Seeing the Unseen:

Data Governance, Trust, and Fraud Protection

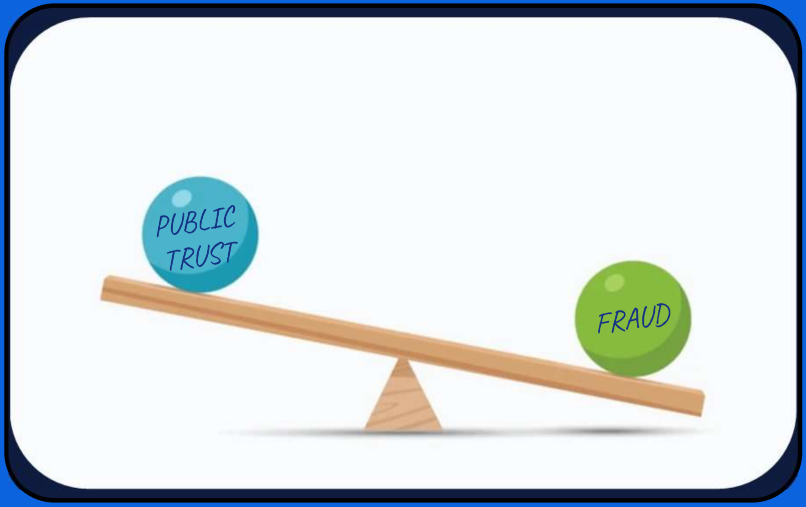
Kyle Rozanitis, Senior Solutions Architect

October 2025

elastic | The Search AI Company

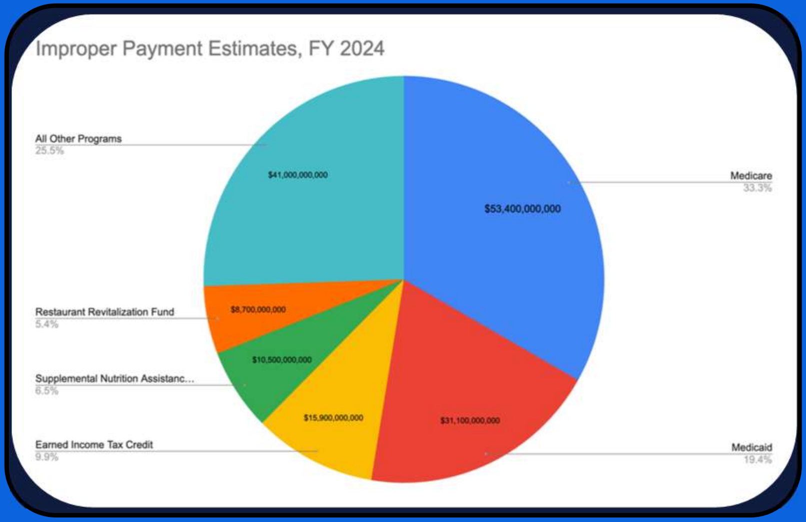
Fraud detection and public trust must move together.

Agencies can’t protect taxpayer dollars without data, and they can’t protect trust without governance.

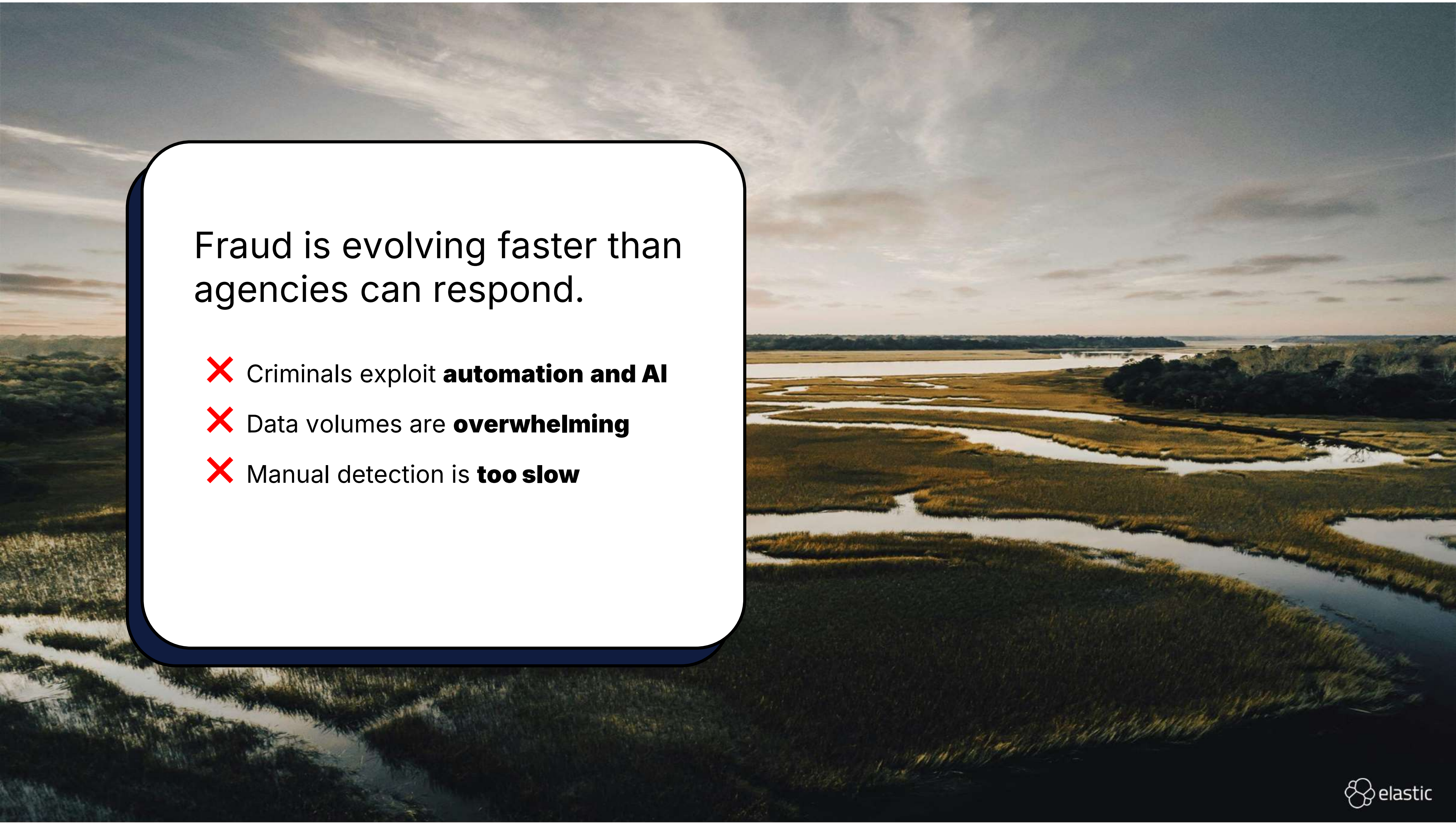


Fraud drains billions and erodes trust.

According to GAO's government-wide estimates based on data from fiscal years 2018-2022, the federal government loses between $233bn to $521bn annually to fraud.



Data sourced from the U.S. Government Accountability Office (GAO).



Fraud is evolving faster than agencies can respond.

- ✗ Criminals exploit **automation and AI**
- ✗ Data volumes are **overwhelming**
- ✗ Manual detection is **too slow**

The Reality on the Ground
v1

Doesn’t scale with the problem

Fraud detection often depends on exporting data into Excel. Analysts spend hours massaging rows and columns instead of investigating. It works in small bursts, but when datasets balloon into millions of rows, Excel buckles.

Searching for only the familiar

Analysts massage the data to find repeat patterns — multiple claims from the same IP, rare routing numbers, disposable email domains. But they only uncover what they already know to look for.

Blind to the unknown

Novel or anomalous fraud behaviors slip through the cracks. Without automation and machine learning, agencies are always one step behind.

elastic

The Reality on the Ground v2

Doesn’t scale with the problem

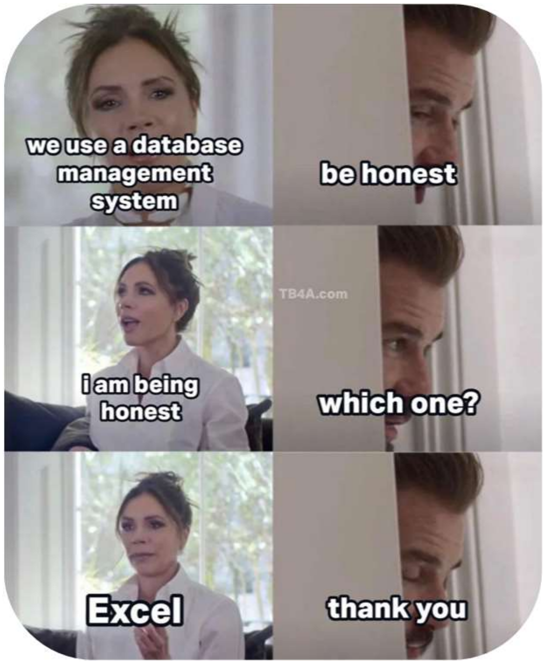
Fraud detection often depends on exporting data into Excel. Analysts spend hours massaging rows and columns instead of investigating. It works in small bursts, but when datasets balloon into millions of rows, Excel buckles.

Searching for only the familiar

Analysts massage the data to find repeat patterns — multiple claims from the same IP, rare routing numbers, disposable email domains. But they only uncover what they already know to look for.

Blind to the unknown

Novel or anomalous fraud behaviors slip through the cracks. Without automation and machine learning, agencies are always one step behind.



Data powers fraud detection—but raises new risks.

The same citizen data that reveals suspicious patterns can undermine trust if misused.

- Identity Data
- Transaction Records
- Network & Behavioral Data

The Governance Triangle

Collect only what’s necessary

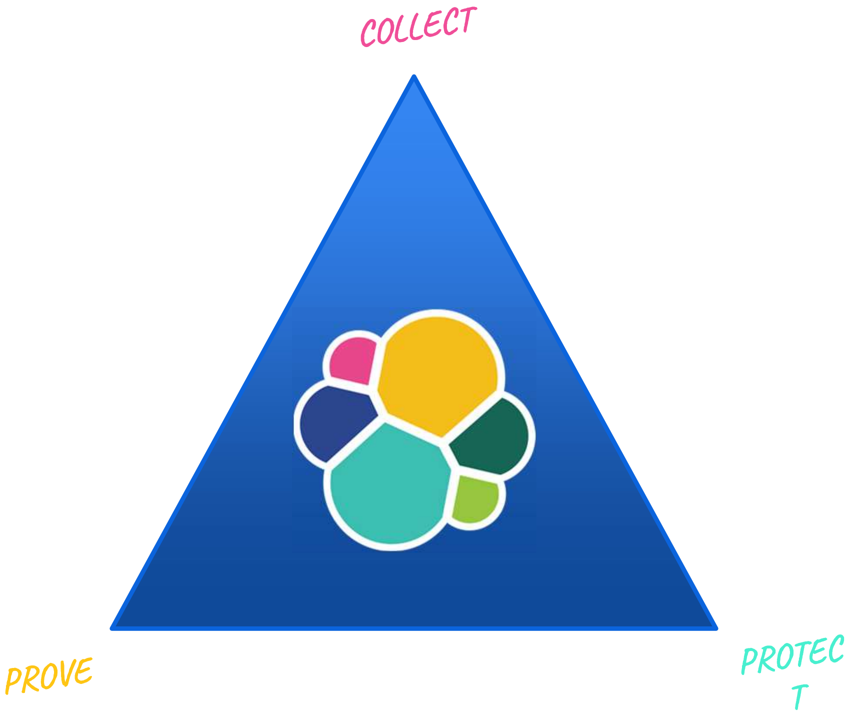
Good governance starts with restraint. Agencies should minimize the data they collect, focusing only on what’s needed for fraud detection and compliance — nothing more.

Protect with layered security

Safeguards must be built in at every level: SSO, SAML, RBAC, and fine-grained controls like document-level and field-based access. Data should be encrypted in transit and at rest, and the systems, servers, and endpoints where that data lives must be hardened against attack.

Prove accountability and compliance

Trust requires visibility. Audit logging shows who accessed what, when, and how. Regular checks against frameworks like NIST CSF and state data policies demonstrate compliance. Transparency with citizens builds confidence that their information is being handled responsibly.



So what does this look like in practice?

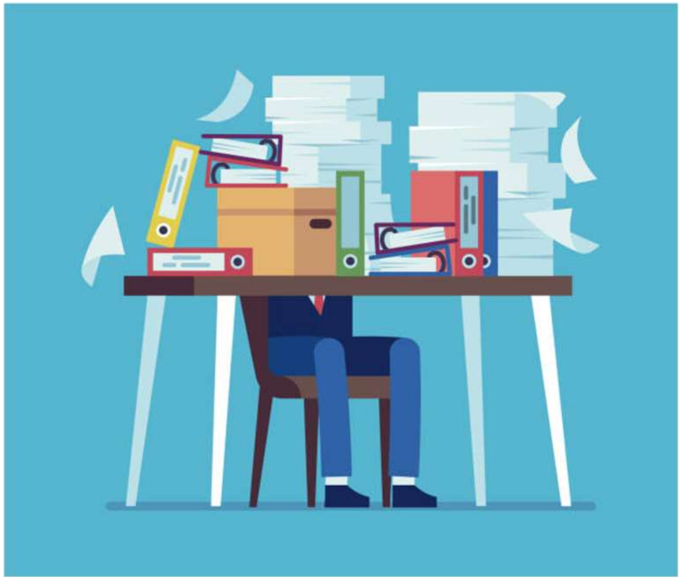
Fraud Detection with Elastic

Spot the Fraud Hidden within the Noise

It’s Monday morning at the Department of Labor.

A new wave of unemployment claims has arrived overnight — just like every day.

Most are legitimate. Some aren’t.



Among the thousands of claims, fraud is hiding:

✕ Multiple emails from the same IP
✕ Identities linked to the same bank account
✕ Suspicious spikes in ZIP codes

Fraud analysts are doing their best, but the tools are limited:

✕ Static reports and spreadsheets that don’t scale
✕ Manual investigations that take hours
✕ Hunting only for known patterns

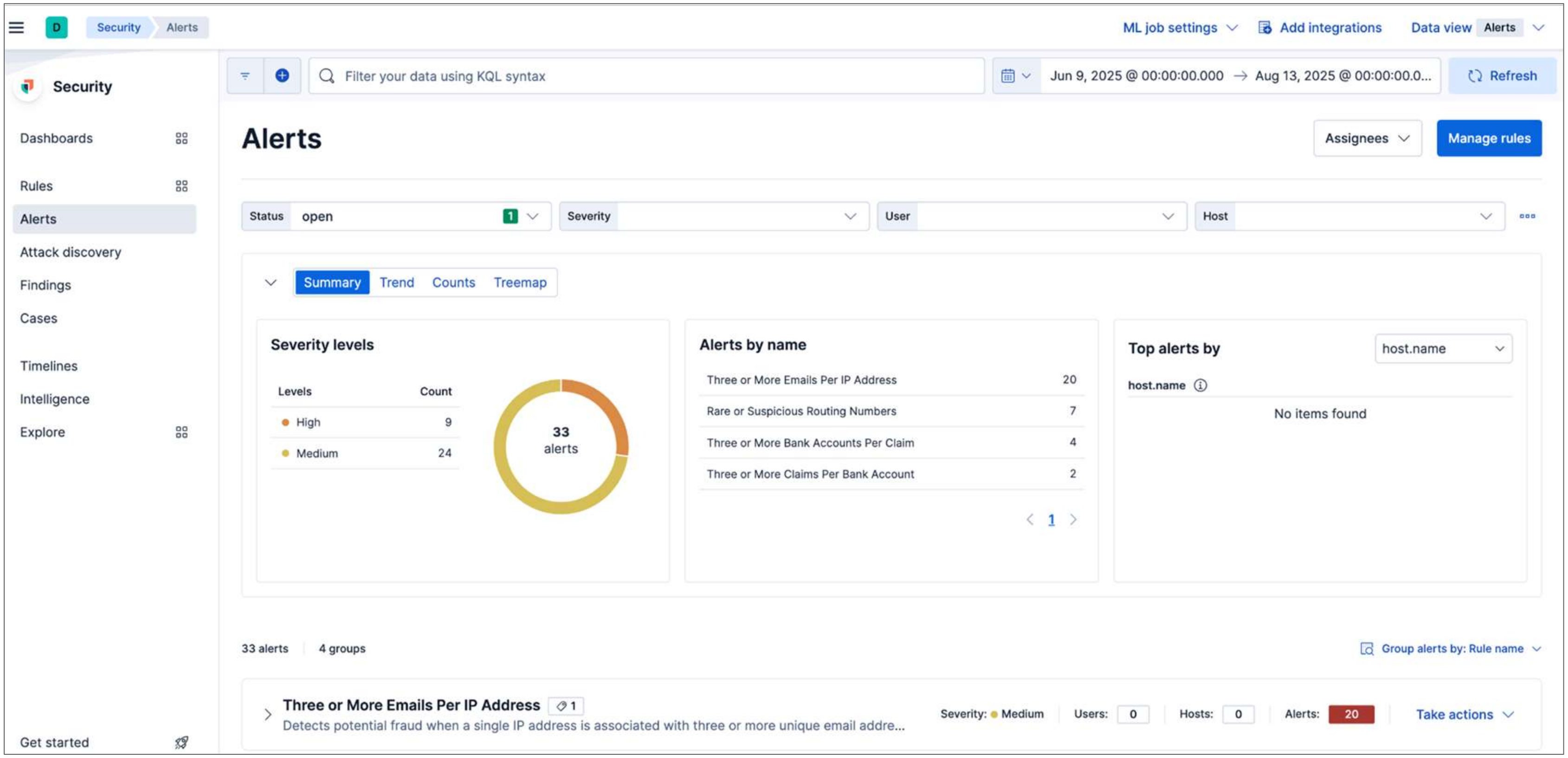
Meanwhile, fraudulent claims are getting approved and payouts are going out the door.

Scene 1:

A Suspicious Spike

Fraud Detection with Elastic

Scene 1: A Suspicious Spike



Filter your data using KQL syntax

Jun 9, 2025 @ 00:00:00.000 → Aug 13, 2025 @ 00:00:00.0...

Alerts

Status: open 1 · Severity · User · Host

Severity levels

Levels	Count
● High	9
● Medium	24

33 alerts

Alerts by name

Three or More Emails Per IP Address	20
Rare or Suspicious Routing Numbers	7
Three or More Bank Accounts Per Claim	4
Three or More Claims Per Bank Account	2

Top alerts by host.name

host.name

No items found

33 alerts | 4 groups

Group alerts by: Rule name

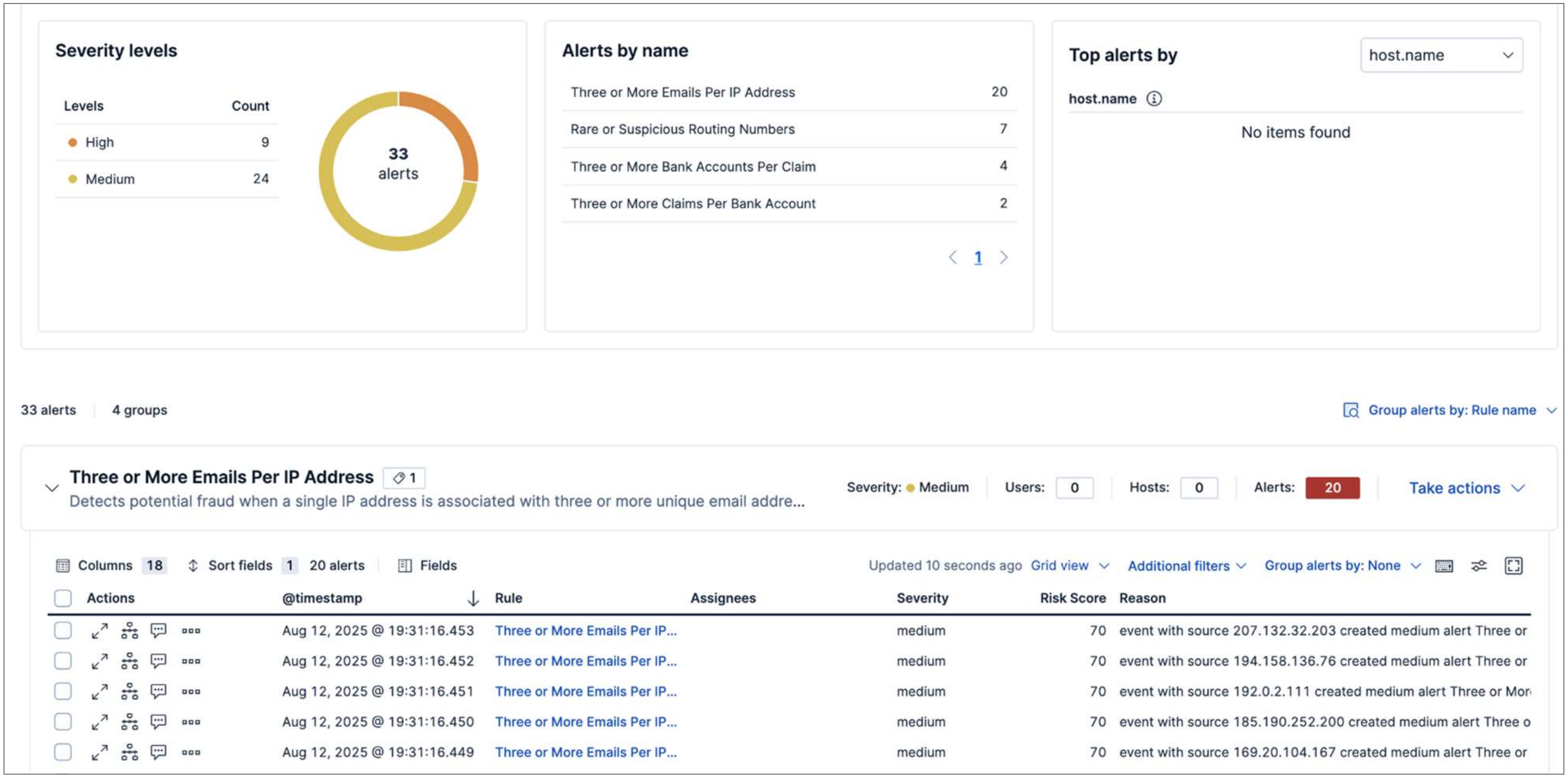
Three or More Emails Per IP Address 1

Detects potential fraud when a single IP address is associated with three or more unique email addre...

