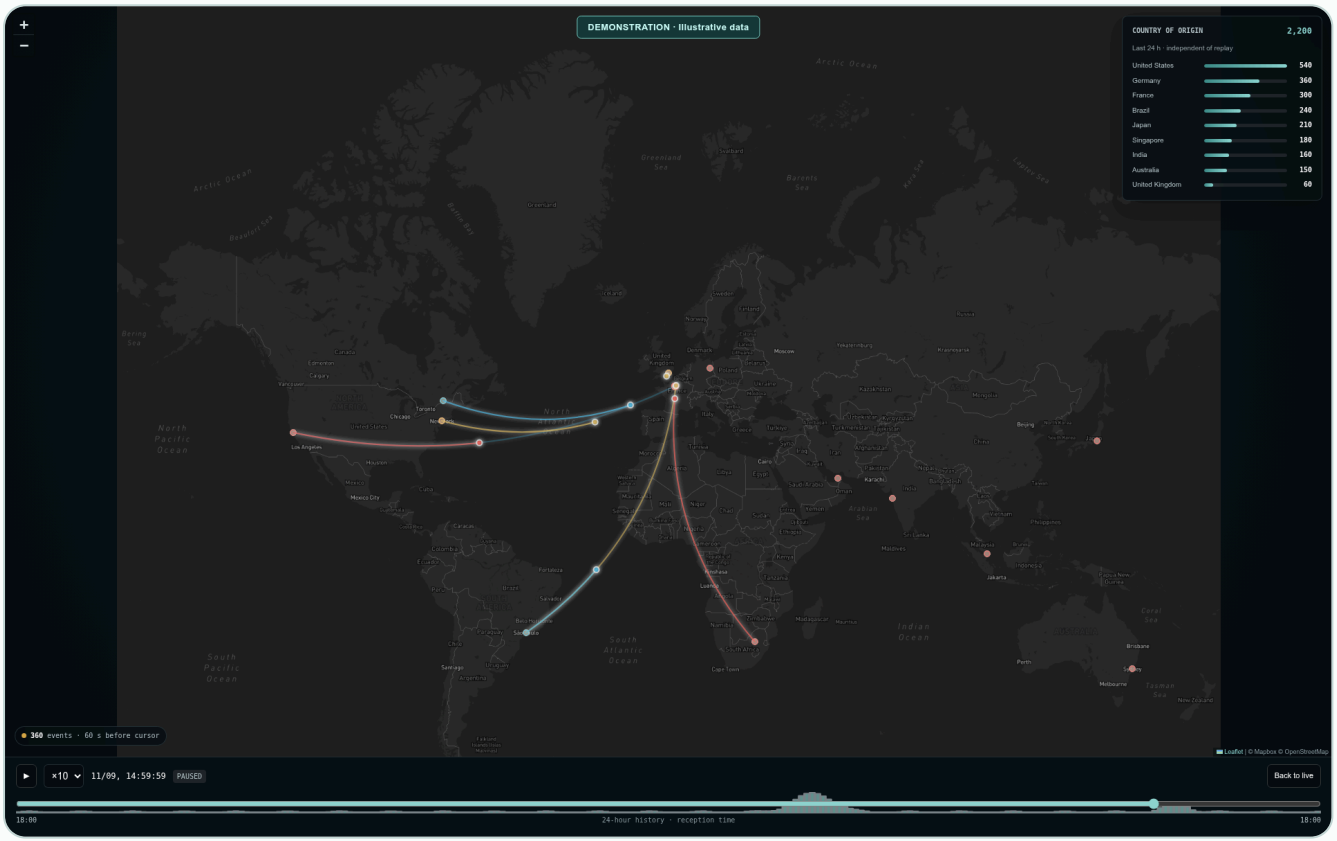
ATTACK ANALYSIS AND INTERNET EXPOSURE

See the Internet behind every alert.

MapAttack, the specialised SIEM that centralises your alerts, reveals their network context and helps you prioritise investigation and substantiate decisions.



Live monitoring and replay to understand a sequence · Current interface, demonstration data.

BGP

Prefix · ASN · operator

Investigation

From the spike to events

Multi-tenant

Scopes and decisions

From scattered alerts to actionable visibility.

