SANS | CYBERSECURITY LEADERSHIP

Co-bots, Not Robots: AI in Security Operations

Mark Orlando

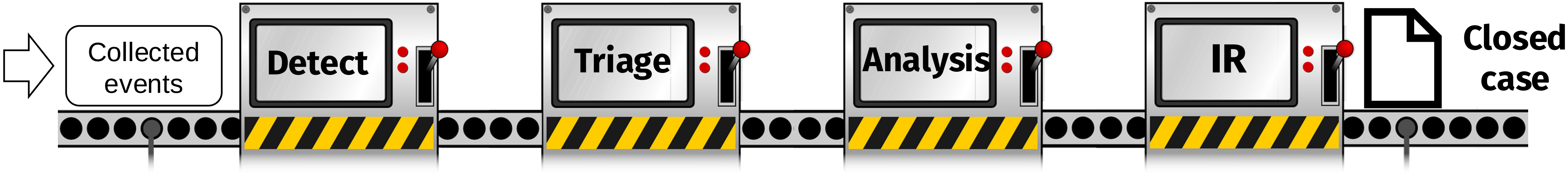
SANS SECURITY WEST 2024

Co-Bots, Not Robots!

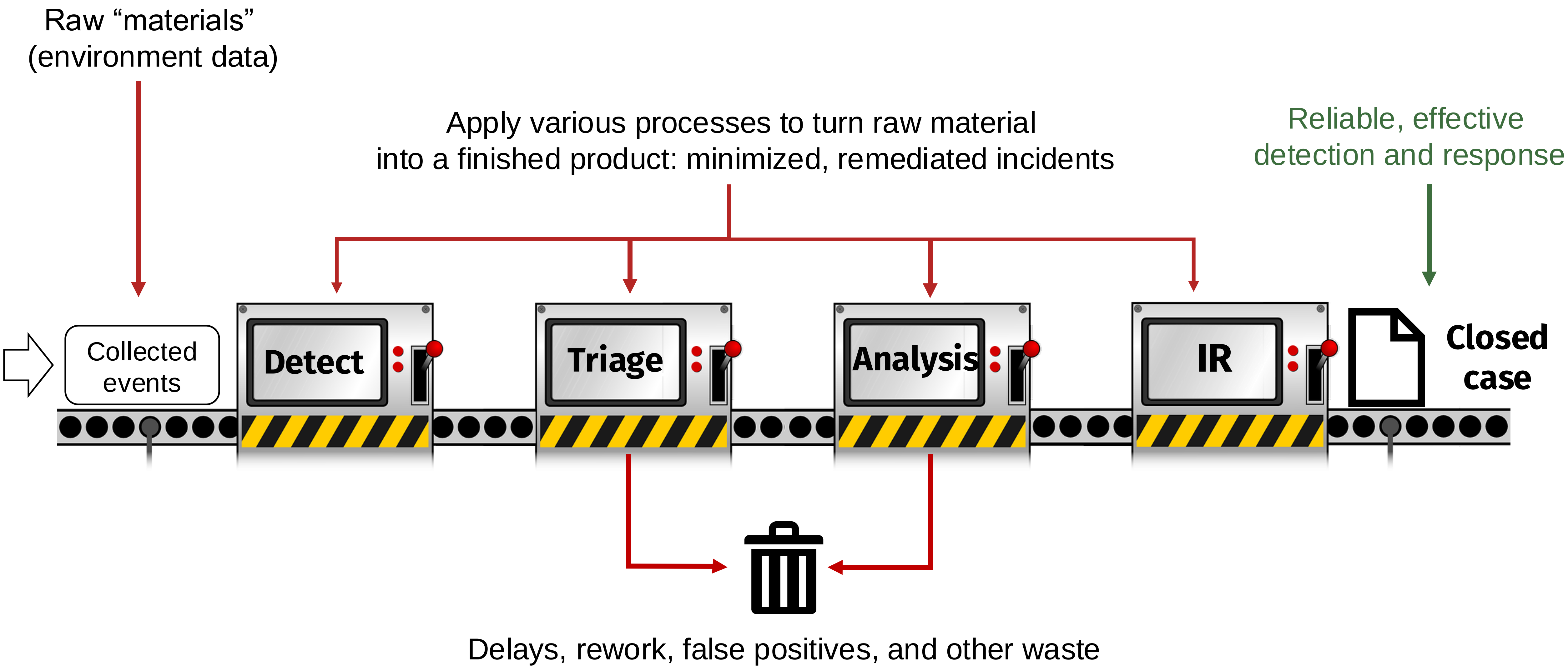
1. The Detection and Response Pipeline
2. Automation Goals
3. AI Product Space
4. AI Challenges in the SOC
5. Evaluating AI Solutions
6. Use Cases and Conclusion

