ITU Cyber Drill - ALERT (Applied Learning for Emergency Response Teams) for CIS Region

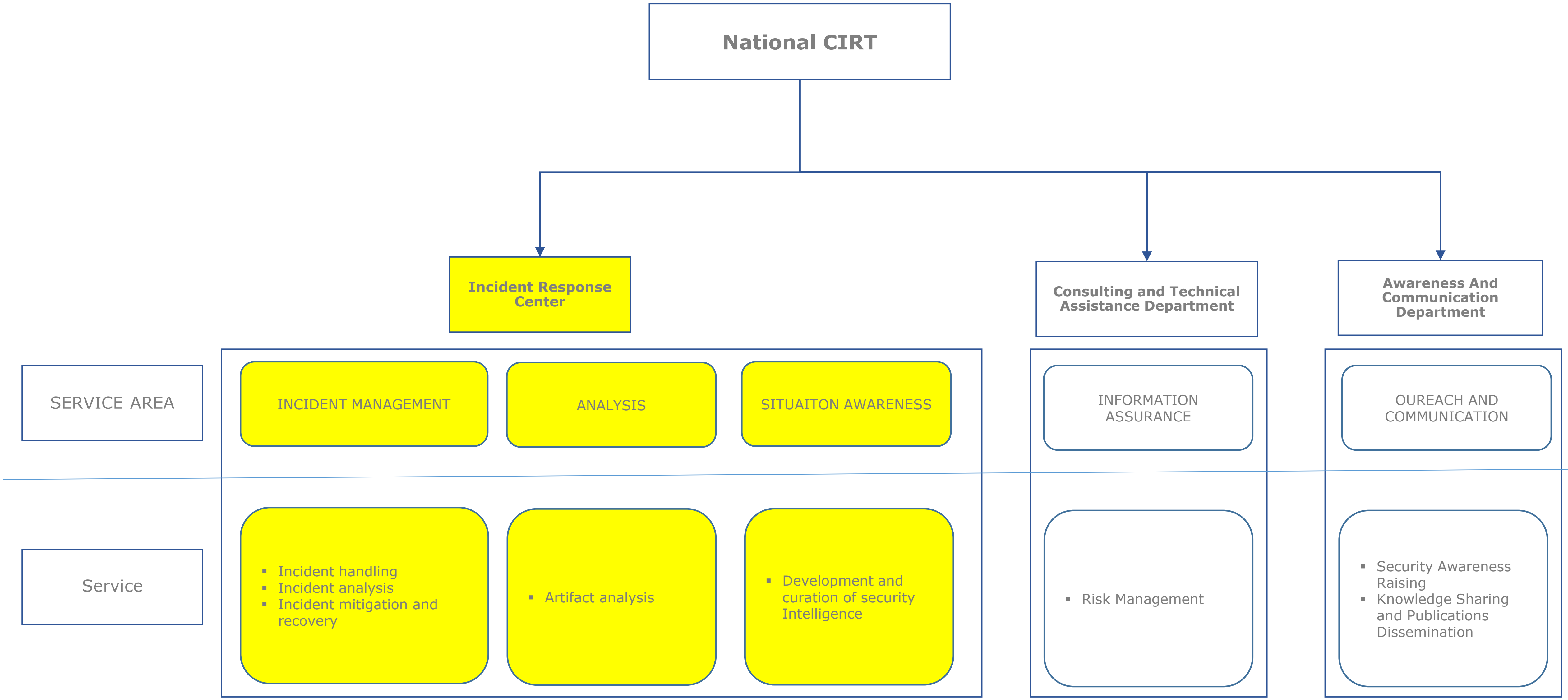
How to Build a CIRT based on Open source tools

Marwan BEN RACHED
Technical Officer - Cybersecurity -ITU-

Grand-Bassam, Côte d'Ivoire, 1-5 October 2018

$0

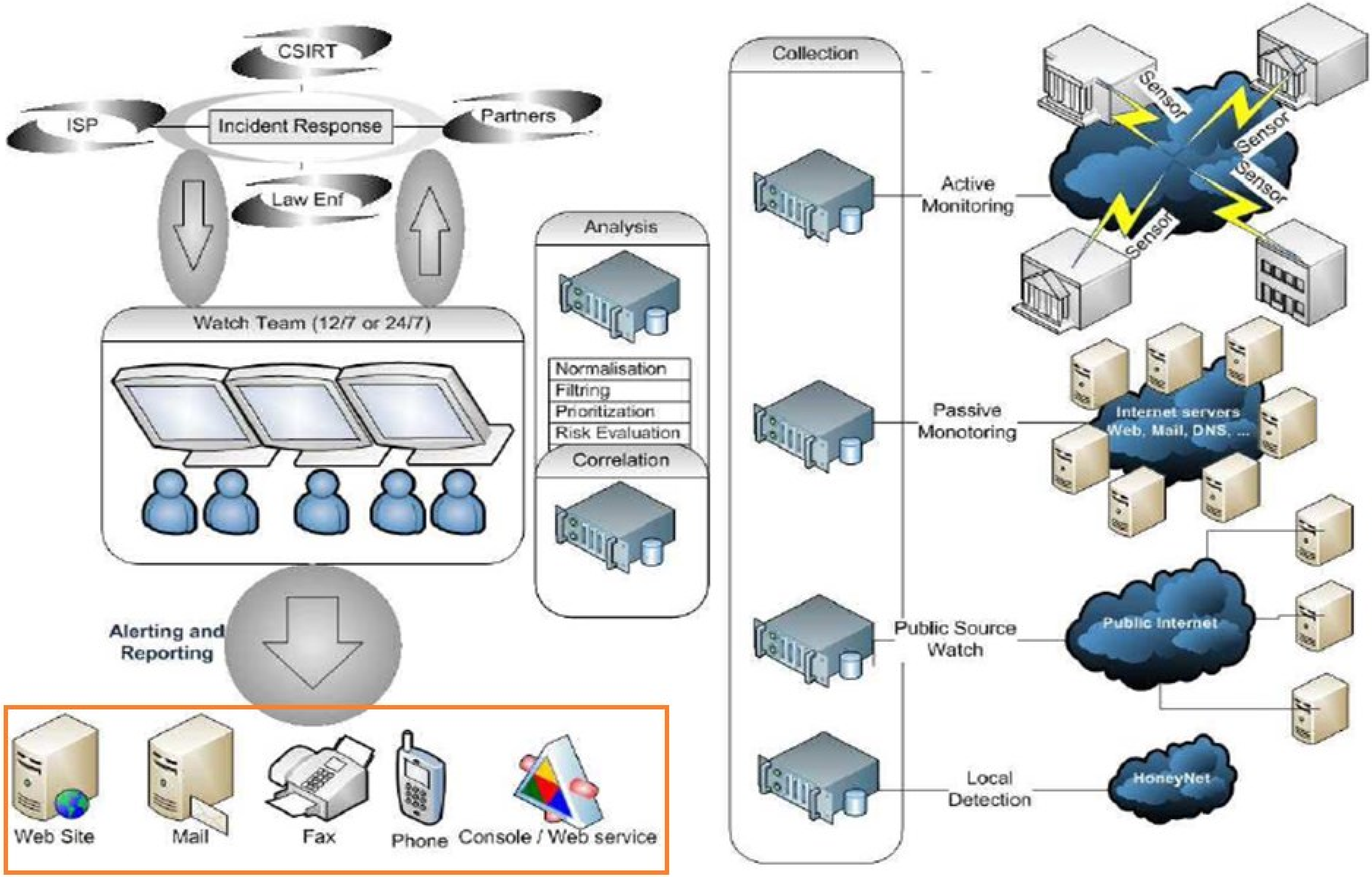
The Basic Services Offered by a National CIRT



National CIRT

	Incident Response Center			**Consulting and Technical Assistance Department**	**Awareness And Communication Department**
SERVICE AREA	INCIDENT MANAGEMENT	ANALYSIS	SITUAITON AWARENESS	INFORMATION ASSURANCE	OUREACH AND COMMUNICATION
Service	▪ Incident handling ▪ Incident analysis ▪ Incident mitigation and recovery	▪ Artifact analysis	▪ Development and curation of security Intelligence	▪ Risk Management	▪ Security Awareness Raising ▪ Knowledge Sharing and Publications Dissemination

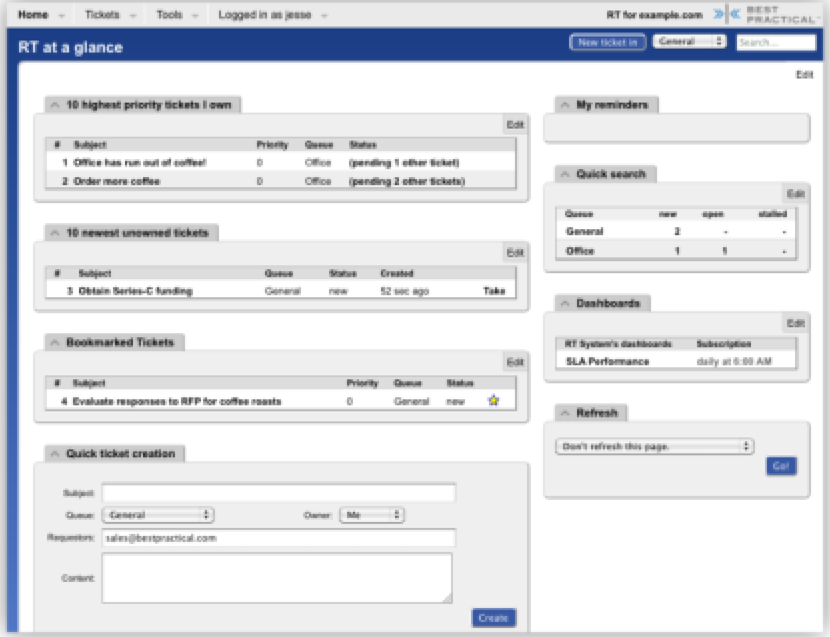
Incident Response Center



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.



RT at a glance

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
3	Obtain Series-C funding	General	new	52 sec ago

Bookmarked Tickets

#	Subject	Priority	Queue	Status
4	Evaluate responses to RFP for coffee roasts	0	General	new

Quick ticket creation

Subject:
Queue: General
Owner: Me
Requestors: sales@bestpractical.com
Content:

My reminders

Quick search

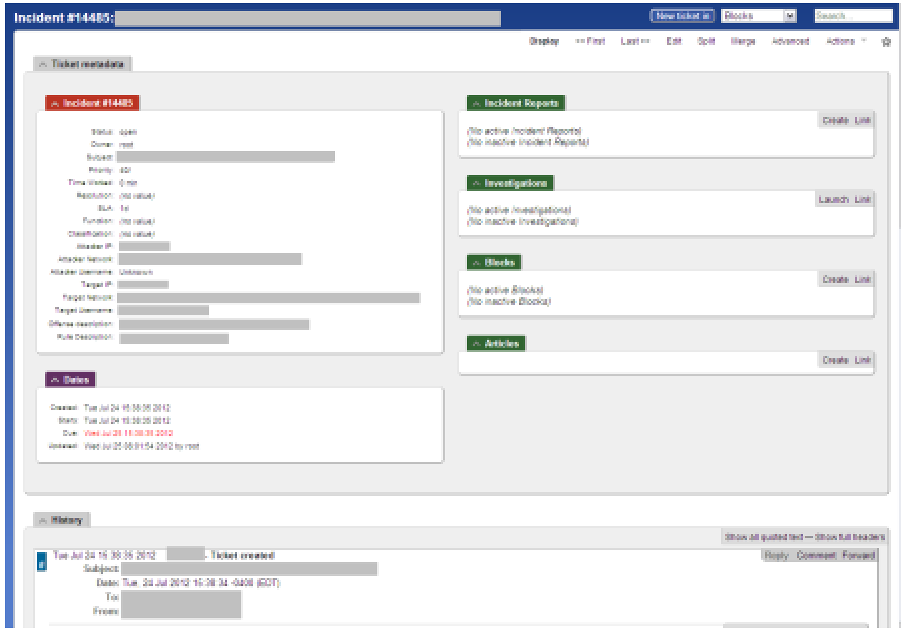
Queue	new	open	stalled
General	2	-	-
Office	1	1	-

Dashboards

RT System's dashboards	Subscription
SLA Performance	daily at 6:00 AM

Refresh

Don't refresh this page.



Incident #14485: [redacted]

Ticket metadata

Incident #14485

Status: open
Owner: root
Subject: [redacted]
Priority: 40
Time Worked: 0 min
Resolution: (no value)
SLA: 1d
Function: (no value)
Classification: (no value)
Attacker IP: [redacted]
Attacker Network: [redacted]
Attacker Username: Unknown
Target IP: [redacted]
Target Network: [redacted]
Target Username: [redacted]
Offense description: [redacted]
Rule Description: [redacted]

Dates

Created: Tue Jul 24 15:38:35 2012
Starts: Tue Jul 24 15:38:35 2012
Due: Wed Jul 25 15:38:35 2012
Updated: Wed Jul 25 08:01:54 2012 by root

Incident Reports

(No active Incident Reports)
(No inactive Incident Reports)

Investigations

(No active Investigations)
(No inactive Investigations)

Blocks

(No active Blocks)
(No inactive Blocks)

Articles

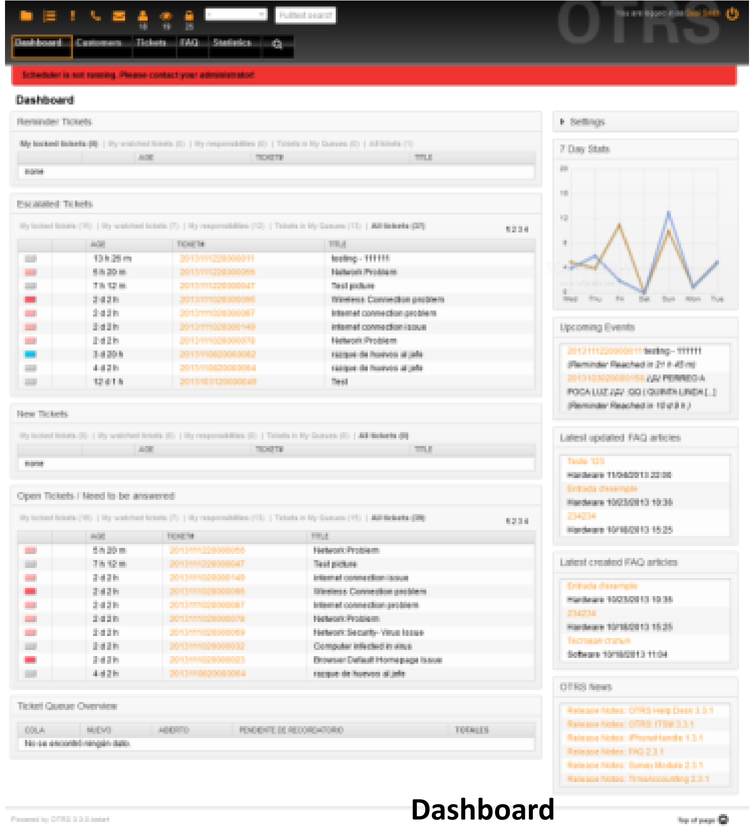
History

Tue Jul 24 15:38:35 2012 [redacted] - Ticket created
Subject: [redacted]
Date: Tue, 24 Jul 2012 15:38:34 -0400 (EDT)
To: [redacted]
From:

Open Technology Real Services (OTRS)

OTRS Open Technology Real Services

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



Scheduler is not running. Please contact your administrator!

Dashboard

Reminder Tickets

My locked tickets (0) | My watched tickets (0) | My responsibilities (0) | Tickets in My Queues (0) | All tickets (1)

		AGE	TICKET#	TITLE
none				

Escalated Tickets

My locked tickets (16) | My watched tickets (7) | My responsibilities (12) | Tickets in My Queues (13) | All tickets (37)   1 2 3 4

	AGE	TICKET#	TITLE
	13 h 29 m	[illegible]	testing - 111111
	5 h 20 m	[illegible]	Network Problem
	7 h 12 m	[illegible]	Test picture
	2 d 2 h	[illegible]	Wireless Connection problem
	2 d 2 h	[illegible]	Internet connection problem
	2 d 2 h	[illegible]	internet connection issue
	2 d 2 h	[illegible]	Network Problem
	3 d 20 h	[illegible]	razque de huevos al jefe
	4 d 2 h	[illegible]	razque de huevos al jefe
	12 d 1 h	[illegible]	Test

New Tickets

My locked tickets (0) | My watched tickets (0) | My responsibilities (0) | Tickets in My Queues (0) | All tickets (0)

		AGE	TICKET#	TITLE
none				

Open Tickets / Need to be answered

My locked tickets (16) | My watched tickets (7) | My responsibilities (13) | Tickets in My Queues (15) | All tickets (28)   1 2 3 4

	AGE	TICKET#	TITLE
	5 h 20 m	[illegible]	Network Problem
	7 h 12 m	[illegible]	Test picture
	2 d 2 h	[illegible]	internet connection issue
	2 d 2 h	[illegible]	Wireless Connection problem
	2 d 2 h	[illegible]	Internet connection problem
	2 d 2 h	[illegible]	Network Problem
	2 d 2 h	[illegible]	Network Security- Virus Issue
	2 d 2 h	[illegible]	Computer infected in virus
	2 d 2 h	[illegible]	Browser Default Homepage Issue
	4 d 2 h	[illegible]	razque de huevos al jefe

Ticket Queue Overview

COLA	NUEVO	ABIERTO	PENDIENTE DE RECORDATORIO	TOTALES
No se encontró ningún dato.				

Settings

7 Day Stats

Upcoming Events

[illegible] testing - 111111 (Reminder Reached in 21 h 45 m)
[illegible] ¡¡¡¡ PERREO A POCA LUZ ¡¡¡¡ OOO (QUINTA LINDA [...] (Reminder Reached in 10 d 8 h)

Latest updated FAQ articles

Teste 123
Hardware 11/04/2013 22:08
Entrada d'exemple
Hardware 10/23/2013 10:36
234234
Hardware 10/18/2013 15:25

Latest created FAQ articles

Entrada d'exemple
Hardware 10/23/2013 10:36
234234
Hardware 10/18/2013 15:25
Тестовая статья
Software 10/18/2013 11:04

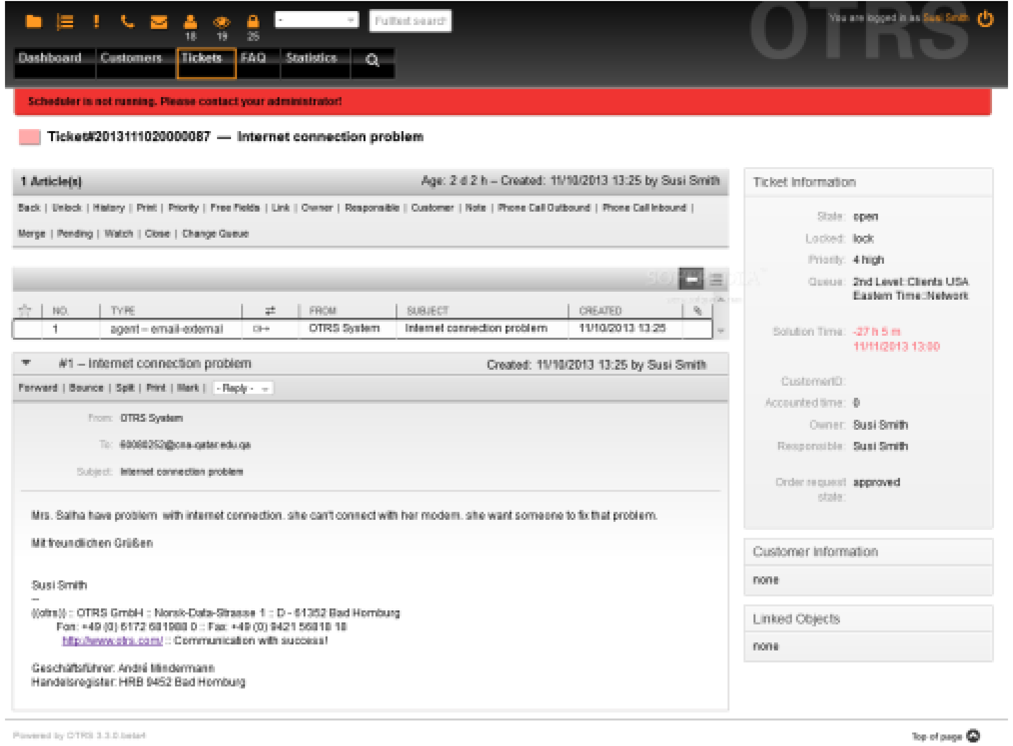
OTRS News

Release Notes: OTRS Help Desk 3.3.1
Release Notes: OTRS::ITSM 3.3.1
Release Notes: iPhoneHandle 1.3.1
Release Notes: FAQ 2.3.1
Release Notes: Survey Module 2.3.1
Release Notes: TimeAccounting 2.3.1

Powered by OTRS 3.3.0.beta4

Top of page

Dashboard



Scheduler is not running. Please contact your administrator!

Ticket#2013111020000087 — Internet connection problem

1 Article(s)   Age: 2 d 2 h – Created: 11/10/2013 13:25 by Susi Smith

Back | Unlock | History | Print | Priority | Free Fields | Link | Owner | Responsible | Customer | Note | Phone Call Outbound | Phone Call Inbound | Merge | Pending | Watch | Close | Change Queue

NO.	TYPE	⇄	FROM	SUBJECT	CREATED
1	agent – email-external	⊡→	OTRS System	Internet connection problem	11/10/2013 13:25

#1 – Internet connection problem   Created: 11/10/2013 13:25 by Susi Smith

Forward | Bounce | Split | Print | Mark | - Reply -

From: OTRS System
To: 60068252@cna-qatar.edu.qa
Subject: Internet connection problem

Mrs. Salha have problem with internet connection. she can't connect with her modem. she want someone to fix that problem.

Mit freundlichen Grüßen

Susi Smith
--
((otrs)) :: OTRS GmbH :: Norsk-Data-Strasse 1 :: D - 61352 Bad Homburg
Fon: +49 (0) 6172 681988 0 :: Fax: +49 (0) 9421 56818 18
http://www.otrs.com/ :: Communication with success!

