Carson Zimmerman

How to Save Your SOC From Stagnation

FIRST 2023

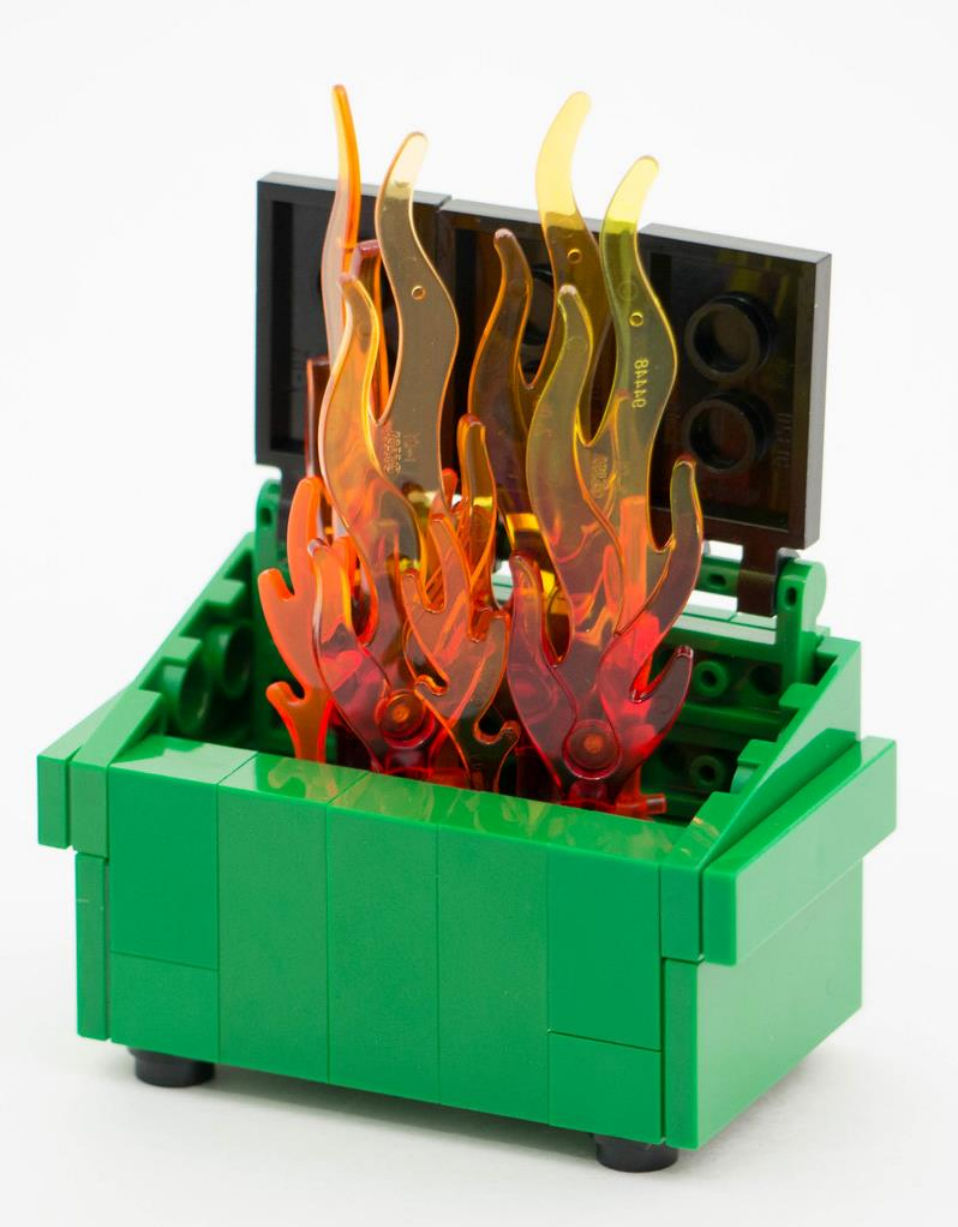
Problem Statement

You work in a
Security Operations Center (SOC)

You're overwhelmed
Alerts are full of FPs
Data is missing
Processes are a tarpit
Everything sucks
Nothing is getting better

Rage quit or ¯_(ツ)_/¯ ???

