Security Onion

https://i.ytimg.com/vi/n8y2_YIK1hM/maxresdefault.jpg

Combining Suricata and Host Data with Security Onion

Doug Burks @dougburks @securityonion

Security Onion Solutions

What is **Security Onion**?

- Free and Open Source Platform
- IDS, NSM, ESM, DFIR, Threat Hunting
- Network and Endpoint Visibility

Doug Burks @dougburks @securityonion

Security Onion Solutions

A Brief History: **2008**

Doug Burks @dougburks @securityonion

Security Onion Solutions

A Brief History: **2009**

THURSDAY, JUNE 4, 2009

The Security Onion LiveCD is now available!

The Security Onion LiveCD is now available! You can download it from the following location:
http://distro.ibiblio.org/pub/linux/distributions/security-onion/

Doug Burks @dougburks @securityonion

Security Onion Solutions

A Brief History: **2010 – Suricata**

TUESDAY, OCTOBER 12, 2010

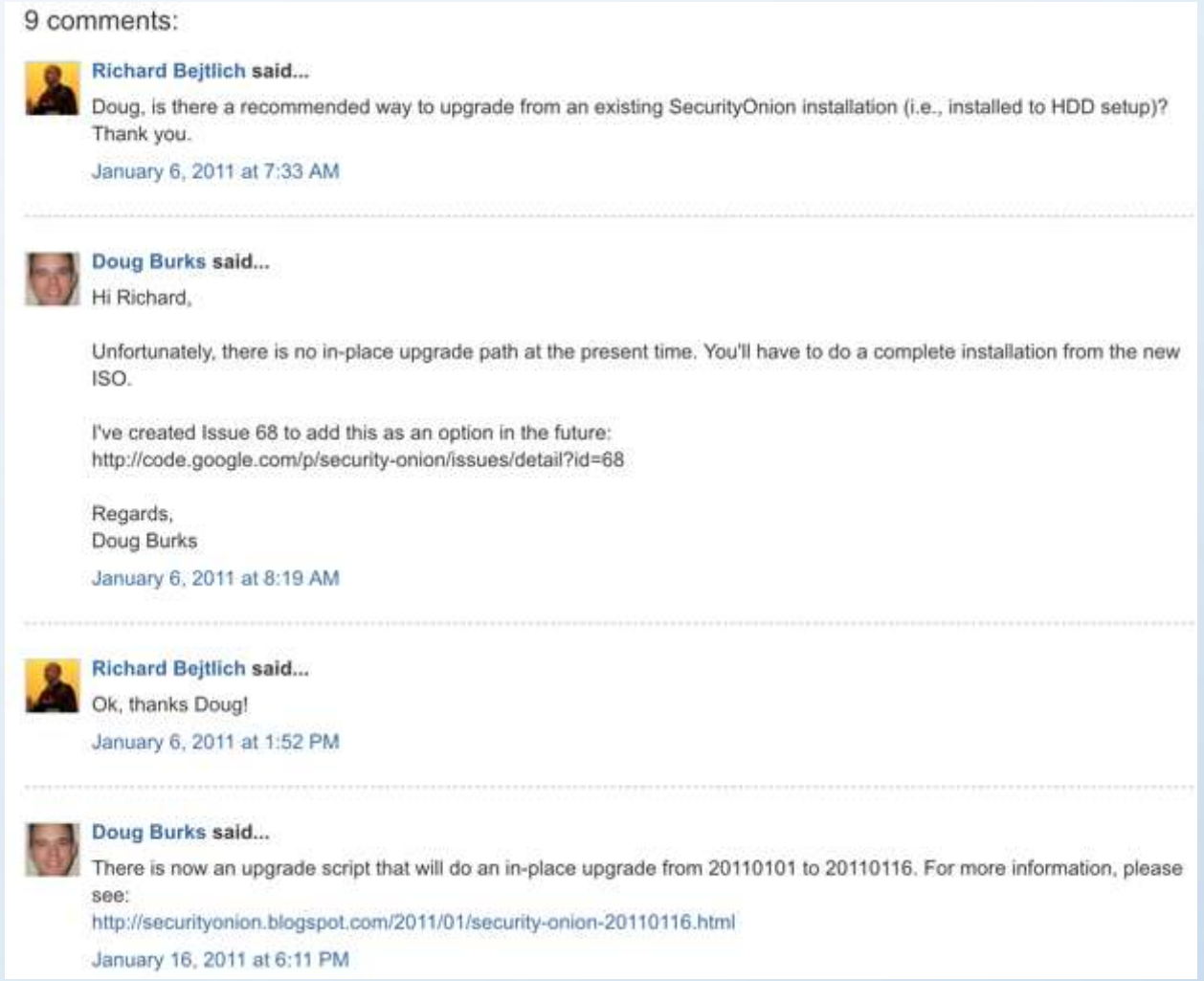
Security Onion Live: 20101010 Edition!

Security Onion Live 20101010 is now available! Thanks to Matt Jonkman and Emerging Threats for hosting!

Doug Burks @dougburks @securityonion

Security Onion Solutions

A Brief History: **2011 - In-place Upgrades**



9 comments:

Richard Bejtlich said...

Doug, is there a recommended way to upgrade from an existing SecurityOnion installation (i.e., installed to HDD setup)? Thank you.

