Squert, Sguil, Kibana in AWS

Alex Appelwick, Hayley Blair, Gregory Harden, and Justin Roysdon

How We Made It - Security Onion - Requirements

Security Onion Hardware requirements

Kibana - 8 GB RAM, 4 CPU Cores

Our “hardware” - AWS Free Tier Limitations

Free Tier Eligible Instance Type Only

1. T2.micro, 1 GB RAM, 1 CPU Core (2.5 GHz)
2. Network Performance - Low to Moderate

Operating System (on ISO) - Ubuntu 16.04.6 LTS

How We Made It - Security Onion - The VM

Download & Install VirtualBox (Version 6.1.4)

https://www.virtualbox.org/wiki/Downloads

Download the Security Onion ISO (ISO installs Linux OS) (Version 16.04.6.6)

https://github.com/Security-Onion-Solutions/security-onion/blob/master/Verify_ISO.md

Create VM - VMDK - 20 GB, 1024 MB RAM, 1 CPU, Network (NAT)

Boot to ISO and Install

Export Appliance (OVA file) - **Open Virtualization Format 2.0**

How We Made It - Security Onion - AWS Upload

Links with Instructions and My Example Files

https://docs.aws.amazon.com/vm-import/latest/userguide/vmimport-image-import.html

https://github.com/WingsLikeEagles/SecurityOnionAWS

Upload to S3 Bucket (s3://bucket-name/SecOnion.ova)

Create IAM Policies (vmimport-role-policy.json and vmimport-trust-policy.json)

Create containers.json

Install AWSCLI locally - *python pip install awscli*

How We Made It - Security Onion - AWS Import

Import the OVA image creating the AMI (Amazon Machine Image)

aws ec2 --region us-west-1 import-image --description "Security Onion" --disk-containers "file://.\containers.json"

Record the "ImportTaskId": "import-ami-04548778fe6c9dbd4"

Check Progress with:

aws ec2 describe-import-image-tasks --region us-west-1 --import-task-ids import-ami-04548778fe6c9dbd4

Should result in the creation of an AMI in EC2 and a Snapshot (these need to be deleted after installation to avoid charges in Free Tier)

How We Made It - Security Onion - Run It

When creating Instance, be sure to create a Key to be able to log in.

Install VcXsrv on local - https://sourceforge.net/projects/vcxsrv/files/latest/download

Install Putty on local and create a profile, then ssh in to instance:

- SSH Tunnel ports - 443:localhost:443
- SSH X11 - Enable X11 forwarding

Run Security Onion Install Script - *sudo ~/Desktop/securityonion-setup.desktop*

Say NO to “configure interfaces”, this will drop your connection

Open local Browser to https://localhost/

From Putty, *squil.tk* (must have VcXsrv running before connecting to ssh session)

How We Made It - Security Onion - Links

https://github.com/WingsLikeEagles/SecurityOnionAWS - Justin's Instructions

https://www.virtualbox.org/wiki/Downloads

https://github.com/Security-Onion-Solutions/security-onion/blob/master/Verify_ISO.md

https://sourceforge.net/projects/vcxsrv/files/latest/download

https://docs.aws.amazon.com/vm-import/latest/userguide/vmimport-image-import.html

Performance Tool Ratings

- Each Security Onion tool we used has its own capabilities and benefits.
- Using them all together can yield better results (like peeling back the layers of an onion.).