https://knowyourmeme.com/photos/962640-this-is-fine



https://www.flickr.com/photos/billward/31471639755

In the next ~20 minutes…

7 tools to integrate empowerment and improvement into the SOC:

- Learn constantly
- Feel heard
- Grow careers
- Translate problems into action

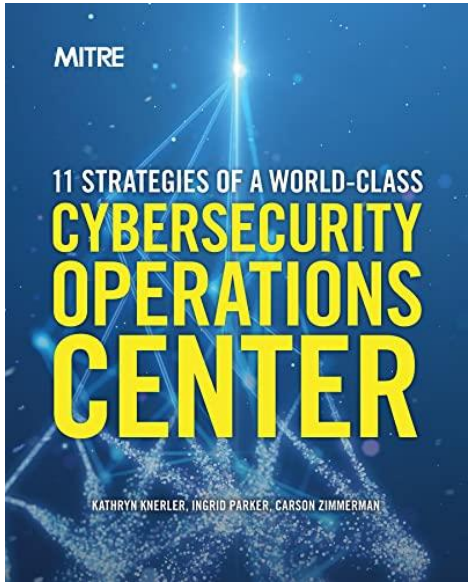
Achieve more effective & efficient detection, analytics, investigation, and response

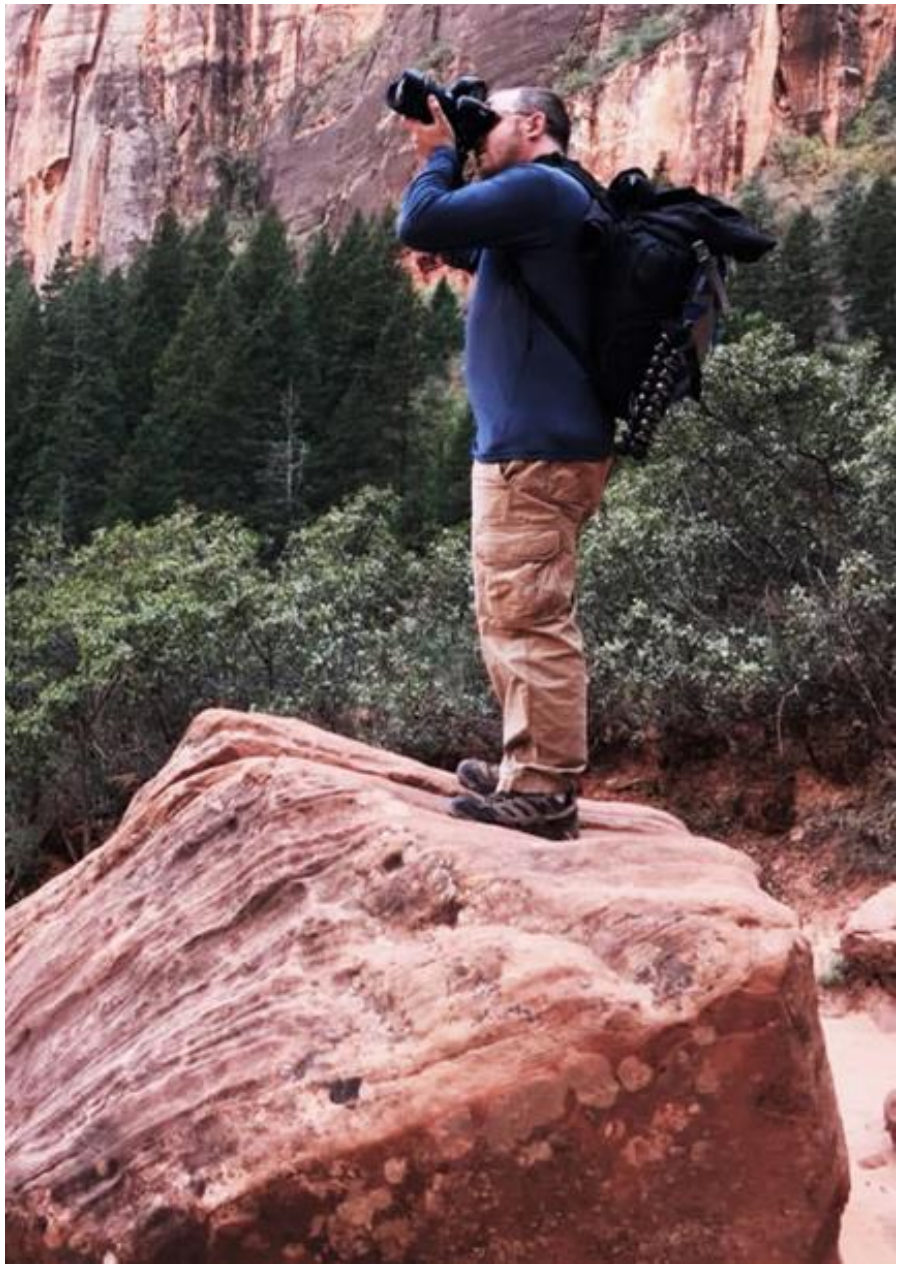
Make at least one of these 7 routine expectation and your life will improve

