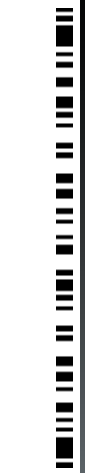
David Ross | Technical Director

The OpenIOC data format

MALWARE IDENTIFICATION

Preview

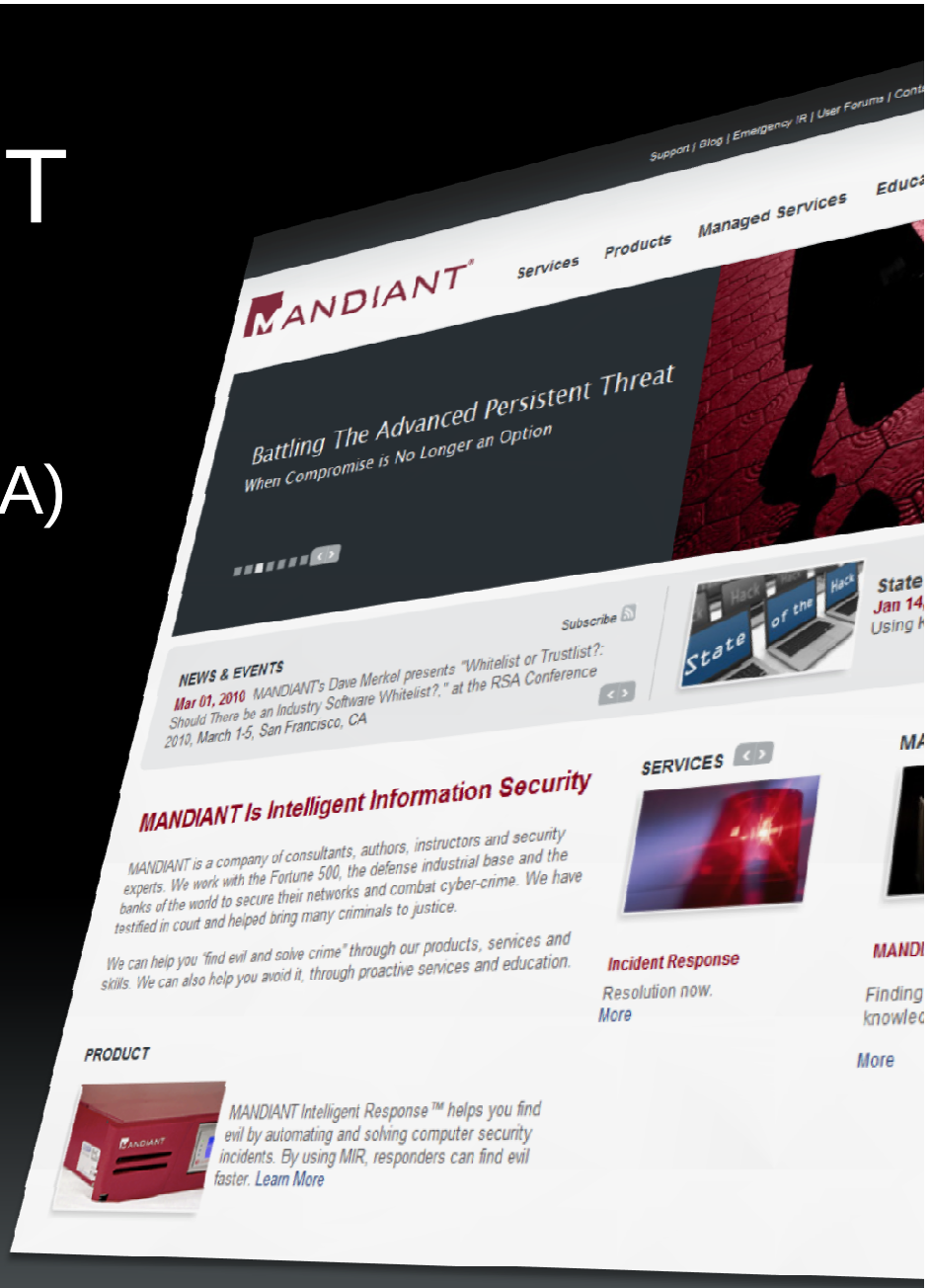
- What is an Indicator?
- What is OpenIOC?
- Why should I care?
- What is the IOCEditor?
- Where can I get this?



MANDIANT

We are MANDIANT

- VISA Qualified Incident Response Assessor (QIRA)
- APT and CDT experts
- Located in
  - Washington
  - New York
  - Los Angeles
  - San Francisco
- Professional and managed services, software and education



MANDIANT

Introductions

DAVID ROSS

- Technical Director
- Created OpenIOC format
- Responded to a half million hosts
  - Just last year

MANDIANT

Important note

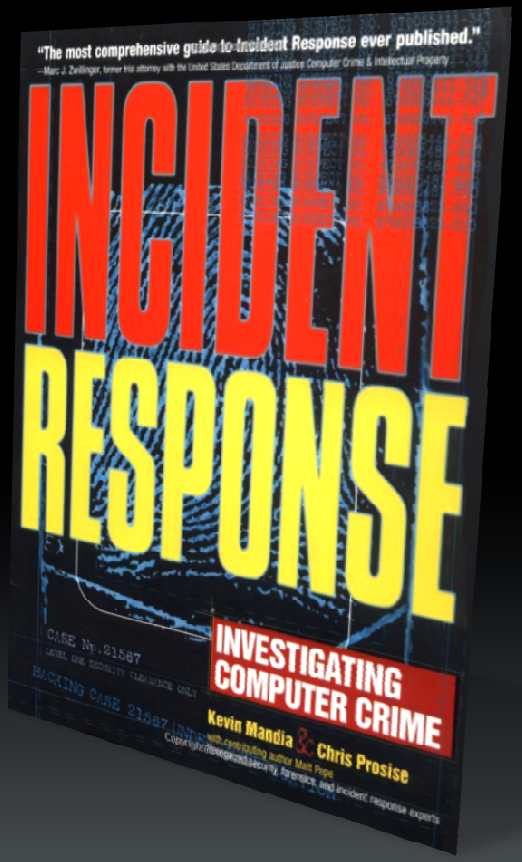
All information is derived from MANDIANT observations in non-classified environments.

Some information has been sanitized to protect our clients' interests.

MANDIANT

What is an IOC?

- Indicator of Compromise
- Intelligence used to find evil
  - On a host or on the wire
  - MD5s, file names, packer type
  - Registry keys, mutexes, drivers
  - DNS, IPs, query strings



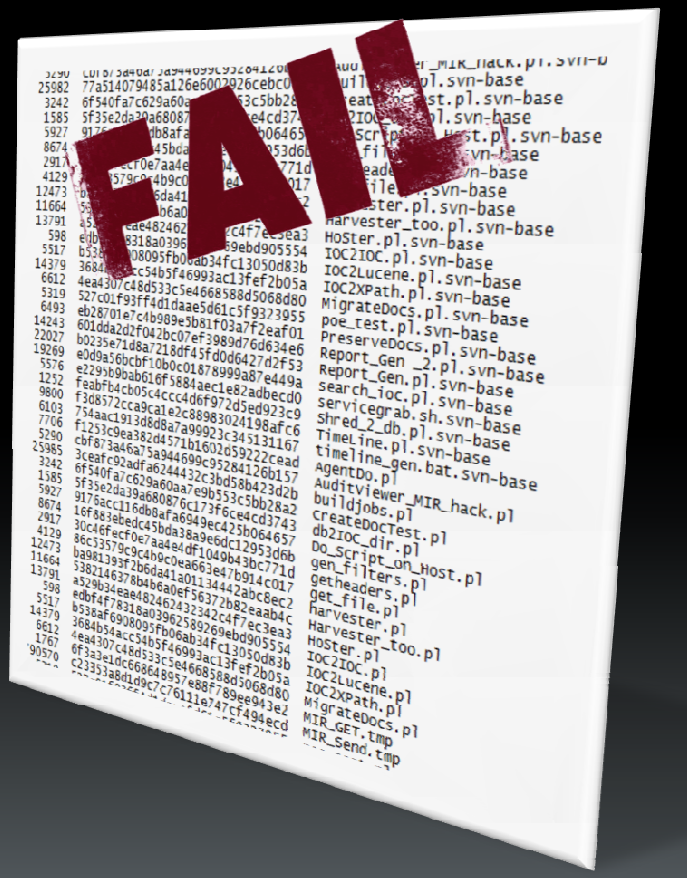
What is OpenIOC?

