ETUDE DE CAS

Détecter les fraudes VoIP

avec ServicePilot

www.servicepilot.com
+33 2 40 60 13 30
info@servicepilot.com

Note: ce document contenant des informations financières relatives au client, ce dernier a demandé à ce que l'étude de cas ne mentionne ni le nom de la société ni celui de ses employés.

CHALLENGE

L'un de nos clients, un important constructeur automobile européen, utilise un système de VoIP SIP et des SBCs Oracle afin de fournir un service téléphonique de qualité à ses 80 000 utilisateurs.

Bien que le protocole SIP soit utilisé par de nombreuses grandes entreprises, et considéré aujourd'hui comme l'un des protocoles de signalisation VoIP les plus répandus, il présente des faiblesses de sécurité qui laissent ses utilisateurs à la merci des hackers.

Avant d'utiliser ServicePilot, notre client avait déjà été victime de plusieurs attaques qui avaient entraîné d'importantes pertes financières (facture de téléphonie anormalement élevées et coûts indirects liés à l'interruption du service VoIP).

SOLUTION

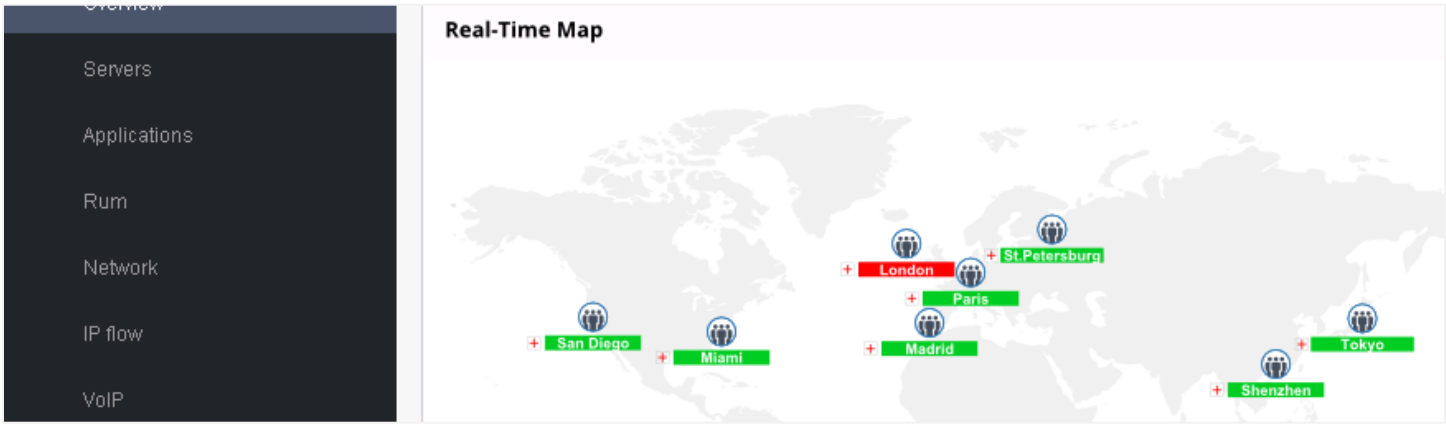
La solution ServicePilot, en plus d'apporter à l'entreprise une visibilité globale de son infrastructure et une plus grande réactivité pour résoudre des incidents, lui a permis de bloquer et prévenir ce genre d'attaques.

1) Collecte du trafic SIP auprès des SBCs

Avant tout, il est important de savoir que ServicePilot collecte des indicateurs auprès de l'ensemble des équipements de l'infrastructure du client (Alcatel-Lucent, Cisco, Lync, Oracle, Sonus). En particulier, notre solution de supervision collecte, sur les SBCs et PBXs, les informations de CDR concernant le volume des appels effectués.

