01 GRAYHATCON 2020 // BLUE TEAM VILLAGE

The Future of Security Automation is Collaborative

MARK ORLANDO | BIONIC CYBER

About me

19 years in security operations

Co-founder & CEO, Bionic

Former White House, DoE, Raytheon, MSSP, MDR

SANS Instructor, SEC450 and MGT551

@markaorlando

About this talk

In security operations, we're often losing the battle.

Automation vendors have sold us a bill of goods.

Robots aren't going to save us, but they CAN help us.

Common challenges in SecOps

Question 1

Where do I spend my time?

Question 2

What alert(s) do I focus on first?

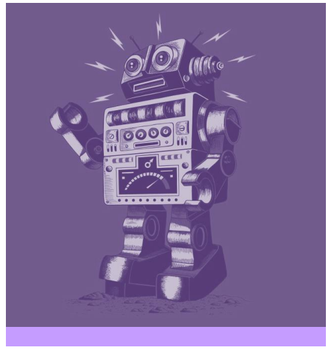
Question 3

What am I not aware of?

Question 4

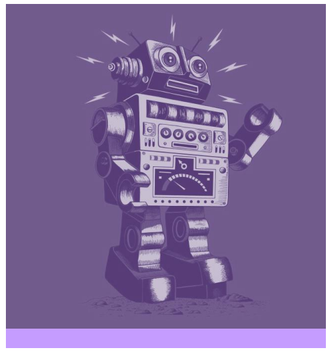
I don’t know where to go from here so is it cool if I just stop?

Security automation today



Orchestration

“Spend 20 hours a month creating and managing an automated playbook and in return I will save you 5 hours a month.”



