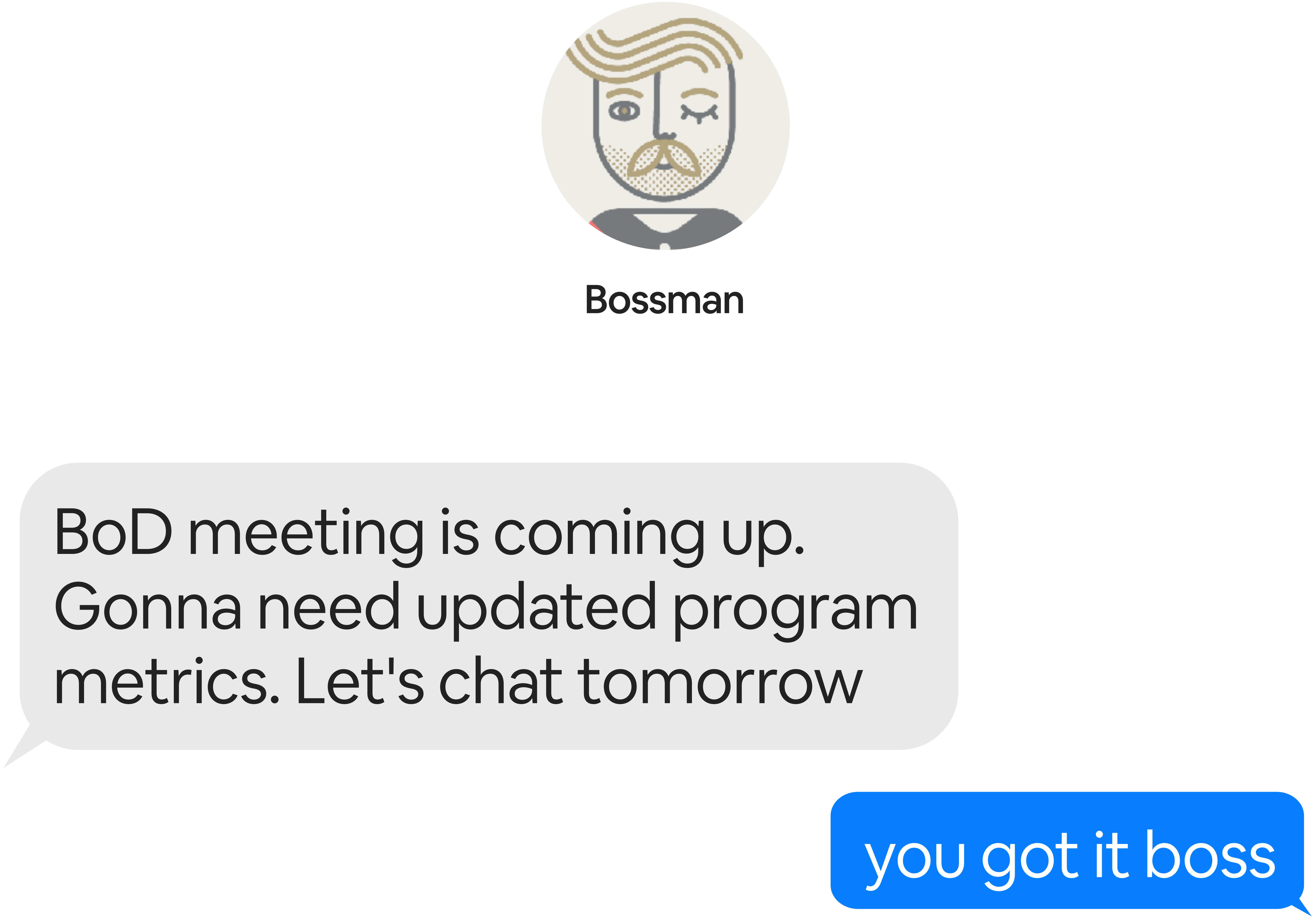
The Fault in Our Metrics

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

"Metrics: You Are What You Measure!"
~Hauser & Katz

"That which is measured, improves"
~Karl Pearson

Why should I care about metrics?

"Metrics reveal data."
~Edward Tufte

"Metrics are an annoying powerpoint
I need to update every month."
~Allyn

Hi ♫
I’m Allyn

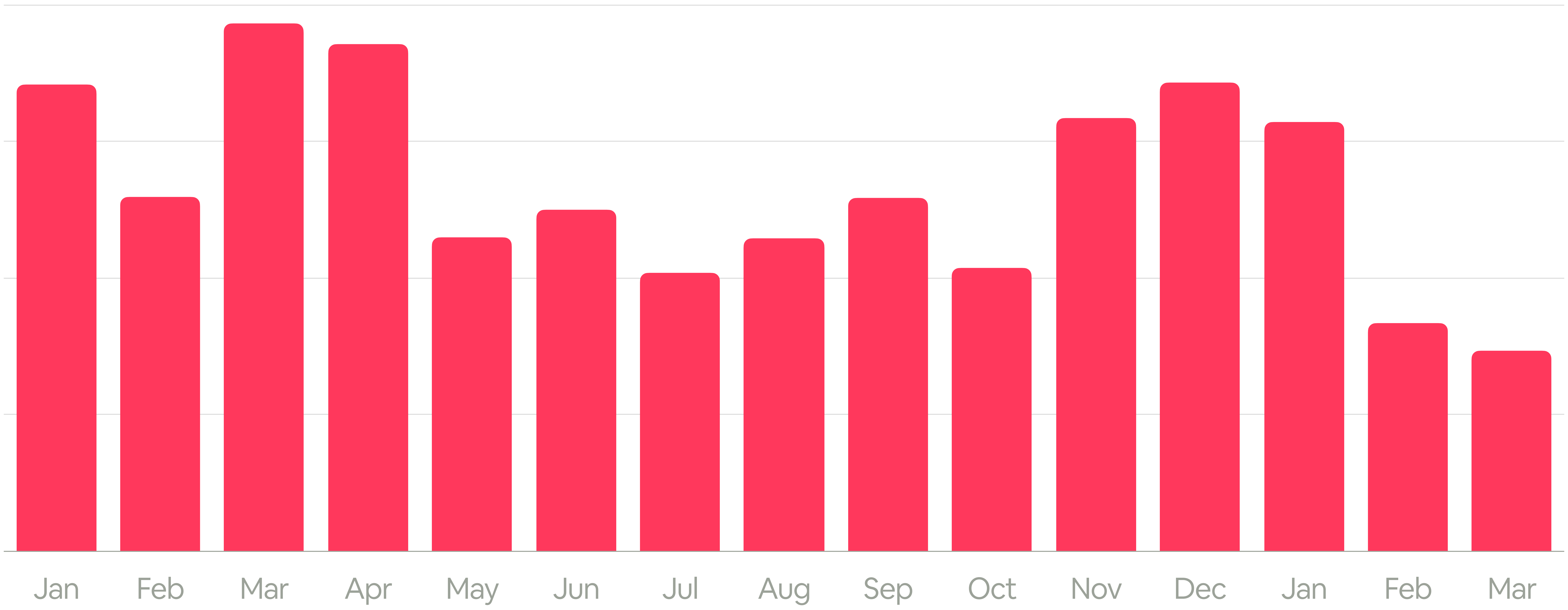
I've made mistakes.

