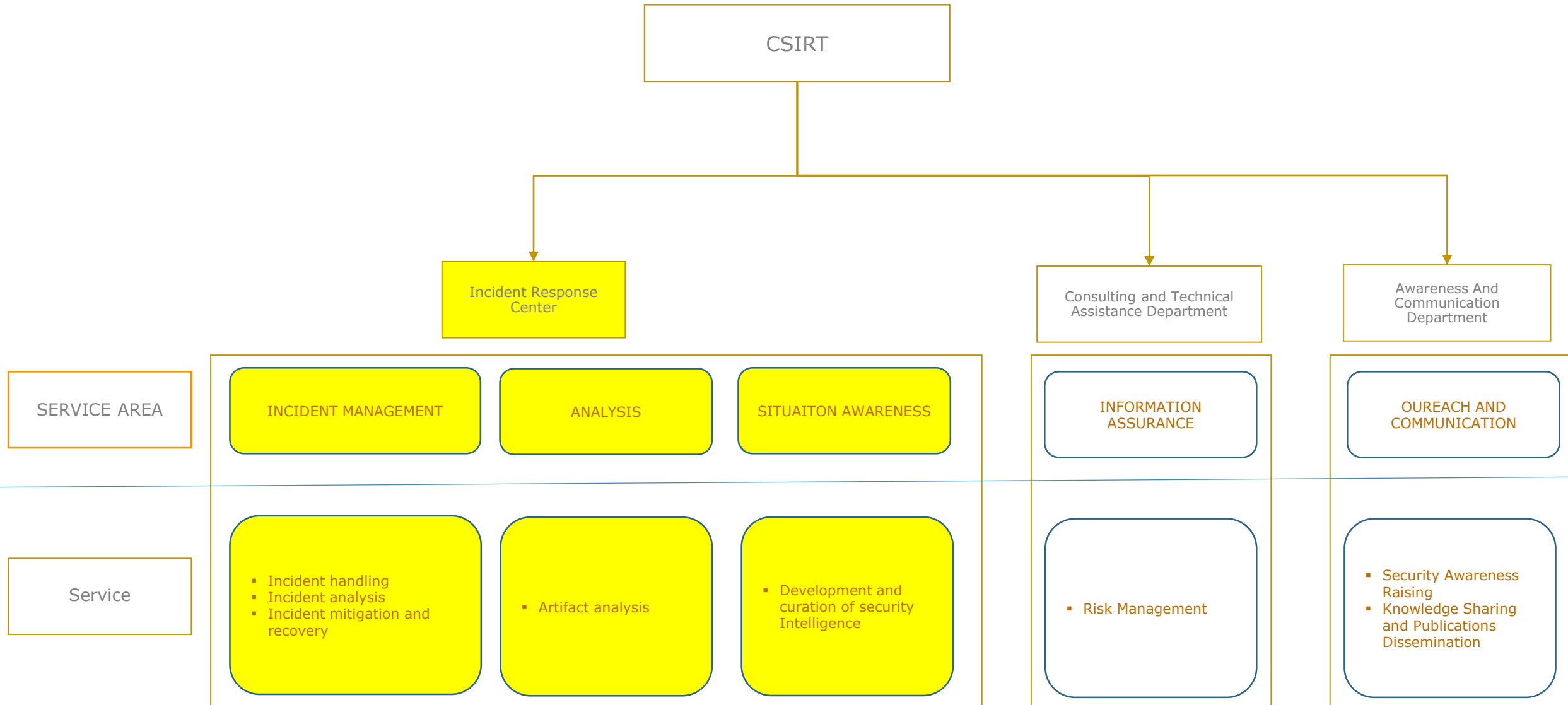




How to Build a CIRT based on open Source Tools

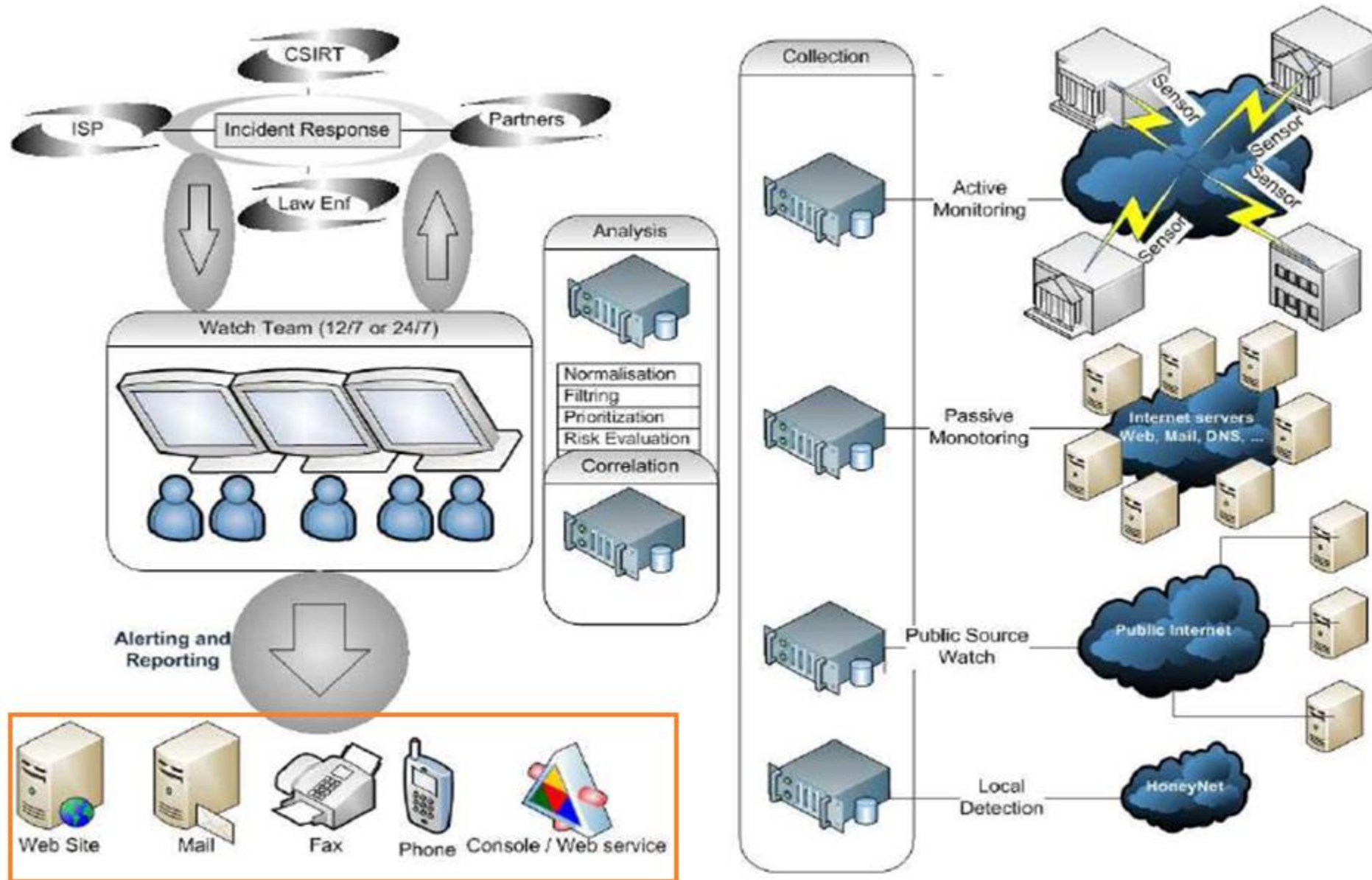


The Basic Services Offered by a CSIRT/SOC





Incident Response Center

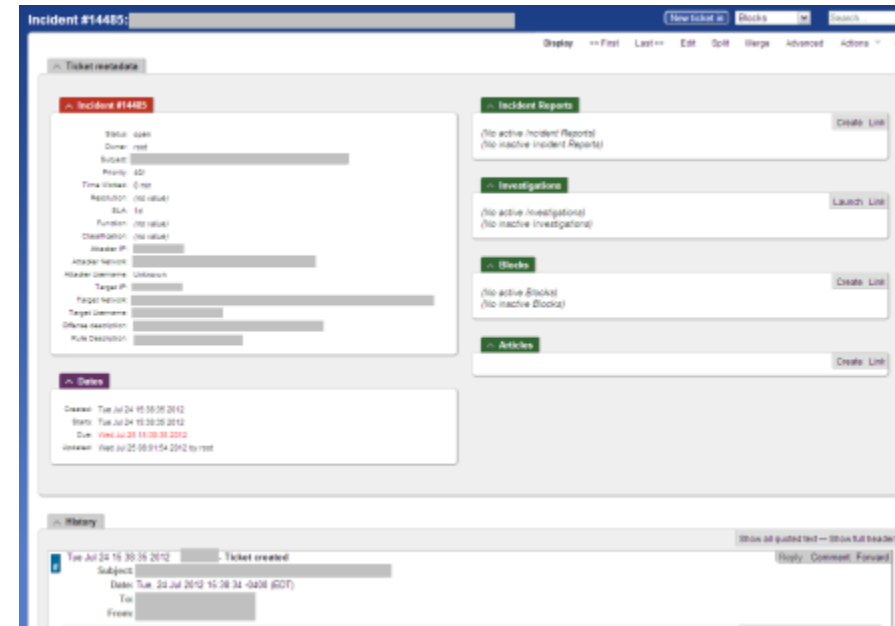
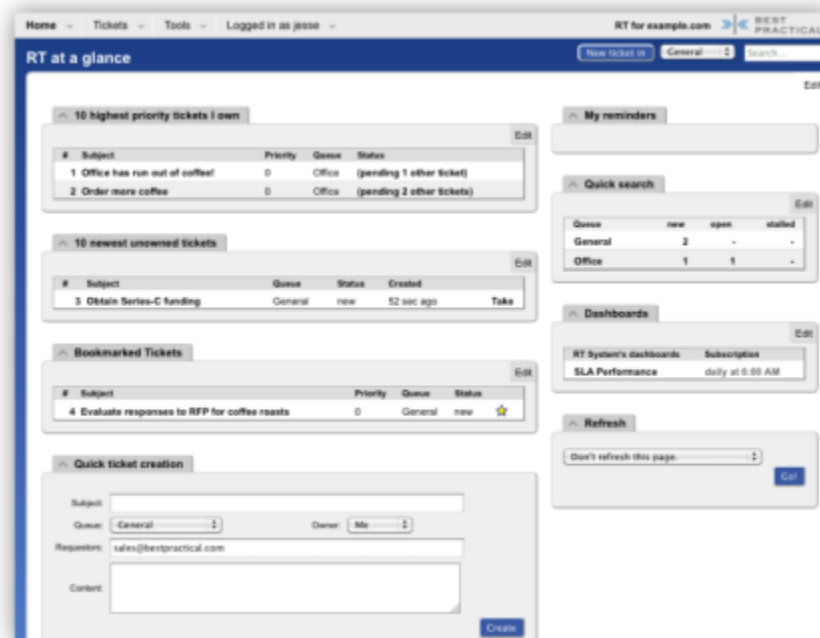




Alerting and Reporting

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.





Alerting and Reporting



Open Technology Real Services (OTRS)

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

The screenshot shows the OTRS Dashboard. At the top, there's a navigation bar with 'Dashboard', 'Customers', 'Tickets', 'FAQ', and 'Statistics'. Below this, a red banner states 'Scheduler is not running. Please contact your administrator!'. The main content area is divided into several sections: 'Dashboard' with a 7-day status graph, 'Escalated Tickets' table, 'New Tickets' table, 'Open Tickets / Need to be answered' table, and 'Ticket Queue Overview' table. A sidebar on the right contains 'Settings', 'Upcoming Events', and 'Latest updated FAQ articles'.

Dashboard

The screenshot shows the OTRS Tickets page for a specific ticket. The navigation bar is the same as the dashboard. A red banner at the top says 'Scheduler is not running. Please contact your administrator!'. The main content area shows 'Ticket#201311102000087 - Internet connection problem'. It includes a 'Ticket Information' sidebar with details like State (open), Priority (4 high), and CustomerID. The main content area shows the ticket details, including the subject 'Internet connection problem', the description 'Mrs. Saha have problem with internet connection...', and the contact information for Susi Smith. The bottom of the page shows 'Powered by OTRS 3.3.6 build4' and 'Top of page'.

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 [Add New Custom Form](#)

Showing 0 forms

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 **emphasis** 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](#) [Diagnose](#)

Email Template Message - osTicket Default Template (HTML)

Message Template: [Go](#)

Message Subject: Email message subject

Message Body: Email message body

We Hear You

Dear .

We received your request and assigned ticket #.

Topic:
Subject:
Submitted:

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

Your Team,

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](#)