January 6, 2011 at 7:33 AM

Doug Burks said...

Hi Richard,

Unfortunately, there is no in-place upgrade path at the present time. You'll have to do a complete installation from the new ISO.

I've created Issue 68 to add this as an option in the future:
http://code.google.com/p/security-onion/issues/detail?id=68

Regards,
Doug Burks

January 6, 2011 at 8:19 AM

Richard Bejtlich said...

Ok, thanks Doug!

January 6, 2011 at 1:52 PM

Doug Burks said...

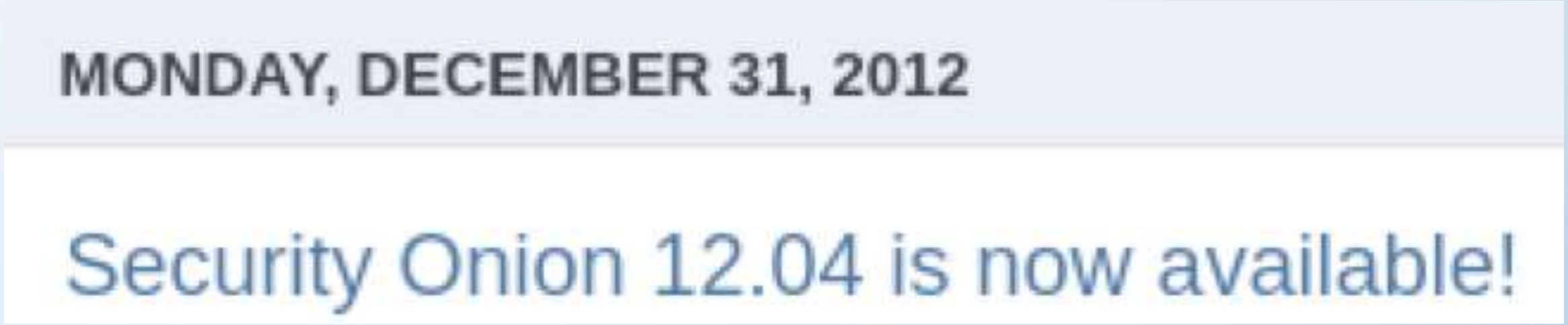
There is now an upgrade script that will do an in-place upgrade from 20110101 to 20110116. For more information, please see:
http://securityonion.blogspot.com/2011/01/security-onion-20110116.html

January 16, 2011 at 6:11 PM

Doug Burks @dougburks @securityonion

Security Onion Solutions

A Brief History: **2012 – Suricata compiled with PF_RING**



Doug Burks @dougburks @securityonion

Security Onion Solutions

A Brief History: **2018**

MONDAY, NOVEMBER 12, 2018

Suricata 4.1.0 now available for Security Onion!

Suricata 4.1.0 was released recently:
https://suricata-ids.org/2018/11/06/suricata-4-1-released/

We've packaged Suricata 4.1.0 and the following packages are now available:
securityonion-suricata - 4.1.0-1ubuntu1securityonion1 (16.04)
securityonion-suricata - 4.1.0-1ubuntu1securityonion2 (14.04)

These packages should resolve the following issue:

Issue 1361: Suricata 4.1.0
https://github.com/Security-Onion-Solutions/security-onion/issues/1361

```
doug@securityonion:~$ suricata -V
This is Suricata version 4.1.0 RELEASE
```

Suricata 4.1.0

Doug Burks @dougburks @securityonion

Security Onion Solutions

Flexible Platform

- Download our **ISO image**
  (help us reach 700,000 downloads!)

