

# Security@nion



Combining Suricata and Host Data with Security Onion

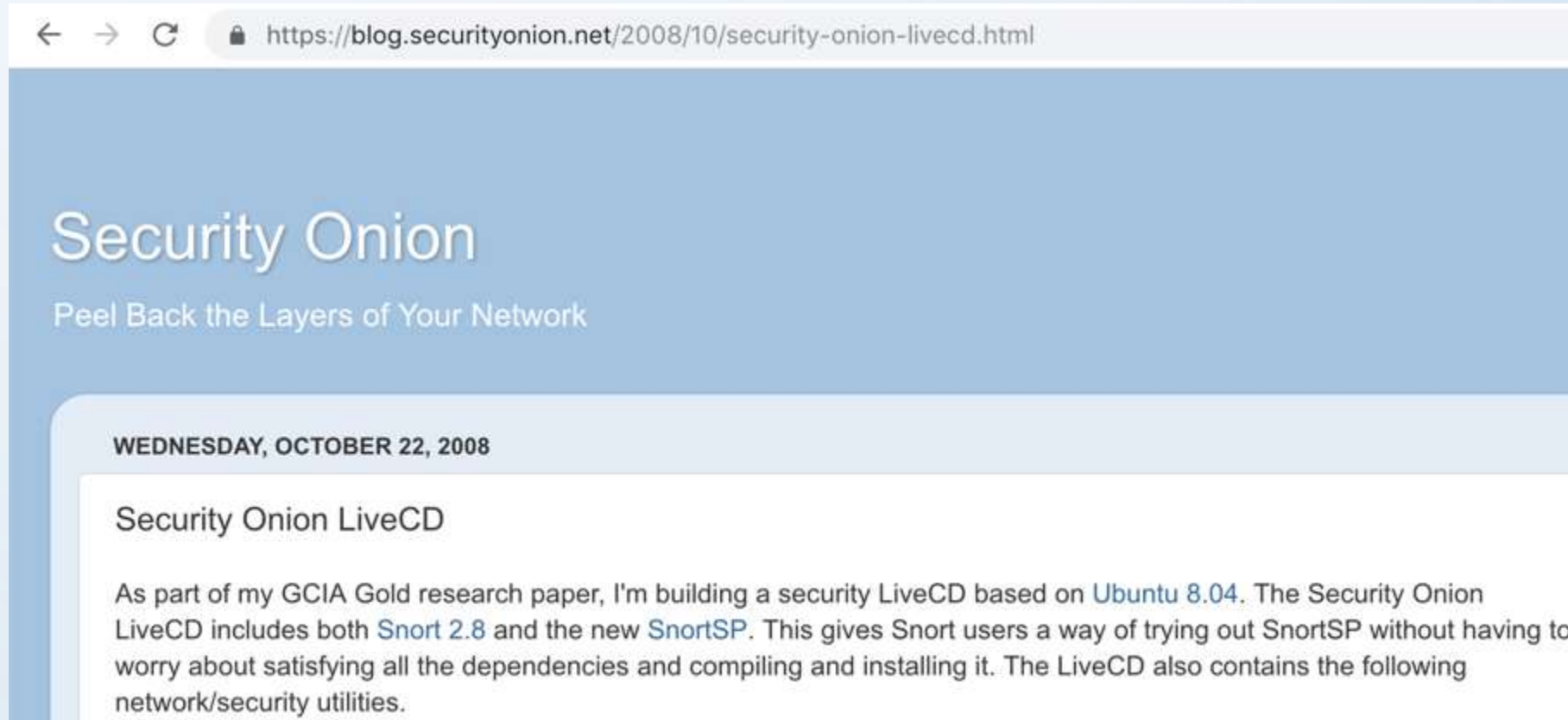
Doug Burks @dougburks @securityonion

Security  
nion  
Solutions

# What is **Security Onion**?

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

# A Brief History: 2008



Doug Burks @dougburks @securityonion



# 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/>

# 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




# 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



# A Brief History: 2012 – Suricata compiled with PF\_RING

MONDAY, DECEMBER 31, 2012

Security Onion 12.04 is now available!