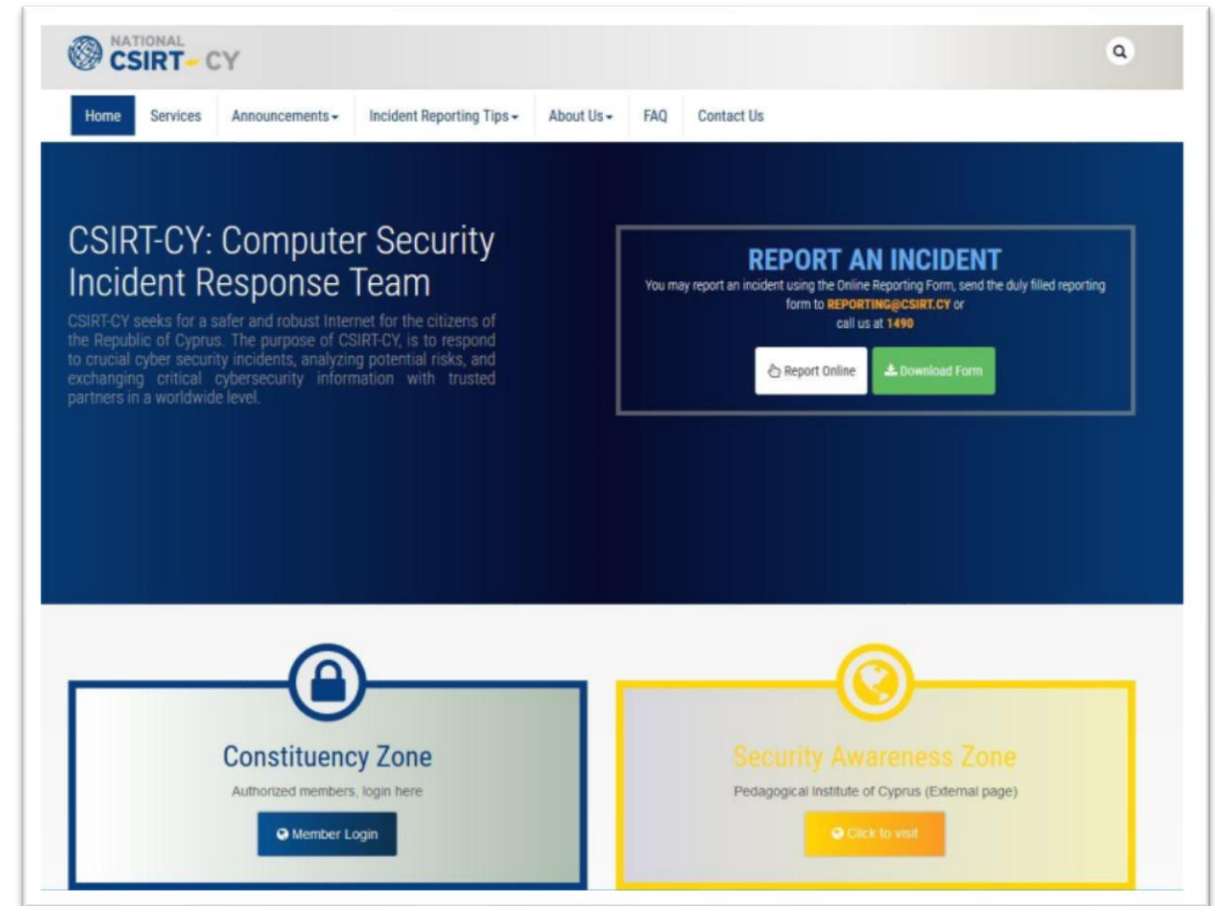
Auto responder



Alerting and Reporting

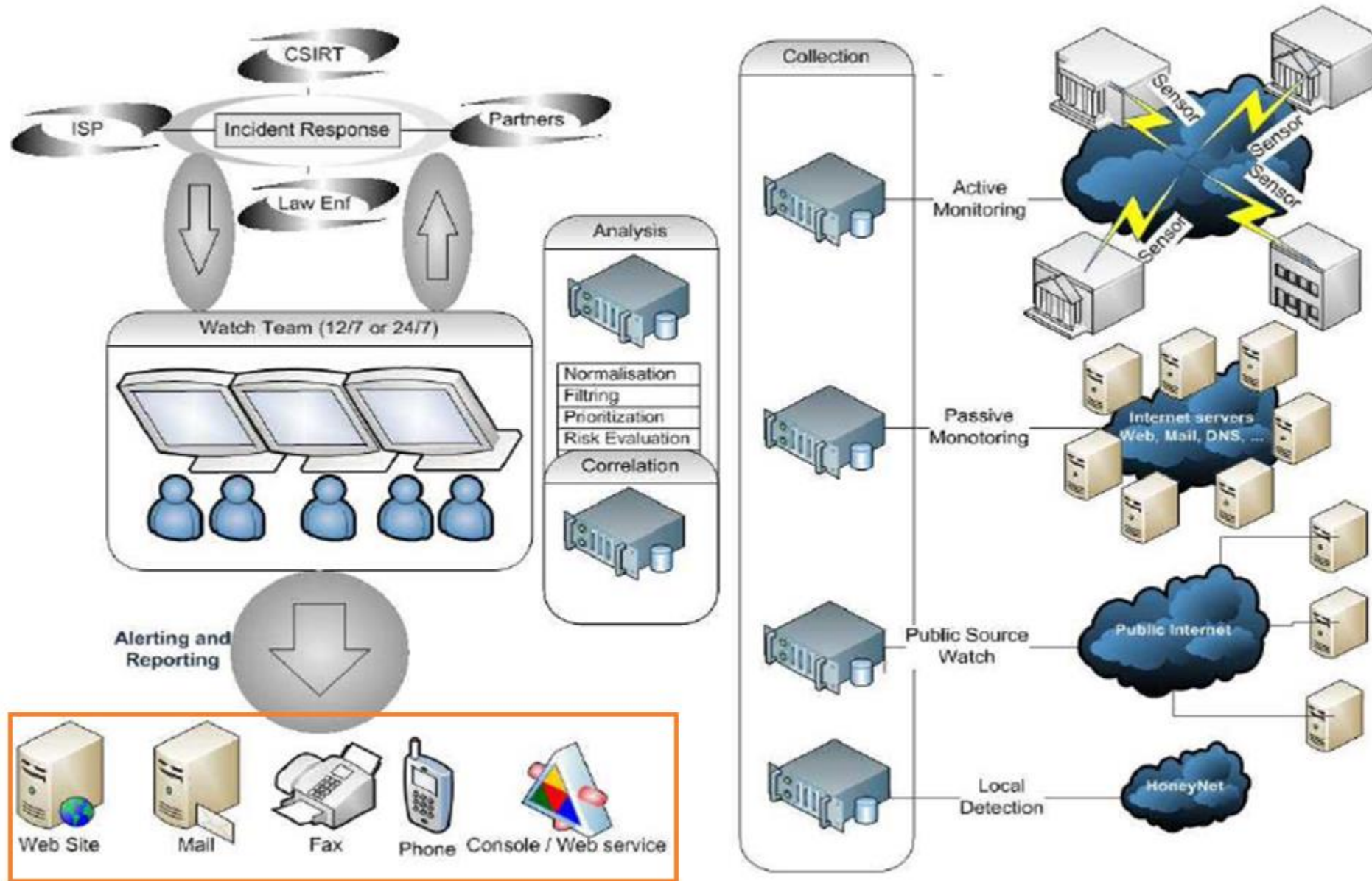
CSIRT Portal

- 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.



