The Fault in Our Metrics

Rethinking How We Measure Detection & Response

Bossman

BoD meeting is coming up. Gonna need updated program metrics. Let's chat tomorrow

you got it boss

Team Chat

BoD metrics... what have we presented in the past?

oh no

bad news, our last manager pretty much just made those up

good news, you’re here and gonna do so much better ;-)

detection response metrics

Why should I care about metrics?

Hi ♫
I’m Allyn

Hi ♫

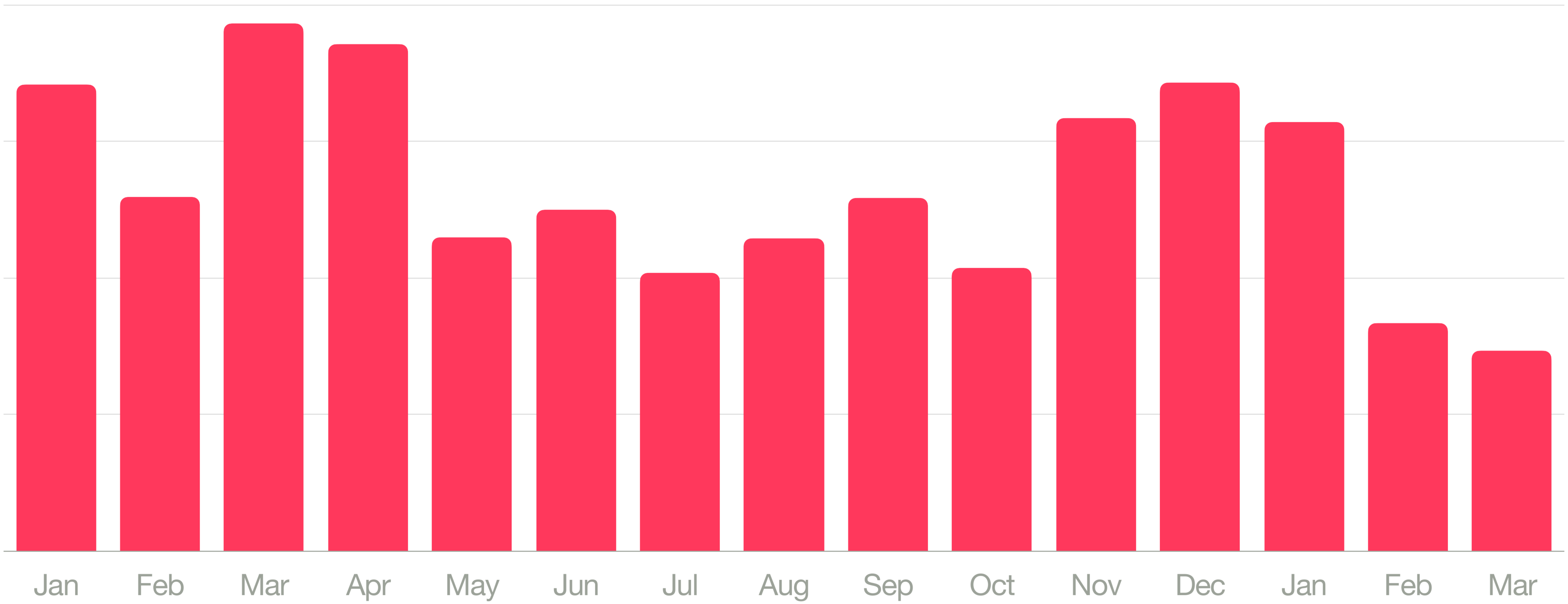
I’m Allyn

I've made mistakes.

5 Terrible Mistakes I’ve Made When Creating Metrics

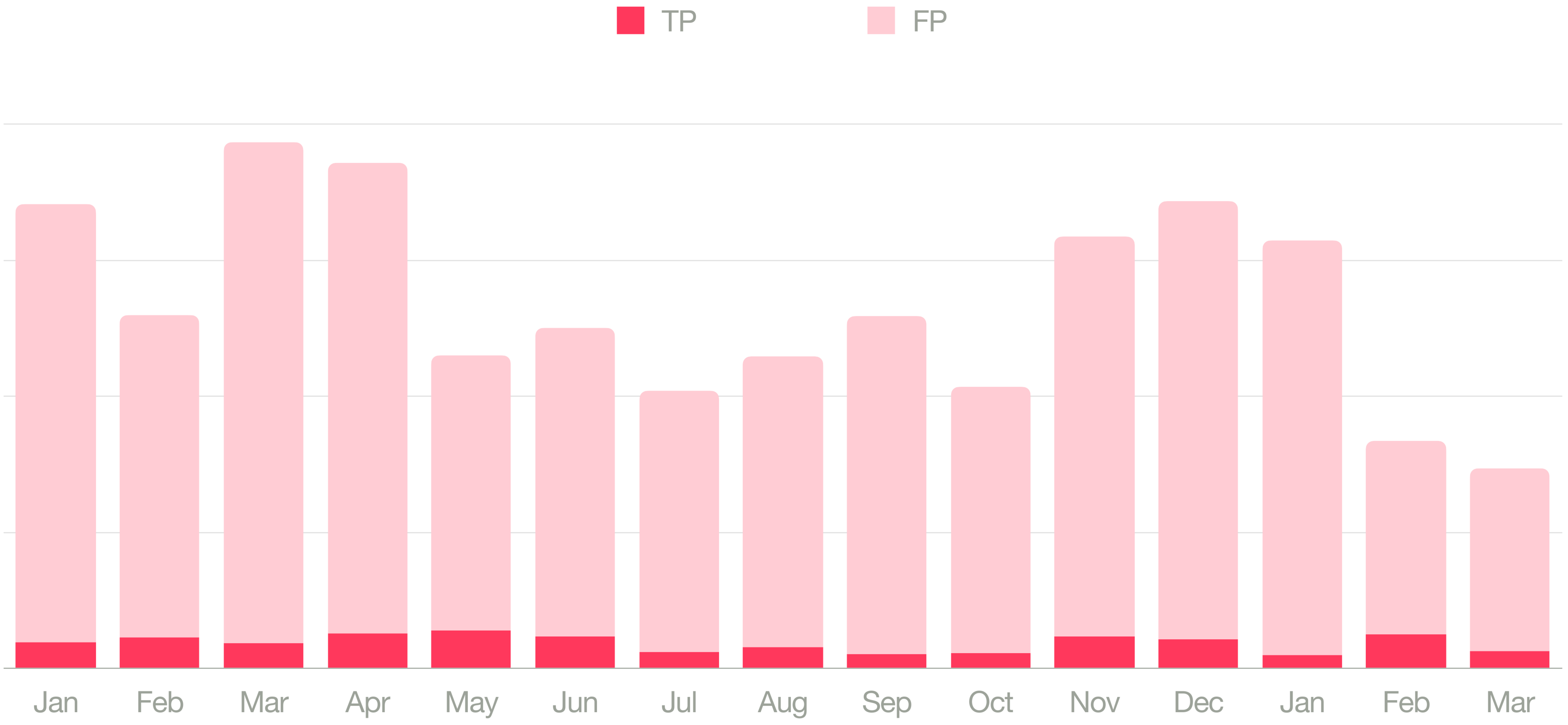
Losing Sight of the Goal

Security Alerts



for illustrative purposes only

Security Alerts



for illustrative purposes only

What do I measure?

