How I Learned to Stop Worrying and ~~Love~~

Build a Modern Detection & Response Program

Hi

I’m Allyn

I’m a worrier.

Worrying can be a superpower.

“...worry illuminates the importance of taking action to prevent an undesirable outcome and keeps the situation at the front of one's mind to ensure that appropriate action is taken.”

Sweeny K., Dooley M. D. (2017). The surprising upsides of worry. Social and Personality Psychology Compass, 11, Article e12311

Red team ➡ Blue team

Detection and Response Programs

Legacy

Modern

Legacy

Reactive

Technology-focused

Manual-heavy

Siloed and disjointed

Modern

Proactive

Business-focused

Automation prioritized

Connected and centralized

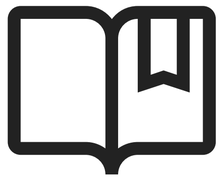
Challenges

Alert fatigue

Expensive tools

Hiring & retention

Firefighting



Organizational Design

A Step-by-Step Approach

Burton et al., 2015

1. Assess the scope and goals
2. Assess the strategy
3. Analyze the structure
4. Assess process and people
5. Analyze coordination
6. Design the architecture
7. Implement the architecture

Assess and analyze

Design and develop

Implement and overcome

Evaluate and report

Assess and analyze

Design and develop

Implement and overcome

Evaluate and report

Stop doing
and start learning

Viewpoints

People

Technology

Vision & mission

Vision & mission

What is unique?

What are the problems?

What are people doing?

Viewpoints

People

Technology

Vision & mission

People

NICE Cybersecurity Workforce Framework

NICE Cybersecurity Workforce Framework

People

Threat Intel Engineer

- All-Source Analyst
- Exploit Analyst
- Language Analyst
- Target Network Analyst
- Threat Warning Analyst
- Collection Manager
- Integration Planner
- Target Developer

Threat Triage Analyst

- Cyber Defense Analyst
- Cyber Operator

Incident Responder

- Incident Responder
- Forensic Analyst
- Vulnerability Analyst
- Counter Intel Analyst
- Crime Investigator
- Legal Advisor
- Privacy Compliance

D&R Engineer

- Software Developer
- Systems Analyst
- Security Architect
- Enterprise Architect
- Infrastructure Support
- Systems Administrator
- Database Administrator
- Research & Development
- Knowledge Manager
- Operations Planner
- Mission Specialist

Forensic Analyst

None

Novice

Intermediate

Expert

Threat Intel Engineer

- All-Source Analyst
- Exploit Analyst
- Language Analyst
- Target Network Analyst
- Threat Warning Analyst
- Collection Manager
- Integration Planner
- Target Developer

Threat Triage Analyst

- Cyber Defense Analyst
- Cyber Operator

Incident Responder

- Incident Responder
- Forensic Analyst
- Vulnerability Analyst
- Counter Intel Analyst
- Crime Investigator
- Legal Advisor
- Privacy Compliance

D&R Engineer

- Software Developer
- Systems Analyst
- Security Architect
- Enterprise Architect
- Infrastructure Support
- Systems Administrator
- Database Administrator
- Research & Development
- Knowledge Manager
- Operations Planner
- Mission Specialist