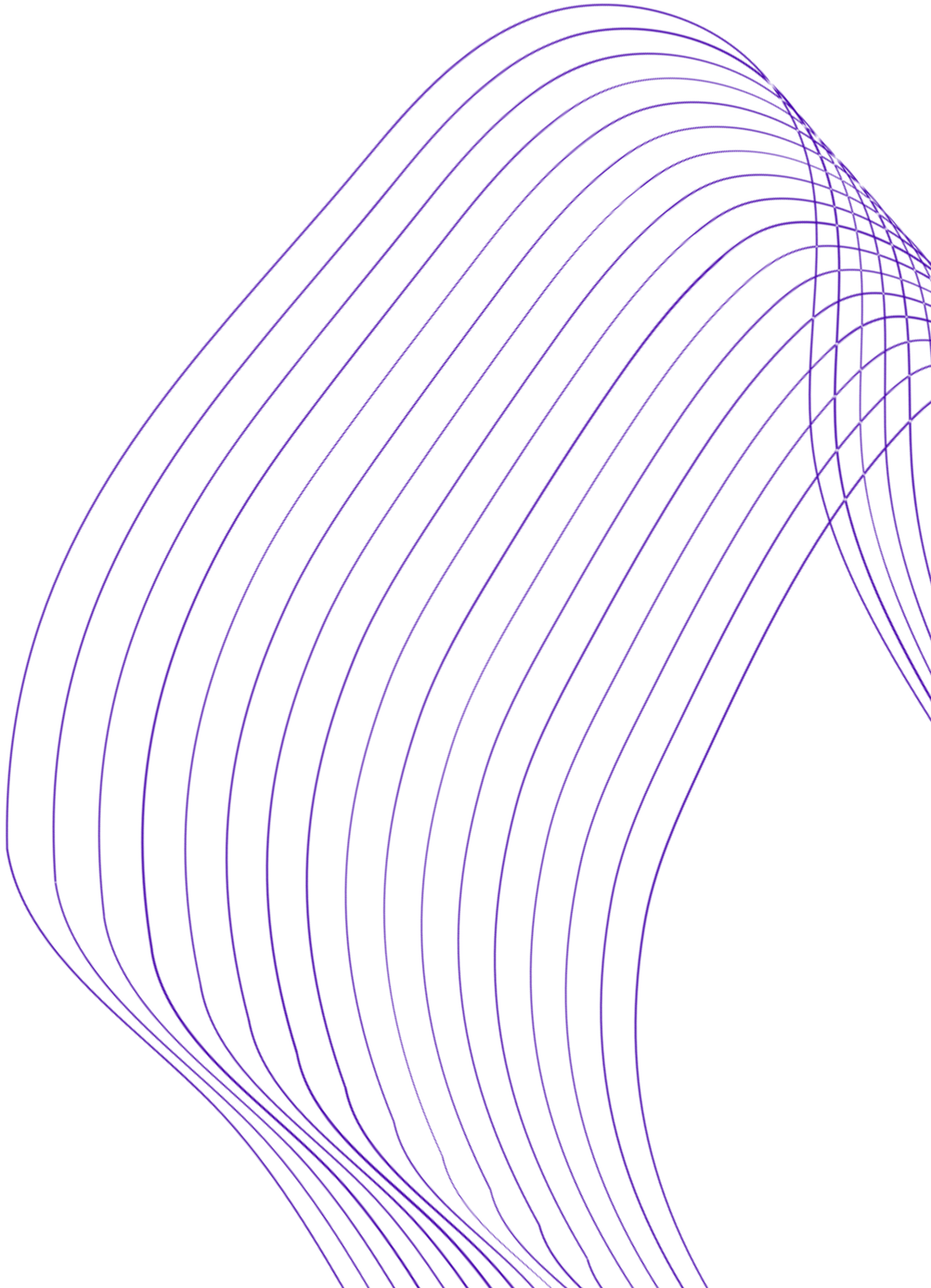
Threat Detection

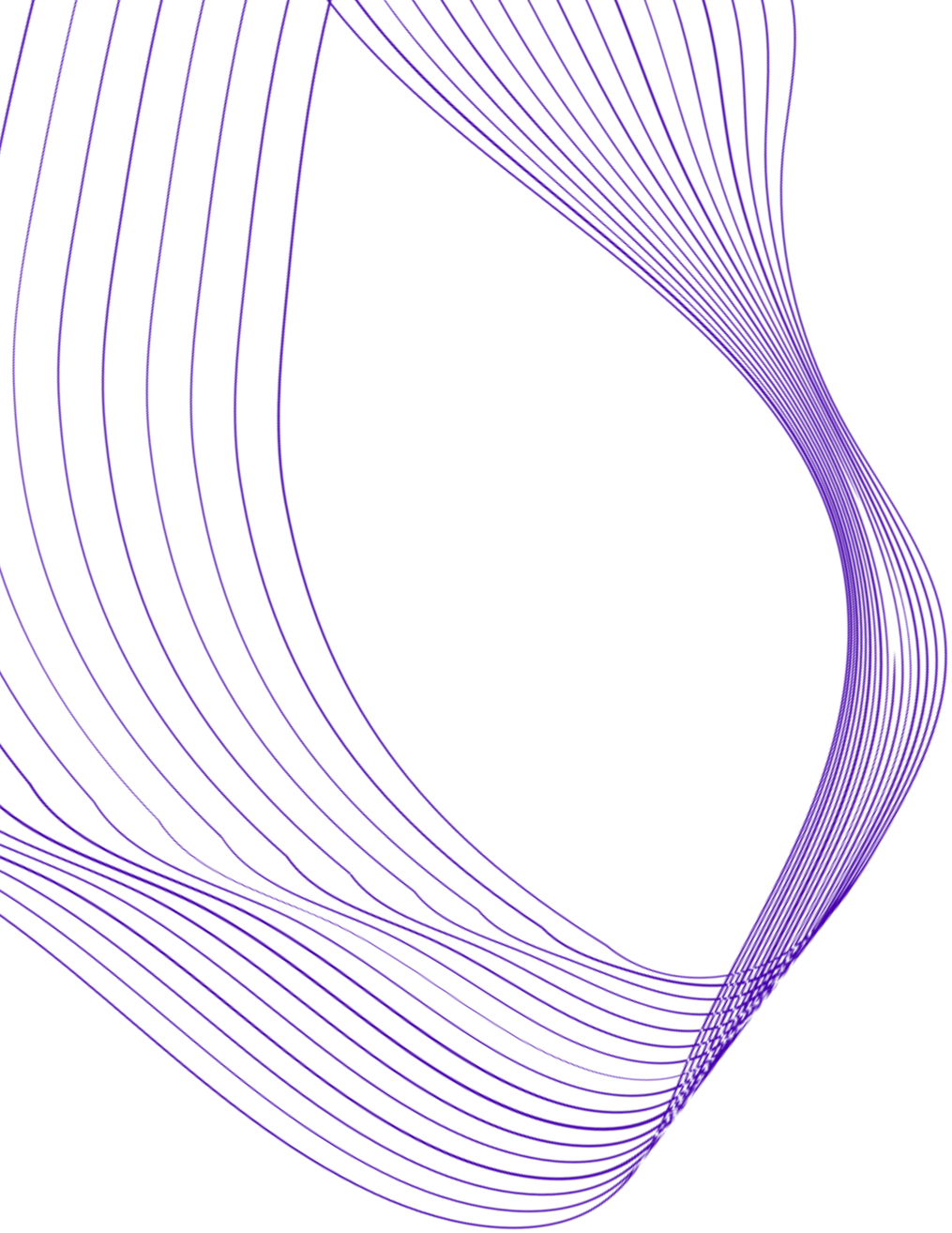
“I’ll find all of the APTs and bespoke zero days you can’t recognize. Most of them are from Europe, you’ve probably never even heard of them.”