Streamlined

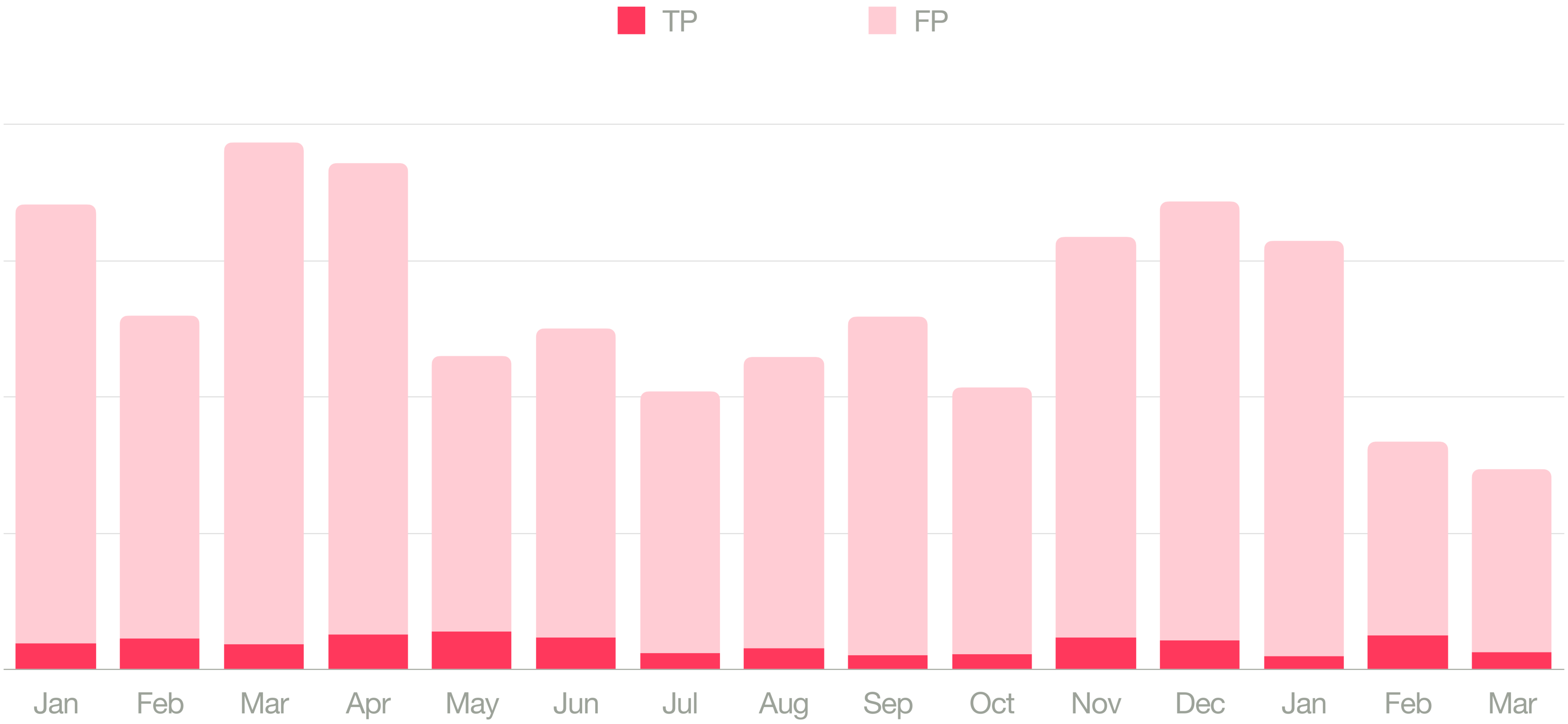
Awareness

Vigilance

Exploration

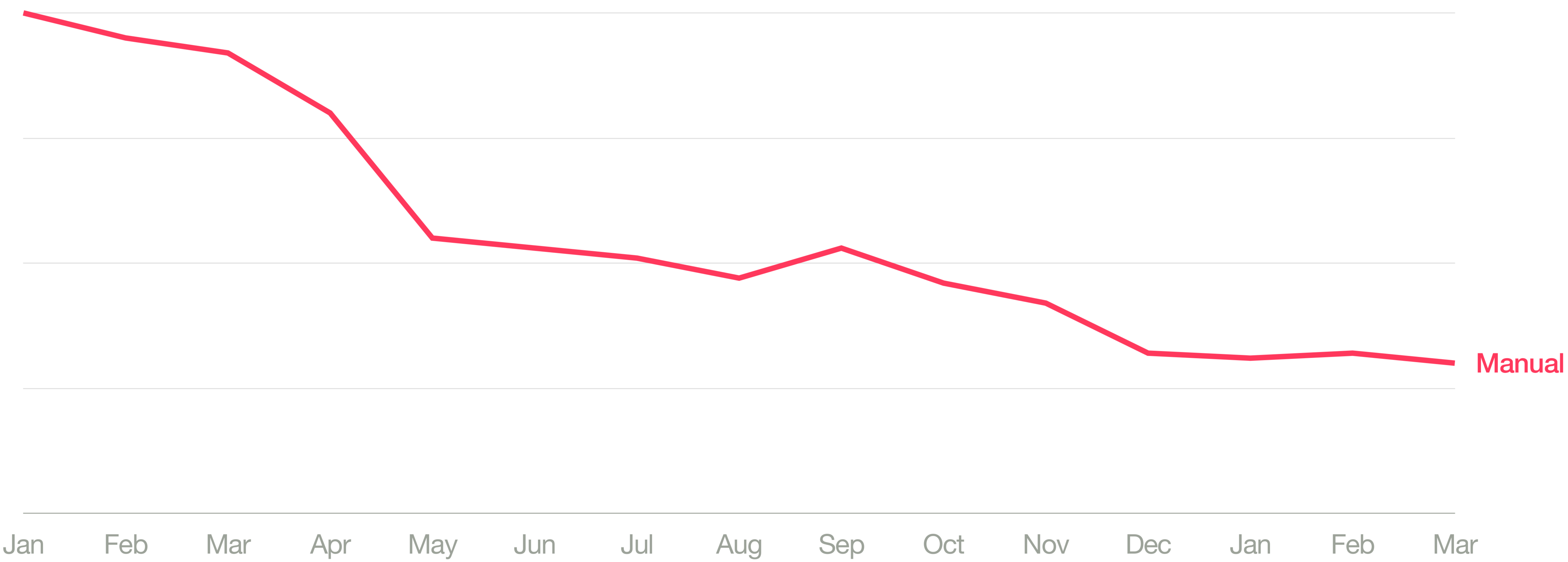
Readiness

Security Alerts



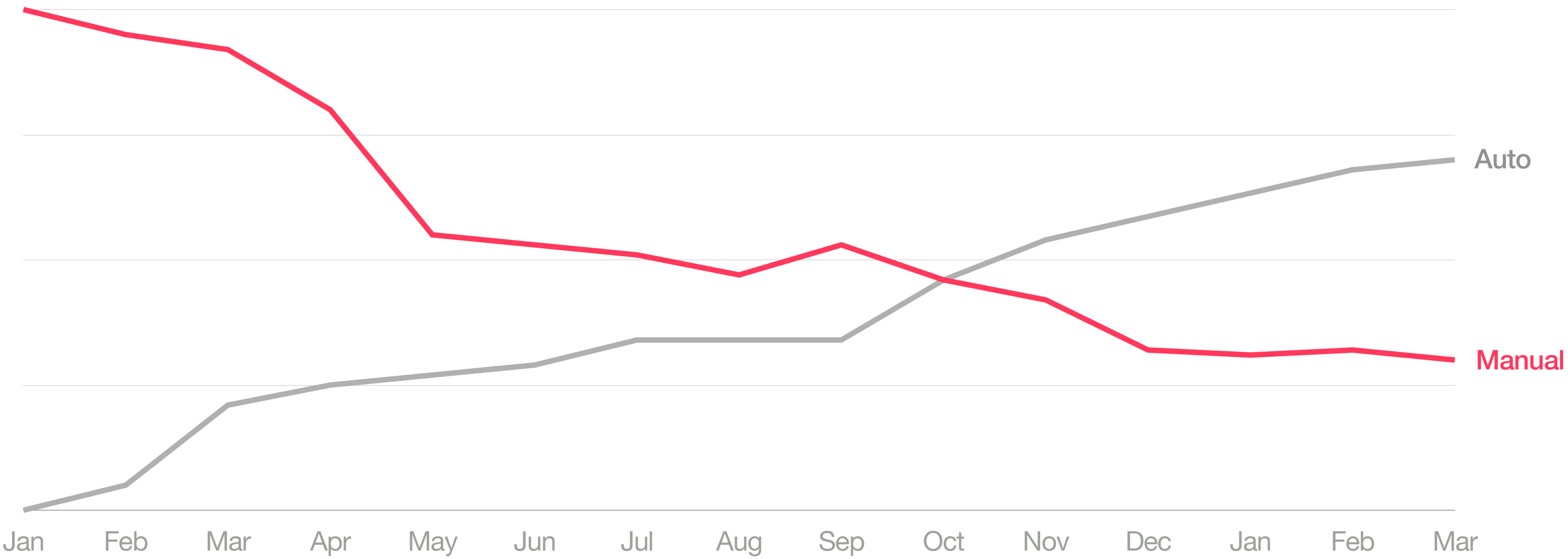
for illustrative purposes only

