King Mongkut's University of Technology North Bangkok

Ripple Down Models

- A Knowledge Acquisition Approach to Detect Network Traffic Anomalies

Akara Prayote, PhD.

Dept. of Computer and Information Science,

Faculty of Applied Science

Contents

1 Background

2 Ripple Down Models

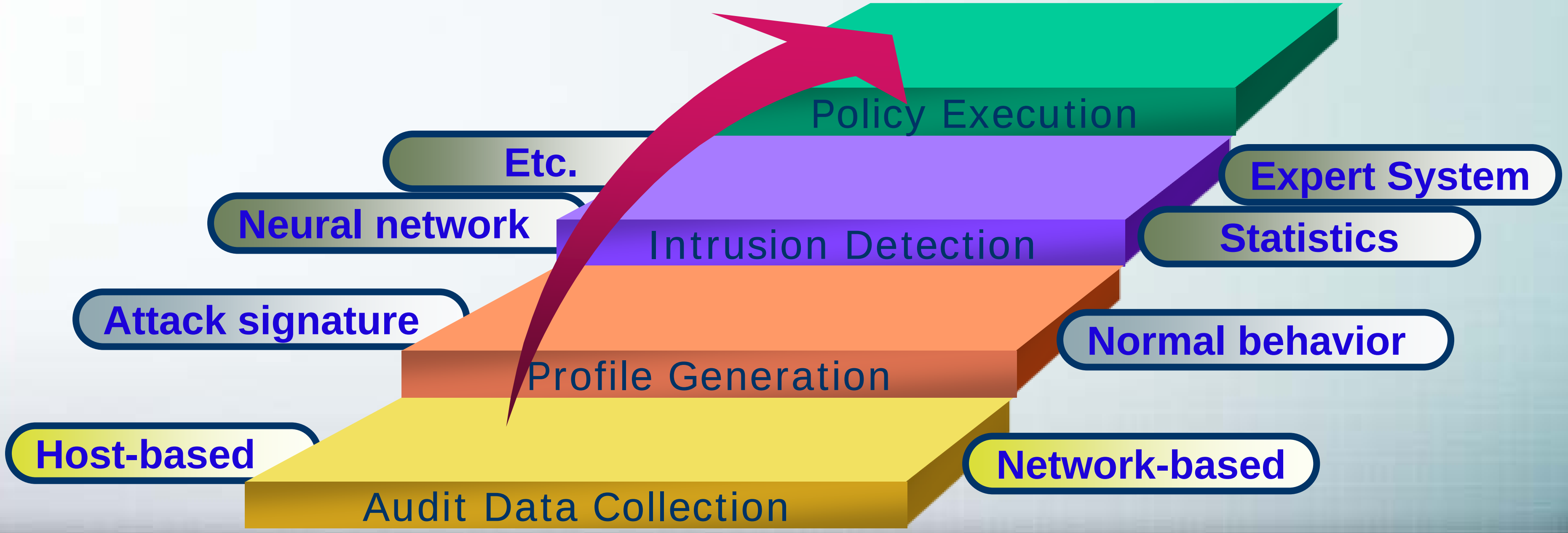
3 System Architecture

4 Experiments and Results

5 Future Plan

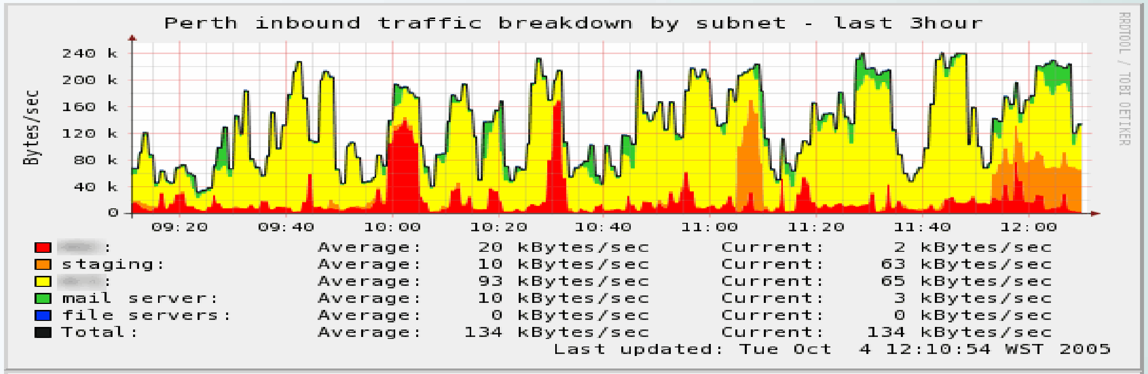
Background

- There are a lot of attempts to gain access to networks illegitimately.
- Network intrusion detection systems are widely used and studied.

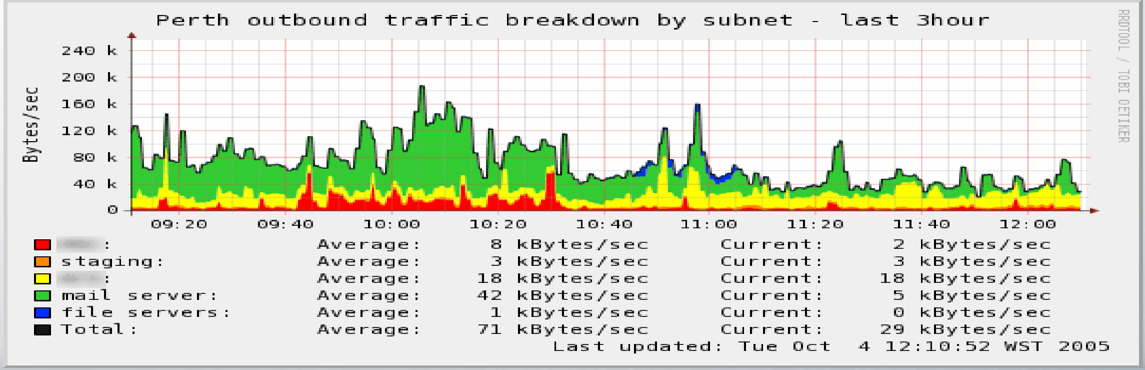


Investigating Network Measurement

- ❖ Can effectively reveal traces of intrusive behavior (Barford and Plonka, 2001; Lakhina, Crovella, and Diot, 2004)



```
🟥 [redacted]:       Average:    20 kBytes/sec      Current:     2 kBytes/sec
🟧 staging:          Average:    10 kBytes/sec      Current:    63 kBytes/sec
🟨 [redacted]:       Average:    93 kBytes/sec      Current:    65 kBytes/sec
🟩 mail server:      Average:    10 kBytes/sec      Current:     3 kBytes/sec
