INTEZER

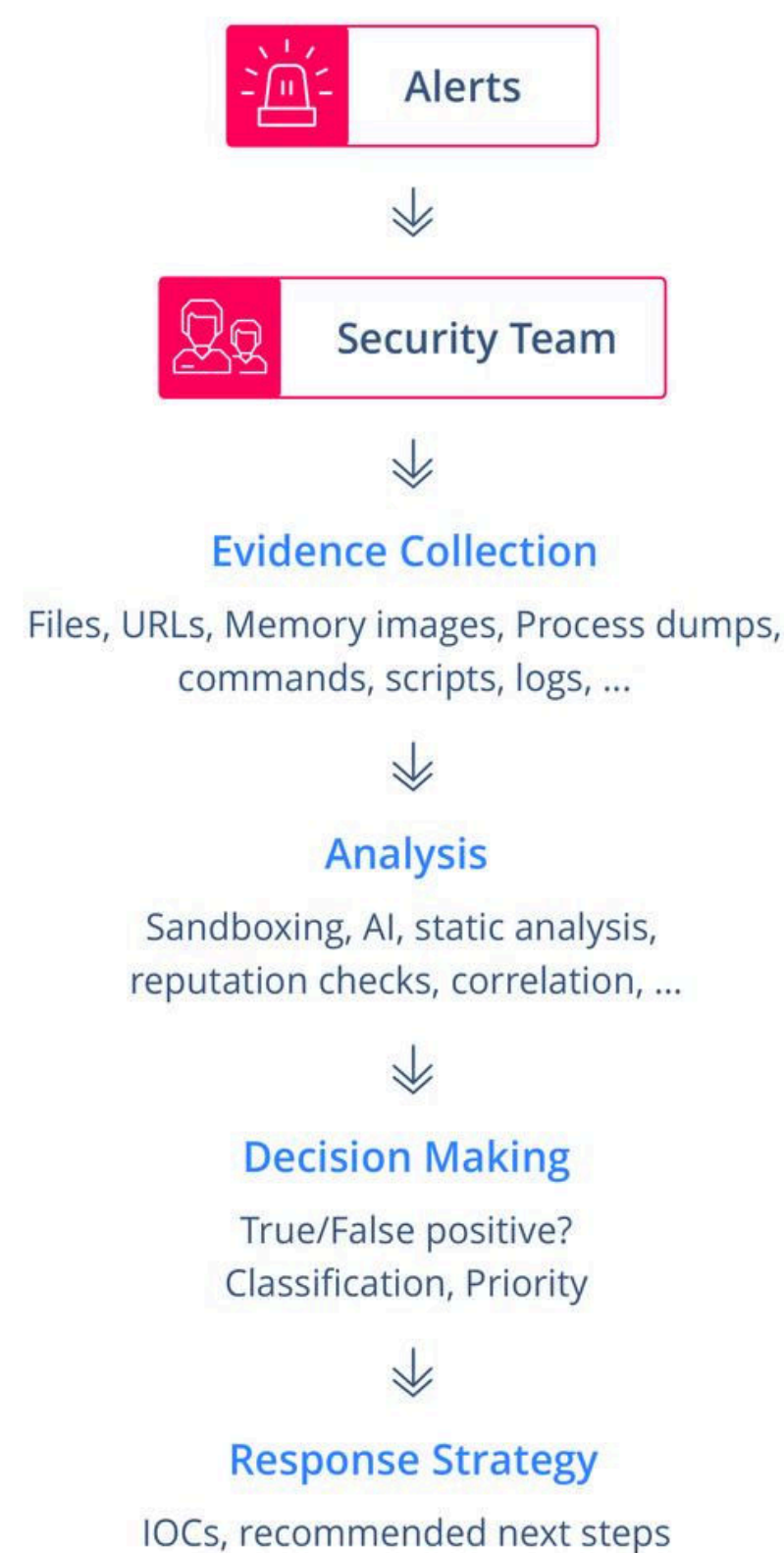# Extend Your Security Team with AI

Deep, AI-powered investigations and fast triage for ingested alerts from your endpoint, phishing, and SIEM tools

Manual Alert Triage

Alerts

⬇

Security Team

⬇

Evidence Collection

Files, URLs, Memory images, Process dumps, commands, scripts, logs, ...

⬇

Analysis

Sandboxing, AI, static analysis, reputation checks, correlation, ...

⬇

Decision Making

True/False positive? Classification, Priority

⬇

Response Strategy

IOCs, recommended next steps

Automated Alert Triage with Intezer

Alerts

⬇

• **Evidence Collection**

⬇

• **Analysis**

⬇

• **Decision Making**

⬇

• **Response Strategy**

⬇

Security Team

Get Only Escalated Alerts

Only 4% of alerts.
Contextualized with IOCs and recommended next steps

Extend Your Team with the Autonomous SOC Platform

Automatically triage and investigate every alert, with the Autonomous SOC Platform working like your Level 1 SOC to escalate only the confirmed, serious threats. Easily connect your security tools to start getting immediate value.

Escalate to your team	Automatically resolve	Alerts are triaged within
4%	**97%**	**2**
of alerts on average	of false positives	minutes on average

Easy to Connect Integrations

Just minutes to set up, no engineering required. Ingest every alert to automatically get detailed investigations, triage assessments and recommended actions from Intezer.

SentinelOne · Microsoft Defender · CROWDSTRIKE · servicenow · DEVO

splunk> SIEM · tines · OBSIDIAN · Jira · mimecast

proofpoint · SUBLIME · CORTEX · elastic · Microsoft 365

See all integrations at intezer.com/integrations

Dashboard

Time Range	Site Names	Account Names
Last Month	All	All

3,584 Ingested alerts
12,507 Monitored devices
1 min **38** sec Average investigation time

3.16% 105 Escalated
23.84% 791 Follow up recommended
73% 2,422 No action needed

Triage

0.0% Critical Threat · 9.0% Generic Threat · 8.7% Suspicious Activity · 14.6% Unwanted Software · 4.0% Admin Activity · 6.4% Inconclusive · 5.5% False Positive · 51.8% Audited

10 sources   Connect sources / Scan

CrowdStrike Endpoint Protection **552 Alerts**
Phishing Emails **543 Alerts**
Palo Alto Firewall **530 Alerts**
Splunk SIEM **424 Alerts**

+ 6 more

200 / 130 / 67 / 0

August 11 — September 10

Response

Top devices at risk   Top artifacts   Artifact type

Trusted by Enterprise and MSSP SOC Teams

EQUIFAX · Adobe · MGM RESORTS INTERNATIONAL · PEPSICO · legato security · RSM

Why Intezer?

Intezer goes beyond automated playbooks, sandboxing, or manual alert enrichment to take action, make smart decisions, and give SOC teams fast recommendations for incident response. Over the years, we've fine-tuned and expanded Intezer's capabilities to automate more and more of the time-consuming or repetitive tasks for security teams.

Intezer's technology is designed with the three pillars of our **Artificial Intelligence Framework:** a proprietary genetic analysis engine, machine learning algorithms, and private instances of generative AI. This comprehensive framework uses the strengths of each to produce accurate results that mimic experienced security analysts and augment your team.