

ITUEvents
ITU 2021 Global
CyberDrill

**Threat Monitoring and Incident
Response for CNI using open
source tools**

**07 October 2021
14:00-16:00 CEST**

**#Cybersecurity
#CyberDrill**



Agenda

Contents:

Introduction to CIRT – Threat Intelligence



CIRT Network Architecture



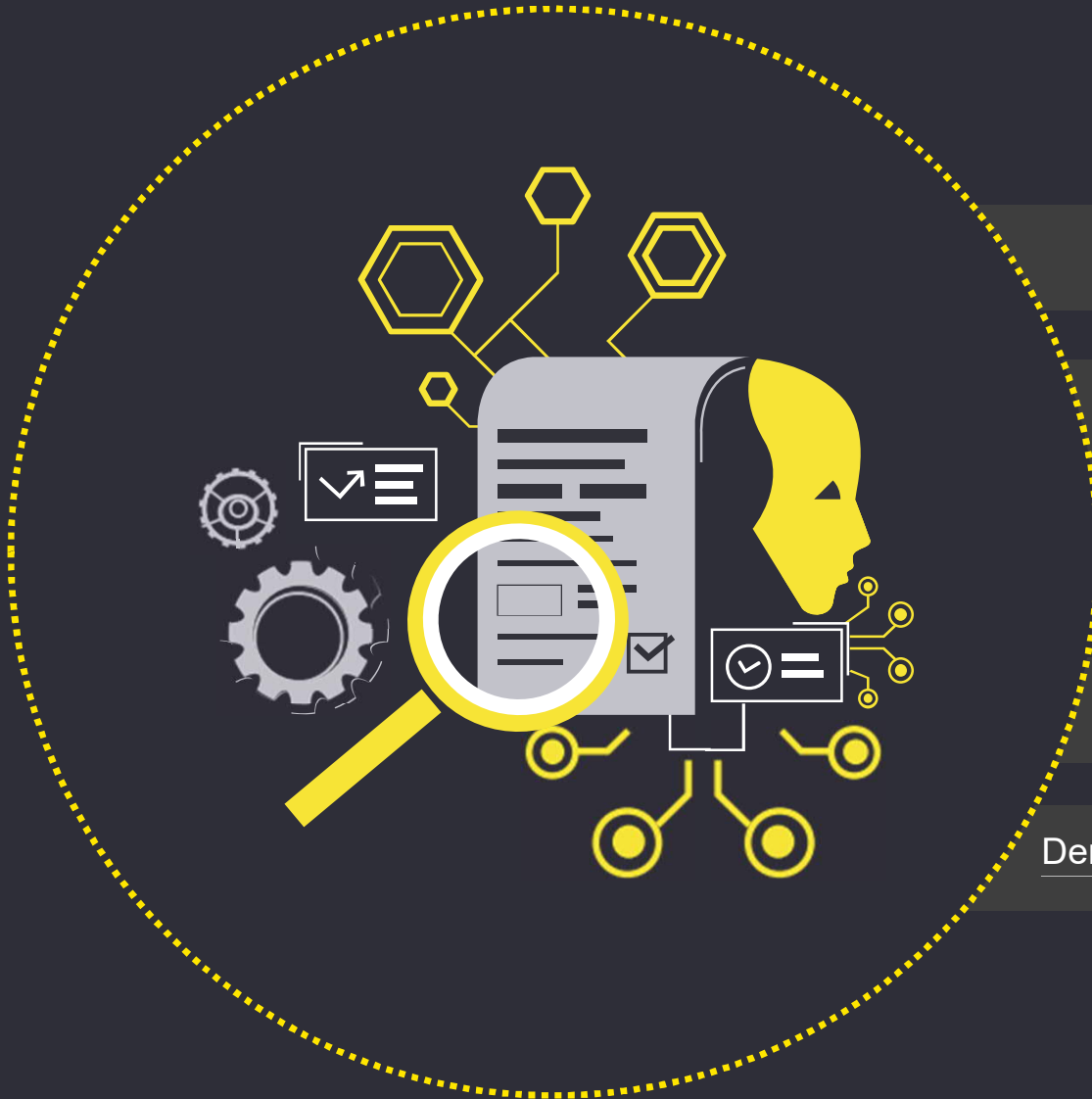
How to build CIRT using Open source tools