5 Terrible Mistakes I’ve Made When Creating Metrics

Losing Sight of the Goal

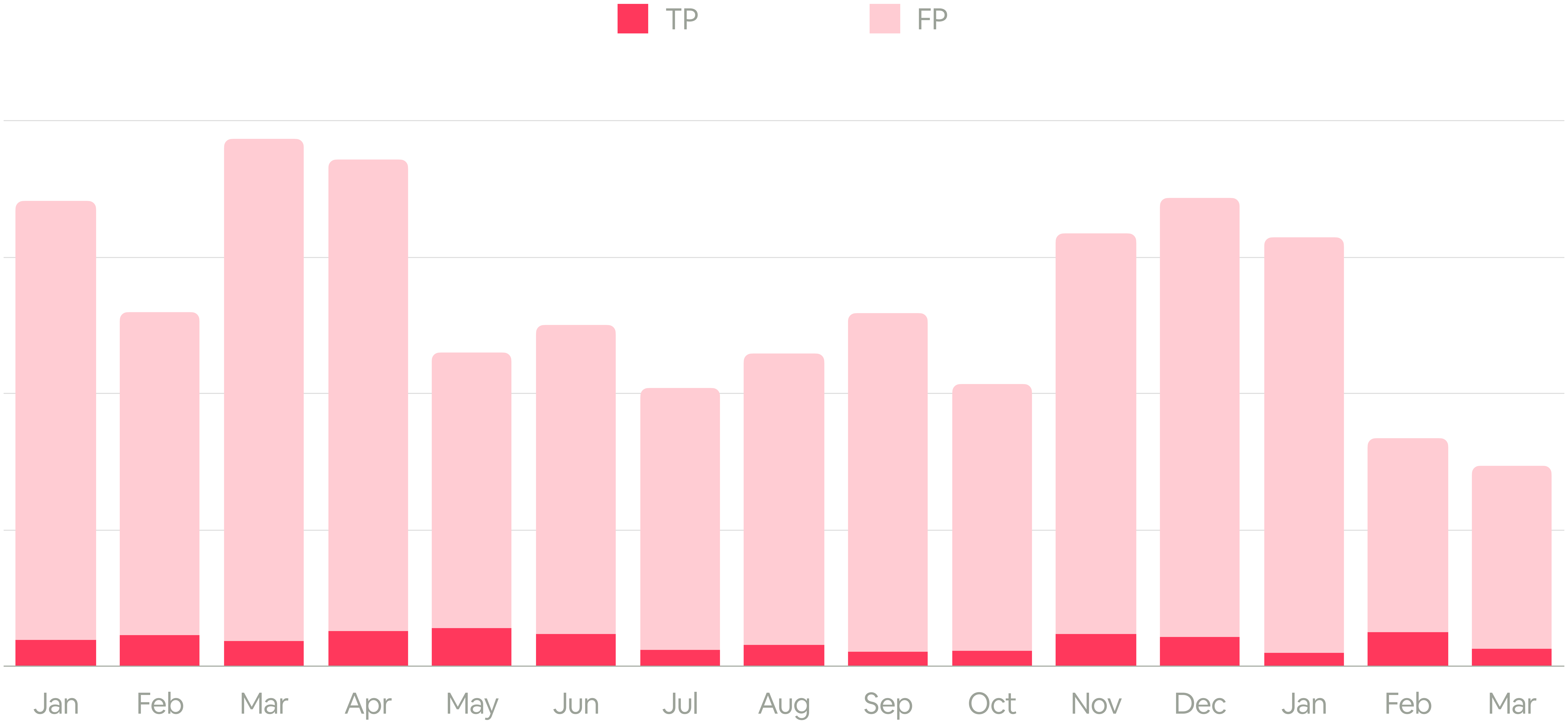
Mistake #1

Security Alerts



for illustrative purposes only

Security Alerts



for illustrative purposes only

What do I measure?

Streamlined

Awareness

Vigilance

Exploration

Readiness

SAVER Categories

Streamlined

Operational efficiency accuracy, and automation.

Awareness

Context and intelligence about existing and emerging threats, vulnerabilities, and risks.

Vigilance

Visibility and detection coverage for known threats.

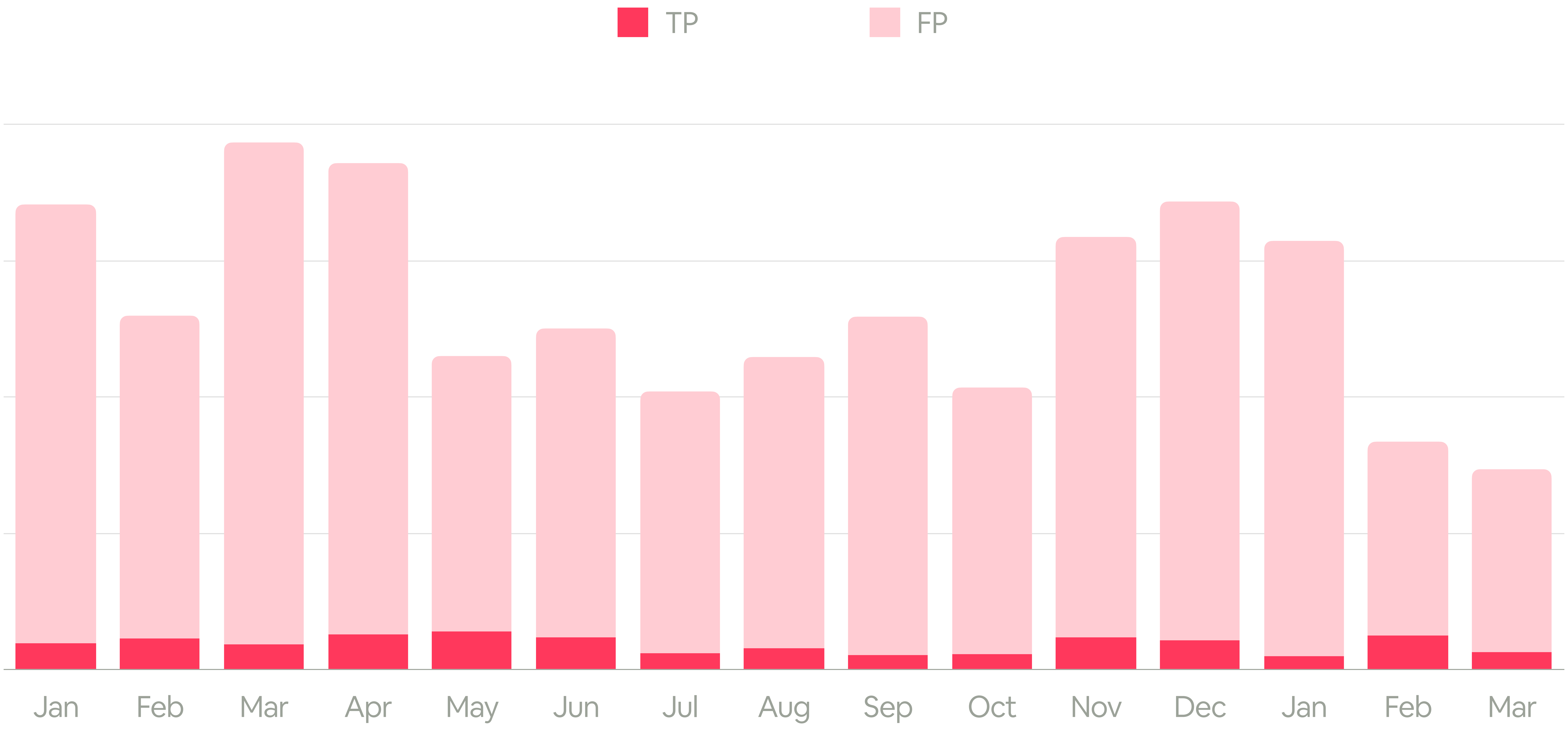
Exploration

Proactive hunts and investigations into the unknown.

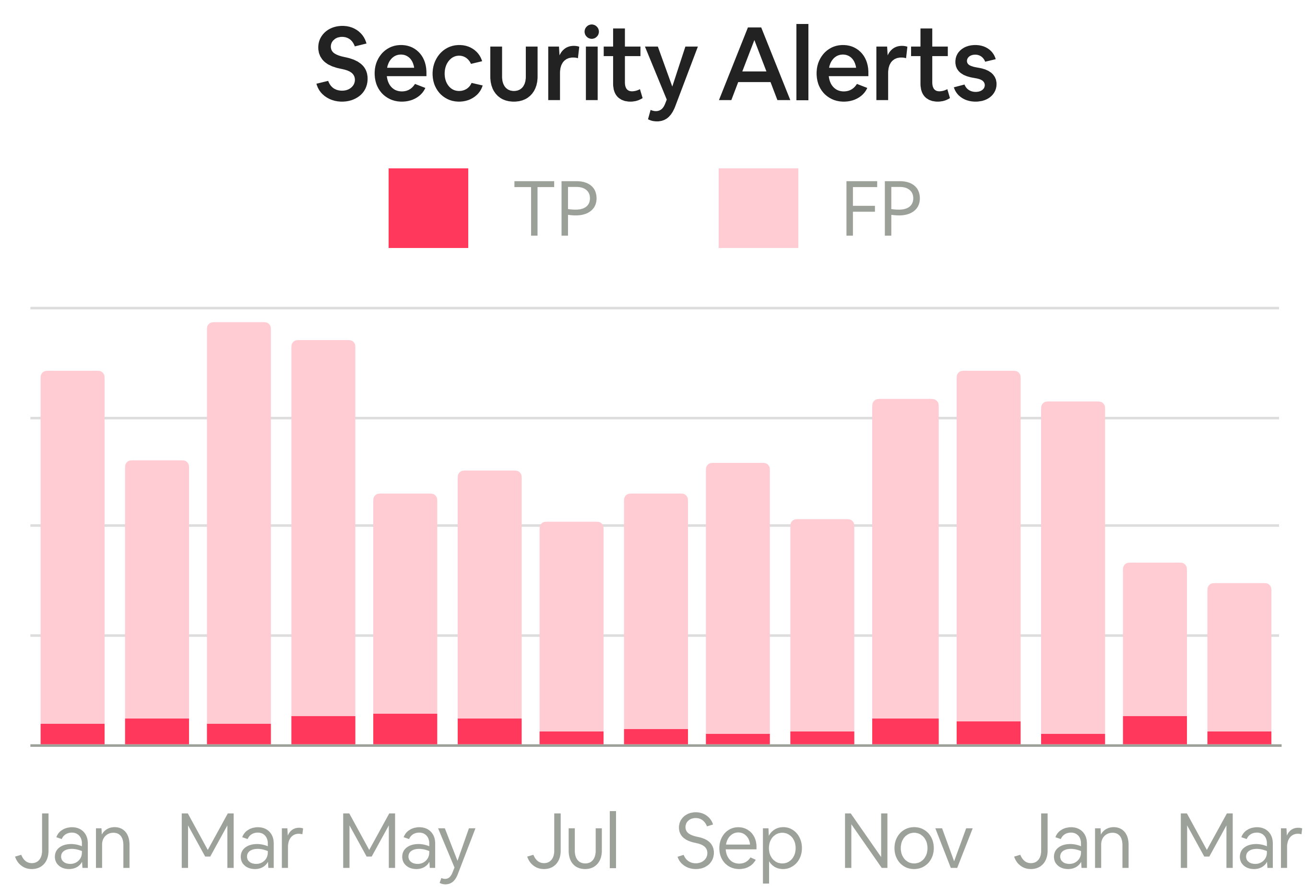
Readiness

Preparation for the next big incident.

