Network Security Monitoring in Minutes

Doug Burks

tcpdump -nnAi eth1 -s0 | grep -A5 "Doug Burks"

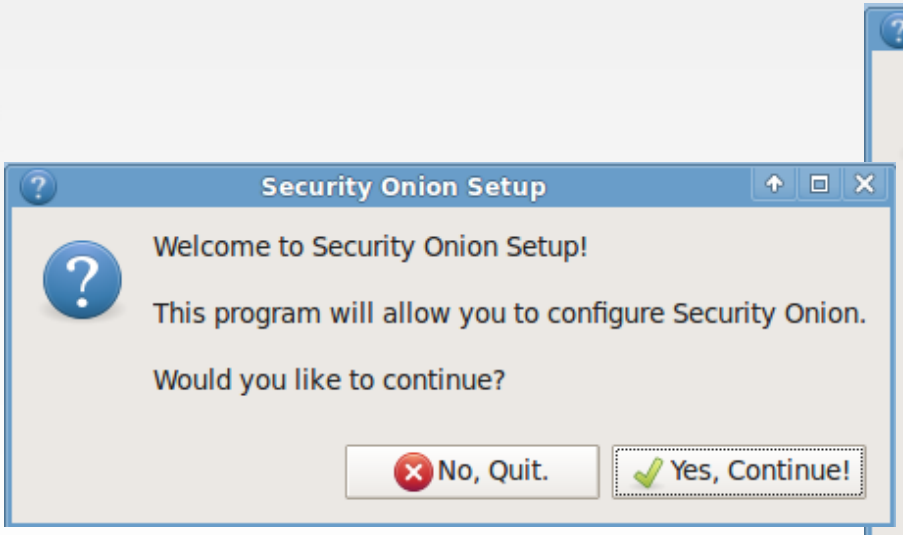
Doug Burks is:

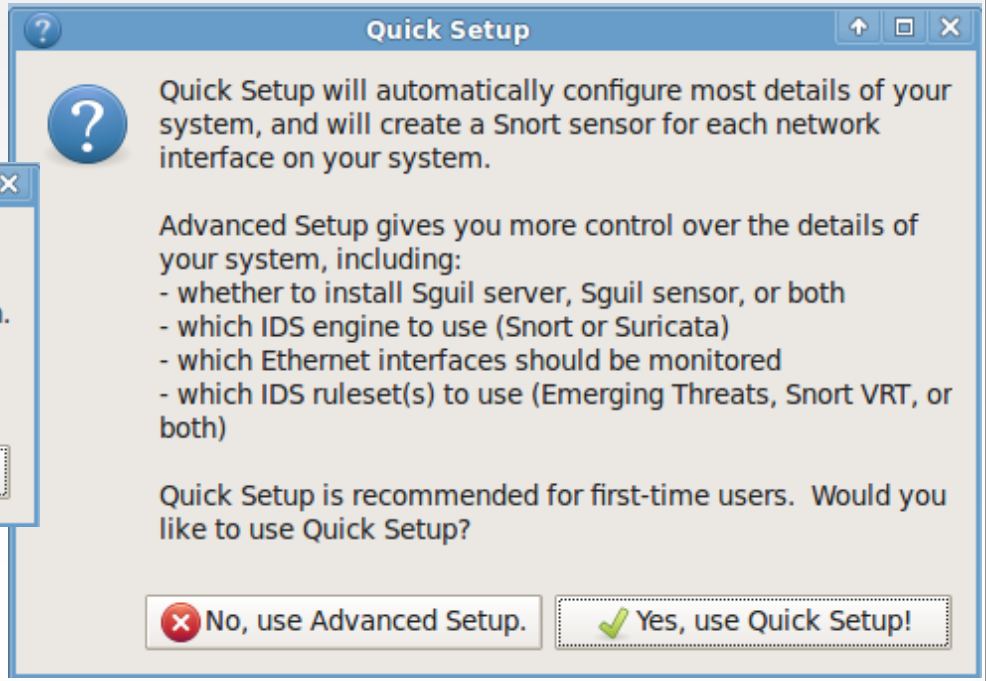
- Christian
- husband and father
- SANS GSE and Community Instructor
- Deputy CSO for Mandiant (we're hiring!)
- @dougburks #securityonion

Security Onion is a FREE Linux distro for Network Security Monitoring (NSM)

Next, Next, Finish for NSM

Setup wizard takes less than 5 minutes!