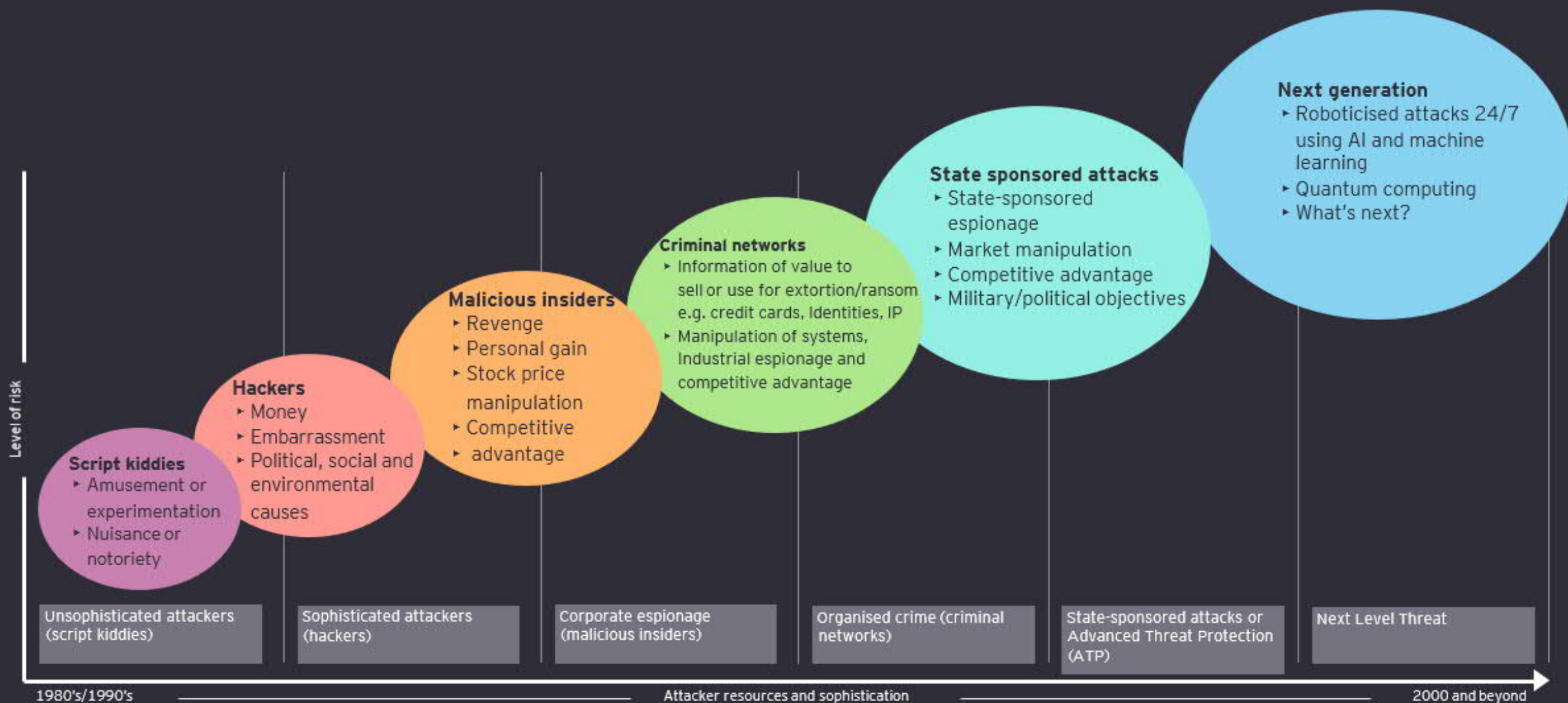
Overview of TheHive and MISP



Demonstration and Q&A



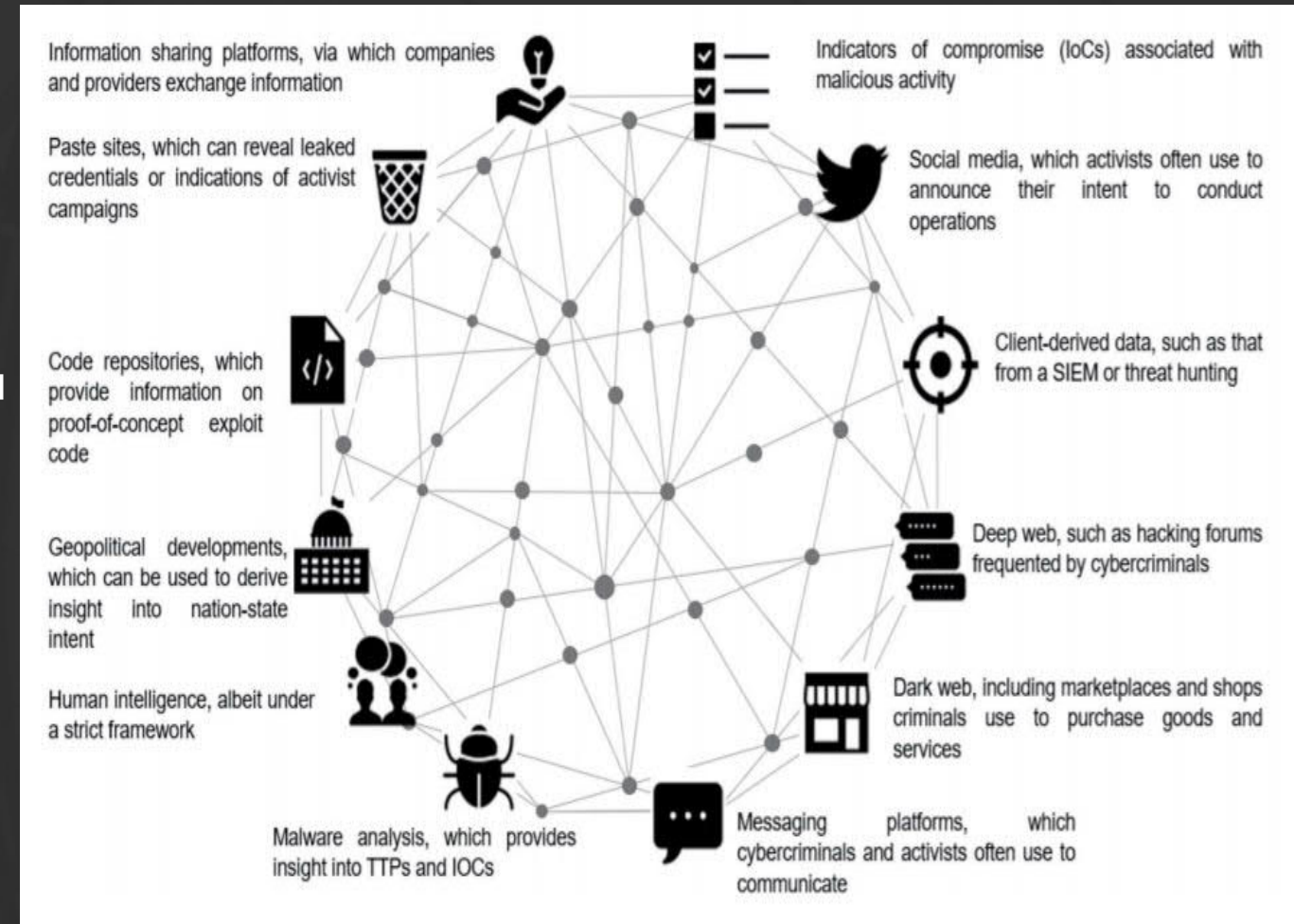
Cyber Attacks are Increasing in sophistication



Computer Incident Response Team (CIRT) - Services Overview



A modern approach to collect cyber threat intelligence involves inter-linking inferences from numerous data sources to provide actionable insights against a specific attacker or an emerging threat



Courtesy: CREST

Threat Intelligence - Our Key Defense Against Cyber Threats

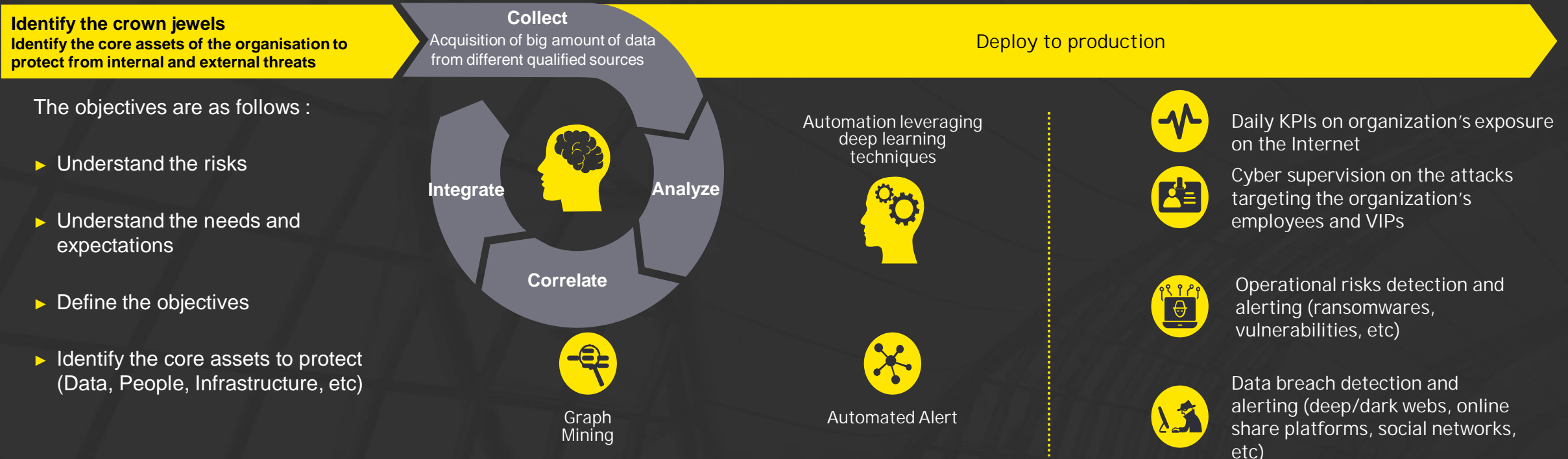
What is Threat Intelligence (CTI)?