Geschäftsführer: André Mindermann
Handelsregister: HRB 9452 Bad Homburg

Ticket Information

State: open
Locked: lock
Priority: 4 high
Queue: 2nd Level::Clients USA Eastern Time::Network
Solution Time: -27 h 5 m 11/11/2013 13:00
CustomerID:
Accounted time: 0
Owner: Susi Smith
Responsible: Susi Smith
Order request state: approved

Customer Information

none

Linked Objects

none

Powered by OTRS 3.3.0.beta4

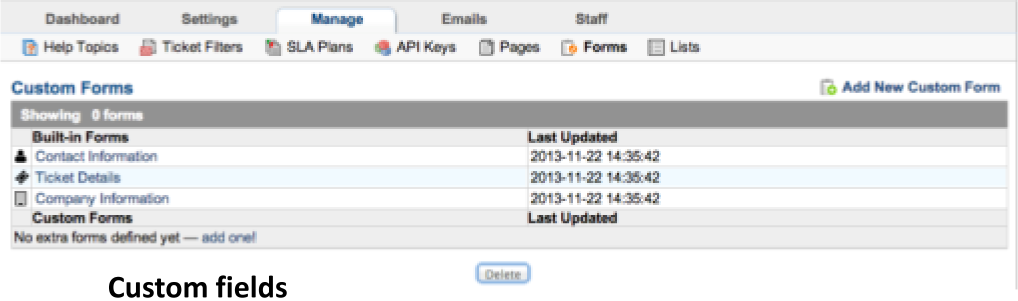
Top of page

Tickets

Alerting and Reporting

osTicket

- http://osticket.com

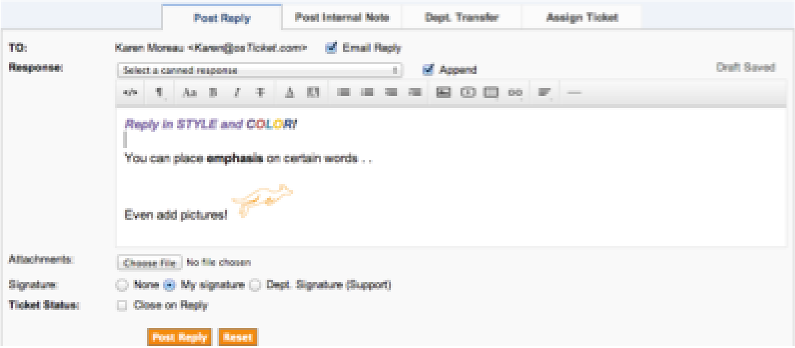


Custom Forms

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!	

Custom fields



TO: Karen Moreau <Karen@osTicket.com> ☑ Email Reply

Response: Select a canned response ☑ Append

Reply in STYLE and COLOR!

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

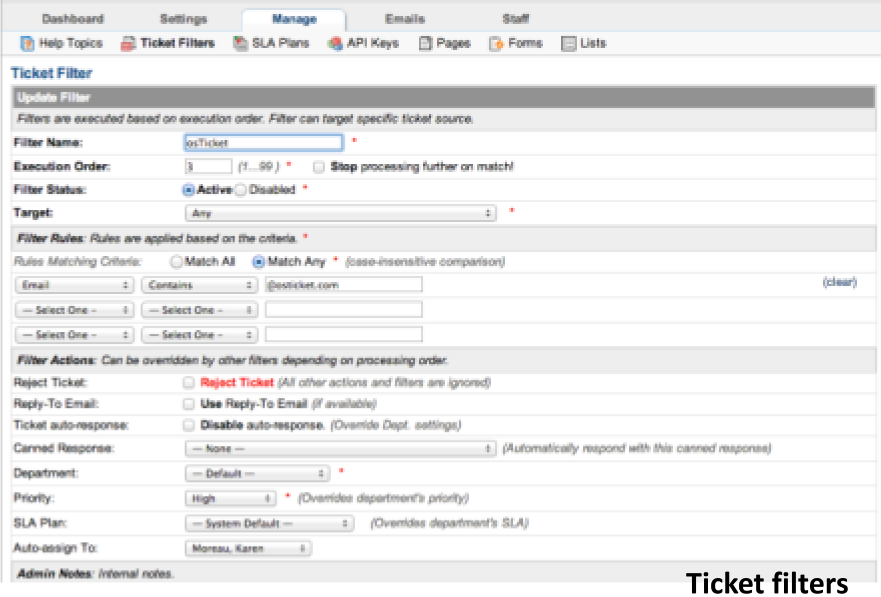
Even add pictures!

Attachments: No file chosen

Signature: ○ None ● My signature ○ Dept. Signature (Support)

Ticket Status: □ Close on Reply

Rich HTML



Ticket Filter

Update Filter

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

Filter Name: osTicket *

Execution Order: 3 (1...99) * □ **Stop** processing further on match!

Filter Status: ● Active ○ Disabled *

Target: Any *

***Filter Rules**: Rules are applied based on the criteria.* *

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

Email | Contains | @osticket.com

— Select One – | — Select One – |

— Select One – | — Select One – |

***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: — None — *(Automatically respond with this canned response)*

Department: — Default — *

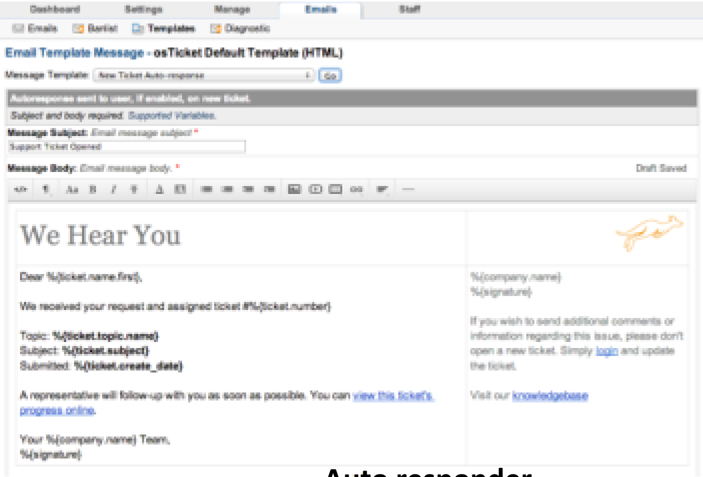
Priority: High * *(Overrides department's priority)*

SLA Plan: — System Default — *(Overrides department's SLA)*

Auto-assign To: Moreau, Karen

***Admin Notes**: Internal notes.*

Ticket filters



Email Template Message - osTicket Default Template (HTML)

Message Template: New Ticket Auto-response

Autoresponse 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.* *

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}

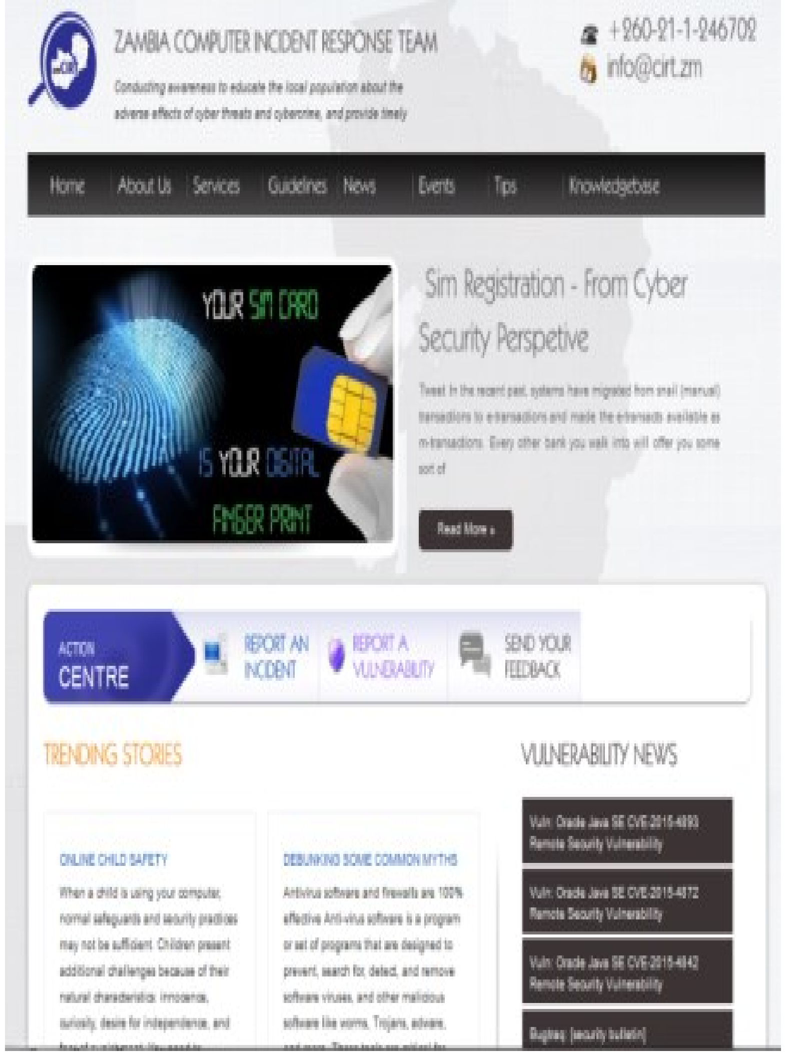
If you wish to send additional comments or information regarding this issue, please don't open a new ticket. Simply login and update the ticket.

Visit our knowledgebase

Auto responder

Alerting and Reporting

CSIRT Web Portal


ZAMBIA COMPUTER INCIDENT RESPONSE TEAM

Conducting awareness to educate the local population about the adverse effects of cyber threats and cybercrime, and provide timely

☎ +260-21-1-246702
info@cirt.zm

Sim Registration - From Cyber Security Perspetive

Tweet In the recent past, systems have migrated from snail (manual) transactions to e-transactions and made the e-transacts available as m-transactions. Every other bank you walk into will offer you some sort of

TRENDING STORIES

ONLINE CHILD SAFETY

When a child is using your computer, normal safeguards and security practices may not be sufficient. Children present additional challenges because of their natural characteristics: innocence, curiosity, desire for independence, and

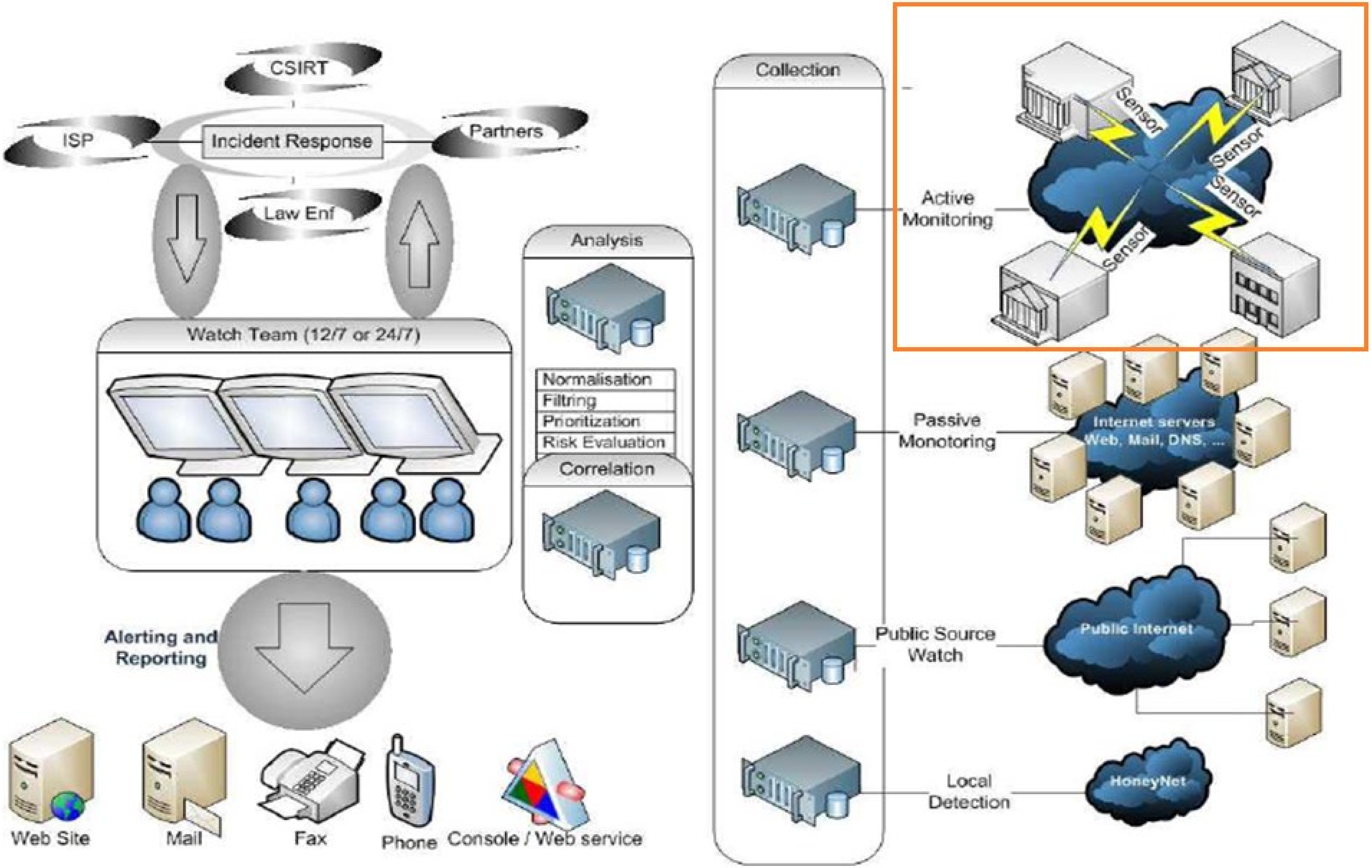
DEBUNKING SOME COMMON MYTHS

Antivirus software and firewalls are 100% effective Anti-virus software is a program or set of programs that are designed to prevent, search for, detect, and remove software viruses, and other malicious software like worms, Trojans, adware,

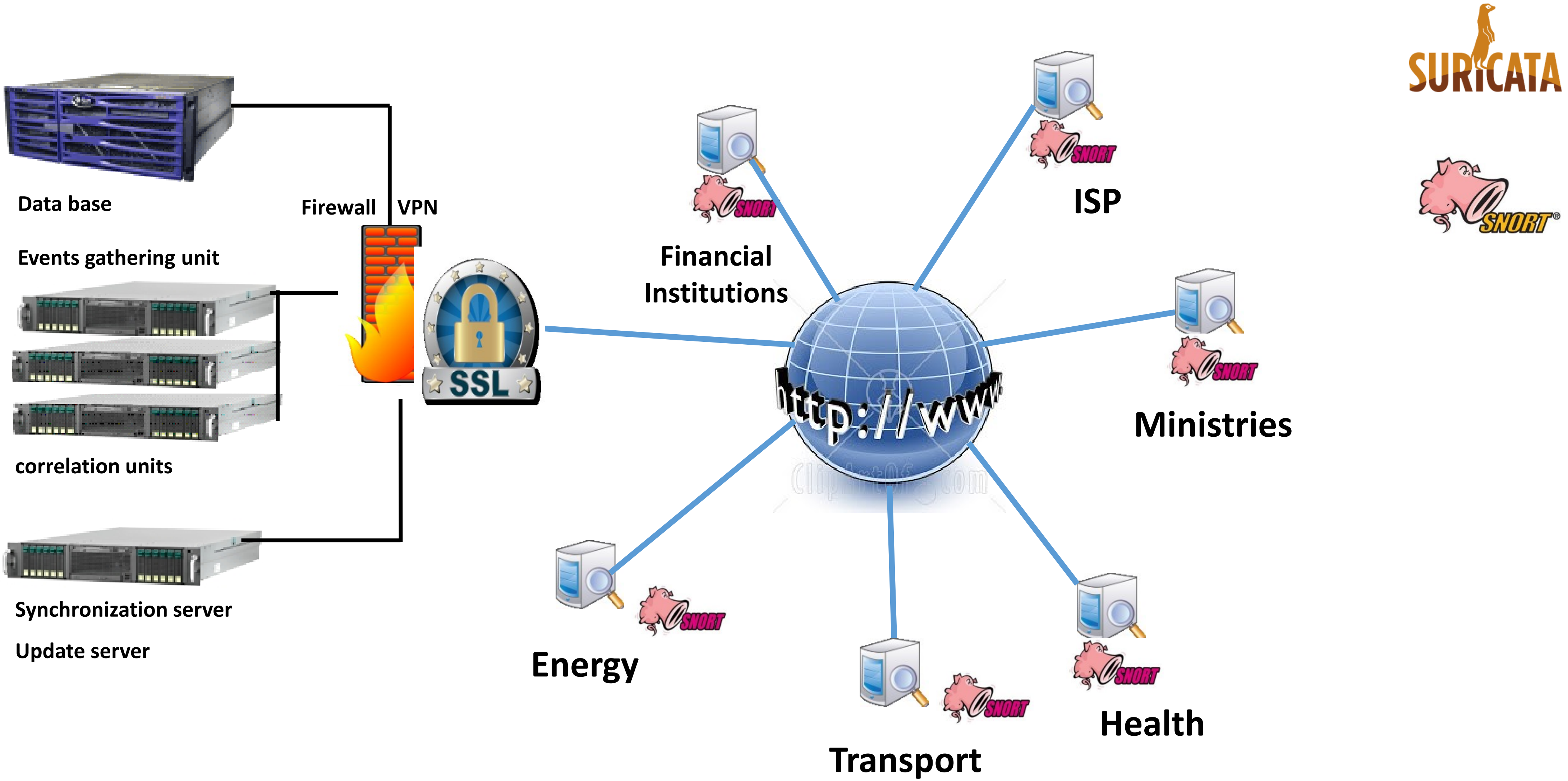
VULNERABILITY NEWS

- Vuln: Oracle Java SE CVE-2015-4893 Remote Security Vulnerability
- Vuln: Oracle Java SE CVE-2015-4872 Remote Security Vulnerability
- Vuln: Oracle Java SE CVE-2015-4842 Remote Security Vulnerability
- Bugtraq: [security bulletin]