Security Alerts



for illustrative purposes only



Outcome

There's always time and effort for TPs

Question

Are we spending time investigating impactful alerts?

Category

Streamlined

Metric control

Alert tuning

Risk reward

Over-tuning alerts, prioritizing based on volume

Data requirements

Alert resolution

Effort cost

Medium

Metric cost

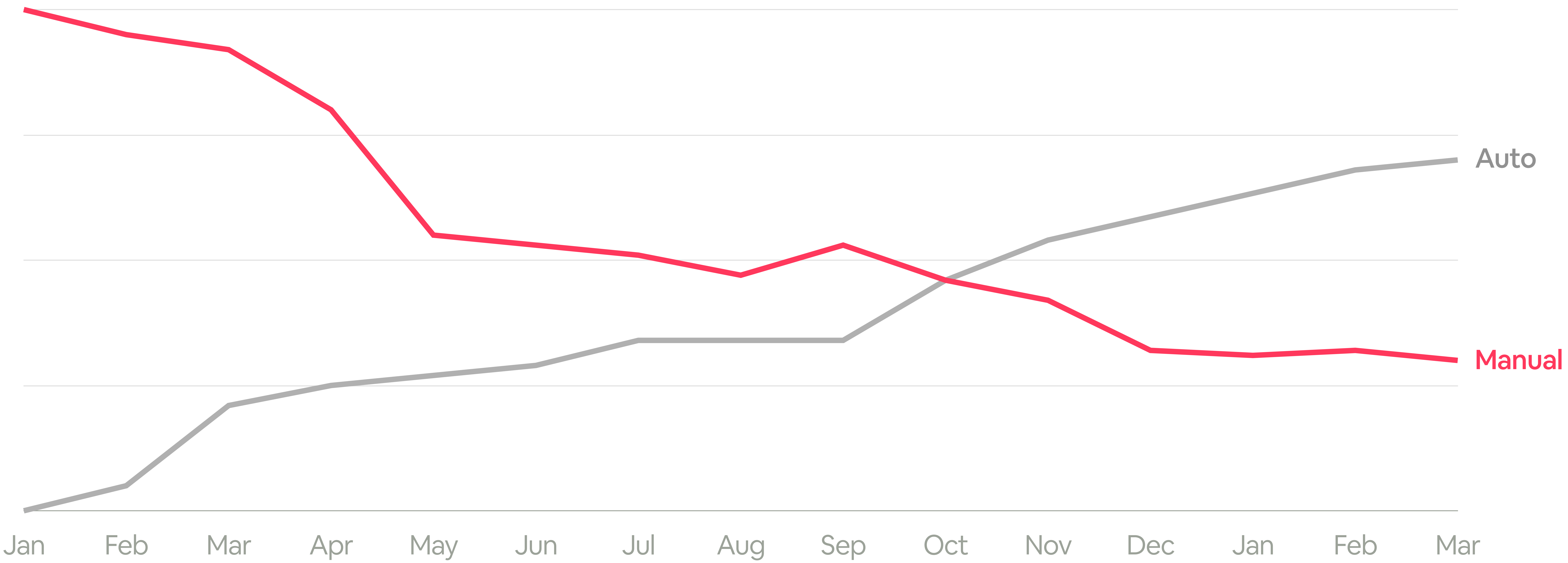
Low

Metric expiration

Automation and enforced detection quality

for illustrative purposes only

Time spent on FPs

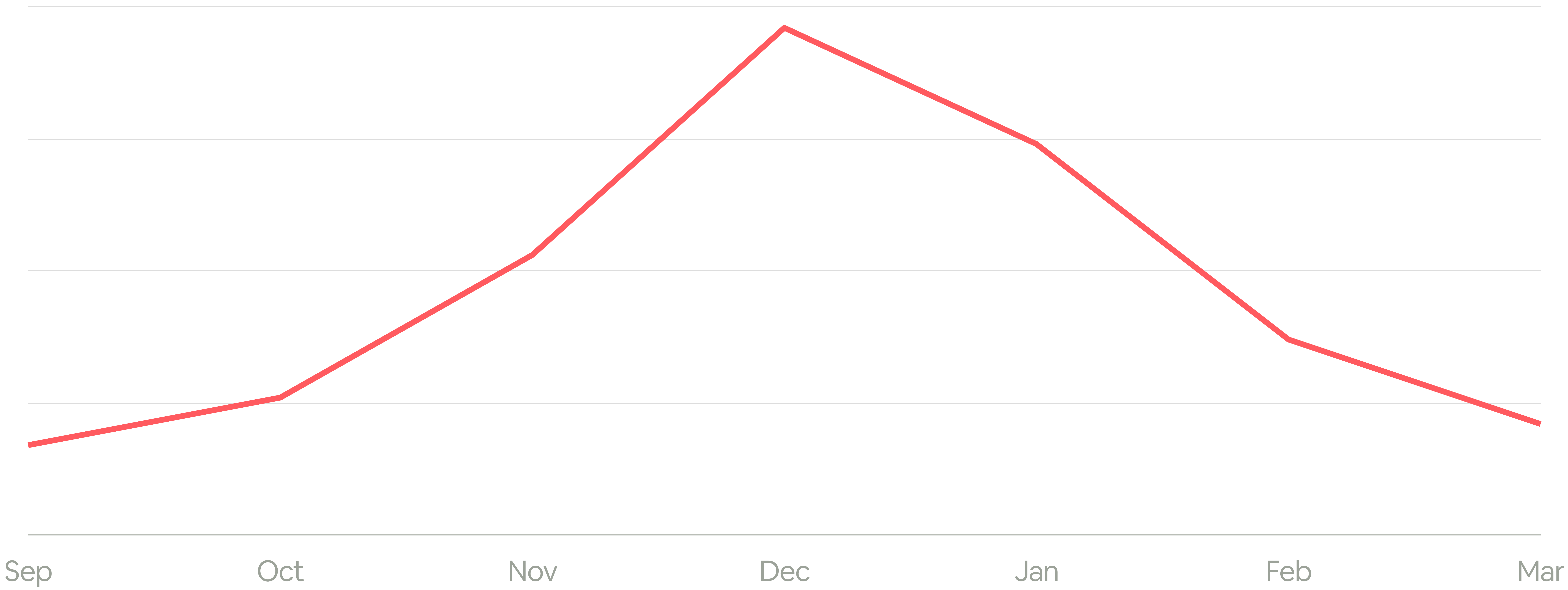


for illustrative purposes only

Using Quantities That Lack Controls

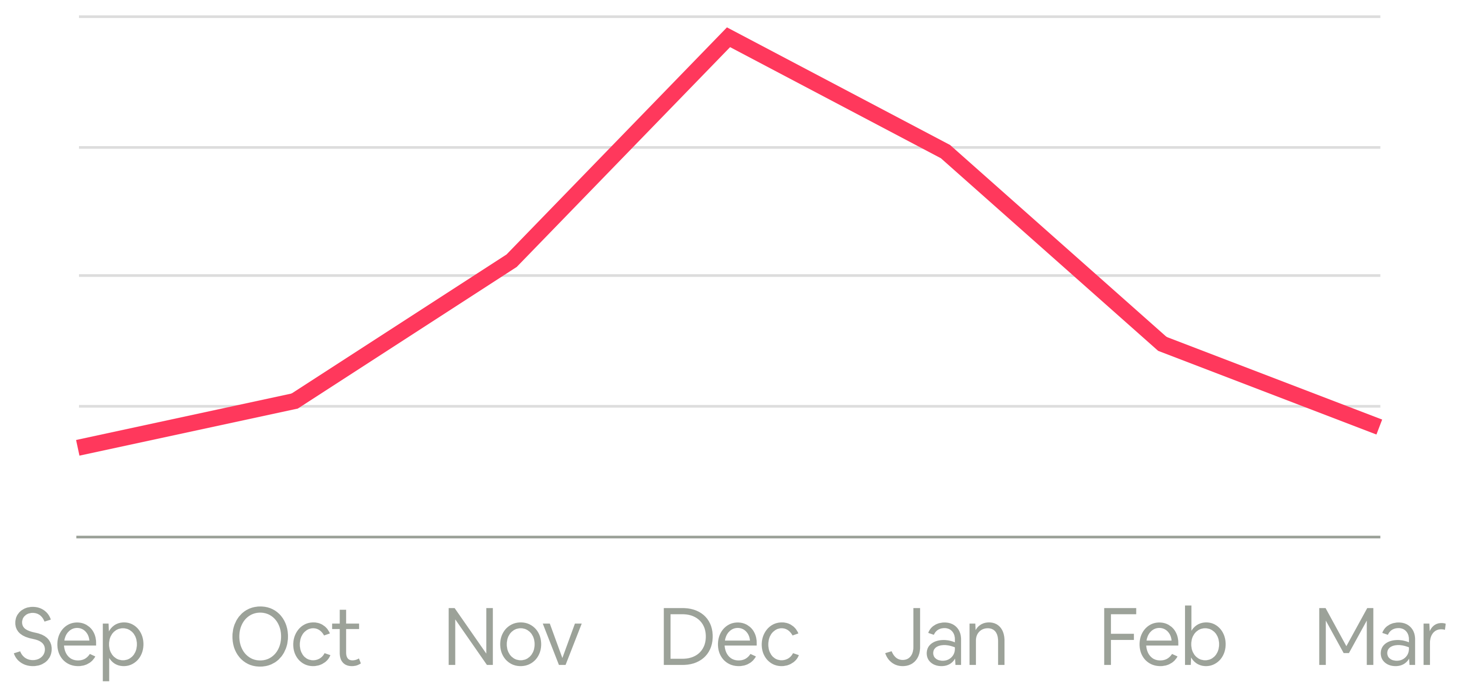
Mistake #2

Mean Time to Recover



for illustrative purposes only

Mean Time to Recover



Outcome

Incidents are resolved quickly and effectively

Question

How long does it take to recover from incidents?