Viewpoints

People

Technology

Vision & mission


Technology

Technical capabilities

not product categories

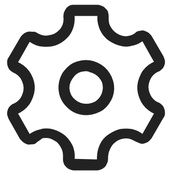
Assess and analyze

Design and develop

Implement and overcome

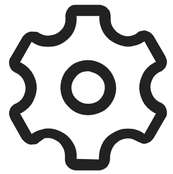
Evaluate and report

Design and develop

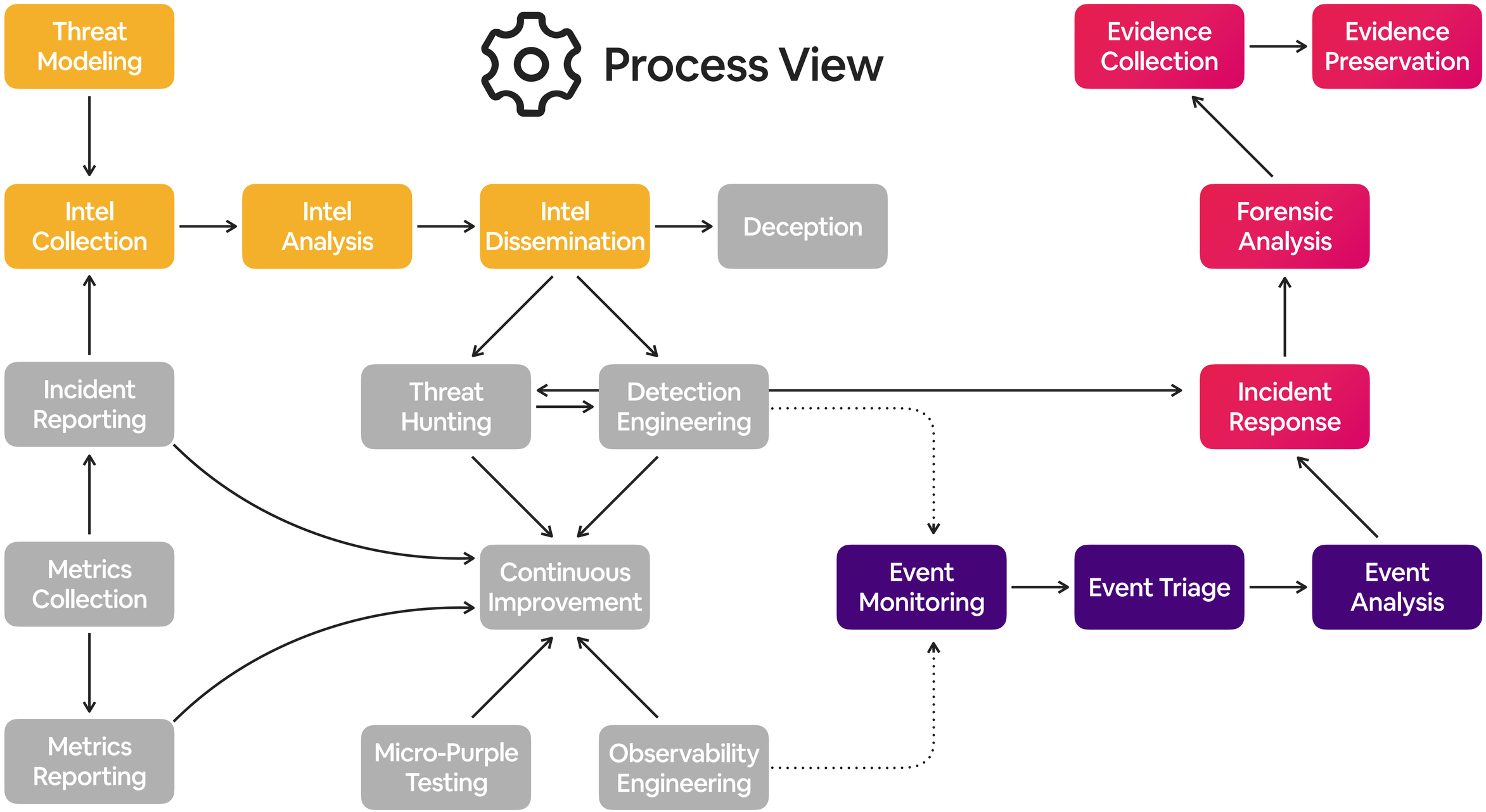


Process view

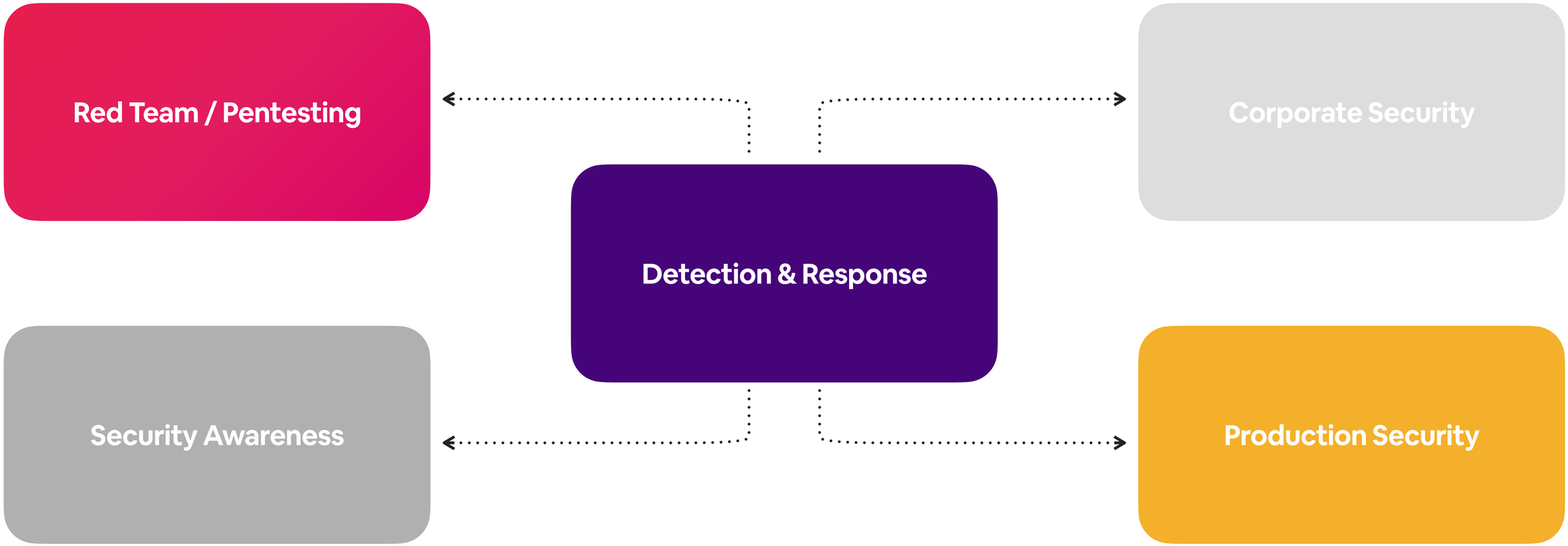
Architecture view



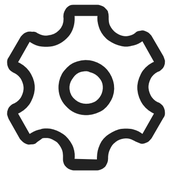
What processes do we need?


Process View
Threat Modeling
Intel Collection
Intel Analysis
Intel Dissemination
Deception
Incident Reporting
Threat Hunting
Detection Engineering
Metrics Collection
Continuous Improvement
Metrics Reporting
Micro-Purple Testing
Observability Engineering
Event Monitoring
Event Triage
Event Analysis
Incident Response
Forensic Analysis
Evidence Collection
Evidence Preservation

Process View



Design and develop



Process view

Architecture view

What capabilities do we need?