The Detection and Response Pipeline (1)

By arranging core security operations functions into a process, we can visualize the SOC as a production line:



The Detection and Response Pipeline (2)


Raw "materials"
(environment data)
Apply various processes to turn raw material
into a finished product: minimized, remediated incidents
Reliable, effective
detection and response
Collected events
Detect
Triage
Analysis
IR
Closed case
Delays, rework, false positives, and other waste

Challenges "Built In" to the Pipeline

- **Scale:** scaling expertise across time (shifts), geography, and individuals with varying specialties and experience
- **Observability:** high-quality alerts with context for analysts, insights into SOC functions for managers
- **Capacity:** the ever-growing volume of alerts and telemetry consumed by SOC teams combined with repetitive and manual workflows
- **Focus:** analysts struggle to decide where best to spend their time which leads to inconsistency, wasted cycles, and process bottlenecks
- **Quality:** Predictable work products relatively free of defects, rework, waste, and other issues

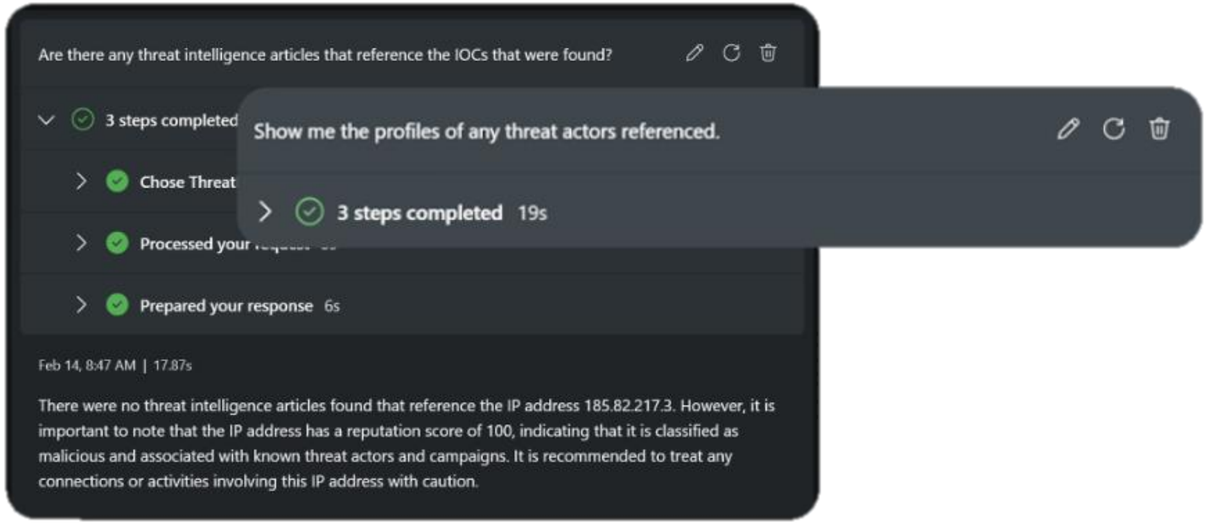
AI is a form of automation we can use to address these!

Automation Goals

- **Address the “missing middle”:** [2]
  - → Where humans and machines work together to amplify each other’s strengths, not divide up the work
- **Increase *speed:*** Reach the next step in the process faster, with less waste or rework
- **Reduce *toil:*** manual, repetitive tasks that “do not add enduring value”
- **Improve *quality* and *consistency*** in our pipeline

The SOC/AI Product Space

- **Generative AI** to gather contextual data, identify potential investigative steps, and summarize investigations
- **Supervised machine learning** to automate triage and response decisions
- **Predictive AI** to generate threat detection use cases or identify malicious content
- **AI models** to adjust alert severity scoring based on deviations in alert details and other context



Are there any threat intelligence articles that reference the IOCs that were found?

