RAW LOG ANALYSIS

Firewall Logs

LOG 1:

```
Sep 9 17:14:23 10.131.24.13/10.131.24.13 panfw_via_panorama|v1: 1,2020/09/09
17:14:23,020100177,THREAT,url,2304,2020/09/09
17:39:51,10.60.3.123,120.44.239.154,19.31.169.76,120.44.239.154,AO - Internet Access
Apps,SE\hweeratunge,,ssl,vsys1,Inside,Internet,ae1.3,ae1.1,LFP - SE Forwarding
Default,2020/09/09 17:39:51,672863,1,64422,443,19882,443,0x40b000,tcp,alert,"settings-
win.data.microsoft.com/",(9999),computer-and-internet-info,informational,client-to-
server,1183853794,0xa000000000000000,10.0.0.0-
10.255.255.255,Singapore,0,,0,,,0,,,,,,,,0,477,481,484,0,,SESYDVIR-
FW01,,,,,0,,0,,N/A,unknown,AppThreat-0-0,0x0,0,4294967295,,"computer-and-internet-info,low-
risk",9bd38d49-07d6-4ddb-a86b-af2ec370d943,0
```

IMPORTANT FIELDS	VALUE MAPPED FROM RAW LOG
Date/time of Event	2020/09/09 17:39:51
Type of Log	THREAT
Threat/content type	url
Souce IP/NAT'd Source IP	10.60.3.123/19.31.169.76
Destinatioin IP/NAT'd Destination IP	120.44.239.154/120.44.239.154
Source User	SE\hweeratunge
Destination User	NA
Source Port/NAT'd Source port	64422/19882
Destination Port/NAT'd Destination port	443/443
Protocol	tcp
Action	alert
URL/File name	"settings-win.data.microsoft.com/"
Severity	informational
Direction	client-to-server
Source Location	10.0.0.0-10.255.255.255
Destination Location	Singapore
Device Name	SESYDVIR-FW01

LOG 2:

```
May 7 04:04:35 10.214.216.13/10.214.216.13 panfw_via_panorama|v1: 1,2021/05/07
04:04:35,063201045145,TRAFFIC,end,2305,2021/05/07
04:04:31,10.192.104.61,20.67.222.222,25.145.141.193,20.67.222.222,AO - Internet Apps
Allowed,,,dns,vsys1,Inside,Internet,ethernet1/19.356,ethernet1/1,LFP - SE Forwarding
Default,2021/05/07
04:04:31,523197,1,62494,53,59830,53,0x400019,udp,allow,254,99,155,2,2021/05/07
04:03:58,0,any,0,28181916916,0x8000000000000000,10.0.0.0-10.255.255.255,United
States,0,1,1,aged-out,477,476,1024,0,,SEWATSV-FW01,from-policy,,,0,,0,,N/A,0,0,0,0,5f9cb952-
e6e1-4af4-8b02-561f10b0aa34,0,0,,,,,,,
```

IMPORTANT FIELDS	VALUE MAPPED FROM RAW LOG
Date/time of Event	May 7 04:04:35
Type of Log	TRAFFIC
Threat/content type	end
Souce IP/NAT'd Source IP	10.192.104.61/25.145.141.193
Destination IP/NAT'd Destination IP	20.67.222.222/20.67.222.222
Source User	NA
Application	dns
Log action	LFP - SE Forwarding Default
Source Port/NAT'd Source port	62494/59830
Destination Port/NAT'd Destination port	53/53
Protocol	udp
Action	allow
Bytes sent	99
Bytes received	155
Source Location	10.0.0.0-10.255.255.255
Destination Location	United States
Packets sent/received	1/1
Session end reason	aged-out
Device name	SEWATSV-FW01

LOG 3:

```
09:39:17,016201007,TRAFFIC,end,2305,2021/06/14
09:39:01,10.48.33.163,124.42.196.205,19.31.174.84,124.42.196.205,AO - Internet Access
Apps,SE\kpatil,,ssl,vsys1,Inside,Internet,ae1.3,ae1.1,LFP – SE Forwarding Default,2021/06/14
09:39:01,897481,1,65021,443,16238,443,0x40001c,tcp,allow,12954,4541,8413,26,2021/06/14
09:38:46,1,computer-and-internet-info,0,857959476,0x8000000000000000,10.0.0.0-
10.255.255.255,United States,0,14,12,tcp-fin,477,481,486,0,,SE-FW01,from-
policy,,,0,,0,,N/A,0,0,0,0,9bd38d49-07d6-4ddb-a86b-af2ec370d943,0,0,,,,,,
```

IMPORTANT FIELDS	VALUE MAPPED FROM RAW LOG
Date/time of Event	2021/06/14 09:39:014
Type of Log	TRAFFIC
Threat/content type	end
Souce IP/NAT'd Source IP	10.48.33.163/19.31.174.84
Destinatioin IP/NAT'd Destination IP	124.42.196.205/124.42.196.205
Source User	SE\kpatil
Destination User	NA
Source Port/NAT'd Source port	65021/16238
Destination Port/NAT'd Destination port	443/443
Protocol	tcp
Action	allow
Bytes sent	4541
Bytes Received	8413
Source Location	10.0.0.0-10.255.255.255
Destination Location	United States
Device Name	SE-FW01