Capability frameworks

MITRE ATT&CK

MITRE D3FEND

Tines.io SOC Automation Matrix

Snowflake's Detection series

Maturity Model

Observability

Proactive Threat Detection

Rapid Response

Observability

Entity & Activity Coverage

Searchability

Contextualization

Enrichment Sourcing

Proactive Threat Detection

Intelligence Sourcing

Coverage & Gaps

Efficacy, Effectiveness, & Efficiency

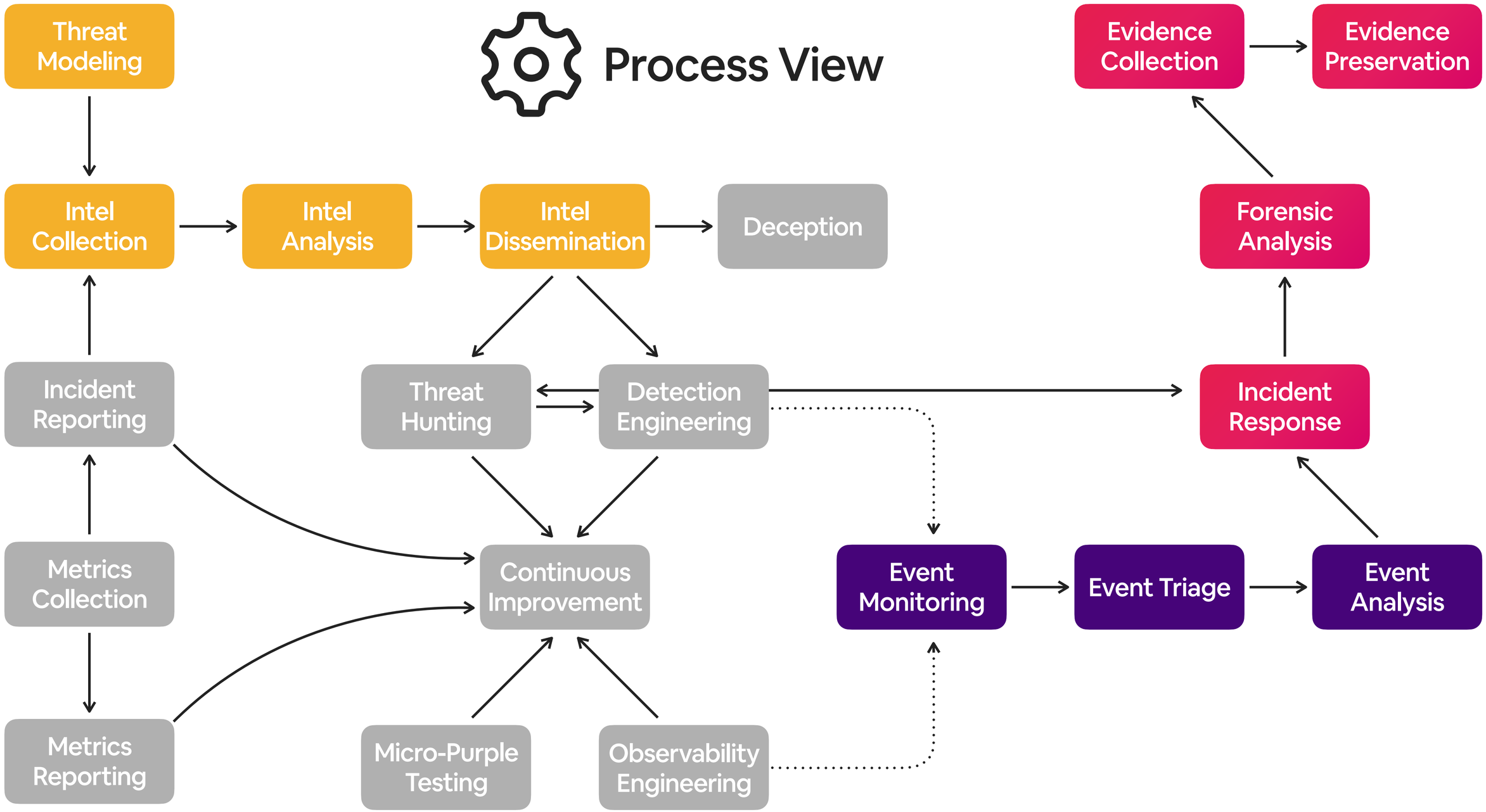
Accuracy

Rapid Response

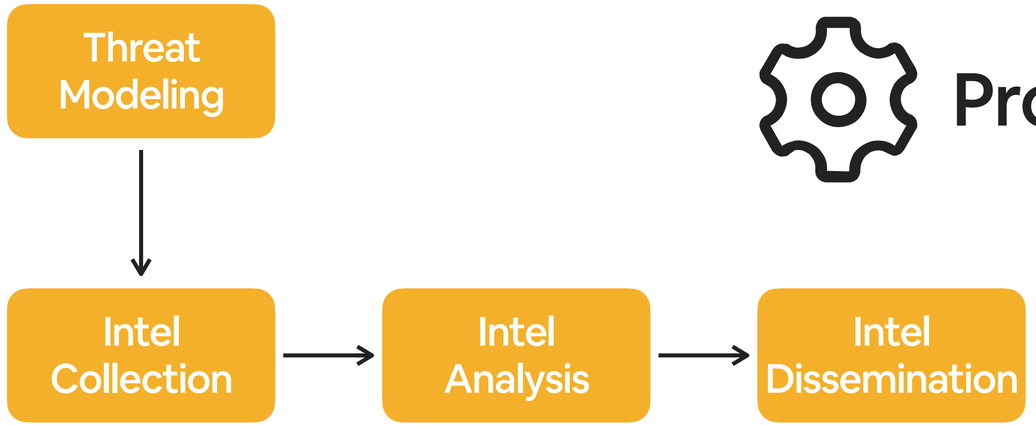
Scenario Coverage

Organizational Coverage

Speed, Accuracy, & Completeness


Process View
Threat Modeling
Intel Collection
Intel Analysis
Intel Dissemination
Deception
Incident Reporting
Threat Hunting
Detection Engineering
Metrics Collection
Continuous Improvement
Metrics Reporting