Severity: ● Medium | Users: 0 | Hosts: 0 | Alerts: 20

Fraud Detection with Elastic

Scene 1: A Suspicious Spike



Severity levels

Levels	Count
● High	9
● Medium	24

Alerts by name

Three or More Emails Per IP Address	20
Rare or Suspicious Routing Numbers	7
Three or More Bank Accounts Per Claim	4
Three or More Claims Per Bank Account	2

Top alerts by host.name

host.name

No items found

33 alerts | 4 groups

Group alerts by: Rule name

Three or More Emails Per IP Address 1

Detects potential fraud when a single IP address is associated with three or more unique email addre...

Severity: ● Medium | Users: 0 | Hosts: 0 | Alerts: 20 | Take actions

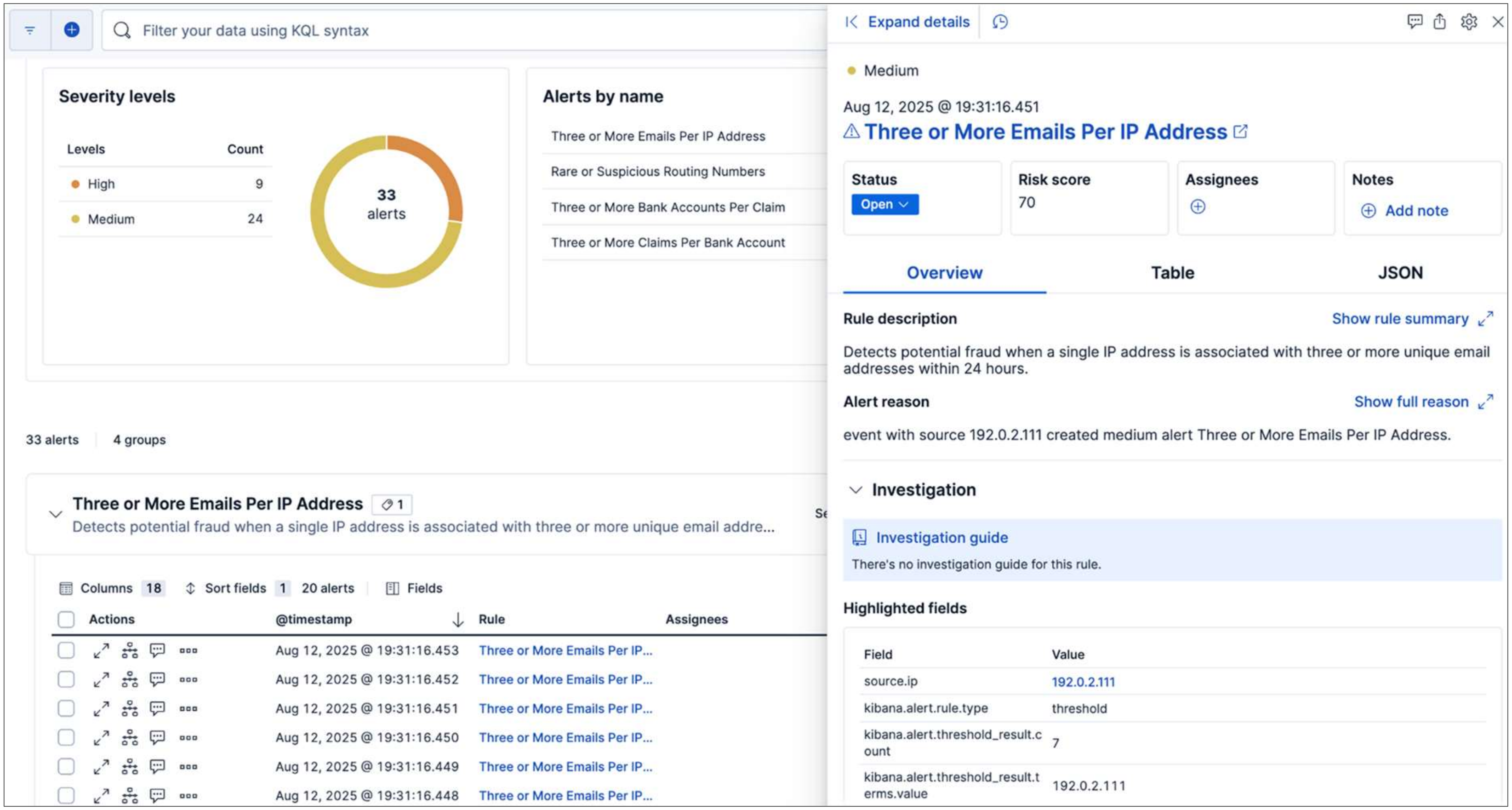
Columns 18 | Sort fields 1 | 20 alerts | Fields

Updated 10 seconds ago | Grid view | Additional filters | Group alerts by: None

☐ Actions	@timestamp	Rule	Assignees	Severity	Risk Score	Reason
☐	Aug 12, 2025 @ 19:31:16.453	Three or More Emails Per IP...		medium	70	event with source 207.132.32.203 created medium alert Three or
☐	Aug 12, 2025 @ 19:31:16.452	Three or More Emails Per IP...		medium	70	event with source 194.158.136.76 created medium alert Three or
☐	Aug 12, 2025 @ 19:31:16.451	Three or More Emails Per IP...		medium	70	event with source 192.0.2.111 created medium alert Three or Mor
☐	Aug 12, 2025 @ 19:31:16.450	Three or More Emails Per IP...		medium	70	event with source 185.190.252.200 created medium alert Three o
☐	Aug 12, 2025 @ 19:31:16.449	Three or More Emails Per IP...		medium	70	event with source 169.20.104.167 created medium alert Three or

Fraud Detection with Elastic

Scene 1: A Suspicious Spike



Severity levels

Levels	Count
● High	9
● Medium	24

Alerts by name

- Three or More Emails Per IP Address
- Rare or Suspicious Routing Numbers
- Three or More Bank Accounts Per Claim
- Three or More Claims Per Bank Account

33 alerts | 4 groups

Three or More Emails Per IP Address 1

Detects potential fraud when a single IP address is associated with three or more unique email addre...

☐ Actions	@timestamp	Rule	Assignees
☐	Aug 12, 2025 @ 19:31:16.453	Three or More Emails Per IP...	
☐	Aug 12, 2025 @ 19:31:16.452	Three or More Emails Per IP...	
☐	Aug 12, 2025 @ 19:31:16.451	Three or More Emails Per IP...	
☐	Aug 12, 2025 @ 19:31:16.450	Three or More Emails Per IP...	
☐	Aug 12, 2025 @ 19:31:16.449	Three or More Emails Per IP...	
☐	Aug 12, 2025 @ 19:31:16.448	Three or More Emails Per IP...	

● Medium

Aug 12, 2025 @ 19:31:16.451

Three or More Emails Per IP Address

Status	Risk score	Assignees	Notes
Open	70	⊕	⊕ Add note

Rule description Show rule summary

Detects potential fraud when a single IP address is associated with three or more unique email addresses within 24 hours.

Alert reason Show full reason

event with source 192.0.2.111 created medium alert Three or More Emails Per IP Address.

Investigation

Investigation guide

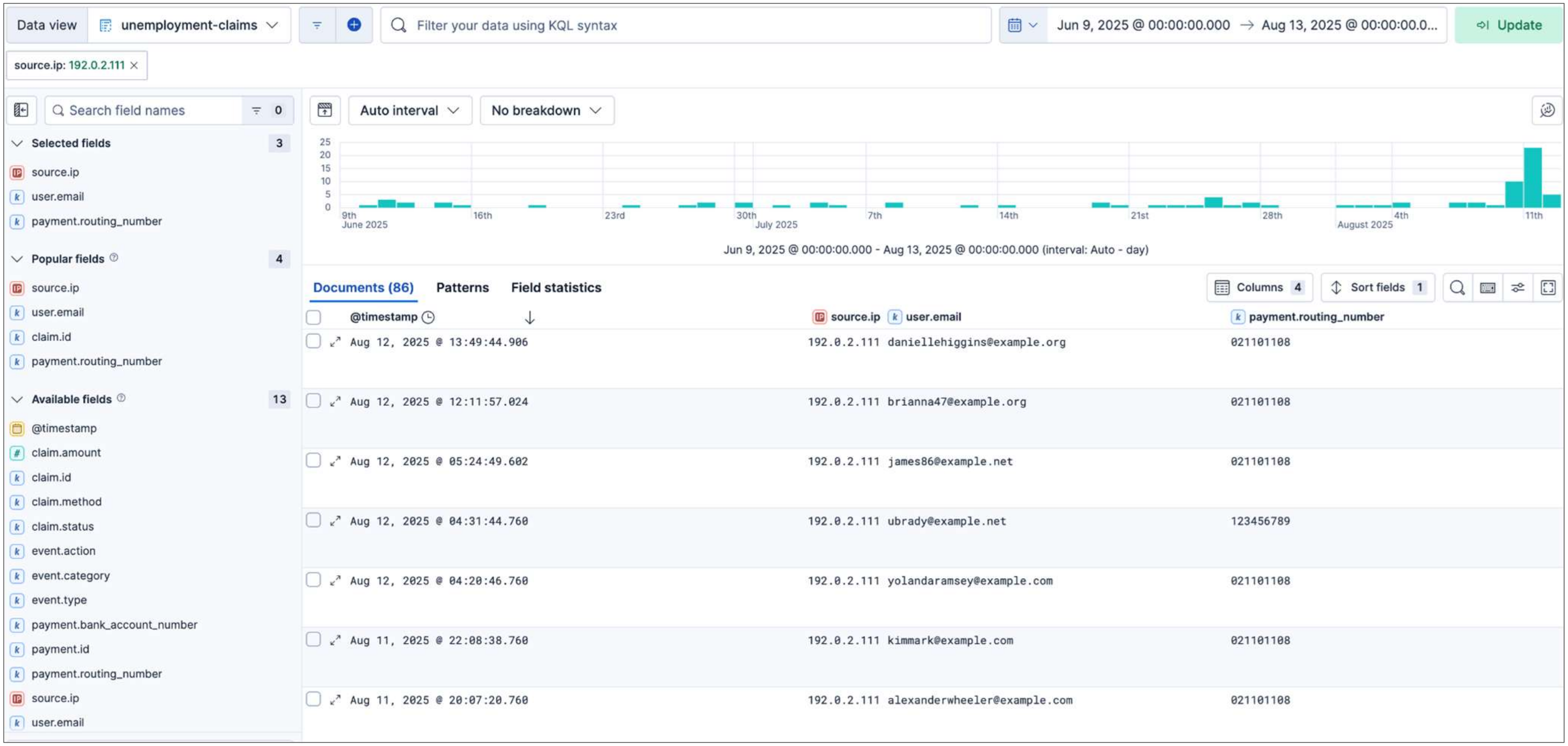
There's no investigation guide for this rule.

Highlighted fields

Field	Value
source.ip	192.0.2.111
kibana.alert.rule.type	threshold
kibana.alert.threshold_result.count	7
kibana.alert.threshold_result.terms.value	192.0.2.111

Fraud Detection with Elastic

Scene 1: A Suspicious Spike



Data view: unemployment-claims

Filter your data using KQL syntax

Jun 9, 2025 @ 00:00:00.000 → Aug 13, 2025 @ 00:00:00.0...

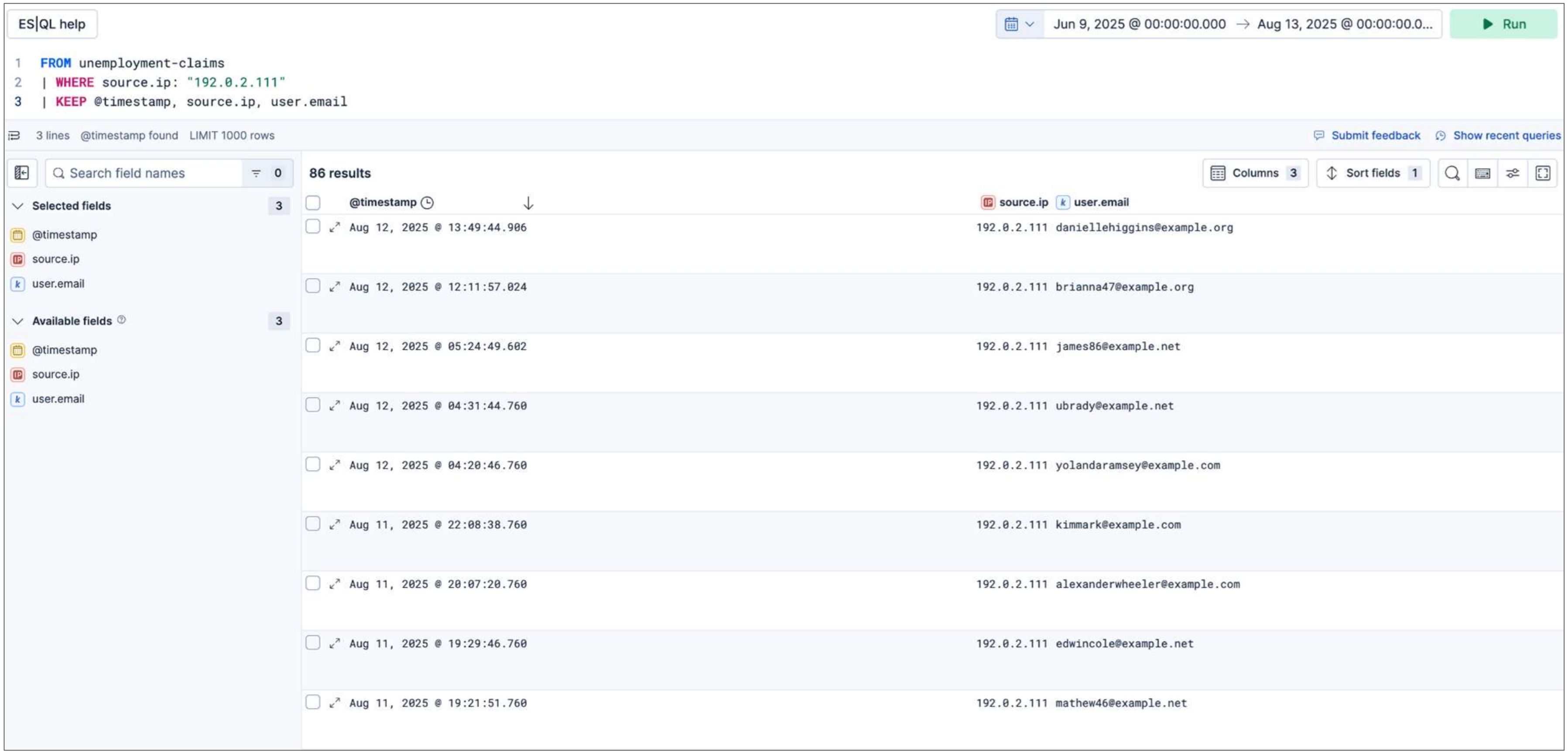
source.ip: 192.0.2.111

Jun 9, 2025 @ 00:00:00.000 - Aug 13, 2025 @ 00:00:00.000 (interval: Auto - day)

@timestamp	source.ip	user.email	payment.routing_number
Aug 12, 2025 @ 13:49:44.906	192.0.2.111	daniellehiggins@example.org	021101108
Aug 12, 2025 @ 12:11:57.024	192.0.2.111	brianna47@example.org	021101108
Aug 12, 2025 @ 05:24:49.602	192.0.2.111	james86@example.net	021101108
Aug 12, 2025 @ 04:31:44.760	192.0.2.111	ubrady@example.net	123456789
Aug 12, 2025 @ 04:20:46.760	192.0.2.111	yolandaramsey@example.com	021101108
Aug 11, 2025 @ 22:08:38.760	192.0.2.111	kimmark@example.com	021101108
Aug 11, 2025 @ 20:07:20.760	192.0.2.111	alexanderwheeler@example.com	021101108

Fraud Detection with Elastic

Scene 1: A Suspicious Spike



```
FROM unemployment-claims
| WHERE source.ip: "192.0.2.111"
| KEEP @timestamp, source.ip, user.email
```