Cyber threat intelligence refers to the collection and analysis of data which can be used by security teams to determine what actions are necessary to help prevent, detect and respond to cyber threats

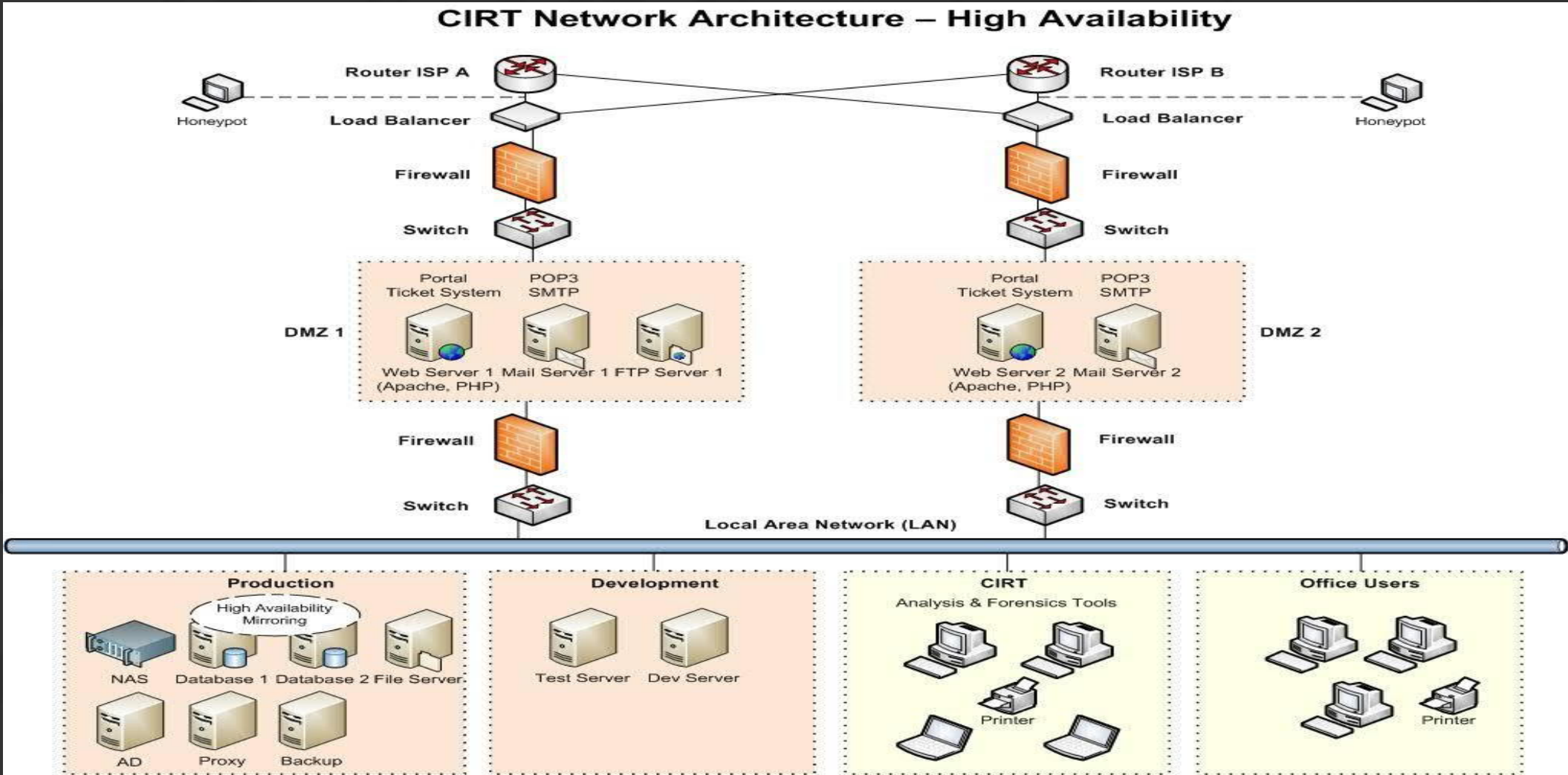
Types of Threat Intelligence

Traditionally, CTI involved collection of simply Technical data like IOCs, CVEs and Incident Analysis Reports. However, a complete approach involves inclusion of Tactical, Operational as well as Strategic intelligence for protecting against threats.

Methodology



CIRT Network Architecture - High Availability Architecture





Building CIRT using Open Source Tools

Building CIRT- Open Source Tools

Active Monitoring

- ▶ SNORT
- ▶ SNORBY



Snorby

Passive Monitoring

- ▶ Nagios
- ▶ Icinga
- ▶ Zabbix

Nagios®

ZABBIX

icinga

Public Source Watch

- ▶ PhishTank
- ▶ ZoneH
- ▶ Malware Domain List

PhishTank®



Local Detection

- ▶ TPOT
- ▶ Honeynet Project



Alerting and Monitoring

- ▶ RTIR
- ▶ OTRS
- ▶ TheHIVE



OTRS

TheHive

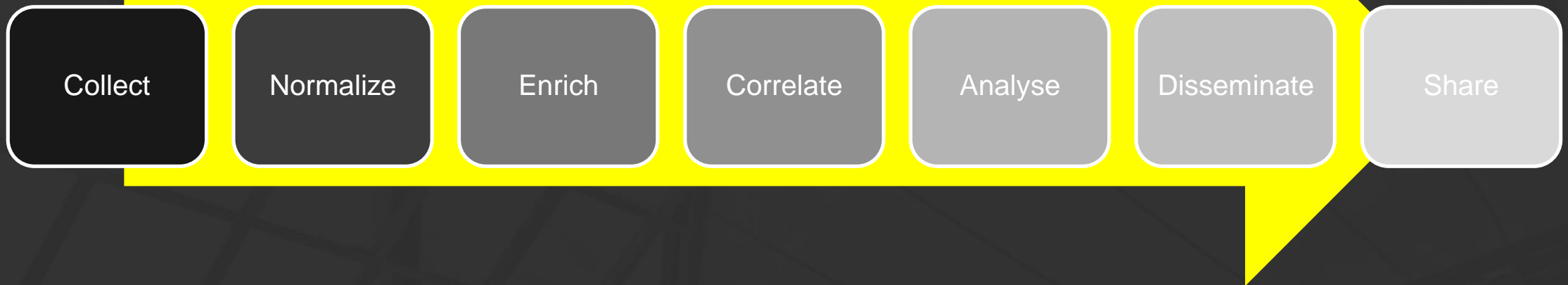
Threat Intel

- ▶ MISP



What is MISP?