Micro-Purple Testing
Observability Engineering
Event Monitoring
Event Triage
Event Analysis
Incident Response
Forensic Analysis
Evidence Collection
Evidence Preservation

Process View



Threat Actor Profiling

Intrusion Set Analysis

Raw Intel Collection

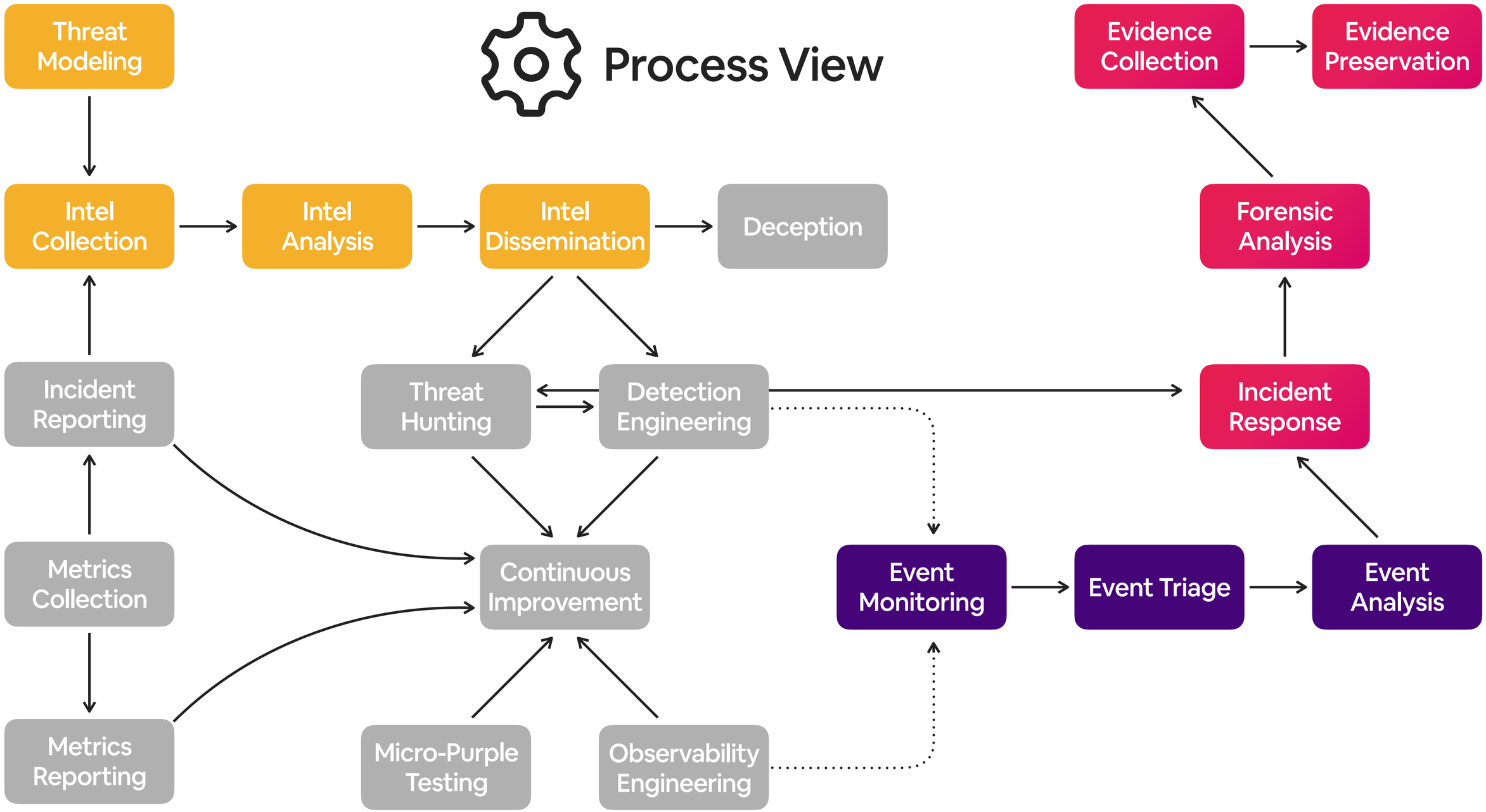
Early Warning

Brand & Reputation Monitoring

Account Takeover Prevention

Collection & Dissemination

Intel Driven Detection


Process View
Threat Modeling
Intel Collection
Intel Analysis
Intel Dissemination
Deception
Incident Reporting
Threat Hunting
Detection Engineering
Metrics Collection
Continuous Improvement
Metrics Reporting
Micro-Purple Testing
Observability Engineering
Event Monitoring
Event Triage
Event Analysis
Incident Response
Forensic Analysis
Evidence Collection
Evidence Preservation