About Carson

- Worked in Security Operations for >20 years
- SOC investigations team lead @ Microsoft
- Check out my book if you haven't already

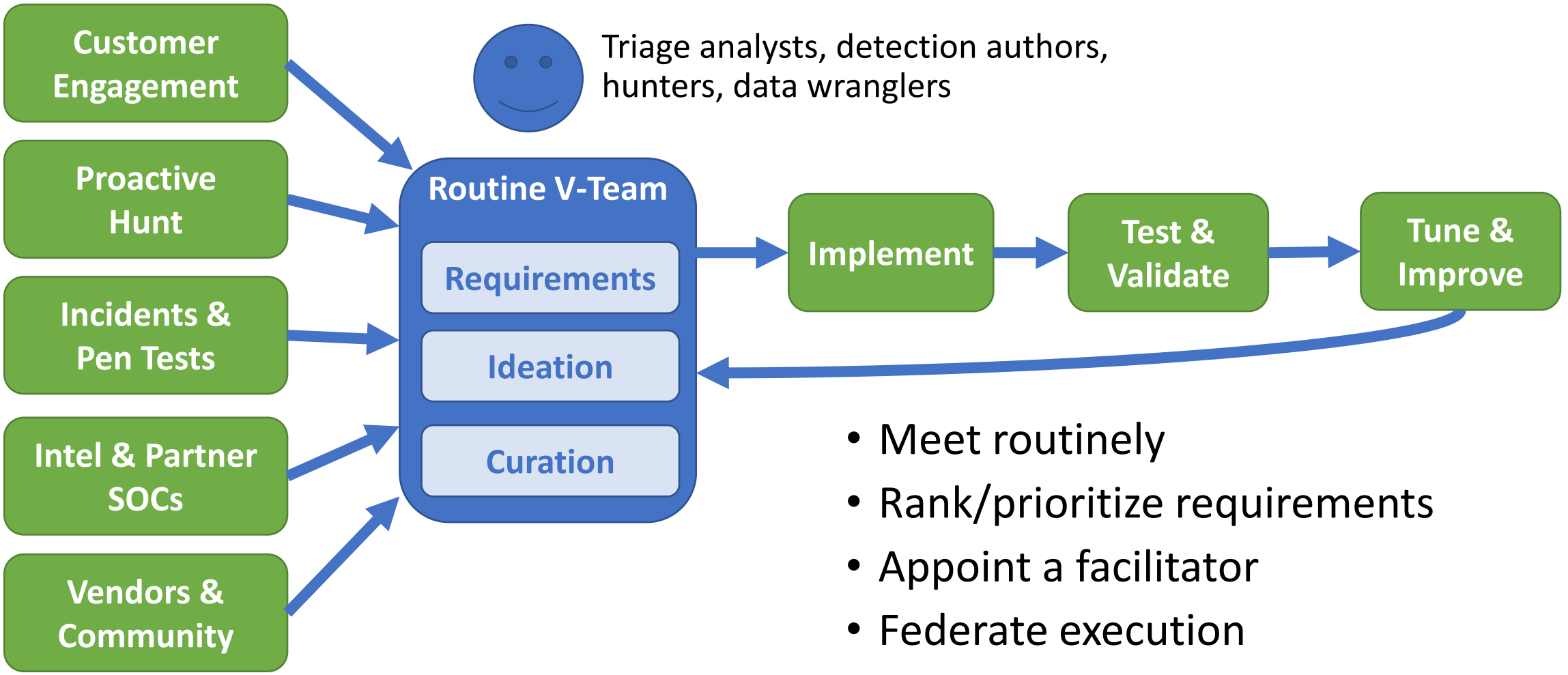
  $0/Free: https://mitre.org/11Strategies





