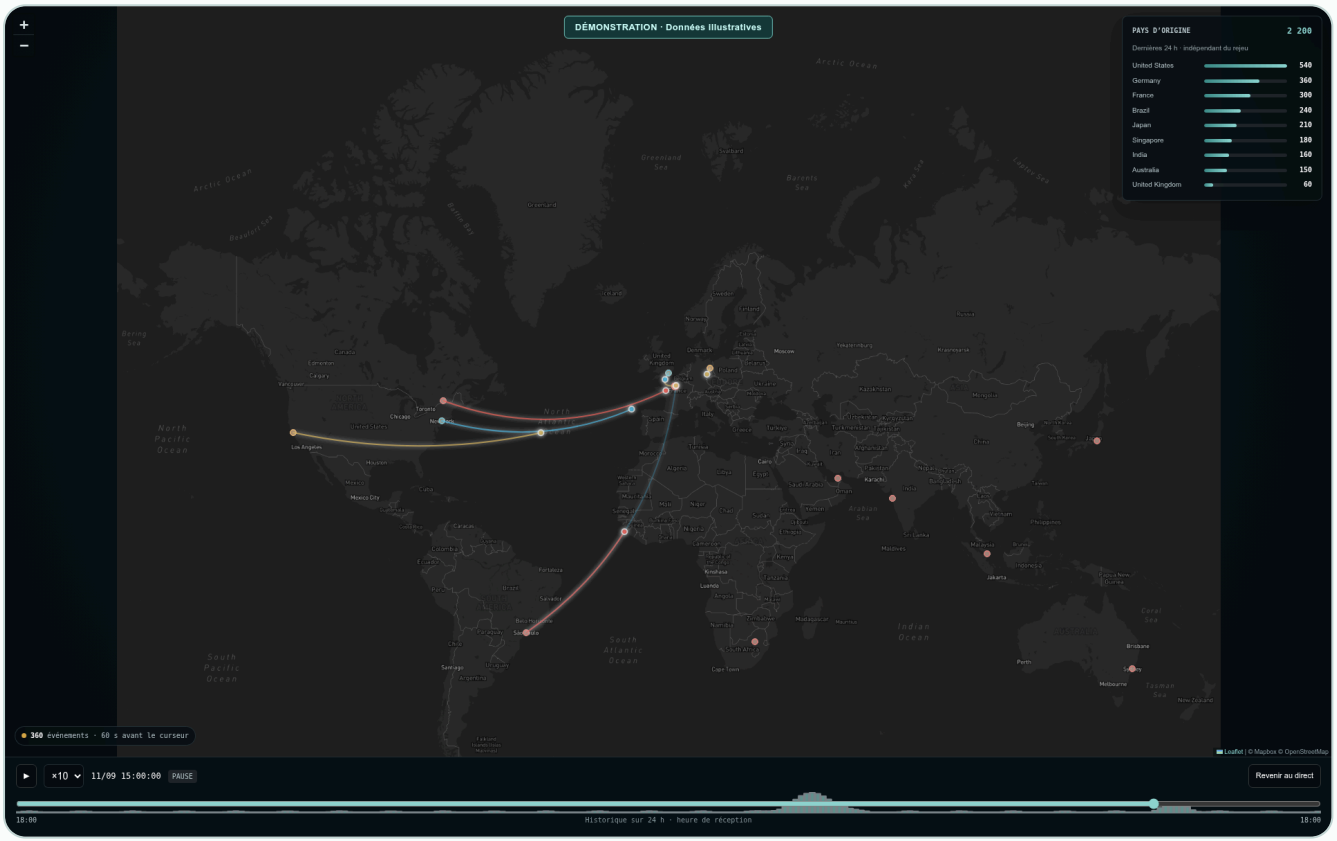
ANALYSE DES ATTAQUES ET EXPOSITION INTERNET

Voyez l’Internet derrière chaque alerte.

MapAttack, le SIEM spécialisé qui centralise vos alertes, révèle leur contexte réseau et vous aide à prioriser l’investigation et à justifier vos décisions.



Le direct et le rejeu pour comprendre une séquence · Interface actuelle, données de démonstration.

BGP

Préfixe · ASN · opérateur

Investigation

Du pic aux événements

Multi-tenant

Périmètres et décisions

Des alertes dispersées à une vision exploitable.

Comprendre les origines, les services visés et les récurrences. Revenir aux faits pour décider et préparer la réponse.

01 / LA VALEUR D'UN SIEM SPÉCIALISÉ

Donnez une dimension réseau à vos alertes.

MapAttack concentre la démarche SIEM — collecte, normalisation, mise en relation et historique — sur les attaques observées sur vos réseaux et services exposés.