Process View

Response Orchestration

Incident Escalation

Forensic Acquire

IP/DNS Blacklisting

Signature-based Blocking

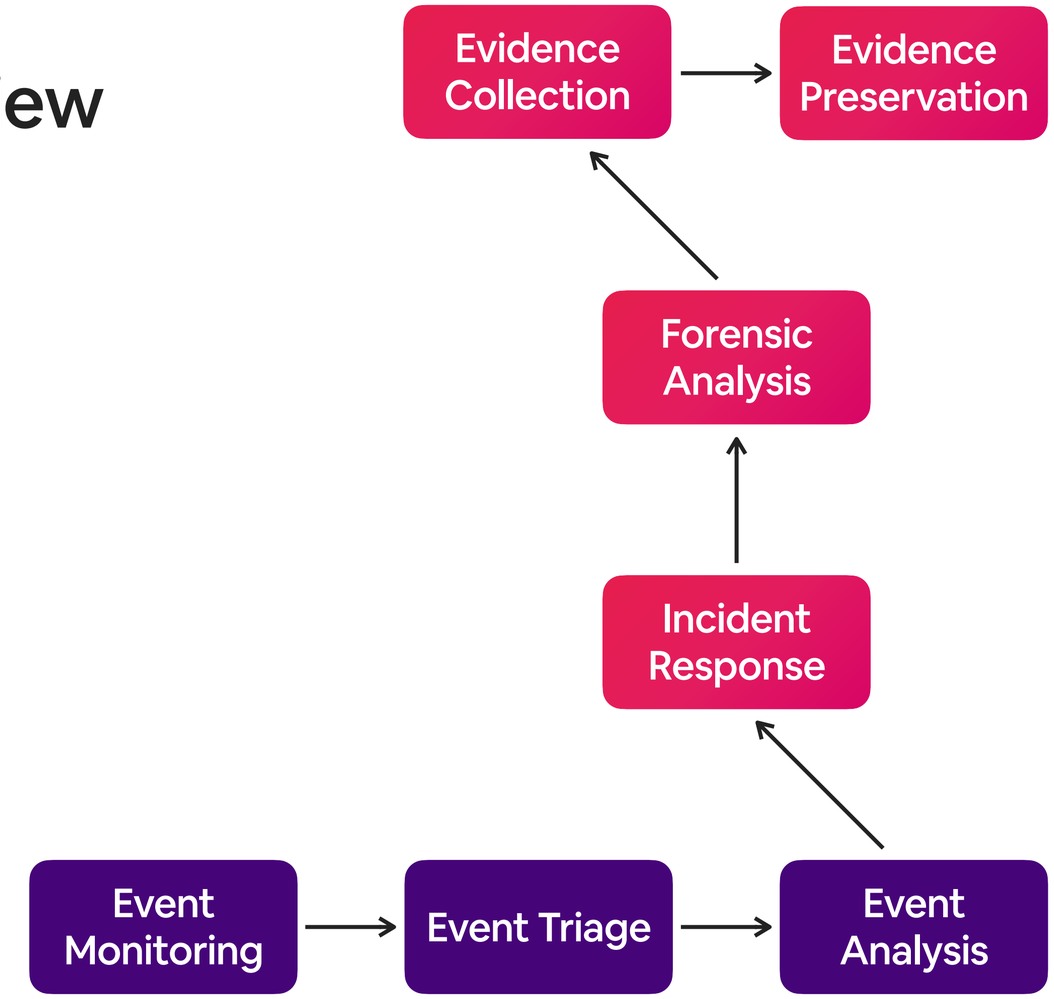
Identity Blocking

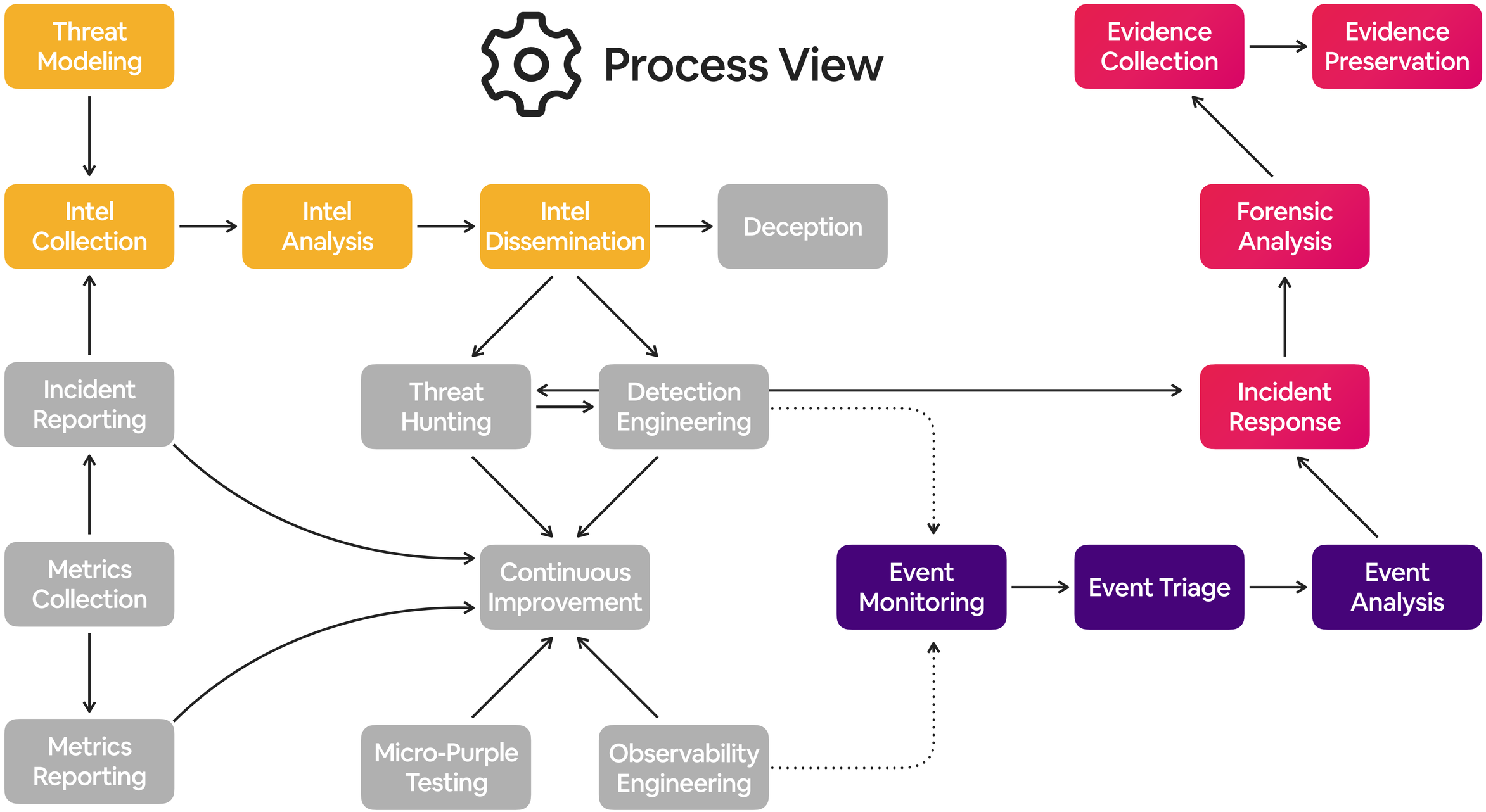
Event Workflow Automate

Event Analysis Automate

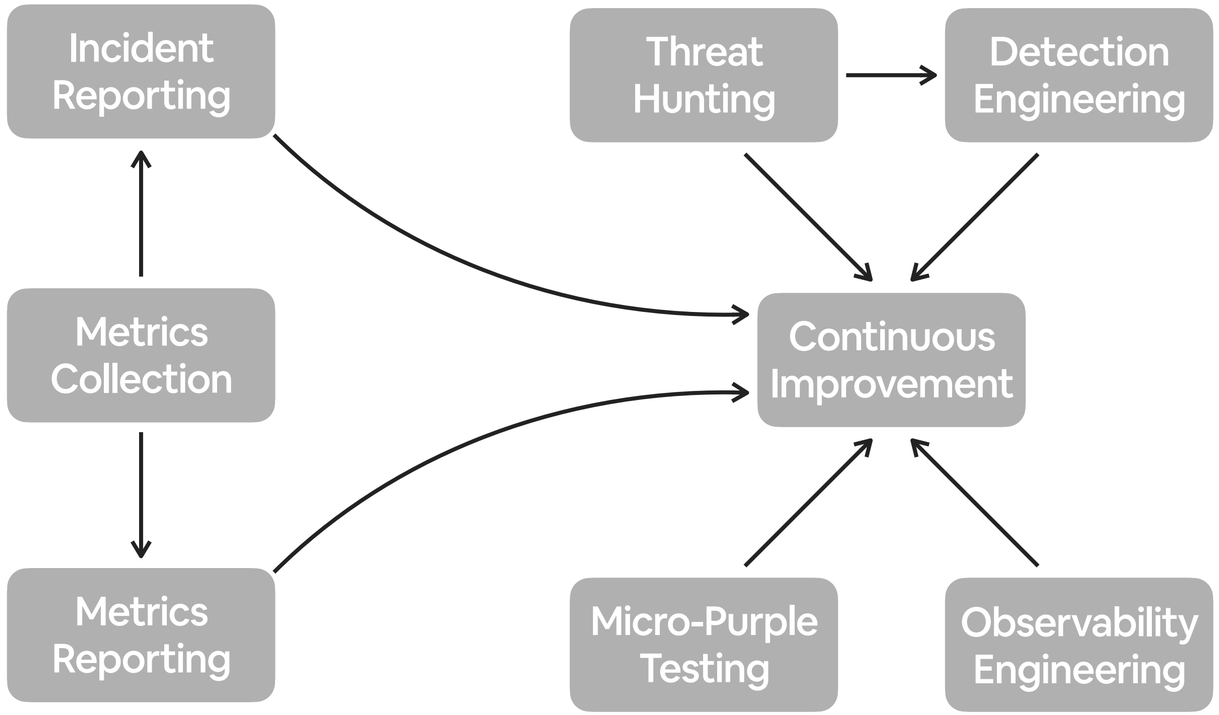
Case Management

Asset Management




Process View
Threat Modeling
Intel Collection
Intel Analysis
Intel Dissemination
Deception
Incident Reporting
Threat Hunting
Detection Engineering
Metrics Collection
Continuous Improvement
Metrics Reporting
Micro-Purple Testing
Observability Engineering
Event Monitoring
Event Triage
Event Analysis
Incident Response
Forensic Analysis
Evidence Collection
Evidence Preservation