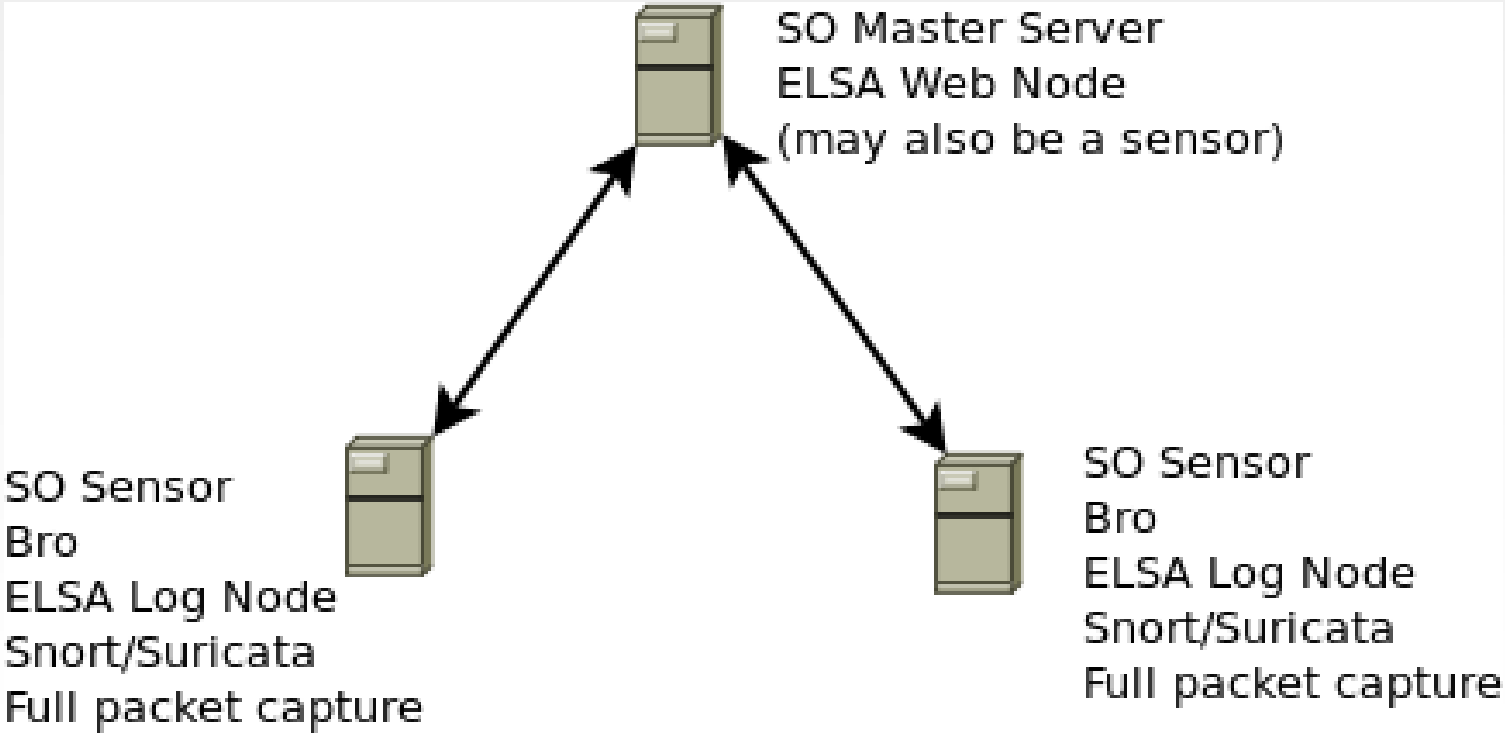
Network Security Monitoring: Data Types

- Alert data (NIDS alerts - Snort/Suricata, HIDS alerts - OSSEC)
- Asset data (Bro and PRADS)
- Session data (Argus, Bro, and PRADS)
- Transaction data (Bro protocol logs: http, ftp, dns, etc.)
- Full content data (netsniff-ng)

