Collecting Home Telemetry

Matthew Gracie
Information Security Engineer

Who Am I And What Am I Talking About?

Security Onion

- Project by Doug Burks (@dougburks)
- Prebuilt Dockerized stack of open source NSM tools
- Available as an appliance ISO
- Can be installed on top of vanilla Ubuntu and RHEL/CentOS
- I’m using the Release Candidate for v2.0, formerly “Hybrid Hunter”
- Requires a Tap or SPAN for traffic capture

So What's Included?

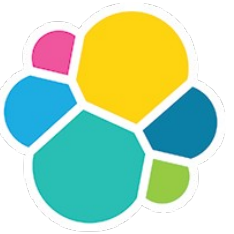
Zeek

- This generates network connection metadata from the observed traffic
- Think of it as Netflow++ – all the connection information of Netflow with some actual layer 7 data as well

Netsniff NG

- Netsniff is a packet capture daemon that writes all of the observed traffic to disk
- Everything is saved in standard pcap format
- This is storage-intensive, but amazing for forensics work

Elastic Stack



- Security Onion uses the Elastic Stack for its main reporting interface
- Data is ingested and parsed in Logstash, then stored in an Elasticsearch backend
- Queries and visualization are done in Kibana

OSQuery

- OSQuery is an open source project from Facebook that allows endpoints to be queried using SQL syntax
- Queries can be real-time or scheduled, with differences logged to a local file
- Security Onion includes the Kolide Fleet management application as well as OSQuery installers for Linux, Mac OS, and Windows

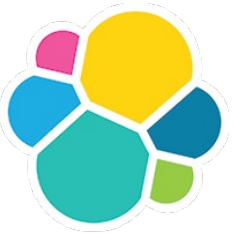
Sysmon

- Sysmon is a free download from Microsoft that runs on an endpoint and writes extra information about running processes to the Event Log
- What events are recorded is configured with an XML file
- The configuration file I use is the one by @SwiftOnSecurity
- Security Onion already has Logstash parsers for Windows Events, including Sysmon

Auditd

- Auditd is a kernel-level auditing framework for Linux that records data to a local file
- Like sysmon, what it monitors is controlled by a configuration file – I like the one from Florian Roth (@cyb3rops)

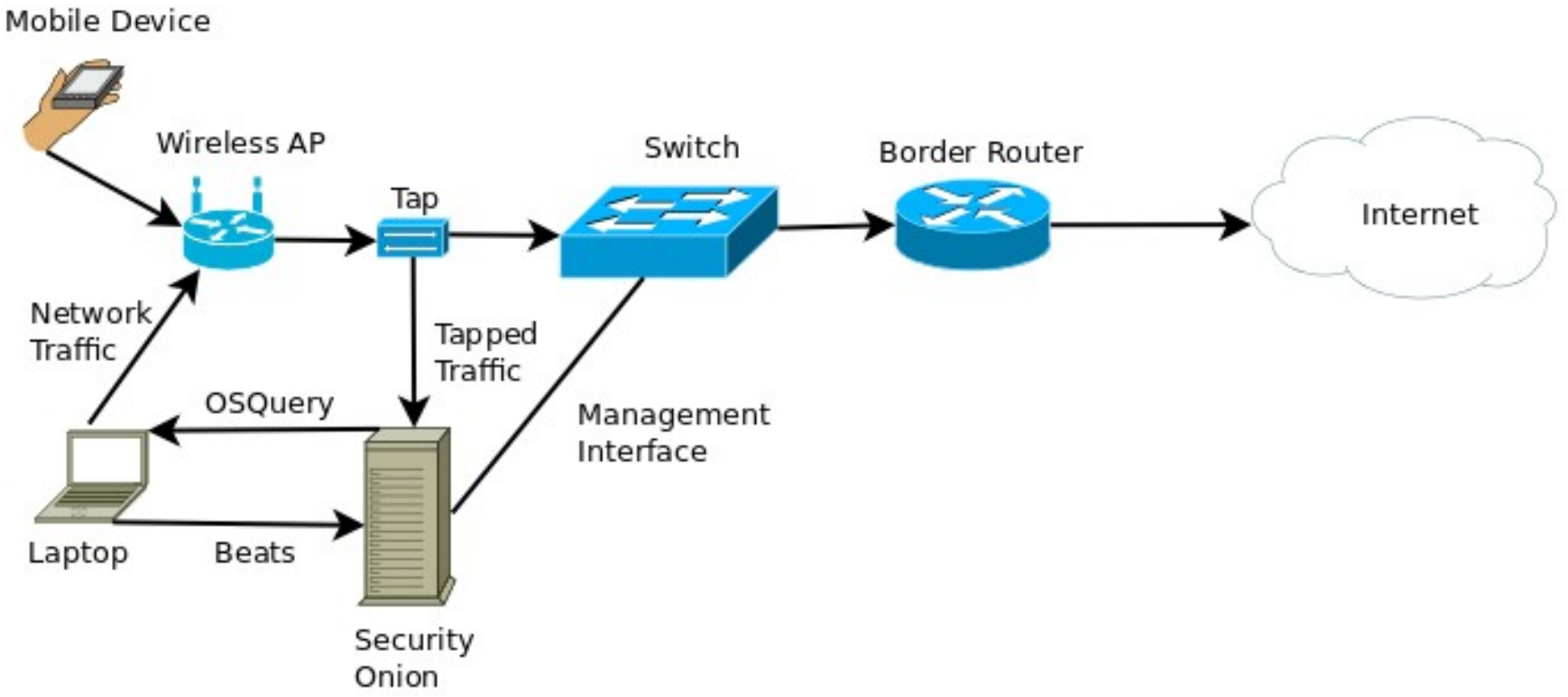
Beats



- Beats are lightweight log shippers that are part of the Elastic Stack
- I collect Windows logs using winlogbeat and Linux logs using filebeat
- What they collect is customizable via YAML
- *Make sure your versions match!*

	Zeek	Netsniff	OSQuery	Sysmon	AuditD	Beats
IoT	*	*				
Mobile/ Un-Managed	*	*				
Windows	*	*	*	*		*
Linux	*	*	*		*	*
Mac OS (in theory)	*	*	*			*

Architecture



End Result

- An NSM platform with full visibility into the wireless traffic on my network
- A log repository pulling in activity from all of my managed endpoints
- Enough space for a month or more of full packet captures
- All tied together with Kibana for searching and visualization

Demonstration