Squert

Pros:

-Gives both NIDS and HIDS alerts

-Gives a broad overview of daily events on the timeplot, so patterns can easily emerge

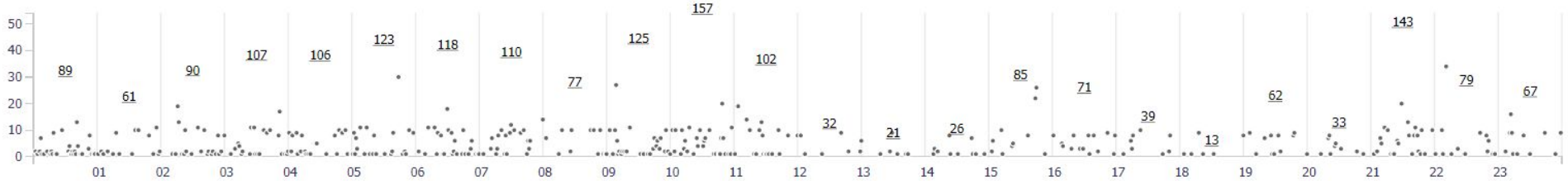
-Can group similar events in a certain time frame

-Does not require a lot of computer resources

Cons:

Very basic information. Will need to pivot to other programs for more in-depth packet capture

Squert Timeplot and Map



GEOGRAPHIC DISTRIBUTION (**8** distinct countries)

Sguil

Pros:
-Intuitive GUI provides access to real-time events, session data, and raw packet captures

-Can configure email notifications, auto-categorizing rules, and alerts

-Can pivot easily to alternate programs like Wireshark, NetworkMiner, and Kibana once an alert is given

Cons:
-Can only use 1024 sockets for receiving communications from sensors. Too many sensors or sniffing agents may overload
.
-Events displayed must be regularly categorized or problems may occur

SGUIL-0.9.0 - Connected To localhost

File Query Reports Sound: Off ServerName: localhost UserName: snailz UserID: 2 2020-07-28 03:39:29 GMT

RealTime Events | Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	snail-onio...	3.7122	2020-07-27 03:25:17	54.38.75.41	56148	172.31.1.105	22	6	ET TOR Known Tor Relay/Router (Not Exit) Node TCP Traffic group 112
RT	1	snail-onio...	3.7123	2020-07-27 03:25:17	54.38.75.41	56148	172.31.1.105	22	6	ET TOR Known Tor Exit Node TCP Traffic group 112
RT	2	snail-onio...	3.7360	2020-07-27 09:37:54	61.177.172.159	46216	172.31.1.105	22	6	ET SCAN Potential SSH Scan
RT	2	snail-onio...	3.7371	2020-07-27 09:54:05	37.49.230.113	45828	172.31.1.105	22	6	ET DROP Dshield Block Listed Source group 1
RT	6	snail-onio...	3.7377	2020-07-27 10:06:29	115.79.137.56	19336	172.31.1.105	22	6	ET SCAN Potential SSH Scan
RT	485	snail-onio...	3.7406	2020-07-27 10:49:31	222.186.52.131	41327	172.31.1.105	22	6	ET SCAN Potential SSH Scan
RT	1	snail-onio...	3.7495	2020-07-27 11:45:50	37.49.224.246	54698	172.31.1.105	22	6	ET DROP Dshield Block Listed Source group 1
RT	1	snail-onio...	3.7538	2020-07-27 12:11:58	51.178.78.154	46847	172.31.1.105	22	6	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 37
RT	1	snail-onio...	3.7646	2020-07-27 13:27:31	145.239.82.87	43681	172.31.1.105	22	6	ET TOR Known Tor Relay/Router (Not Exit) Node TCP Traffic group 13
RT	1	snail-onio...	3.7647	2020-07-27 13:27:31	145.239.82.87	43681	172.31.1.105	22	6	ET TOR Known Tor Exit Node TCP Traffic group 13
RT	7	snail-onio...	3.7889	2020-07-27 16:28:00	222.186.42.57	16981	172.31.1.105	22	6	ET SCAN SSH BruteForce Tool with fake PUTTY version
RT	3	snail-onio...	3.7891	2020-07-27 16:28:21	222.186.42.57	14980	172.31.1.105	22	6	ET SCAN Potential SSH Scan
RT	2	snail-onio...	3.8002	2020-07-27 17:49:49	222.186.42.213	34921	172.31.1.105	22	6	ET SCAN SSH BruteForce Tool with fake PUTTY version
RT	1	snail-onio...	3.8005	2020-07-27 17:50:10	222.186.42.213	39132	172.31.1.105	22	6	ET SCAN Potential SSH Scan
RT	1	snail-onio...	3.8196	2020-07-27 20:30:33	37.49.230.118	59323	172.31.1.105	22	6	ET DROP Dshield Block Listed Source group 1
RT	2	snail-onio...	3.8266	2020-07-27 21:25:18	54.36.61.172	24681	172.31.1.105	22	6	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 40
RT	1	snail-onio...	3.8556	2020-07-28 01:07:29	65.49.20.66	52826	172.31.1.105	22	6	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 64

