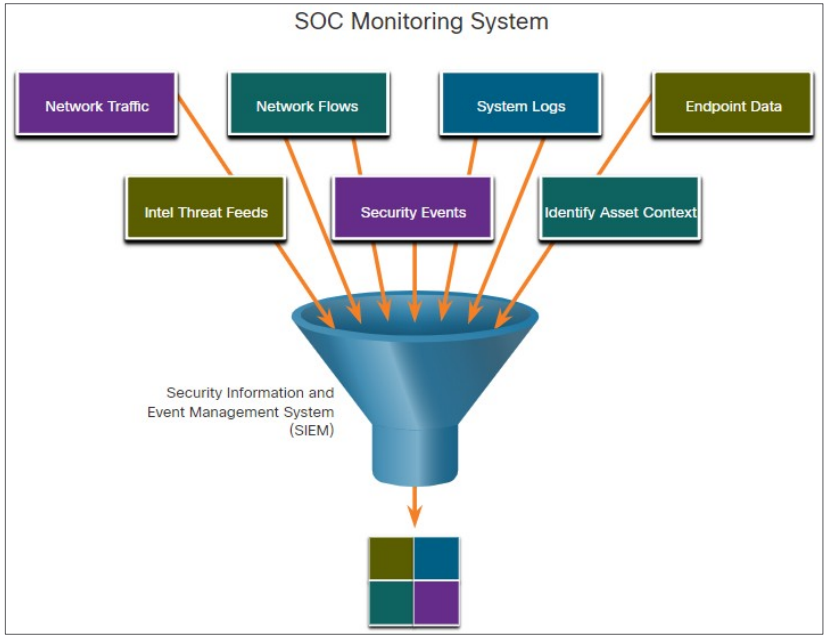
Processus du SOC

- Un analyste de cybersécurité est requis pour surveiller les files d'attente d'alertes de sécurité et enquêter sur les alertes assignées. Un système de billetterie est utilisé pour affecter ces alertes à la file d'attente de l'analyste.
- Le logiciel qui génère des alertes peut déclencher de fausses alarmes. L'analyste doit donc vérifier qu'une alerte correspond réellement à un incident.
- Après la vérification, l'incident peut être transmis aux enquêteurs ou à d'autres équipes de sécurité, ou désigné comme une fausse alerte. Sinon, l'alerte peut être rejetée en tant que fausse alarme.
- Si un ticket ne peut pas être résolu, l'analyste de cybersécurité de niveau 1 le transmettre à un analyste de gestionnaires des incidents de niveau 2 qui l'examinera plus en détail.
- Si l'analyste de gestionnaires des incidents de niveau 2 ne peut pas résoudre le ticket, il le transmettra à un analyste de niveau 3 qui dispose de connaissances plus poussées et de compétences en matière de détection de menaces.



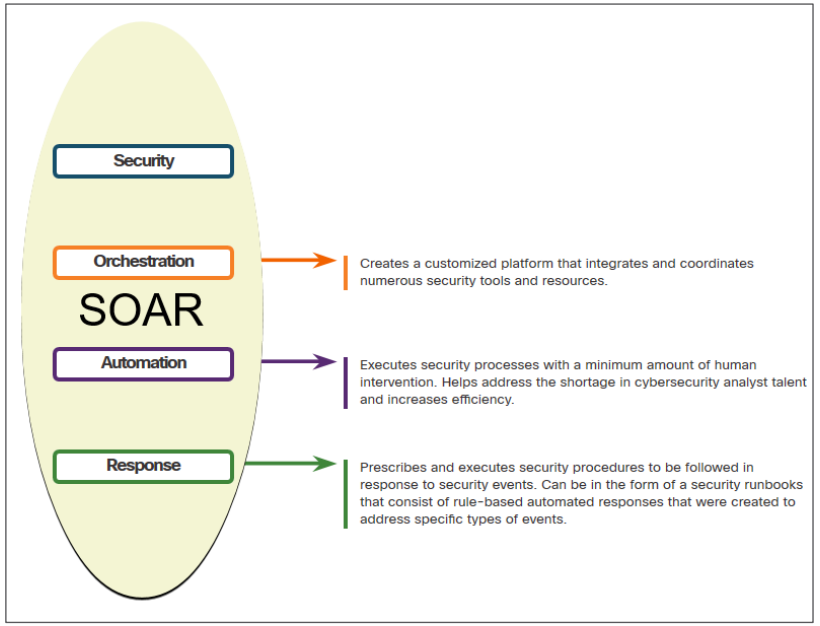
Technologies d'un SOC: SIEM

- Un système de gestion des informations et des événements de sécurité (SIEM) prend en compte toutes les données générées par les pare-feu, les appliances réseau, les systèmes de détection d'intrusion et d'autres périphériques.
- Les systèmes SIEM collectent et filtrent les données, et détectent, classifient, analysent et enquêtent sur les menaces. Ils peuvent également gérer les ressources nécessaires pour mettre en œuvre des mesures préventives et faire face aux menaces futures.



