Yeti
Forensics Intelligence

An open-source story…

An open source story…

- A story about a **problem** that needed to get **fixed**
- How we **attempted** to fix that problem
- The ~~friends we made~~ **lessons** we learned along the way
- Flipping our problem **upside down**

new phone who dis?

Thomas Chopitea

@tomchop_

Creator and core dev Yeti

DFIR @ Google

Sébastien Larinier

@sebdraven

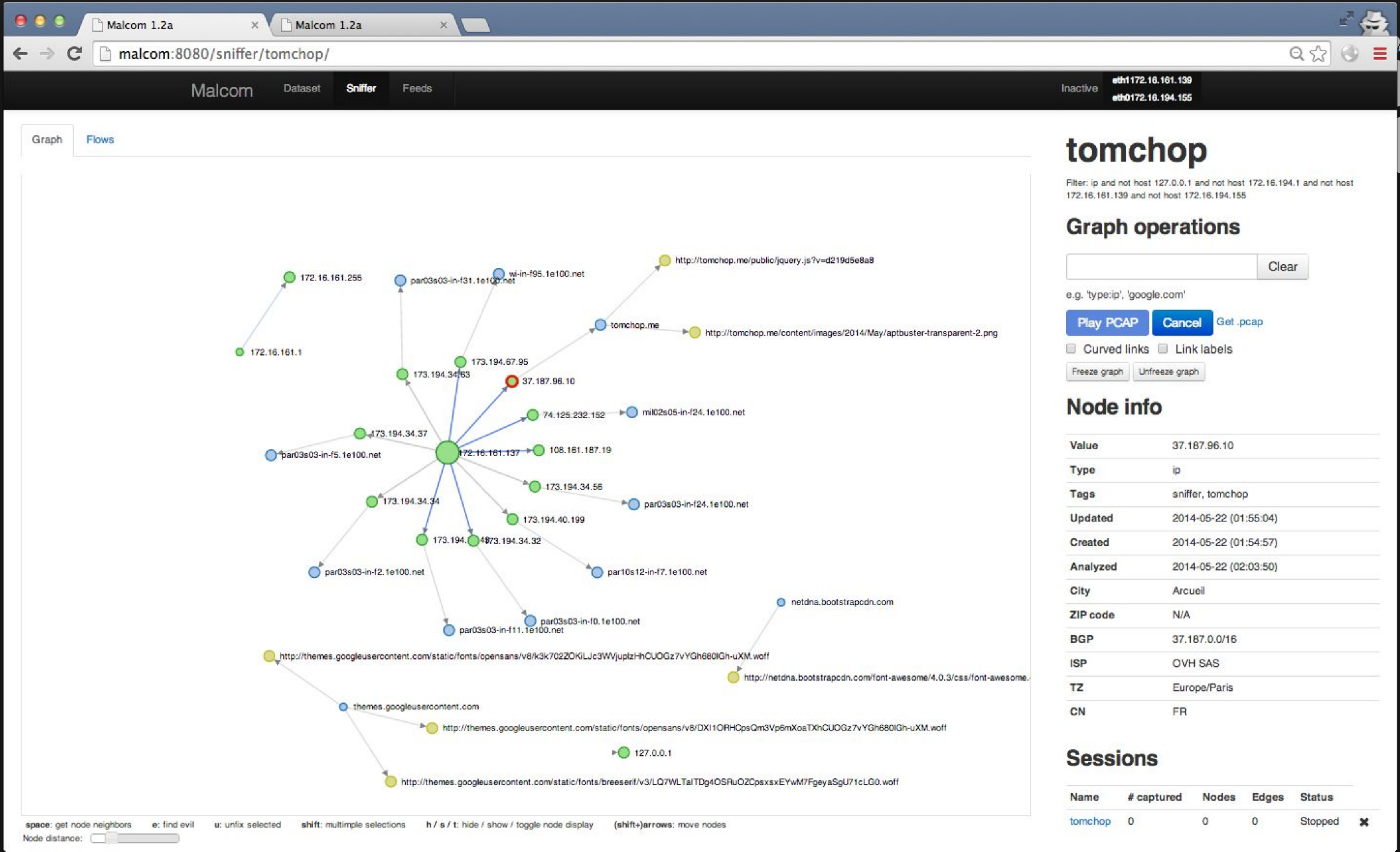
Core dev Yeti

Security Researcher/Teacher at ESIEA

wtf is Tom looking at?

What is Tom looking at?

- Reverse engineering is hard and no one has time for it (esp. IR)
- Network indicators are much better
  - Easy to collect and search for
  - Just need tcpdump + ebpf
- Run sample, extract network indicators, search in knowledge base


Malcom 1.2a
Malcom 1.2a
malcom:8080/sniffer/tomchop/
Malcom
Dataset
Sniffer
Feeds
Inactive
eth1172.16.161.139
eth0172.16.194.155
Graph
Flows
172.16.161.255
172.16.161.1
par03s03-in-f31.1e100.net
wi-in-f95.1e100.net
http://tomchop.me/public/jquery.js?v=d219d5e8a8
tomchop.me
http://tomchop.me/content/images/2014/May/aptbuster-transparent-2.png
173.194.67.95
173.194.34.63
37.187.96.10
74.125.232.152
mil02s05-in-f24.1e100.net
173.194.34.37
par03s03-in-f5.1e100.net
172.16.161.137
108.161.187.19
173.194.34.56
par03s03-in-f24.1e100.net
173.194.34.34
173.194.40.199
173.194.
48
173.194.34.32
par03s03-in-f2.1e100.net
par10s12-in-f7.1e100.net
netdna.bootstrapcdn.com
par03s03-in-f0.1e100.net
par03s03-in-f11.1e100.net
http://themes.googleusercontent.com/static/fonts/opensans/v8/k3k702ZOKiLJc3WVjuplzHhCUOGz7vYGh680lGh-uXM.woff
http://netdna.bootstrapcdn.com/font-awesome/4.0.3/css/font-awesome.
themes.googleusercontent.com
http://themes.googleusercontent.com/static/fonts/opensans/v8/DXI1ORHCpsQm3Vp6mXoaTXhCUOGz7vYGh680lGh-uXM.woff
127.0.0.1
http://themes.googleusercontent.com/static/fonts/breeserif/v3/LQ7WLTaITDg4OSRuOZCpsxsxEYwM7FgeyaSgU71cLG0.woff
Node distance:
Clear
Play PCAP
Cancel
Get .pcap
Freeze graph
Unfreeze graph

space: get node neighbors **e**: find evil **u**: unfix selected **shift**: multimple selections **h / s / t**: hide / show / toggle node display **(shift+)arrows**: move nodes

tomchop

Filter: ip and not host 127.0.0.1 and not host 172.16.194.1 and not host 172.16.161.139 and not host 172.16.194.155

Graph operations

e.g. 'type:ip', 'google.com'

☐ Curved links ☐ Link labels

Node info

Value	37.187.96.10
Type	ip
Tags	sniffer, tomchop
Updated	2014-05-22 (01:55:04)
Created	2014-05-22 (01:54:57)
Analyzed	2014-05-22 (02:03:50)
City	Arcueil
ZIP code	N/A
BGP	37.187.0.0/16
ISP	OVH SAS
TZ	Europe/Paris
CN	FR

Sessions

Name	# captured	Nodes	Edges	Status	
tomchop	0	0	0	Stopped	✖

Malcom

- Simple API, *insane* amounts of JavaScript, really what was I thinking
- ***LIVE*** network captures x “threat feed” ingestor
- Result: overengineered way of visualizing badness in network traffic
- It worked okay! But we needed **more…**

Seb got into the game

- In 2014, Suricata (IDS) has an unix socket to send a pcap file.
- So,I try to replace scapy by Suricata to extract IOCs, send to Malcom and tag IOCs network with metadata of alerts Suricata
    - Suricata extract all in 2014 in json file
    - Many issues of synchronisation

- I’m focused on FastIR with my team at Sekoia (Live Forensic Endpoint)

“ok, let’s start from scratch”

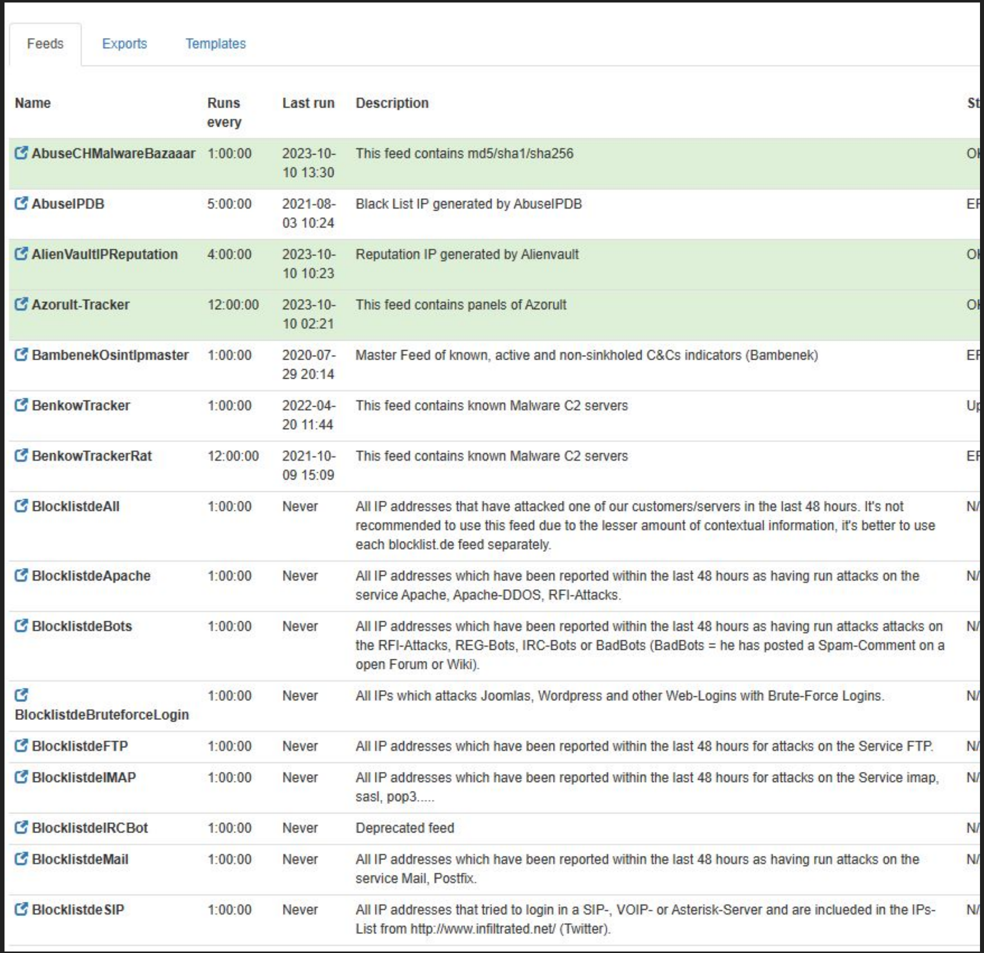
— *tom, ca. 2014*

Yeti, Your Everyday Threat Intelligence

- “Observables”, “Indicators”, “Entities”
- Lots of **tags** everywhere
- Python (Flask), JavaScript (again!), Bootstrap CSS
- MongoDB (oops), Redis

