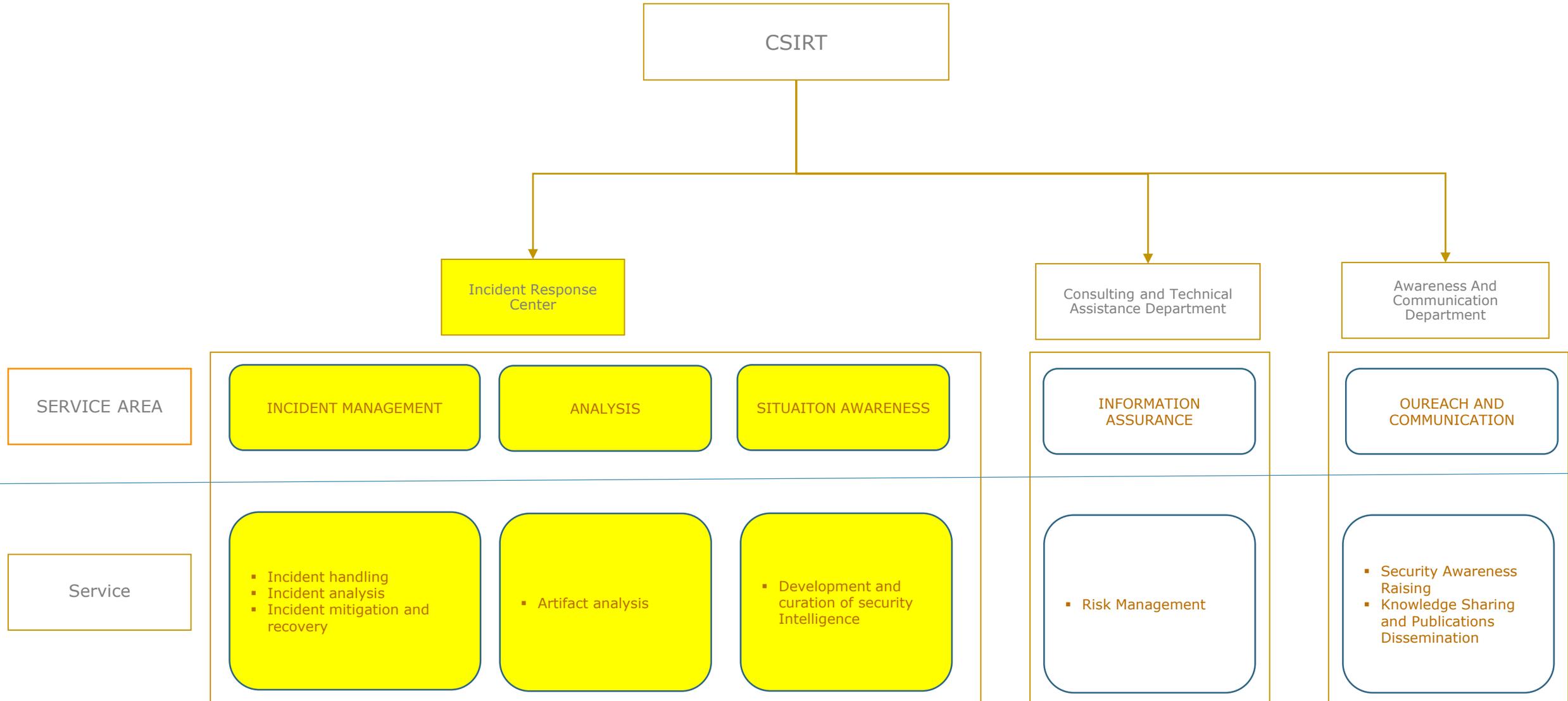




How to Build a CIRT based on open Source Tools

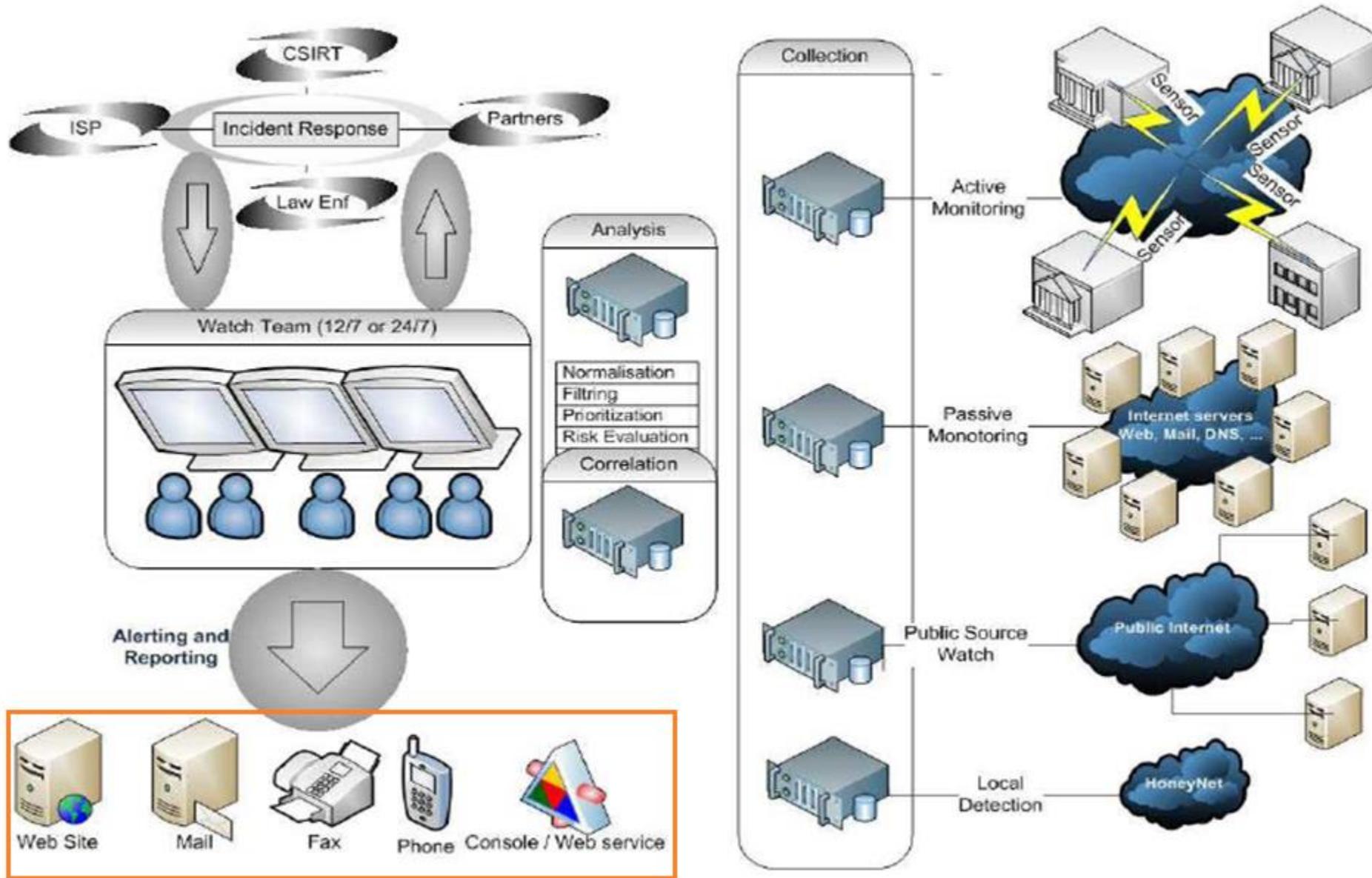


The Basic Services Offered by a CSIRT/SOC





Incident Response Center





Alerting and Reporting

Request Tracker for Incident Response (RTIR)

- <https://www.bestpractical.com/rtir>
- Purposely-built for CSIRT
- Developed in cooperation with many security teams to ensure it meets the needs of incident response.



The screenshot shows the RTIR dashboard with the following sections:

- RT at a glance**: Overview of ticket management.
- 10 highest priority tickets I own**:

#	Subject	Priority	Queue	Status
1	Office has run out of coffee!	0	Office	(pending 1 other ticket)
2	Order more coffee	0	Office	(pending 2 other tickets)
- 10 newest unowned tickets**:

#	Subject	Queue	Status	Created	Take
3	Obtain Series-C funding	General	new	52 sec ago	Take
- Bookmarked Tickets**:

#	Subject	Priority	Queue	Status
4	Evaluate responses to RFP for coffee roasts	0	General	new
- Quick search**:

Queue	new	open	stalled
General	2	-	-
Office	1	1	-
- Dashboards**: RT System's dashboards, SLA Performance (daily at 6:00 AM).
- Refresh**: Don't refresh this page.
- Quick ticket creation**: Form for creating new tickets with fields for Subject, Queue, Owner, Requester, and Content.

The screenshot shows the details for Incident #14485:

- Ticket metadata**:
 - Status: open
 - Owner: root
 - Subject: [redacted]
 - Priority: 0
 - Time Visible: 0 min
 - Resolution: (no value)
 - SLA: 1d
 - Function: (no value)
 - Classification: (no value)
 - Queue Name: [redacted]
 - Requester Name: Unknown
 - Target IP: [redacted]
 - Target Name: [redacted]
 - Office description: [redacted]
 - Rule Description: [redacted]
- Incident Reports**: (No active Incident Reports) (No inactive Incident Reports) [Create Link]
- Investigations**: (No active Investigations) (No inactive Investigations) [Launch Link]
- Blocks**: (No active Blocks) (No inactive Blocks) [Create Link]
- Articles**: [Create Link]
- Dates**:
 - Created: Tue Jul 24 15:35:05 2012
 - Start: Tue Jul 24 15:35:05 2012
 - Due: Wed Jul 25 15:35:05 2012
 - Updated: Wed Jul 25 00:01:54 2012 by root
- History**:
 - Tue Jul 24 15:35:05 2012: Ticket created [Reply, Comment, Forward]



Alerting and Reporting



Open Technology Real Services (OTRS)

- <http://www.otrs.com/software>
- The Flexible Open Source Service Management Software

The dashboard provides a comprehensive overview of the service management system. It includes sections for 'Escalated Tickets', 'New Tickets', and 'Open Tickets | Need to be answered'. A '7 Day Stats' chart shows ticket trends. Navigation tabs at the top include Dashboard, Customers, Tickets, FAQ, and Statistics. A red banner at the top indicates 'Scheduler is not running. Please contact your administrator!'.

Dashboard

The ticket details page shows the specific issue: 'Ticket#201311102000087 - Internet connection problem'. It includes a list of articles, the ticket's history, and a detailed description of the problem. The ticket is currently in an 'open' state with a priority of '4 high'. The customer information is listed as '2nd Level: Clients USA Eastern Time-Webwork'. The ticket was created on 11/10/2013 at 13:25 by Susi Smith.

Tickets



Alerting and Reporting

osTicket

- <http://osticket.com>



Dashboard Settings **Manage** Emails Staff
Help Topics Ticket Filters SLA Plans API Keys Pages Forms Lists

Custom Forms

Showing 0 forms [Add New Custom Form](#)

Built-in Forms	Last Updated
Contact Information	2013-11-22 14:35:42
Ticket Details	2013-11-22 14:35:42
Company Information	2013-11-22 14:35:42

Custom Forms
Last Updated

No extra forms defined yet — [add one!](#)

[Delete](#)

Custom fields

Post Reply Post Internal Note Dept. Transfer Assign Ticket

TO: Karen Moreau <Karen@osticket.com> Email Reply

Response: Append Draft Saved

Reply in *STYLE* and *COLOR*!

You can place **emphais** on certain words . . .

Even add pictures! 

Attachments: No file chosen

Signature: None My signature Dept. Signature (Support)

Ticket Status: Close on Reply

Rich HTML

Dashboard Settings **Manage** Emails Staff
Help Topics Ticket Filters SLA Plans API Keys Pages Forms Lists

Ticket Filter

Update Filter

Filters are executed based on execution order. Filter can target specific ticket source.

Filter Name:

Execution Order: (1...99) Stop processing further on match!

Filter Status: Active Disabled

Target:

Filter Rules: Rules are applied based on the criteria.

Rules Matching Criteria: Match All Match Any (case-insensitive comparison)

Email: (clear)

Filter Actions: Can be overridden by other filters depending on processing order.

Reject Ticket: **Reject Ticket** (All other actions and filters are ignored)

Reply-To Email: Use Reply-To Email (if available)

Ticket auto-response: Disable auto-response. (Override Dept. settings)

Canned Response: (Automatically respond with this canned response)

Department:

Priority: (Overrides department's priority)

SLA Plan: (Overrides department's SLA)

Auto-assign To:

Admin Notes: Internal notes

Ticket filters

Dashboard Settings **Manage** Emails Staff
Emails **Barlist** **Templates** **Diagnosis**

Email Template Message - osTicket Default Template (HTML)

Message Template:

Autorecponses sent to user, if enabled, on new ticket.
Subject and body required. Supported Variables.

Message Subject: Email message subject

Support Ticket Opened

Message Body: Email message body Draft Saved

We Hear You

Dear **%(ticket.name.first)**,

We received your request and assigned ticket **%(ticket.number)**

Topic: **%(ticket.topic.name)**
Subject: **%(ticket.subject)**
Submitted: **%(ticket.create_date)**

A representative will follow-up with you as soon as possible. You can [view this ticket's progress online](#).

Your **%(company.name) Team**,
%(signature)

%(company.name)
%(signature)

If you wish to send additional comments or information regarding this issue, please don't open a new ticket. Simply [login](#) and update the ticket.

