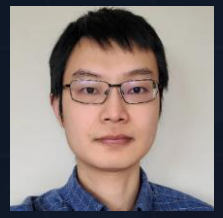
Dropzone AI

SANS Cyber Solutions Fest

Use GenAI to Maximize Detection Coverage in the SOC

Agenda

- How AI helps with SOC automation
  - SOAR automation
  - AI assistants
  - AI SOC analysts
- Discussion on SOC coverage



Edward Wu

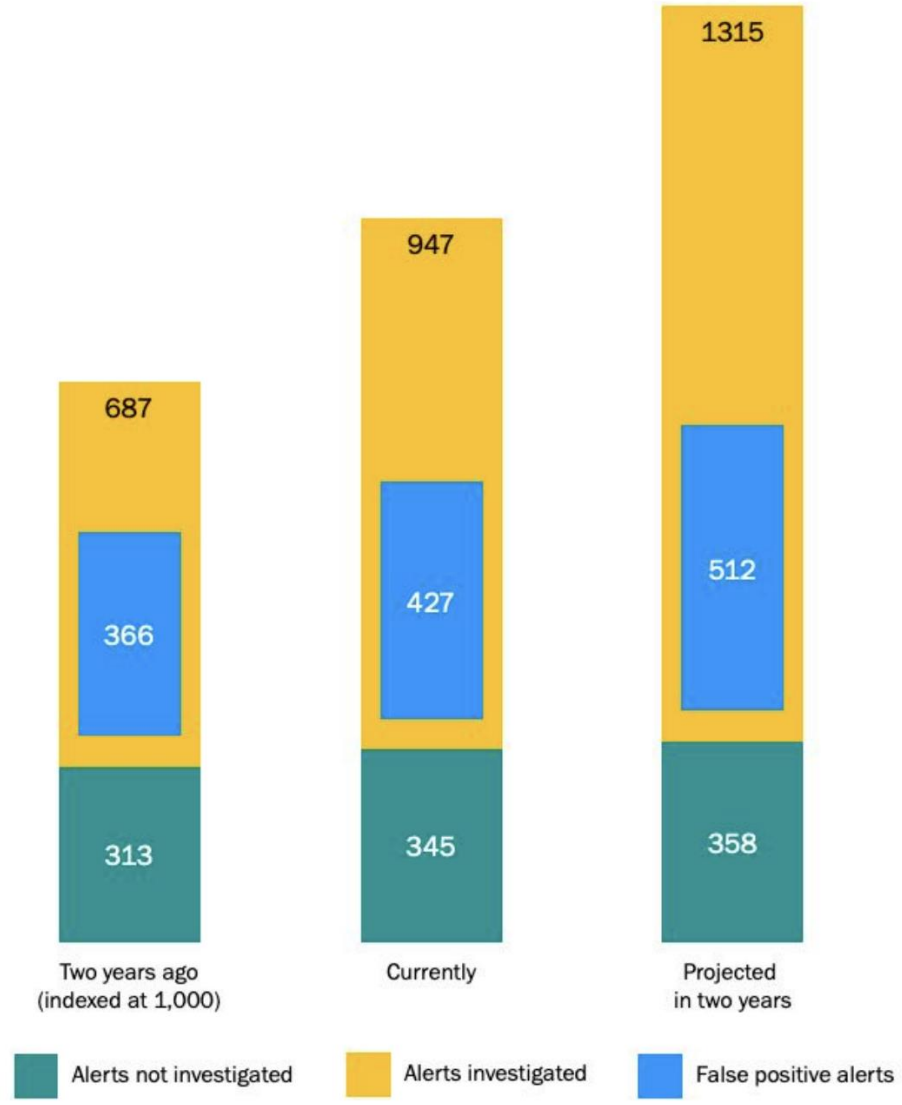
