RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **OST-R02**

Peel Back the Layers of Your Enterprise and Make Your Adversaries Cry

Doug Burks

CEO
Security Onion Solutions, LLC
@dougburks

My Incident Response Horror Story

Incident Response Lessons Learned

- IR is going to be slow and difficult if you don't have the right data at your fingertips
- Traditional security tools can be prohibitively expensive
- It's **fundamentally unjust** that attackers have amazing free tools but defenders can't afford the tools to defend themselves

Security Onion

- Started in 2008
- Free and open source platform
- IDS, NSM, ESM, DFIR, Threat Hunting
- Network and Endpoint Visibility

Security Onion – Flexible Platform

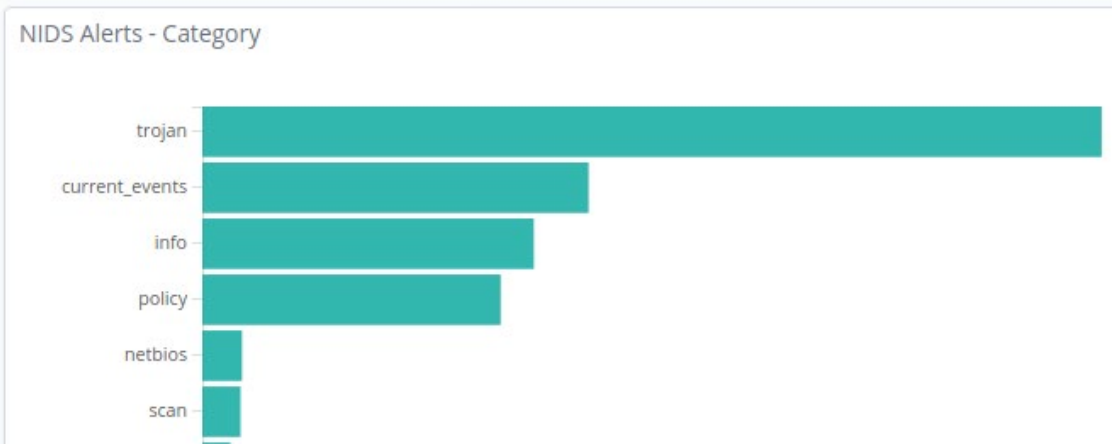
- Download our ISO image
  (over 900,000 downloads!)

  OR

- Install our packages on top of Ubuntu
  (moving towards container deployment…more on that later)

