



Intel Framework

What is intelligence?

Intel framework defines intelligence as an atomic bit of data with associated metadata

Things you want to know about!

Motivations

- Intelligence based searching is incredibly common
- Through abstraction we can expand the utilization of intelligence
- Creating a format for importing intelligence makes Bro target-able for intelligence providers

How common is it?

- Numerous open intelligence feeds
- Numerous security industry reports
- Numerous private intelligence sharing communities
- Many organizations are building their own internal intelligence teams

Benefits of Abstraction?

- **Reduce**
 - If multiple feeds have the same data, we don't need to store it multiple times
- **Reuse**
 - Look for IP addresses anywhere they show up instead of just in IP headers, etc.
- **Optimize**
 - There will be memory and performance optimizations we'll do under the hood



Intelligence Format

- Bro's intelligence indicator format is incredibly terse by default but extensible
- Data can be stored in a database or text files and updates at runtime

```
#fields indicator indicator_type meta.source meta.desc meta.url
1.2.3.4 Intel::ADDR source1 Sending phishing email http://source1.com/badhosts/1.2.3.4
a.b.com Intel::DOMAIN source2 Name used for exfiltration -
```

Design Limitation

- Asynchronous lookups
 - You can't use “do I know about this?” in a normal if statement

Currently Deployed

- 13,469 Indicators across 6 feeds
- Running at a few sites
- Seems to be working well
- Data feeds have issues of lack of context and sometimes old data

Questions?

- Next we have some exercises that are linked from the agenda