- A threat intel platform oriented towards DFIRers

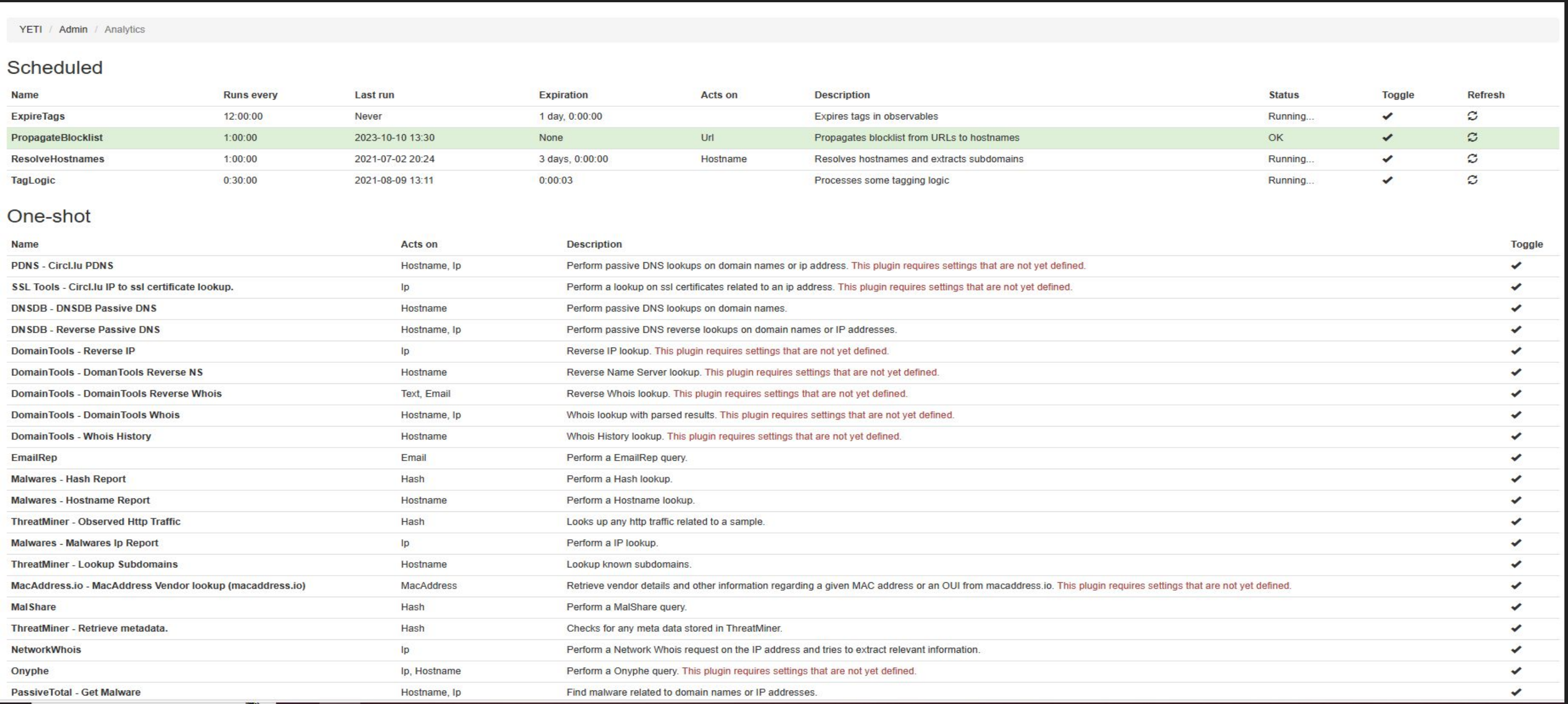
Feeds



Feeds | Exports | Templates

Name	Runs every	Last run	Description	St
AbuseCHMalwareBazaaar	1:00:00	2023-10-10 13:30	This feed contains md5/sha1/sha256	O
AbuseIPDB	5:00:00	2021-08-03 10:24	Black List IP generated by AbuseIPDB	E
AlienVaultIPReputation	4:00:00	2023-10-10 10:23	Reputation IP generated by Alienvault	O
Azorult-Tracker	12:00:00	2023-10-10 02:21	This feed contains panels of Azorult	O
BambenekOsintIpmaster	1:00:00	2020-07-29 20:14	Master Feed of known, active and non-sinkholed C&Cs indicators (Bambenek)	E
BenkowTracker	1:00:00	2022-04-20 11:44	This feed contains known Malware C2 servers	U
BenkowTrackerRat	12:00:00	2021-10-09 15:09	This feed contains known Malware C2 servers	E
BlocklistdeAll	1:00:00	Never	All IP addresses that have attacked one of our customers/servers in the last 48 hours. It's not recommended to use this feed due to the lesser amount of contextual information, it's better to use each blocklist.de feed separately.	N/
BlocklistdeApache	1:00:00	Never	All IP addresses which have been reported within the last 48 hours as having run attacks on the service Apache, Apache-DDOS, RFI-Attacks.	N/
BlocklistdeBots	1:00:00	Never	All IP addresses which have been reported within the last 48 hours as having run attacks attacks on the RFI-Attacks, REG-Bots, IRC-Bots or BadBots (BadBots = he has posted a Spam-Comment on a open Forum or Wiki).	N/
BlocklistdeBruteforceLogin	1:00:00	Never	All IPs which attacks Joomlas, Wordpress and other Web-Logins with Brute-Force Logins.	N/
BlocklistdeFTP	1:00:00	Never	All IP addresses which have been reported within the last 48 hours for attacks on the Service FTP.	N/
BlocklistdeIMAP	1:00:00	Never	All IP addresses which have been reported within the last 48 hours for attacks on the Service imap, sasl, pop3.....	N/
BlocklistdeIRCBot	1:00:00	Never	Deprecated feed	N/
BlocklistdeMail	1:00:00	Never	All IP addresses which have been reported within the last 48 hours as having run attacks on the service Mail, Postfix.	N/
BlocklistdeSIP	1:00:00	Never	All IP addresses that tried to login in a SIP-, VOIP- or Asterisk-Server and are inclueded in the IPs-List from http://www.infiltrated.net/ (Twitter).	N/

Analytics



YETI / Admin / Analytics

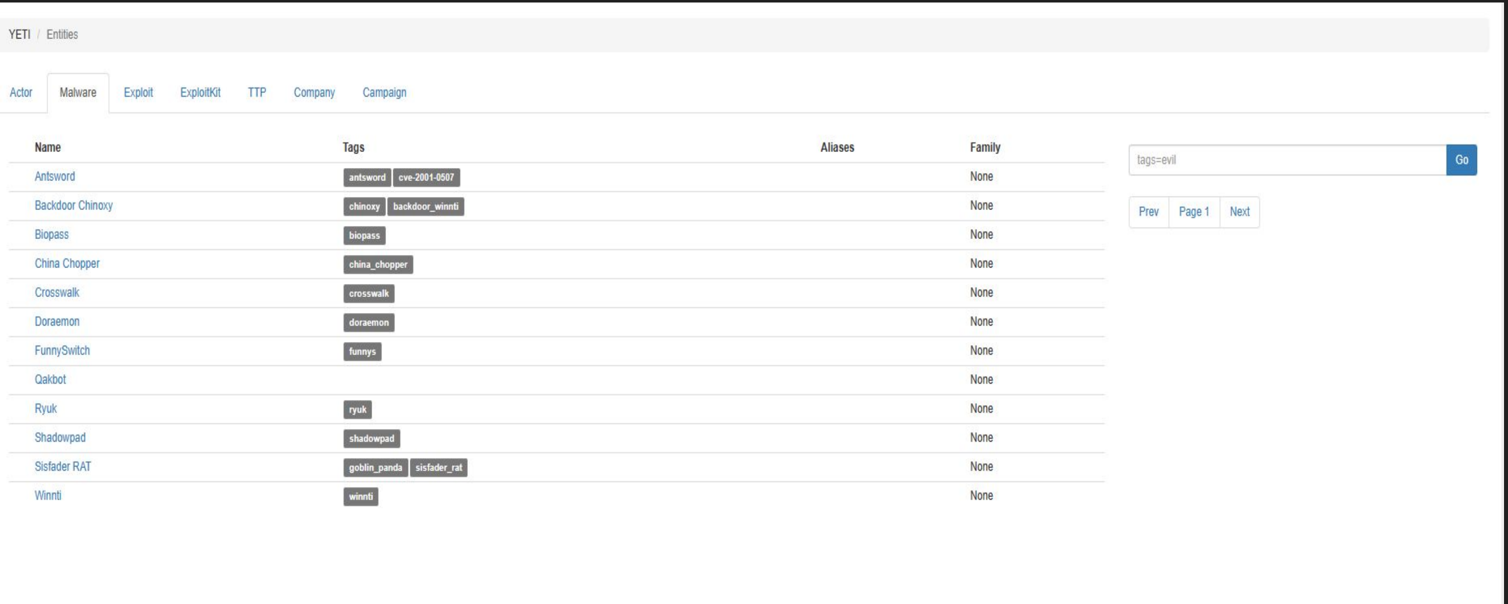
Scheduled

Name	Runs every	Last run	Expiration	Acts on	Description	Status	Toggle	Refresh
ExpireTags	12:00:00	Never	1 day, 0:00:00		Expires tags in observables	Running...	✓	↻
PropagateBlocklist	1:00:00	2023-10-10 13:30	None	Url	Propagates blocklist from URLs to hostnames	OK	✓	↻
ResolveHostnames	1:00:00	2021-07-02 20:24	3 days, 0:00:00	Hostname	Resolves hostnames and extracts subdomains	Running...	✓	↻
TagLogic	0:30:00	2021-08-09 13:11	0:00:03		Processes some tagging logic	Running...	✓	↻

One-shot

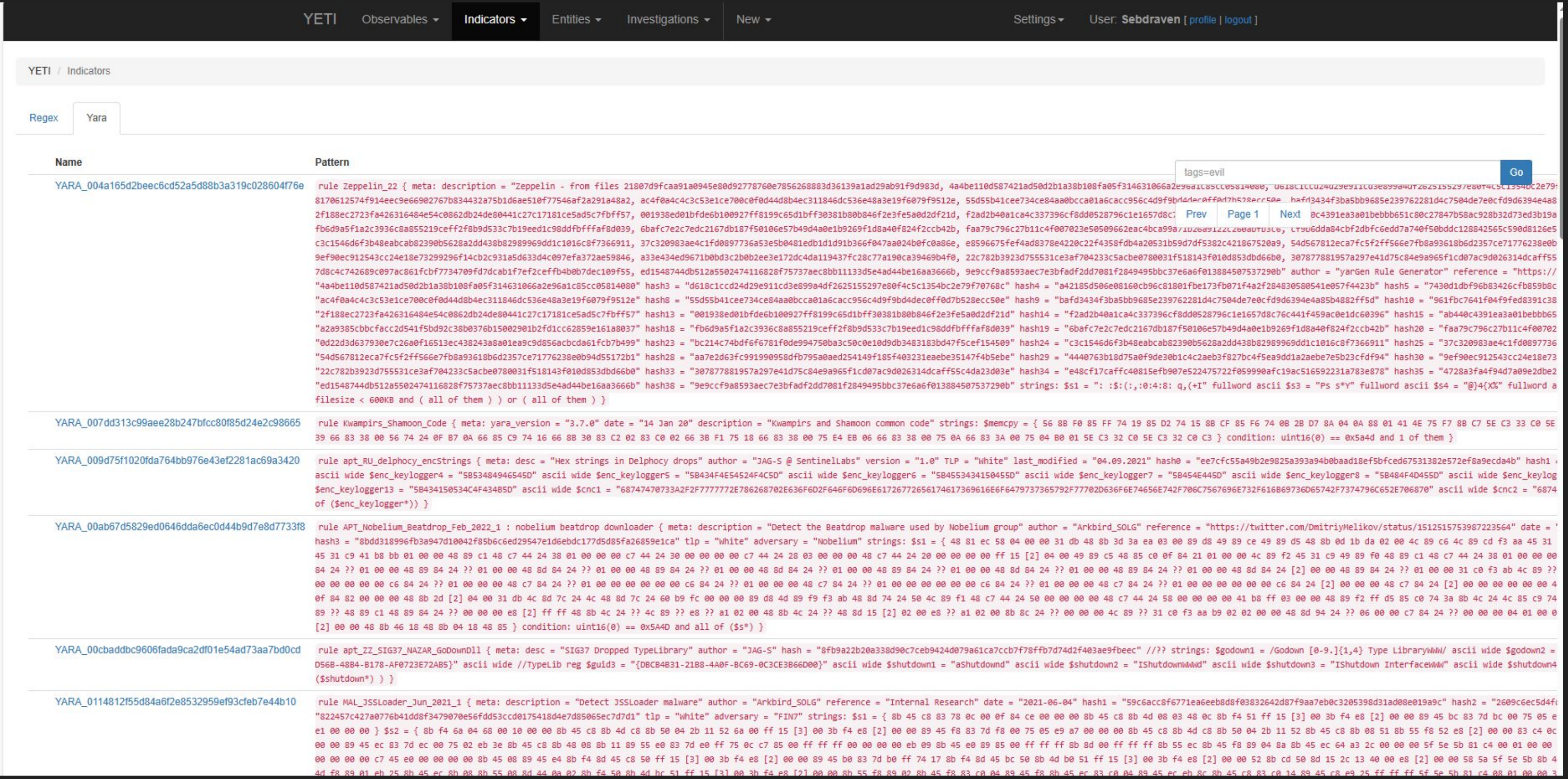
Name	Acts on	Description	Toggle
PDNS - Circl.lu PDNS	Hostname, Ip	Perform passive DNS lookups on domain names or ip address. This plugin requires settings that are not yet defined.	✓
SSL Tools - Circl.lu IP to ssl certificate lookup.	Ip	Perform a lookup on ssl certificates related to an ip address. This plugin requires settings that are not yet defined.	✓
DNSDB - DNSDB Passive DNS	Hostname	Perform passive DNS lookups on domain names.	✓
DNSDB - Reverse Passive DNS	Hostname, Ip	Perform passive DNS reverse lookups on domain names or IP addresses.	✓
DomainTools - Reverse IP	Ip	Reverse IP lookup. This plugin requires settings that are not yet defined.	✓
DomainTools - DomanTools Reverse NS	Hostname	Reverse Name Server lookup. This plugin requires settings that are not yet defined.	✓
DomainTools - DomainTools Reverse Whois	Text, Email	Reverse Whois lookup. This plugin requires settings that are not yet defined.	✓
DomainTools - DomainTools Whois	Hostname, Ip	Whois lookup with parsed results. This plugin requires settings that are not yet defined.	✓
DomainTools - Whois History	Hostname	Whois History lookup. This plugin requires settings that are not yet defined.	✓
EmailRep	Email	Perform a EmailRep query.	✓
Malwares - Hash Report	Hash	Perform a Hash lookup.	✓
Malwares - Hostname Report	Hostname	Perform a Hostname lookup.	✓
ThreatMiner - Observed Http Traffic	Hash	Looks up any http traffic related to a sample.	✓
Malwares - Malwares Ip Report	Ip	Perform a IP lookup.	✓
ThreatMiner - Lookup Subdomains	Hostname	Lookup known subdomains.	✓
MacAddress.io - MacAddress Vendor lookup (macaddress.io)	MacAddress	Retrieve vendor details and other information regarding a given MAC address or an OUI from macaddress.io. This plugin requires settings that are not yet defined.	✓
MalShare	Hash	Perform a MalShare query.	✓
ThreatMiner - Retrieve metadata.	Hash	Checks for any meta data stored in ThreatMiner.	✓
NetworkWhois	Ip	Perform a Network Whois request on the IP address and tries to extract relevant information.	✓
Onyphe	Ip, Hostname	Perform a Onyphe query. This plugin requires settings that are not yet defined.	✓
PassiveTotal - Get Malware	Hostname, Ip	Find malware related to domain names or IP addresses.	✓

