AI is For More Than Just Finding Threats

Mollie Breen

CEO and Co-Founder,

Perygee Inc.

AI is for more than finding threats

Mollie Breen

CEO & Co-Founder of Perygee

AI is driving threat intel spend to increase 10%

Anomaly Detection

- Email: identifying phishing
- Network traffic: Spotting unusual data exfiltration
- Endpoint Activity: detecting privilege escalation
- User behavior analytics: flagging compromised accounts

Threat Identification

- Suspicious device discovery
- Malware classification
- Vulnerability prioritization
- Automated threat hunting queries

Incident Response

- Alert triage
- Automated playbook execution
- Enrichment

The AI opportunity we are missing

AI isn't just for within tools

Overlooked AI Opportunities

1. Executive dashboards
2. Compliance reporting
3. Approval workflows
4. Policy drift checks
5. Stakeholder communications

AI attacks?
Still hypothetical.

Manual busywork? Very real.

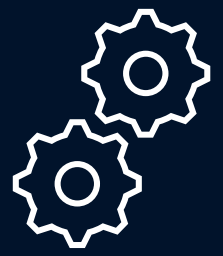
Security analysts spend 3 hrs/day manually triaging alerts.

- IBM X-Force tracked **800k dark web posts** and didn't find AI-engineered attacks at scale

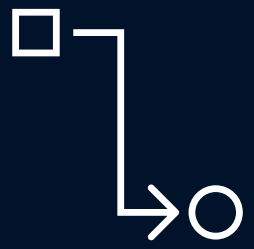
- Reporting, approvals, compliance checks are **slowing** teams down

- We automated defenses for future threats while forgetting **today's time-sinks**

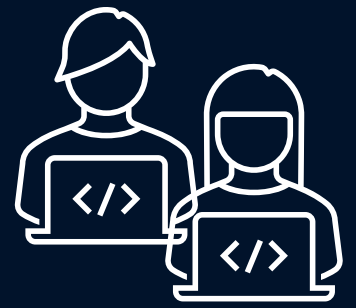
The barriers to automating all aspects of security operations



Tool Fragmentation



Custom Processes



Engineering Investment

A framework for addressing hidden AI opportunities

Four steps to identify and automate overlooked workflows

1. Discovery
2. Prioritization
3. Engage Actual End User(s)
4. Choose the right tool for the job

1. Discovery

Find the workflows worth automating:

- What tasks does your team do more than once?
- What takes the most time each week?
- Where do people complain about "busy work"?
- What would you do if you had a summer intern?

2. Prioritization

ROI matters but so does:

- Number of systems
- Ease of access to related systems
- Number of stakeholders
- Complexity of workflows

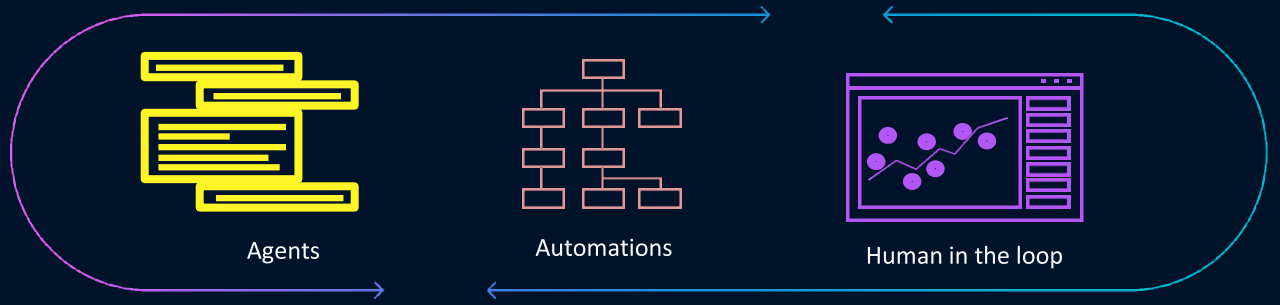
3. Engage the actual end user(s)

Talk to the people doing the work

- Understand the real workflow, not the documented one
- Identify pain points and manual steps
- Get buy-in early