Category

Readiness

Metric control

Playbooks and preventions

Risk reward

Speed ≠ Accuracy or effectiveness

Data requirements

Timestamps for each incident phase

Effort cost

Dependent on complexity of incidents

Metric cost

Low

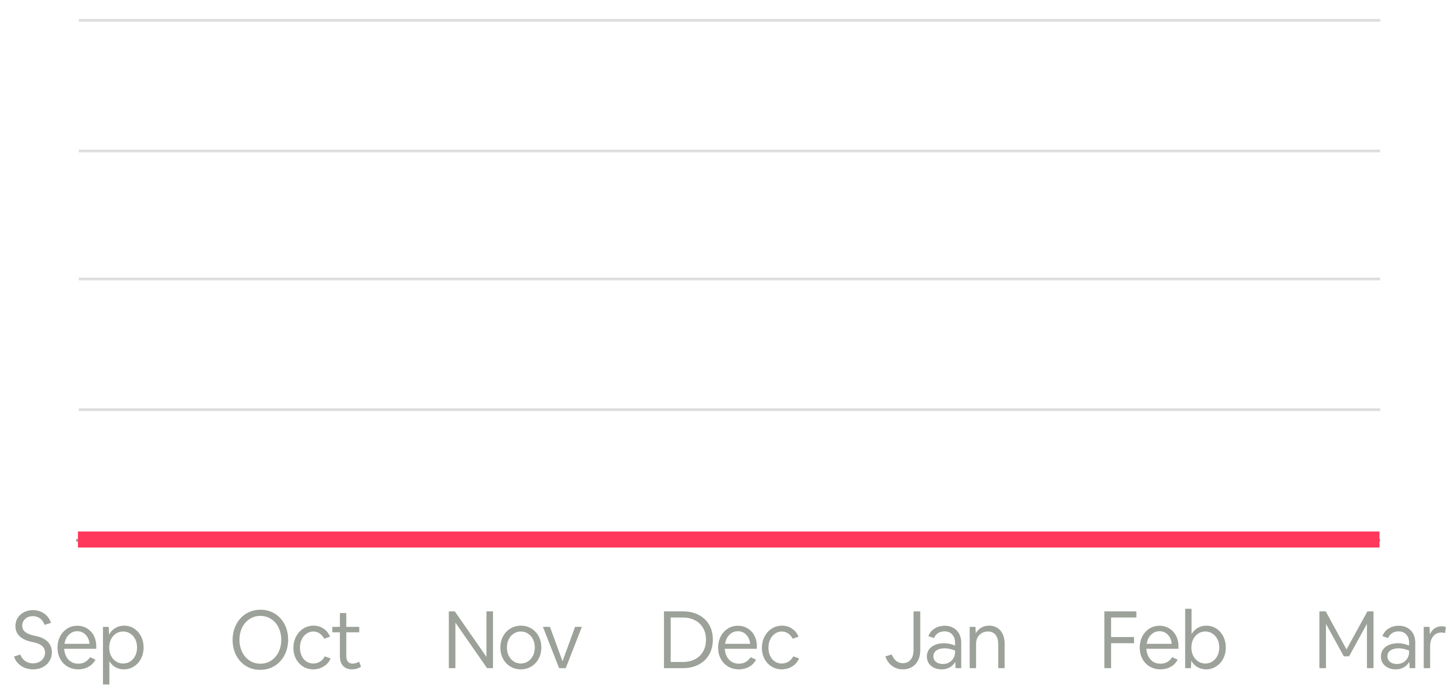
Metric expiration

Prevention cost ≤ Response cost

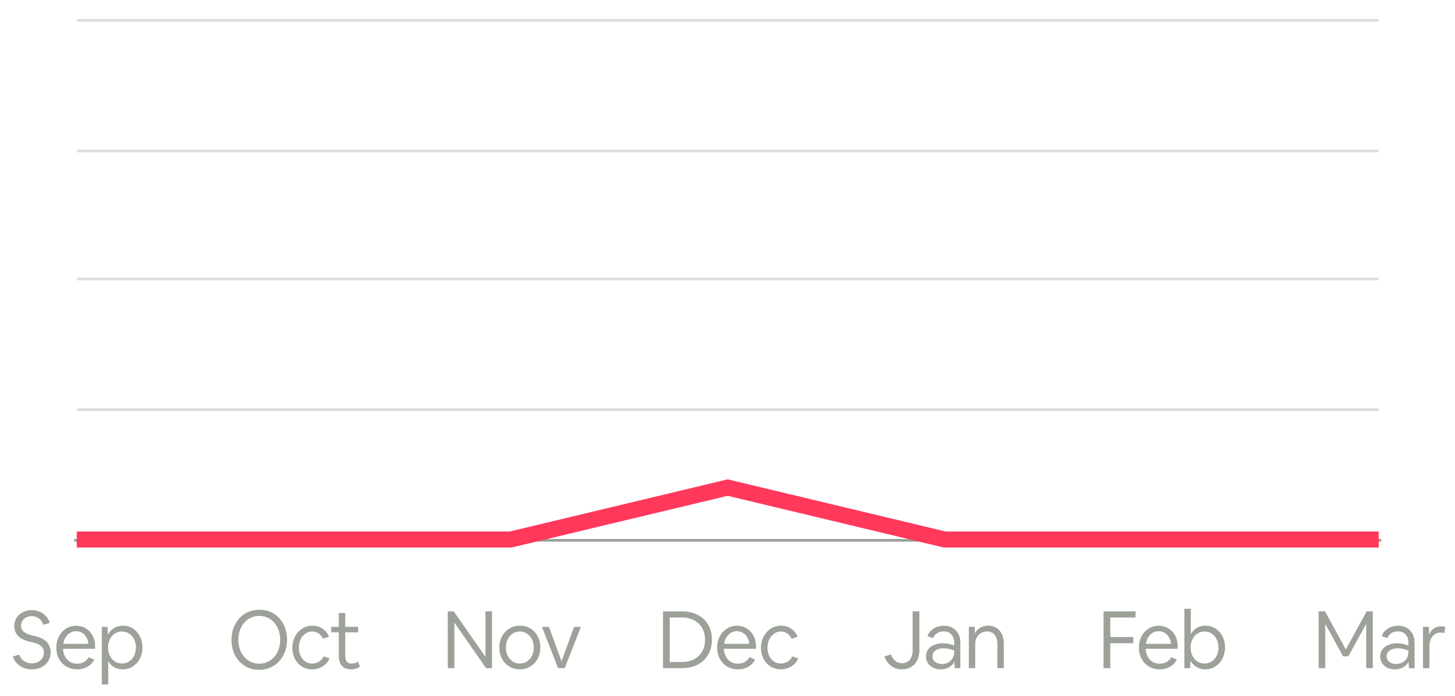
for illustrative purposes only

Response Readiness Metrics

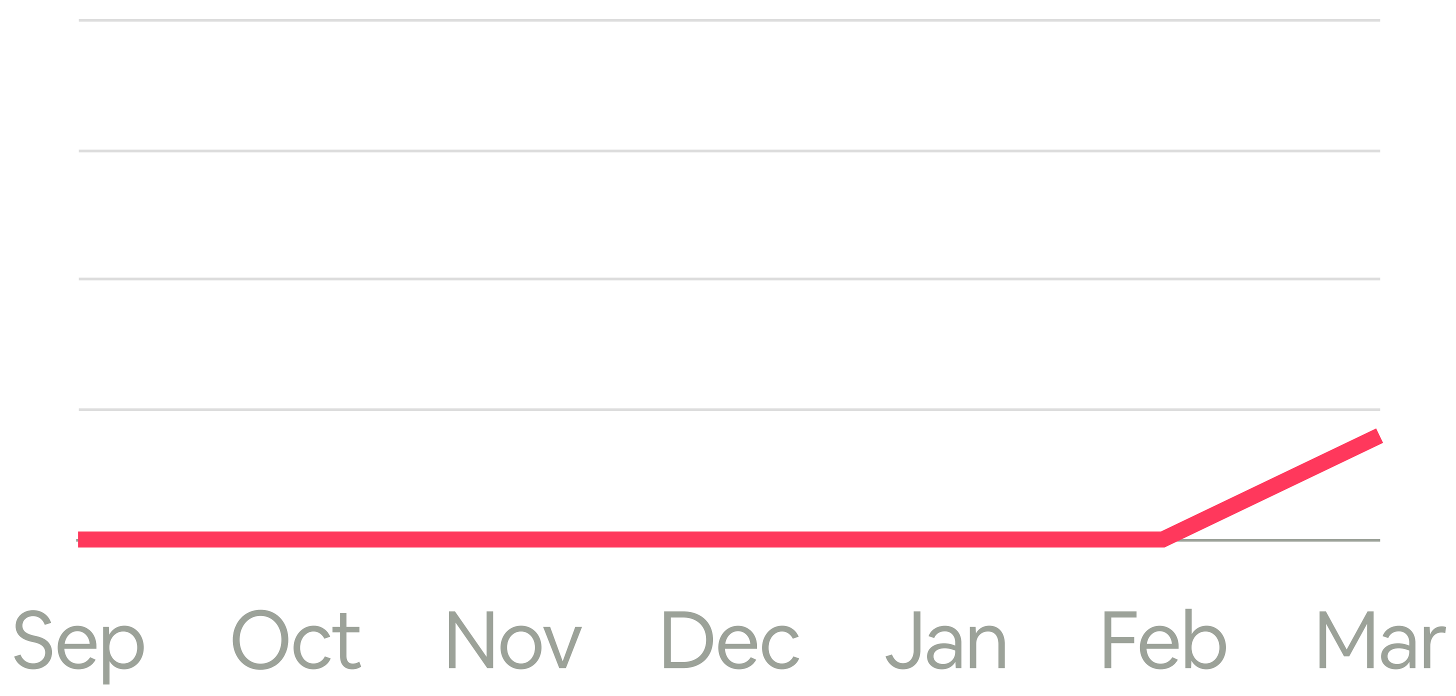
Triage & Analysis
(filtered)



