INTEZER AISHIELD

Autonomous Security Operations

INTEZER

Security operations are changing

More adversaries

More attack surfaces

More security products

=

RESOURCE SHORTAGE

86%

of security teams overwhelmed with volume of alerts

73%

orgs had at least one breach partially attributed to gap in cyber skills

68%

organizations struggle to recruit, hire and retain cyber talent

INTEZER

The Human Bottleneck In Security Automation

Detection

Automated by security products (EDR, NDR, CNAPP, ...)

Fast

Investigation

Manually done by thinking humans

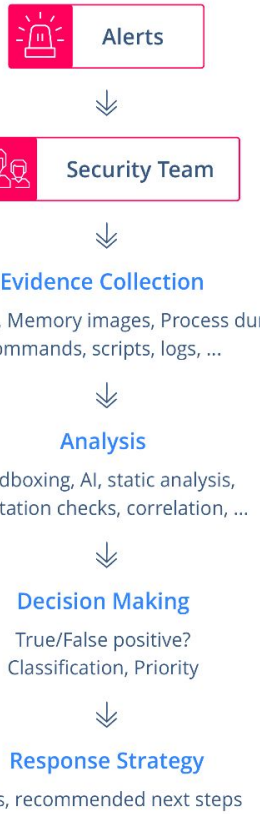
Slow

Response

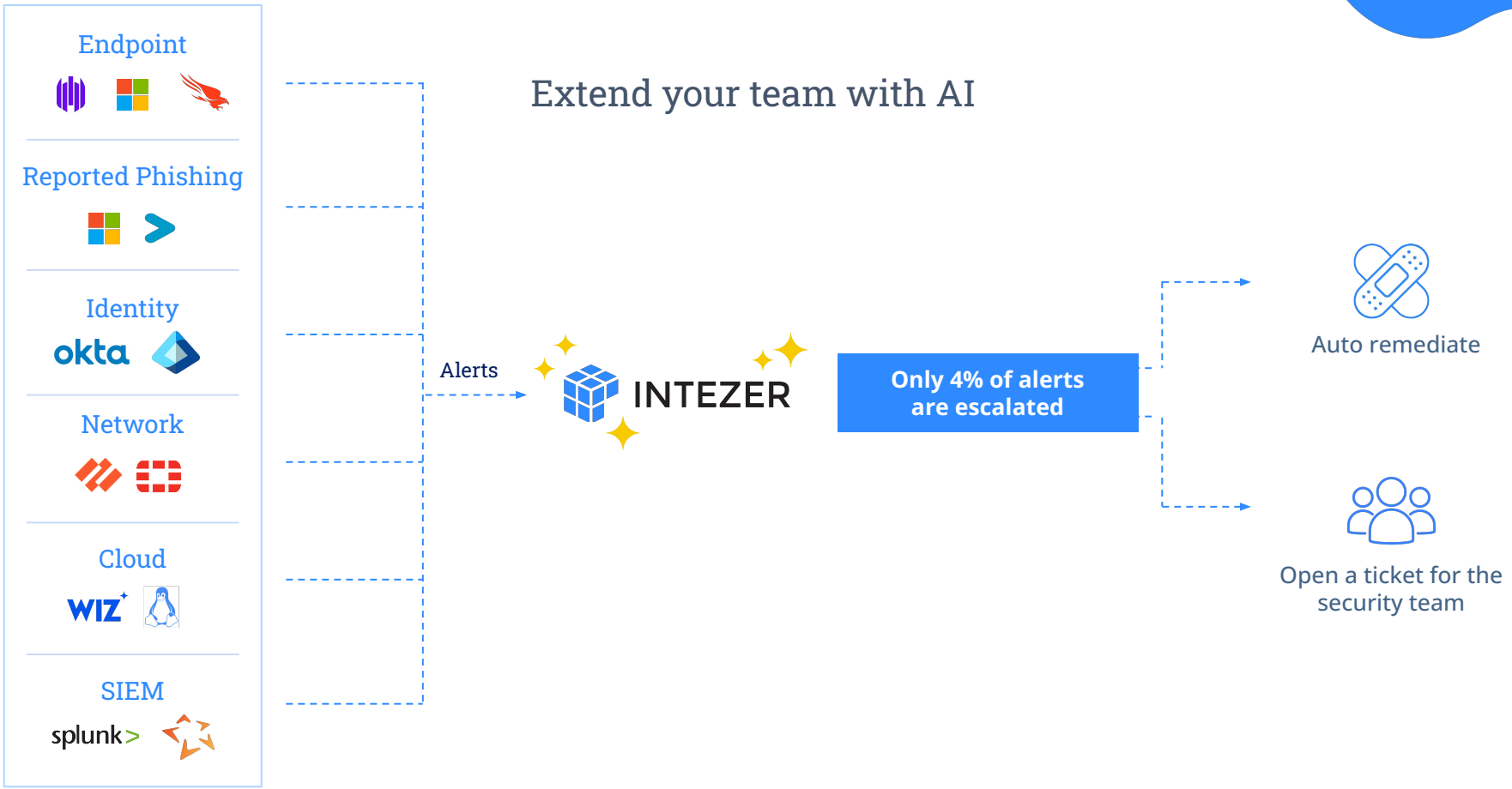
Automated via SOAR

Fast

Introducing Agentic AI That Emulates SOC Analysts



Extend your team with AI

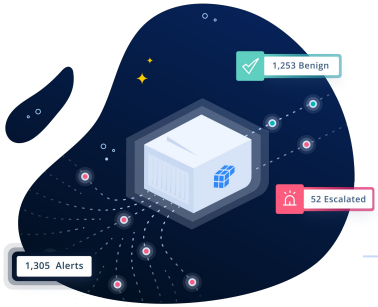


Next-Gen SOC Leaders Trust Intezer


Models
LLM & Proprietary
Memory
Global & Org-specific
Agent Crew
Alert
Decision, Context, Next Steps
Evidence Collection Agent
Analysis Agent
Correlation and Triage Agent
Response Planner Agent
Remediation Agent
Collection Tools
File collection, memdump, cmdline extract, log collection, SIEM query, end-user feedback, etc.
Analysis Tools
Genetic analysis, sandbox, VirusTotal, recursive URL scan, reputation checker, IP analysis, script/macro analyzer, etc.
Response Tools
IOC block, credential reset, isolate machine, etc.

AI Analysts That Never Rest

1



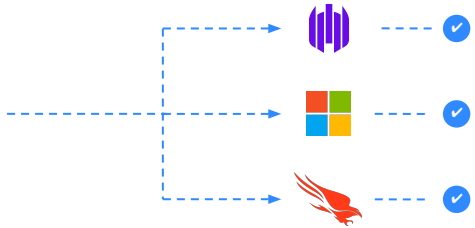
Automatically triage & investigate **every** alert (including low severity) to ensure attacks aren't missed

2

Automatically generate results within 2 minutes

- Investigation summary
- Root cause analysis
- Recommended next steps

3



Automatically respond

- Auto-resolve false positives
- Optionally automate the execution of the recommended response plan (disable user account, isolate machine, ..)

Escalated to your team

4%

Of security alerts on average

Average Triage Time

2 Minutes

Accuracy Benchmark

97.6%

INTEZER

Thank you!

www.intezer.com | contact@intezer.com

AISHIELD