- A format to organize your intelligence
- Logical groupings
- Extendable for any indicator type
- XML (of course)

MANDIANT

Before OpenIOC

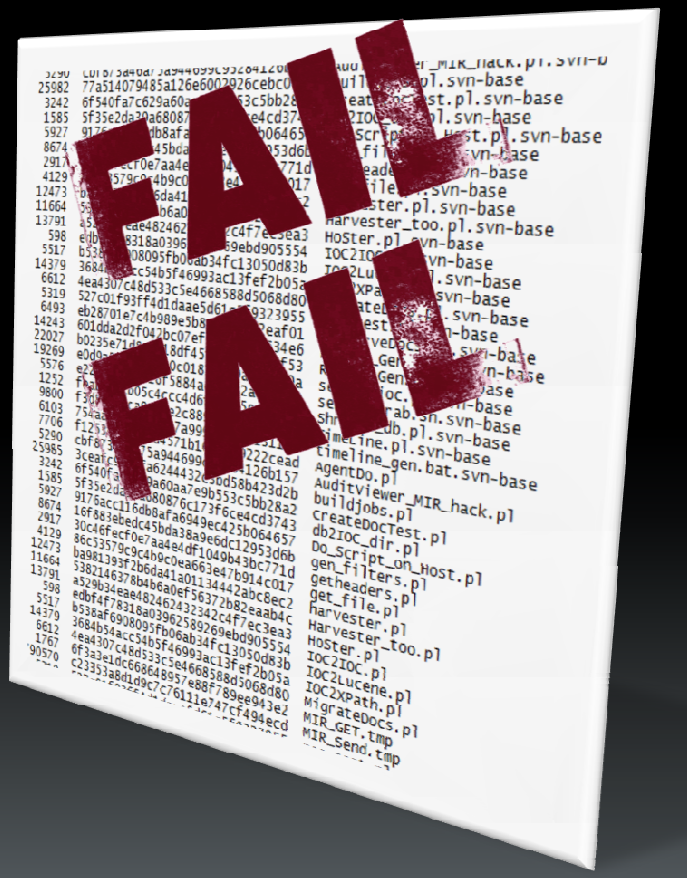
- Lists of stuff to find evil
  - Easy to create
  - Difficult to maintain
  - Terrible to share



MANDIANT®

Before OpenIOC

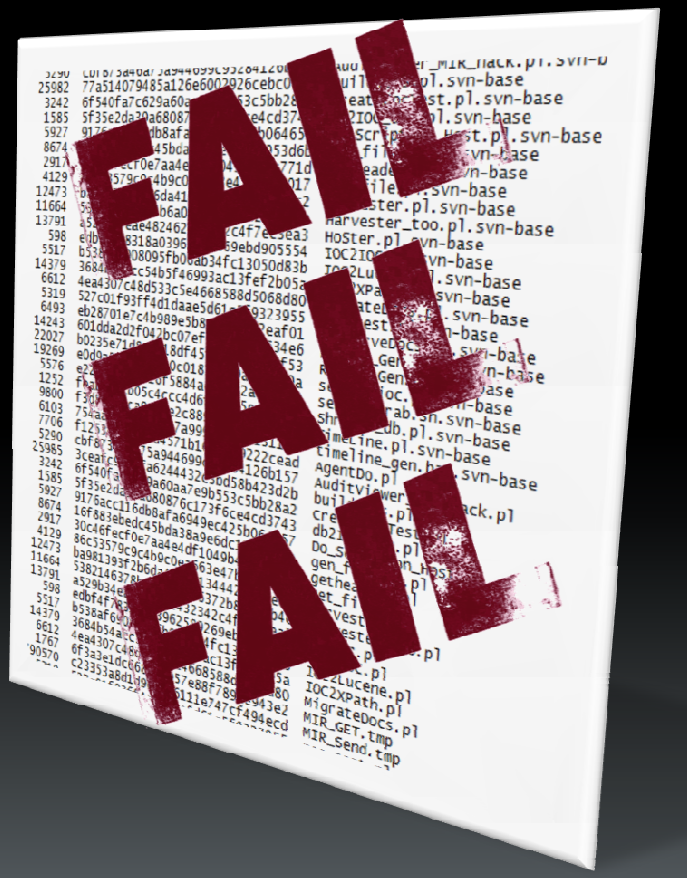
- Lists do not provide context
  - An MD5 of what??
  - Who gave me this??
  - Where is the report?
  - Where is the intelligence??



MANDIANT®

Or, worse yet…

- Proprietary languages
  - Only works in their product
- Complicated databases
  - I'm not a DBA
- Black box definitions
  - Who knows what's in there



MANDIANT®

Takeaway

Lists lose relevance

You can not determine:

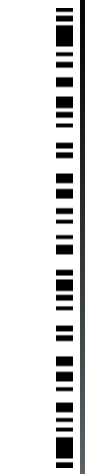
- why you were looking
  - what else is related

Takeaway

Lists are too rigid

Need to look for a new keyword type?

You need to make a new list.



MANDIANT

OpenIOC

- A format to organize Indicators
- Turns your data into intelligence
- Designed for data sharing
- Intentionally extendable

MANDIANT

OpenIOC is technology agnostic

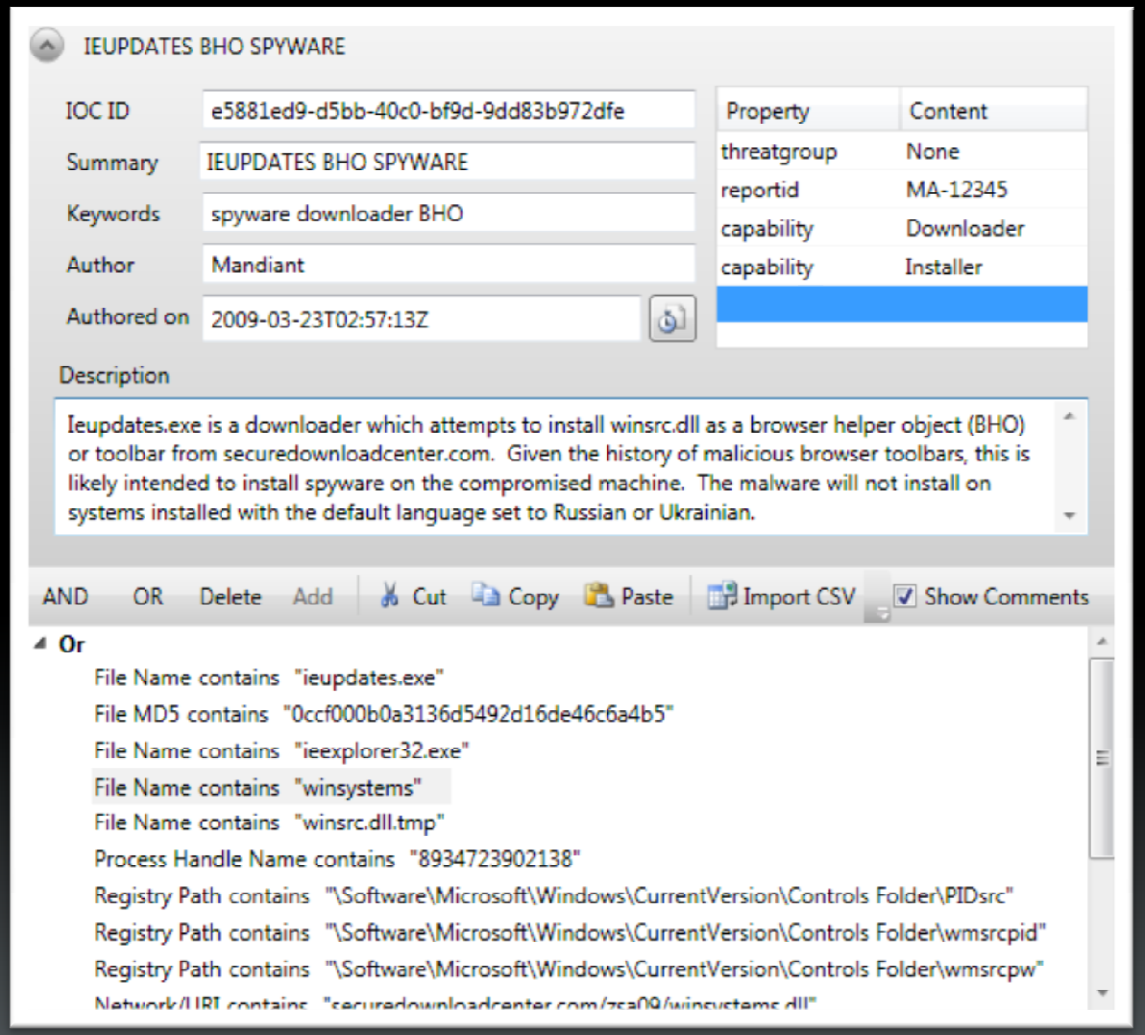
- Does not require any product
- Easily converts to needed formats
  - We have some pre-built
  - It is just XML after all
- It is used by MIR
  - Really comes alive with MIR

In use for over two years

- Used by MANDIANT
- Based on lessons learned in the field
- Made public by customer request
- 9 out of 10 consultants prefer OpenIOC

THIS is OpenIOC!!!