IP Resolution | Agent Status | Snort Statistics | System Msgs | User Msgs

☑ Reverse DNS ☑ Enable External DNS

Src IP:	54.38.75.41
Src Name:	ip41.ip-54-38-75.eu
Dst IP:	172.31.1.105
Dst Name:	ip-172-31-1-105.us-west-1.compute.internal

Whois Query: ◉ None ○ Src IP ○ Dst IP

☑ Show Packet Data ☑ Show Rule

```
alert tcp [54.36.108.162,54.37.16.241,54.38.75.41,54.38.75.42,54.38.75.44,54.38.81.231,54.39.16.73,54.76.120.237,54.94.167.229,5.79.109.48]
any -> $HOME_NET any (msg:"ET TOR Known Tor Exit Node TCP Traffic group 112"; flags:S;
reference:url,doc.emergingthreats.net/bin/view/Main/TorRules; threshold: type limit, track by_src, seconds 60, count 1; classtype:misc-attack;
```

	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
IP	54.38.75.41	172.31.1.105	4	5	0	60	39375	2	0	39	35605

	Source Port	Dest Port	R 1	R 0	URG	ACK	PSH	RST	SYN	FIN	Seq #	Ack #	Offset	Res	Window	Urp	ChkSum
TCP	56148	22	.	.	.	.	.	.	X	.	2589017720	0	10	0	29200	0	44632

DATA	None.	None.

Search Packet Payload ○ Hex ◉ Text ☐ NoCase

Kibana

Pros:
-Has many visual representations of data like histograms, line graphs, pie charts, and heat maps.

-Integrates well with ElasticSearch, which is a popular analytics and search engine, Kibana is the default choice for visualizing data from Elastisearch.

-Comes with mapping support so you can layer geographical information on top of data.

-Machine can learn normal patterns and detect when anomalies occur in data.

Cons:
-Requires more resources to work, which is why we were unable to use it on the free version of AWS.

-Search results in dashboards are limited to the first ten results for a query. Adjusting the size to more may affect performance.

-Searches will also time out, but the timeout value can also be adjusted to wait longer for results.

kibana

Dashboard / Bro - Connections

Full screen | Share | Clone | Edit | Auto-refresh | Last 24 hours

>_ *

Options | Update

Add a filter +

- Discover
- Visualize
- Dashboard
- Timelion
- Dev Tools
- Management
- Squert
- Logout

Navigation

Home
Help

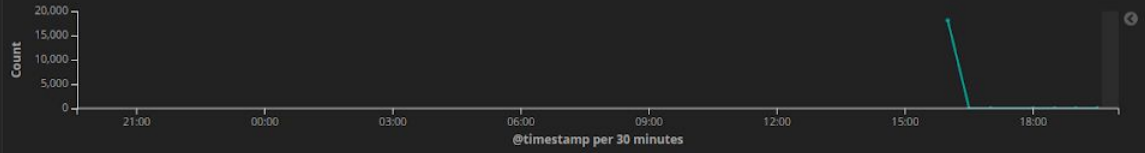
Alert Data
Bro Notices
ElastAlert
HIDS
NIDS