Best of Breed Open Source Tools for Network Security Monitoring

- NIDS alerts
- Protocol metadata
- Full packet capture



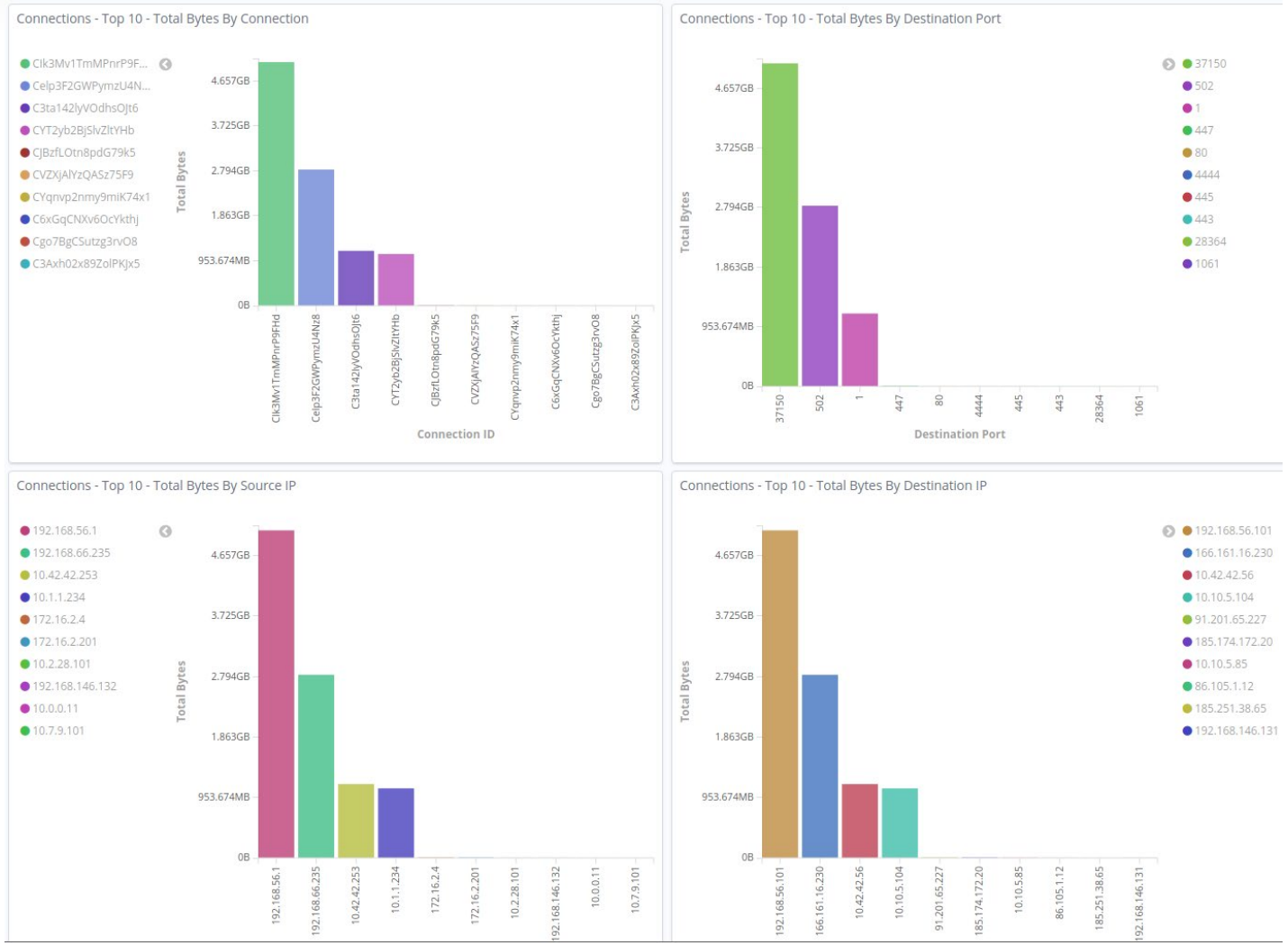
Zeek Hunting

- 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
- X.509

```
SRC: GET /files/go.exe HTTP/1.1
SRC: Accept: */*
SRC: Accept-Encoding: gzip, deflate
SRC: User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2;
enter PC 6.0; .NET4.0C; .NET4.0E)
SRC: Host: 51.15.252.131
SRC: Connection: Keep-Alive
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Date: Thu, 28 Feb 2019 13:17:28 GMT
DST: Server: Apache/2.4.18 (Ubuntu)
DST: Last-Modified: Thu, 28 Feb 2019 10:20:44 GMT
DST: ETag: "88e00-582f1a49c7700"
DST: Accept-Ranges: bytes
DST: Content-Length: 560640
DST: Connection: close
DST: Content-Type: application/x-msdos-program
DST:
DST: MZ.....@.....!..L.!This program cannot be run in DOS mode.
DST:
DST: $.......@.d..z
DST: O.z
DST: O.z
DST: O.(.O.z
DST: O.(.O{z
DST: O#.qO
DST: z
DST: O.z.O|z
DST: O.(.O(z
DST: O.(.O.z
DST: O.(.O.z
DST: ORich.z
DST: O.....PE..L...T.b[.....p...0..... d.....p....@.....
H.....UPX0.....UPX1....p.....h.....@....rsrc....0...p...
@.....
.....3.95.UPX!
```

Best of Breed Open Source Tools for Slicing and Dicing Logs

- Elasticsearch
- Logstash
- Kibana



Integrates with Best of Breed Tools for Endpoint Telemetry

- Wazuh HIDS
- Elastic Beats
- Sysmon
- Autoruns
- osquery

OSSEC Alerts - Event Summary

Description	Agent	Username	Count
Integrity checksum changed.	securityonion		259
New dpkg (Debian Package) installed.	securityonion		50
Dpkg (Debian Package) half configured.	securityonion		48
PAM: Login session opened.	securityonion		33
Missing	securityonion		32
PAM: Login session closed.	securityonion		25
File added to the system.	securityonion		24
User successfully changed UID.	securityonion	root	21
Unknown problem somewhere in the system.	securityonion		10
Received 0 packets in designated time interval (defined in ossec.conf). Please check interface, cabling, and tap/span!	securityonion		7