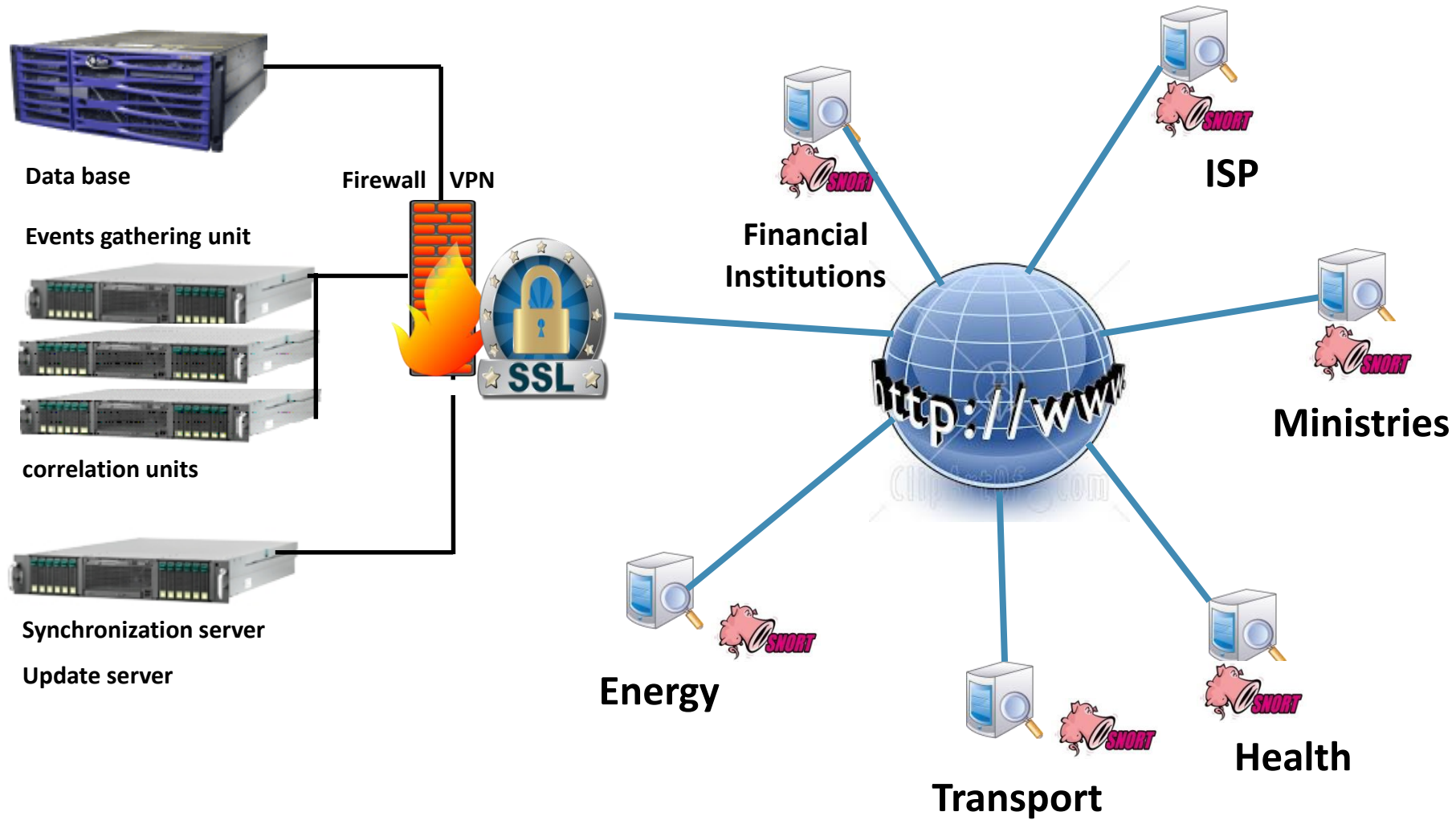


Incident Response Center





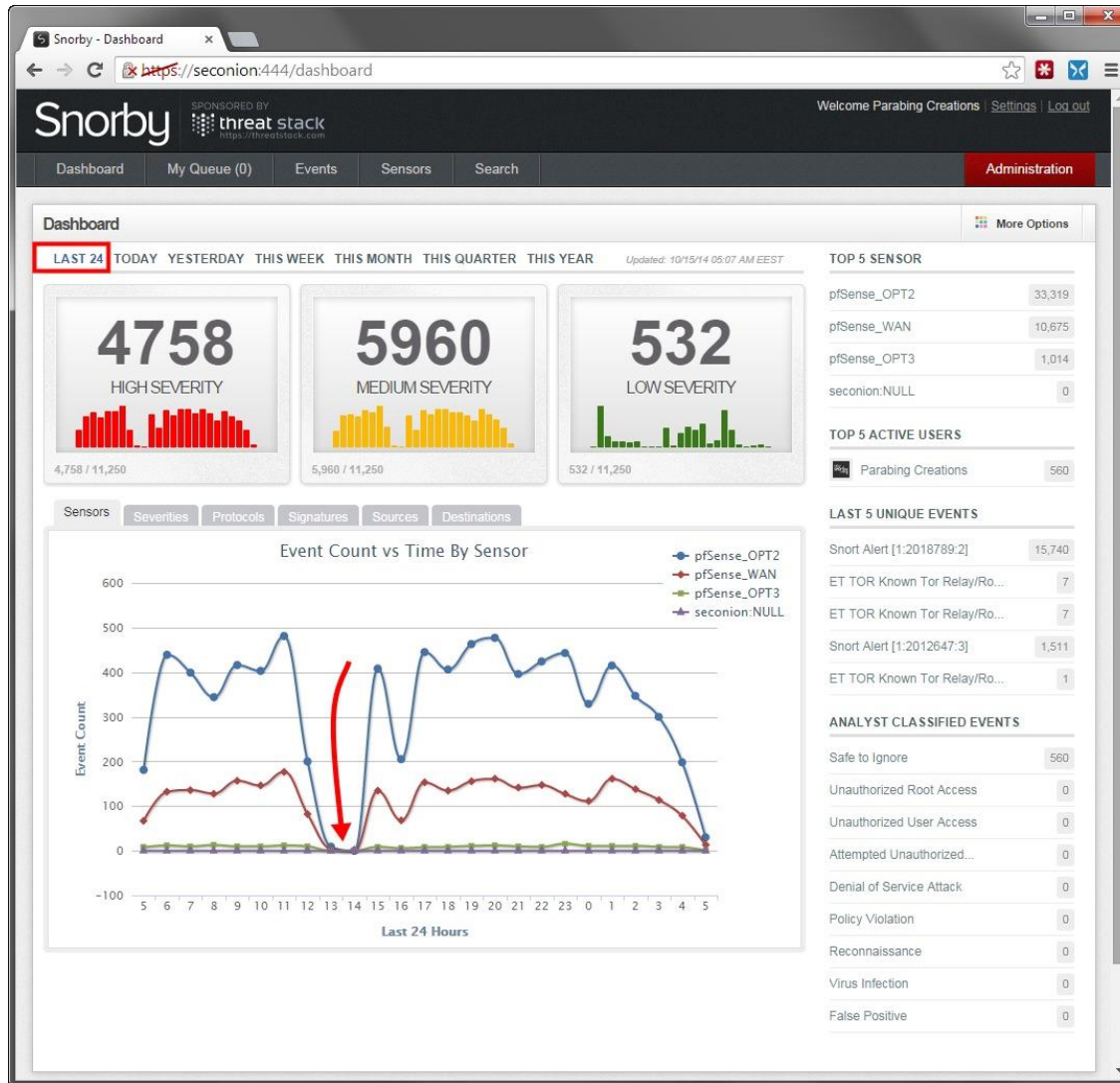
Active Monitoring





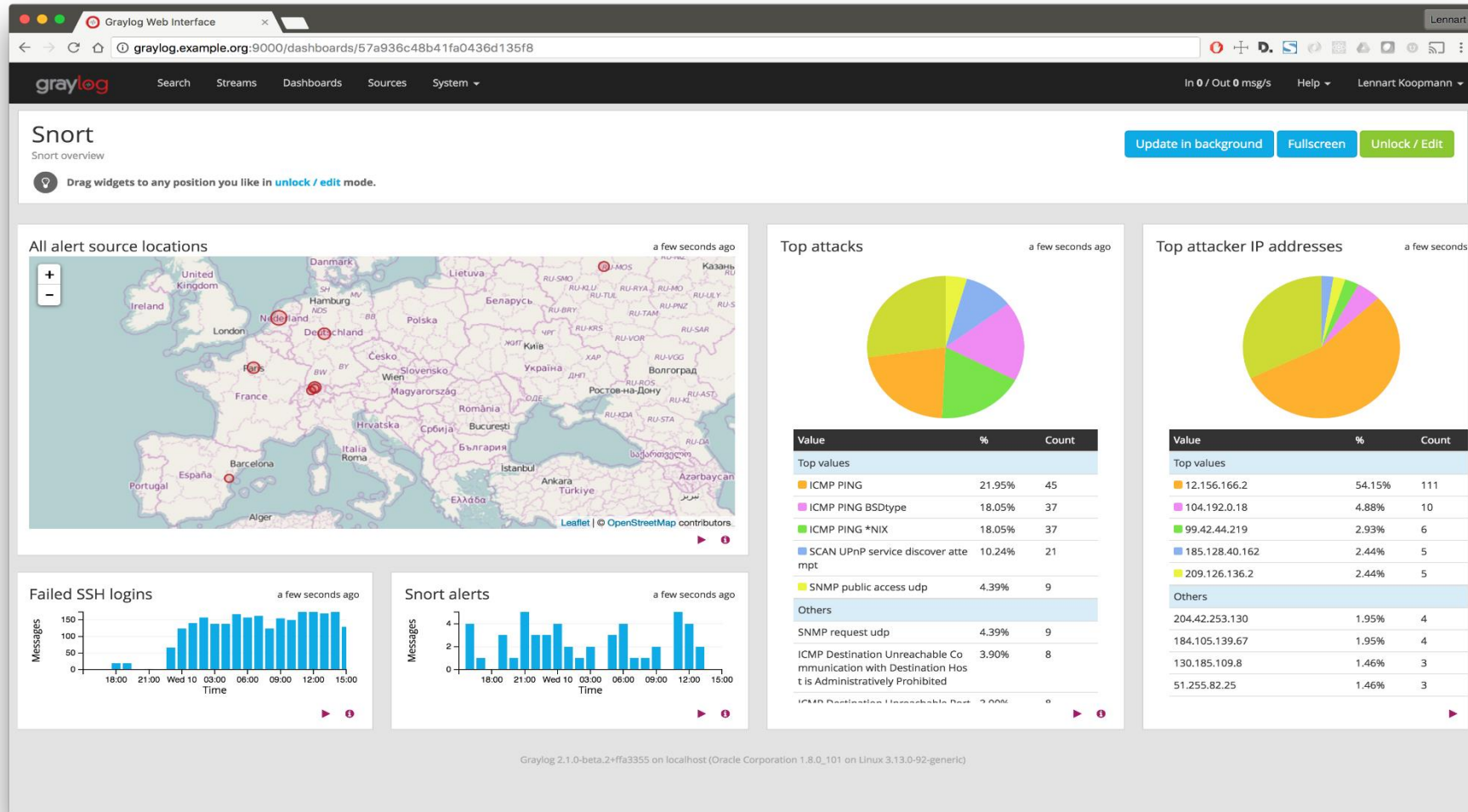
Active Monitoring

<https://github.com/Snorby>



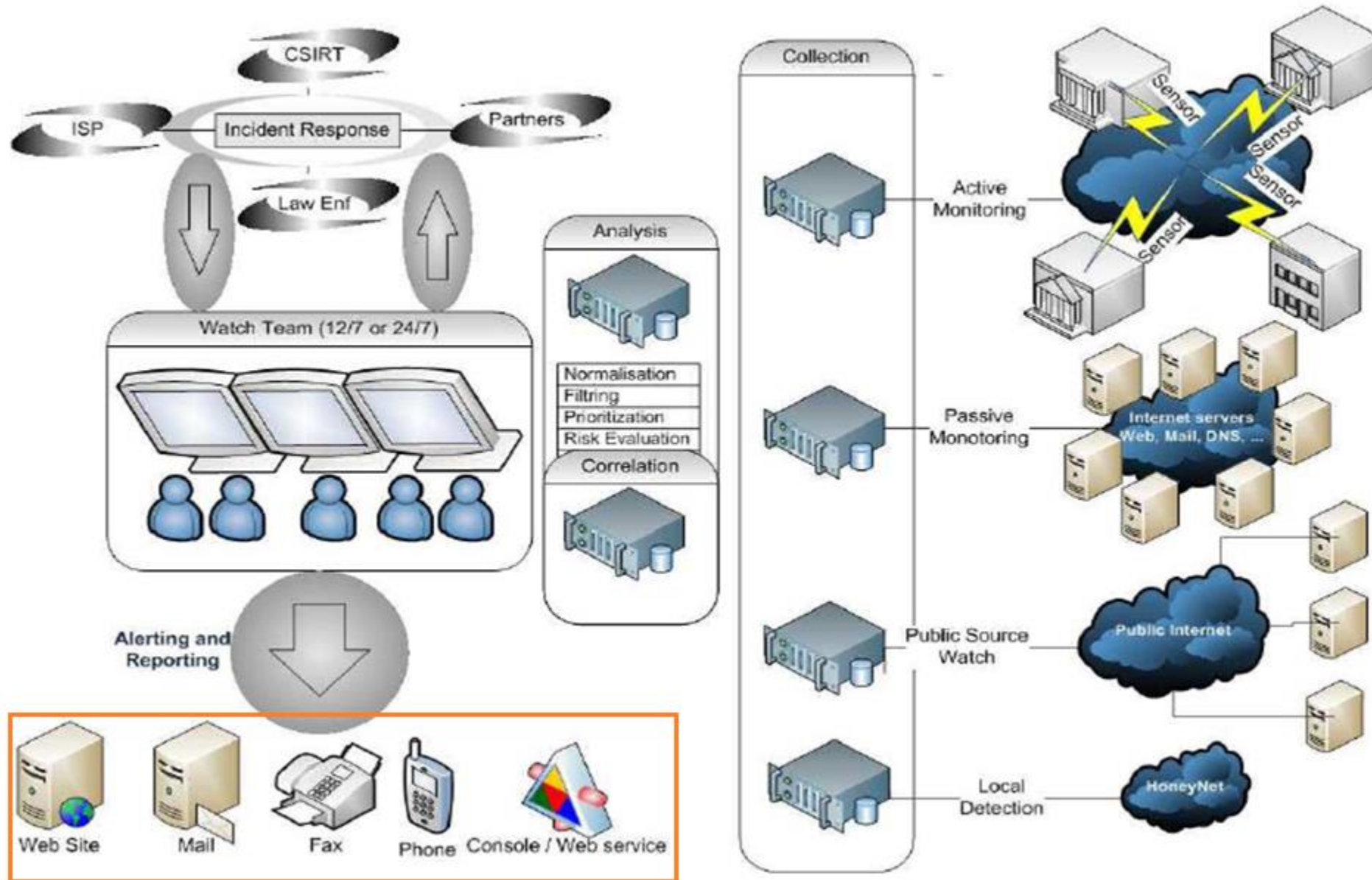


Active Monitoring



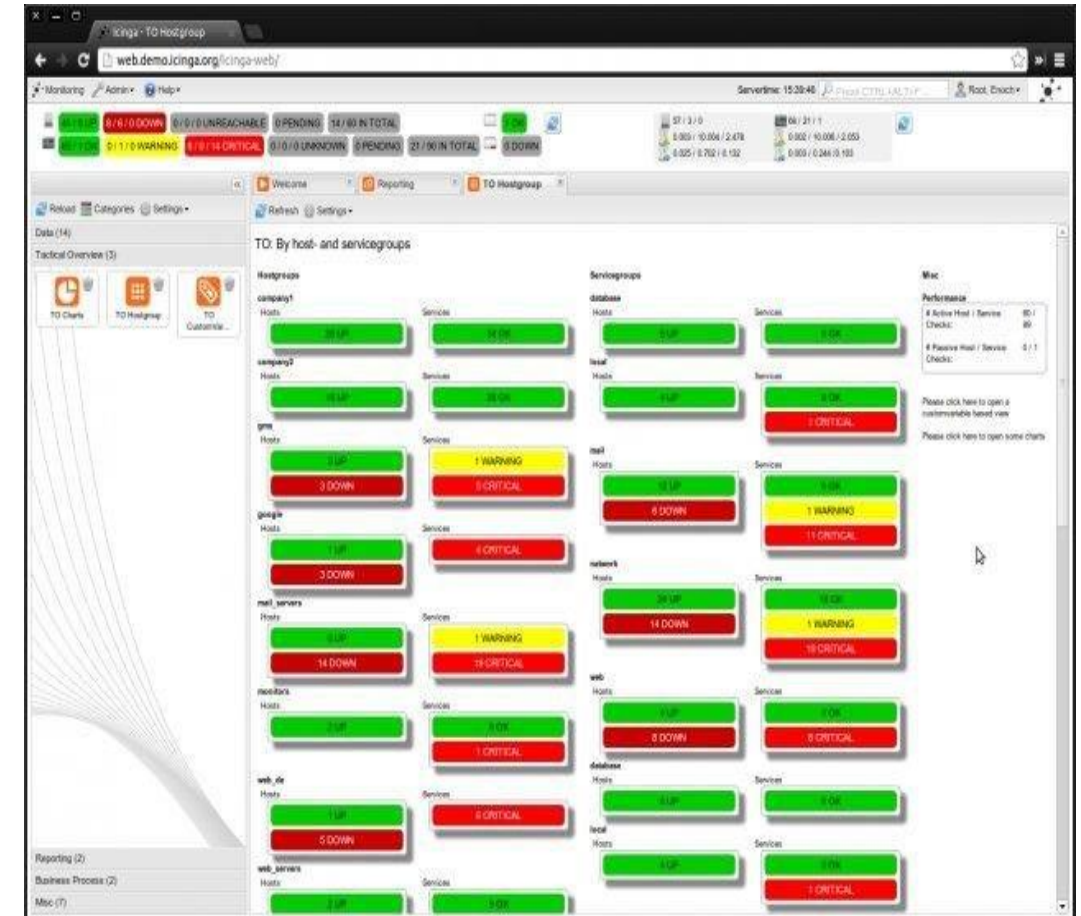


Incident Response Center



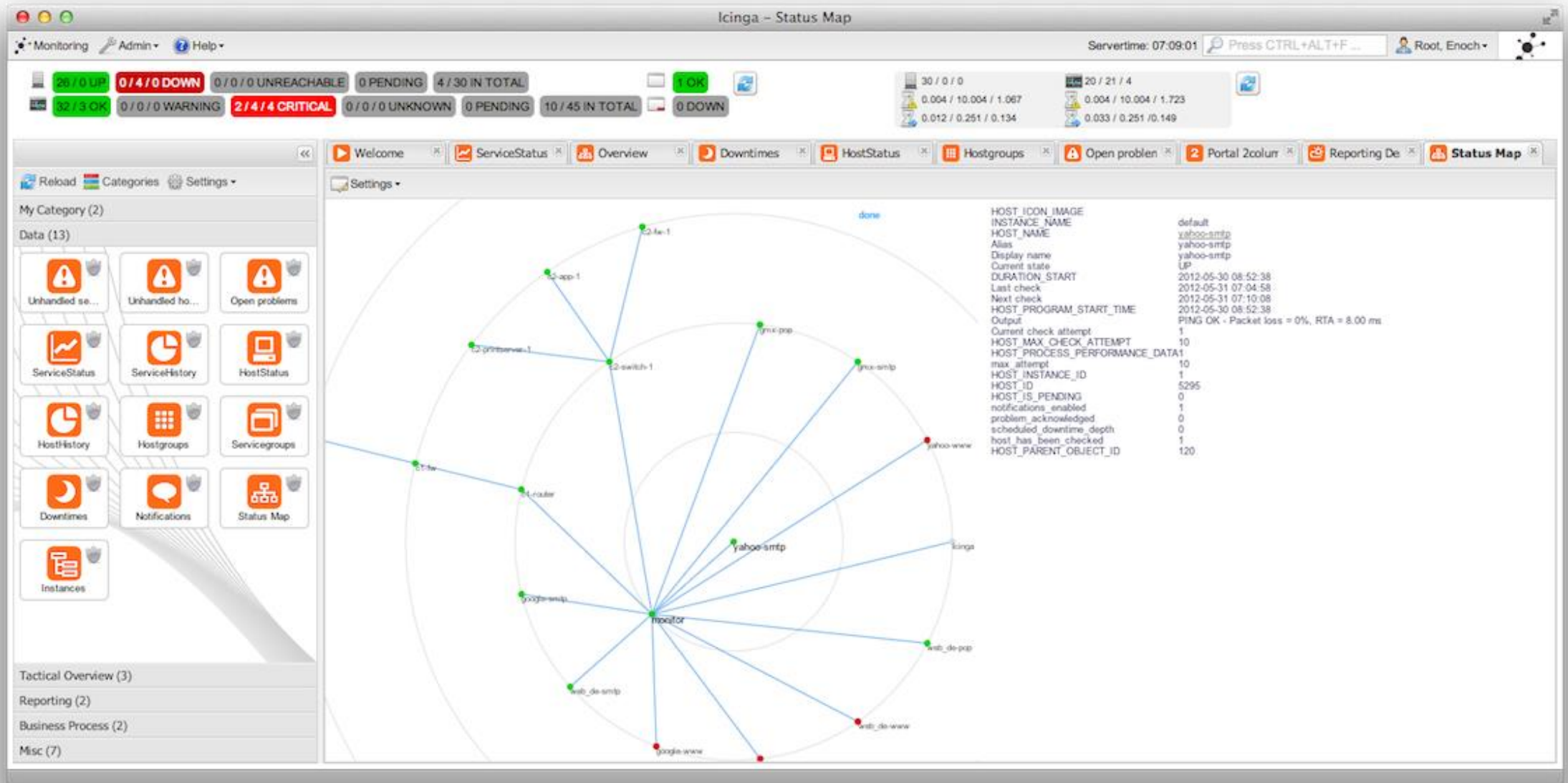


Passive Monitoring





Passive Monitoring





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

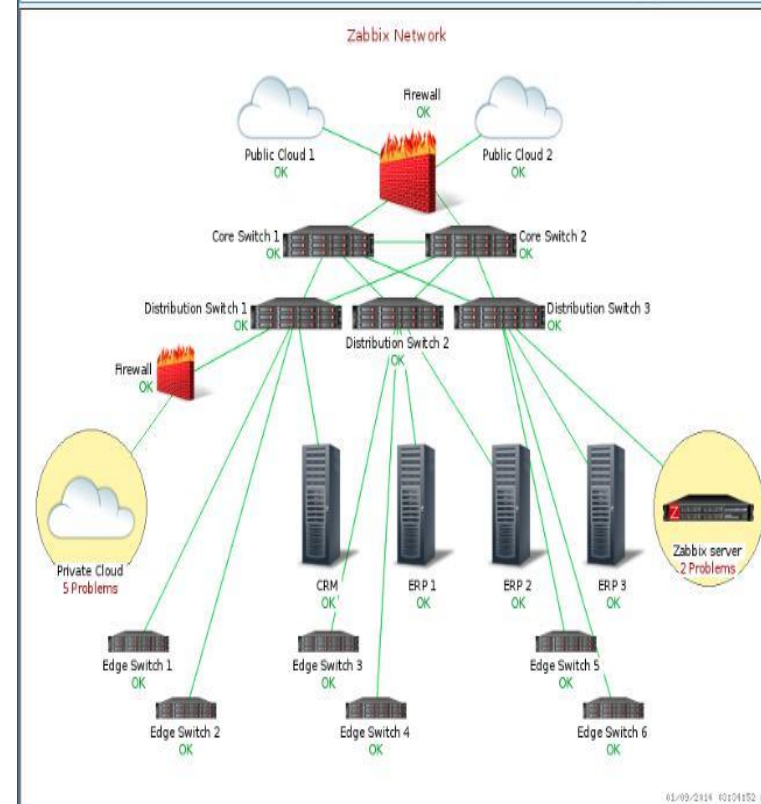
Dashboard Overview Web Latest data Triggers Events Graphs Screens Maps Discovery IT services

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

NETWORK MAPS

Zabbix Network

Maps Zabbix Network Minimum severity Not classified (default)

