

Doug Wilson | Principal Consultant



Approaching Real-Time Information Sharing with OpenIOC

21-August 2012
GFIRST
Marriott Marquis
Atlanta Georgia



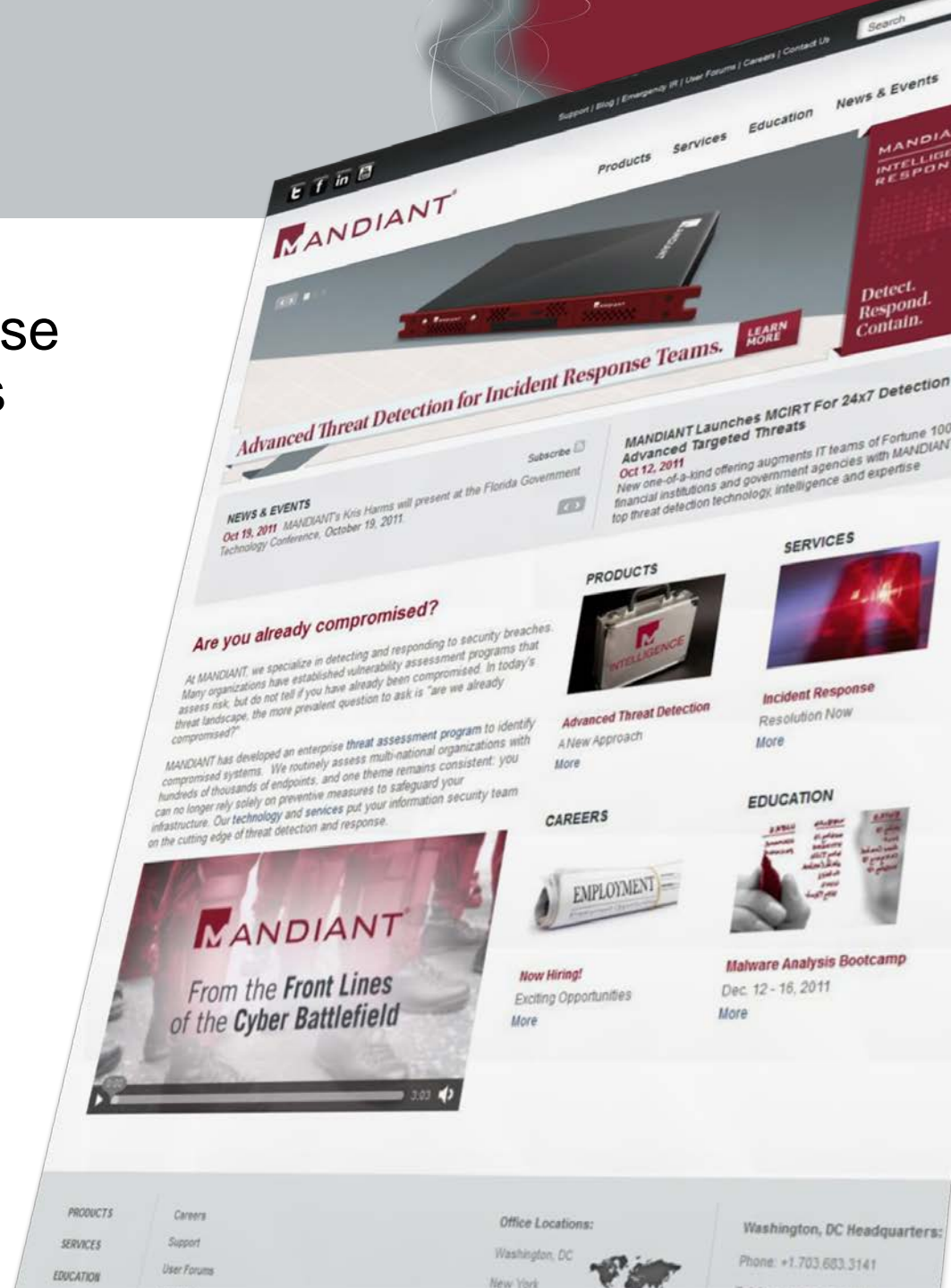
DOUG WILSON

- Principal Consultant
- OpenIOC Advocate
- Background
 - Decade + in Infosec
 - Web Hosting
 - Incident Response
 - Multi-Tiered Applications



We are Mandiant

- Threat detection, response and containment experts
- Software, professional & managed services, and education
- Application and network security evaluations
- Offices in
 - Washington
 - New York
 - Los Angeles
 - San Francisco



Why are we here today?



- Needs
- Problems
- Solutions

NEEDS?



PREVENTION
PREVENTION
PREVENTION
PREVENTION
PREVENTION
PREVENTION
PREVENTION
PREVENTION
PREVENTION
PREVENTION

~~PREVENTION~~



~~PREVENTION~~

DETECT

RESPOND

CONTAIN



- Threat Information/Threat Intelligence
- The ability to scale to the Enterprise
- The ability to share Threat Intelligence with others

PROBLEMS!



How do we share?
OF COURSE!

We write reports.

Lots and lots of reports
and
documents/pdfs/bulletins
/etc/ad/nauseum



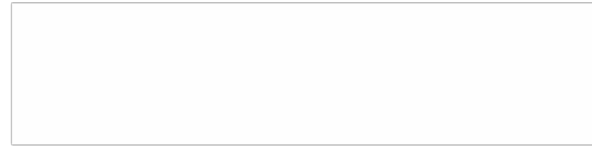
Reports empower
processes that work at
“paper” speed

Reports don't empower
much else

without some work



Lost



Time

Resources

Money

Value of Intel



- Threat Information/Threat Intelligence
 - Recorded by Humans as they go.
 - In a Human Readable Format.
- The ability to scale to the Enterprise
 - Humans don't scale (at least not efficiently).
 - Machines scale.
 - Translating from Human to Machine costs resources
- The ability to share Threat Intelligence with others
 - Transferring between organizations requires a LOT of resources, AND translation, even if just Human to Human

Well, that was cheery . . .

SOLUTIONS(?)



