Network Security Monitoring in Minutes

Doug Burks

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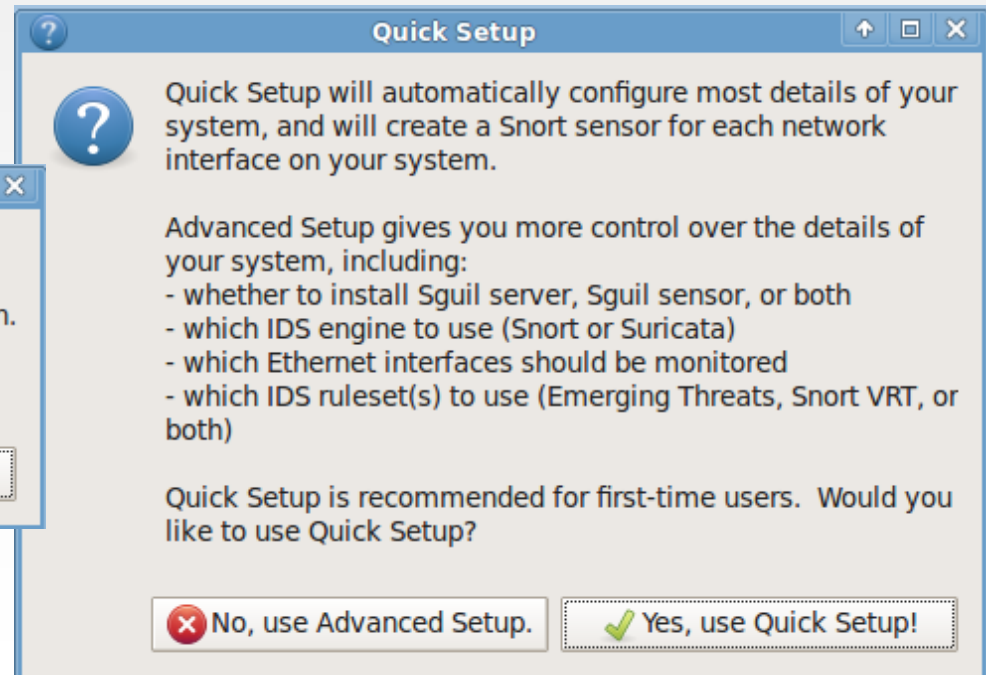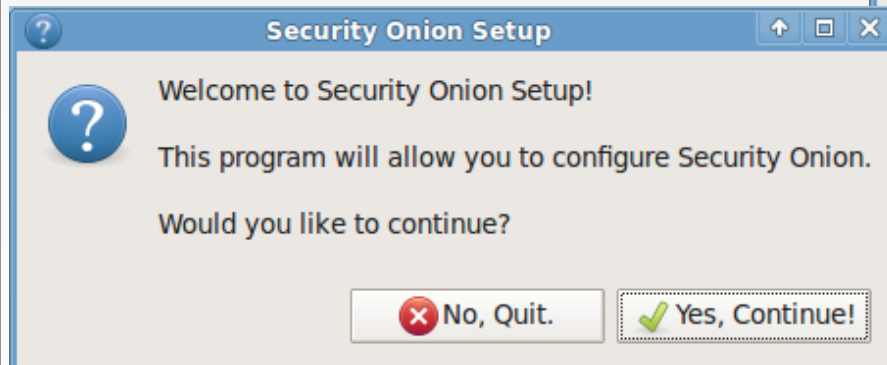
Doug Burks is:

- 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

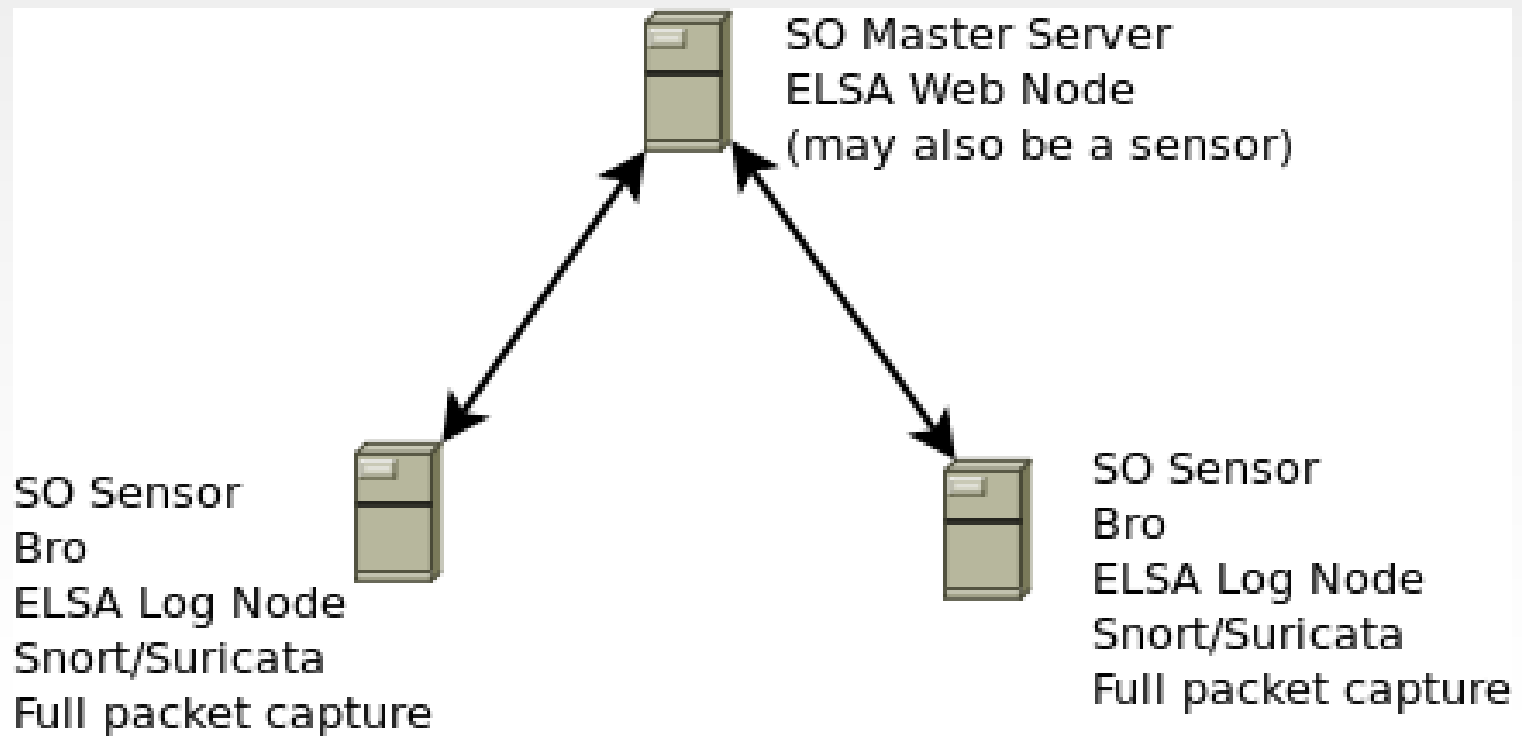Setup wizard takes less than 5 minutes!

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

SO Master Server
ELSA Web Node
(may also be a sensor)

SO Sensor
Bro
ELSA Log Node
Snort/Suricata
Full packet capture

SO Sensor
Bro
ELSA Log Node
Snort/Suricata
Full packet capture

ELSA

Bro IDS

Bro Events

Legend: ■ Vulnerable_SW ■ Downloads ■ SQLi ■ Self-Signed SSL ■ DNS SERVFAIL

X-axis: 12:00 PM, 2:00 PM, 4:00 PM, 6:00 PM, 8:00 PM, 10:00 PM, 12:00 AM
Y-axis: 0, 5,000, 10,000, 15,000, 20,000

Aug 11, 2012 · Aug 12, 2012 · Aug 13, 2012 · Aug 14, 2012

Self-Signed SSL Destinations
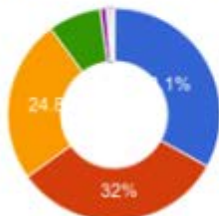
- ■ 69.28.69.85
- ■ 65.197.254.80
- ■ 204.238.52.28
- ■ 210.173.216.40
- ■ 12.230.219.149
- ■ 207.230.34.120

1% ... 24.5 ... 32%

▲ 1/2 ▼

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