Doug Burks @dougburks @securityonion



# 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





# Flexible Platform

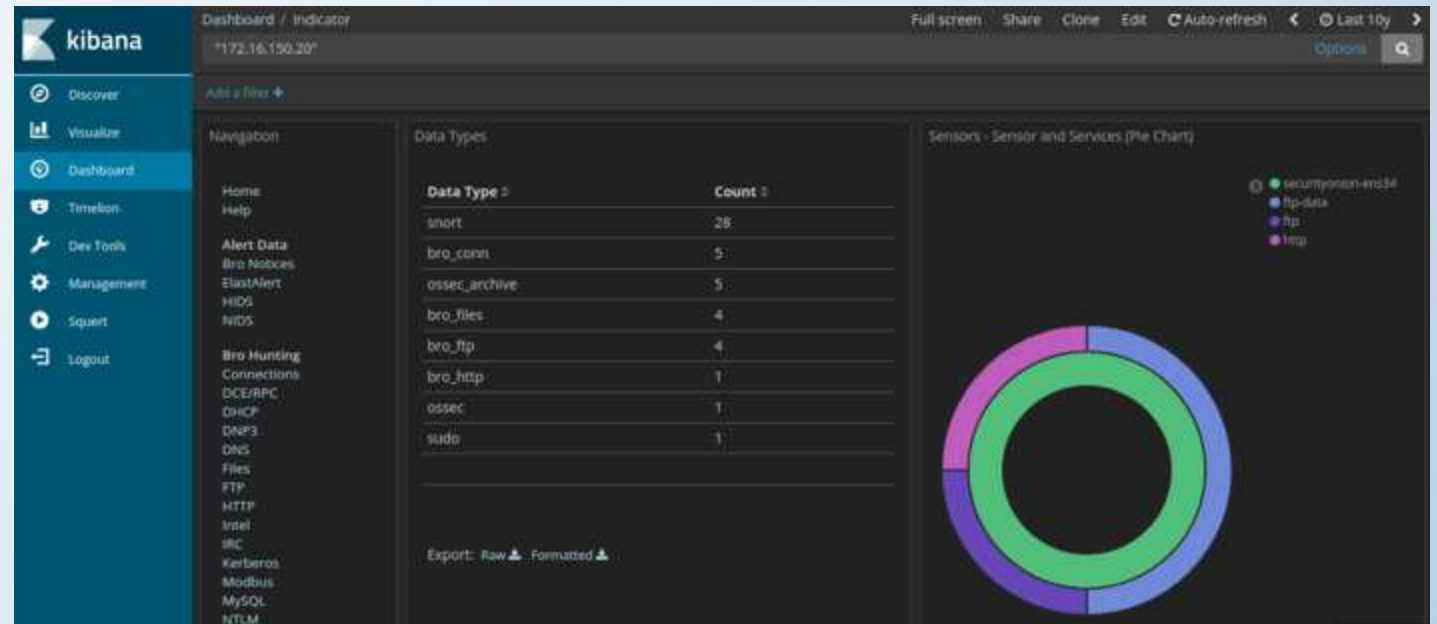
- Download our **ISO image**  
(help us reach 700,000 downloads!)

OR

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

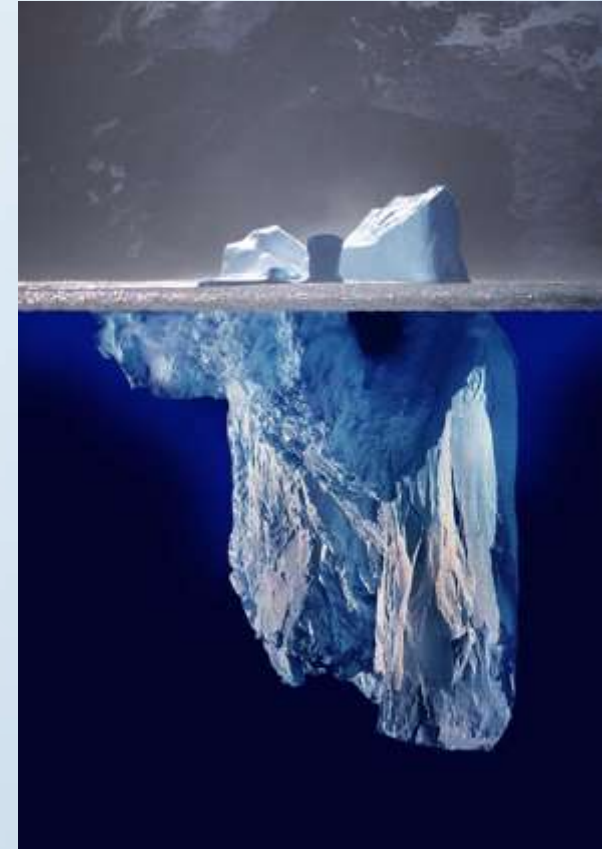
# Slicing and Dicing Logs

- Elasticsearch
- Logstash
- Kibana



# 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>

# Endpoint Telemetry

- Beats
- Wazuh HIDS
- Sysmon
- autoruns
- osquery

# Wazuh HIDS

- **Wazuh Agent:**
  - log collection
  - encrypted log transport
  - file integrity checking
  - rootkit detection
- **Wazuh Server** analyzes logs and generates alerts