Understand origins, targeted services and recurrence. Return to the evidence to decide and prepare a response.

01 / THE VALUE OF A SPECIALISED SIEM

Give your alerts a network dimension.

MapAttack focuses the SIEM approach — collection, normalisation, correlation and history — on attacks observed against your networks and exposed services.

Understand the network behind the IP

The most specific BGP prefix, ASN and operator add a network dimension to an alert. RIPE, RDAP and geographic information supplement the available context.

Return to the evidence

The rule, source, target and policy remain accessible. Open a count to inspect the events that explain activity and support a decision.

Connect live activity with history

Monitoring, search and replay share the same collection chain. Locate a spike, open its period and revisit the sequence at your own pace.

Organise work by customer

Tenants, roles, network exceptions and decision reasons structure the handling of several scopes with explicit responsibilities.

Collection built for operations

Checkpoints, deduplication, durable journalling and monitored services provide control points to track ingestion and resume processing.

Prepare usable response data

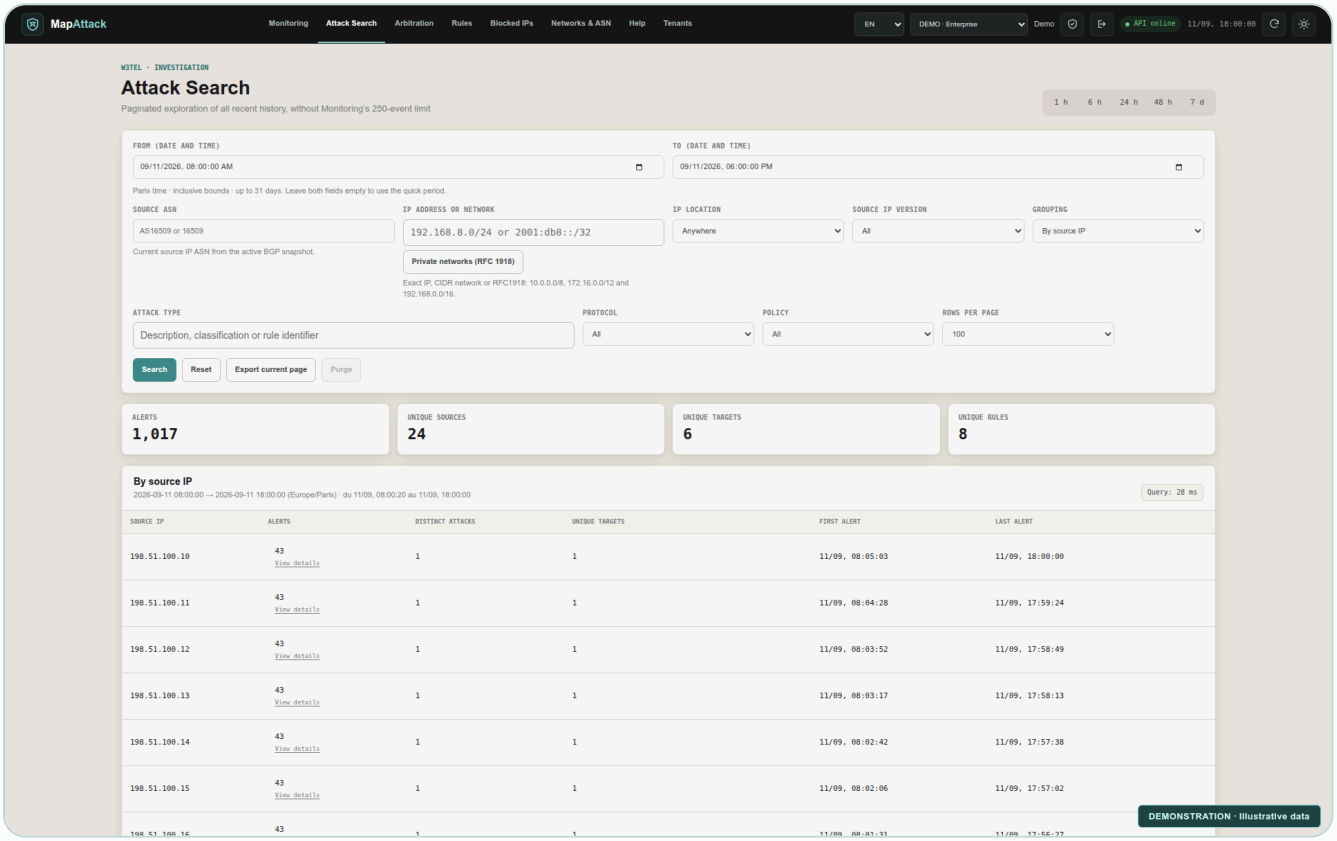
Tenant-specific IPv4/IPv6 feeds and ASN route exports provide formats that support firewall configuration work and existing scripts.

