The TIP of the Stinger:

Efficiently Using Threat Intelligence With TheHive

Matthew Gracie
Information Security Engineer

BlueCross BlueShield
of Western New York

# whoami

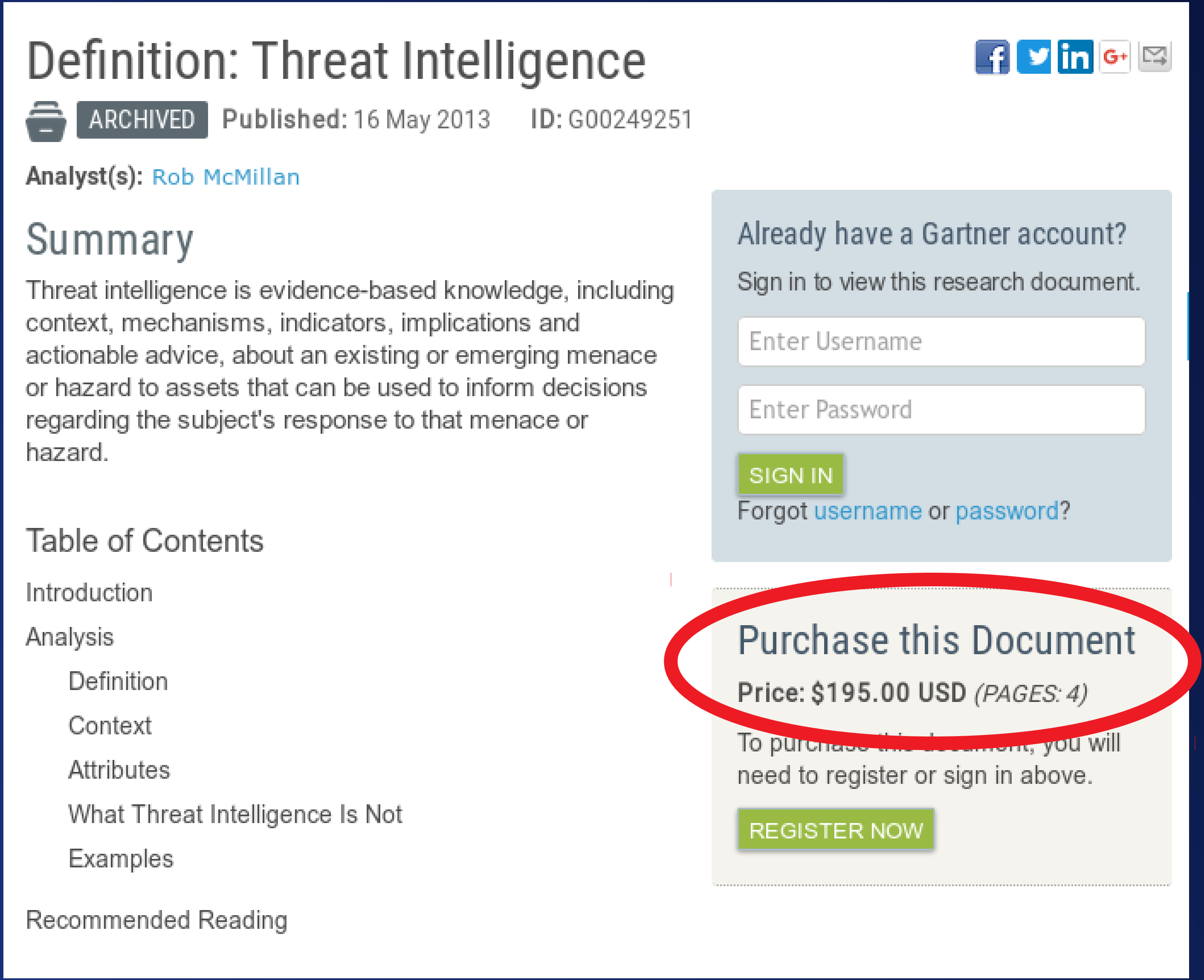
PEOPLE WHO
BUY THINGS
ARE SUCKERS
quickmeme.com

What am I talking about today?

What is Threat Intelligence?

“Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.” --Gartner *

* https://www.gartner.com/doc/2487216/definition-threat-intelligence



Definition: Threat Intelligence

ARCHIVED **Published:** 16 May 2013 **ID:** G00249251

Analyst(s): Rob McMillan

Summary

Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.

Table of Contents

Already have a Gartner account?

Sign in to view this research document.

Forgot username or password?

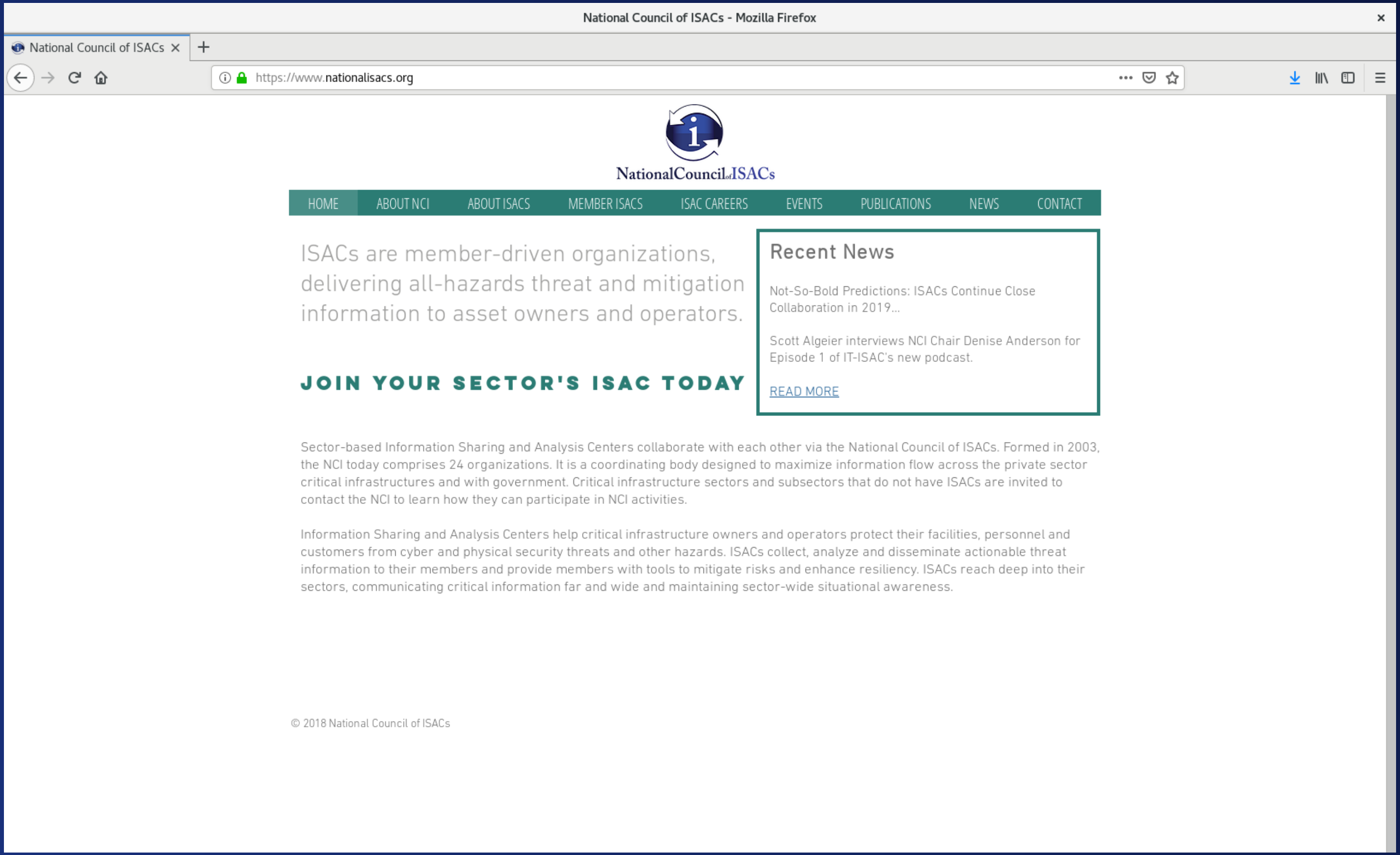
Purchase this Document

Price: $195.00 USD *(PAGES: 4)*

To purchase this document, you will need to register or sign in above.

PEOPLE WHO
BUY THINGS
ARE SUCKERS
quickmeme.com

WHERE DOES HE GET THOSE WONDERFUL IOCS?
imgflip.com



ISACs are member-driven organizations, delivering all-hazards threat and mitigation information to asset owners and operators.

JOIN YOUR SECTOR'S ISAC TODAY

Recent News

Not-So-Bold Predictions: ISACs Continue Close Collaboration in 2019...

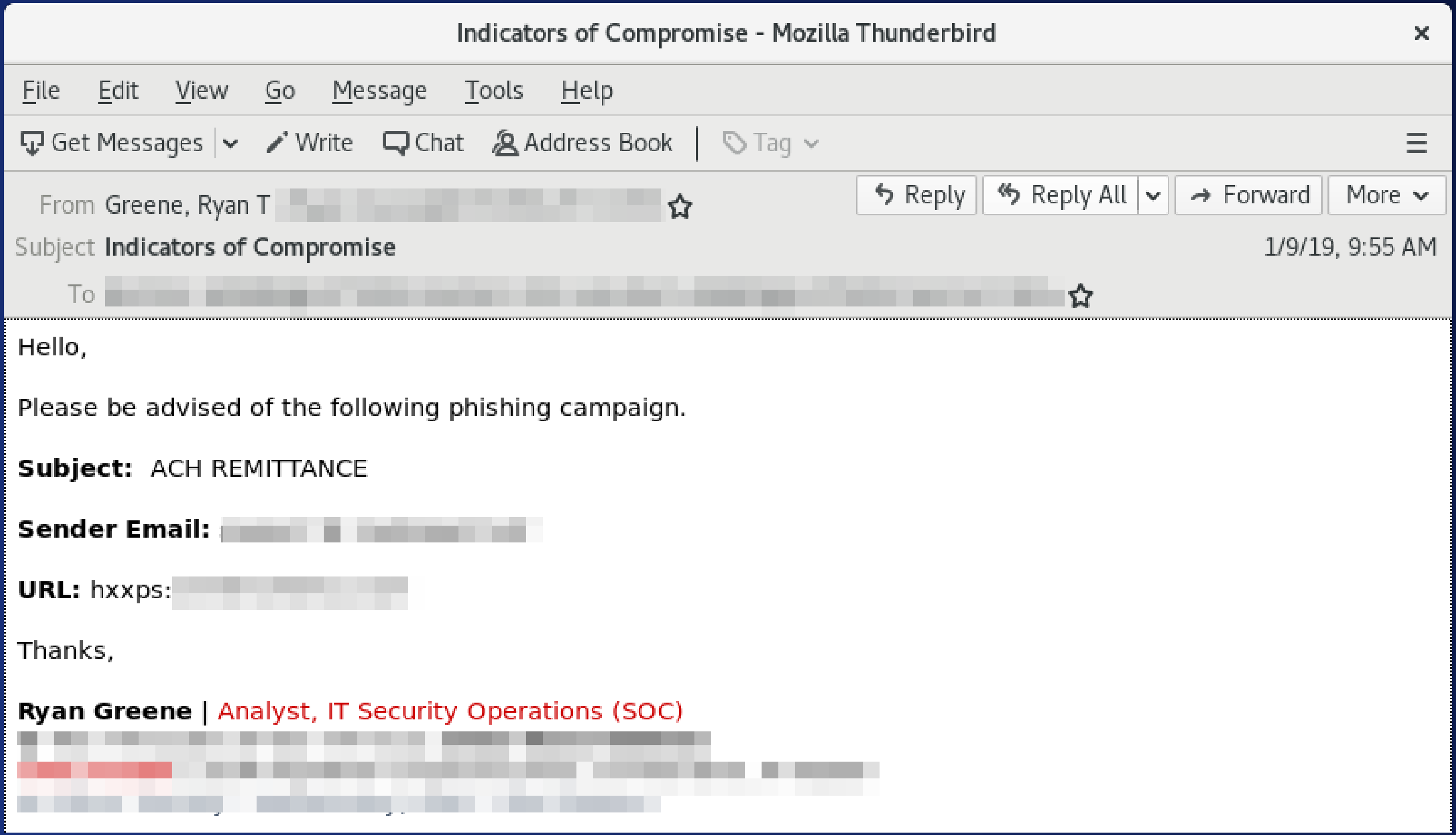
Scott Algeier interviews NCI Chair Denise Anderson for Episode 1 of IT-ISAC's new podcast.

READ MORE

Sector-based Information Sharing and Analysis Centers collaborate with each other via the National Council of ISACs. Formed in 2003, the NCI today comprises 24 organizations. It is a coordinating body designed to maximize information flow across the private sector critical infrastructures and with government. Critical infrastructure sectors and subsectors that do not have ISACs are invited to contact the NCI to learn how they can participate in NCI activities.

Information Sharing and Analysis Centers help critical infrastructure owners and operators protect their facilities, personnel and customers from cyber and physical security threats and other hazards. ISACs collect, analyze and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency. ISACs reach deep into their sectors, communicating critical information far and wide and maintaining sector-wide situational awareness.

© 2018 National Council of ISACs



From Greene, Ryan T [redacted]

Subject Indicators of Compromise

1/9/19, 9:55 AM

To [redacted]

Hello,

Please be advised of the following phishing campaign.