# 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!

# Sysmon

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

# Sysmon

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



# Sysmon

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

# 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

# Wazuh – Sysmon - Autoruns

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

# Use Cases

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

# Case Study: Real World Data Breach

Doug Burks @dougburks @securityonion



Dashboard / Indicator Full screen Share Clone Edit Auto-refresh Last 10y

"172.16.150.20" Options

Add a filter +

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

Data Types

Data Type	Count
ossec_archive	5,869
sysmon	3,536
ossec	199
autoruns	85
snort	14
bro_conn	5
bro_files	4
bro_ftp	4
sshd	2
bro_http	1

Export: Raw Formatted

1 2 »

Sensors - Sensor and Services (Pie Chart)

- securityonion-ens34
- ftp-data
- ftp
- http

Doug Burks @dougburks @securityonion



## 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

---

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 66.32.119.38 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; nocase; 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.....@.....!..!This program cannot be run in DOS mode.



```
DST: .}>*K.
DST: .....D.
DST: !...*.
DST: %...~&.
DST: -...].
DST: .
DST: .}.
DST: ..Za.T.
DST: .....?t..G..7.40j..].....W...2.....^.....N.....QQVP.-...Y.f.>.u.....u.f.>.t.....N....48...h.....6...P..5...W.-...z...ucj.....P.u.....h..!9..?.j.....P.t.....M.;u-.0...P..
@...Pj.j.j.j.j.....PS.....*.....advpack...!..hk7..~Pj..^..j.j.....3..h....._..j..@.....u.h,....?..j..*.....
DST: .....Pj.j.....E...
DST: ...=.....u...%.....t}....._..W...4.
DST: ...Q...K.....f.
DST: .k.....Y...<2f.y.t...Q.....Y...t.V..Y..V..].....X-...u.P.....P.....a.....StubPath.(.SOFTWARE\Classes\http\shell\open\commandV.5.Software\Microsoft\Active Setup\I
nstalled Components\).
DST: ..tigers....
DST: 221.54.197.32.....E...tigers.
DST: .....svchostsA....B...explorer.exe....)!VoqA.I4-...svchosts.exe.....
DST: .....
DST:
DST: ..U.....u.h.....
DST: ..W.....SOFTWARE\Microsoft\Windows\CurrentVersion\Run.W.....u.....E.Ph?...j.WQ.V5h.....Pj.j.....P.u..V=u.V1.....U...u.....~.V...
```

Sensor Name: securityonion-ens34

Timestamp: 2012-04-28 02:01:05

Connection ID: CLI

Src IP: 172.16.150.20

Dst IP: 221.54.197.32

Src Port: 1300

Dst Port: 443

OS Fingerprint: 172.16.150.20:1300 - Windows 2000 SP2+, XP SP1+ (seldom 98)

OS Fingerprint -> 221.54.197.32:443 (distance 0, link: ethernet/modem)

SRC: {.%...v...v~...%...v...Z.....rP&r{j.Du.0^E.'}v.;z.A...H.....]H...].e.^..8RG.4.....8D.Jql{\$.P..DI..b`.....B.f...s.n....0.)H/\_6CuAt.(.....h.E)8e..q.l6D....9m.&.....~...c.V...+...Z.....[W..&.....\_.....p.Y.....G.....R..

DST: q.V.r.q.....W.@...Y.8.h..A@.....o...a.M.....F.G..[u+.Xc)wC.@...."....s.....W.H]oWN.Tj.-?...^V+(...Z....

DST: p.....9#.....mG..R."J.'Z....=E.

DST: .....Og>(e.u...i.%r..R.[...^d...%...!.....j.3.....).<...t%0...9...~7.....~j.Z..

DST: ....os.q`f.B.:2.%j.U...o2.9.yOk.....%axE-.x.`gk{&H.z.....'6[t...l.....gu...2.NP.U...XI./.. .....J.z@

DST: ....3\$%1^..W.(d.....JSM..N.p.y!...;q<u...&.....W.....!^@)..K..\$tE..j.[l.J.....<cu..R7.\*.g.9.....ZJv.\*.