Time spent on FPs



for illustrative purposes only

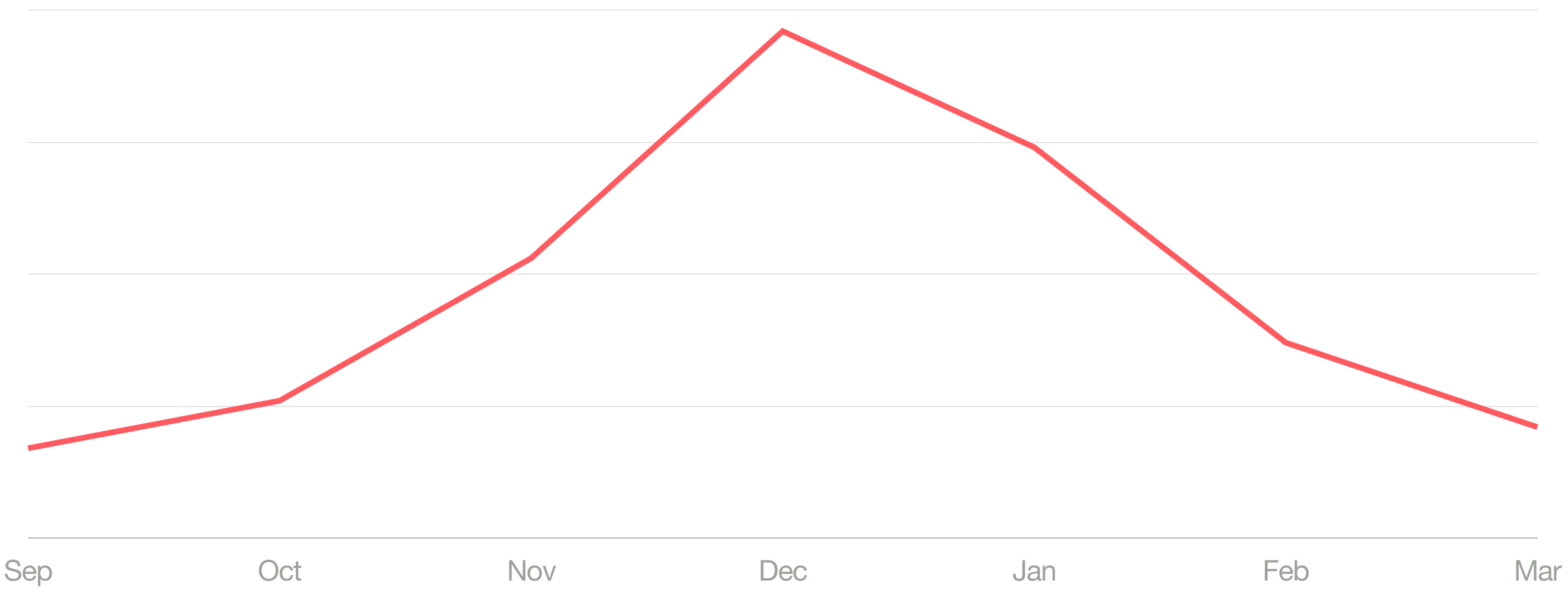
Time spent on FPs



for illustrative purposes only

Using Quantities That Lack Controls