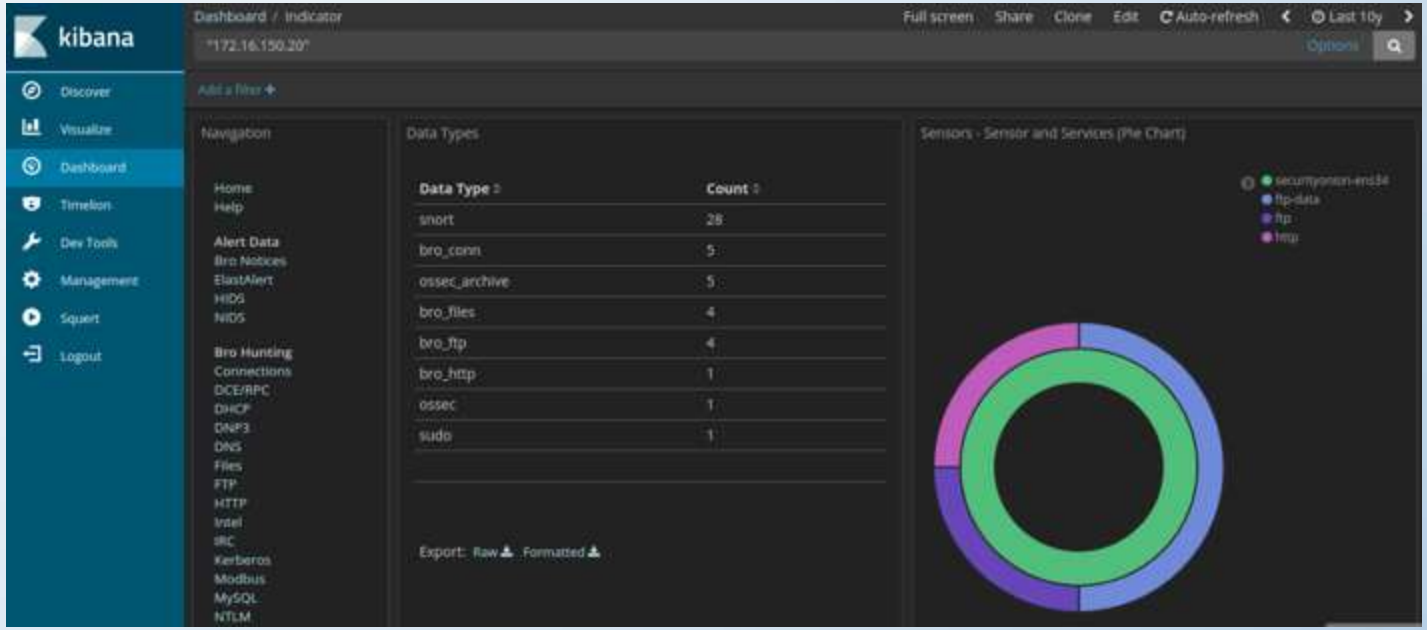
  OR

- install our packages on top of **Ubuntu 16.04**

Security Onion Solutions

Slicing and Dicing Logs

- Elasticsearch
- Logstash
- Kibana



Security Onion Solutions

Doug Burks @dougburks @securityonion

We've got great network telemetry, but what about the endpoints?

- What **process** actually generated those network connections?
- **What else did that process do** besides those network connections?

https://upload.wikimedia.org/wikipedia/commons/a/ac/Iceberg.jpg

Security Onion Solutions

Doug Burks @dougburks @securityonion

Endpoint Telemetry

- Beats
- Wazuh HIDS
- Sysmon
- autoruns
- osquery

Doug Burks @dougburks @securityonion

Security Onion Solutions

Wazuh HIDS

- Wazuh **Agent**:
  - log collection
  - encrypted log transport
  - file integrity checking
  - rootkit detection

- Wazuh **Server** analyzes logs and generates alerts

Security Onion Solutions

Wazuh agent installation

- run **so-allow** so agent can connect to Wazuh server
- create agent key on Wazuh server
- export agent key
- install MSI on endpoint
- import agent key
- Yes, this process can be automated!

Security Onion Solutions

Sysmon

- Comprehensive host logging
- Correlate network connections to the process that generated them

Security Onion Solutions

Sysmon

- Download Sysmon from:
  https://docs.microsoft.com/en-us/sysinternals/downloads/Sysmon
- Install Sysmon:
  sysmon -i -accepteula

Doug Burks @dougburks @securityonion

Security Onion Solutions

Sysmon

- @SwiftOnSecurity has a great sysmon config:
  https://github.com/SwiftOnSecurity/sysmon-config
- Load config:
  sysmon -c sysmonconfig-export.xml

Security Onion Solutions

Autoruns

- Look for persistence mechanisms!
- Download Autoruns from:
  https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns
- Configure it to run on a periodic basis

Doug Burks @dougburks @securityonion

Security Onion Solutions

Wazuh – Sysmon - Autoruns

- Configure Wazuh to monitor **Microsoft-Windows-Sysmon/Operational**
- Configure Wazuh to monitor **autoruns log**