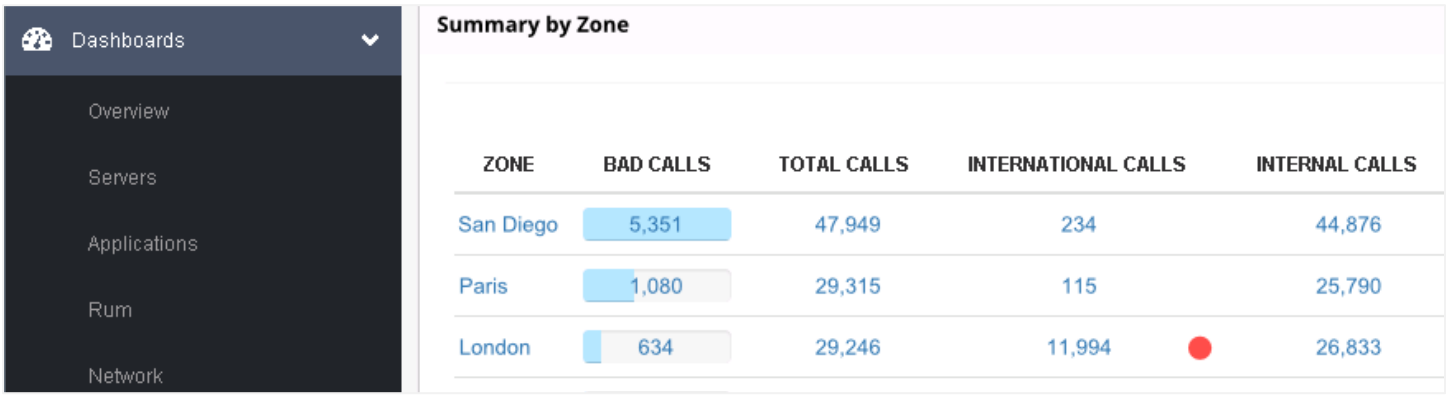
2) Paramétrage des zones et des alertes

De plus, le client a pu paramétrer l'outil de manière à ce que ses données soient affichées par zone géographique, et créer des alertes avec seuils personnalisés, pour détecter les évolutions anormales du volume d'appels.



3) Détection des attaque grâce à des alertes et rapports personnalisés

C'est donc après avoir déployé ServicePilot que l'équipe Voix du client a reçu une alerte indiquant que l'un de ses SBCs faisait l'objet d'une augmentation soudaine du volume d'appels sortants vers l'international (voir la zone « London » ci-dessous). En effet, des centaines d'appels étaient en train d'être effectués depuis une adresse IP inhabituelle et passant par l'un des SBCs Oracle du groupe.



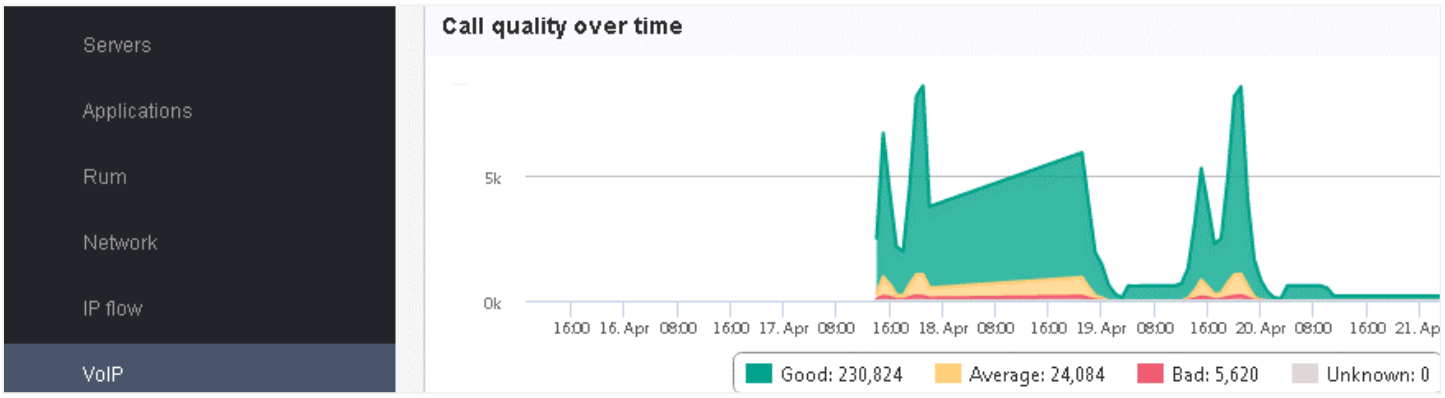
4) Blocage de l'attaque et prévention de fraudes futures

C'est grâce à ce diagnostic précis que l'équipe Voix a pu modifier la configuration du SBC en question afin de bloquer l'IP dont venait l'attaque.

BENEFICES

En réagissant rapidement, le client a ainsi pu :

- limiter l'impact financier de cette attaque et protéger son système des futures attaques venant du hacker
- éviter que des interruptions de service n'affectent le service fourni aux utilisateurs du système.



Selon le Directeur des Télécommunications du client :

"Les alertes et tableaux de bord personnalisés de ServicePilot nous ont aidé à identifier les comportements causés par les hackers VoIP. Leur solution nous a également permis d'éviter des factures téléphoniques très élevées ainsi que de nombreux emails et appels d'utilisateurs mécontents. "

www.servicepilot.com
+33 2 40 60 13 30
info@servicepilot.com