Subject: ACH REMITTANCE

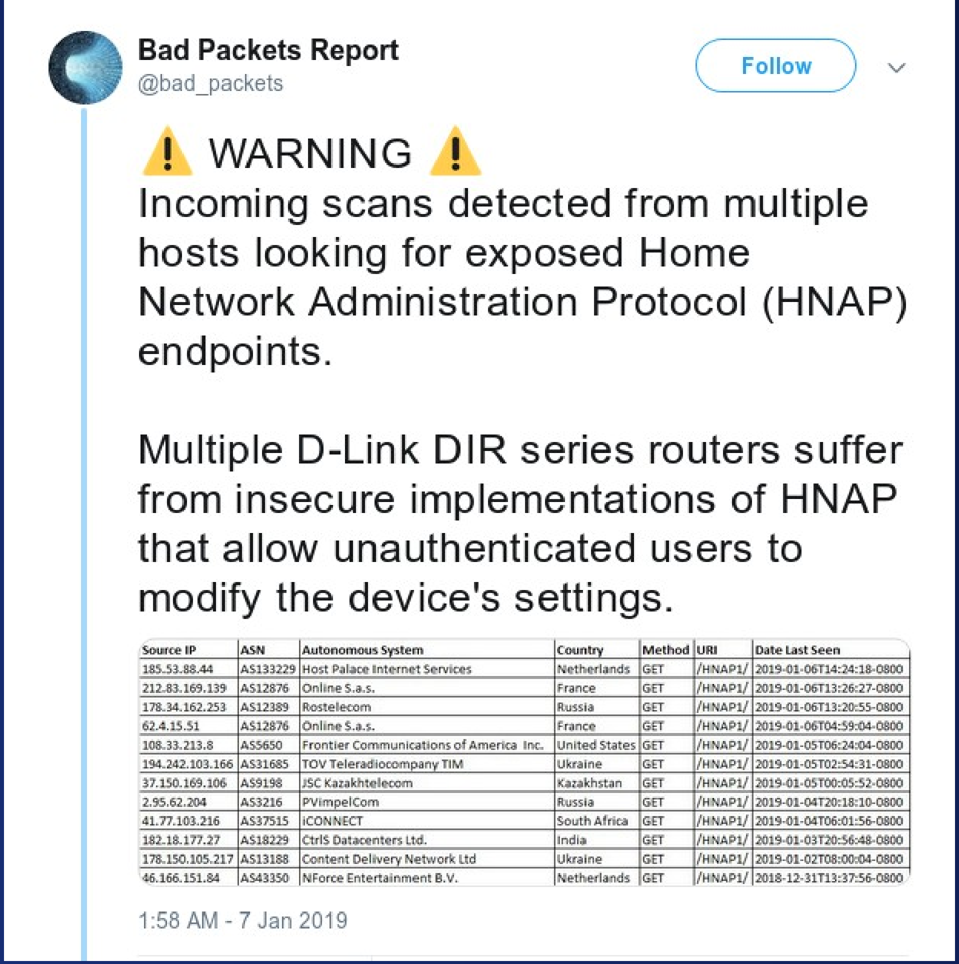
Sender Email: [redacted]

URL: hxxps:[redacted]

Thanks,

Ryan Greene | Analyst, IT Security Operations (SOC)

[redacted]



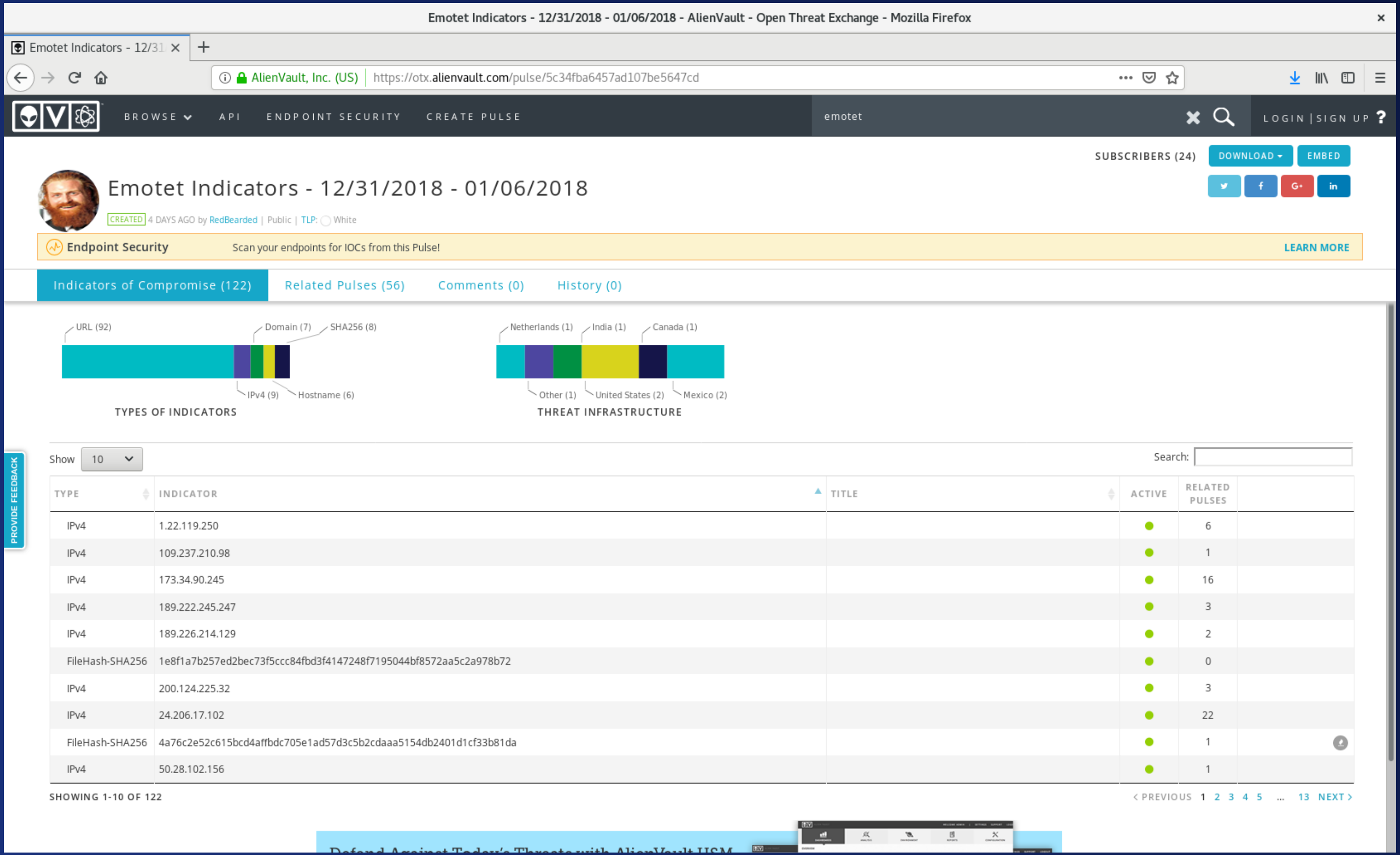
Bad Packets Report
@bad_packets

⚠️ WARNING ⚠️
Incoming scans detected from multiple hosts looking for exposed Home Network Administration Protocol (HNAP) endpoints.

Multiple D-Link DIR series routers suffer from insecure implementations of HNAP that allow unauthenticated users to modify the device's settings.

Source IP	ASN	Autonomous System	Country	Method	URI	Date Last Seen
185.53.88.44	AS133229	Host Palace Internet Services	Netherlands	GET	/HNAP1/	2019-01-06T14:24:18-0800
212.83.169.139	AS12876	Online S.a.s.	France	GET	/HNAP1/	2019-01-06T13:26:27-0800
178.34.162.253	AS12389	Rostelecom	Russia	GET	/HNAP1/	2019-01-06T13:20:55-0800
62.4.15.51	AS12876	Online S.a.s.	France	GET	/HNAP1/	2019-01-06T04:59:04-0800
108.33.213.8	AS5650	Frontier Communications of America Inc.	United States	GET	/HNAP1/	2019-01-05T06:24:04-0800
194.242.103.166	AS31685	TOV Teleradiocompany TIM	Ukraine	GET	/HNAP1/	2019-01-05T02:54:31-0800
37.150.169.106	AS9198	JSC Kazakhtelecom	Kazakhstan	GET	/HNAP1/	2019-01-05T00:05:52-0800
2.95.62.204	AS3216	PVimpelCom	Russia	GET	/HNAP1/	2019-01-04T20:18:10-0800
41.77.103.216	AS37515	iCONNECT	South Africa	GET	/HNAP1/	2019-01-04T06:01:56-0800
182.18.177.27	AS18229	CtrlS Datacenters Ltd.	India	GET	/HNAP1/	2019-01-03T20:56:48-0800
178.150.105.217	AS13188	Content Delivery Network Ltd	Ukraine	GET	/HNAP1/	2019-01-02T08:00:04-0800
46.166.151.84	AS43350	NForce Entertainment B.V.	Netherlands	GET	/HNAP1/	2018-12-31T13:37:56-0800

1:58 AM - 7 Jan 2019


Emotet Indicators - 12/31/2018 - 01/06/2018 - AlienVault - Open Threat Exchange - Mozilla Firefox
Emotet Indicators - 12/31
AlienVault, Inc. (US)
https://otx.alienvault.com/pulse/5c34fba6457ad107be5647cd
BROWSE
API
ENDPOINT SECURITY
CREATE PULSE
emotet
LOGIN | SIGN UP
SUBSCRIBERS (24)
DOWNLOAD
EMBED
PROVIDE FEEDBACK

Emotet Indicators - 12/31/2018 - 01/06/2018

CREATED 4 DAYS AGO by RedBearded | Public | TLP: ○ White

Endpoint Security Scan your endpoints for IOCs from this Pulse! LEARN MORE

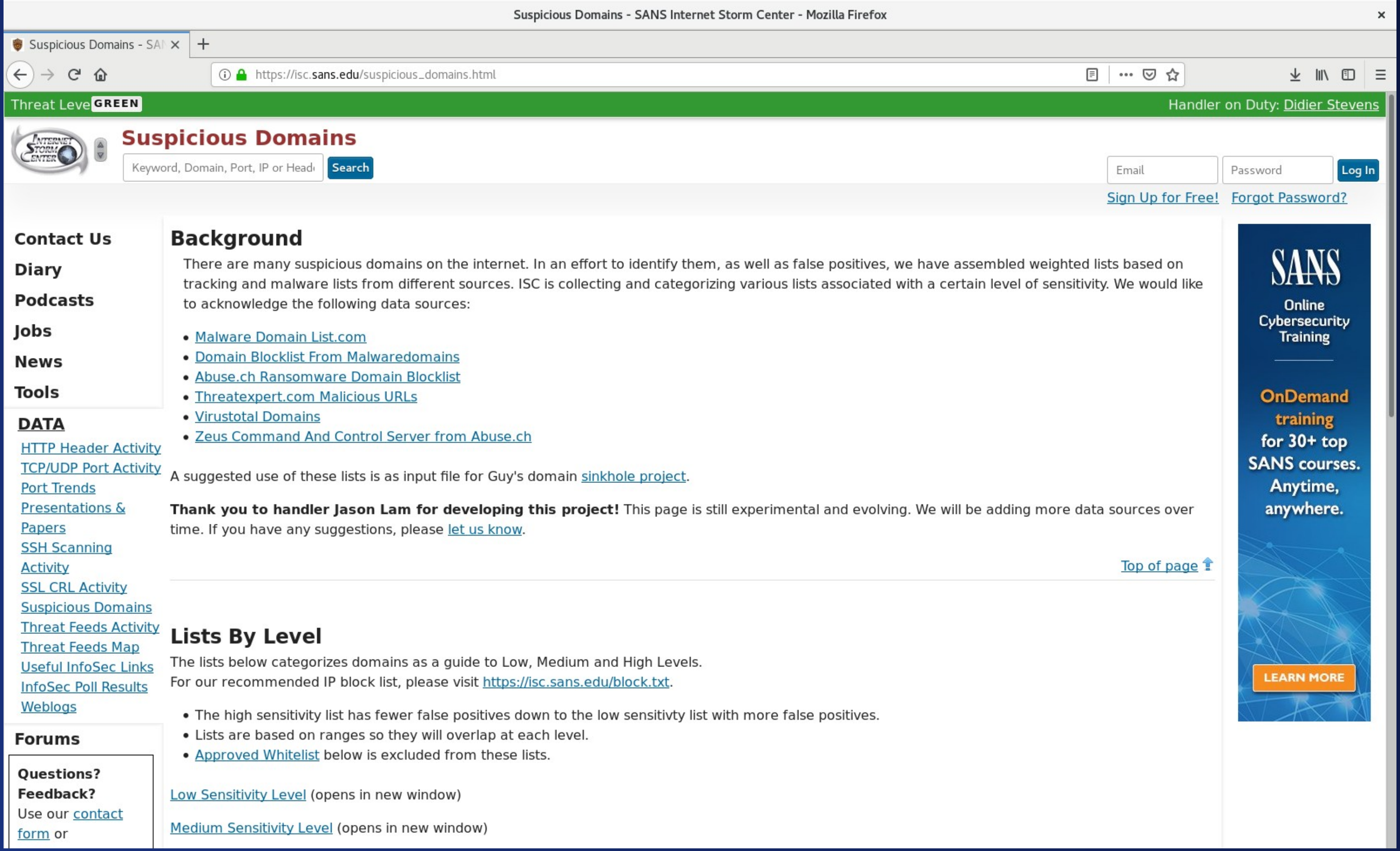
Indicators of Compromise (122) Related Pulses (56) Comments (0) History (0)

Show 10 Search:

TYPE	INDICATOR	TITLE	ACTIVE	RELATED PULSES
IPv4	1.22.119.250		●	6
IPv4	109.237.210.98		●	1
IPv4	173.34.90.245		●	16
IPv4	189.222.245.247		●	3
IPv4	189.226.214.129		●	2
FileHash-SHA256	1e8f1a7b257ed2bec73f5ccc84fbd3f4147248f7195044bf8572aa5c2a978b72		●	0
IPv4	200.124.225.32		●	3
IPv4	24.206.17.102		●	22
FileHash-SHA256	4a76c2e52c615bcd4affbdc705e1ad57d3c5b2cdaaa5154db2401d1cf33b81da		●	1
IPv4	50.28.102.156		●	1

SHOWING 1-10 OF 122

< PREVIOUS 1 2 3 4 5 ... 13 NEXT >



Suspicious Domains

Background

There are many suspicious domains on the internet. In an effort to identify them, as well as false positives, we have assembled weighted lists based on tracking and malware lists from different sources. ISC is collecting and categorizing various lists associated with a certain level of sensitivity. We would like to acknowledge the following data sources:

- Malware Domain List.com
- Domain Blocklist From Malwaredomains
- Abuse.ch Ransomware Domain Blocklist
- Threatexpert.com Malicious URLs
- Virustotal Domains
- Zeus Command And Control Server from Abuse.ch

A suggested use of these lists is as input file for Guy's domain sinkhole project.

Thank you to handler Jason Lam for developing this project! This page is still experimental and evolving. We will be adding more data sources over time. If you have any suggestions, please let us know.

Top of page

Lists By Level

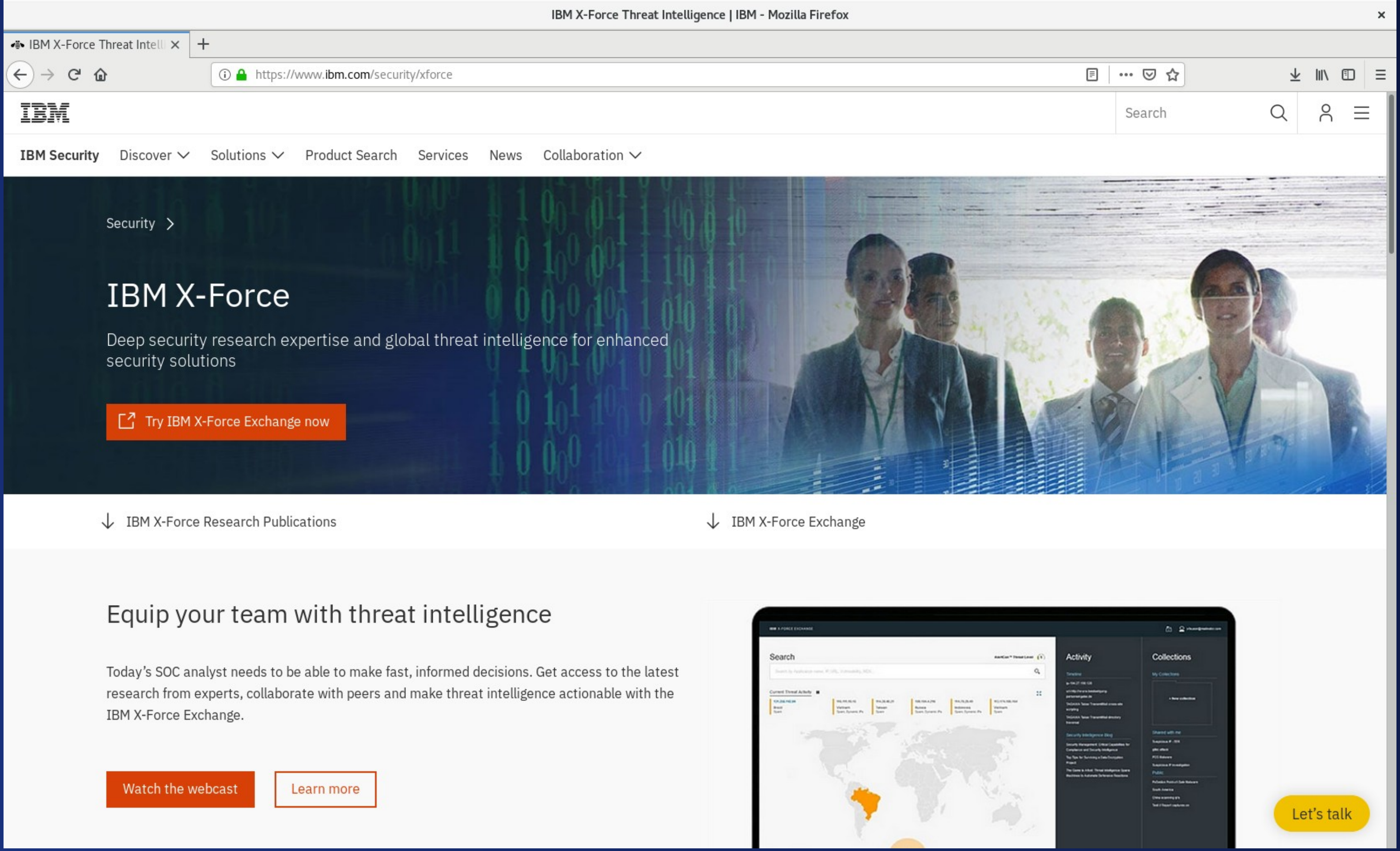
The lists below categorizes domains as a guide to Low, Medium and High Levels.
For our recommended IP block list, please visit https://isc.sans.edu/block.txt.

