How to Tune Automation to Avoid False Positives

Gita Ziaabari
Senior Consultant III
PS Advisory Services at Verizon

Wall of Sheep
DEF CON 26
Proprietary statement.

This document and any attached materials are the sole property of Verizon and are not to be used by you other than to evaluate Verizon's service.

This document and any attached materials are not to be disseminated, distributed or otherwise conveyed throughout your organization to employees without a need for this information or to any third parties without the express written permission of Verizon.

© 2017 Verizon. All rights reserved. The Verizon name and logo and all other names, logos and slogans identifying Verizon’s products and services are trademarks and service marks or registered trademarks and service marks of Verizon Trademark Services LLC or its affiliates in the United States and/or other countries.

All other trademarks and service marks are the property of their respective owners.
Agenda

• Techniques to design a reliable automated tool
• Threat intelligence feeds
• How to generate high quality feeds
Techniques to design a reliable automated tool.
Define reason for automation.

- Accelerated response times
- Consistency
- Scalability
- Efficiency
- Risk reduction
- Simplified IR process
- Empowering users
What to automate.

- Bad ideas lead to false positives
- Automation needs to be done with intelligence
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
Planning the automation.

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

- Chain of dependent processes
- Too many servers to connect
- Nagios
Be your own QA!

Compare expected results and obtained results for following testing phases:

- Unit testing
- Feature testing
- Performance testing
Threat intelligence feeds.
What is cyber threat intelligence?

- Indicator-based threat intelligence feeds
- Domains, URLs, IP addresses and hashes
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
Generating High Quality Feeds.
Databases.

Consider using a database for storing and mining data.
Handling false positives.

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

- De-duplicate IOCs prior saving them in database.
Whitelisting.

- Third party open sources
- Whitelisting internally
Third-party sources.

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

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

Data

Top 1000 list from third-party sources

Internal sources

Filtered Data
Scoring.
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
Scoring indicators.
Scoring algorithm.

1. **get_indicator**
   - **exists_database**
     - **True**
       - **scoring**
         - **common_sources**
           - **score**
             - **update_query**
           - **Quantity of Detected Sources**
2. **exists_database**
   - **False**
     - **scoring**
       - **score_sources**
         - **insert_query**
       - **Scoring Sources**
         - **scoring**
           - **score_source**
             - **Scoring Sources**
Filtering.
Filter highly-scored indicators.
Building up queries.

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

- Accurate results
- Less false positives
- Current results
- Selecting true positives
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