Visit our [knowledgebase](#)

Auto responder



Alerting and Reporting

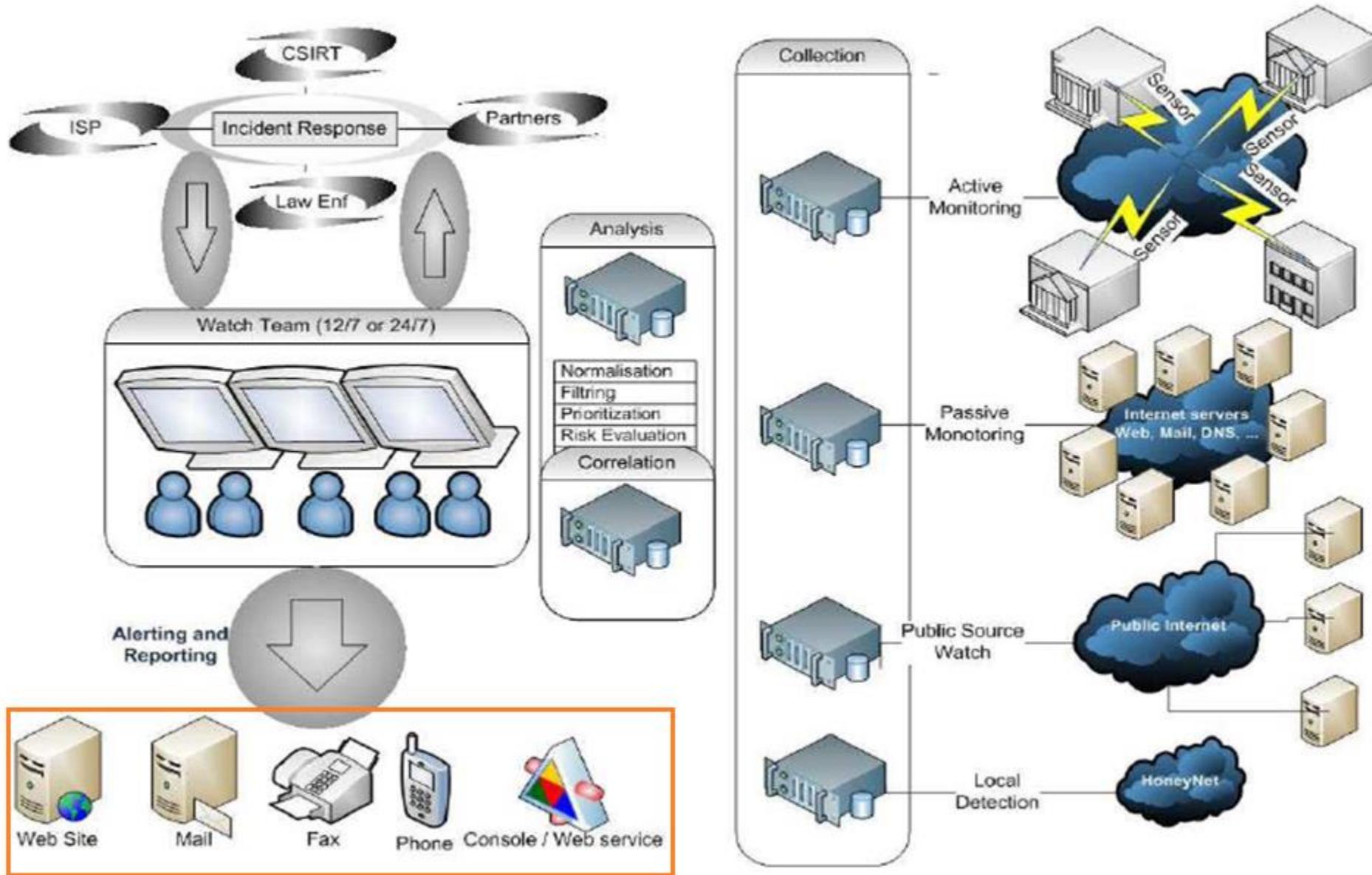
CSIRT Portal

- Focal point where people will go and look for information on the CSIRT
- The portal will facilitate the distribution of information to the constituents.
- It will display latest security news, vulnerability news, advisories, etc.

The screenshot shows the homepage of the National CSIRT-CY website. At the top, there is a navigation menu with links for Home, Services, Announcements, Incident Reporting Tips, About Us, FAQ, and Contact Us. The main content area features a large blue banner with the text "CSIRT-CY: Computer Security Incident Response Team" and a sub-header "REPORT AN INCIDENT". Below this, there is a call to action: "You may report an incident using the Online Reporting Form, send the duly filled reporting form to REPORTING@CSIRT.CY or call us at 1490". Two buttons are provided: "Report Online" and "Download Form". Below the banner, there are two distinct zones: the "Constituency Zone" (green background) for authorized members to login, and the "Security Awareness Zone" (yellow background) for the Pedagogical Institute of Cyprus, with a "Click to visit" button.

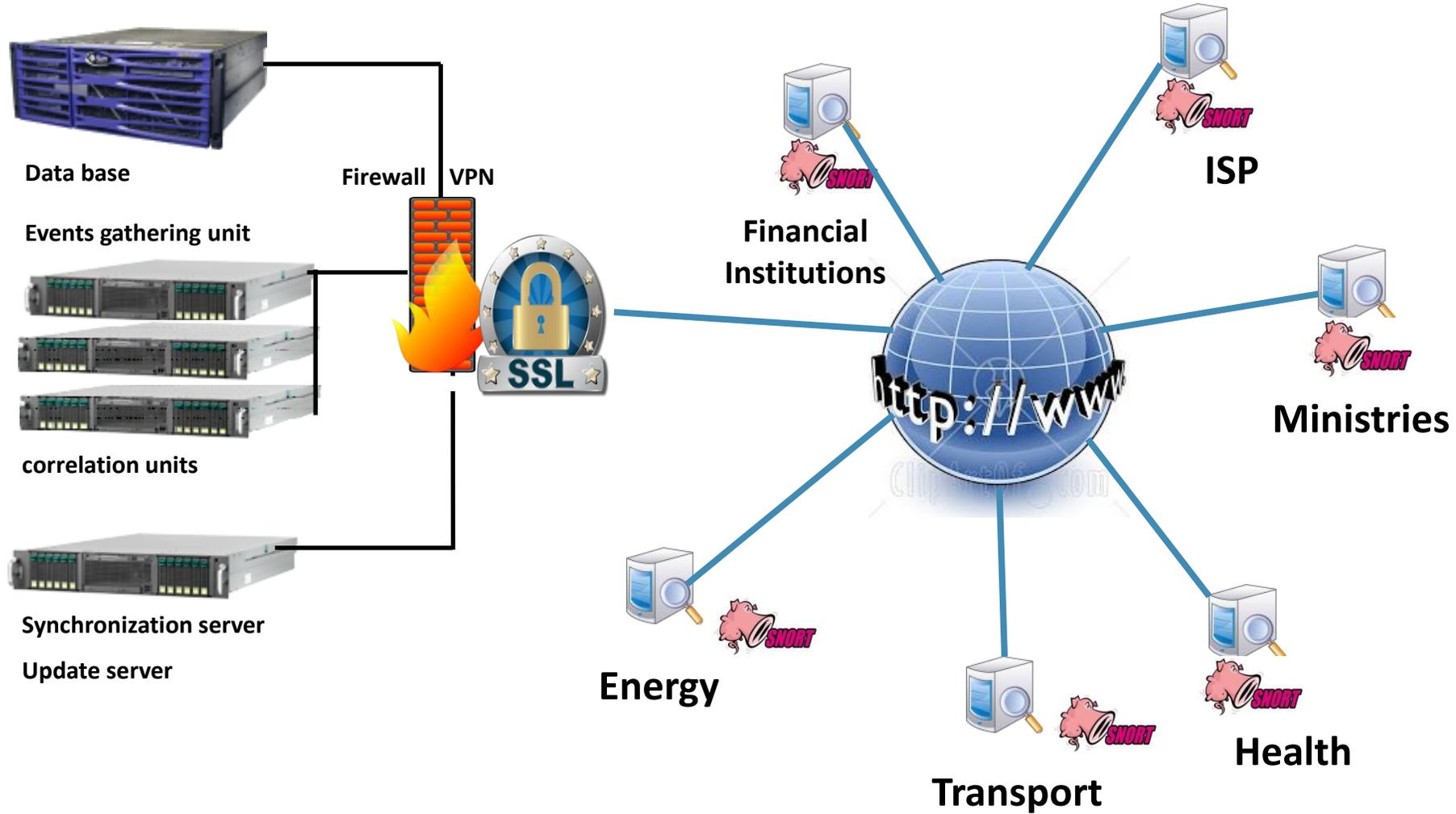


Incident Response Center





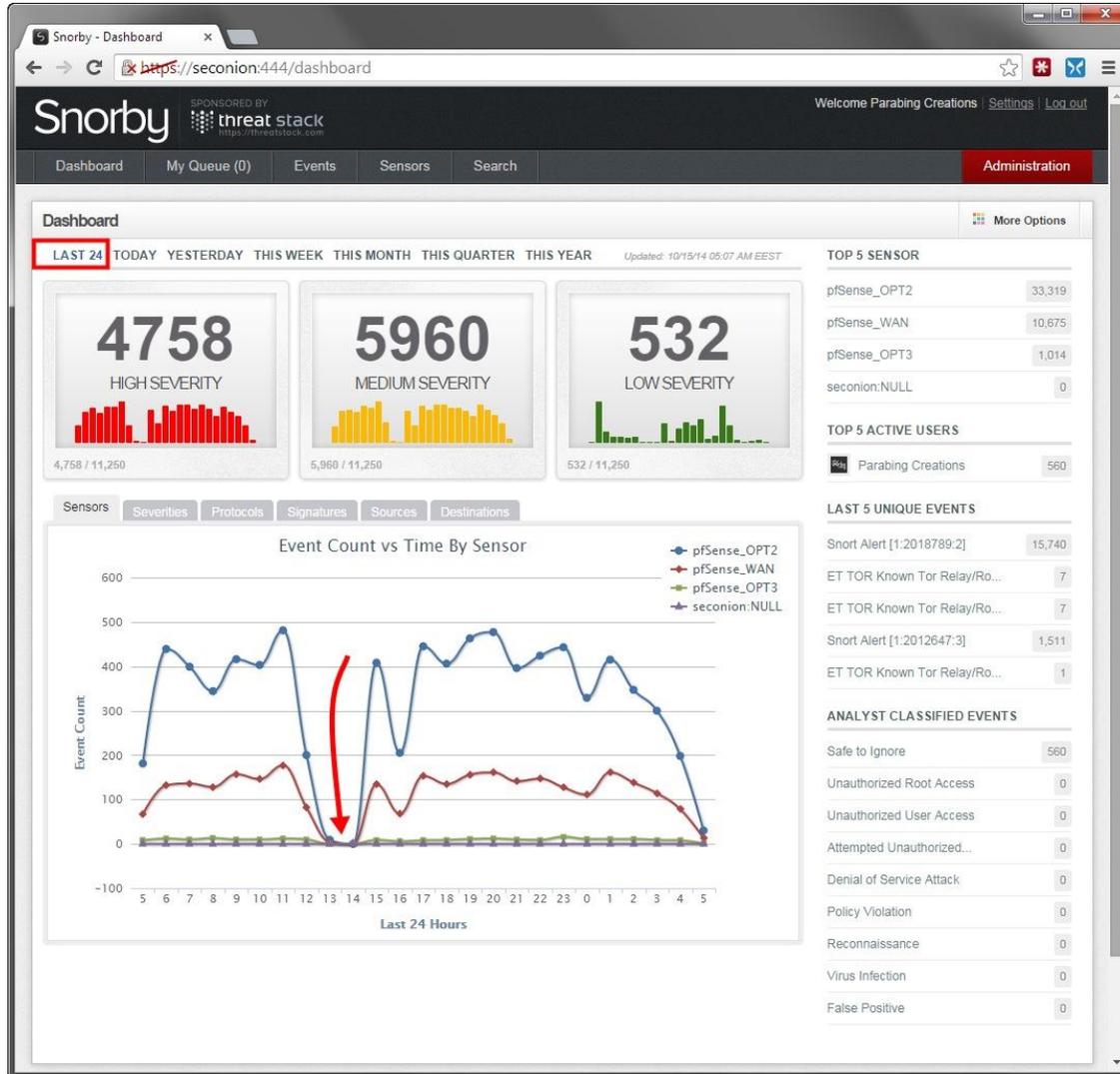
Active Monitoring





Active Monitoring

<https://github.com/Snorby>





Active Monitoring

Snort
Snort overview

Update in background Fullscreen Unlock / Edit

Drag widgets to any position you like in [unlock / edit mode](#).

All alert source locations

Failed SSH logins

Snort alerts

Top attacks

Value	%	Count
Top values		
ICMP PING	21.95%	45
ICMP PING BSDtype	18.05%	37
ICMP PING *NIX	18.05%	37
SCAN UPnP service discover attempt	10.24%	21
SNMP public access udp	4.39%	9
Others		
SNMP request udp	4.39%	9
ICMP Destination Unreachable Communication with Destination Host is Administratively Prohibited	3.90%	8
ICMP Destination Unreachable Port	3.90%	8

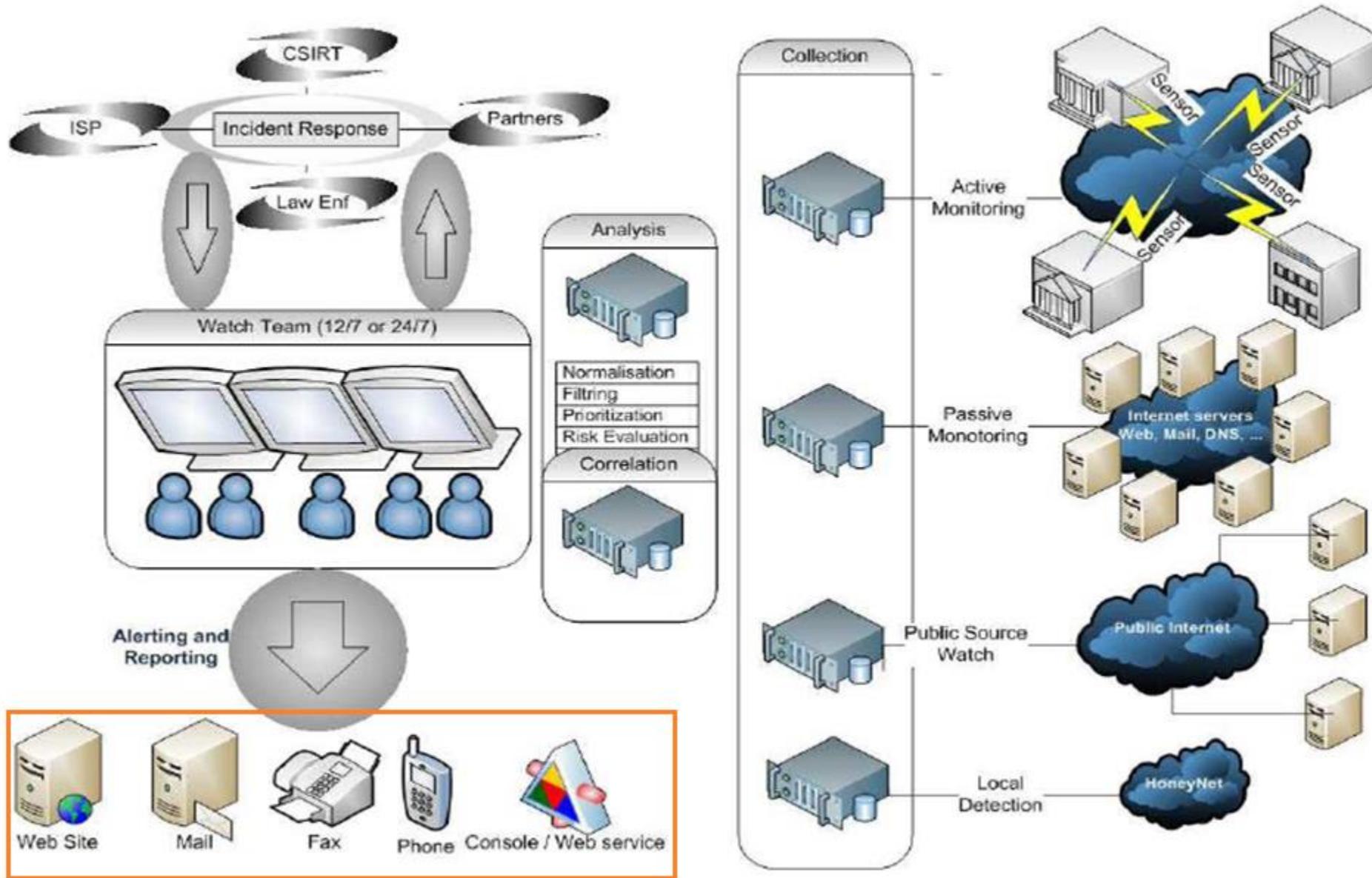
Top attacker IP addresses

Value	%	Count
Top values		
12.156.166.2	54.15%	111
104.192.0.18	4.88%	10
99.42.44.219	2.93%	6
185.128.40.162	2.44%	5
209.126.136.2	2.44%	5
Others		
204.42.253.130	1.95%	4
184.105.139.67	1.95%	4
130.185.109.8	1.46%	3
51.255.82.25	1.46%	3