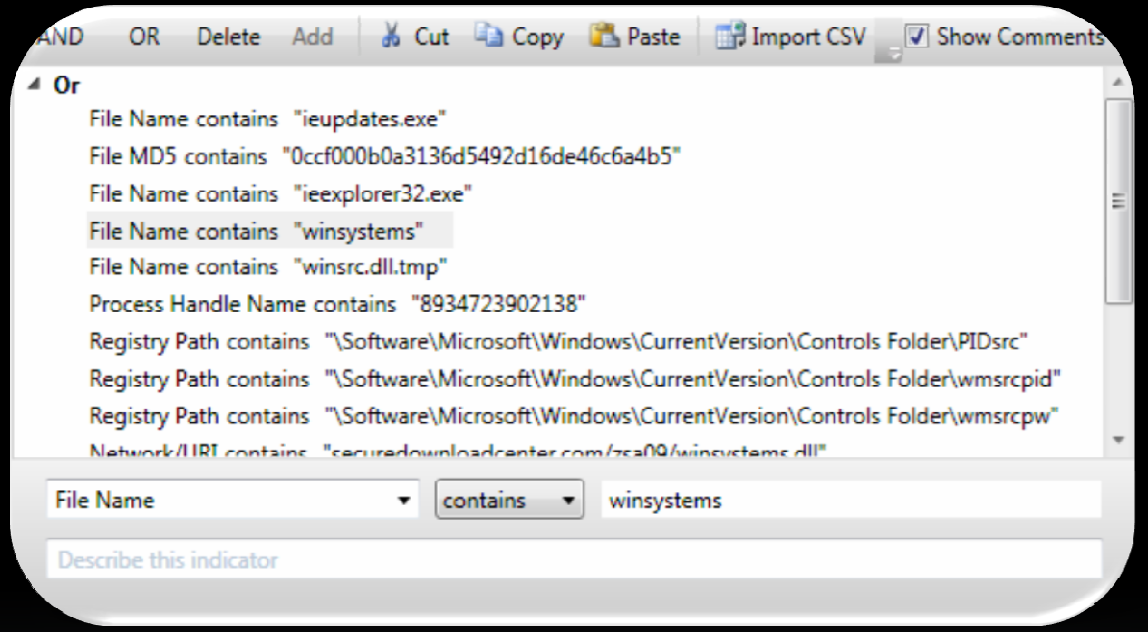
- The Why
- The What



MANDIANT

Stores what we are looking for

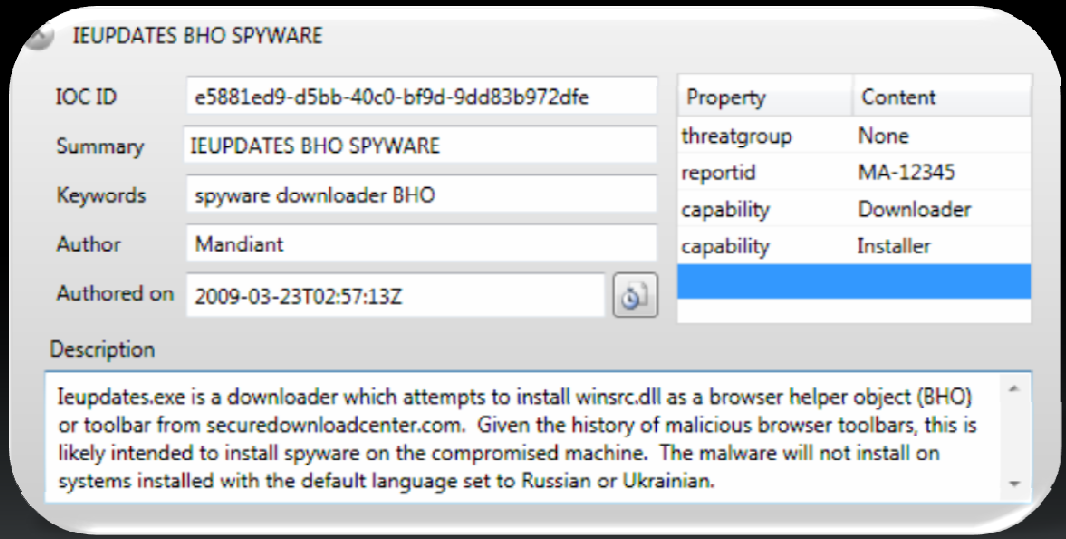
- Content
  - Keyword
- Context
  - Keyword Type
- Construct
  - Logic
  - We'll get into this later



MANDIANT®

Along with the ‘who’ and ‘why’

- Name, Description, Author, Category…
- External references
  - Data sources
  - Reports
  - Threat groups



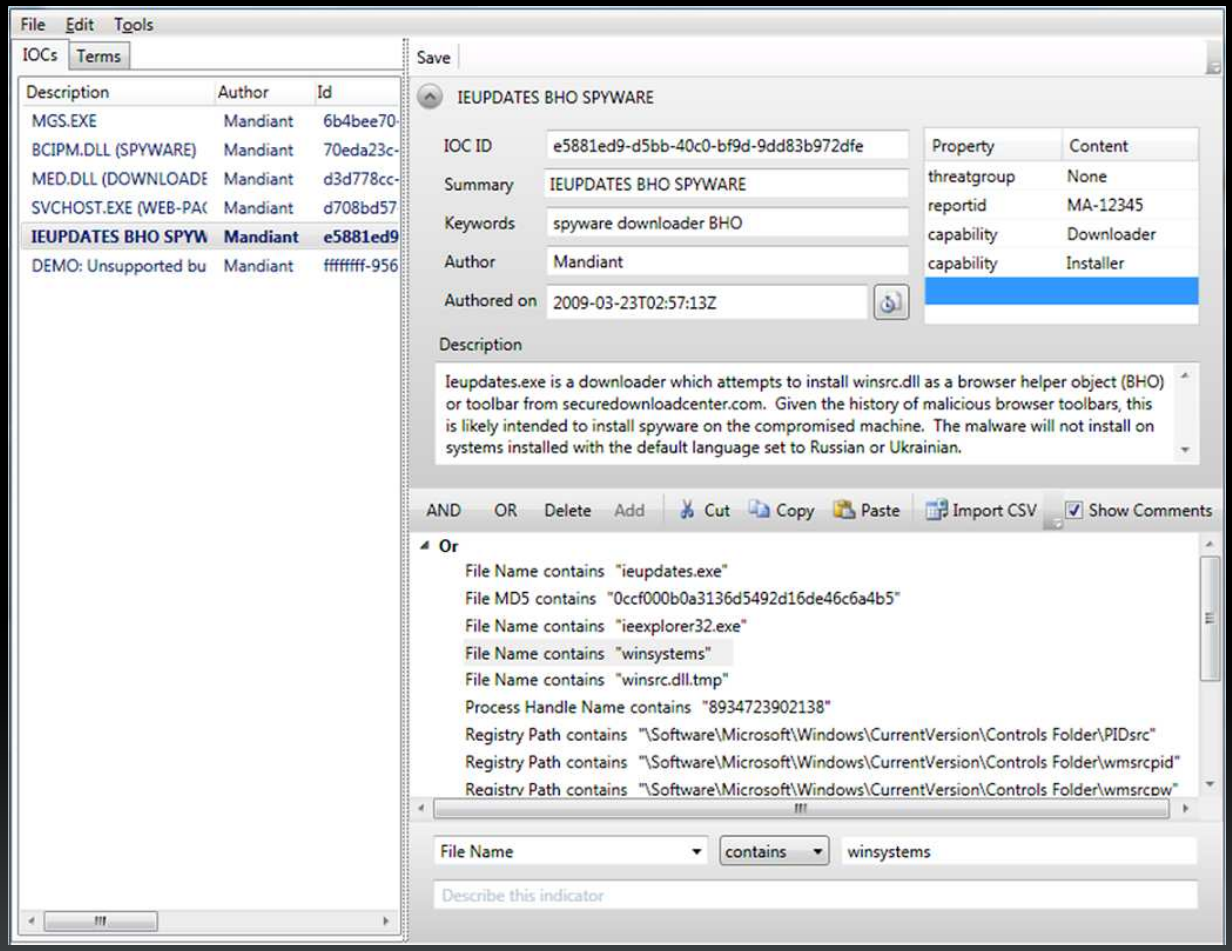
Advantages

- Keeps indicators with context
  - Quickly determine “why” from “what”
- Sharing with others
  - Easy to combine
  - Generate indicators from multiple sources
  - No more formatting questions

Advantages

- Scalability
  - Thousands of indicators in hundreds of IOCs
- It's only XML
  - Convert to ANY format needed
    - We have lots of examples for this!
- OpenIOC = Force Organizer