3 steps completed

Chose Threat

Processed your

Prepared your response 6s

Show me the profiles of any threat actors referenced.

3 steps completed 19s

Feb 14, 8:47 AM | 17.87s

There were no threat intelligence articles found that reference the IP address 185.82.217.3. However, it is important to note that the IP address has a reputation score of 100, indicating that it is classified as malicious and associated with known threat actors and campaigns. It is recommended to treat any connections or activities involving this IP address with caution.

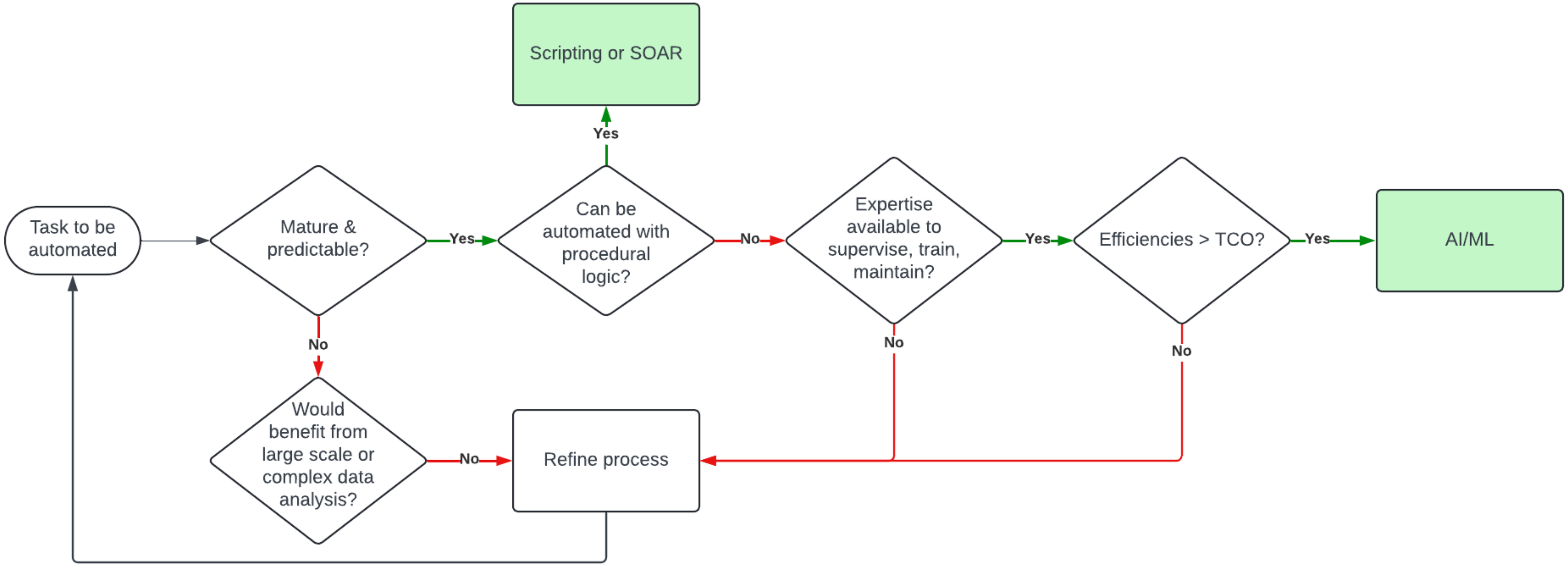
Microsoft Copilot for Security

Challenges in SOC Use Cases

- **Ground truth**
  - → SecOps is often an unbounded problem
  - → For example: reduce false positives in our detection function
    - – A false positive and a true positive may have 99.9% identical attributes
- **Training data**
  - → Aggregated logs, alerts, analyst inputs (actions, case notes) are dubious source of truth
    - – Log data may be missing fields and/or parsed incorrectly
    - – Key data points like alert disposition may not be captured or available
  - → Training data may be sensitive, i.e. incident history, security policies, etc.
- **Transparency**
  - → If “x” is bad, why?
  - → Mainly an issue with unsupervised machine learning and predictive AI
  - → Modern networks have TONS of weird things going on that are legitimate

