Threat Hunting Process

Security Defense Center at ING

User Experiences

- MITRE ATT&CK Workshop
- May 2020

Quick intro

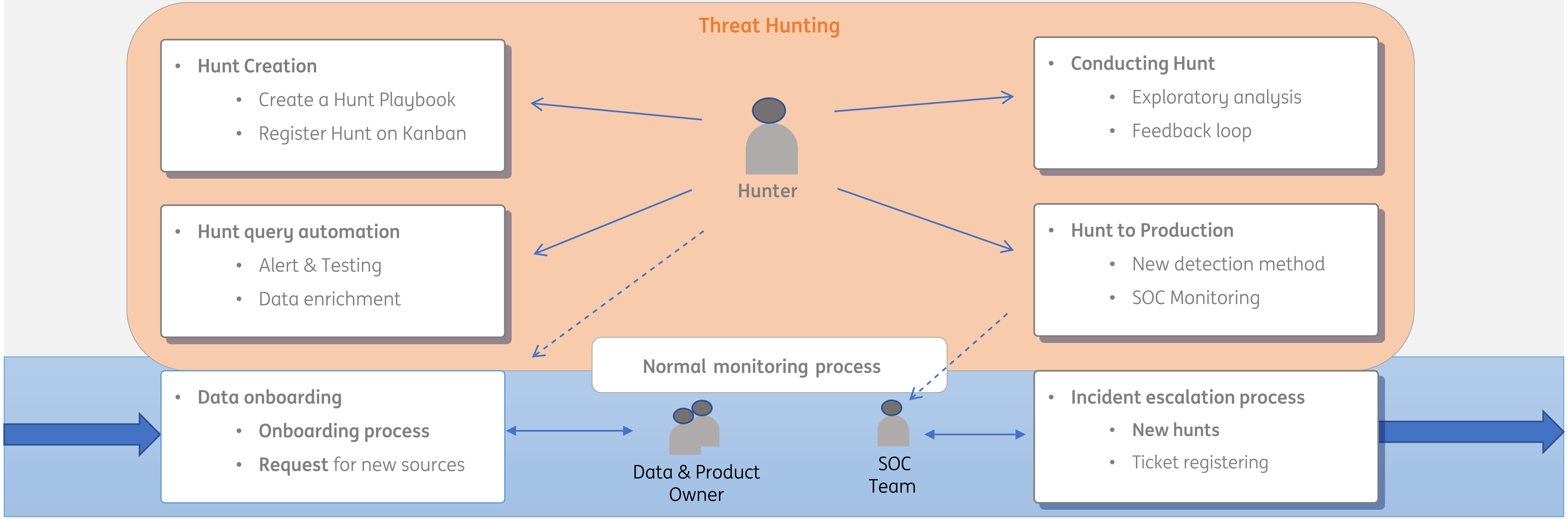
Renato Fontana

- From .br
- 1st time speaking
- Threat Hunting Lead at ING SDC (~2 years)

Twitter: @rcfontana

Threat Hunting Process

- Hunts are investigative efforts that yield high fidelity insights
- Aim to detect what conventional monitoring appliances won't capture



Threat Hunting

- **Hunt Creation**
  - Create a Hunt Playbook
  - Register Hunt on Kanban

- **Conducting Hunt**
  - Exploratory analysis
  - Feedback loop

Hunter

- **Hunt query automation**
  - Alert & Testing
  - Data enrichment

- **Hunt to Production**
  - New detection method
  - SOC Monitoring

Normal monitoring process

- **Data onboarding**
  - **Onboarding process**
  - **Request** for new sources

Data & Product Owner

SOC Team

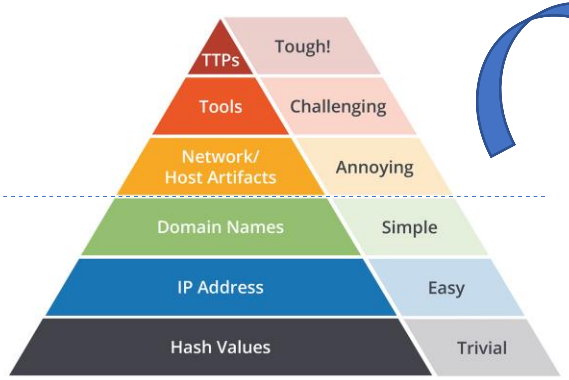
- **Incident escalation process**
  - **New hunts**
  - Ticket registering

Threat Hunting Core

Hunting scope

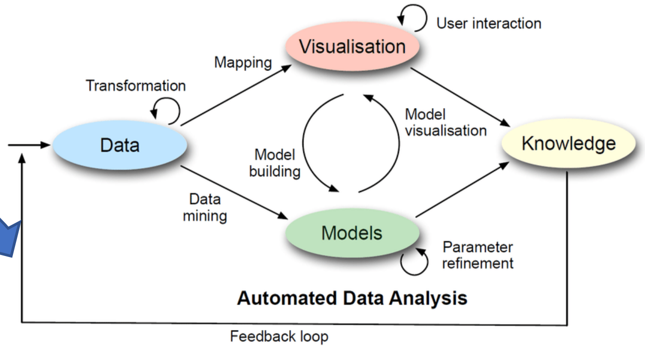
Methodology

- Iterative approach
- Pursuit of attacks
- Proactively search
- Various hunting techniques