Entities



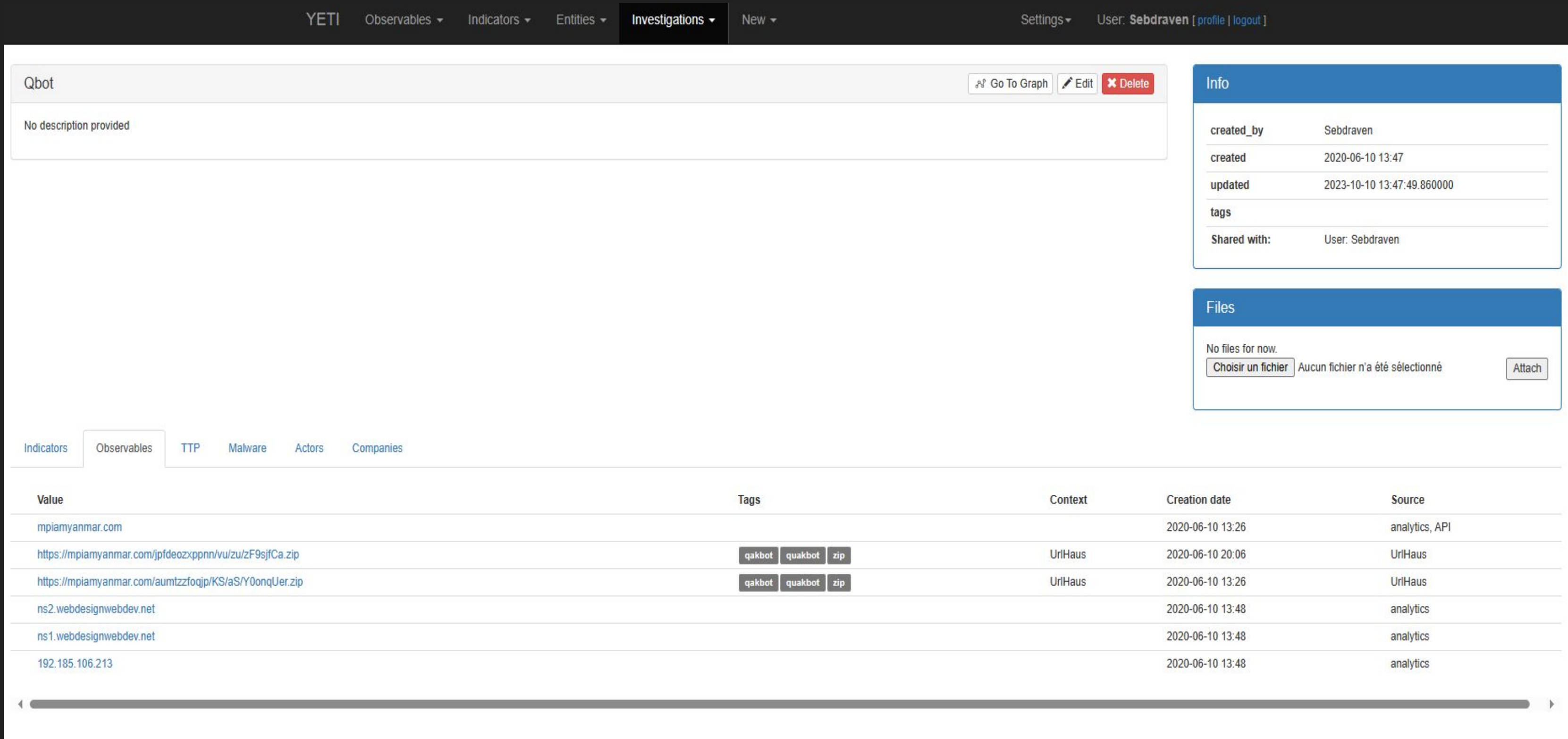
Name	Tags	Aliases	Family
Antsword	antsword cve-2001-0507		None
Backdoor Chinoxy	chinoxy backdoor_winnti		None
Biopass	biopass		None
China Chopper	china_chopper		None
Crosswalk	crosswalk		None
Doraemon	doraemon		None
FunnySwitch	funnys		None
Qakbot			None
Ryuk	ryuk		None
Shadowpad	shadowpad		None
Sisfader RAT	goblin_panda sisfader_rat		None
Winnti	winnti		None

Indicators



Name	Pattern
YARA_004a165d2beec6cd52a5d88b3a319c028604f76e	rule Zeppelin_22 { meta: description = "Zeppelin - from files 21807d9fcaa91a0945e80d92778760e7856268883d36139a1ad29ab91f9d983d, 4a4be110d587421ad50d2b1a38b108fa05f314631066a2e96a1c85cc05814080, d618c1ccd24d29e911cd3e899a4df2625155297e80f4c5c1354bc2e79f 8170612574f914eec9e66902767b834432a75b1d6ae510f77546af2a291a48a2, ac4f0a4c4c3c53e1ce700c0f0d44d8b4ec311846dc536e48a3e19f6079f9512e, 55d55b41cee734ce84aa0bcca01a6cacc956c4d9f9bd4dec0ff0d7b528ecc50e, bafd3434f3ba5bb9685e239762281d4c7504de7e0cfd9d6394e4a8 2f188ec2723fa426316484e54c0862db24de80441c27c17181ce5ad5c7fbff57, 001938ed01bfde6b100927ff8199c65d1bff30381b80b846f2e3fe5a0d2df21d, f2ad2b40a1ca4c337396cf8dd0528796c1e1657d8c7 0c4391ea3a01bebbb651c80c27847b58ac928b32d73ed3b19a fb6d9a5f1a2c3936c8a855219ceff2f8b9d533c7b19eed1c98ddfbfffaf8d039, 6bafc7e2c7edc2167db187f50106e57b49d4a0e1b9269f1d8a40f824f2ccb42b, faa79c796c27b11c4f007023e50509662eac4bca99a71b26a9122c260abfb3c6, cf9b6dda84cbf2dbfc6edd7a740f50bddc128842565c590d8126e5 c3c1546d6f3b48eabcab82390b5628a2dd438b82989969dd1c1016c8f7366911, 37c320983ae4c1fd0897736a53e5b0481edb1d1d91b366f047aa024b0fc0a86e, e8596675fef4ad8378e4220c22f4358fdb4a20531b59d7df5382c421867520a9, 54d567812eca7fc5f2ff566e7fb8a93618b6d2357ce71776238e0b 9ef90ec912543cc24e18e73299296f14cb2c931a5d633d4c097efa372ae59846, a33e434ed9671b0bd3c2b0b2ee3e172dc4da119437fc28c77a190ca39469b4f0, 22c782b3923d755531ce3af704233c5acbe0780031f518143f010d853dbd66b0, 307877881957a297e41d75c84e9a965f1cd07ac9d026314dcaff55 7d8c4c742689c097ac861fcbf7734709fd7dcab1f7ef2ceffb4b0b7dec109f55, ed1548744db512a5502474116828f75737aec8bb11133d5e4ad44be16aa3666b, 9e9ccf9a8593aec7e3bfadf2dd7081f2849495bbc37e6a6f013884507537290b" author = "yarGen Rule Generator" reference = "https:// "4a4be110d587421ad50d2b1a38b108fa05f314631066a2e96a1c85cc05814080" hash3 = "d618c1ccd24d29e911cd3e899a4df2625155297e80f4c5c1354bc2e79f70768c" hash4 = "a42185d506e08160cb96c81801fbe173fb071f4a2f284830580541e057f4423b" hash5 = "7430d1dbf96b83426cfb859b8c "ac4f0a4c4c3c53e1ce700c0f0d44d8b4ec311846dc536e48a3e19f6079f9512e" hash8 = "55d55b41cee734ce84aa0bcca01a6cacc956c4d9f9bd4dec0ff0d7b528ecc50e" hash9 = "bafd3434f3ba5bb9685e239762281d4c7504de7e0cfd9d6394e4a85b4882ff5d" hash10 = "961fbc7641f04f9fed8391c38 "2f188ec2723fa426316484e54c0862db24de80441c27c17181ce5ad5c7fbff57" hash13 = "001938ed01bfde6b100927ff8199c65d1bff30381b80b846f2e3fe5a0d2df21d" hash14 = "f2ad2b40a1ca4c337396cf8dd0528796c1e1657d8c76c441f459ac0e1dc60396" hash15 = "ab440c4391ea3a01bebbb65 "a2a9385cbbcfacc2d541f5bd92c38b0376b15002901b2fd1cc62859e161a8037" hash18 = "fb6d9a5f1a2c3936c8a855219ceff2f8b9d533c7b19eed1c98ddfbfffaf8d039" hash19 = "6bafc7e2c7edc2167db187f50106e57b49d4a0e1b9269f1d8a40f824f2ccb42b" hash20 = "faa79c796c27b11c4f00702 "0d22d3d637930e7c26a0f16513ec438243a8a01ea9c9d856acbcda61fcb7b499" hash23 = "bc214c74bdf6f6781f0de994750ba3c50c0e10d9db3483183bd47f5cef154509" hash24 = "c3c1546d6f3b48eabcab82390b5628a2dd438b82989969dd1c1016c8f7366911" hash25 = "37c320983ae4c1fd0897736 "54d567812eca7fc5f2ff566e7fb8a93618b6d2357ce71776238e0b94d55172b1" hash28 = "aa7e2d63fc991990958dfb795a0aed254149f185f403231eaebe35147f4b5ebe" hash29 = "4440763b18d75a0f9de30b1c4c2aeb3f827bc4f5ea9dd1a2aebe7e5b23cfdf94" hash30 = "9ef90ec912543cc24e18e73 "22c782b3923d755531ce3af704233c5acbe0780031f518143f010d853dbd66b0" hash33 = "307877881957a297e41d75c84e9a965f1cd07ac9d026314dcaff55c4da23d03e" hash34 = "e48cf17caffc40815efb907e522475722f059990afc19ac516592231a783e878" hash35 = "4728a3fa4f94d7a09e2dbe2 "ed1548744db512a5502474116828f75737aec8bb11133d5e4ad44be16aa3666b" hash38 = "9e9ccf9a8593aec7e3bfadf2dd7081f2849495bbc37e6a6f013884507537290b" strings: $s1 = ": :$:(:,:0:4:8: q,(+I" fullword ascii $s3 = "Ps s*Y" fullword ascii $s4 = "@}4{X%" fullword a filesize < 600KB and (all of them)) or (all of them) }
YARA_007dd313c99aee28b247bfcc80f85d24e2c98665	rule Kwampirs_Shamoon_Code { meta: yara_version = "3.7.0" date = "14 Jan 20" description = "Kwampirs and Shamoon common code" strings: $memcpy = { 56 8B F0 85 FF 74 19 85 D2 74 15 8B CF 85 F6 74 0B 2B D7 8A 04 0A 88 01 41 4E 75 F7 8B C7 5E C3 33 C0 5E 39 66 83 38 00 56 74 24 0F B7 0A 66 85 C9 74 16 66 8B 30 83 C2 02 83 C0 02 66 3B F1 75 18 66 83 38 00 75 E4 EB 06 66 83 38 00 75 0A 66 83 3A 00 75 04 B0 01 5E C3 32 C0 5E C3 32 C0 C3 } condition: uint16(0) == 0x5a4d and 1 of them }
YARA_009d75f1020fda764bb976e43ef2281ac69a3420	rule apt_RU_delphocy_encStrings { meta: desc = "Hex strings in Delphocy drops" author = "JAG-S @ SentinelLabs" version = "1.0" TLP = "White" last_modified = "04.09.2021" hash0 = "ee7cfc55a49b2e9825a393a94b0baad18ef5bfced67531382e572ef8a9ecda4b" hash1 = ascii wide $enc_keylogger4 = "5B53484946545D" ascii wide $enc_keylogger5 = "5B434F4E54524F4C5D" ascii wide $enc_keylogger6 = "5B4553434150455D" ascii wide $enc_keylogger7 = "5B454E445D" ascii wide $enc_keylogger8 = "5B484F4D455D" ascii wide $enc_keylog $enc_keylogger13 = "5B434150534C4F434B5D" ascii wide $cnc1 = "68747470733A2F2F7777772E786268702E636F6D2F646F6D696E61726772656174617369616E6F6479737365792F77702D636F6E74656E742F706C7567696E732F616B69736D65742F7374796C652E706870" ascii wide $cnc2 = "6874 of ($enc_keylogger*)) }
YARA_00ab67d5829ed0646dda6ec0d44b9d7e8d7733f8	rule APT_Nobelium_Beatdrop_Feb_2022_1 : nobelium beatdrop downloader { meta: description = "Detect the Beatdrop malware used by Nobelium group" author = "Arkbird_SOLG" reference = "https://twitter.com/DmitriyMelikov/status/1512515753987223564" date = " hash3 = "8bdd318996fb3a947d10042f85b6c6ed29547e1d6ebdc177d5d85fa26859e1ca" tlp = "White" adversary = "Nobelium" strings: $s1 = { 48 81 ec 58 04 00 00 31 db 48 8b 3d 3a ea 03 00 89 d8 49 89 ce 49 89 d5 48 8b 0d 1b da 02 00 4c 89 c6 4c 89 cd f3 aa 45 31 45 31 c9 41 b8 bb 01 00 00 48 89 c1 48 c7 44 24 38 01 00 00 00 c7 44 24 30 00 00 00 00 c7 44 24 28 03 00 00 00 48 c7 44 24 20 00 00 00 00 ff 15 [2] 04 00 49 89 c5 48 85 c0 0f 84 21 01 00 00 4c 89 f2 45 31 c9 49 89 f0 48 89 c1 48 c7 44 24 38 01 00 00 00 84 24 ?? 01 00 00 48 89 84 24 ?? 01 00 00 48 8d 84 24 ?? 01 00 00 48 89 84 24 ?? 01 00 00 48 8d 84 24 ?? 01 00 00 48 89 84 24 ?? 01 00 00 48 8d 84 24 [2] 00 00 48 89 84 24 ?? 01 00 00 31 c0 f3 ab 4c 89 ?? 00 00 00 00 00 c6 84 24 ?? 01 00 00 00 48 c7 84 24 ?? 01 00 00 00 00 00 00 c6 84 24 ?? 01 00 00 00 48 c7 84 24 ?? 01 00 00 00 00 00 00 c6 84 24 [2] 00 00 00 48 c7 84 24 [2] 00 00 00 00 00 00 4 0f 84 82 00 00 00 48 8b 2d [2] 04 00 31 db 4c 8d 7c 24 4c 48 8d 7c 24 60 b9 fc 00 00 00 89 d8 4d 89 f9 f3 ab 48 8d 74 24 50 4c 89 f1 48 c7 44 24 50 00 00 00 00 48 c7 44 24 58 00 00 00 00 41 b8 ff 03 00 00 48 89 f2 ff d5 85 c0 74 3a 8b 4c 24 4c 85 c9 74 89 ?? 48 89 c1 48 89 84 24 ?? 00 00 00 e8 [2] ff ff 48 8b 4c 24 ?? 4c 89 ?? e8 ?? a1 02 00 48 8b 4c 24 ?? 48 8d 15 [2] 02 00 e8 ?? a1 02 00 8b 8c 24 ?? 00 00 00 4c 89 ?? 31 c0 f3 aa b9 02 02 00 00 48 8d 94 24 ?? 06 00 00 c7 84 24 ?? 00 00 00 04 01 00 0 [2] 00 00 48 8b 46 18 48 8b 04 18 48 85 } condition: uint16(0) == 0x5A4D and all of ($s*) }
YARA_00cbaddbc9606fada9ca2df01e54ad73aa7bd0cd	rule apt_ZZ_SIG37_NAZAR_GoDownDll { meta: desc = "SIG37 Dropped TypeLibrary" author = "JAG-S" hash = "8fb9a22b20a338d90c7ceb9424d079a61ca7ccb7f78ffb7d74d2f403ae9fbeec" //?? strings: $godown1 = /Godown [0-9.]{1,4} Type LibraryWWW/ ascii wide $godown2 = D56B-48B4-B178-AF0723E72AB5}" ascii wide //TypeLib reg $guid3 = "{DBCB4B31-21B8-4A0F-BC69-0C3CE3B66D00}" ascii wide $shutdown1 = "aShutdownd" ascii wide $shutdown2 = "IShutdownWWWd" ascii wide $shutdown3 = "IShutdown InterfaceWWW" ascii wide $shutdown4 ($shutdown*)) }
YARA_0114812f55d84a6f2e8532959ef93cfeb7e44b10	rule MAL_JSSLoader_Jun_2021_1 { meta: description = "Detect JSSLoader malware" author = "Arkbird_SOLG" reference = "Internal Research" date = "2021-06-04" hash1 = "59c6acc8f6771ea6eeb8d8f03832642d87f9aa7eb0c3205398d31ad08e019a9c" hash2 = "2609c6ec5d4f "822457c427a0776b41dd8f3479070e56fdd53ccd0175418d4e7d85065ec7d7d1" tlp = "White" adversary = "FIN7" strings: $s1 = { 8b 45 c8 83 78 0c 00 0f 84 ce 00 00 00 8b 45 c8 8b 4d 08 03 48 0c 8b f4 51 ff 15 [3] 00 3b f4 e8 [2] 00 00 89 45 bc 83 7d bc 00 75 05 e e1 00 00 00 } $s2 = { 8b f4 6a 04 68 00 10 00 00 8b 45 c8 8b 4d c8 8b 50 04 2b 11 52 6a 00 ff 15 [3] 00 3b f4 e8 [2] 00 00 89 45 f8 83 7d f8 00 75 05 e9 a7 00 00 00 8b 45 c8 8b 4d c8 8b 50 04 2b 11 52 8b 45 c8 8b 08 51 8b 55 f8 52 e8 [2] 00 00 83 c4 0c 00 00 89 45 ec 83 7d ec 00 75 02 eb 3e 8b 45 c8 8b 48 08 8b 11 89 55 e0 83 7d e0 ff 75 0c c7 85 00 ff ff ff 00 00 00 00 eb 09 8b 45 e0 89 85 00 ff ff ff 8b 8d 00 ff ff ff 8b 55 ec 8b 45 f8 89 04 8a 8b 45 ec 64 a3 2c 00 00 00 5f 5e 5b 81 c4 00 01 00 00 00 00 00 00 c7 45 e0 00 00 00 00 8b 45 08 89 45 e4 8b f4 8d 45 c8 50 ff 15 [3] 00 3b f4 e8 [2] 00 00 89 45 b0 83 7d b0 ff 74 17 8b f4 8d 45 bc 50 8b 4d b0 51 ff 15 [3] 00 3b f4 e8 [2] 00 00 52 8b cd 50 8d 15 2c 13 40 00 e8 [2] 00 00 58 5a 5f 5e 5b 8b 4 4d f8 89 01 eb 25 8b 45 ec 8b 08 8b 55 08 8d 44 0a 02 8b f4 50 8b 4d bc 51 ff 15 [3] 00 3b f4 e8 [2] 00 00 8b 55 f8 89 02 8b 45 f8 83 c0 04 89 45 f8 8b 45 ec 83 c0 04 89 45 ec eb 8c 8b 45 c8 83 c0 14 89 45 c8 e9 25 ff ff ff 5f 5e 5b 81 c4 08 01 00 00 3