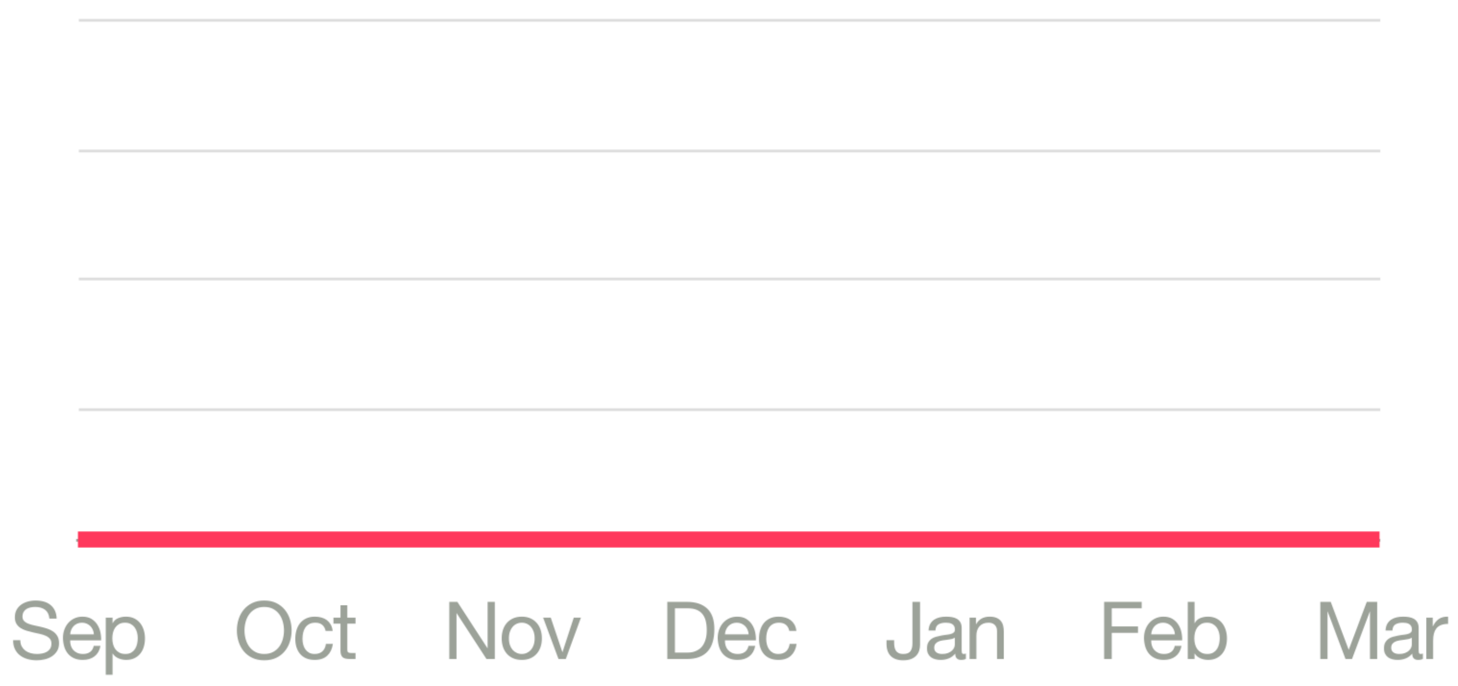
Mean Time to Recover



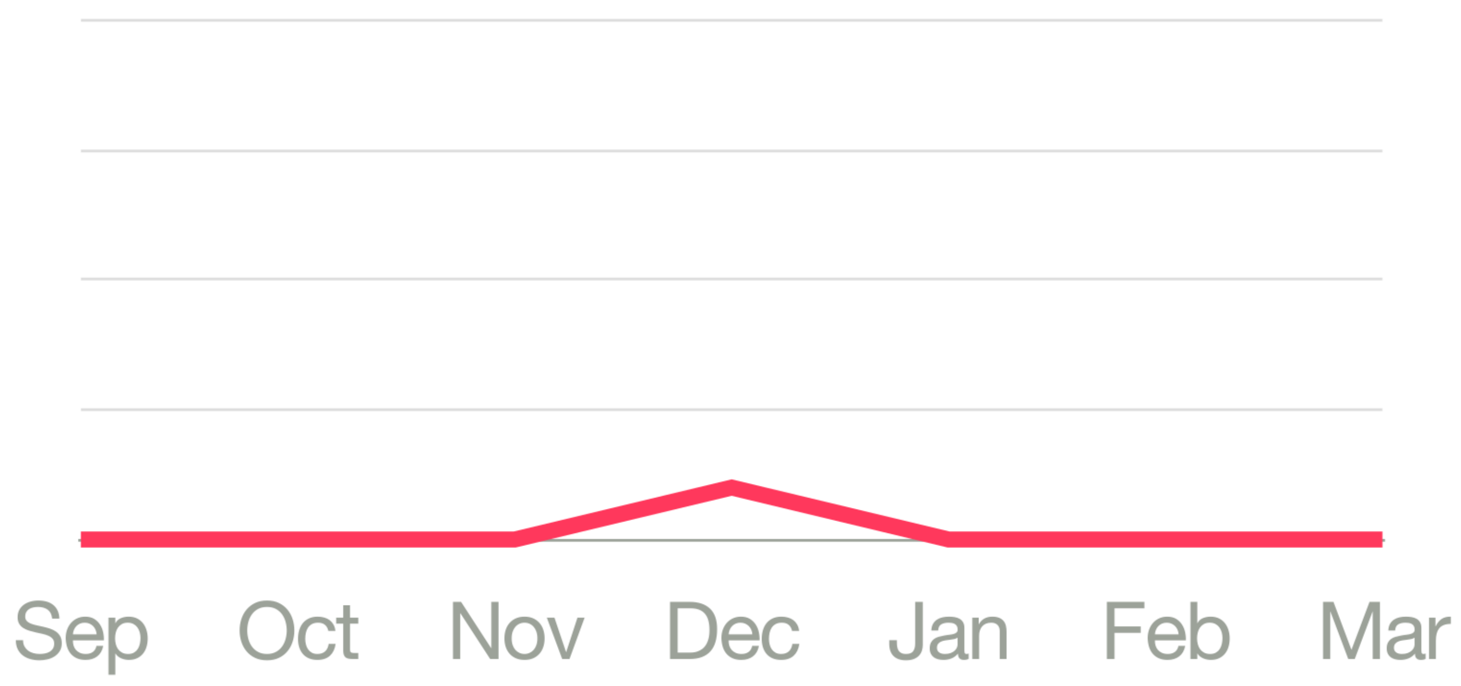
for illustrative purposes only

Response Readiness Metrics

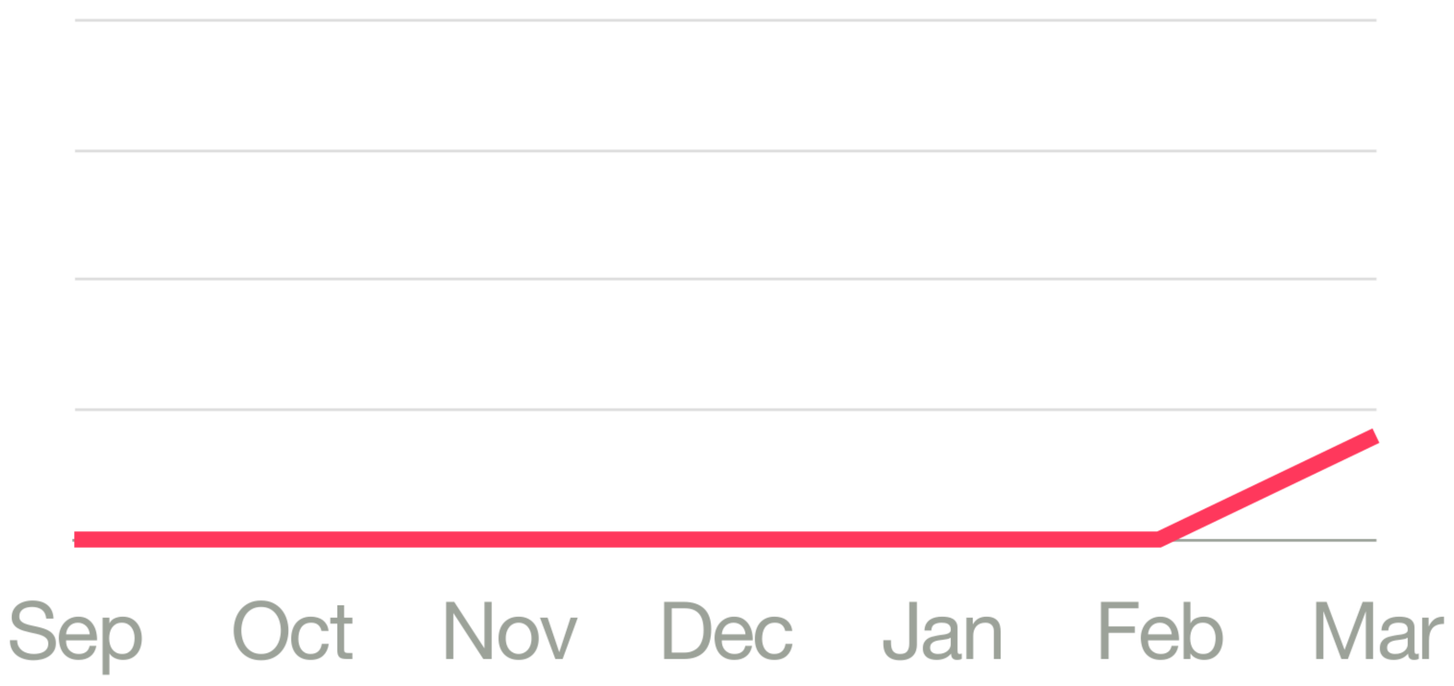
Triage & Analysis
(filtered)



