INTEZER

AI-Powered SOC: Goodbye to False Promises and False Positives

Itai Tevet, CEO and founder

1

The SOC Resource Problem: Too Many Alerts, Not Enough Time or Analysts

2

The Promise and Reality of Generative AI

3

Practical Advice and Tips for Adopting AI

Security Operations Are BROKEN

More adversaries

More attack surfaces

More security products

=

RESOURCE SHORTAGE

86%

of security teams are overwhelmed with the volume of alerts

73%

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

68%

organizations struggle to recruit, hire and retain cyber talent

Outsourcing Is Not a Silver Bullet

MDRs are too expensive

Surface-level investigation

Inconsistent service

Gartner peerinsights™

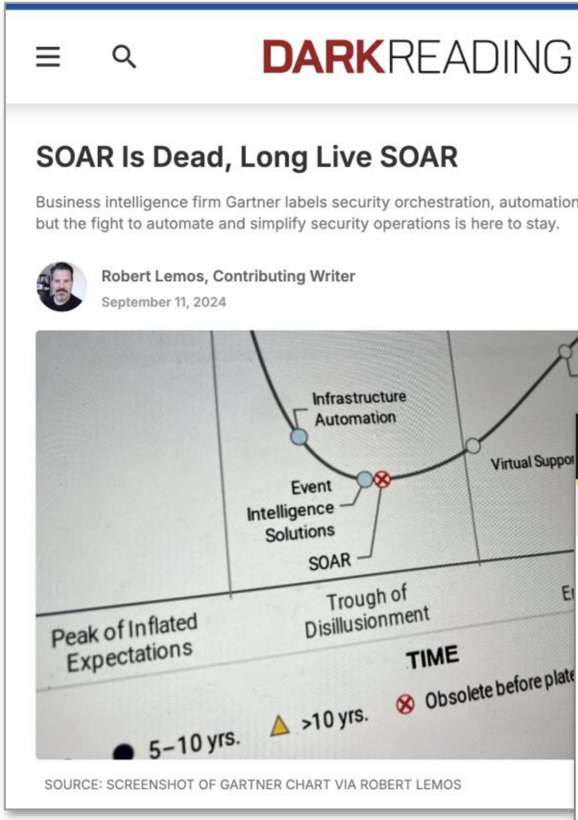
★★☆☆☆

“Lacking in execution, continuity, and responsiveness”

- Security and Risk Manager, on outsourced SOC provider

INTEZER

The Legacy of False Promises



DARKREADING

SOAR Is Dead, Long Live SOAR

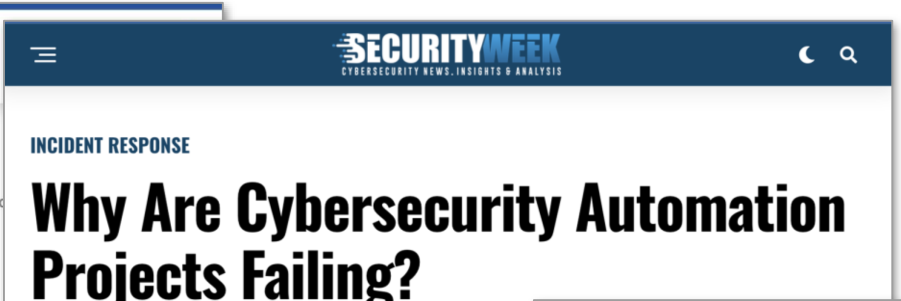
Business intelligence firm Gartner labels security orchestration, automation, and
but the fight to automate and simplify security operations is here to stay.

Robert Lemos, Contributing Writer

September 11, 2024

Infrastructure Automation
Event Intelligence Solutions
SOAR
Virtual Suppo
Softw Man
Peak of Inflated Expectations
Trough of Disillusionment
E
TIME
5–10 yrs.
>10 yrs.
Obsolete before plat

SOURCE: SCREENSHOT OF GARTNER CHART VIA ROBERT LEMOS



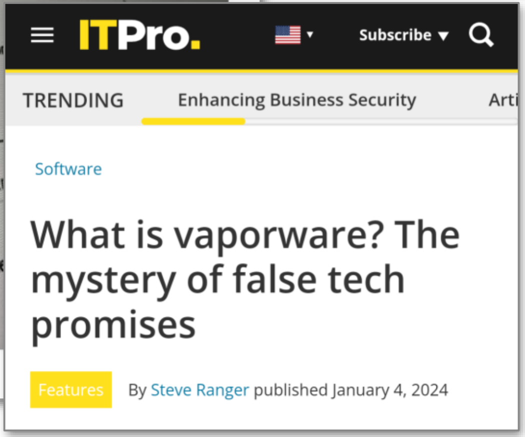
SECURITYWEEK

CYBERSECURITY NEWS, INSIGHTS & ANALYSIS

INCIDENT RESPONSE

Why Are Cybersecurity Automation Projects Failing?