Investigation



Qbot

No description provided

Info

created_by	Sebdraven
created	2020-06-10 13:47
updated	2023-10-10 13:47:49.860000
tags	
Shared with:	User: Sebdraven

Files

No files for now.

Aucun fichier n'a été sélectionné

Value	Tags	Context	Creation date	Source
mpiamyanmar.com			2020-06-10 13:26	analytics, API
https://mpiamyanmar.com/jpfdeozxppnn/vu/zu/zF9sjfCa.zip	qakbot quakbot zip	UrlHaus	2020-06-10 20:06	UrlHaus
https://mpiamyanmar.com/aumtzzfoqjp/KS/aS/Y0onqUer.zip	qakbot quakbot zip	UrlHaus	2020-06-10 13:26	UrlHaus
ns2.webdesignwebdev.net			2020-06-10 13:48	analytics
ns1.webdesignwebdev.net			2020-06-10 13:48	analytics
192.185.106.213			2020-06-10 13:48	analytics

Time passed…

Meanwhile, in Veracruz…

- MISP becomes the **golden standard** of CTI sharing
- Commercial vendors enter the game
- (2017) **STIX2**
- (late 2016-2017) Hippocampe, Cortex, TheHive
- (jan 2018) MITRE ATT&CK
- (late 2018) OpenCTI

As for Yeti…

- **Few significant** external contributions
- Core devs had **competing priorities**
- **Licencing problems** + rotting codebase…
- Intermediary rewrite (**TibetanBrownBear**) in 2018

- Some people **still using** Yeti!

“ok, let’s start from scratch”

— *tom, ca. 2018*

“ok, let’s start from scratch”

no wait lol

Lessons learned (OR DID WE??)

- Do **less** things, do them **well**
- **Don’t pre-optimize for** use-cases you don’t have
- Simple & clear >>>>> elegant
- **Healthier codebase**: code smell, tech debt, code churn, toil…
- **Testing** is trusting

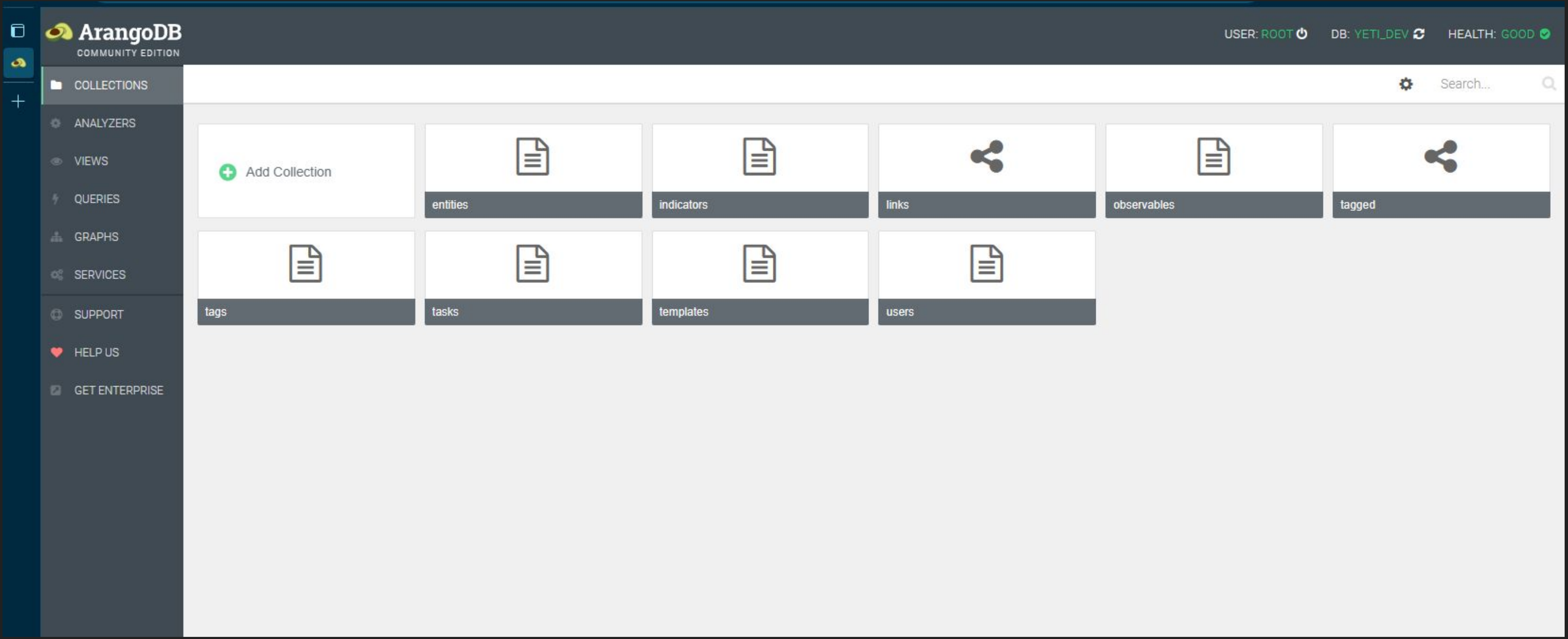
Some changes…

- **Apache 2.0** licenses everywhere
- Fully **embracing the graph** (ArangoDB 🥑) + redis
- (still) lots of **tags** everywhere
- Python 3.10 ✨ (FastAPI, Pydantic)
- Frontend… in VueJS (JavaScript!!!1 not again!!)

Some changes…

- Data model ***based*** on STIX2, but not *really* STIX2
- Easy to **import** MITRE ATT&CK, MISP galaxies
- Support for more **indicator types**: Yara, Sigma, generic queries
- Vendor agnostic

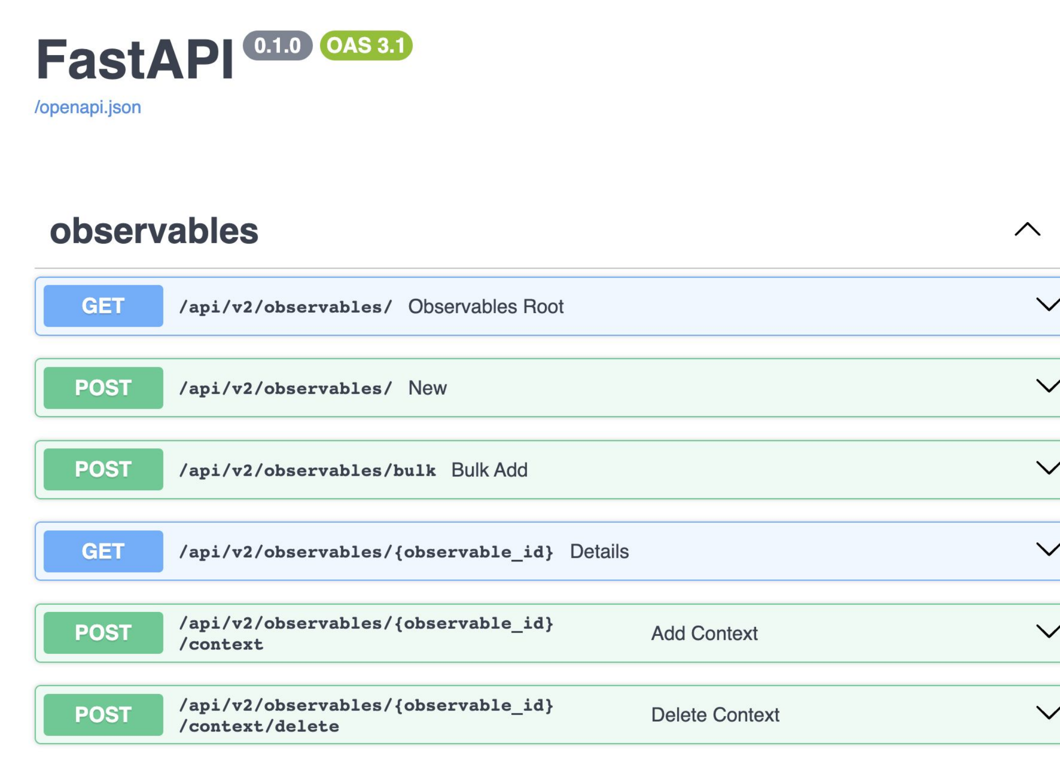
Arango with YETI



USER: ROOT DB: YETI_DEV HEALTH: GOOD

FastAPI ❤️ Pydantic

- **Strict** data model validation
- Full JSON serialisation
- **Self-documenting** API



