How to Tune Automation to Avoid False Positives

Gita Ziabari
Senior Consultant IIII
PS Advisory Services at Verizon

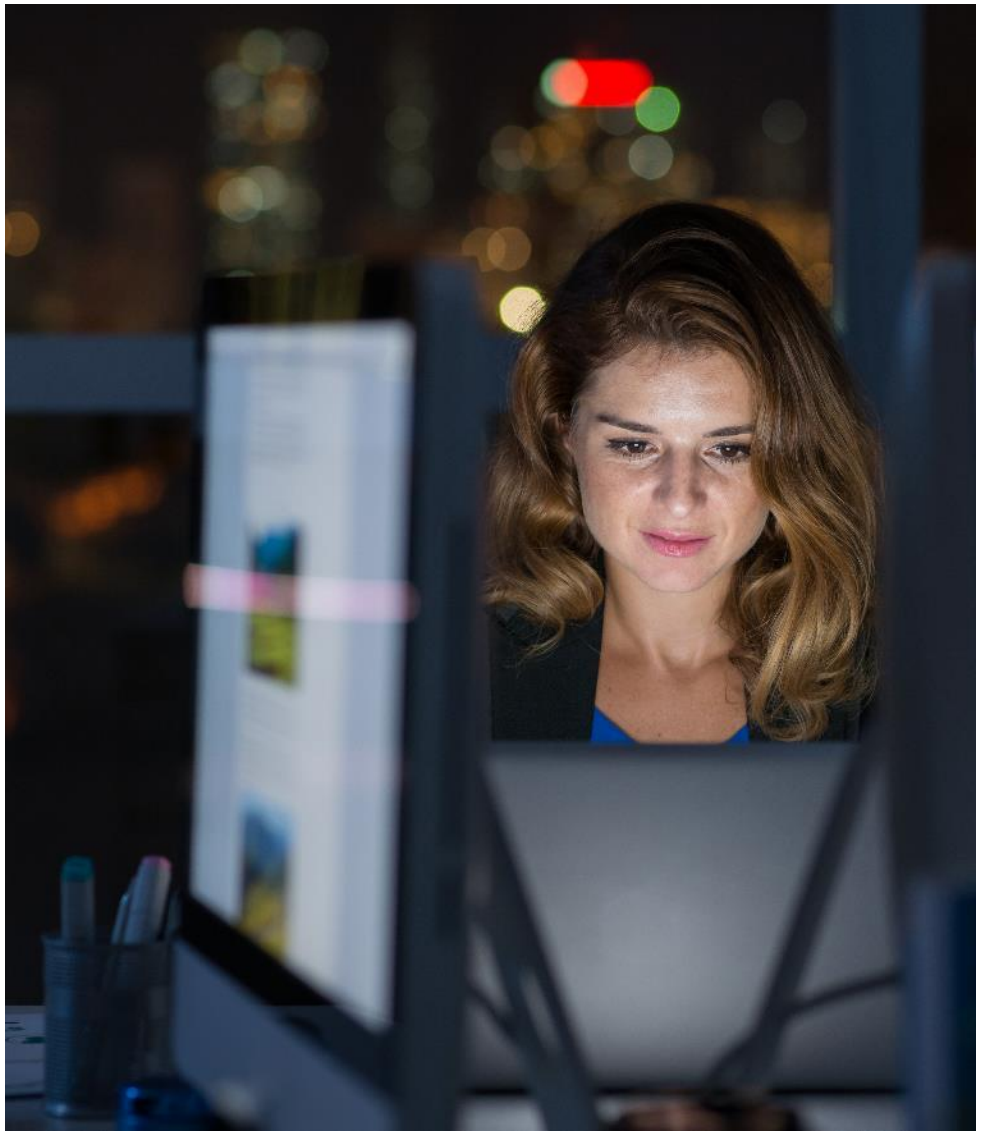
Wall of Sheep

DEF CON 26

Proprietary statement.