- The high sensitivity list has fewer false positives down to the low sensitivty list with more false positives.
- Lists are based on ranges so they will overlap at each level.
- Approved Whitelist below is excluded from these lists.

Low Sensitivity Level (opens in new window)

Medium Sensitivity Level (opens in new window)

Questions? Feedback?
Use our contact form or


IBM X-Force Threat Intelligence | IBM - Mozilla Firefox
IBM X-Force Threat Intell
https://www.ibm.com/security/xforce
IBM
Search
IBM Security
Discover
Solutions
Product Search
Services
News
Collaboration
Security
Try IBM X-Force Exchange now
IBM X-Force Research Publications
IBM X-Force Exchange
Search
Activity
Collections
Watch the webcast
Learn more
Let's talk

IBM X-Force

Deep security research expertise and global threat intelligence for enhanced security solutions

Equip your team with threat intelligence

Today's SOC analyst needs to be able to make fast, informed decisions. Get access to the latest research from experts, collaborate with peers and make threat intelligence actionable with the IBM X-Force Exchange.

So How Do We Use It?

MISP

- MISP is an open source Threat Intel Platform
- Collects, sanitizes, and distributes IOCs
- Supports tagging, TLP, galaxies, taxonomies, and much more
- Robust import and export capabilities
- This is an excellent “system of record”

Getting Data Into MISP

- Manual entry in web console
- Import local MISP JSON or CSV files
- Share data with other MISP instances
- Import .IOC files, Threatconnect, PDF, etc.
- Many third party extensions and add-ons

How Does MISP Structure Data?

- Events
- Attributes
- Tags
- Threat and Analysis Level
- Distribution

Security Onion

- Project by Doug Burks (@dougburks)
- Prebuilt Dockerized stack of open source NSM tools
- Available as an appliance ISO
- Can be installed on top of vanilla Ubuntu and RHEL/CentOS
- Commercial support and training available
- Can be used live or for pcap processing
- Requires a network tap or SPAN port for live usage

Suricata

- Security Onion comes with either Snort or Suricata
- These compare network traffic to defined signatures and raise alerts when a match is found
- By default, free Emerging Threats rules available
- Easily leveraged with threat intelligence

Zeek / Bro

- This generates network connection metadata from the observed traffic
- Think of it as Netflow++ – all the connection information of Netflow with some actual layer 7 data as well
- The Bro_Intel framework can be used to check metadata for IOCs

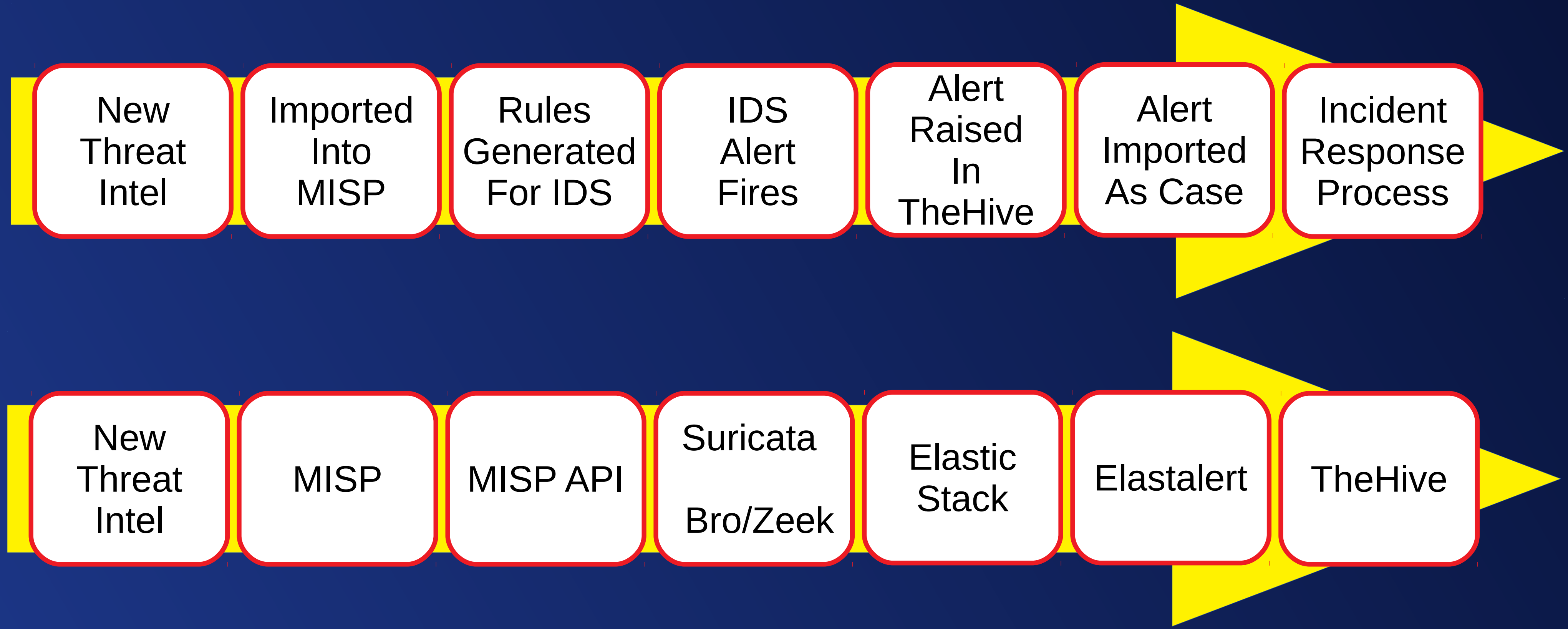
Elastic Stack

- Security Onion uses the Elastic Stack for its main reporting interface
- Data is stored in an Elasticsearch backend
- Queries and visualization is done in Kibana
- Elastalert is also integrated

TheHive

- TheHive is an open source SOAR platform
- Allows real-time IR collaboration
- Dashboards and reporting
- Integrates with MISP for threat intel functions
- Alerts, Cases, and Case Templates
- New observables can export back to MISP

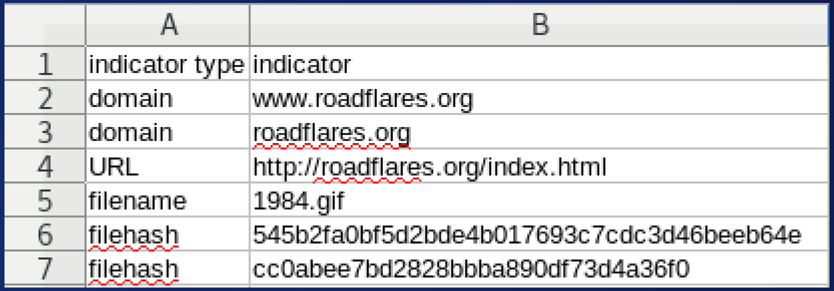
Hunting IOCs



New Threat Intel → Imported Into MISP → Rules Generated For IDS → IDS Alert Fires → Alert Raised In TheHive → Alert Imported As Case → Incident Response Process

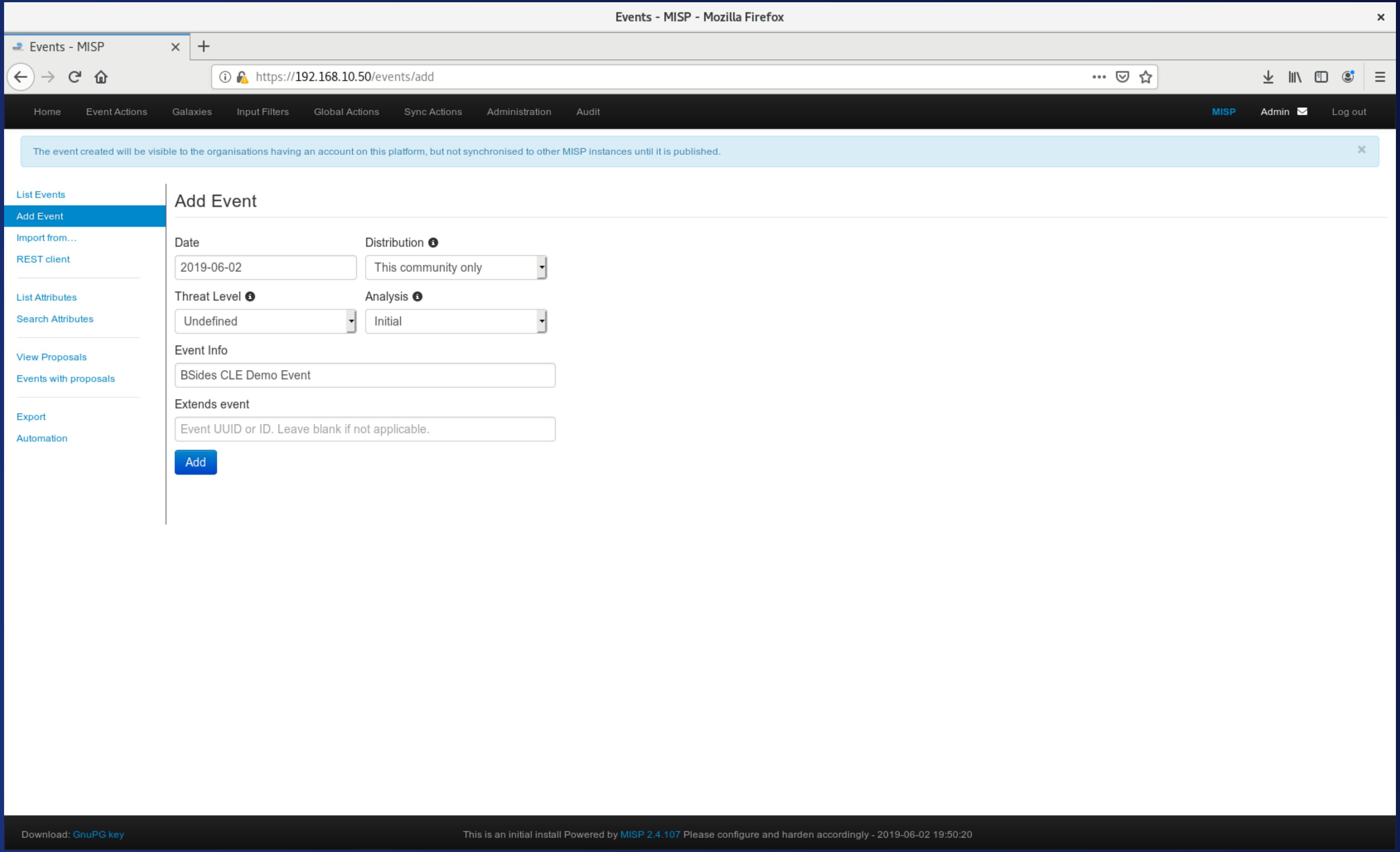
New Threat Intel → MISP → MISP API → Suricata Bro/Zeek → Elastic Stack → Elastalert → TheHive

Demonstration



	A	B
1	indicator type	indicator
2	domain	www.roadflares.org
3	domain	roadflares.org
4	URL	http://roadflares.org/index.html
5	filename	1984.gif
6	filehash	545b2fa0bf5d2bde4b017693c7cdc3d46beeb64e
7	filehash	cc0abee7bd2828bbba890df73d4a36f0

** Please note, this is just an example using my personal domain, not anything actually malicious.*



The event created will be visible to the organisations having an account on this platform, but not synchronised to other MISP instances until it is published.

Add Event

Date: 2019-06-02

Distribution: This community only

Threat Level: Undefined

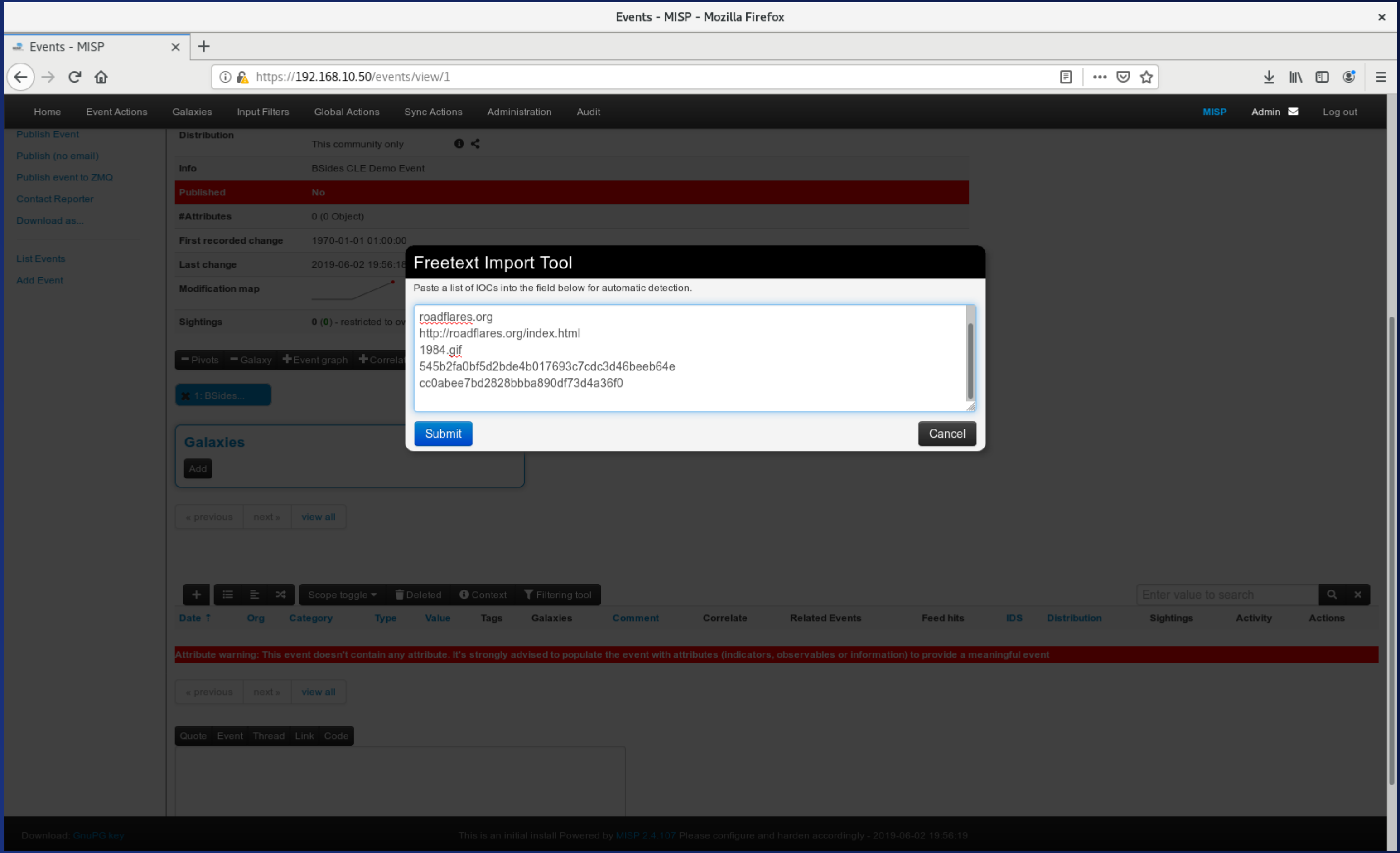
Analysis: Initial

Event Info: BSides CLE Demo Event

Extends event: Event UUID or ID. Leave blank if not applicable.