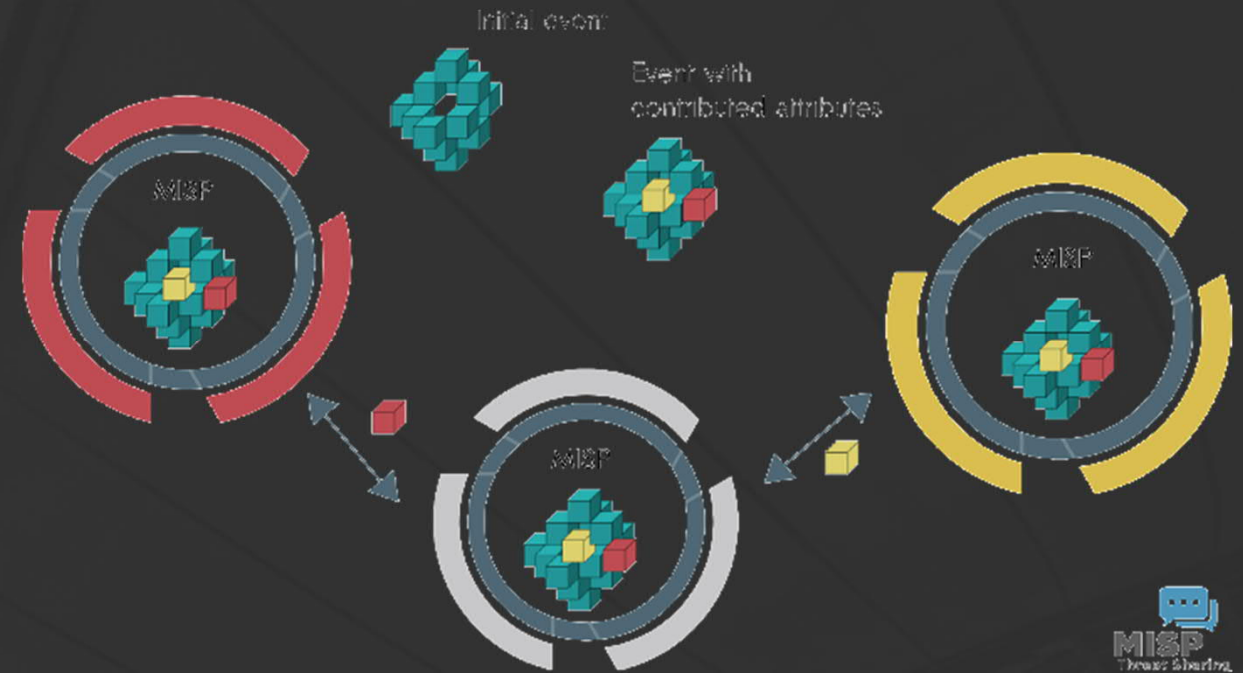
- ▶ MISP stands for Malware Information Sharing Platform. It is a Threat sharing platform



- ▶ Free and Open Source and exists >10 years
- ▶ CIRCL leads development
- ▶ Used by >6000 organisations worldwide
- ▶ Security teams, national and government CSIRTs, commercial providers

Functions of MISP

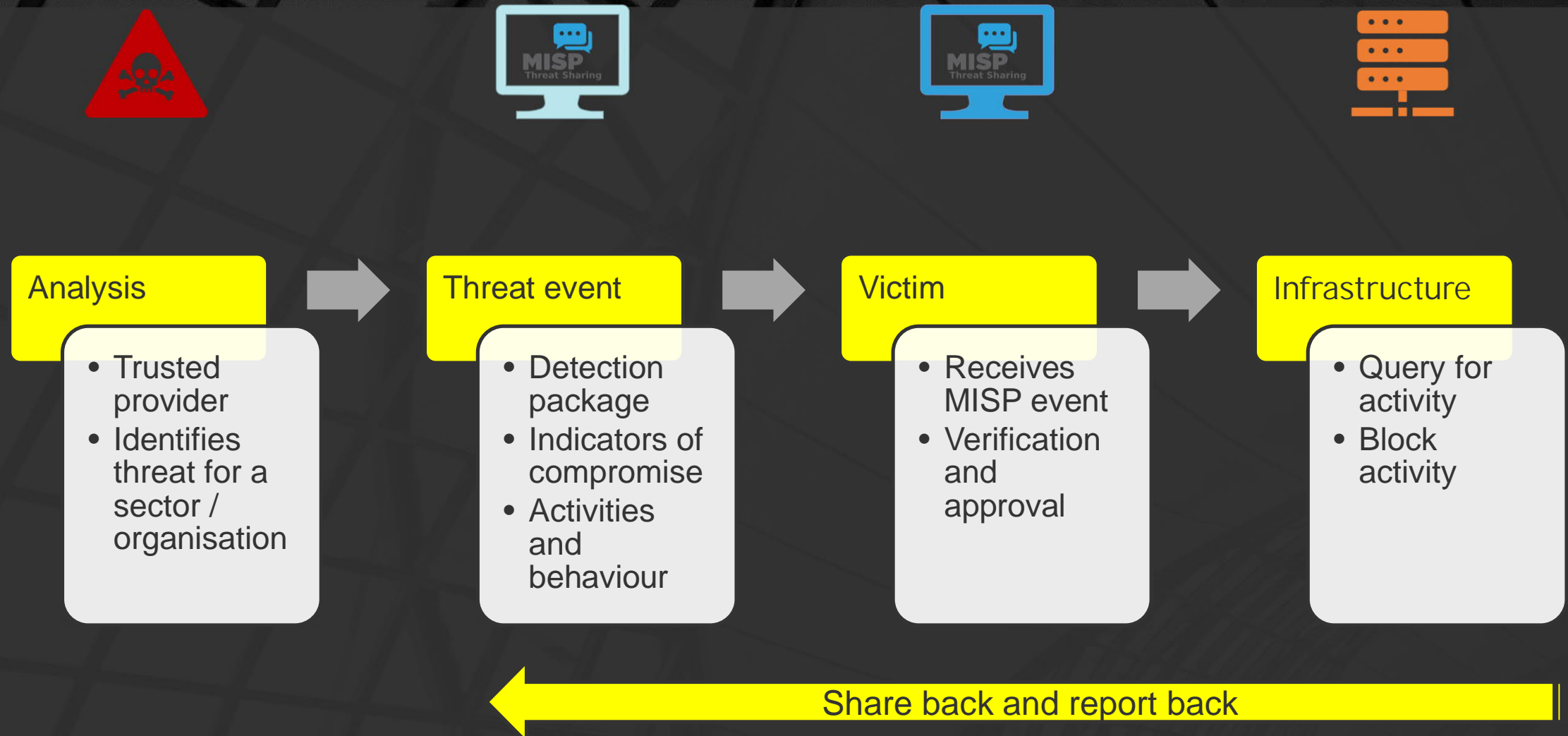
- ▶ Core functionality is sharing
- ▶ Everyone can be a consumer and/ or a contributor/producer
- ▶ Quick benefit without the obligation to contribute
- ▶ Low barrier to get acquainted to the system



How does MISP work?