FastAPI 0.1.0 OAS 3.1

/openapi.json

observables

GET `/api/v2/observables/` Observables Root

POST `/api/v2/observables/` New

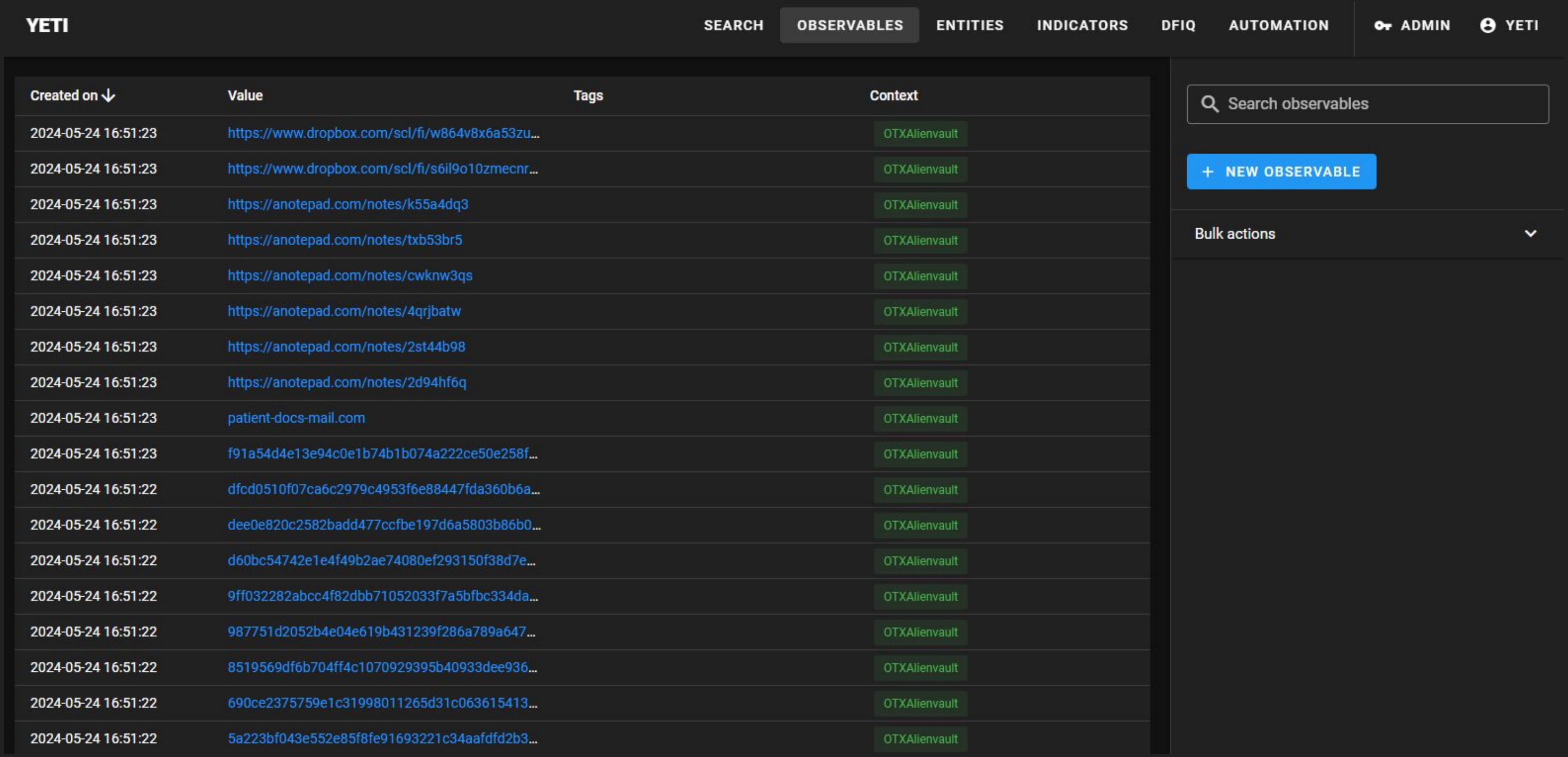
POST `/api/v2/observables/bulk` Bulk Add

GET `/api/v2/observables/{observable_id}` Details

POST `/api/v2/observables/{observable_id}/context` Add Context

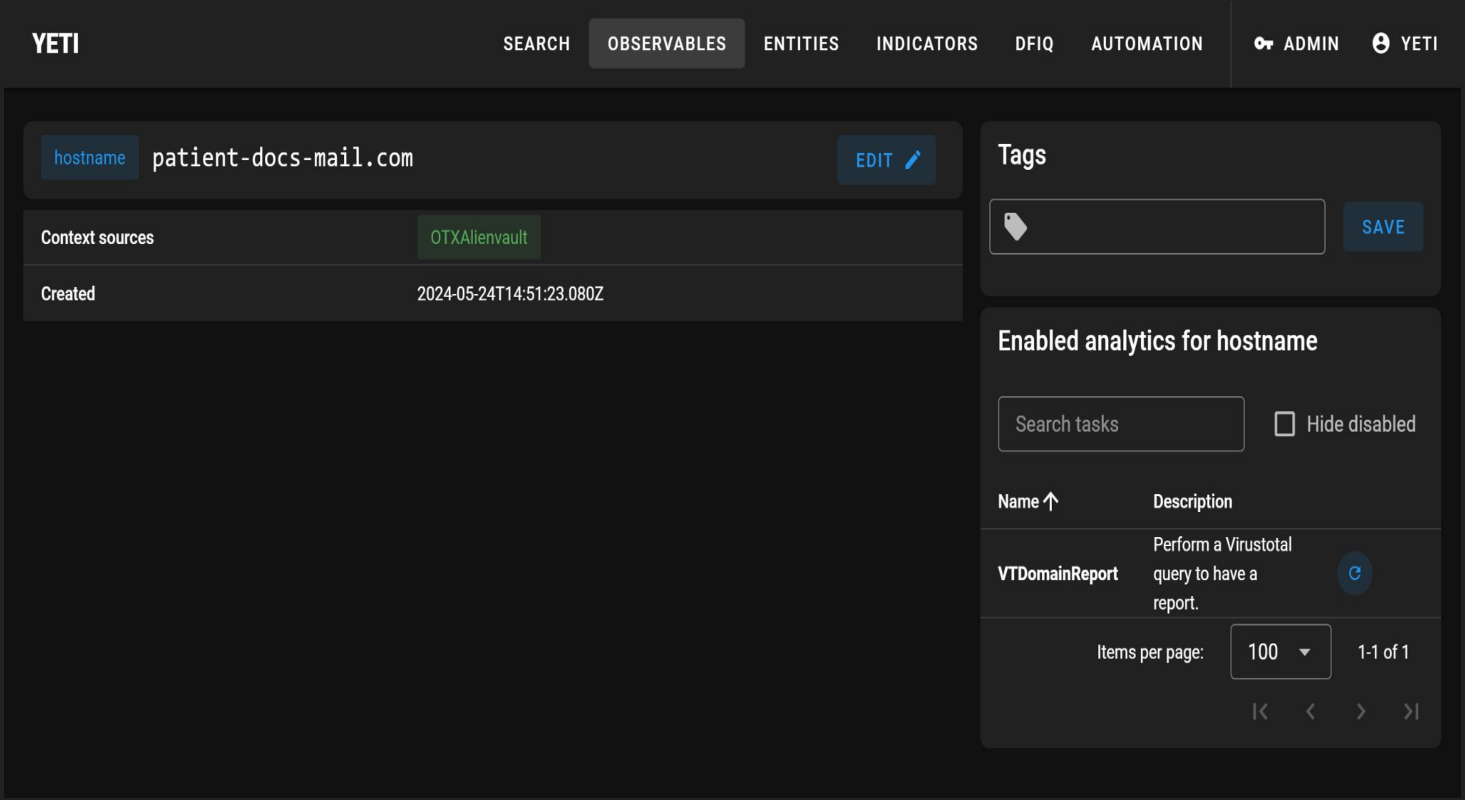
POST `/api/v2/observables/{observable_id}/context/delete` Delete Context

Shiny new VueJS UI ✨



Created on ↓	Value	Tags	Context
2024-05-24 16:51:23	https://www.dropbox.com/scl/fi/w864v8x6a53zu...		OTXAlienvault
2024-05-24 16:51:23	https://www.dropbox.com/scl/fi/s6il9o10zmecnr...		OTXAlienvault
2024-05-24 16:51:23	https://anotepad.com/notes/k55a4dq3		OTXAlienvault
2024-05-24 16:51:23	https://anotepad.com/notes/txb53br5		OTXAlienvault
2024-05-24 16:51:23	https://anotepad.com/notes/cwknw3qs		OTXAlienvault
2024-05-24 16:51:23	https://anotepad.com/notes/4qrjbatw		OTXAlienvault
2024-05-24 16:51:23	https://anotepad.com/notes/2st44b98		OTXAlienvault
2024-05-24 16:51:23	https://anotepad.com/notes/2d94hf6q		OTXAlienvault
2024-05-24 16:51:23	patient-docs-mail.com		OTXAlienvault
2024-05-24 16:51:23	f91a54d4e13e94c0e1b74b1b074a222ce50e258f...		OTXAlienvault
2024-05-24 16:51:22	dfcd0510f07ca6c2979c4953f6e88447fda360b6a...		OTXAlienvault
2024-05-24 16:51:22	dee0e820c2582badd477ccfbe197d6a5803b86b0...		OTXAlienvault
2024-05-24 16:51:22	d60bc54742e1e4f49b2ae74080ef293150f38d7e...		OTXAlienvault
2024-05-24 16:51:22	9ff032282abcc4f82dbb71052033f7a5bfbc334da...		OTXAlienvault
2024-05-24 16:51:22	987751d2052b4e04e619b431239f286a789a647...		OTXAlienvault
2024-05-24 16:51:22	8519569df6b704ff4c1070929395b40933dee936...		OTXAlienvault
2024-05-24 16:51:22	690ce2375759e1c31998011265d31c063615413...		OTXAlienvault
2024-05-24 16:51:22	5a223bf043e552e85f8fe91693221c34aafdfd2b3...		OTXAlienvault

Analytics



hostname patient-docs-mail.com

Context sources	OTXAlienvault
Created	2024-05-24T14:51:23.080Z

Tags

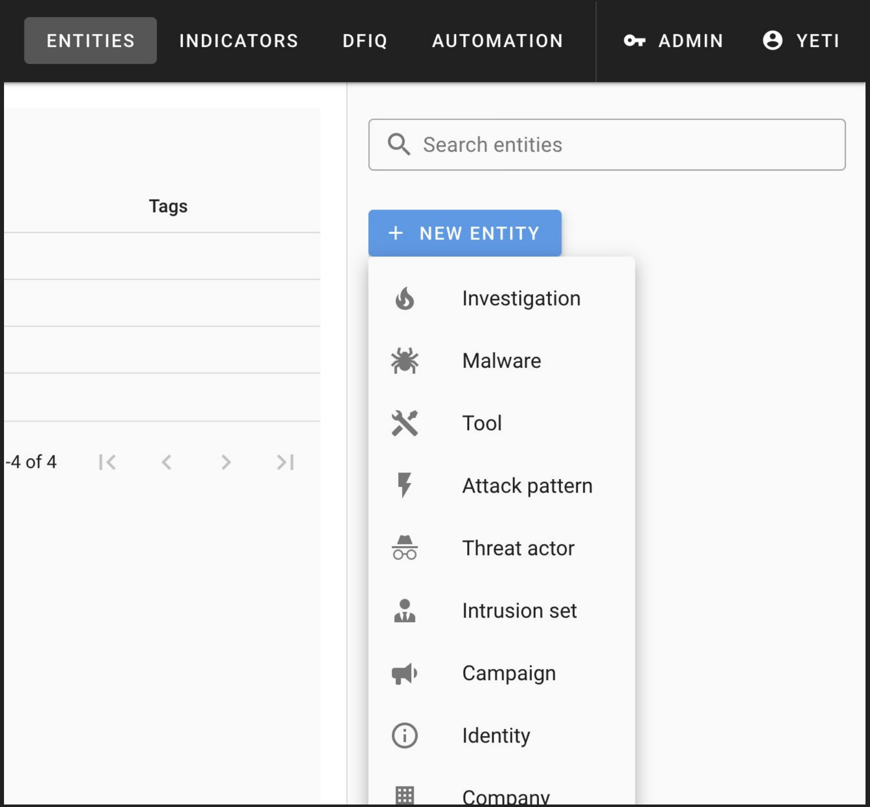
Enabled analytics for hostname

Name ↑	Description
VTDomainReport	Perform a Virustotal query to have a report.

Items per page: 100 1-1 of 1

The CTI we all know and love

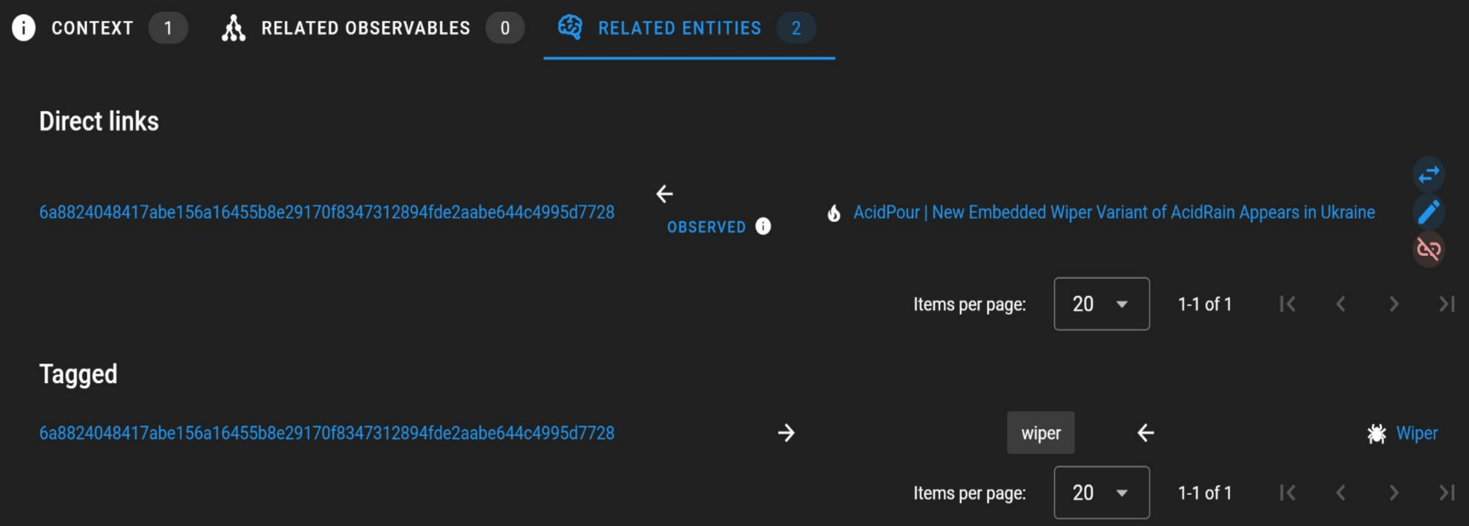
- Entities
  - Malware, tools…
- Indicators
  - Yara, Regex…
- Observables
  - IPs, hashes…



Heavy focus on graphs

- **Threat graph**: Entities ← → Indicators
  - APT28 → uses → XAgentOSX
  - YaraRule → detects → XAgentOSX
- **Tag graph**: Observables ← → Entities
  - Observable → tag ← Entity {malware,group,etc.}

Graphs



Direct links

6a8824048417abe156a16455b8e29170f8347312894fde2aabe644c4995d7728 ← OBSERVED AcidPour | New Embedded Wiper Variant of AcidRain Appears in Ukraine

Items per page: 20 1-1 of 1

Tagged

6a8824048417abe156a16455b8e29170f8347312894fde2aabe644c4995d7728 → wiper ← Wiper

Items per page: 20 1-1 of 1

wait, didn’t you say this was about DFIR wait, didn’t you say this was about DFIR 😅

wtf am Tom looking at?

wtf am Tom looking at?

what *should* Tom be looking at?