LOG 4:

```
Jun 14 09:39:12 10.131.24.13/10.131.24.13 panfw_via_panorama|v1: 1,2021/06/14
09:39:12,016201016113,THREAT,url,2305,2021/06/14
09:39:12,10.138.40.51,17.37.97.229,138.117.201.152,17.37.97.229,AO - Internet Apps
Allowed,SE\szapata,,ssl,vsys1,Inside,Internet,ethernet1/3,ethernet1/2,LFP - SE Forwarding
Default,2021/06/14
09:39:12,188179,1,59947,443,44581,443,0x40b000,tcp,alert,"unitedstates.smartscreen.microsoft.
com/",(9999),computer-and-internet-info,informational,client-to-
server,2661862397,0xa000000000000000,10.0.0.0-10.255.255.255,United
States,0,,0,,,0,,,,,,,,0,477,476,1077,0,,SE-FW01,,,,,0,,0,,N/A,unknown,AppThreat-0-
0,0x0,0,4294967295,,"computer-and-internet-info,low-risk",5f9cb952-e6e1-4af4-8b02-
561f10b0aa34,0,
```

IMPORTANT FIELDS	VALUE MAPPED FROM RAW LOG
Date/time of Event	2021/06/14 09:39:12
Type of Log	THREAT
Threat/content type	url
Souce IP/NAT'd Source IP	10.138.40.51/138.117.201.152
Destinatioin IP/NAT'd Destination IP	17.37.97.229/17.37.97.229
Source User	SE\szapata
Destination User	NA
Source Port/NAT'd Source port	59947/44581
Destination Port/NAT'd Destination port	443/443
Protocol	tcp
Action	alert
URL/File name	"unitedstates.smartscreen.microsoft.com/"
Severity	informational
Direction	client-to-server
Source Location	10.0.0.0-10.255.255.255
Destination Location	United States
Device Name	SE-FW01

Antivirus Logs

LOG 1:

```
Jun 14 05:47:32 SE-SEP03/10.192.106.31 SymantecSEP: SymantecServer:
SEMINL16GPM8,Local Host IP: 192.168.0.22,Local Port: 17500,Local Host MAC:
E318D18F30,Remote Host IP: 175.193.13.3,Remote Host Name: ,Remote Port: 17500,Remote
Host MAC: FFFFFFFFFFFF,UDP,Outbound,Begin: 2021-06-14 05:04:51,End Time: 2021-06-14
05:04:51,Occurrences: 5,Application: C:/Program Files (x86)/Dropbox/Client/Dropbox.exe,Rule:
Block Malicious IP-1,Location: Out of Network,User Name: jtauer,Domain Name: SE,Action:
Blocked,SHA-256:
7462b5db619e77833d7cebcdca98352976154ba72d24080eb20edb01925accb6,MD-5:
6B532CE4B97BC0F4D6CFA12E9637CBF5
```

IMPORTANT FIELDS	VALUE MAPPED FROM RAW LOG
Date/time of Event	Jun 14 05:47:32
Local Host IP	192.168.0.22
Local Host MAC	E318D18F30
Remote Host IP	175.193.13.3
Source Port/NAT'd Source port	17500
Protocol	UDP
Application	C:/Program Files (x86)/Dropbox/Client/Dropbox.exe
Action	Blocked
User name	jtauer
SHA-256	7462b5db619e77833d7cebcdca98352976154ba72d24080eb20edb01925accb6
MD-5	6B532CE4B97BC0F4D6CFA12E9637CBF5

LOG 2:

```
May 4 14:07:50 SE1BTSEP03/10.192.106.31 SymantecSEP: SymantecServer:
SEAZUEBTDAXOCR01,Event Description: [SID: 27517] Attack: OpenSSL Heartbleed CVE-2014-
0160 3 attack detected but not blocked. Application path: C:\PROGRAM FILES (X86)\FILEZILLA
SERVER\FILEZILLA SERVER.EXE,Local Host IP: 192.168.99.4,Local Host MAC:
000000000000,Remote Host Name: ,Remote Host IP: 168.215.65.86,Remote Host MAC:
000000000000,Inbound,TCP,Intrusion ID: 0,Begin: 2021-05-04 14:05:15,End Time: 2021-05-04
14:05:15,Occurrences: 1,Application: C:/PROGRAM FILES (X86)/FILEZILLA SERVER/FILEZILLA
SERVER.EXE,Location: Default,User Name: ANIL, Domain Name: ,Local Port: 1911,Remote Port:
41132,CIDS Signature ID: 27517,CIDS Signature string: Attack: OpenSSL Heartbleed CVE-2014-
0160 3,CIDS Signature SubID: 75149,Intrusion URL: ,Intrusion Payload URL: ,SHA-256:
EEBCC1D79679BB23F1D8C8F7FA1DD07FE2A0DE0444FC7985D29803C51B61FF3A,MD-5:
```

IMPORTANT FIELDS	VALUE MAPPED FROM RAW LOG
Date/time of Event	May 4 14:07:50
Attack	OpenSSL Heartbleed CVE-2014-0160
Local Host IP	192.168.99.4
Local Host MAC	NA
Remote Host IP	168.215.65.86
Local Port/Remote port	1911/41132
Protocol	TCP
File name	C:\PROGRAM FILES (X86)\FILEZILLA SERVER\FILEZILLA SERVER.EXE
Action	attack detected but not blocked
User name	ANIL
SHA-256	EEBCC1D79679BB23F1D8C8F7FA1DD07FE2A0DE0444FC7985D29803C51B61FF3A
MD-5	NA