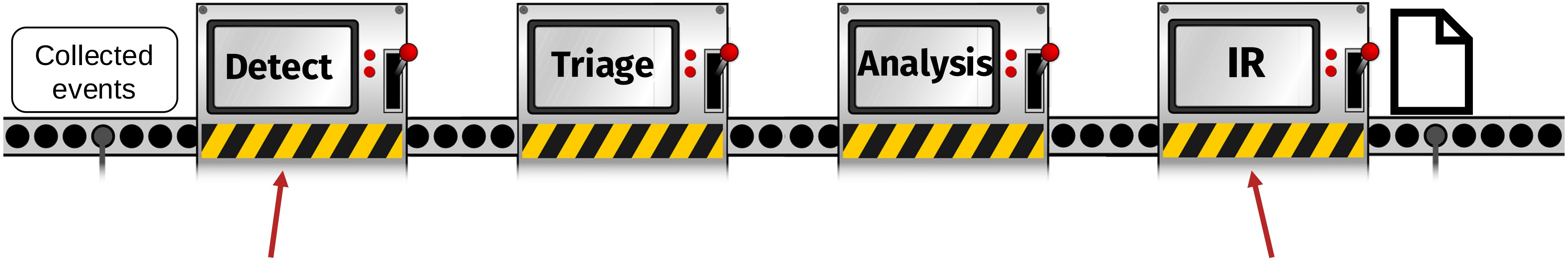
Feasibility Analysis

- Total cost of any automation should not exceed cost savings *unless* it provides measurable strategic value (“we would not have found x without this solution”)
- Value determination requires **metrics** on utilization, performance, quality


Task to be automated
Mature & predictable?
Yes
No
Can be automated with procedural logic?
Yes
Scripting or SOAR
No
Expertise available to supervise, train, maintain?
Yes
No
Efficiencies > TCO?
Yes
AI/ML
No
Would benefit from large scale or complex data analysis?
No
Refine process

Choosing the Right Solution

- Not all improvements address the real bottleneck(s), and not all have equal value
- Some tasks should be at least partially manual
- Consider **lead measures** for your SOC pipeline and the **theory of constraints**



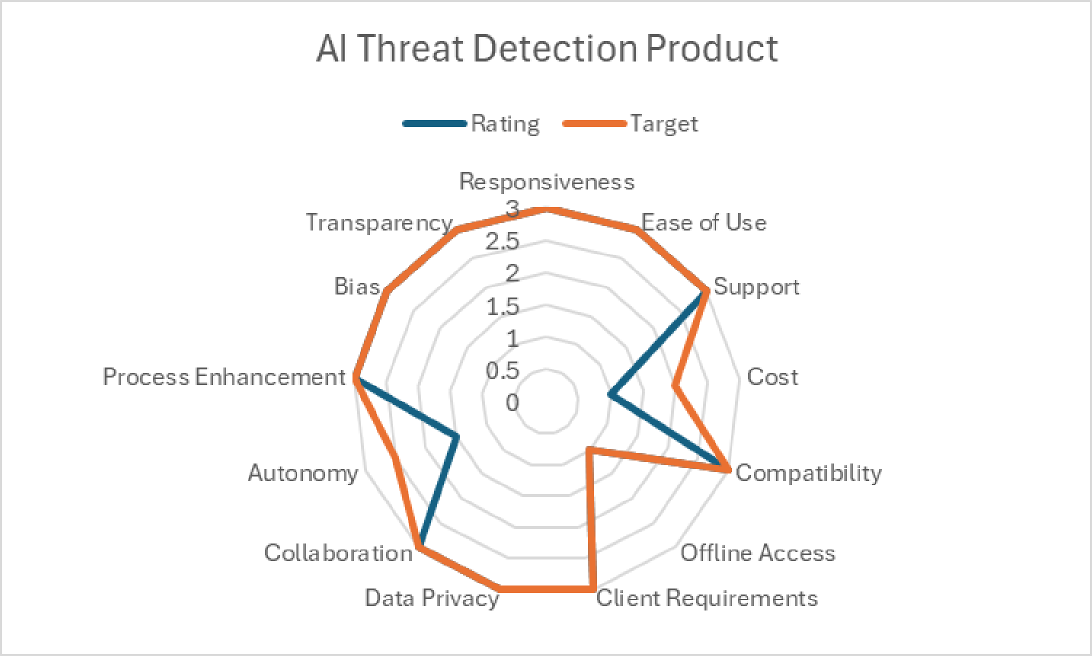
If the bottleneck is here… …improvements here won't help!