Agenda

- Techniques to design a reliable automated tool
- Threat intelligence feeds
- How to generate high quality feeds



verizon

Techniques to design a reliable automated tool.

verizon

Define reason for automation.

- Accelerated response times
- Consistency
- Scalability
- Efficiency
- Risk reduction
- Simplified IR process
- Empowering users

verizon

What to automate.

- Bad ideas lead to false positives
- Automation needs to be done with intelligence

verizon

Simplicity and intelligence.

- Design the framework simply
- See it in five years
- Make it user-friendly
- Document the designed framework
- Think about those inheriting the framework

Integration into existing systems.

- Small and simple platform
- Minimum dependency on other servers
- Independent of other frameworks with possibility of integrations

verizon

Planning the automation.

- CLI or GUI?
- Who will use the tool and what do they need
- Avoid writing platforms in different languages

verizon

Broken chain!

- Chain of dependent processes
- Too many servers to connect
- Nagios

verizon

Be your own QA!

Compare expected results and obtained results
for following testing phases:

- Unit testing
- Feature testing
- Performance testing

Threat intelligence feeds.

verizon

What is cyber threat intelligence?

- Indicator-based threat intelligence feeds
- Domains, URLs, IP addresses and hashes

verizon

Threat Intelligence Feeds.

Third party feeds:

- Open sources
- Community
- Commercial
- Government

Internal feeds:

- Malware Analyst
- Automated data mining tools

Main issues.

- Poor quality control
- Overlapped indicators
- False positives
- Noise

verizon

Generating High Quality Feeds.

verizon

Databases.

Consider using a database for storing and mining data.

verizon

Handling false positives.

- De-duplicating
- Whitelisting
- Filtering
- Scoring
- Aging

verizon

De-duplicating.

- De-duplicate IOCs prior saving them in database.

verizon

Whitelisting.

- Third party open sources
- Whitelisting internally

verizon

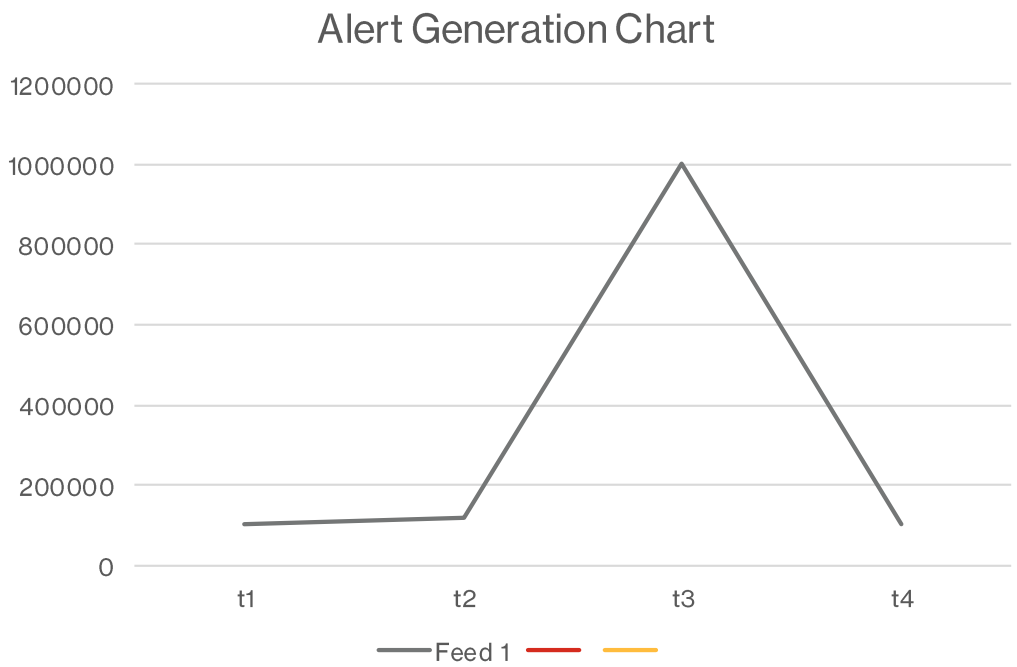
Third-party sources.