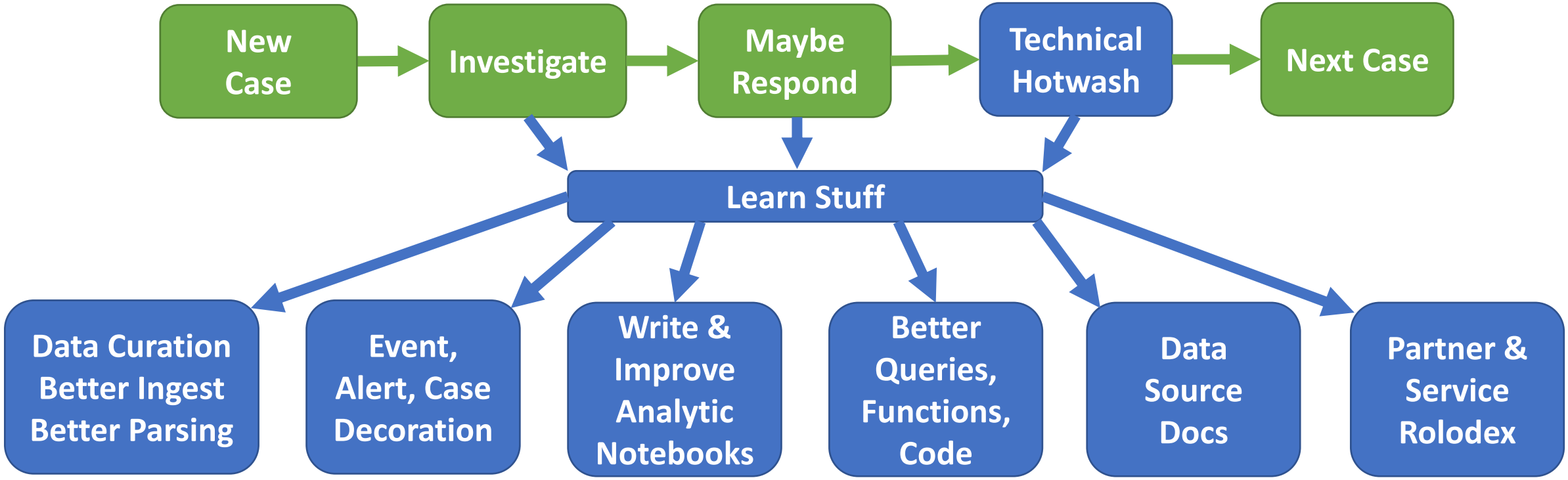
Not speaking on behalf of my employer, past or present;
any opinions expressed are my own.

Tool 1: Detection V-Team



- Meet routinely
- Rank/prioritize requirements
- Appoint a facilitator
- Federate execution
- Consider Agile for requirements and execution management