Use Cases

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

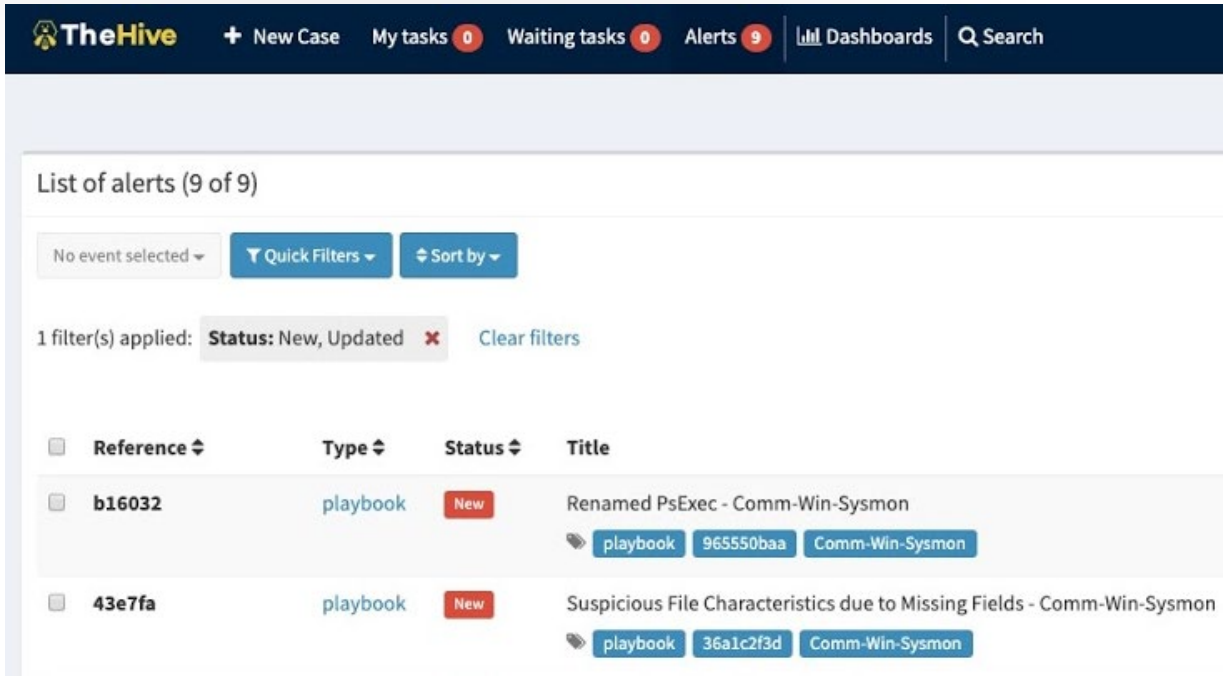
Case Study: Real World Incident

New! Security Onion Hybrid Hunter

- Ubuntu packages → Docker containers
- Orchestrated via saltstack
- Supports both Ubuntu and RedHat/CentOS
- Currently in testing

Security Onion Hybrid Hunter – New Additions

- TheHive
- Osquery
- ATT&CK integration
- Sigma integration
- Our custom Playbook workflow



Security Onion Solutions

Summary

- Let's give defenders more advantages
- Let's be ready when the next attack comes
- Ready to peel back the layers of your enterprise and make your adversaries cry?
  https://securityonion.net

Apply What You Have Learned Today

- Next week you should:
  - Download Security Onion from https://securityonion.net, install in a VM, and use so-import-pcap to get a quick feel for the platform
- In the first month following this presentation you should:
  - Build a production Security Onion box collecting live traffic and logs
  - Review alerts and do some threat hunting
  - Peel back the layers of your enterprise!
- Within two months you should:
  - Expand your Security Onion box to a distributed deployment to cover blind spots in your visibility
  - Make your adversaries cry!