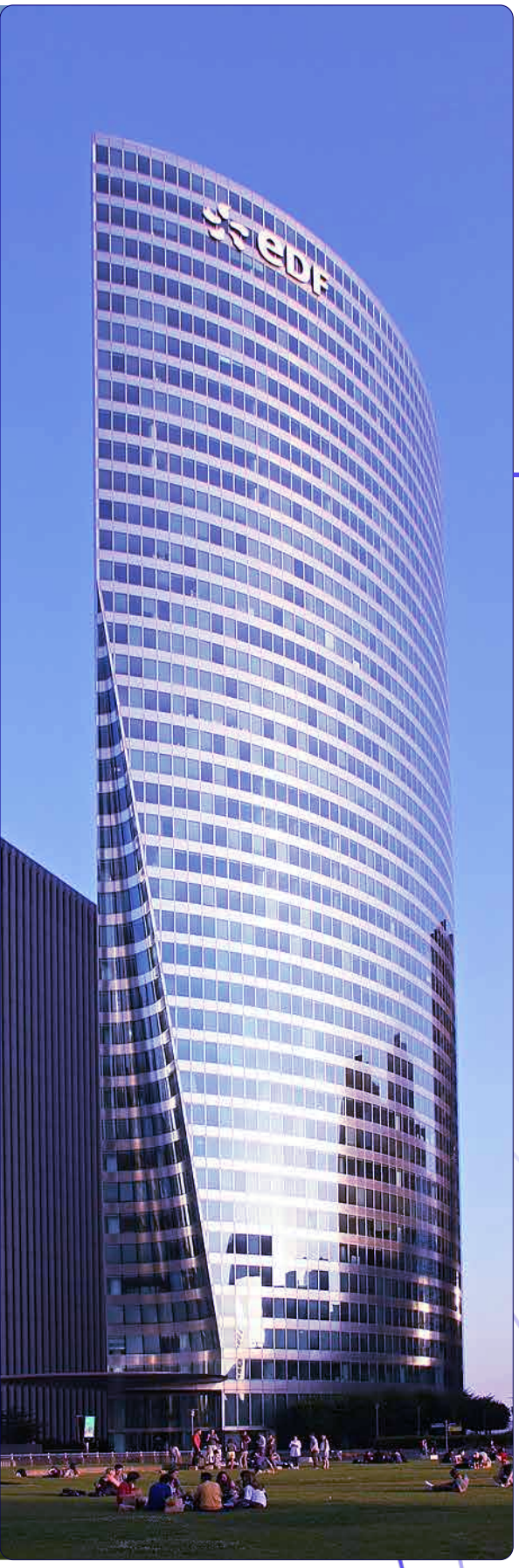
Retour d'expérience client FR

Renseignements sur les menaces

Quels sont les chiffres-clés mesurables ?

Avec EDF



EDF, un groupe mondial à sécuriser

L'équipe SOC de la direction transformation et efficacité opérationnelle du Groupe EDF a pour fonction de prévenir, détecter et répondre aux incidents de sécurité pouvant cibler les salariés et infrastructures du groupe. Le périmètre de cette équipe s'étend majoritairement en Europe ainsi qu'aux États-Unis et en Chine. Cette équipe surveille et sécurise environ 200 000 équipements.

Quel était le besoin ?

L'équipe SOC était à la recherche d'un flux d'information souverain, de confiance permettant de détecter les cyber menaces pouvant cibler le Groupe EDF. Ces informations devaient être suffisamment contextualisées et pertinentes pour permettre à l'équipe de les intégrer directement dans le SIEM et dans les outils de sécurité sans effectuer un traitement préalable.

Le choix de la CTI Sekoia.io

Un POC a été mené pendant une durée de 12 mois en collaboration avec les équipes EDF, les équipes de Threat Quotient (SIEM) et de **Sekoia.io**. Ce POC a été exigeant dans son intégration et a permis d'atteindre l'objectif initial. Cette intégration a permis d'apporter une large couverture de détection des menaces courantes (Phishing, Ransomware, Malware) pouvant cibler le groupe EDF.

Du fait d'un flux de qualité et d'un taux de faux positif quasi nul, l'automatisation était un critère déterminant dans le choix de la solution et la faisabilité de ce projet. Malgré plusieurs POC en parallèle, **Sekoia.io** a été retenue pour la forte expertise, la réactivité et la disponibilité de ses équipes.