> **A clear role in your security operations.**
>
> MapAttack can serve as the analysis tool for this scope or complement a broader SIEM. Its specialisation brings together Internet context, events and decisions relevant to operations.

02 / FROM OBSERVATION TO INVESTIGATION

A spike draws attention. Evidence informs the decision.

Identify recurring sources, examine attack types and find the affected services within the same search.



Grouping highlights recurring sources · Current interface, demonstration data.

Focus on what matters

Dates and times, source ASN, IP or CIDR, destination, protocol and policy. A shortcut covers RFC1918 private IPv4 networks.

Change the scale

Group by source, attack or IP/attack pair to examine concentrations of activity.

Return to the events

Each count opens its group with the same filters, providing accessible evidence for the investigation.

Review the sequence

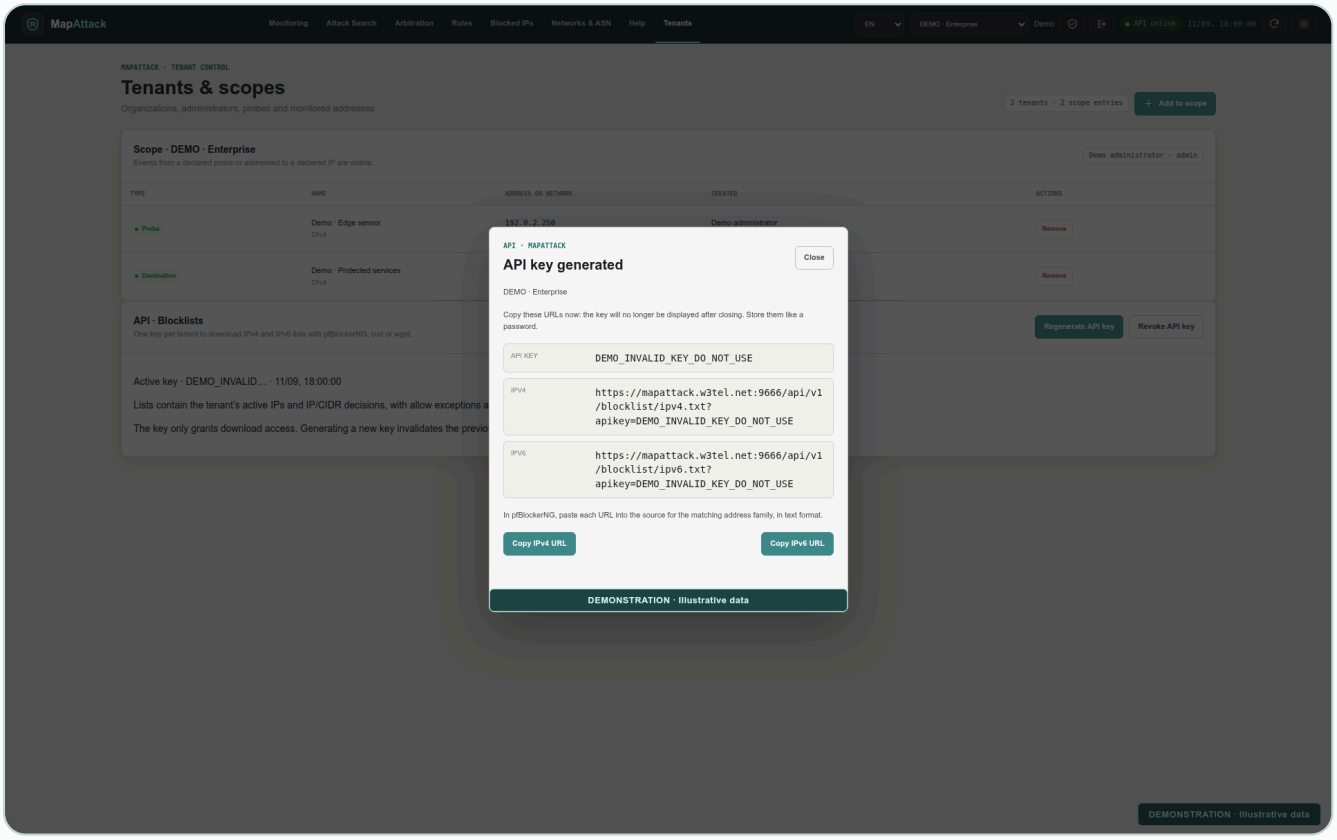
Map, pause and playback up to ×20, including ×10. Country totals remain independent of replay.