Graylog 2.1.0-beta.2+ffa3355 on localhost (Oracle Corporation 1.8.0_101 on Linux 3.13.0-92-generic)



Incident Response Center





Passive Monitoring

Icinga - Status Map

Servvertime: 07:09:01 | Press CTRL+ALT+F ... | Root, Enoch

26 / 0 UP | **0 / 4 / 0 DOWN** | 0 / 0 / 0 UNREACHABLE | 0 PENDING | 4 / 30 IN TOTAL | 1 OK

32 / 3 OK | 0 / 0 / 0 WARNING | **2 / 4 / 4 CRITICAL** | 0 / 0 / 0 UNKNOWN | 0 PENDING | 10 / 45 IN TOTAL | 0 DOWN

30 / 0 / 0 | 0.004 / 10.004 / 1.067 | 20 / 21 / 4 | 0.004 / 10.004 / 1.723 | 0.012 / 0.251 / 0.134 | 0.033 / 0.251 / 0.149

Monitoring | Admin | Help

Welcome | ServiceStatus | Overview | Downtimes | HostStatus | Hostgroups | Open problem | Portal Zoolur | Reporting De | **Status Map**

Reload | Categories | Settings

My Category (2)

Data (13)

- Unhandled se...
- Unhandled ho...
- Open problems
- ServiceStatus
- ServiceHistory
- HostStatus
- HostHistory
- Hostgroups
- Servicegroups
- Downtimes
- Notifications
- Status Map
- Instances

Tactical Overview (3)

Reporting (2)

Business Process (2)

Misc (7)

```
graph TD; router((router)) --- switch-1((2-switch-1)); router --- app-1((1-app-1)); router --- printer-1((2-printer-1)); router --- web-de-ntp((web-de-ntp)); router --- google-www((google-www)); router --- web-de-www((web-de-www)); router --- web-de-ntp((web-de-ntp)); router --- kinga((kinga)); router --- yahoo-www((yahoo-www)); router --- yahoo-sntp((yahoo-sntp)); router --- mysql-ntp((mysql-ntp)); router --- done((done));
```

HOST_ICON_IMAGE	default
INSTANCE_NAME	yahoo-sntp
HOST_NAME	yahoo-sntp
Alias	yahoo-sntp
Display name	LP
Current state	UP
DURATION_START	2012-05-30 08:52:38
Last check	2012-05-31 07:04:58
Next check	2012-05-31 07:10:08
HOST_PROGRAM_START_TIME	2012-05-30 08:52:38
Output	PING OK - Packet loss = 0%, RTA = 8.00 ms
Current check attempt	1
HOST_MAX_CHECK_ATTEMPT	10
HOST_PROCESS_PERFORMANCE_DATA1	
max_attempt	10
HOST_INSTANCE_ID	1
HOST_ID	5295
HOST_IS_PENDING	0
notifications_enabled	1
problem_acknowledged	0
scheduled_downtime_depth	0
host_has_been_checked	1
HOST_PARENT_OBJECT_ID	120



Passive Monitoring

ZABBIX

Monitoring Inventory Reports Configuration Administration

Dashboard Overview Web Latest data Triggers Events Graphs Screens Maps Discovery IT services

Dashboard

Favourite maps

Local network
Maps

Favourite graphs

New host: CPU load
Graphs

Favourite screens

Zabbix server
Screens Slide shows

Last 20 issues

HOST	ISSUE	LAST CHANGE	AGE	INFO	ACK	ACTIONS
Zabbix server 1	Version of zabbix-agent(d) was changed on Zabbix server 1	2016-01-11 22:36:06	1m 39s		No	1
Zabbix server 1	Lack of free swap space on Zabbix server 1	2015-08-11 23:29:28	5m 3d		Yes	4

2 of 2 issues are shown Updated: 22:37:45

System status

HOST GROUP	DISASTER	HIGH	AVERAGE	WARNING	INFORMATION	NOT CLASSIFIED
Discovered hosts	0	0	0	1	1	0
Network devices	0	0	0	0	0	0
SNMP hosts	0	0	0	0	0	0
Zabbix servers	0	0	0	1	1	0

Updated: 22:37:45

Host status

HOST GROUP	WITHOUT PROBLEMS	WITH PROBLEMS	TOTAL
Discovered hosts	7	1	8
Network devices	1	0	1
SNMP hosts	2	0	2
Zabbix servers	0	1	1

Updated: 22:37:44

Discovery status

DISCOVERY RULE	UP	DOWN
Local network2	6	1

Updated: 22:37:44

Status of Zabbix

PARAMETER	VALUE	DETAILS
Zabbix server is running	Yes	localhost:10051
Number of hosts (enabled/disabled /templates)	54	10 / 1 / 43
Number of items (enabled/disabled/not supported)	356	350 / 0 / 6
Number of triggers (enabled/disabled [problem/ok])	95	94 / 1 [2 / 92]
Number of users (online)	3	2
Required server performance, new values per second	4.79	

Updated: 22:37:45

Web monitoring

HOST GROUP	OK	FAILED	UNKNOWN
Discovered hosts	1	0	0
Zabbix servers	1	0	0

Updated: 22:37:44

Debug

ZABBIX

Help | Get support | Print | Profile | Logout

Monitoring Inventory Reports Configuration Administration

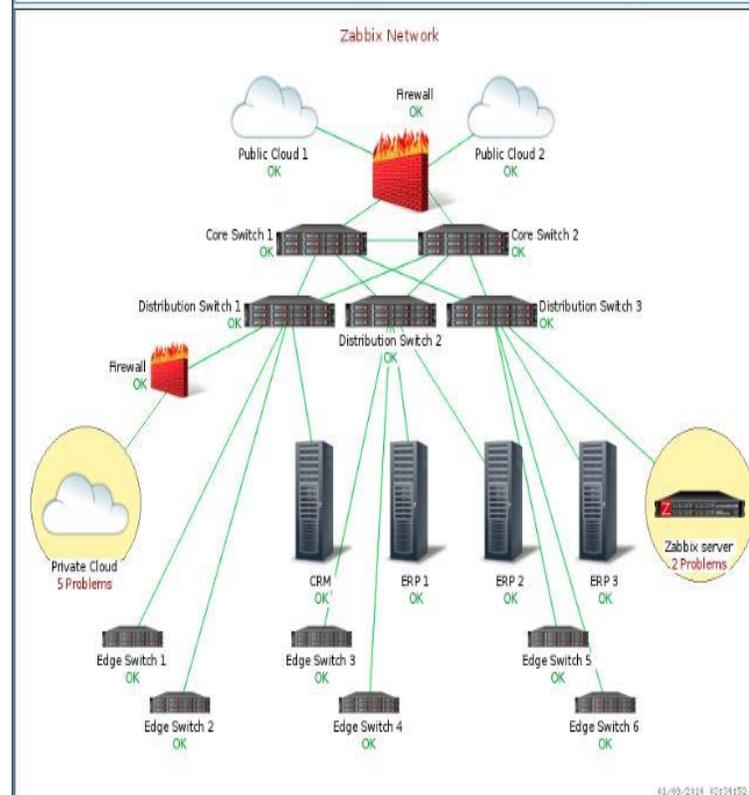
Dashboard Overview Web Latest data Triggers Events Graphs Screens Maps Discovery IT services

History: Latest data » History » Status of triggers » Latest events » Network maps

NETWORK MAPS

Zabbix Network

Maps Zabbix Network Minimum severity Not classified (default)

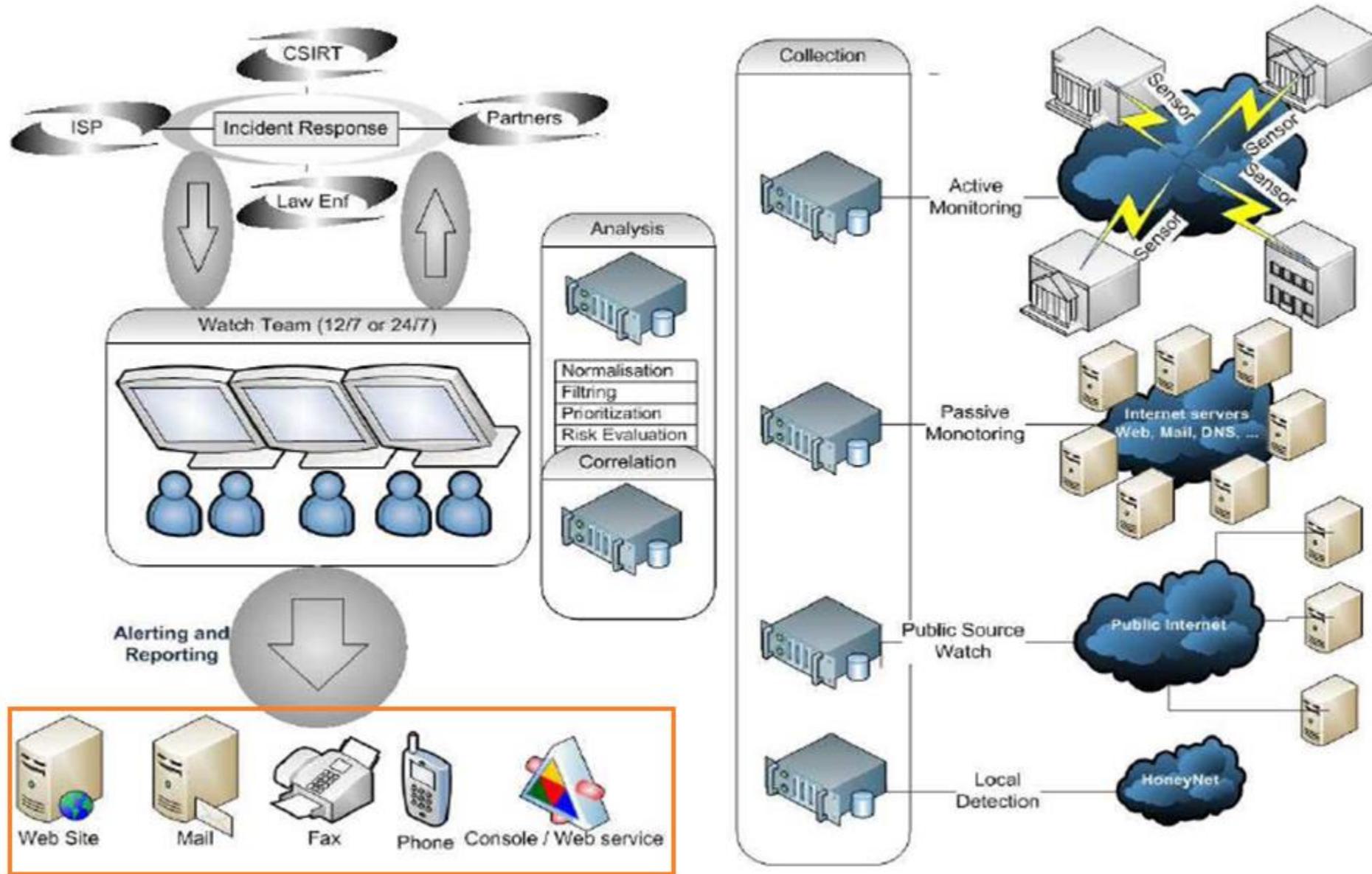


Zabbix 2.2.0 Copyright 2001-2013 by Zabbix SIA

Connected as 'Admin'



