Field/context definition for custom threat signatures

1. ftp-req-params
This field including all parameters for single command which pointed by qualifier 1.

For example:
USER paloaltonetworks

you can match the pattern "paloaltonetworks" in this field.

2. ftp-rsp-banner
This field including all response banner

For example:
220 Serv-U ftp server is ready

you can match the pattern "Serv-U ftp server" in this field.

3. http-req-headers
This field including all http request headers

For example:
Cookie: paloaltonetworks_visit_time=20;

you can match the pattern "Cookie: paloaltonetworks_" in this field.

4. http-req-host-header
This field including all http request headers

For example:
Host: www.paloaltonetworks.com

you can match the pattern "www.paloaltonetworks.com" in this field.

5. http-req-mime-form-data
This field including POST form data

For example:
POST /cgi-bin/upload.cgi HTTP/1.1
Host: 10.1.4.8
Content-Type: multipart/form-data; boundary=---------------------------28956326772403
Content-Length: 111888
---------------------------28956326772403
Content-Disposition: form-data; name="photo1"; filename=""
Content-Type: application/octet-stream
---------------------------28956326772403

Content-Disposition: form-data; name="photo2"; filename="DP0005.pdf"
Content-Type: application/pdf

you can match the pattern "name=\"photo1\"" in this field.

6. http-req-params
This field including all QUERY_STRING in http request

For example:
GET /cgi-bin/upload.cgi?url=www.paloaltonetworks.com HTTP/1.1

you can match the pattern "url=www.paloalto" in this field.

7. http-req-uri-path
This field including all uri in http request

For example:
GET /cgi-bin/upload.cgi?url=www.paloaltonetworks.com HTTP/1.1
you can match the pattern "cgi-bin/upload.cgi" in this field.

8. http-rsp-headers
This field including all http response headers

For example:
HTTP/1.1 404 Not Found
Date: Thu, 17 Sep 2009 22:54:59 GMT
Server: Apache/2.2.8 (Ubuntu)
Content-Length: 289
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

you can match the pattern "Server: Apache" in this field.

9. imap-req-cmd-line
This field including all data in one command

For example:
=> USER abcd
<= +OK
=> PASS Hello
<= +OK
=> Userdefinedhackcommand

you can match the pattern "hackcommand" in this field.

10. imap-req-first-param
This field including the first parameter of the single command pointed by qualifier 1

For example:
=> USER panlabnetworks
<= +OK
=> PASS Hello
<= +OK

you can match the pattern "panlabnetworks" in this field.

11. ssl-rsp-certificate
This field is the server certificate

For example:
No example available because this is binary data. Contact Support for more information.

12. ssl-req-client-hello
This field is the client hello field
For example:
No example available because this is binary data. Contact Support for more information.

13. ssl-rsp-server-hello
This field is the server hello field

For example:
No example available because this is binary data. Contact Support for more information.

14. imap-req-params-after-first-param
This filed including the left data after first parameter

For example:
=> USER panlabnetworks
<= +OK
=> PASS Hello
<= +OK
=> FETCH cmd.ref 100 BODY.len

You can match the pattern "100 BODY.len" in this field.

15. smtp-req-argument
This field including all data in single command pointed by qualifier 1

For example:
=> HELO hackserver.com

you can match the pattern "hackserver" in this field.

16. smtp-rsp-content
This field including response content

For example:
=> HELO hackserver.com
<= 200 OK Go AHEAD

you can match the pattern "Go AHEAD" in this field.

17. file-html-body alias panav-rsp-html-message-body

This field including html/txt file content

For example:
HTTP/1.1 200 OK
Date: Wed, 13 Jan 2010 19:54:24 GMT
Server: Apache/2.2.3 (Fedora)
Connection: close
Content-Length:50
Content-Type: text/html; charset=ISO-8859-1
<html>testedinformation</html>

you can match the pattern "testedinformation" in this field.

18. file-office-content alias panav-rsp-office-content
This field including Micrisoft office file content

For example:
No example available because this is binary data. Contact Support for more information.