Traditional Threat Information Sharing

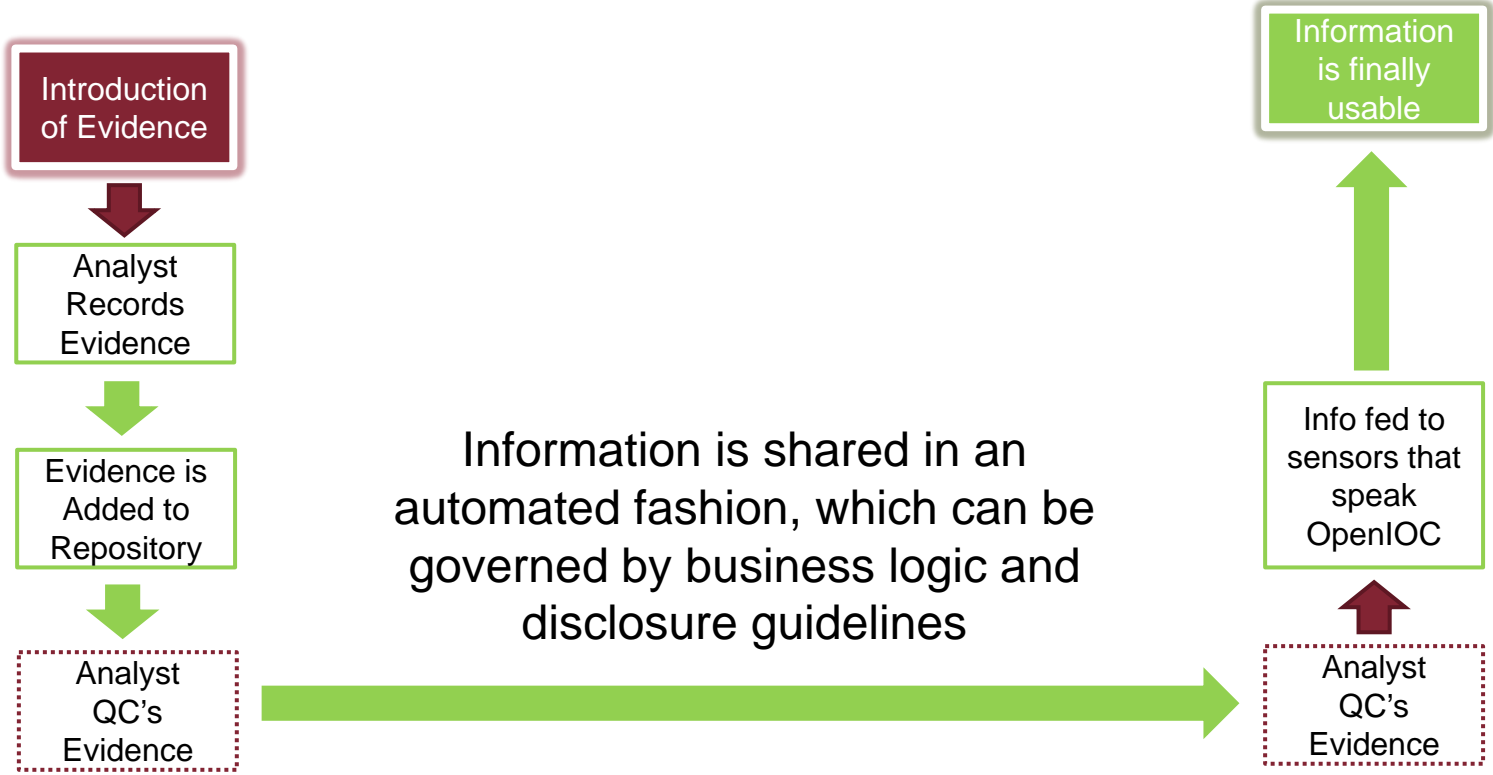


= Automated Process

= Optional Step

= Manual Process

Automated Threat Information Sharing



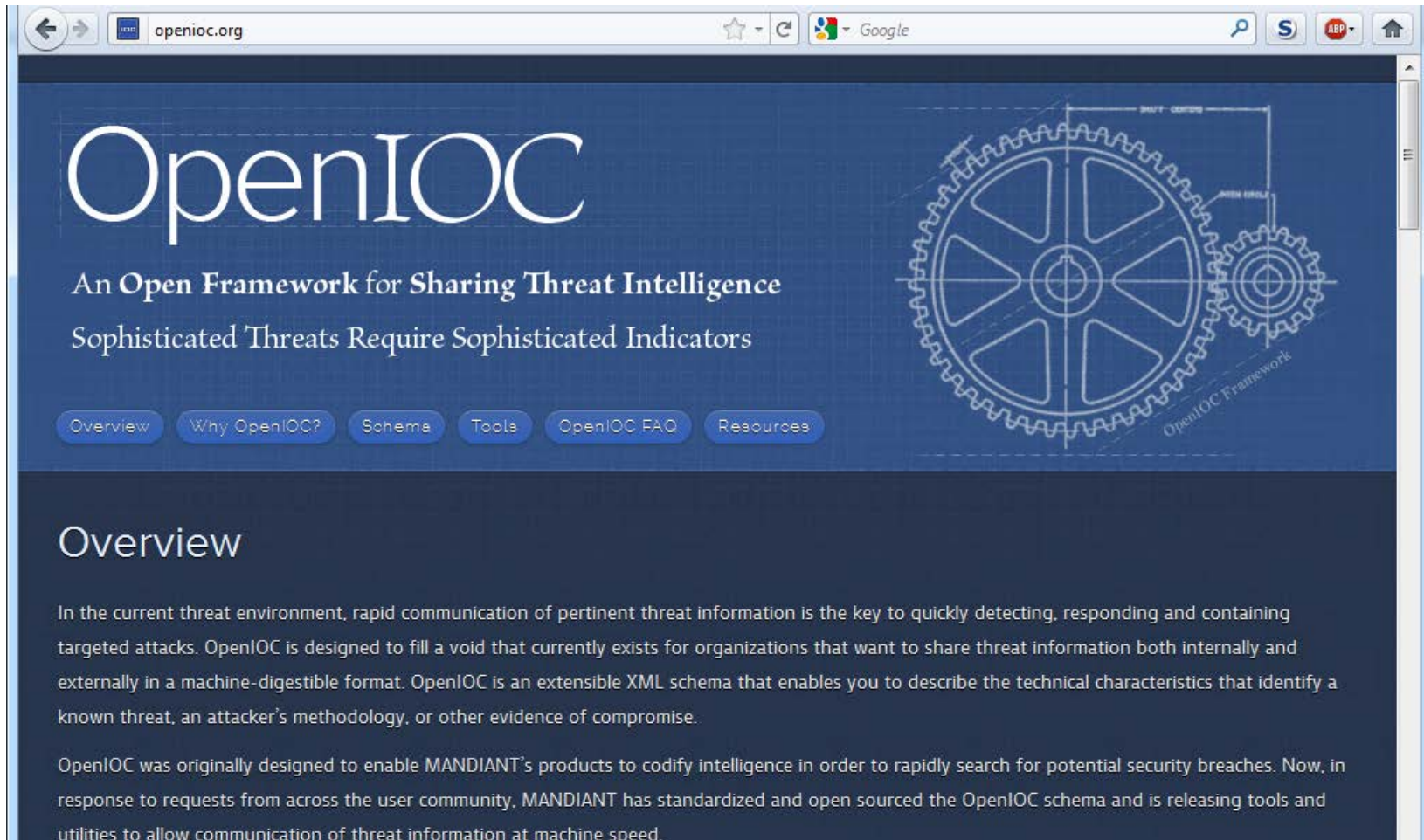
= Automated Process = Optional Step = Manual Process

- Threat Information/Threat Intelligence
 - Record it in a machine readable format at the start.
- The ability to scale to the Enterprise
 - Machines scale.
- The ability to share Threat Intelligence with others
 - You still have layer 8 problems to tackle.
 - But many of those are going to require decisions and translation. If those can be automated . . .
 - There might be some hope!

A Proposal:

Sharing of Threat Intelligence is becoming a **requirement** for **surviving** in the the current threat landscape.

Automated Sharing of Threat Intelligence can only be arrived at through **adopting common languages**.



The screenshot shows a web browser window with the address bar set to openioc.org. The page features a dark blue background with the OpenIOC logo in large white letters. Below the logo is the tagline "An Open Framework for Sharing Threat Intelligence" and the subtitle "Sophisticated Threats Require Sophisticated Indicators". A navigation menu contains buttons for Overview, Why OpenIOC?, Schema, Tools, OpenIOC FAQ, and Resources. To the right is a technical diagram of interlocking gears labeled "OpenIOC Framework". The main content area is titled "Overview" and contains two paragraphs of text.

OpenIOC

An Open Framework for Sharing Threat Intelligence
Sophisticated Threats Require Sophisticated Indicators

[Overview](#) [Why OpenIOC?](#) [Schema](#) [Tools](#) [OpenIOC FAQ](#) [Resources](#)

Overview

In the current threat environment, rapid communication of pertinent threat information is the key to quickly detecting, responding and containing targeted attacks. OpenIOC is designed to fill a void that currently exists for organizations that want to share threat information both internally and externally in a machine-digestible format. OpenIOC is an extensible XML schema that enables you to describe the technical characteristics that identify a known threat, an attacker's methodology, or other evidence of compromise.

OpenIOC was originally designed to enable MANDIANT's products to codify intelligence in order to rapidly search for potential security breaches. Now, in response to requests from across the user community, MANDIANT has standardized and open sourced the OpenIOC schema and is releasing tools and utilities to allow communication of threat information at machine speed.

The OpenIOC format

- IOC = “Indicator of Compromise”

- OpenIOC =
 - Organize your Threat Intelligence
 - Logical groupings of forensic artifacts
 - Based on real world experience
 - Extendable & expandable XML
 - NOT just for malware

- Lists of stuff to find evil
 - Easy to create
 - Difficult to maintain
 - Terrible to share
- Lists do not provide context
 - An MD5 of what?
 - Who gave me this?
 - Where is the report?
 - Where is the intelligence??
- Lists encourage reliance on easily mutable forensic artifacts



OpenIOC allows this...

```
OR
... File Name is sunjre16.exe
... File Name is eic16ux.sys
... File Name is e216ee.msi
... File Name is webserv32.exe
... File Name is 60927ux.sys
... File Name is b26092.msi
... File Name is uddi16.exe
... File Name is aic16ux.sys
... File Name is b216ee.msi
... File MD5 is 5611458A5A03998CB1268190E2818C63
... File MD5 is 711F4FE93EAOE8F253FA0643E273FE8B
... File MD5 is 4BFDB1ACBB32348E3D4572CD88B9A6FC
... File MD5 is CB8990122D2675990C874B4959306793
... File MD5 is 8B911B2D548FF26AE6C236D3DA2DDF2C
... File MD5 is 402366D37A54CCA71238A0FC771DEE30
... File MD5 is 98A9DF9AC85A1755CB3EBE1d4AEA5498
... File Name is commdl64.exe
... File Name is ai3lux.sys
... File Name is b30ee.msi
... File Name is smscfg32.exe
... File Name is a0c77ux.sys
... File Name is b087ee.msi
... File MD5 is 1954EB413FDAADE614031B2231E35C7B
... File Name contains \Application Data\Microsoft\Media Player\DefaultStore32.exe
... File Name contains \Application Data\Microsoft\Media Index\wmplibrary32.db
... File Name contains \Favorites\janny.jpg
... Process Handle Name is www.TW0901.2.org
... Process Handle Name is www.UG0902.2.org
... Process Handle Name is www.UG0905.1.org
... Process Handle Name is 1.2.UD0804.1z
... Process Handle Name is www.WW0902.1.org
```

...to become this

The screenshot shows a software interface for defining a malware indicator. The main window is titled "STUXNET VIRUS (METHODOLOGY)".

Metadata:

- Name: STUXNET VIRUS (METHODOLOGY)
- Author: Mandiant
- GUID: ea3cab0c-72ad-40cc-abbf-90846fa4:

Description:

Generic indicator for the stuxnet virus. When loaded, stuxnet spawns lsass.exe in a suspended state. The malware then maps in its own executable section and fixes up the CONTEXT to point to the newly mapped in section. This is a common task performed by malware and allows the malware to execute under the pretense of a known and trusted process.

Definition:

The definition is a tree structure of logical conditions:

- OR
 - File Section Name contains .stub
 - File Name contains mdmcpq3.PNF
 - File Name contains mdmeric3.PNF
 - File Name contains oem6C.PNF
 - File Name contains oem7A.PNF
 - File Section Name contains .stub
 - AND
 - DriverItem/DeviceItem/AttachedToDriverName contains fs_rec.sys
 - DriverItem/DeviceItem/AttachedToDriverName contains mrxsmb.sys
 - DriverItem/DeviceItem/AttachedToDriverName contains sr.sys
 - DriverItem/DeviceItem/AttachedToDriverName contains fastfat.s
 - AND
 - File Name contains mrxcls.sys
 - File CertificateSubject contains Realtek Semiconductor Corp

Buttons for "Item", "AND", "OR", "Delete", and "Save" are visible.



- 37 terms shown (out of over 500)
- MANDIANT terms drawn from real world
- Terms easily added if needed.

Characteristics	Definition of Characteristic
File Accessed Time	Last access time of a file
File Attribute	Attributes of a file (Read-only, Hidden, System Directory, etc.)
File Changed Time	File name modified of a file
File Compile Time	Checks the compile time of a file
File Created Time	Creation time of a file
File Digital Signature Description	Description of whether the signature is verified or not
File Digital Signature Exists	Verifies that a digital signature exists
File Digital Signature Verified	Verifies a digital signature is valid
File Export Function	Export function declared by a file
File Extension	Extension of a file
File Full Path	Full path for a file
File Import Function	Import function declared by a file
File Import Name	Import name declared by a file
File MD5	MD5 of the file
File Modified Time	Modified time of a file
File Name	Name of a file
File Owner	Owner of the file
File Path	Path of a file
File PE Type	Checks the PE type of a file

Characteristics	Definition of Characteristic
File PeakEntropy	Peak entropy of a file
File Raw Checksum	Calculated checksum of a file
File Size	Size of the file
File Strings	Readable strings of a file's binary data
Network DNS	DNS queries on a network
Network String URI	URI associated with network traffic
Network String User Agent	User agent associated with network traffic
Process Handle Name	Name of a process handle
Process Name	Name of a process
Registry Key ModDate	Modification time of a registry key
Registry NumSubKeys	Checks the total number of subkeys associated to a registry key
Registry Path	Path of a registry item
Registry Text	Contents of the registry text field
Service Descriptive Name	Description text of a service
Service DLL	DLL implemented by a service
Service Name	Name of a Service
Service Path	Path to the service file
Service Status	Checks the current status of a service

IOCs and the Investigative Process



IOCs allow you to:

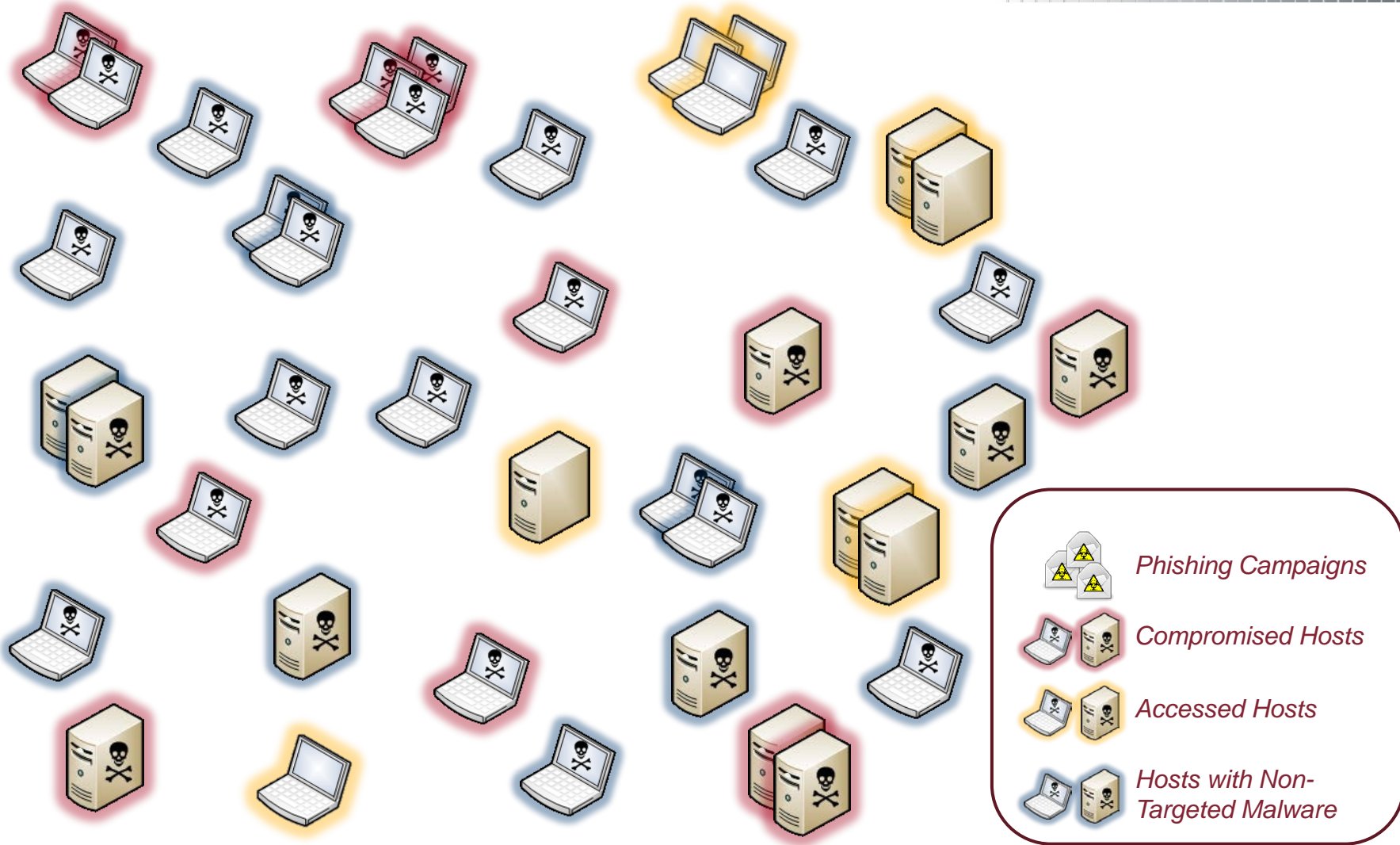
- Automate the sharing of threat intelligence.
- Find attackers across ALL systems.
 - not just ones with malware.

Traditional IR is following Breadcrumbs

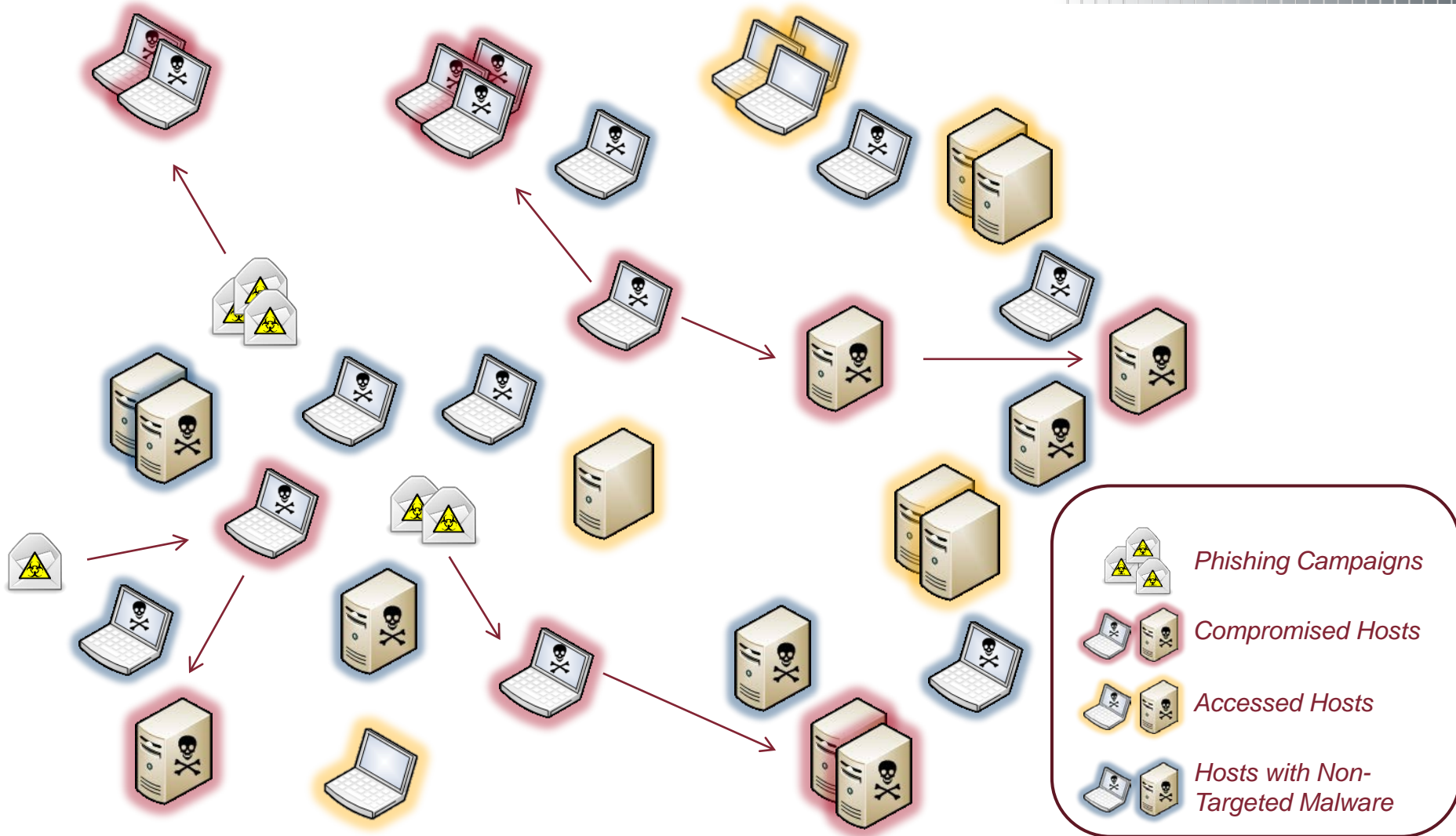


Breadcrumbs will not show the whole picture

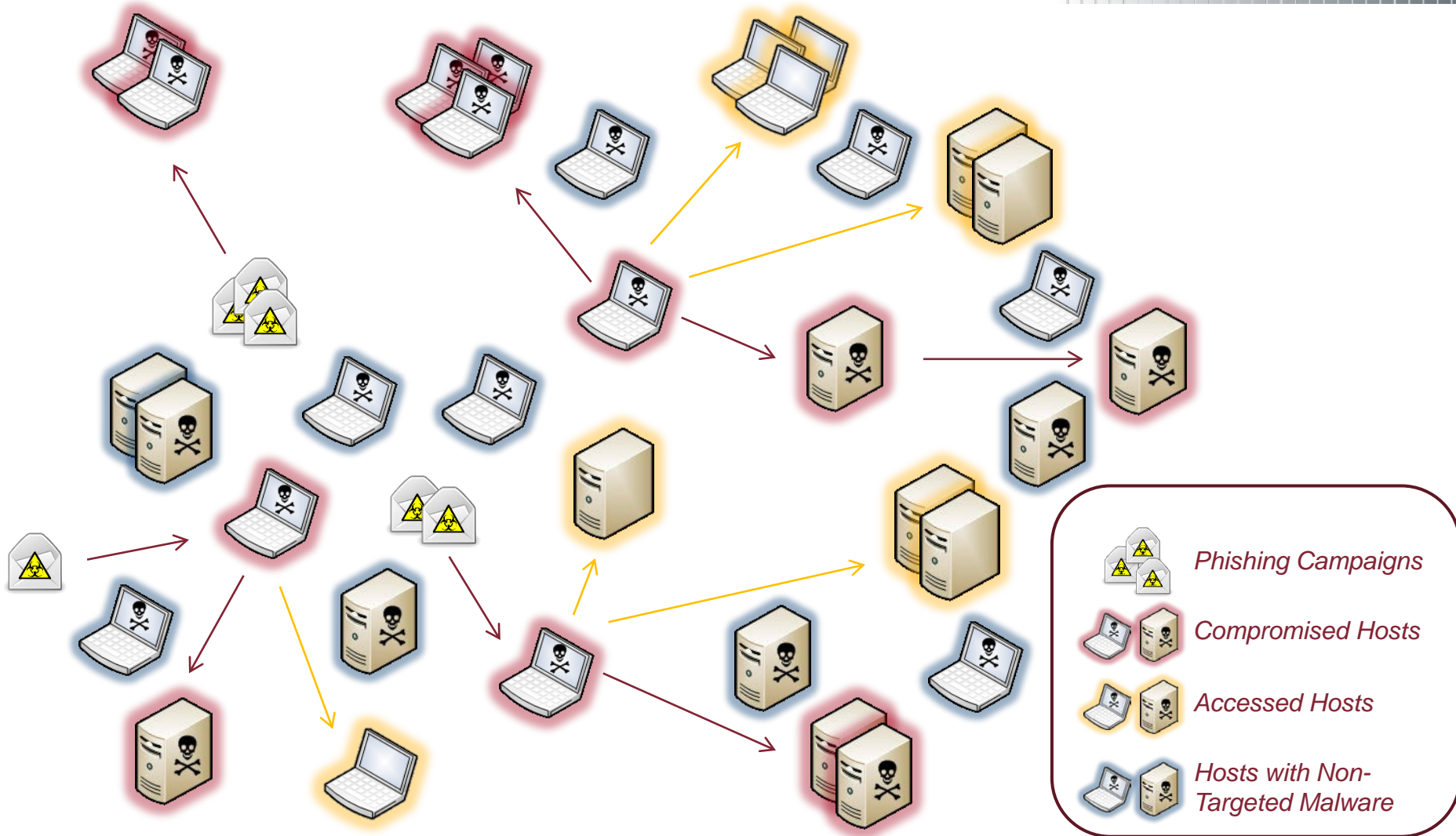
What's out there(?)