86 results

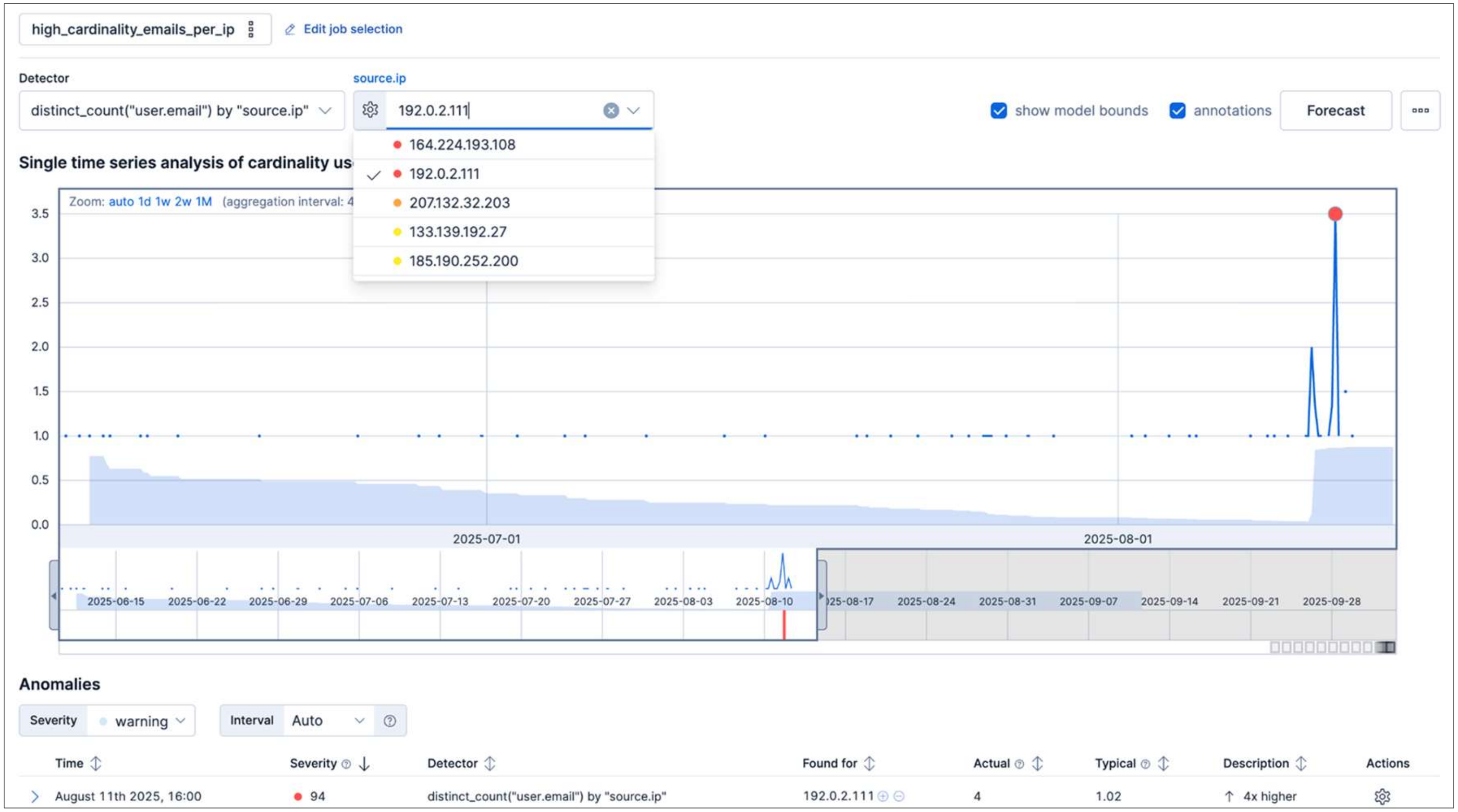
@timestamp	source.ip	user.email
Aug 12, 2025 @ 13:49:44.906	192.0.2.111	daniellehiggins@example.org
Aug 12, 2025 @ 12:11:57.024	192.0.2.111	brianna47@example.org
Aug 12, 2025 @ 05:24:49.602	192.0.2.111	james86@example.net
Aug 12, 2025 @ 04:31:44.760	192.0.2.111	ubrady@example.net
Aug 12, 2025 @ 04:20:46.760	192.0.2.111	yolandaramsey@example.com
Aug 11, 2025 @ 22:08:38.760	192.0.2.111	kimmark@example.com
Aug 11, 2025 @ 20:07:20.760	192.0.2.111	alexanderwheeler@example.com
Aug 11, 2025 @ 19:29:46.760	192.0.2.111	edwincole@example.net
Aug 11, 2025 @ 19:21:51.760	192.0.2.111	mathew46@example.net

Scene 2:

Backed by ML: This Isn’t Normal Behavior

Fraud Detection with Elastic

Scene 2: Backed by ML: This Isn’t Normal Behavior



Detector: distinct_count("user.email") by "source.ip"

source.ip: 192.0.2.111

Anomalies

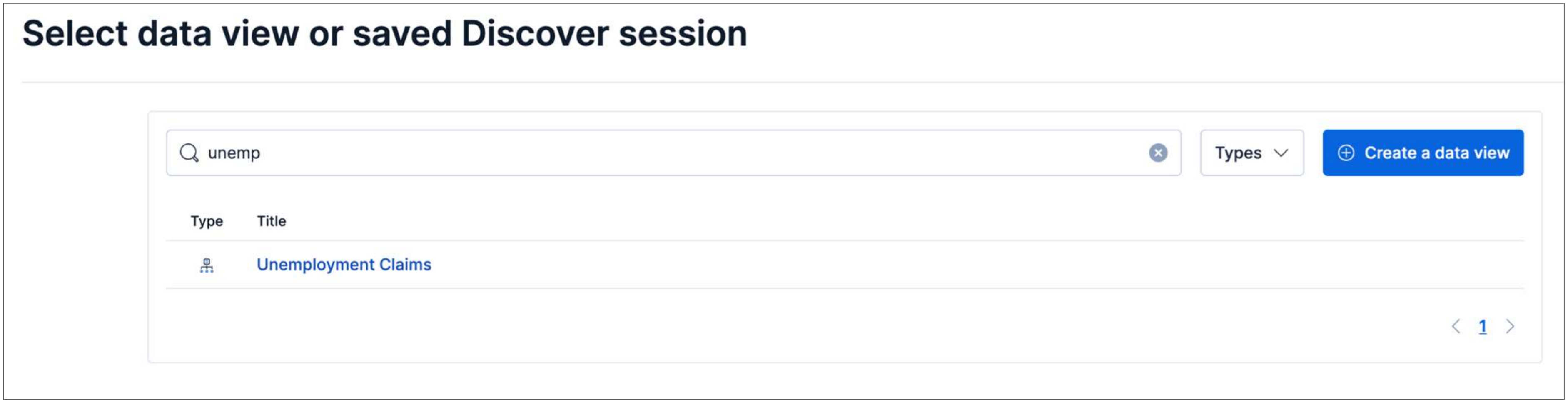
Severity: warning

Interval: Auto

Time	Severity	Detector	Found for	Actual	Typical	Description	Actions
August 11th 2025, 16:00	● 94	distinct_count("user.email") by "source.ip"	192.0.2.111	4	1.02	↑ 4x higher	

Fraud Detection with Elastic

Scene 2: Backed by ML: This Isn’t Normal Behavior

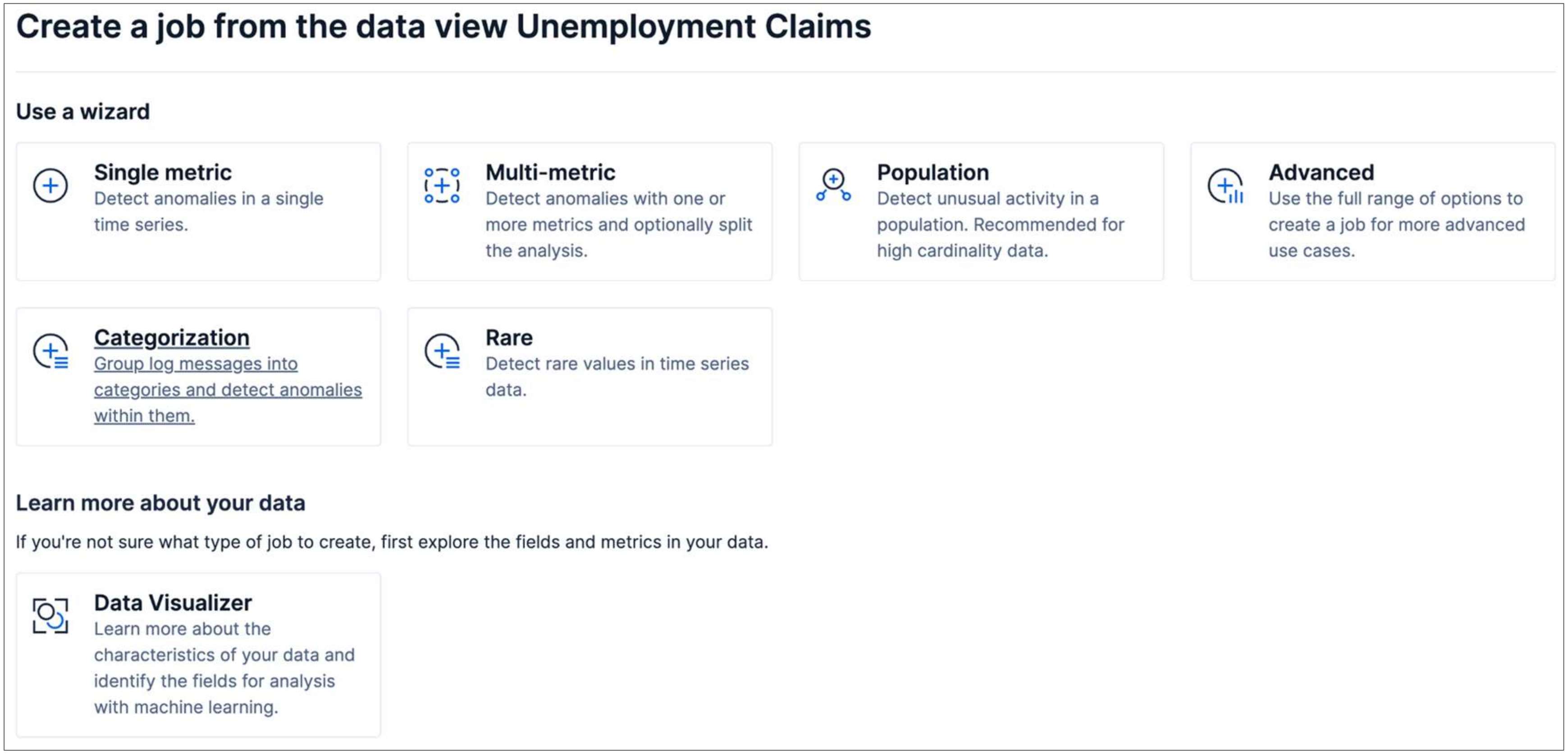


Select data view or saved Discover session

Type	Title
	Unemployment Claims

Fraud Detection with Elastic

Scene 2: Backed by ML: This Isn't Normal Behavior



Create a job from the data view Unemployment Claims

Use a wizard

Single metric
Detect anomalies in a single time series.

Multi-metric
Detect anomalies with one or more metrics and optionally split the analysis.

Population
Detect unusual activity in a population. Recommended for high cardinality data.

Advanced
Use the full range of options to create a job for more advanced use cases.

Categorization
Group log messages into categories and detect anomalies within them.

Rare
Detect rare values in time series data.

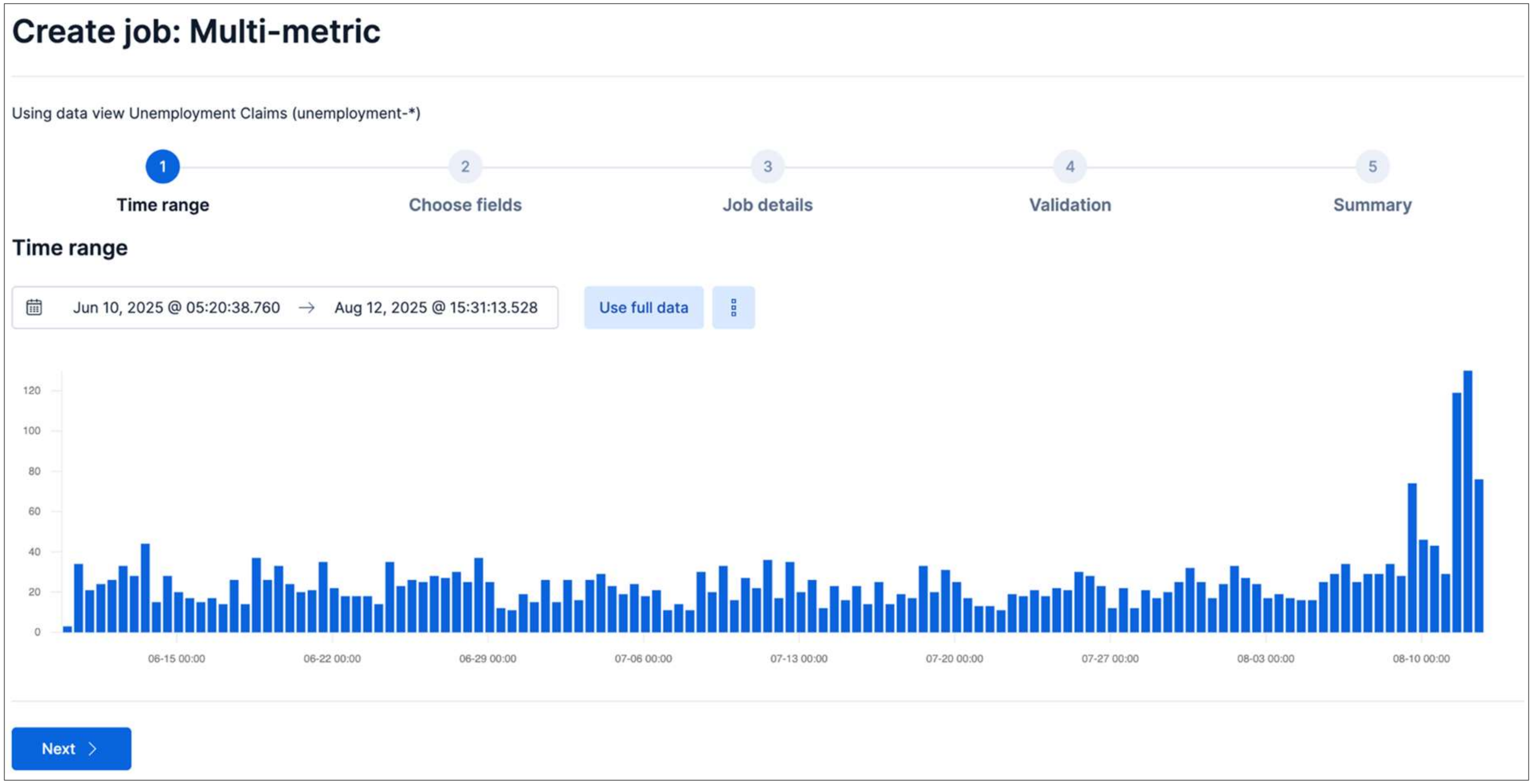
Learn more about your data

If you're not sure what type of job to create, first explore the fields and metrics in your data.

Data Visualizer
Learn more about the characteristics of your data and identify the fields for analysis with machine learning.

Fraud Detection with Elastic

Scene 2: Backed by ML: This Isn’t Normal Behavior



Create job: Multi-metric

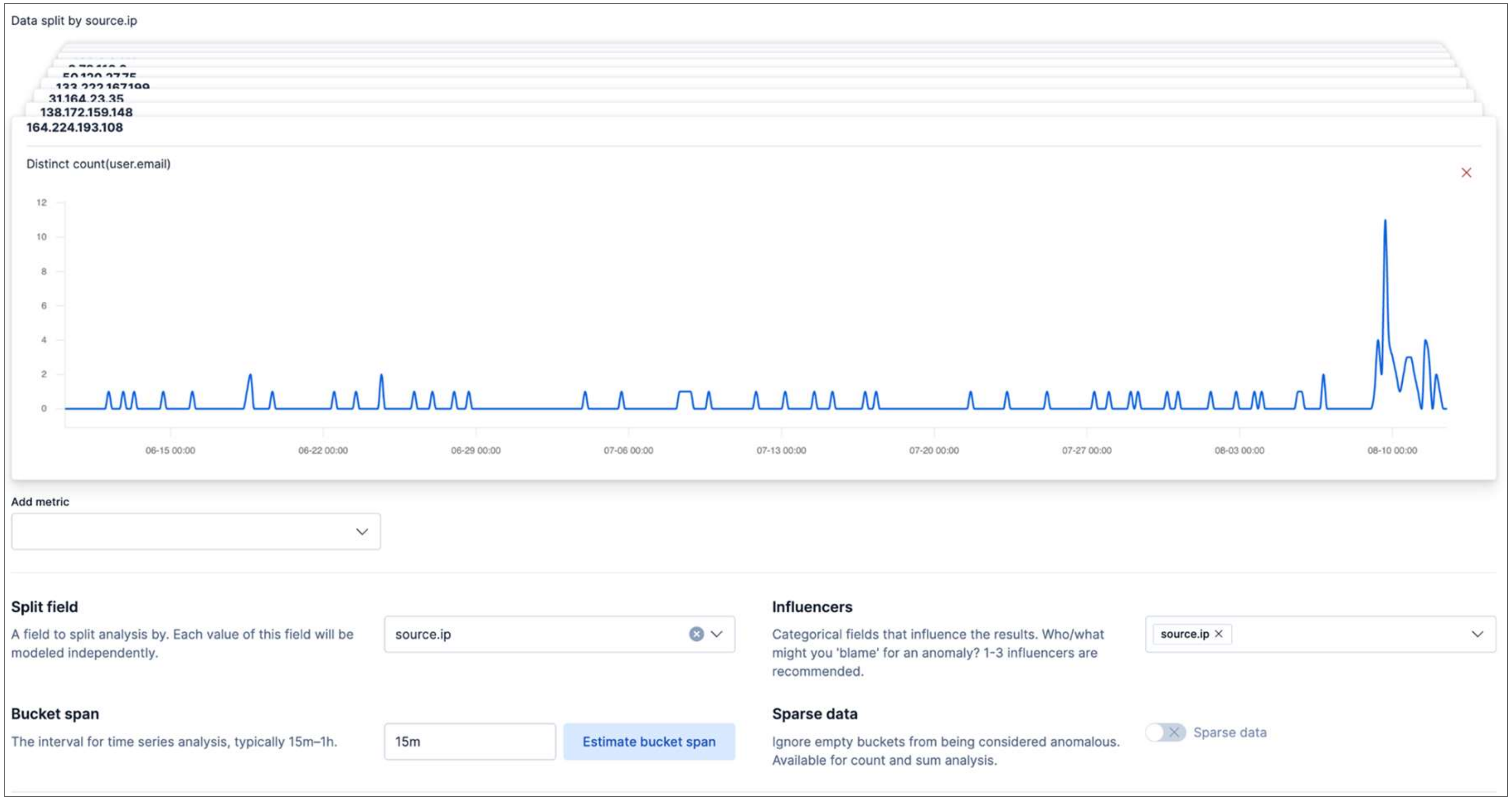
Using data view Unemployment Claims (unemployment-*)

Time range

Jun 10, 2025 @ 05:20:38.760 → Aug 12, 2025 @ 15:31:13.528

Fraud Detection with Elastic

Scene 2: Backed by ML: This Isn’t Normal Behavior



Data split by source.ip

31.164.23.35

138.172.159.148

164.224.193.108

Distinct count(user.email)

Add metric

Split field

A field to split analysis by. Each value of this field will be modeled independently.

source.ip

Influencers

Categorical fields that influence the results. Who/what might you 'blame' for an anomaly? 1-3 influencers are recommended.

source.ip ×

Bucket span

The interval for time series analysis, typically 15m–1h.

15m

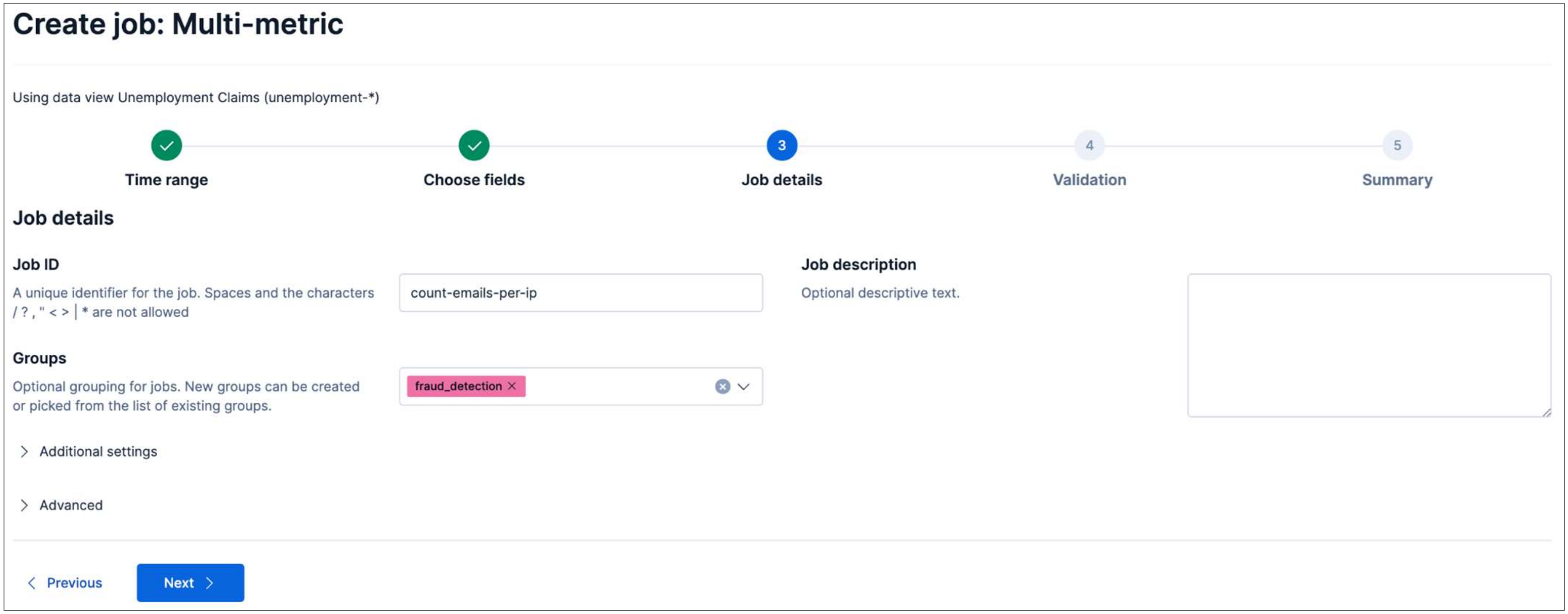
Sparse data

Ignore empty buckets from being considered anomalous. Available for count and sum analysis.