Comprendre le réseau derrière l'IP

Le préfixe BGP le plus spécifique, l'ASN et l'opérateur donnent une dimension réseau à l'alerte. Les renseignements RIPE, RDAP et géographiques complètent le contexte disponible.

Revenir aux faits

La règle, la source, la cible et la politique restent consultables. Ouvrez un compteur pour examiner les événements qui expliquent une activité et étayent une décision.

Relier le direct à l'historique

Supervision, recherche et rejeu utilisent la même chaîne de collecte. Repérez un pic, ouvrez sa période et revenez sur la séquence à votre rythme.

Organiser le travail par client

Les tenants, les rôles, les exceptions réseau et les motifs de décision structurent le traitement de plusieurs périmètres avec des responsabilités explicites.

Une collecte conçue pour l'exploitation

Checkpoints, déduplication, journalisation durable et services supervisables donnent à l'exploitant des points de contrôle pour suivre l'ingestion et reprendre les traitements.

Préparer une réponse exploitable

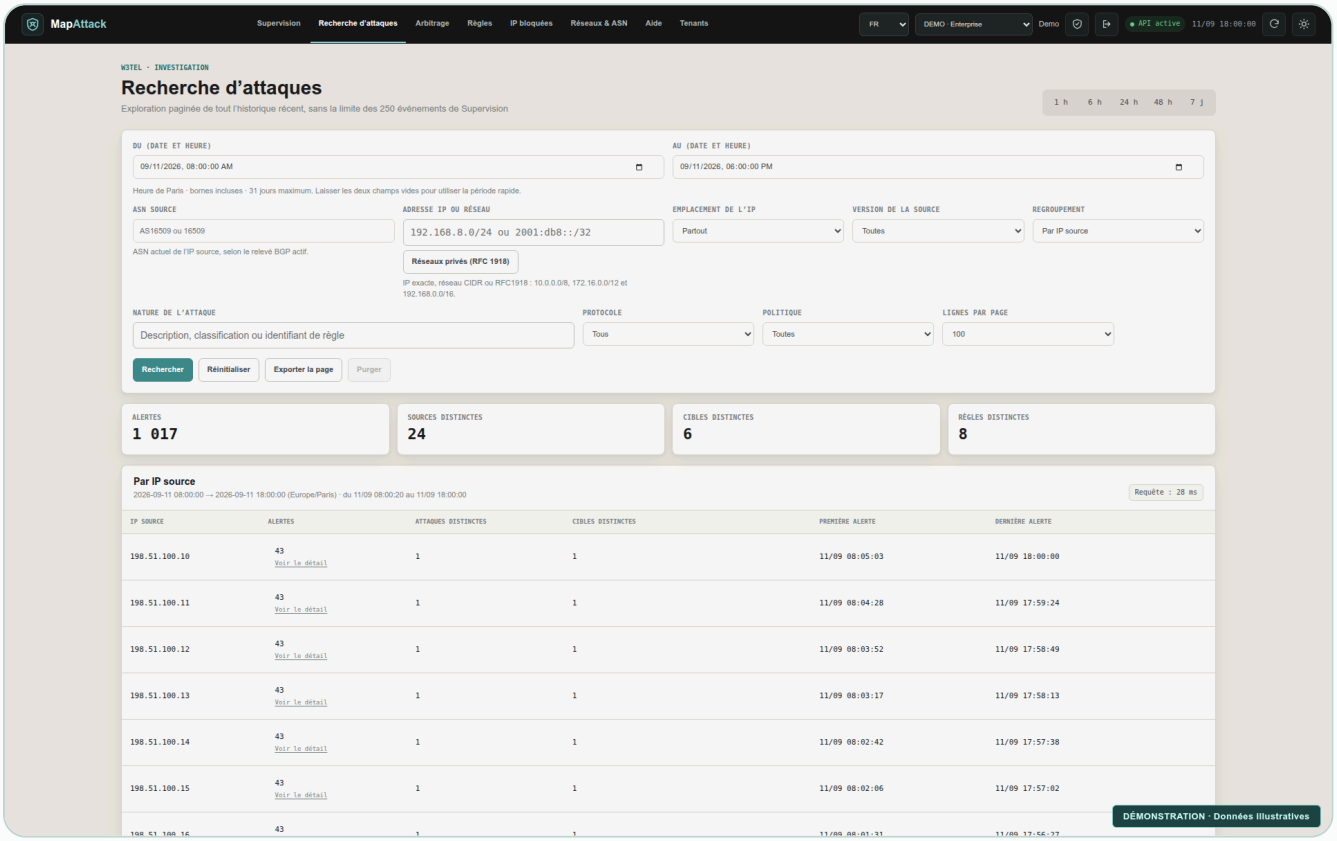
Les listes IPv4/IPv6 par tenant et les exports de routes ASN fournissent les formats utiles au travail sur les firewalls et aux scripts existants.