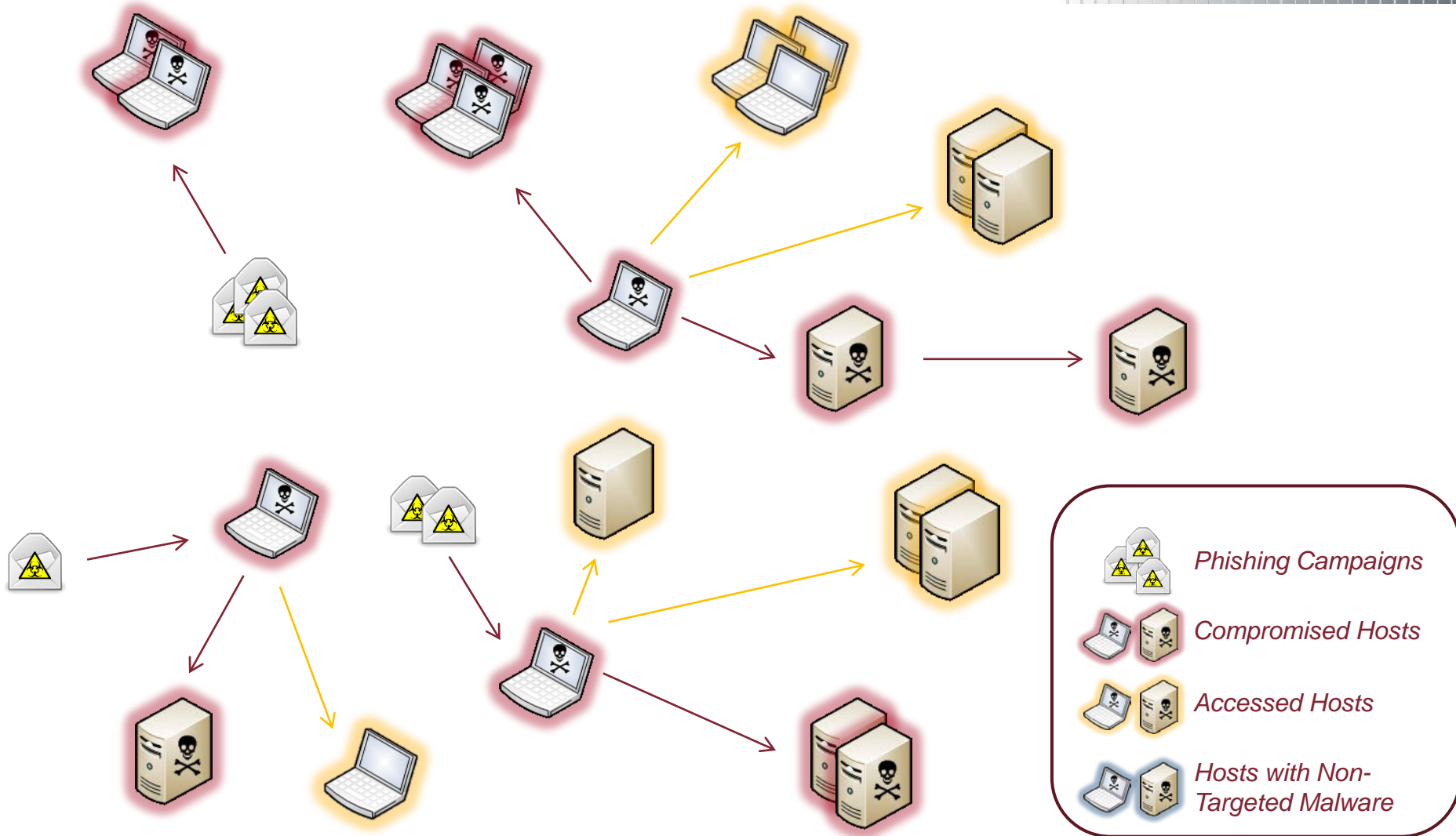
What's out there(?)



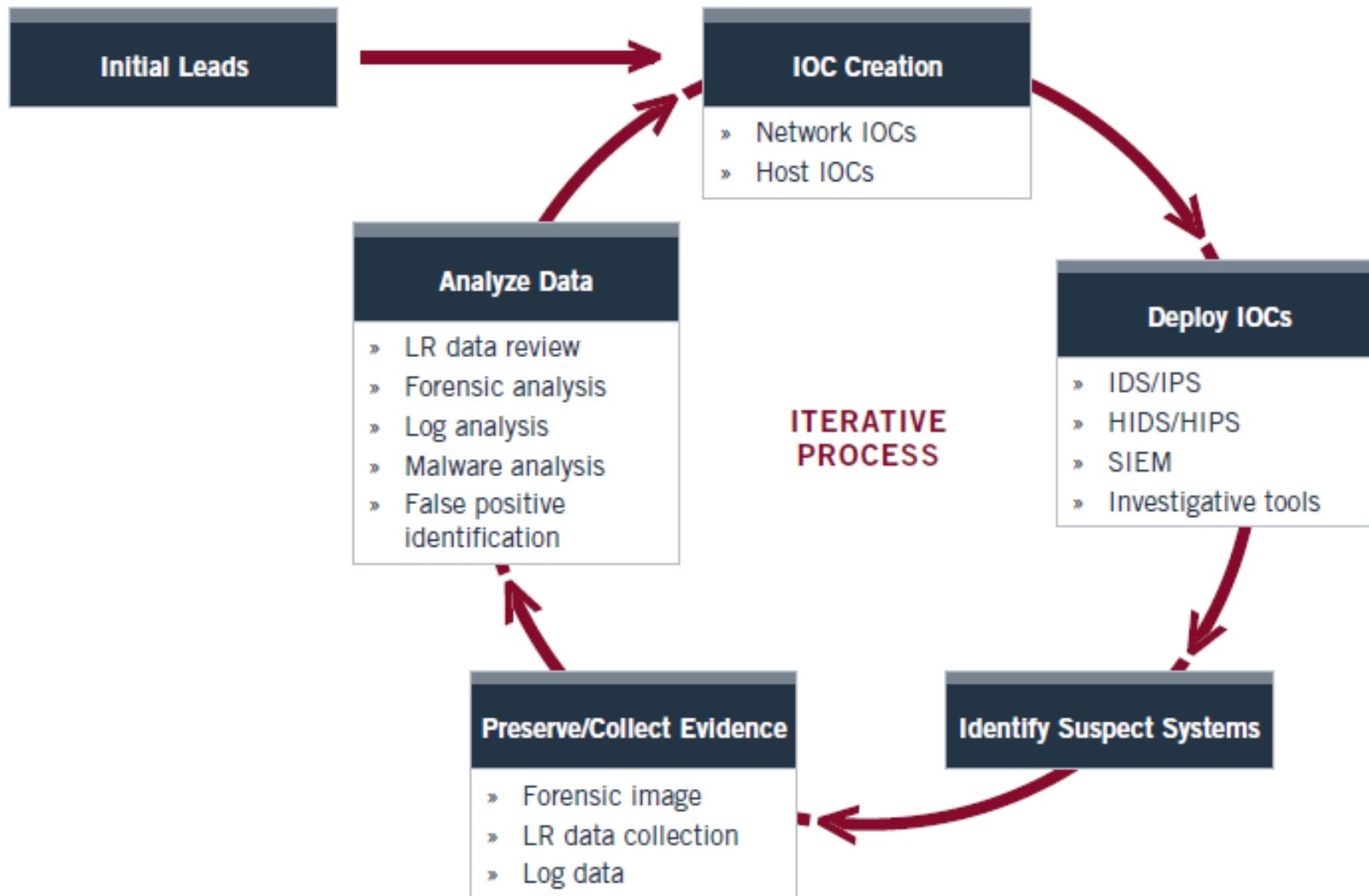
What's out there(?)



What's out there(?)

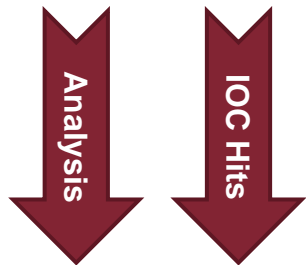


Using IOCs in the investigative lifecycle

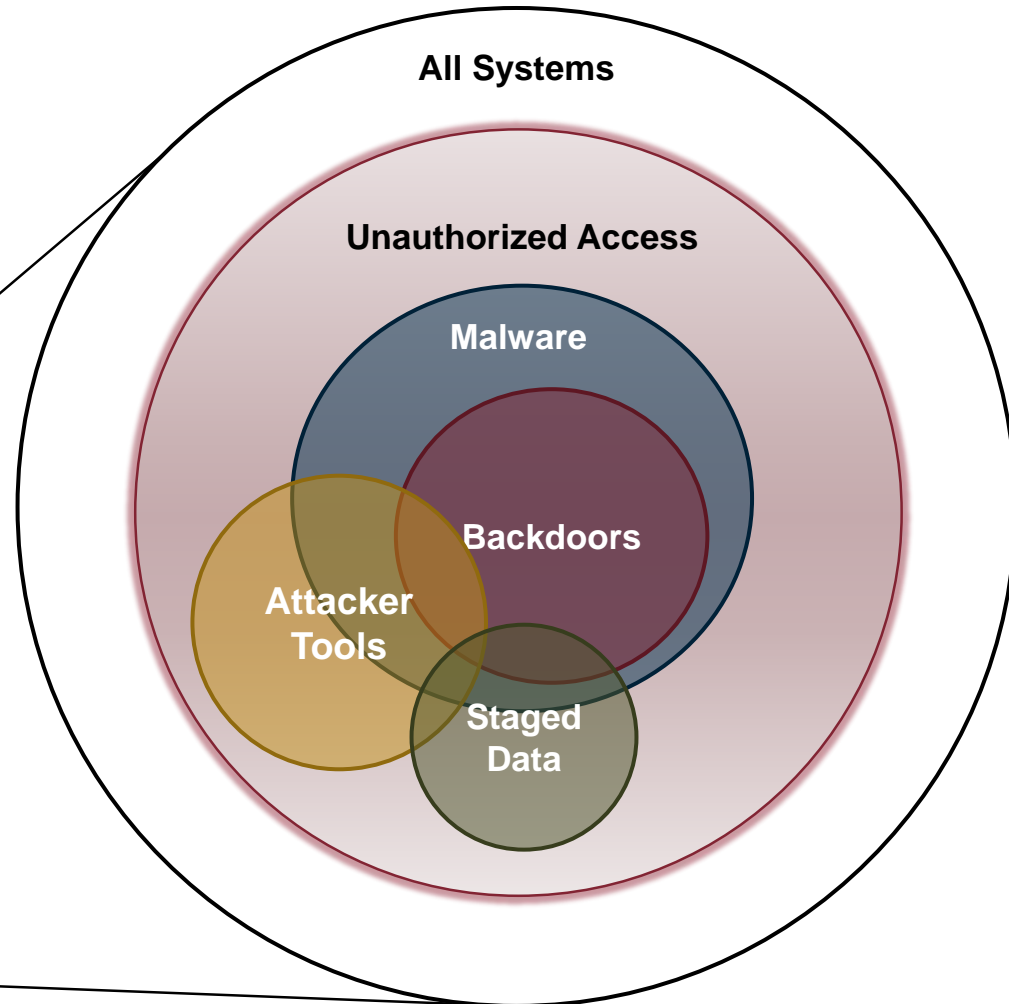


Scoping the incident

What are you really trying to detect?