Sparse data

Fraud Detection with Elastic

Scene 2: Backed by ML: This Isn't Normal Behavior



Create job: Multi-metric

Using data view Unemployment Claims (unemployment-*)

Job details

Job ID
A unique identifier for the job. Spaces and the characters / ? , " < > | * are not allowed

count-emails-per-ip

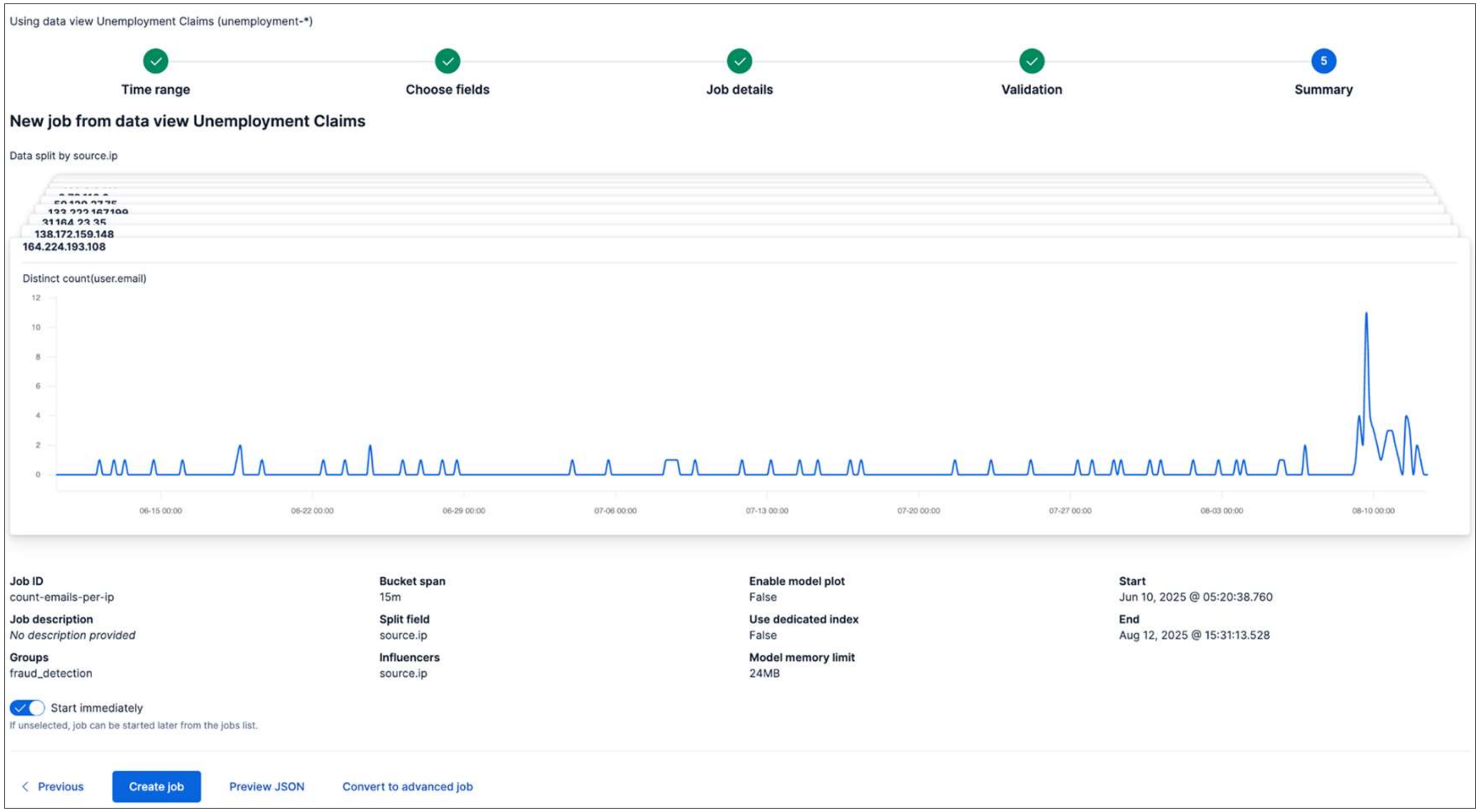
Groups
Optional grouping for jobs. New groups can be created or picked from the list of existing groups.

fraud_detection

Job description
Optional descriptive text.

Fraud Detection with Elastic

Scene 2: Backed by ML: This Isn’t Normal Behavior



Using data view Unemployment Claims (unemployment-*)

New job from data view Unemployment Claims

Data split by source.ip

Job ID
count-emails-per-ip

Job description
No description provided

Groups
fraud_detection

Bucket span
15m

Split field
source.ip

Influencers
source.ip

Enable model plot
False

Use dedicated index
False

Model memory limit
24MB

Start
Jun 10, 2025 @ 05:20:38.760

End
Aug 12, 2025 @ 15:31:13.528

☑ Start immediately
If unselected, job can be started later from the jobs list.

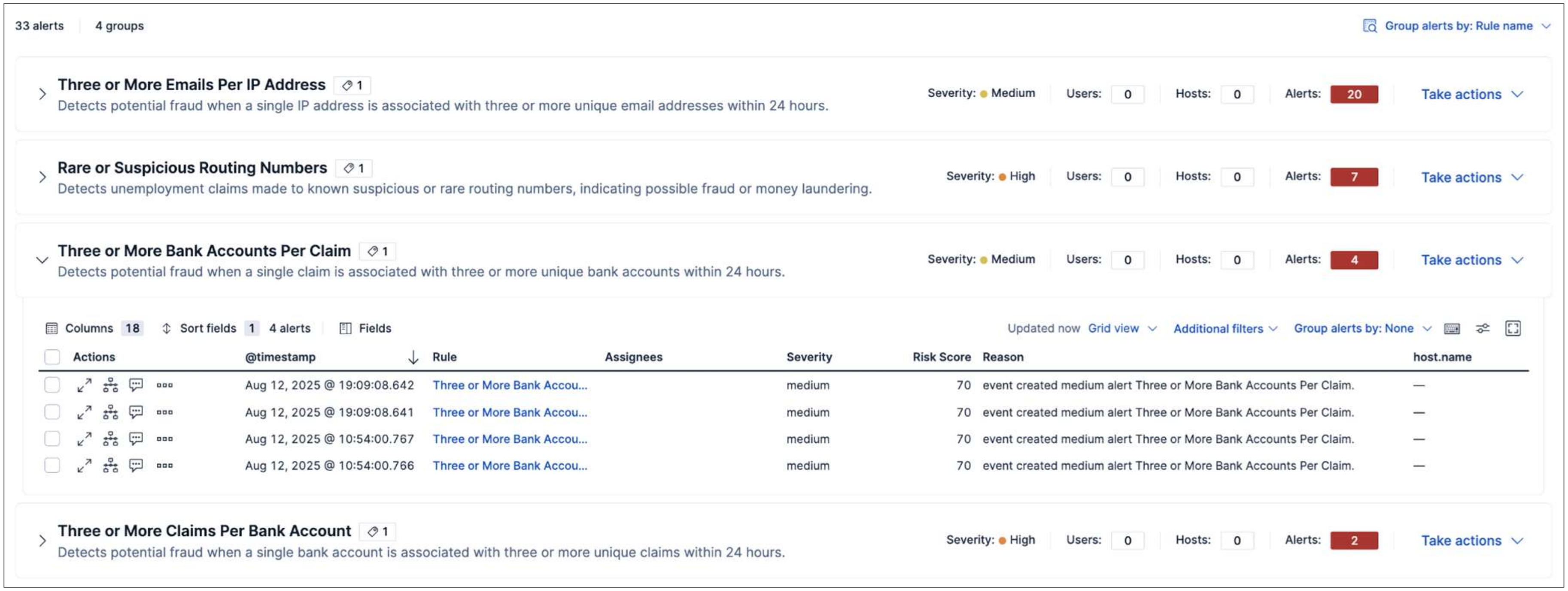
elastic

Scene 3:

Tracing the Web — Bank Account Reuse

Fraud Detection with Elastic

Scene 3: Tracing the Web — Bank Account Reuse



33 alerts | 4 groups

Three or More Emails Per IP Address 1
Detects potential fraud when a single IP address is associated with three or more unique email addresses within 24 hours.
Severity: Medium | Users: 0 | Hosts: 0 | Alerts: 20

Rare or Suspicious Routing Numbers 1
Detects unemployment claims made to known suspicious or rare routing numbers, indicating possible fraud or money laundering.
Severity: High | Users: 0 | Hosts: 0 | Alerts: 7

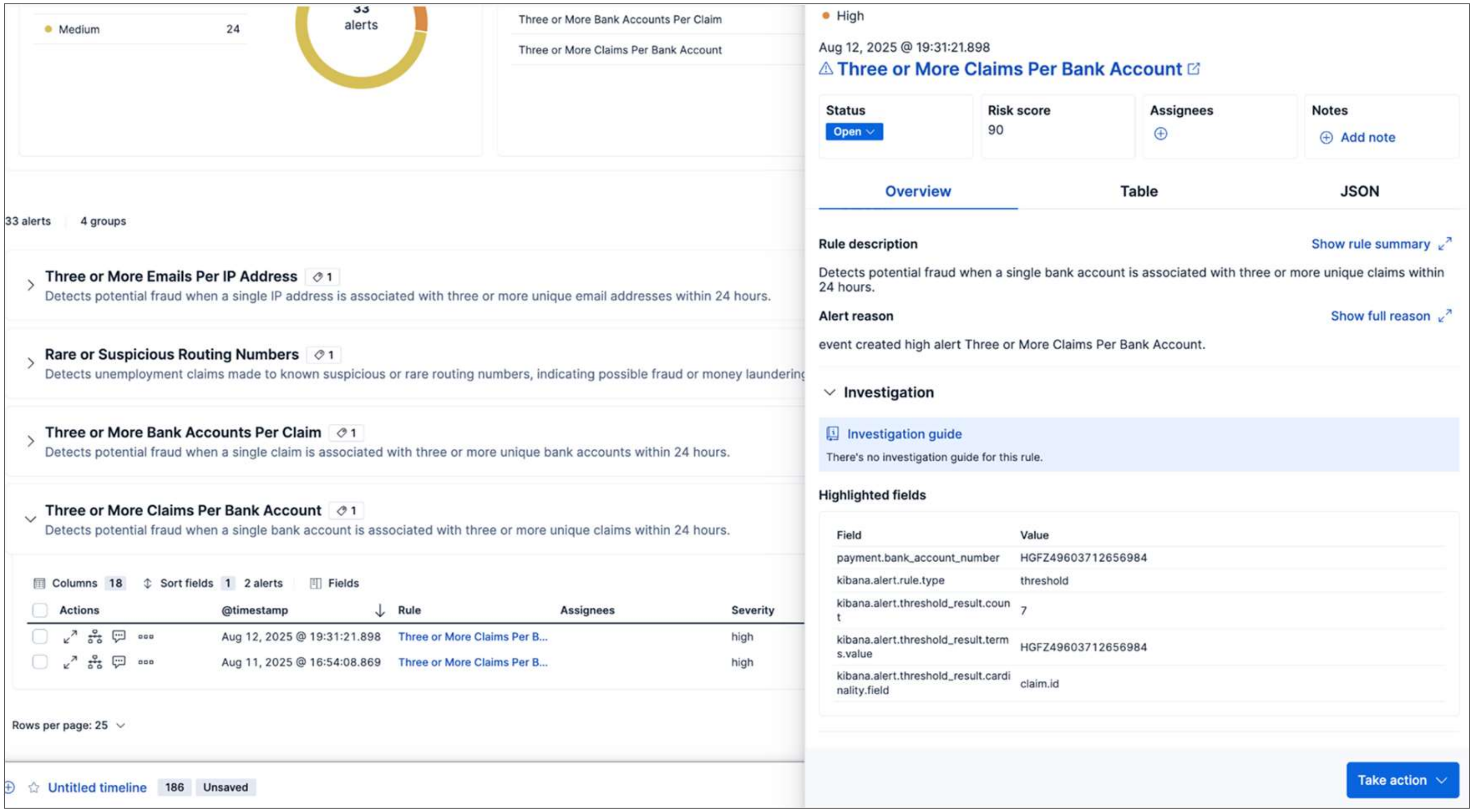
Three or More Bank Accounts Per Claim 1
Detects potential fraud when a single claim is associated with three or more unique bank accounts within 24 hours.
Severity: Medium | Users: 0 | Hosts: 0 | Alerts: 4

☐ Actions	@timestamp	Rule	Assignees	Severity	Risk Score	Reason	host.name
☐	Aug 12, 2025 @ 19:09:08.642	Three or More Bank Accou...		medium	70	event created medium alert Three or More Bank Accounts Per Claim.	—
☐	Aug 12, 2025 @ 19:09:08.641	Three or More Bank Accou...		medium	70	event created medium alert Three or More Bank Accounts Per Claim.	—
☐	Aug 12, 2025 @ 10:54:00.767	Three or More Bank Accou...		medium	70	event created medium alert Three or More Bank Accounts Per Claim.	—
☐	Aug 12, 2025 @ 10:54:00.766	Three or More Bank Accou...		medium	70	event created medium alert Three or More Bank Accounts Per Claim.	—

Three or More Claims Per Bank Account 1
Detects potential fraud when a single bank account is associated with three or more unique claims within 24 hours.
Severity: High | Users: 0 | Hosts: 0 | Alerts: 2

Fraud Detection with Elastic

Scene 3: Tracing the Web — Bank Account Reuse



Medium 24
33 alerts
Three or More Bank Accounts Per Claim
Three or More Claims Per Bank Account

33 alerts | 4 groups

Three or More Emails Per IP Address 1
Detects potential fraud when a single IP address is associated with three or more unique email addresses within 24 hours.

Rare or Suspicious Routing Numbers 1
Detects unemployment claims made to known suspicious or rare routing numbers, indicating possible fraud or money laundering

Three or More Bank Accounts Per Claim 1
Detects potential fraud when a single claim is associated with three or more unique bank accounts within 24 hours.

Three or More Claims Per Bank Account 1
Detects potential fraud when a single bank account is associated with three or more unique claims within 24 hours.

Columns 18 | Sort fields 1 | 2 alerts | Fields

☐	Actions	@timestamp	Rule	Assignees	Severity
☐		Aug 12, 2025 @ 19:31:21.898	Three or More Claims Per B...		high
☐		Aug 11, 2025 @ 16:54:08.869	Three or More Claims Per B...		high

Rows per page: 25

Untitled timeline 186 Unsaved

● High

Aug 12, 2025 @ 19:31:21.898

Three or More Claims Per Bank Account

Status	Risk score	Assignees	Notes
Open	90		Add note

Rule description

Show rule summary

Detects potential fraud when a single bank account is associated with three or more unique claims within 24 hours.

Alert reason

Show full reason

event created high alert Three or More Claims Per Bank Account.

Investigation

Investigation guide

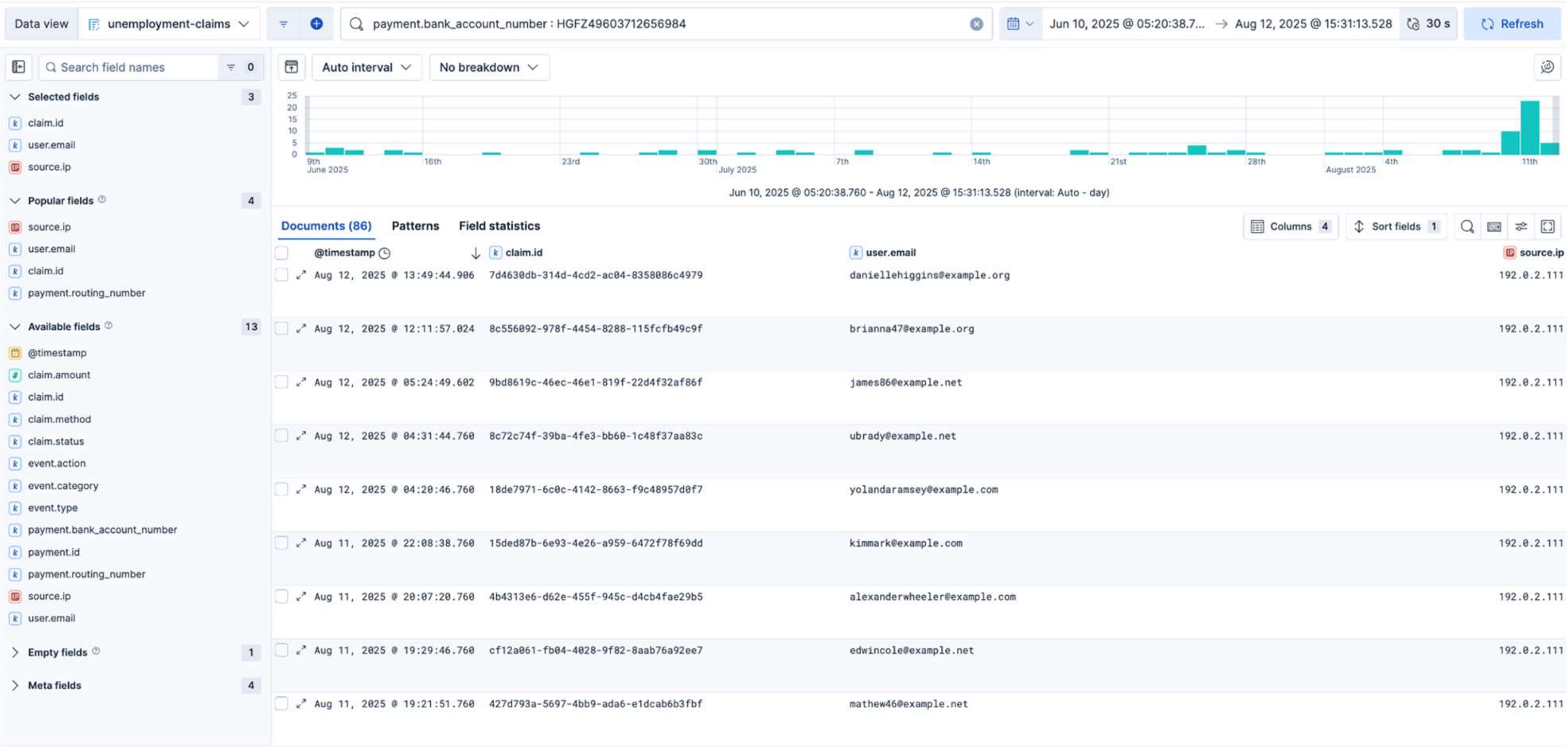
There's no investigation guide for this rule.