Process View



Deception

Log Collection

Log Normalization

Log Enrichment

Data / Traffic Aggregate

Event Correlation

Historical Context

Search Optimize

Threat Behavior Analytics

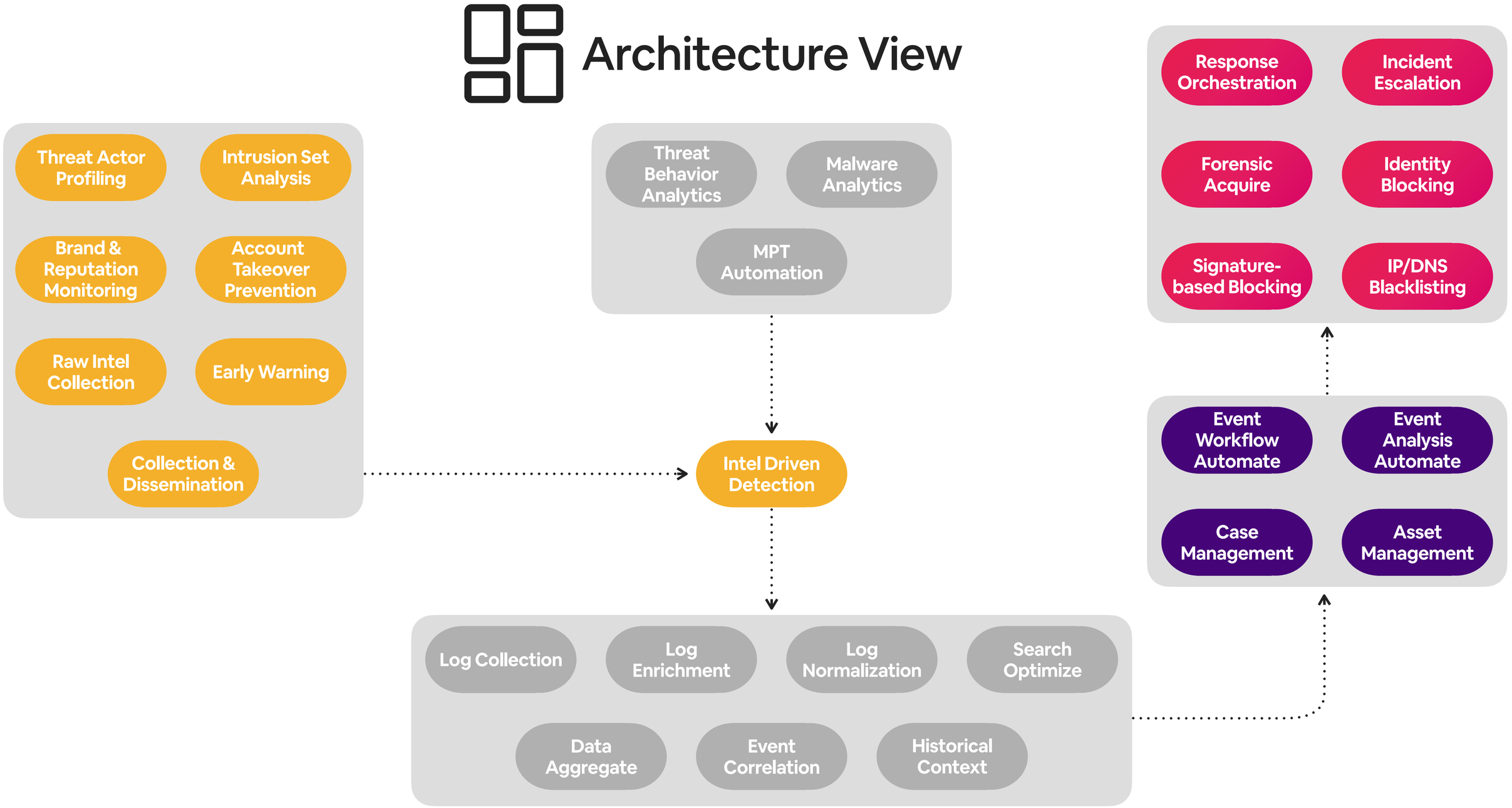
Malware Analytics

MPT Automation

Architecture View

- Threat Actor Profiling
- Intrusion Set Analysis
- Log Collection
- Log Normalization
- Response Orchestration
- Incident Escalation
- Brand & Reputation Monitoring
- Account Takeover Prevention
- Log Enrichment
- Data Aggregate
- Forensic Acquire
- Signature-based Blocking
- Raw Intel Collection
- Early Warning
- Event Correlation
- Historical Context
- Event Workflow Automate
- Event Analysis Automate
- Collection & Dissemination
- Threat Behavior Analytics
- Search Optimize
- Identity Blocking
- Asset Management
- Malware Detection
- Intel Driven Detection
- Malware Analytics
- MPT Automation
- IP/DNS Blacklisting
- Case Management

Architecture View



Assess and analyze

Design and develop

Implement and overcome

Evaluate and report

Implement and overcome

Hire and outsource

Build and buy

Overcome operations

Assess and analyze

Design and develop

Implement and overcome

Evaluate and report

Evaluate and report

Legacy

Modern

Legacy

Reactive

Event count focused

One-dimensional

Lacks business relevance

Modern

Proactive

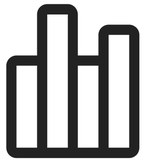
Threat focused

Three-dimensional

Quantifies business risk

Evaluate and report

Observability



Metrics

Narratives

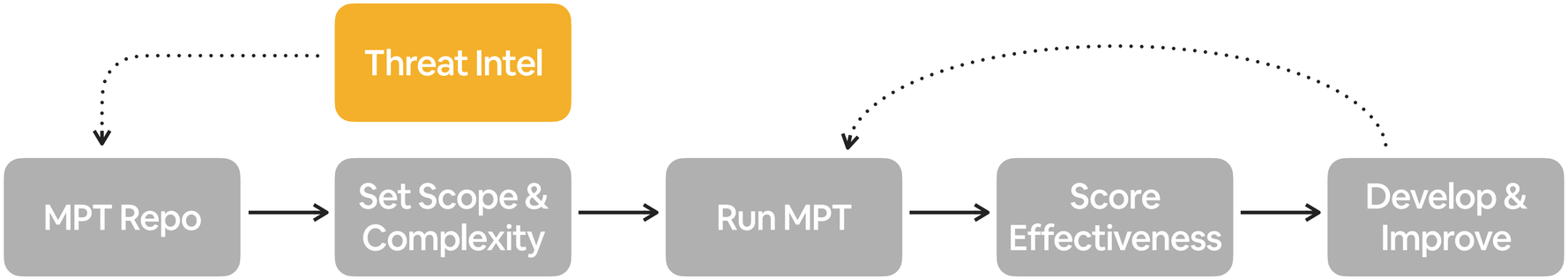
Roadmap

What can we detect today?

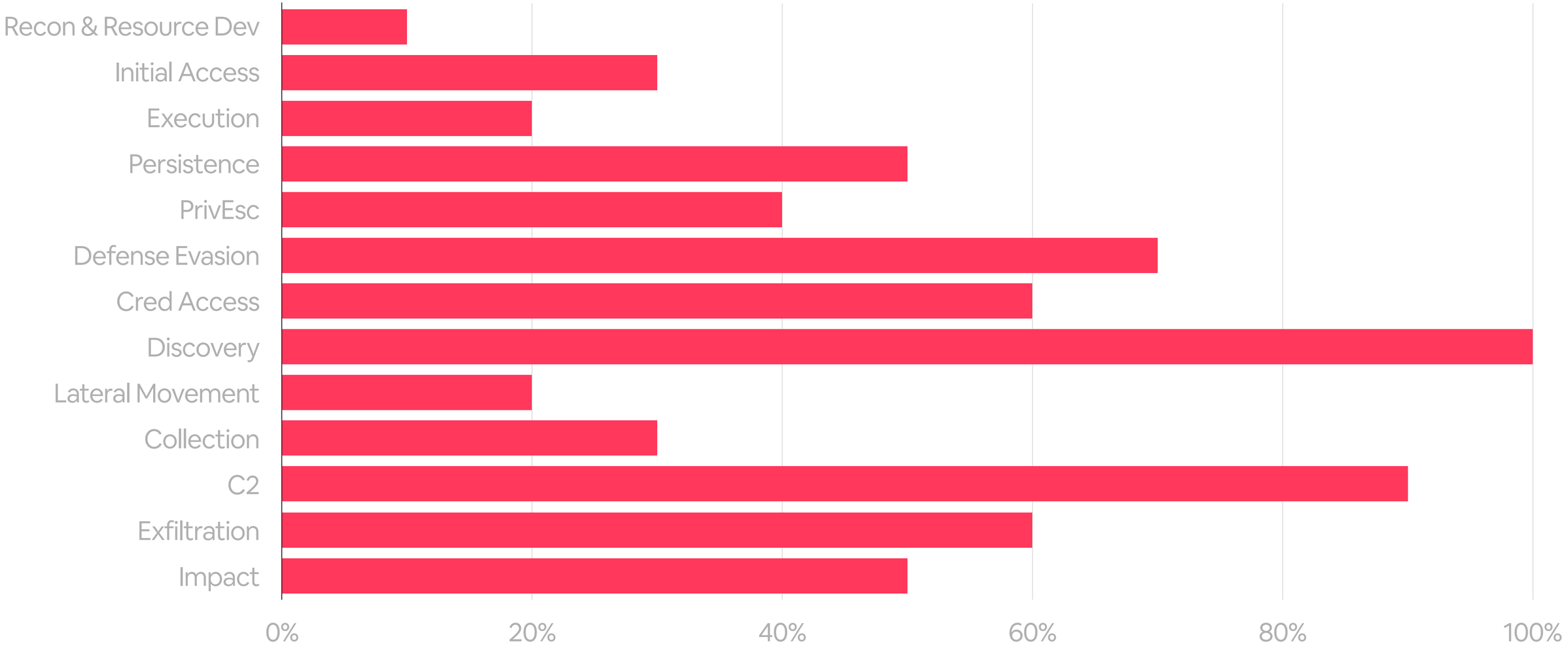
What's our landscape coverage?