DST: ..qQ/..]n.....)B..zMQj...\_lU.@...[L.-m.....X.t.o:.....<TS.@F.6.'F6.VM...c.....w-r.P.D.>.9.....-l.wk...%.....0.....L.

DST: ..e.....as...%...Ol..F.A.Q..Hm.ed

DST: .Jk

DST: 2.8.g}.....!...Pu2\*.^}b.OG...wq.%k:/.....Sr7...d.8.6gg3W...N...|...P/D'.Q'.C...+l...v.l.p. ]j0...'.fk.....}.1...76.Nh..).UH....(J/'V.....3G.....E\_6E.....8.)M...|[\*...(.O.D....o.P..

DST: D..F....Y&...7j}l.j.O.....{m\*.%z/).e...)R...:of.

DST: ...YF..=N".....S..hs...t..Tlv...O.....r..l.....o.....k/X.Qn.O.j....Bk|l&..G?..

DST: JTub..^\_Y...L.....B...+h7v.x-...!..l..

DST: {z.

DST: r-..m...6...D.l.

DST: .M.....Q.\$\_g!.....%4..bkL.[].7c.-l.f..J....gu....2.NP.Uy:.

DST: N.%..fQ\_..E.kn....d.Y...%.s.1....g..Gi.b.)9.....6p..0l&w....Tt....\_e.J.G...\$.A.N.T....Sf.f.&.8e.n.=5..8J{...<z;a..Z...j.d....}5.i.....5.....)w..kW8..=NU.....U..