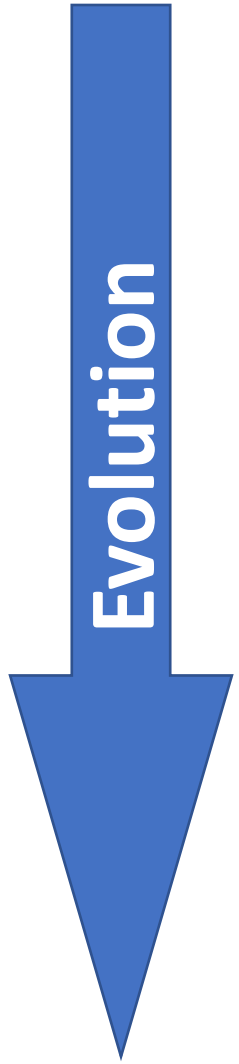
Tool 2: Investigation Improvements



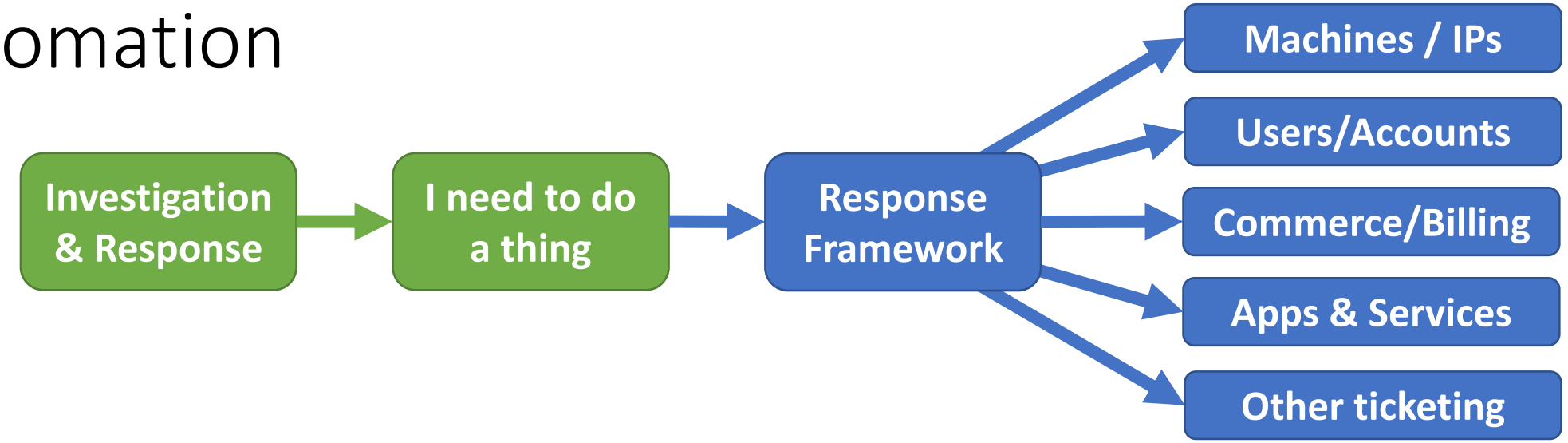
- Technical hotwash: “show and tell” of how you did it -> informal training
- Every major and new type of incident should yield this
- Plan capacity for this: do it now, or put it in the backlog

Maturing the SOC's Data Estate

	In SIEM	Not in SIEM
Pain	Data doesn't exist	
Extra pain	Data exists, SOC has no access	
One of us can use it in an emergency	One person has ad hoc access; Non-standard location	
One of us can use it routinely	Ingested, Poorly Parsed	One person has access
All of us use it routinely	Parsed, Documented	App / group access, Documented
Use it efficiently & effectively	Notebooks, Stored Queries, SOP(s)	
Depend on it	SLOs for entire data pipeline	Data contract with owning team



Tool 3: Response Automation



Just getting started?

- Focus on high benefit / low regret
- Consider automation that makes human <-> human comms faster: tickets, APIs, users “was this you”
- Can be human in the loop / drive 2-person integrity

- Avoid becoming a “spam cannon”
- Doesn’t have to be a SOAR product
- Eviction may not be our goal

For more: *11 Strategies:* Section 8.4
https://github.com/JHUAPL/Low-Regret-Methodology