19. file-pdf-body alias panav-rsp-pdf-body
This field including pdf file content

For example:
341 0 obj
<</MarkInfo<</LetterspaceFlags 0/Marked true>>/Outlines 66 0 R/Metadata 119 0 R/PieceInfo

you can match the pattern "LetterspaceFlags" in this field.

20. ftp-req-param-len
This value indicated the length of single command which pointed by qualifier 1

For example:
USER ABCD\r\n

ftp-req-param-len should be 6 ("ABCD\r\n")

21. http-req-content-length
This value is the length get from Content-length

For example:
POST /cgi-bin/upload.cgi HTTP/1.1
Host: 10.1.4.8
Content-Type: multipart/form-data; boundary=---------------------------28956326772403
Content-Length: 111888

http-req-content-length should be 111888

22. http-req-header-length
This value indicated length of customer header which point by qualifier 2

For example:
POST /cgi-bin/upload.cgi HTTP/1.1
Host: 10.1.4.8
Content-Type: multipart/form-data; boundary=---------------------------28956326772403
Content-Length: 111888

http-req-header-length will be count from "Host:" and ended after "111888\r\n\r\n"

23. http-req-param-length
This value indicated the QUERY_STRING length

For example:
GET /cgi-bin/upload.cgi?url=www.paloaltonetworks.com HTTP/1.1

http-req-param-length will be the length of string "url=www.paloaltonetworks.com".

24. http-req-uri-path-length
This value indicated the request URI length

For example:
GET /cgi-bin/upload.cgi?url=www.paloaltonetworks.com HTTP/1.1

http-req-uri-path-length will be the length of string "/cgi-bin/upload.cgi"

25. http-rsp-code

This value indicated the response code

For example:
HTTP/1.1 216 OK

http-rsp-code will be 216

26. http-rsp-content-length
This value is the length get from Content-length

For example:
HTTP/1.1 200 OK
Date: Wed, 13 Jan 2010 19:54:24 GMT
Server: Apache/2.2.3 (Fedora)
Connection: close
Content-Length:50

http-rsp-content-length will be 50.

27. http-rsp-total-headers-len
Indicated all header length of response

For example:
HTTP/1.1 200 OK
Date: Wed, 13 Jan 2010 19:54:24 GMT
Server: Apache/2.2.3 (Fedora)
Connection: close
Content-Length:50

http-rsp-total-headers-len will be count from "Date:" and ended after "Length:50\r\n\r\n"

28. imap-req-cmd-param-len
This value indicated length of single command parameter

For example:
=> USER ABCD
<= +OK
=> hackyouthe server

The last imap-req-cmd-param-len will be the length of "hackyouthe"

29. imap-req-first-param-len
This value indicated length of first parameter

For example:
=> USER ABCD
<= +OK

=> hackyouthe server

The last imap-req-first-param-len will be the length of "server"

30. imap-req-param-len-from-second
This value indicated length of parameter after first one

For example:
=> USER ABCD
<= +OK
=> hackyouthe server I am not

The last imap-req-param-len-from-second will be the length of "I am not"

31. smtp-req-mail-argument-length
This value indicated length of MAIL/SEND/SAML/SOML command parameters

For example:
=> HELO pan lab network
<= 200 ok
=> MAIL FROM: test@eepan.com

smtp-req-mail-argument-length will be the length of "test@eepan.com"

32. smtp-req-helo-argument-length
This value indicated length of HELO/EHLO command parameters

For example:
=> HELO pan lab network
<= 200 ok
=> MAIL FROM: test@eepan.com

smtp-req-helo-argument-length will be the length of "pan lab network"

33. smtp-req-rcpt-argument-length
This value indicated length of RCTP command parameters

For example:
=> HELO pan lab network
<= 200 ok
=> MAIL FROM: test@eepan.com
<= 200 OK
=> RCPT TO: test2@pan.com
smtp-req-rcpt-argument-length will be the length of "test2@pan.com"