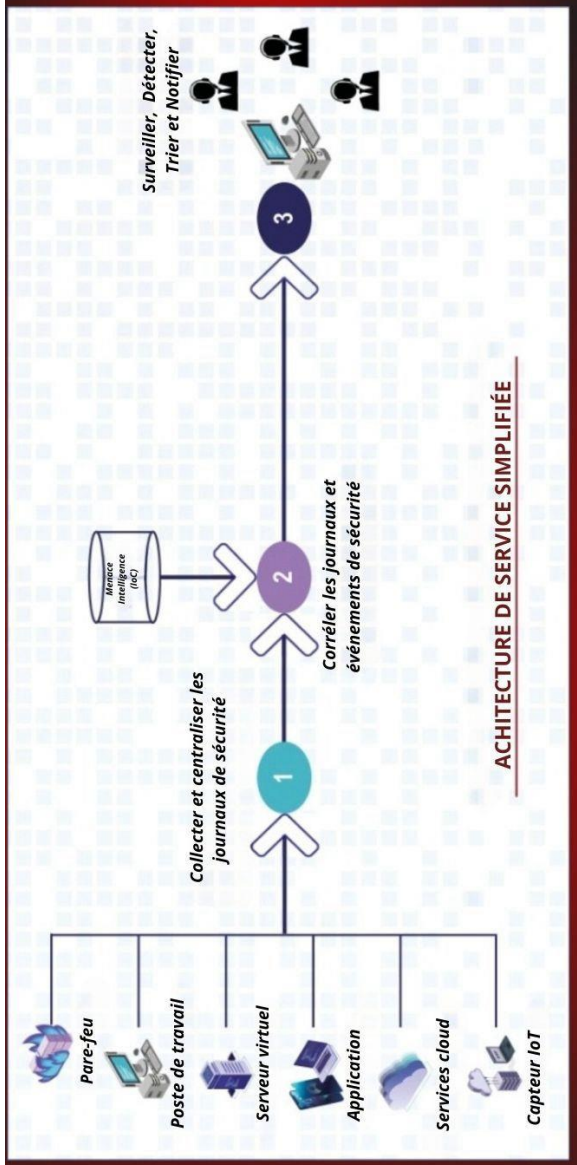
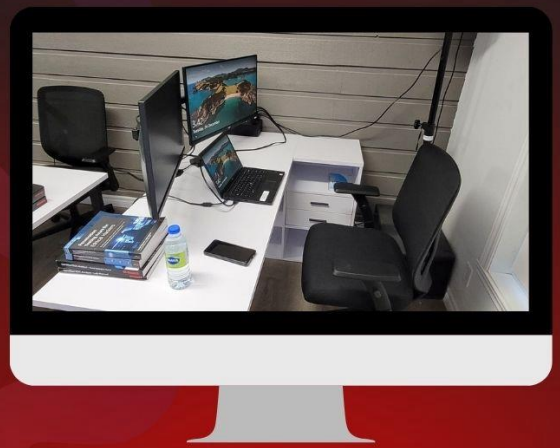
ACHITECTURE DE SERVICE SIMPLIFIÉE