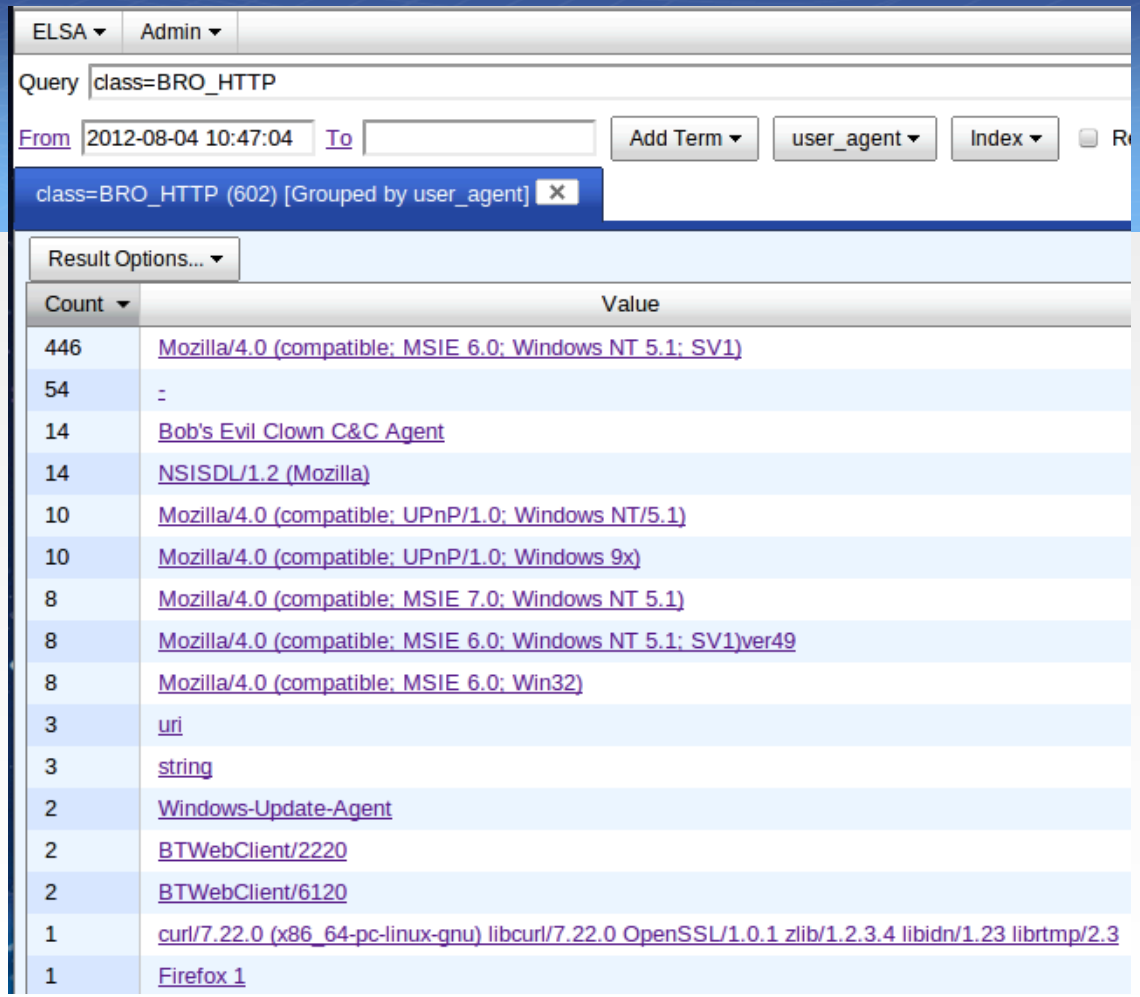
Analysis at Scale

- Download our ISO image (based on Xubuntu 12.04 **64-bit**)
  OR
  Start with your preferred flavor of Ubuntu 12.04 (Ubuntu, Kubuntu, Lubuntu, Xubuntu, or **Ubuntu Server**) 32-bit or **64-bit**, add our PPA and install our packages
- High performance:
  - Snort/Suricata/Bro running on **PF_RING**
  - Netsniff-ng uses **zero-copy** for high-speed full-packet capture
- ELSA (like a free version of Splunk) – **distributed** database with central web interface