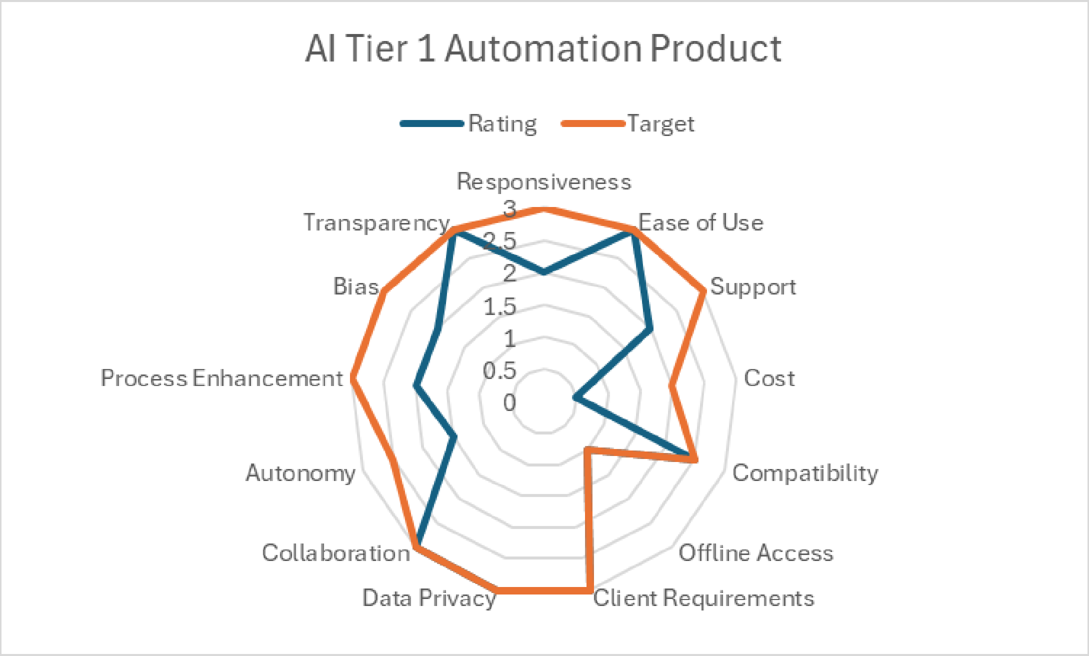
A Framework for Evaluating AI Solutions (1)

CRITERIA	DEFINITION
Responsiveness	Speed and accuracy of responses
Ease of Use	Intuitiveness of the interface
Support	Availability of support channels/community
Cost	Licensing, labor, and usage costs
Compatibility	Supports operating systems, browsers, and integrations
Offline Access	Sufficient availability of offline functionality
Client Requirements	Requirements for additional downloads/client software
Data Privacy	Data protection and user control
Collaboration	Collaborative features or enablement
Autonomy	Enables meaningful learning/results without significant oversight
Process Enhancement	Range of cognitive tasks supported
Bias	Bias mitigation built into the solution
Transparency	Decision-making process or output can be clearly explained

A Framework for Evaluating AI Solutions (2)