Tool 4: Proactive Hunt

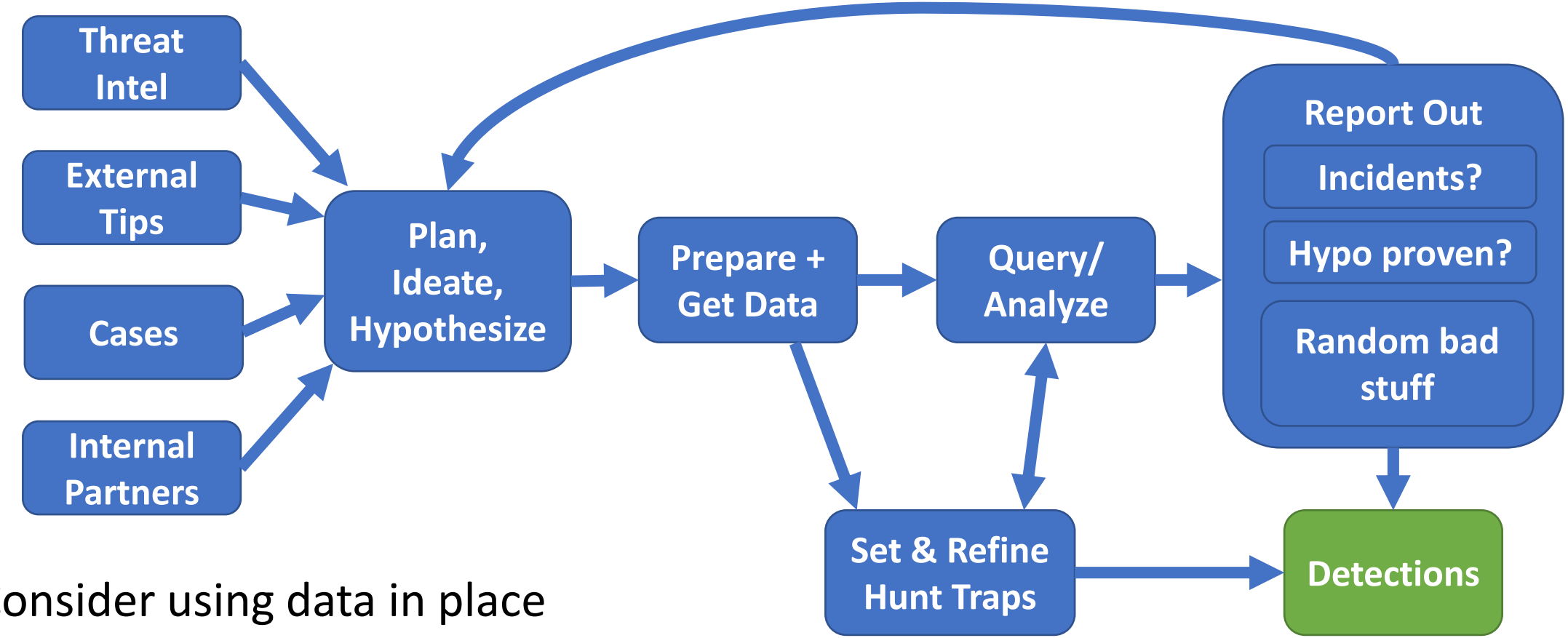
~~Ordinary Alert Investigation~~

~~Wandering Aimlessly In Data~~

Cyber threat hunting is a proactive search through networks, endpoints, services, cloud resources, and data to discover malicious or suspicious activities that have evaded detection by existing, routine tools and monitoring.

(definition adapted from Trellix)

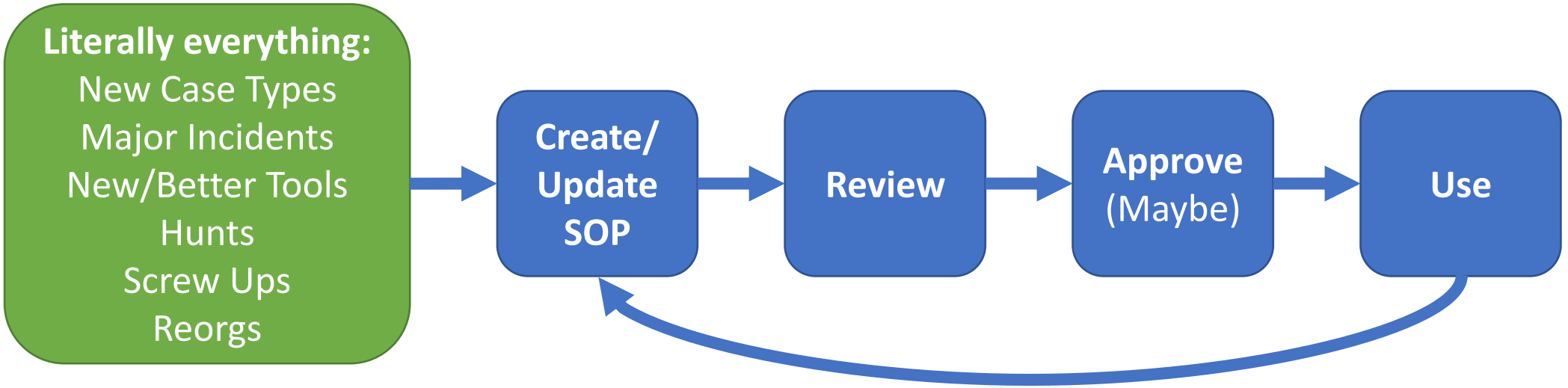
Proactive Hunt



- Consider using data in place
- Leverage query-on-timer for your traps
- Be clear about when you transition a hunt to a routine detection