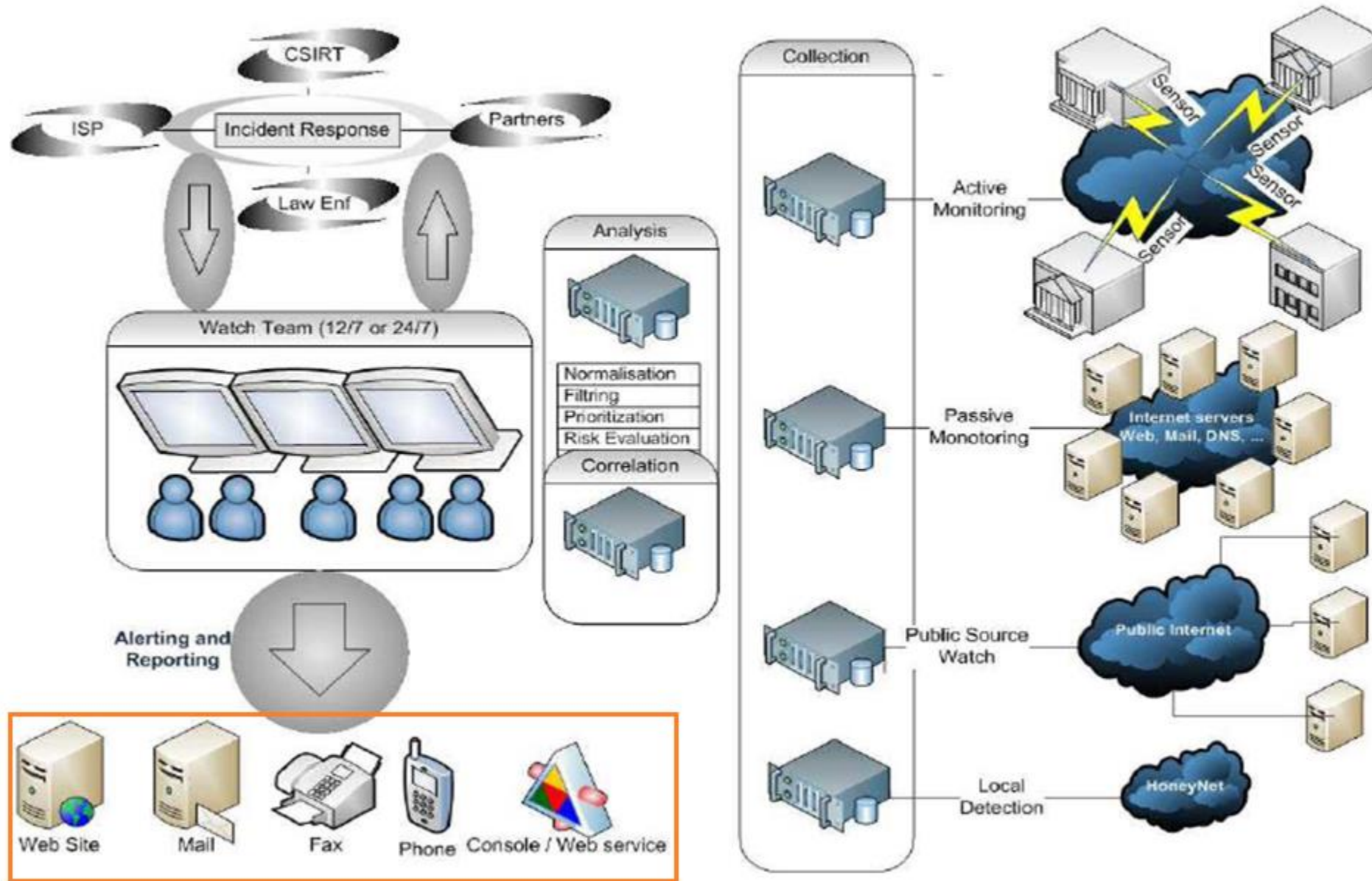


Zabbix 2.2.0 Copyright 2001-2013 by Zabbix SIA

Connected as 'Admin'



Incident Response Center





Public Feeds

Malwares infections, C&C servers , malicious IPS

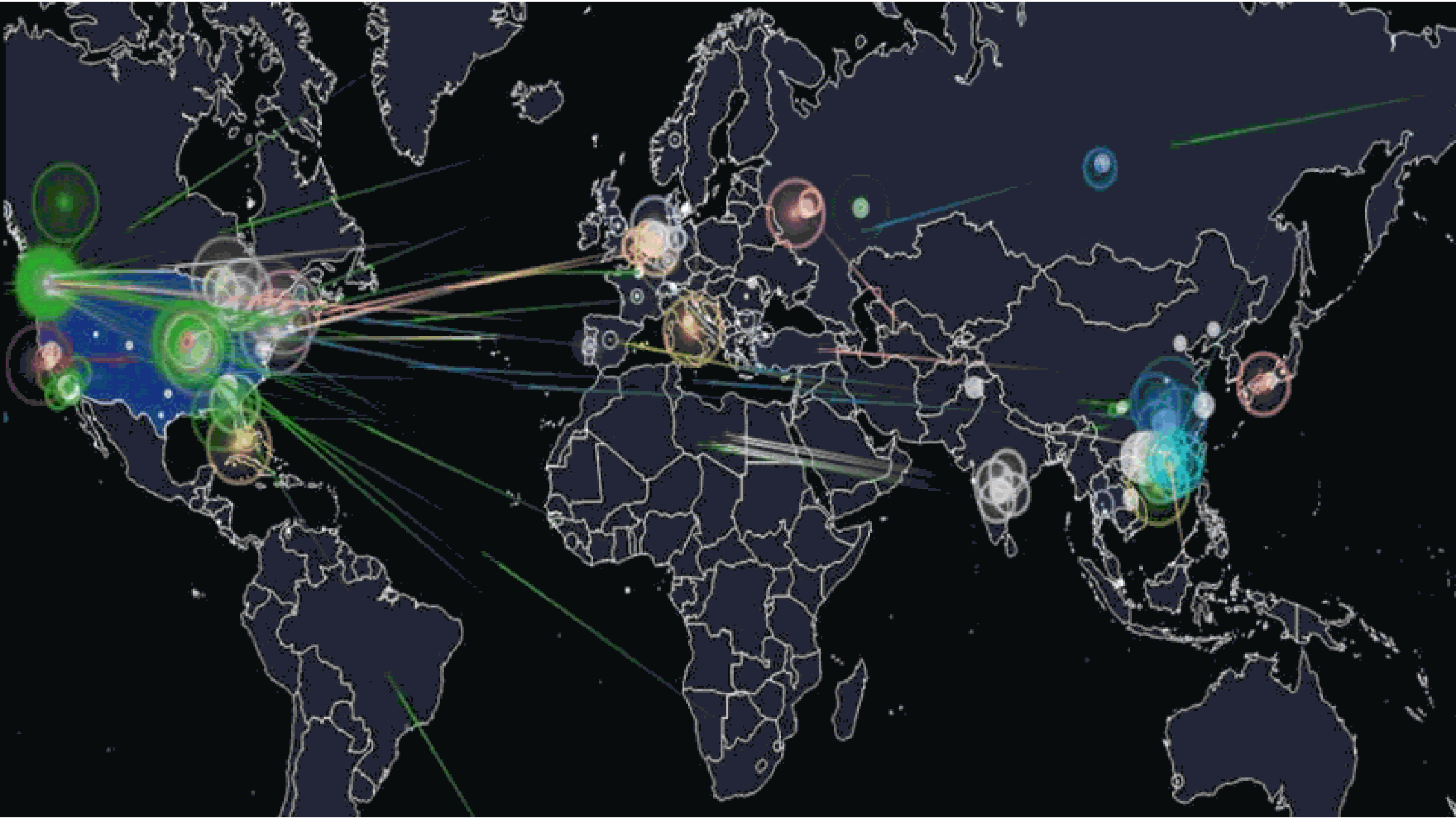
<http://danger.rulez.sk/index.php/bruteforceblocker/>
<http://www.senderbase.org>
<http://www.malwaredomains.com>
<https://feodotracker.abuse.ch/>
<https://hosts-file.net/rss.asp>
<http://malc0de.com/rss/>
<http://www.malwaredomainlist.com/mdlcsv.php>
<http://www.malwaredomainlist.com/updatescsv.php>
<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.ipspamlst.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 

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 Al		M			 biomasscon.uplb.edu.ph/anoncod...	Linux	mirror
2016/01/04	Unknown Al		M			 dche.uplb.edu.ph/anoncoders.htm	Linux	mirror
2016/01/04	Unknown Al		M			 des.uplb.edu.ph/anoncoders.htm	Linux	mirror



Public Feeds

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

PhishTank > Search by ASN

www.phishtank.com/asn_search.php?asn=9821&valid=All&active=y&Search=Search

PhishTank is operated by [OpenDNS](#), a free service that makes your Internet safer, faster, and smarter. [Get started today!](#)

PhishTank® Out of the Net, into the Tank.

username Sign In
[Register](#) | [Forgot Password](#)

Home Add A Phish Verify A Phish **Phish Search** Stats FAQ Developers Mailing Lists My Account

[Phish Archive](#) [Search by Targeted Brand](#) Search by ASN

Search by ASN : DOST-PH-AP Department of Science and Technology,PH (?) [RSS](#)

ASN: ([ASN Lookup](#)) Valid? Online?

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

[Friends of PhishTank](#) | [Terms of Use](#) | [Privacy](#) | [Contact](#)
PhishTank is operated by [OpenDNS](#). Learn more about [PhishTank](#) or [OpenDNS](#).

Server: ws001.phishtank.com



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 223782		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 ZeusS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist.

495

+ Subscribe

2

Tinybanker / Tinba

Bambenek Consulting

Welcome!

with offices in Chicago, IL and Schaumburg, IL, we are close to heart of the business community in this region. Whether you need to build a business, an IT business, or a consulting business, we have the resources and expertise to help you succeed. Our services include: Business Development, Marketing, Sales, and more. We are a full-service consulting firm, and we are proud to be a part of your success.

Champaign Location

Schaumburg Location

99

+ 3

(0)

Zeus Tracker: Binaries

abuse.ch Zeus Tracker

Welcome to the Zeus Tracker

Zeus Tracker tracks ZeusS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist. If you have some quick statistics about the Zeus Tracker:

1. Zeus Tracker tracks ZeusS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist. If you have some quick statistics about the Zeus Tracker:

2. Zeus Tracker tracks ZeusS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist. If you have some quick statistics about the Zeus Tracker:

3. Zeus Tracker tracks ZeusS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist. If you have some quick statistics about the Zeus Tracker:

4. Zeus Tracker tracks ZeusS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist. If you have some quick statistics about the Zeus Tracker:

5. Zeus Tracker tracks ZeusS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist. If you have some quick statistics about the Zeus Tracker:

6. Zeus Tracker tracks ZeusS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist. If you have some quick statistics about the Zeus Tracker:

7. Zeus Tracker tracks ZeusS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist. If you have some quick statistics about the Zeus Tracker:

8. Zeus Tracker tracks ZeusS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist. If you have some quick statistics about the Zeus Tracker:

9. Zeus Tracker tracks ZeusS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist. If you have some quick statistics about the Zeus Tracker:

10. Zeus Tracker tracks ZeusS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist. If you have some quick statistics about the Zeus Tracker:

55

+ 2

(0)

SSL Blacklist (SSLBL)

SSL Blacklist

SSL Blacklist (SSLBL) is a project maintained by abuse.ch. The goal is to provide a list of "bad" SSL certificates that are considered to be malicious. This list is used by many security products to block connections to these certificates. If you are interested in SSL in general or are looking for a way to implement SSL security, you might be interested in the SSL Blacklist.

Overview of blocked SSL certificates:

345

+ 2

(0)

Zeus Tracker: Configs

abuse.ch Zeus Tracker

Welcome to the Zeus Tracker

Zeus Tracker tracks ZeusS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist. If you have some quick statistics about the Zeus Tracker:

1. Zeus Tracker tracks ZeusS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist. If you have some quick statistics about the Zeus Tracker:

2. Zeus Tracker tracks ZeusS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist. If you have some quick statistics about the Zeus Tracker:

3. Zeus Tracker tracks ZeusS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist. If you have some quick statistics about the Zeus Tracker:

4. Zeus Tracker tracks ZeusS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist. If you have some quick statistics about the Zeus Tracker:

5. Zeus Tracker tracks ZeusS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist. If you have some quick statistics about the Zeus Tracker:

6. Zeus Tracker tracks ZeusS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist. If you have some quick statistics about the Zeus Tracker:

7. Zeus Tracker tracks ZeusS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist. If you have some quick statistics about the Zeus Tracker:

8. Zeus Tracker tracks ZeusS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist. If you have some quick statistics about the Zeus Tracker:

9. Zeus Tracker tracks ZeusS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist. If you have some quick statistics about the Zeus Tracker:

10. Zeus Tracker tracks ZeusS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist. If you have some quick statistics about the Zeus Tracker:

95

+ 2

(0)

Zeus Tracker: Drop Zones

abuse.ch Zeus Tracker

Welcome to the Zeus Tracker

Zeus Tracker tracks ZeusS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist. If you have some quick statistics about the Zeus Tracker:

1. Zeus Tracker tracks ZeusS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist. If you have some quick statistics about the Zeus Tracker:

2. Zeus Tracker tracks ZeusS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist. If you have some quick statistics about the Zeus Tracker:

3. Zeus Tracker tracks ZeusS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist. If you have some quick statistics about the Zeus Tracker:

4. Zeus Tracker tracks ZeusS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist. If you have some quick statistics about the Zeus Tracker:

5. Zeus Tracker tracks ZeusS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist. If you have some quick statistics about the Zeus Tracker:

6. Zeus Tracker tracks ZeusS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist. If you have some quick statistics about the Zeus Tracker:

7. Zeus Tracker tracks ZeusS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist. If you have some quick statistics about the Zeus Tracker:

8. Zeus Tracker tracks ZeusS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist. If you have some quick statistics about the Zeus Tracker:

9. Zeus Tracker tracks ZeusS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist. If you have some quick statistics about the Zeus Tracker:

10. Zeus Tracker tracks ZeusS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist. If you have some quick statistics about the Zeus Tracker:

50

+ 2

(0)

SpyEye: Domain Block List

SET SpyEye

Welcome to the SpyEye Tracker

The SpyEye Tracker is a project by abuse.ch. It is a web-based tool that allows you to track and block SpyEye malware. It provides a list of domains and IP addresses that are associated with SpyEye malware. You can use this information to block connections to these domains and IP addresses. If you are interested in SpyEye malware, you might be interested in the SpyEye Tracker.

127

+ 2

(0)

SpyEye: IP Block List

SET SpyEye

Welcome to the SpyEye Tracker

The SpyEye Tracker is a project by abuse.ch. It is a web-based tool that allows you to track and block SpyEye malware. It provides a list of domains and IP addresses that are associated with SpyEye malware. You can use this information to block connections to these domains and IP addresses. If you are interested in SpyEye malware, you might be interested in the SpyEye Tracker.

84

+ 2

(0)

Palevo: Domain Block List

Platform Tracker 1.0 Home

Platform Tracker is a project by abuse.ch. It is a web-based tool that allows you to track and block Palevo malware. It provides a list of domains and IP addresses that are associated with Palevo malware. You can use this information to block connections to these domains and IP addresses. If you are interested in Palevo malware, you might be interested in the Platform Tracker.