Highlighted fields

Field	Value
payment.bank_account_number	HGFZ49603712656984
kibana.alert.rule.type	threshold
kibana.alert.threshold_result.count	7
kibana.alert.threshold_result.terms.value	HGFZ49603712656984
kibana.alert.threshold_result.cardinality.field	claim.id

Fraud Detection with Elastic

Scene 3: Tracing the Web — Bank Account Reuse



payment.bank_account_number : HGFZ49603712656984

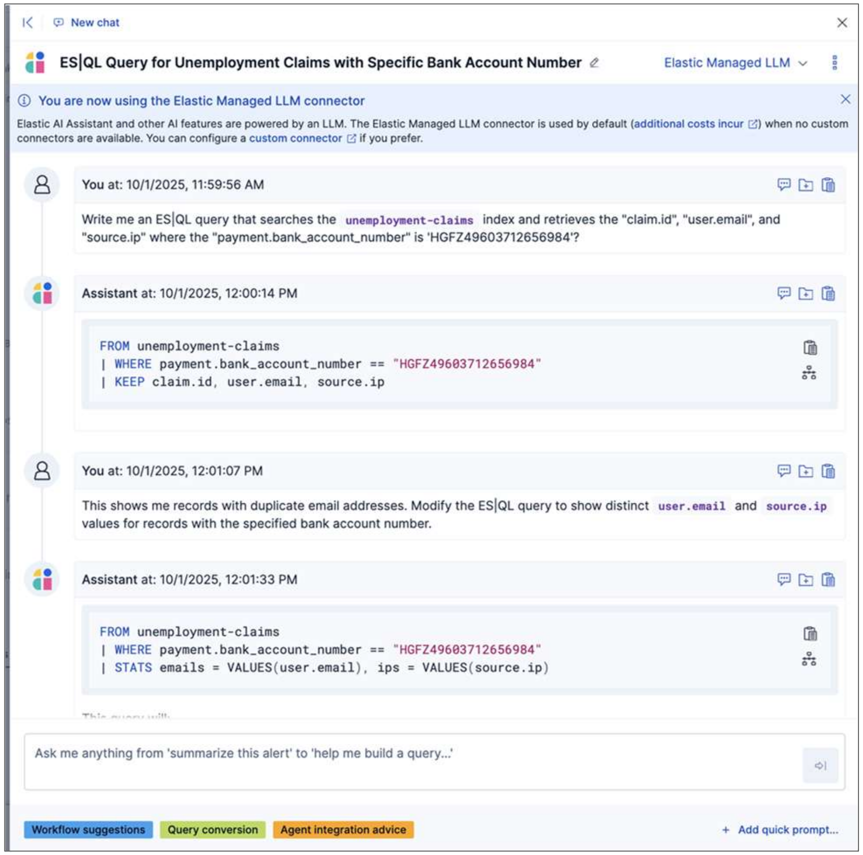
Jun 10, 2025 @ 05:20:38.7... → Aug 12, 2025 @ 15:31:13.528

Jun 10, 2025 @ 05:20:38.760 - Aug 12, 2025 @ 15:31:13.528 (interval: Auto - day)

@timestamp	claim.id	user.email	source.ip
Aug 12, 2025 @ 13:49:44.906	7d4630db-314d-4cd2-ac04-8358086c4979	daniellehiggins@example.org	192.0.2.111
Aug 12, 2025 @ 12:11:57.024	8c556092-978f-4454-8288-115fcfb49c9f	brianna47@example.org	192.0.2.111
Aug 12, 2025 @ 05:24:49.602	9bd8619c-46ec-46e1-819f-22d4f32af86f	james86@example.net	192.0.2.111
Aug 12, 2025 @ 04:31:44.760	8c72c74f-39ba-4fe3-bb60-1c48f37aa83c	ubrady@example.net	192.0.2.111
Aug 12, 2025 @ 04:20:46.760	18de7971-6c0c-4142-8663-f9c48957d0f7	yolandaramsey@example.com	192.0.2.111
Aug 11, 2025 @ 22:08:38.760	15ded87b-6e93-4e26-a959-6472f78f69dd	kimmark@example.com	192.0.2.111
Aug 11, 2025 @ 20:07:20.760	4b4313e6-d62e-455f-945c-d4cb4fae29b5	alexanderwheeler@example.com	192.0.2.111
Aug 11, 2025 @ 19:29:46.760	cf12a061-fb04-4028-9f82-8aab76a92ee7	edwincole@example.net	192.0.2.111
Aug 11, 2025 @ 19:21:51.760	427d793a-5697-4bb9-ada6-e1dcab6b3fbf	mathew46@example.net	192.0.2.111

Fraud Detection with Elastic

Scene 3: Tracing the Web — Bank Account Reuse


New chat
ES|QL Query for Unemployment Claims with Specific Bank Account Number
Elastic Managed LLM

You are now using the Elastic Managed LLM connector

Elastic AI Assistant and other AI features are powered by an LLM. The Elastic Managed LLM connector is used by default (additional costs incur) when no custom connectors are available. You can configure a custom connector if you prefer.

You at: 10/1/2025, 11:59:56 AM

Write me an ES|QL query that searches the `unemployment-claims` index and retrieves the "claim.id", "user.email", and "source.ip" where the "payment.bank_account_number" is 'HGFZ49603712656984'?

Assistant at: 10/1/2025, 12:00:14 PM

```
FROM unemployment-claims
| WHERE payment.bank_account_number == "HGFZ49603712656984"
| KEEP claim.id, user.email, source.ip
```

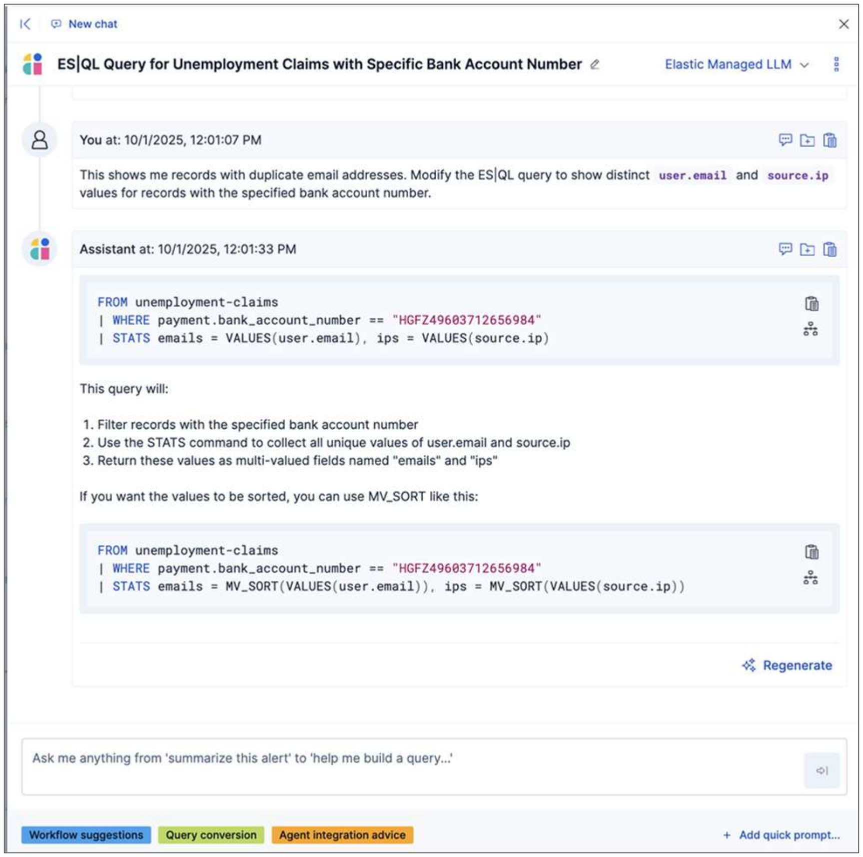
You at: 10/1/2025, 12:01:07 PM

This shows me records with duplicate email addresses. Modify the ES|QL query to show distinct `user.email` and `source.ip` values for records with the specified bank account number.

Assistant at: 10/1/2025, 12:01:33 PM

```
FROM unemployment-claims
| WHERE payment.bank_account_number == "HGFZ49603712656984"
| STATS emails = VALUES(user.email), ips = VALUES(source.ip)
```

Ask me anything from 'summarize this alert' to 'help me build a query...'
Workflow suggestions
Query conversion
Agent integration advice
+ Add quick prompt...


New chat
ES|QL Query for Unemployment Claims with Specific Bank Account Number
Elastic Managed LLM

You at: 10/1/2025, 12:01:07 PM

This shows me records with duplicate email addresses. Modify the ES|QL query to show distinct `user.email` and `source.ip` values for records with the specified bank account number.

Assistant at: 10/1/2025, 12:01:33 PM

```
FROM unemployment-claims
| WHERE payment.bank_account_number == "HGFZ49603712656984"
| STATS emails = VALUES(user.email), ips = VALUES(source.ip)
```

This query will:

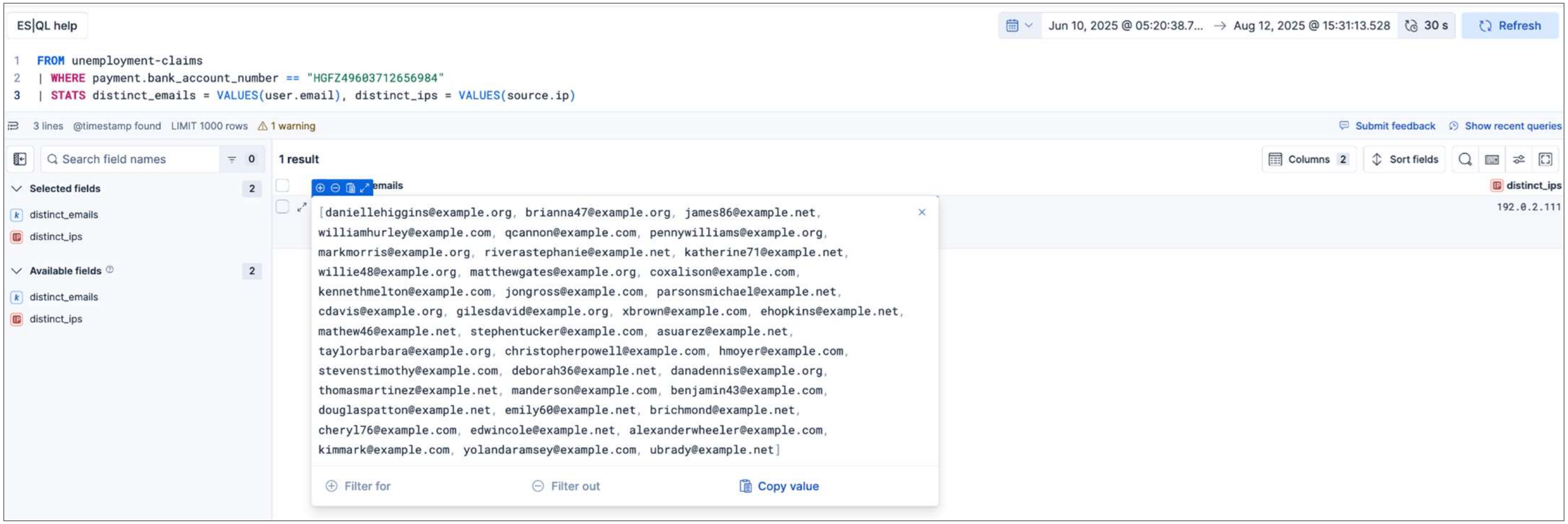
1. Filter records with the specified bank account number
2. Use the STATS command to collect all unique values of user.email and source.ip
3. Return these values as multi-valued fields named "emails" and "ips"

If you want the values to be sorted, you can use MV_SORT like this:

```
FROM unemployment-claims
| WHERE payment.bank_account_number == "HGFZ49603712656984"
| STATS emails = MV_SORT(VALUES(user.email)), ips = MV_SORT(VALUES(source.ip))
```

Fraud Detection with Elastic

Scene 3: Tracing the Web — Bank Account Reuse



```
FROM unemployment-claims
| WHERE payment.bank_account_number == "HGFZ49603712656984"
| STATS distinct_emails = VALUES(user.email), distinct_ips = VALUES(source.ip)
```

```
[daniellehiggins@example.org, brianna47@example.org, james86@example.net,
williamhurley@example.com, qcannon@example.com, pennywilliams@example.org,
markmorris@example.org, riverastephanie@example.net, katherine71@example.net,
willie48@example.org, matthewgates@example.org, coxalison@example.com,
kennethmelton@example.com, jongross@example.com, parsonsmichael@example.net,
cdavis@example.org, gilesdavid@example.org, xbrown@example.com, ehopkins@example.net,
mathew46@example.net, stephentucker@example.com, asuarez@example.net,
taylorbarbara@example.org, christopherpowell@example.com, hmoyer@example.com,
stevenstimothy@example.com, deborah36@example.net, danadennis@example.org,
thomasmartinez@example.net, manderson@example.com, benjamin43@example.com,
douglaspatton@example.net, emily60@example.net, brichmond@example.net,
cheryl76@example.com, edwincole@example.net, alexanderwheeler@example.com,
kimmark@example.com, yolandaramsey@example.com, ubrady@example.net]
```

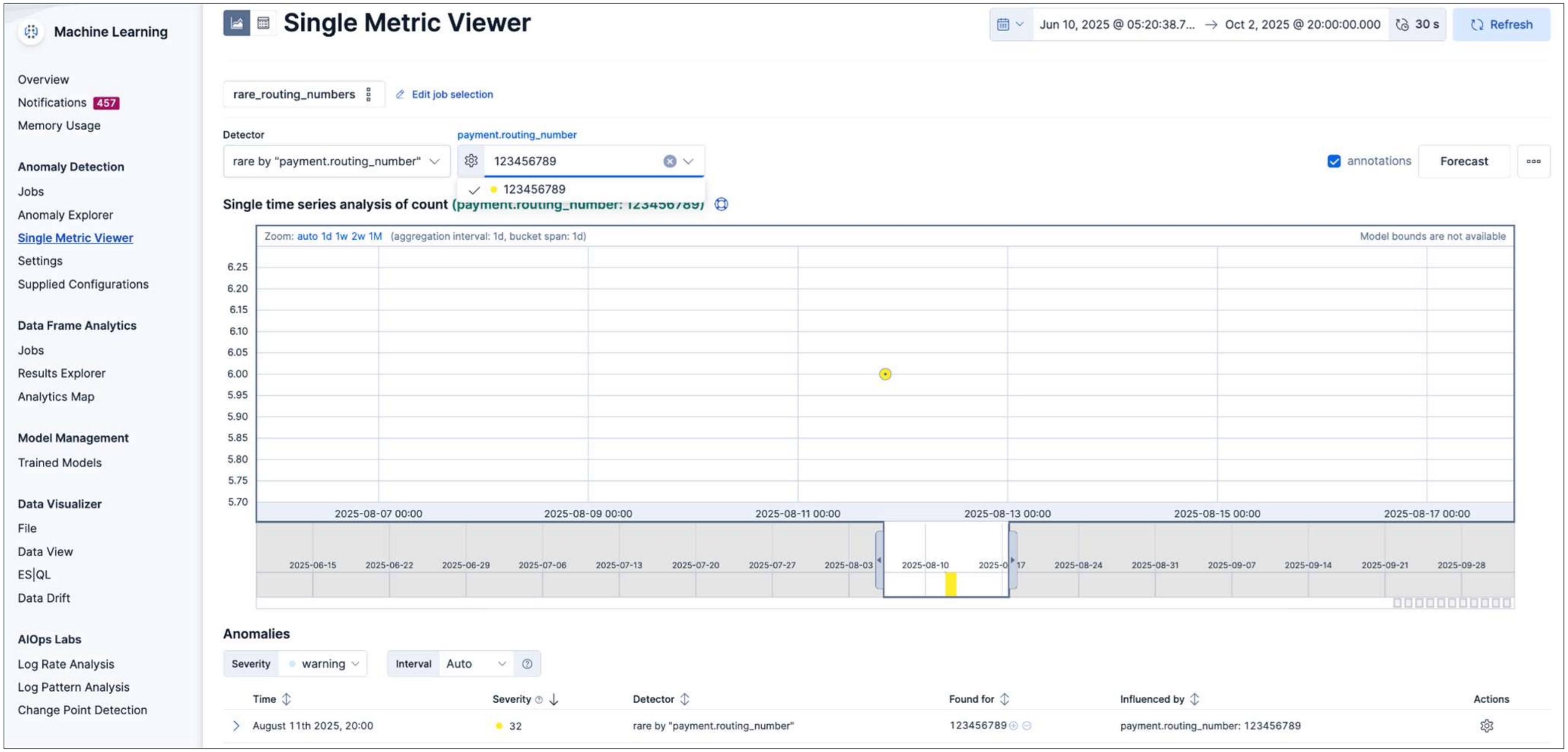
```
192.0.2.111
```

Scene 4:

A Rare Routing Number Emerges

Fraud Detection with Elastic

Scene 4: A Rare Routing Number Emerges



Jun 10, 2025 @ 05:20:38.7… → Oct 2, 2025 @ 20:00:00.000 30 s

rare_routing_numbers

Detector: rare by "payment.routing_number"

payment.routing_number: 123456789

☑ annotations

Single time series analysis of count (payment.routing_number: 123456789)

(aggregation interval: 1d, bucket span: 1d)

Anomalies

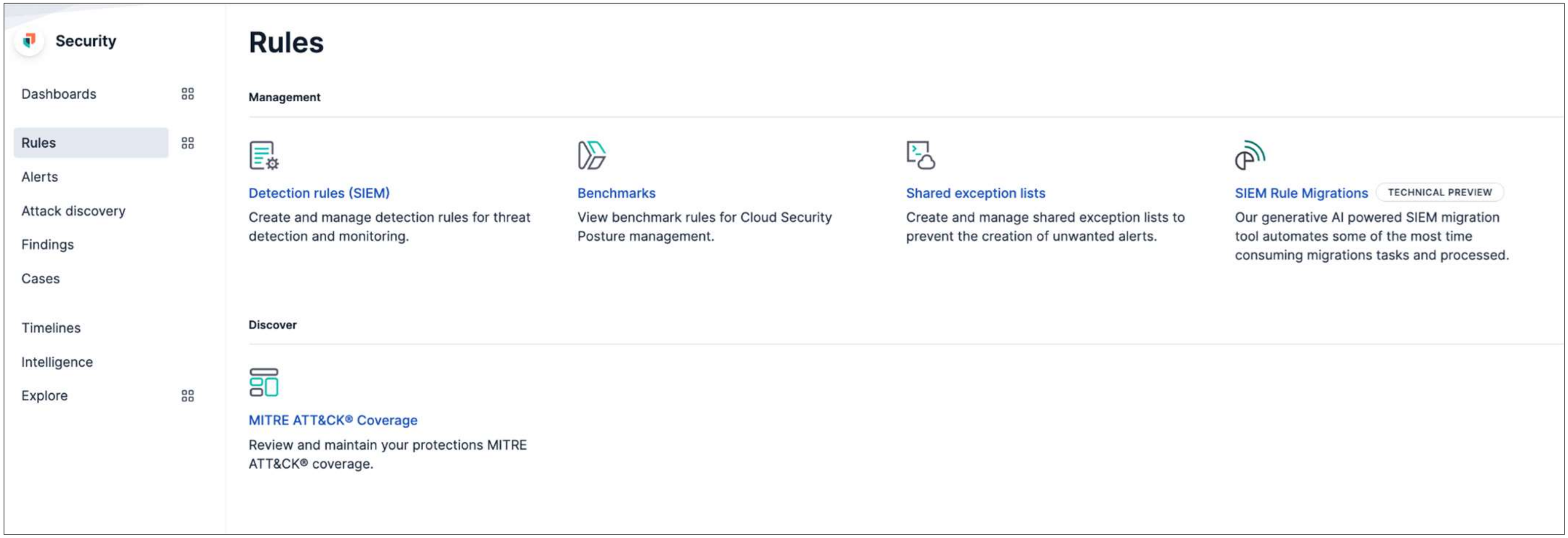
Severity: warning

Interval: Auto

Time	Severity	Detector	Found for	Influenced by	Actions
August 11th 2025, 20:00	● 32	rare by "payment.routing_number"	123456789	payment.routing_number: 123456789	

Fraud Detection with Elastic

Scene 4: A Rare Routing Number Emerges



Rules

Management

Detection rules (SIEM)

Create and manage detection rules for threat detection and monitoring.

Benchmarks

View benchmark rules for Cloud Security Posture management.

Shared exception lists

Create and manage shared exception lists to prevent the creation of unwanted alerts.

SIEM Rule Migrations TECHNICAL PREVIEW

Our generative AI powered SIEM migration tool automates some of the most time consuming migrations tasks and processed.

