IBM Security

Incidents de sécurité informatique

Analyse et remédiation

Patrice Villemagne - Tech Data France
Market Manager IBM Software (Security, Mobility, CyberSecurity, GDPR, Digital)
Legal Entity Privacy Coordinator Tech Data France (GDPR / DPO / 27001)
Email : patrice.villemagne@techdata.com

Dominique Willot - IBM Security France
Technical leader Data Protection
Membre du Technical Expert Council IBM France, Membre du CLUSIF
Email : dominique_willot@fr.ibm.com

Sécurité Business Club, Paris le 6 Février 2019

Solutions IBM Sofware SIEM (Gestion des vulnérabilité), SIRP (Remédiation) et mise en place d'un SOC managé

SIEM (Security Information and Event Managment)

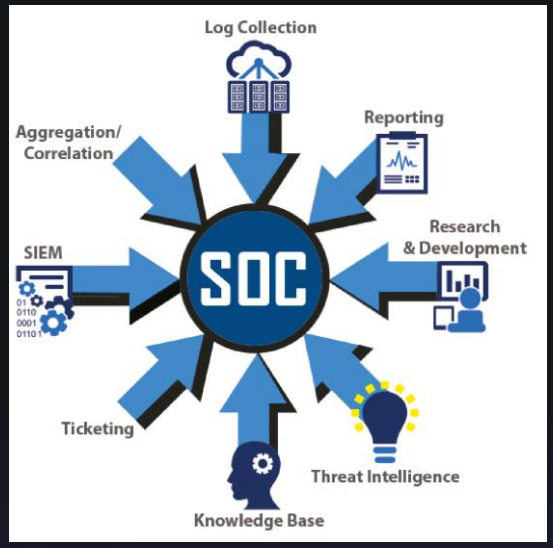
Solution : IBM Qradar

Solution : IBM QRadar SIEM détecte les anomalies, débusque les menaces sophistiquées et filtre les faux positifs. Il consolide les données des événements historisés et des flux réseau issues des milliers de nœuds finaux et applications répartis sur l'ensemble d'un réseau. Il utilise ensuite un moteur d'analyse Sense Analytics sophistiqué pour normaliser et corréler ces données, et identifie les infractions à la sécurité qui nécessitent une enquête. En option, il peut également proposer IBM X-Force® Threat Intelligence, qui génère une liste des adresses IP potentiellement malveillantes (ex. : hôtes de logiciels malveillants, sources de spams et autres menaces). QRadar SIEM peut être installé sur site ou dans le cloud.

SIRP (Security Incidence Response Platform)

Solution : IBM Resilient

Solution : IBM Resilient aide à combattre des menaces complexes avec la plate-forme de réponse aux incidents résilients (IRP). Le dispositif IRP résilient permet à votre équipe de sécurité d'intégrer ses technologies de sécurité et de créer des flux de travail puissants et agiles capables d'automatiser le processus de réponse. En conséquence, vos analystes disposent des outils nécessaires pour enquêter et résoudre les incidents de sécurité, et peuvent continuellement affiner leurs processus.



SOC (Security Operations Center)

Solution : IBM Qradar & IBM Resilient

Solution : Le Security Operating Center est un centre de supervision et d'administration de la sécurité. Le terme SOC désigne ainsi une plateforme dont la fonction est de fournir des services de détection des incidents de sécurité, mais aussi de fournir des services pour y répondre. Le centre de sécurité va ainsi collecter les événements (sous forme de logs notamment) remontés par les composants de sécurité, les analyser, détecter les anomalies et définir des réactions en cas d'émission d'alerte.