🟦 file servers:     Average:     0 kBytes/sec      Current:     0 kBytes/sec
⬛ Total:            Average:   134 kBytes/sec      Current:   134 kBytes/sec
                                   Last updated: Tue Oct  4 12:10:54 WST 2005
```



```
🟥 [redacted]:       Average:     8 kBytes/sec      Current:     2 kBytes/sec
🟧 staging:          Average:     3 kBytes/sec      Current:     3 kBytes/sec
🟨 [redacted]:       Average:    18 kBytes/sec      Current:    18 kBytes/sec
🟩 mail server:      Average:    42 kBytes/sec      Current:     5 kBytes/sec
🟦 file servers:     Average:     1 kBytes/sec      Current:     0 kBytes/sec
⬛ Total:            Average:    71 kBytes/sec      Current:    29 kBytes/sec
                                   Last updated: Tue Oct  4 12:10:52 WST 2005
```

Intrusion Detection on Traffic Volume

- Brutlag (2000) - Holt-Winters algorithm
- Barford et al. (2002) – wavelet filters
- Krishnamurthy et al. (2003) – Sketch
- Lakhina, Crovella, and Diot (2004) - Principal Component Analysis
- Mandjes, Saniee, and Stolyar(2005) - simple statistical measurements, e.g., mean, variance.
- Etc.