The cybersecurity industry has taken limited action to re
reduce mundane tasks and improve overall user experie



ITPro.

Subscribe ▾

TRENDING Enhancing Business Security Arti

Software

What is vaporware? The mystery of false tech promises

Features By Steve Ranger published January 4, 2024

SECURITY MANAGERS BE LIKE
SPENT $100K ON A NEW SECURITY TOOL
JUST REALIZED TEAM IS TOO BUSY TO USE IT

3 Reasons Security Automation Failed to Live Up to Its Promises

1

Complex setup

Requires extensive custom engineering, preventing meaningful automation even after years of effort.

2

Maintenance

Automated workflows need constant upkeep, from bug fixes to API changes to license management of third party tools.

3

Decision-making bottleneck

Simple playbooks and if/else logic can't replicate human decision-making, leaving many workflows dependent on human intervention.

Automation’s Next Chapter: AI

Why does AI make a difference NOW?

1

AI maturity

Well-trained Large Language Models (LLMs) can ingest needed context and provide accurate analysis—if used wisely.

2

Foundations are already established

Earlier generations of automation tools paved the way with an open API ecosystem, case management, and more.

3

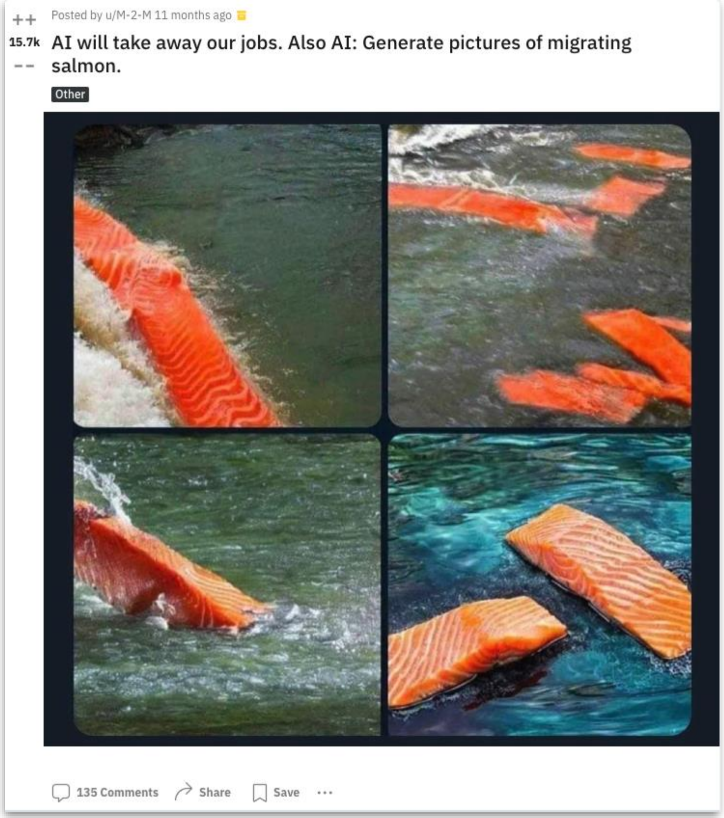
The bad guys are already using AI

They code faster, produce more authentic-looking phishing campaigns at scale, and more.

Reference: DHS

Can Cybersecurity Pros REALLY Trust AI?

In short: if it’s being used in the right places.



Posted by u/M-2-M 11 months ago

15.7k

AI will take away our jobs. Also AI: Generate pictures of migrating salmon.

Where GenAI Promises Succeed …and Where They Fail

GenAI is really good at:

- Analyzing textual artifacts in host telemetry (process names, command lines, registry, autoruns, …)
- Analyzing and detecting malicious activities in scripts / plain text code
- Generating and converting rules/queries
- Detecting things that exploit the human eye (namesquatting)
- Generating incident reports

GenAI is really not good at:

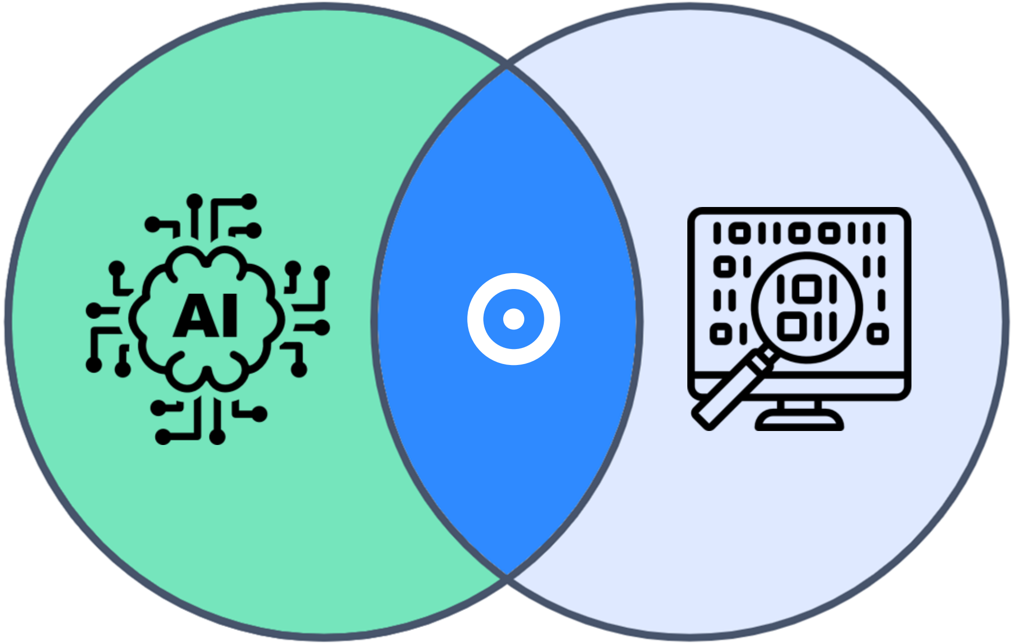
- Critical thinking
- Collecting evidence
- Analysis of non text-based artifacts (links, URLs, files, software)
- Operative actions (e.g. asking the end user)
- Advanced forensic analysis (memory forensics, reverse engineering binary code, …)

Challenges in Adopting GenAI

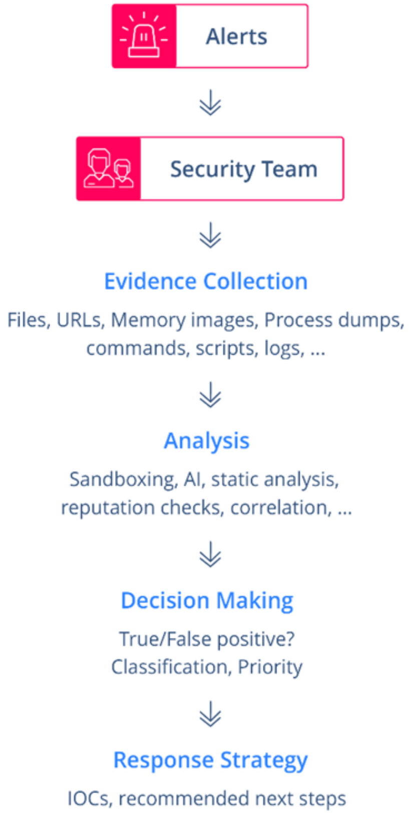
- 🔒 Privacy
- ✨ No magic prompt / input to solve it all
- ⌛ Lots of trial & error that requires time, data, expertise
- 💰 Cost can go high very quickly in enterprise scale

SOC Automation in Real Life

The right solution: a combination of both AI and deterministic analysis methods



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, ...