- ▶ The MISP structure consists of events, feeds, communities, and subscribers
- ▶ Normally an event is a threat entry containing information related to the threat and the associated IOCs.
- ▶ Once an event has been created, a user assigns it to a specific feed that acts as a centralized list of events belonging to a specific organization and containing certain events or grouping specifications.

MISP Process



Sample Use cases

Block IP
address on
firewall

Block
malicious URL
on proxy

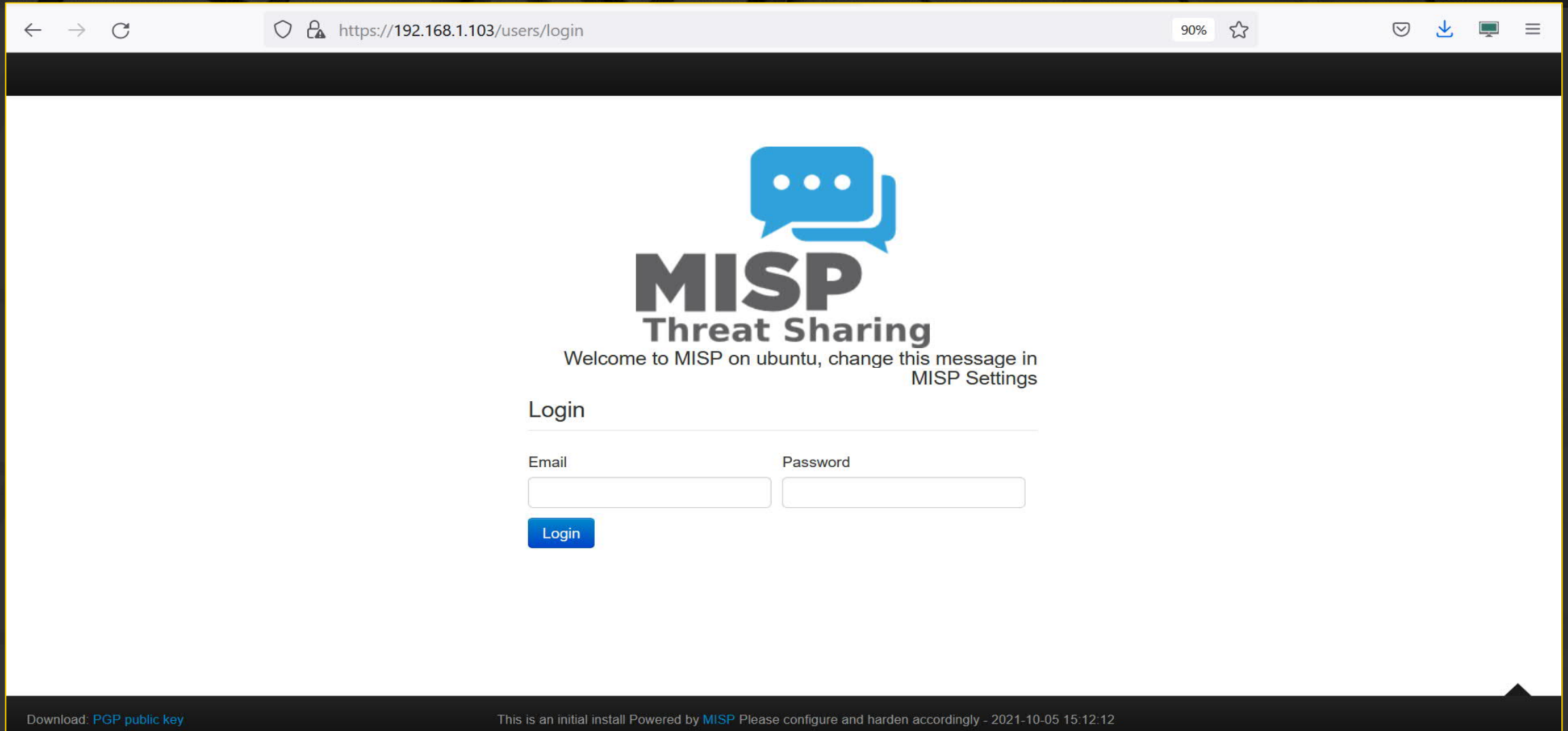
Query logs for
activity

Scan
endpoints with
custom rules







IDS signatures


SIEM alerts

Glimpse of MISP



The screenshot shows a web browser window with the address bar displaying `https://192.168.1.103/users/login`. The page features the MISP logo, which consists of two blue speech bubbles above the text "MISP Threat Sharing". Below the logo, a welcome message reads: "Welcome to MISP on ubuntu, change this message in MISP Settings". A "Login" section follows, containing two input fields labeled "Email" and "Password", and a blue "Login" button. At the bottom of the page, there is a footer with a link to "Download: PGP public key" and a status message: "This is an initial install Powered by MISP Please configure and harden accordingly - 2021-10-05 15:12:12".

← → ↻  `https://192.168.1.103/users/login` 90%     



MISP Threat Sharing

Welcome to MISP on ubuntu, change this message in MISP Settings

Login

Email

Password

Login

Download: [PGP public key](#) This is an initial install Powered by MISP Please configure and harden accordingly - 2021-10-05 15:12:12

Glimpse of MISP

← → ↺

https://192.168.1.103/events/index/searchall:ransom

90% ☆

📧 ⬇️ 🖥️ ☰

HomeEvent ActionsDashboardGalaxiesInput FiltersGlobal ActionsSync ActionsAdministrationLogsAPI★MISPVardan Bansal✉️Log out

List EventsAdd EventImport from...REST clientList AttributesSearch AttributesView ProposalsEvents with proposalsView delegation requestsExportAutomation

Events

« previous12345next »

🔍

Filters: All: ransom ✕

My Events

Org Events

📄

ransomFilter

☐ Published

Creator org


Owner org

ID

Clusters

Tags

☐ ✓



EY LLP

🔴 1511

Malpedia 🔍
🔗 LockBit 🔍 ☰
Ransomware 🔍
🔗 LockBit 🔍 ☰

🔗 type:OSINT 🔗 osint:lifetime="perpetual" 🔗 osint:certainty="50

☐ ✓

CUDES0

EY LLP

🟢 134

Attack Pattern 🔍
🔗 Phishing - T1566 🔍 ☰
🔗 Remote Access Software - T1219 🔍 ☰

🔗 tlp:white

☐ ✓

CUDES0


EY LLP

🟢 129

Ransomware 🔍
🔗 Conti 🔍 ☰
Malware 🔍
🔗 Cobalt Strike - S0154 🔍 ☰

🔗 tlp:white

☐ ✓



EY LLP

🔴 1504

Ransomware 🔍
🔗 Sodinokibi 🔍 ☰
Attack Pattern 🔍
🔗 Data Encrypted for Impact - T1486 🔍 ☰