Incident Response Center





Public Feeds

Malwares infections, C&C servers , malicious IPS

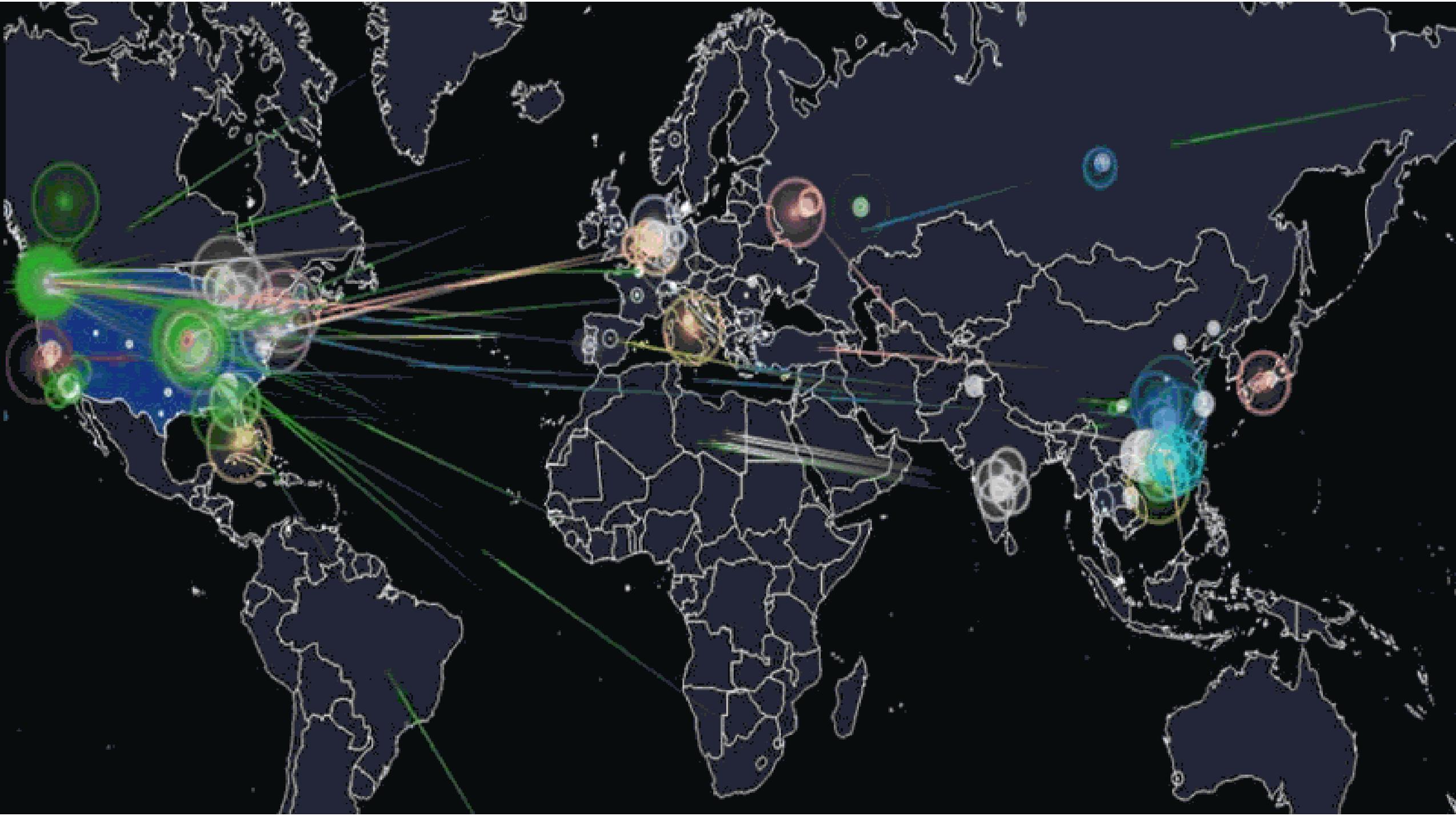
<http://danger.rulez.sk/index.php/bruteforceblocker/>
<http://www.senderbase.org>
<http://www.malwaredomains.com>
<https://feodotracker.abuse.ch/>
<https://hosts-file.net/rss.asp>
<http://malc0de.com/rss/>
<http://www.malwaredomainlist.com/mdlcsv.php>
<http://www.malwaredomainlist.com/updatescsv.php>
<http://www.nothink.org/>
<https://otx.alienvault.com/>
<http://vxvault.net/ViriList.php>
<http://www.urlvir.com/>
<https://www.autoshun.org/>
<https://www.normshield.com/>
<http://data.netlab.360.com/mirai-c2/>
<http://data.netlab.360.com/feeds/dga/dga.txt>
http://www.ipspamlist.com/public_feeds.csv

<https://amtrckr.info/>
<https://www.circl.lu/doc/misp/feed-osint/>
<http://www.botvrij.eu/data/feed-osint/>
<https://feeds.inthreat.com/osint/misp/>
<https://zeustracker.abuse.ch/>
<https://ransomwaretracker.abuse.ch/feeds/csv/>
<https://rules.emergingthreats.net/blockrules/compromised-ips.txt>
<https://panwdbl.appspot.com/lists/mdl.txt>
<http://cybercrime-tracker.net/>
<https://www.badips.com/>
<https://lists.blocklist.de/lists/all.txt>



Public Feeds

- <http://map.norsecorp.com/#/>
- <https://intel.malwaretech.com/pewpew.html>





Public Feeds

- Web defacement
 - <http://www.zone-h.org/archive/special=1>

zone-h
unrestricted information

Home News Events Archive Archive ★ Onhold Notify Stats Register Login search...

NOTIFIER DOMAIN

Special defacements only Fulltext/Wildcard Onhold (Unpublished) only

Date :

Total notifications: **8,707** of which **2,827** single ip and **5,880** mass defacements

Legend:
 H - Homepage defacement
 M - Mass defacement (click to view all defacements of this IP)
 R - Redefacement (click to view all defacements of this site)
 L - IP address location
 ★ - Special defacement (special defacements are important websites)

Date	Notifier	H	M	R	L	★ Domain	OS	View
2016/01/12	BD BLACK HAT	H	M			homeorigins.ph	Linux	mirror
2016/01/12	BloodSecurity			M		ppur.puertoprincesa.ph/bloodse...	Win 2008	mirror
2016/01/12	aAn					www.brainsparks.ph/aan.txt	Linux	mirror
2016/01/11	MuhmadEmad			M		www.toyotacabanatuan.com.ph/kr...	Unknown	mirror
2016/01/09	masterband01	H	M			leahtm.com.ph	Linux	mirror
2016/01/09	masterband01	H		R		pinnacle.ph	Linux	mirror
2016/01/08	jok3r					www.livegreen.ph/H.htm	Linux	mirror
2016/01/07	w4l3XzY3			R		nast.ph/w.htm	Linux	mirror
2016/01/07	MuhmadEmad			R		www.lyceumsubicbay.com.ph/krd....	Unknown	mirror
2016/01/07	ZoRRoKiN	H				czar.ph	Linux	mirror
2016/01/06	n3far1ous	H				help.happyplus.com.ph	Linux	mirror
2016/01/06	d3b~X	H	M			www.vtech.com.ph	Linux	mirror
2016/01/05	AlfabetoVirtual					www.bir.gov.ph/a.htm	Linux	mirror
2016/01/04	jok3r			R		www.coa.gov.ph/H.htm	Win 2008	mirror
2016/01/04	Unknown AI		M			biomasscon.uplb.edu.ph/anoncod...	Linux	mirror
2016/01/04	Unknown AI		M			dche.uplb.edu.ph/anoncoders.htm	Linux	mirror
2016/01/04	Unknown AI		M			des.uplb.edu.ph/anoncoders.htm	Linux	mirror



Public Feeds

- Phishing
 - https://www.phishtank.com/asn_search.php

The screenshot shows a web browser displaying the PhishTank search results for ASN 9821. The page title is "Search by ASN : DOST-PH-AP Department of Science and Technology,PH (?)". The search criteria are ASN: 9821, Valid?: All, and Online?: Online. A single result is shown in a table:

ID	Phish URL	Submitted	Valid?	Online?
3612666	http://www.pcaarrd.dost.gov.ph/home/momentum/libraries/vicfiles/Doc/Go... added on Nov 15th 2015 11:13 PM	by cleanmx	VALID PHISH	ONLINE



Public Feeds

- Malware

- <https://www.malwaredomainlist.com/mdl.php>

MALWARE DOMAIN LIST

[Homepage](#) | [Forums](#) | [Recent Updates](#) | [RSS update feed](#) | [Contact us](#)

WARNING: All domains on this website should be considered dangerous. If you do not know what you are doing here, it is recommended you leave right away. This website is a resource for security professionals and enthusiasts.

Search: All ▼ Results to return: 50 ▼ Include inactive sites

Page [0](#) [1](#) ... [33](#)

Date (UTC)	Domain	IP	Reverse Lookup	Description	Registrant	ASN
↑ ↓	↑ ↓	↑ ↓	↑ ↓	↑ ↓	↑ ↓	↑ ↓
2016/03/09_09:35	marketing-material.ieiworld.com/	173.255.219.191	li229-191.members.li node.com.	compromised site leads to Angler EK	Registrar Abuse Contact abuse@web.com	6939
2016/03/09_09:35	www.saintlouis-viry.fr/infos- pratiques/documents-a-telecharg er.html	5.135.11.9	-	compromised site leads to Angler EK	support@alcyonweb.fr	16276
2016/03/08_14:13	ozono.org.es/k7j6h5gf	217.160.232.15	clienteservidor.es.	Locky ransomware	-	8560
2016/03/08_14:13	ministerepuissanceje sus.com/o097jhg4g5	69.89.31.133	box333.bluehost.com.	Locky ransomware	Registrar Abuse Contact abuse@dynadot.com	46606
2016/03/08_13:42	lahmar.choukri.perso .neuf.fr/78hg4wg	86.65.123.70	70.123.65.86.rev.sfr.net.	Locky ransomware	domains@sfr.com	15557
2016/03/08_10:58	lhs-mhs.org/9uj8n76b5.exe	208.131.141.2	rageresearch.com.	trojan	Gene Mathis / gcm@gc mathis.com	29854
2016/03/08_10:58	reclamus.com/9uj8n76b5.exe	198.63.208.35	vserv.cifnet.com.	trojan	-	14585
2016/03/08_10:58	stopmeagency.free.fr /9uj8n76b5.exe	212.27.63.112	perso112-g5.free.fr.	trojan	skolaric@online.net	12322
2016/03/08_10:51	izzy-cars.nl/9uj8n76b5.exe	46.235.47.134	srv047134.webreus.nl.	trojan	-	34233
2016/03/07_21:39	softworksbd.com/73tgbf334	59.152.100.158	-	trojan Locky	-	63969



Public Feeds

- Botnet

- <https://zeustracker.abuse.ch/monitor.php>

ZeuS Tracker :: Monitor

Below is a list of all ZeuS C&Cs as well as Fake URLs which are currently known to ZeuS Tracker. You can browse the ZeuS Tracker to get a list of ZeuS C&Cs and FakeURLs for a specified country or AS. Additionally, ZeuS Tracker provides a feature which allows to filter the ZeuS C&Cs for specified nameservers, level, status and many more.

Each ZeuS C&C or FakeURL is tagged with a *level*. The level indicates which kind of IP the Host is hosted on. Here is an overview about the levels and its meaning:

Level	Description
Level 1	Bulletproof hosted
Level 2	Hacked webserver
Level 3	Free hosting service
Level 4	Unknown
Level 5	Hosted on a FastFlux botnet

Additionally, every host is at least in one of the following category:

- Hosts which are tagged as **CC** are ZeuS Command&Control servers
- Hosts which are tagged as **FU** are referenced by ZeuS as FakeURLs

You can also search the ZeuS Tracker for domains, IPs, urls, MD5 hashes or FakeURLs:

Browse: [ZeuS BinaryURLs](#) | [ZeuS ConfigURLs](#) | [ZeuS Dropzones](#)

Malware family filter: [ZeuS](#) | [Ice IX](#) | [Citadel](#) | [KINS](#)

Set a filter for the list below: [Remove filter \(Show all\)](#) | [online ZeuS hosts](#) | [offline ZeuS hosts](#) | [ZeuS hosts with files online](#) | [order by lastupdated](#)

Filter C&C server tagged with level: [Level 1 \(Bulletproof\)](#) | [Level 2 \(HiJacked sites\)](#) | [Level3 \(Free webhosting\)](#) | [Level 4 \(Unknown\)](#) | [Level 5 \(FastFlux hosted\)](#)

[Subscribe this list via RSS feed](#)

Dateadded	Malware	Host	IP address	Level	Status	Files Online	SBL	Country	AS number	Uptime
2016-03-11	VMZeuS	outthere.com	205.234.197.147	2	online	2	SBL 288979		AS23352	00:56:23
2016-03-04	VMZeuS	162.223.94.56	162.223.94.56	4	unknown	2	SBL 288050		AS19084	-
2016-02-20	VMZeuS	fulsexhikayeleri.org	185.51.166.107	2	online	2	Not listed		AS36351	472:34:54
2016-02-09	VMZeuS	95.211.153.134	95.211.153.134	4	unknown	2	Not listed		AS60781	-
2016-01-03	ZeuS	www.demexsoft.com	65.182.101.221	2	online	1	SBL 281145		AS33055	838:59:59
2015-09-13	VMZeuS	wayufilm.com	119.59.120.8	2	online	2	SBL 274938		AS56067	838:59:59
2014-11-15	ZeuS	championbft.com	104.207.130.93	4	online	1	Not listed		AS20473	838:59:59
2014-10-30	ZeuS	hotelavalon.org	104.207.130.93	4	online	1	Not listed		AS20473	838:59:59
2014-05-29	Citadel	www.loongweed.com	202.142.215.16	2	online	1	SBL 228782		AS7654	838:59:59



Semi-Public Feeds

- Data feeds provided to non-profit organisation or specific community such as CSIRT
 - Shadow Server
 - <https://www.shadowserver.org/wiki/pmwiki.php/Involve/GetReportsOnYourNetwork>
 - Team Cymru
 - <http://www.team-cymru.org/CSIRT-AP.html>



https://intel.criticalstack.com

CRITICAL STACK // Feed
Sensors
Collections
Feeds
Client
Dustin Webber ▾ Help ▾

Collections word (44,180)

[+ Create New Collection](#)

[My Feeds \(4\)](#)

[+ Add More Feeds](#)

MANAGE COLLECTION

[Edit This Collection](#)

[Delete This Collection](#)

ORDER FEEDS

[🔍 Most Indicators](#)

[✔ Most Subscribers](#)

[🔊 Recently Added](#)

[🕒 Recently Updated](#)

Zeus Tracker: Domain Block List

Zeus Tracker tracks ZeuS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist.

🔍 495 +2

+ Subscribe

SSL Blacklist (SSLBL)

SSL Blacklist (SSLBL) is a project maintained by alexch. The goal is to provide a list of "bad" SSL certificates and provide you a domain- and a IP-blocklist.

🔍 345 +2

★ ★ ★ ★ ★ (0)

SpyEye: Domain Block List

The SpyEye Tracker is a project maintained by alexch. The goal is to provide a list of "bad" SSL certificates and provide you a domain- and a IP-blocklist.

🔍 127 +2

★ ★ ★ ★ ★ (0)

Tinybanker / Tinba

Bambenek Consulting is a web consulting firm focused on cybersecurity and cybercrime. They will track a website about malware command and control servers (hosts) around the world and provides you a domain- and a IP-blocklist.

🔍 99 +3

★ ★ ★ ★ ★ (0)

Zeus Tracker: Configs

Zeus Tracker tracks ZeuS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist.

🔍 95 +2

★ ★ ★ ★ ★ (0)

SpyEye: IP Block List

The SpyEye Tracker is a project maintained by alexch. The goal is to provide a list of "bad" SSL certificates and provide you a domain- and a IP-blocklist.

🔍 84 +2

★ ★ ★ ★ ★ (0)

Zeus Tracker: Binaries

Zeus Tracker tracks ZeuS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist.

🔍 55 +2

Zeus Tracker: Drop Zones

Zeus Tracker tracks ZeuS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist.

🔍 50 +2

Palevo: Domain Block List

Palevo Tracker tracks ZeuS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist.