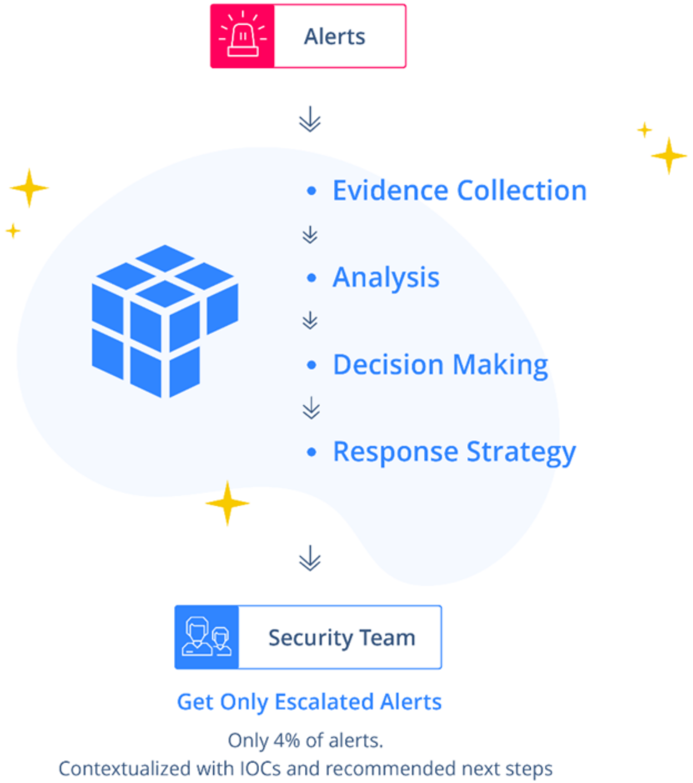
Decision Making

True/False positive?
Classification, Priority

Response Strategy

IOCs, recommended next steps

Automated Alert Triage with Intezer



Alerts

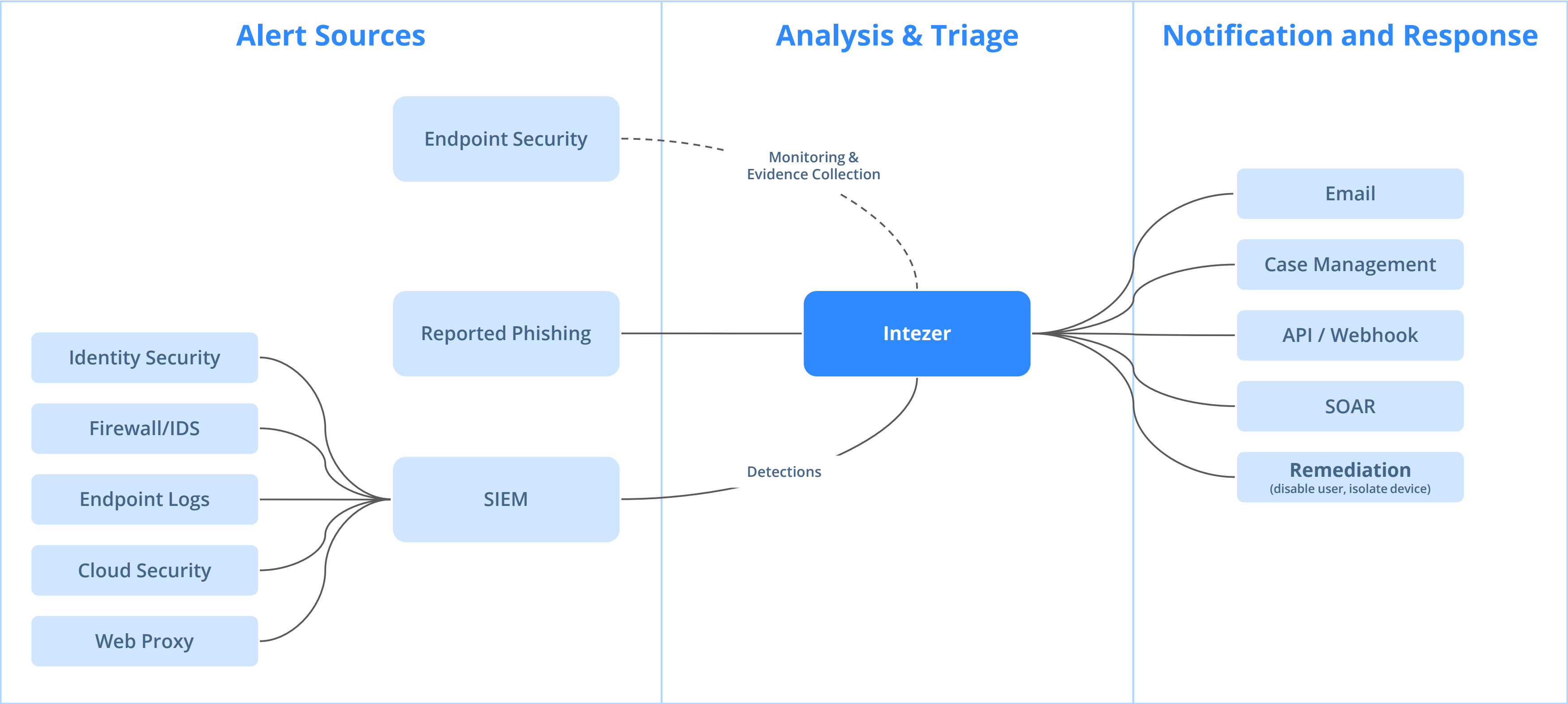
- Evidence Collection
- Analysis
- Decision Making
- Response Strategy