Issues

- A universal or generic model
  - Complexity
  - Training
- New events
  - Reconstruct models?
- Ad-hoc events
- Ultimately, human experts are needed

Aims

- **Gradually learns system behavior from human experts (network admin)**
  - Regular events
  - Ad-hoc events
- **Detects anomalies**

Ripple Down Models

- **Incremental knowledge acquisition**
  - Any new and benign event can be added
- **Anomaly detection algorithm**
  - Robust for small amount of data
  - Adaptive

RDM- Incremental KA

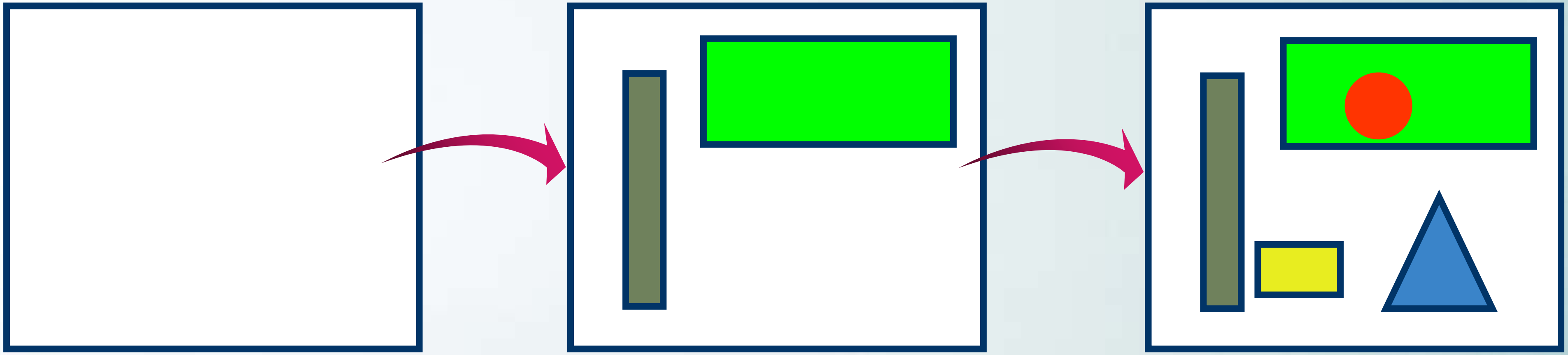
- Ripple Down Rules (Compton, 1988)
- Knowledge is a justification in a context and can be reused within the same context
- Knowledge and context is captured into rules
- Structured organization without Expert or KE

RDR Application

- Classification
- Resource allocation
- Heuristic search
- Configuration
- Image processing
- Etc.