🔍 18 +2

Critical Stack, Inc © 2015 <http://criticalstack.com>

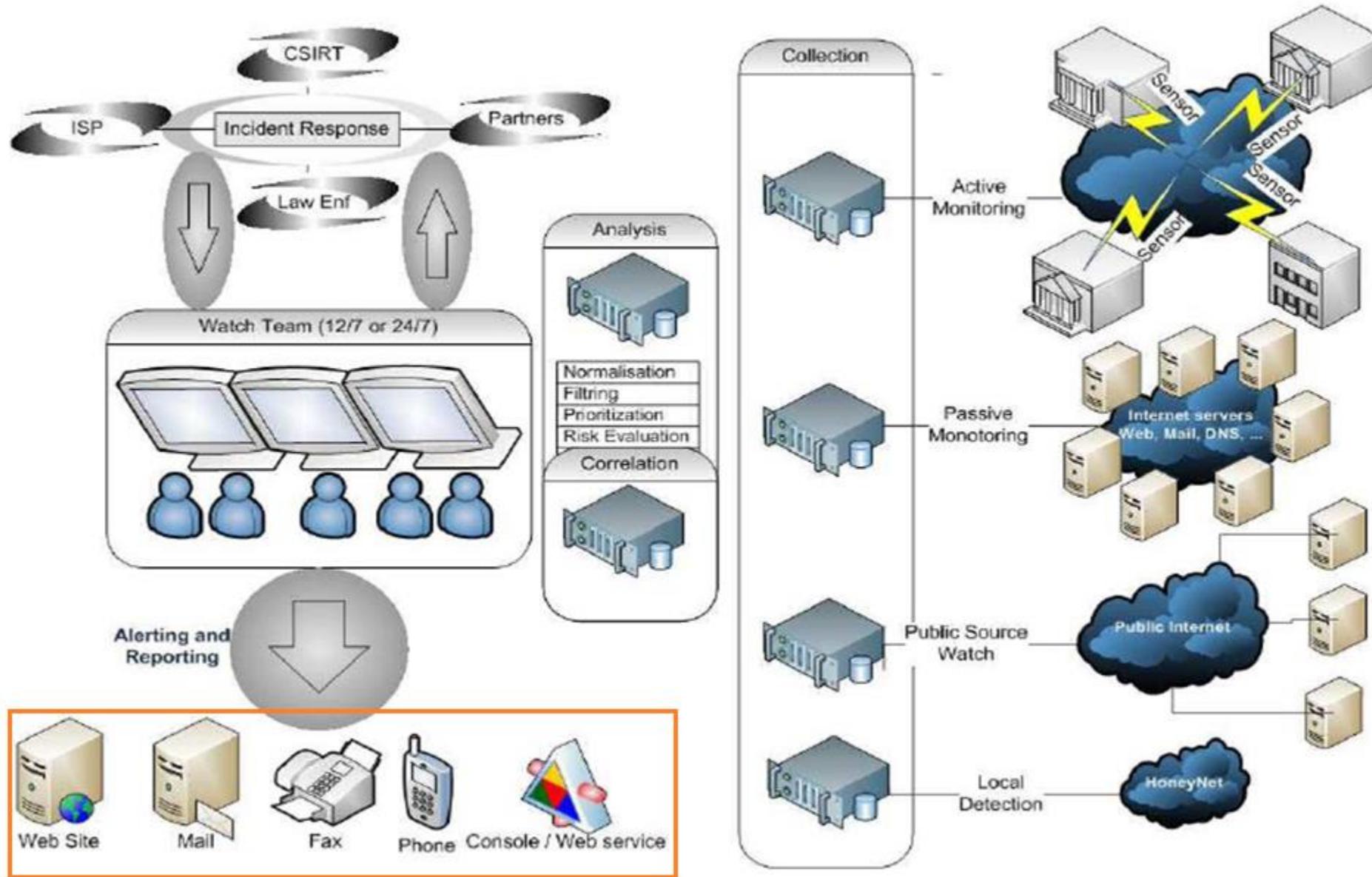
?

Help

25

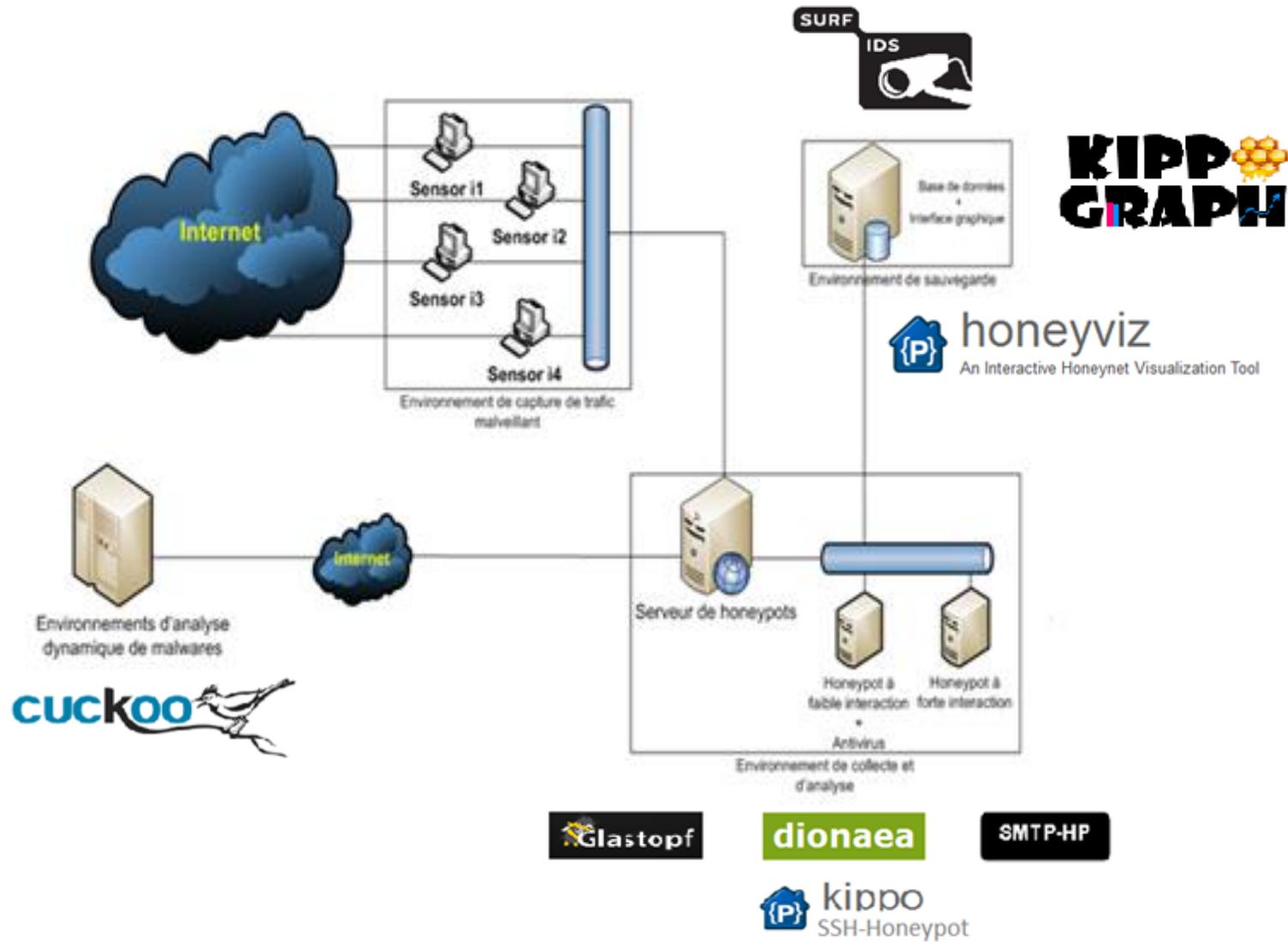


Incident Response Center





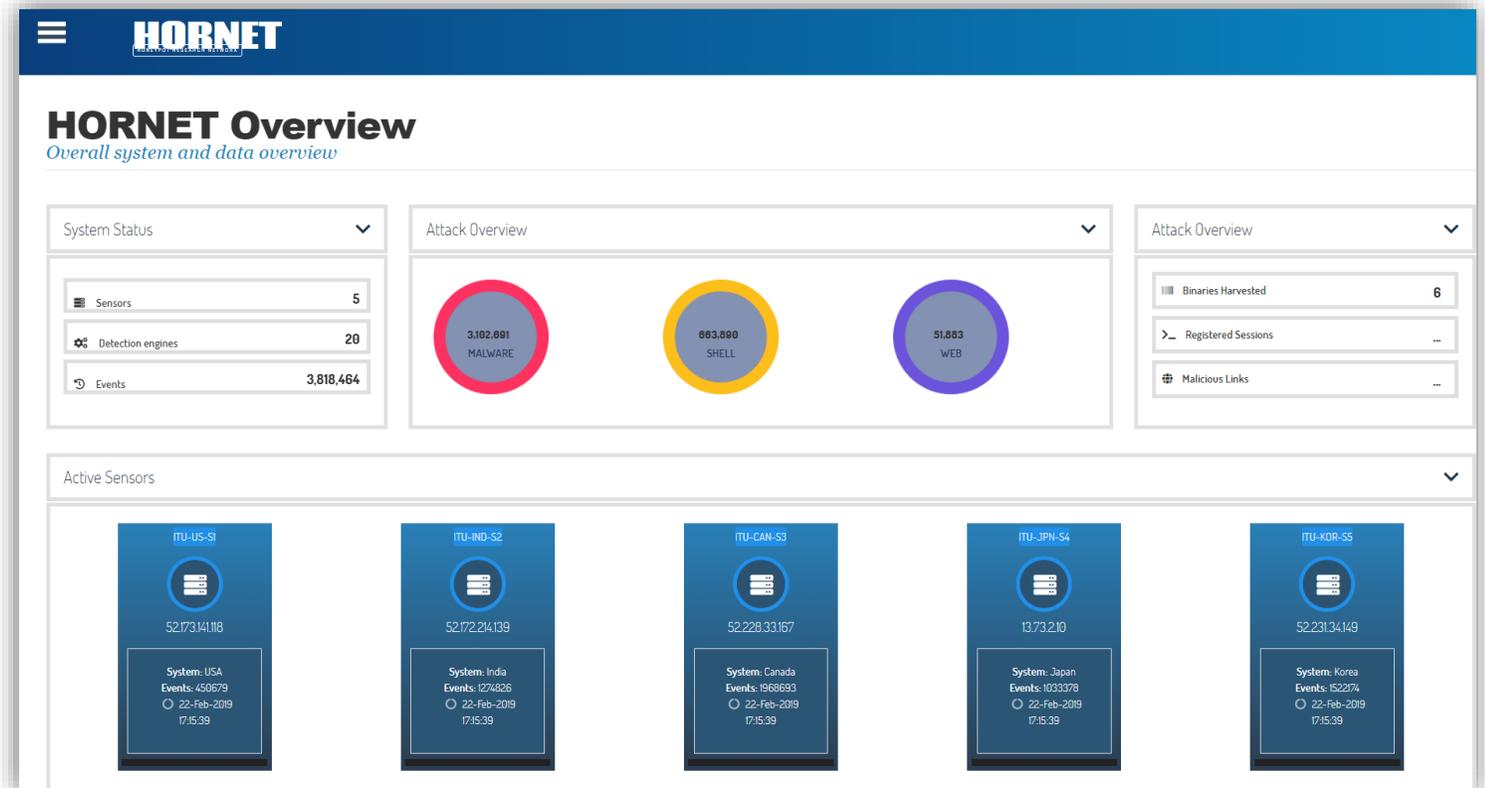
HoneyNet Platforms





HoneyNet Platforms

HoneyPot Research Network (HORNET) :
HoneyNet Platform is a solution for cyber threats monitoring through various external sources.