Download: GnuPG key

This is an initial install Powered by MISP 2.4.107 Please configure and harden accordingly - 2019-06-02 19:50:20



Distribution	This community only
Info	BSides CLE Demo Event
Published	No
#Attributes	0 (0 Object)
First recorded change	1970-01-01 01:00:00
Last change	2019-06-02 19:56:1
Modification map	
Sightings	0 (0) - restricted to ov

Attribute warning: This event doesn't contain any attribute. It's strongly advised to populate the event with attributes (indicators, observables or information) to provide a meaningful event

Freetext Import Tool

Paste a list of IOCs into the field below for automatic detection.

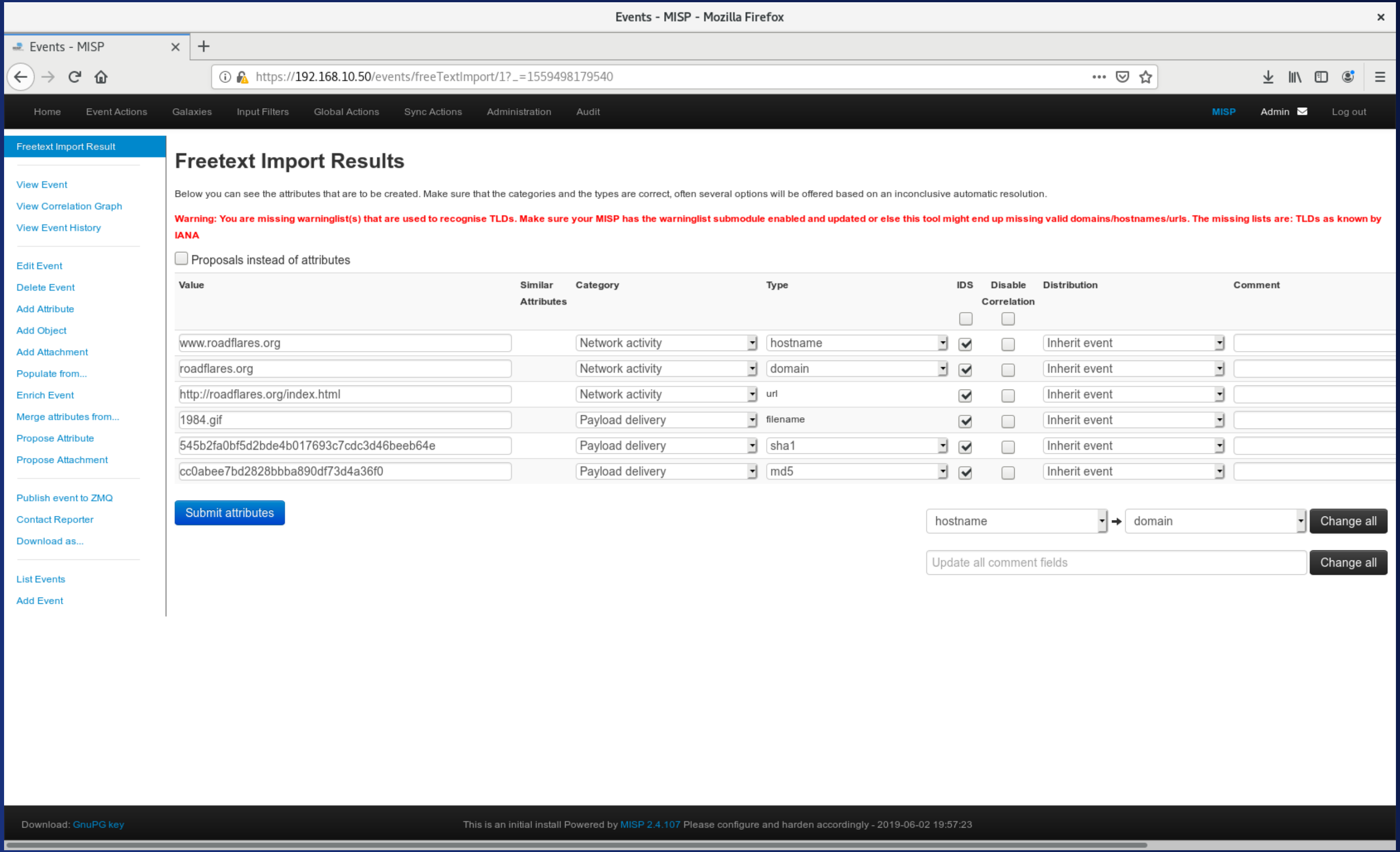
```
roadflares.org
http://roadflares.org/index.html
1984.gif
545b2fa0bf5d2bde4b017693c7cdc3d46beeb64e
cc0abee7bd2828bbba890df73d4a36f0
```

Submit

Cancel

Download: GnuPG key

This is an initial install Powered by MISP 2.4.107 Please configure and harden accordingly - 2019-06-02 19:56:19



Freetext Import Results

Below you can see the attributes that are to be created. Make sure that the categories and the types are correct, often several options will be offered based on an inconclusive automatic resolution.

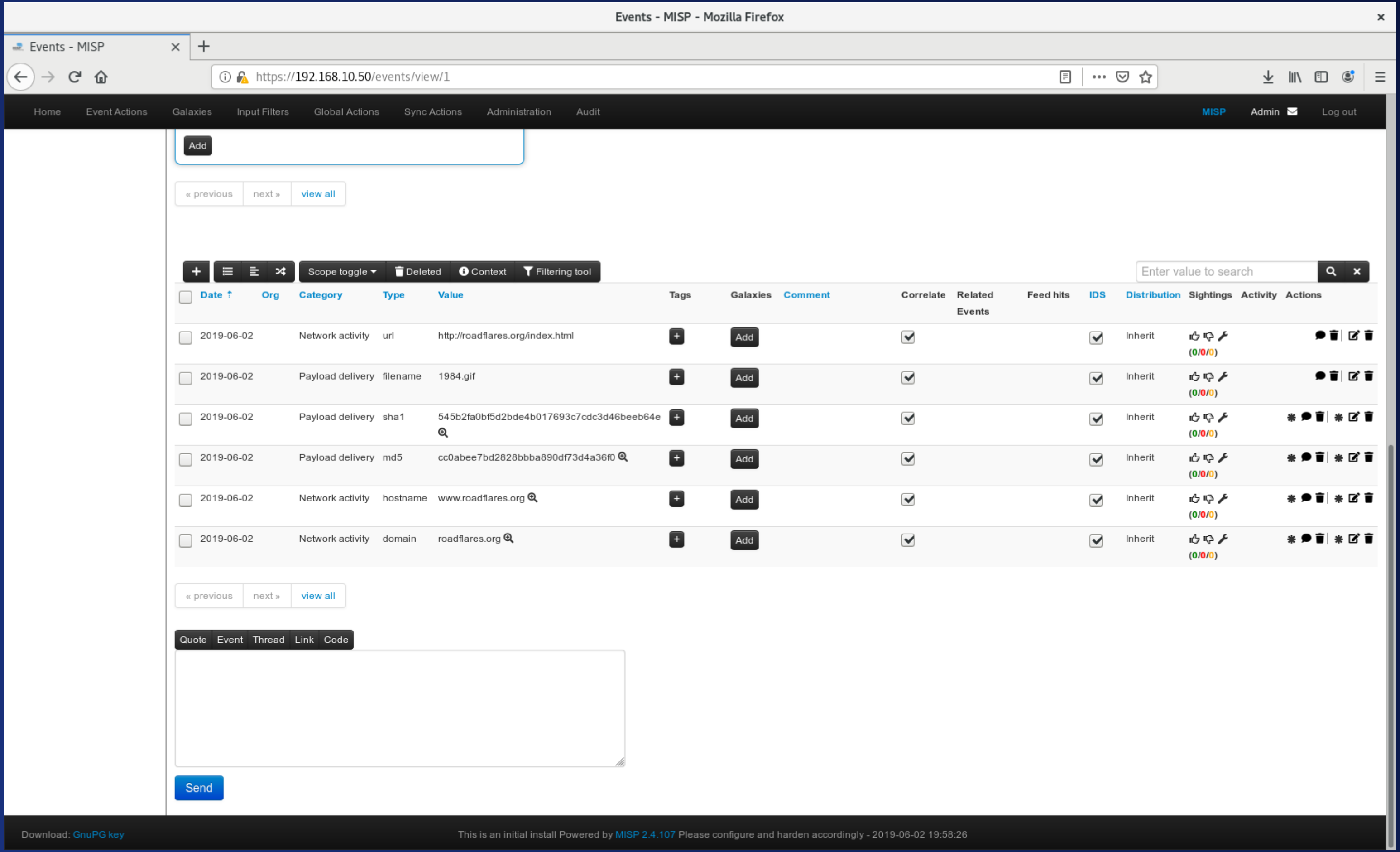
Warning: You are missing warninglist(s) that are used to recognise TLDs. Make sure your MISP has the warninglist submodule enabled and updated or else this tool might end up missing valid domains/hostnames/urls. The missing lists are: TLDs as known by IANA

☐ Proposals instead of attributes

Value	Similar Attributes	Category	Type	IDS ☐	Disable Correlation ☐	Distribution	Comment
www.roadflares.org		Network activity	hostname	☑	☐	Inherit event	
roadflares.org		Network activity	domain	☑	☐	Inherit event	
http://roadflares.org/index.html		Network activity	url	☑	☐	Inherit event	
1984.gif		Payload delivery	filename	☑	☐	Inherit event	
545b2fa0bf5d2bde4b017693c7cdc3d46beeb64e		Payload delivery	sha1	☑	☐	Inherit event	
cc0abee7bd2828bbba890df73d4a36f0		Payload delivery	md5	☑	☐	Inherit event	

Download: GnuPG key

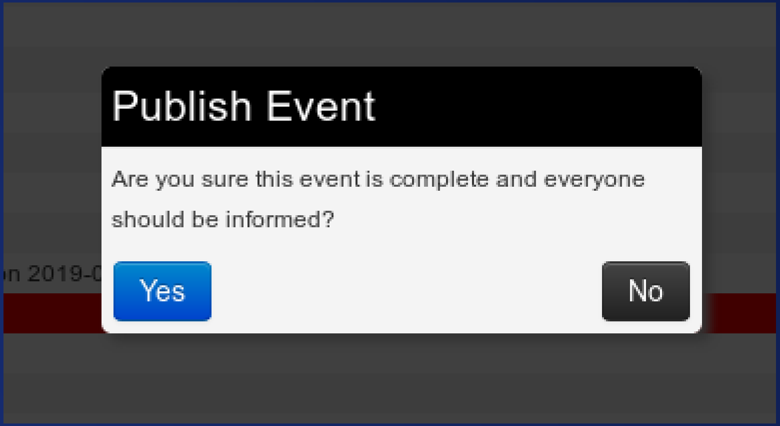
This is an initial install Powered by MISP 2.4.107 Please configure and harden accordingly - 2019-06-02 19:57:23



□	Date ↑	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Actions
□	2019-06-02		Network activity	url	http://roadflares.org/index.html	+	Add		☑			☑	Inherit	(0/0/0)		
□	2019-06-02		Payload delivery	filename	1984.gif	+	Add		☑			☑	Inherit	(0/0/0)		
□	2019-06-02		Payload delivery	sha1	545b2fa0bf5d2bde4b017693c7cdc3d46beeb64e	+	Add		☑			☑	Inherit	(0/0/0)		
□	2019-06-02		Payload delivery	md5	cc0abee7bd2828bbba890df73d4a36f0	+	Add		☑			☑	Inherit	(0/0/0)		
□	2019-06-02		Network activity	hostname	www.roadflares.org	+	Add		☑			☑	Inherit	(0/0/0)		
□	2019-06-02		Network activity	domain	roadflares.org	+	Add		☑			☑	Inherit	(0/0/0)		

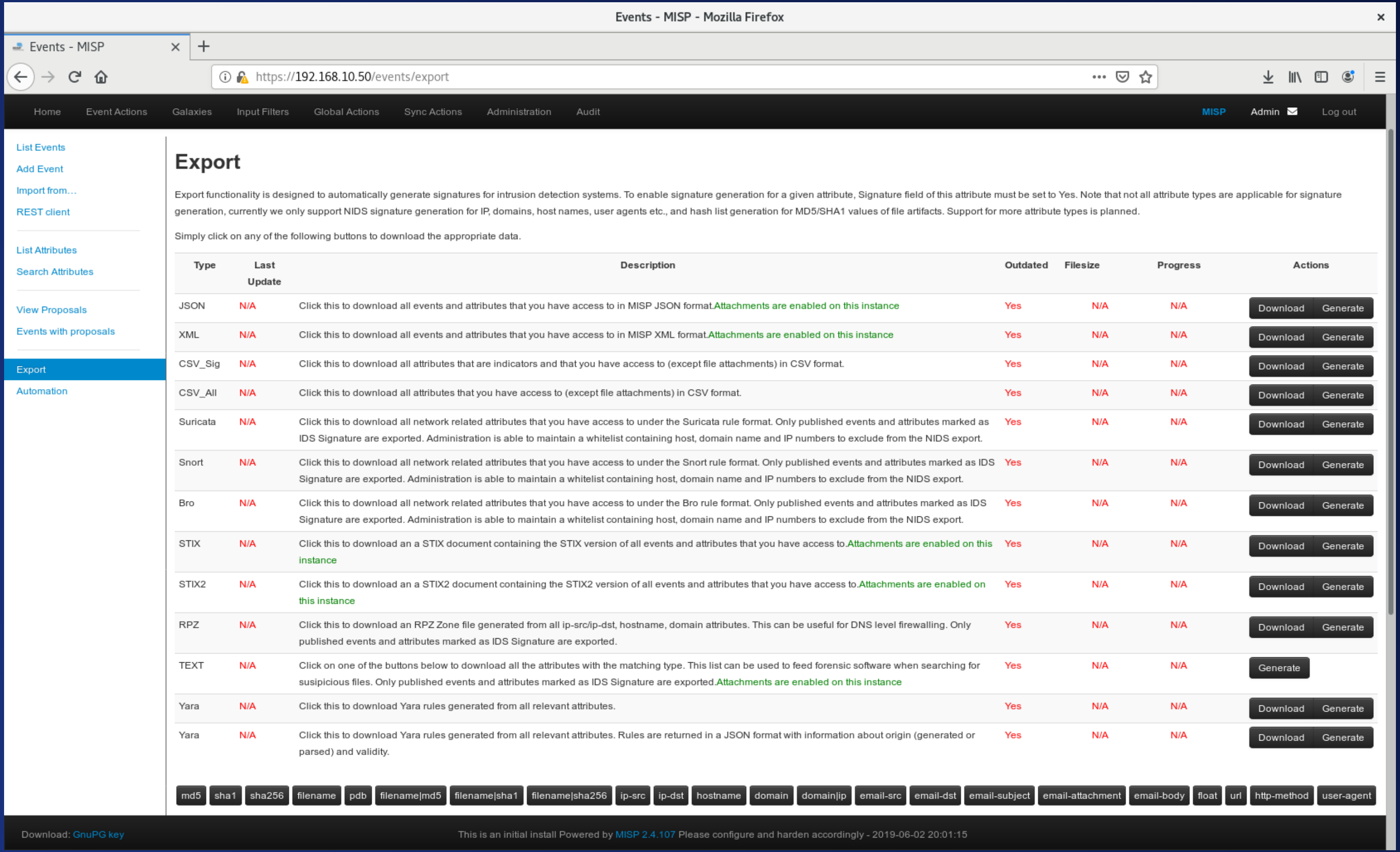
Download: GnuPG key

This is an initial install Powered by MISP 2.4.107 Please configure and harden accordingly - 2019-06-02 19:58:26



Publish Event

Are you sure this event is complete and everyone should be informed?