What's our overall visibility into threats?

Micro-Purple Testing and Continuous Improvement

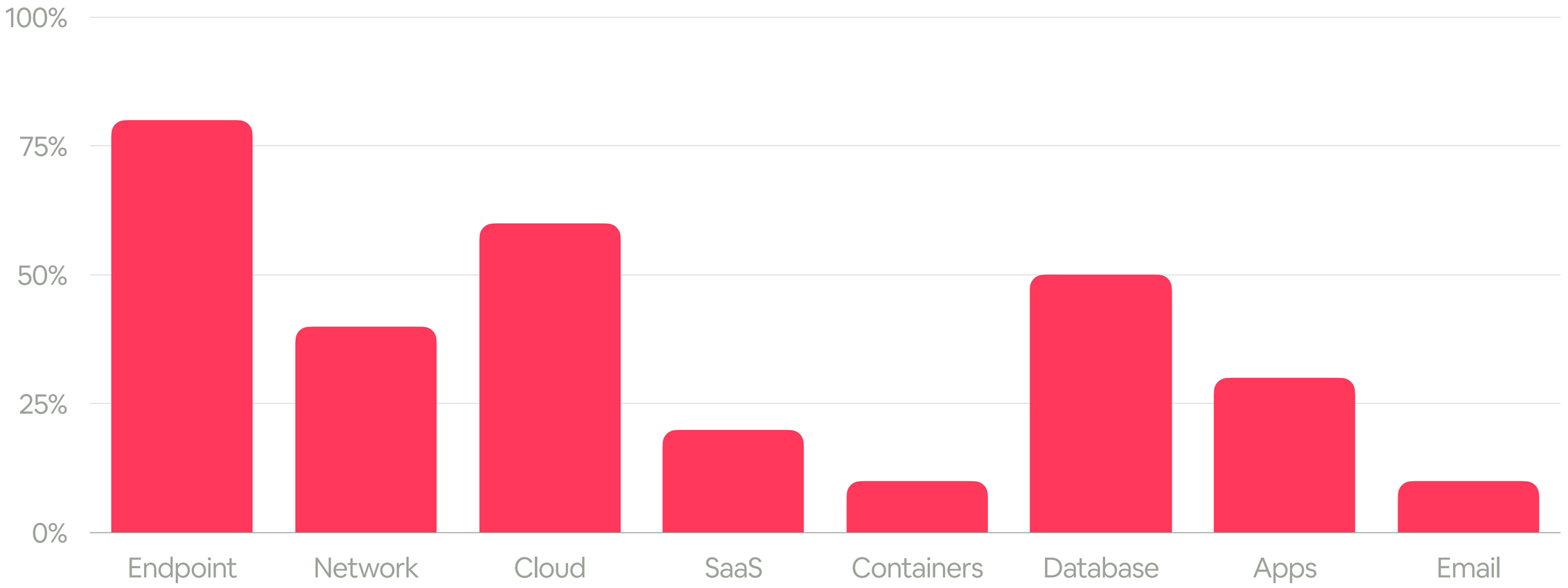


What can we detect today?



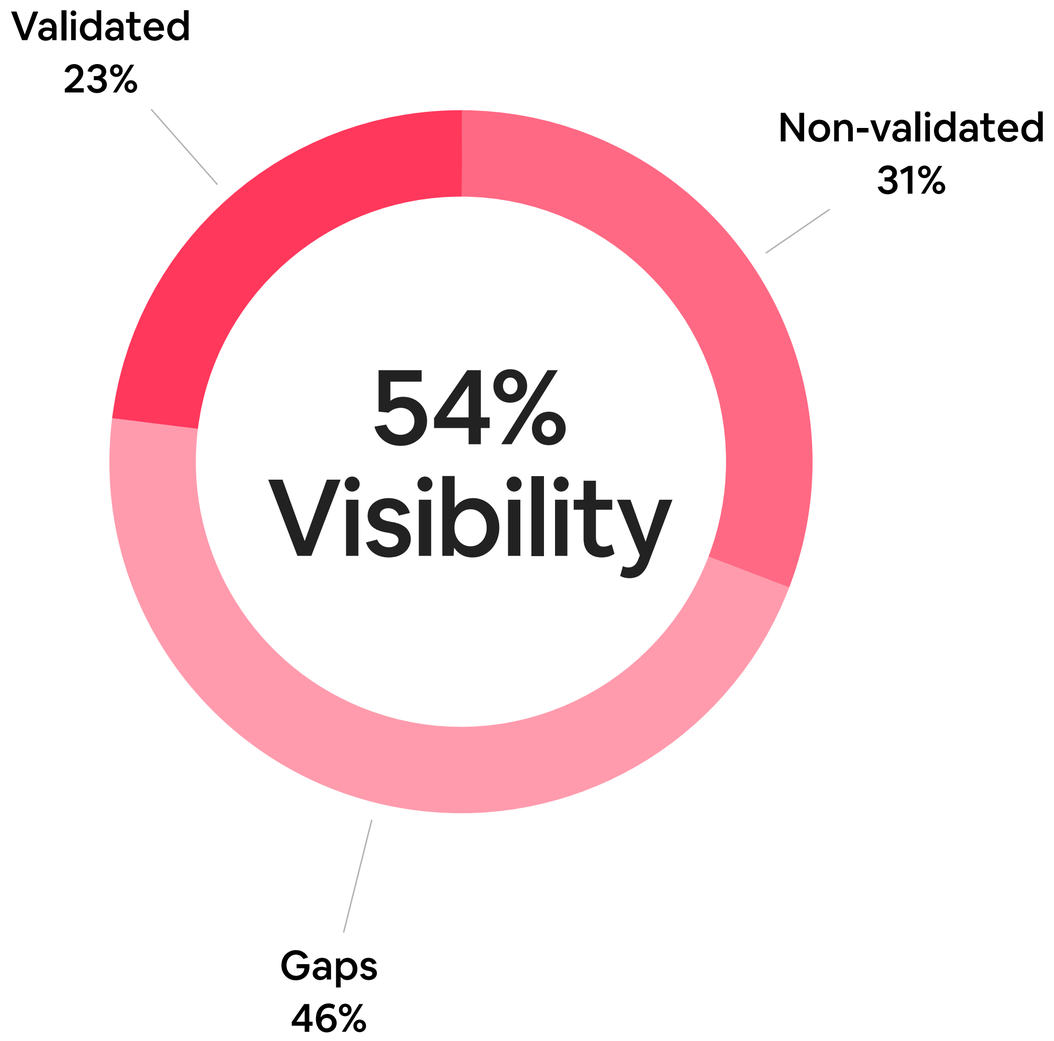
for illustrative purposes only

What's our landscape coverage?



for illustrative purposes only

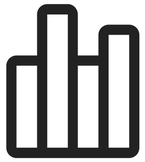
What's our overall visibility into threats?



for illustrative purposes only

Evaluate and report

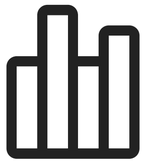
Observability



Metrics

Narratives

Roadmap



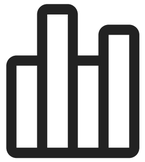
What are the top threats?