Security Team

Get Only Escalated Alerts

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

Autonomous SOC Architecture



The Autonomous SOC as an Extension of Your Team

EVERY alert is triaged at a granular level

Immediate time-to-value

Accurate, fast, and consistent

⚡ Performance Metrics

4%

Escalation ratio

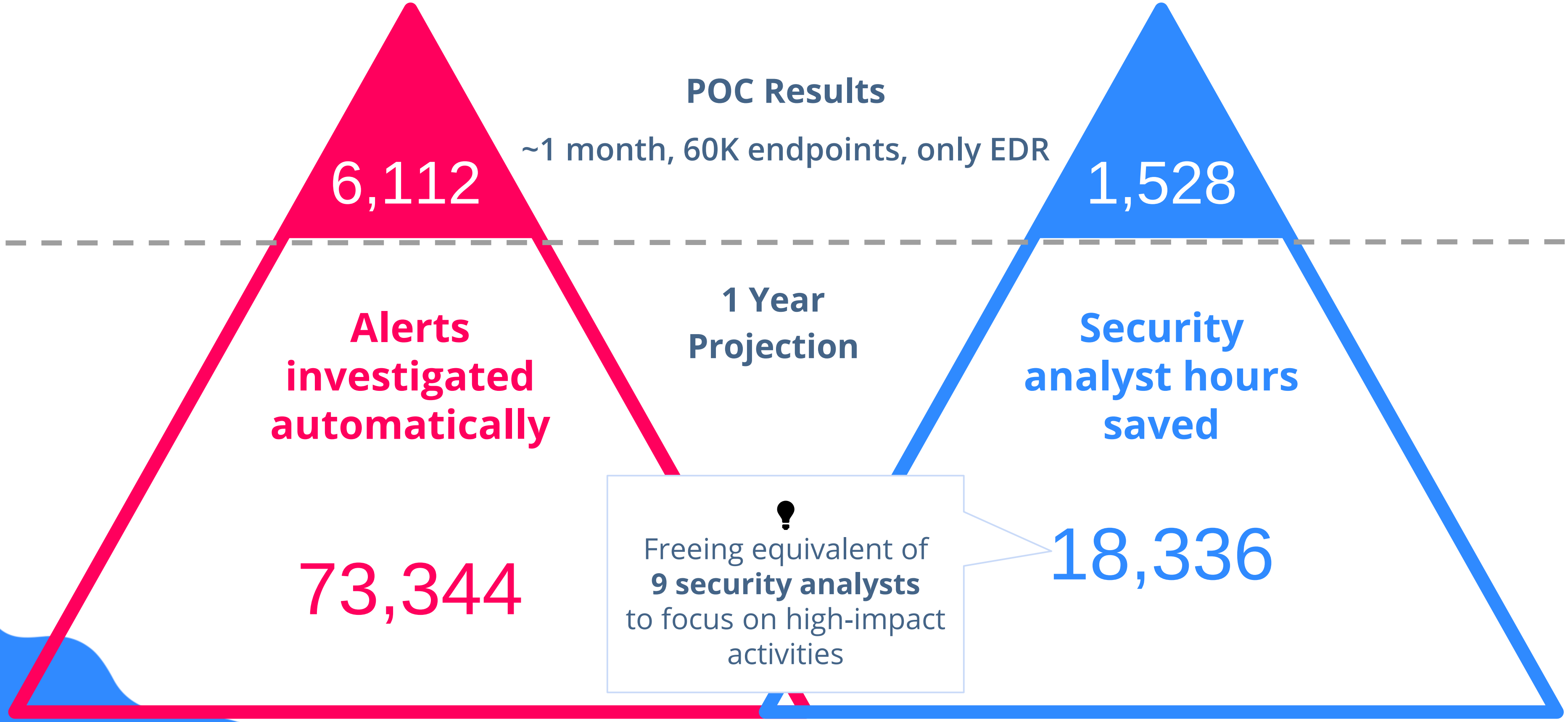
92 %

Escalation accuracy

2 mins

Avg alert triage speed

ROI - Example POC Results



POC Results

~1 month, 60K endpoints, only EDR

6,112

1,528

1 Year Projection

Alerts investigated automatically

73,344

Security analyst hours saved

18,336

Freeing equivalent of **9 security analysts** to focus on high-impact activities

INTEZER

Intezer Live Demo:
Autonomous SOC Platform

INTEZER

Thank you!

www.intezer.com | contact@intezer.com