18

+ 2

(0)

Critical Stack, Inc © 2015

<http://criticalstack.com>

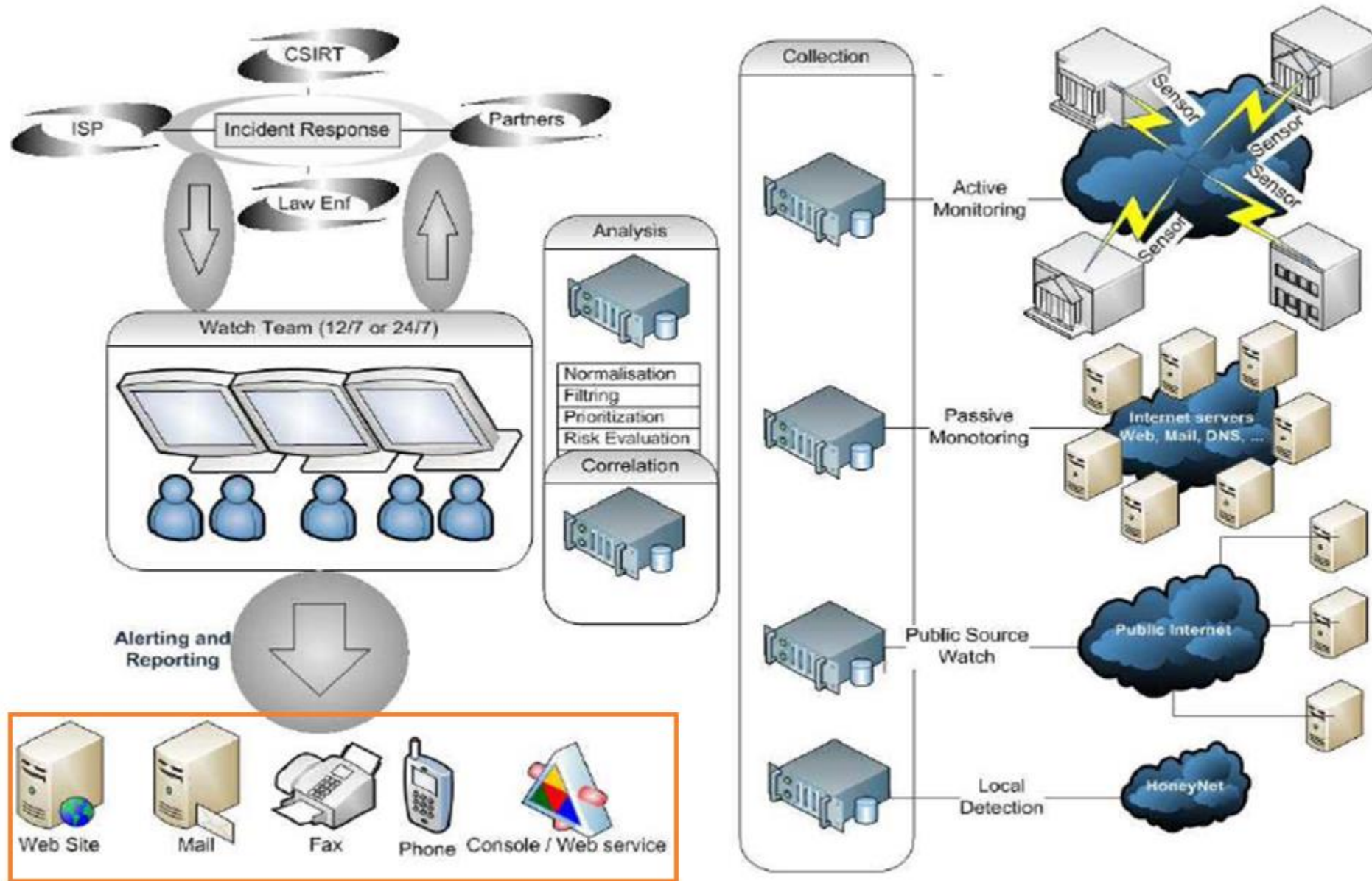
?