- External whitelisting sources
- Top 1000 is the most reliable IOCs
- As quantity increases, possibility of false positives increases

verizon

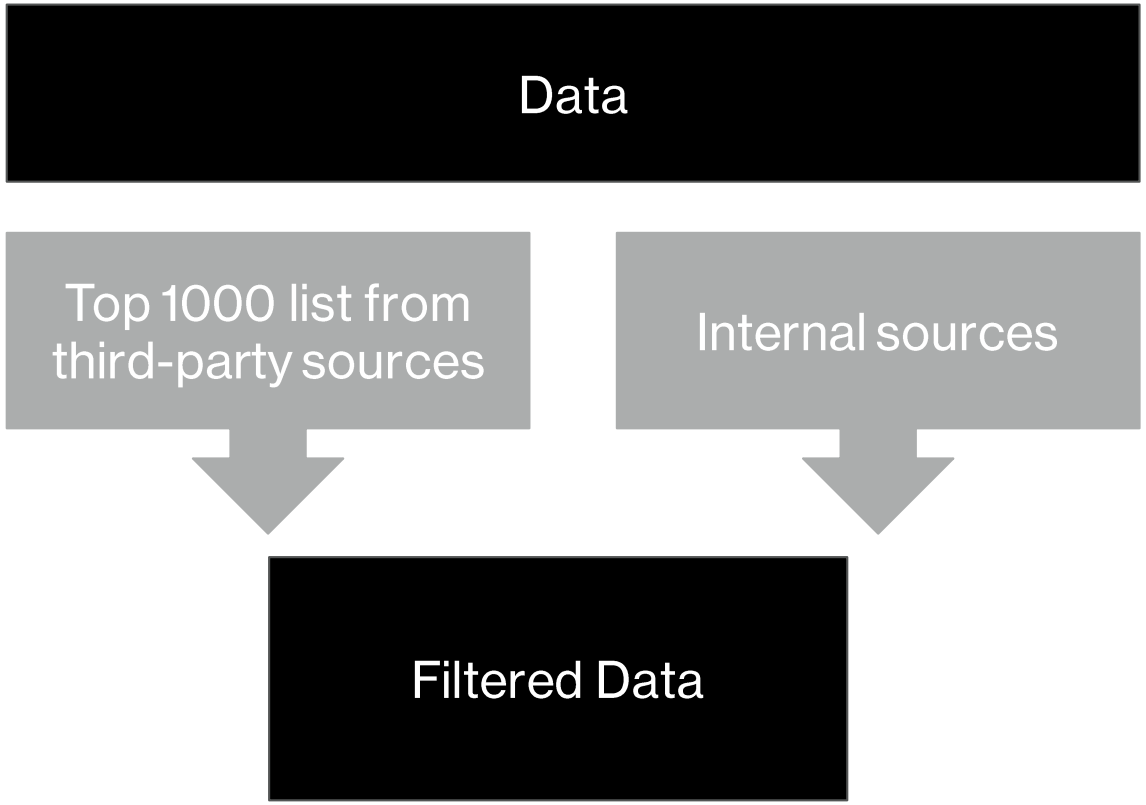
Internal whitelisting.

- Manual whitelisting based on false positives
- One bad indicator results in many hits (100k+)



verizon

Whitelisting.