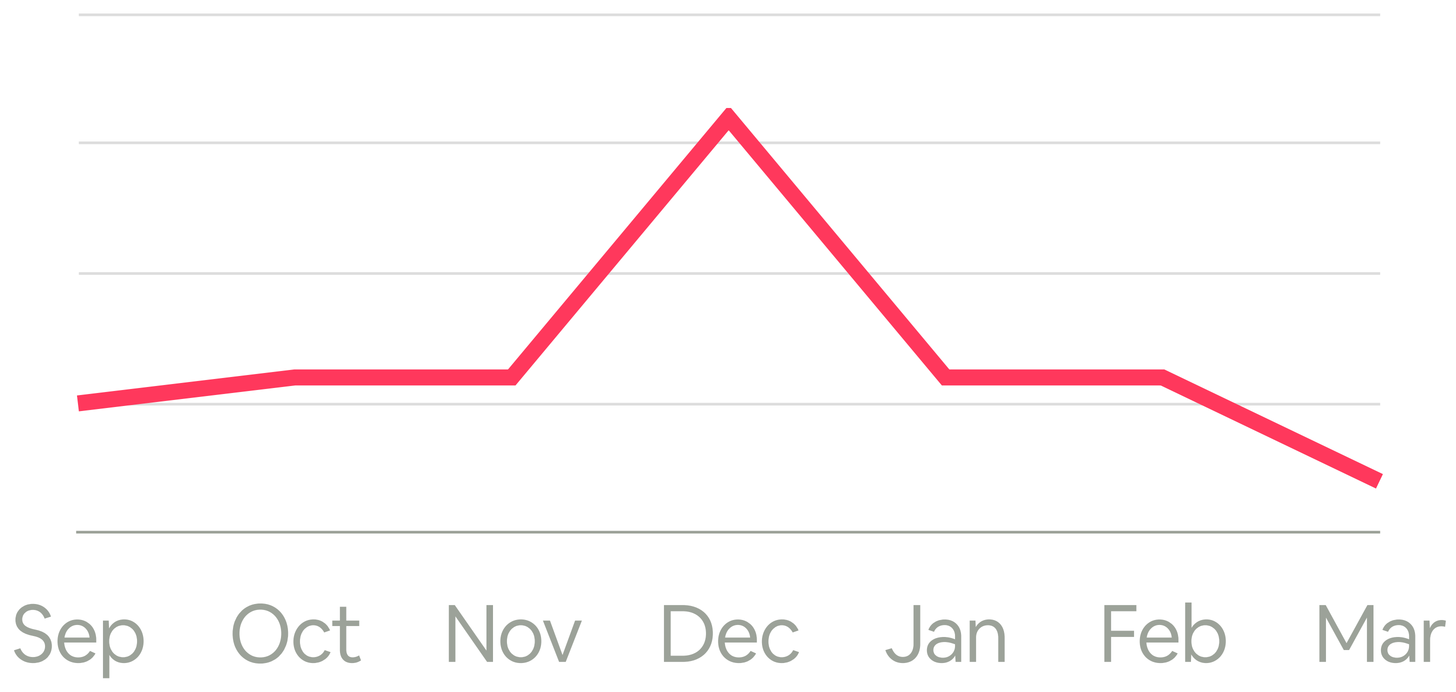
Incident Spin Up Time
(filtered)



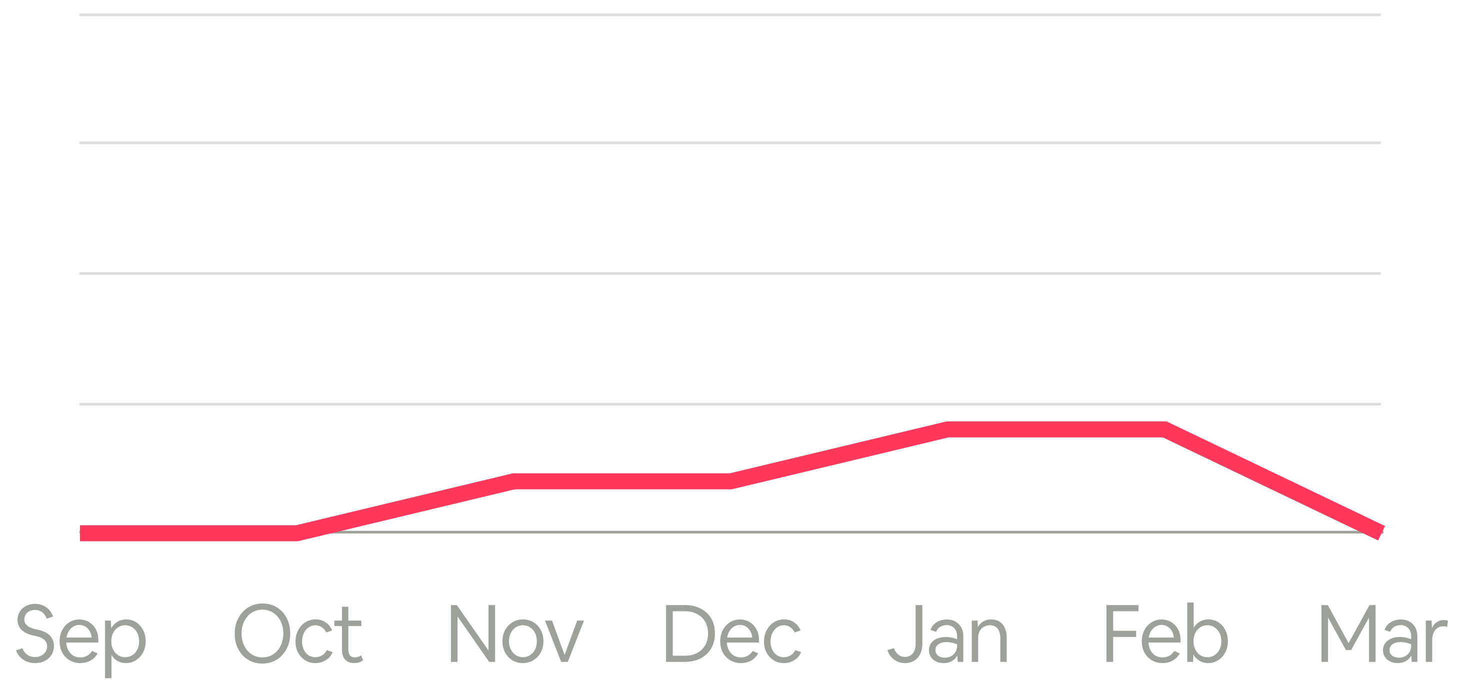
Contain
(filtered)



Remediate
(filtered)



Recover
(filtered)