Export

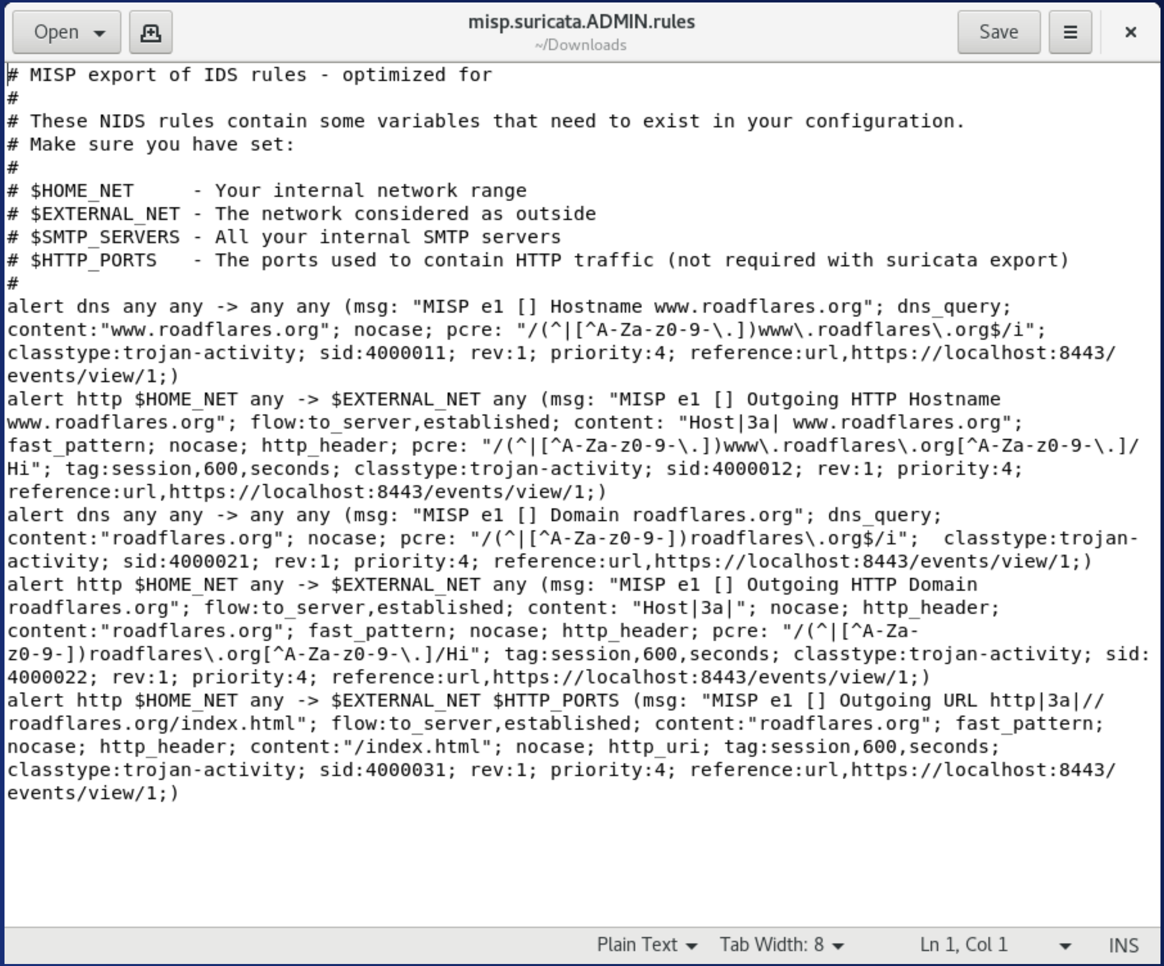
Export functionality is designed to automatically generate signatures for intrusion detection systems. To enable signature generation for a given attribute, Signature field of this attribute must be set to Yes. Note that not all attribute types are applicable for signature generation, currently we only support NIDS signature generation for IP, domains, host names, user agents etc., and hash list generation for MD5/SHA1 values of file artifacts. Support for more attribute types is planned.

Simply click on any of the following buttons to download the appropriate data.

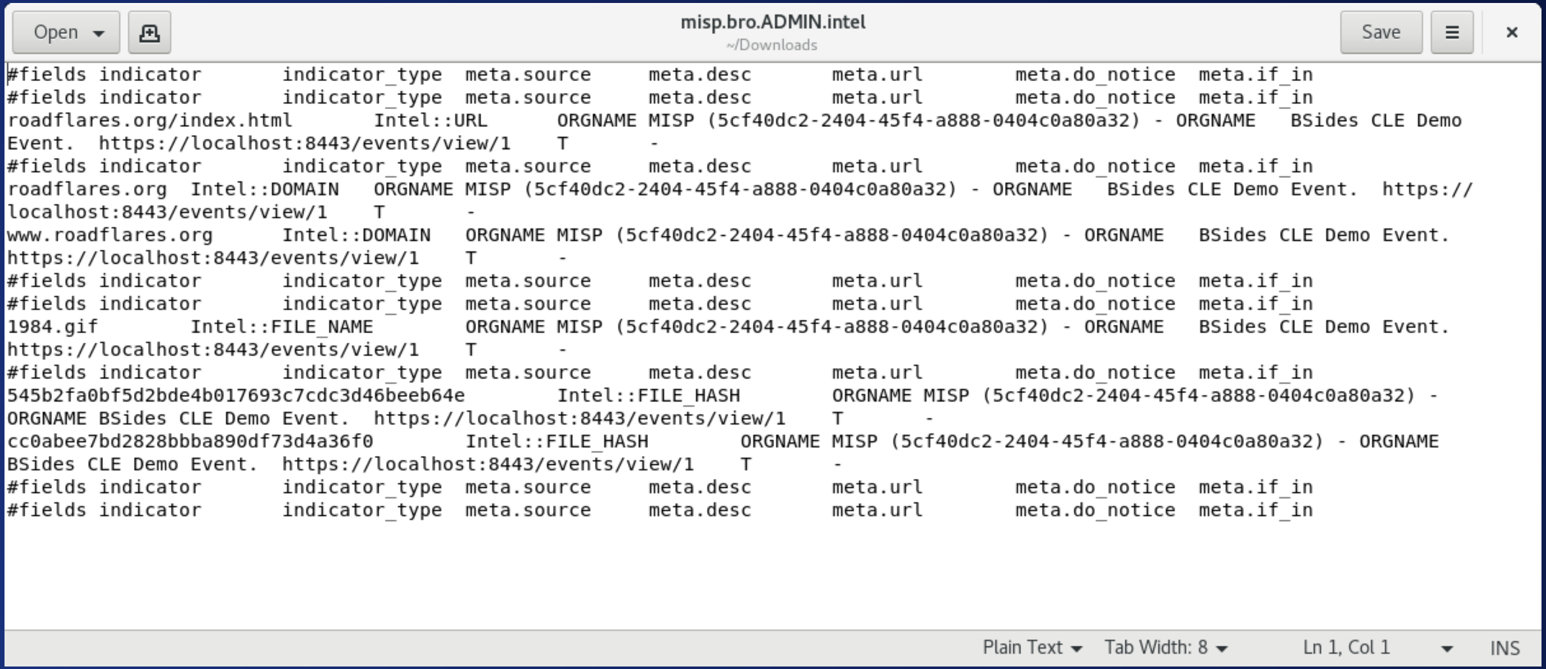
Type	Last Update	Description	Outdated	Filesize	Progress	Actions
JSON	N/A	Click this to download all events and attributes that you have access to in MISP JSON format.Attachments are enabled on this instance	Yes	N/A	N/A	Download Generate
XML	N/A	Click this to download all events and attributes that you have access to in MISP XML format.Attachments are enabled on this instance	Yes	N/A	N/A	Download Generate
CSV_Sig	N/A	Click this to download all attributes that are indicators and that you have access to (except file attachments) in CSV format.	Yes	N/A	N/A	Download Generate
CSV_All	N/A	Click this to download all attributes that you have access to (except file attachments) in CSV format.	Yes	N/A	N/A	Download Generate
Suricata	N/A	Click this to download all network related attributes that you have access to under the Suricata rule format. Only published events and attributes marked as IDS Signature are exported. Administration is able to maintain a whitelist containing host, domain name and IP numbers to exclude from the NIDS export.	Yes	N/A	N/A	Download Generate
Snort	N/A	Click this to download all network related attributes that you have access to under the Snort rule format. Only published events and attributes marked as IDS Signature are exported. Administration is able to maintain a whitelist containing host, domain name and IP numbers to exclude from the NIDS export.	Yes	N/A	N/A	Download Generate
Bro	N/A	Click this to download all network related attributes that you have access to under the Bro rule format. Only published events and attributes marked as IDS Signature are exported. Administration is able to maintain a whitelist containing host, domain name and IP numbers to exclude from the NIDS export.	Yes	N/A	N/A	Download Generate
STIX	N/A	Click this to download an a STIX document containing the STIX version of all events and attributes that you have access to.Attachments are enabled on this instance	Yes	N/A	N/A	Download Generate
STIX2	N/A	Click this to download an a STIX2 document containing the STIX2 version of all events and attributes that you have access to.Attachments are enabled on this instance	Yes	N/A	N/A	Download Generate
RPZ	N/A	Click this to download an RPZ Zone file generated from all ip-src/ip-dst, hostname, domain attributes. This can be useful for DNS level firewalling. Only published events and attributes marked as IDS Signature are exported.	Yes	N/A	N/A	Download Generate
TEXT	N/A	Click on one of the buttons below to download all the attributes with the matching type. This list can be used to feed forensic software when searching for susipicious files. Only published events and attributes marked as IDS Signature are exported.Attachments are enabled on this instance	Yes	N/A	N/A	Generate
Yara	N/A	Click this to download Yara rules generated from all relevant attributes.	Yes	N/A	N/A	Download Generate
Yara	N/A	Click this to download Yara rules generated from all relevant attributes. Rules are returned in a JSON format with information about origin (generated or parsed) and validity.	Yes	N/A	N/A	Download Generate