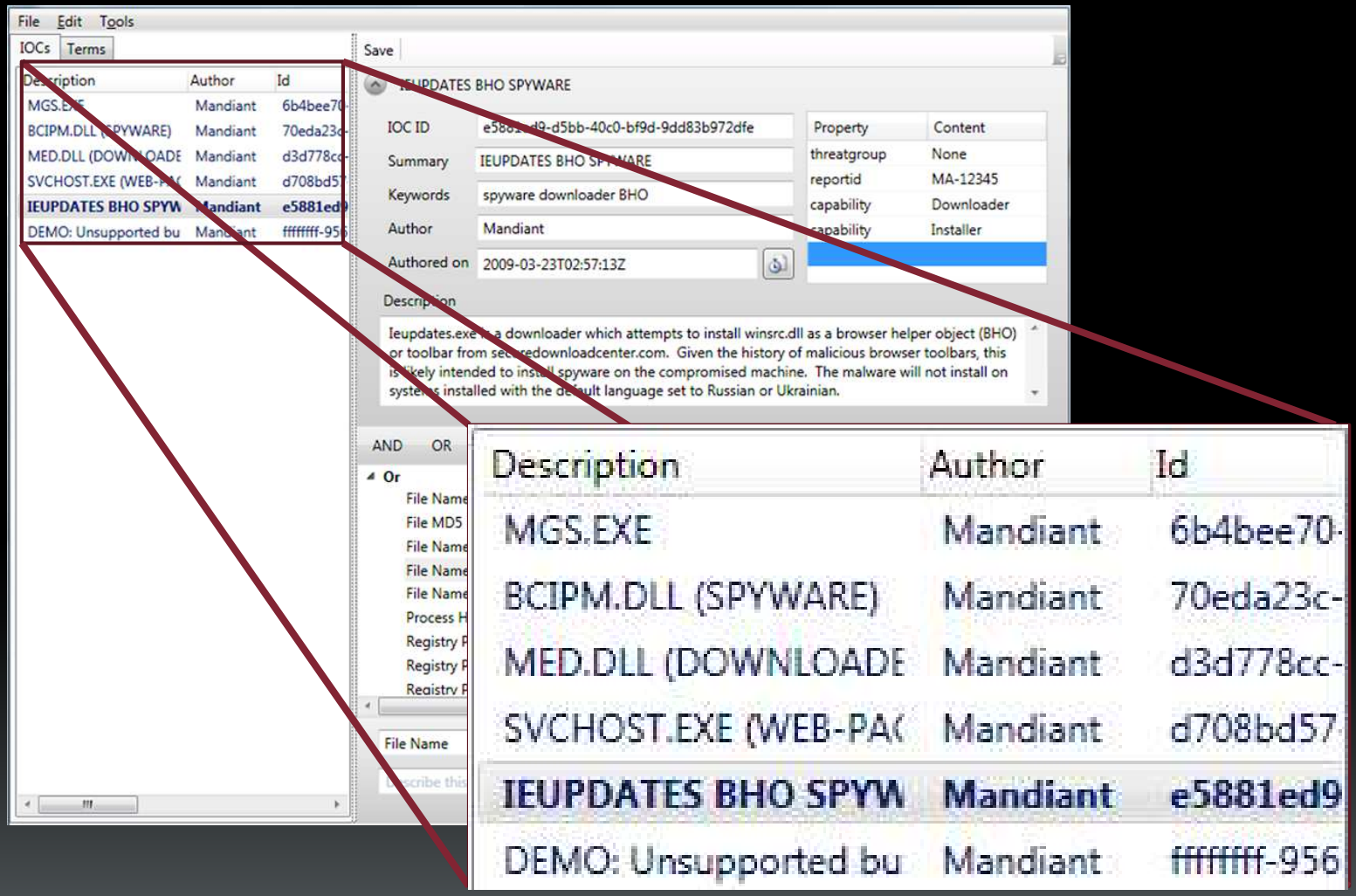
The IOCEditor



Pretty cool, huh?