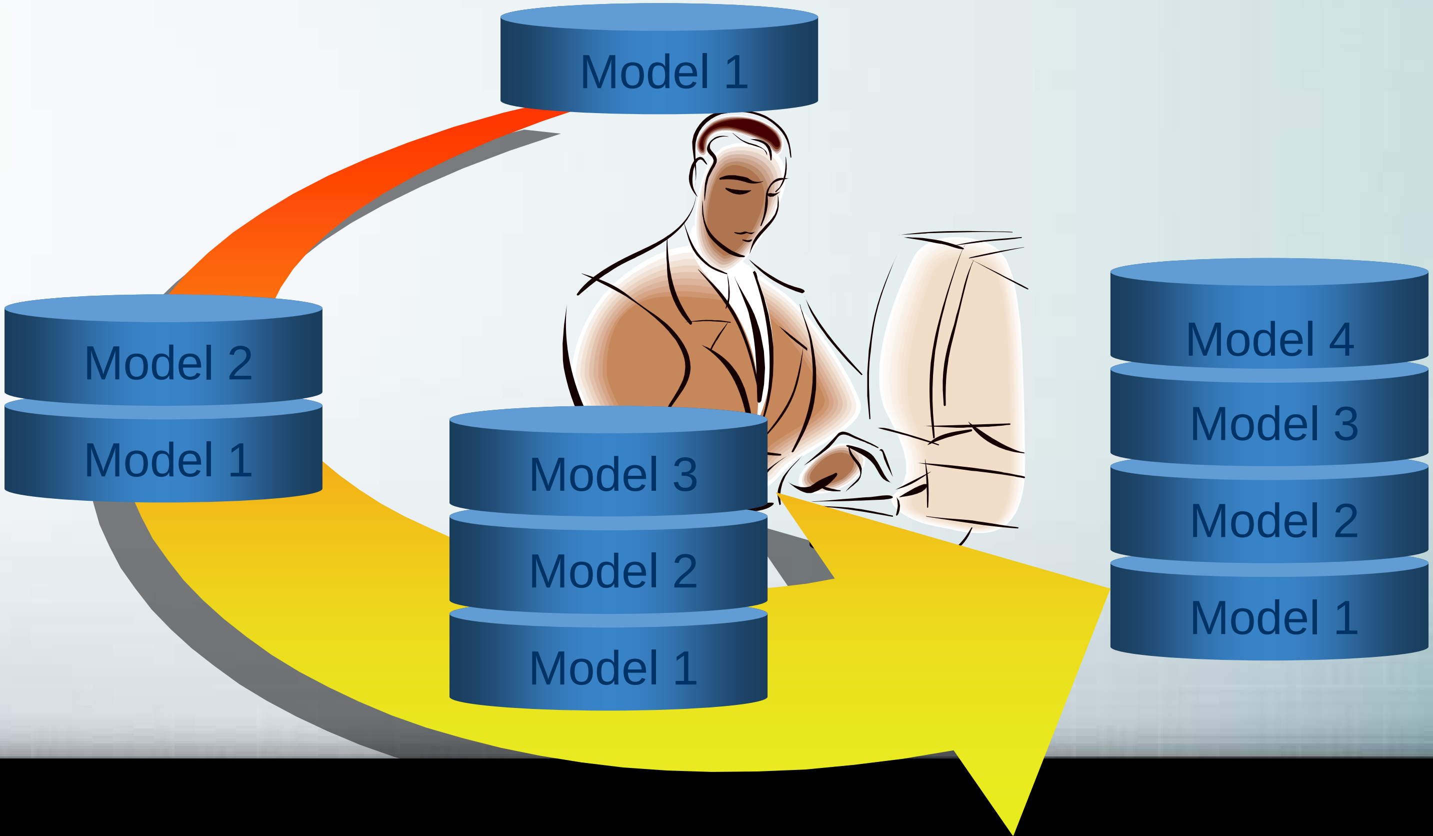
RDR and Partitioning

- RDR can naturally partition a search space into smaller well-defined regions



Incremental Models