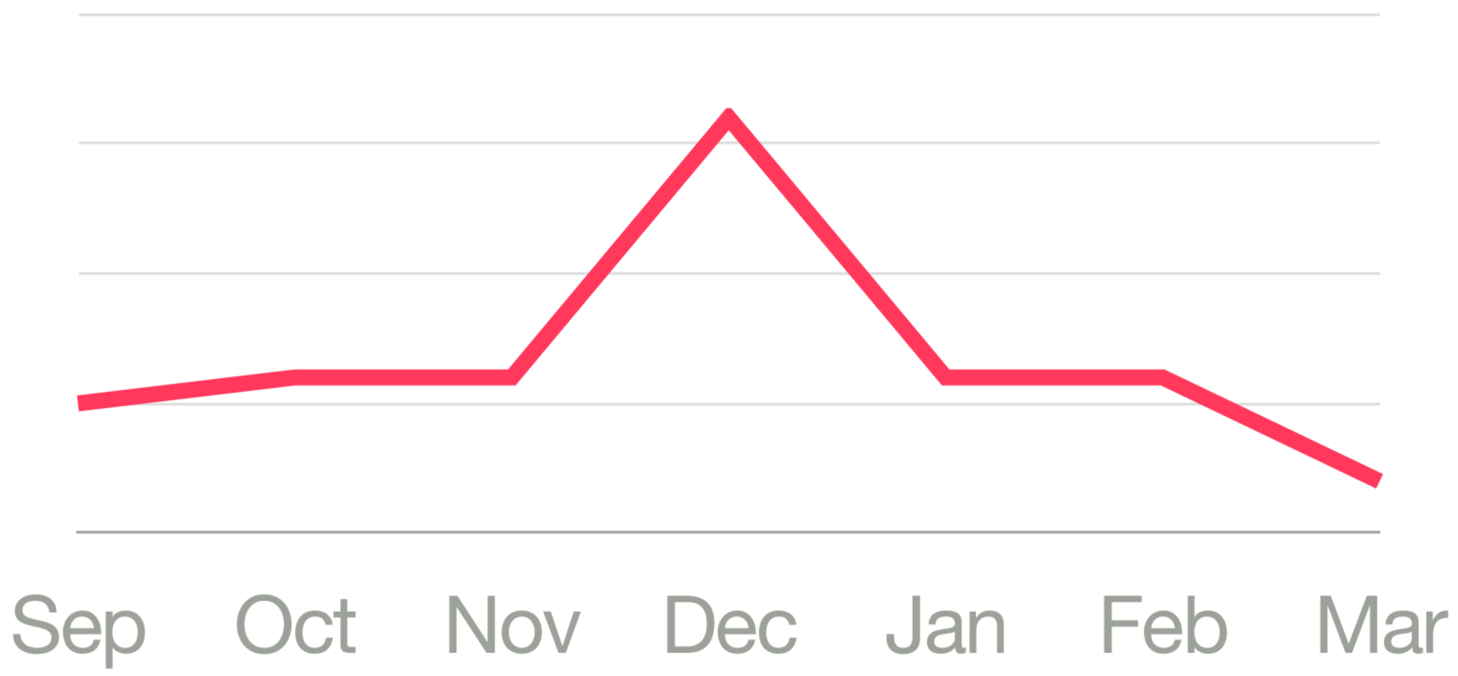
Incident Spin Up Time
(filtered)



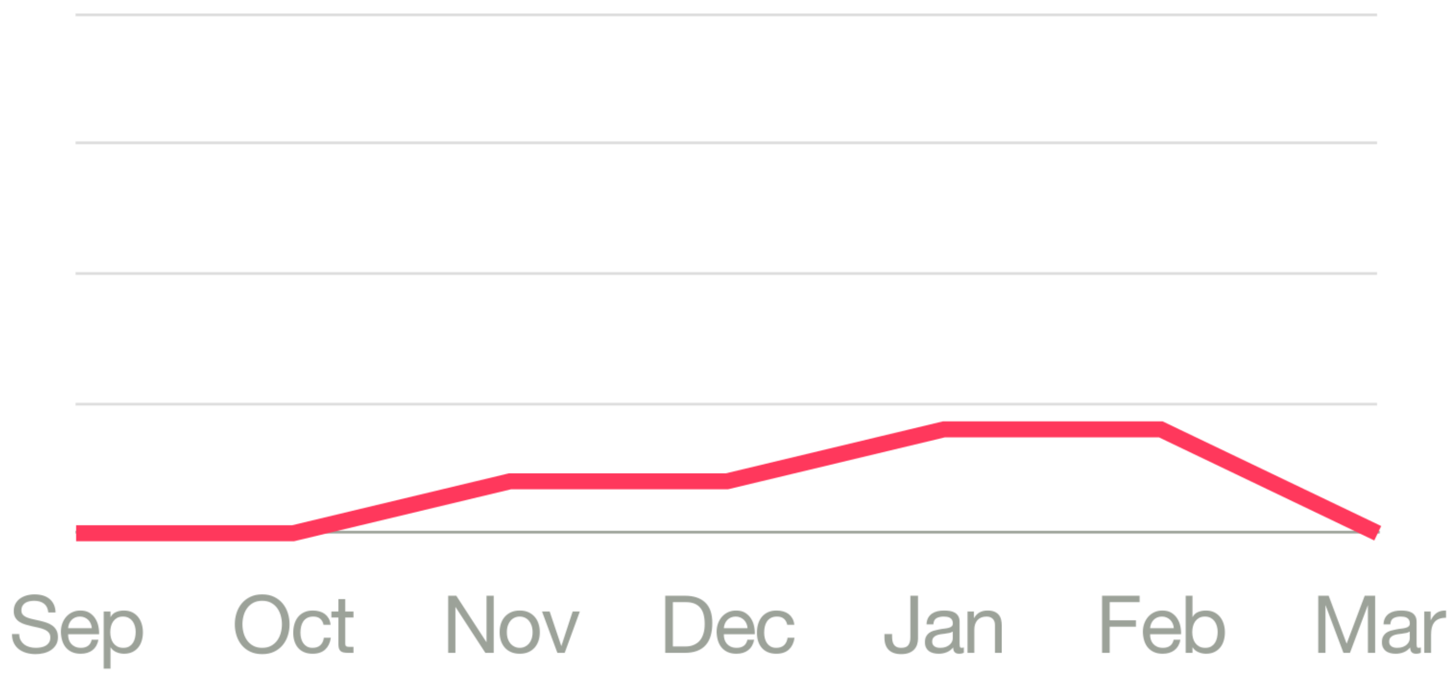
Contain
(filtered)



Remediate
(filtered)



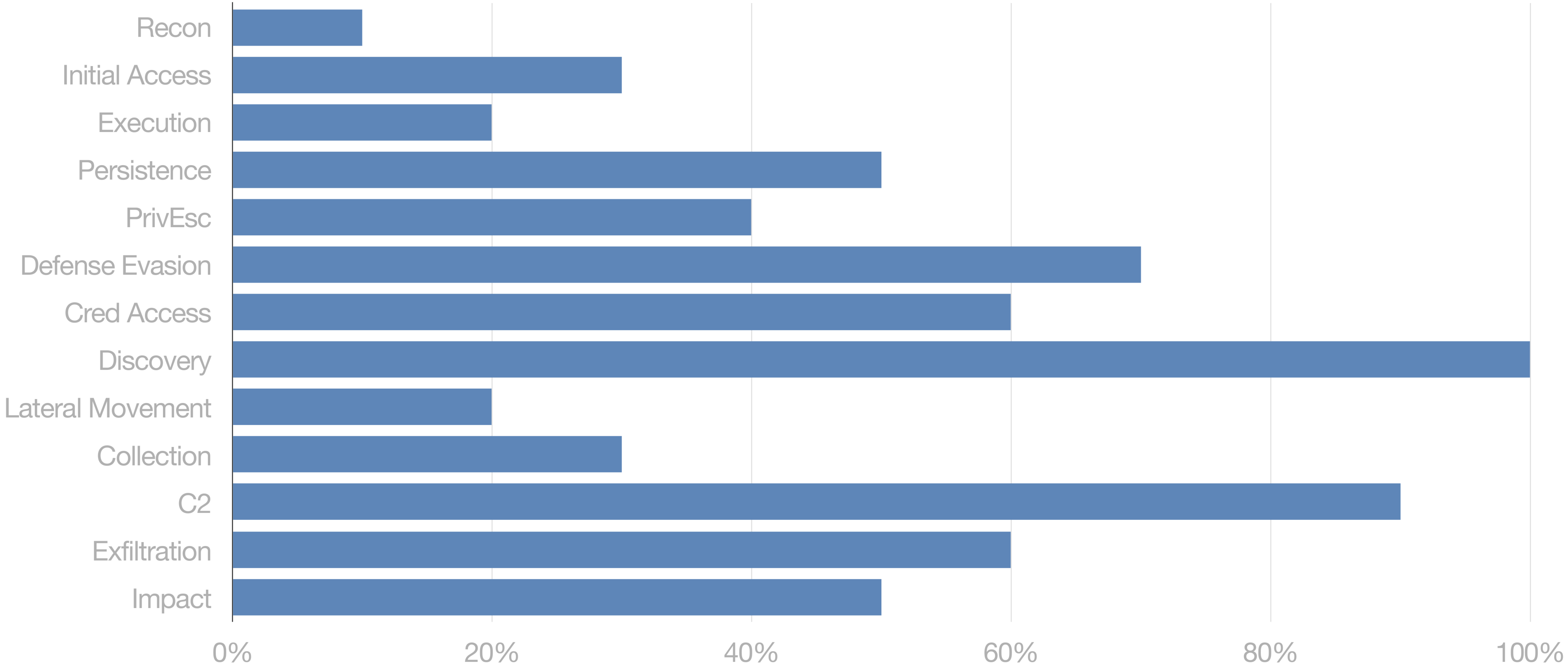
Recover
(filtered)