Search uses retained logs; custom intervals span up to 31 days in Paris time. Replay covers up to 24 available hours of geolocated events. CSV export covers the current page.

03 / PREPARE A DOCUMENTED RESPONSE

From context to decisions. From decisions to lists.

Review rules and network exceptions, retain the reasons and provide the data your equipment expects.



Tenant-specific IPv4 and IPv6 lists — fictional, unusable key · Current interface, demonstration data.

Explicit decisions

Recent activity, conflicts and reasons. Handle up to 200 selected rules in one batch operation.

A key per tenant

Generate, rotate or revoke a key dedicated to list downloads for the customer scope.

Simple formats

One IP or CIDR per line. Two URLs for text-list consumers and Linux scripts.

The ASN perspective

Export an ASN's IPv4 prefixes, IPv6 prefixes or both when preparing a firewall alias or rule.

API feeds apply imported state and IP/CIDR decisions; ASNs are not expanded automatically. ASN exports use the active snapshot. Downloading and enforcement are configured on the equipment, including pfBlockerNG.

04 / THREE NEEDS, A SHARED CONTEXT

A perspective that serves your operations.

Understand what is being targeted, connect sources with their networks and organise decisions within the appropriate scopes.

SECURITY TEAM

Understand a spike against a service

Open the period, filter by destination and group alerts by attack, then by source. Examine the rules and ASNs involved, then share the events supporting the analysis.

HOSTING PROVIDER OR OPERATOR

Find the network behind the addresses

Connect IPs with BGP context, search activity from an ASN and examine the targets. Export its prefixes when preparing a firewall alias or rule.

SERVICE PROVIDER OR MSP

Structure handling by customer

Select a tenant, review its events and document its decisions. Scopes, roles and dedicated IP feeds help organise the service and explain the work performed.

> **The common thread: analysis you can share.**
>
> Find the events, understand the network involved and explain why a decision was made.

Illustrative workflows, without customer references or claims of measured gains. Network context locates activity; it does not by itself identify the person responsible for an attack.

05 / BUILT FOR EVERYDAY OPERATIONS

Visibility your team can use and share.

A specialised SIEM adds value through collection continuity, organised workflows and traceable decisions.

Collection continuity

Checkpoint-based recovery, deduplication and durable journalling. Jobs and services operators can monitor to track ingestion.

Scopes and responsibilities

Tenants, sensors, destinations and roles organise viewing, decisions and administration.

Explainable decisions

Activity, policy, network exceptions and reasons remain connected to the investigation. Decisions are audited.

Strong methods

FIDO2/WebAuthn keys, including YubiKey, and a TOTP app for the relevant operations.

Targeted, archived removal

Purging requires strong confirmation and archives events with the actor, tenant and filters.

Supported onboarding

French and English help explains workflows, examples and action scope.

> **Understand. Prioritise. Decide with evidence.**
>
> Request a demonstration based on your detection sources, exposed services and customer scopes.

Coverage depends on integrated sensors and formats. Network attribution uses available sources and the active BGP snapshot. Screenshots are illustrative; displayed volumes and timings are not production or performance measurements.