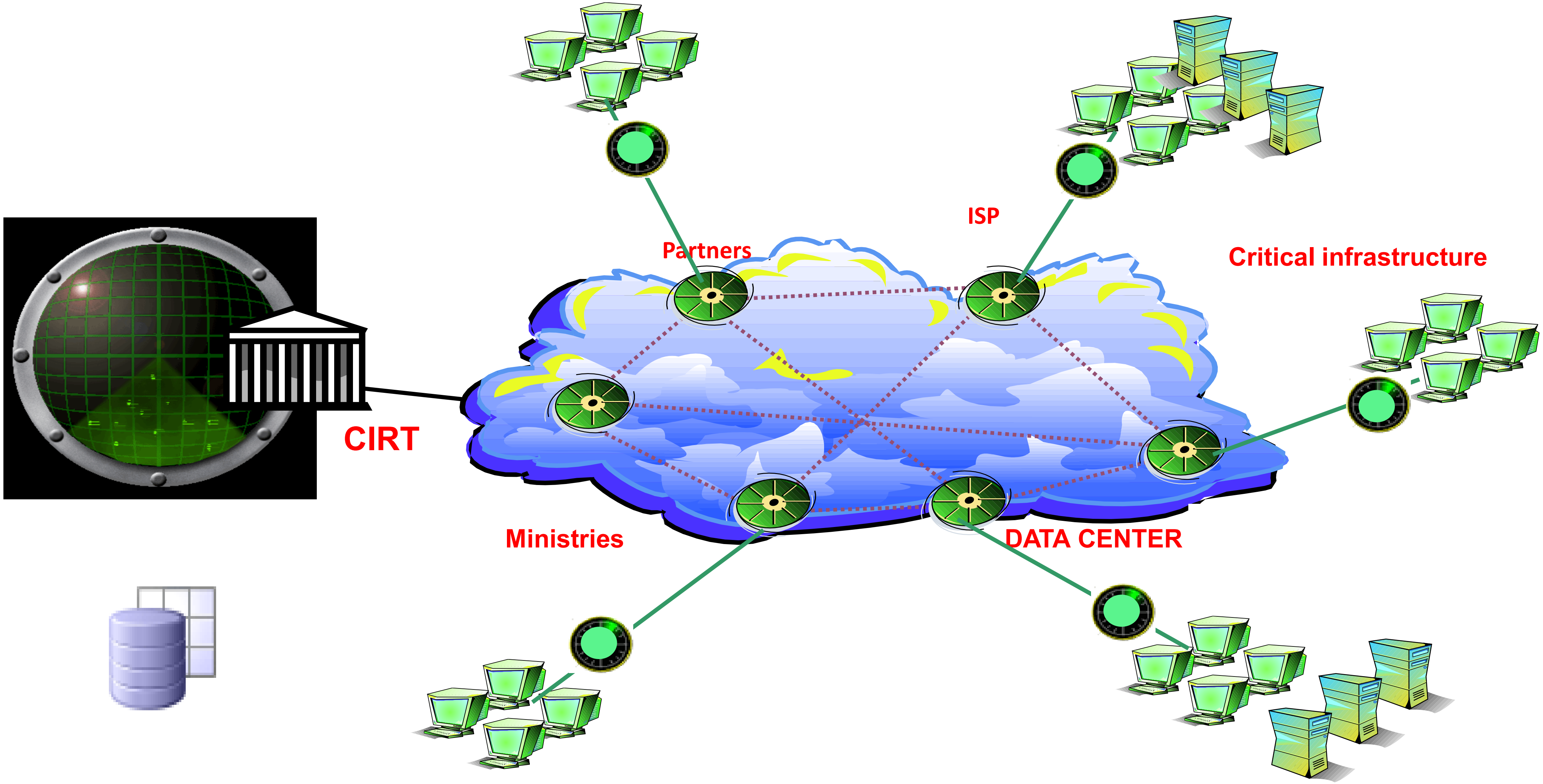
Incident Response Center



Active Monitoring

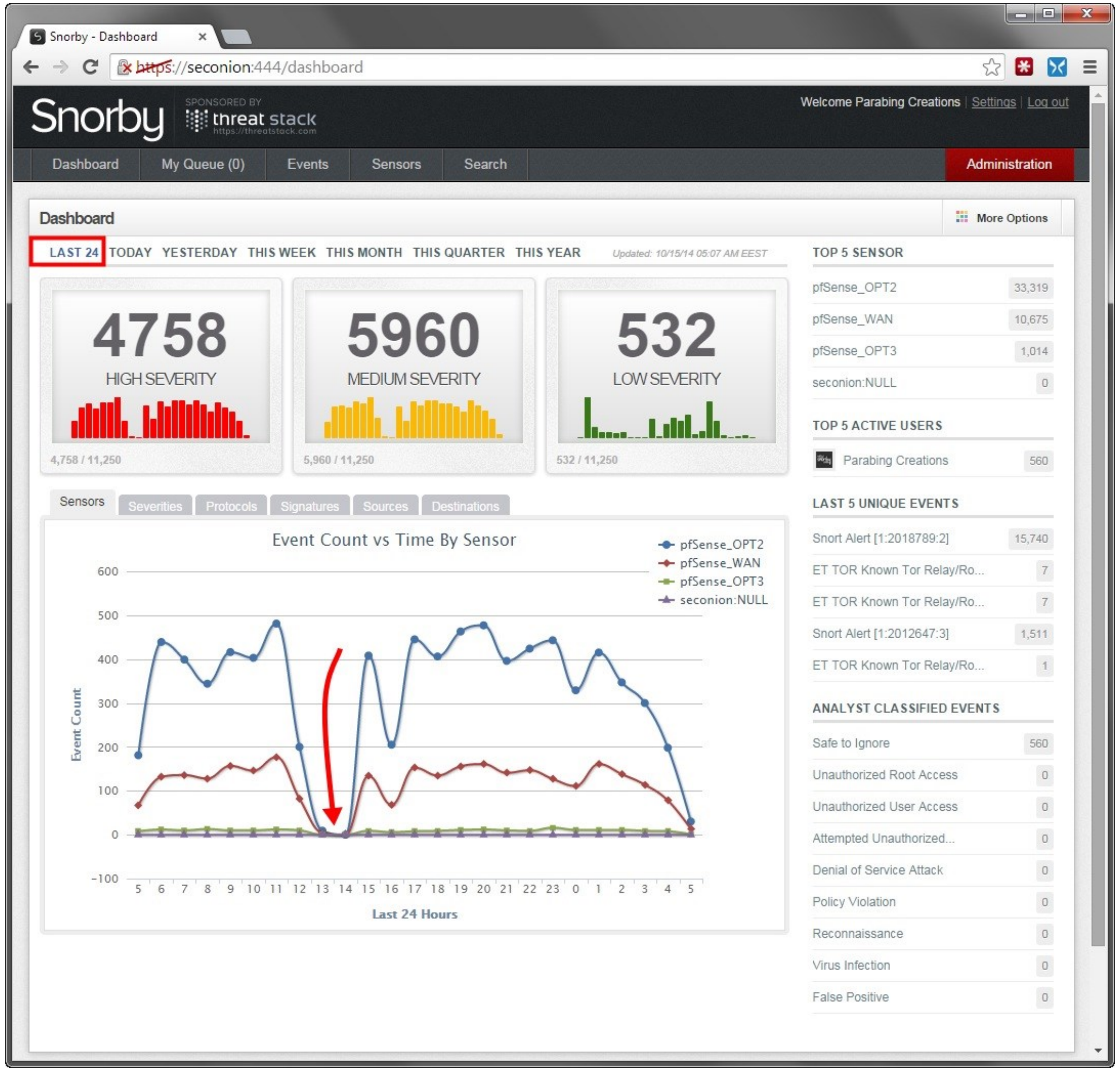


Active Monitoring



Active Monitoring

https://github.com/**Snorby**

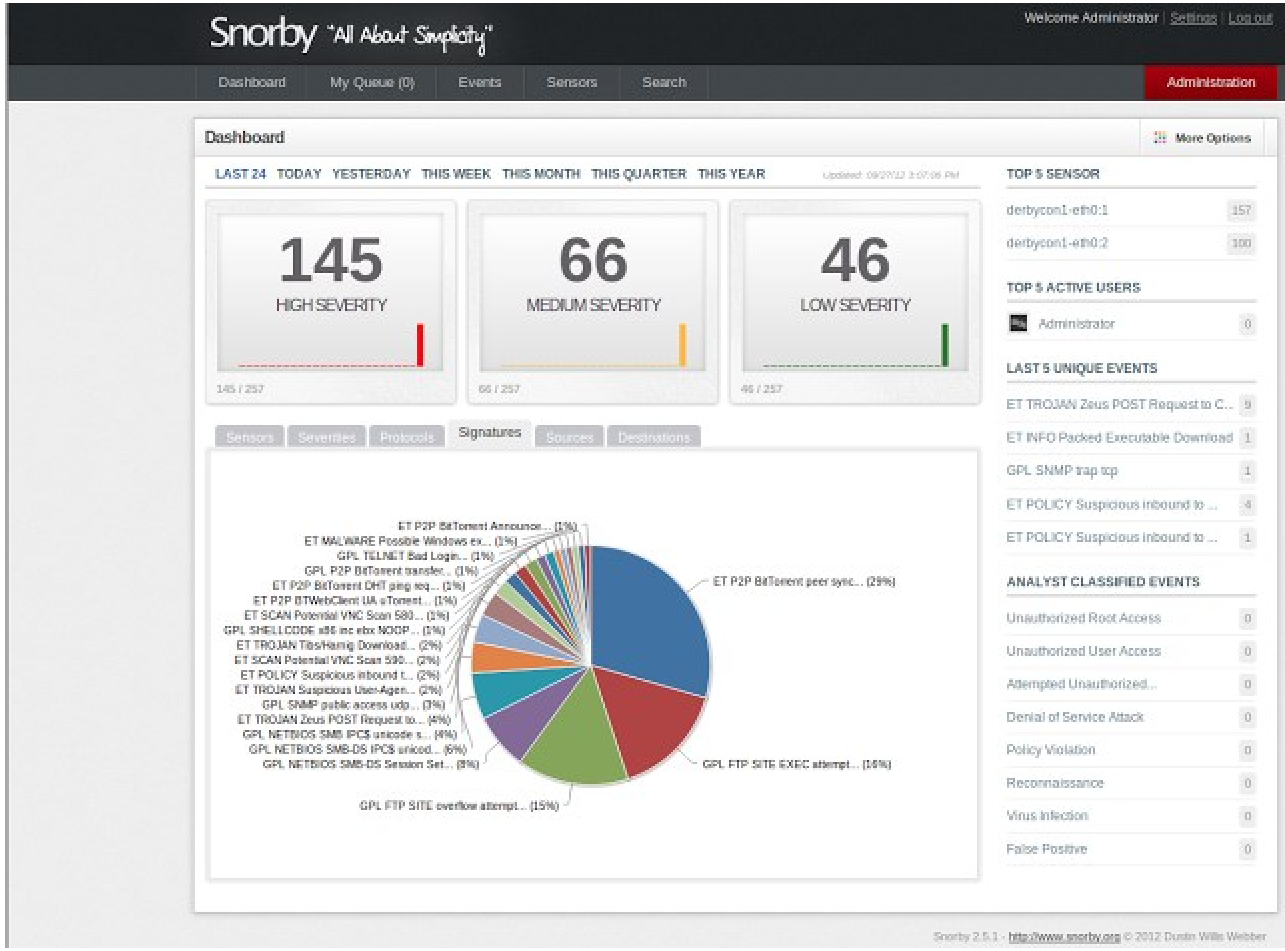


TOP 5 SENSOR	
pfSense_OPT2	33,319
pfSense_WAN	10,675
pfSense_OPT3	1,014
seconion:NULL	0

TOP 5 ACTIVE USERS	
Parabing Creations	560

LAST 5 UNIQUE EVENTS	
Snort Alert [1:2018789:2]	15,740
ET TOR Known Tor Relay/Ro...	7
ET TOR Known Tor Relay/Ro...	7
Snort Alert [1:2012647:3]	1,511
ET TOR Known Tor Relay/Ro...	1

ANALYST CLASSIFIED EVENTS	
Safe to Ignore	560
Unauthorized Root Access	0
Unauthorized User Access	0
Attempted Unauthorized...	0
Denial of Service Attack	0
Policy Violation	0
Reconnaissance	0
Virus Infection	0
False Positive	0


Snorby "All About Simplicity"
Welcome Administrator | Settings | Log out
Dashboard
My Queue (0)
Events
Sensors
Search
Administration
Dashboard
More Options
LAST 24
TODAY
YESTERDAY
THIS WEEK
THIS MONTH
THIS QUARTER
THIS YEAR
Updated: 09/27/12 3:07:06 PM
145
HIGH SEVERITY
145 / 257
66
MEDIUM SEVERITY
66 / 257
46
LOW SEVERITY
46 / 257
Sensors
Severities
Protocols
Signatures
Sources
Destinations
ET P2P BitTorrent Announce... (1%)
ET MALWARE Possible Windows ex... (1%)
GPL TELNET Bad Login... (1%)
GPL P2P BitTorrent transfer... (1%)
ET P2P BitTorrent DHT ping req... (1%)
ET P2P BTWebClient UA uTorrent... (1%)
ET SCAN Potential VNC Scan 580... (1%)
GPL SHELLCODE x86 inc ebx NOOP... (1%)
ET TROJAN Tibs/Harnig Download... (2%)
ET SCAN Potential VNC Scan 590... (2%)
ET POLICY Suspicious inbound t... (2%)
ET TROJAN Suspicious User-Agen... (2%)
GPL SNMP public access udp... (3%)
ET TROJAN Zeus POST Request to... (4%)
GPL NETBIOS SMB IPC$ unicode s... (4%)
GPL NETBIOS SMB-DS IPC$ unicod... (6%)
GPL NETBIOS SMB-DS Session Set... (8%)
ET P2P BitTorrent peer sync... (29%)
GPL FTP SITE EXEC attempt... (16%)
GPL FTP SITE overflow attempt... (15%)

TOP 5 SENSOR	
derbycon1-eth0:1	157
derbycon1-eth0:2	100

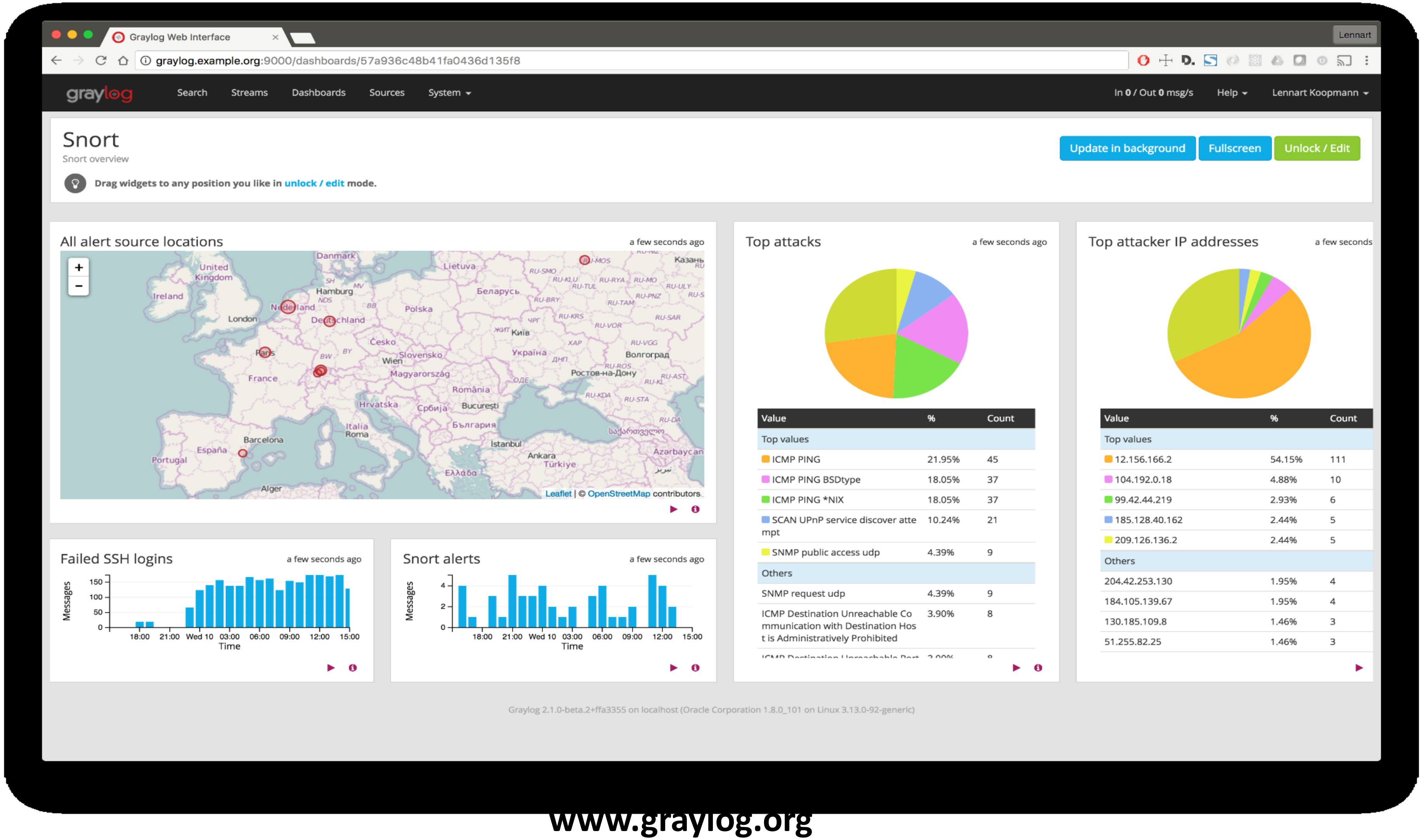
TOP 5 ACTIVE USERS	
Administrator	0

LAST 5 UNIQUE EVENTS	
ET TROJAN Zeus POST Request to C...	9
ET INFO Packed Executable Download	1
GPL SNMP trap tcp	1
ET POLICY Suspicious inbound to ...	4
ET POLICY Suspicious inbound to ...	1

ANALYST CLASSIFIED EVENTS	
Unauthorized Root Access	0
Unauthorized User Access	0
Attempted Unauthorized...	0
Denial of Service Attack	0
Policy Violation	0
Reconnaissance	0
Virus Infection	0
False Positive	0

Snorby 2.5.1 - http://www.snorby.org © 2012 Dustin Willis Webber

Active Monitoring



Snort

Snort overview

Drag widgets to any position you like in unlock / edit mode.

All alert source locations — a few seconds ago

Top attacks — a few seconds ago

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 — a few seconds

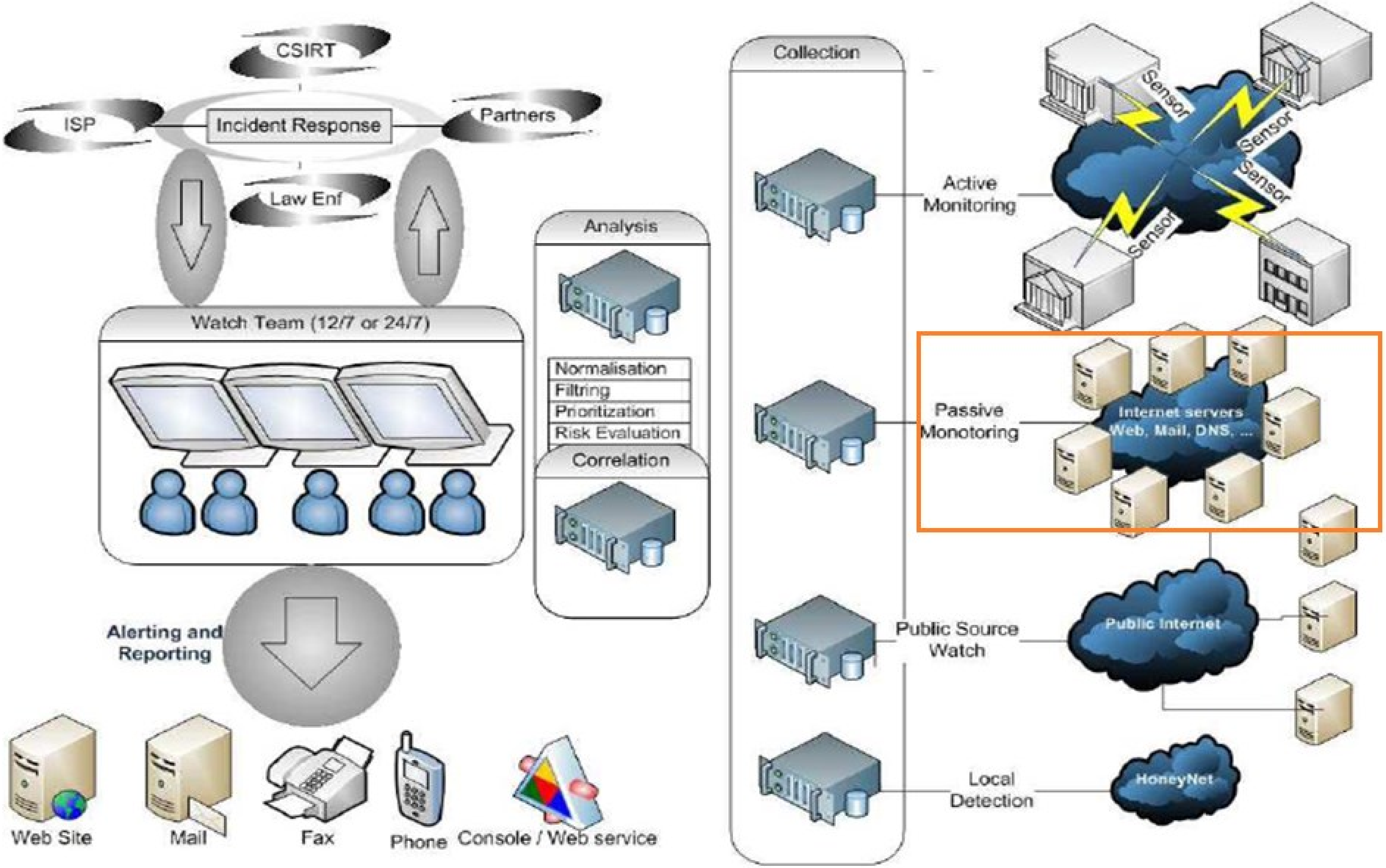
Value	%	Count
Top values		
🟧 12.156.166.2	54.15%	111
🟪 104.192.0.18	4.88%	10
🟩 99.42.44.219	2.93%	6
🟦 185.128.40.162	2.44%	5
🟨 209.126.136.2	2.44%	5
Others		
204.42.253.130	1.95%	4
184.105.139.67	1.95%	4
130.185.109.8	1.46%	3
51.255.82.25	1.46%	3

Failed SSH logins — a few seconds ago

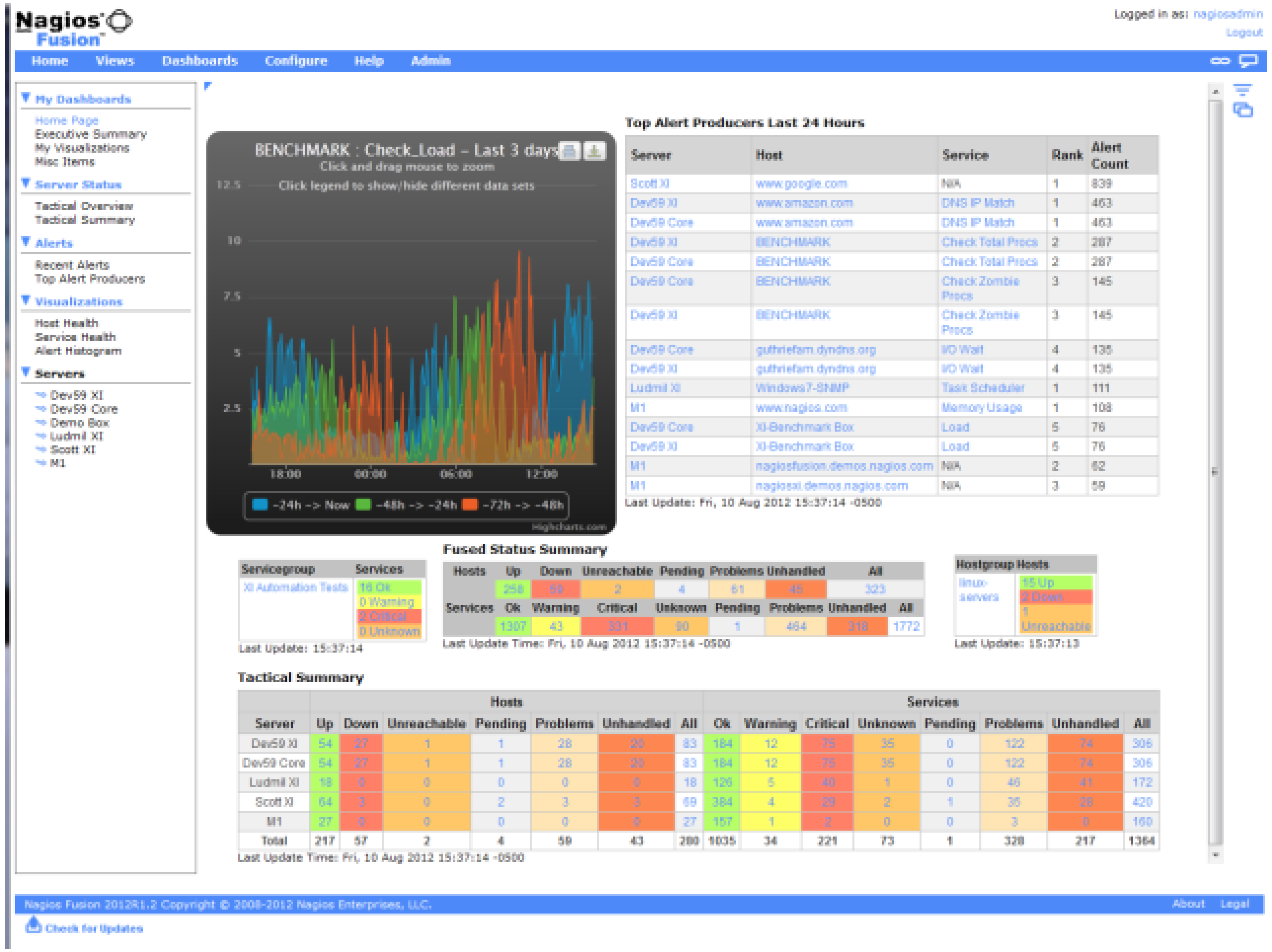
Snort alerts — a few seconds ago

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



Top Alert Producers Last 24 Hours

Server	Host	Service	Rank	Alert Count
Scott XI	www.google.com	N/A	1	839
Dev59 XI	www.amazon.com	DNS IP Match	1	463
Dev59 Core	www.amazon.com	DNS IP Match	1	463
Dev59 XI	BENCHMARK	Check Total Procs	2	287
Dev59 Core	BENCHMARK	Check Total Procs	2	287
Dev59 Core	BENCHMARK	Check Zombie Procs	3	145
Dev59 XI	BENCHMARK	Check Zombie Procs	3	145
Dev59 Core	guthriefam.dyndns.org	I/O Wait	4	135
Dev59 XI	guthriefam.dyndns.org	I/O Wait	4	135
Ludmil XI	Windows7-SNMP	Task Scheduler	1	111
M1	www.nagios.com	Memory Usage	1	108
Dev59 Core	XI-Benchmark Box	Load	5	76
Dev59 XI	XI-Benchmark Box	Load	5	76
M1	nagiosfusion.demos.nagios.com	N/A	2	62
M1	nagiosxi.demos.nagios.com	N/A	3	59