for illustrative purposes only

Thinking Proxy Metrics Are Bad

MITRE ATT&CK Coverage



for illustrative purposes only

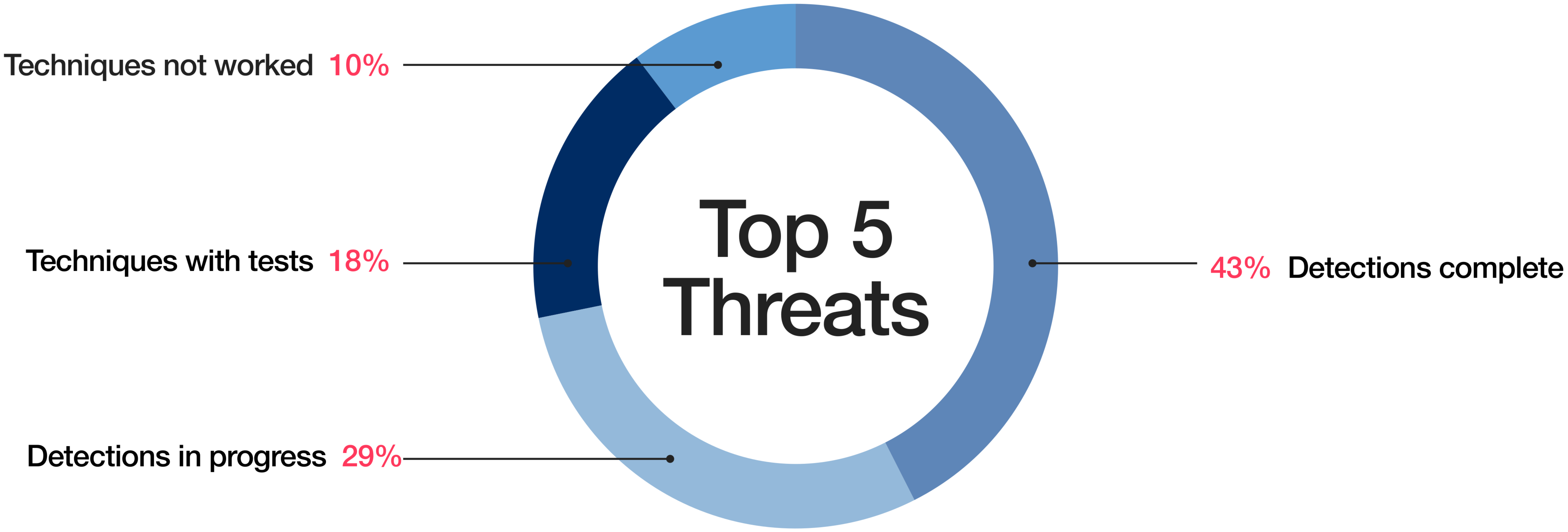
Top 5 Threats

External Threat Intel

Internal Incident Trends

Organization Security Risks

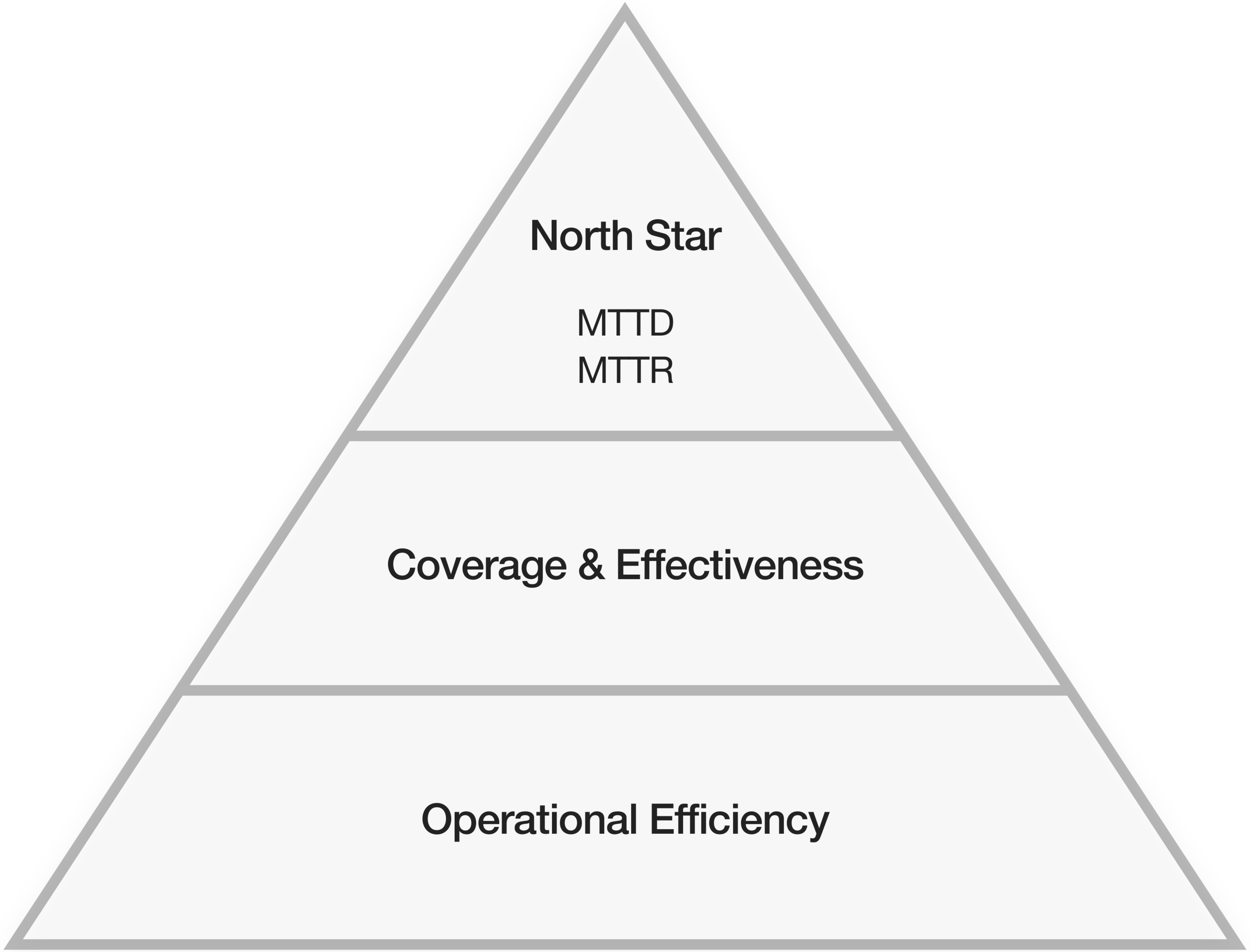
Detection Prioritization



for illustrative purposes only

Not Adjusting to the Altitude

Cost of an Incident or Breach



North Star

MTTD
MTTR

Coverage & Effectiveness

Operational Efficiency

Asking "Why?" instead of "How?"