Founder and CEO, Dropzone AI

Daniel Miessler

Founder, Unsupervised Learning

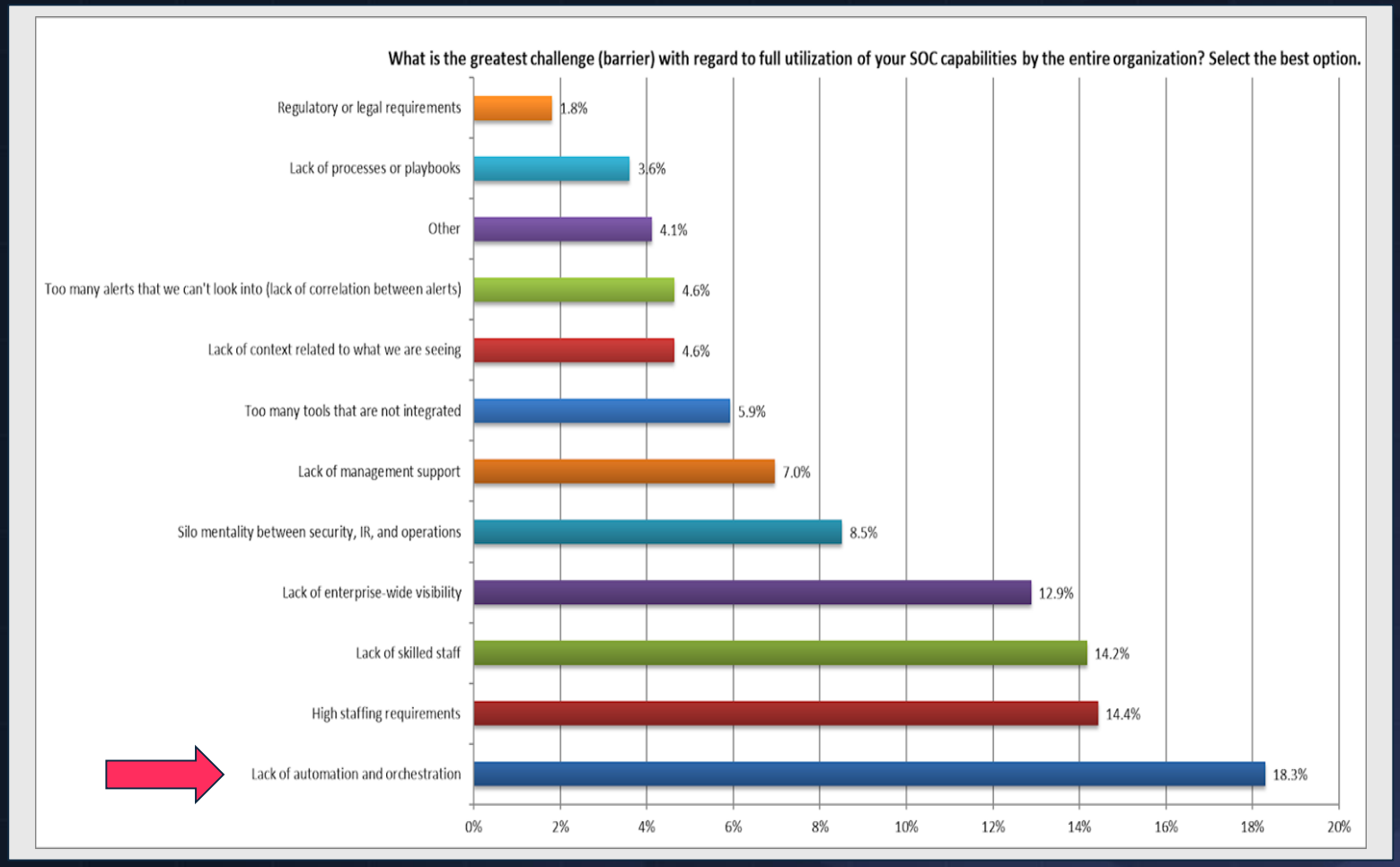
Defenders have a resourcing problem

Figure 3
Number of alerts investigated and not investigated per day—and false positives
Number of alerts per day indexed on 1,000 daily alerts



Source: Osterman Research (2024)