Download: GnuPG key

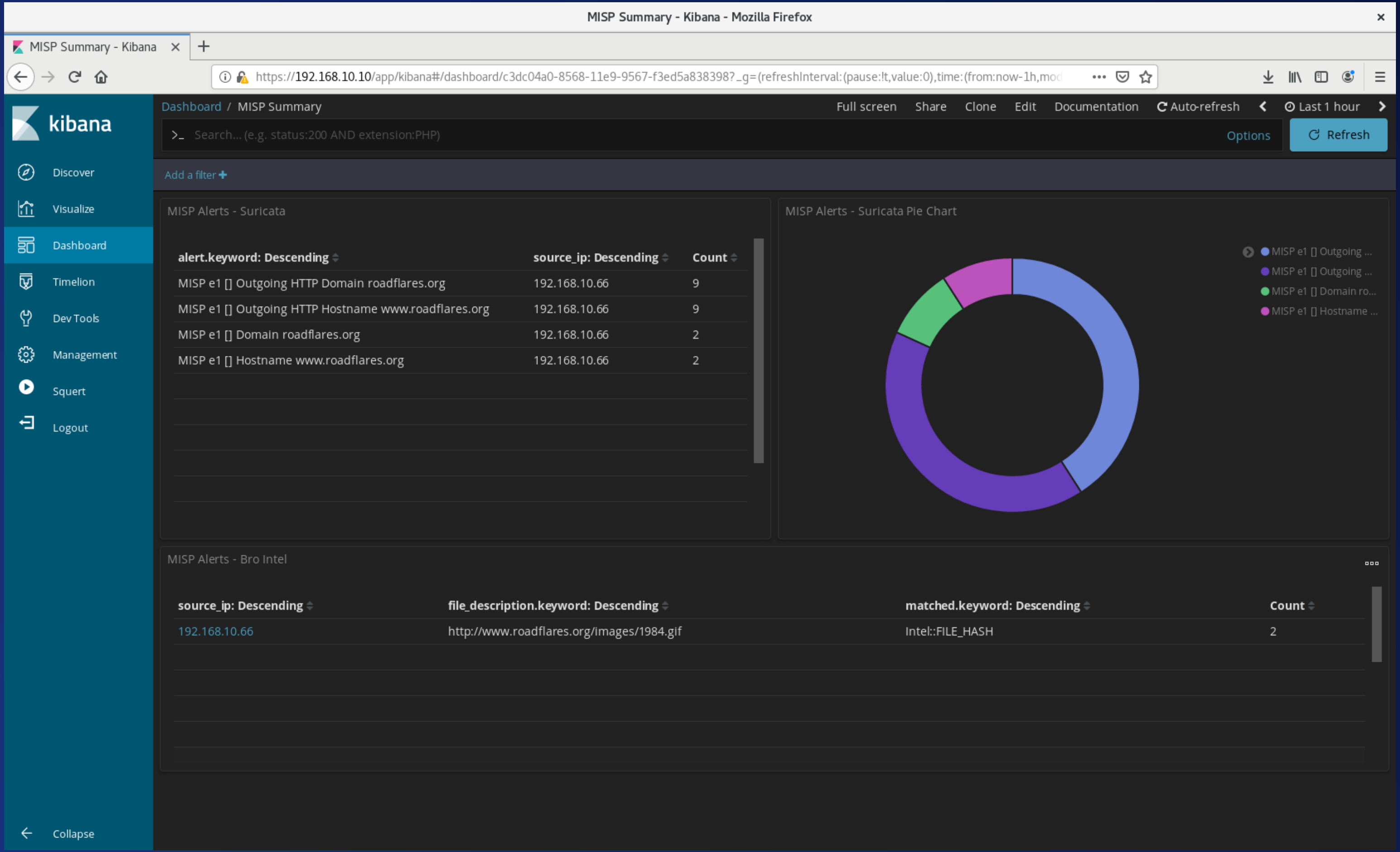
This is an initial install Powered by MISP 2.4.107 Please configure and harden accordingly - 2019-06-02 20:01:15



```
# MISP export of IDS rules - optimized for
#
# These NIDS rules contain some variables that need to exist in your configuration.
# Make sure you have set:
#
# $HOME_NET     - Your internal network range
# $EXTERNAL_NET - The network considered as outside
# $SMTP_SERVERS - All your internal SMTP servers
# $HTTP_PORTS   - The ports used to contain HTTP traffic (not required with suricata export)
#
alert dns any any -> any any (msg: "MISP e1 [] Hostname www.roadflares.org"; dns_query;
content:"www.roadflares.org"; nocase; pcre: "/(^|[^A-Za-z0-9-\.])www\.roadflares\.org$/i";
classtype:trojan-activity; sid:4000011; rev:1; priority:4; reference:url,https://localhost:8443/
events/view/1;)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg: "MISP e1 [] Outgoing HTTP Hostname
www.roadflares.org"; flow:to_server,established; content: "Host|3a| www.roadflares.org";
fast_pattern; nocase; http_header; pcre: "/(^|[^A-Za-z0-9-\.])www\.roadflares\.org[^A-Za-z0-9-\.]/
Hi"; tag:session,600,seconds; classtype:trojan-activity; sid:4000012; rev:1; priority:4;
reference:url,https://localhost:8443/events/view/1;)
alert dns any any -> any any (msg: "MISP e1 [] Domain roadflares.org"; dns_query;
content:"roadflares.org"; nocase; pcre: "/(^|[^A-Za-z0-9-])roadflares\.org$/i";  classtype:trojan-
activity; sid:4000021; rev:1; priority:4; reference:url,https://localhost:8443/events/view/1;)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg: "MISP e1 [] Outgoing HTTP Domain
roadflares.org"; flow:to_server,established; content: "Host|3a|"; nocase; http_header;
content:"roadflares.org"; fast_pattern; nocase; http_header; pcre: "/(^|[^A-Za-
z0-9-])roadflares\.org[^A-Za-z0-9-\.]/Hi"; tag:session,600,seconds; classtype:trojan-activity; sid:
4000022; rev:1; priority:4; reference:url,https://localhost:8443/events/view/1;)
alert http $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg: "MISP e1 [] Outgoing URL http|3a|//
roadflares.org/index.html"; flow:to_server,established; content:"roadflares.org"; fast_pattern;
nocase; http_header; content:"/index.html"; nocase; http_uri; tag:session,600,seconds;
classtype:trojan-activity; sid:4000031; rev:1; priority:4; reference:url,https://localhost:8443/
events/view/1;)
```



```
#fields indicator       indicator_type  meta.source     meta.desc       meta.url        meta.do_notice  meta.if_in
#fields indicator       indicator_type  meta.source     meta.desc       meta.url        meta.do_notice  meta.if_in
roadflares.org/index.html       Intel::URL      ORGNAME MISP (5cf40dc2-2404-45f4-a888-0404c0a80a32) - ORGNAME   BSides CLE Demo
Event.  https://localhost:8443/events/view/1    T       -
#fields indicator       indicator_type  meta.source     meta.desc       meta.url        meta.do_notice  meta.if_in
roadflares.org  Intel::DOMAIN   ORGNAME MISP (5cf40dc2-2404-45f4-a888-0404c0a80a32) - ORGNAME   BSides CLE Demo Event.  https://
localhost:8443/events/view/1    T       -
www.roadflares.org      Intel::DOMAIN   ORGNAME MISP (5cf40dc2-2404-45f4-a888-0404c0a80a32) - ORGNAME   BSides CLE Demo Event.
https://localhost:8443/events/view/1    T       -
#fields indicator       indicator_type  meta.source     meta.desc       meta.url        meta.do_notice  meta.if_in
#fields indicator       indicator_type  meta.source     meta.desc       meta.url        meta.do_notice  meta.if_in
1984.gif        Intel::FILE_NAME        ORGNAME MISP (5cf40dc2-2404-45f4-a888-0404c0a80a32) - ORGNAME   BSides CLE Demo Event.
https://localhost:8443/events/view/1    T       -
#fields indicator       indicator_type  meta.source     meta.desc       meta.url        meta.do_notice  meta.if_in
545b2fa0bf5d2bde4b017693c7cdc3d46beeb64e        Intel::FILE_HASH        ORGNAME MISP (5cf40dc2-2404-45f4-a888-0404c0a80a32) -
ORGNAME BSides CLE Demo Event.  https://localhost:8443/events/view/1    T       -
cc0abee7bd2828bbba890df73d4a36f0        Intel::FILE_HASH        ORGNAME MISP (5cf40dc2-2404-45f4-a888-0404c0a80a32) - ORGNAME
BSides CLE Demo Event.  https://localhost:8443/events/view/1    T       -
#fields indicator       indicator_type  meta.source     meta.desc       meta.url        meta.do_notice  meta.if_in
#fields indicator       indicator_type  meta.source     meta.desc       meta.url        meta.do_notice  meta.if_in
```

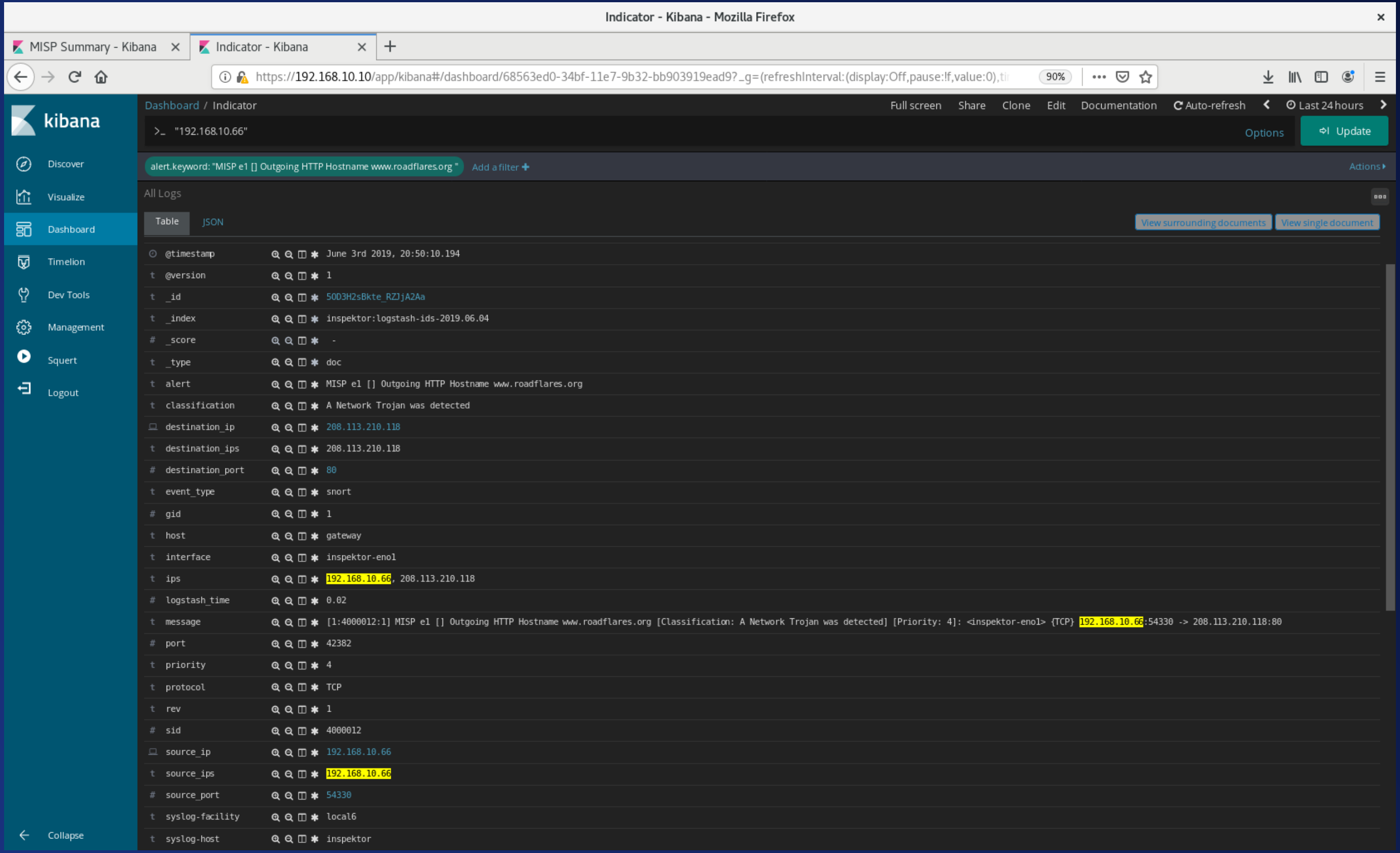


MISP Alerts - Suricata

alert.keyword: Descending	source_ip: Descending	Count
MISP e1 [] Outgoing HTTP Domain roadflares.org	192.168.10.66	9
MISP e1 [] Outgoing HTTP Hostname www.roadflares.org	192.168.10.66	9
MISP e1 [] Domain roadflares.org	192.168.10.66	2
MISP e1 [] Hostname www.roadflares.org	192.168.10.66	2

MISP Alerts - Bro Intel

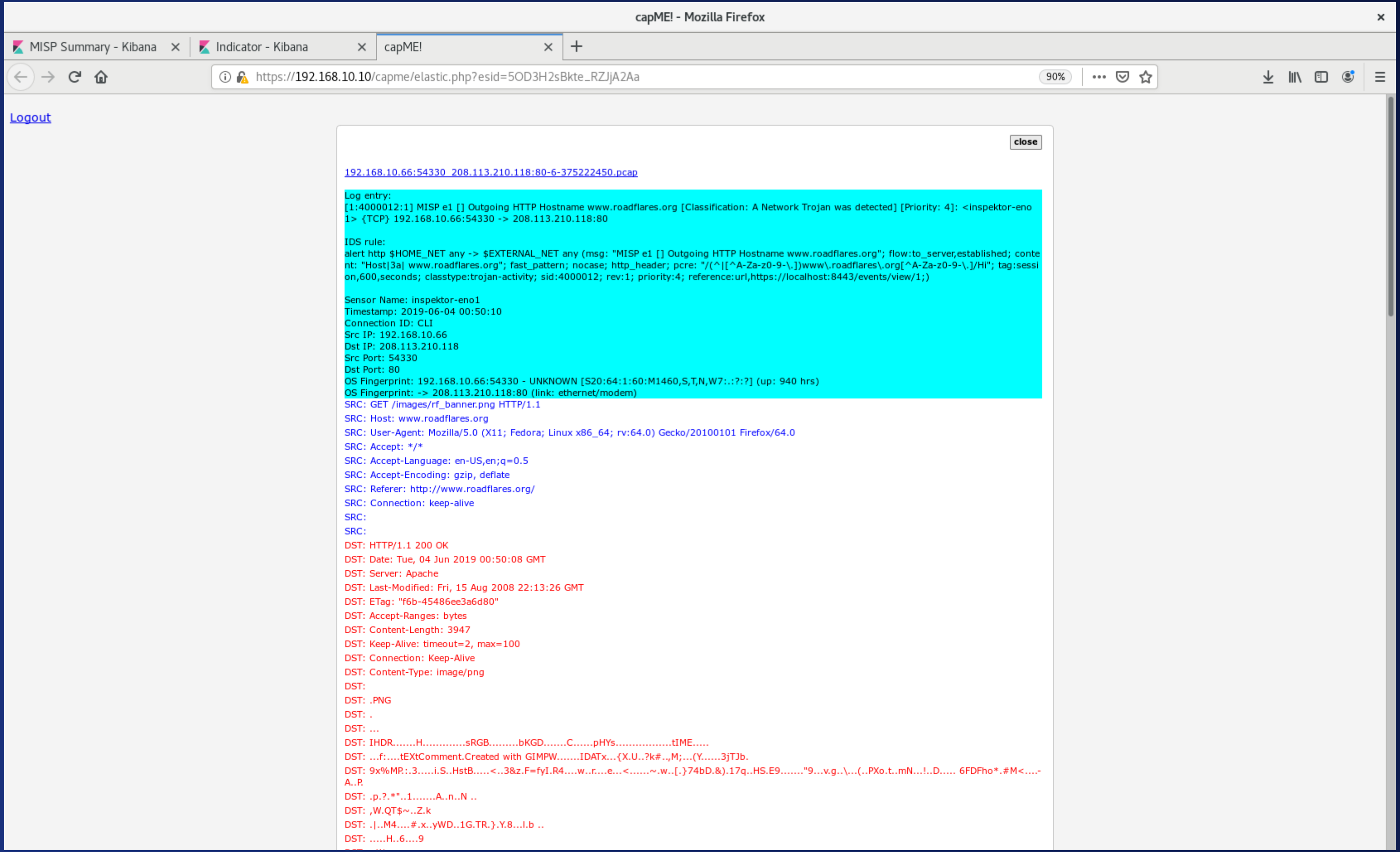
source_ip: Descending	file_description.keyword: Descending	matched.keyword: Descending	Count
192.168.10.66	http://www.roadflares.org/images/1984.gif	Intel::FILE_HASH	2



>_ "192.168.10.66"

alert.keyword: "MISP e1 [] Outgoing HTTP Hostname www.roadflares.org "

	@timestamp	June 3rd 2019, 20:50:10.194
t	@version	1
t	_id	5OD3H2sBkte_RZJjA2Aa
t	_index	inspektor:logstash-ids-2019.06.04
#	_score	-
t	_type	doc
t	alert	MISP e1 [] Outgoing HTTP Hostname www.roadflares.org
t	classification	A Network Trojan was detected
	destination_ip	208.113.210.118
t	destination_ips	208.113.210.118
#	destination_port	80
t	event_type	snort
#	gid	1
t	host	gateway
t	interface	inspektor-eno1
t	ips	192.168.10.66, 208.113.210.118
#	logstash_time	0.02
t	message	[1:4000012:1] MISP e1 [] Outgoing HTTP Hostname www.roadflares.org [Classification: A Network Trojan was detected] [Priority: 4]: <inspektor-eno1> {TCP} 192.168.10.66:54330 -> 208.113.210.118:80
#	port	42382
t	priority	4
t	protocol	TCP
t	rev	1
#	sid	4000012
	source_ip	192.168.10.66
t	source_ips	192.168.10.66
#	source_port	54330
t	syslog-facility	local6
t	syslog-host	inspektor