🔗 type:OSINT 🔗 osint:lifetime="perpetual" 🔗 osint:certainty="50

Glimpse of MISP

← → ↻ <https://192.168.1.103/events/view/134> 90% ☆

Home Event Actions Dashboard Galaxies Input Filters Global Actions Sync Actions Administration Logs API ★ MISP Vardan Bansal Log out

+ ≡ ✕ Scope toggle Deleted Decay score SightingDB Context Related Tags Filtering tool Enter value

<input type="checkbox"/>	Date ↑	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution
<input type="checkbox"/>	2021-08-30		External analysis	link	https://www.ic3.gov/Media/News/2021/210825.pdf	🌐+ 👤+	🌐+ 👤+		✓		2	<input type="checkbox"/>	Inherit
<input type="checkbox"/>	2021-08-30		Network activity	url	https://www.sendspace.com	🌐+ 👤+	🌐+ 👤+		✓		2	<input type="checkbox"/>	Inherit
<input type="checkbox"/>	2021-08-30		Network activity	url	https://ufile.io	🌐+ 👤+	🌐+ 👤+		✓		2	<input type="checkbox"/>	Inherit
<input type="checkbox"/>	2021-08-30		Network activity	url	https://send.exploit.in	🌐+ 👤+	🌐+ 👤+		✓		2	<input type="checkbox"/>	Inherit
<input type="checkbox"/>	2021-08-30		Network activity	url	https://mega.nz	🌐+ 👤+	🌐+ 👤+		✓		2	<input type="checkbox"/>	Inherit
<input type="checkbox"/>	2021-08-30		Network activity	url	https://anonfiles.com	🌐+ 👤+	🌐+ 👤+		✓		2	<input type="checkbox"/>	Inherit
<input type="checkbox"/>	2021-08-30		Other	other	wevtutil.exe cl application	🌐+ 👤+	🌐+ 👤+	Other commands / IOCs	✓		2	<input type="checkbox"/>	Inherit
<input type="checkbox"/>	2021-08-30		Other	other	bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures	🌐+ 👤+	🌐+ 👤+	Other commands / IOCs	✓		2	<input type="checkbox"/>	Inherit
<input type="checkbox"/>	2021-08-30		Other	other	bcdedit.exe /set {default} recoveryenabled no	🌐+ 👤+	🌐+ 👤+	Other commands	✓		2	<input type="checkbox"/>	Inherit

Attack Pattern - Phishing

Download: [PGP public key](#) This is an initial install Powered by MISP 2.4.148 Please configure and harden accordingly - 2021-10-05 15:14:41

Glimpse of MISP - Ransomware

← → ↺

https://192.168.1.103/events/view/186

90% ☆

🔒 ⬇️ 🖨️ ☰

Home Event Actions Dashboard Galaxies Input Filters Global Actions Sync Actions Administration Logs API

★ MISP Vardan Bansal 📧 Log out

+

☰

☒

Scope toggle ▾ Deleted 📉 Decay score 🏠 SightingDB ⓘ Context 🏷️ Related Tags 🔍 Filtering tool

Enter value

<input type="checkbox"/>	Date ↕	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution
<input type="checkbox"/>	2021-06-03		Payload delivery	md5	a3d964aaf642d626474f02ba3ae4f49b	<div><div>🔍 PAP:WHITE x</div><div>🔍 course-of-action:passive="detect" x</div><div>🔍 course-of-action:active="deny" x</div><div>🔍 + 👤 +</div></div>	<div>🌐 + 👤 +</div>		<input checked="" type="checkbox"/>	237	2	<input checked="" type="checkbox"/>	Inherit
<input type="checkbox"/>	2021-06-03		Payload delivery	md5	ec0e75c477fc54c92c47788bb9ccc034	<div><div>🔍 PAP:WHITE x</div><div>🔍 course-of-action:passive="detect" x</div><div>🔍 course-of-action:active="deny" x</div><div>🔍 + 👤 +</div></div>	<div>🌐 + 👤 +</div>	Enigma Packed Windows Ransomware Sample	<input checked="" type="checkbox"/>		2	<input checked="" type="checkbox"/>	Inherit
<input type="checkbox"/>	2021-06-03		Payload delivery	md5	84c1567969b86089cc33dccf41562bcd	<div><div>🔍 PAP:WHITE x</div><div>🔍 course-of-action:passive="detect" x</div><div>🔍 course-of-action:active="deny" x</div><div>🔍 + 👤 +</div></div>	<div>🌐 + 👤 +</div>		<input checked="" type="checkbox"/>	237	2	<input checked="" type="checkbox"/>	Inherit
<input type="checkbox"/>	2021-06-03		Payload delivery	md5	b0fd45162c2219e14bdccab76f33946e	<div><div>🔍 PAP:WHITE x</div><div>🔍 course-of-action:passive="detect" x</div><div>🔍 course-of-action:active="deny" x</div><div>🔍 + 👤 +</div></div>	<div>🌐 + 👤 +</div>	Linux Ransomware Samples	<input checked="" type="checkbox"/>	237	2	<input checked="" type="checkbox"/>	Inherit
<input type="checkbox"/>	2021-06-03		Payload delivery	md5	85547c6e720886c33bdacae81c180c46	<div><div>🔍 PAP:WHITE x</div><div>🔍 course-of-action:passive="detect" x</div><div>🔍 course-of-action:active="deny" x</div><div>🔍 + 👤 +</div></div>	<div>🌐 + 👤 +</div>	Linux Ransomware Samples	<input checked="" type="checkbox"/>		2	<input checked="" type="checkbox"/>	Inherit

Download: [PGP public key](#)

This is an initial install Powered by [MISP 2.4.148](#) Please configure and harden accordingly - 2021-10-05 15:16:26

Glimpse of MISP - Ransomware Search in Virustotal

← → ↺

🔒

https://www.virustotal.com/gui/file/bfb31c96f9e6285f5bb60433f2e45898b8a7183a2591157dc1d766be16c29893