Help

25

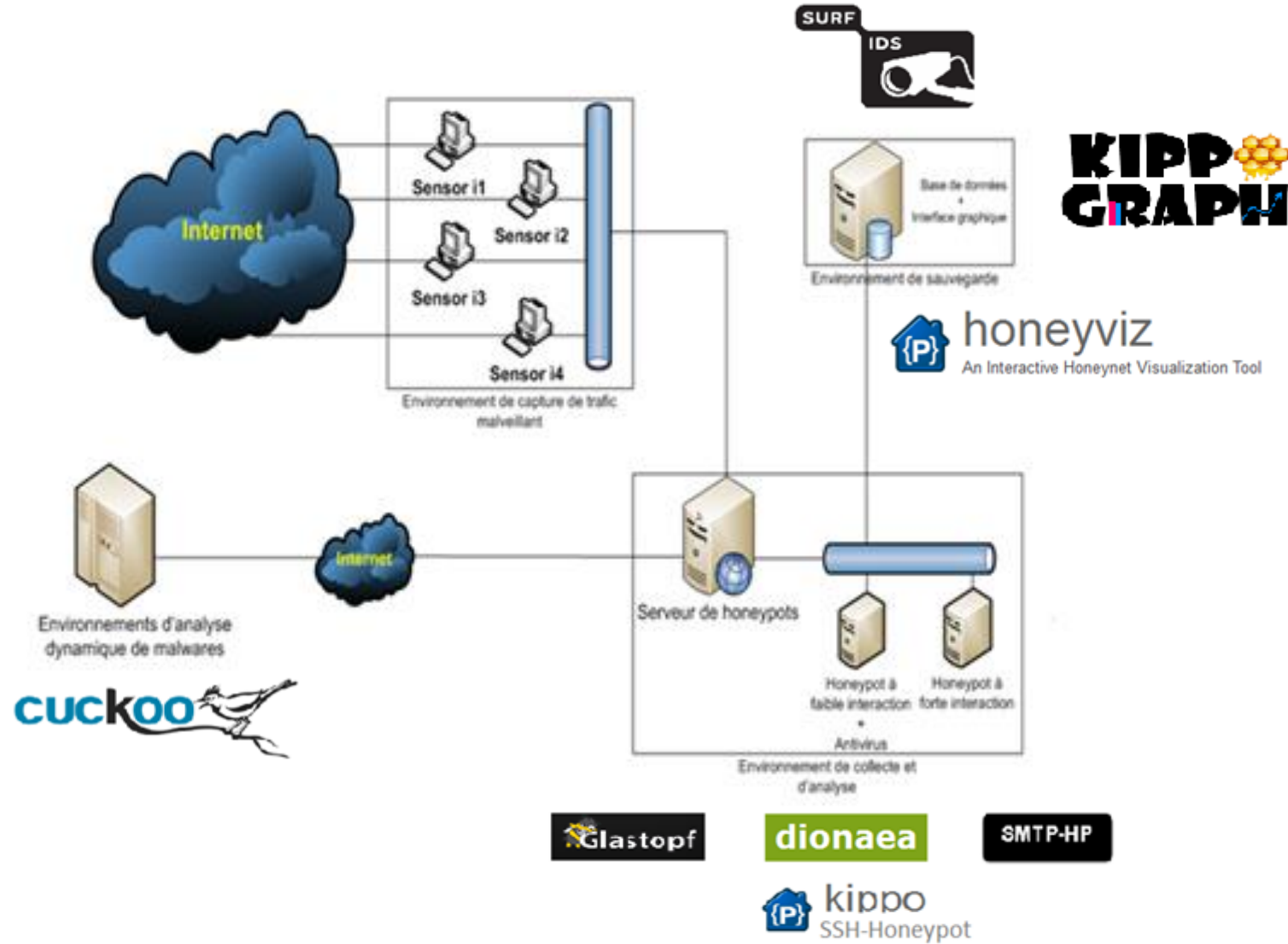


Incident Response Center





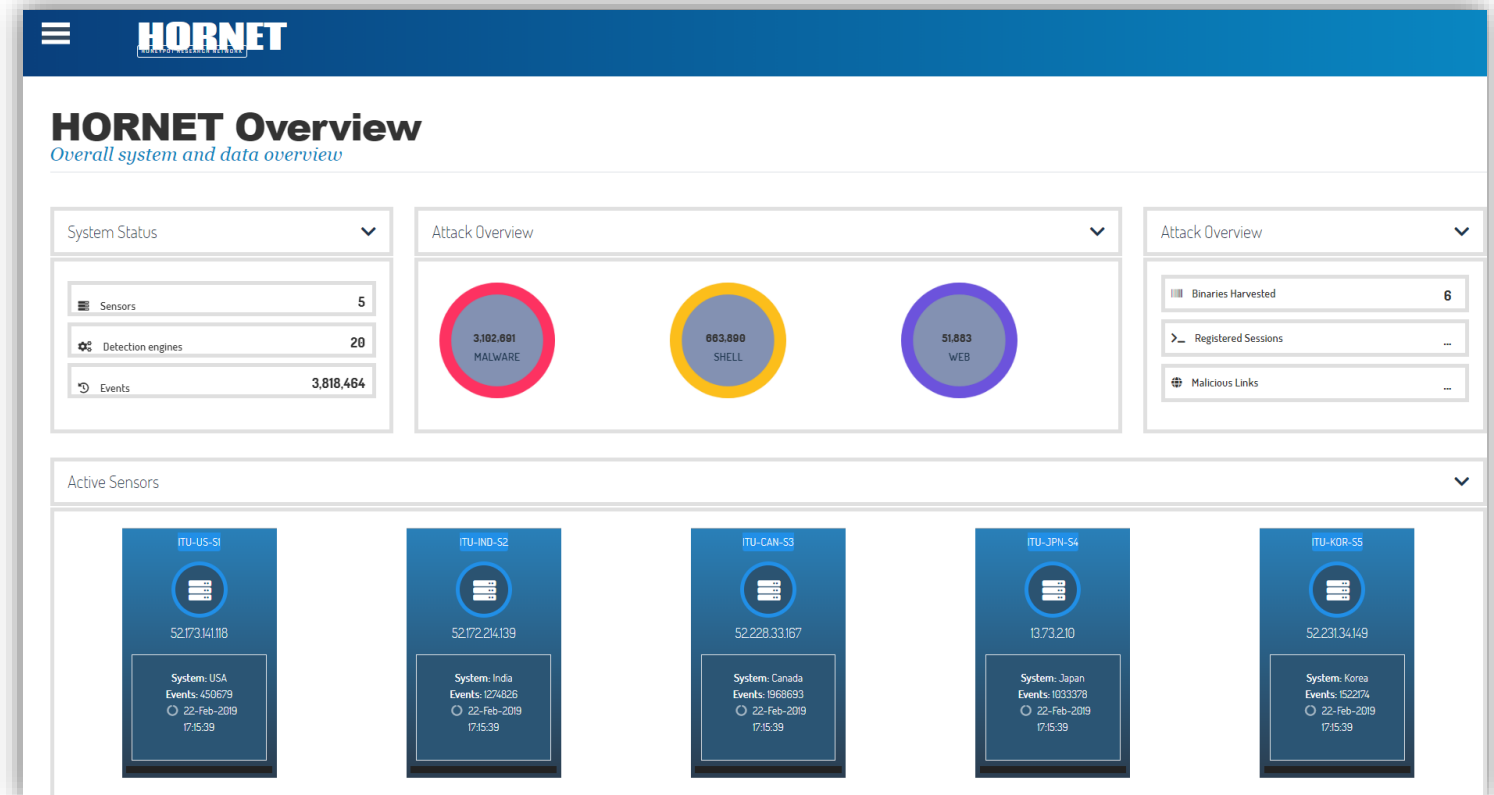
HoneyNet Platforms





HoneyNet Platforms

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

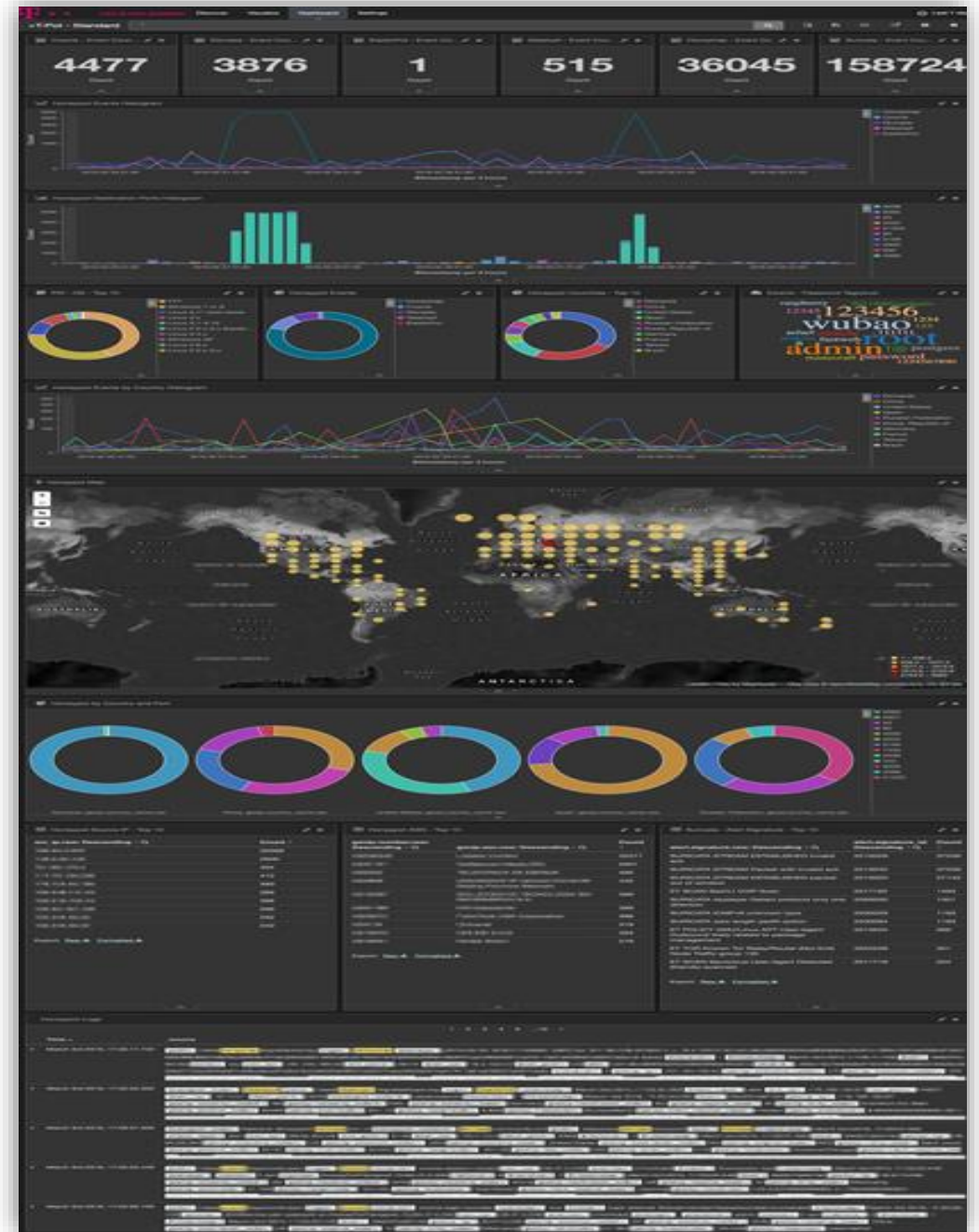




HoneyNet Platforms

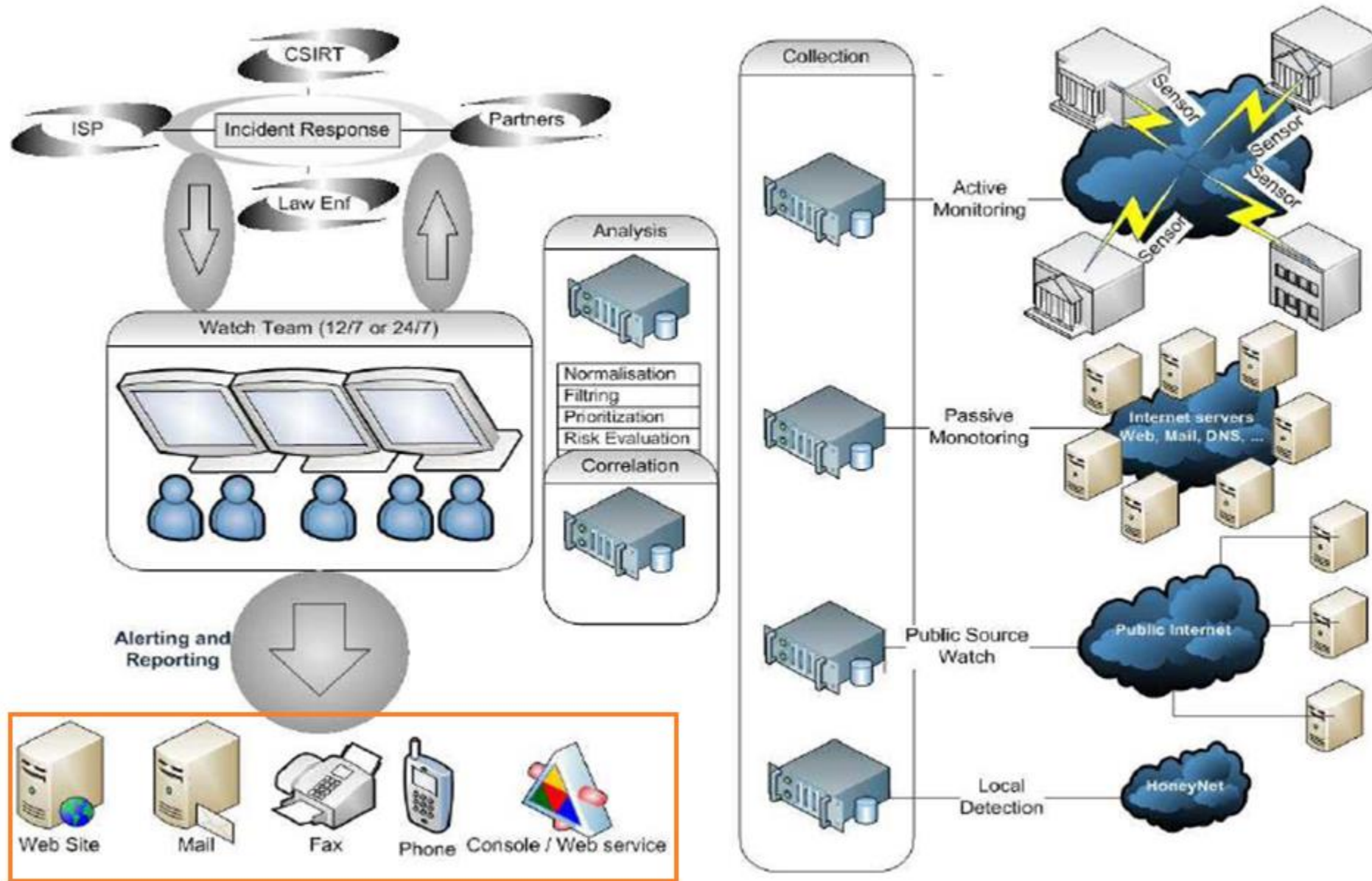
T-POT : Honeypot platform

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





Incident Response Center



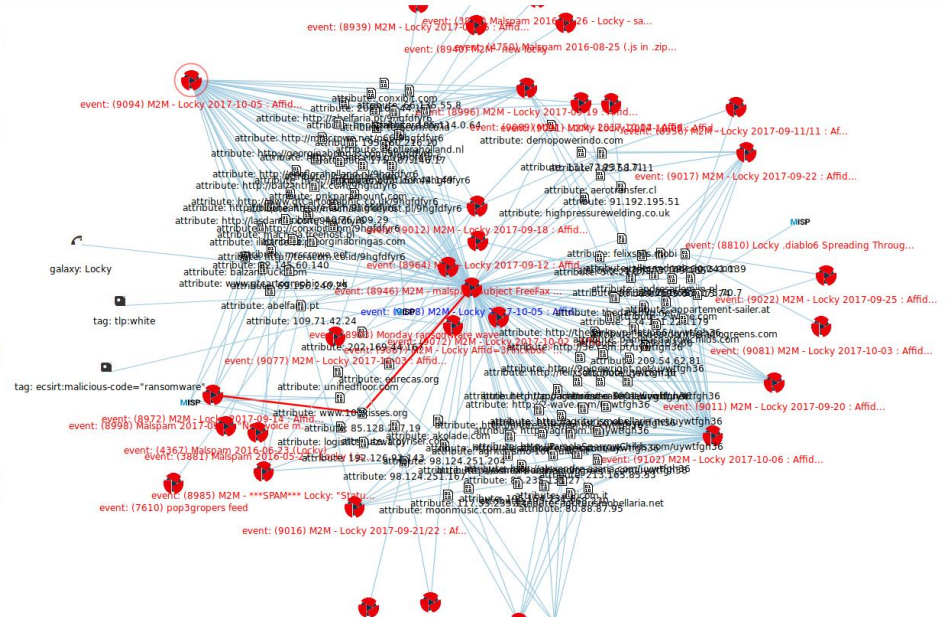


MISP Open Source Threat Intelligence and Sharing Platform



Hover target

Attribute: 1140609
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, "ykol": "Invoice INV000123" - "Invoice
INV000123.72"
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

Q

My Org

Published

Org

Owner Org

Id

Tags

#Attr

Email

Date

Threat Level

Analysis

Info

Distribution

Actions

✓

CUDES0

ORNAME

93

tip:white

16

admin@admin.test

2016-03-23

Medium

Completed

SAMSAM: THE DOCTOR WILL SEE YOU AFTER HE PAYS THE RANSOM

All

🔗

🗑️

✓

CUDES0

ORNAME

91

tip:white

3

admin@admin.test

2016-03-07

Low

Completed

Ad Serving Platform Used By PUJA Also Delivers Magnitude Exploit Kit

All

🔗

🗑️

✓

CUDES0

ORNAME

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

ORNAME

5

tip:white

Type:OSINT

84

admin@admin.test

2016-02-13

Medium

Completed

OSINT - Turia - Harnessing SSL Certificates Using Infrastructure Chaining

All

👤

🔗

🗑️

✗

CIRCL

ORNAME

43

tip:white

Type:OSINT

70

admin@admin.test

2016-03-21

Low

Completed

OSINT - STOP SCANNING MY MACRO

All

👤

🔗

🗑️

✓

CIRCL

ORNAME

10

tip:white

circularincident-classification="system-compromise"

847

admin@admin.test

2016-03-17

Low

Initial

Potential SpamBots (2016-03-17)

All

🔗

🗑️

✓

CIRCL

ORNAME

44

tip:white

circularincident-classification="malware"

290

admin@admin.test

2016-03-17

Low

Initial

Malspam (2016-03-17) - All Dridex (122), Locky

All

🔗

🗑️

✓

CIRCL

ORNAME

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

🔗

🗑️

✓

CUDES0

ORNAME

71

tip:white

25

admin@admin.test

2016-03-11

Low

Completed

PowerSniff Malware Used in Macro-based Attacks

All

🔗

🗑️

✓

CIRCL

ORNAME

25

malware_classification=malware-category="Ransomware"

32

admin@admin.test

2016-03-16

Low

Initial

Locky (2016-03-16)

All

🔗

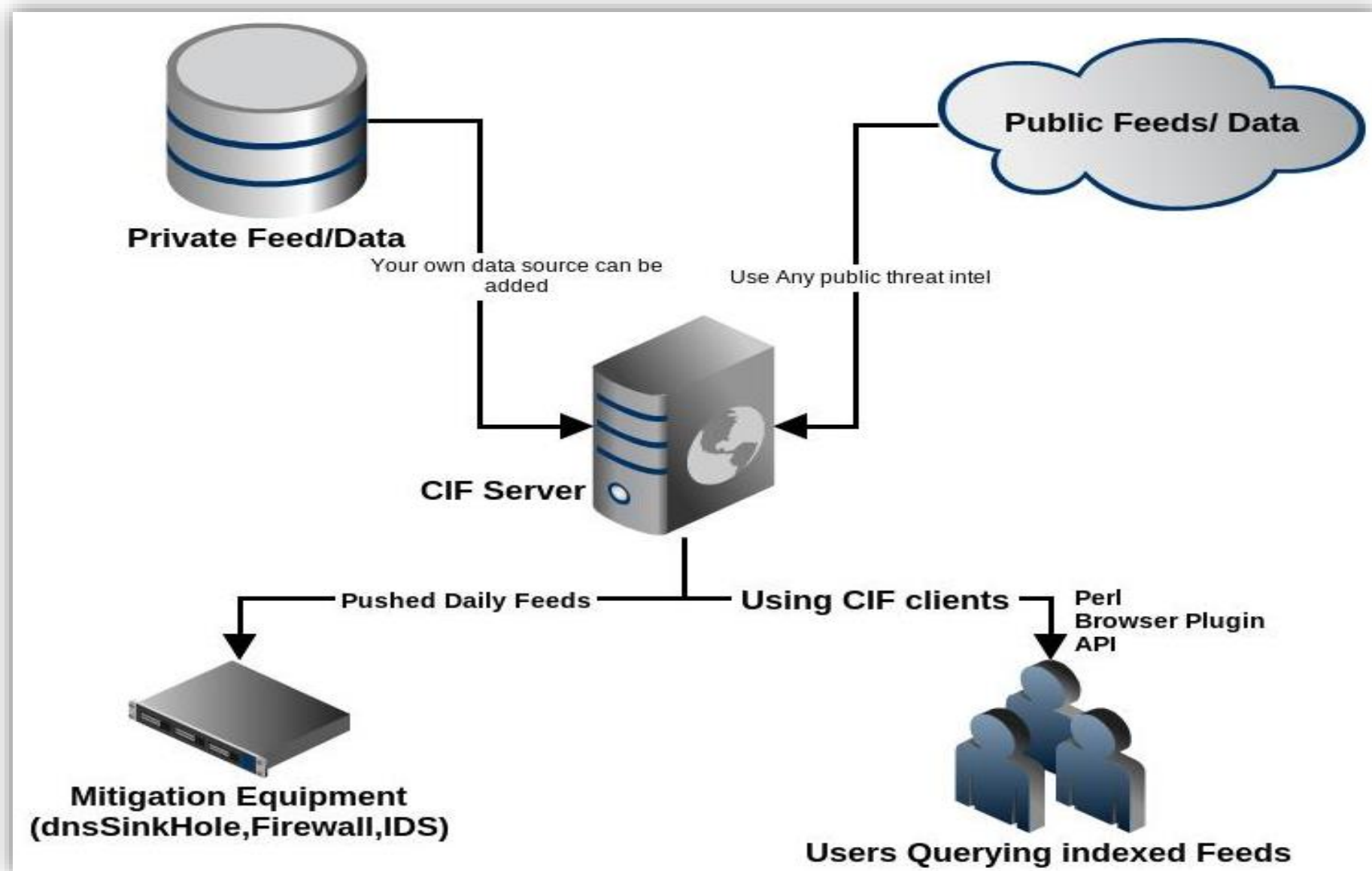
🗑️

Download: PGP/GPG key

Powered by MISP 2.4.28

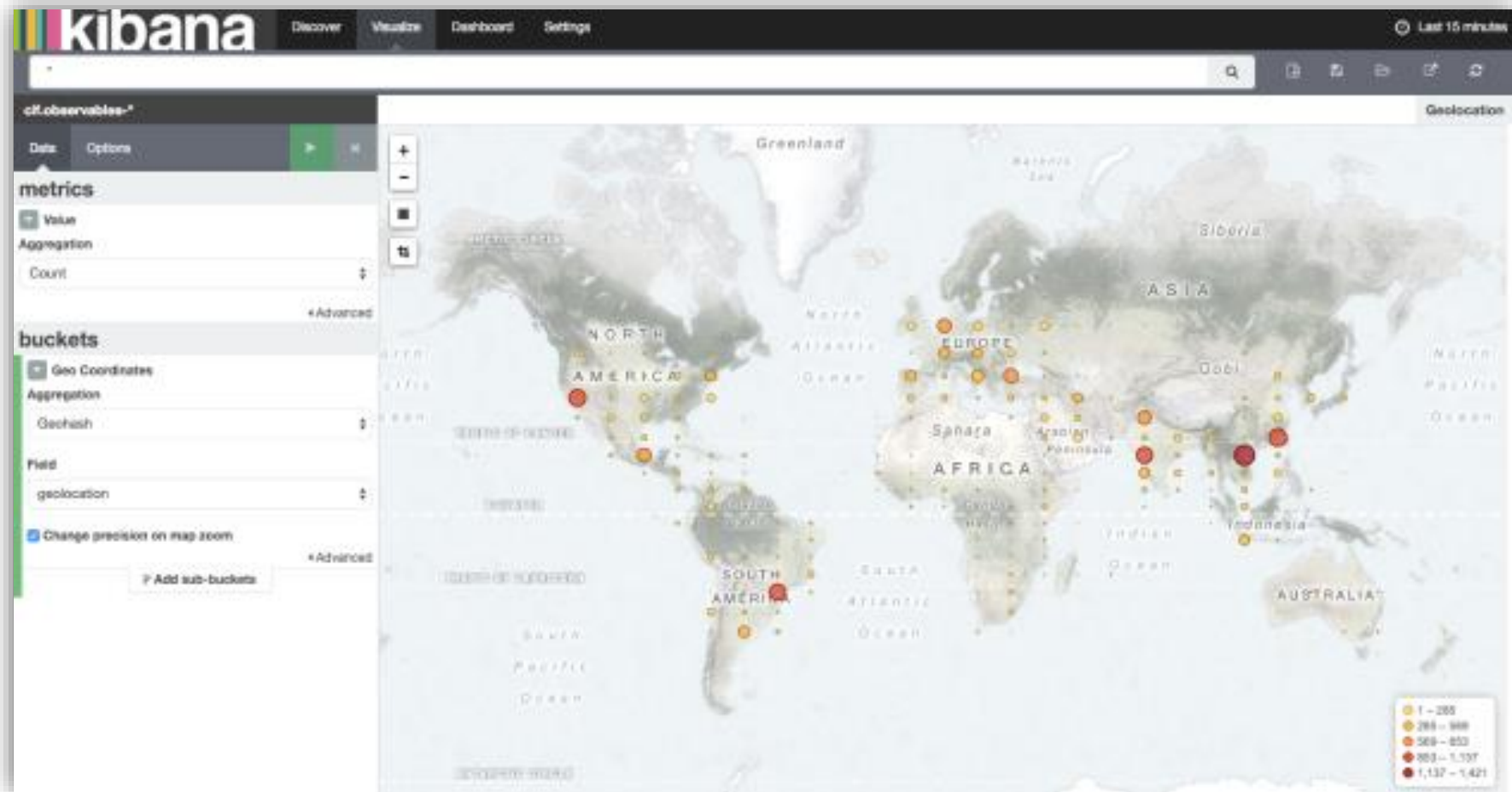


Collective Intelligence Framework (CIF)