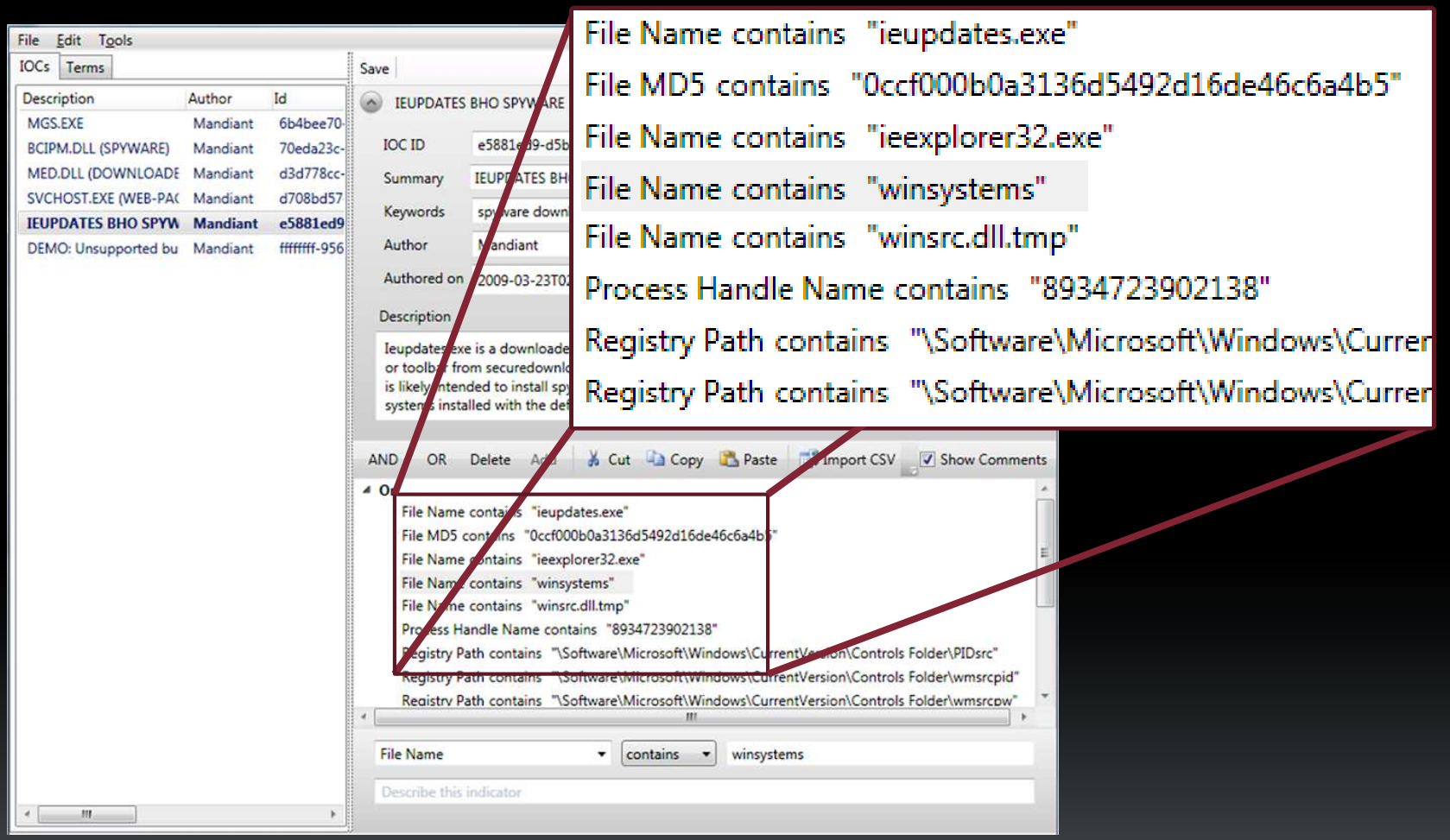
MANDIANT

OpenIOC data feed



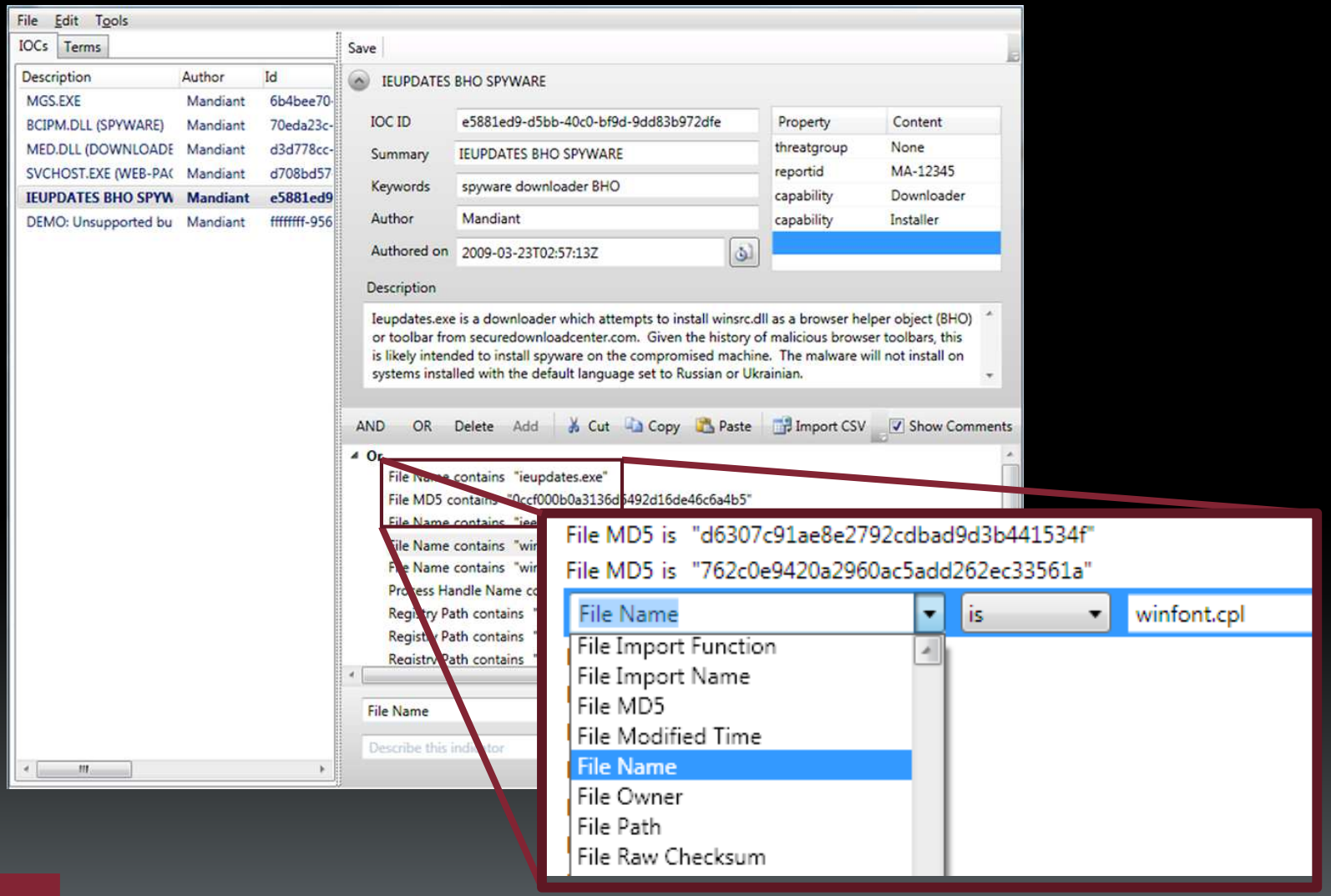
MANDIANT

What we are looking for



MANDIANT

Easy to create indicators



MANDIANT

Extendable keywords

- Can use ANY keyword type
- You can create new keywords
- It's just XML after all

EventLogItem/EID	EventLog ID
EventLogItem/genTime	EventLog GenTime
EventLogItem/message	EventLog Message

File Name	
File Path	
File Full Path	
File MD5	
File Modified Time	
File Base Address	
File Detected Anomalies	
File EntryPoint Sig Name	
File EntryPoint Sig Type	
File Export Function	
File Export Count	
File Extra Bytes	FileItem/PEInfo/ExtraBytesAfterLastSection
File Import Function	FileItem/PEInfo/ImportedModules/Module/ImportedFunct
File Import Name	FileItem/PEInfo/ImportedModules/Module/Name
File Computed Checksum	FileItem/PEInfo/PECheckSum/PEComputedAPI

HookItem/HookedFunction	
HookItem/HookingModule	
HookItem/HookedModule	
UserItem/Username	
ServiceItem/name	
ServiceItem/serviceDLL	Service DLL
ServiceItem/path	
RegistryItem/Path	
RegistryItem/Text	

ProcessItem/name	Process Name
ProcessItem/HandleList/Handle/Name	Process Handle Name
ProcessItem/SectionList/MemorySection/Name	Process Section Name
PortItem/remoteIP	Port Remote IP
PortItem/Path	Port Path

Email/Subject	Email Subject
Email/From	Email Sender
Email/To	Email Recipients
Email/Date	Email Date (Sent)
Email/Body	Email Body Text
Email/AttachmentCount	Email Attachment Count
Email/Attachment/Name	Email Attachment Name
Email/Attachment/SizeInBytes	Email Attachment Size
Email/Attachment/MIMEType	Email Attachment MIME Type

MANDIANT

The Indicator Terms document

```
<?xml version="1.0"?>
<ioctermlist
        last-modified="2010-03-12T00:41:57.2994379Z"
        description="These terms describe what might be acquired
  <ioctерm text          = "Email/Subject"
           title         = "Email Subject"
           data-type     = "xs:string"
           display-type  = "string"
           term-source   = "example/emailaudit" />
  <ioctерm text          = "ProcessItem/HandleList/Handle/Name"
           title         = "Process Handle Name"
           data-type     = "xs:string"
           display-type  = "string"
           term-source   = "application/vnd.mandiant.mir" />
 <ioctерm text          = "FileItem/Md5sum"
          title         = "File MD5"
          data-type     = "Md5Sum"
          display-type  = "md5"
          term-source   = "application/vnd.mandiant.mir" />
</ioctерm>
```