- ❑ Backdoored systems
- ❑ Systems with malware
- ❑ Accessed systems
- ❑ Systems with staged data
- ❑ Compromised credentials



- IOCs can evolve during investigations
- Record investigative logic in IOCs
- Lets you look “beyond the malware”
 - Hosts can be accessed without malware
 - Go after attackers by methodology
- Helps increase confidence by covering the entire enterprise

A Quick Case Study

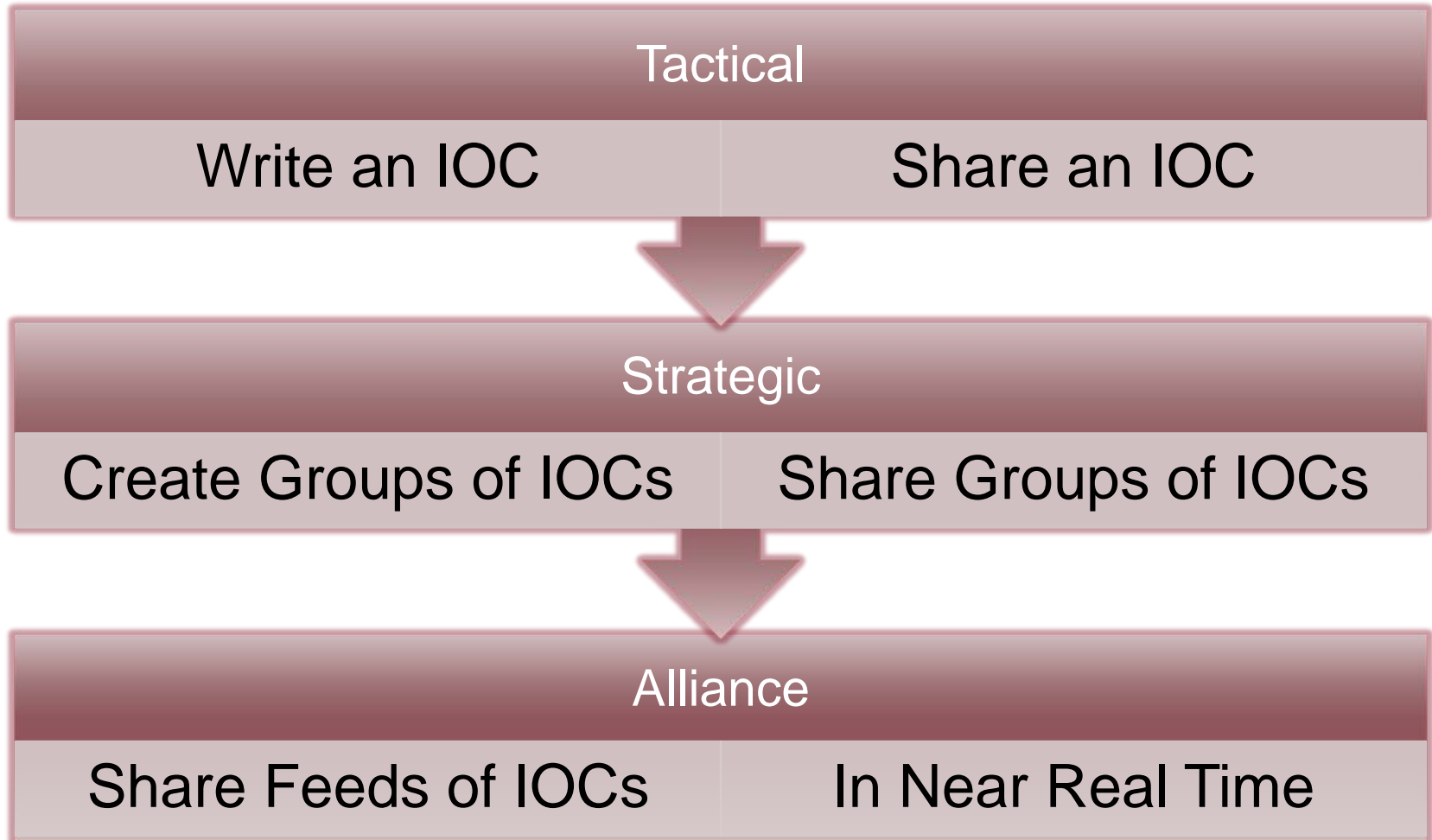


- A previous year at MIRCon
 - FFRDC Piloting MIR. MIR uses OpenIOC for IOCs.
 - Developed IOCs, used them to track Adversaries and observe them in their network.
 - IR occurred – including observation before remediation.
 - Management forced remediation after seeing exfiltration.
 - Remediation occurred, and everyone called it a week.

- There was this other lab, see . . .
 - In the same vertical (very much so)
 - Being attacked by the same Adversary
 - At the same time

- Persistent Adversaries adapt. So, when one door closed . . . They went to town on the other.

- The second lab was owned, with no subtlety
- They hit the panic button
- Many agencies who responded to incidents, well . . . responded.
- But what could they find in a day or two?
 - Not much
- Someone from the first lab suggested that maybe they should try looking for what they had described in their IOCs.
- And?



Lessons Learned (in our first year)



- Writing good IOCs is hard!
 - Much like IR knowledge . . .
 - Need to find ways to share more tribal knowledge
- Tools that use IOCs are good. More tools are better.
 - Constantly talking to new groups and vendors who want to use OpenIOC
- We are not in a vacuum!
 - There are other projects out there, and we look forward to working with them.
 - This ONLY works if we work together.
 - Check out HHS presentation after this, STIX & TAXII

The Future?



A humble proposition

A standard, machine readable format ✓

Build Communities ✓

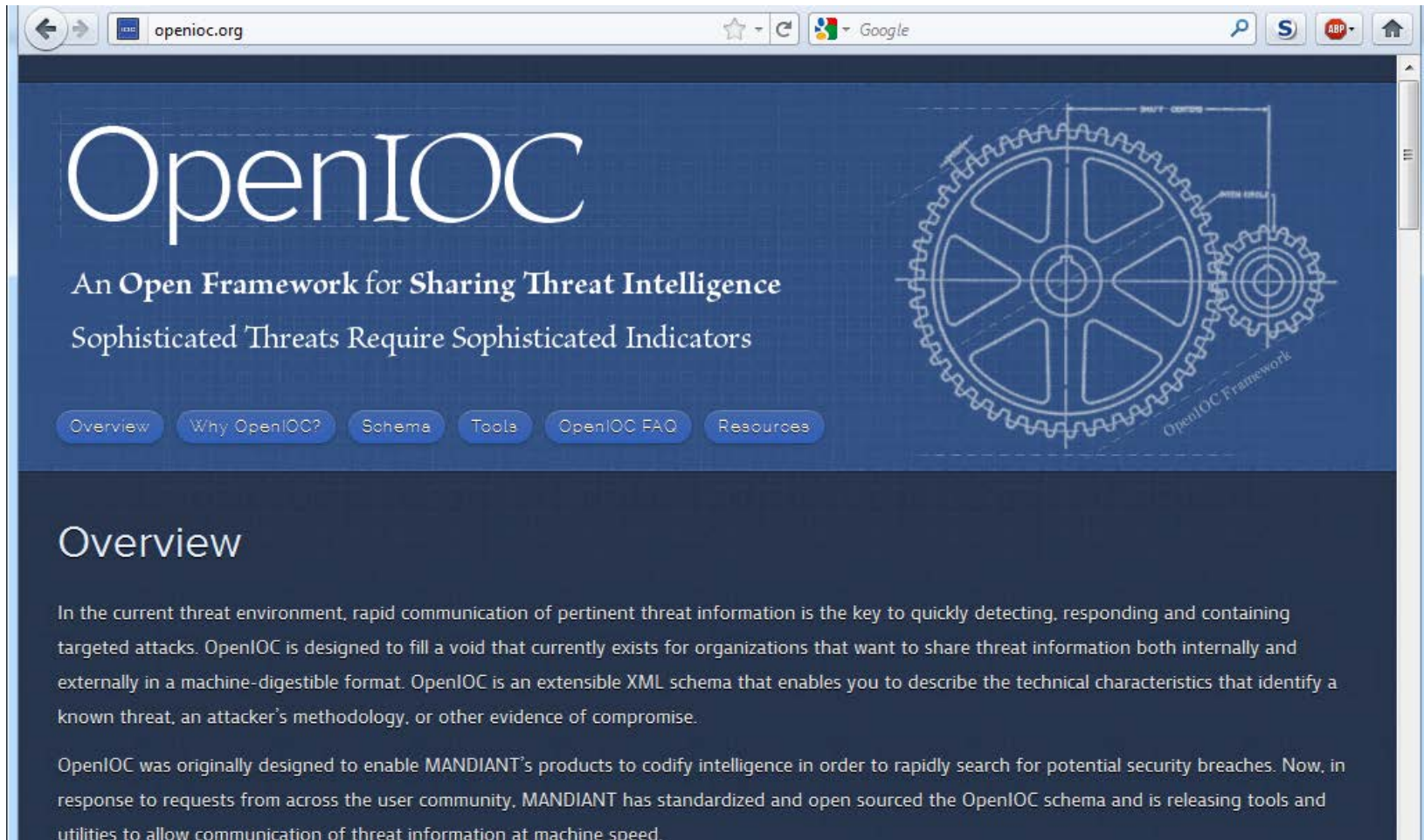
Build SMARTER Communities ✓

Speed up the rate of sharing ?

Automate more as you learn to trust ?

The bad guys have them, do you?





The screenshot shows a web browser window with the address bar displaying "openioc.org". The page features a dark blue background with the "OpenIOC" logo in large white letters. Below the logo, the text reads "An Open Framework for Sharing Threat Intelligence" and "Sophisticated Threats Require Sophisticated Indicators". A navigation menu contains buttons for "Overview", "Why OpenIOC?", "Schema", "Tools", "OpenIOC FAQ", and "Resources". On the right side, there is a technical diagram of interlocking gears with labels "SHIFT GEAR", "WHEEL GEAR", and "OpenIOC Framework". The "Overview" section is expanded, showing a paragraph about the current threat environment and the purpose of OpenIOC, followed by another paragraph about its origin at MANDIANT.

OpenIOC

An Open Framework for Sharing Threat Intelligence
Sophisticated Threats Require Sophisticated Indicators

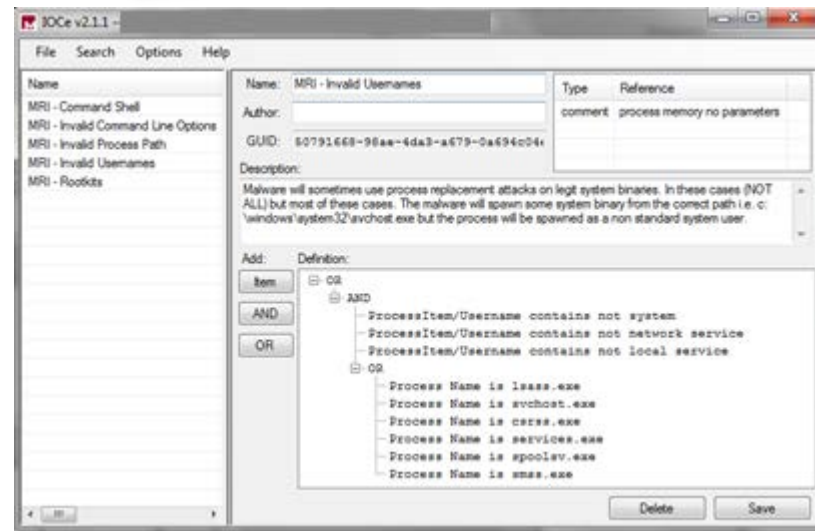
[Overview](#) [Why OpenIOC?](#) [Schema](#) [Tools](#) [OpenIOC FAQ](#) [Resources](#)

Overview

In the current threat environment, rapid communication of pertinent threat information is the key to quickly detecting, responding and containing targeted attacks. OpenIOC is designed to fill a void that currently exists for organizations that want to share threat information both internally and externally in a machine-digestible format. OpenIOC is an extensible XML schema that enables you to describe the technical characteristics that identify a known threat, an attacker's methodology, or other evidence of compromise.