Doug Burks @dougburks @securityonion

Security Onion Solutions

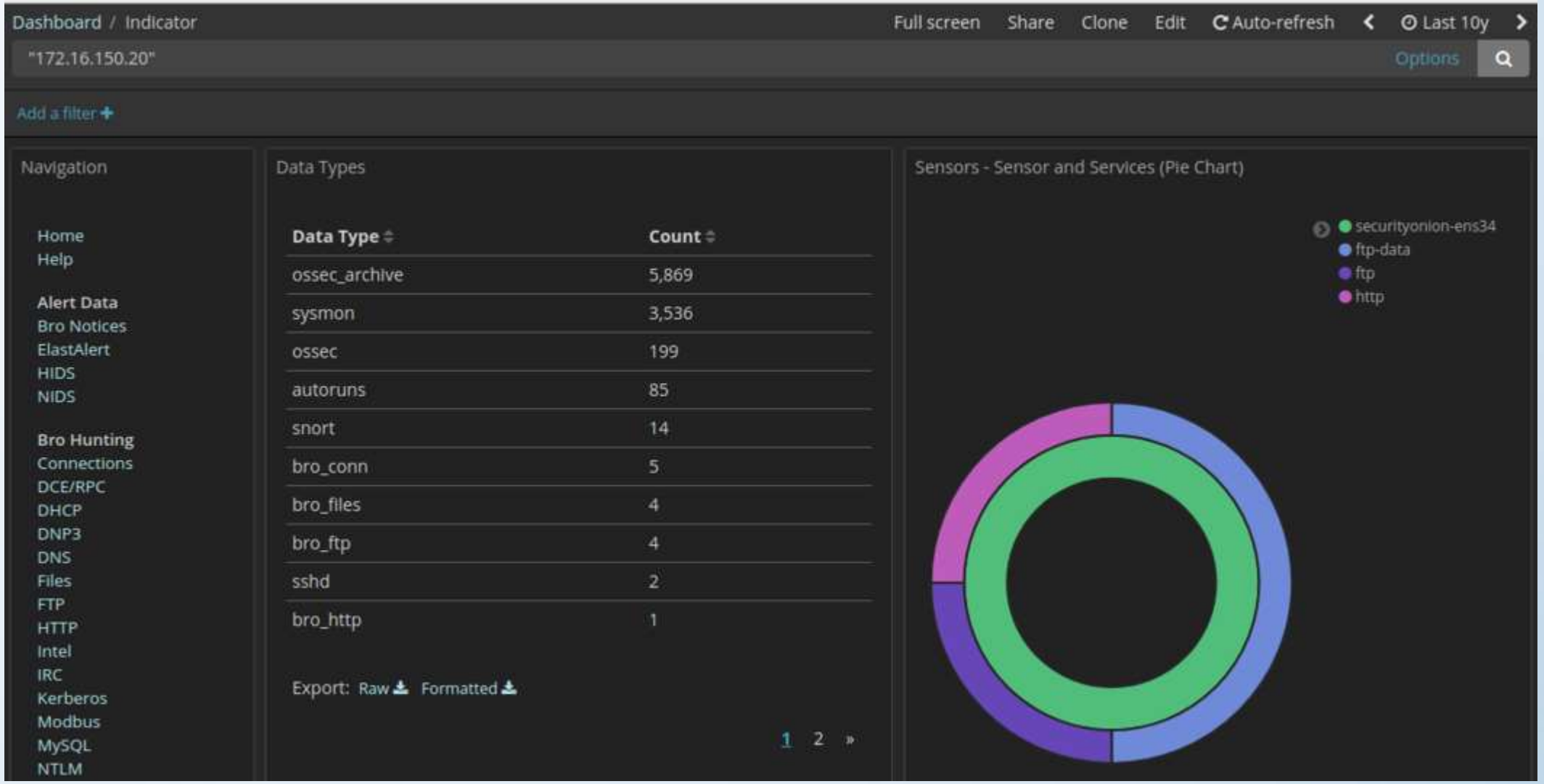
Use Cases

- Production Deployment – Standalone
- Production Deployment – Distributed
  - Master Server
  - Multiple Forward Nodes
  - Multiple Storage Nodes
- Small Forensics VM
  import pcaps and/or logs

Security Onion Solutions

Case Study: Real World Data Breach

Doug Burks @dougburks @securityonion



Doug Burks @dougburks @securityonion

Security Onion Solutions

NIDS - Alerts

alert.keyword: Descending	Count
ET INFO SUSPICIOUS Dotted Quad Host MZ Response	6
ET POLICY PE EXE or DLL Windows file download HTTP	6
ET INFO Executable Download from dotted-quad Host	1
ET POLICY SUSPICIOUS *.doc.exe in HTTP URL	1