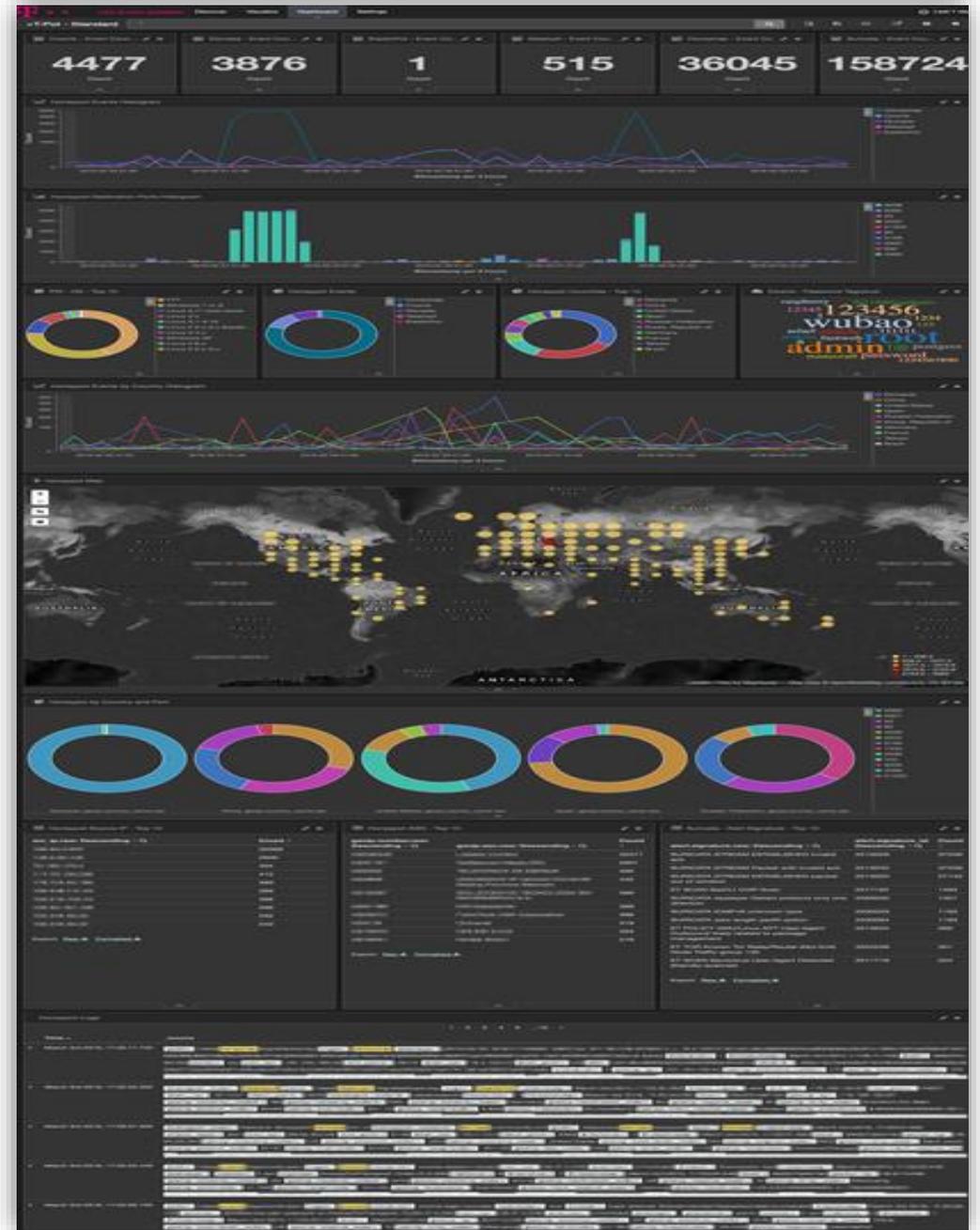




HoneyNet Platforms

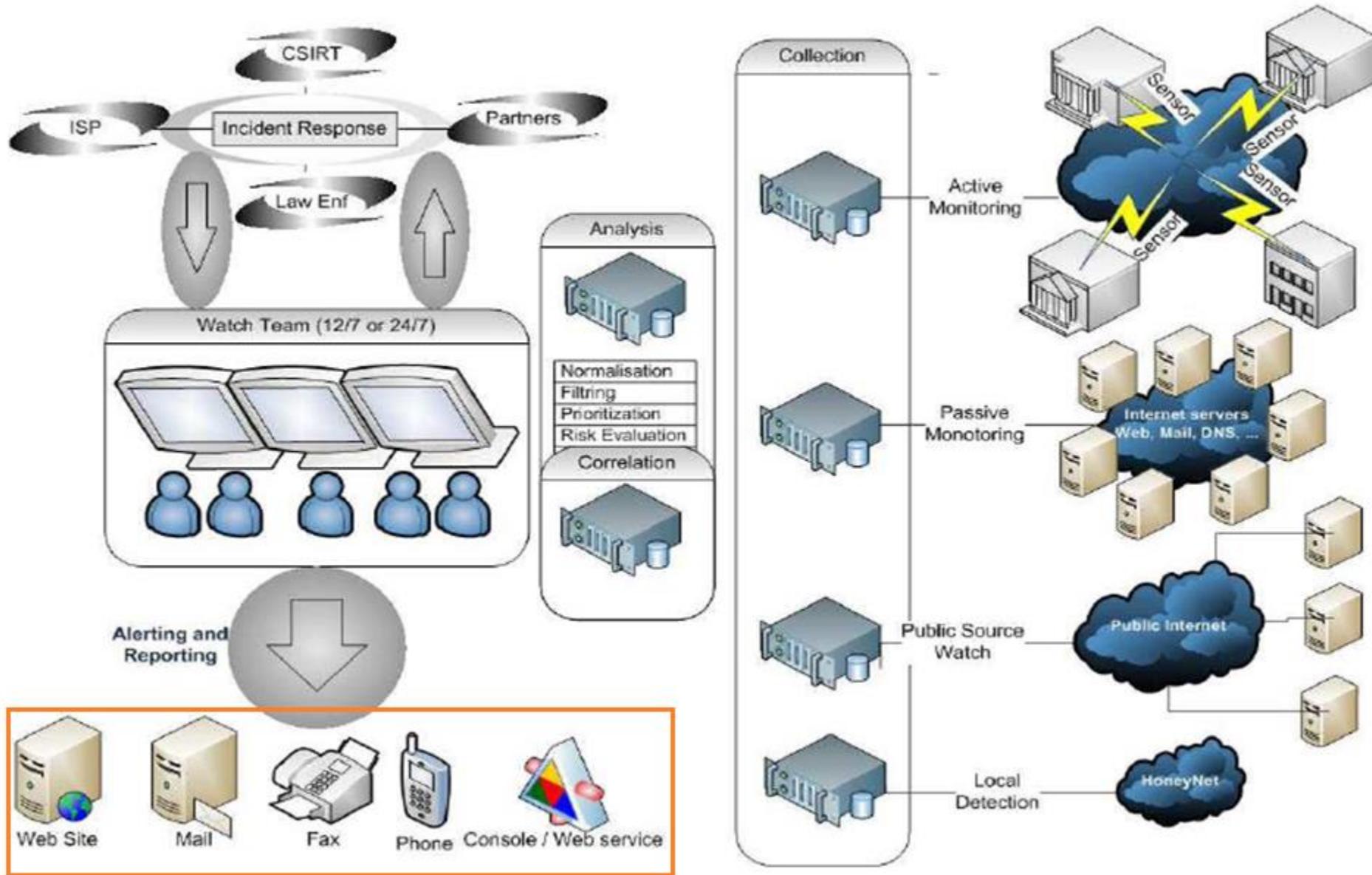
T-POT : Honeypot platform

<http://dtag-dev-sec.github.io/>





Incident Response Center





MISP Open Source Threat Intelligence and Sharing Platform



Hover target

Attribute: 1140909
 Name: 85.128.227.19
 Category:
 Type: attribute
 Comment: logistics.nazwa.pl
 Actions

Selected

Event: 9094
 Info: M2M - Locky 2017-10-05 ; Affid-3,
 offline, "ykool"; "Invoice INV000123" - "Invoice
 INV000123.7z"
 Date: 2017-10-06
 Analysis: Ongoing
 Org: CIRCL
 Actions
 Go to event
 Expand (x)

Home Event Actions Input Filters Global Actions Sync Actions Administration Audit Discussions MISP Admin Log out

List Events

Add Event
 Import From MISP Export

List Attributes
 Search Attributes

View Proposals
 Events with proposals

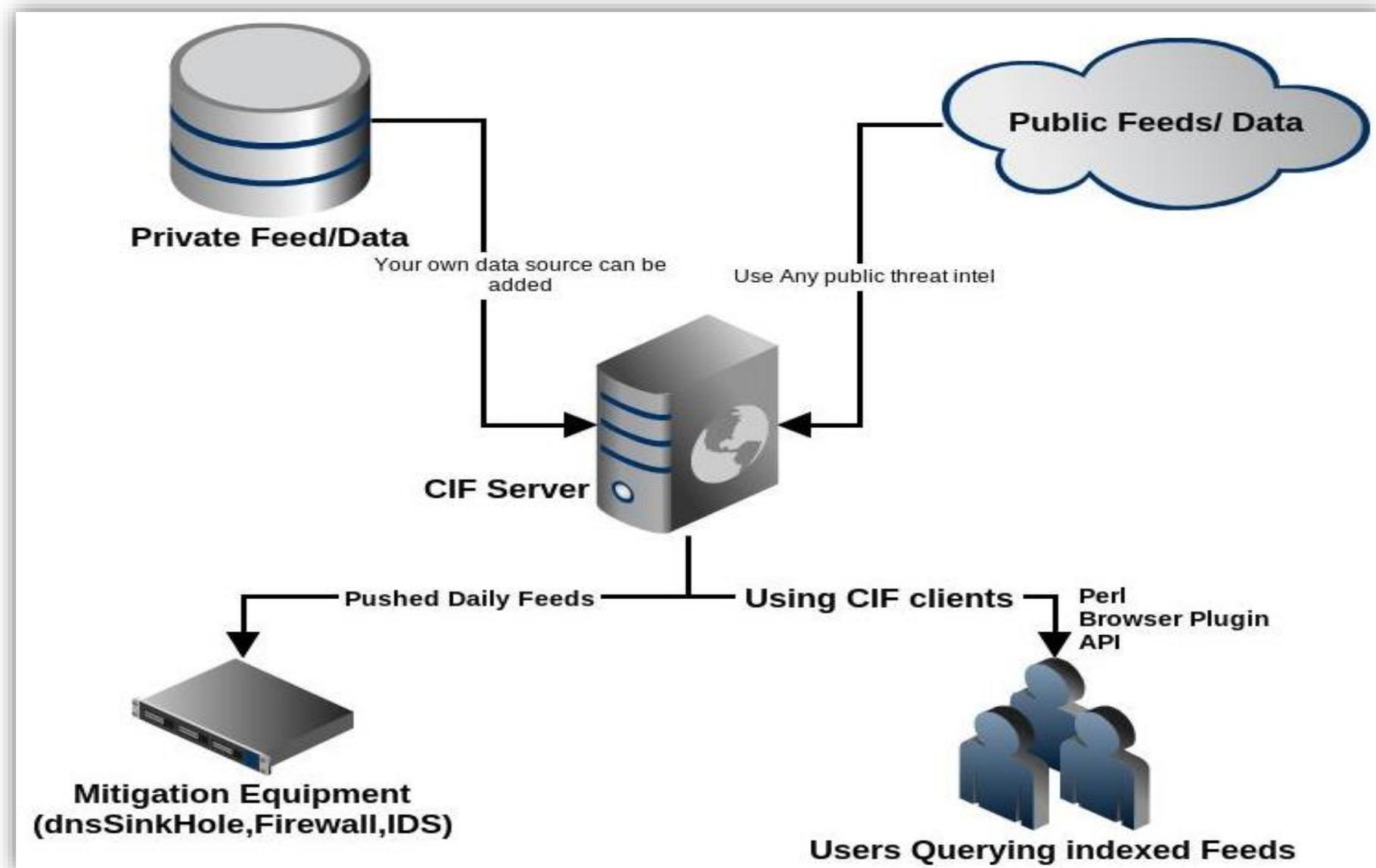
Export
 Automation

Published	Org	Owner Org	Id	Tags	#Attr	Email	Date	Threat Level	Analysis	Info	Distribution	Actions
✓	CUDESO	ORGNAM	93	tip:white	16	admin@admin.test	2016-03-23	Medium	Completed	SAMSAM: THE DOCTOR WILL SEE YOU AFTER HE PAYS THE RANSOM	All	🗑️ 📄
✓	CUDESO	ORGNAM	91	tip:white	3	admin@admin.test	2016-03-07	Low	Completed	Ad Serving Platform Used By PUJA Also Delivers Magnitude Exploit Kit	All	🗑️ 📄
✓	CUDESO	ORGNAM	92	tip:white	3	admin@admin.test	2016-03-25	Low	Completed	PETYA Crypto-ransomware Overwrites MBR to Lock Users Out of Their Computers	All	🗑️ 📄
✗	CIRCL	ORGNAM	5	tip:white Type:OSINT	84	admin@admin.test	2016-02-13	Medium	Completed	OSINT - Turla - Harnessing SSL Certificates Using Infrastructure Chaining	All	🗑️ 📄
✗	CIRCL	ORGNAM	43	tip:white Type:OSINT	70	admin@admin.test	2016-03-21	Low	Completed	OSINT - STOP SCANNING MY MACRO	All	🗑️ 📄
✓	CIRCL	ORGNAM	10	tip:white	847	admin@admin.test	2016-03-17	Low	Initial	Potential SpamBots (2016-03-17)	All	🗑️ 📄
✓	CIRCL	ORGNAM	44	tip:white	280	admin@admin.test	2016-03-17	Low	Initial	Malspam (2016-03-17) - All Dridex (122), Locky	All	🗑️ 📄
✓	CIRCL	ORGNAM	16	tip:white	92	admin@admin.test	2016-03-16	Low	Completed	OSINT - AceDeceiver: First iOS Trojan Exploiting Apple DRM Design Flaws to Infect Any iOS Device	All	🗑️ 📄
✓	CUDESO	ORGNAM	71	tip:white	25	admin@admin.test	2016-03-11	Low	Completed	PowerSniff Malware Used in Macro-based Attacks	All	🗑️ 📄
✓	CIRCL	ORGNAM	25	malware_classification:malware-category=Ransomware	32	admin@admin.test	2016-03-16	Low	Initial	Locky (2016-03-16)	All	🗑️ 📄

Download: PGP/GPG key Powered by MISP 2.4.28

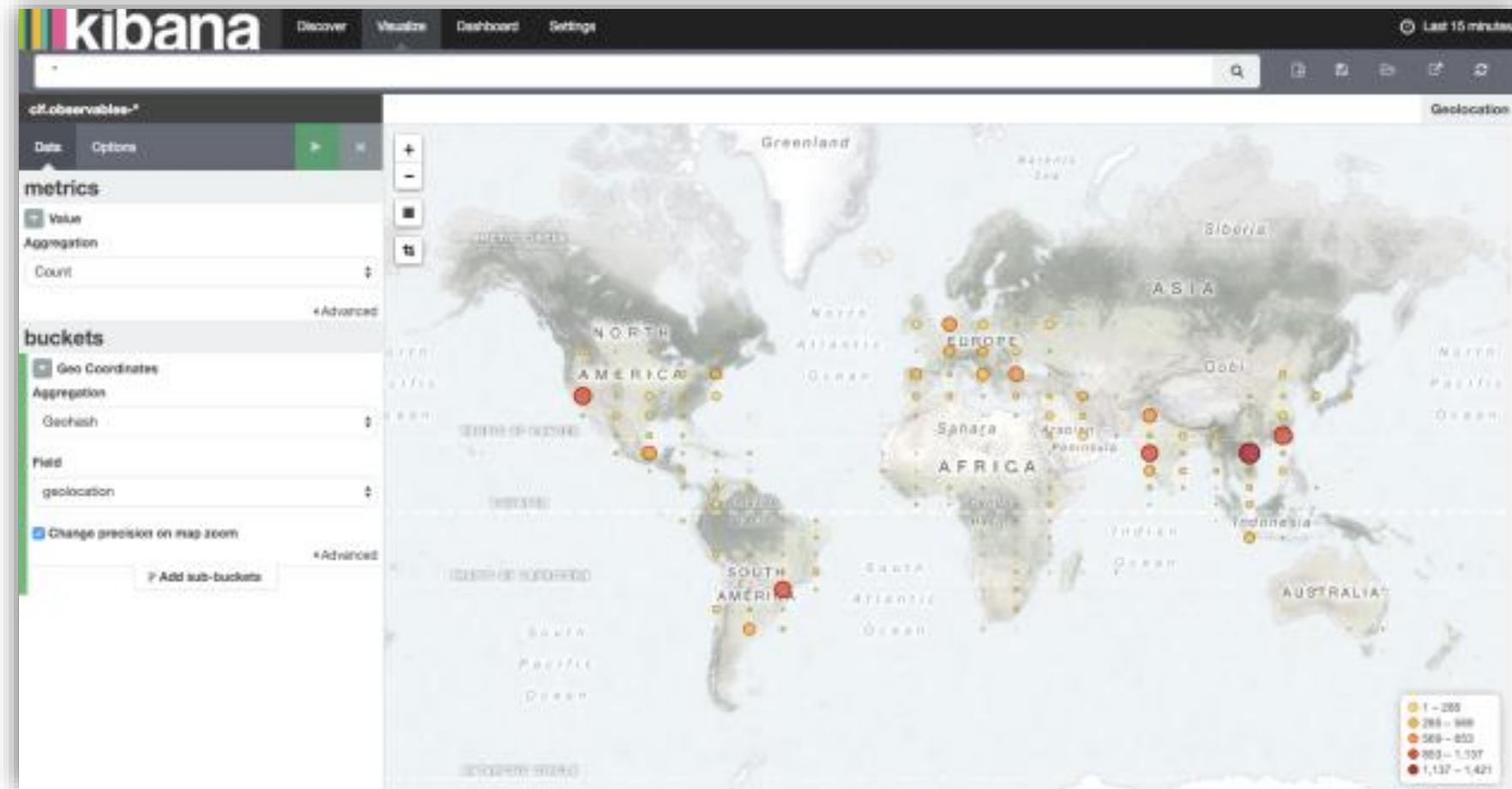


Collective Intelligence Framework (CIF)