Technologies du SOC: SOAR

- Le SIEM et l'orchestration, l'automatisation et la réponse (SOAR) de la sécurité sont souvent jumelés, car ils disposent de capacités qui se complètent mutuellement.
- Les équipes de grandes opérations de sécurité (SecOps) utilisent les deux technologies pour optimiser leur SOC.
- Les plateformes SOAR sont similaires aux solutions SIEM, car elles regroupent, mettent en corrélation et analysent les alertes. La technologie SOAR intégre des informations sur les menaces en automatisant les flux de travail d'enquête et de réponse sur les incidents basés sur des playbooks développés par l'équipe de sécurité.



Technologies du SOC: SOAR (Suite)

- Plateformes de sécurité SOAR :
  - Recueillir les données d'alarme de chaque composant du système.
  - Fournir des outils qui permettent de faire des recherches, d'évaluer et d'enquêter sur les cas.
  - Mettre l'accent sur l'intégration comme moyen d'automatiser les workflows complexes de réponse aux incidents qui permettent une intervention plus rapide et des stratégies de défense adaptatives.
  - Inclure des playbooks prédéfinis qui permettent une réponse automatique à des menaces spécifiques. Les playbooks peuvent être lancés automatiquement selon des règles prédéfinies ou peuvent être déclenchés par le personnel de sécurité.

Mesures d'un SOC

- Qu'il s'agisse de l'interne d'une organisation ou de la prestation de services à plusieurs organisations, il est important de comprendre dans quelle mesure le COS fonctionne de façon à ce que des améliorations puissent être apportées aux personnes, aux processus et aux technologies qui composent le COS.
- De nombreux indicateurs de performance (KPI) peuvent être conçus pour mesurer différents aspects de la performance des SOC. Toutefois, cinq mesures sont couramment utilisées comme mesures SOC par les gestionnaires SOC.

Indicateurs	Définition
Temps d'immobilisation	Temps moyen pendant laquelle les acteurs de menace ont accès à un réseau avant qu'ils ne soient détectés et que leur accès ne soit arrêté
MTTD (Mean Time to Detect)	Le temps moyen nécessaire au personnel du SOC pour identifier les incidents de sécurité valides s'est produit sur le réseau.
MTTR (Mean Time to Respond)	le temps moyen qu'il faut pour arrêter un incident de sécurité et y remédier
MTTC (Mean Time to Contain)	le temps nécessaire pour empêcher l'incident de causer d'autres dommages aux systèmes ou aux données
Temps de contrôle	Le temps nécessaire pour arrêter la propagation des logiciels malveillants dans le réseau

Sécurité professionnelle et sécurité gérée

- Pour les réseaux moyens et grands, l'organisation bénéficiera de la mise en place d'un SOC au niveau de l'entreprise, qui est une solution interne complète.
- Les grandes entreprises peuvent aussi externaliser au moins une partie du centre pour la confier à un fournisseur de solutions de sécurité.
- Nous proposons une large gamme de fonctionnalités de gestion des incidents, de préparation et d'administration y compris:
    - Service Cisco Smart Net Total Care pour une résolution rapide des problèmes
    - Équipe Cisco chargée de traiter les incidents liés à la sécurité des produits (PSIRT)
    - Équipe Cisco chargée de traiter les incidents liés à la sécurité informatique (CSIRT, Computer Security Incident Response Team)
    - Services infogérés par Cisco
    - Équipe des opérations tactiques Cisco (TacOps)
    - Programme de sécurité physique Cisco

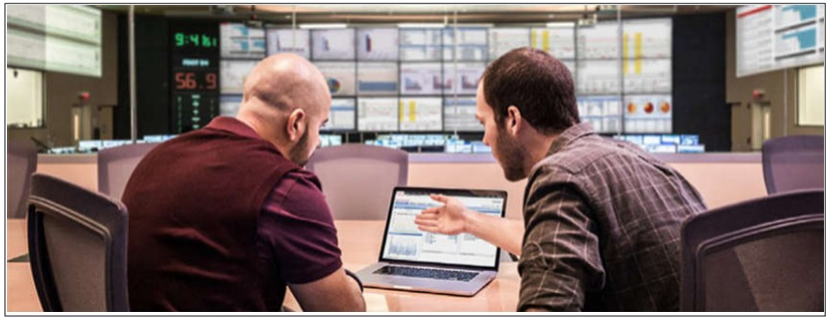
Comparaison entre la sécurité et la disponibilité

- Le personnel de sécurité sait que pour atteindre ses objectifs prioritaires, le réseau d'une entreprise doit être disponible.
- Les entreprises ou les secteurs d'activité en général ne tolèrent que peu les interruptions du réseau. Ce degré de tolérance dépend généralement de la comparaison entre le coût de l'interruption et le coût de la protection contre les interruptions.
- La sécurité ne peut pas être trop forte au point d'interférer avec les besoins des collaborateurs ou avec les activités de l'entreprise. Il convient toujours de trouver un compromis entre sécurité poussée et fonctionnement efficace de l'entreprise.