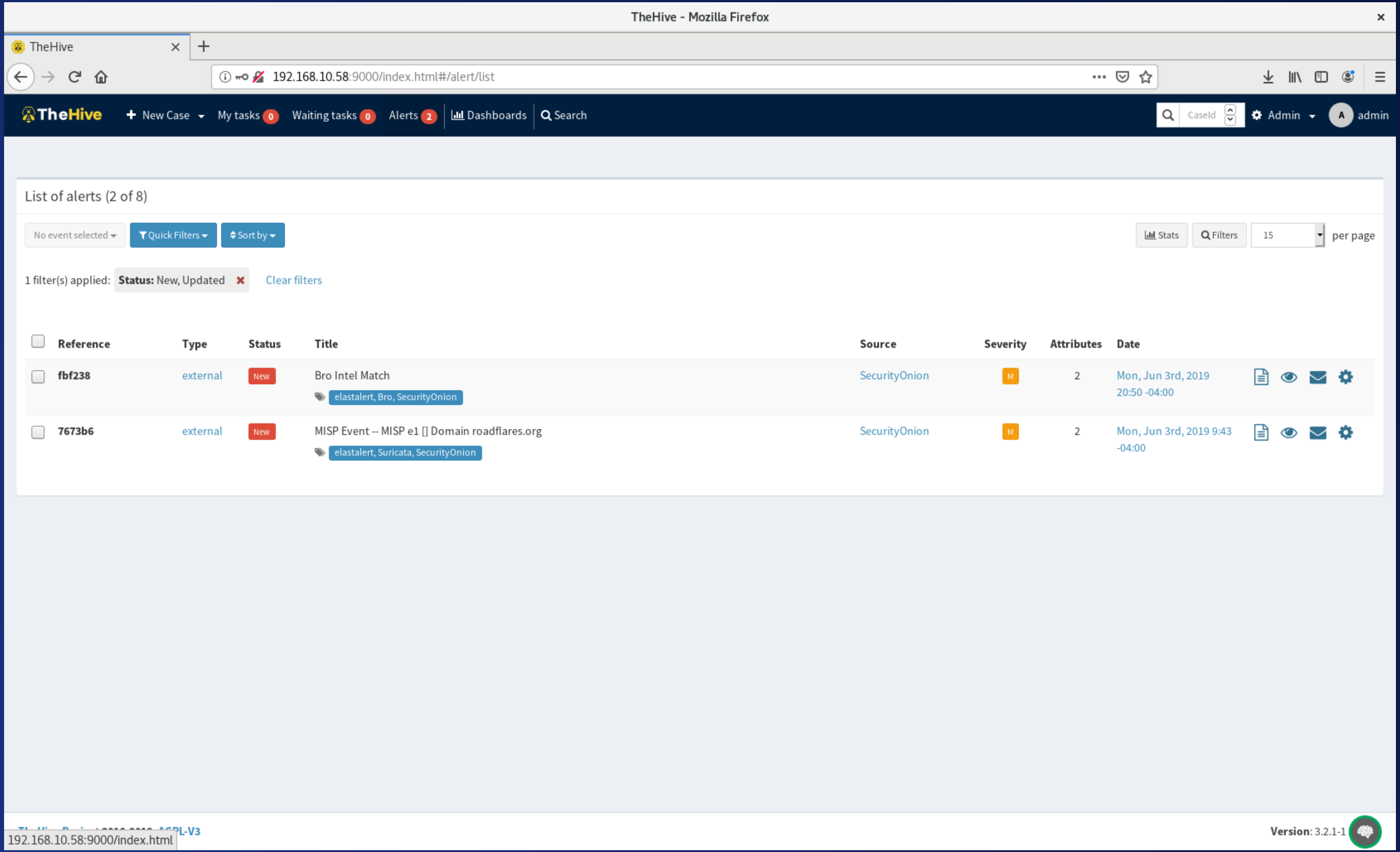


192.168.10.66:54330_208.113.210.118:80-6-375222450.pcap

```
Log entry:
[1:4000012:1] MISP e1 [] Outgoing HTTP Hostname www.roadflares.org [Classification: A Network Trojan was detected] [Priority: 4]: <inspektor-eno
1> {TCP} 192.168.10.66:54330 -> 208.113.210.118:80

IDS rule:
alert http $HOME_NET any -> $EXTERNAL_NET any (msg: "MISP e1 [] Outgoing HTTP Hostname www.roadflares.org"; flow:to_server,established; conte
nt: "Host|3a| www.roadflares.org"; fast_pattern; nocase; http_header; pcre: "/(^|[^A-Za-z0-9-\.])www\.roadflares\.org[^A-Za-z0-9-\.]/Hi"; tag:sessi
on,600,seconds; classtype:trojan-activity; sid:4000012; rev:1; priority:4; reference:url,https://localhost:8443/events/view/1;)

Sensor Name: inspektor-eno1
Timestamp: 2019-06-04 00:50:10
Connection ID: CLI
Src IP: 192.168.10.66
Dst IP: 208.113.210.118
Src Port: 54330
Dst Port: 80
OS Fingerprint: 192.168.10.66:54330 - UNKNOWN [S20:64:1:60:M1460,S,T,N,W7:.:?:?] (up: 940 hrs)
OS Fingerprint: -> 208.113.210.118:80 (link: ethernet/modem)
SRC: GET /images/rf_banner.png HTTP/1.1
SRC: Host: www.roadflares.org
SRC: User-Agent: Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:64.0) Gecko/20100101 Firefox/64.0
SRC: Accept: */*
SRC: Accept-Language: en-US,en;q=0.5
SRC: Accept-Encoding: gzip, deflate
SRC: Referer: http://www.roadflares.org/
SRC: Connection: keep-alive
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Date: Tue, 04 Jun 2019 00:50:08 GMT
DST: Server: Apache
DST: Last-Modified: Fri, 15 Aug 2008 22:13:26 GMT
DST: ETag: "f6b-45486ee3a6d80"
DST: Accept-Ranges: bytes
DST: Content-Length: 3947
DST: Keep-Alive: timeout=2, max=100
DST: Connection: Keep-Alive
DST: Content-Type: image/png
DST:
DST: .PNG
DST: .
DST: ...
DST: IHDR.......H.............sRGB.........bKGD.......C......pHYs.................tIME.....
DST: ...f:....tEXtComment.Created with GIMPW.......IDATx...{X.U..?k#..,M;...(Y......3jTJb.
DST: 9x%MP.:.3.....i.S..HstB.....<..3&z.F=fyI.R4....w..r....e...<......~.w..[.}74bD.&).17q..HS.E9......."9...v.g..\...(..PXo.t..mN...!..D..... 6FDFho*.#M<....-
A..P.
DST: .p.?.*"..1.......A..n..N ..
DST: ,W.QT$~..Z.k
DST: .|..M4....#.x..yWD..1G.TR.}.Y.8...l.b ..
DST: .....H..6....9
```

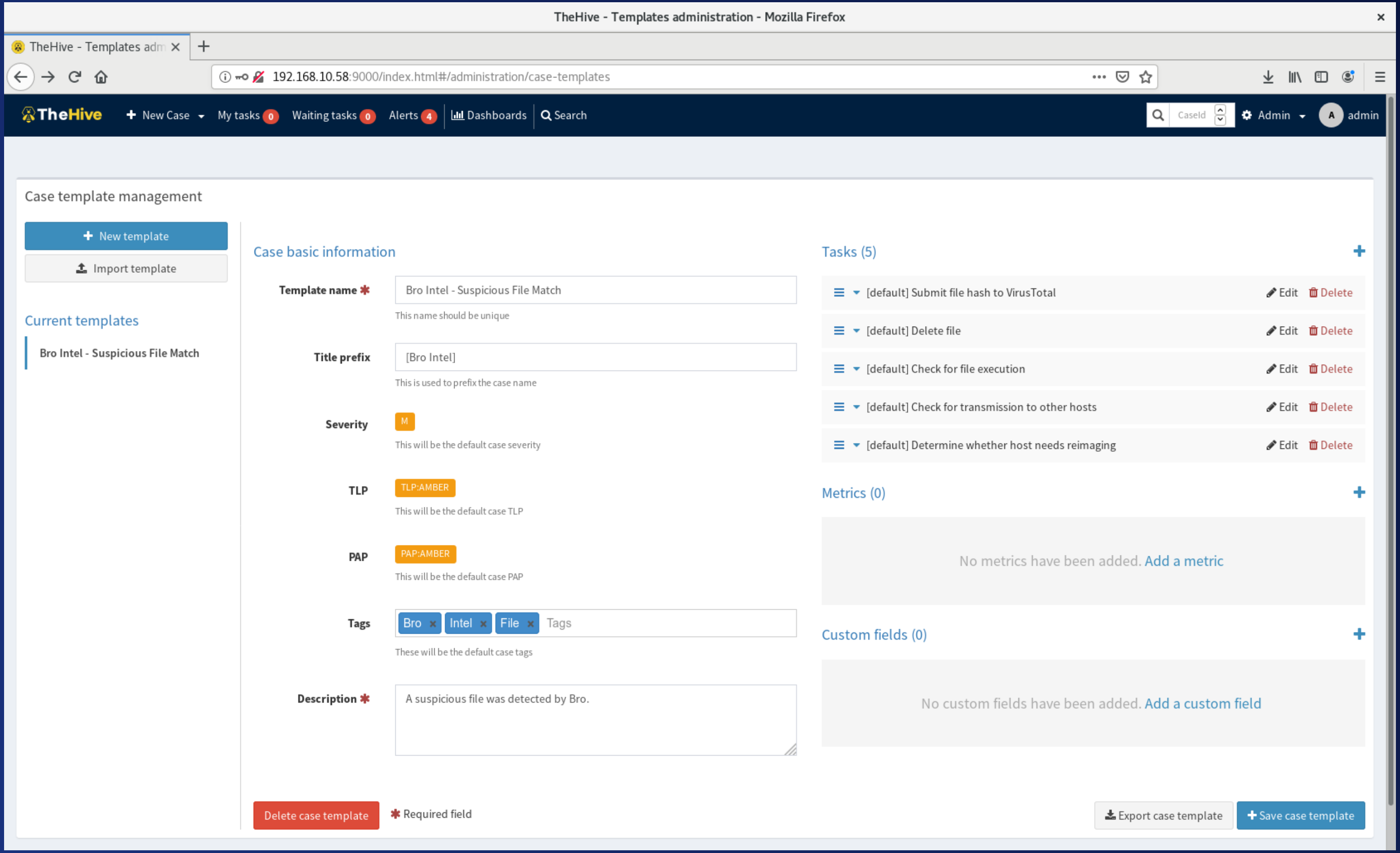


List of alerts (2 of 8)

1 filter(s) applied: **Status:** New, Updated

☐	Reference	Type	Status	Title	Source	Severity	Attributes	Date
☐	**fbf238**	external	New	Bro Intel Match elastalert, Bro, SecurityOnion	SecurityOnion	M	2	Mon, Jun 3rd, 2019 20:50 -04:00
☐	**7673b6**	external	New	MISP Event -- MISP e1 [] Domain roadflares.org elastalert, Suricata, SecurityOnion	SecurityOnion	M	2	Mon, Jun 3rd, 2019 9:43 -04:00

Version: 3.2.1-1



Case template management

Current templates

Bro Intel - Suspicious File Match

Case basic information

Template name * Bro Intel - Suspicious File Match
This name should be unique

Title prefix [Bro Intel]
This is used to prefix the case name

Severity M
This will be the default case severity

TLP TLP:AMBER
This will be the default case TLP

PAP PAP:AMBER
This will be the default case PAP

Tags Bro × Intel × File × Tags
These will be the default case tags

Description * A suspicious file was detected by Bro.

* Required field

Tasks (5)

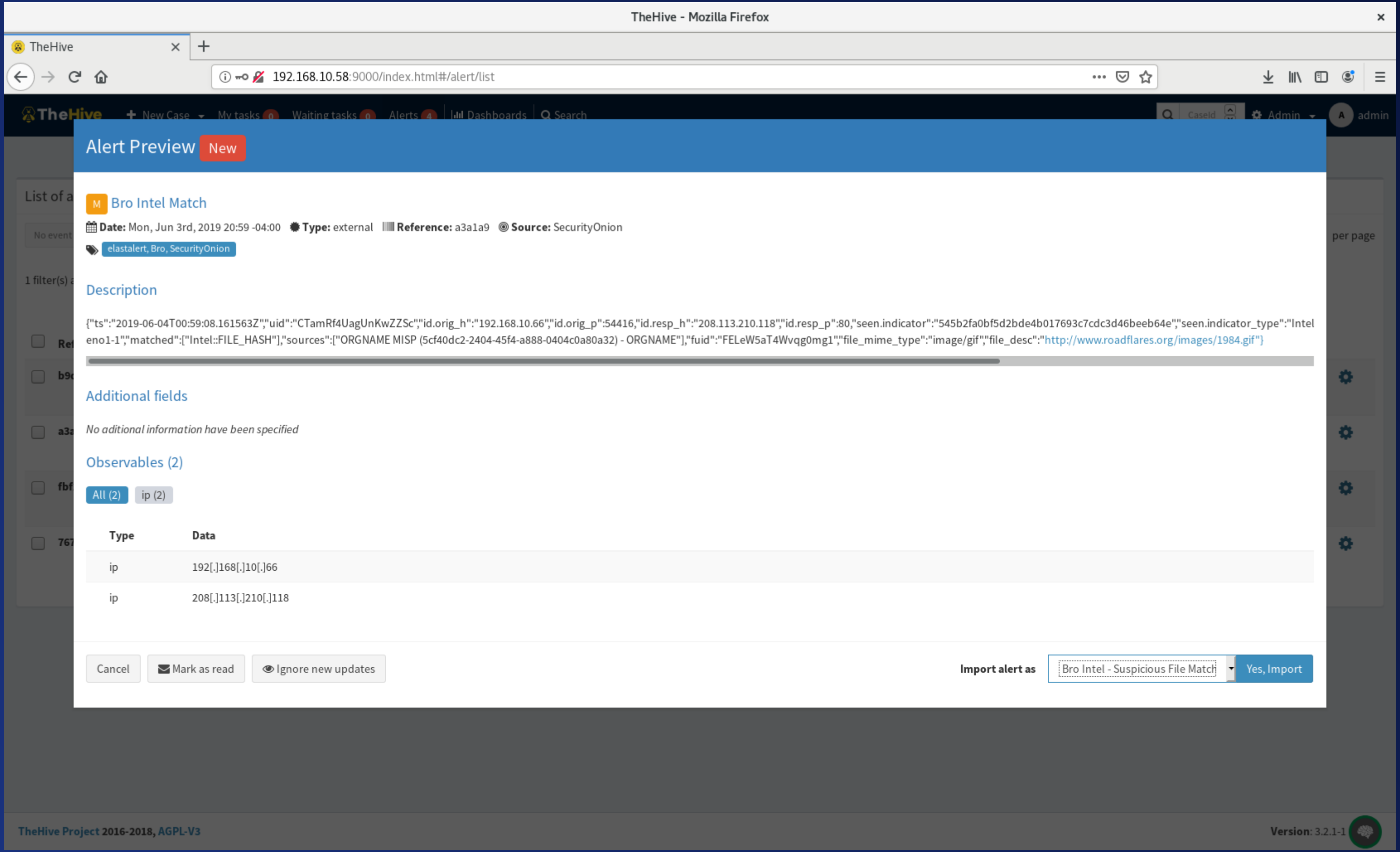
- [default] Submit file hash to VirusTotal
- [default] Delete file
- [default] Check for file execution
- [default] Check for transmission to other hosts
- [default] Determine whether host needs reimaging

Metrics (0)

No metrics have been added. Add a metric

Custom fields (0)

No custom fields have been added. Add a custom field



Alert Preview New

M Bro Intel Match

Date: Mon, Jun 3rd, 2019 20:59 -04:00 Type: external Reference: a3a1a9 Source: SecurityOnion

elastalert, Bro, SecurityOnion

Description

```
{"ts":"2019-06-04T00:59:08.161563Z","uid":"CTamRf4UagUnKwZZSc","id.orig_h":"192.168.10.66","id.orig_p":54416,"id.resp_h":"208.113.210.118","id.resp_p":80,"seen.indicator":"545b2fa0bf5d2bde4b017693c7cdc3d46beeb64e","seen.indicator_type":"Intel
eno1-1","matched":["Intel::FILE_HASH"],"sources":["ORGNAME MISP (5cf40dc2-2404-45f4-a888-0404c0a80a32) - ORGNAME"],"fuid":"FELeW5aT4Wvqg0mg1","file_mime_type":"image/gif","file_desc":"http://www.roadflares.org/images/1984.gif"}
```