OpenIOC was originally designed to enable MANDIANT's products to codify intelligence in order to rapidly search for potential security breaches. Now, in response to requests from across the user community, MANDIANT has standardized and open sourced the OpenIOC schema and is releasing tools and utilities to allow communication of threat information at machine speed.

- <http://www.mandiant.com/resources/download/ioc-editor/>
- Create an IOC from scratch
- Edit an IOC in a GUI
- Compare/Diff IOCs
- Export to XPATH queries



- <http://www.mandiant.com/resources/download/redline/>
- Single host investigation tool
- Do audits of memory, disk, registry & more
- Use IOCs to create audits and match against audits



- <http://openioc.org>
- @openioc
- <https://groups.google.com/forum/#!forum/openioc>
- <https://forums.mandiant.com/>

- <http://ioc.forensicartifacts.com>
- @digital4rensics – Keith Gilbert
- <http://labs.alienvault.com/labs/>
- @jaimeblascob – Jaime Blasco
- <http://www.malwaretracker.com/>
- @mwtracker

- Free tools
 - Redline
 - IOC Finder
 - Memoryze
 - Highlighter
 - IOC Editor
 - Audit Viewer
 - Red Curtain
 - Web Historian
 - First Response
- Online Resources
 - M-trends
 - M-unitions Blog
 - Mandiant Forums
- Education
 - Black Hat classes
 - Custom classes
- Webinar series
 - Sign up

- Find indicators of compromise on thousands of hosts
- Live IR on thousands of systems at once
- From disk images to registry keys to live memory forensics
- It's part of almost every response we do



- Third annual **M**andiant **I**ncident **R**esponse **c**onvention
- FREE (while supplies last)
- Washington DC
- 17 & 18 October, 2012
- <http://www.mandiant.com/events/mircon/>
- NOT just Mandiant presenters
 - Past have included Tony Sager, Richard Clarke, Michael Chertoff, Gordon Snow (FBI), Halvar Flake (Zynamics/Google), Richard Bejtlich, and others.
- Look for news on OpenIOC!!

Comments/Questions?

Doug Wilson

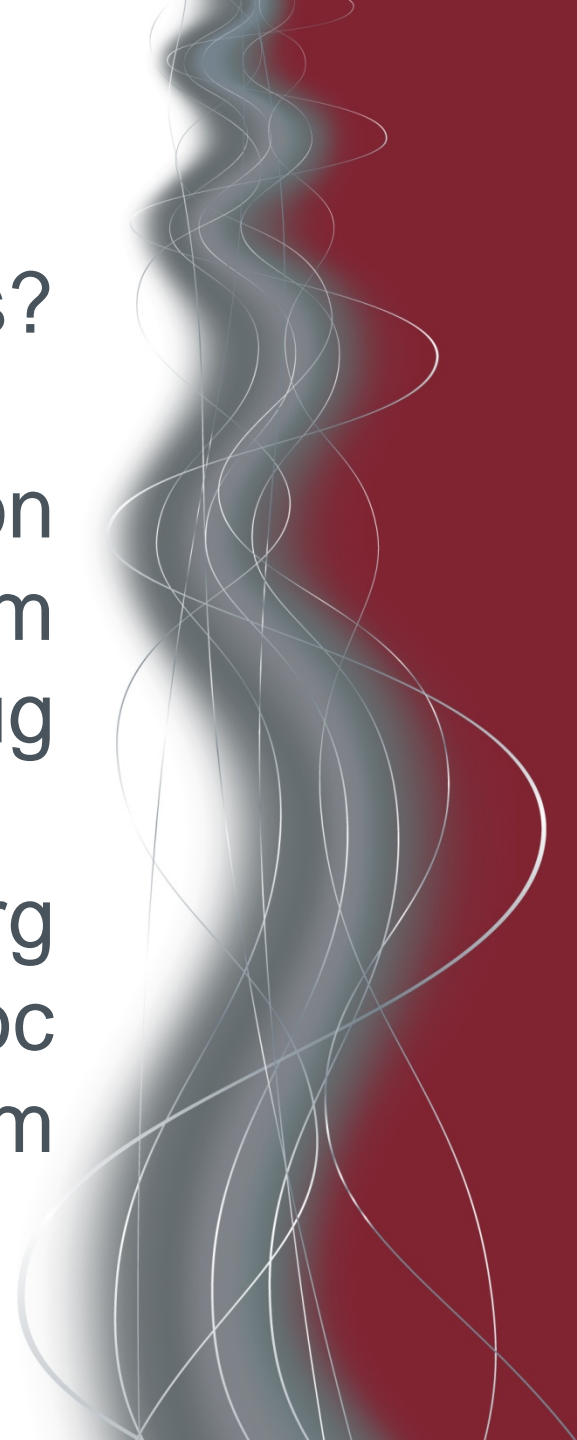
douglas.wilson@mandiant.com

[@dallendoug](#)

<http://openioc.org>

[@openioc](#)

<http://www.mandiant.com>



Doug Wilson | Principal Consultant



Approaching Real-Time Information Sharing with OpenIOC

21-August 2012
GFIRST
Marriott Marquis
Atlanta Georgia



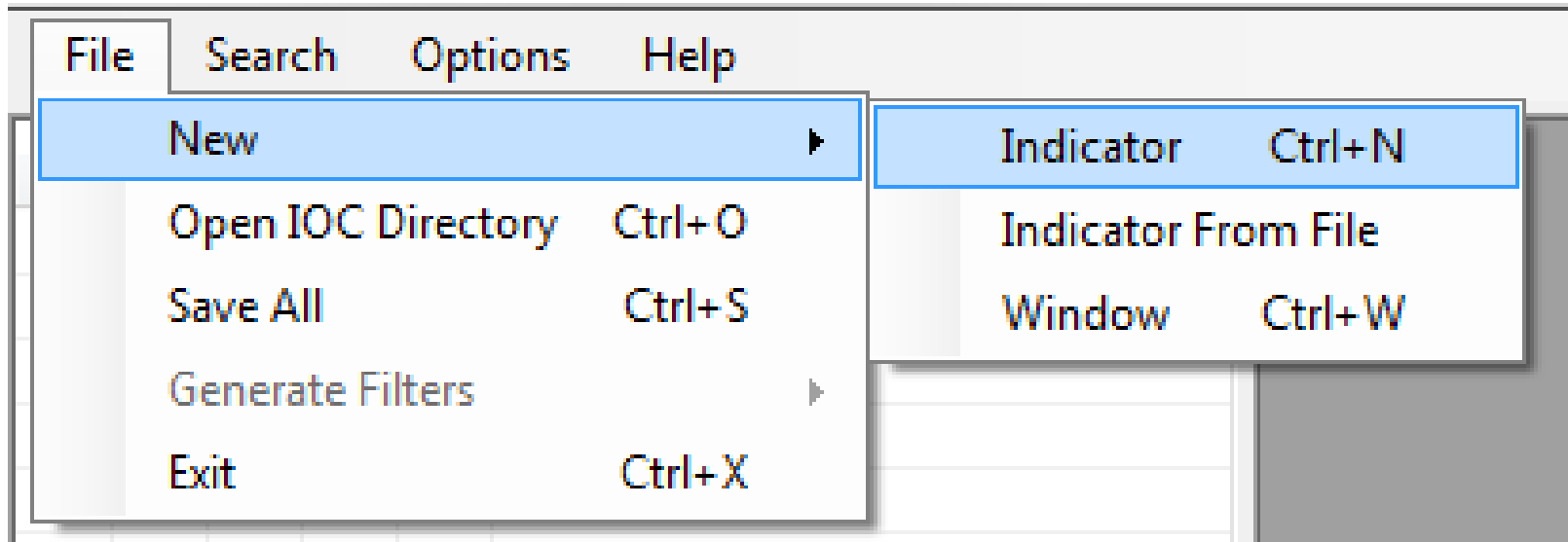
Bonus Slides from IOcing Red
Webcast (available at
Mandiant.com)



- IOC Editor
 - Free IOC creation tool available from the Mandiant website
 - Terms contained in IOC Editor can be used directly with IOCFinder or Redline
- ABC's of writing IOCs
 - If a condition, or boolean expression, evaluates to true, you have a IOC hit
 - The “is” keyword indicates an exact match
 - The “contains” keyword indicates a substring match

- APT Compromise
 - 10 systems identified
- Malware information
 - Installed as the service “lansvc”
 - ServiceDLL - “%systemroot%\system32\lansvr.dll”
 - Lansvr.dll MD5 5626906beb90b77903c3b4f43b46b450
 - File size 24,030 bytes
 - File modified 2011-09-18 17:06:15Z