@MARKAORLANDO

But seriously

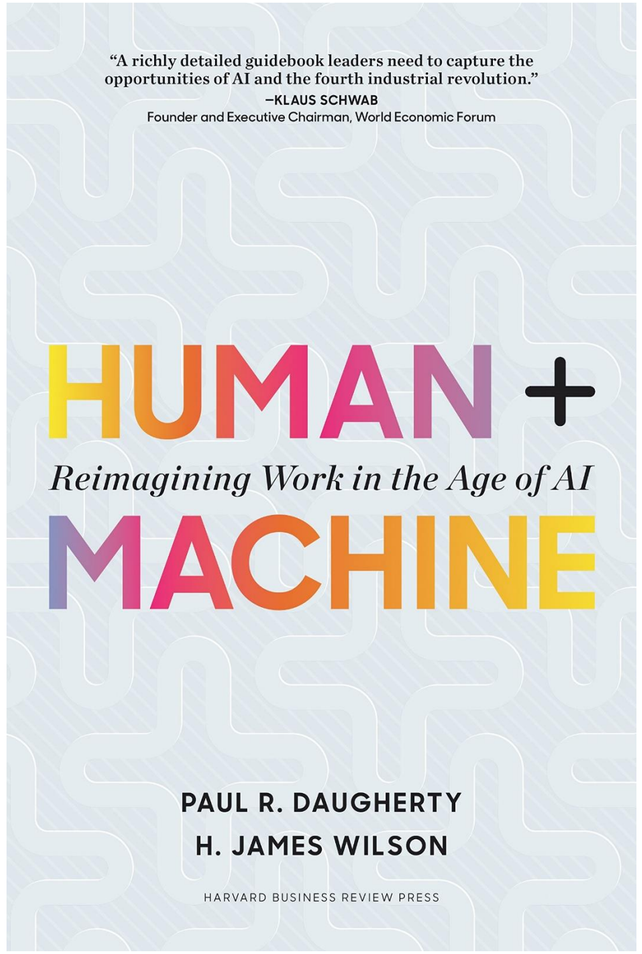
- Are we really automating response, or renaming robotic process automation?
- Playbooks usually have a one:one relationship to SOC workflows.
- Humans are still better than machines at creating detections.





Good news

- You probably don't need "next gen" tools to find all the things.
- We just need to take what we already know and apply that knowledge at scale.
- We CAN use tech to do this!