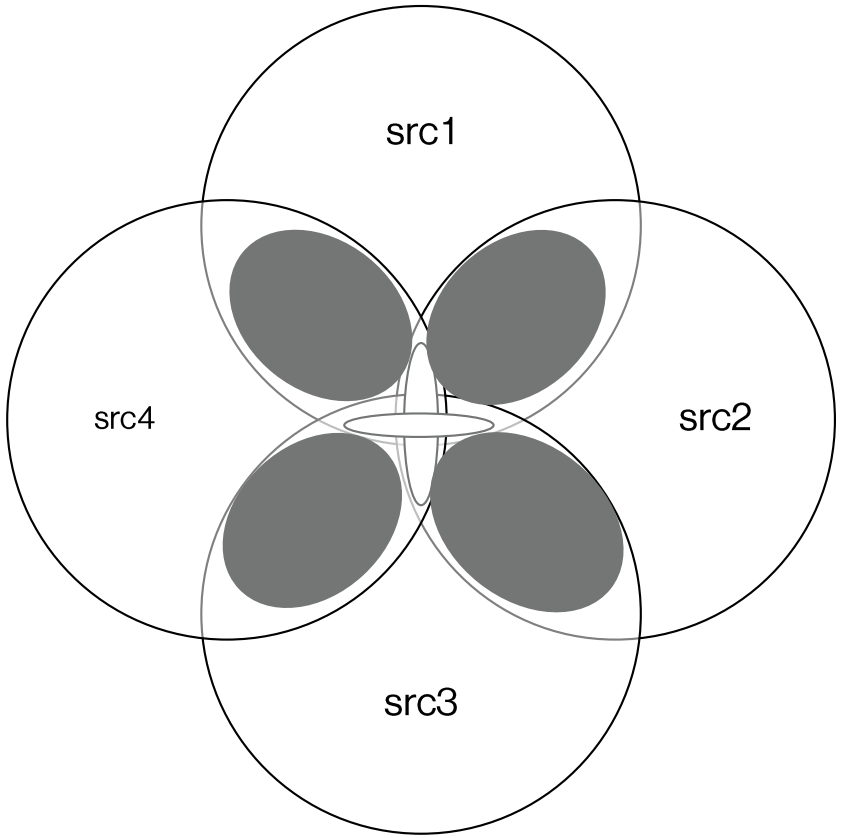


verizon

Scoring.

verizon

Scoring indicators.

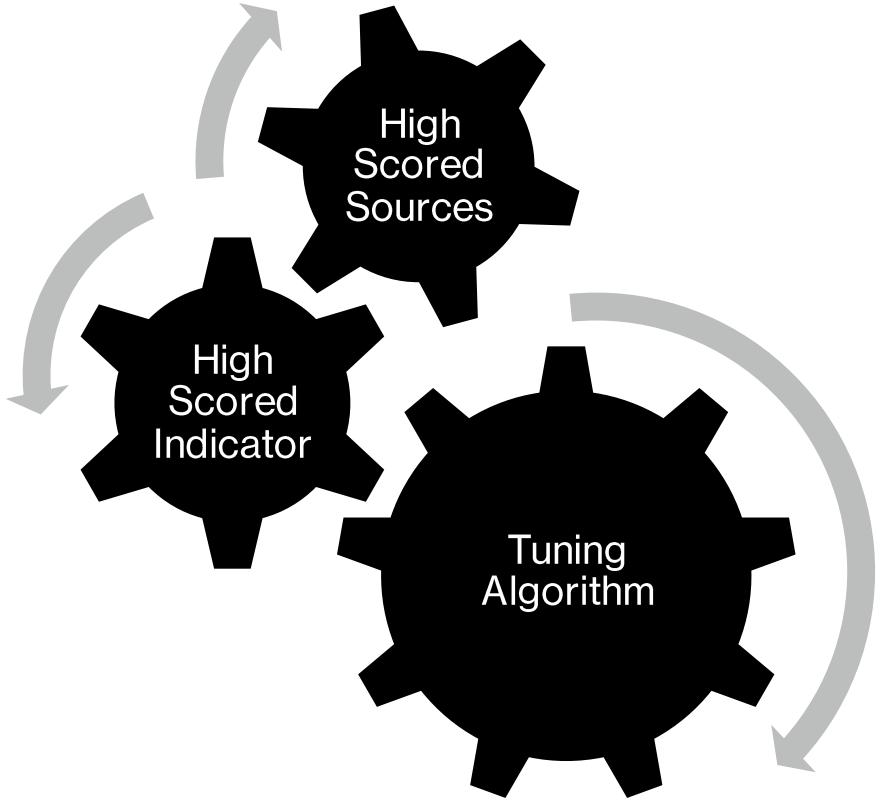


Score sources.