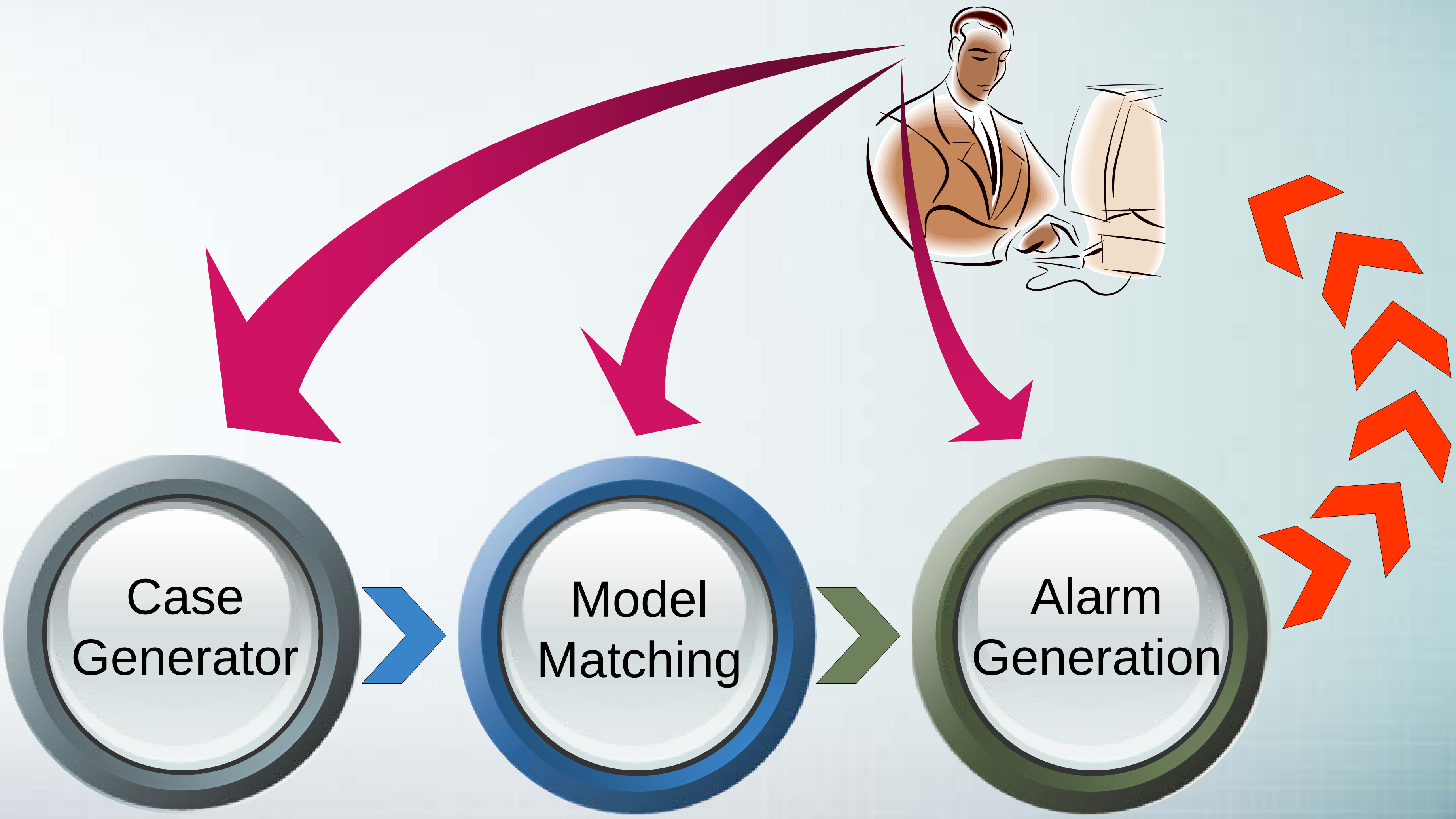
- No single general model
- Models for particular situations
- A model can be created when a new event is discovered