> **Un rôle clair dans votre dispositif de sécurité.**
>
> MapAttack peut être l'outil d'analyse de ce périmètre ou compléter un SIEM transverse. Sa spécialisation réunit le contexte Internet, les événements et les décisions utiles à l'exploitation.

02 / PASSER DE L'OBSERVATION À L'ENQUÊTE

Un pic attire l'attention. Les faits orientent la décision.

Identifiez les sources récurrentes, examinez les attaques et retrouvez les services concernés dans une même recherche.



Les regroupements font ressortir la récurrence des sources · Interface actuelle, données de démonstration.

Cibler ce qui compte

Dates et heures, ASN source, IP ou réseau CIDR, destination, protocole et politique. Raccourci pour les IPv4 privées RFC1918.

Changer d'échelle

Regroupez par source, par attaque ou par couple IP/attaque pour examiner les concentrations d'activité.

Revenir aux événements

Chaque compteur ouvre les alertes du groupe avec les mêmes filtres : des éléments consultables pour étayer l'analyse.

Reconstituer la séquence

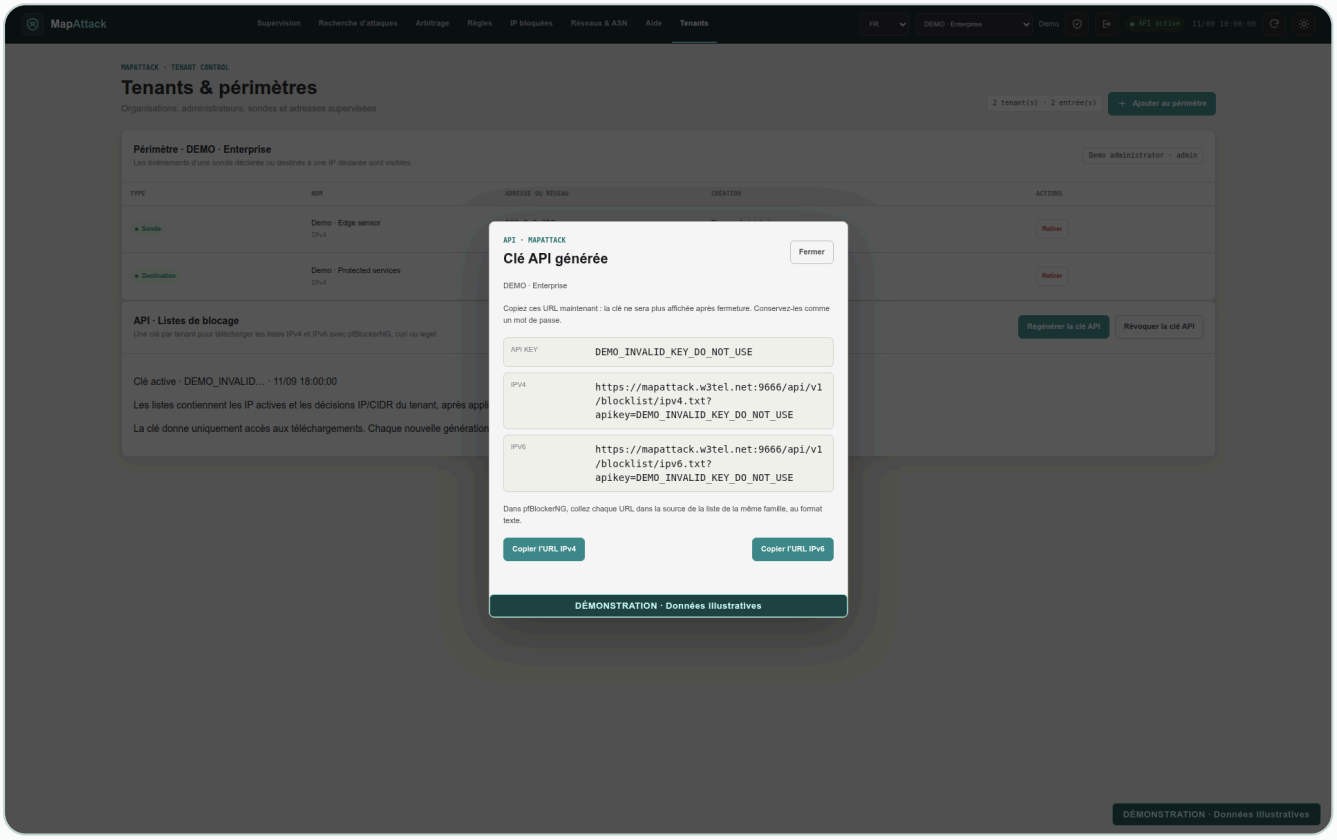
Carte, pause et rejeu jusqu'à ×20, avec un palier ×10. Les totaux pays restent indépendants de la lecture.

