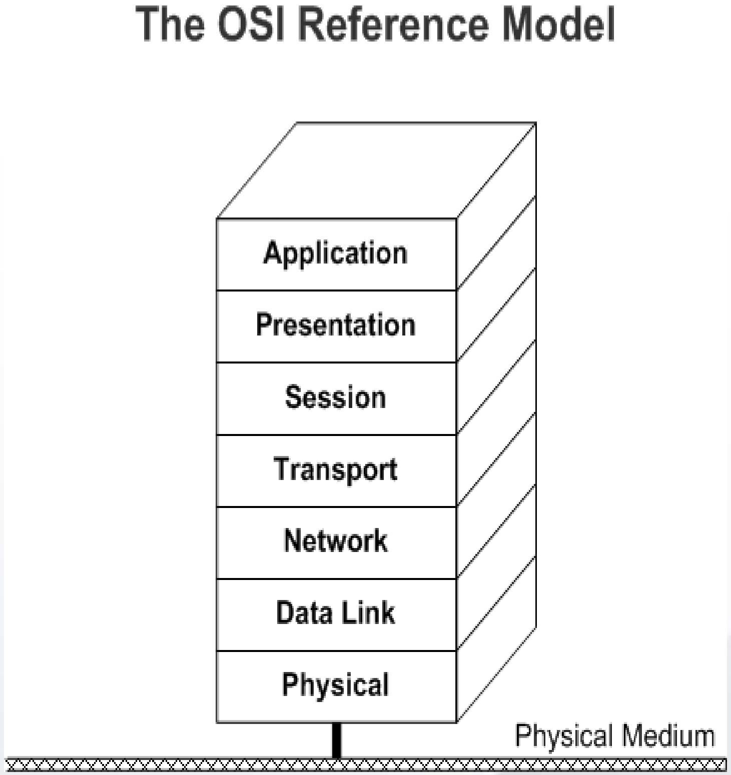
Using Layer 7 Metadata to Augment Flow Analysis

Tim Ray

Security Analyst

Overview

- Who are we?
- What are we doing?
- What can you get out of this?
- Questions and Answers



21CT

- 12 year old firm headquartered in Austin, TX with offices in Washington D.C. and San Antonio, TX
- Experienced DoD and military vendor
- LYNXeon is our flagship product
- Partner with CERT to use YAF in our products
- We have a really nice break room.

Tim Ray

- Began in the IT field in 1995
- Security training and CISSP in 2007
- Worked in financial sector, for an MSSP and the State of Texas, Department of Information Resources as a security analyst
- Plays with cars

Where are we now?

- Analyst logs into SIEM and starts to sort out false positive results.
- Analyst finds actionable event from signature based source.
- Analyst investigates event and brings in flow and pcap
- Analyst validates alert and reports to stakeholders/fixers

The Way it Ought To Be

- Analyst initiates proactive analysis using flow + layer 7.
- Analyst finds suspicious traffic.
- Analyst validates the event using flow and other sources.
- Analyst calls in the alert to stakeholders/fixers.

PCAP, Flow and Goldilocks

- PCAP is widely understood and trusted
- Flow is less understood and less utilized
- Both have advantages and disadvantages
- There is a happy medium which is Just Right!
- But I’m much more comfortable with cars, so…

Full Packet Capture

-Versatile and complete

-Widely available

-Bulky = short search horizon

-Hard to search

Custom Flow Analysis Toolset

-Every install is unique

-Easy to store

-Minimalist

-Often open source

Flow+Layer 7 Metadata

-Versatile

-Easy to store

-Customizable (which apps do you want)

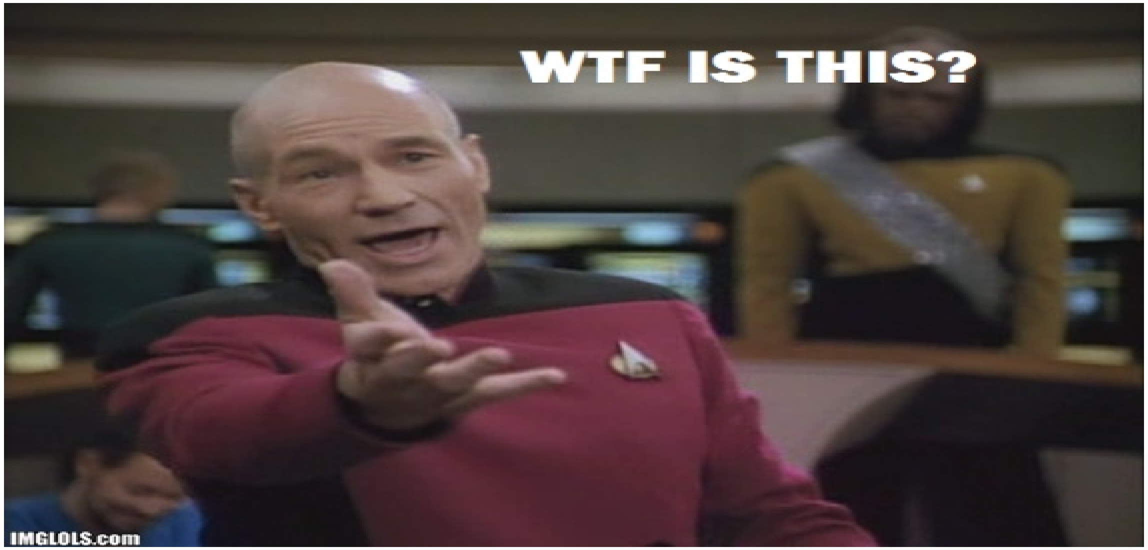
-Fast to search

Layer 7 Metadata

- YAF inspects but does not store the payload.
- The metadata collected is different for each application.
- DNS
  - Query Response
  - Qname
  - Qrtype
  - TTL
- HTTP
  - Referrer
  - Host
  - Browser

- Enough to enrich the flow experience without slowing down the system.

Why is it worth doing?



- More detail than in pure flows
- The right amount of data: http://www.peopleofwalmart.com is enough information
- You get an additional axis of analysis

Examples

- Visiting a URL that is blacklisted
- Apps running on wrong port
- Visiting a fast-flux domain (check TTL)
- DNS requests for odd URLs
- New application active on a known IP address
- False positive elimination

False Positive

Why Do We Need This?

- If analysts continue to depend on signature based systems, we lose the long fight
- If analysts continue to use JUST flow, it’s not enough
- We need a lightweight but extensible way of looking at network traffic

Questions?

tray@21technologies.com
Twitter: securitytim