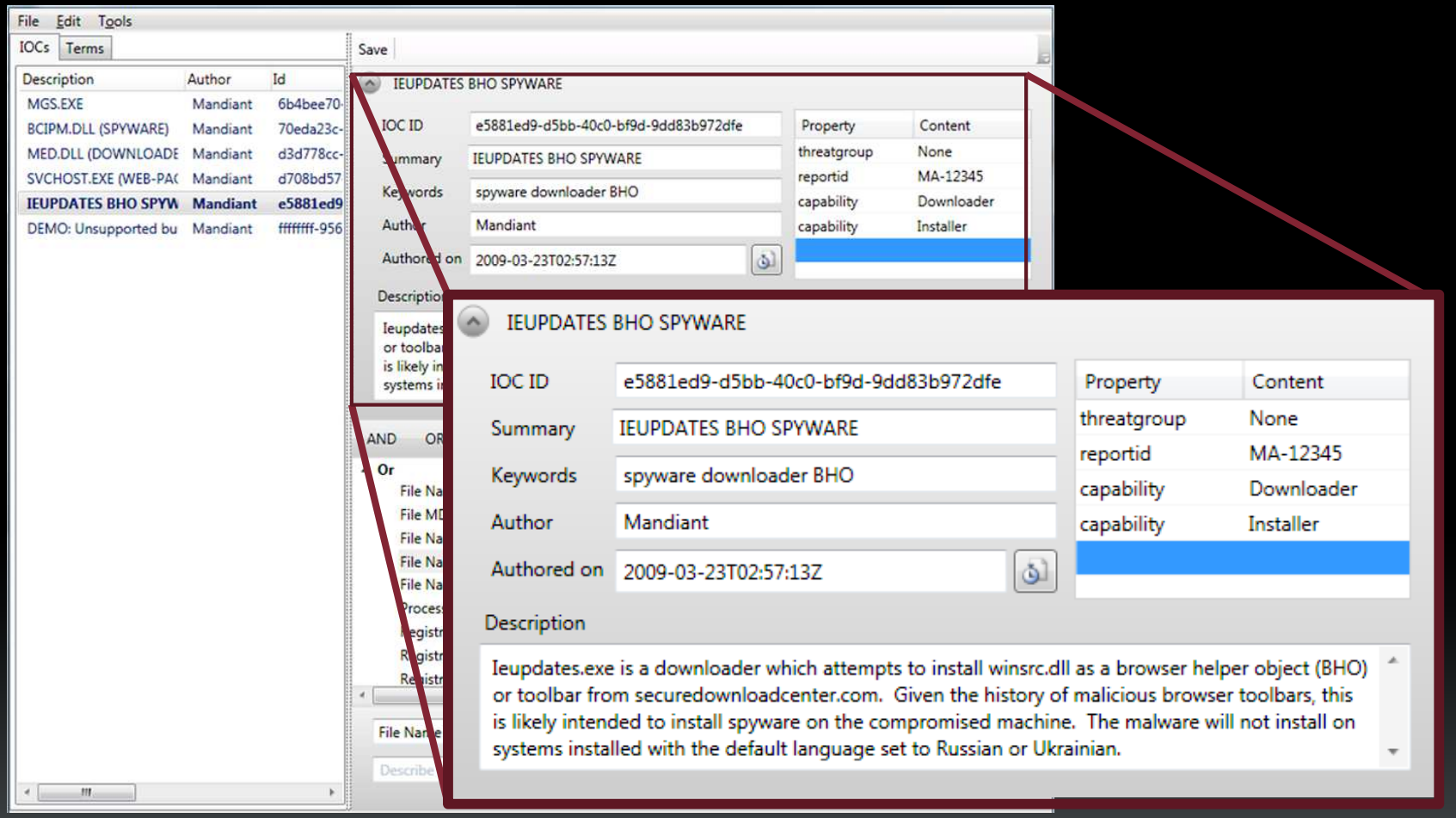
MANDIANT

Duplicating meaning

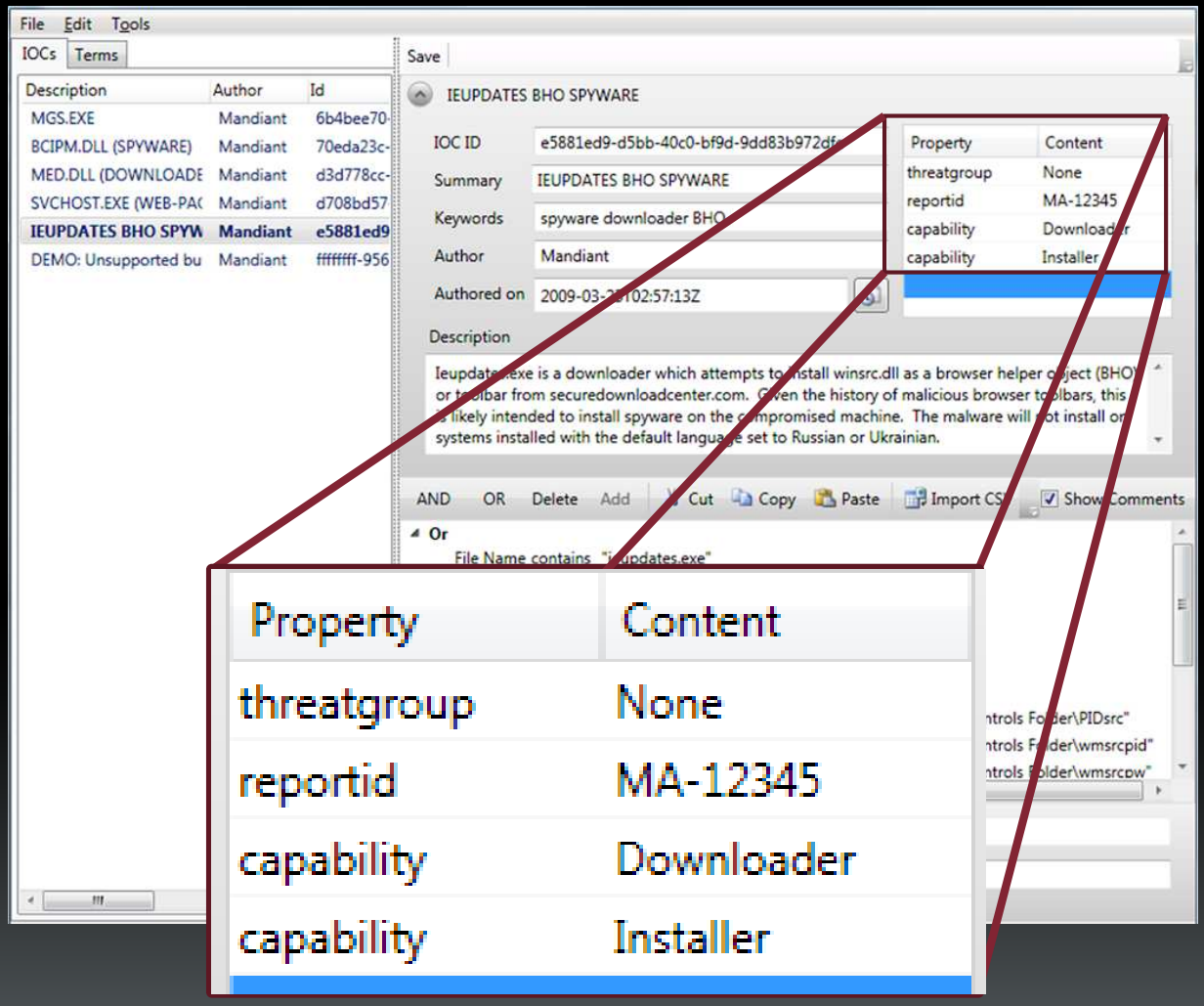
- Same problem as proprietary lists
- Use existing terms
- Publish your terms!
- Make mappings


```
FileItem/PEInfo/ImportedModules/Module/Name
```

Why we are looking for it



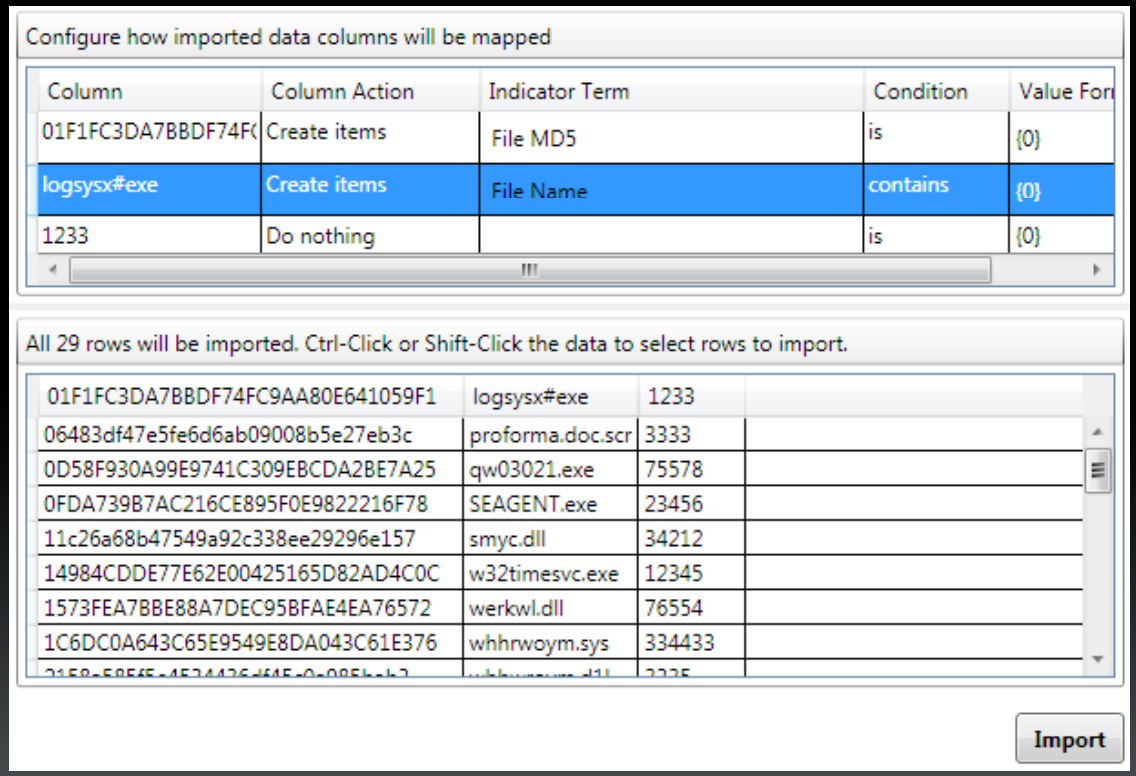
Refer to external data



MANDIANT

Importing your old lists

- Included feature in IOCEditor
  - Trivial to script (It's only XML)



MANDIANT

OpenIOC in the Field

- MANDIANT uses OpenIOC every day
  - Centralized all of our intelligence
    - No more private lists
  - Rapid exchange of data across teams

Every consultant knows what every other consultant knows.

Converting OpenIOC

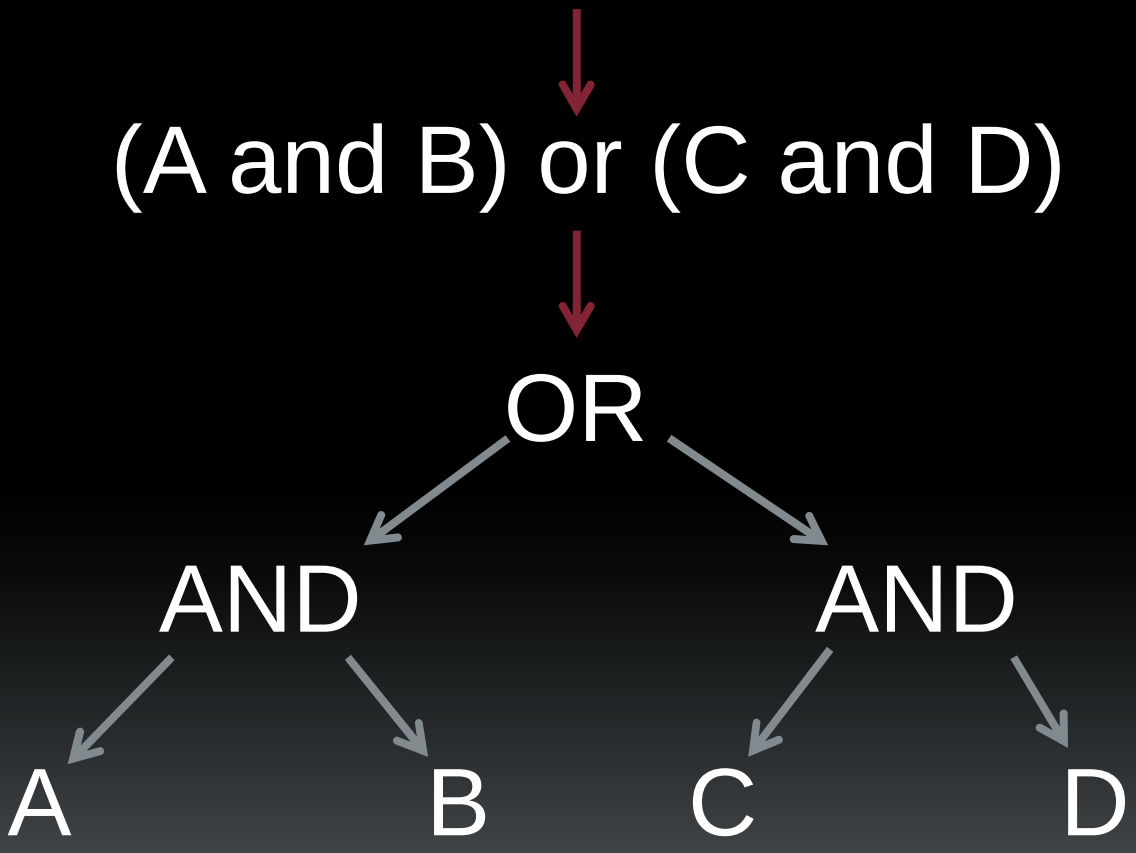
- Your old flat lists of indicators
- HTML
- XPath
- Lucene
- Snort
- Reporting statistics
- Word documents (really)
- Pie charts
- …it's just xml

Advanced definition constructs

- Why just keywords?
  - Is everything just a string match?
- OpenIOC supports logic
  - AND, OR
    - is, isnot
    - contains, containsnot