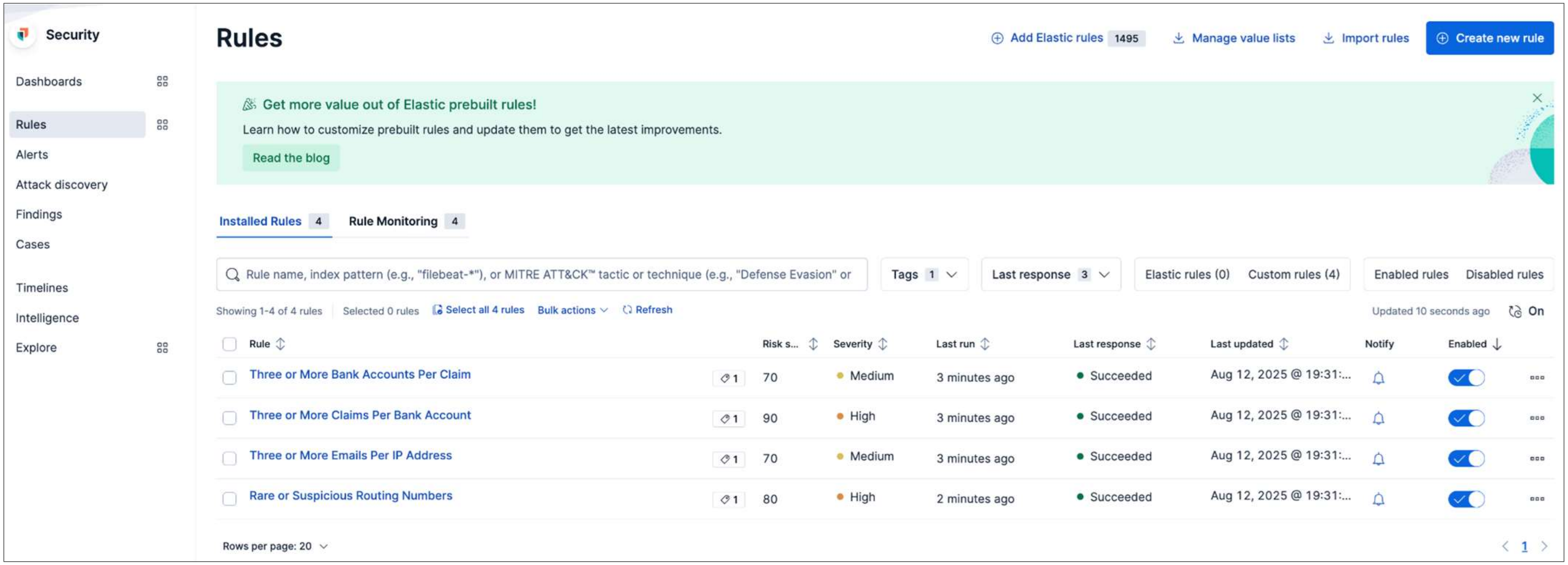
Discover

MITRE ATT&CK® Coverage

Review and maintain your protections MITRE ATT&CK® coverage.

Fraud Detection with Elastic

Scene 4: A Rare Routing Number Emerges



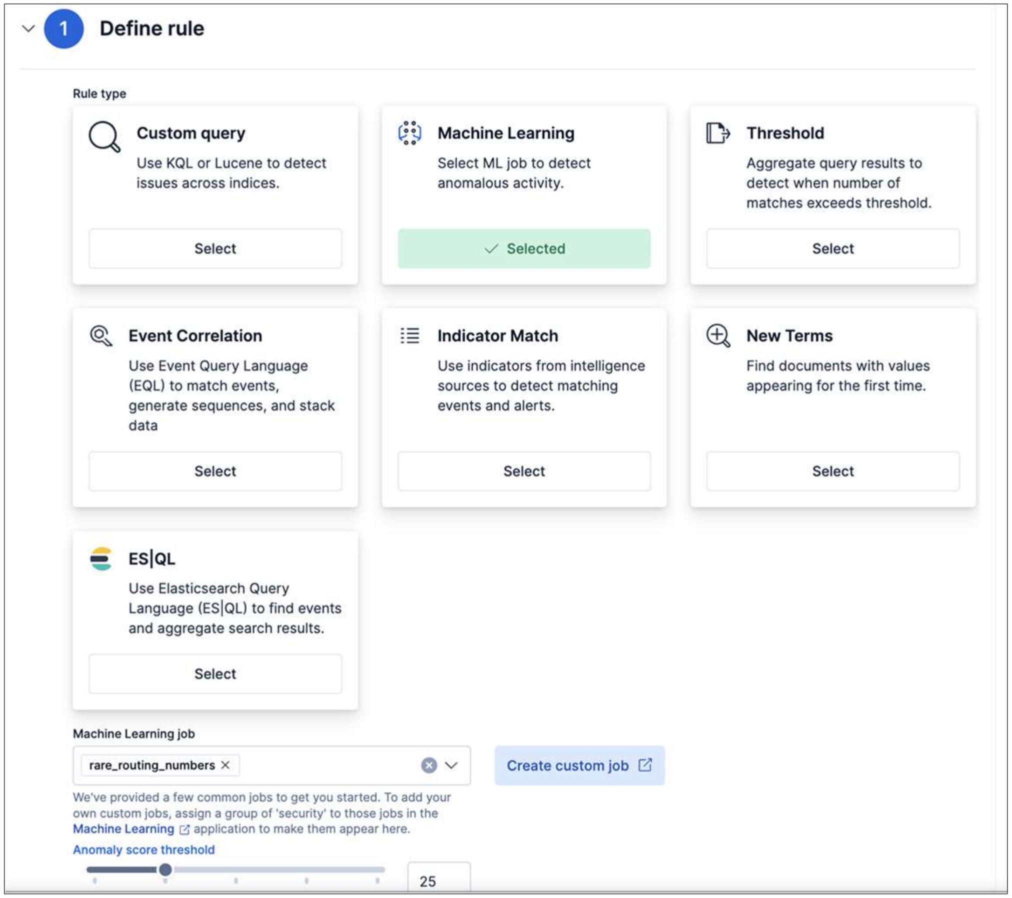
Get more value out of Elastic prebuilt rules!

Learn how to customize prebuilt rules and update them to get the latest improvements.

Rule		Risk s...	Severity	Last run	Last response	Last updated
Three or More Bank Accounts Per Claim	1	70	Medium	3 minutes ago	Succeeded	Aug 12, 2025 @ 19:31:...
Three or More Claims Per Bank Account	1	90	High	3 minutes ago	Succeeded	Aug 12, 2025 @ 19:31:...
Three or More Emails Per IP Address	1	70	Medium	3 minutes ago	Succeeded	Aug 12, 2025 @ 19:31:...
Rare or Suspicious Routing Numbers	1	80	High	2 minutes ago	Succeeded	Aug 12, 2025 @ 19:31:...

Fraud Detection with Elastic

Scene 4: A Rare Routing Number Emerges



Define rule

Rule type

Custom query
Use KQL or Lucene to detect issues across indices.
Select

Machine Learning
Select ML job to detect anomalous activity.
✓ Selected

Threshold
Aggregate query results to detect when number of matches exceeds threshold.
Select

Event Correlation
Use Event Query Language (EQL) to match events, generate sequences, and stack data
Select

Indicator Match
Use indicators from intelligence sources to detect matching events and alerts.
Select

New Terms
Find documents with values appearing for the first time.
Select

ES|QL
Use Elasticsearch Query Language (ES|QL) to find events and aggregate search results.
Select

Machine Learning job: rare_routing_numbers

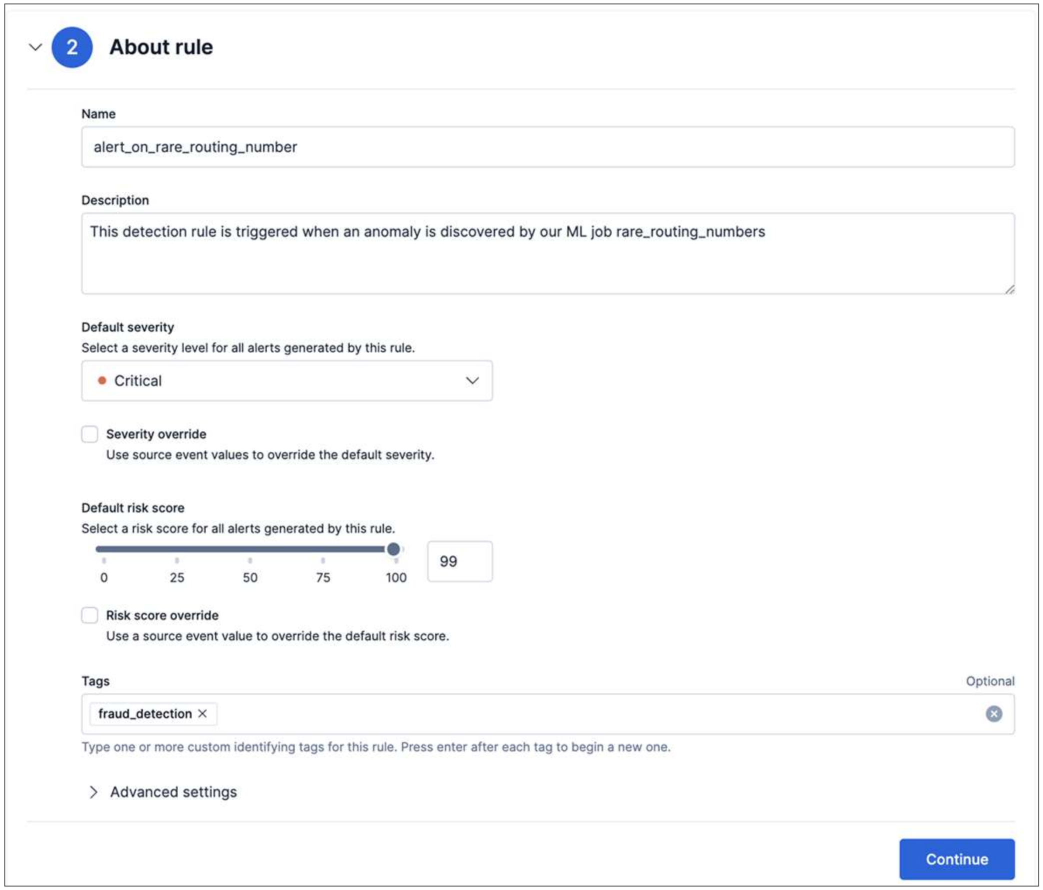
Create custom job

We've provided a few common jobs to get you started. To add your own custom jobs, assign a group of 'security' to those jobs in the Machine Learning application to make them appear here.

Anomaly score threshold: 25

Fraud Detection with Elastic

Scene 4: A Rare Routing Number Emerges



Name: alert_on_rare_routing_number

Description: This detection rule is triggered when an anomaly is discovered by our ML job rare_routing_numbers

Default severity
Select a severity level for all alerts generated by this rule.
● Critical

☐ Severity override
Use source event values to override the default severity.

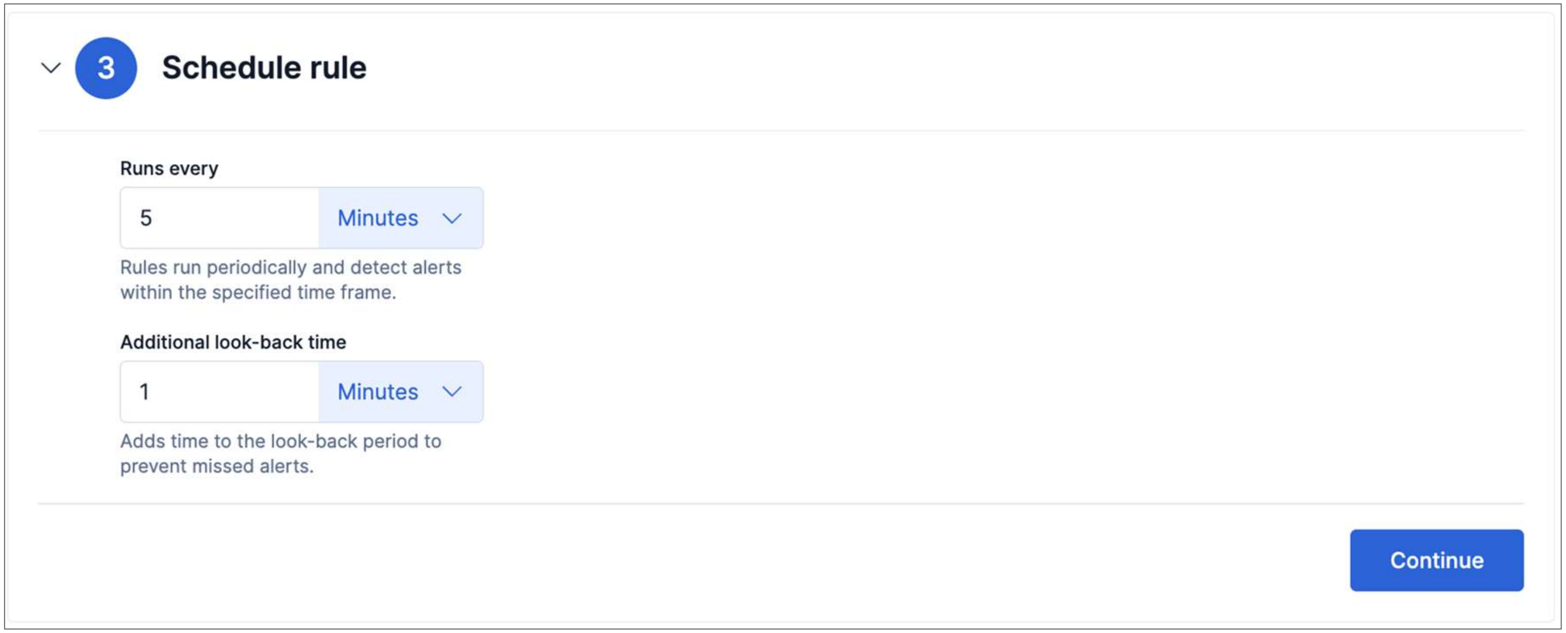
Default risk score
Select a risk score for all alerts generated by this rule.
99

☐ Risk score override
Use a source event value to override the default risk score.

Tags (Optional): fraud_detection
Type one or more custom identifying tags for this rule. Press enter after each tag to begin a new one.

Fraud Detection with Elastic

Scene 4: A Rare Routing Number Emerges



Runs every: 5 Minutes

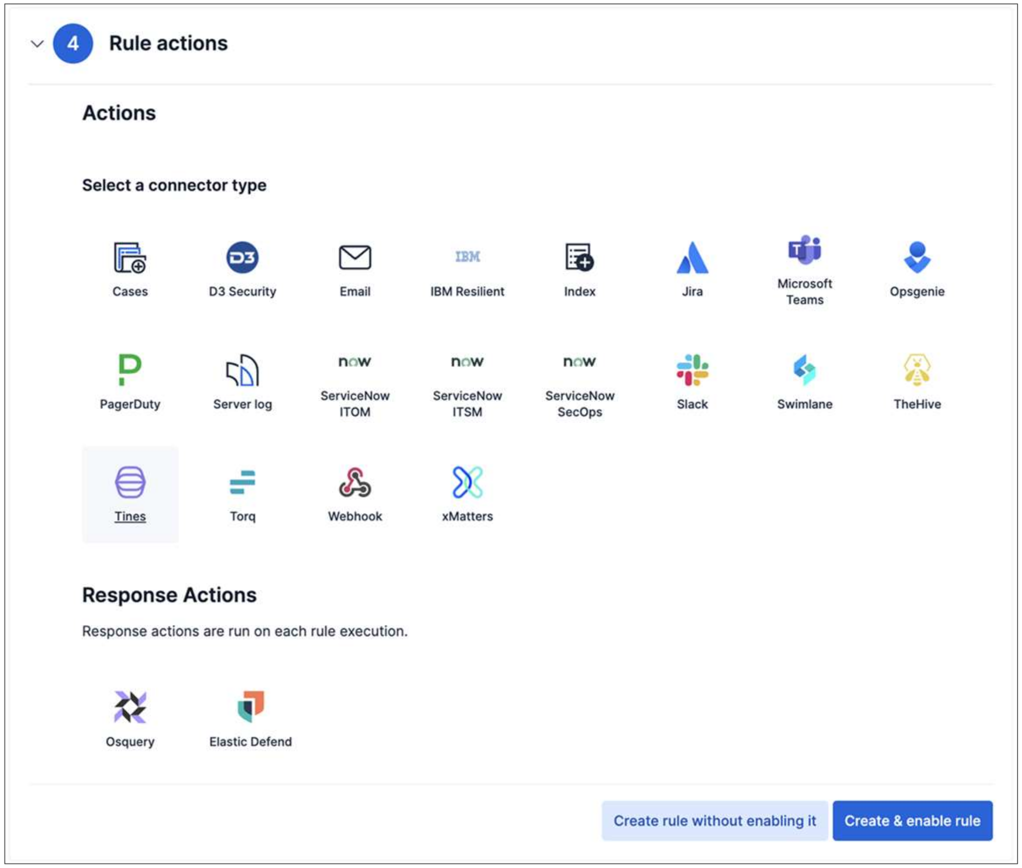
Rules run periodically and detect alerts within the specified time frame.

Additional look-back time: 1 Minutes

Adds time to the look-back period to prevent missed alerts.

Fraud Detection with Elastic

Scene 4: A Rare Routing Number Emerges

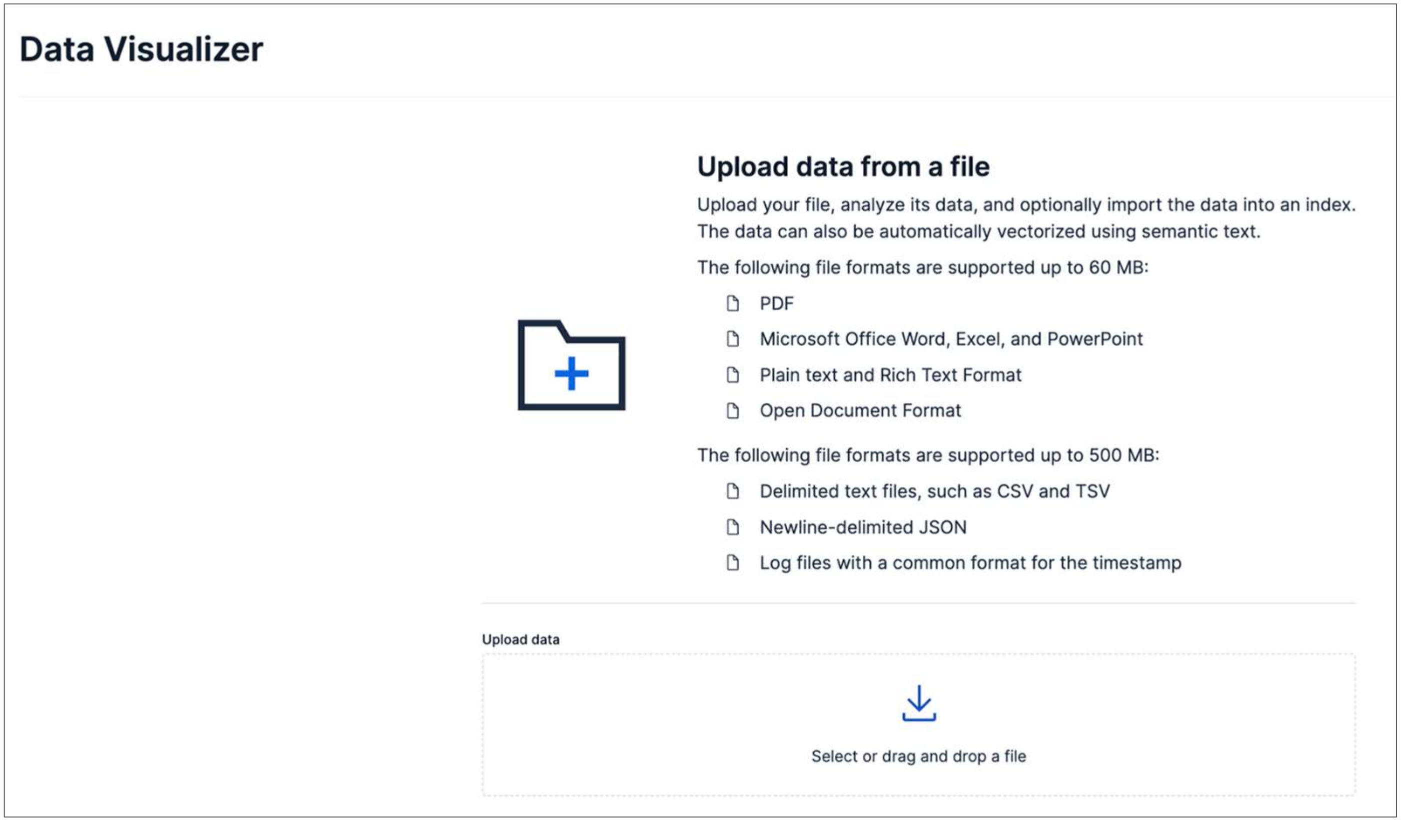


Scene 5:

A Call from Medicare

Fraud Detection with Elastic

Scene 5: A Call from Medicare



Data Visualizer

Upload data from a file

Upload your file, analyze its data, and optionally import the data into an index. The data can also be automatically vectorized using semantic text.