Additional fields

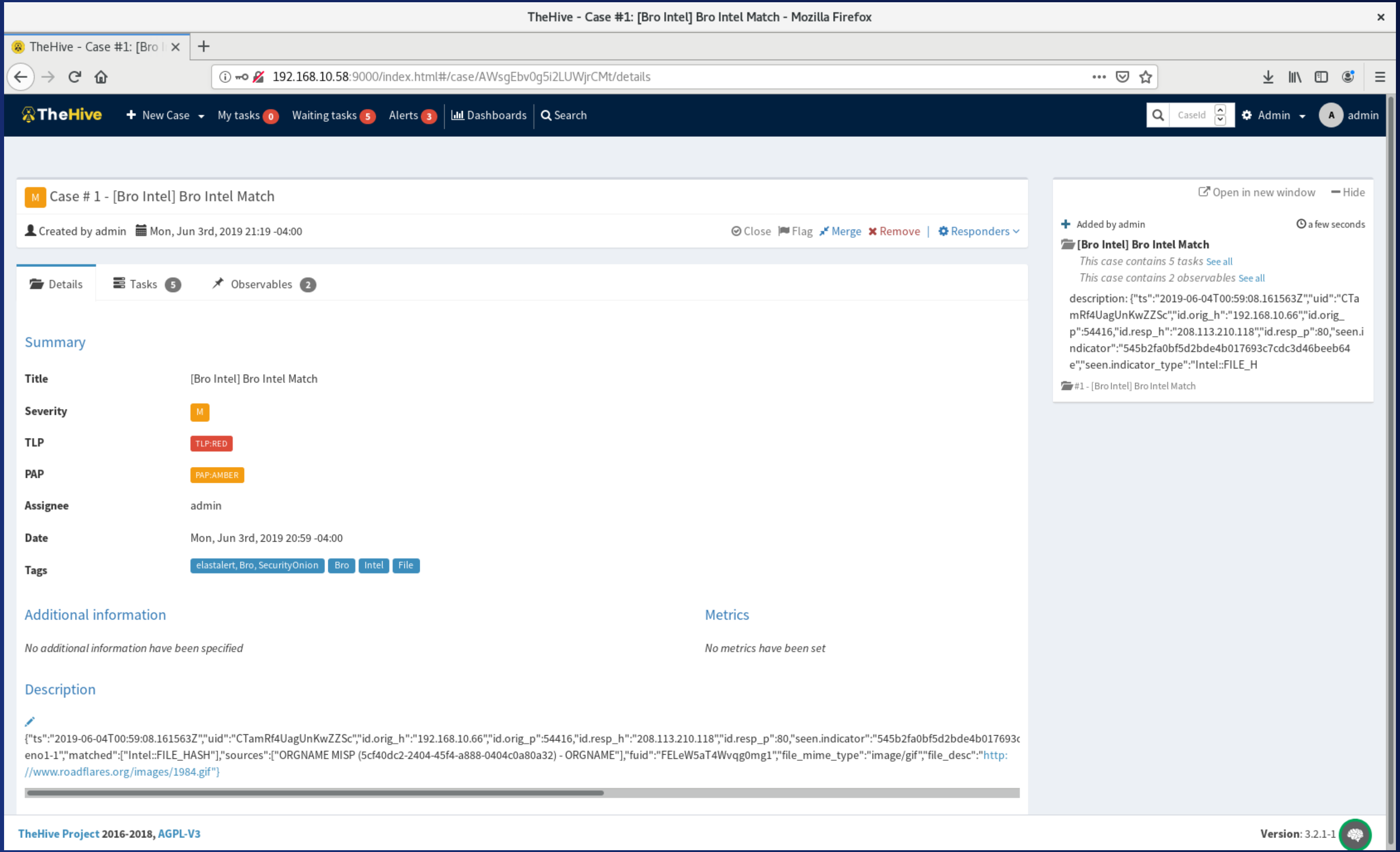
No aditional information have been specified

Observables (2)

All (2) ip (2)

Type	Data
ip	192[.]168[.]10[.]66
ip	208[.]113[.]210[.]118

Import alert as: Bro Intel - Suspicious File Match



Case # 1 - [Bro Intel] Bro Intel Match

Created by admin Mon, Jun 3rd, 2019 21:19 -04:00

Summary

Title	[Bro Intel] Bro Intel Match
Severity	M
TLP	TLP:RED
PAP	PAP:AMBER
Assignee	admin
Date	Mon, Jun 3rd, 2019 20:59 -04:00
Tags	elastalert, Bro, SecurityOnion Bro Intel File

Additional information

No additional information have been specified

Metrics

No metrics have been set

Description

```
{"ts":"2019-06-04T00:59:08.161563Z","uid":"CTamRf4UagUnKwZZSc","id.orig_h":"192.168.10.66","id.orig_p":54416,"id.resp_h":"208.113.210.118","id.resp_p":80,"seen.indicator":"545b2fa0bf5d2bde4b017693c
eno1-1","matched":["Intel::FILE_HASH"],"sources":["ORGNAME MISP (5cf40dc2-2404-45f4-a888-0404c0a80a32) - ORGNAME"],"fuid":"FELeW5aT4Wvqg0mg1","file_mime_type":"image/gif","file_desc":"http:
//www.roadflares.org/images/1984.gif"}
```

Added by admin a few seconds

[Bro Intel] Bro Intel Match

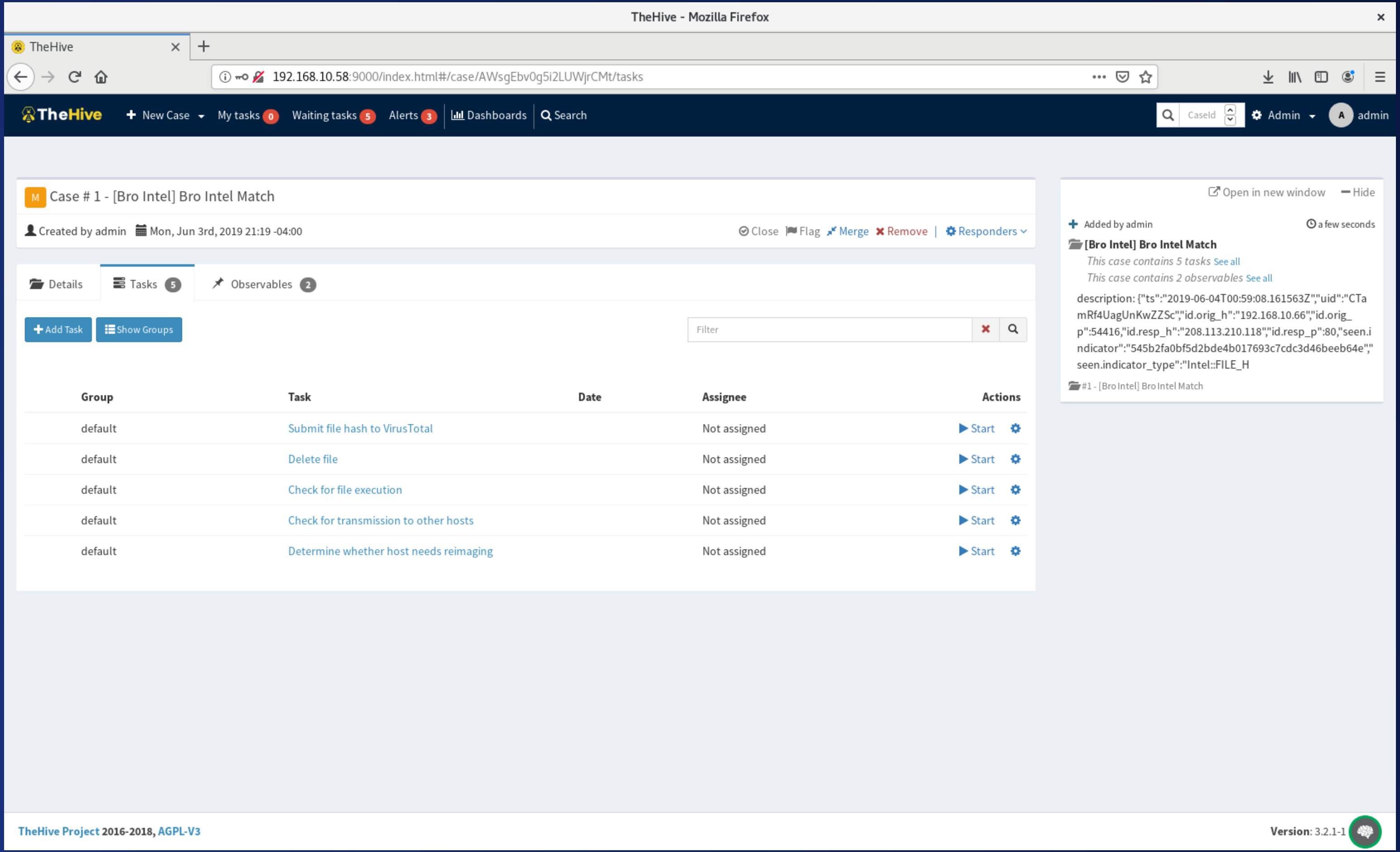
This case contains 5 tasks See all

This case contains 2 observables See all

```
description: {"ts":"2019-06-04T00:59:08.161563Z","uid":"CTa
mRf4UagUnKwZZSc","id.orig_h":"192.168.10.66","id.orig_
p":54416,"id.resp_h":"208.113.210.118","id.resp_p":80,"seen.i
ndicator":"545b2fa0bf5d2bde4b017693c7cdc3d46beeb64
e","seen.indicator_type":"Intel::FILE_H
```

#1 - [Bro Intel] Bro Intel Match

Version: 3.2.1-1



Case # 1 - [Bro Intel] Bro Intel Match

Created by admin Mon, Jun 3rd, 2019 21:19 -04:00

Group	Task	Date	Assignee	Actions
default	Submit file hash to VirusTotal		Not assigned	▶ Start
default	Delete file		Not assigned	▶ Start
default	Check for file execution		Not assigned	▶ Start
default	Check for transmission to other hosts		Not assigned	▶ Start
default	Determine whether host needs reimaging		Not assigned	▶ Start

Added by admin a few seconds

[Bro Intel] Bro Intel Match

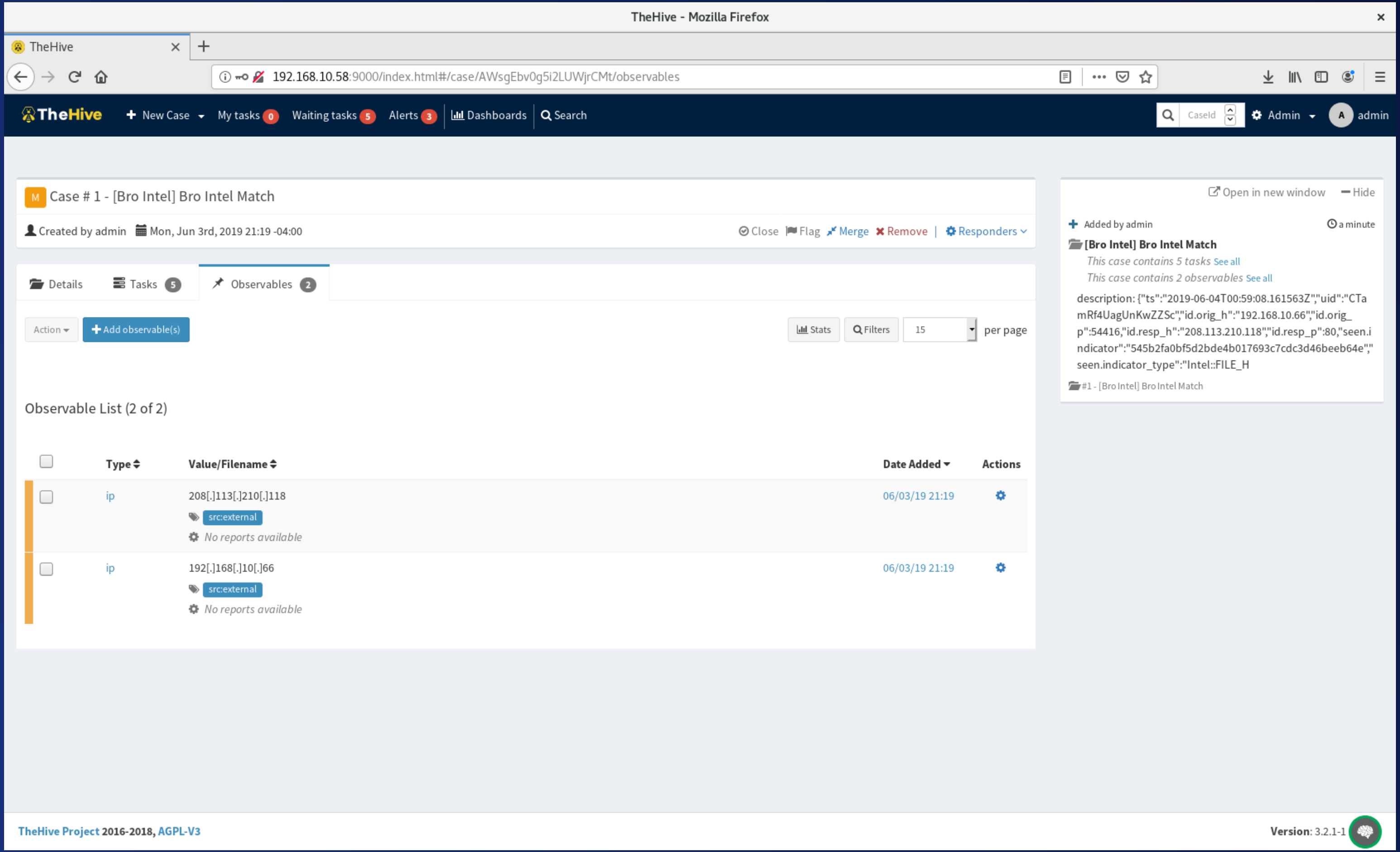
This case contains 5 tasks See all

This case contains 2 observables See all

description: {"ts":"2019-06-04T00:59:08.161563Z","uid":"CTamRf4UagUnKwZZSc","id.orig_h":"192.168.10.66","id.orig_p":54416,"id.resp_h":"208.113.210.118","id.resp_p":80,"seen.indicator":"545b2fa0bf5d2bde4b017693c7cdc3d46beeb64e","seen.indicator_type":"Intel::FILE_H

#1 - [Bro Intel] Bro Intel Match

TheHive Project 2016-2018, AGPL-V3



Case # 1 - [Bro Intel] Bro Intel Match

Created by admin   Mon, Jun 3rd, 2019 21:19 -04:00

Observable List (2 of 2)

	Type	Value/Filename	Date Added	Actions
□	ip	208[.]113[.]210[.]118 src:external *No reports available*	06/03/19 21:19	
□	ip	192[.]168[.]10[.]66 src:external *No reports available*	06/03/19 21:19	

Added by admin   a minute

[Bro Intel] Bro Intel Match

This case contains 5 tasks See all

This case contains 2 observables See all

description: {"ts":"2019-06-04T00:59:08.161563Z","uid":"CTamRf4UagUnKwZZSc","id.orig_h":"192.168.10.66","id.orig_p":54416,"id.resp_h":"208.113.210.118","id.resp_p":80,"seen.indicator":"545b2fa0bf5d2bde4b017693c7cdc3d46beeb64e","seen.indicator_type":"Intel::FILE_H

#1 - [Bro Intel] Bro Intel Match

TheHive Project 2016-2018, AGPL-V3

Version: 3.2.1-1

How Can I Play With This?

- TheHive VM: https://github.com/TheHive-Project/TheHiveDocs/blob/master/training-material.md
- MISP VM: https://www.circl.lu/services/misp-training-materials/
- MISP / TheHive / Cortex VM: https://www.circl.lu/misp-training-images/
- Security Onion is freely downloadable: https://securityonion.net/

Questions?

For More Information

@InfosecGoon

infosecgoon@roadflares.org

https://github.com/InfosecGoon/stinger/