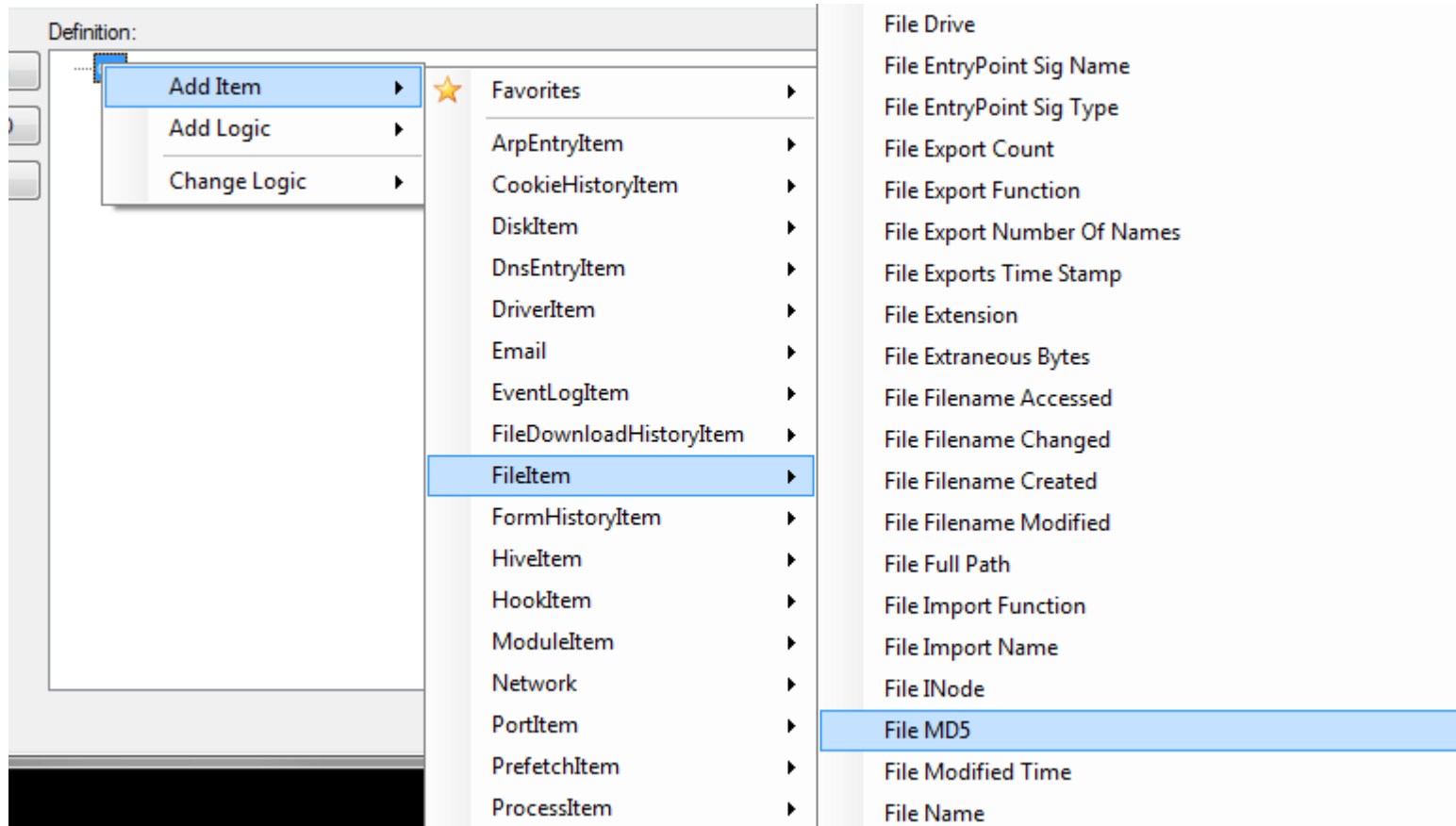
- Create a new IOC



- Fill in metadata
 - IOC name and author
 - Descriptions makes sharing easier

Name:	LANSVR.DLL (BACKDOOR)	Type	R..
Author:	William Gibb		
GUID:	1f5ecf78-e153-4e7a-b7be-251cb5d2!		
Description:	LANSVR.DLL is a backdoor which operates over HTTP protocol. Capabilites include spawning a reverse shell, enumerating and transferring files, and screen capture.		
Add:	Definition:		
Item OR		
AND			
OR			

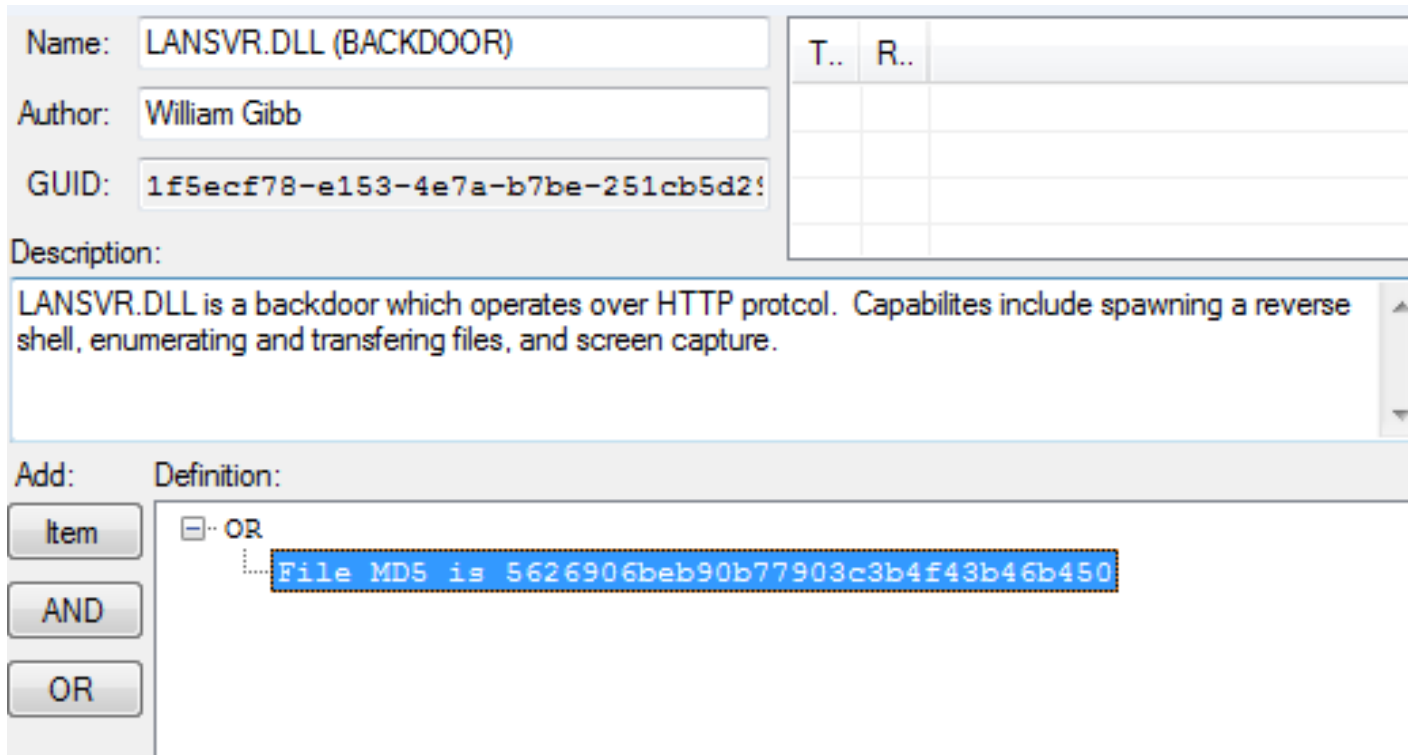
■ FileItem information



The screenshot shows the 'Definition:' pane in the IOC Editor. A context menu is open over the 'Add Item' button, with options: 'Add Item', 'Add Logic', and 'Change Logic'. The 'FileItem' category is highlighted in the main list. The right pane displays a list of file-related indicators:

- File Drive
- File EntryPoint Sig Name
- File EntryPoint Sig Type
- File Export Count
- File Export Function
- File Export Number Of Names
- File Exports Time Stamp
- File Extension
- File Extraneous Bytes
- File Filename Accessed
- File Filename Changed
- File Filename Created
- File Filename Modified
- File Full Path
- File Import Function
- File Import Name
- File INode
- File MD5
- File Modified Time
- File Name

- Add in the known MD5 hash
 - Useful for referencing the IOC and malware sample



Name: LANSVR.DLL (BACKDOOR)

Author: William Gibb

GUID: 1f5ecf78-e153-4e7a-b7be-251cb5d2!

Description:

LANSVR.DLL is a backdoor which operates over HTTP protocol. Capabilities include spawning a reverse shell, enumerating and transferring files, and screen capture.

Add: Definition:

Item OR

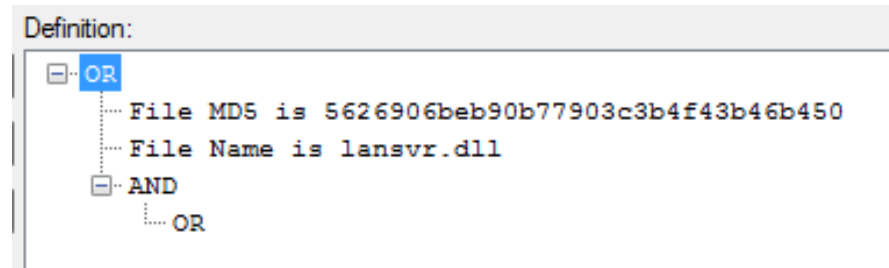
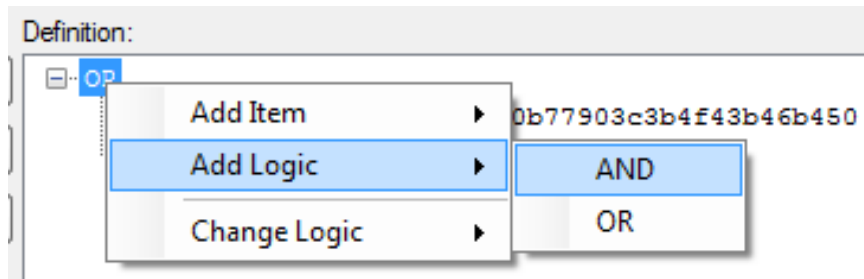
File MD5 is 5626906beb90b77903c3b4f43b46b450

T..	R..

- Add in the FileName
 - Filename of this malware is unique

```
Definition:  
[-] OR  
  ... File MD5 is 5626906beb90b77903c3b4f43b46b450  
  ... File Name is lansvr.dll
```

- Add logic to support the file modified & file size terms
 - Utilize AND/OR structure



- Add in the remaining FileItem terms
 - Date time format: YYYY-MM-DDTHH:MM:SSZ

```
Definition:
├── OR
│   ├── File MD5 is 5626906beb90b77903c3b4f43b46b450
│   ├── File Name is lansvr.dll
│   └── AND
│       ├── File Modified Time is 2011-09-18T17:06:15Z
│       └── OR
│           ├── File PE Type is Dll
│           └── File Size is 24030
```

- Read as a boolean expression – (PE Type contains DLL OR Size contains 24030) AND Modified Date is 2011-09-18T17:06:15Z

- Add in service information
 - Service DLL
 - Service DLL MD5
 - Service Name
 - Could also add Signature information as well, if a legitimate service is hijacked

FileItem	▶	Service DLL Certificate Subject
FormHistoryItem	▶	Service DLL MD5
HiveItem	▶	Service DLL Sha1sum
HookItem	▶	Service DLL Sha256sum
ModuleItem	▶	Service DLL Signature Description
Network	▶	Service DLL Signature Verified
PortItem	▶	Service DLLSignature Exists
PrefetchItem	▶	Service mode
ProcessItem	▶	Service Name
RegistryItem	▶	Service Path
RouteEntryItem	▶	Service Path Certificate Issuer
ServiceItem	▶	Service Path Certificate Subject
Snort	▶	Service Path MD5
SystemInfoItem	▶	Service Path Sha1sum
SystemRestoreItem	▶	Service Path Sha256sum

- ServiceItem terms added
 - “Service Name is lansvc” – we do not want to return wlansvc service

Definition:

```
[-] OR
  ... File MD5 is 5626906beb90b77903c3b4f43b46b450
  ... File Name is lansvr.dll
  ... Service DLL contains lansvr.dll
  ... Service Name is lansvc
  ... Service DLL MD5 is 5626906beb90b77903c3b4f43b46b450
  [-] AND
    ... File Modified Time is 2011-09-18T17:06:15Z
    [-] OR
      ... File PE Type is Dll
      ... File Size is 24030
```

- Malware analysis reveals additional information about lansvr.dll
 - Connects to www.a11thewidgets.com
 - Looks for C2 information in the HTML comment “<-- @\$robo”
 - User-agent string “Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 4.0; robo)”

- Add NetworkInfo items
 - DNS, Strings, User Agent strings are all useful
 - Can feed IOC data into network monitoring systems