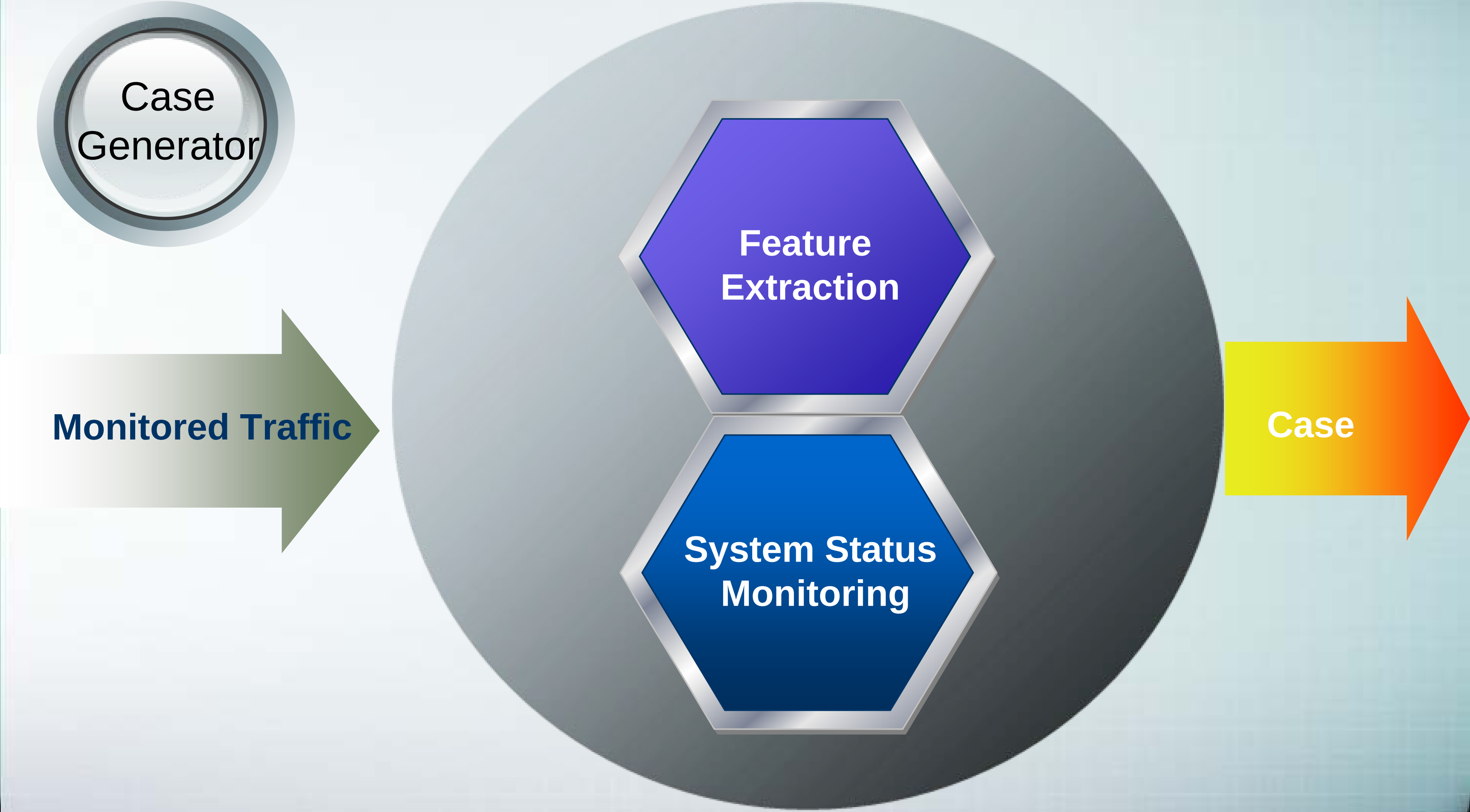
RDM – Anomaly Detection Algorithm

- **No training!**
  - A model is created for an event and being used immediately
- **Detecting outliers while learning**
  - Probability that a new value is outlier based on seen data
- **Statistical measurement**
  - Mean, median, min-values, max-values, standard deviation, etc.