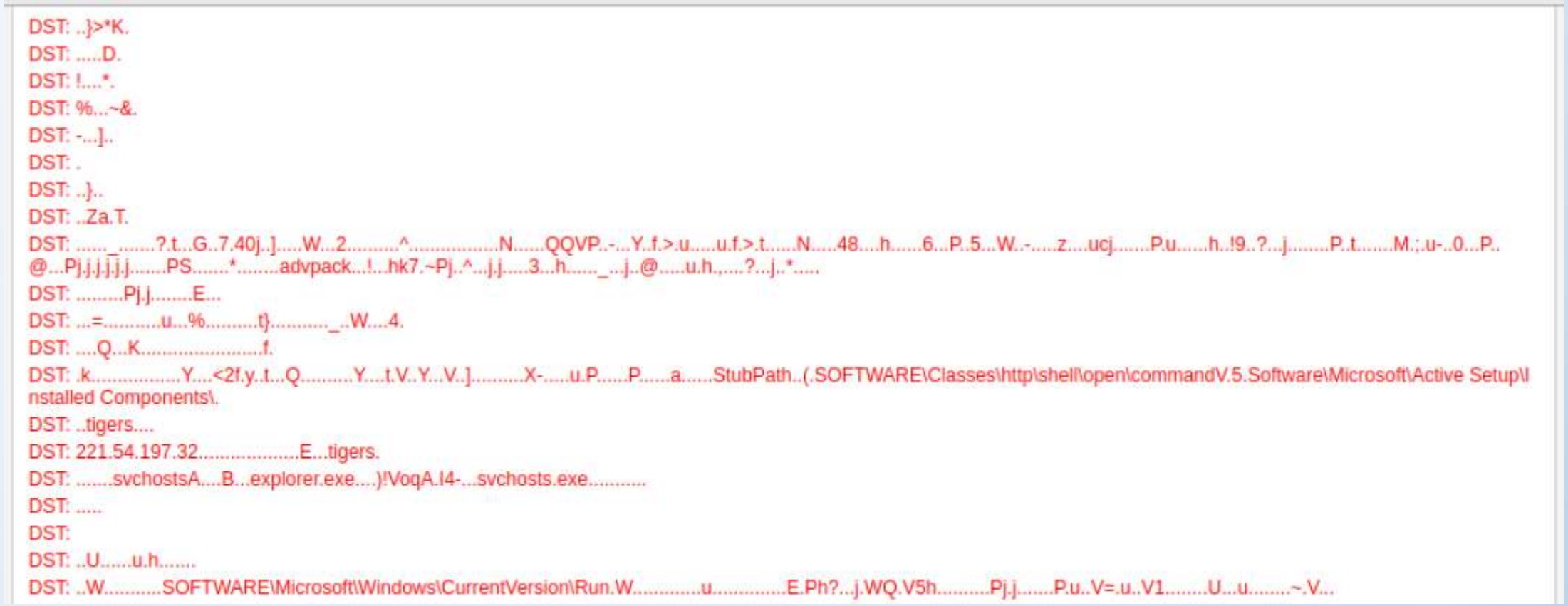
Security Onion Solutions

close

172.16.150.20:1294_66.32.119.38:80-6-841234777.pcap

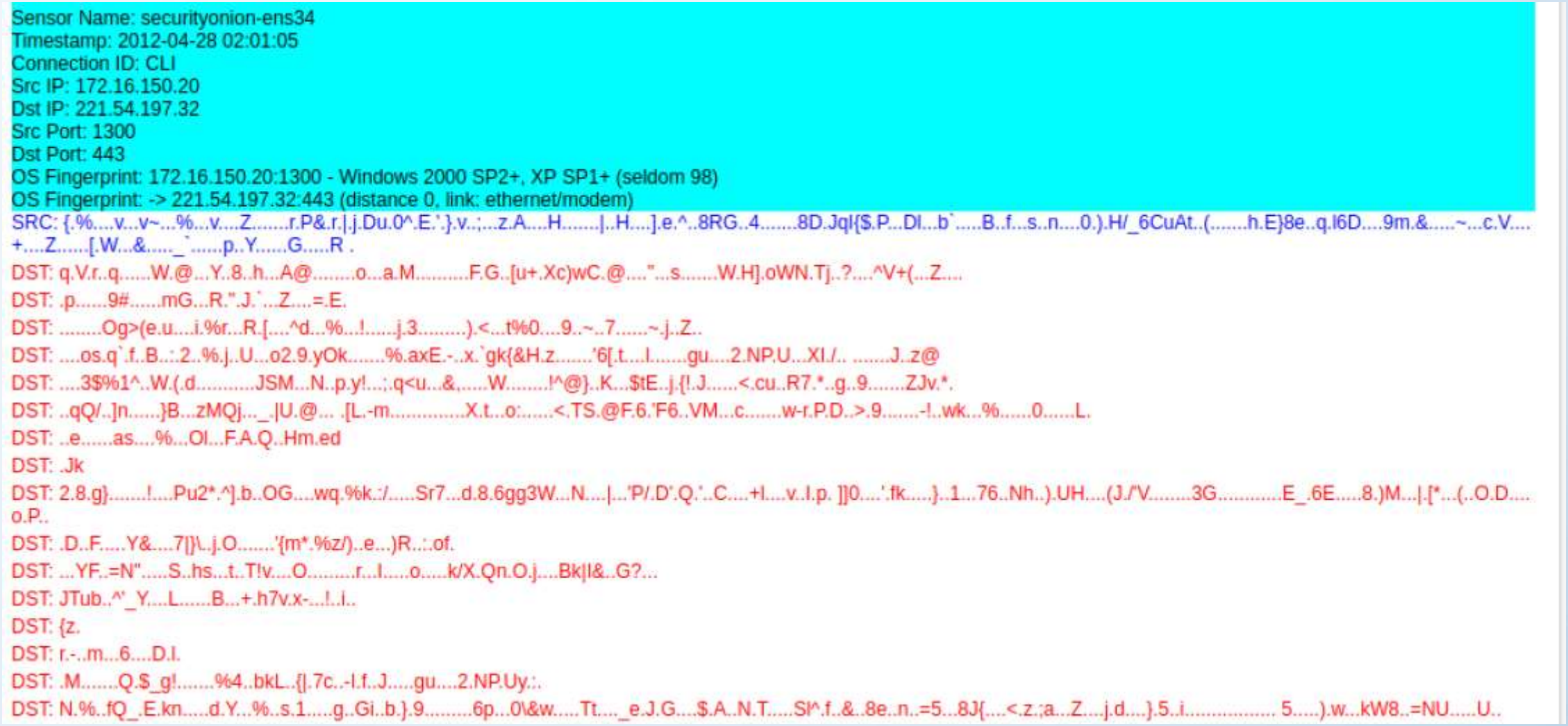
```
Log entry:
21:02:58 pid(17409) Alert Received: 0 2 bad-unknown securityonion-ens34 {2012-04-28 02:00:59} 3 16 {ET POLICY SUSPICIOUS *.doc.exe in HTTP URL} 172.16.150.20 66.3
2.119.38 6 1294 80 1 2013475 2 2 2

IDS rule:
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET POLICY SUSPICIOUS *.doc.exe in HTTP URL"; flow:to_server,established; content:".doc.exe"; http_uri; nocas
e; classtype:bad-unknown; sid:2013475; rev:2; metadata:created_at 2011_08_26, updated_at 2011_08_26;)

Sensor Name: securityonion-ens34
Timestamp: 2012-04-28 02:00:59
Connection ID: CLI
Src IP: 172.16.150.20
Dst IP: 66.32.119.38
Src Port: 1294
Dst Port: 80
OS Fingerprint: 172.16.150.20:1294 - Windows 2000 SP2+, XP SP1+ (seldom 98)
OS Fingerprint: -> 66.32.119.38:80 (distance 0, link: ethernet/modem)
SRC: GET /tigers/BrandonInge/Diagnostics/swing-mechanics.doc.exe HTTP/1.1
SRC: Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*
SRC: Accept-Language: en-us
SRC: Accept-Encoding: gzip, deflate
SRC: User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
SRC: Host: 66.32.119.38
SRC: Connection: Keep-Alive
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Date: Fri, 27 Apr 2012 17:40:31 GMT
DST: Server: Apache/2.2.16 (Ubuntu)
DST: Last-Modified: Sat, 14 Apr 2012 09:34:10 GMT
DST: ETag: "42d3b-2000-4bda04a8ed053"
DST: Accept-Ranges: bytes
DST: Content-Length: 8192
DST: Keep-Alive: timeout=15, max=100
DST: Connection: Keep-Alive
DST: Content-Type: application/x-msdos-program
DST:
DST: MZ.....@.....!..L.!This program cannot be run in DOS mode.
```