Last Update: Fri, 10 Aug 2012 15:37:14 -0500

Servicegroup	Services
XI Automation Tests	16 Ok 0 Warning 2 Critical 0 Unknown

Last Update: 15:37:14

Fused Status Summary

Hosts	Up	Down	Unreachable	Pending	Problems	Unhandled	All
	258	59	2	4	61	45	323
Services	**Ok**	**Warning**	**Critical**	**Unknown**	**Pending**	**Problems**	**Unhandled**	**All**
	1307	43	331	90	1	464	318	1772

Last Update Time: Fri, 10 Aug 2012 15:37:14 -0500

Hostgroup	Hosts
linux-servers	15 Up 2 Down 1 Unreachable

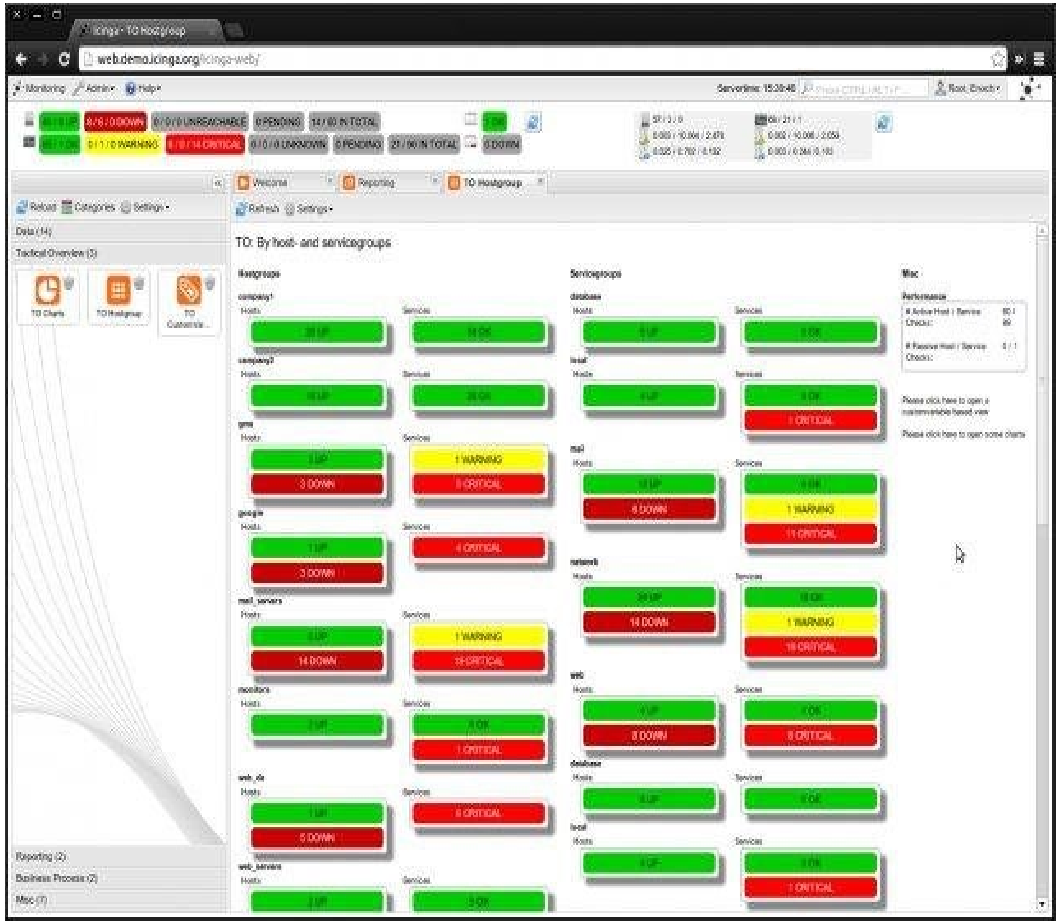
Last Update: 15:37:13

Tactical Summary

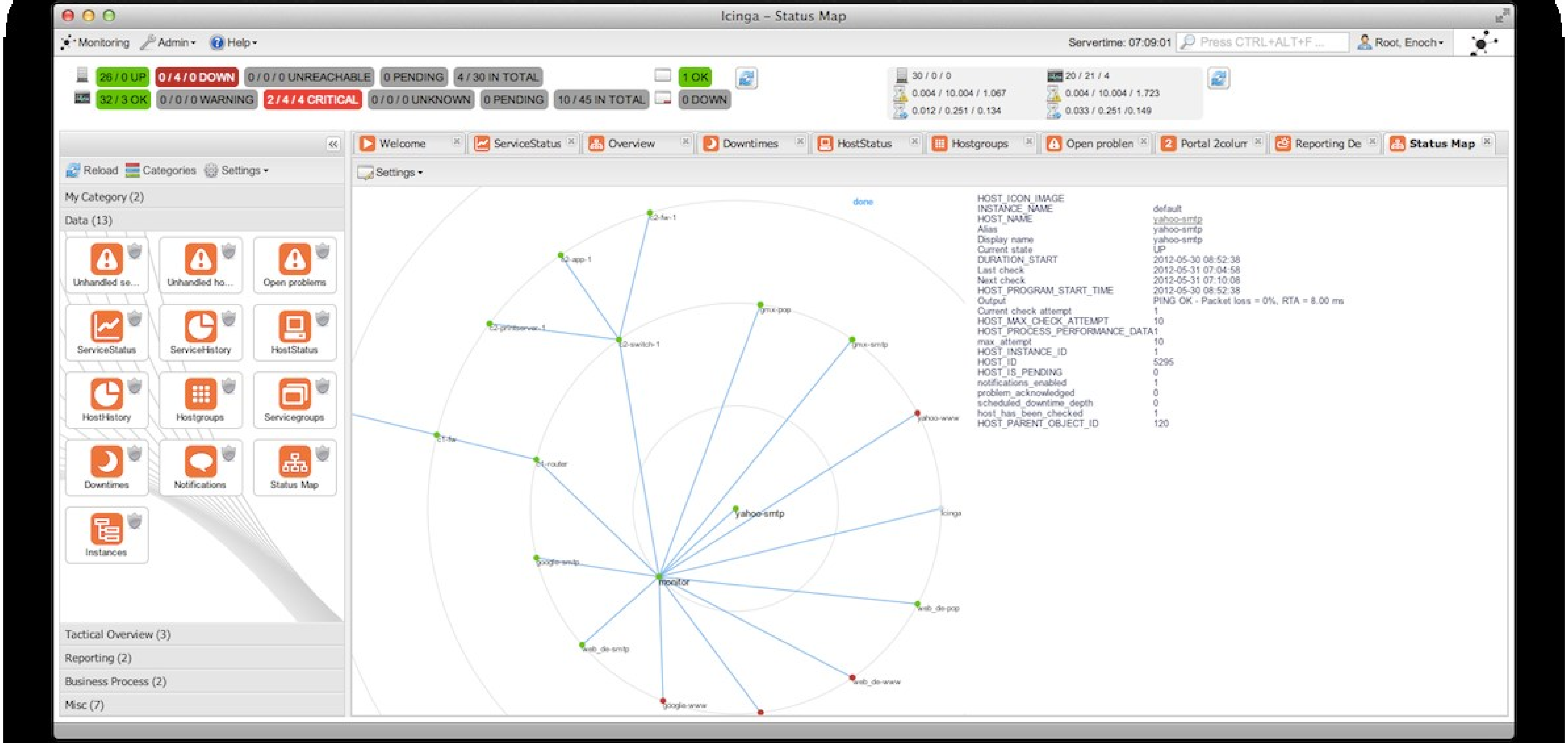
	Hosts							Services							
Server	Up	Down	Unreachable	Pending	Problems	Unhandled	All	Ok	Warning	Critical	Unknown	Pending	Problems	Unhandled	All
Dev59 XI	54	27	1	1	28	20	83	184	12	75	35	0	122	74	306
Dev59 Core	54	27	1	1	28	20	83	184	12	75	35	0	122	74	306
Ludmil XI	18	0	0	0	0	0	18	126	5	40	1	0	46	41	172
Scott XI	64	3	0	2	3	3	69	384	4	29	2	1	35	28	420
M1	27	0	0	0	0	0	27	157	1	2	0	0	3	0	160
Total	217	57	2	4	59	43	280	1035	34	221	73	1	328	217	1364

Last Update Time: Fri, 10 Aug 2012 15:37:14 -0500

Nagios Fusion 2012R1.2 Copyright © 2008-2012 Nagios Enterprises, LLC.