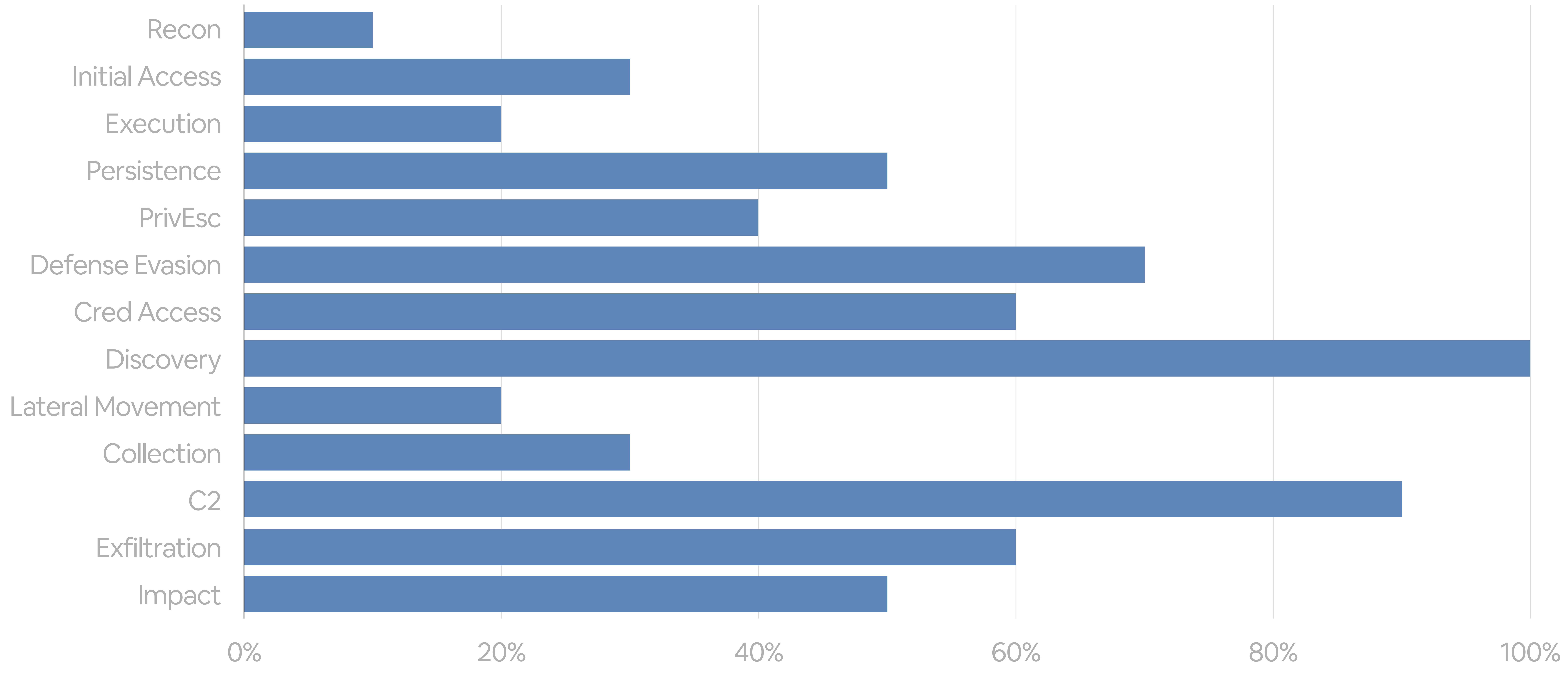


for illustrative purposes only

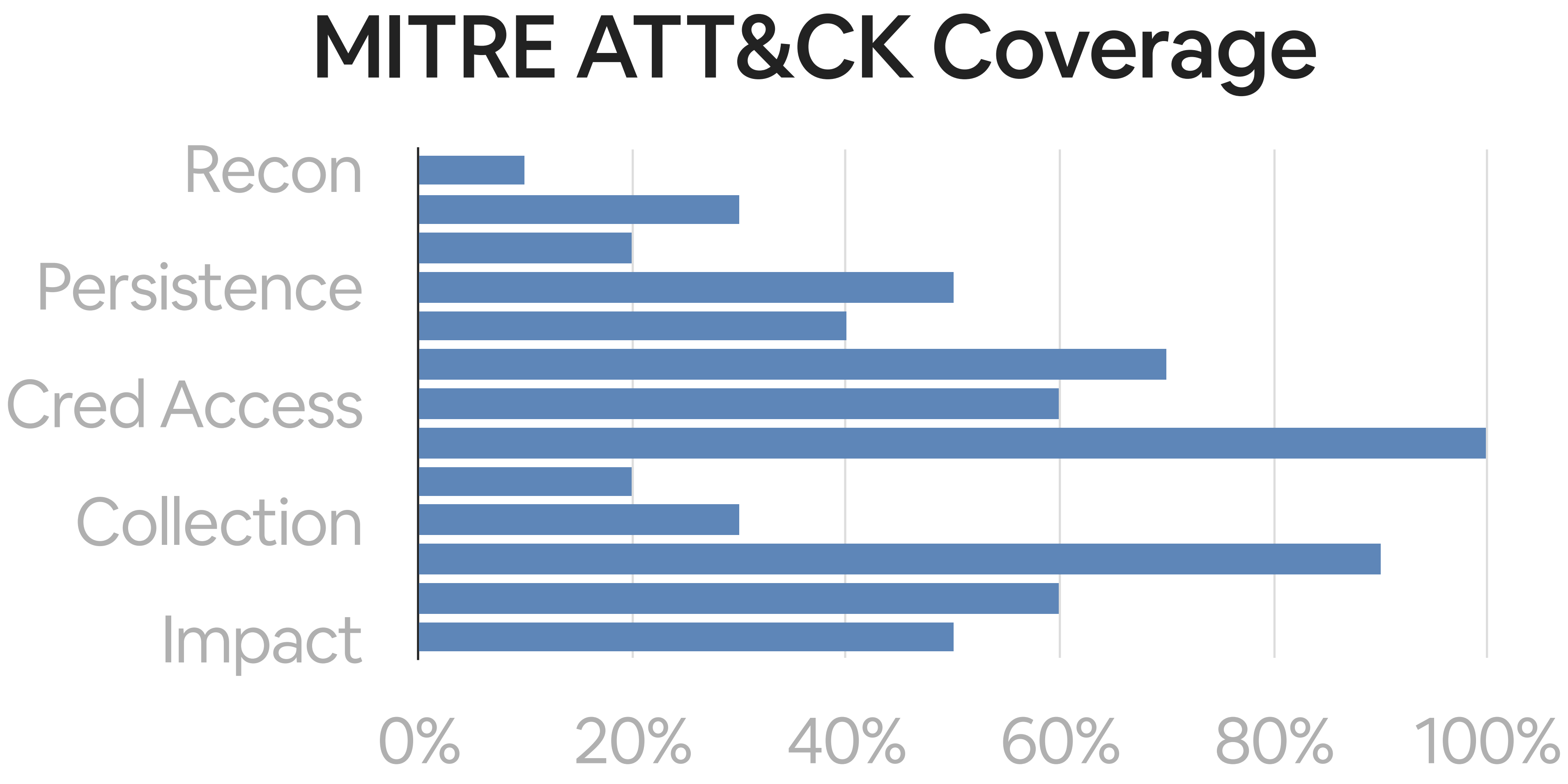
Thinking Proxy Metrics Are Bad

Mistake #3

MITRE ATT&CK Coverage



for illustrative purposes only



Outcome

Detection coverage for known threat techniques

Question

Where do we have gaps in our detections?