Why?

How?

Maturity Models

Where are we now?

Where are we going?

How will we get there?

TDR Maturity Model

Observability

- Entity & Activity Coverage
- Searchability
- Contextualization
- Enrichment

Proactive Threat Detection

- Intelligence
- Detection Coverage
- Detection Engineering
- Threat Hunting

Rapid Response

- Preparation
- Triage & Analysis
- Forensics
- Response

☆ Maturity Levels

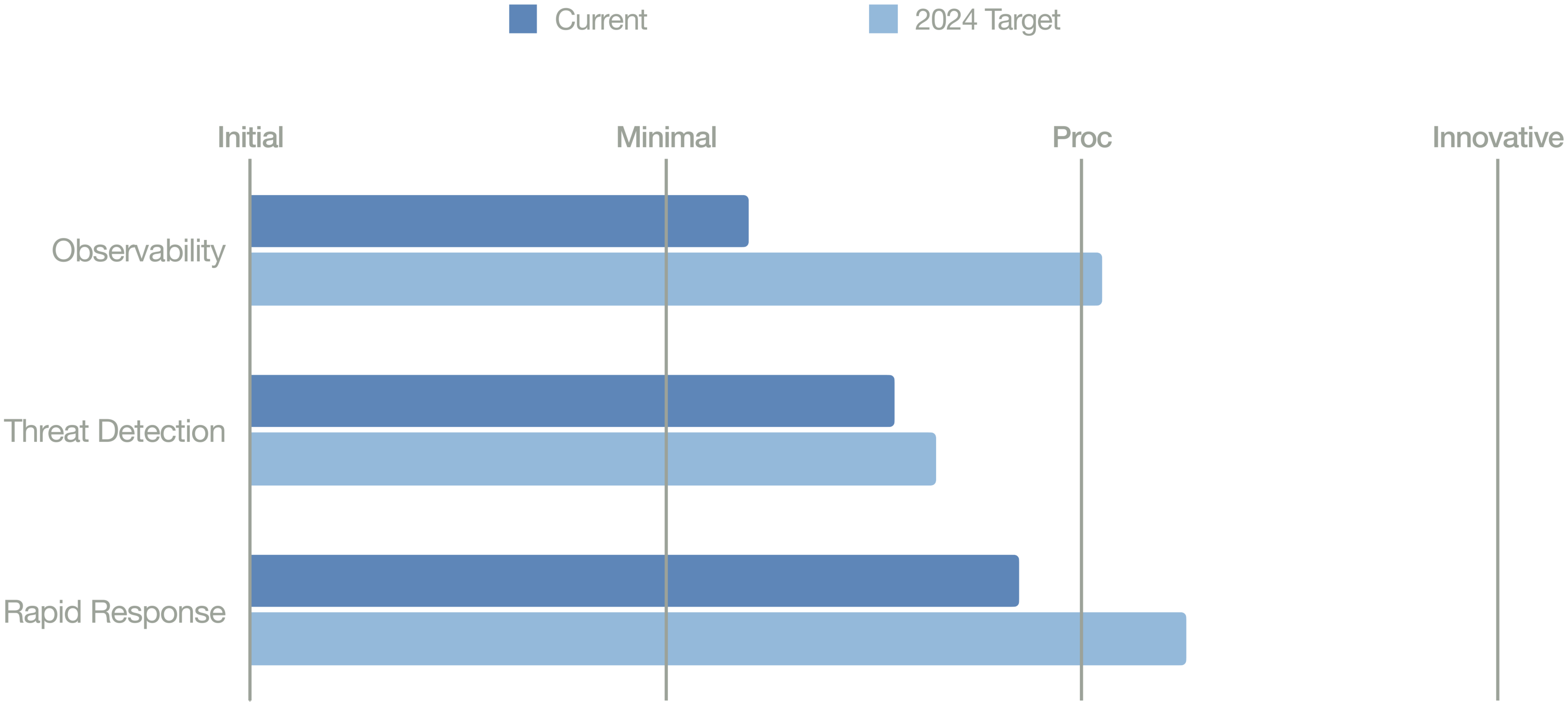
	Initial	Minimal	Procedural	Innovative	Leading
Process	All manual	20-40%	40-60% all criticals	60-80% all criticals and highs	Automated and mature
Tools	Ad-hoc	Defined but not enforced	Centralized	Optimized	AI/ML powered
Docs	None	Mostly knowledge sharing	Complete but manual	Automatic	Live
Testing	None	Some manual	Complete but manual	Enforced	Continuous

Detection Engine

	Initial	Minimal	Procedural	Innovative	Leading
Process	All manual	[✓ 20-40%]	40-60% all criticals	60-80% all criticals and highs	Automated and mature
Tools	Ad-hoc	Defined but not enforced	[✓ Centralized]	Optimized	AI/ML powered
Docs	None	[✓ Knowledge sharing]	Complete but manual	Automatic	Live
Testing	[✓ None]	Some manual	Complete but manual	Enforced	Continuous

for illustrative purposes only

TDR Maturity



for illustrative purposes only

SAVER Metrics

Questions & Outcome

Category

Control & Risk reward

Expiration

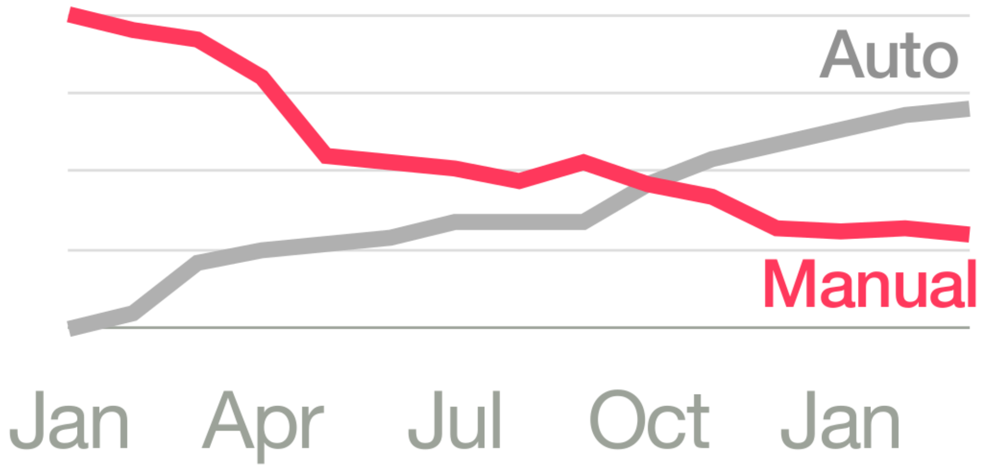
Data requirements, Effort & Cost

Change is hard.