CONTACTEZ-NOUS

Tél: (+1) 418-261-7460

Adresse: 20 Rue St-Nicolas, Québec, QC, GIK 6T2,

Site web: captosec.com

Email: info@captosec.com

captosec

captosec

captosec

CAP2SEC

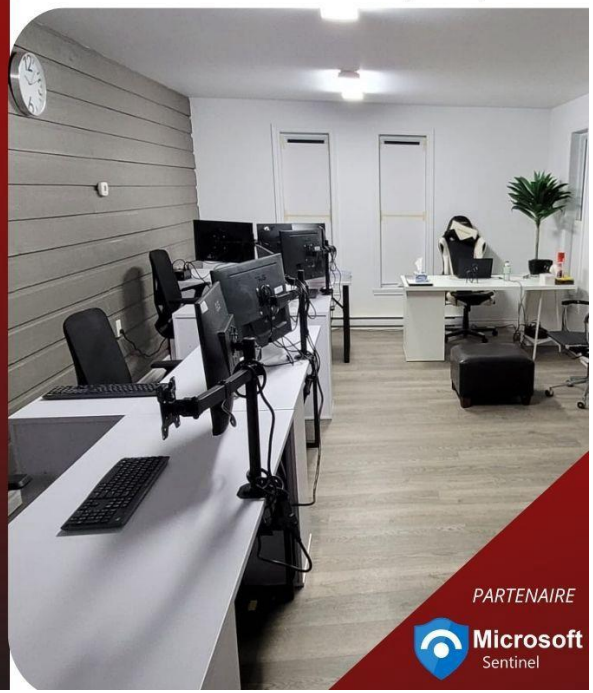
A consulting & InfoSec solutions firm

OFFRE DE SERVICE DE SURVEILLANCE ET DE DÉTECTION DE MENACE ET D'INTRUSION

LA CYBERSÉCURITÉ DE NOS CLIENTS AU CENTRE DE NOS PRÉOCCUPATIONS

Des services de sécurité gérés pour répondre à vos besoins de cybersécurité

Des technologies, outils et processus appropriés pour faire face aux menaces et cyberattaques



PARTENAIRE

Microsoft Sentinel

TECHNOLOGIES

Notre service de surveillance et de détection d'intrusion repose sur des outils Microsoft Sentinel (SIEM, SOAR, UEBA) et SecurityOnion (NIDS). Nous utilisons aussi OSQuery, Sysmon et Syslog pour collecter et envoyer les événements et journaux de sécurité vers nos outils SIEM. Notre SIEM assure la corrélation, l'alertage et la détection des menaces et des intrusions dans vos environnements TI.

PRINCIPAUX OUTILS

NIDS, HIDS, EDR, XDR, SIEM, SOAR et UEBA.
L'intelligence des menaces s'appuie entre autres sur Microsoft Defender Threat Intelligence, OSINT et une base de données personnalisées des IoC avec MISP.
Les agents spécifiques peuvent être déployés sur certains dispositifs comme les postes de travail et serveurs.

RESSOURCES

Nos analystes dotés de compétences variées s'appuient sur des technologies de pointe, des processus et procédures (playbooks) adaptés, ainsi que sur leurs expertises et expériences.
Nous avons des partenaires technologiques et stratégiques reconnus en cybersécurité tels Microsoft et Security Onion.

NOTRE SERVICE DE SURVEILLANCE ET DÉTECTION DE MENACE ET D'INTRUSION

COMMENT EN BÉNÉFICIER ?

1. **Le client contacte Captosec et exprime son besoin de surveillance**
2. **Captosec analyse le besoin et soumet au client une offre sur mesure pour approbation**
3. **Le client approuve l'offre et signe l'entente de service**
4. **Captosec déploie les éléments nécessaires et débute la surveillance**

ÉQUIPES

Nos équipes sont formées adéquatement pour répondre à vos besoins de surveillance et détection de menaces sophistiquées.
La plupart des membres sont certifiés CISSP, SC-200, CSA, Security+, CEH, CHFI, CCSK.

PRINCIPAUX LIVRABLES

- Surveillance et détection proactive 24/7 des menaces et attaques sur vos actifs
- Notification sur les attaques et vulnérabilités (ex. IoC)
- Alertage en temps réel et différé de vos équipes de réponse aux incidents
- Rapport d'analyse d'attaque
- Conseils et recommandations en matière de surveillance et détection des menaces et attaques
- Architecture de surveillance et de détection d'intrusion

BÉNÉFICES

- Anticipation des menaces et attaques sophistiquées
- Respect de la conformité (Ex. PCI-DSS)
- Amélioration de la visibilité de sécurité du réseau et des systèmes
- Collecte des IOC et des preuves pour des besoins d'investigation
- Amélioration du processus de réponse aux incidents

CAP2SEC
A consulting & InfoSec solutions firm