2.2 Devenir un acteur de la protection

Certifications

- Diverses certifications de cybersécurité importantes pour des postes dans un centre opérationnel de sécurité sont dispensées.
  - Certification Cisco Certified CyberOps Associate
  - CompTIA Cybersecurity Analyst Certification
  - (ISC)² Information Security Certifications
  - GIAC
    (Global Information Assurance Certification)
- Recherchez «certifications de cybersécurité» sur l' internet pour trouver plus d'informations sur les autres fournisseurs et les autres certifications indépendantes.



Formation continue

- **Diplômes**: Pour vous lancer dans une carrière dans la cybersécurité, envisagez de passer un diplôme technique ou un master en informatique, en génie électrique, en technologies de l'information ou en sécurité de l'information.
- **Programmation Python**: La programmation informatique est essentielle pour tous ceux qui souhaitent poursuivre une carrière dans la cybersécurité. Si vous n'avez jamais appris de langage de programmation, Python pourrait être un bon point de départ.
- **Compétences Linux**: Linux est largement utilisé dans les SOC et d'autres environnements de mise en réseau et de sécurité. Les compétences Linux sont un ajout précieux à votre ensemble de compétences alors que vous travaillez pour développer une carrière dans le domaine de la cybersécurité.

Sources d'informations sur les carrières

- De nombreux sites web et applications mobiles diffusent des offres d'emploi dans le domaine informatique. Chaque site est destiné à divers candidats et propose différents outils pour rechercher le poste idéal.
- De nombreux sites sont en réalité des agrégateurs, c'est-à-dire des sites qui centralisent les résultats de recherche d'autres sites et pages d'emploi des entreprises.
    - Indeed.com
    - CareerBuilder.com
    - USAJobs.gov
    - Porte vitre
    - LinkedIn

Acquérir de l'expérience

- **Stages:** Les stages sont parfaits pour démarrer dans le domaine de la cybersécurité. Ils se transforment parfois en postes à durée indéterminée. Cependant, même un stage temporaire vous permet d'acquérir de l'expérience et de découvrir le fonctionnement interne d'une entreprise du secteur de la cybersécurité.

- **Bourses d'études et prix**: Pour aider à combler le manque de compétences en matière de sécurité, des organisations comme Cisco et INFOSEC ont
mis en place des programmes de bourses et de prix.

- **Agences de travail temporaire**: De nombreuses entreprises font appel à des agences de travail temporaire pour embaucher quelqu'un les 90 premiers jours. Si l'employé est un bon candidat, l'organisme peut le convertir en un poste permanent à temps plein.

- **Votre premier emploi:** Si vous n'avez aucune expérience dans le domaine de la cybersécurité, travailler pour un centre d'appel ou un service d'assistance peut être la première étape pour acquérir l'expérience nécessaire pour progresser dans votre carrière.

Travaux pratiques – Devenir un acteur de protection

Lors de ces travaux pratiques, vous découvrirez les conditions requises pour devenir un acteur de la protection.

2.3 Récapitulation des combattants de la guerre contre la cybercriminalité

Récapitulation des combattants de la guerre contre la cybercriminalité

Qu'est-ce que j'ai appris dans ce module?

- Les principaux éléments d'un centre opérationnel de sécurité sont les suivants (SOC) y compris les personnes, les processus et la technologie.
- Ces rôles comprennent un analyste des alertes de niveau 1, un intervenant en cas d'incident de niveau 2, un chasseur de menaces de niveau 3 et un gestionnaire du SOC.
- Au niveau 1, les analystes surveillent et créent des tickets, et prennent des mesures basiques d'élimination des menaces.
- Les systèmes SIEM collectent et filtrent les données, détectent et classent les menaces, analysent et examinent les menaces.
- La technologie SOAR intégre des informations sur les menaces en automatisant les flux de travail d'enquête et de réponse sur les incidents basés sur des playbooks développés par l'équipe de sécurité.
- Les indicateurs clés de performance (KPI) sont conçus pour mesurer les différents aspects des performances du SOC. Les mesures communes comprennent le temps de Dwell, le temps moyen de détection (MTTD), le temps moyen de réponse (MTTR), le temps moyen de confinement (MTTC) et le temps de contrôle.

Récapitulation des combattants de la guerre contre la cybercriminalité

Qu'est-ce que j'ai appris dans ce module? (suite)

- Il doit y avoir un équilibre entre la sécurité et la disponibilité des réseaux. La sécurité ne peut pas être trop forte au point d'interférer avec les collaborateurs ou avec les activités de l'entreprise.
- Diverses certifications de cybersécurité importantes pour des postes dans un centre opérationnel de sécurité sont dispensées dans plusieurs organismes.


CISCO