…right, DFIR 💡

- I want my **tools** to tell me **where** to look at
- **Where's** the malware?
- How do I find **lateral movement**?
- Where do I see **persistence**?
- Where are ***all*** the binaries?

what do you mean… all the binaries?

Cyber Threat 🦠 Intelligence?

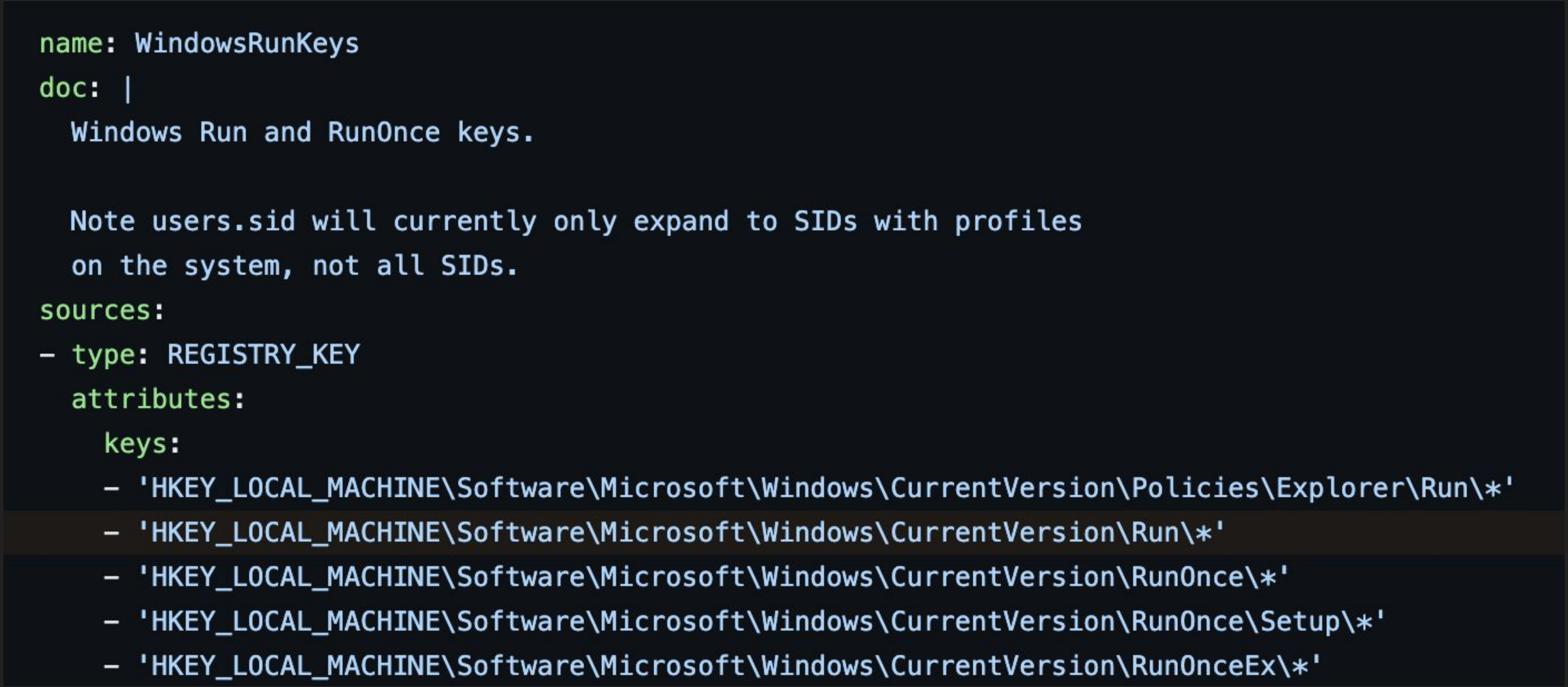
~~Cyber Threat 🦠 Intelligence?~~

Forensics 🔬 intelligence

Non-malicious indicators

- **Classification** rules (e.g. “$mz at 0”)
- Simple **feature extraction** (e.g. “this log line contains an IP address”)
- artifact **catalog** (e.g. “where is persistence? browser history?”)
- hashr, LOLBAS, LOOBins, LOLDrivers, GTFOBins
- ForensicArtifacts

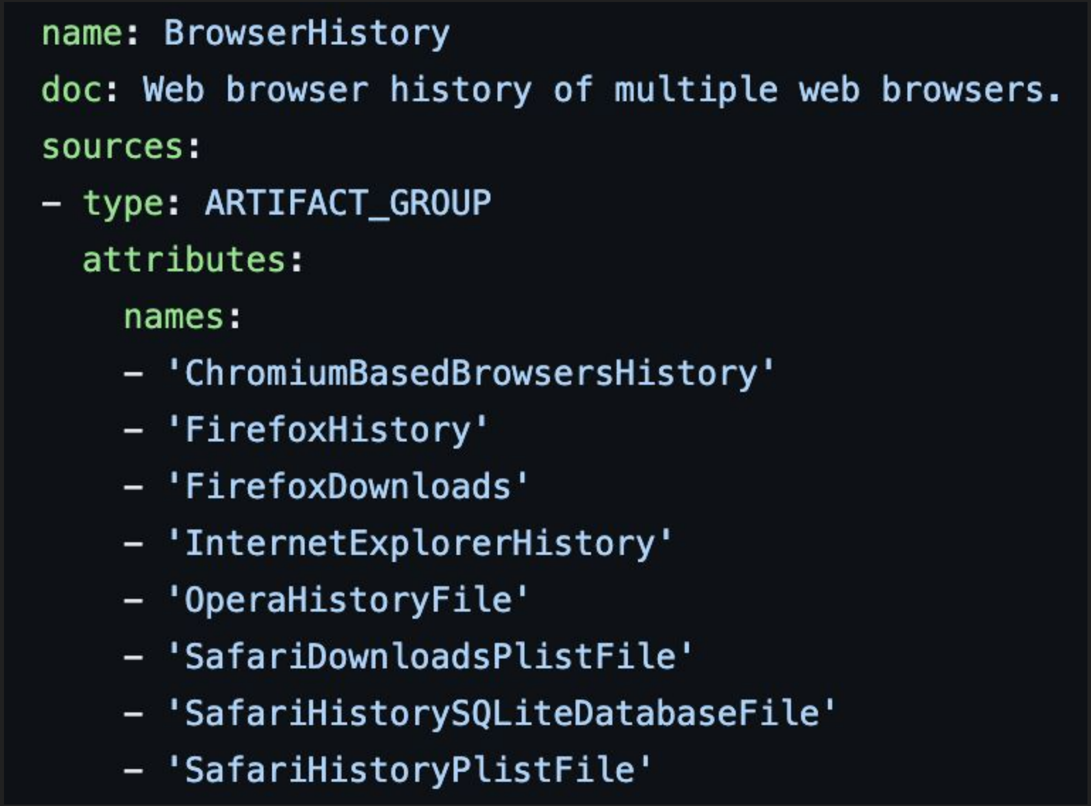
https://github.com/ForensicArtifacts/artifacts



```
name: WindowsRunKeys
doc: |
  Windows Run and RunOnce keys.

  Note users.sid will currently only expand to SIDs with profiles
  on the system, not all SIDs.
sources:
- type: REGISTRY_KEY
  attributes:
    keys:
    - 'HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\*'
    - 'HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\*'
    - 'HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce\*'
    - 'HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup\*'
    - 'HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx\*'
```

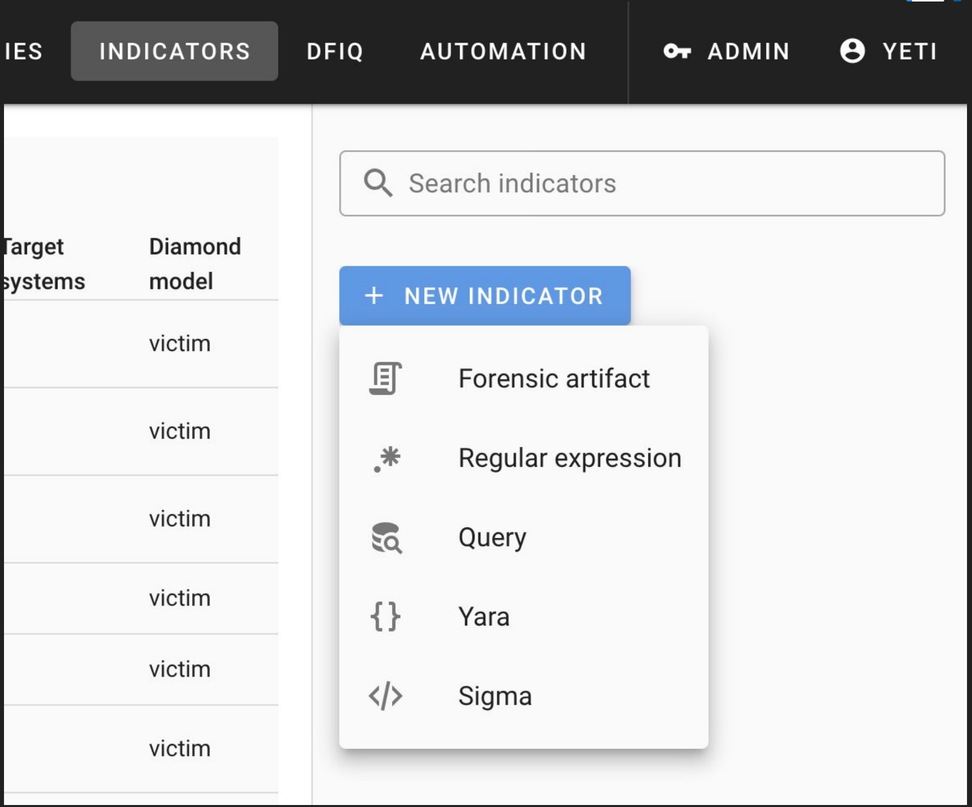
https://github.com/ForensicArtifacts/artifacts



```yaml
name: BrowserHistory
doc: Web browser history of multiple web browsers.
sources:
- type: ARTIFACT_GROUP
  attributes:
    names:
    - 'ChromiumBasedBrowsersHistory'
    - 'FirefoxHistory'
    - 'FirefoxDownloads'
    - 'InternetExplorerHistory'
    - 'OperaHistoryFile'
    - 'SafariDownloadsPlistFile'
    - 'SafariHistorySQLiteDatabaseFile'
    - 'SafariHistoryPlistFile'
```

DFIR-oriented indicators

- Forensic Artifacts
- Regexes
- Queries
- Yara
- Sigma



cool combos - noisy for hunting, good for analysis

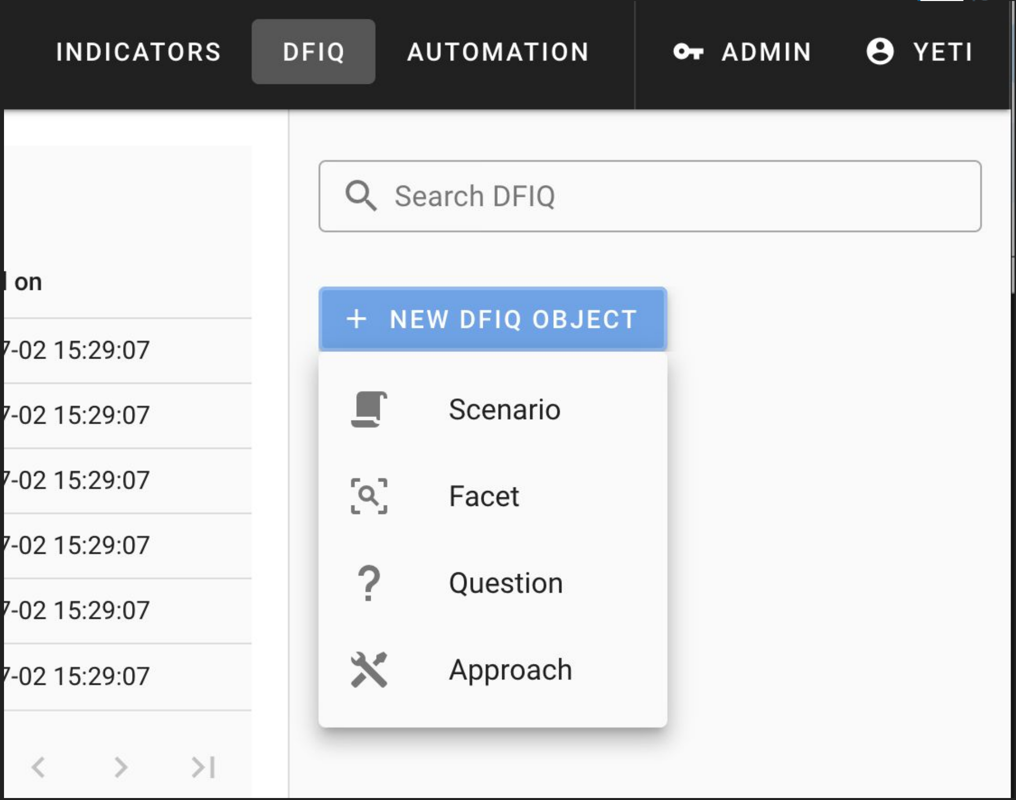
- [execution] + [base64 blob]
- [lolbas] + [{domain, IP}]
- [file creation] + [ELF] - [known good]
- [SSH login] - [known networks]