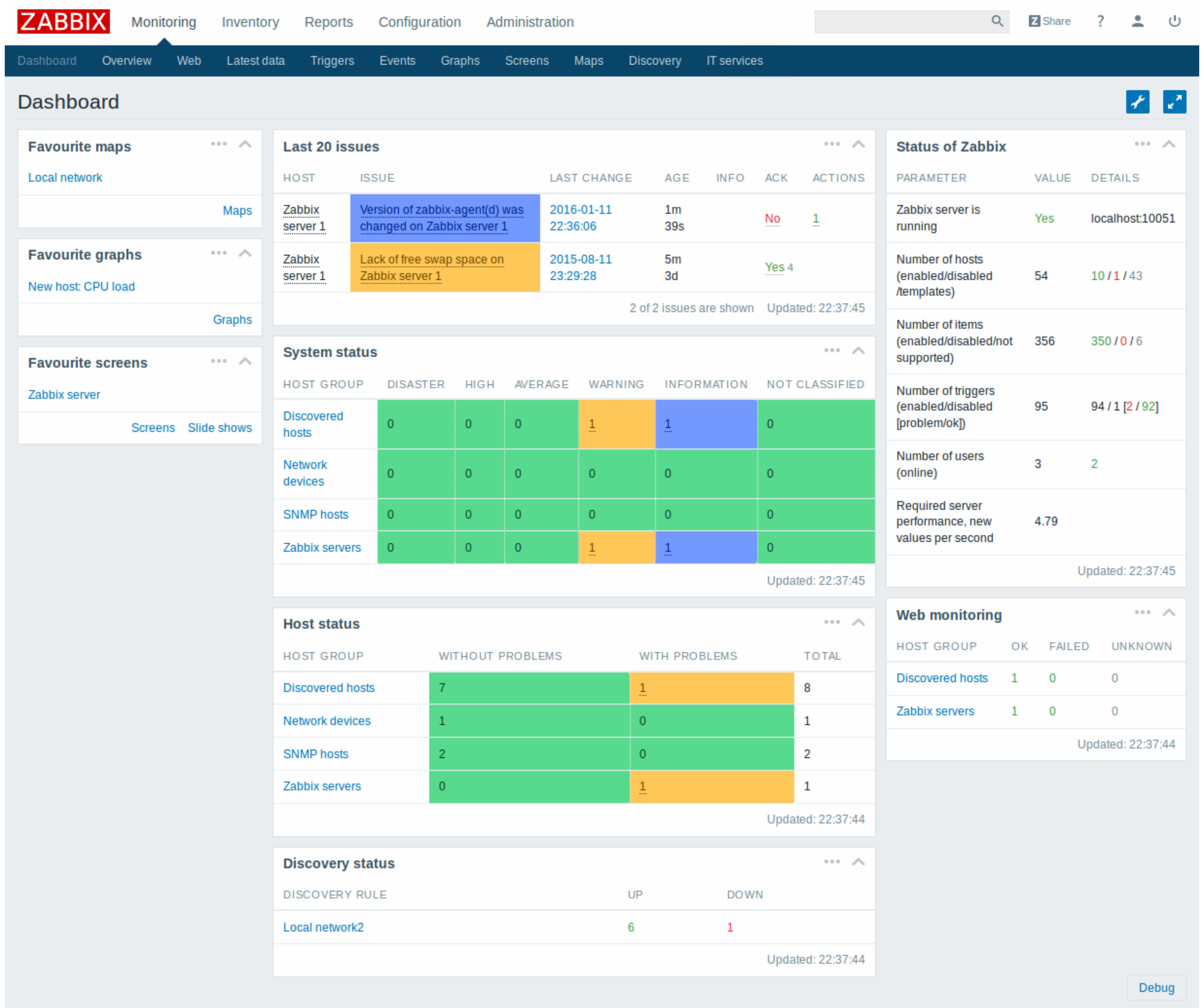


Passive Monitoring



```
HOST_ICON_IMAGE
INSTANCE_NAME                    default
HOST_NAME                        yahoo-smtp
Alias                            yahoo-smtp
Display name                     yahoo-smtp
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



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	

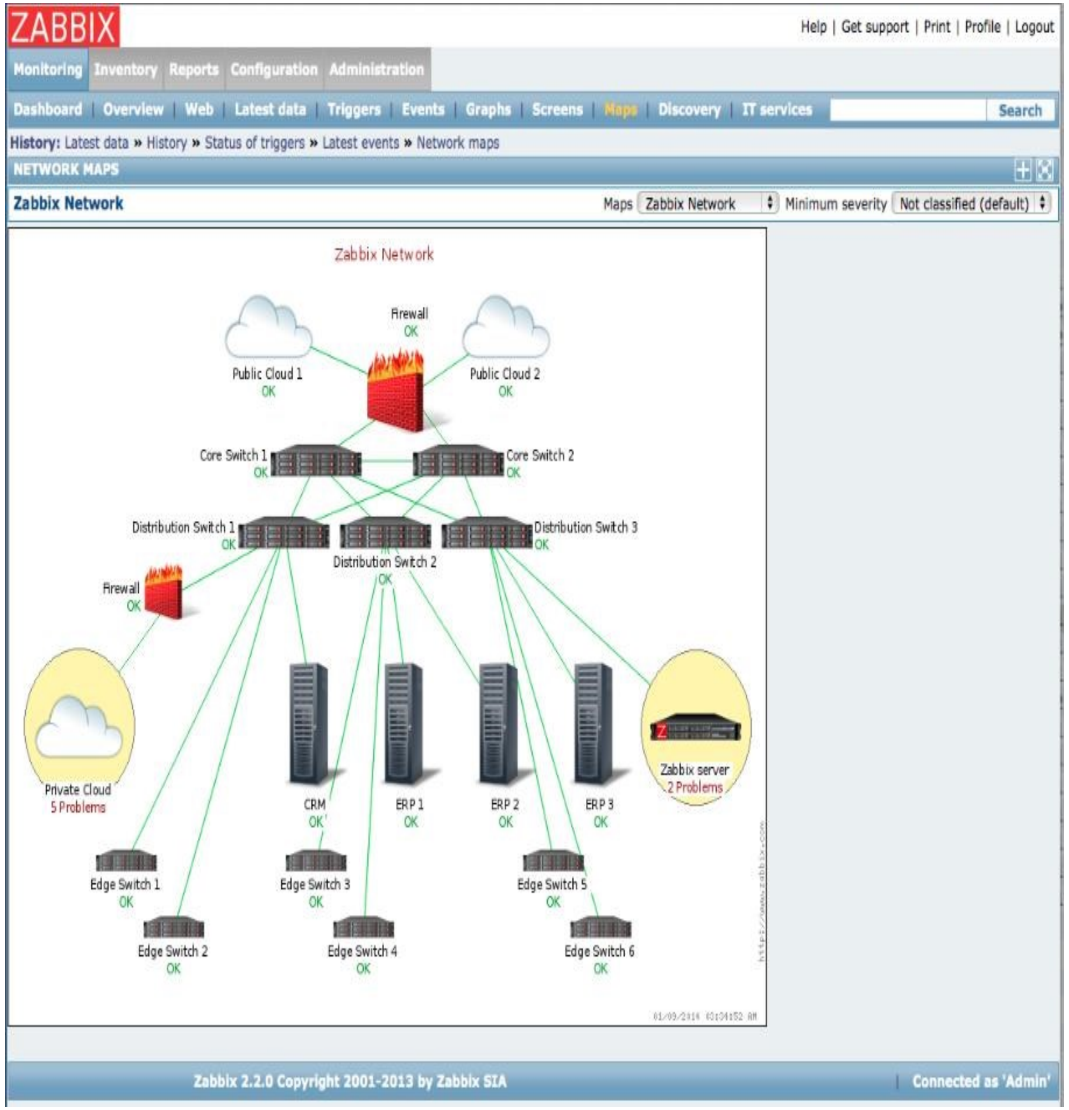
Updated: 22:37:45

Web monitoring

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

Updated: 22:37:44

Debug



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

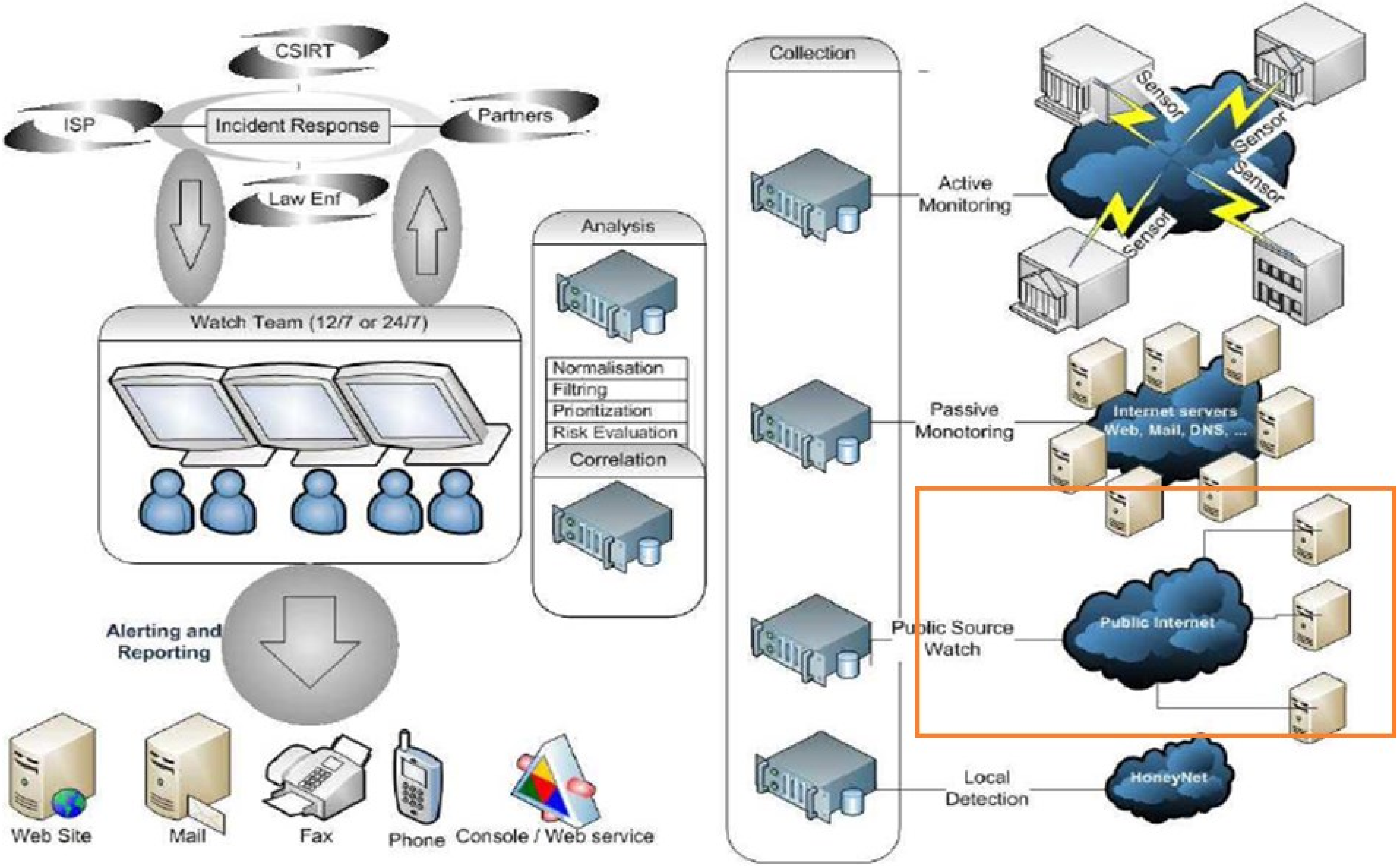
Zabbix Network

Maps: Zabbix Network Minimum severity: Not classified (default)

Zabbix 2.2.0 Copyright 2001-2013 by Zabbix SIA

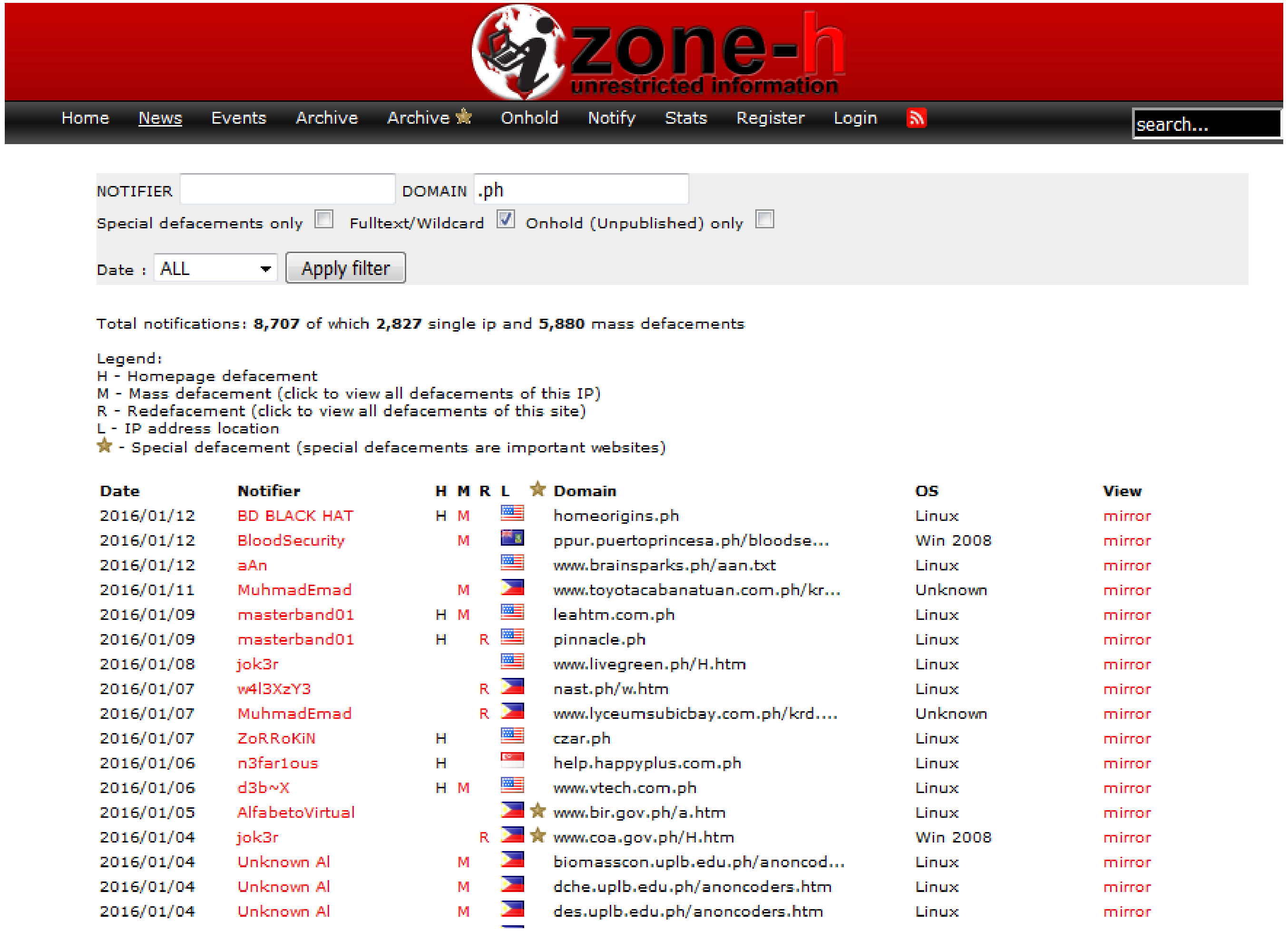
Connected as 'Admin'

Incident Response Center



Public Feeds

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



NOTIFIER DOMAIN .ph

Special defacements only □ Fulltext/Wildcard ☑ Onhold (Unpublished) only □

Date : ALL Apply filter

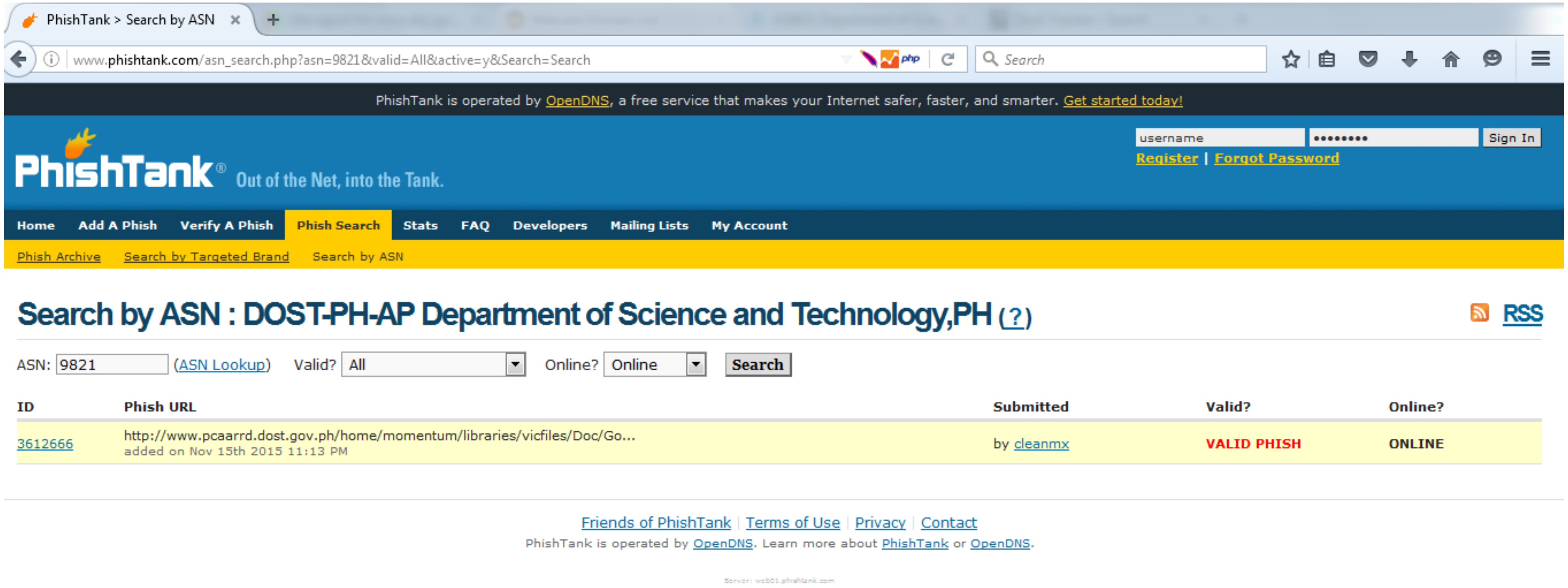
Total notifications: **8,707** of which **2,827** single ip and **5,880** mass defacements

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
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: 9821 (ASN Lookup) Valid? All Online? Online **Search**

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

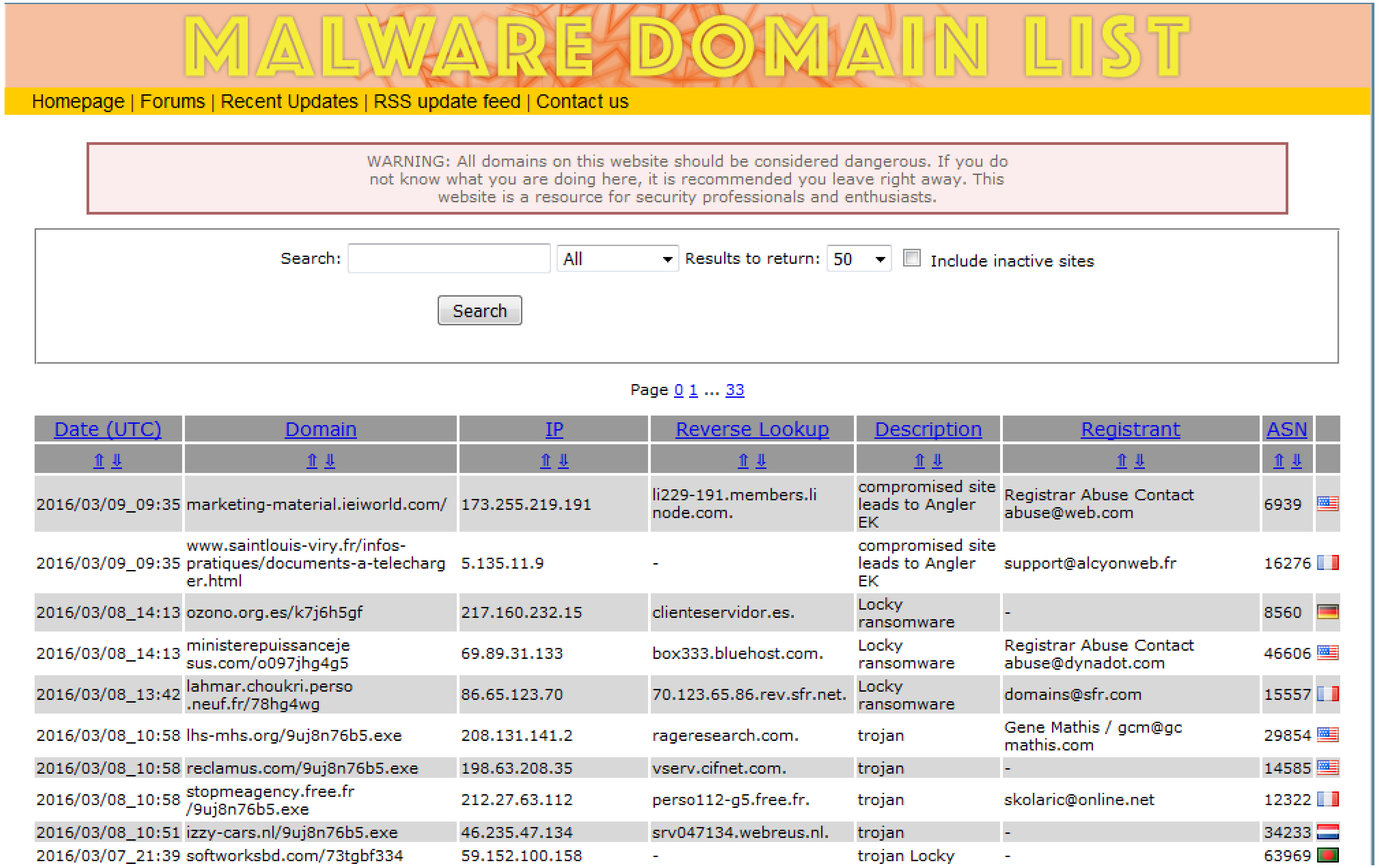
Friends of PhishTank | Terms of Use | Privacy | Contact

PhishTank is operated by OpenDNS. Learn more about PhishTank or OpenDNS.

Server: web01.phishtank.com

Public Feeds

- Malware
  - https://www.malwaredomainlist.com/mdl.php



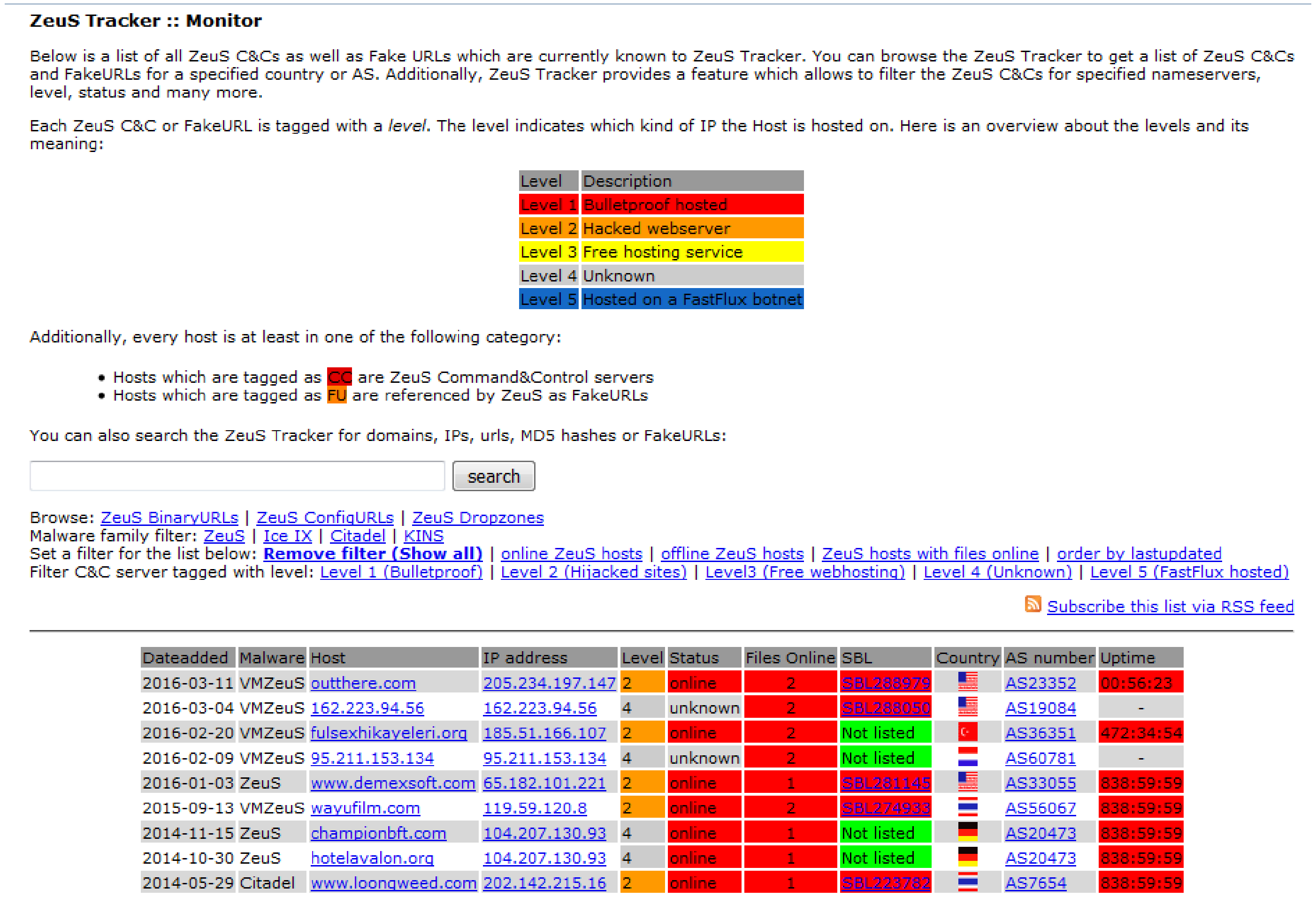
WARNING: All domains on this website should be considered dangerous. If you do not know what you are doing here, it is recommended you leave right away. This website is a resource for security professionals and enthusiasts.

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.linode.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-telecharger.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	ministerepuissancejesus.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@gcmathis.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:

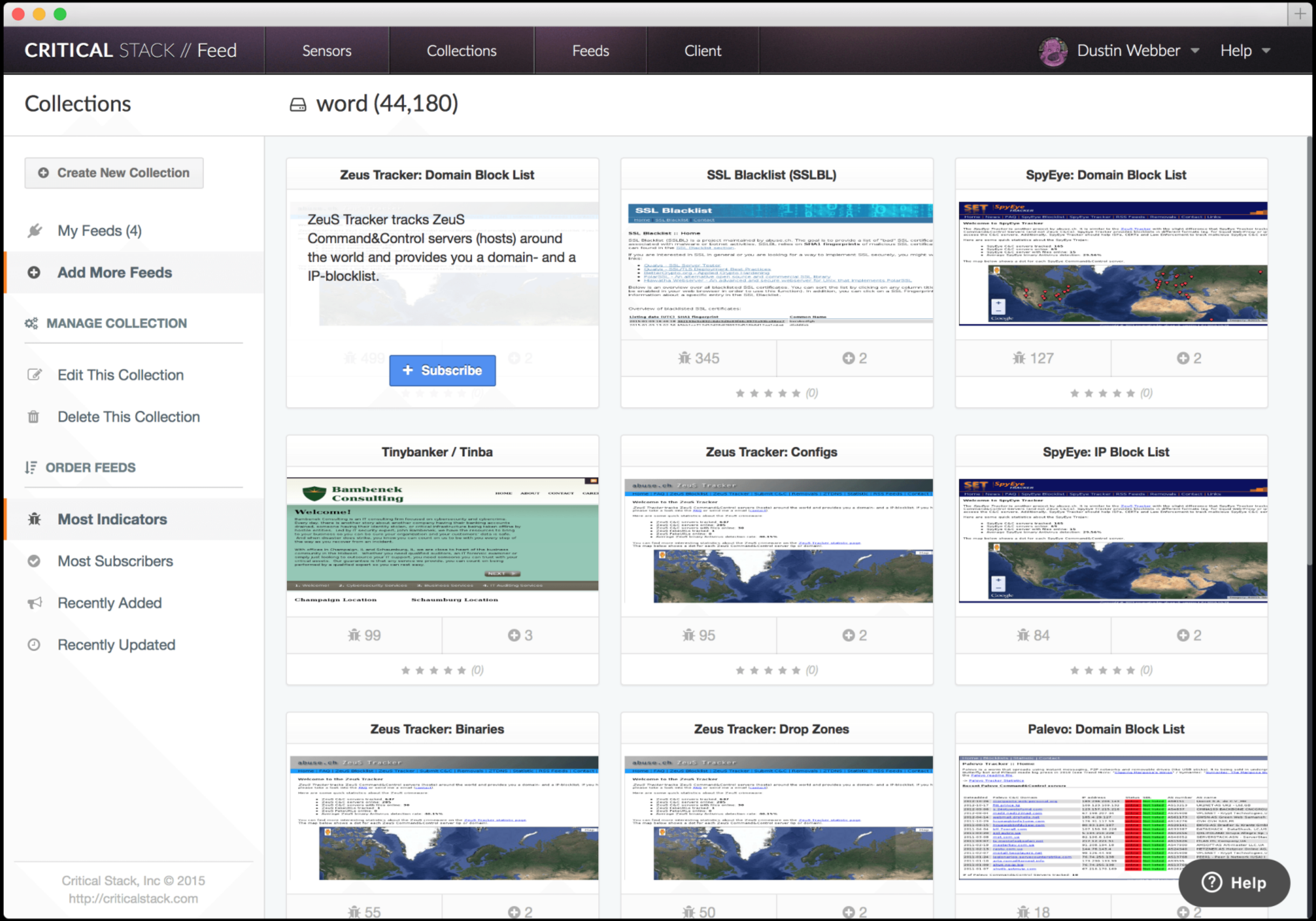
search

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	SBL288979	🇺🇸	AS23352	00:56:23
2016-03-04	VMZeuS	162.223.94.56	162.223.94.56	4	unknown	2	SBL288050	🇺🇸	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	SBL281145	🇺🇸	AS33055	838:59:59
2015-09-13	VMZeuS	wayufilm.com	119.59.120.8	2	online	2	SBL274933	🇹🇭	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	SBL223782	🇹🇭	AS7654	838:59:59

Public Feeds



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

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

Zeus Tracker: Domain Block List

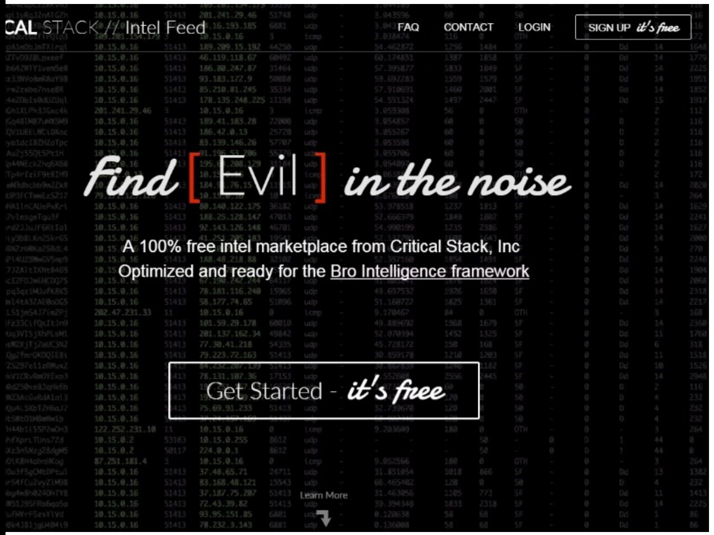
ZeuS Tracker tracks ZeuS Command&Control servers (hosts) around the world and provides you a domain- and a IP-blocklist.