Bro Hunting
Connections
DCE/RPC
DHCP
DNP3
DNS
Files
FTP
HTTP
Intel
IRC
Kerberos
Modbus
MySQL
NTLM
PE
RADIUS
RDP
RFB
SIP
SMB
SMTP
SNMP
Software
SSH
SSL
Syslog
Tunnels
Weird

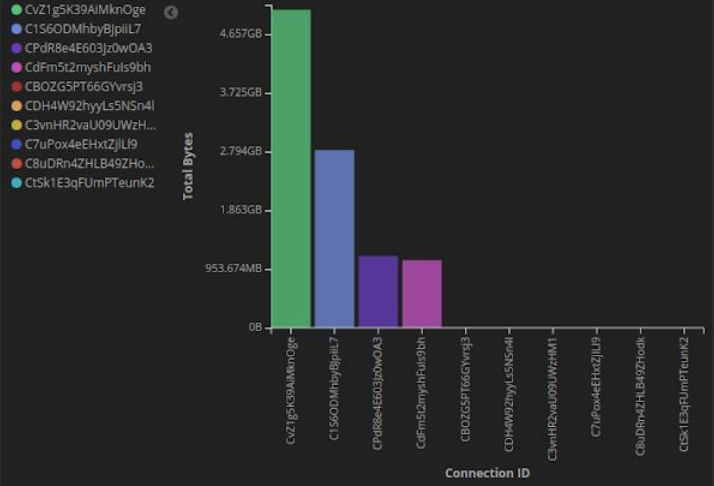
Connections - Log Count

18,132

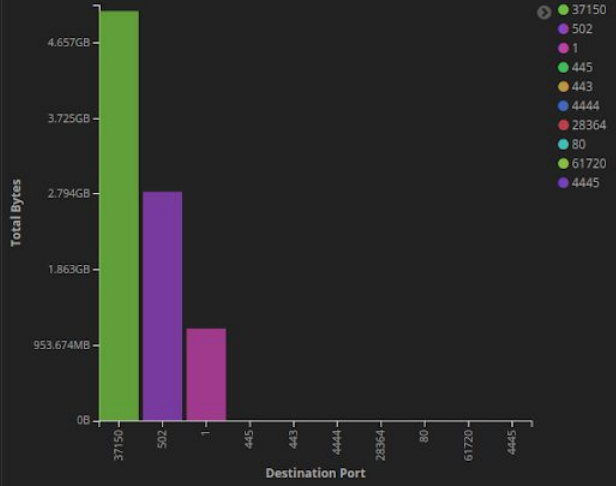
Connections - Log Count Over Time



Connections - Top 10 - Total Bytes By Connection



Connections - Top 10 - Total Bytes By Destination Port



Wireshark

Pros:
-Lets you see the fine details of what is happening on the network. Can show everything in a packet to the a very granular level

-Easy to filter information using capture and display filters

-A good resource for pivoting to find more information after a more general IDS finds an anomaly

Cons:
-Packet capture files can take up a lot of space on your computer

-Can be overwhelming to start here because it shows so much data. Can be easier to see a broader view on other programs