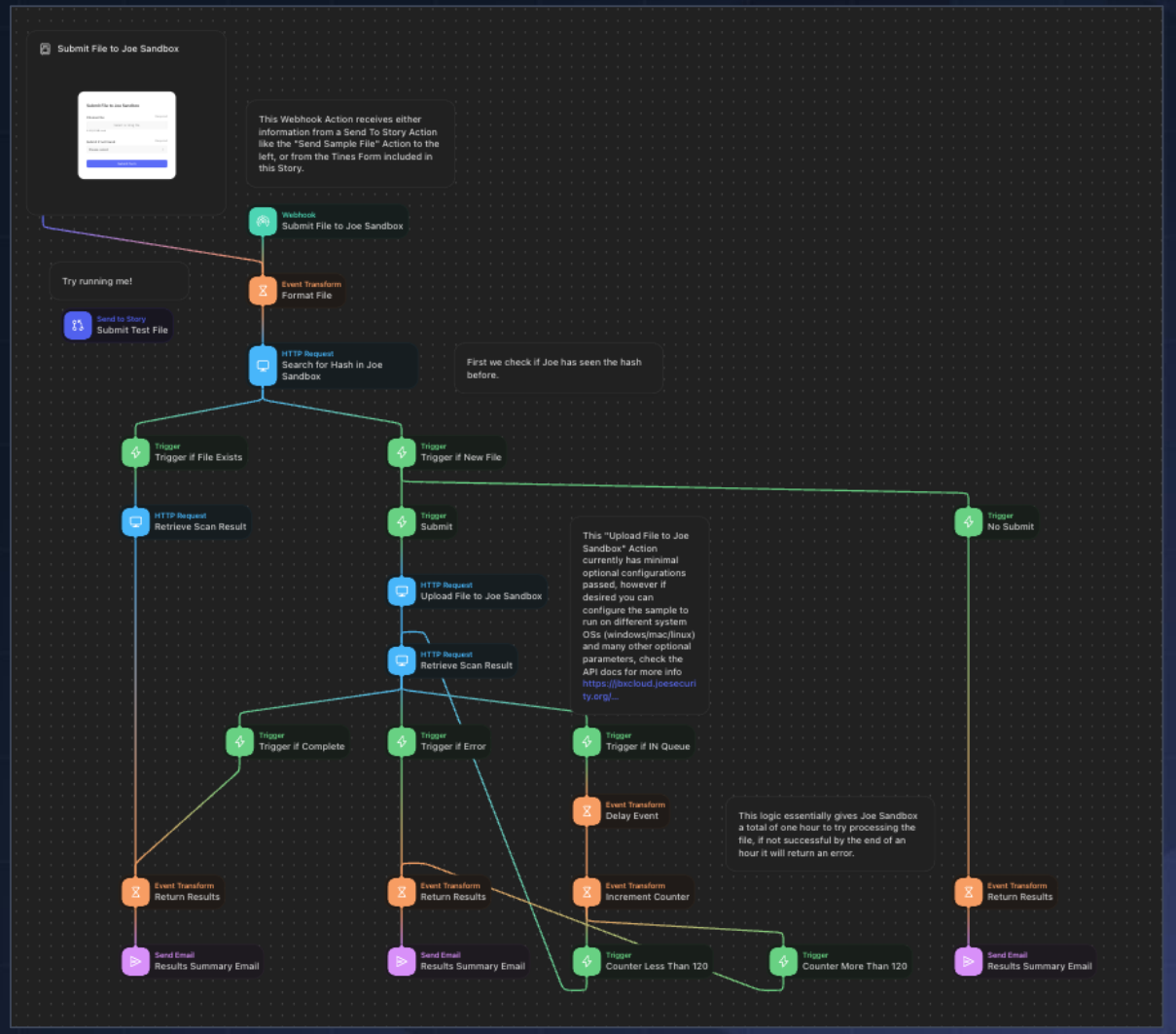
Automation is the biggest gap



Why Is Automation Hard?