Enter the "Missing Middle"

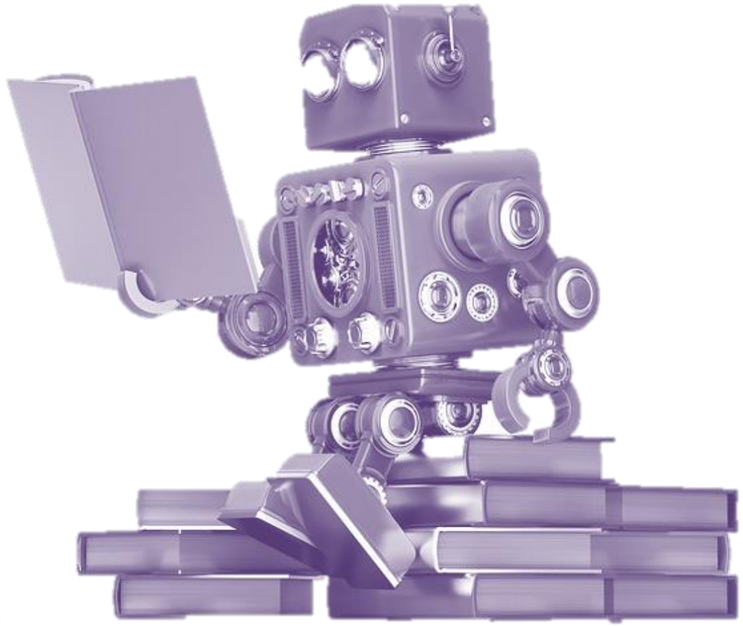
The place where humans and machines work together to amplify each other's strengths, not divide up the work.

Security operations is a team sport, but collaboration is an overlooked "missing middle" when it comes to automation.

Collaborative intelligence, or CQ, enables teams to better recognize individual gaps and fill them with shared knowledge and expertise.

Successful detection & response requires*:

1. Integration of both technical and social processes, i.e. collaboration and communication
2. A learning climate where we can quickly assimilate and act upon new information
3. Behavioral influences like regular feedback
4. Analysts empowered to do what they do best: think creatively, make decisions, and solve problems**



*“Improving the Social Maturity of Incident Response Teams” by Tetrick, Zaccaro et. al.

** https://www.usenix.org/system/files/conference/soups2015/soups15-paper-sundaramurthy.pdf

Implications for security automation

- RPA != Automated response
- Time to rethink or expand what we consider to be “security automation”
- We must refocus on improving CQ and filling the missing middle