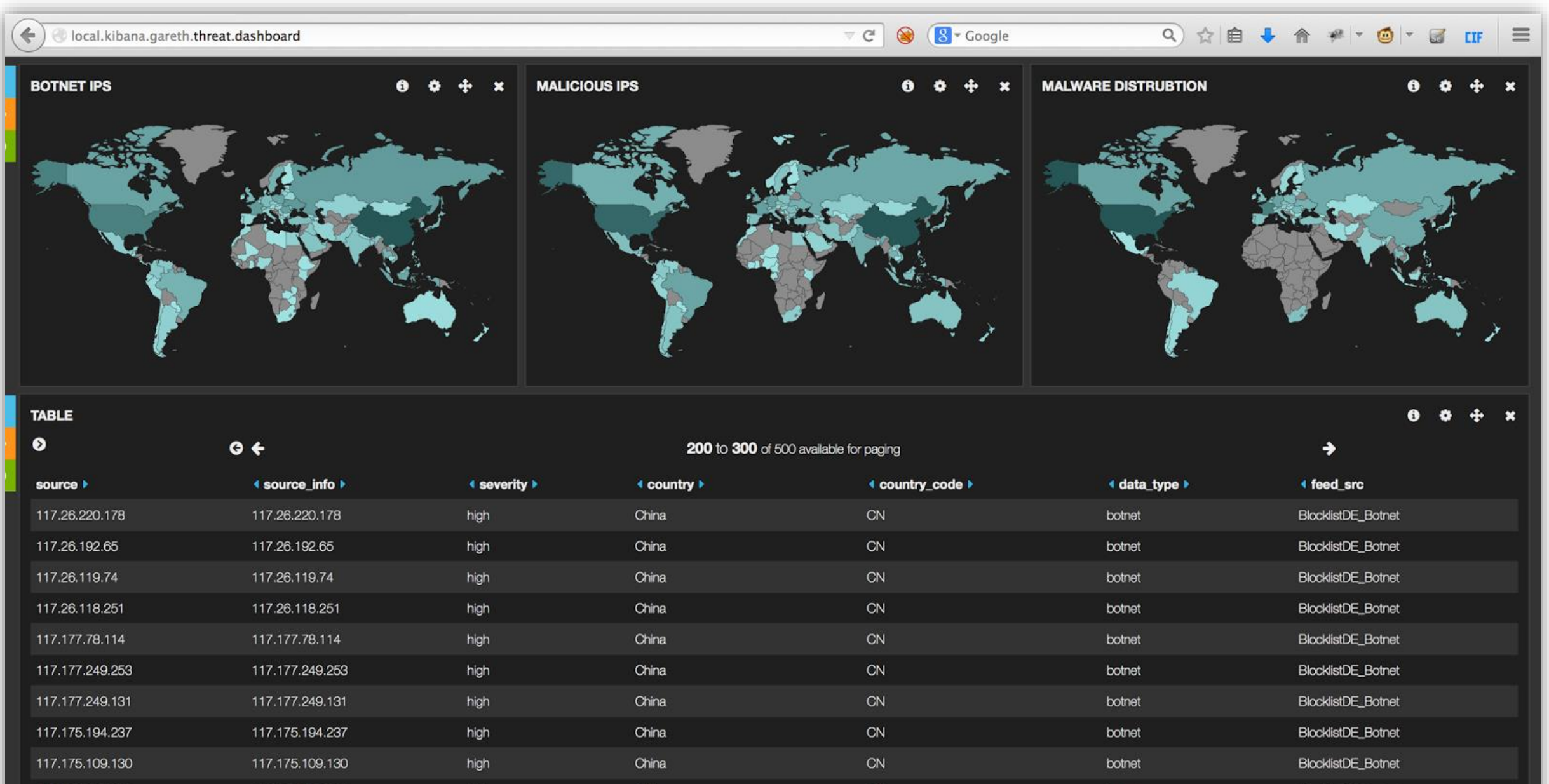


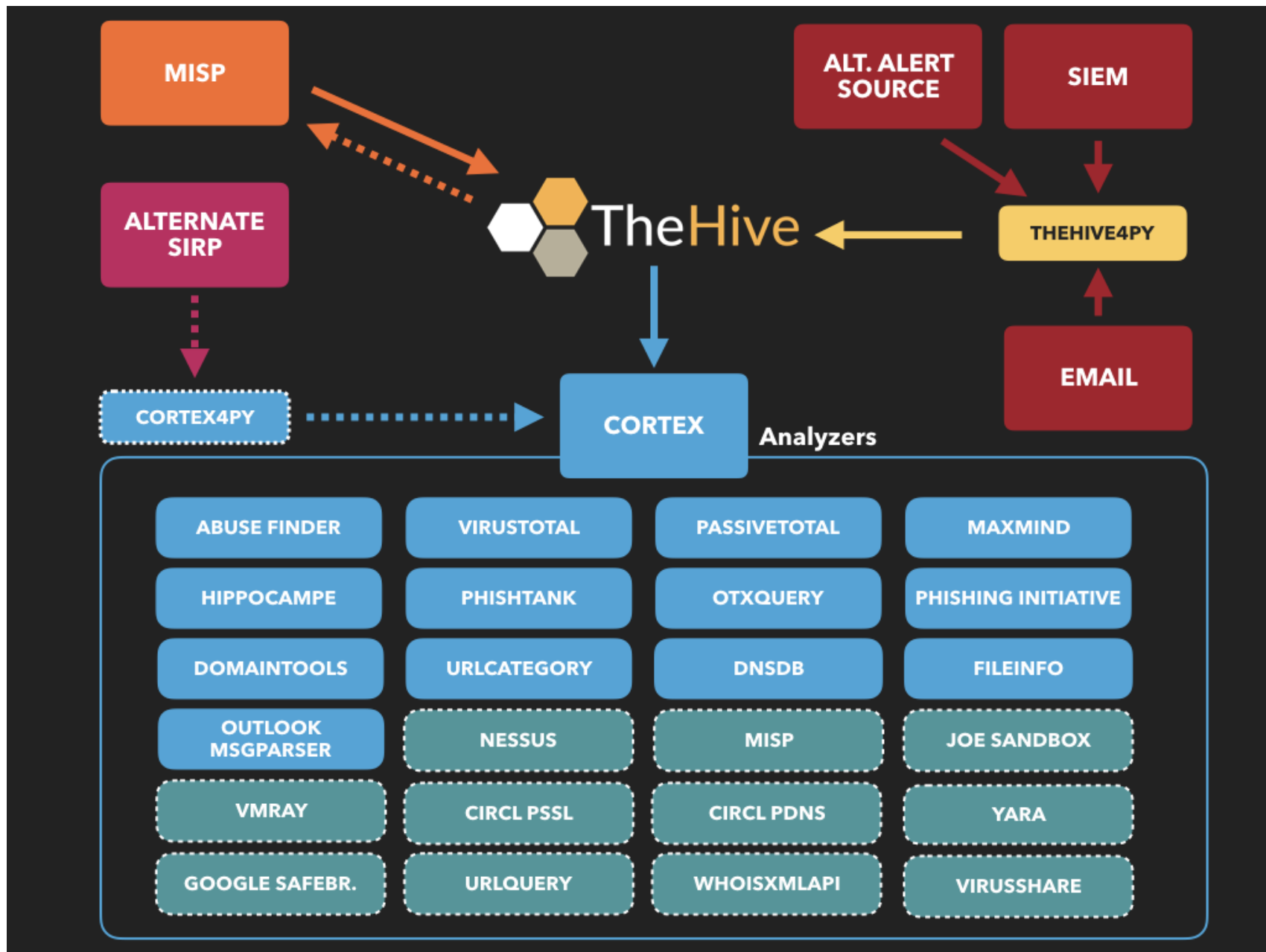
Collective Intelligence Framework (CIF)





Collective Intelligence Framework (CIF)







Example of Digital Forensic Tools



Digital Forensic Tools



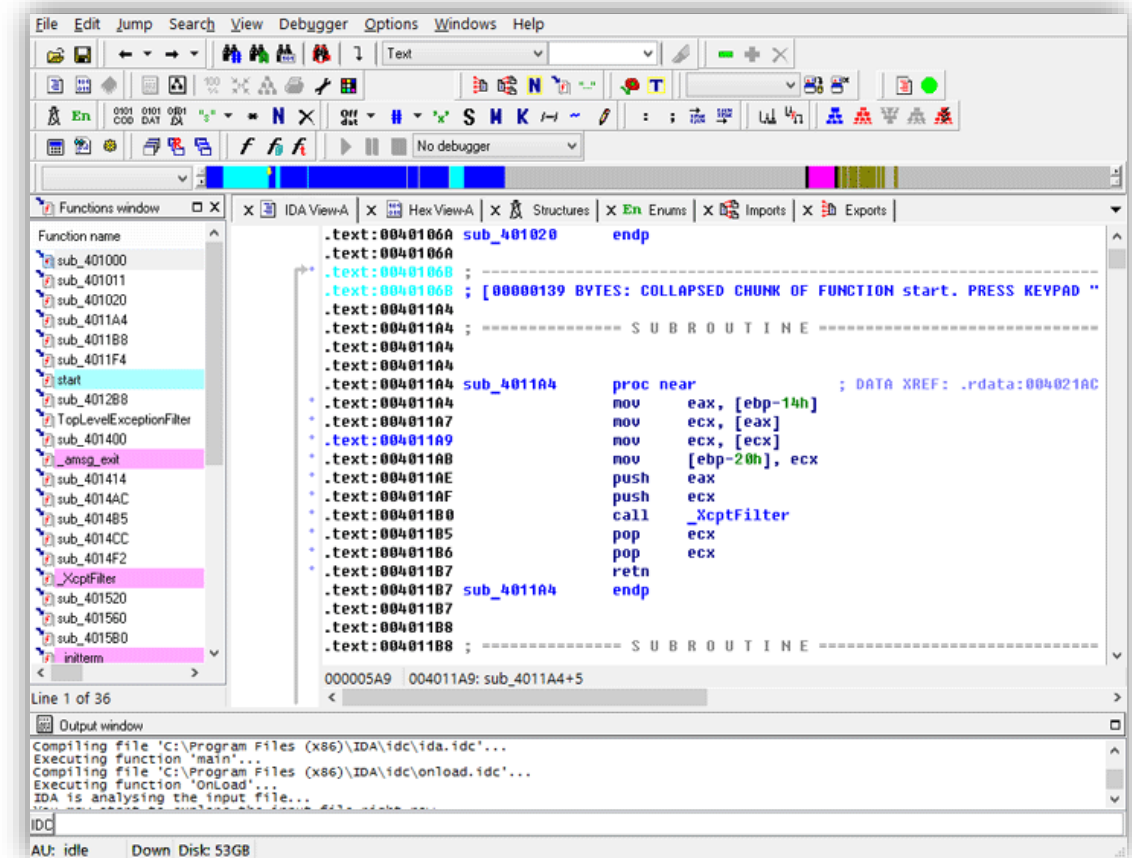
REMnux: A Linux Toolkit for Reverse-Engineering and Analyzing Malware



MALWARE AND MEMORY FORENSICS



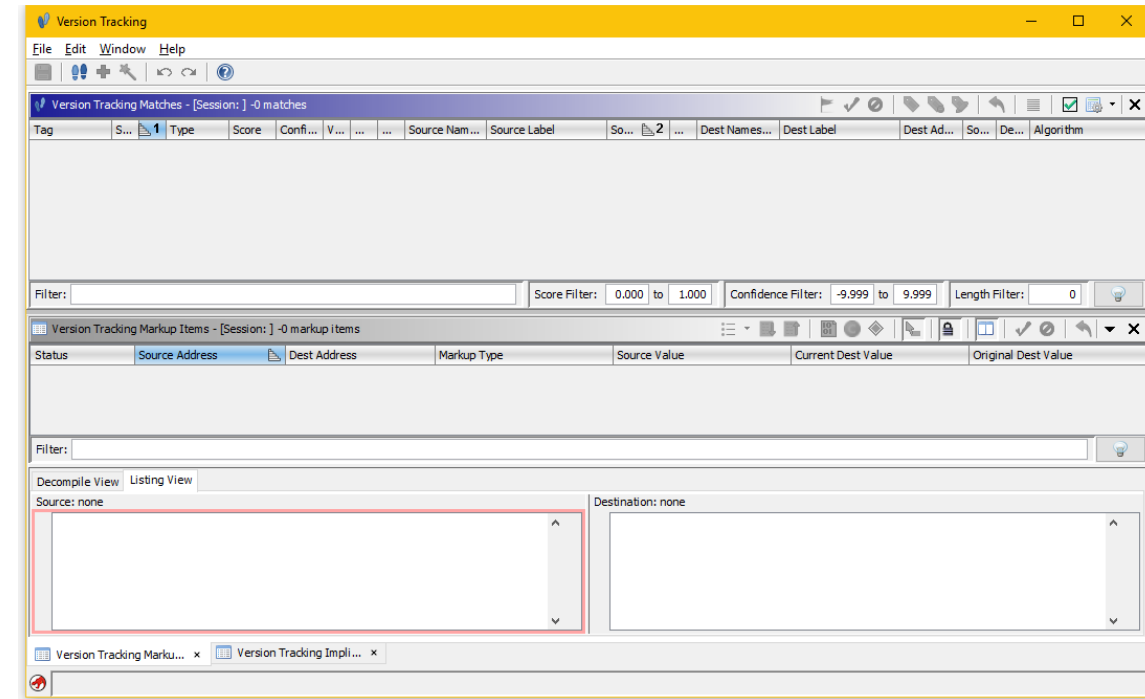
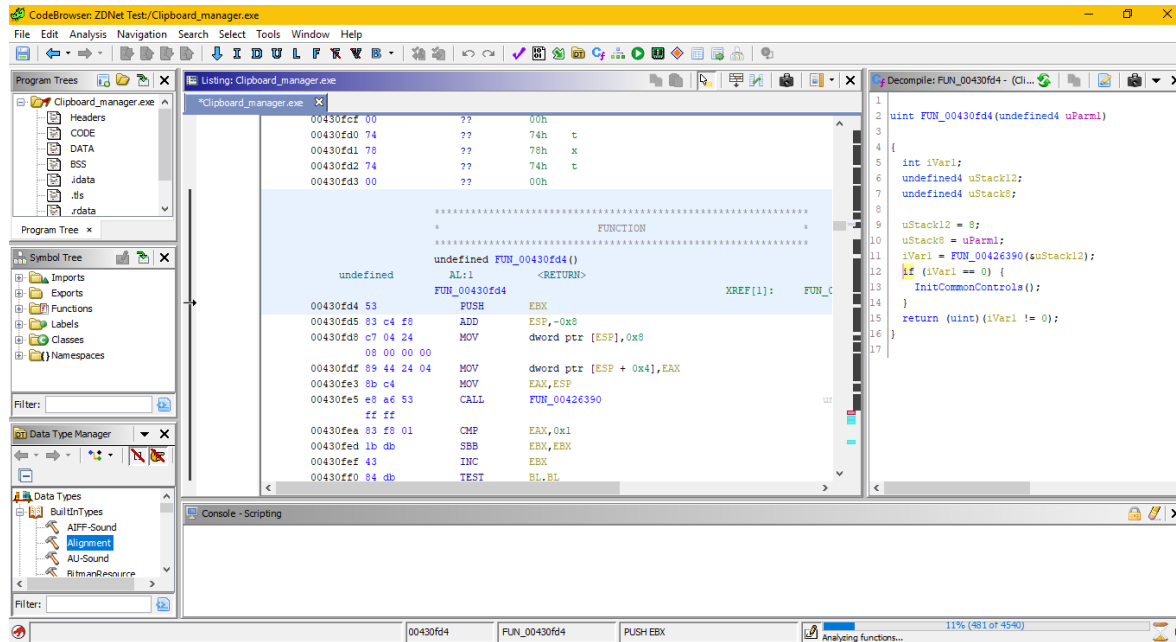
The Interactive Disassembler (IDA)



<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.