Collective Intelligence Framework (CIF)





Collective Intelligence Framework (CIF)

local.kibana.gareth.threat.dashboard

Google

BOTNET IPS

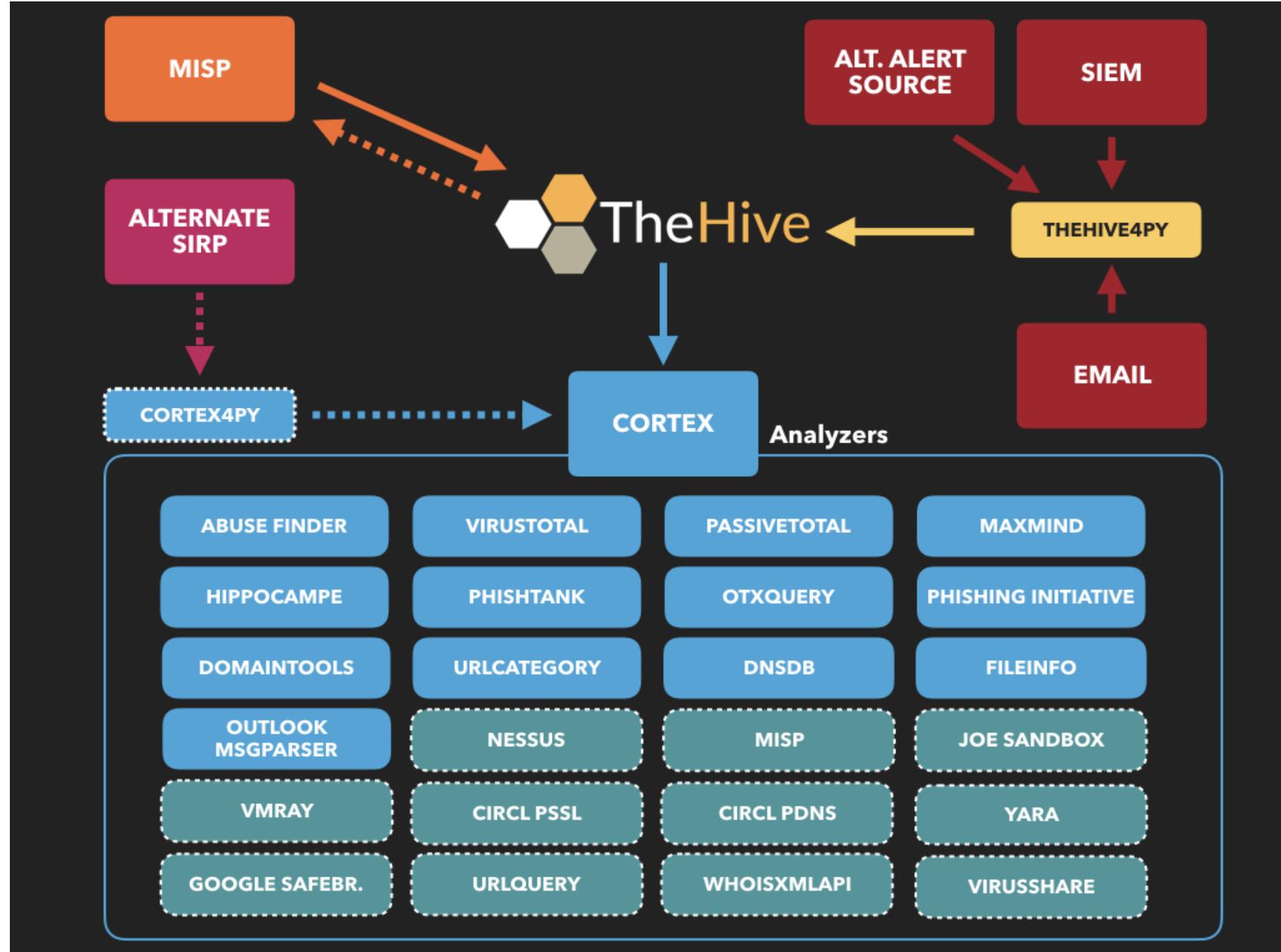
MALICIOUS IPS

MALWARE DISTRIBUTION

TABLE

200 to 300 of 500 available for paging

source	source_info	severity	country	country_code	data_type	feed_src
117.26.220.178	117.26.220.178	high	China	CN	botnet	BlocklistDE_Botnet
117.26.192.65	117.26.192.65	high	China	CN	botnet	BlocklistDE_Botnet
117.26.119.74	117.26.119.74	high	China	CN	botnet	BlocklistDE_Botnet
117.26.118.251	117.26.118.251	high	China	CN	botnet	BlocklistDE_Botnet
117.177.78.114	117.177.78.114	high	China	CN	botnet	BlocklistDE_Botnet
117.177.249.253	117.177.249.253	high	China	CN	botnet	BlocklistDE_Botnet
117.177.249.131	117.177.249.131	high	China	CN	botnet	BlocklistDE_Botnet
117.175.194.237	117.175.194.237	high	China	CN	botnet	BlocklistDE_Botnet
117.175.109.130	117.175.109.130	high	China	CN	botnet	BlocklistDE_Botnet





Example of Digital Forensic Tools



Digital Forensic Tools



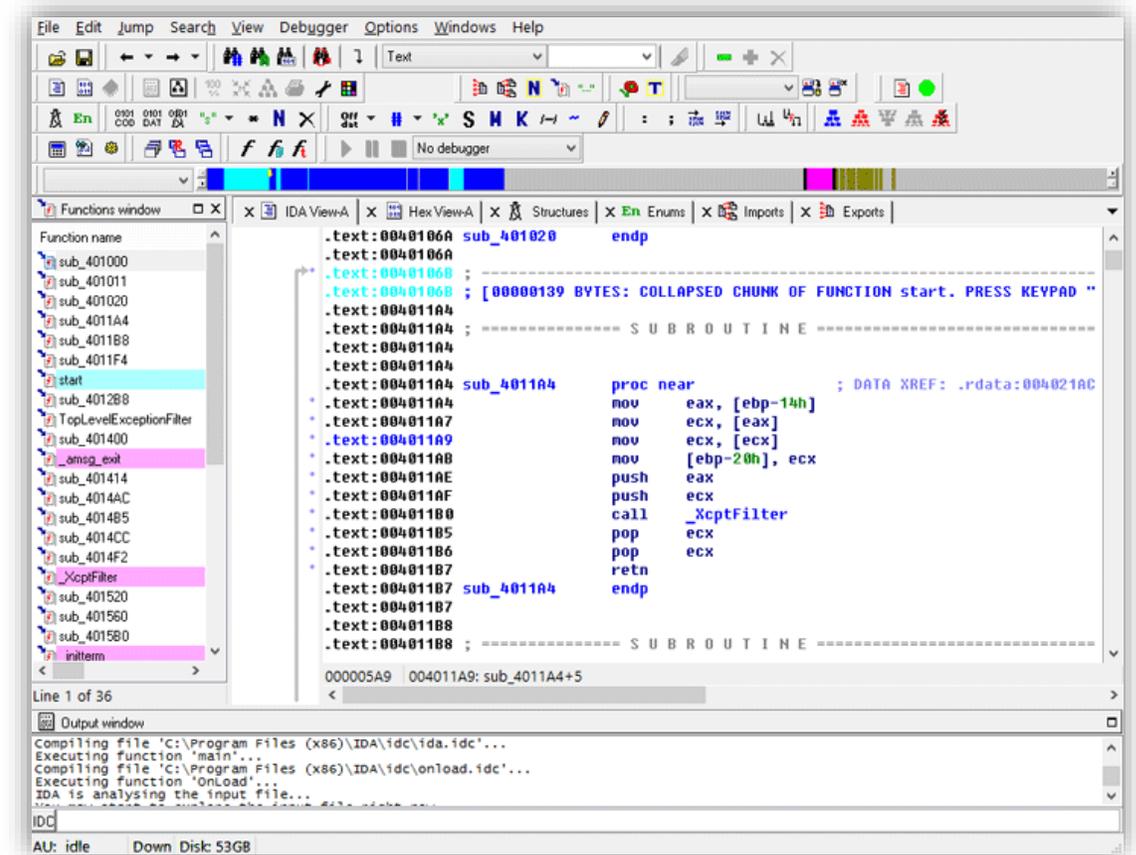
REMnux: A Linux Toolkit for Reverse-Engineering and Analyzing Malware



MALWARE AND MEMORY FORENSICS



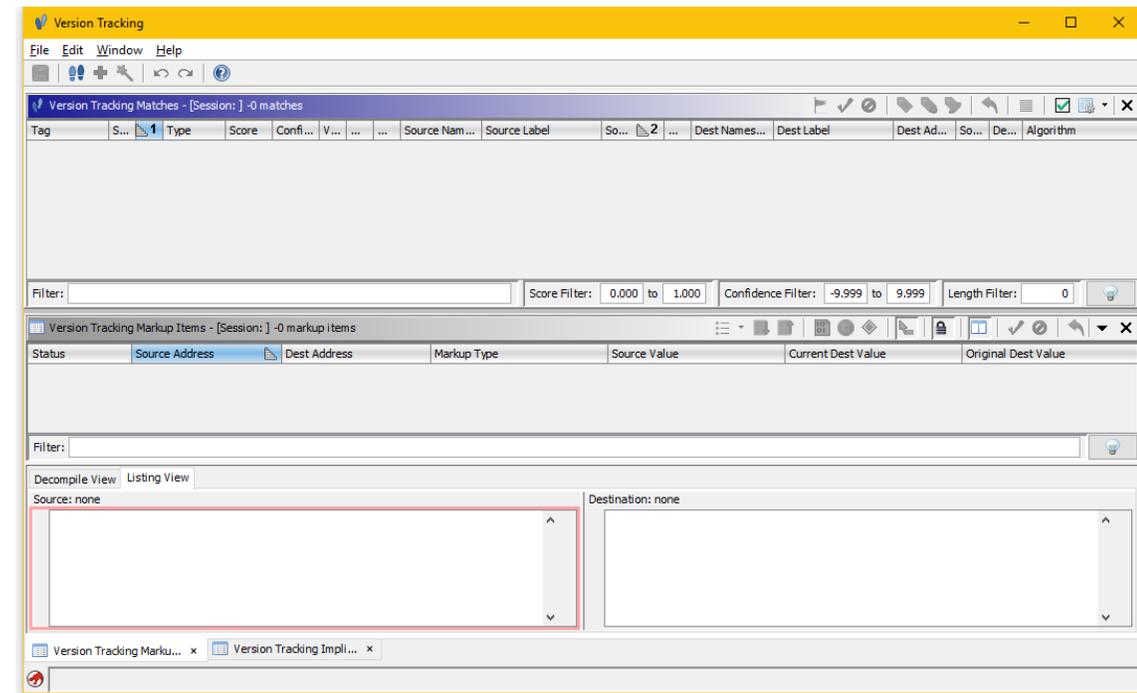
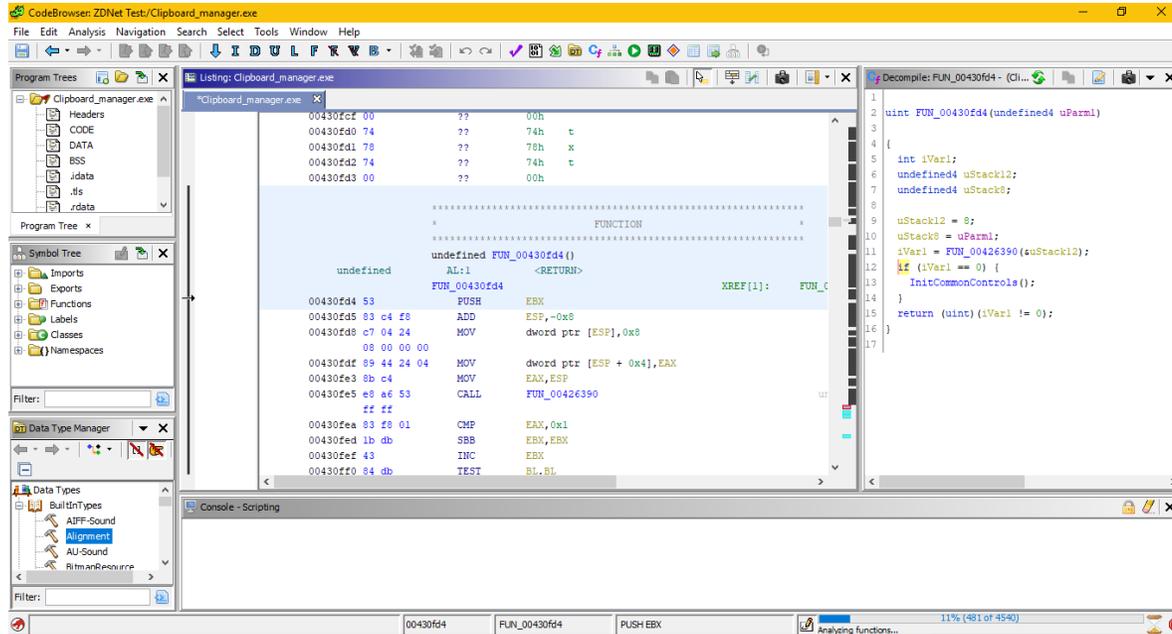
The Interactive Disassembler (IDA)



<https://www.hex-rays.com>



GHIDRA open source reverse engineering tool





Digital Forensic Tools

Cuckoo Sandbox is a malware analysis system.