What risks and impacts are we seeing from incidents?

What top preventative controls would reduce risk and impact?

Evaluate and report

Observability



Metrics

Narratives

Roadmap

In recent incidents:

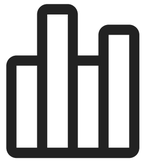
How did the processes perform?

Technologies?

People roles?

Evaluate and report

Observability



Metrics

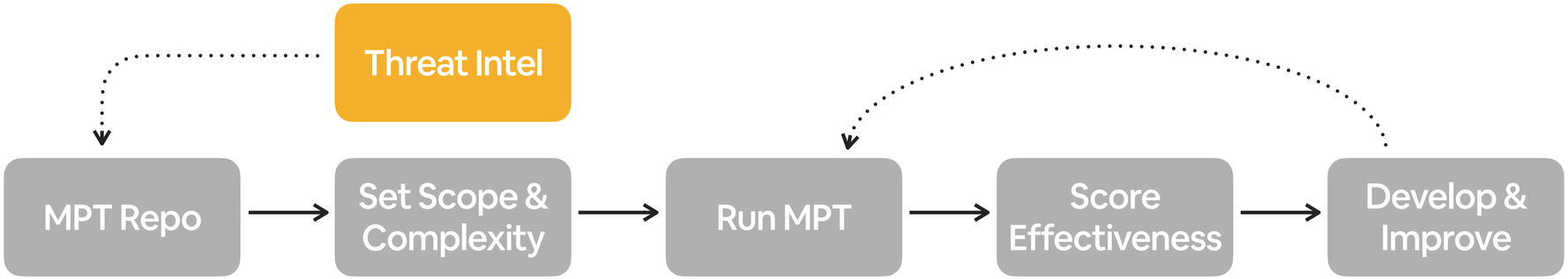
Narratives

Roadmap

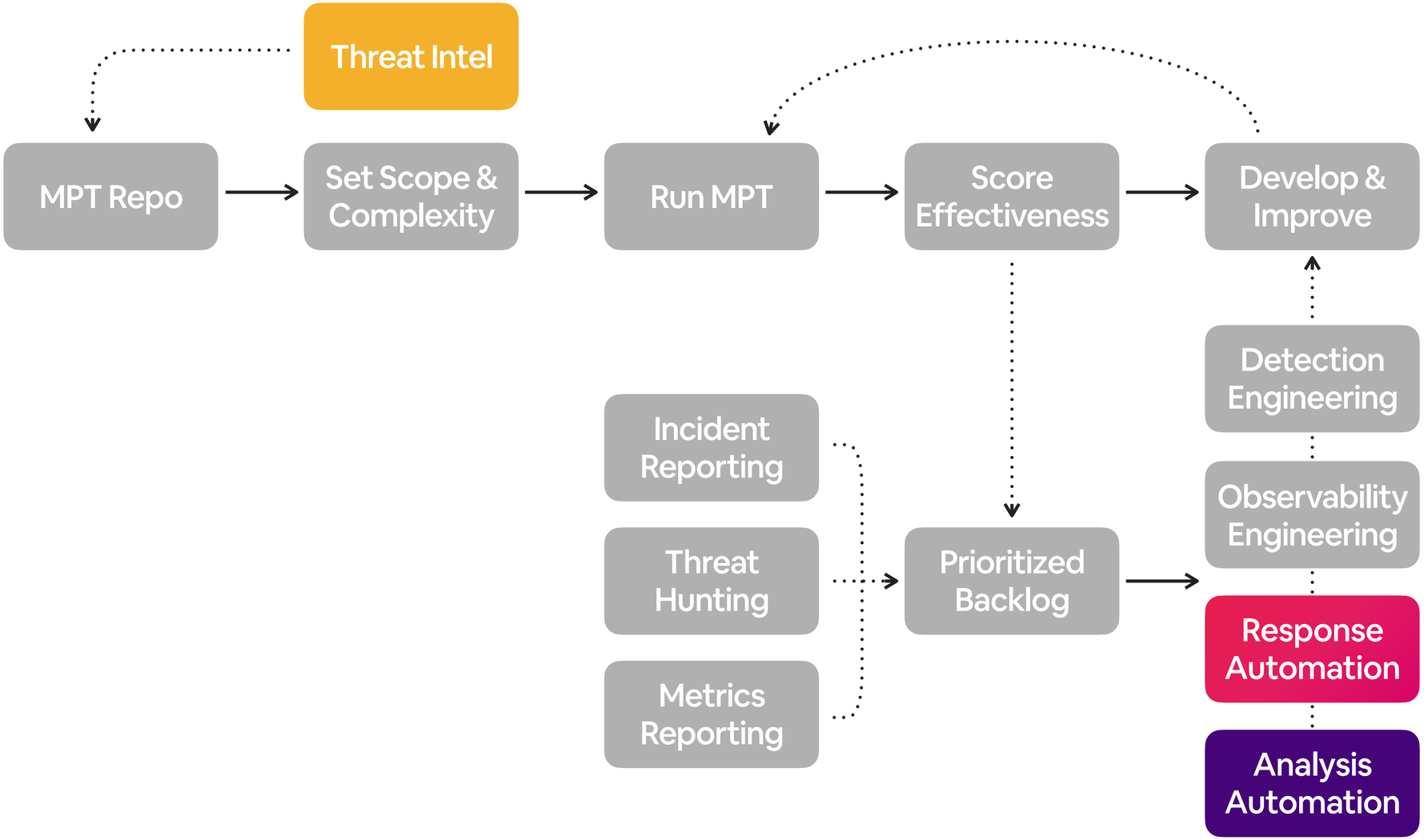
What are our priorities?

What is our roadmap to close the gaps?

Micro-Purple Testing and Continuous Improvement



Micro-Purple Testing and Continuous Improvement



Build a Modern Detection & Response Program

Before		After
Hiring based on number of detection alerts	→	Data driven resource requests
Threat hunting because it "sounded cool"	→	Processes defined, measured, and proving value
Buying based on "Gartner says you need it"	→	Vision and architecture guides your investments
Telling leadership "yeah we might detect it"	→	Metrics for coverage and performance

meoward.co

allyn.stott@airbnb.com