☆

📧

⬇

🔍

📄

🗃

💬

Sign in

🔍

bfb31c96f9e6285f5bb60433f2e45898b8a7183a2591157dc1d766be16c29893

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 11

Acronis (Static ML)	⚠ Suspicious	Ad-Aware	⚠ Trojan.GenericKD.46218430
AhnLab-V3	⚠ Ransomware/Win.DarkSide.C4401014	Alibaba	⚠ Ransom:Win32/DarkSide.d859587e
ALYac	⚠ Trojan.Ransom.DarkSide	Antiy-AVL	⚠ Trojan/Generic.ASMalwS.31FF7CE
SecureAge APEX	⚠ Malicious	Avast	⚠ Win32:DarkSide-D [Ransom]
AVG	Win32:DarkSide-D [Ransom] ⚠ Win32:DarkSide-D [Ransom]	Avira (no cloud)	⚠ TR/Crypt.XPACK.Gen
BitDefender	⚠ Trojan.GenericKD.46218430	BitDefenderTheta	⚠ AI:Packer.CFA3AD501E
Bkav Pro	⚠ W32.AIDetect.malware1	ClamAV	⚠ Win.Packed.DarkSide-9860993-0
Comodo	⚠ Malware@#3og5yey4ivj8q	CrowdStrike Falcon	⚠ Win/malicious_confidence_100% (D)
Cybereason	⚠ Malicious.af642d	Cylance	⚠ Unsafe
Cynet	⚠ Malicious (score: 100)	Cyren	⚠ W32/Trojan.GDUN-2720
DrWeb	⚠ Trojan.Encoder.33650	eGambit	⚠ Unsafe.AI_Score_56%
Elastic	⚠ Malicious (high Confidence)	Emisoft	⚠ Trojan.GenericKD.46218430 (P)

Demonstration





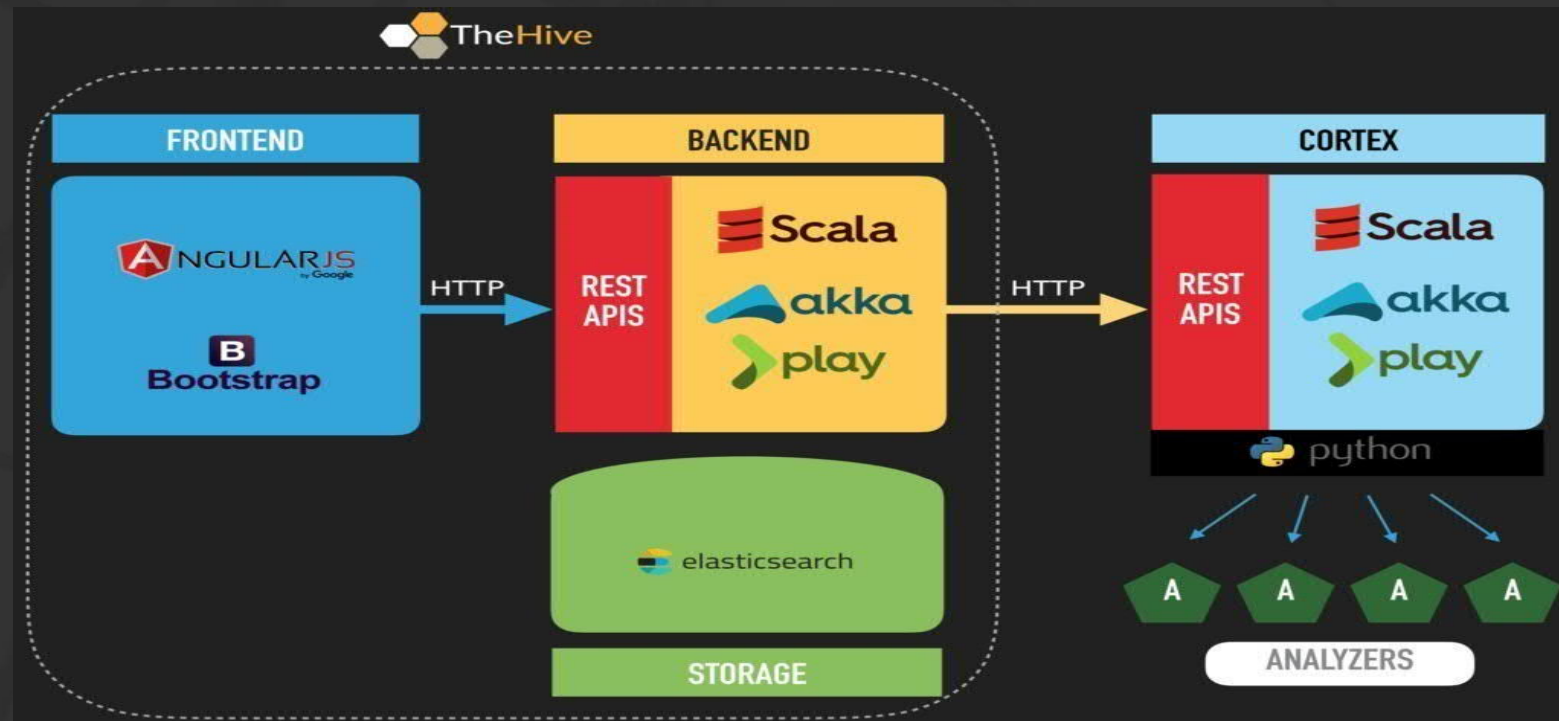
TheHive



- ▶ Collaborate in real-time
- ▶ Handle & respond to incidents
- ▶ Perform forensics analysis
- ▶ Organise, structure and archive incidents
- ▶ Correlate & merge incident
- ▶ Custom case templates: incident workflows
- ▶ Augment your processes with metrics & custom feeds
- ▶ Generate fully customisable dashboards: track activity, follow KPIs...
- ▶ Feeders: get alerts from MISP, CTI providers, SIEM, emails, ...
- ▶ Find similarities across cases & alerts
- ▶ REST API
- ▶ Webhook support

Hive Architecture


TheHive is written in Scala and uses ElasticSearch to store and access data on the back end. The front end uses AngularJS and Bootstrap. A number of REST API endpoints are also provided to allow for integrations and bulk actions.



What is Security Case Management?

The case management functionality allows a security team to escalate investigations with detailed information and logs gathered on a single dashboard.

It facilitates easier compliance and quick response to security events as soon as they are detected or identified. Case management fast-tracks the investigation.