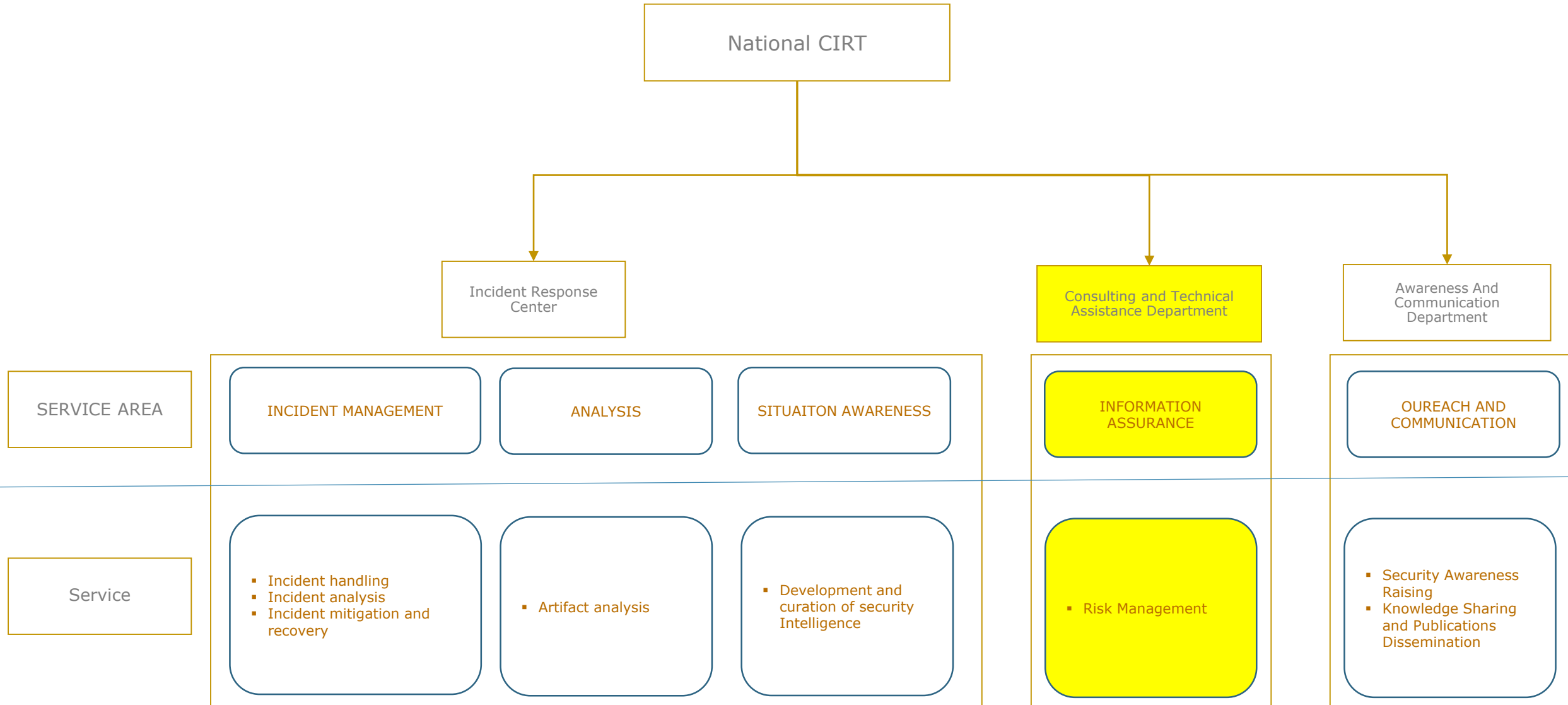


Malwr : Automated Malware Analysis Sandboxes and Services





The Basic Services Offered by a CSIRT/SOC





Example of Security Assessment tools



Security Assessment tools



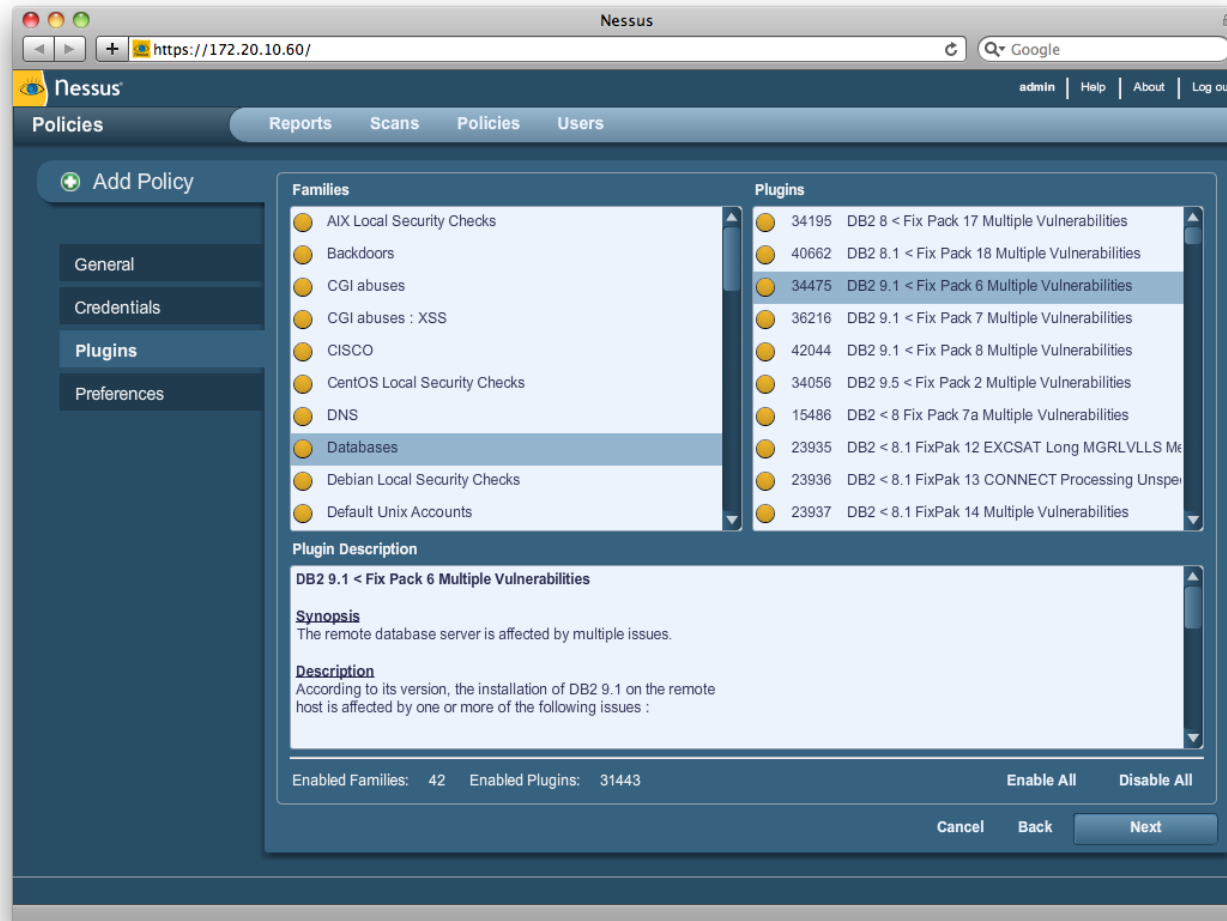
```
Applications Places Tue Aug 12, 4:21 PM root
root@vineet:~# aireplay-ng -l 8 -a 00:1E:58:85:88:18 -h 00:1E:58:85:88:18
16:01:06 Waiting for beacon from 00:1E:58:85:88:18
16:01:06 Sending Authentication
16:01:06 Authentication successful
16:01:06 Sending Association Request
16:01:06 Association successful
root@vineet:~# aireplay-ng -l 8 -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
You should also start airodump-ng
^C^C 412601 packets (got 99%)
root@vineet:~#
```

```
File Edit View Search Terminal Help
64 bytes from kul01s07-in-f0.1e100.net (173.194.126.0): icmp_req=18 ttl=128 time=94.1 ms
64 bytes from kul01s07-in-f0.1e100.net (173.194.126.0): icmp_req=19 ttl=128 time=92.2 ms
64 bytes from kul01s07-in-f0.1e100.net (173.194.126.0): icmp_req=20 ttl=128 time=92.9 ms
64 bytes from kul01s07-in-f0.1e100.net (173.194.126.0): icmp_req=21 ttl=128 time=92.5 ms
64 bytes from kul01s07-in-f0.1e100.net (173.194.126.0): icmp_req=22 ttl=128 time=99.8 ms
64 bytes from kul01s07-in-f0.1e100.net (173.194.126.0): icmp_req=23 ttl=128 time=93.8 ms
64 bytes from kul01s07-in-f0.1e100.net (173.194.126.0): icmp_req=24 ttl=128 time=102 ms
64 bytes from kul01s07-in-f0.1e100.net (173.194.126.0): icmp_req=25 ttl=128 time=92.8 ms
64 bytes from kul01s07-in-f0.1e100.net (173.194.126.0): icmp_req=26 ttl=128 time=98.9 ms
64 bytes from kul01s07-in-f0.1e100.net (173.194.126.0): icmp_req=27 ttl=128 time=97.8 ms
64 bytes from kul01s07-in-f0.1e100.net (173.194.126.0): icmp_req=28 ttl=128 time=93.2 ms
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/>



OPEN SOURCE WEB APPLICATION VULNERABILITY SCANNER, PROXY AND PLATFORM



static code analysis

path / file: d:\cipher3\timeclock\ ☒ 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`

requires:

```
155: if($state == "start") else
159: if($act_status != "working") else
```

Userinput is passed through function parameters.

- 18: `insert project into database ($_POST['projec`

requires:

```
9: if(isset($_GET['action']))
10: switch($_GET['action'])
13: case "start_work" :
17: if(!isset($_POST['project'])) else
```

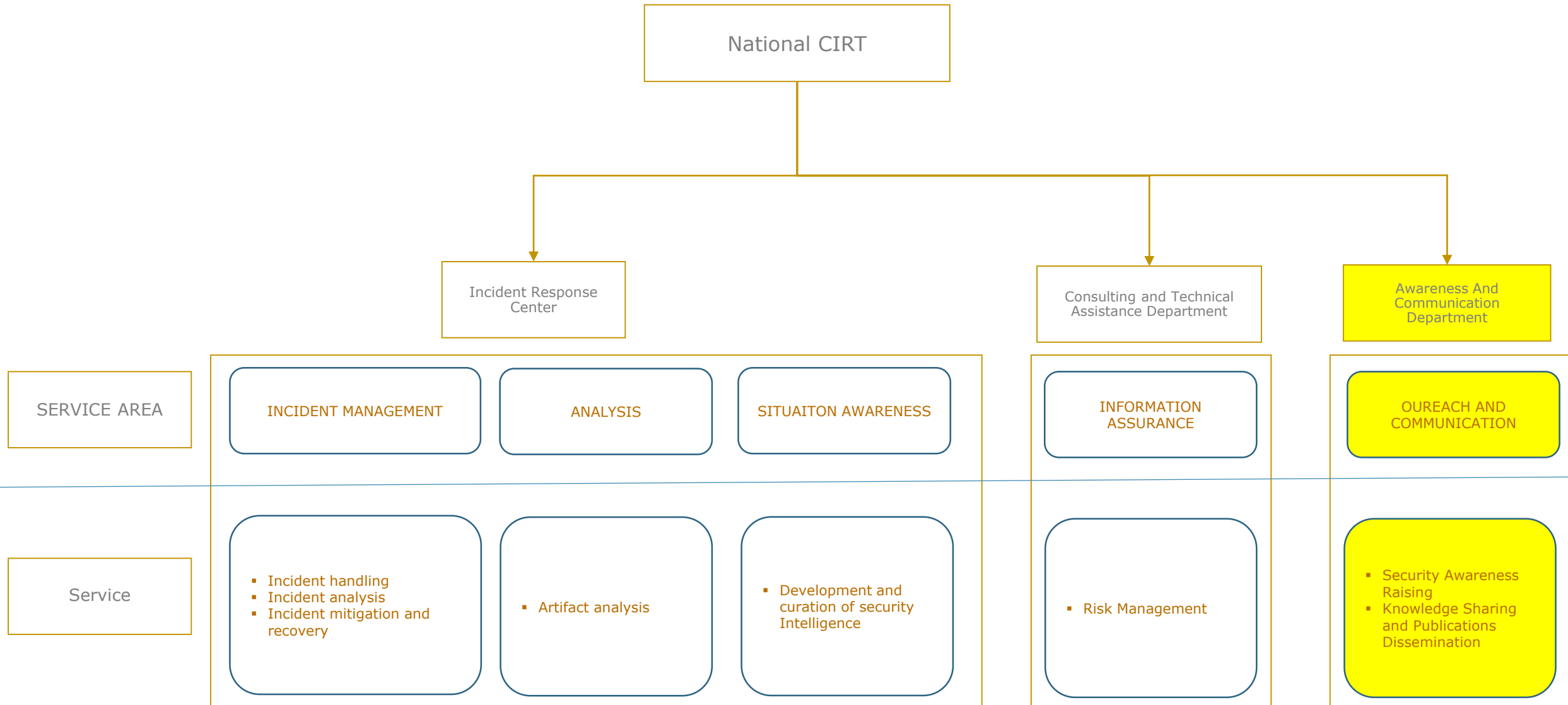
CodeViewer - D:\cipher3\timeclock\work_functions.php

```
154 }
155 else{
156     if($act_status != "working"){
157         html_error("Cipher - time clock - Error","You haven't start a project. Please <a href='\"#\"'>start a project.
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         if(!$result){
164             html_error("Cipher - time clock - Database error","Can't get the id of the last project.
165         }
166         if(system__($result) == 0){
167             html_error("Cipher - time clock - Error","The project you have specified has already been started.
168         }
169         if(system__($result) > 1){
170             while($row=mysql_fetch_array($result)){
171                 $id = $row["id"];
172             }
173         }
174     }
175 }
```

rips-scanner.sourceforge.net/



The Basic Services Offered by a CSIRT/SOC





Example of Alerts, Warnings and Announcements Tools



Alerts, Warnings and Announcements Tools

powered by:
[PHP] + [MySQL]

phplist

logout

main page

configure

help

about

logout

English

System Functions

setup	Setup phplist
dbcheck	Check Database structure
eventlog	View the eventlog
close	

Configuration functions

configure	configure phplist
attributes	Configure Attributes
spage	Configure Subscribe pages
close	

List and user functions

list	List the current lists
users	List all Users
reconcileusers	Reconcile the user database
import	Import Users
export	Export Users
close	

lists

send a message

users

manage users

subscribe pages

messages

templates

process queue

process bounces

view bounces

eventlog

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

Taranis architecture

