Cisco live!

# Introduction to Snort Rule Writing

TALOS

# Snort Rule Syntax

```
# rule header
alert tcp any any -> 192.168.1.0/24 111 (
```

- rule action
- protocol
- src address
- src port
- dst address
- dst port

# Snort Rule Syntax

```
# rule option format
alert tcp any any -> 192.168.1.0/24 111 (
    msg:"Rule Message"; \
```

rule option argument

rule option

# rule option: content

```
# content match example
alert tcp any any -> 192.168.1.0/24 111 (
    content:"ABCD"; \
    # is equivalent to:
    content:"|41 42 43 44|"; \
```

The content match finds a static pattern in network data.

# content modifiers: nocase

```
# content match modifiers: nocase
alert tcp any any -> 192.168.1.0/24 111 (
    # match "ABCD" or "abcd" etc.
    content:"ABCD"; nocase;
```

nocase makes a content match case insensitive.
content matches are case sensitive by default.

# content modifiers: offset

```
# content match modifiers: offset
alert tcp any any -> 192.168.1.0/24 111 (
    # skip 2 bytes before searching for "ABCD"
    content:"ABCD"; offset:2;
```

offset requires the match to occur after the designated offset in network data.

# content modifiers: depth

```
# content match modifiers: depth
alert tcp any any -> 192.168.1.0/24 111 (
    # match "ABCD" within the first 4 bytes of the payload
    content:"ABCD"; depth:4;
```

depth restricts how far Snort should search for the specified pattern.

# content modifiers: distance

```
# content match modifiers: distance
alert tcp any any -> 192.168.1.0/24 111 (
    # find "DEF" 1 byte after "ABC"
    content:"ABC"; content:"DEF"; distance:1;
```

distance specifies how far into a payload Snort should ignore before starting to search for the specified pattern relative to the end of the previous pattern match.

# content modifiers: within

```
# content match modifiers: within
alert tcp any any -> 192.168.1.0/24 111 (
    # find "EFG" within 10 bytes of "ABC"
    content:"ABC"; content:"EFG"; within:10;
```

within makes sure that at most N bytes are between pattern matches.

# negated content match

```
# negated content match
alert tcp any any -> 192.168.1.0/24 111 (
    # make sure "EFG" is NOT within 10 bytes of "ABC"
    content:"ABC"; content:!"EFG"; within:10;
```

content matches can be negated.

# content buffers

```
# content buffer example
alert tcp any any -> 192.168.1.0/24 111 (
    # match "ABC" within the HTTP URI
    content:"ABC"; http_uri;
```

content matches can be restricted to a payload location, such as the HTTP URI.

# content buffers

```
POST /index.php HTTP/1.1
Host: example.com
Content-Length: 28
Content-Type: application/x-www-form-urlencoded
Cookie: this_is_a_cookie=this_is_its_value

firstparam=one&secondparam=two

Buffers: http_method http_uri http_header http_cookie
http_client_body
```

# content modifiers: fast_pattern

```
# fast_pattern example
alert tcp any any -> 192.168.1.0/24 111 (
    # set "ABC" as the rule fast_pattern
    content:"ABC"; fast_pattern;
```

fast_pattern explicitly specifies the content match within a rule to be used with the fast pattern matcher. The fast_pattern serves as the “entrance” condition for rule evaluation.

# content modifiers: fast_pattern

```
# fast_pattern:only; example
alert tcp any any -> 192.168.1.0/24 111 (
    # set "ABC" as the rule fast_pattern
    content:"ABC"; fast_pattern:only;
```

fast_pattern:only; selects the content match to be used in the fast pattern matcher for the rule and also specifies that this match will not be evaluated again when the rule “enters”.