+ Subscribe

Zeus Tracker: Domain Block List	499	2	
SSL Blacklist (SSLBL)	345	2	★★★★★ (0)
SpyEye: Domain Block List	127	2	★★★★★ (0)
Tinybanker / Tinba	99	3	★★★★★ (0)
Zeus Tracker: Configs	95	2	★★★★★ (0)
SpyEye: IP Block List	84	2	★★★★★ (0)
Zeus Tracker: Binaries	55	2	
Zeus Tracker: Drop Zones	50	2	
Palevo: Domain Block List	18	2	

? Help

criticalstack®



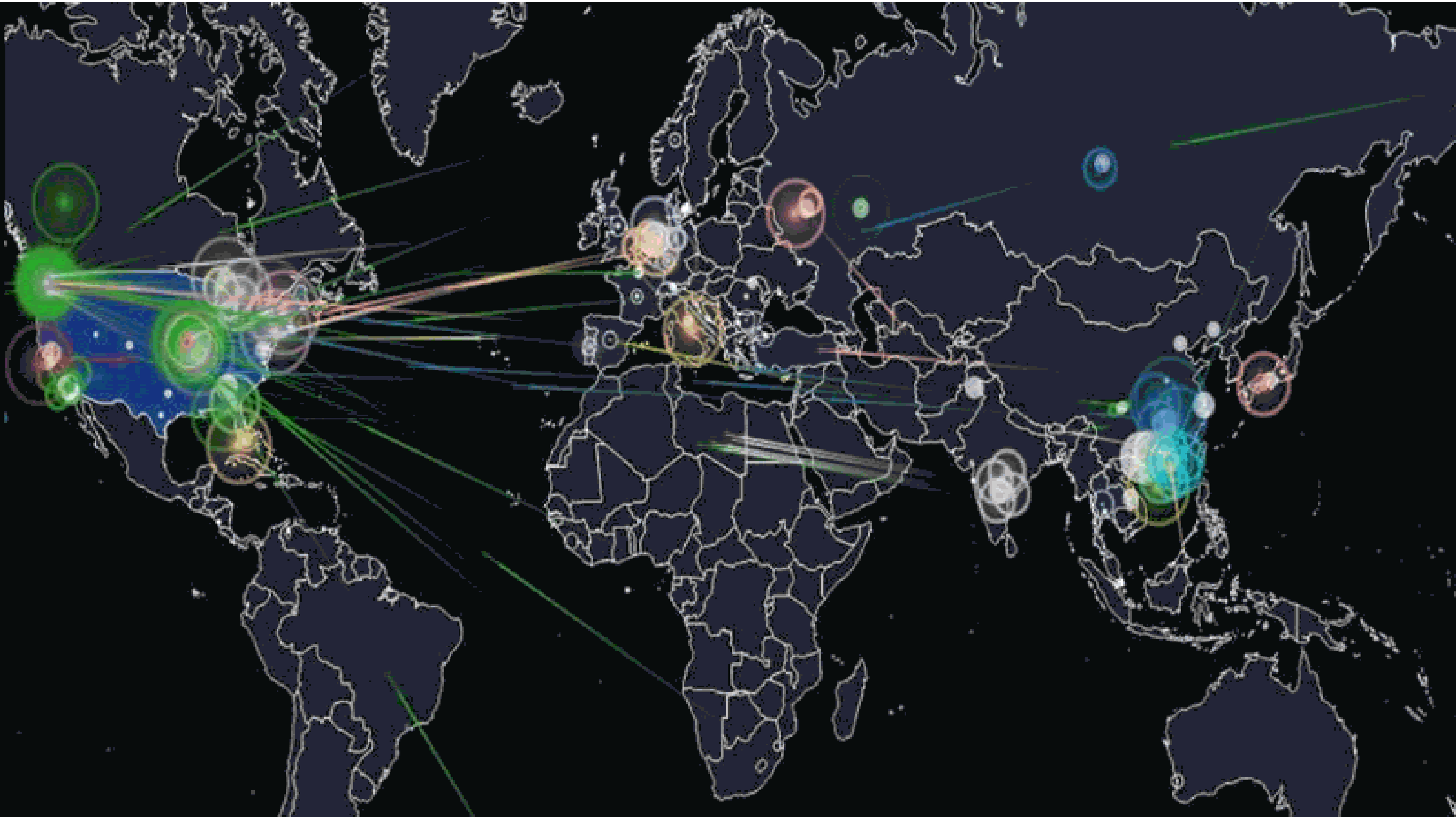
CAL STACK // Intel Feed | FAQ | CONTACT | LOGIN | SIGN UP it's free

Find [Evil] in the noise

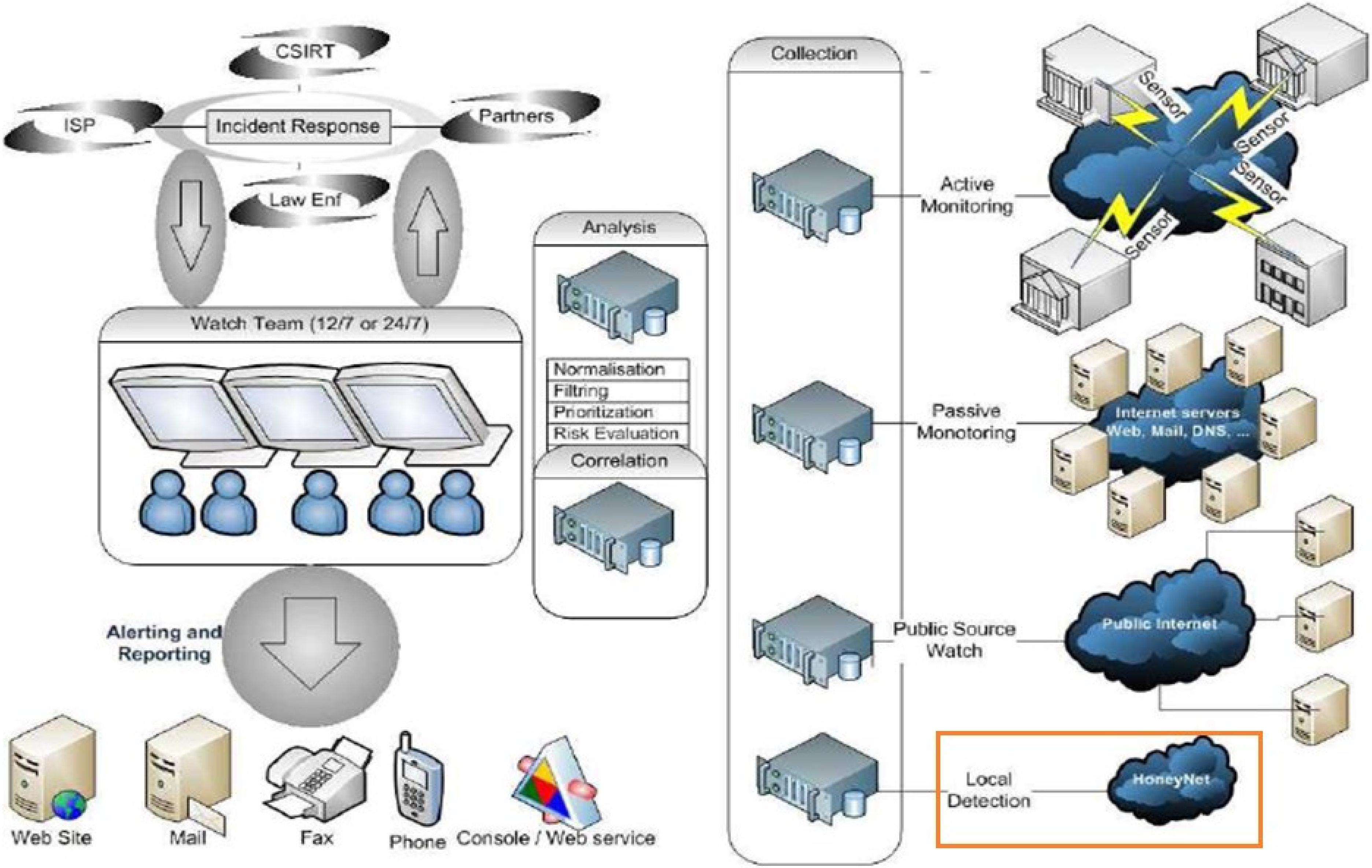
A 100% free intel marketplace from Critical Stack, Inc
Optimized and ready for the Bro Intelligence framework

Get Started - it's free

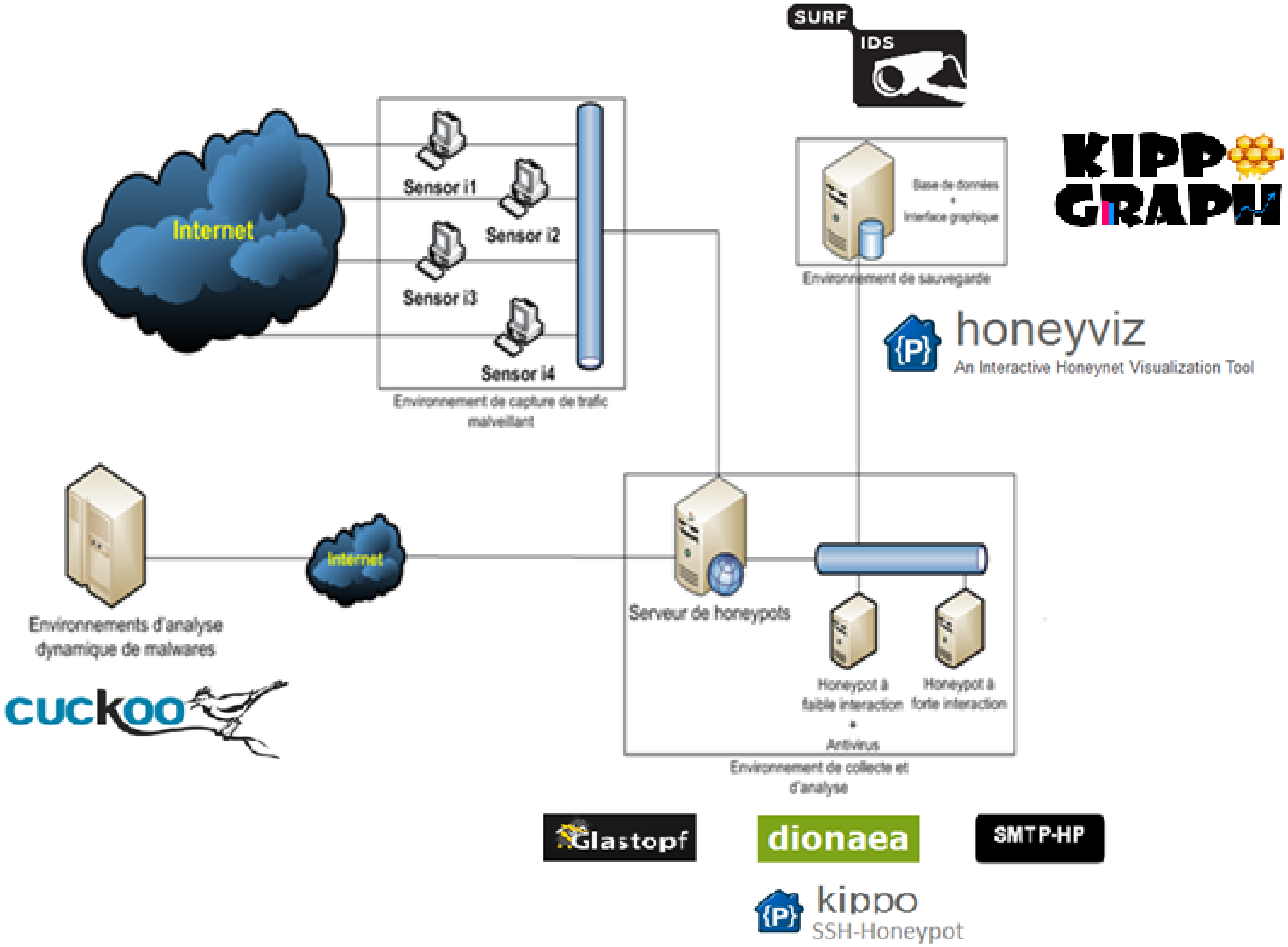
Learn More



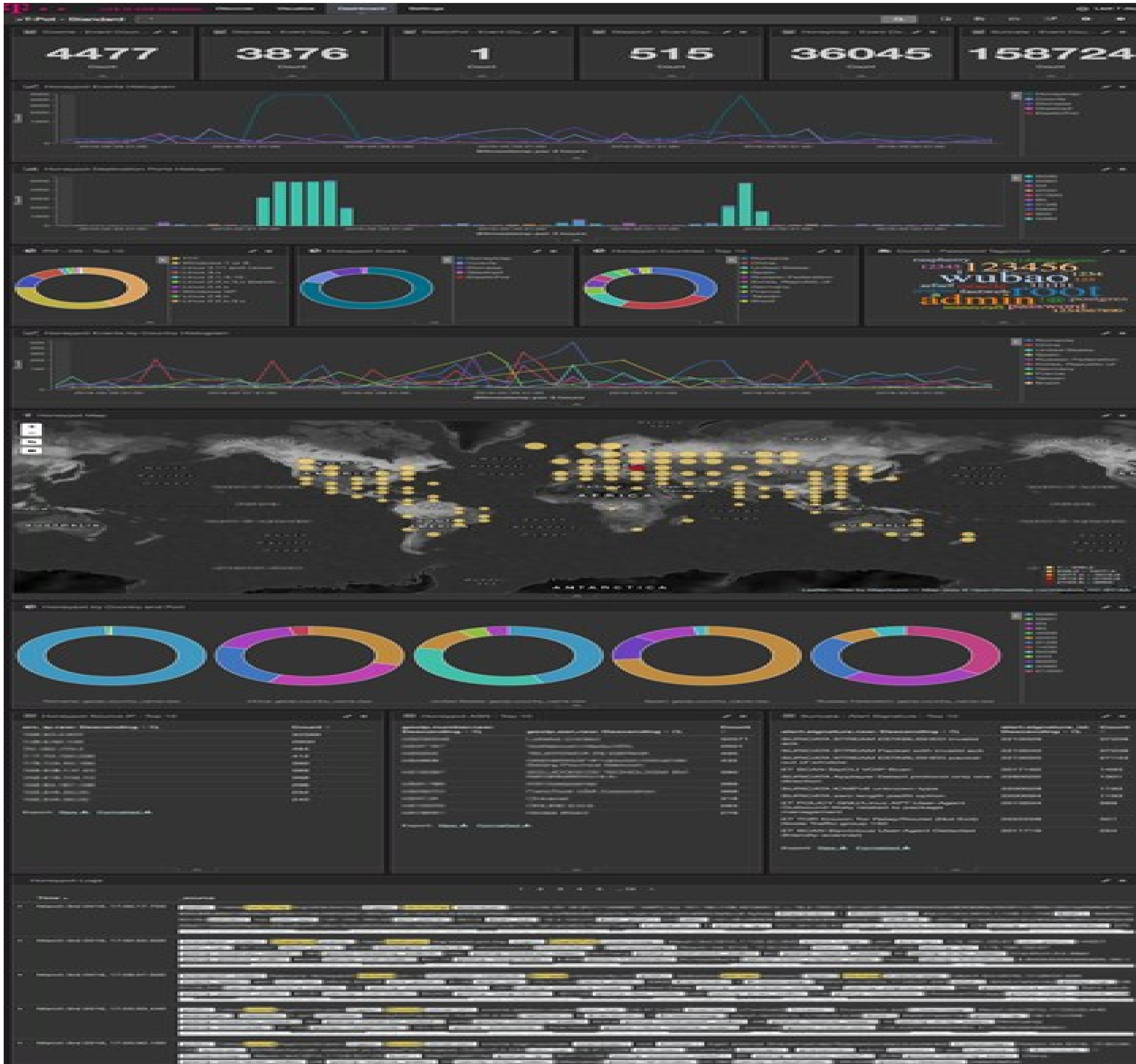
Incident Response Center



HoneyNet Platforms


SURF IDS
Internet
Sensor i1
Sensor i2
Sensor i3
Sensor i4
Environnement de capture de trafic malveillant
Base de données
+
Interface graphique
Environnement de sauvegarde
KIPPO GRAPH
honeyviz
An Interactive Honeynet Visualization Tool
Internet
Environnements d'analyse dynamique de malwares
cuckoo
Serveur de honeypots
Honeypot à faible interaction
+
Antivirus
Honeypot à forte interaction
Environnement de collecte et d'analyse
Glastopf
dionaea
SMTP-HP
kippo
SSH-Honeypot

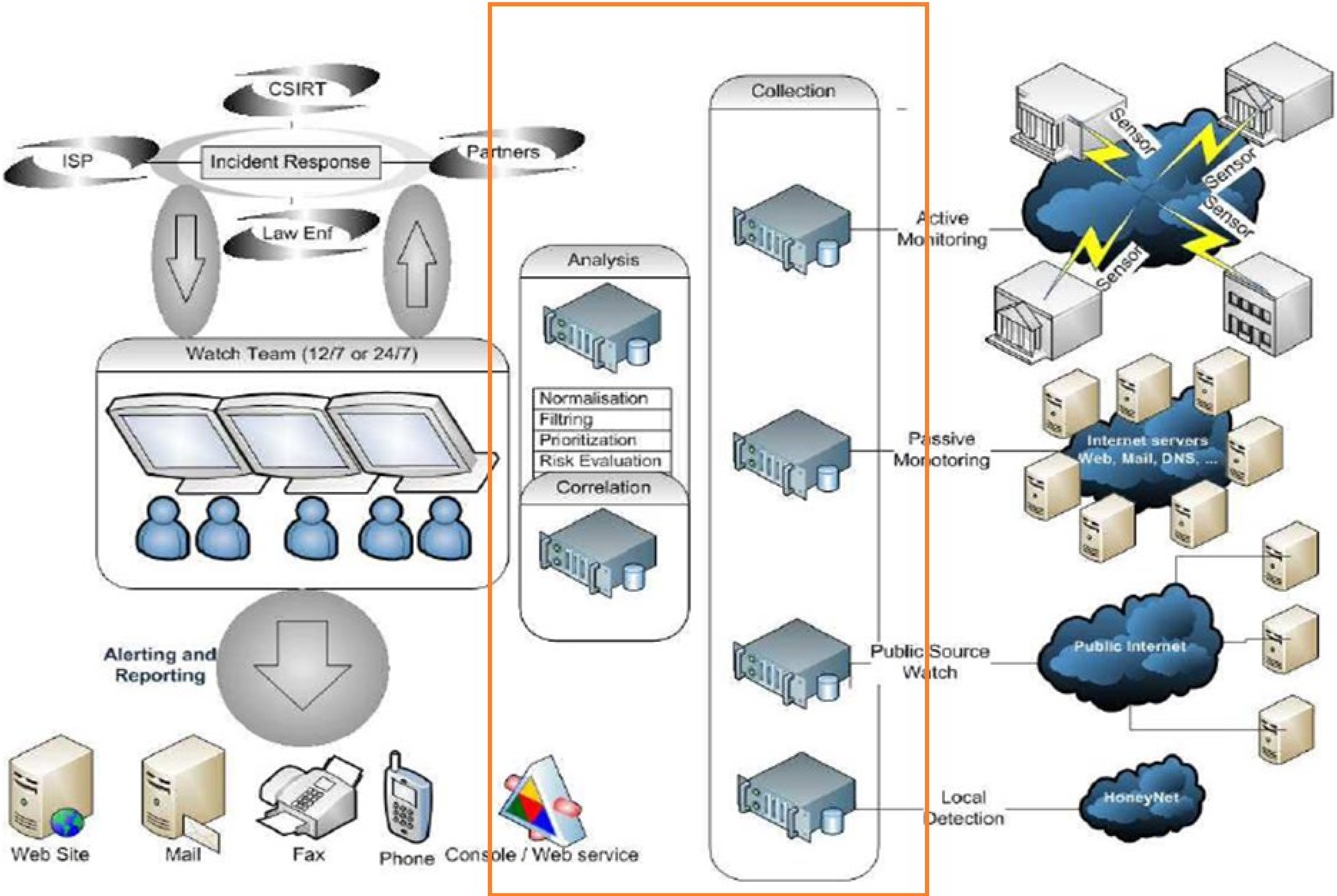
HoneyNet Platforms



T-POT : Honeypot platform

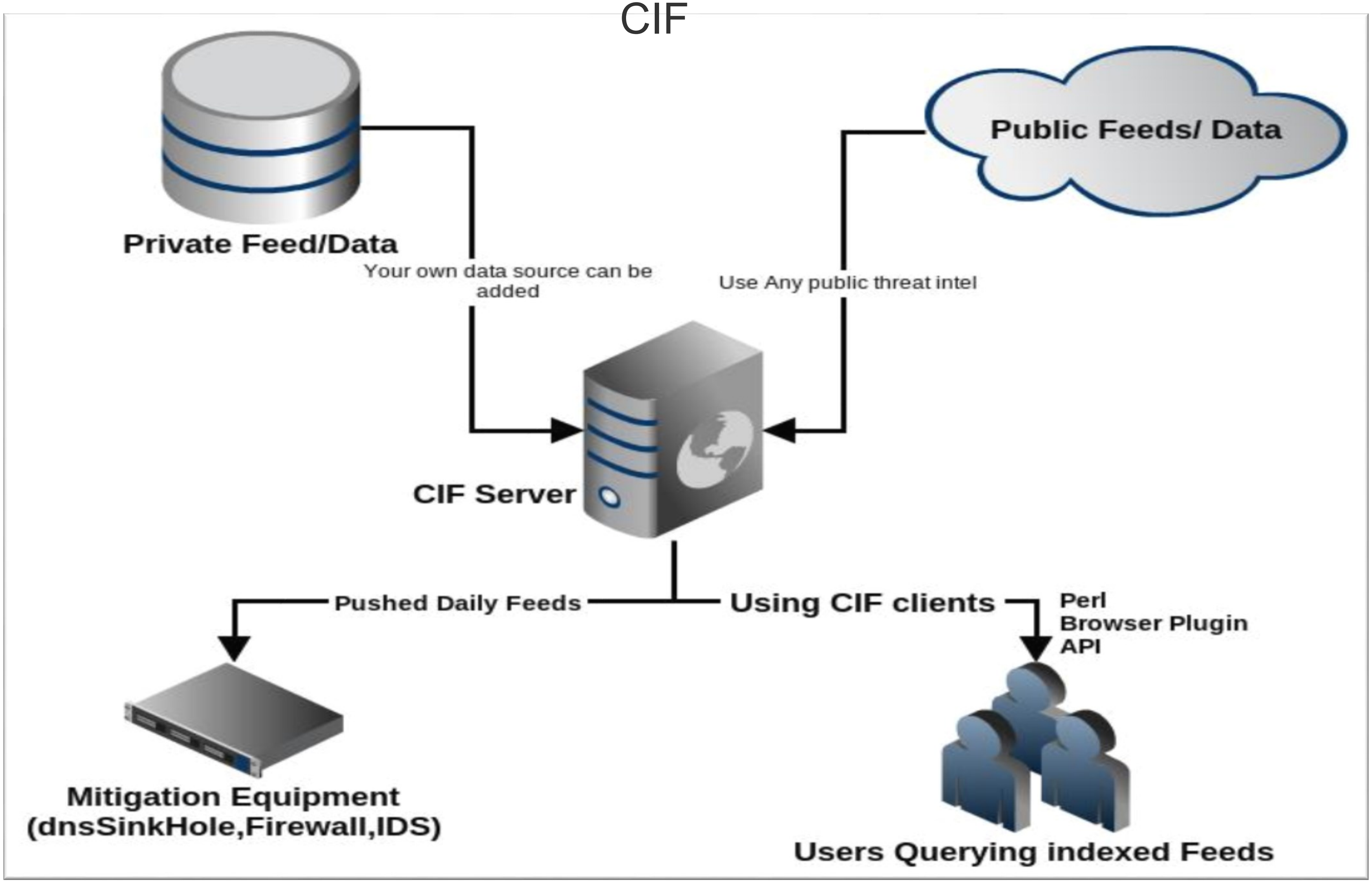
http://dtag-dev-sec.github.io/

Incident Response Center



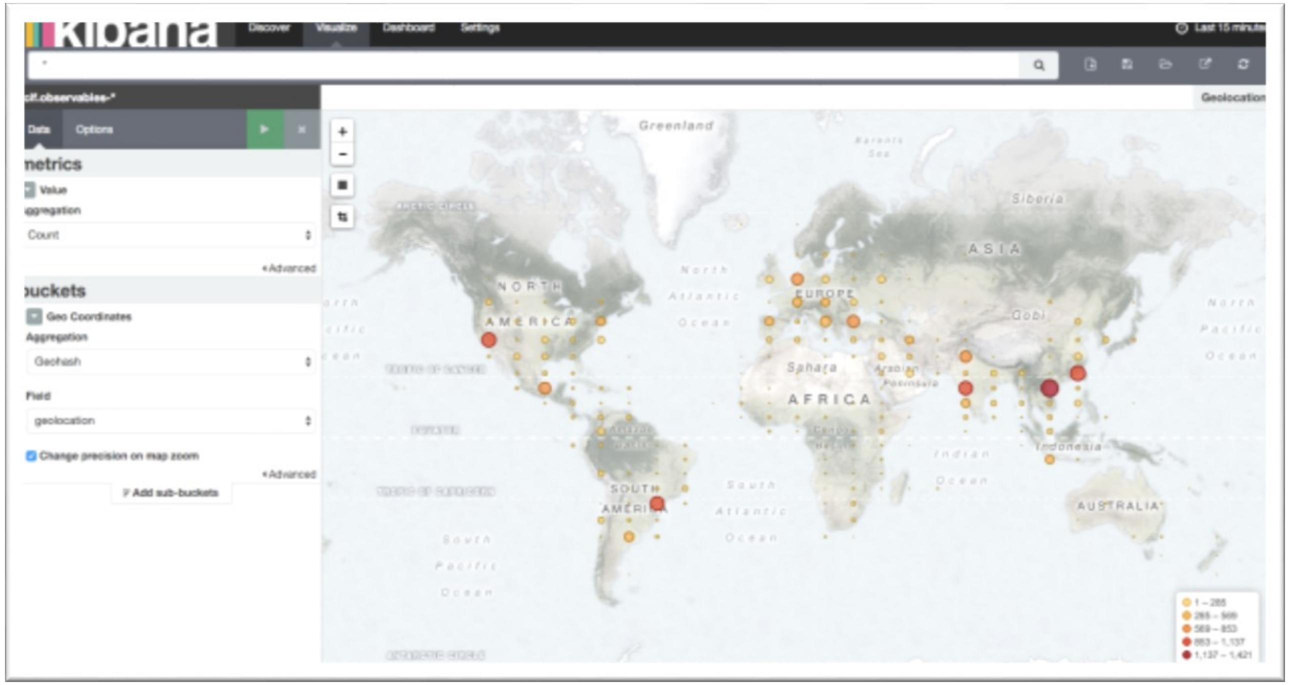
Collective Intelligence Framework CIF

csirtgadgets.org/



Private Feed/Data
Your own data source can be added
Public Feeds/ Data
Use Any public threat intel
CIF Server
Pushed Daily Feeds
Using CIF clients
Perl
Browser Plugin
API
Mitigation Equipment (dnsSinkHole,Firewall,IDS)
Users Querying indexed Feeds

Collective Intelligence Framework
CIF



cif.observables-*

metrics

Value

Aggregation: Count

« Advanced

buckets

Geo Coordinates

Aggregation: Geohash

Field: geolocation

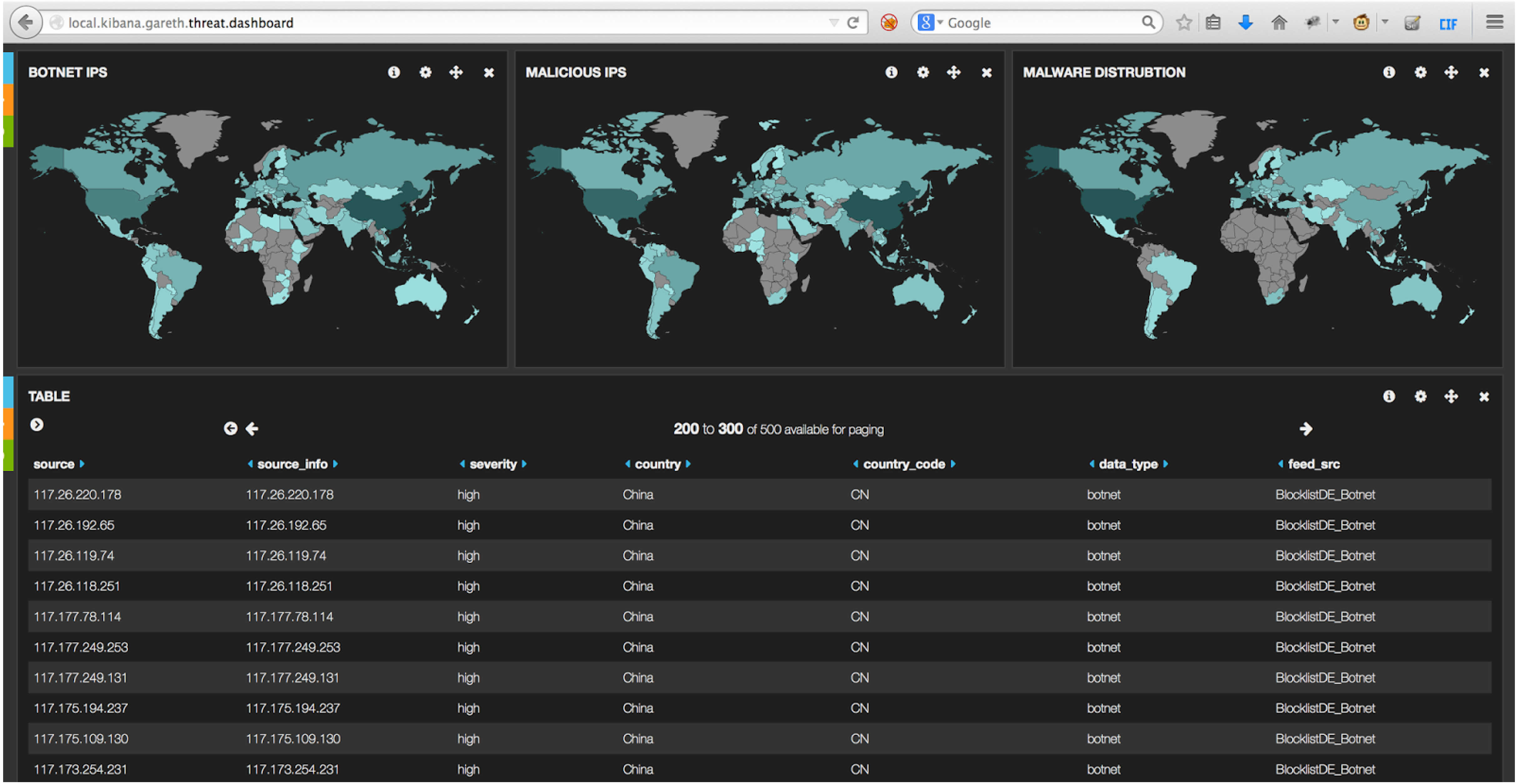
☑ Change precision on map zoom

« Advanced

Add sub-buckets

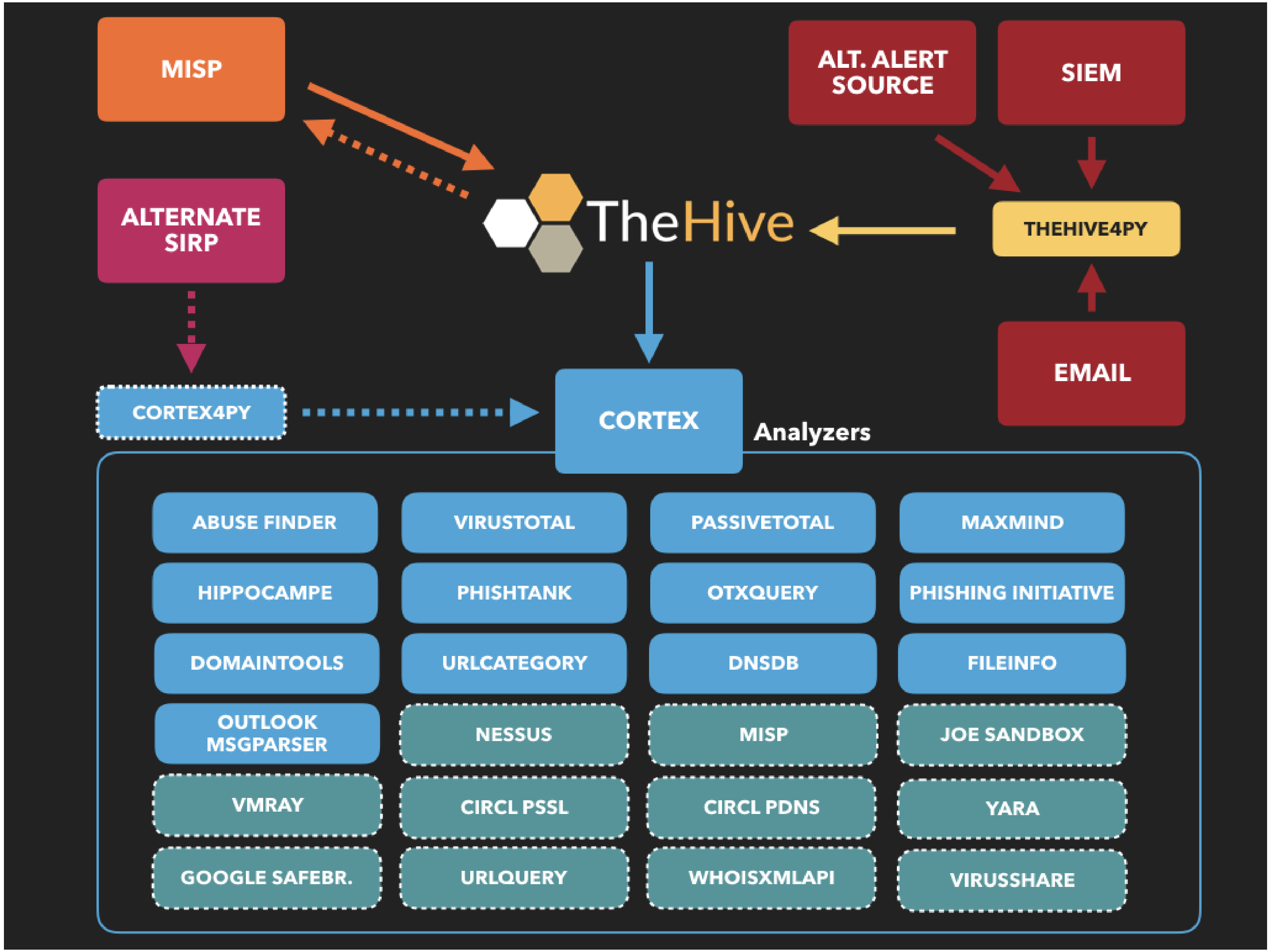
Collective Intelligence Framework

CIF



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
117.173.254.231	117.173.254.231	high	China	CN	botnet	BlocklistDE_Botnet


MISP
ALT. ALERT SOURCE
SIEM
ALTERNATE SIRP
TheHive
THEHIVE4PY
EMAIL
CORTEX4PY
CORTEX
Analyzers
ABUSE FINDER
VIRUSTOTAL
PASSIVETOTAL
MAXMIND
HIPPOCAMPE
PHISHTANK
OTXQUERY
PHISHING INITIATIVE
DOMAINTOOLS
URLCATEGORY
DNSDB
FILEINFO
OUTLOOK MSGPARSER
NESSUS
MISP
JOE SANDBOX
VMRAY
CIRCL PSSL
CIRCL PDNS
YARA
GOOGLE SAFEBR.
URLQUERY
WHOISXMLAPI
VIRUSSHARE

TheHive

Digital Forensic Tools

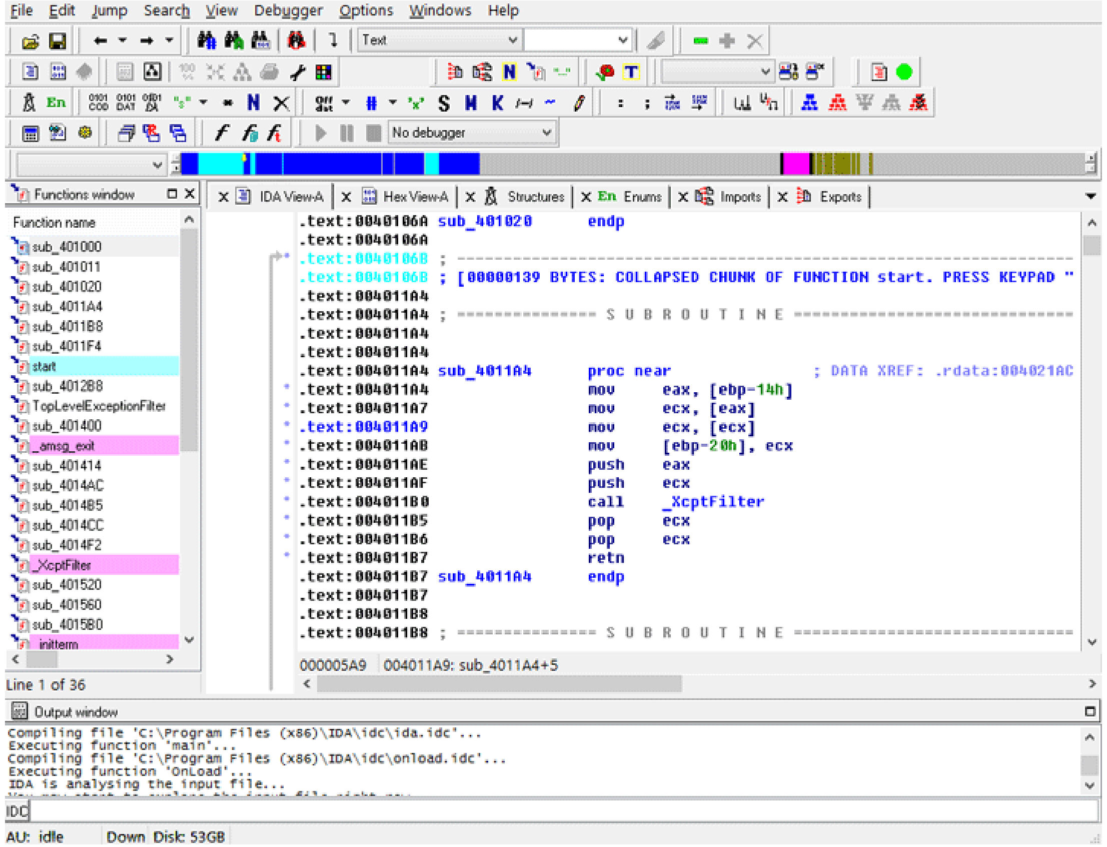
Digital Forensic Tools

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

MALWARE AND MEMORY FORENSICS

Digital Forensic Tools

The Interactive Disassembler (IDA)