Security Onion Solutions



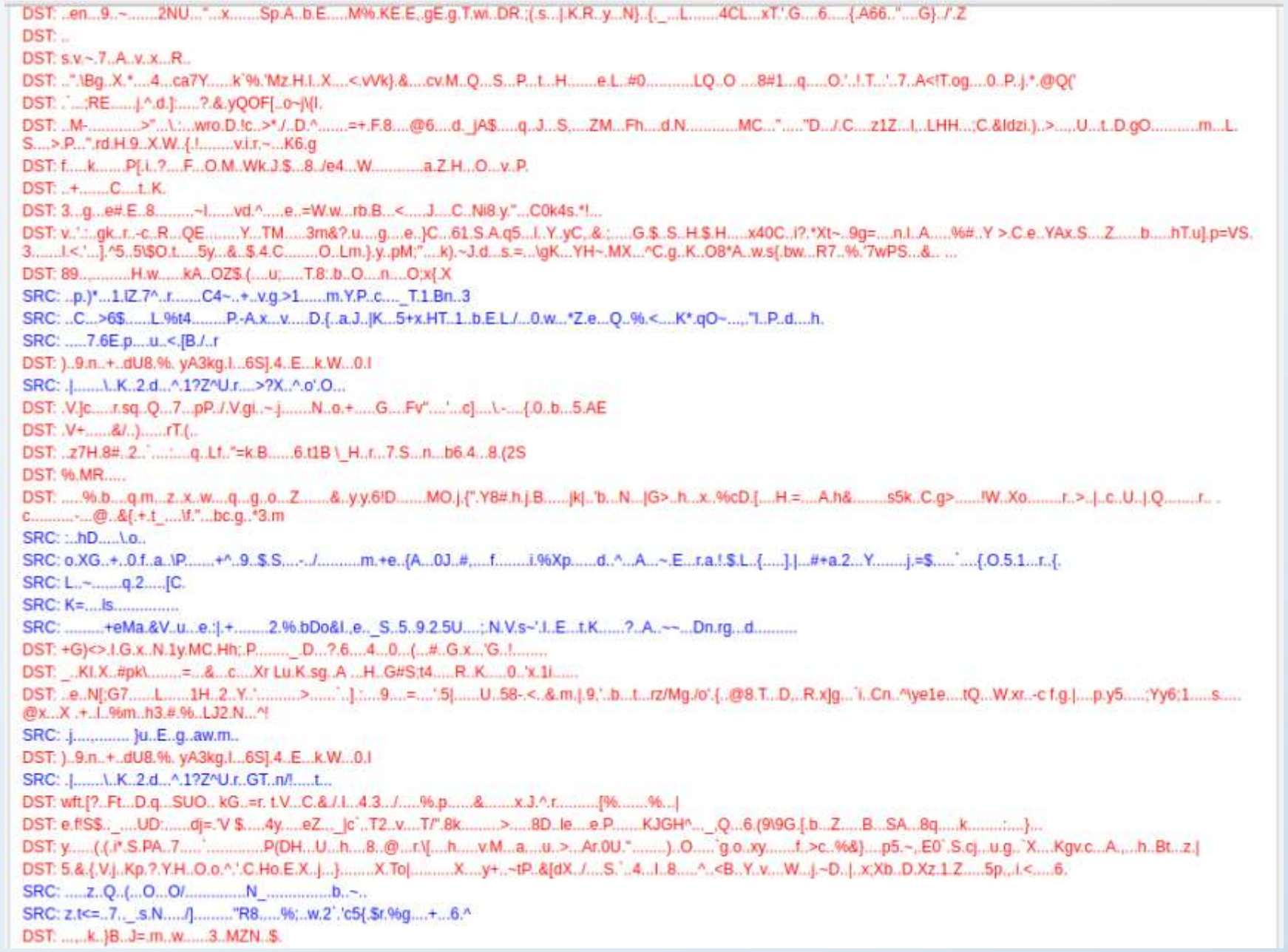
Doug Burks @dougburks @securityonion

Security Onion Solutions



Doug Burks @dougburks @securityonion

Security Onion Solutions



Doug Burks @dougburks @securityonion

Security Onion Solutions

```
Src IP: 172.16.150.20
Dst IP: 66.32.119.38
Src Port: 1367
Dst Port: 21
OS Fingerprint: 172.16.150.20:1367 - Windows 2000 SP2+, XP SP1+ (seldom 98)
OS Fingerprint: -> 66.32.119.38:21 (distance 0, link: ethernet/modem)
DST: 220 (vsFTPd 2.3.0)
DST:
SRC: USER jack
SRC:
DST: 331 Please specify the password.
DST:
SRC: PASS 2awes0me
SRC:
DST: 230 Login successful.
DST:
SRC: TYPE I
SRC:
DST: 200 Switching to Binary mode.
DST:
SRC: PORT 172,16,150,20,5,89
SRC:
DST: 200 PORT command successful. Consider using PASV.
DST:
SRC: STOR 1.txt
SRC:
DST: 150 Ok to send data.
DST:
DST: 226 Transfer complete.
DST:
SRC: TYPE A
SRC:
DST: 200 Switching to ASCII mode.
DST:
SRC: PORT 172,16,150,20,5,90
SRC:
DST: 200 PORT command successful. Consider using PASV.
DST:
SRC: STOR 2.txt
SRC:
DST: 150 Ok to send data.
DST:
DST: 226 Transfer complete.
```


Security Onion Solutions

```
Sensor Name: securityonion-ens34
Timestamp: 2012-04-28 02:13:23
Connection ID: CLI
Src IP: 172.16.150.20
Dst IP: 66.32.119.38
Src Port: 1370
Dst Port: 20
OS Fingerprint: 66.32.119.38:20 - UNKNOWN [S4:63:1:60:M1460,S,T,N,W4:.:?:?] (up: 71 hrs)
OS Fingerprint: -> 172.16.150.20:1370 (link: ethernet/modem)
SRC: gsecdump v0.7 by Johannes Gumbel (johannes.gumbel@truesec.se)
SRC:
SRC: usage: gsecdump [options]
SRC:
SRC:
SRC:
SRC: options:
SRC: -a [ --dump_all ] dump all secrets
SRC: -s [ --dump_hashes ] dump hashes from SAM/AD
SRC: -l [ --dump_lsa ] dump lsa secrets
SRC: -u [ --dump_usedhashes ] dump hashes from active logon sessions
SRC: -w [ --dump_wireless ] dump microsoft wireless connections
SRC: -h [ --help ] show help
SRC: -S [ --system ] run as localsystem
SRC:
```

Doug Burks @dougburks @securityonion

Security Onion Solutions

```
Sensor Name: securityonion-ens34
Timestamp: 2012-04-28 02:13:11
Connection ID: CLI
Src IP: 172.16.150.20
Dst IP: 66.32.119.38
Src Port: 1369
Dst Port: 20
OS Fingerprint: 66.32.119.38:20 - UNKNOWN [S4:63:1:60:M1460,S,T,N,W4:.:?:?] (up: 71 hrs)
OS Fingerprint: -> 172.16.150.20:1369 (link: ethernet/modem)
SRC: Rar!.....s..
```

Doug Burks @dougburks @securityonion

Security Onion Solutions

OSSEC Alerts - Event Summary

Description	Host	Username
Sysmon - Suspicious Process - svchost.exe	securityonion	DESKTOP-SV8HSSB\Doug Burks

Doug Burks @dougburks @securityonion

Security Onion Solutions

```
2018 Nov 13 15:24:29 WinEvtLog: Microsoft-Windows-Sysmon/Operational: INFORMATION(3): Microsoft-Windows-Sysmon: SYSTE
M: NT AUTHORITY: DESKTOP-SV8HSSB: Network connection detected:  RuleName:   UtcTime: 2018-11-13 20:24:31.067  ProcessG
uid: {DE1D5306-32F2-5BEB-0000-00100C512E01}  ProcessId: 6852  Image: C:\Users\Doug Burks\Downloads\App\Firefox64\firef
ox.exe  User: DESKTOP-SV8HSSB\Doug Burks  Protocol: tcp  Initiated: true  SourceIsIpv6: false  SourceIp: 172.16.150.20
  SourceHostname: DESKTOP-SV8HSSB  SourcePort: 51222  SourcePortName:   DestinationIsIpv6: false  DestinationIp: 54.19
2.22.93  DestinationHostname: server-54-192-22-93.dfw54.r.cloudfront.net  DestinationPort: 443  DestinationPortName: h
ttps
```

```
gateway
```

```
1542140670.349217
```

```
C:\Users\Doug Burks\Downloads\App\Firefox64\firefox.exe
```

```
172.16.150.20, 54.192.22.93
```