DST: .en.9.~.2NU..x.....Sp.A.b.E...M%KE.E.gE.G.T.wi.DR.(.s.j.K.R.y.N).{.L.....4CL.xT.G..6...{A66."...G}./Z  
DST: ..  
DST: s.v~.7.A.v.x..R..  
DST: ".\Bg.X.\*.4..ca7Y...k%'MzH.I.X.<.vVk).&...cv.M.Q...S..P..L.H.....e.L.#0.....LQ.O...8#1.q...O'.IT.'7.A<ITog...0.P.j.\*@Q(  
DST: .~RE...j.^d.].?&.yQOF[.o~]l.  
DST: .M-.....>"\..wro.D.l.c.>\*/.D.^.....=+F.8...@6...d.jA\$.q.J.S...ZM.Fh...d.N.....MC..".D../C.z1Z..I.LHH..C.&ldzl.).>...U..t.D.gO.....m..L.S.>P..rd.H.9.X.W.{!.....vi.r.~.K6.g  
DST: f..k.....P[l.?.F..O.M.Wk.J.S..8./e4..W.....a.Z.H..O..v.P.  
DST: .+.....C...t.K.  
DST: 3..g..e#E.8.....-l.....vd.^.....e.=W.w..rb.B.<...J..C.Ni8y"...C0k4s.\*!..  
DST: v.'.:gk.r.-c.R.QE.....Y.TM...3m&?u.g...e.]C..61.S.A.q5..I.Y.yC.&...G\$.S.H.\$H...x40C.l?.\*Xt~.9g=...n.l.A...%#..Y>C.e.YAx.S...Z....b....hT.u]p=VS.  
3.....l.<'.j.^5.5\$O.t...5y.&.\$4.C.....O.Lm.).y.pM"...k).~J.d..s.=.lgK.YH~.MX...^C.g.K.O8^A.w.s{bw..R7..%.7wPS...&...  
DST: 89.....H.w...kA.OZS.(...u;...T.8:b.O...n...O;x{X  
SRC: .p.)\*.1.lZ.7^r...C4~.+..v.g>1...m.Y.P.c...T.1.Bn.3  
SRC: .C.>6\$.L.%t4.....P.A.x.v...D.{.a.J.}K..5+x.HT.1.b.EL/.0.w.\*Z.e..Q..%<...K\*.qO~...T.P.d...h.  
SRC: .....7.6E.p...u.<[B./r  
DST: ).9.n.+..dU8.%yA3kg.l...6S]4.E..k.W..0.l  
SRC: .j.....\..K..2.d..^1?Z^U.r.>?X.^o'.O..  
DST: .V.jc...r.sq.Q..7..pP./V.gi.-j.....N.o.+...G..Fv"...c]...l-...{0.b..5.AE  
DST: .V+...&/.)...rT.(.  
DST: .z7H.8#.2.'.....q.Lf."=k.B...6.t1B\H.r..7.S..n..b6.4..8(2S  
DST: %MR....  
DST: ....%b..q.m..z.x.w..q.g.o.Z.....&.yy6ID.....MO.j{".Y8#h.j.B...|k|.b..N.|G>.h.x.%cD[...H=...A.h&.....s5k.C.g>...W.Xo.....r.>|.c.U.|Q.....r..c.....@.&[+t.V"...bc.g."3.m  
SRC: .hD...l.o..  
SRC: o.XG.+..0.f.a.lP.....+^..9.S.S..-./.....m.+e.{A..0J.#..f.....i%Xp...d.^..A..~E..ra!\$L.{...}]...#+a2.Y.....j=\$.....{0.5.1...r.{  
SRC: L..~.....q.2...[C.  
SRC: K=...ls.....  
SRC: .....+eMa.&V.u..e.]+.....2.%bDo&l.e..S.5.9.2.5U...;N.V.s~'l.E..t.K.....?..A..~..Dn.rg..d.....  
DST: +G)<>.l.G.x.N.l.y.MC.Hh;P.....\_D...?6...4..0..{.#.G.x.'G..!.....  
DST: .\_Kl.X.#pk.....=&.c..Xr.Lu.K.sg..A...H.G#S;t4...R.K...0.'x.1i.....  
DST: .e.Nj;G7...L...1H.2.Y.'.....>...].:9..='5].....U.58.<.&m.j.9'.b..t.rz/Mg./o'(.@8.T..D..R.xjg..'i.Cn.^ye1e..tQ..W.xr.-c.f.g.]...p.y5....Yy6:1....s....@x.X.+..l.%m.h3.#.%LJ2.N..^!  
SRC: j.....]u.E.g.aw.m..  
DST: ).9.n.+..dU8.%yA3kg.l...6S]4.E..k.W..0.l  
SRC: .j.....\..K..2.d..^1?Z^U.r.GT.n/l...t..  
DST: wft[?..Ft..D.q..SUO..kG..=r.t.V..C.&/l.4.3./...%p...&...x.J.^r.....[%.....%..|  
DST: e.f\$\$.UD:.....dj='V\$.4y..eZ..\_j^T2.v..T'^8k.....>..8D.le..eP...KJGH^..\_Q..6(9I9G[b.Z..B..SA..8q...k.....]...  
DST: y.....{(P.S.PA.7.....P(DH..U..h..8..@..t[l..h..v.M..a..u..>..Ar.OU"...).O...g.o.xy...f.>c.%&]...p5..~.E0'.S.cj..u.g.'X...Kgv.c..A...h.Bt..z.]  
DST: 5.&{V.j.Kp.?Y.H.O.o.^.'C.Ho.E.X.j.}.X.To].....X..y+..-IP.&[dX./...S'.4.l.8...^<B..Y.v..W..j.-D..j.xXb.D.Xz.1.Z...5p..l.<...6.  
SRC: .....z.Q..{..O..O/.....N.....b..-..  
SRC: z.t<..7..\_s.N...f]....."R8...%;w.2.'c5{.Sr.%g...+..6.^  
DST: ....k.jB.J.=m.w....3.MZN.\$

Doug Burks @dougburks @securityonion



```
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.
```

```
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:
```

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..

## OSSEC Alerts - Event Summary

**Description** ⇅

**Host** ⇅

**Username** ⇅

Sysmon - Suspicious Process -  
svchost.exe

securityonion

DESKTOP-SV8HSSB\Doug  
Burks

```
2018 Nov 13 15:24:29 WinEvtLog: Microsoft-Windows-Sysmon/Operational: INFORMATION(3): Microsoft-Windows-Sysmon: SYSTEM: NT AUTHORITY: DESKTOP-SV8HSSB: Network connection detected: RuleName: UtcTime: 2018-11-13 20:24:31.067 ProcessGuid: {DE1D5306-32F2-5BEB-0000-00100C512E01} ProcessId: 6852 Image: C:\Users\Doug Burks\Downloads\App\Firefox64\firefox.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: 54.192.22.93 DestinationHostname: server-54-192-22-93.dfw54.r.cloudfront.net DestinationPort: 443 DestinationPortName: https
```

gateway

1542140670.349217

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

172.16.150.20, 54.192.22.93



```
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"}
```

# 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](https://www.youtube.com/watch?v=MVZ33P_tN-g)

PF\_RING → AF\_PACKET

Doug Burks @dougburks @securityonion



# Just Released! **Hybrid Hunter 1.0.3**

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

# More osquery integration coming!



Doug Burks @dougburks @securityonion



# 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