```
Function name
sub_401000
sub_401011
sub_401020
sub_4011A4
sub_4011B8
sub_4011F4
start
sub_4012B8
TopLevelExceptionFilter
sub_401400
_amsg_exit
sub_401414
sub_4014AC
sub_4014B5
sub_4014CC
sub_4014F2
_XcptFilter
sub_401520
sub_401560
sub_4015B0
initterm
```

Line 1 of 36

```
.text:0040106A sub_401020      endp
.text:0040106A
.text:0040106B ; ---------------------------------------------------------------------------
.text:0040106B ; [00000139 BYTES: COLLAPSED CHUNK OF FUNCTION start. PRESS KEYPAD "
.text:004011A4
.text:004011A4 ; =============== S U B R O U T I N E ===============================
.text:004011A4
.text:004011A4
.text:004011A4 sub_4011A4      proc near               ; DATA XREF: .rdata:004021AC
.text:004011A4                 mov     eax, [ebp-14h]
.text:004011A7                 mov     ecx, [eax]
.text:004011A9                 mov     ecx, [ecx]
.text:004011AB                 mov     [ebp-20h], ecx
.text:004011AE                 push    eax
.text:004011AF                 push    ecx
.text:004011B0                 call    _XcptFilter
.text:004011B5                 pop     ecx
.text:004011B6                 pop     ecx
.text:004011B7                 retn
.text:004011B7 sub_4011A4      endp
.text:004011B7
.text:004011B8
.text:004011B8 ; =============== S U B R O U T I N E ===============================
```

000005A9 004011A9: sub_4011A4+5

```
Compiling file 'C:\Program Files (x86)\IDA\idc\ida.idc'...
Executing function 'main'...
Compiling file 'C:\Program Files (x86)\IDA\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
```

AU: idle Down Disk: 53GB

https://www.hex-rays.com

Digital Forensic Tools

Cuckoo Sandbox is a malware analysis system.

https://**cuckoosandbox**.org/

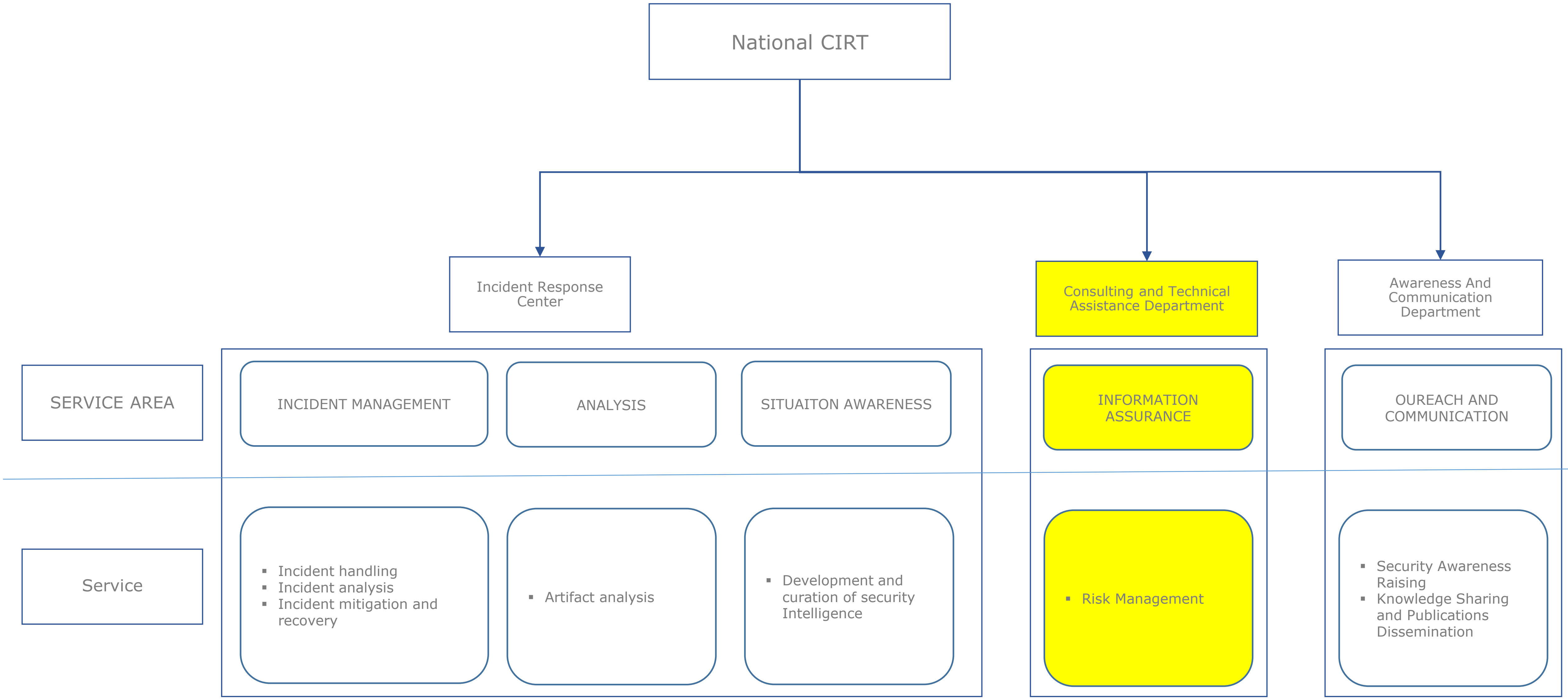
VirusTotal is a free service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

https://www.**virustotal**.com/

Malwr : Automated Malware Analysis Sandboxes and Services

https://**malwr**.com/

The Basic Services Offered by a National CIRT



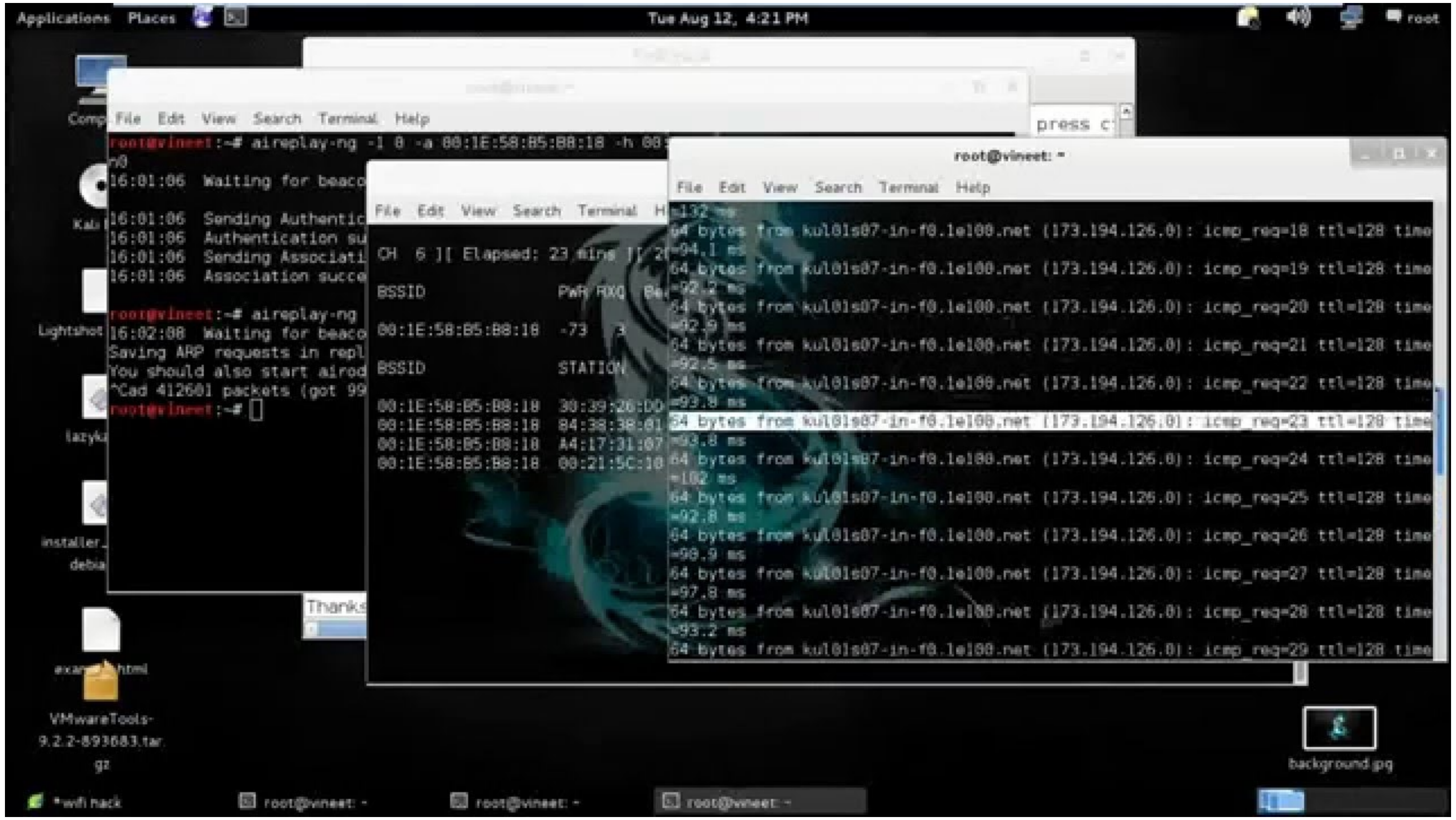
National CIRT

- Incident Response Center
- Consulting and Technical Assistance Department
- Awareness And Communication Department

	Incident Response Center			Consulting and Technical Assistance Department	Awareness And Communication Department
SERVICE AREA	INCIDENT MANAGEMENT	ANALYSIS	SITUAITON AWARENESS	INFORMATION ASSURANCE	OUREACH AND COMMUNICATION
Service	▪ Incident handling ▪ Incident analysis ▪ Incident mitigation and recovery	▪ Artifact analysis	▪ Development and curation of security Intelligence	▪ Risk Management	▪ Security Awareness Raising ▪ Knowledge Sharing and Publications Dissemination

Example of Security Assessment tools

Security Assessment tools



```
root@vineet:~# aireplay-ng -1 0 -a 00:1E:58:B5:B8:18 -h 00:
n0
16:01:06  Waiting for beaco