The following file formats are supported up to 60 MB:

- PDF
- Microsoft Office Word, Excel, and PowerPoint
- Plain text and Rich Text Format
- Open Document Format

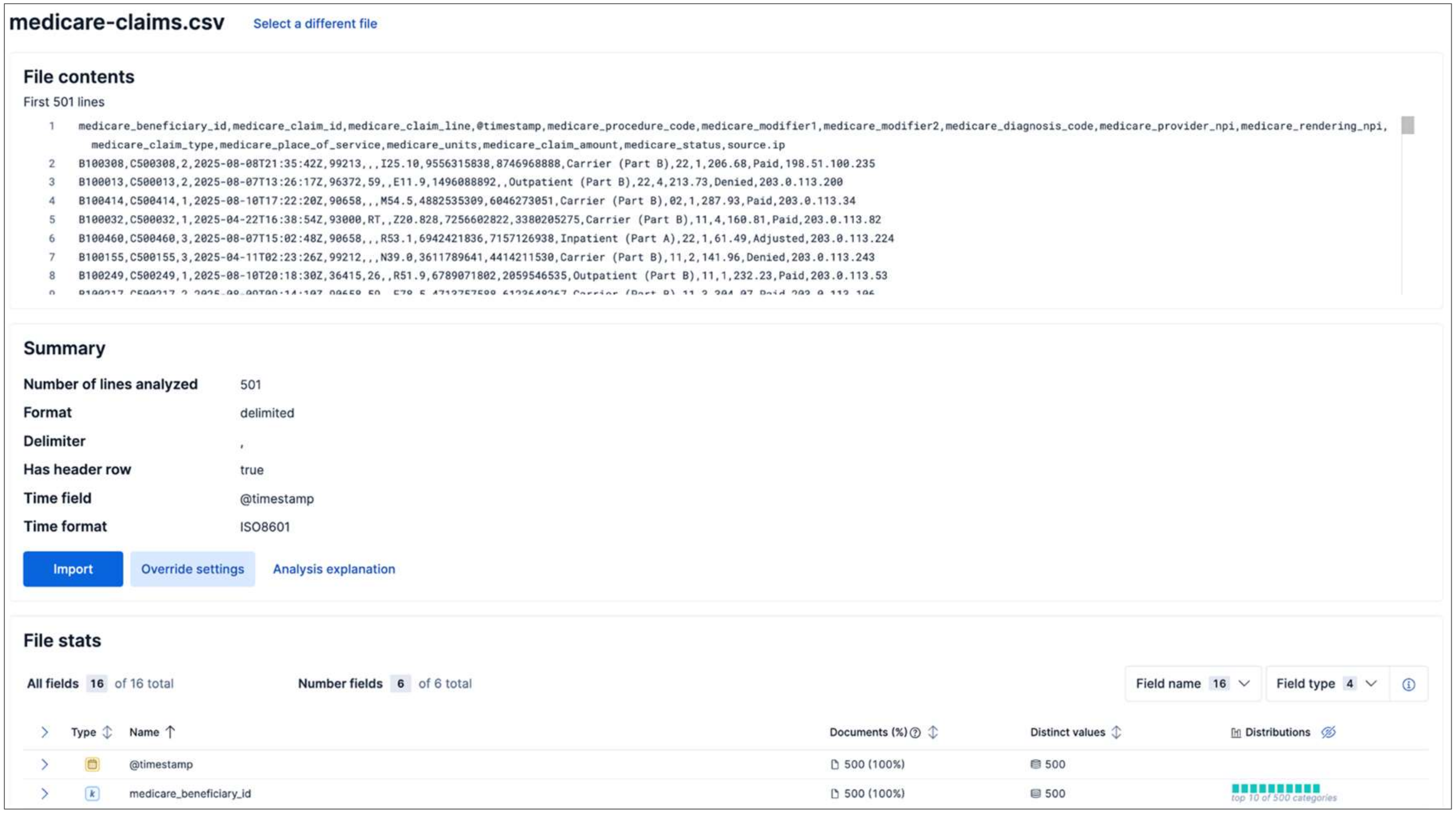
The following file formats are supported up to 500 MB:

- Delimited text files, such as CSV and TSV
- Newline-delimited JSON
- Log files with a common format for the timestamp

Upload data

Fraud Detection with Elastic

Scene 5: A Call from Medicare



medicare-claims.csv Select a different file

File contents

First 501 lines

```
medicare_beneficiary_id,medicare_claim_id,medicare_claim_line,@timestamp,medicare_procedure_code,medicare_modifier1,medicare_modifier2,medicare_diagnosis_code,medicare_provider_npi,medicare_rendering_npi,
  medicare_claim_type,medicare_place_of_service,medicare_units,medicare_claim_amount,medicare_status,source.ip
B100308,C500308,2,2025-08-08T21:35:42Z,99213,,,I25.10,9556315838,8746968888,Carrier (Part B),22,1,206.68,Paid,198.51.100.235
B100013,C500013,2,2025-08-07T13:26:17Z,96372,59,,E11.9,1496088892,,Outpatient (Part B),22,4,213.73,Denied,203.0.113.200
B100414,C500414,1,2025-08-10T17:22:20Z,90658,,,M54.5,4882535309,6046273051,Carrier (Part B),02,1,287.93,Paid,203.0.113.34
B100032,C500032,1,2025-04-22T16:38:54Z,93000,RT,,Z20.828,7256602822,3380205275,Carrier (Part B),11,4,160.81,Paid,203.0.113.82
B100460,C500460,3,2025-08-07T15:02:48Z,90658,,,R53.1,6942421836,7157126938,Inpatient (Part A),22,1,61.49,Adjusted,203.0.113.224
B100155,C500155,3,2025-04-11T02:23:26Z,99212,,,N39.0,3611789641,4414211530,Carrier (Part B),11,2,141.96,Denied,203.0.113.243
B100249,C500249,1,2025-08-10T20:18:30Z,36415,26,,R51.9,6789071802,2059546535,Outpatient (Part B),11,1,232.23,Paid,203.0.113.53
```

Summary

Number of lines analyzed	501
Format	delimited
Delimiter	,
Has header row	true
Time field	@timestamp
Time format	ISO8601

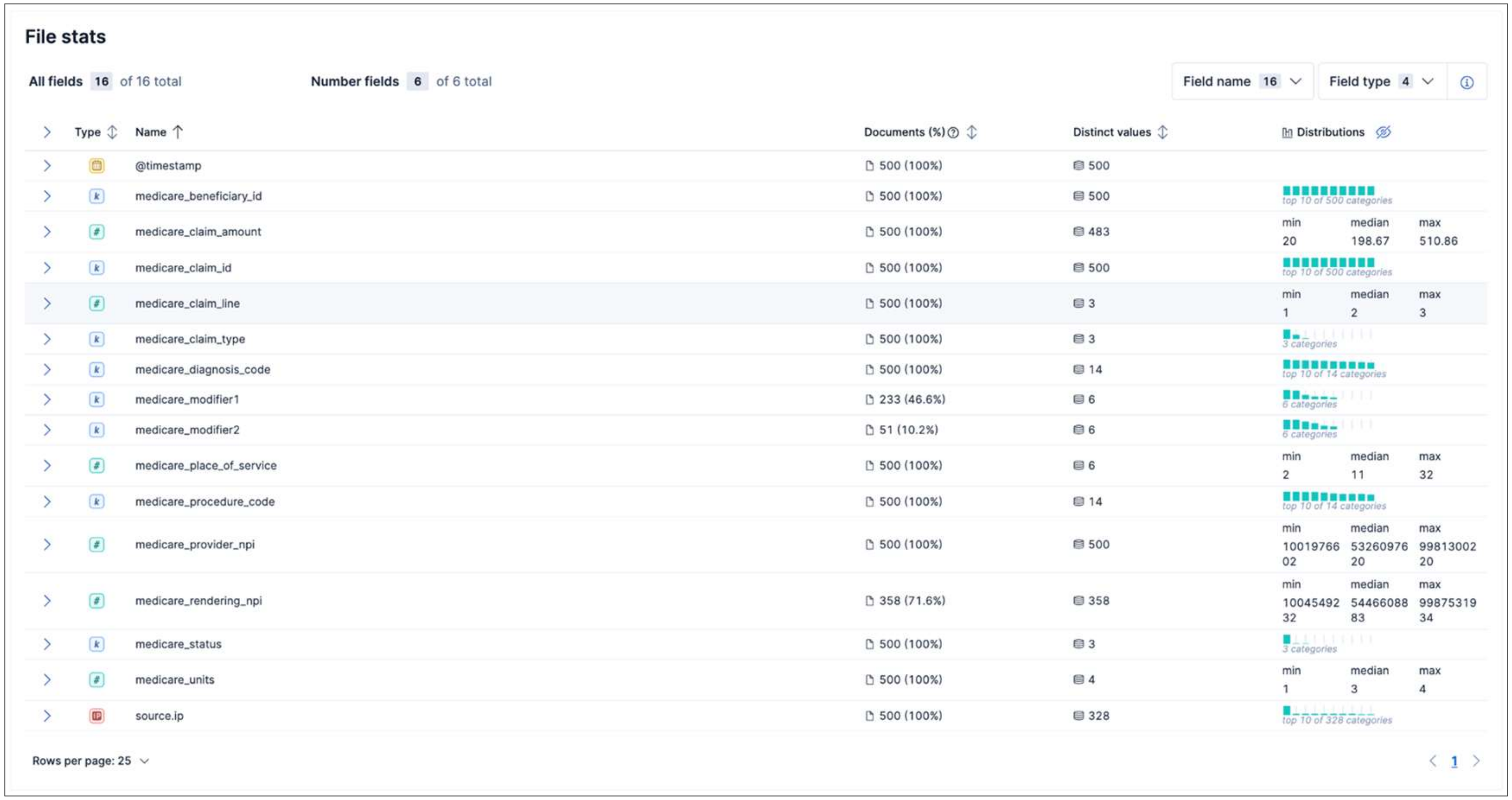
File stats

All fields 16 of 16 total **Number fields** 6 of 6 total

Type	Name	Documents (%)	Distinct values	Distributions
	@timestamp	500 (100%)	500	
k	medicare_beneficiary_id	500 (100%)	500	top 10 of 500 categories

Fraud Detection with Elastic

Scene 5: A Call from Medicare



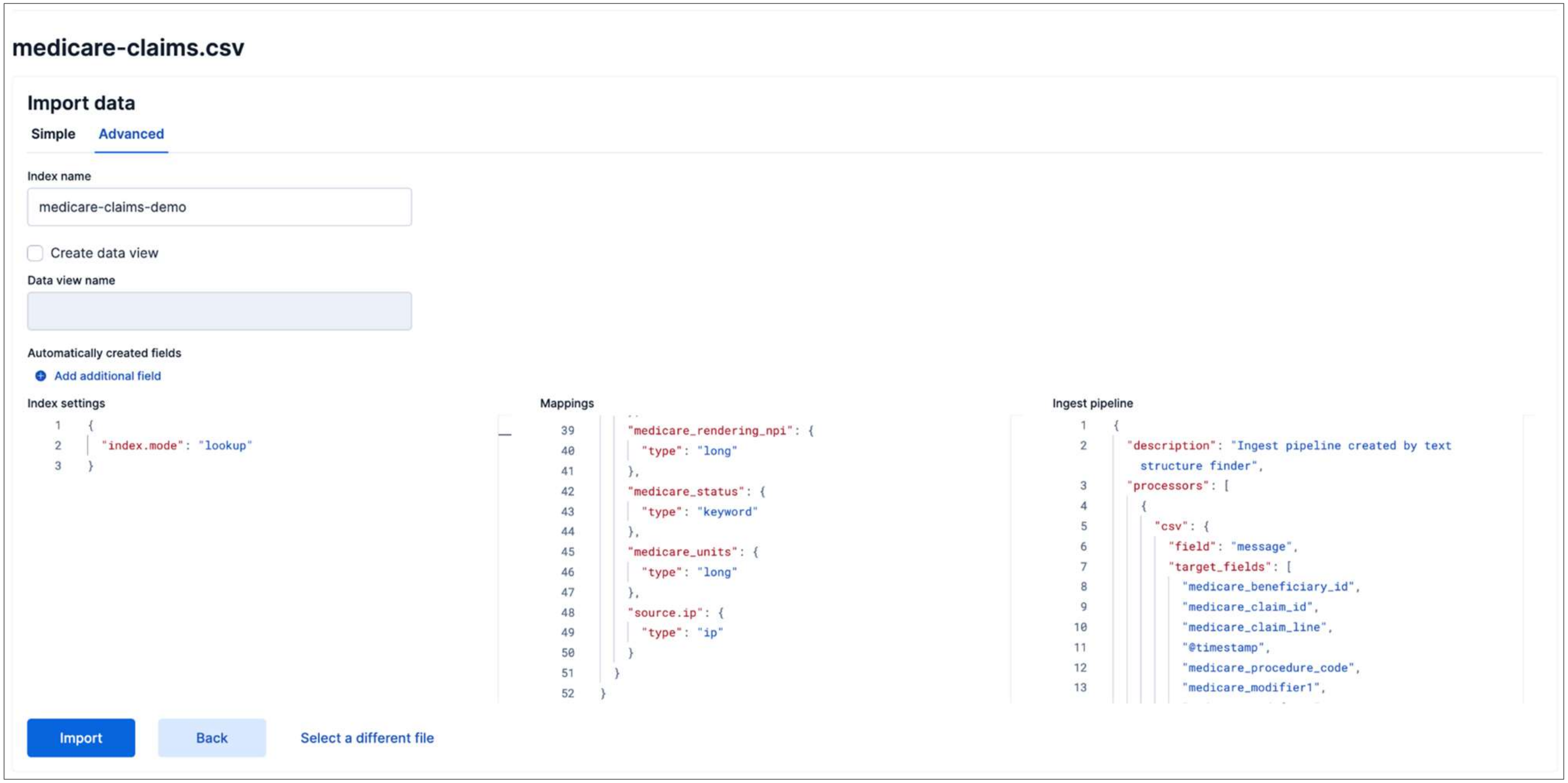
File stats

All fields 16 of 16 total **Number fields** 6 of 6 total

Type	Name	Documents (%)	Distinct values	Distributions
	@timestamp	500 (100%)	500	
k	medicare_beneficiary_id	500 (100%)	500	top 10 of 500 categories
#	medicare_claim_amount	500 (100%)	483	min 20 median 198.67 max 510.86
k	medicare_claim_id	500 (100%)	500	top 10 of 500 categories
#	medicare_claim_line	500 (100%)	3	min 1 median 2 max 3
k	medicare_claim_type	500 (100%)	3	3 categories
k	medicare_diagnosis_code	500 (100%)	14	top 10 of 14 categories
k	medicare_modifier1	233 (46.6%)	6	6 categories
k	medicare_modifier2	51 (10.2%)	6	6 categories
#	medicare_place_of_service	500 (100%)	6	min 2 median 11 max 32
k	medicare_procedure_code	500 (100%)	14	top 10 of 14 categories
#	medicare_provider_npi	500 (100%)	500	min 1001976602 median 5326097620 max 9981300220
#	medicare_rendering_npi	358 (71.6%)	358	min 1004549232 median 5446608883 max 9987531934
k	medicare_status	500 (100%)	3	3 categories
#	medicare_units	500 (100%)	4	min 1 median 3 max 4
IP	source.ip	500 (100%)	328	top 10 of 328 categories

Fraud Detection with Elastic

Scene 5: A Call from Medicare



medicare-claims.csv

Import data

Index name: medicare-claims-demo

☐ Create data view

Data view name:

Automatically created fields

Index settings

```
{
  "index.mode": "lookup"
}
```

Mappings

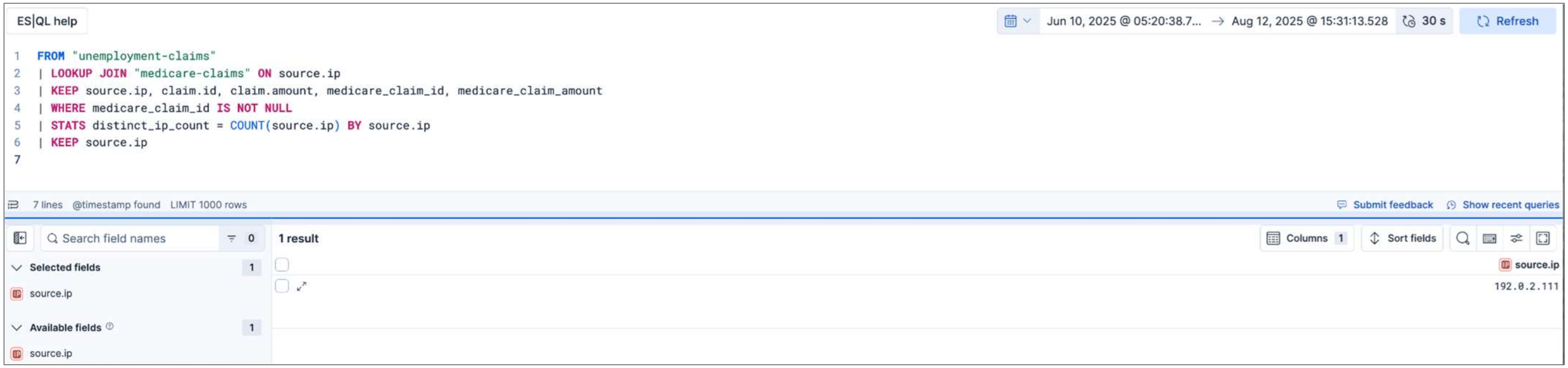
```
    "medicare_rendering_npi": {
      "type": "long"
    },
    "medicare_status": {
      "type": "keyword"
    },
    "medicare_units": {
      "type": "long"
    },
    "source.ip": {
      "type": "ip"
    }
  }
}
```

Ingest pipeline

```
{
  "description": "Ingest pipeline created by text
   structure finder",
  "processors": [
    {
      "csv": {
        "field": "message",
        "target_fields": [
          "medicare_beneficiary_id",
          "medicare_claim_id",
          "medicare_claim_line",
          "@timestamp",
          "medicare_procedure_code",
          "medicare_modifier1",
```

Fraud Detection with Elastic

Scene 5: A Call from Medicare



Jun 10, 2025 @ 05:20:38.7... → Aug 12, 2025 @ 15:31:13.528 30 s

```
FROM "unemployment-claims"
| LOOKUP JOIN "medicare-claims" ON source.ip
| KEEP source.ip, claim.id, claim.amount, medicare_claim_id, medicare_claim_amount
| WHERE medicare_claim_id IS NOT NULL
| STATS distinct_ip_count = COUNT(source.ip) BY source.ip
| KEEP source.ip
```