Category

Vigilance

Metric control

Building and buying new detections

Risk reward

Low quality detections or tests to quickly get coverage

Data requirements

Testing across the entire MITRE ATT&CK framework

Effort cost

Very high

Metric cost

Very high

Metric expiration

MITRE ATT&CK ≠ Detection priorities

for illustrative purposes only

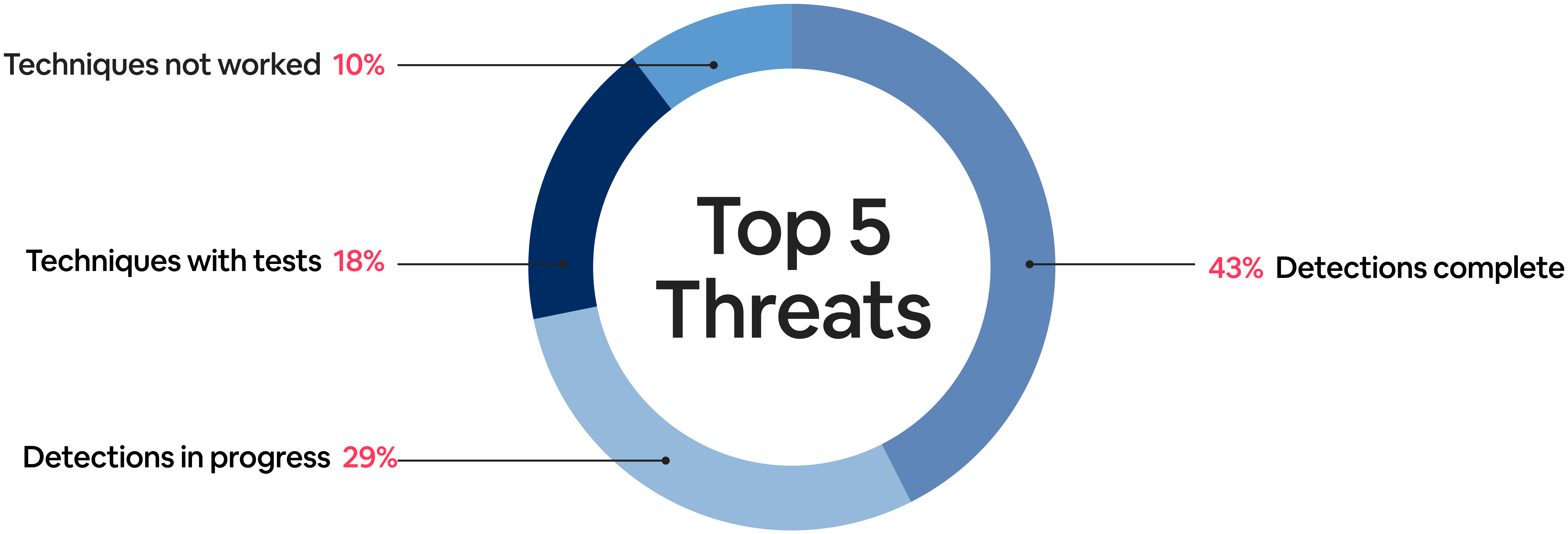
Top 5 Threats

External Threat Intel

Internal Incident Trends

Organization Security Risks

Detection Prioritization

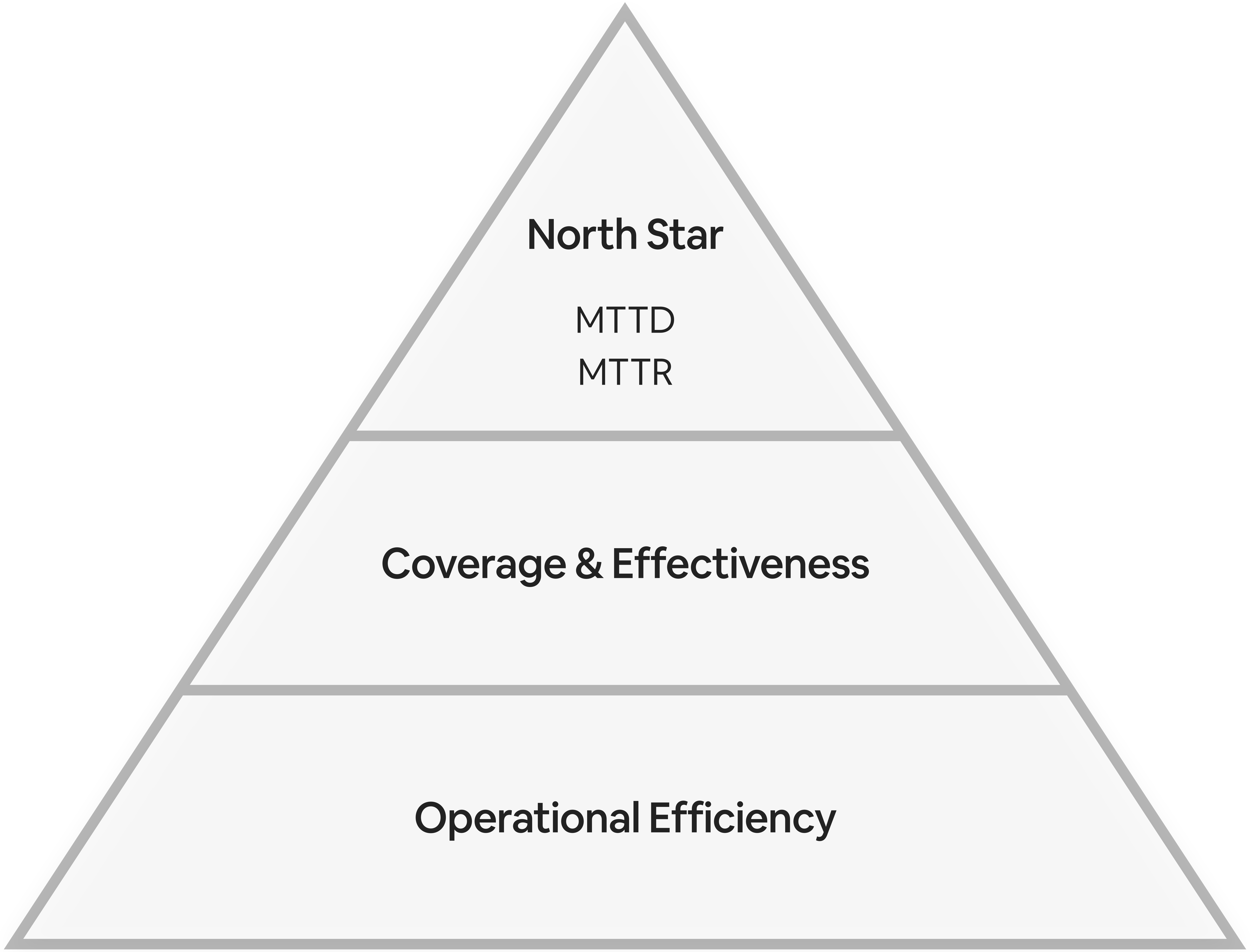


for illustrative purposes only

Not Adjusting to the Altitude

Mistake #4

Cost of an Incident or Breach



North Star

MTTD
MTTR

Coverage & Effectiveness

Operational Efficiency

Asking "Why?" instead of "How?"

Mistake #5

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

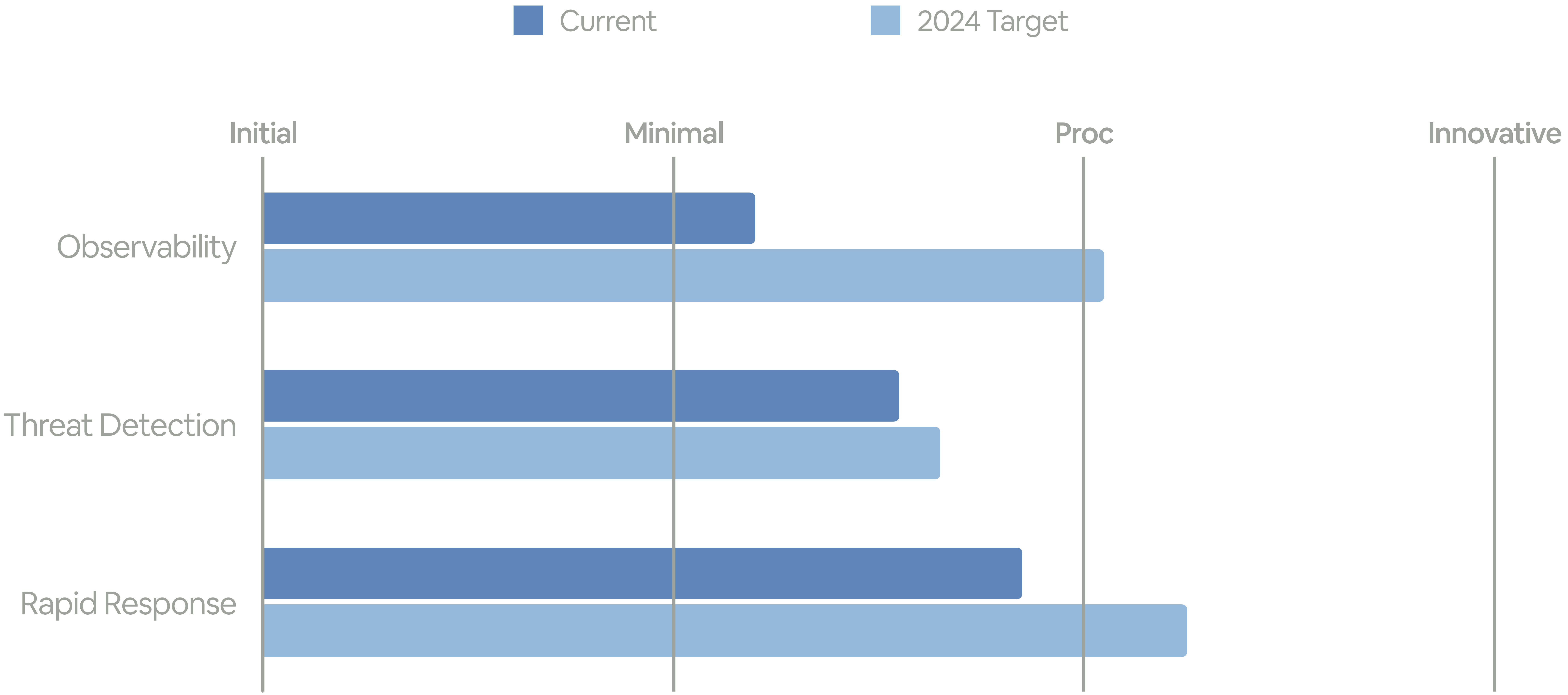
	Initial	Minimal	Procedural	Innovative	Leading
Process	All manual	20-40%	40-60% all criticals	60-80% all criticals and highs	Automated and mature
Tools	Ad-hoc	Defined but not enforced	Centralized	Optimized	AI/ML powered
Docs	None	Mostly knowledge sharing	Complete but manual	Automatic	Live
Testing	None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

What are the results?

Are we getting better?

What data is driving our decisions?

SAVER Metrics

Questions & Outcome

Category

Control & Risk reward

Expiration

Data requirements, Effort & Cost

SAVER Metrics

Outcome

What is the goal of measuring this metric?

Question

What question (north star) does this metric answer?

Category

Which SAVER category does this metric fall under?

Metric control

How do we control this metric today?

Risk reward

What risks could this measurement reward?

Data requirements

What data and sample size is required?

Effort cost

How much new effort is needed to improve this metric?

Metric cost

What is the cost to collect this metric?