- Don’t confuse finding “random bad stuff” with confirming a hypothesis
- Bounded timelines

Tool 5: Standard Operating Procedures (SOPs)

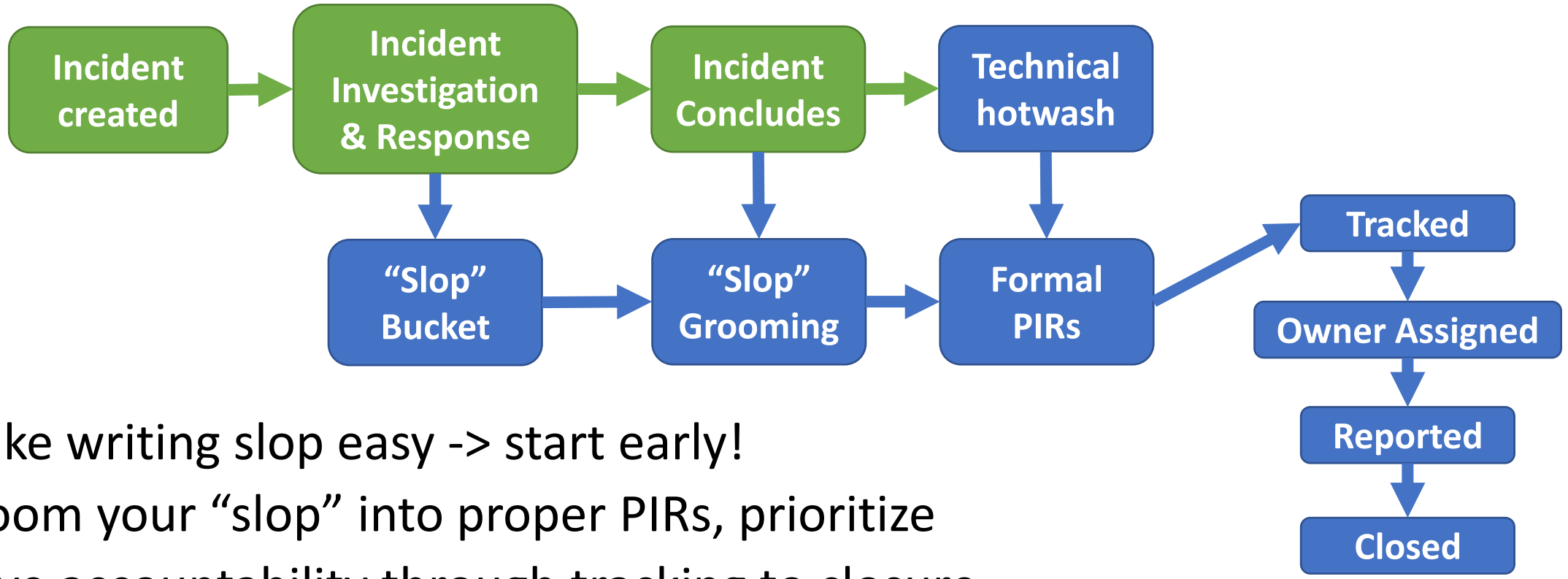


- #1 Defense against turnover, mistakes
- Everyone follows them: most junior -> most senior
- Writing and updating SOPs is expected of literally everyone
- Nothing important is contained in just one person's head

- Who/what/when/where/why
- Concise: "meat" < 4 pages
- Metadata for tracking
- Wiki? OneNote? Git? Whatever works!
- Level of review & approval depends on criticality/risk