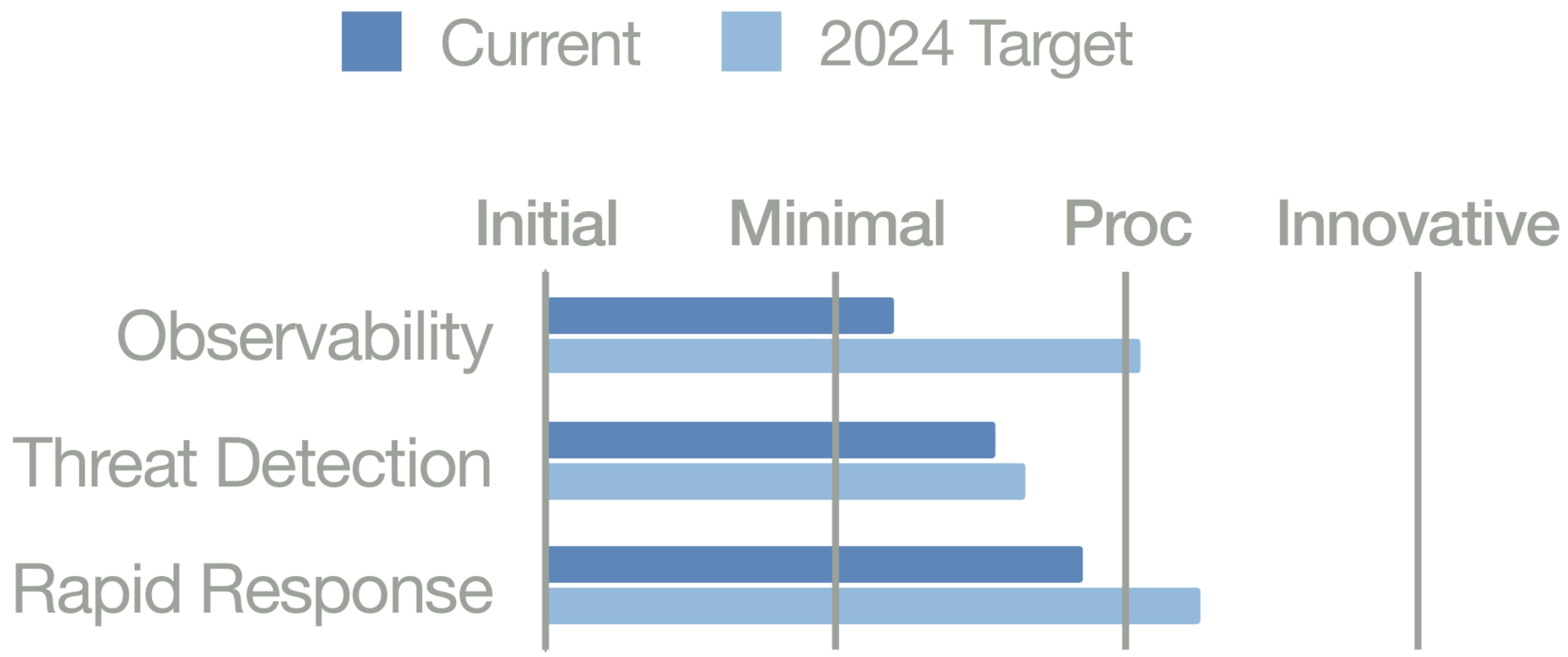
Detection & Response

Streamlined

Time spent on FPs



Program Maturity



Exploration

New Gaps Found

1. MFA resets unverified
2. Antivirus is out-of-date
3. No USB drive usage logs

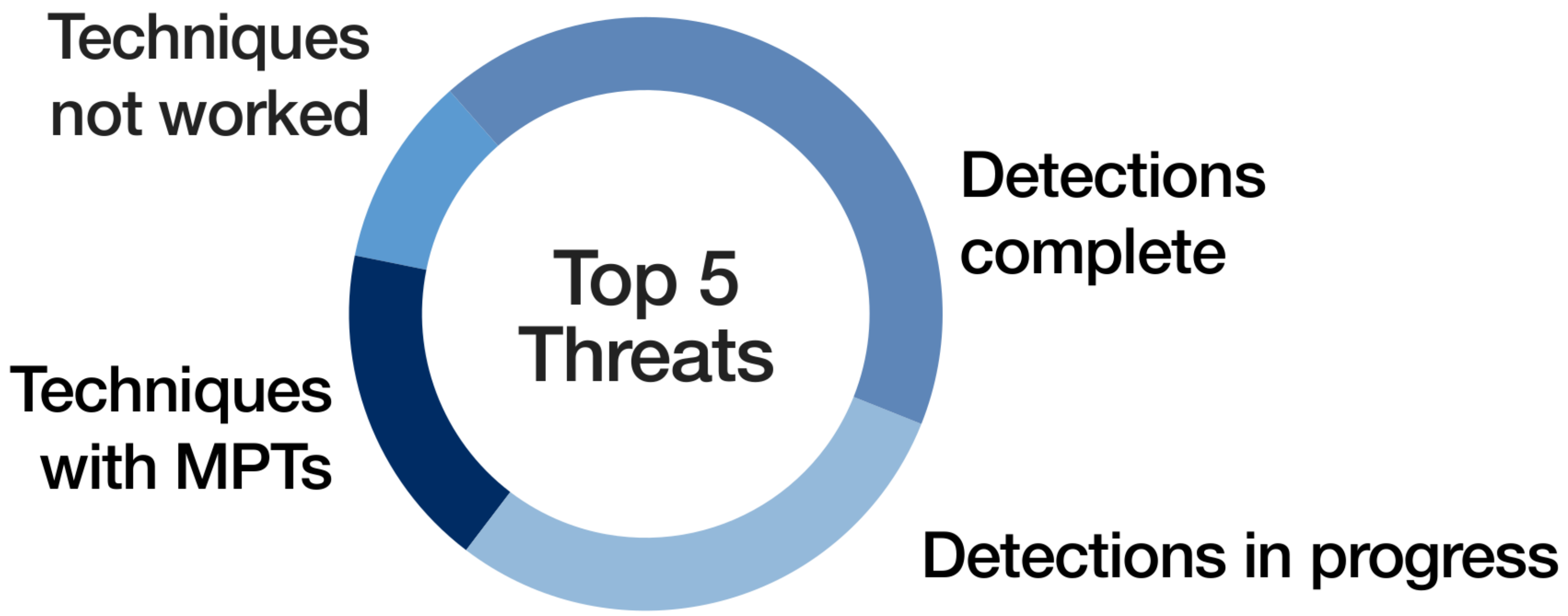
Awareness

Top 5 Threats

1. Phishing
2. Account takeover
3. Commodity malware
4. Vishing
5. Data exfiltration

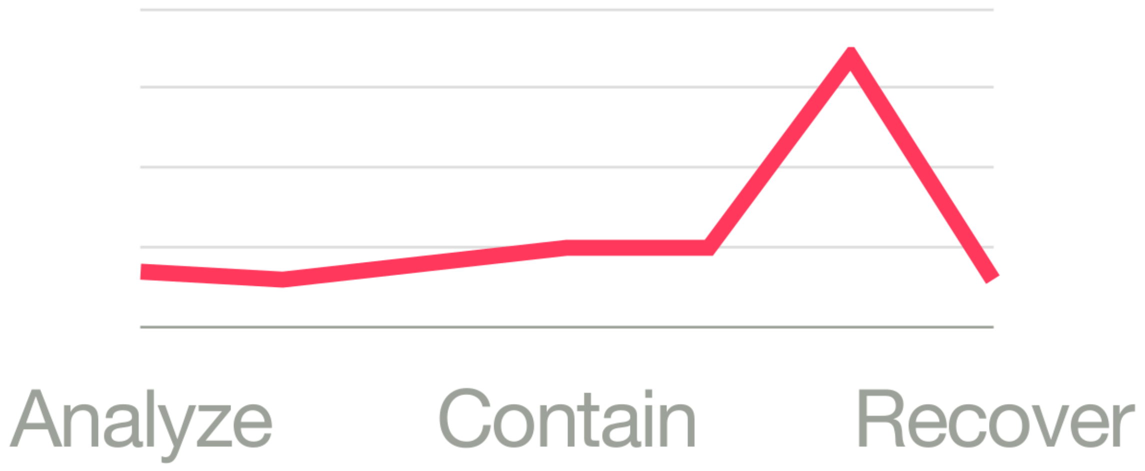
Vigilance

Detection Engineering



Readiness

Response Time



for illustrative purposes only

Rethinking How We Measure Detection & Response

TDRMM: measure tools & capabilities

SAVER: build better metrics

Top 5 Threats: not "100% ATT&CK"

linktr.ee/meoward