Logic Trees

A and B or C and D

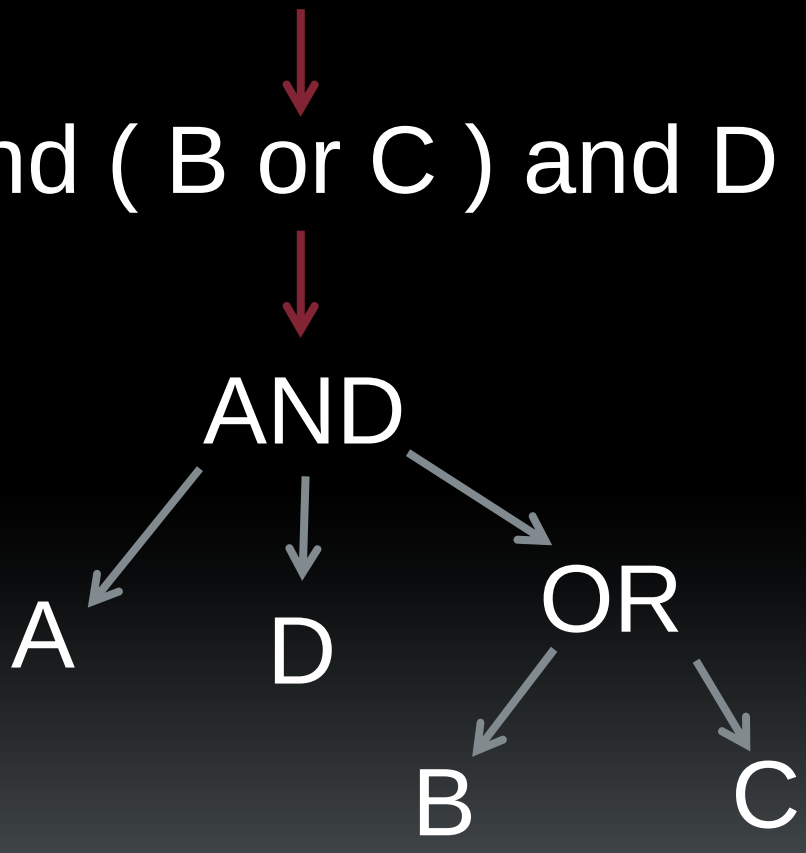


(A and B) or (C and D)