Recherche dans les logs conservés, intervalle personnalisé de 31 jours maximum en heure de Paris. Rejeu sur 24 h géolocalisées disponibles au maximum. CSV de la page courante.

03 / PRÉPARER UNE RÉPONSE DOCUMENTÉE

Du contexte à la décision. De la décision aux listes.

Examinez les règles et les exceptions réseau, conservez les motifs et fournissez les données attendues par vos équipements.



Listes IPv4 et IPv6 par tenant — clé fictive, inutilisable · Interface actuelle, données de démonstration.

Décisions explicites

Activité récente, conflits et motifs. Traitez jusqu'à 200 règles sélectionnées par opération groupée.

Une clé par tenant

Générez, remplacez ou révoquez une clé dédiée au téléchargement des listes du périmètre client.

Des formats simples

Une IP ou un CIDR par ligne. Deux URL utilisables par les consommateurs de listes texte et les scripts Linux.

L'échelle d'un ASN

Exportez les préfixes IPv4, IPv6 ou les deux d'un ASN pour préparer un alias ou une règle de firewall.

Les listes API appliquent l'état importé et les décisions IP/CIDR ; les ASN ne sont pas développés automatiquement. Les exports ASN utilisent le relevé actif. Téléchargement et application sont configurés sur l'équipement, notamment pfBlockerNG.

04 / TROIS BESOINS, UN MÊME CONTEXTE

Une lecture utile à votre métier.

Comprendre ce qui est visé, relier les sources à leurs réseaux et organiser les décisions dans les bons périmètres.

ÉQUIPE SÉCURITÉ

Comprendre un pic sur un service

Ouvrez la période, filtrez la destination et regroupez les alertes par attaque puis par source. Examinez les règles et les ASN concernés, puis partagez les événements qui étayent l'analyse.

HÉBERGEUR OU OPÉRATEUR

Retrouver le réseau derrière les adresses

Rapprochez les IP de leur contexte BGP, recherchez l'activité d'un ASN et examinez les cibles visées. Exportez ses préfixes lorsque vous préparez un alias ou une règle de firewall.

PRESTATAIRE OU MSP

Structurer le traitement par client

Sélectionnez le tenant, examinez ses événements et documentez ses décisions. Les périmètres, les rôles et les listes IP dédiées permettent d'organiser le service et d'expliquer le travail réalisé.

> **Le fil conducteur : rendre l'analyse partageable.**
>
> Retrouver les événements, comprendre le réseau concerné et expliquer pourquoi une décision a été prise.

Scénarios d'usage illustratifs, sans référence client ni gain chiffré revendiqué. Le contexte réseau situe l'activité ; il n'identifie pas à lui seul l'auteur d'une attaque.

05 / CONÇU POUR L'EXPLOITATION QUOTIDIENNE

Une visibilité que votre équipe peut exploiter et partager.

La valeur du SIEM spécialisé se prolonge dans la continuité de collecte, l'organisation du travail et la traçabilité des décisions.

Continuité de la collecte

Reprise par checkpoint, déduplication et journalisation durable. Des traitements et services supervisables pour suivre l'ingestion.

Périmètres et responsabilités

Tenants, sondes, destinations et rôles structurent les consultations, les décisions et l'administration.

Décisions explicables

Activité, politique, exceptions réseau et motifs restent reliés au travail d'analyse. Les décisions sont auditées.

Méthodes fortes

Clés FIDO2/WebAuthn, dont YubiKey, et application TOTP pour les opérations concernées.

Retraits ciblés et archivés

La purge demande une confirmation forte et archive les événements avec l'acteur, le tenant et les filtres.

Prise en main accompagnée

Une aide française et anglaise explique les parcours, les exemples et la portée des actions.

> **Comprendre. Prioriser. Décider avec des faits.**
>
> Demandez une démonstration à partir de vos sources de détection, de vos services exposés et de vos périmètres clients.

Périmètre dépendant des sondes et formats intégrés. Attribution réseau selon les sources disponibles et le relevé BGP actif. Les captures sont illustratives : leurs volumes et temps ne sont pas des mesures de production ou de performance.