- Test your feeds over network
- Get the list of detected false positives and whitelist them
- Determine sources generating more false positive indicators and lower their score

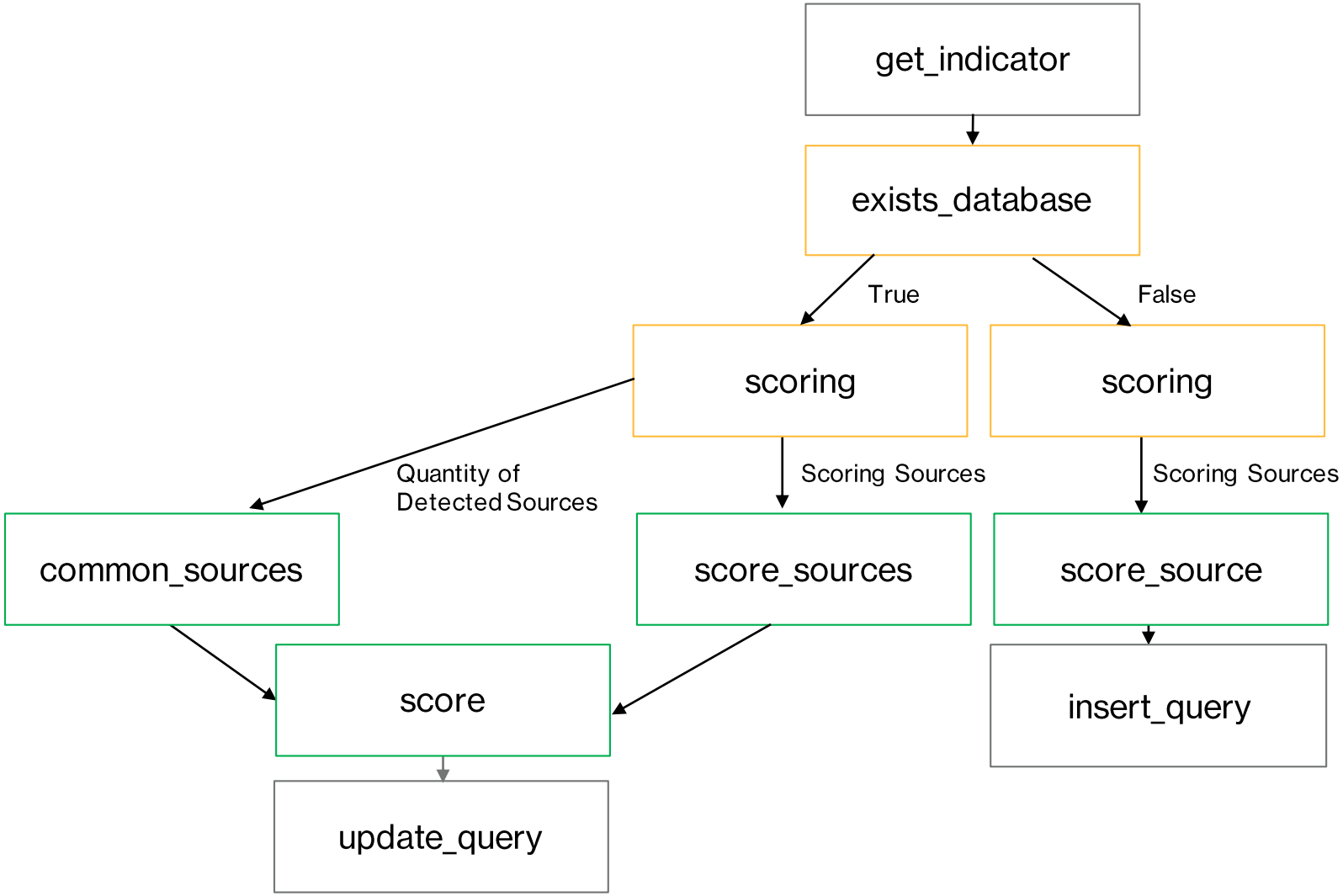
verizon