# rule option: pcre

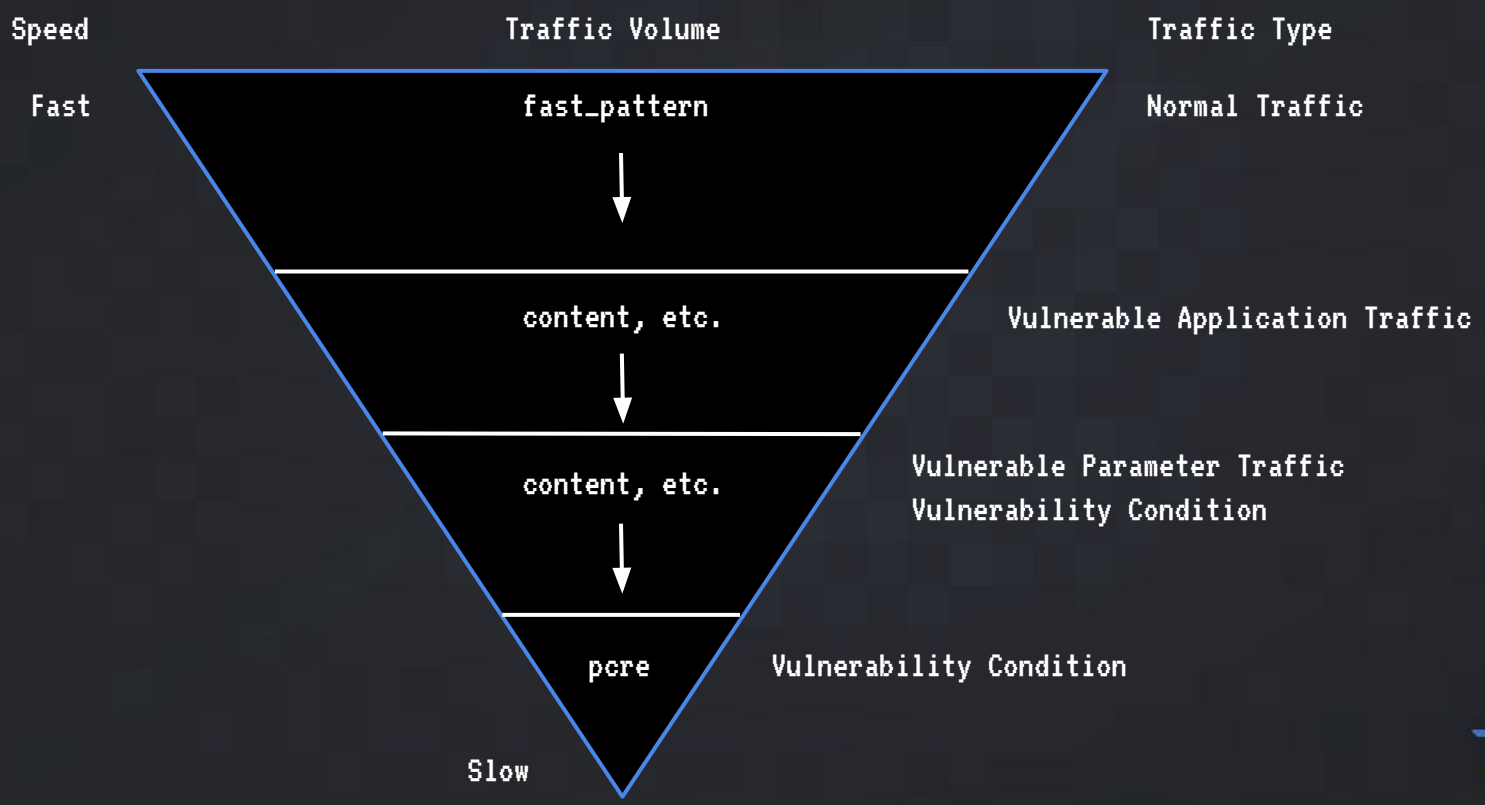
```
# pcre rule option example
alert tcp any any -> 192.168.1.0/24 111 (
    # match the following regex
    pcre:"/A[BC]D/i"; \
```

pcre declares a Perl compatible regular expression for matching on payload data.

Flags can be specified after the slash.

e.g. /i for case insensitivity.

# Traffic Triage and Isolation



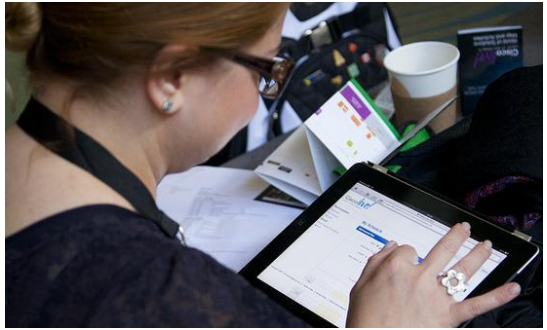
# Call to Action

- Related sessions:
  - Introduction to Snort Rule Writing
  - Detection Strategies with Snort [DevNet-1126]
- Visit the World of Solutions for
  - Cisco Campus
  - Walk in Labs
  - Technical Solution Clinics
- Meet the Engineer - Available immediately after this talk.

# Complete Your **Online Session Evaluation**

- Please complete your online session evaluations after each session. Complete 4 session evaluations & the Overall Conference Evaluation (available from Thursday) to receive your Cisco Live T-shirt.

- All surveys can be completed via the Cisco Live Mobile App or the Communication Stations

Brandon Stultz
talosintel.com
@talossecurity