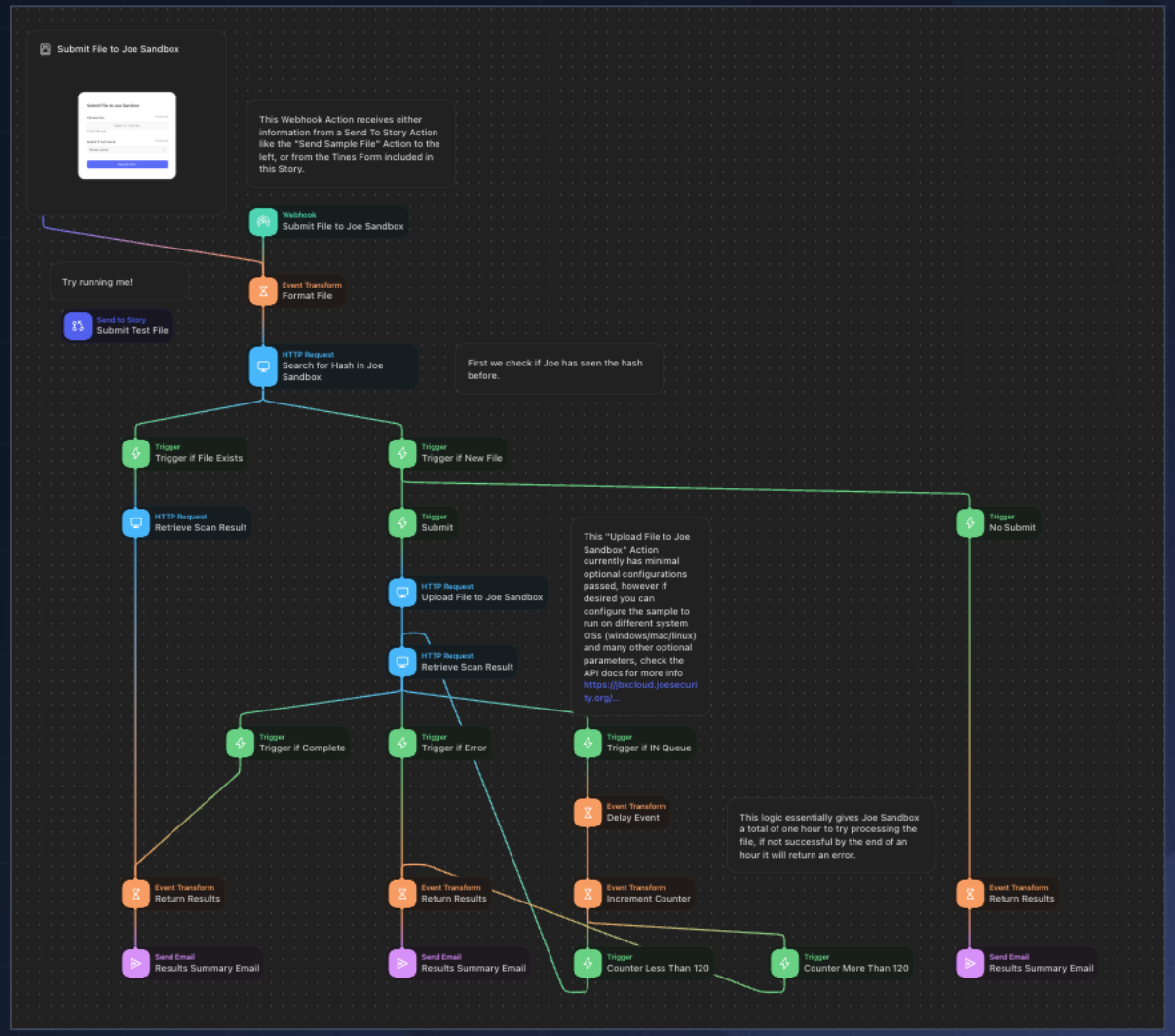
Playbook-based Automation

- The only/best way to automate in the last decade
- Requires robotically spelling out exactly what to do in great detail
- Very deterministic and rigid



Limitations of Playbook-based Automation

- Playbooks are difficult to write
- You need a lot of them
- Expertise required to write playbooks are rare



In the 2024 SANS SOC survey, SOAR ranked:

- #1 in Purchased not implemented
- Bottom 10 in the product GPA

How GenAI Can Help with SOC Automation

Writing SOAR playbooks	Use GenAI to create and update SOAR playbooks
AI copilot/assistant	Boosts productivity in a tool
AI SOC analysts	Replicates Tier 1 SOC analyst investigations

How AI Can Help with SOC Automation

	AI SOC analyst	AI assistant	SOAR playbooks
Percentage of alerts automated	100%	0%	30%
End-to-end alert investigation	✓	✗	✗
No code or prompts	✓	✗	✗
Response automation	~	~	✓
Vendor agnostic	✓	✗	✓

Coverage with Human-Only SOC

The problem of coverage in detection and response is a resources problem

Our threat model

What our current tooling potentially covers

What detections we have built or enabled

Alerts we are staffed to investigate

Alerts we investigate in a timely manner