Scoring indicators.



verizon

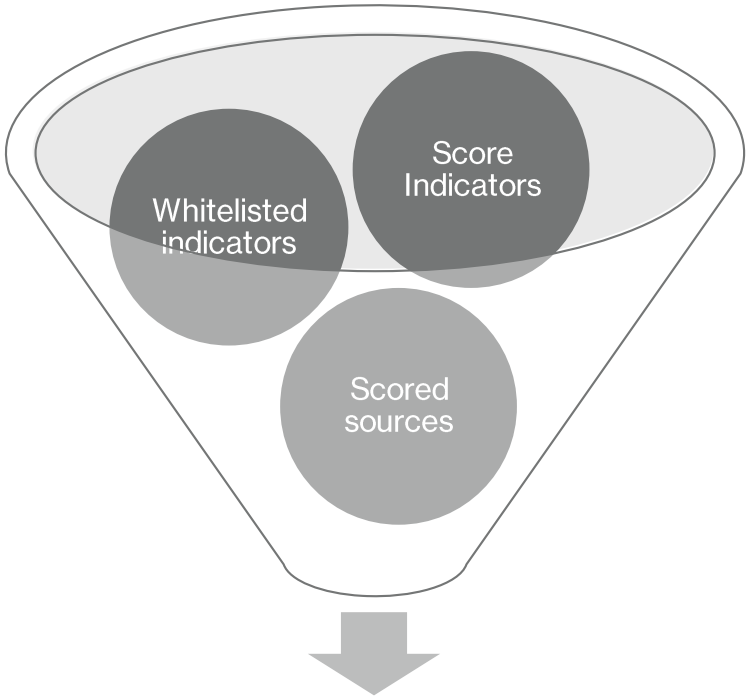
Scoring algorithm.



Filtering.

verizon

Filter highly-scored indicators.



verizon

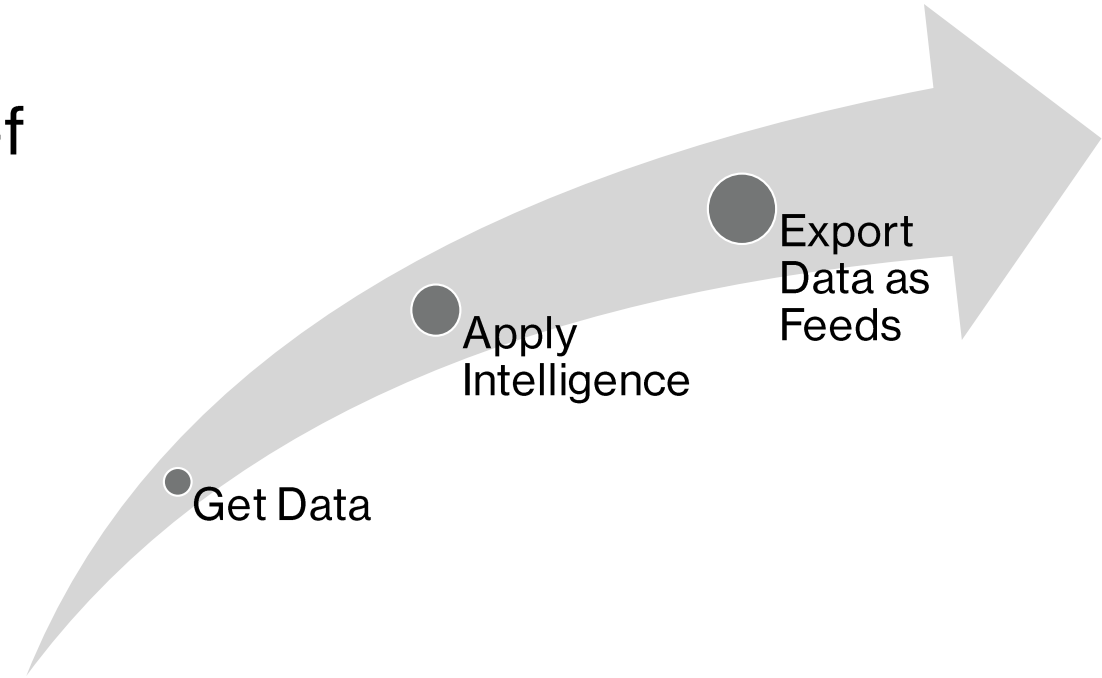
Building up queries.