Metric expiration

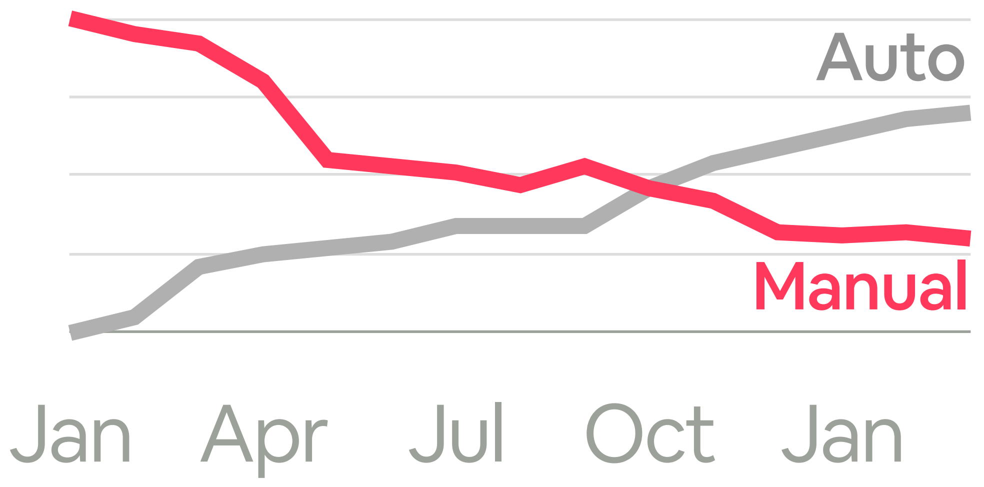
When will this metric no longer be relevant or needed?

Change is hard.

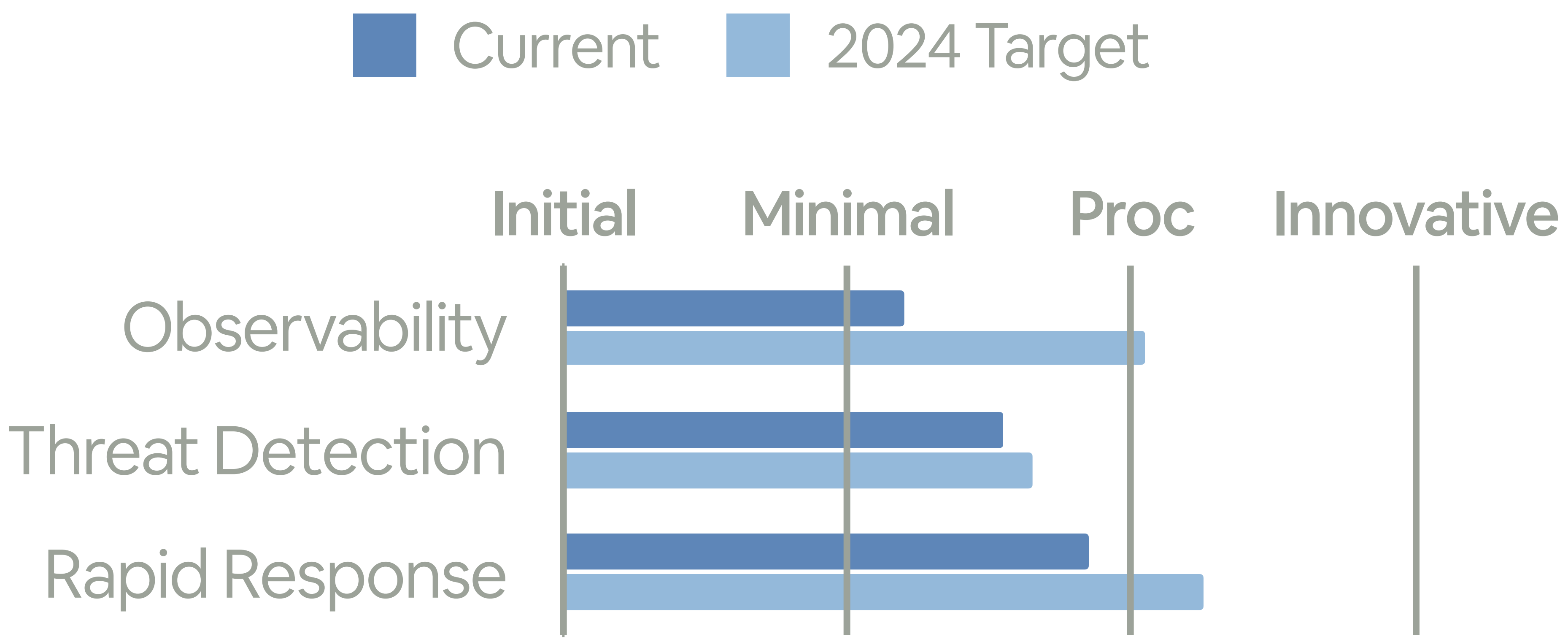
Detection & Response

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

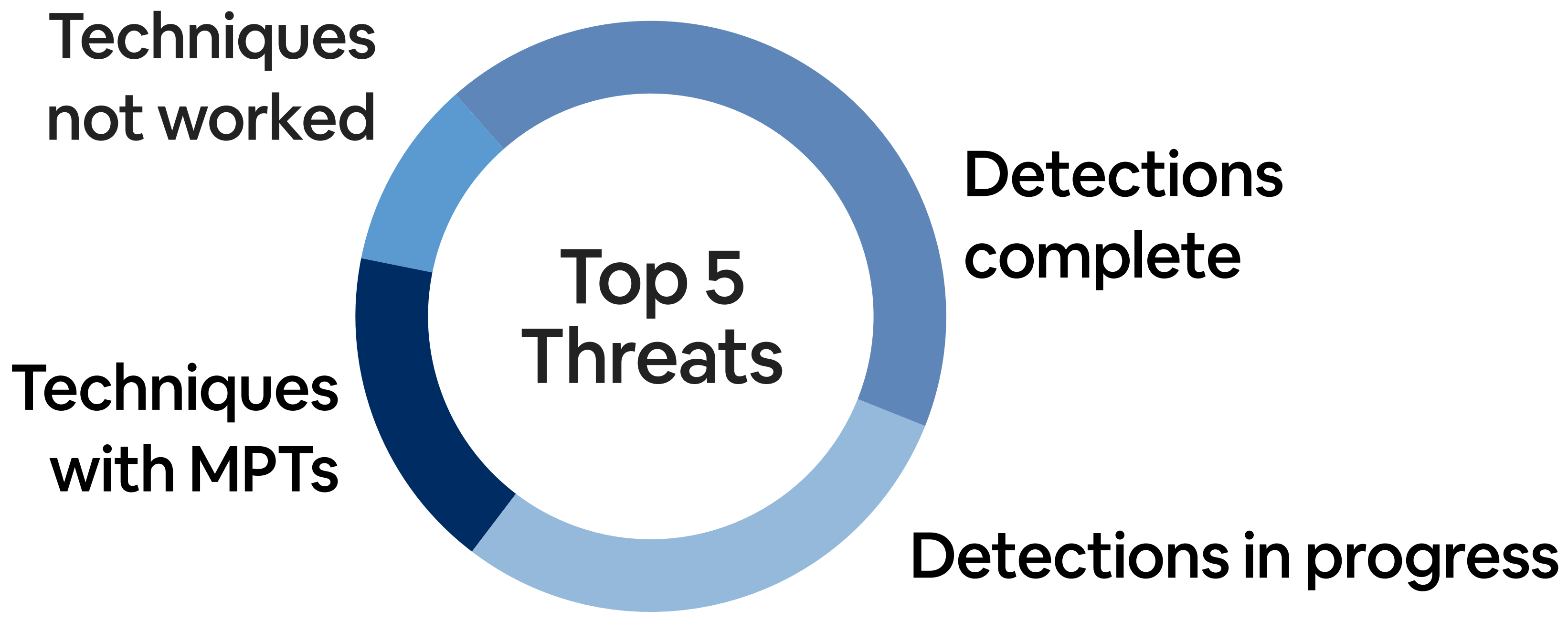
Awareness

Top 5 Threats

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

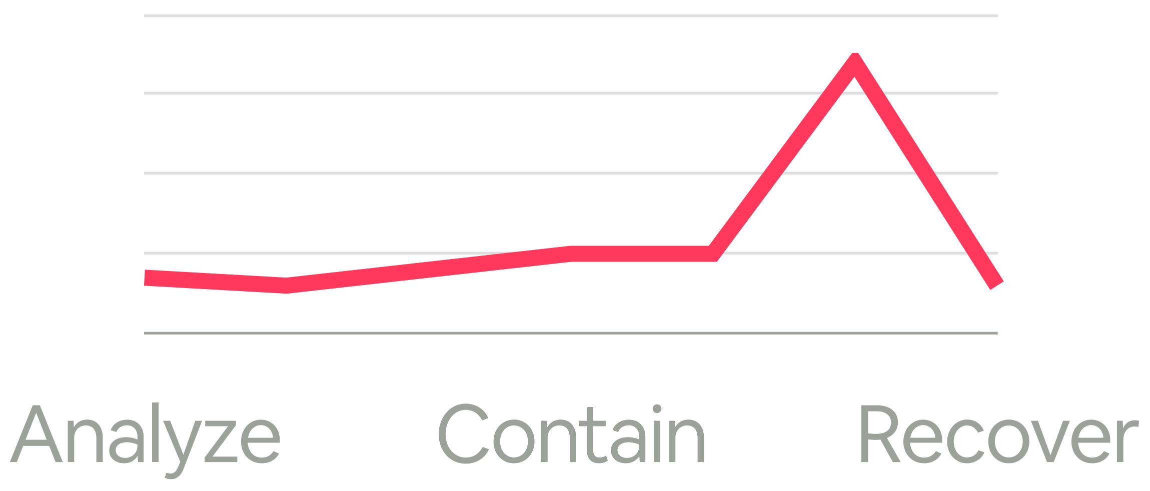
Vigilance

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