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 0 | Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.7.9.101	65.99.252.112	TCP	66	49230 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.000044	65.99.252.112	10.7.9.101	TCP	58	80 → 49230 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
3	0.000084	10.7.9.101	65.99.252.112	TCP	54	49230 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
4	0.000177	10.7.9.101	65.99.252.112	HTTP	122	GET /Yb/ HTTP/1.1
5	0.000218	65.99.252.112	10.7.9.101	TCP	54	80 → 49230 [ACK] Seq=1 Ack=69 Win=64240 Len=0
6	0.001243	65.99.252.112	10.7.9.101	TCP	1342	80 → 49230 [PSH, ACK] Seq=1 Ack=69 Win=64240 Len=1288 [TCP segment of a reassembled PDU]
7	0.002265	65.99.252.112	10.7.9.101	TCP	1342	80 → 49230 [PSH, ACK] Seq=1289 Ack=69 Win=64240 Len=1288 [TCP segment of a reassembled PDU]
8	0.003288	65.99.252.112	10.7.9.101	TCP	1342	80 → 49230 [PSH, ACK] Seq=2577 Ack=69 Win=64240 Len=1288 [TCP segment of a reassembled PDU]
9	0.004310	65.99.252.112	10.7.9.101	TCP	1342	80 → 49230 [PSH, ACK] Seq=3865 Ack=69 Win=64240 Len=1288 [TCP segment of a reassembled PDU]
10	0.004351	10.7.9.101	65.99.252.112	TCP	54	49230 → 80 [ACK] Seq=69 Ack=5153 Win=64240 Len=0
11	0.005374	65.99.252.112	10.7.9.101	TCP	1342	80 → 49230 [PSH, ACK] Seq=5153 Ack=69 Win=64240 Len=1288 [TCP segment of a reassembled PDU]
12	0.006401	65.99.252.112	10.7.9.101	TCP	1342	80 → 49230 [PSH, ACK] Seq=6441 Ack=69 Win=64240 Len=1288 [TCP segment of a reassembled PDU]
13	0.006438	10.7.9.101	65.99.252.112	TCP	54	49230 → 80 [ACK] Seq=69 Ack=7729 Win=64240 Len=0
14	0.007461	65.99.252.112	10.7.9.101	TCP	1342	80 → 49230 [PSH, ACK] Seq=7729 Ack=69 Win=64240 Len=1288 [TCP segment of a reassembled PDU]
15	0.008485	65.99.252.112	10.7.9.101	TCP	1342	80 → 49230 [PSH, ACK] Seq=9017 Ack=69 Win=64240 Len=1288 [TCP segment of a reassembled PDU]
16	0.008525	10.7.9.101	65.99.252.112	TCP	54	49230 → 80 [ACK] Seq=69 Ack=10305 Win=64240 Len=0
17	0.009552	65.99.252.112	10.7.9.101	TCP	1342	80 → 49230 [PSH, ACK] Seq=10305 Ack=69 Win=64240 Len=1288 [TCP segment of a reassembled PDU]
18	0.010574	65.99.252.112	10.7.9.101	TCP	1342	80 → 49230 [PSH, ACK] Seq=11593 Ack=69 Win=64240 Len=1288 [TCP segment of a reassembled PDU]
19	0.010613	10.7.9.101	65.99.252.112	TCP	54	49230 → 80 [ACK] Seq=69 Ack=12881 Win=61664 Len=0
20	0.010654	10.7.9.101	65.99.252.112	TCP	54	[TCP Window Update] 49230 → 80 [ACK] Seq=69 Ack=12881 Win=64240 Len=0
21	0.011679	65.99.252.112	10.7.9.101	TCP	1342	80 → 49230 [PSH, ACK] Seq=12881 Ack=69 Win=64240 Len=1288 [TCP segment of a reassembled PDU]
22	0.012702	65.99.252.112	10.7.9.101	TCP	1342	80 → 49230 [PSH, ACK] Seq=14169 Ack=69 Win=64240 Len=1288 [TCP segment of a reassembled PDU]

```
▶ Frame 4: 122 bytes on wire (976 bits), 122 bytes captured (976 bits)
▶ Ethernet II, Src: 00:08:02:1c:47:ae, Dst: 20:e5:2a:b6:93:f1
▶ Internet Protocol Version 4, Src: 10.7.9.101, Dst: 65.99.252.112
▼ Transmission Control Protocol, Src Port: 49230, Dst Port: 80, Seq: 1, Ack: 1, Len: 68
    Source Port: 49230
    Destination Port: 80
    [Stream index: 0]
    [TCP Segment Len: 68]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 69    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  ▶ Flags: 0x018 (PSH, ACK)
    Window size value: 64240
    [Calculated window size: 64240]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x14f2 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▶ [SEQ/ACK analysis]
  ▶ [Timestamps]
    TCP payload (68 bytes)
▼ Hypertext Transfer Protocol
  ▼ GET /Yb/ HTTP/1.1\r\n
    ▼ [Expert Info (Chat/Sequence): GET /Yb/ HTTP/1.1\r\n]
        [GET /Yb/ HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /Yb/
      Request Version: HTTP/1.1
    Host: primerplano.org\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://primerplano.org/Yb/]
    [HTTP request 1/1]
    [Response in frame: 135]
```

```
0000  20 e5 2a b6 93 f1 00 08  02 1c 47 ae 08 00 45 00   ··*····· ··G···E·
0010  00 6c 03 9c 40 00 80 06  a5 b0 0a 07 09 65 41 63   ·l··@··· ·····eAc
0020  fc 70 c0 4e 00 50 b9 22  f6 15 2b 24 65 eb 50 18   ·p·N·P·" ··+$e·P·
0030  fa f0 14 f2 00 00 47 45  54 20 2f 59 62 2f 20 48   ····· GE T /Yb/ H
0040  54 54 50 2f 31 2e 31 0d  0a 48 6f 73 74 3a 20 70   TTP/1.1· ·Host: p
0050  72 69 6d 65 72 70 6c 61  6e 6f 2e 6f 72 67 0d 0a   rimerpla no.org··
0060  43 6f 6e 6e 65 63 74 69  6f 6e 3a 20 4b 65 65 70   Connecti on: Keep
0070  2d 41 6c 69 76 65 0d 0a  0d 0a                     -Alive··· ··
```