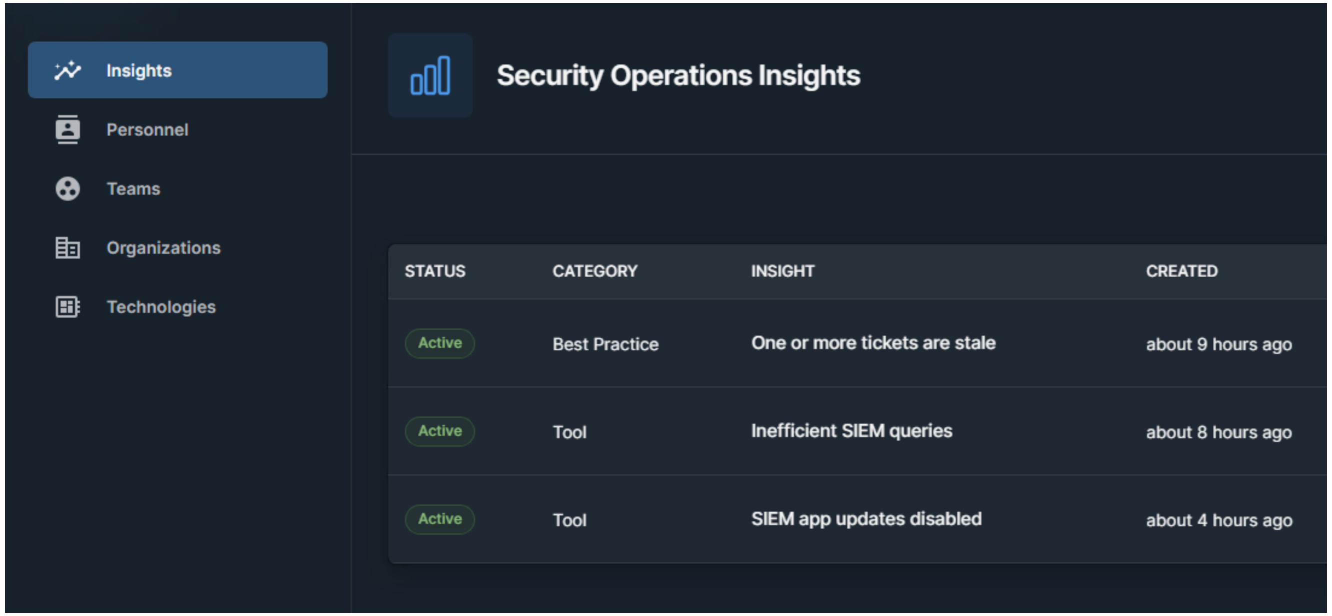
- Criteria rated on scale of 1-3
- Compare to solution requirements (target)
- Some examples:





AI Use Cases for the SOC

- **Aggregation and summarization**
  - → Threat intelligence
  - → Incident/investigation reports
- **Structured brainstorming**
  - → Hypothesis generation for hunting
- **Recommendation engine**
  - → Suggested use cases or playbooks
  - → Hypothesis generation for hunting
- **Supporting tasks or insights**
  - → Automate repetitive actions
  - → Identify interesting patterns/relationships/insights
  - → Provide context for alerts, vulnerabilities, playbooks



Security Operations Insights

STATUS	CATEGORY	INSIGHT	CREATED
Active	Best Practice	One or more tickets are stale	about 9 hours ago
Active	Tool	Inefficient SIEM queries	about 8 hours ago
Active	Tool	SIEM app updates disabled	about 4 hours ago

SOC workflow insights and recommendations in Bionic's ARM platform

Conclusions

- **AI is an exciting and potentially powerful ally in extending SOC capabilities**
  - A manual detection and response pipeline supported by a team requires immense effort to sustain
  - Skilled workers isn’t the problem, applying and scaling their expertise is
  - <u>We need co-bots, not robots</u>
- **Transparency is key**
  - Generative insights can be useful if not conclusive
  - Good metrics for SOC functions can shed light on efficiencies gained through AI
- **Objective approach** necessary to gather requirements, evaluate solutions, and select the right tool

Additional Resources

- **David Hoelzer on the Blueprint Podcast**
  - → https://www.sans.org/cyber-security-courses/applied-data-science-machine-learning/
- **Generative AI Insights with SANS Fellow Frank Kim**
  - → https://www.youtube.com/watch?v=L6Z0GxxiHBI&t=511s
- **Human + Machine: Reimagining Work in the Age of AI by Paul Daugherty and H. James Wilson**
- **SANS SEC595: Applied Data Science and AI/Machine Learning for Cybersecurity Professionals**
- **SANS LDR551: Building and Leading Security Operations Centers**

SANS | CYBERSECURITY LEADERSHIP

Thank You

Mark Orlando
mark@bioniccyber.com
https://www.linkedin.com/in/marko16/