16:01:06  Sending Authentic
16:01:06  Authentication su
16:01:06  Sending Associati
16:01:06  Association succe

root@vineet:~# aireplay-ng
16:02:08  Waiting for beaco
Saving ARP requests in repl
You should also start airod
^Cad 412601 packets (got 99
root@vineet:~# 
```

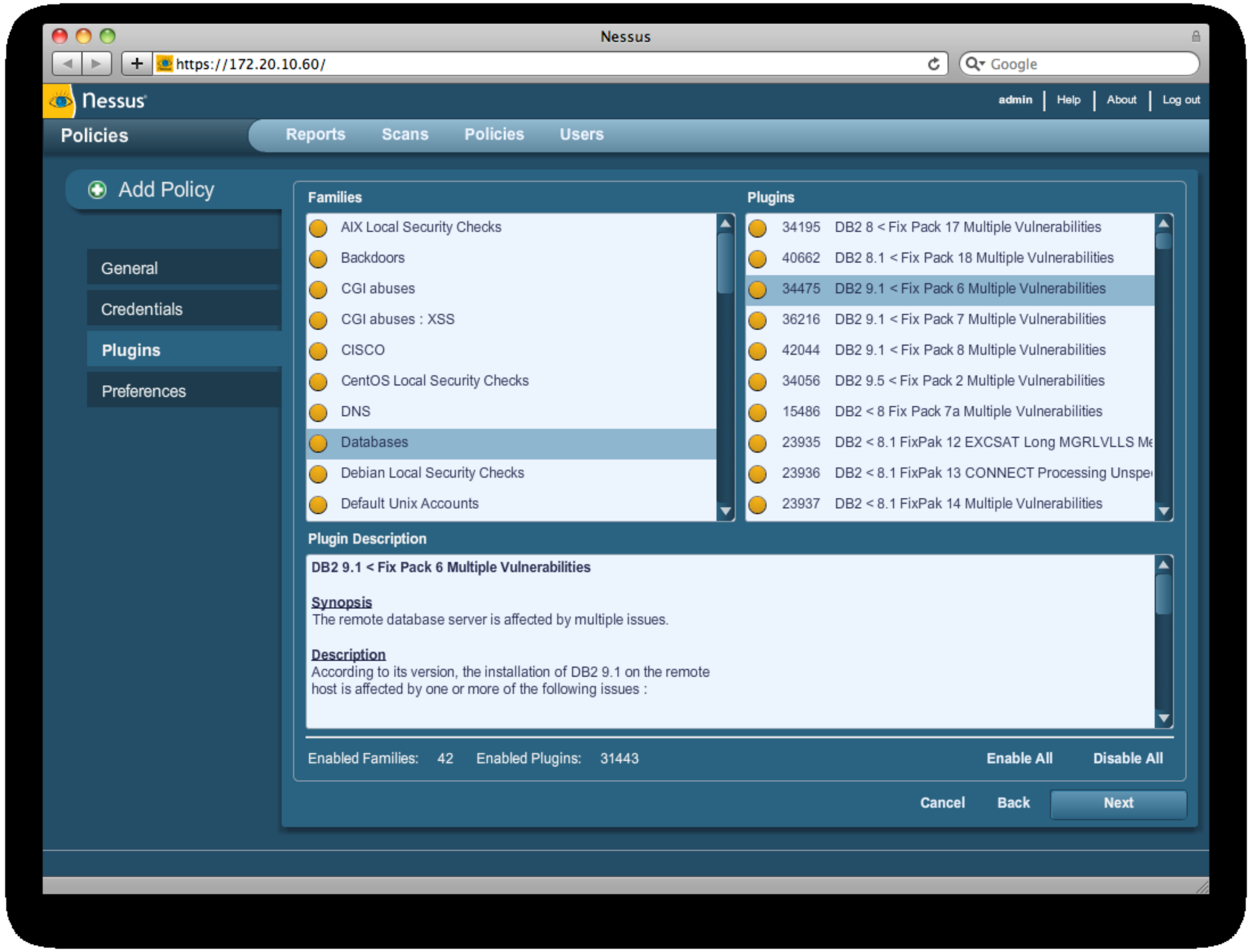
```
CH  6 ][ Elapsed: 23 mins ][ 2

BSSID              PWR RXQ  Be

00:1E:58:B5:B8:18  -73    3

BSSID              STATION

00:1E:58:B5:B8:18  30:39:26:DD
00:1E:58:B5:B8:18  84:38:38:01
00:1E:58:B5:B8:18  A4:17:31:07
00:1E:58:B5:B8:18  00:21:5C:10
```

root@vineet: ~

```
=132 ms
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
=93.8 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
=90.9 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
```

www.kali.org

Security Assessment tools



Nessus

https://172.20.10.60/

Families

- AIX Local Security Checks
- Backdoors
- CGI abuses
- CGI abuses : XSS
- CISCO
- CentOS Local Security Checks
- DNS
- Databases
- Debian Local Security Checks
- Default Unix Accounts

Plugins

34195	DB2 8 < Fix Pack 17 Multiple Vulnerabilities
40662	DB2 8.1 < Fix Pack 18 Multiple Vulnerabilities
34475	DB2 9.1 < Fix Pack 6 Multiple Vulnerabilities
36216	DB2 9.1 < Fix Pack 7 Multiple Vulnerabilities
42044	DB2 9.1 < Fix Pack 8 Multiple Vulnerabilities
34056	DB2 9.5 < Fix Pack 2 Multiple Vulnerabilities
15486	DB2 < 8 Fix Pack 7a Multiple Vulnerabilities
23935	DB2 < 8.1 FixPak 12 EXCSAT Long MGRLVLLS Me
23936	DB2 < 8.1 FixPak 13 CONNECT Processing Unspe
23937	DB2 < 8.1 FixPak 14 Multiple Vulnerabilities

Plugin Description

DB2 9.1 < Fix Pack 6 Multiple Vulnerabilities

Synopsis
The remote database server is affected by multiple issues.

Description
According to its version, the installation of DB2 9.1 on the remote host is affected by one or more of the following issues :

Enabled Families: 42 Enabled Plugins: 31443

https://www.tenable.com/

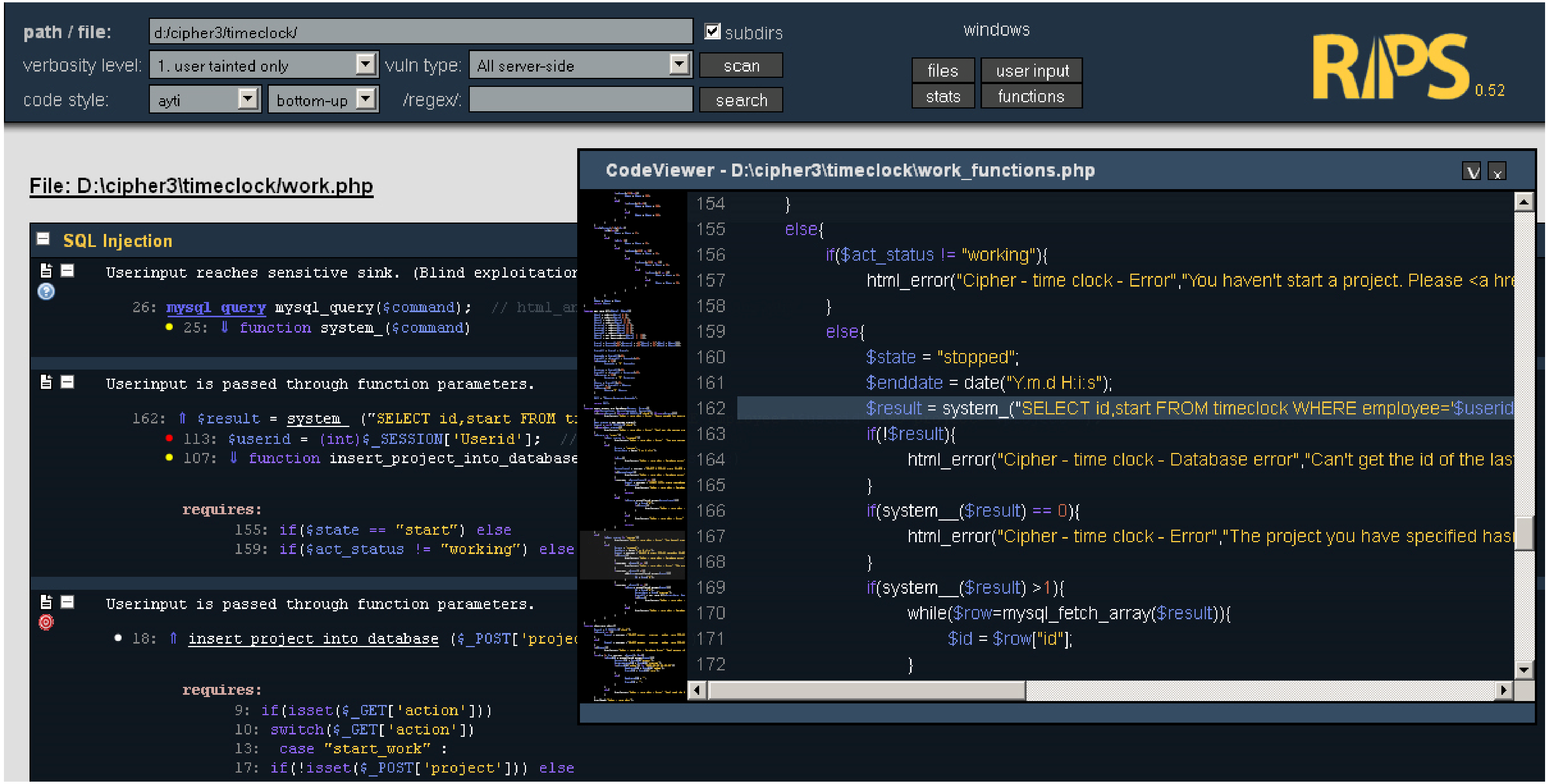
Nessus® vulnerability scanner

zmap

VEGA BETA RELEASE

OPEN SOURCE WEB APPLICATION VULNERABILITY SCANNER, PROXY AND PLATFORM

static code analysis



path / file: d:/cipher3/timeclock/ ☑ subdirs
verbosity level: 1. user tainted only vuln type: All server-side
code style: ayti bottom-up /regex/:

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

SQL Injection

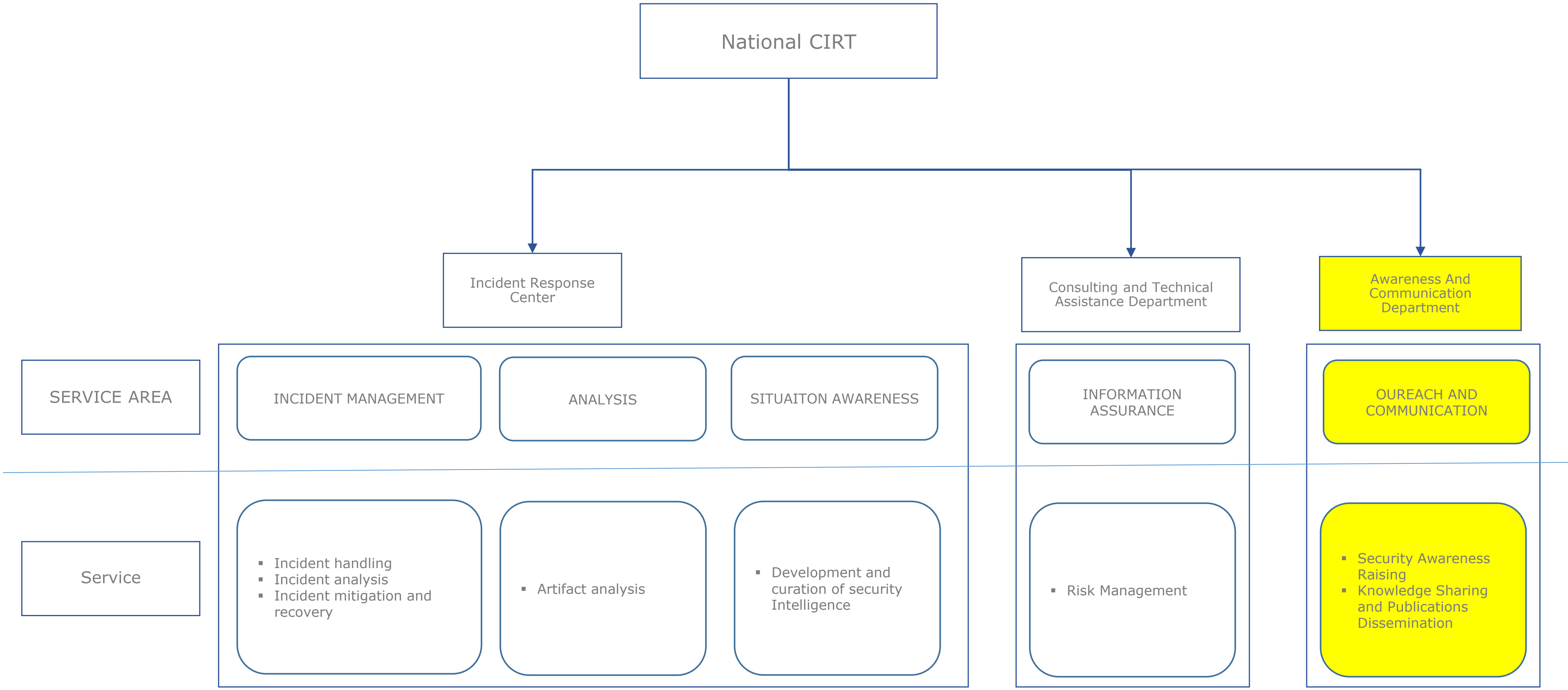
```
Userinput reaches sensitive sink. (Blind exploitatior

    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 hre
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(!$result){
164                     html_error("Cipher - time clock - Database error","Can't get the id of the las
165                 }
166                 if(system__($result) == 0){
167                     html_error("Cipher - time clock - Error","The project you have specified has
168                 }
169                 if(system__($result) >1){
170                     while($row=mysql_fetch_array($result)){
171                         $id = $row["id"];
172                     }
```

rips-scanner.sourceforge.net/

The Basic Services Offered by a National CIRT



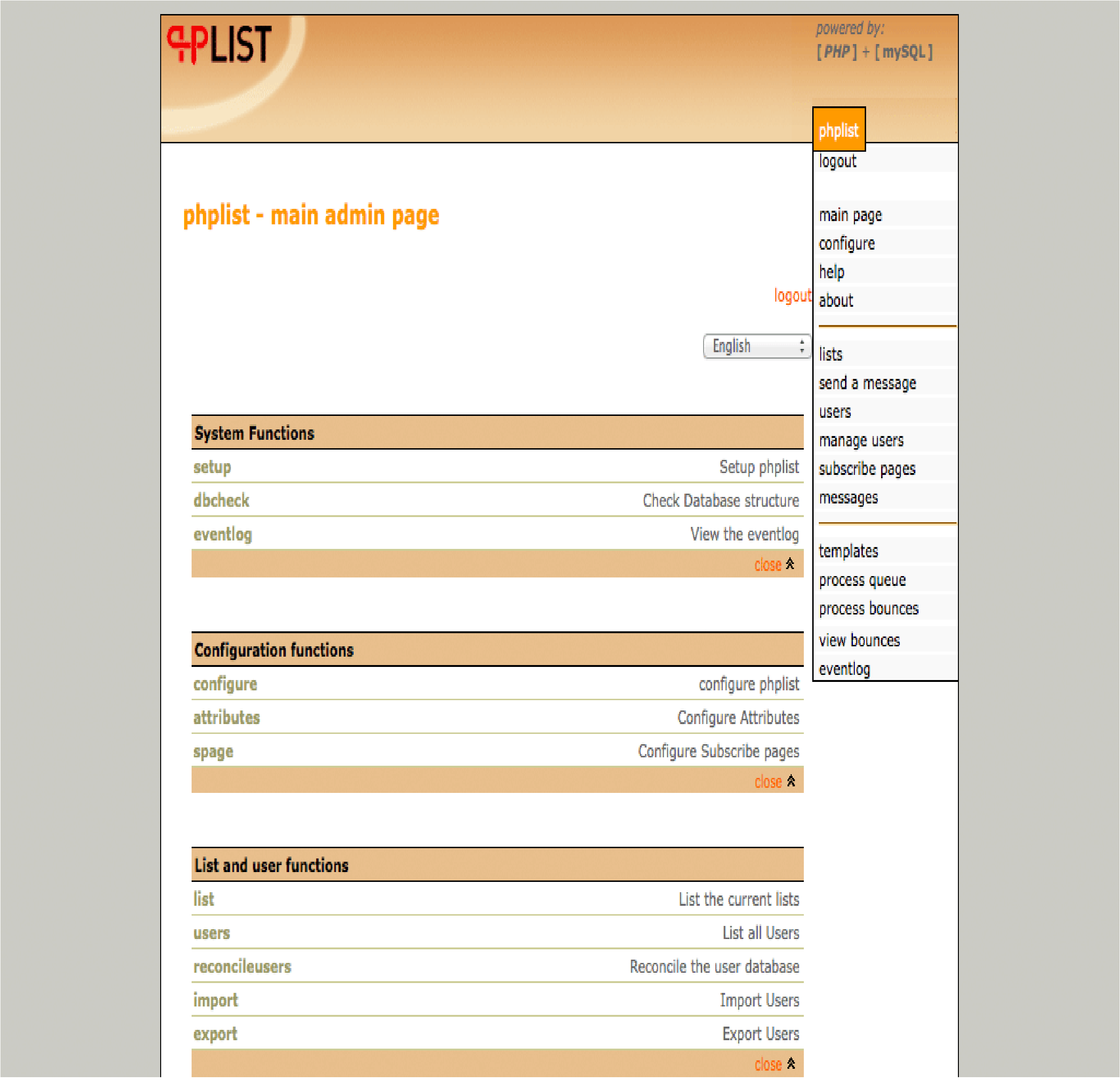
National CIRT

	Incident Response Center			Consulting and Technical Assistance Department	Awareness And Communication Department
SERVICE AREA	INCIDENT MANAGEMENT	ANALYSIS	SITUAITON AWARENESS	INFORMATION ASSURANCE	OUREACH AND COMMUNICATION
Service	▪ Incident handling ▪ Incident analysis ▪ Incident mitigation and recovery	▪ Artifact analysis	▪ Development and curation of security Intelligence	▪ Risk Management	▪ Security Awareness Raising ▪ Knowledge Sharing and Publications Dissemination

Example of Alerts, Warnings and Announcements Tools

Alerts, Warnings and Announcements Tools

phpList



phplist - main admin page

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

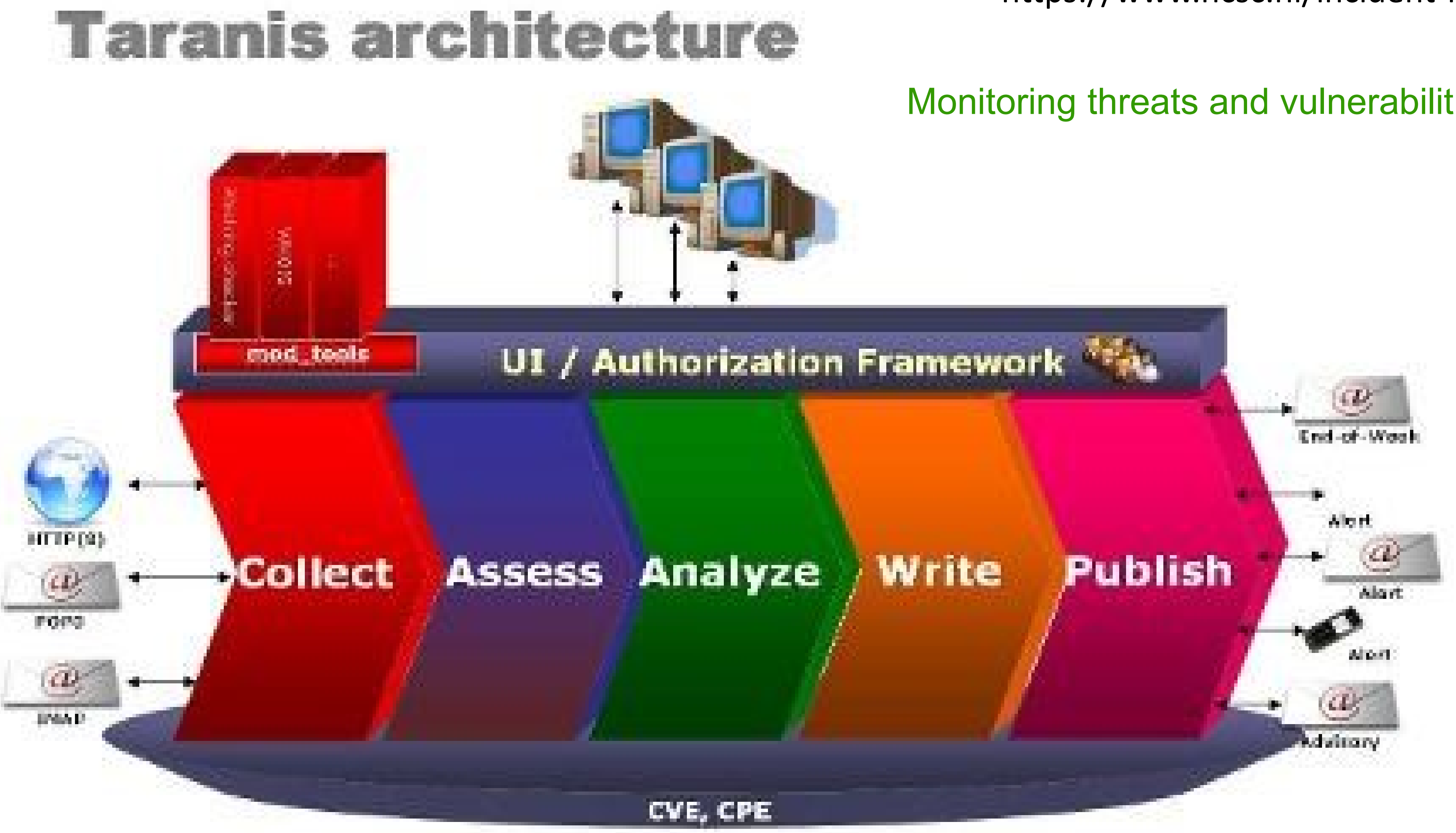
list	List the current lists
users	List all Users
reconcileusers	Reconcile the user database
import	Import Users
export	Export Users
	close

https://www.**phplist**.com/

Alerts, Warnings and Announcements Tools

https://www.ncsc.nl/incident-response/taranis.html

Monitoring threats and vulnerabilities


Taranis architecture
mod_tools
UI / Authorization Framework
HTTP(S)
POP3
IMAP
Collect
Assess
Analyze
Write
Publish
End-of-Week
Alert
Alert
Alert
Advisory
CVE, CPE