Wireshark · Follow TCP Stream (tcp.stream eq 0) · 10.7.9.101_49230_65.99.252.112_80-6.raw

```
GET /Yb/ HTTP/1.1
Host: primerplano.org
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Mon, 09 Jul 2018 14:53:23 GMT
Server: Apache
X-Powered-By: PHP/5.5.38
Expires: Tue, 01 Jan 1970 00:00:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, max-age=0, post-check=0, pre-check=0
Pragma: no-cache
Content-Disposition: attachment; filename="5319.exe"
Content-Transfer-Encoding: binary
Last-Modified: Mon, 09 Jul 2018 14:53:23 GMT
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: application/octet-stream

4000
MZ......................@.......................................        .!..L.!This program cannot be run in DOS mode.

$.......PE..L....LC[.................0.................@....@.................................7W.v.................................
(...d.......,.........p..@.......................................@..h....1..H....................text...Z#.......0.................
..`.rdata...A...@...P...@.............@..@.data...............................@...CONST....,........
0..................@..@.......................................................................................................
.......................................................................................................................
.......................................................................................................................
.......................................................................................................................
.......................................................................................................................
.......................................................................................................................
.......................................................................................................................
.......................................................................................................................
.......................................................................................................................
.......................................................................................................................
```

1 client pkt(s), 87 server pkt(s), 1 turn(s).