- Be specific
- More indicators faster results
- Critical attributes
  - Indicator
  - Indictor type: (Hash, URL, Domain, IP)
  - Unique index based on sources
  - List of sources
  - Score
  - Date of insertion
  - Malware type

verizon

Update feeds frequently.

Make importing and exporting of data from database as feeds frequent.

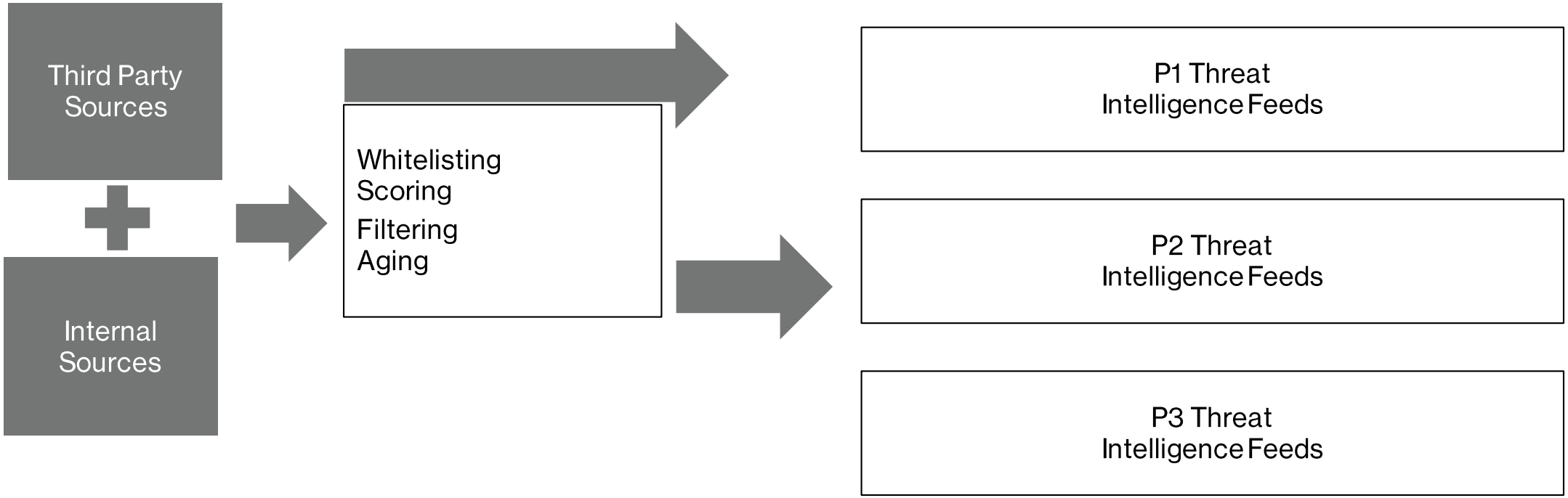


Be selective!