Network ▶	Network DNS
PortItem ▶	Network String General
PrefetchItem ▶	Network String HTTP Referr
ProcessItem ▶	Network String URI
RegistryItem ▶	Network String User Agent

- Network items added

Definition:

```
[-] OR
  ... File MD5 is 5626906beb90b77903c3b4f43b46b450
  ... File Name is lansvr.dll
  ... Service DLL contains lansvr.dll
  ... Service Name is lansvc
  ... Service DLL MD5 is 5626906beb90b77903c3b4f43b46b450
  ... Network DNS contains allthewidgets.com
  ... Network String User Agent contains Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 4.0; robo)
  ... Network String General contains <-- @$robo
[-] AND
  ... File Modified Time is 2011-09-18T17:06:15Z
  [-] OR
    ... File PE Type is Dll
    ... File Size is 24030
```

- Additional investigation reveals that most instances of lansvr.dll were installed laterally by the user “blawson”
- Investigation also reveals evidence of attacker tools
 - C:\temp\rar.exe
 - C:\temp\psexec.exe
 - C:\temp\gsecdump.exe

- An IOC to track this incident response (IR)
 - A new IOC to track data about the incident, not the malware

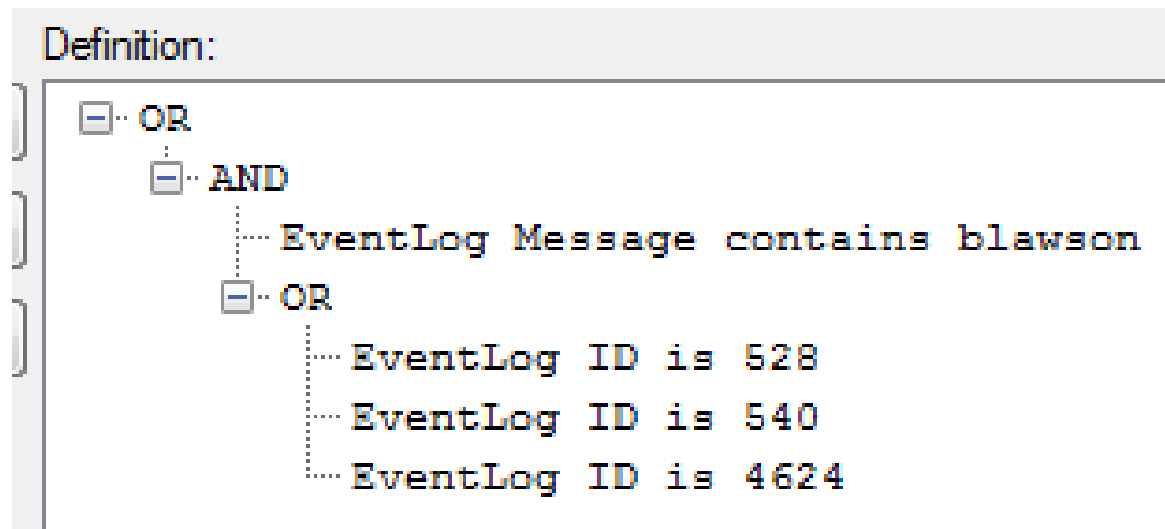
Name:	Incident Response 2012-001
Author:	William Gibb
GUID:	442505b0-a093-46bf-9c45-beb14293b1
Description:	Data collected about case 2012-001.

- Start with “blawson” information
- EventLog terms – message and event ID

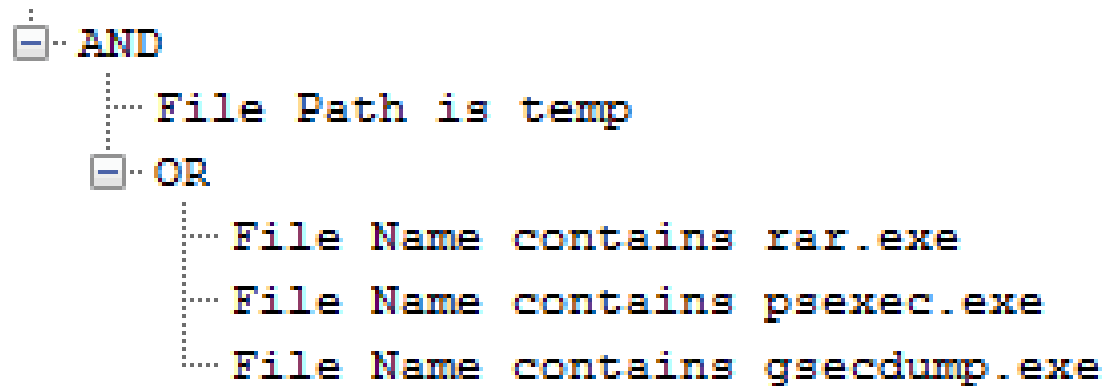
Name:	Incident Response 2012-001	T..	R..	
Author:	William Gibb			
GUID:	442505b0-a093-46bf-9c45-beb142931			
Description:	Data collected about case 2012-001.			

Add:	Definition:
<input type="button" value="Item"/>	<input type="checkbox"/> OR
<input type="button" value="AND"/>	<input type="checkbox"/> AND
<input type="button" value="OR"/>	EventLog Message contains blawson
	<input type="checkbox"/> OR
	EventLog ID contains 528
	EventLog ID contains 540

- EventLog Event IDs chosen were limited to Windows 2000, 2003 and XP
- Need to account for differences across Windows versions when writing IOCs



- Add in the malicious tool information
- C:\temp\rar.exe has the following terms:
 - File FullPath – C:\temp\rar.exe
 - File Name: - rar.exe
 - File Path: - temp



- Create IOCs with IOC Editor
- Document both your specific intelligence, and your IR intelligence

Real World IOCs



- When writing an IOC for malware
 - Capture all intelligence you can
 - More intelligence is better than less
- When writing an IOC to capture an IR activity
 - Use it to document intelligence you have about an attacker
 - Typically not related to a specific malware sample

- Expand upon the lansvr.dll IOC to generically detect identify it
 - Unique combinations of file imports can be used to identify a malware sample.

```
[-] AND
... File Import Function is LoadLibraryA
... File Import Function is GetProcAddress
... File Import Function is CreateNamedPipe
... File Import Function is PeekNamedPipe
... File Import Function is InternetOpenUrl
... File Import Function is InternetReadFile
... File Import Name is ws2_32.dll
```

- Expand upon the lansvr.dll IOC to generically detect identify it
 - Some malware will utilize legitimate Windows file version information – IOC that too!

```
[-] AND
  ... File Name contains not wzcsvc.dll
  ... File Digital Signature Verified is false
[-] OR
  ... File PEInfo Version Info InternalName contains wzcsvc.dll
  ... File PEInfo Version Info OriginalFilename contains wzcsvc.dll
```

- Identify malicious services, such as PsExec

```
Definition:
├── OR
│   ├── EventLog Message contains PsExec service
│   └── AND
│       ├── EventLog Message contains blawson
│       └── OR
│           ├── EventLog ID is 528
│           ├── EventLog ID is 540
│           └── EventLog ID is 4624
└── AND
    ├── File Path contains temp
    └── OR
        ├── File Name is rar.exe
        ├── File Name is psexec.exe
        └── File Name is gsecdump.exe
```

- Identify WinRAR execution on a host with a known compromised account

Directories created by WinRAR usage, targeting known compromised accounts.

Add: Definition:

Item

AND

OR

OR

AND

OR

OR

File Attribute contains Directory

File Path contains WinRAR

OR

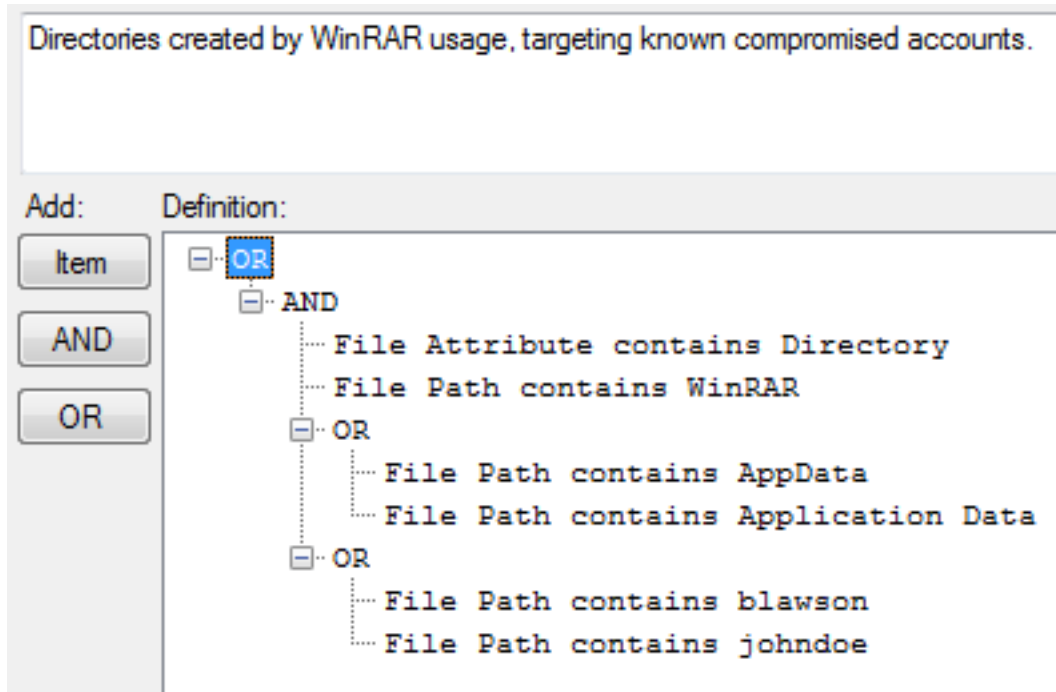
File Path contains AppData

File Path contains Application Data

OR

File Path contains blawson

File Path contains johndoe



- Identify unknown files in legitimate directories
 - Whitelist known files, by name or hash

Definition:

```
[-] OR
  [-] AND
    ..... File Attribute contains Archive
    ..... File MD5 is not 7d11d1e304cb72ecda92f6e3c6526735
    ..... File MD5 is not a1abb80a3e54cdd2549492050baff18c
    ..... File MD5 is not 19065c3f8710578fe2ef2e8f5f6eb1b9
    ..... File Name is not FOOBAR_Login.bat
    ..... File Name is not FOOBAR.exe
    ..... File Name is not FOOBAR_Printer.vbs
    ..... File Path is FOOBAR
```

- Write an IOC for malware with random filenames
- Typically done through a combination of different IOC terms

```
Definition:
├─ OR
│   └─ AND
│       ├── File Path contains temp
│       ├── File PE Type is Executable
│       └─ OR
│           ├── File Size contains 105000 TO 115000
│           ├── File Compile Time contains 2010-08-01T00:00:01Z TO 2010-08-08T23:59:59Z
│           └─ AND
│               ├── File Detected Anomalies is checksum_is_zero
│               └─ File Detected Anomalies is contains_eof_data
```

- Capture all of your intelligence related to an incident
- Capture intelligence about methods and techniques, not just malware