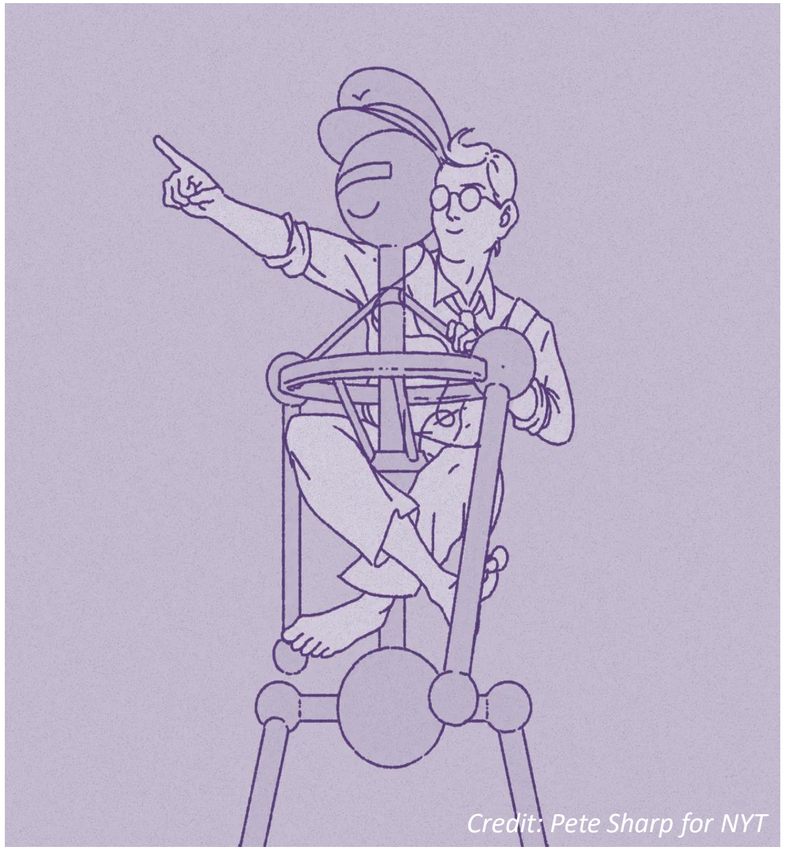
A new approach

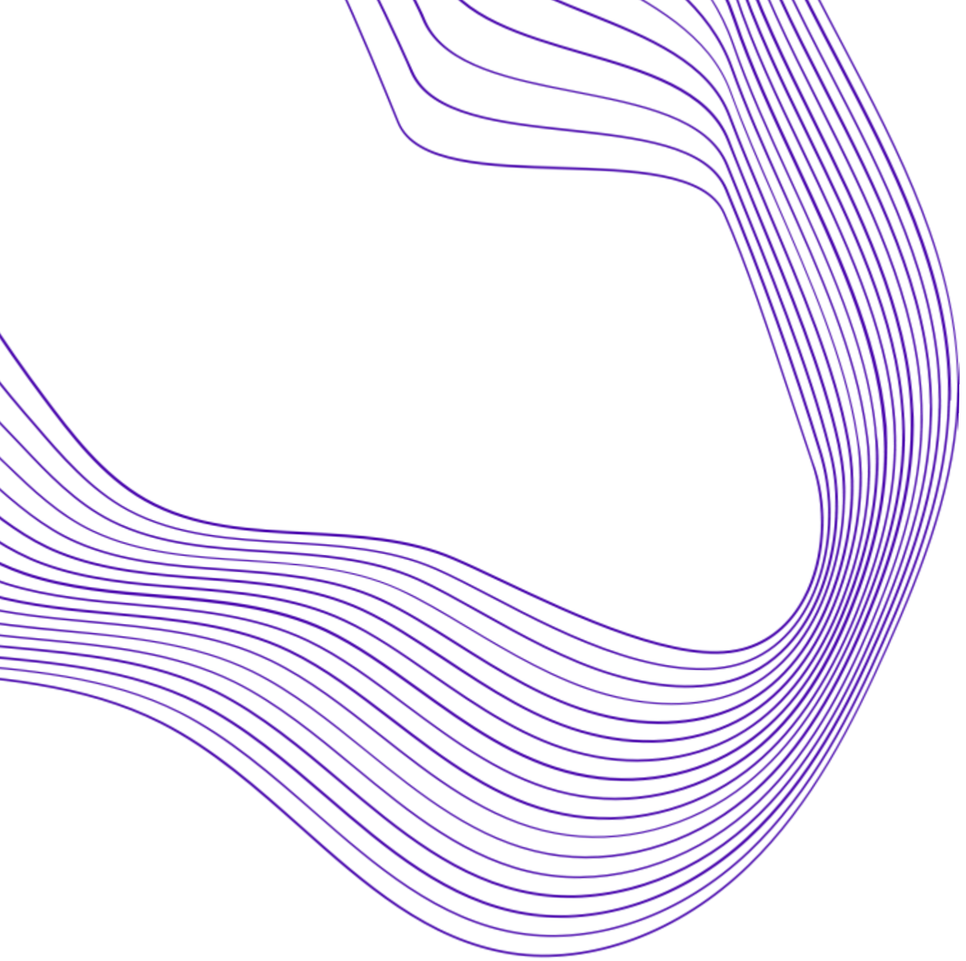
1. Identify actions that demonstrate knowledge and expertise we're looking for.