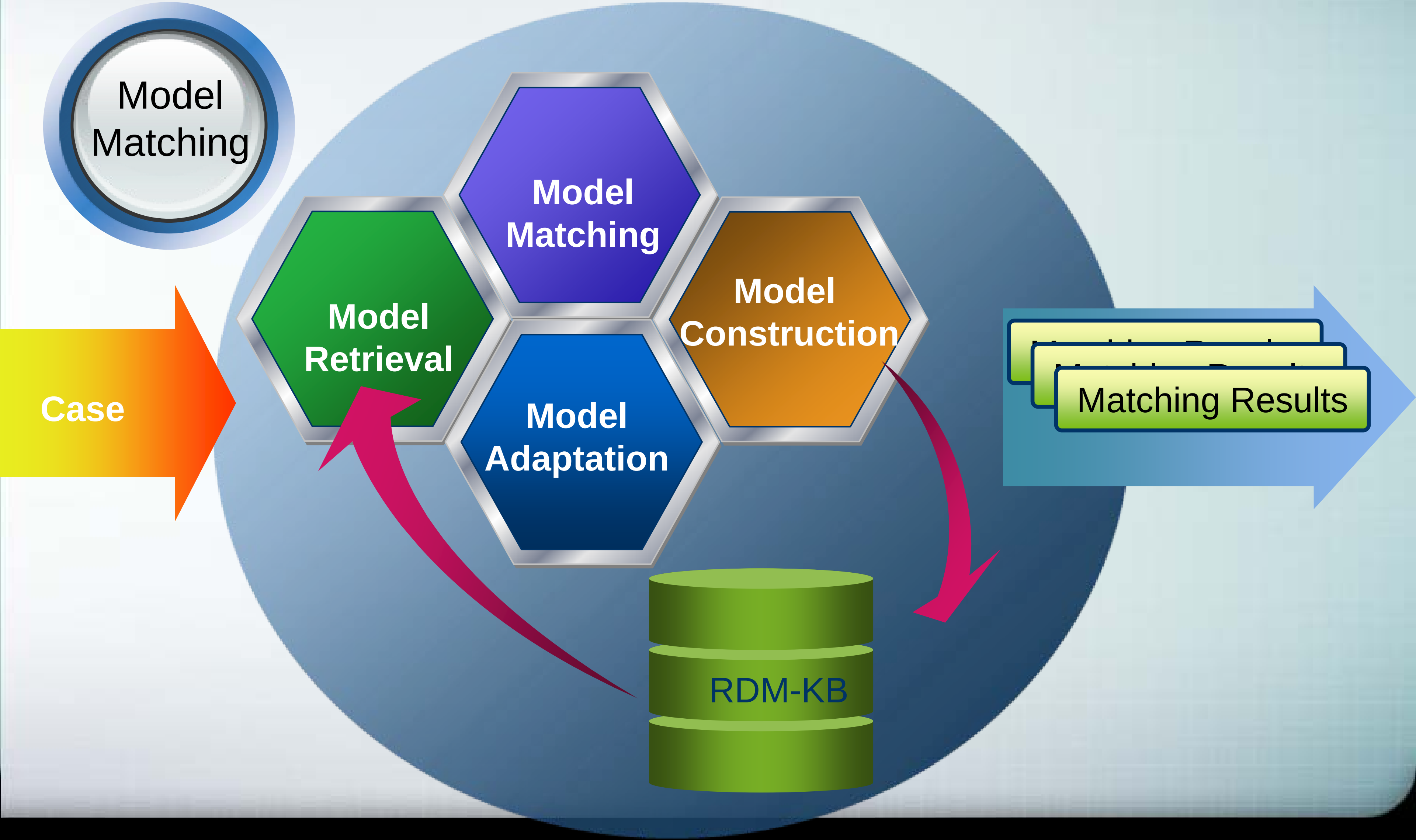
System Architecture



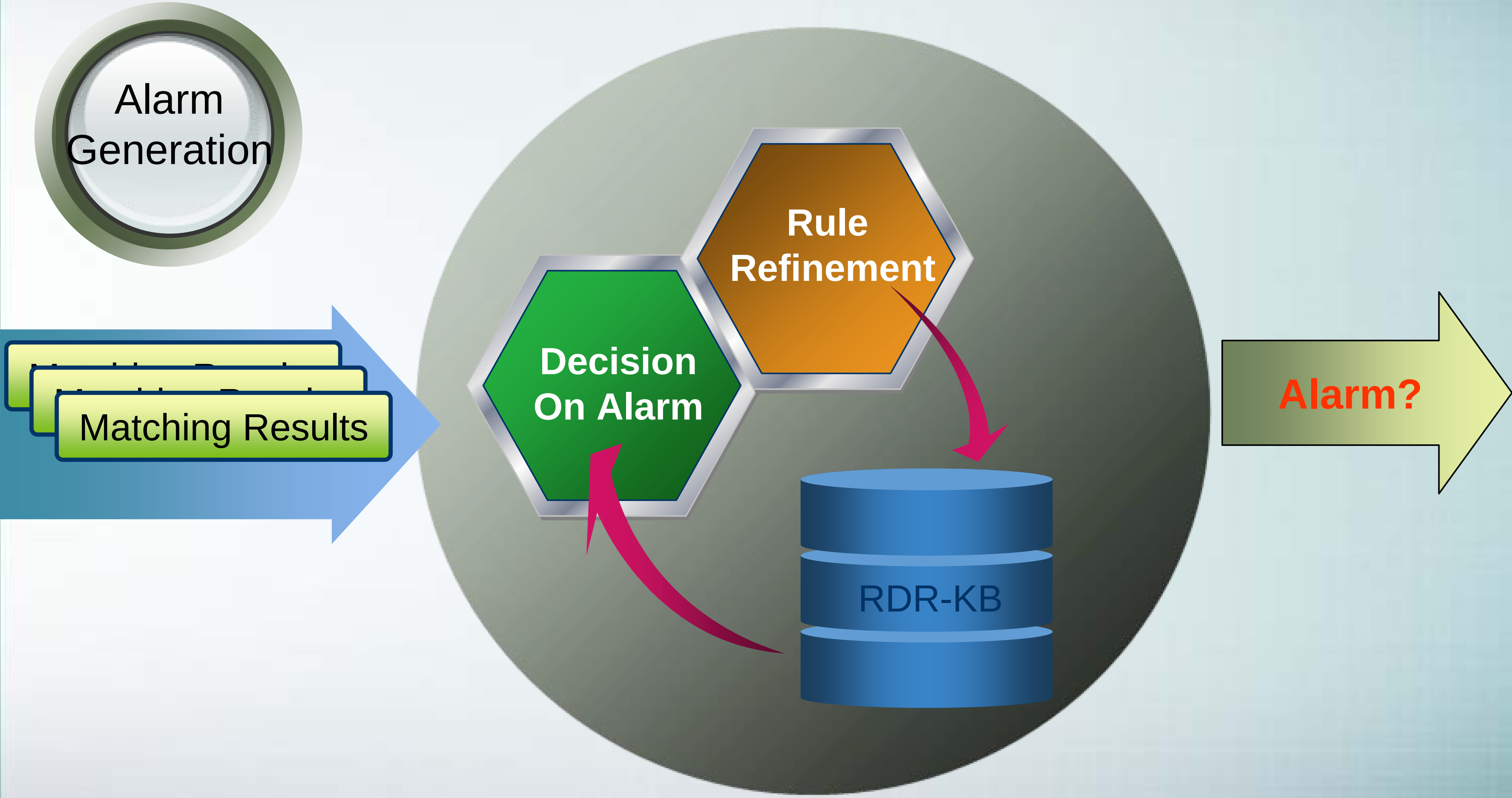
System Architecture



System Architecture



System Architecture



Alarm Generation

Matching Results

Decision On Alarm

Rule Refinement

RDR-KB

Alarm?

Experimental Results

- **8064 cases**
  - 26 sessions for new models
  - 16 sessions for warning policy
  - 103 sessions for fps.
- **Consultation ≈ 5 times a day**
- **Better than HW**

Future Plan

- Interim outlier detection algorithm
- Combining multiple tests
- Redundancy of partitions
- Correlation between models

Thank You !

- Sa-Wad-Dee Krab