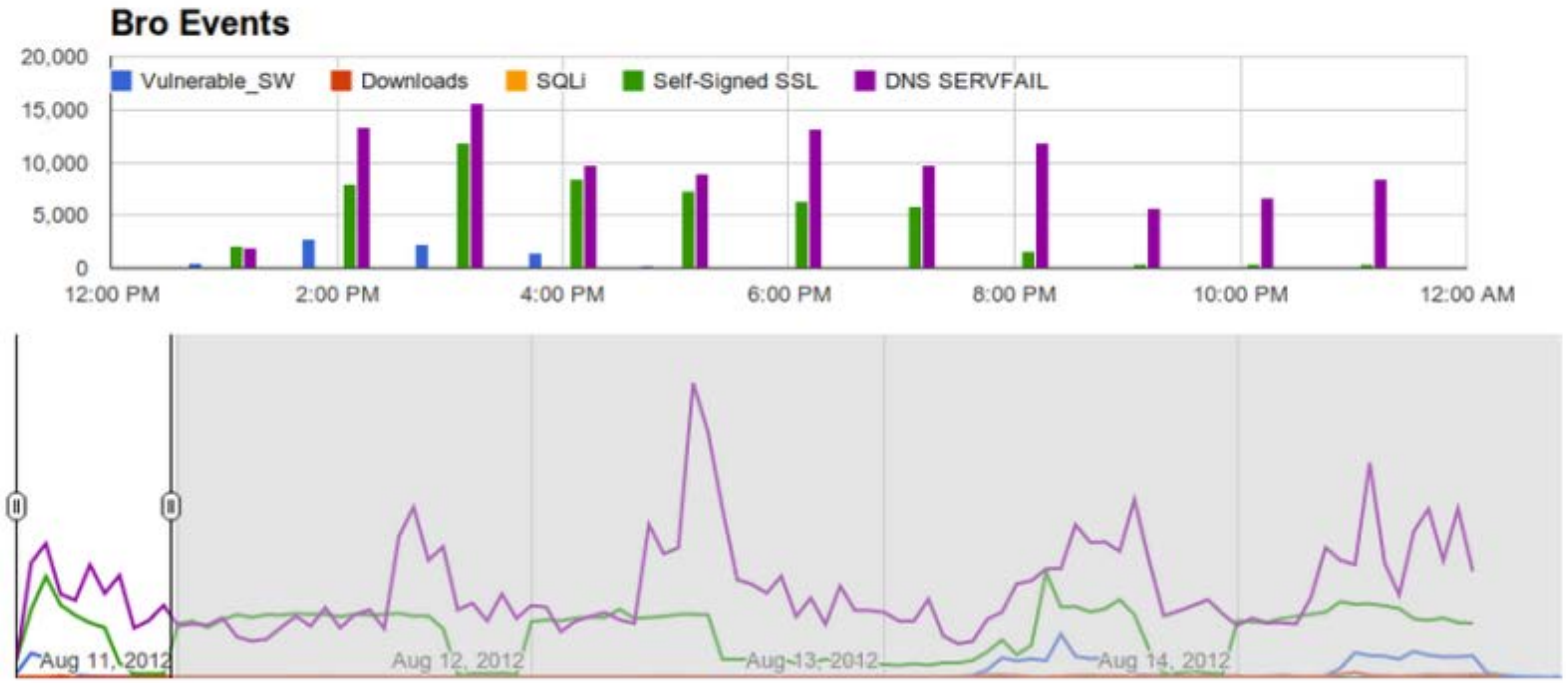
Distributed Deployment

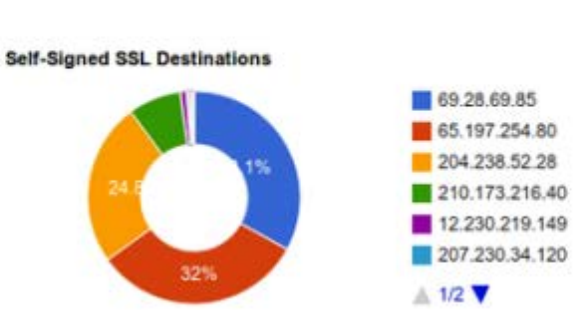


ELSA


ELSA
Admin
Query class=BRO_HTTP
From 2012-08-04 10:47:04
To
Add Term
user_agent
Index
class=BRO_HTTP (602) [Grouped by user_agent]
Result Options...
Count
Value
446 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
54 -
14 Bob's Evil Clown C&C Agent
14 NSISDL/1.2 (Mozilla)
10 Mozilla/4.0 (compatible; UPnP/1.0; Windows NT/5.1)
10 Mozilla/4.0 (compatible; UPnP/1.0; Windows 9x)
8 Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)
8 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)ver49
8 Mozilla/4.0 (compatible; MSIE 6.0; Win32)
3 uri
3 string
2 Windows-Update-Agent
2 BTWebClient/2220
2 BTWebClient/6120
1 curl/7.22.0 (x86_64-pc-linux-gnu) libcurl/7.22.0 OpenSSL/1.0.1 zlib/1.2.3.4 libidn/1.23 librtmp/2.3
1 Firefox 1

Bro IDS





subject
emailAddress=admin@wiredsolar.net,CN=secure.wiredsolar.net,OU=IT,O=Wired Solar,L=Flagler,ST=Florida,C=US
CN=rsip.monitoredsecurity.com,OU=IT Security,O=Symantec Corporation,L=Northern
emailAddress=dhoover@centonline.com,CN=Dean Hoover,OU=Network Admin,O=Ce Berlin,ST=Wisconsin,C=US
ST=Tokyo,OU=Remote Service,O=RICOH COMPANY\,LTD.,L=Aoyama,C=JP,CN=G
CN=mcs1hkg.live.citrixonline.com,OU=Operations,O=Citrix Online LLC,L=Fort Lauder
C=CA
C=US,CN=mail.tytix.com
CN=TrustedSourceServer_IMQA01

Where do we go now?

http://securityonion.blogspot.com

Updates are announced here and it also has the following links:

- Download/Install
- FAQ
- Mailing Lists
- IRC #securityonion on irc.freenode.net