Entire conversation (111 kB) | Show and save data as ASCII | Stream 0

Find: | Find Next

Filter Out This Stream | Print | Save as | Back | Close | Help

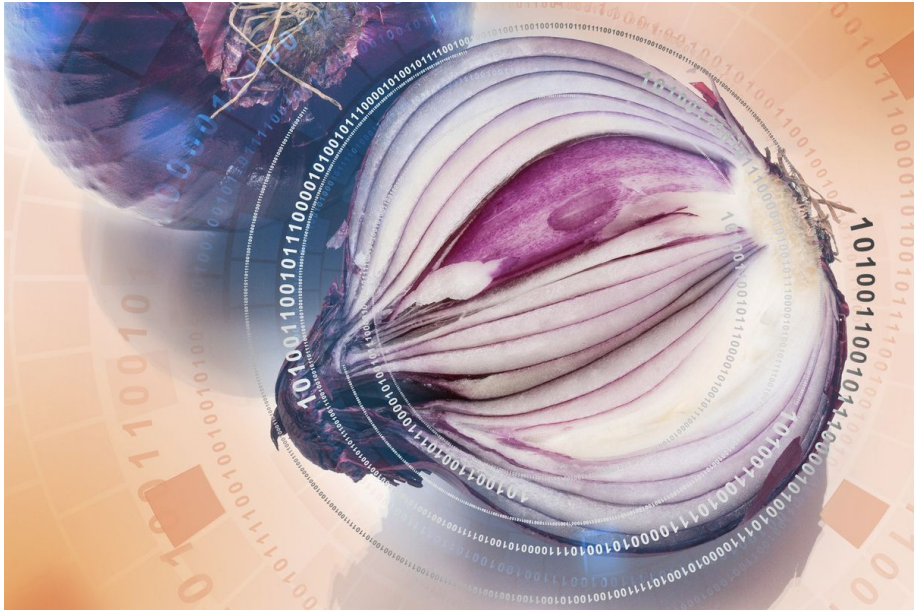
Types of Intrusions:

1. Suspicious login attempts
2. DDoS attacks
3. UDP floods
    a. During limited scan, no malware reported

Recommendations:

1. Software only is supported on x86 & x64 bit processors, 3-8 physical cores
    a. In software types of monitoring tools need more processing requirement, up to 10 vCPUs
2. Logs can add up quickly, large enough storage size for >= 30 days (16TB)
    a. Local storage; SAN, iSCSI
    b. more disk space you have, the more PCAP retention.
3. Memory required 8-16GB
    a. Similar requirements as a corporate workstation standard.

Any questions?



ected To localhost

s Sound: Off ServerName: localhost UserName: snailz UserID: 2

Escalated Events

nsor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort
ail-onio...	3.7122	2020-07-27 03:25:17	54.38.75.41	56148	172.31.1.105	22
ail-onio...	3.7123	2020-07-27 03:25:17	54.38.75.41	56148	172.31.1.105	22
ail-onio...	3.7360	2020-07-27 09:37:54	61.177.172.159	46216	172.31.1.105	22
ail-onio...	3.7371	2020-07-27 09:54:05	37.49.230.113	45828	172.31.1.105	22
ail-onio...	3.7377	2020-07-27 10:06:29	115.79.137.56	19336	172.31.1.105	22
ail-onio...	3.7406	2020-07-27 10:49:31	222.186.52.131	41327	172.31.1.105	22
ail-onio...	3.7495	2020-07-27 11:45:50	37.49.224.246	54698	172.31.1.105	22
ail-onio...	3.7538	2020-07-27 12:11:58	51.178.78.154	46847	172.31.1.105	22

Agent Status | Snort Statistics | System Msgs | User Msgs

Enable External DNS

78.154

267.ip-51-178-78.eu

1.105

1-1-105.us-west-1.compute.internal

lone Src IP Dst IP

Show Packet Data

alert tcp
[51.15.217.202,51.15.230.2
.15.54.140,51.15.58.180,51
1.158.114.166,51.158.114.7
0,51.161.34.239,51.178.78.
.254.167.166,51.254.197.14
$HOME_NET any (msg:"ET
threshold: type limit, track b
attack_target Any, deploym
/nsm/server_data/securityo

IP	Source IP
	51.178.78.154
TCP	Source Port / Dest Port

snail@snail-onion: ~

```
Server Command Recieved: SensorStatusUpd
sec ossec {2020-07-28 03:43:14} 1} 2 {sn
20-07-28 03:44:23} 1} 3 {snail-onion-eth
3:43:22} 1}}
```

SGUIL-0.9.0

Sguil - A tcl/tk interface for network security monitoring

Copyright (C) 2002-2013 Robert (Bamm) Visscher <bamm@sguil.net>

This program is distributed under the terms of version 3 of the GNU Public License. See LICENSE for further details.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

Select Network(s) to Monitor

snail-onion-eth0	snail-onion-ossec
unmonitored	unmonitored

Select All | Start SGUIL | Exit