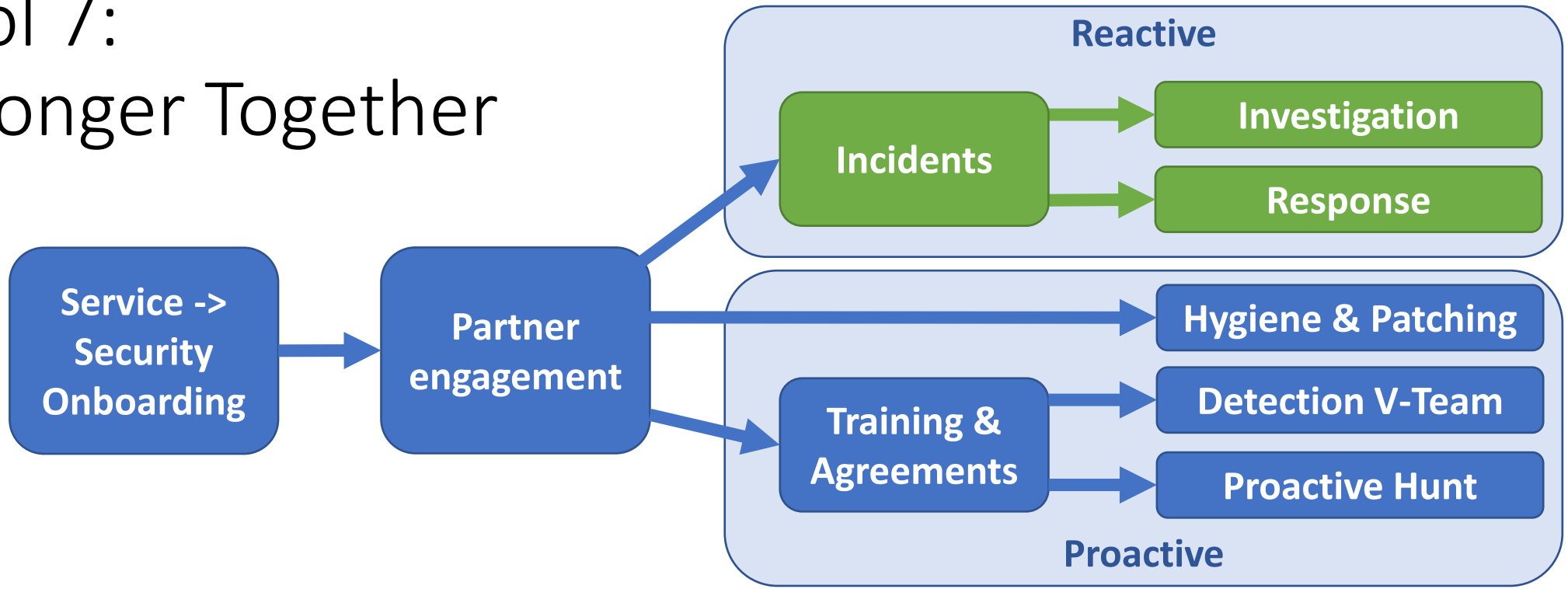
Tool 6: Post Incident Review

- Post Incident Review/Response (PIR): the things that didn't go well this time that should be fixed for "next time" -> external AND internal



- Make writing slop easy -> start early!
- Groom your "slop" into proper PIRs, prioritize
- Drive accountability through tracking to closure
- Embrace the red! Do not be afraid to call out ugly

Tool 7:
Stronger Together



Why: Prevention, detection, response in the context of the business

- Convert noisy & high-needs customers into self-service, engaged partners
- Offset personnel resourcing challenges

Enablers:

- Familiar data platforms
- Data access & sharing rules
- Escalation & response guardrails

Making it happen

Tips for Doing Less	Do More
Look at your biggest labor draws	Long-term investment planning (every 6-12 months)
Useless alerts & detections	Regular resource planning & coordination Maybe Agile Scrum -> Consider lightweight approaches
Intensive box checking? Talk to your compliance people & lawyers	
Use these 7 techniques to compress what you're already doing	Hold team members accountable to regular progress!

Conclusion

You can implement any of these processes today with the staff you have, no matter your SOC's age or size!

These seven tools should feel as important to your team as smashing alerts and flipping cases

They will *want* to make time for it!

If you're doing this right, analysts will feel like they have capacity buffer for when the next "big one" hits

Questions!

The 7 Techniques:

1. Detection V-Team
2. Investigation Improvements
3. Response Automation
4. Proactive Hunt
5. Updating SOPs & Playbooks
6. Post Incident Review
7. Deputize Stakeholders