Security Onion

Ending the Tyranny of Expensive Security Tools:
A New Hope
Security Isn’t About Managing Tools

- Good information security (and engineering) is about solving problems.
- You don’t always need to buy a product.
- Be Creative.
So Many Tools....
So Little Budget
What is Security Onion?

Security Onion is a FREE Linux distro for:

- intrusion detection
- network security monitoring
- log management
What’s Inside?

- Snort
- Suricata
- Bro Network Security Monitor
- Argus and Ra
- Xplico
- Network Miner
- Squil and Snorby
- ELSA
What data does it give me?

- Flow data from Argus, Bro, and PRADS
- Alert data
  - NIDS alerts from Snort/Suricata
  - HIDS alerts from OSSEC
- Syslog data received by syslog-ng or sniffed by Bro
- Asset data from Bro and PRADS
- Transaction data – http/ftp/dns/ssl/other logs from Bro
- Full content data from netsniff-ng
Does it scale?

- Big Onions – 64-bit
- Big Traffic – PF_RING
- Big Data – ELSA
### Central Service Association

#### Suricata Alerts

**Vulnerable Java**

<table>
<thead>
<tr>
<th>Time</th>
<th>Host</th>
<th>alert.signature</th>
<th>src_ip</th>
<th>src_port</th>
<th>dest_ip</th>
<th>dest_port</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 22nd 2016, 16:12:33.178</td>
<td>nsm-64.csai.com</td>
<td>ET POLICY Vulnerable Java Version 1.7.x Detected</td>
<td>10.26.30.100</td>
<td>50.232</td>
<td>23.67.91.168</td>
<td>80</td>
</tr>
</tbody>
</table>

**Time**

- @timestamp: 2016-06-22T16:12:32.378
- _id: 1
- _index: suricata-2016-06-22
- _type: suricata_log
- alert.action: allowed
- alert.category: Potentially Bad Traffic
- alert.signature: ET POLICY Vulnerable Java Version 1.7.x Detected

**JSON**

```json

```
Squert web interface
Where do we go now?

http://securityonion.net

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

- Download/Install
- FAQ
- Mailing Lists
- IRC #securityonion on irc.freenode.net
- @securityonion
- Security Onion classes throughout 2014!
Questions?