4. Choose the right tool for the job

AI should be in conjunction with automation and human-in-the-loop



AI-powered transformation vuln mgmt

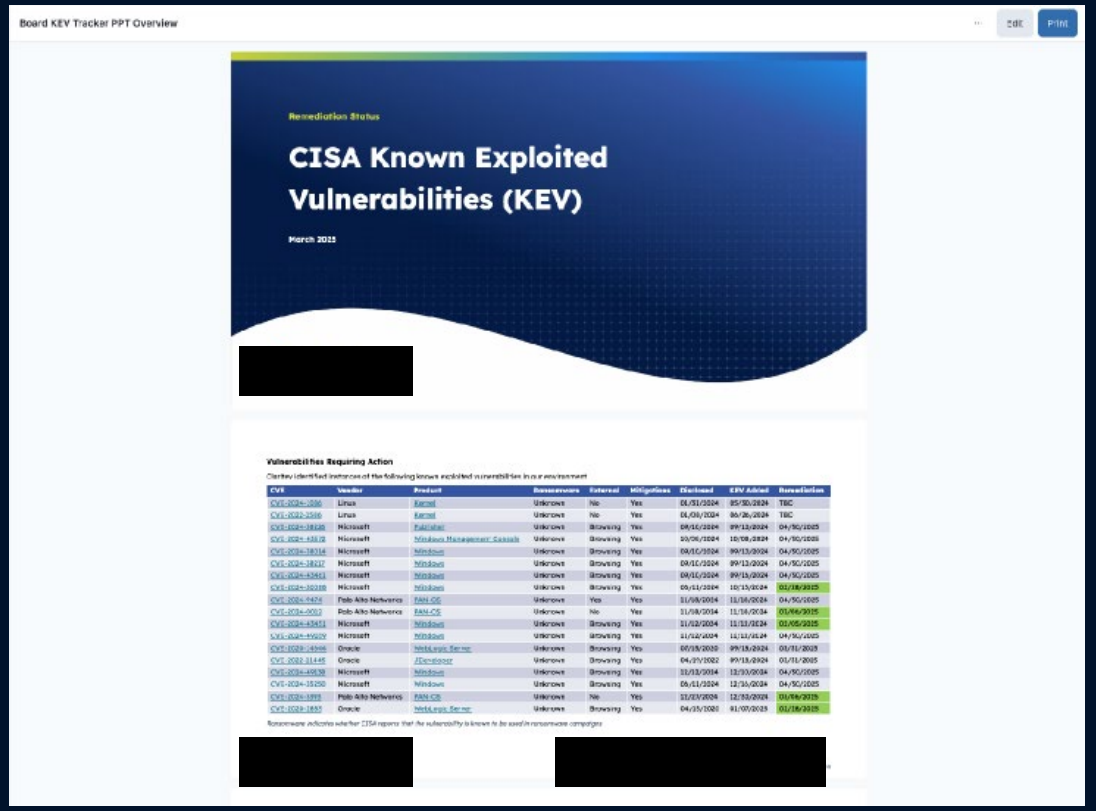
BEFORE

- ✗ CISA releases new Known Exploited Vulnerabilities everyday
- ✗ 12 hrs/week creating a PPT with applicable vulnerabilities

AFTER

- ✓ Automation pulls all vulnerabilities from CISA
- ✓ AI model detects whats relevant
- ✓ Human-in-loop pages for auto-generated PowerPoint

*Security team saves 12hrs/week, extended workflow to **2 new sources**, and **discovered unhandled KEVs** missed in manual tracking*



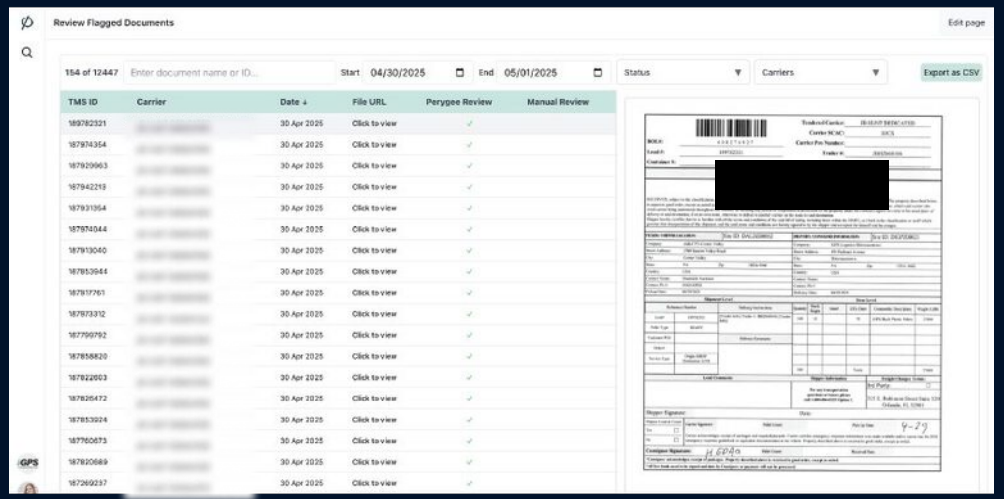
AI-powered transformation proof-of-deliveries

BEFORE

- ✗ Industry relies on paper to track 1000s of deliveries/month
- ✗ Tracking down missing pallets is a key loss

AFTER

- ✓ Automation pulls all forms
- ✓ AI model detects and approves valid forms
- ✓ Suspicious forms are flagged and reviewed with UI



IT team saves ~80hrs/mon, increases cash flow by ~2 days, and improves customer experience-- creating a competitive advantage in a fast growing industry

Key Myths

Myth #1

✗ Start with processes that are already documented

✓ Start small and iterate

Myth #2

✗ Success is measured in time

✓ Business metrics (fewer returns, more sales)

Myth #3

✗ Avoid people who don't want to adopt AI

✓ Lead with answers not AI

Myth #4

✗ AI is for insights

✓ AI is for insights and action

GETTING STARTED TODAY

1. Pick ONE workflow that takes >2 hours/week
2. Talk to the person doing it (not their manager)
3. Map the real process, not the documented one
4. Start small - automate one step

- AI is for more than just threats
- Start with what hurts
- Automate to completion not just insights
- Small wins build momentum

AI predictions

- AI taking on multiple steps
- AI moves from application to workflows
- AI iteration speed becomes the competitive moat

Q&A