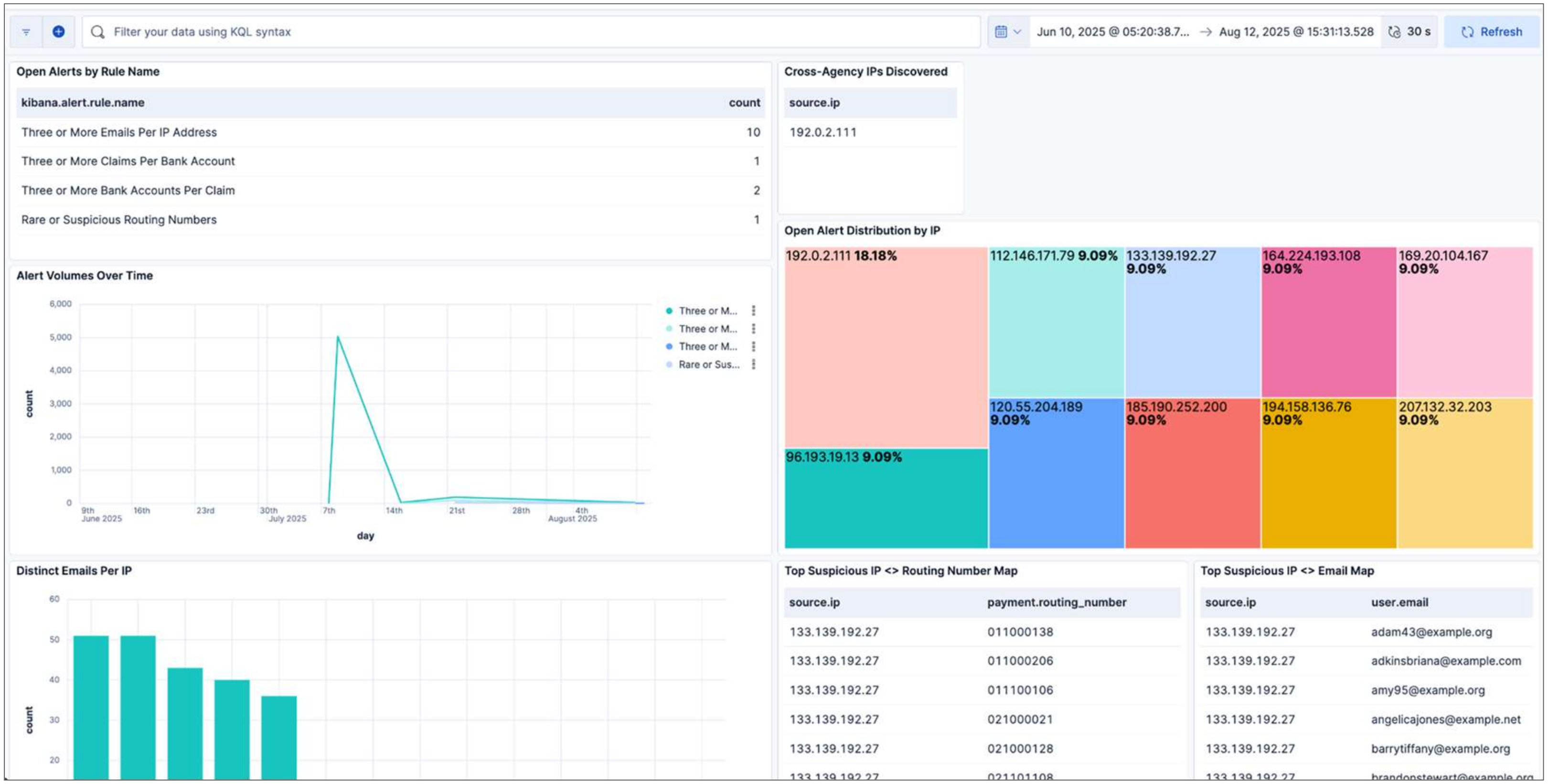
7 lines @timestamp found LIMIT 1000 rows

1 result

source.ip
192.0.2.111

Fraud Detection with Elastic

Scene 6: Reporting Upstream


Filter your data using KQL syntax
Jun 10, 2025 @ 05:20:38.7... → Aug 12, 2025 @ 15:31:13.528
30 s
Refresh

Open Alerts by Rule Name

kibana.alert.rule.name	count
Three or More Emails Per IP Address	10
Three or More Claims Per Bank Account	1
Three or More Bank Accounts Per Claim	2
Rare or Suspicious Routing Numbers	1

Cross-Agency IPs Discovered

source.ip
192.0.2.111

Alert Volumes Over Time

Open Alert Distribution by IP

Distinct Emails Per IP

Top Suspicious IP <> Routing Number Map

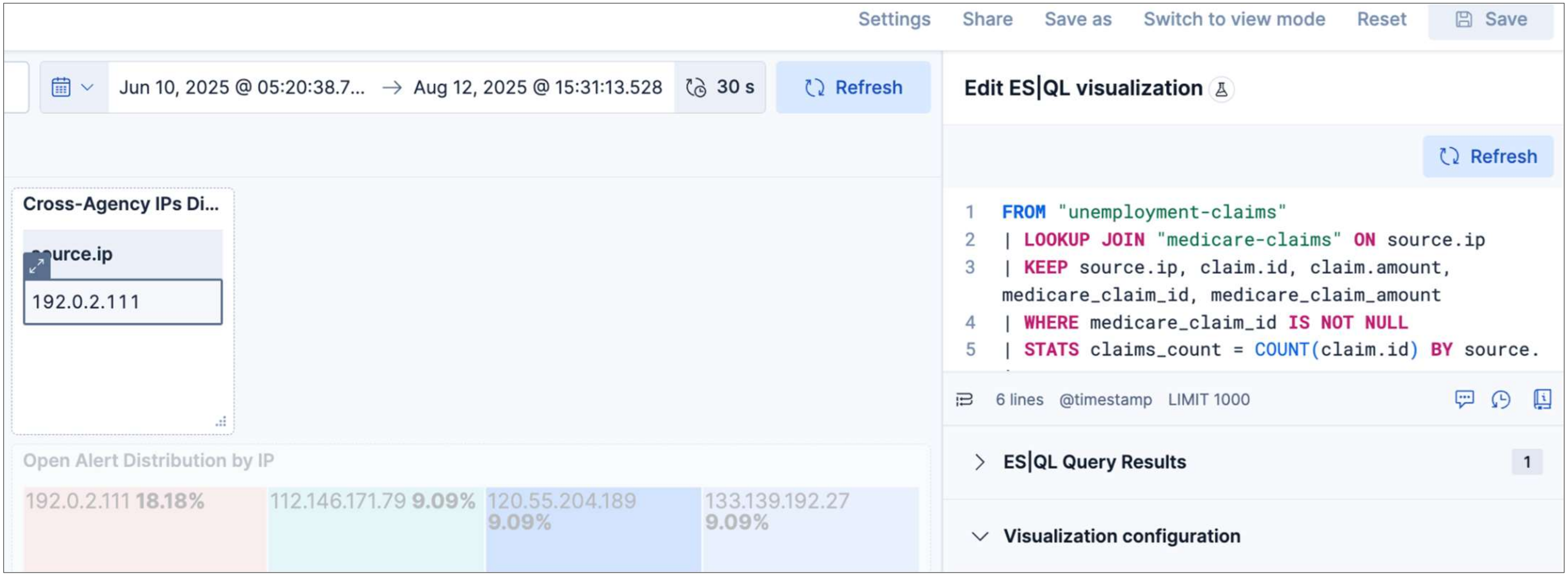
source.ip	payment.routing_number
133.139.192.27	011000138
133.139.192.27	011000206
133.139.192.27	011100106
133.139.192.27	021000021
133.139.192.27	021000128
133.139.192.27	021101108

Top Suspicious IP <> Email Map

source.ip	user.email
133.139.192.27	adam43@example.org
133.139.192.27	adkinsbriana@example.com
133.139.192.27	amy95@example.org
133.139.192.27	angelicajones@example.net
133.139.192.27	barrytiffany@example.org
133.139.192.27	brandonstewart@example.org

Fraud Detection with Elastic

Scene 6: Reporting Upstream

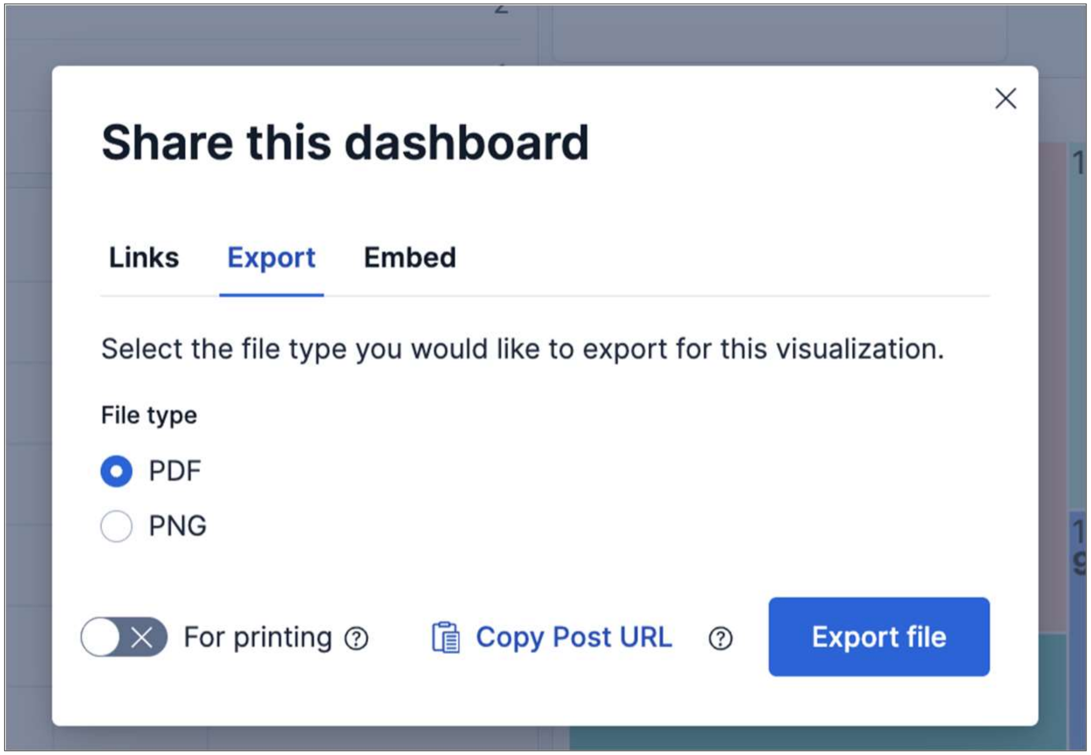


source.ip
192.0.2.111

```
FROM "unemployment-claims"
| LOOKUP JOIN "medicare-claims" ON source.ip
| KEEP source.ip, claim.id, claim.amount,
medicare_claim_id, medicare_claim_amount
| WHERE medicare_claim_id IS NOT NULL
| STATS claims_count = COUNT(claim.id) BY source.
```

Fraud Detection with Elastic

Scene 6: Reporting Upstream



Share this dashboard

Select the file type you would like to export for this visualization.

File type

● PDF

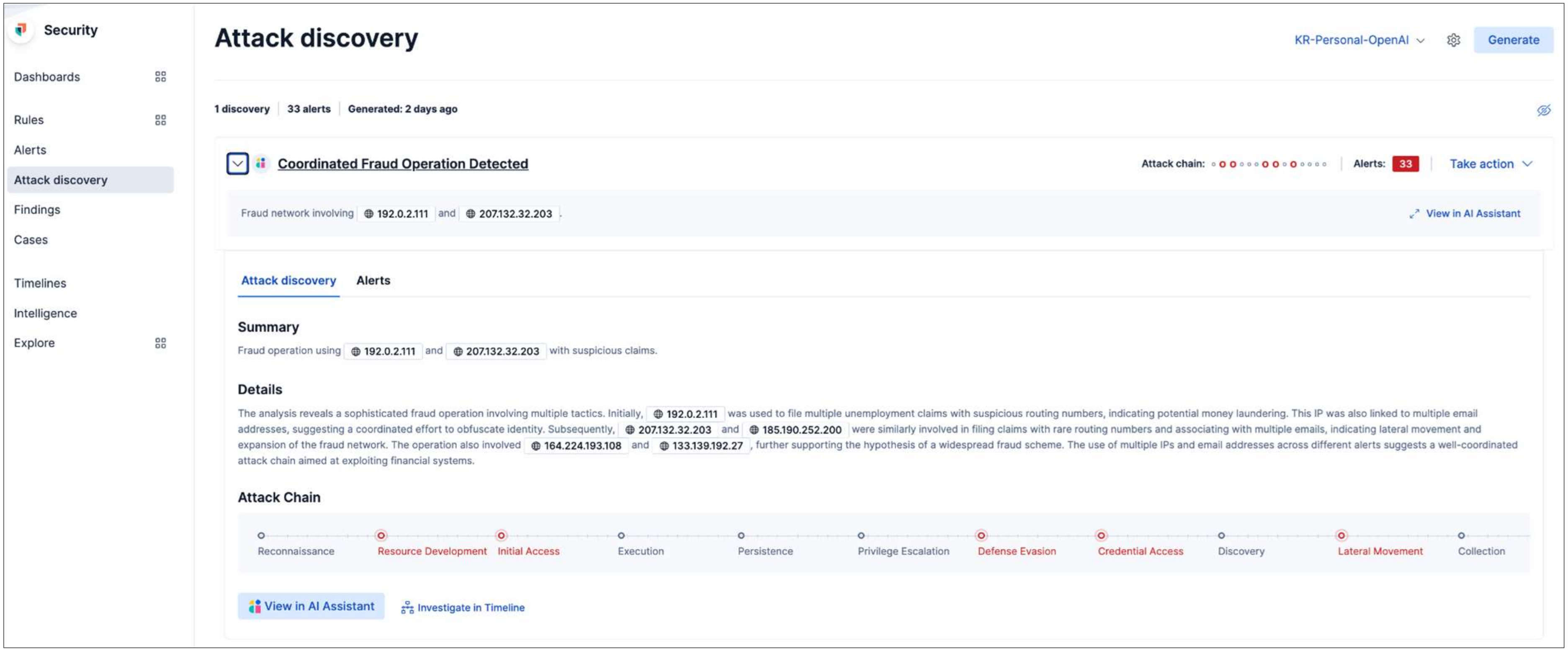
○ PNG

Scene 7:

Attack Discovery for Fraud Detection? Can it really work?

Fraud Detection with Elastic

Scene 7: Attack Discovery for Fraud Detection? Can it really work?



Attack discovery

1 discovery | 33 alerts | Generated: 2 days ago

Coordinated Fraud Operation Detected

Fraud network involving 192.0.2.111 and 207.132.32.203 .

Summary

Fraud operation using 192.0.2.111 and 207.132.32.203 with suspicious claims.

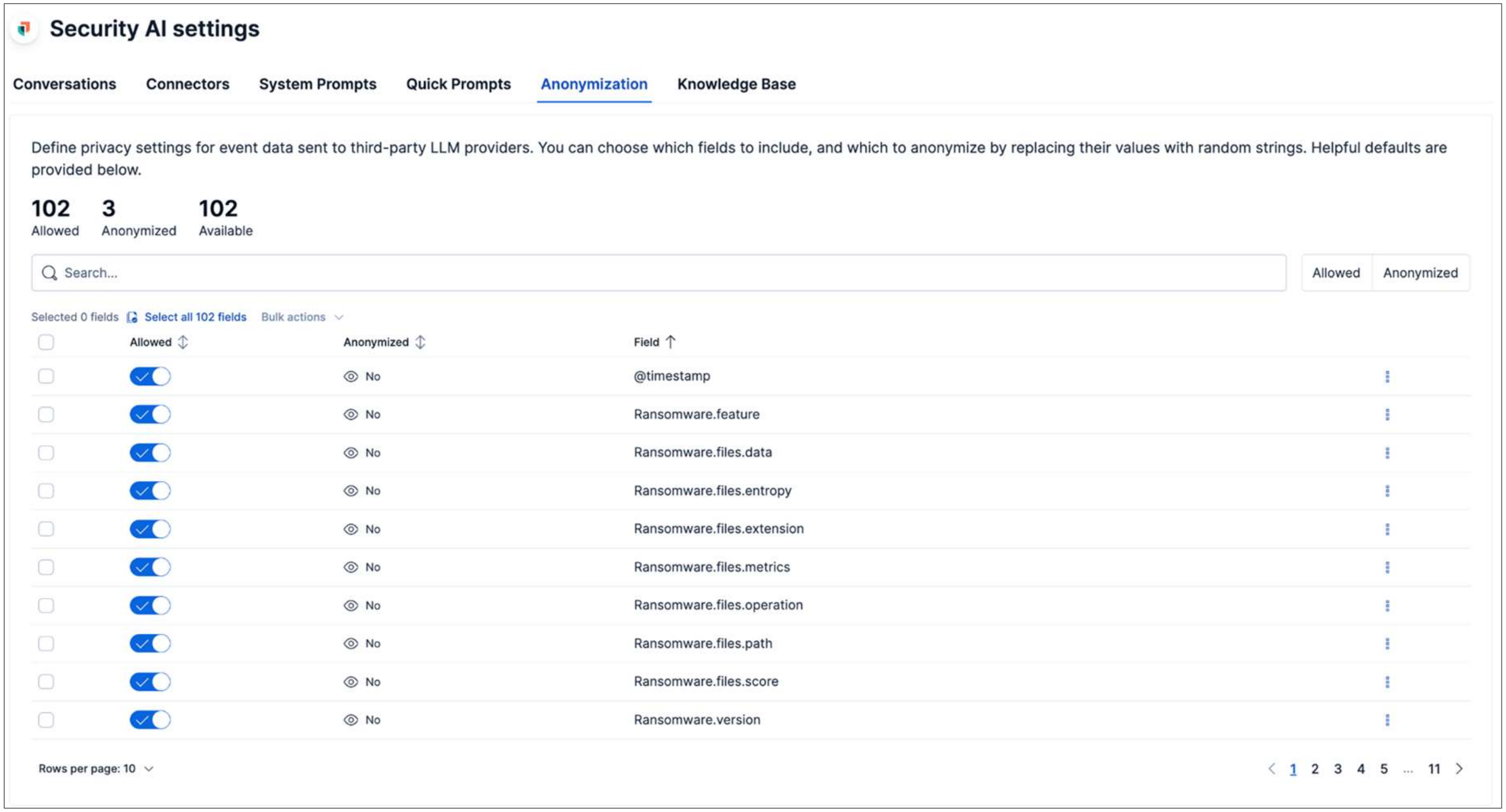
Details

The analysis reveals a sophisticated fraud operation involving multiple tactics. Initially, 192.0.2.111 was used to file multiple unemployment claims with suspicious routing numbers, indicating potential money laundering. This IP was also linked to multiple email addresses, suggesting a coordinated effort to obfuscate identity. Subsequently, 207.132.32.203 and 185.190.252.200 were similarly involved in filing claims with rare routing numbers and associating with multiple emails, indicating lateral movement and expansion of the fraud network. The operation also involved 164.224.193.108 and 133.139.192.27 , further supporting the hypothesis of a widespread fraud scheme. The use of multiple IPs and email addresses across different alerts suggests a well-coordinated attack chain aimed at exploiting financial systems.

Attack Chain

Fraud Detection with Elastic

Scene 7: Attack Discovery for Fraud Detection? Can it really work?

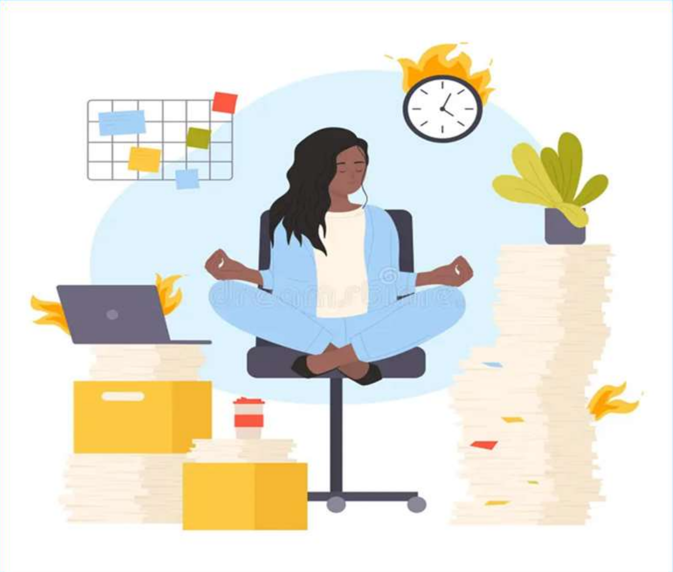


Security AI settings

Define privacy settings for event data sent to third-party LLM providers. You can choose which fields to include, and which to anonymize by replacing their values with random strings. Helpful defaults are provided below.

102 Allowed
3 Anonymized
102 Available

☐	Allowed	Anonymized	Field
☐	✓	No	@timestamp
☐	✓	No	Ransomware.feature
☐	✓	No	Ransomware.files.data
☐	✓	No	Ransomware.files.entropy
☐	✓	No	Ransomware.files.extension
☐	✓	No	Ransomware.files.metrics
☐	✓	No	Ransomware.files.operation
☐	✓	No	Ransomware.files.path
☐	✓	No	Ransomware.files.score
☐	✓	No	Ransomware.version



With Elastic for Fraud Detection

- Detect fraud faster, before it becomes payout
- Correlate patterns across IPs, emails, bank accounts, and locations
- Scale discovery and analysis without scaling headcount
- Provide explainable, defensible insights to leadership and investigators
- Utilize AI to reduce the time and effort required to correlate alerts

Strengthen Fraud Prevention. Strengthen Trust.

Detect smartly

Use data and analytics to find fraud faster.

Govern responsibly

Protect citizen data with strong controls.

Build trust continuously

Prove accountability and transparency every step of the way.

Fraud Detection Value

−

Data Risk Exposure

+

Governance Maturity

=

Public Trust

What's the next step your agency can take to balance fraud prevention with citizen trust?

Thank You

Questions?

Kyle Rozanitis
kyle.rozanitis@elastic.co
https://www.linkedin.com/in/kyle-rozanitis/

Learn more at elastic.co