Can be captured as **Queries**, ingested in e.g. Timesketch

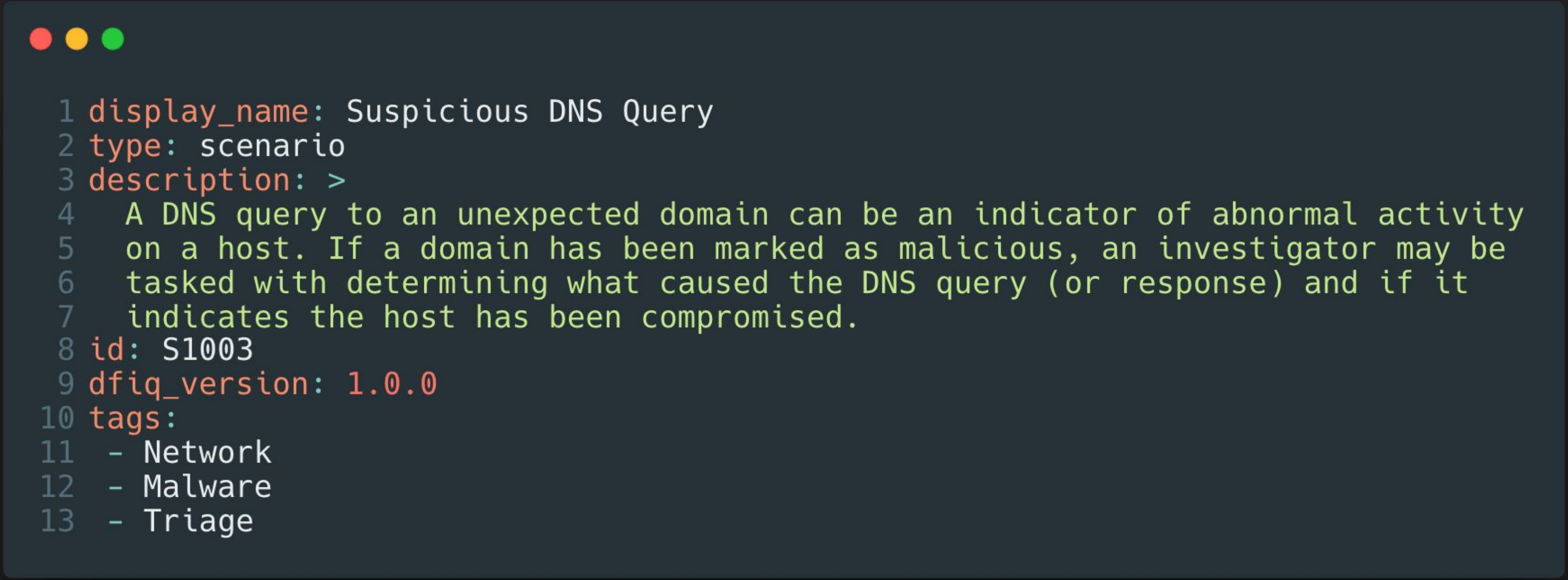
DFIQ

DFIQ - Digital Forensics Investigative Questions

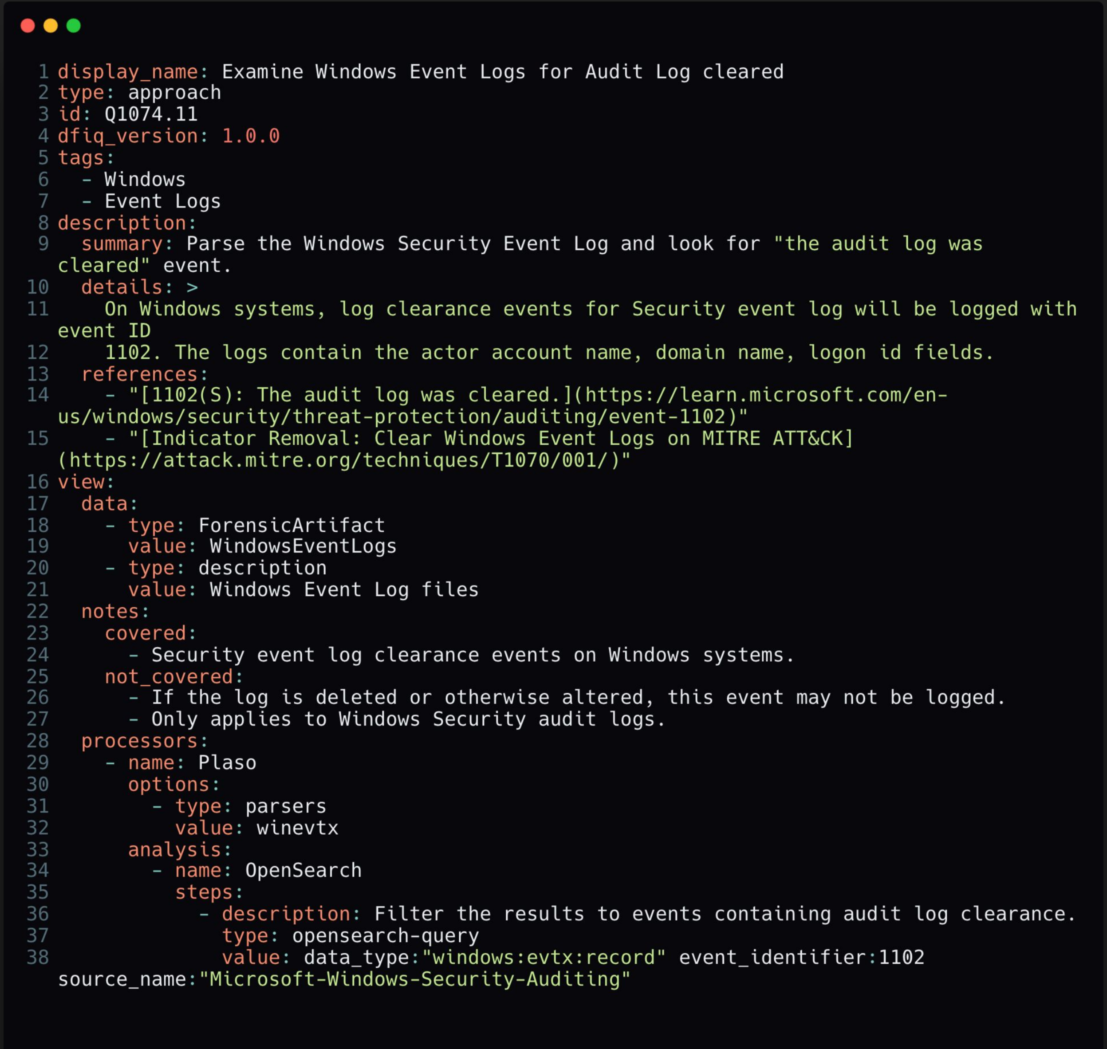
- forensics questions & answers
- YAML markdown
- https://DFIQ.org/



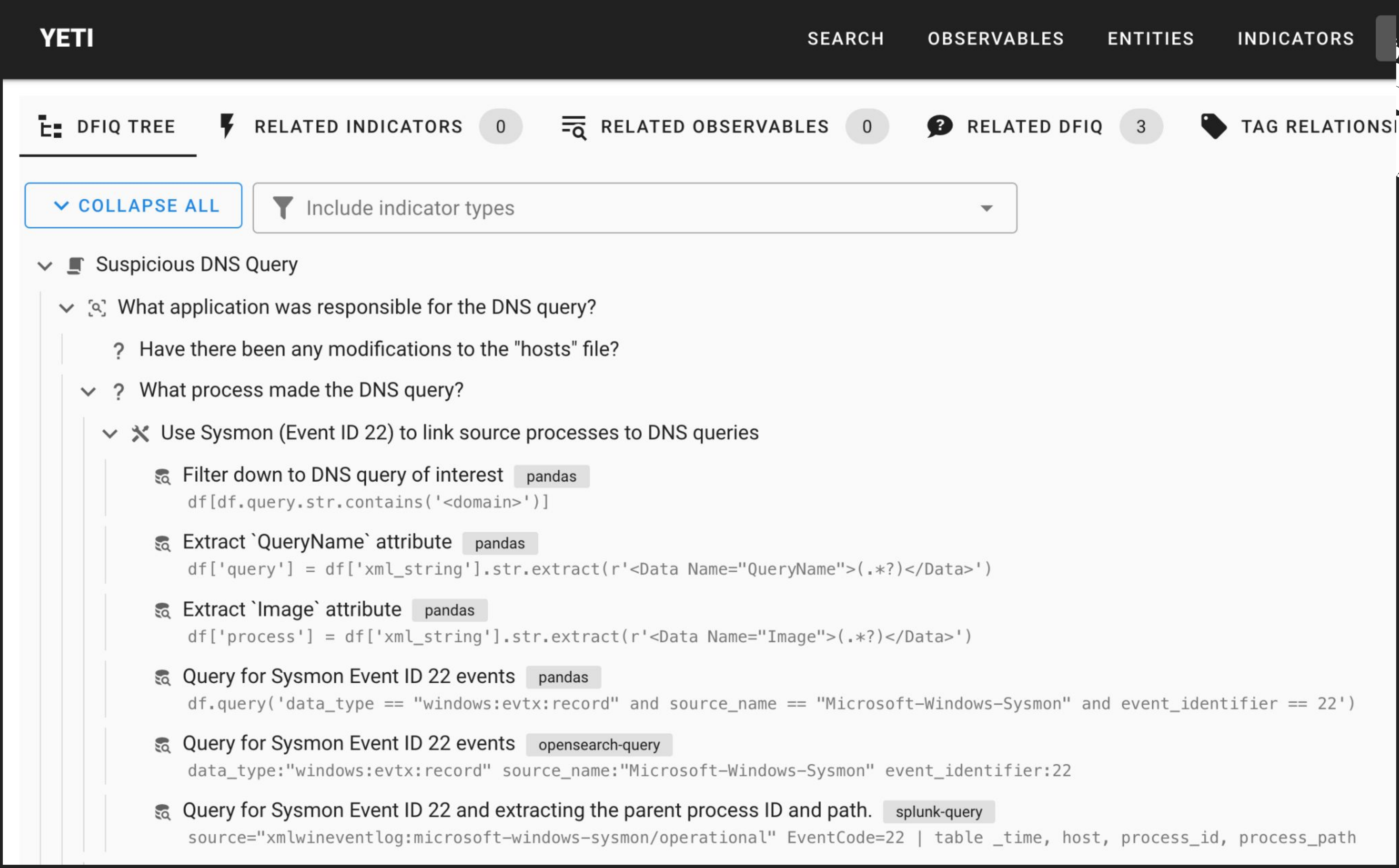
DFIQ - Digital Forensics Investigative Questions



```
display_name: Suspicious DNS Query
type: scenario
description: >
  A DNS query to an unexpected domain can be an indicator of abnormal activity
  on a host. If a domain has been marked as malicious, an investigator may be
  tasked with determining what caused the DNS query (or response) and if it
  indicates the host has been compromised.
id: S1003
dfiq_version: 1.0.0
tags:
 - Network
 - Malware
 - Triage
```



```yaml
display_name: Examine Windows Event Logs for Audit Log cleared
type: approach
id: Q1074.11
dfiq_version: 1.0.0
tags:
  - Windows
  - Event Logs
description:
  summary: Parse the Windows Security Event Log and look for "the audit log was cleared" event.
  details: >
    On Windows systems, log clearance events for Security event log will be logged with event ID
    1102. The logs contain the actor account name, domain name, logon id fields.
  references:
    - "[1102(S): The audit log was cleared.](https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-1102)"
    - "[Indicator Removal: Clear Windows Event Logs on MITRE ATT&CK](https://attack.mitre.org/techniques/T1070/001/)"
view:
  data:
    - type: ForensicArtifact
      value: WindowsEventLogs
    - type: description
      value: Windows Event Log files
  notes:
    covered:
      - Security event log clearance events on Windows systems.
    not_covered:
      - If the log is deleted or otherwise altered, this event may not be logged.
      - Only applies to Windows Security audit logs.
  processors:
    - name: Plaso
      options:
        - type: parsers
          value: winevtx
      analysis:
        - name: OpenSearch
          steps:
            - description: Filter the results to events containing audit log clearance.
              type: opensearch-query
              value: data_type:"windows:evtx:record" event_identifier:1102 source_name:"Microsoft-Windows-Security-Auditing"
```



- Suspicious DNS Query
  - What application was responsible for the DNS query?
    - ? Have there been any modifications to the "hosts" file?
    - ? What process made the DNS query?
      - Use Sysmon (Event ID 22) to link source processes to DNS queries
        - Filter down to DNS query of interest `pandas`

          ```
          df[df.query.str.contains('<domain>')]
          ```
        - Extract `QueryName` attribute `pandas`

          ```
          df['query'] = df['xml_string'].str.extract(r'<Data Name="QueryName">(.*?)</Data>')
          ```
        - Extract `Image` attribute `pandas`

