

INTEZER AUTONOMOUS SOC PLATFORM

INSTANT THREAT INSIGHTS AND RESPONSE.
AUTOMATED, ACTIONABLE, AND ACCURATE.

Meet Your AI Analysts

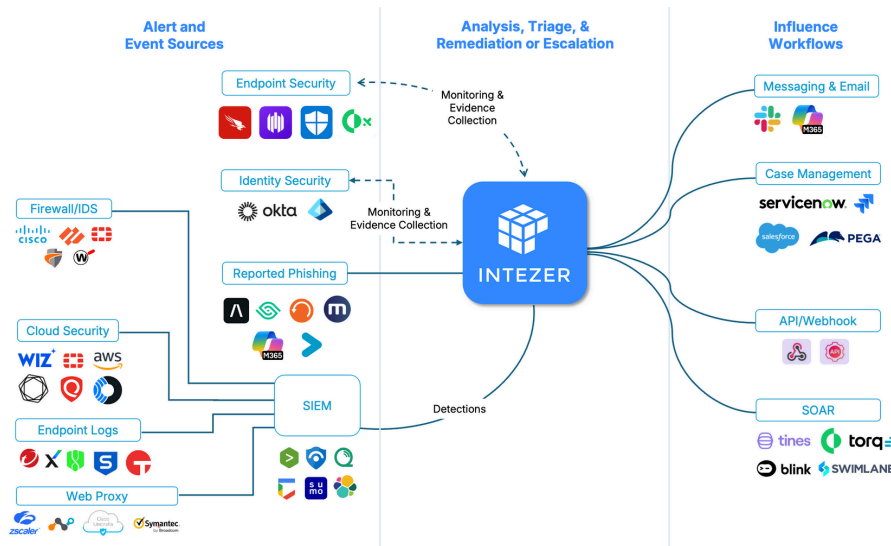
Adopting Intezer's Autonomous SOC Platform is like onboarding a team of world-class security analysts, ready to start solving problems from day one.

Unlike traditional SOC tools, this AI-driven solution doesn't just automate surface-level tasks. It dives deep into each alert with reverse engineering-level expertise and comes with a full toolkit for investigation, triage, and remediation, ensuring seamless operations within your existing security stack.

How Does it Work?

Intezer leverages proprietary artificial intelligence models, a variety of trusted techniques, and a unique Genetic Code Analysis technology. For crafting the bottom-line incident triage assessments, Intezer uses machine learning and AI models that account for the multiple analysis results for each individual piece of evidence alongside information from the user's existing security tools.

Intezer's automated alert triage process starts by collecting all evidence associated with an alert (file, process, command line, IP, URL, memory image, etc.), deeply analyzes each artifact, and then builds an overall assessment for the incident and executes remediation based on the verdict.



CATCH THE CYBERATTACKS BURIED IN THE FLOOD OF ALERTS

Automatically triage and investigate every alert, with **the Autonomous SOC Platform working like your L1 and L2 SOC analysts** 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
Triage Within



Key Features And Benefits

• Granular Triage:

Every alert is thoroughly analyzed at a detailed level, ensuring that no threat is missed. On average 4% of alerts are escalated while auto-closing 97% of false positives.

• Immediate Value:

Quick to integrate and deliver results, with no engineering effort required for setup.

• Cost-Effective:

A more affordable solution compared to hiring additional staff or outsourcing to Managed Detection and Response (MDR) services.

• Broad Alert Coverage:

Supports a wide range of alert sources, including endpoint security, phishing reports, and SIEM alert pipelines, ensuring comprehensive monitoring and response.

• No Incidents Overlooked:

Every alert, including those marked as medium or lower severity by your security tools, is triaged to ensure no incidents slip through.

Visit Us at:

<https://intezer.com/autonomous-soc>

Get a Demo at:

<https://intezer.com/get-a-demo/>

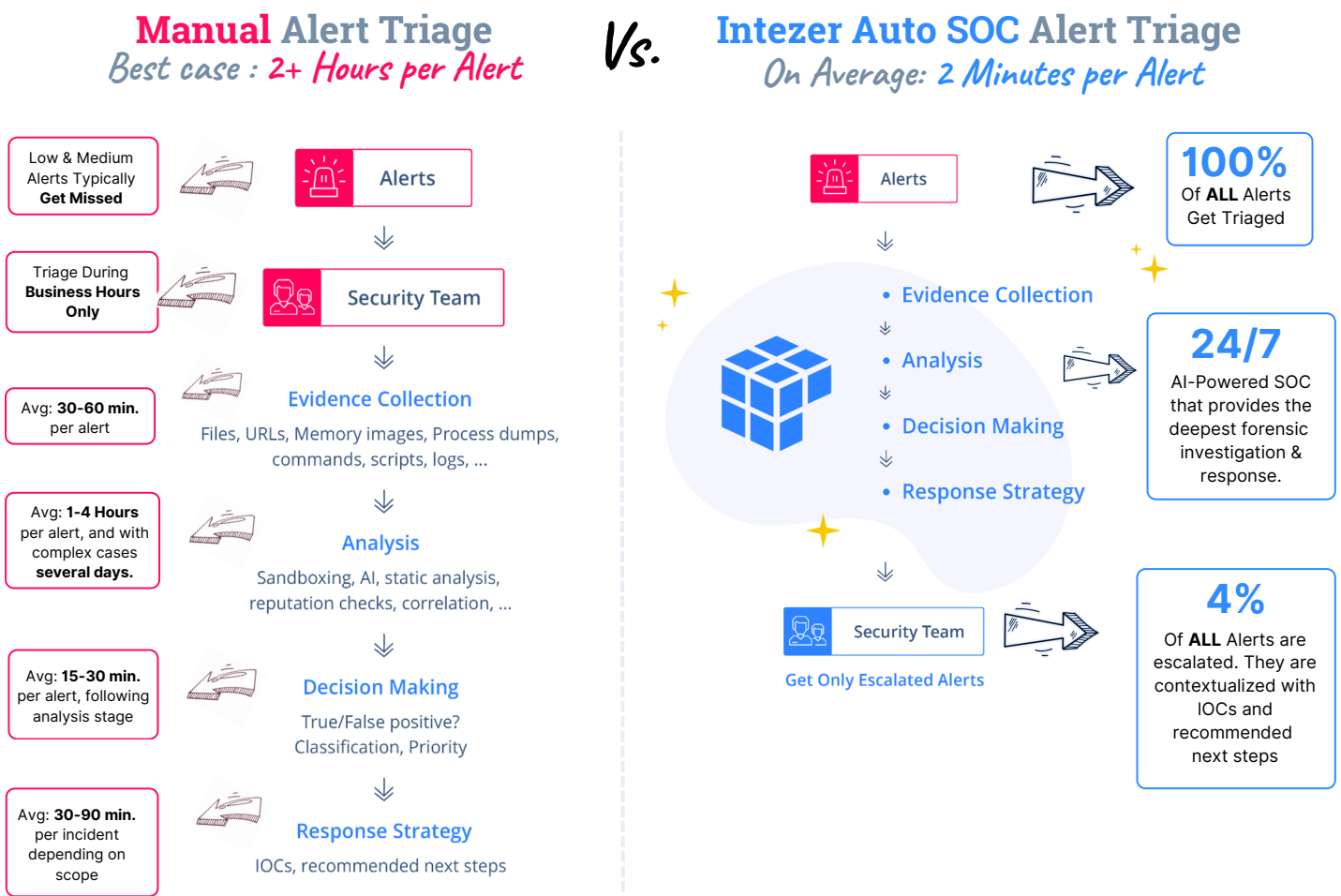
Have Questions:

Contact@intezer.com

How Intezer Stands Out in a Crowded Market

The cybersecurity industry is buzzing with AI-driven SOC tools, **but not all platforms are created equal**. Here's what sets Intezer apart:

- Depth of Analysis:**
 Most AI tools focus on keyword matches, heuristic scoring, or surface-level behavior analysis. Intezer digs deeper, identifying malware signatures and behaviors that others simply cannot detect.
- Precision and Consistency**
 Intezer eliminates inconsistencies caused by human error or subjective judgment. Every alert gets the same high level of scrutiny.
- Speed Without Sacrificing Accuracy**
 Traditional reverse engineering can take hours or even days. Intezer delivers the same insights in seconds, saving valuable time.
- All-in-One Functionality:**
 Many platforms require multiple third-party integrations to achieve similar results. Intezer bundles everything into a single platform, ensuring you're operational immediately.



Unlock the Power of Your SOC

[Schedule Your Demo Today](#) and visit us at intezer.com

Intezer's Autonomous SOC doesn't just automate tasks; it empowers your team with the tools and insights needed to stay ahead of even the most sophisticated threats. By bringing reverse engineering to the forefront and eliminating inefficiencies in the triage process, Intezer transforms your security operations into a powerhouse of speed, accuracy, and effectiveness.