MANDIANT

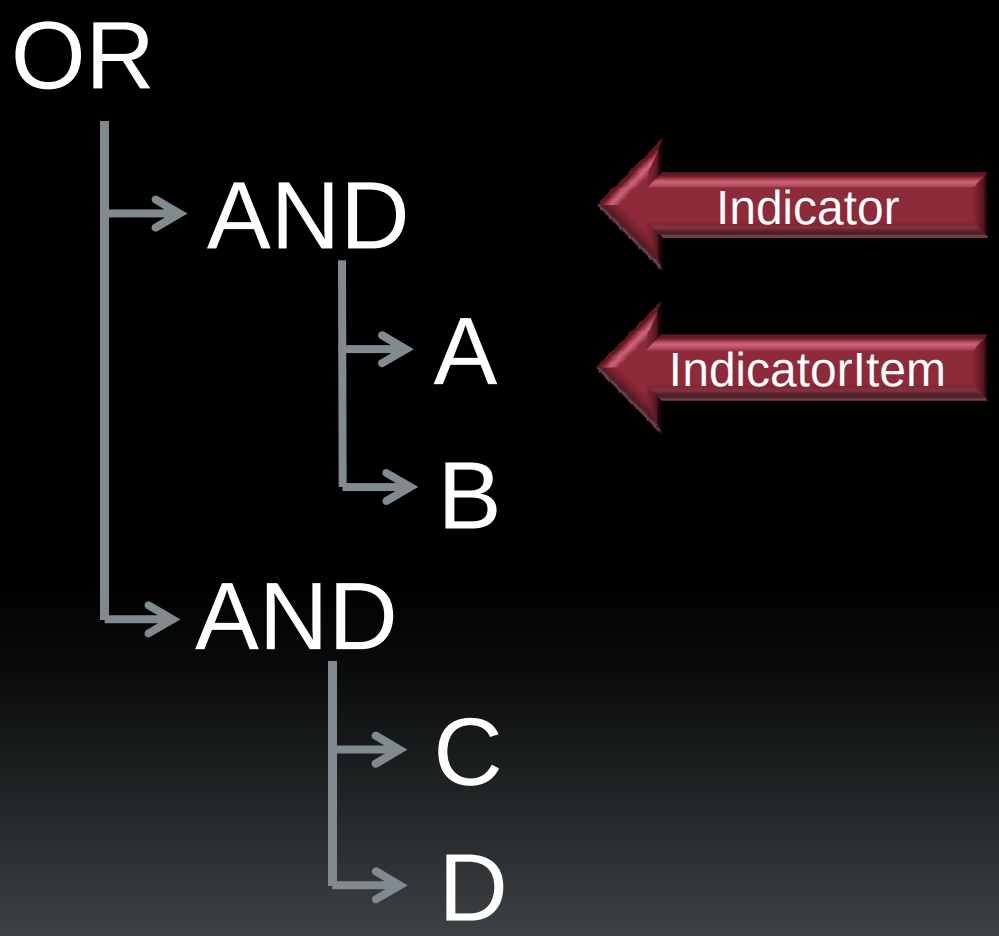
Logic Trees

A and B or C and D



A and (B or C) and D

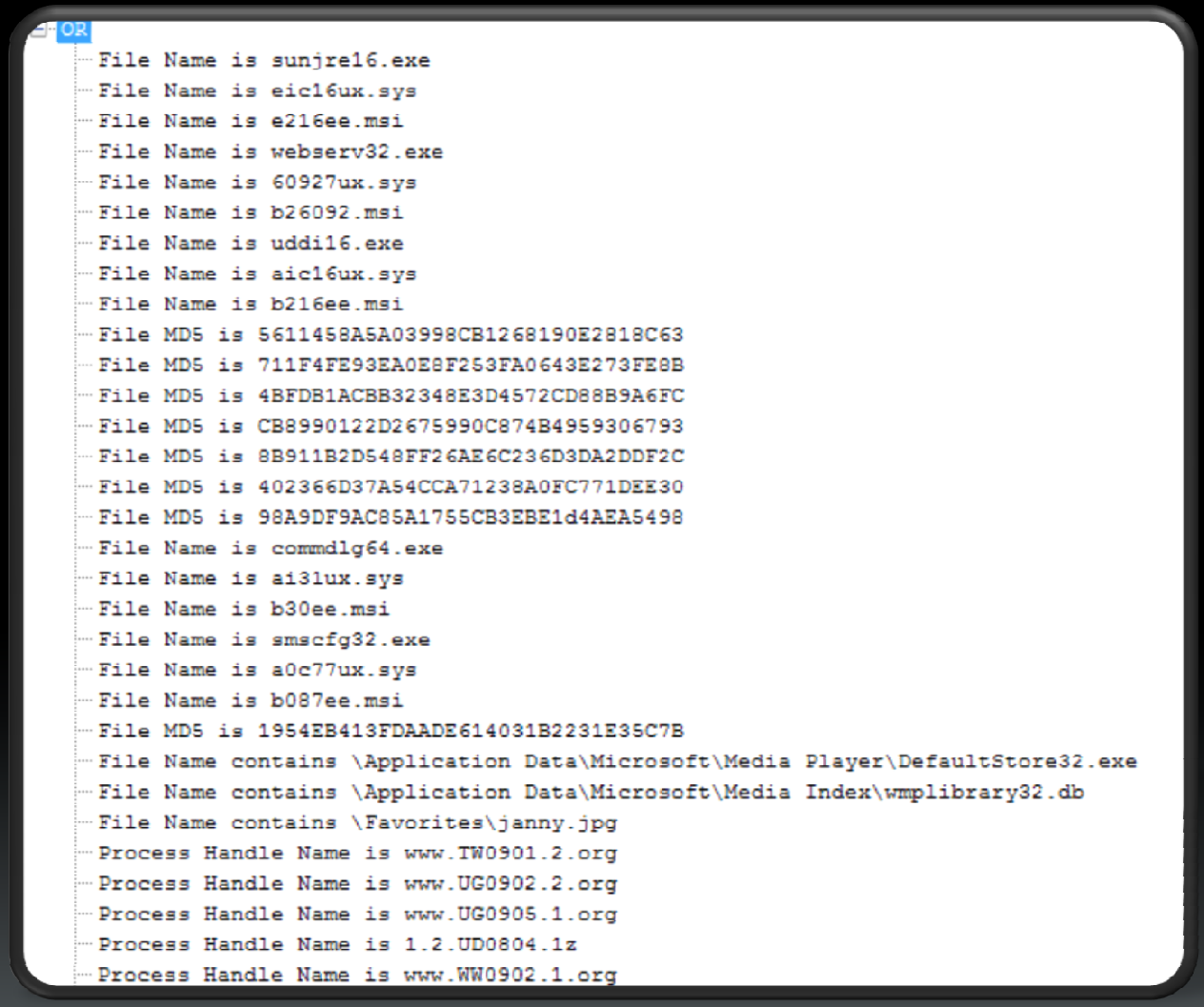
IOC Logic Tree



- Indicators are ANDs and ORs
- IndicatorItems are the leaf nodes of data

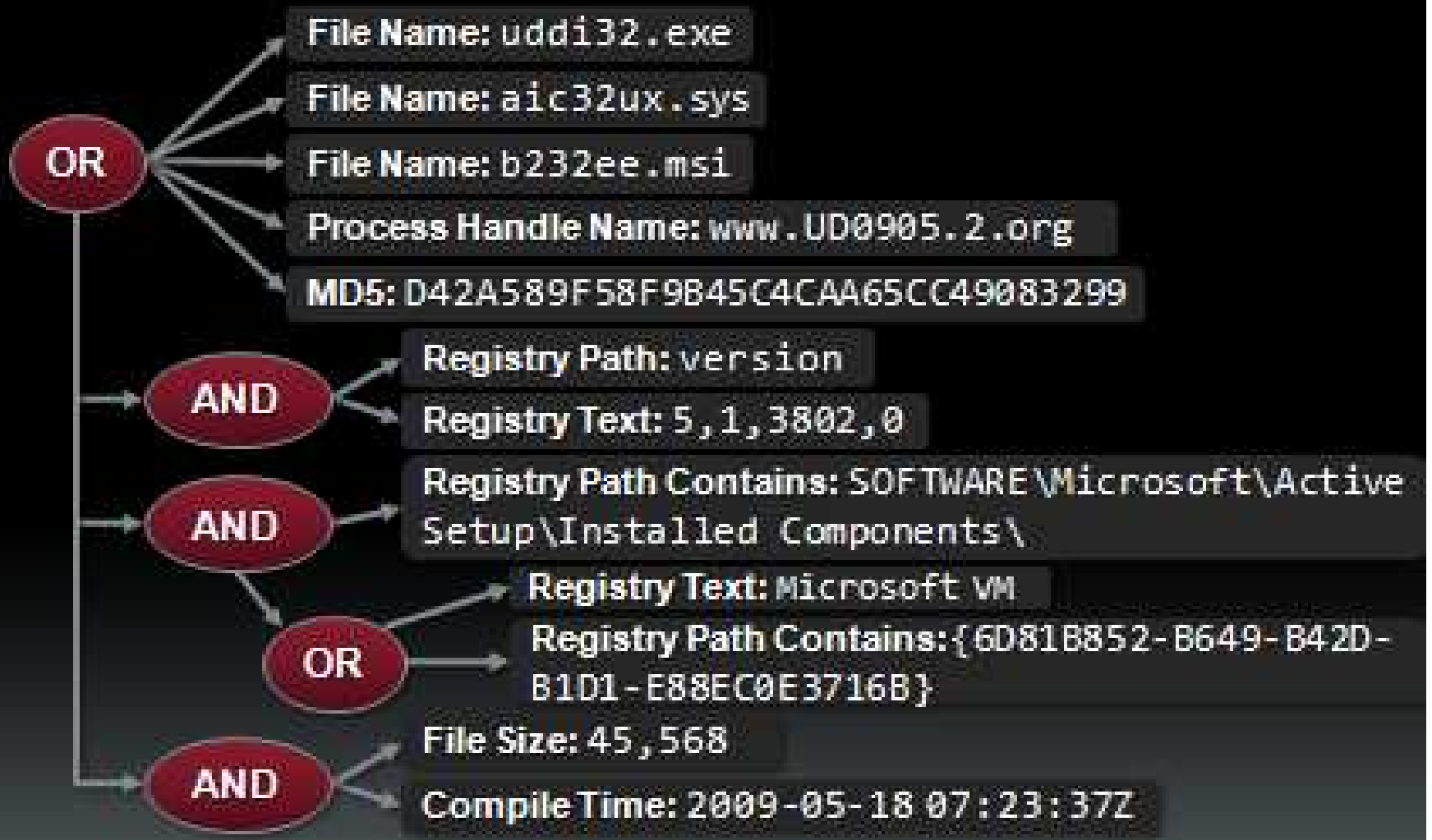
MANDIANT®

Allows this…



MANDIANT®

…to become this

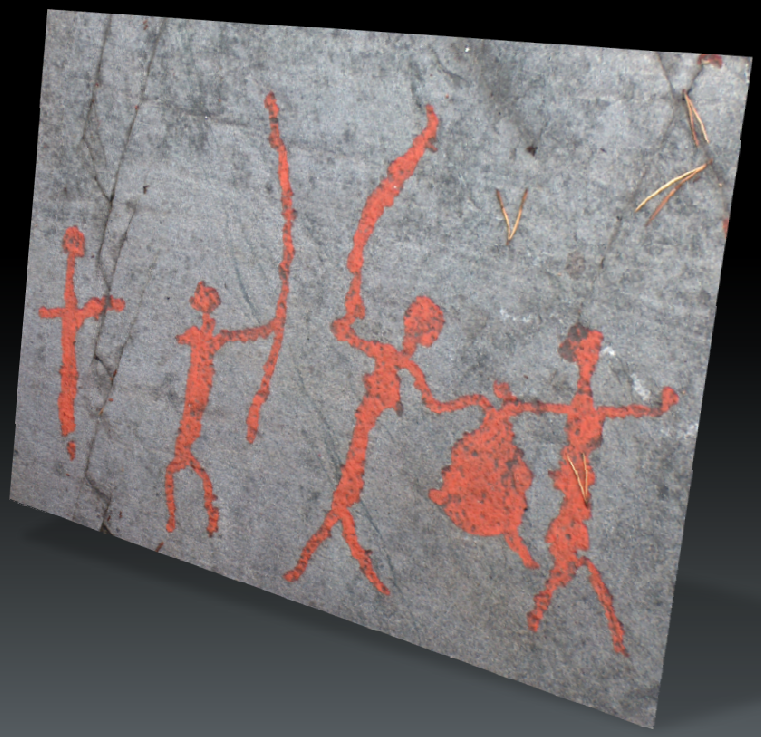


Takeaway

Easily describe the attacker's TTPs in ways that are difficult or expensive to evade.

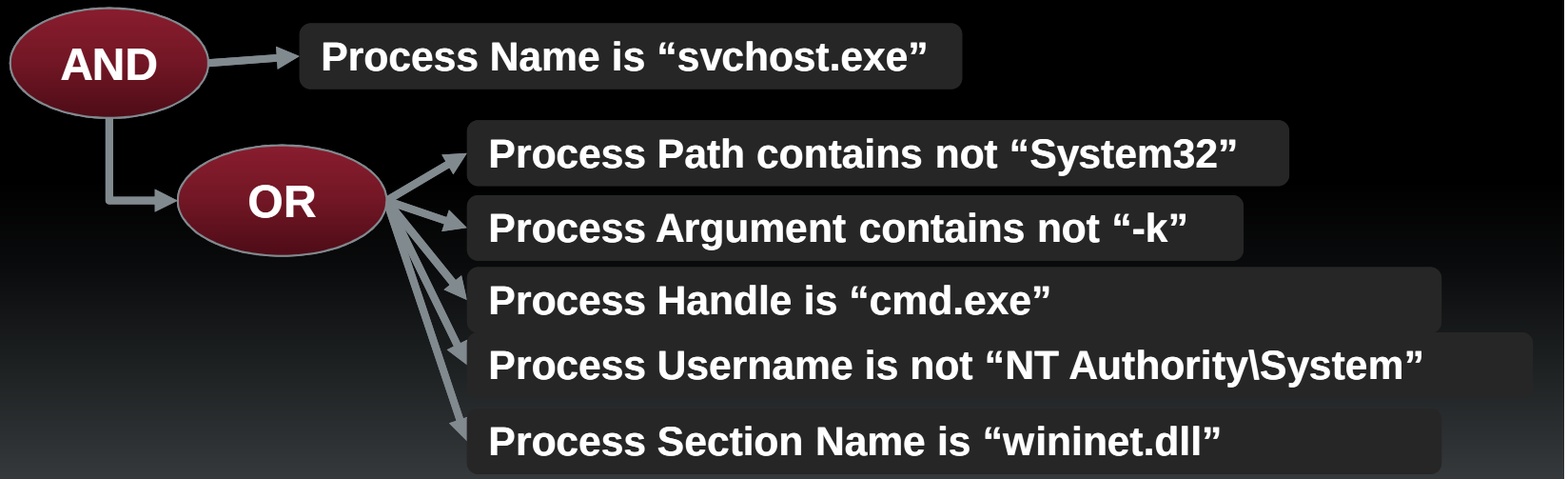
Storing general IR process

- Store general IR knowledge
- Generate ‘Generic Indicators’
- Share ‘tribal knowledge’



A thousand words in one IOC

"When you see svchost.exe running out of something other than 'system32' or it doesn't have that dash k at the end or it's not being run as System or…"



Where do I get it?

- www.mandiant.com/products/free_software/ioce/
- IOCe the editor
- Schemas
- XML and XSLT examples
- Much, much more!

MANDIANT®

Q&A

- david.ross@mandiant.com

- More MANDIANT info
  - http://www.mandiant.com/
  - http://www.twitter.com/mandiant
  - info@mandiant.com

MANDIANT

MANDIANT®