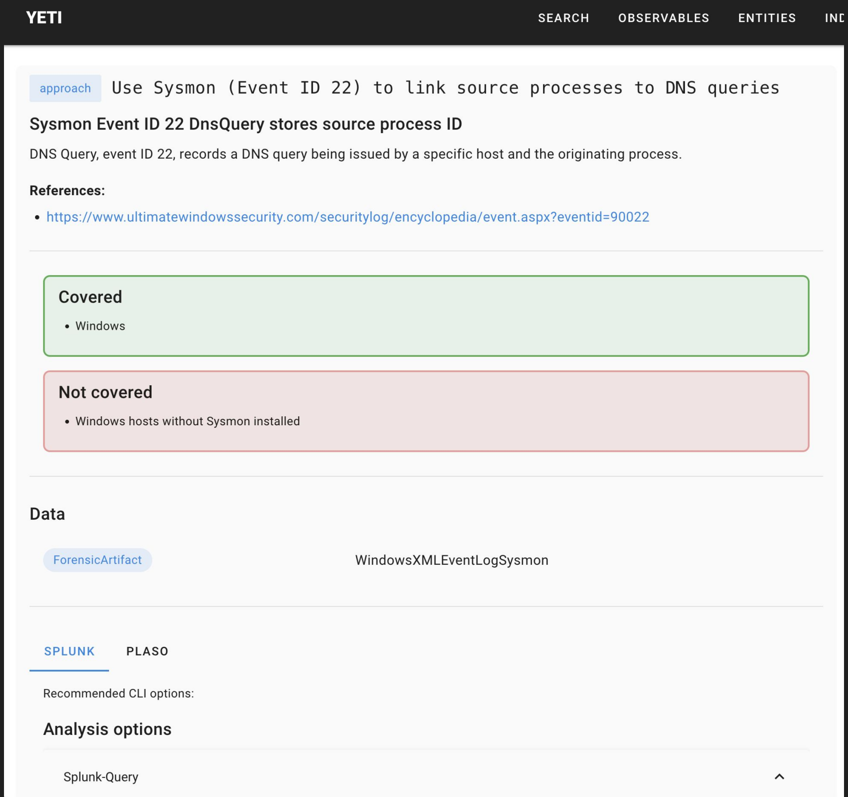
          ```
          df['process'] = df['xml_string'].str.extract(r'<Data Name="Image">(.*?)</Data>')
          ```
        - Query for Sysmon Event ID 22 events `pandas`

          ```
          df.query('data_type == "windows:evtx:record" and source_name == "Microsoft-Windows-Sysmon" and event_identifier == 22')
          ```
        - Query for Sysmon Event ID 22 events `opensearch-query`

          ```
          data_type:"windows:evtx:record" source_name:"Microsoft-Windows-Sysmon" event_identifier:22
          ```
        - Query for Sysmon Event ID 22 and extracting the parent process ID and path. `splunk-query`

          ```
          source="xmlwineventlog:microsoft-windows-sysmon/operational" EventCode=22 | table _time, host, process_id, process_path
          ```

DFIQ - Digital Forensics Investigative Questions



approach Use Sysmon (Event ID 22) to link source processes to DNS queries

Sysmon Event ID 22 DnsQuery stores source process ID

DNS Query, event ID 22, records a DNS query being issued by a specific host and the originating process.

References:

- https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=90022

Covered

- Windows

Not covered

- Windows hosts without Sysmon installed

Data

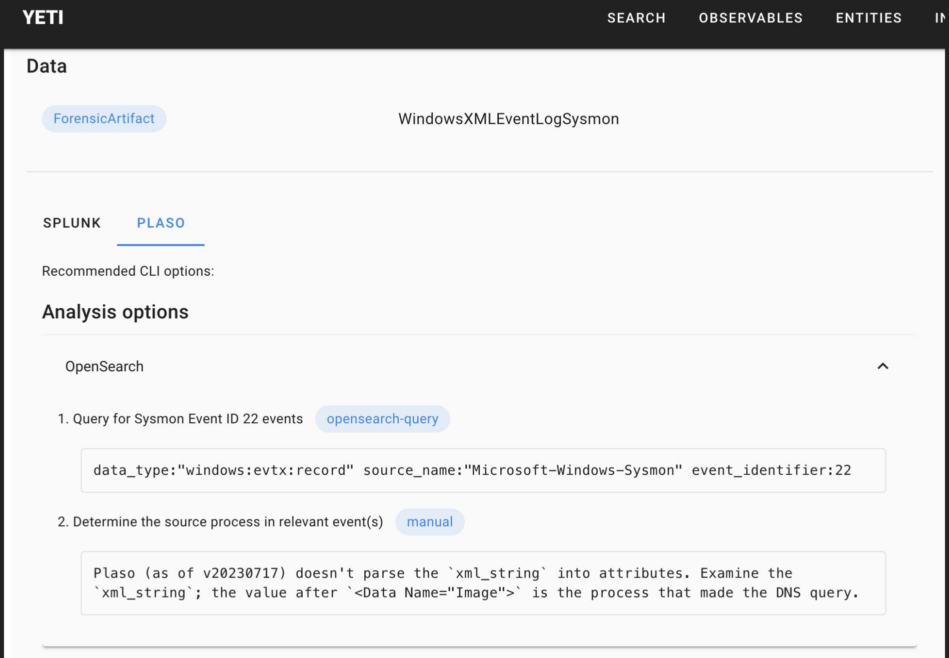
ForensicArtifact WindowsXMLEventLogSysmon

SPLUNK PLASO

Recommended CLI options:

Analysis options

Splunk-Query



Data

ForensicArtifact WindowsXMLEventLogSysmon

SPLUNK PLASO

Recommended CLI options:

Analysis options

OpenSearch

1. Query for Sysmon Event ID 22 events opensearch-query

```
data_type:"windows:evtx:record" source_name:"Microsoft-Windows-Sysmon" event_identifier:22
```

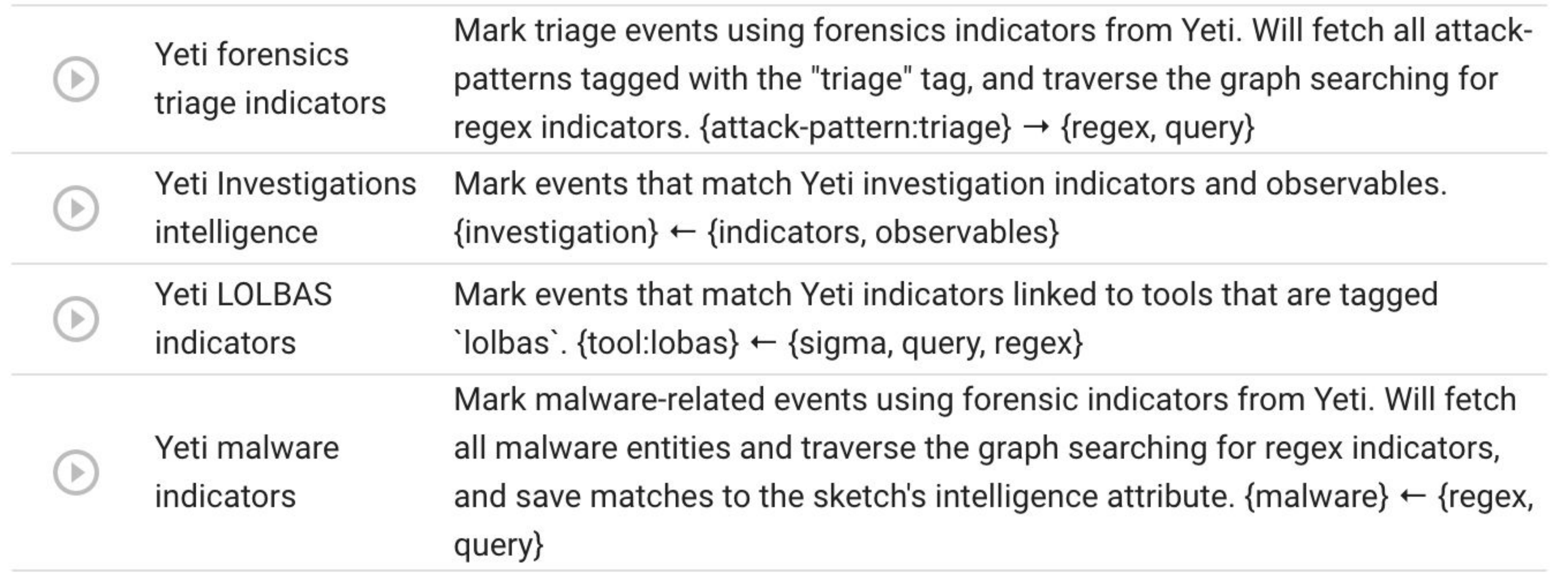
2. Determine the source process in relevant event(s) manual

```
Plaso (as of v20230717) doesn't parse the `xml_string` into attributes. Examine the
`xml_string`; the value after `<Data Name="Image">` is the process that made the DNS query.
```

Integration avenues

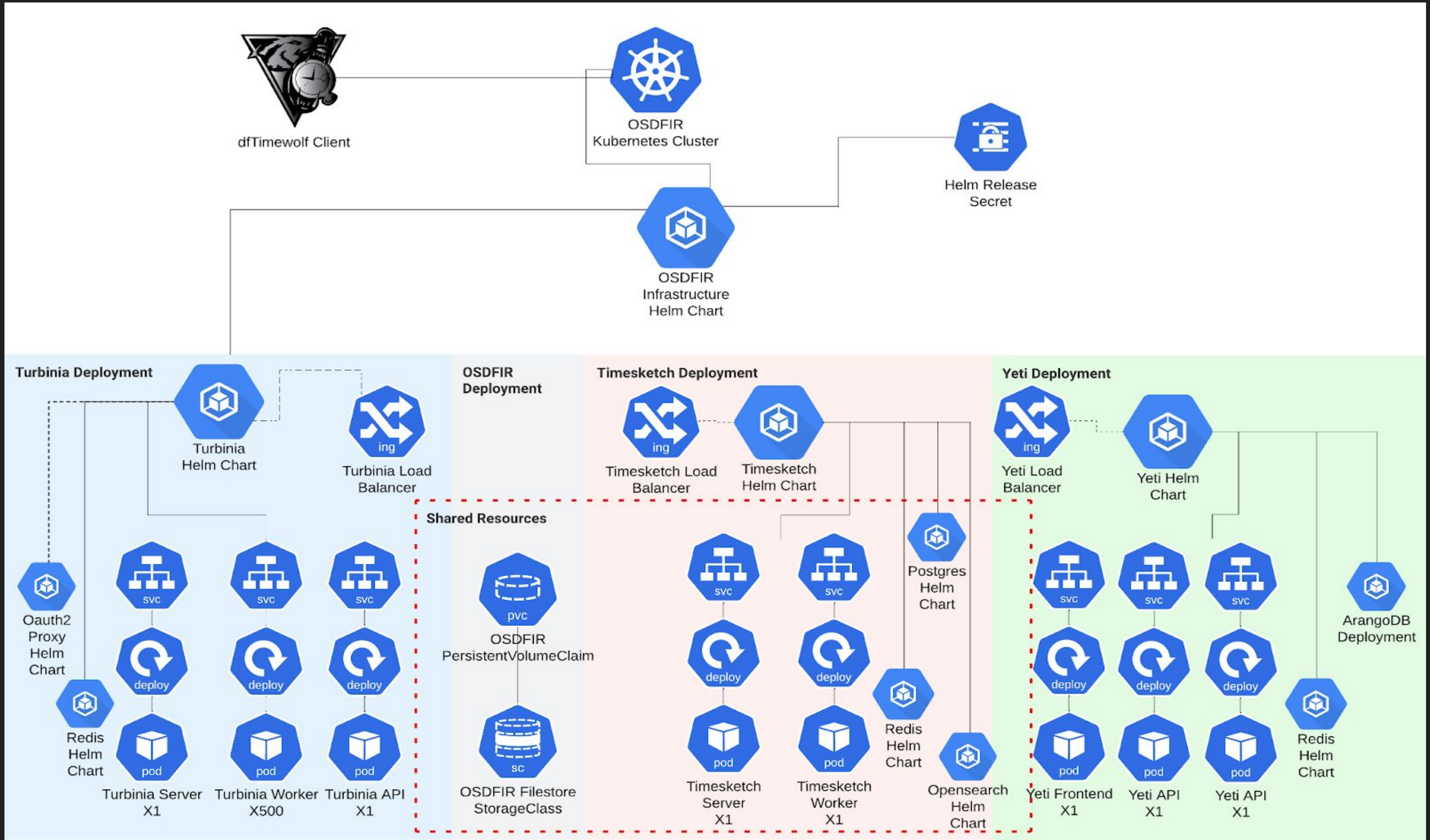
- Yeti is an open **Forensics Intelligence** store
- **Timesketch** analyzers
- Send classification Yara rules to **Turbinia / plaso**
- Store, share, improve, iterate upon **useful queries**
- DFIQ: **sharing approaches** to investigations

Integration avenues



▷	Yeti forensics triage indicators	Mark triage events using forensics indicators from Yeti. Will fetch all attack-patterns tagged with the "triage" tag, and traverse the graph searching for regex indicators. {attack-pattern:triage} → {regex, query}
▷	Yeti Investigations intelligence	Mark events that match Yeti investigation indicators and observables. {investigation} ← {indicators, observables}
▷	Yeti LOLBAS indicators	Mark events that match Yeti indicators linked to tools that are tagged \`lolbas\`. {tool:lobas} ← {sigma, query, regex}
▷	Yeti malware indicators	Mark malware-related events using forensic indicators from Yeti. Will fetch all malware entities and traverse the graph searching for regex indicators, and save matches to the sketch's intelligence attribute. {malware} ← {regex, query}

Part of the https://osdfir.blogspot.com/ family



Demo time

roadmap 🗺️

- MISP integration
- Graph visualization
- Dynamic artifact generation (eg from tagged Observables)
- RBAC, dashboards, review system…

takeaways

- Yeti moves from a CTI platform to a **DFI platform**
- Acts as a automated, reusable **forensics KB**, leveraging **DFIQ**
- Helps forensic analysts automatically weed out the bad by providing ways to **slice and dice data**

(Tom can’t help it and keeps doing full software rewrites)

Thanks!

Documentation	https://yeti-platform.io/
GitHub org	https://github.com/yeti-platform/