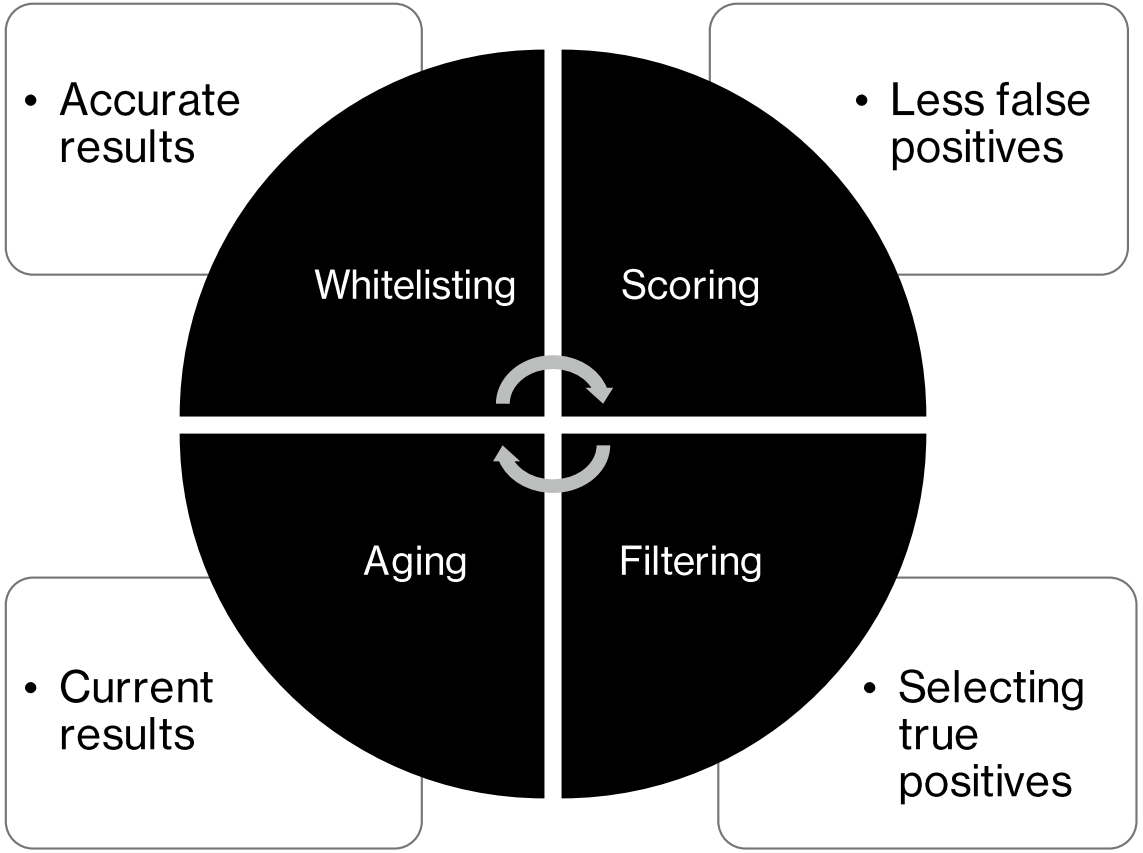
- Score of indicator
- Type of indicator
- Sources of indicator
- Malware type

Aging.

Threat Intelligence Feed with low false positives.



Less false positives!



verizon

Questions?

Thank you.

Gita Ziabari

Senior Consultant III
PS Advisory Services at Verizon

@gitaziabari
gita.ziabari@verizon.com

For more information on:

- Verizon Threat Intelligence Platform Service (VTIPS)
- Verizon Threat Research Advisory Center (VTRAC)
- Global Security Services

VTRAC-Intel@Verizon.com

verizon