2. Distill items that are useful in multiple contexts – for example, understanding the environment or threat model.

3. Use those items to bridge the gap between automated tasks and human judgement.

4. We can't automate what we can't anticipate - modular, assistive automation may be better for lots of SOC tasks!





Use Cases

Use Case #1:

Alert triage and investigation

- Alerts coming in from multiple sources, not everything captured in a SIEM
- Wide variety of contextual information, lots of social dynamics at play – many VIPs, urgent items not necessarily aligned to a cyber threat model
- Evidence of cherry-picking alerts, inconsistent assignment of tasks and investigations

Use Case #1: Approach

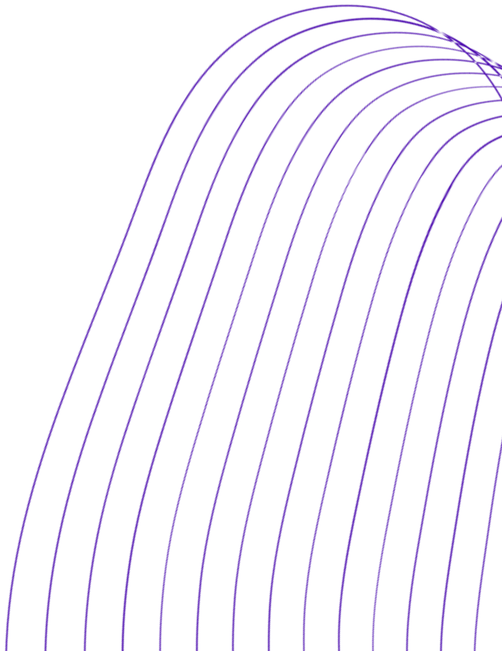
- Survey analysts
- Model analyst interaction with security tools – what event sources do they access most, what queries do they run, which result in incident tickets
- Align data sources to threat model and TTP visibility
  - ✓ What threats does the org care about most?
  - ✓ What can we see based on the data we have?

Use Case #1: Approach (cont.)

- Threat model + visibility = priorities
- Prompt analyst to prioritize alerts and queries more aligned to threat model
- Enrich alerts with user, group, or threat info that makes triage clearer/easier
- Create remedial training and security sprints

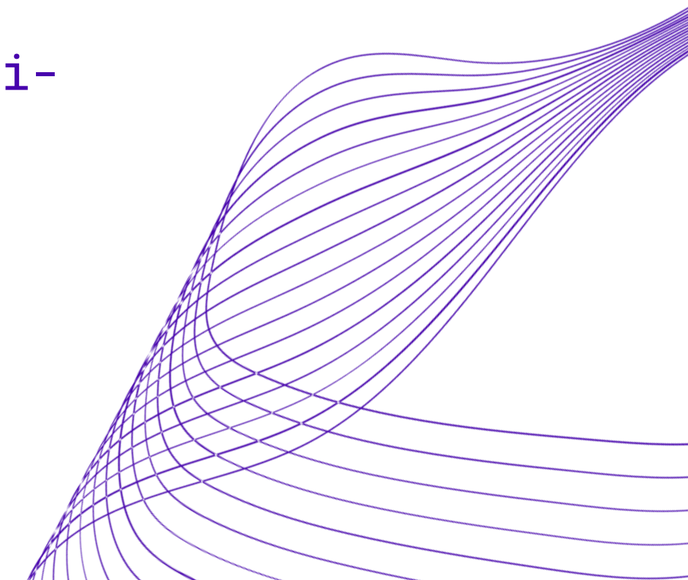
Use Case #2: Adaptive playbooks

- Playbooks can be overly rigid when used exclusively to guide an investigation
- Questions or tasks are sometimes situational within a given incident type, i.e. phishing a VIP
- Completeness of an investigation often depends on validation by other team members