Source: David J. Bianco, personal blog

Effort



- Continuous feedback loop
- Quality Assurance
- **Tracking Hunt development**

Scope and Prioritization

ATT&CK™

Adversarial Tactics, Techniques & Common Knowledge

- Data Source coverage
- Techniques visibility
- Detection capability
- Global mapping

DeTT&CT

- **Intelligence Input & Overview**

Investigation telemetry

Supporting Operations

- Networking Appliances
- Signature based detection
- SOC Monitoring
- IOC Matching

- Threat Hunting Process
- High Fidelity Notifications
- Hunting Backlog
- Ticket tracking

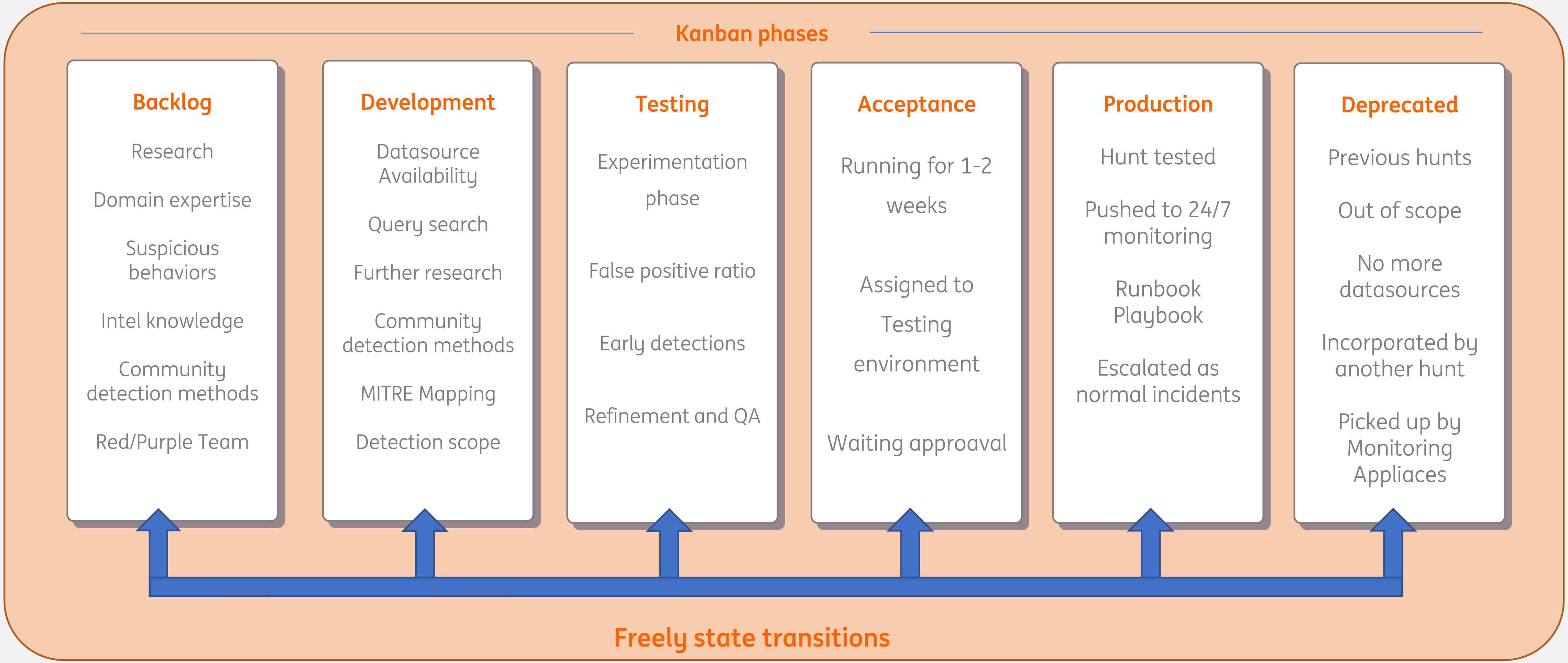
- Threat Intelligence Platform
- Threat Actors Profiles
- Intel sharing
- External notifications

Standard Monitoring | **Hunting** | **Intelligence**

Source: Renato Fontana

Hunt development

- ! Hunting capabilities are highly depended on existing data sources
- ! Querying environment and specific tool set for exploratory analysis



Kanban phases

Backlog

- Research
- Domain expertise
- Suspicious behaviors
- Intel knowledge
- Community detection methods
- Red/Purple Team

Development

- Datasource Availability
- Query search
- Further research
- Community detection methods
- MITRE Mapping
- Detection scope

Testing

- Experimentation phase
- False positive ratio
- Early detections
- Refinement and QA

Acceptance

- Running for 1-2 weeks
- Assigned to Testing environment
- Waiting approaval

Production

- Hunt tested
- Pushed to 24/7 monitoring
- Runbook Playbook
- Escalated as normal incidents

Deprecated

- Previous hunts
- Out of scope
- No more datasources
- Incorporated by another hunt
- Picked up by Monitoring Appliaces

Freely state transitions

Thank you!

Twitter @rcfontana

- MITRE ATT&CK Workshop
- May 2020