Une CTI de qualité au ROI incontestable

L'implémentation du flux de CTI de **Sekoia.io** a permis :

Un ROI mesurable : la qualité et la pertinence de l'information a permis de ne pas solliciter les analystes vde l'équipe SOC.

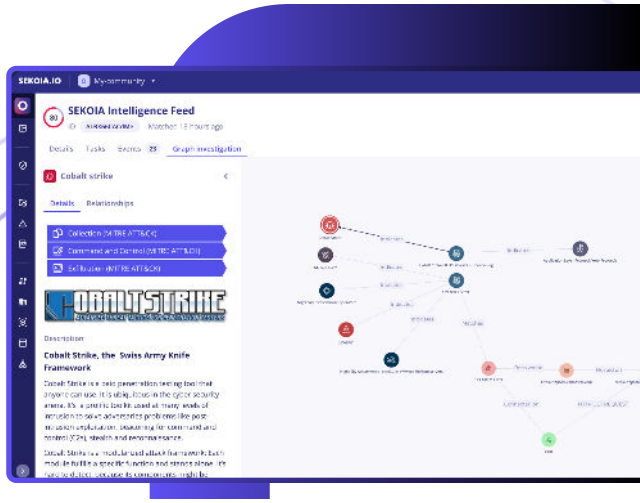
Un **gain de temps** a été dégagé et les équipes n'ont pas eu besoin de recruter pour contextualiser les données.

+10%

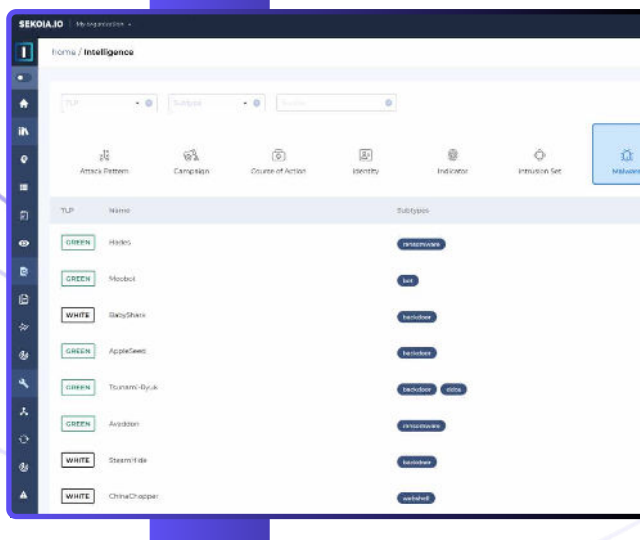
Un enrichissement de l'information menant à une augmentation de 10% du **volume de détections** des menaces.

Des détections pertinentes ayant permis d'éviter des attaques.

Une baisse du volume de faux positifs passant **à moins de 10** pour plus d'un 1 000 000 d'indicateurs.



*Visualisation d'une page Alerte avec le graphique des investigations dans la plateforme **Sekoia.io***



*Liste des indicateurs de compromission structuré au format STIX 2.1 dans la plateforme **Sekoia.io***

Déroulement du Proof-of-Concept

PHASE 1 | Préparation

Une réunion de lancement est organisée pour permettre la transmission aux équipes d'EDF

PHASE 2 | Évaluation du renseignement

- Test des IoCs
- Test des sources
- Test des trackers
- Test des fiches de malwares et groupe d'attaquants
- Test des rapports quotidien FL|INT (Flash Intelligence Report)

PHASE 3 | Bilan du POC

En réunion de bilan, la décision est prise par les équipes EDF de généraliser ce POC.

DUREE | 12 mois

*« On a retenu la solution **Sekoia.io** pour la forte expertise, la réactivité et la disponibilité des équipes. Les équipes Sekoia.io restent disponibles avant, pendant et après l'acte d'achat. Lorsque nous posons une question nous avons généralement une réponse en 24/48h. Lorsque nous faisons des suggestions d'amélioration, elles sont prises en compte dans l'amélioration de la donnée remontée, ce qui est très important pour nous. »*

Thomas BURNOUF

Manager Adjoint du SOC,
Groupe EDF

Vision unifiée.Contrôle total.

www.sekoia.io

contact@sekoia.io