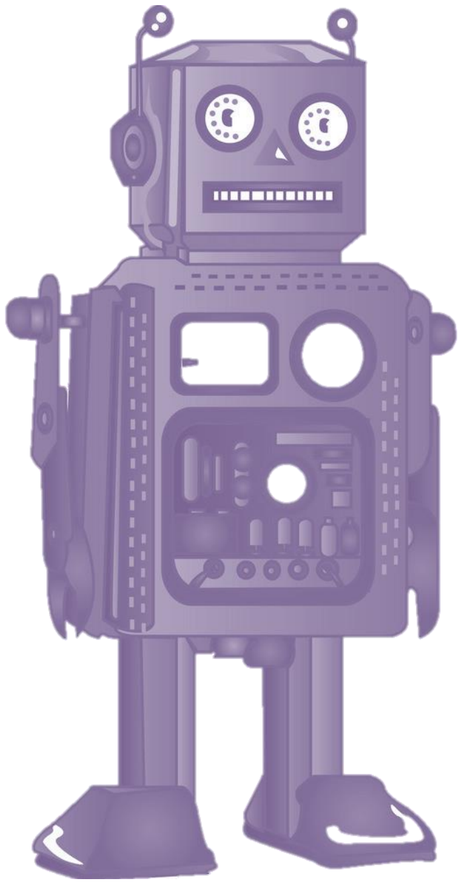
Use Case #2: Approach

- Analyze initial data entry and case notes
- Identify and enrich key data points
- Prompt analyst for situation-specific tasks or questions
- Why not use custom drop downs and dynamic fields or multi-step playbooks that take user input? Because…



Conclusion

- We often say there is no easy button in security but then pay $$$$ for prospective easy buttons
- Can’t always rely on pre-built playbooks or AI-driven voodoo magic
- RPA is still important and necessary
- Best automation is that which enables people and computers to work more effectively together

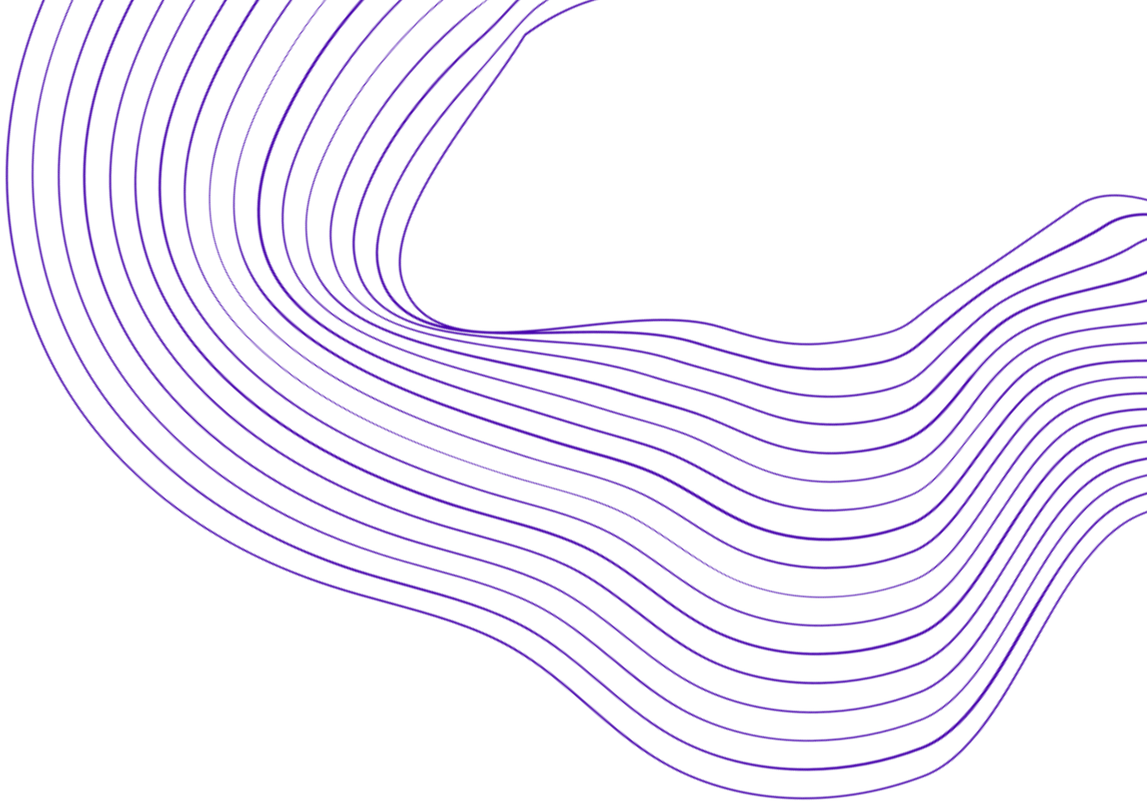


LET’S KEEP IN TOUCH

@markaorlando

mark@bioniccyber.com

https://bioniccyber.com



Thank you!