Doug Burks @dougburks @securityonion

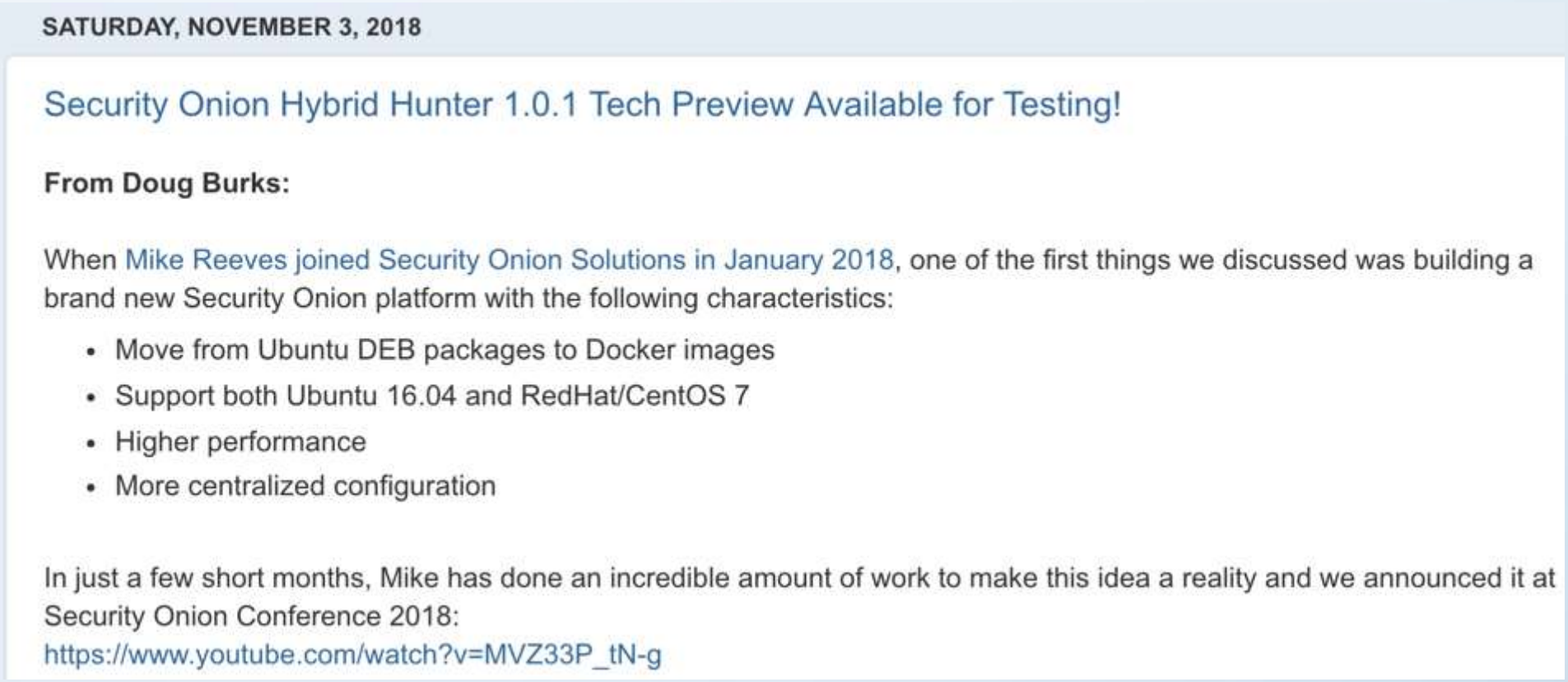
Security Onion Solutions

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
11/13/2018 15:28:47
autoruns
⚠ AR-LOG|win001|11/13/2018 15:28:47||HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run|svchost|enabled|Logon|System-wide||||File not found: c:\users\doug\Downloads\svchost.exe.exe||c:\users\doug\Downloads\svchost.exe|||||
gateway
win001
1542140994.352479
\logs\ar-normalized.log
0.006
⚠ securityonion
c:\users\doug\Downloads\svchost.exe
{"timestamp":"2018-11-13T20:29:54.988+0000","agent":{"id":"001","name":"win001","ip":"172.16.150.20"},"manager":{"name":"securityonion"},"id":"1542140994.352479","full_log":"AR-LOG|win001|11/13/2018 15:28:47||HKLM\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run|svchost|enabled|Logon|System-wide||||File not found: c:\\users\\doug\\Downloads\\svchost.exe.exe||c:\\users\\doug\\Downloads\\svchost.exe||||||","decoder":{},"location":"\\logs\\ar-normalized.log"}

Doug Burks @dougburks @securityonion

Security Onion Solutions

New Platform! **Hybrid Hunter**



SATURDAY, NOVEMBER 3, 2018

Security Onion Hybrid Hunter 1.0.1 Tech Preview Available for Testing!

From Doug Burks:

When Mike Reeves joined Security Onion Solutions in January 2018, one of the first things we discussed was building a brand new Security Onion platform with the following characteristics:

- Move from Ubuntu DEB packages to Docker images
- Support both Ubuntu 16.04 and RedHat/CentOS 7
- Higher performance
- More centralized configuration

In just a few short months, Mike has done an incredible amount of work to make this idea a reality and we announced it at Security Onion Conference 2018:
https://www.youtube.com/watch?v=MVZ33P_tN-g

PF_RING → AF_PACKET

Doug Burks @dougburks @securityonion

Security Onion Solutions

Just Released! **Hybrid Hunter 1.0.3**

- Includes **Suricata 4.1**
- Asks if you want to enable Suricata protocol logging

Doug Burks @dougburks @securityonion

Security Onion Solutions

More osquery integration coming!

Security Onion Conference 2018: Integrating Osquery into Security Onion by Josh Brower

Doug Burks @dougburks @securityonion

Security Onion Solutions

How do I get Security Onion?

- Free download!
  https://securityonion.net
- Try new Hybrid Hunter!
  https://blog.securityonion.net

https://securityonionsolutions.com

Doug Burks @dougburks @securityonion

Security Onion Solutions