VirusTotal is a free service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

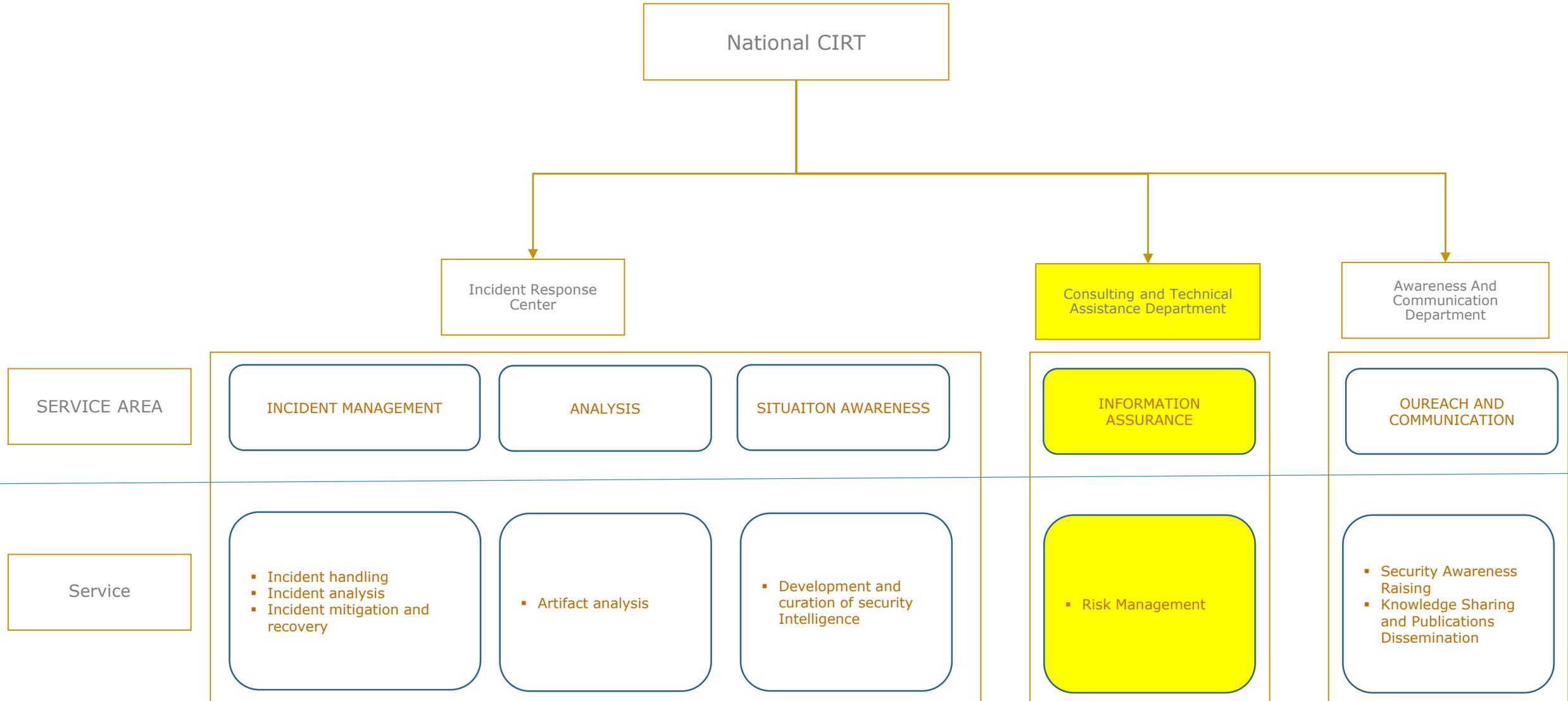


Malwr : Automated Malware Analysis Sandboxes and Services





The Basic Services Offered by a CSIRT/SOC





Example of Security Assessment tools



Security Assessment tools



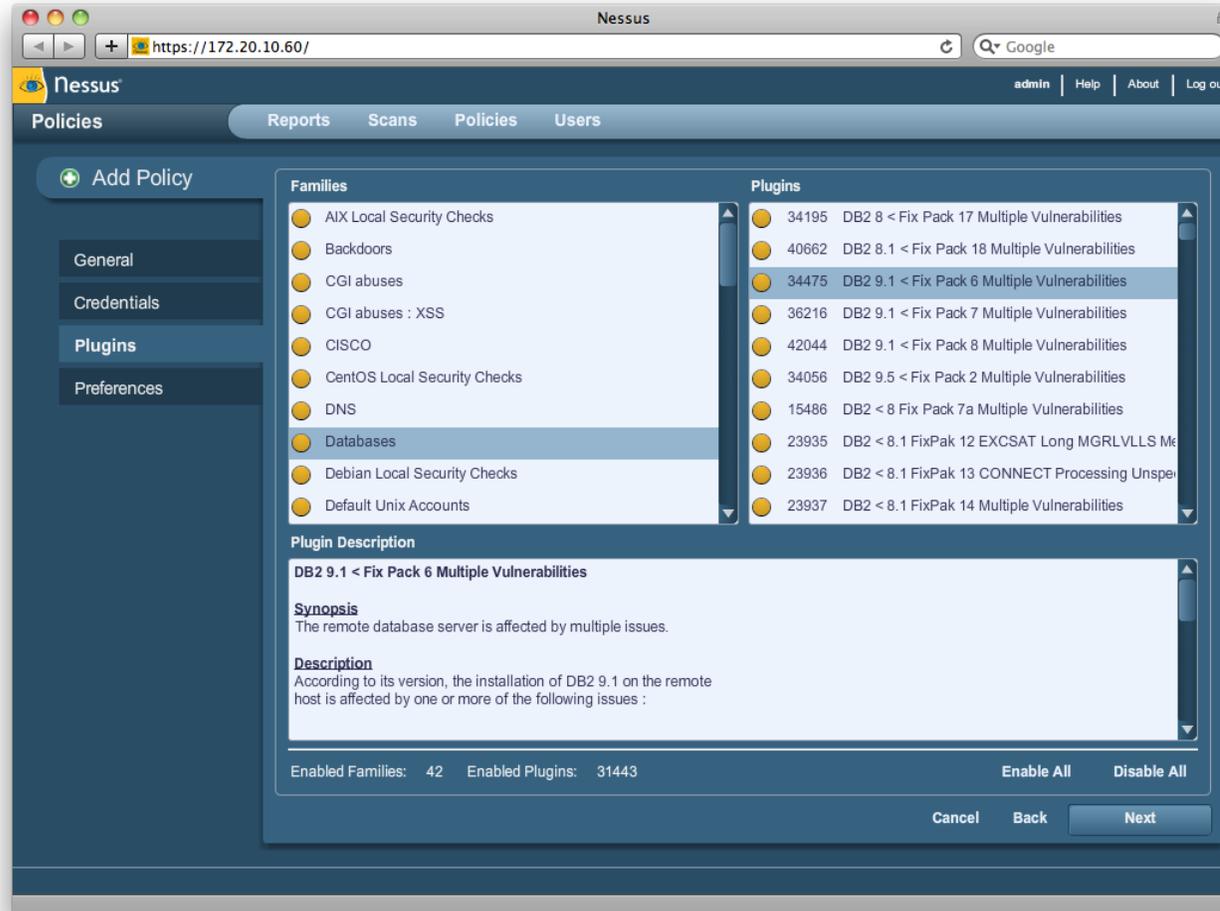
```
Applications Places Tue Aug 12, 4:21 PM root
root@vineet:~# aircrack-ng -l 0 -a 00:1E:58:85:88:18 -h 00:1E:58:85:88:18
16:01:06 Waiting for beacon from 00:1E:58:85:88:18
16:01:06 Sending Authentication request to 00:1E:58:85:88:18
16:01:06 Authentication successful
16:01:06 Sending Association Request to 00:1E:58:85:88:18
16:01:06 Association successful
root@vineet:~# aircrack-ng -l 0 -a 00:1E:58:85:88:18 -h 00:1E:58:85:88:18
16:02:08 Waiting for beacon from 00:1E:58:85:88:18
Saving ARP requests in replay mode
*Captured 412601 packets (got 999999)
root@vineet:~#

File Edit View Search Terminal Help
BSSID PWR RXQ Bea Elapsed: 23 mins 11:24:13.2 ms
00:1E:58:85:88:18 -73 3 64 bytes from kul01s07-in-f0.1e100.net (173.194.126.0): icmp_req=18 ttl=128 time=94.1 ms
00:1E:58:85:88:18 -73 3 64 bytes from kul01s07-in-f0.1e100.net (173.194.126.0): icmp_req=19 ttl=128 time=92.2 ms
00:1E:58:85:88:18 -73 3 64 bytes from kul01s07-in-f0.1e100.net (173.194.126.0): icmp_req=20 ttl=128 time=92.9 ms
00:1E:58:85:88:18 -73 3 64 bytes from kul01s07-in-f0.1e100.net (173.194.126.0): icmp_req=21 ttl=128 time=92.5 ms
00:1E:58:85:88:18 -73 3 64 bytes from kul01s07-in-f0.1e100.net (173.194.126.0): icmp_req=22 ttl=128 time=93.8 ms
00:1E:58:85:88:18 -73 3 64 bytes from kul01s07-in-f0.1e100.net (173.194.126.0): icmp_req=23 ttl=128 time=93.8 ms
00:1E:58:85:88:18 -73 3 64 bytes from kul01s07-in-f0.1e100.net (173.194.126.0): icmp_req=24 ttl=128 time=92.8 ms
00:1E:58:85:88:18 -73 3 64 bytes from kul01s07-in-f0.1e100.net (173.194.126.0): icmp_req=25 ttl=128 time=92.8 ms
00:1E:58:85:88:18 -73 3 64 bytes from kul01s07-in-f0.1e100.net (173.194.126.0): icmp_req=26 ttl=128 time=96.9 ms
00:1E:58:85:88:18 -73 3 64 bytes from kul01s07-in-f0.1e100.net (173.194.126.0): icmp_req=27 ttl=128 time=97.8 ms
00:1E:58:85:88:18 -73 3 64 bytes from kul01s07-in-f0.1e100.net (173.194.126.0): icmp_req=28 ttl=128 time=93.2 ms
00:1E:58:85:88:18 -73 3 64 bytes from kul01s07-in-f0.1e100.net (173.194.126.0): icmp_req=29 ttl=128 time=93.2 ms
```

www.kali.org



Security Assessment tools



<https://www.tenable.com/>





static code analysis

path / file: subdirs windows

verbosity level: 1. user tainted only vuln type: All server-side scan files user input

code style: ayti bottom-up /regex/ search stats functions

RIPS 0.52

File: D:\cipher3\timeclock\work.php

SQL Injection

- Userinput reaches sensitive sink. (Blind exploitation)
 - 26: `mysql_query mysql_query($command); // html_ar`
 - 25: `function system_($command)`
- Userinput is passed through function parameters.
 - 162: `$result = system_ ("SELECT id,start FROM t`
 - 113: `$userid = (int)$_SESSION['Userid']; //`
 - 107: `function insert_project_into_database`
- Userinput is passed through function parameters.
 - 18: `insert project into database ($_POST['projec`

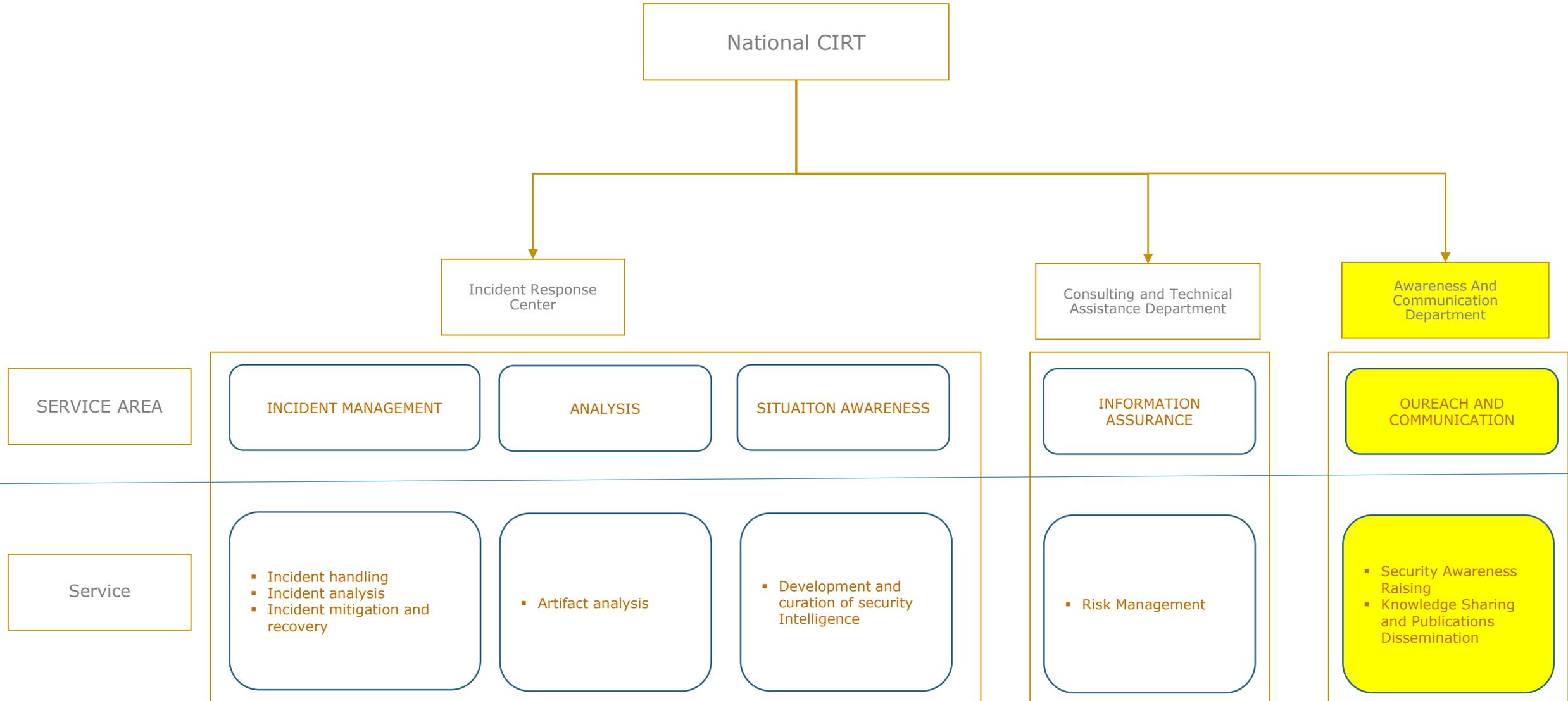
CodeViewer - D:\cipher3\timeclock\work_functions.php

```
154     }
155     else{
156         if($act_status != "working"){
157             html_error("Cipher - time clock - Error","You haven't start a project. Please <a href
158         }
159     } else{
160         $state = "stopped";
161         $enddate = date("Y.m.d H:i:s");
162         $result = system_ ("SELECT id,start FROM timeclock WHERE employee=$userid
163     }
164     if(!$result){
165         html_error("Cipher - time clock - Database error","Can't get the id of the las
166     }
167     if(system_($result) == 0){
168         html_error("Cipher - time clock - Error","The project you have specified has
169     }
170     if(system_($result) >1){
171         while($row=mysql_fetch_array($result)){
172             $id = $row["id"];
173         }
174     }
```

rips-scanner.sourceforge.net/



The Basic Services Offered by a CSIRT/SOC





Example of Alerts, Warnings and Announcements Tools



Alerts, Warnings and Announcements Tools

<https://www.phplist.com/>

Taranis architecture

Tracking, analyzing and describing threats and vulnerabilities