Streamlined Security Case Management

Comprehensive Reporting and Analysis

Interactive Real Time Analysis & Collaboration

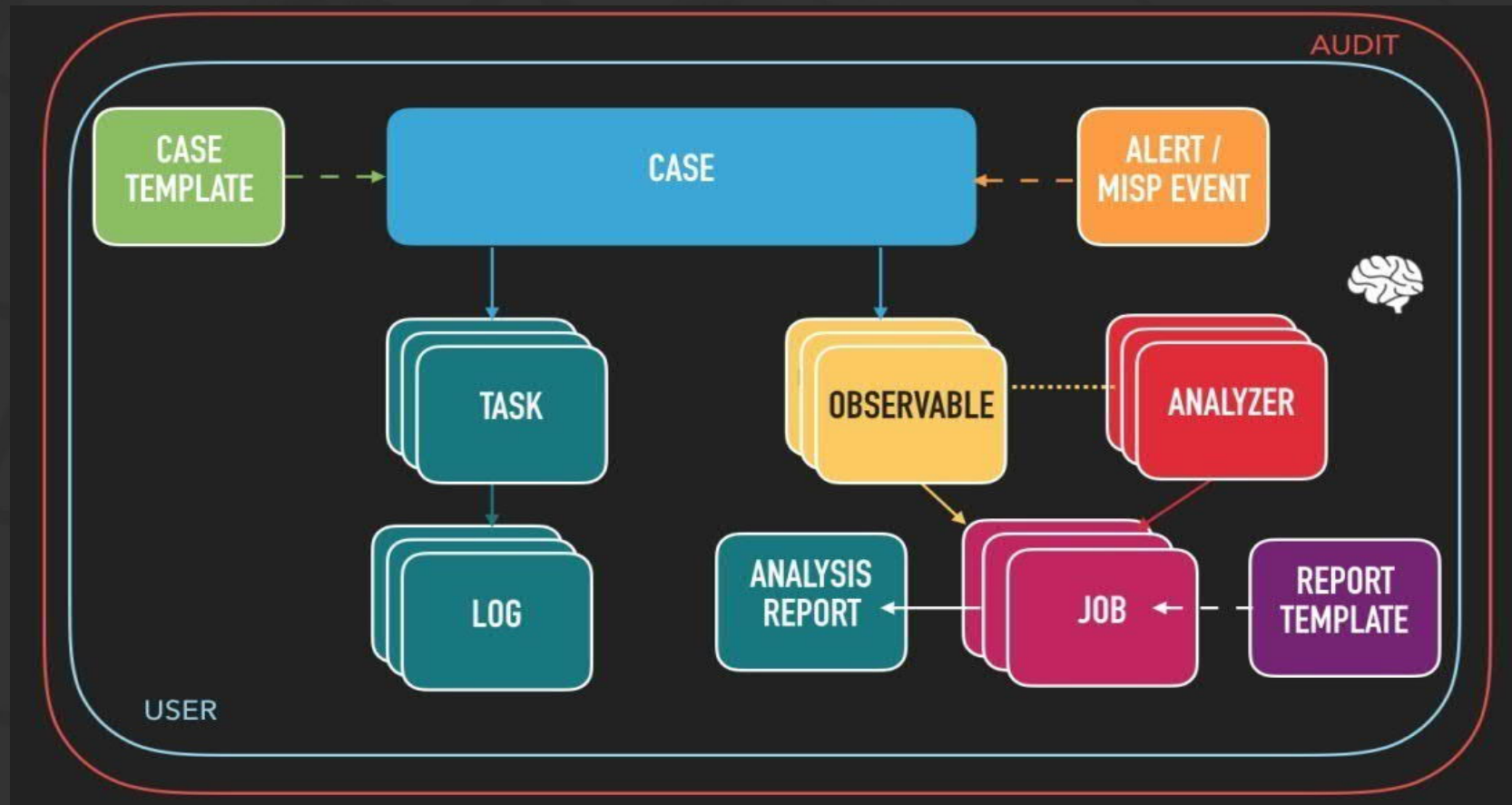
Seamless Integration

Minimum Response Time

Cases

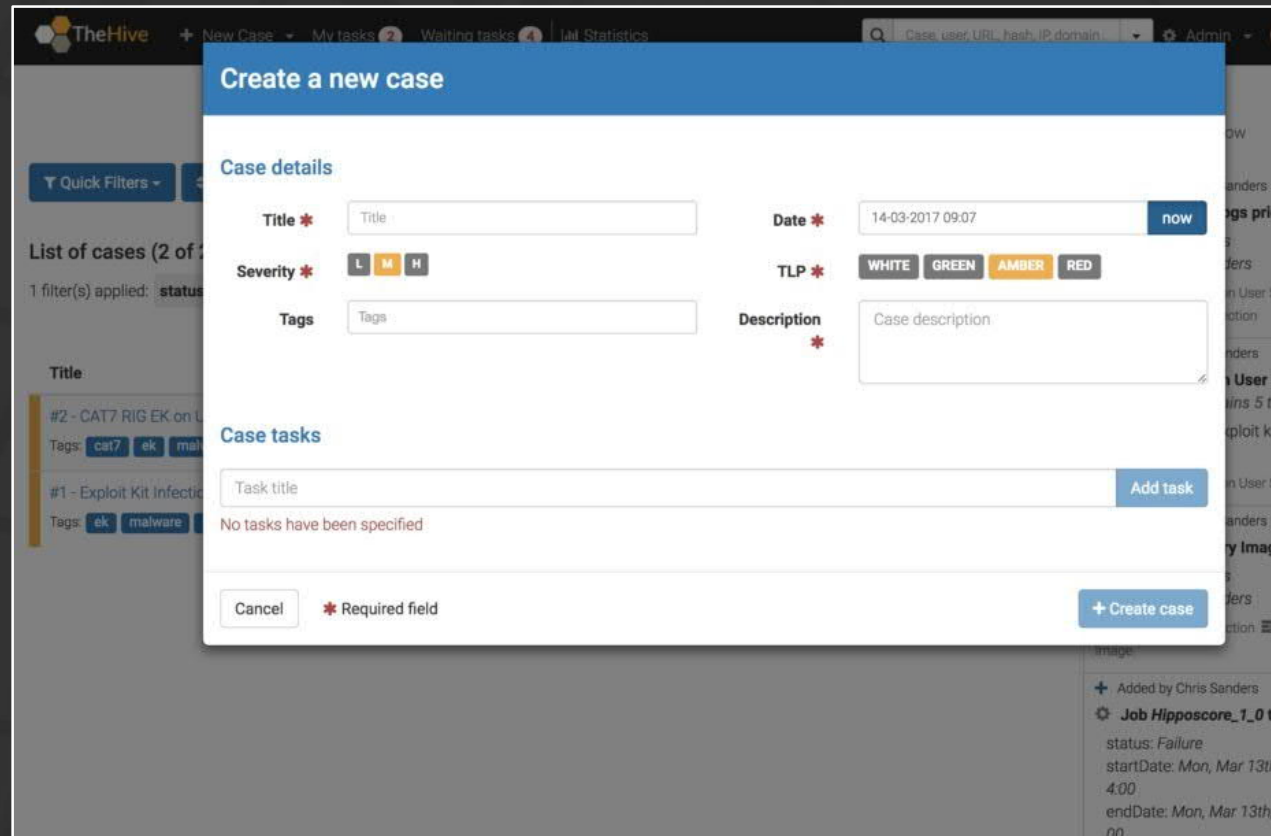
The core construct of TheHive is the investigation case.

A case can be generated from an alert or created from scratch.



Case Management

Since, case is the core construct of most security investigations, whether you're reviewing alerts, reverse engineering malware, or working a declared incident, all the data you put into a case is easily searchable from the search bar at the top of the screen



The screenshot shows the 'Create a new case' modal in TheHive. The modal is divided into two main sections: 'Case details' and 'Case tasks'.

Case details:

- Title ***: A text input field with the placeholder 'Title'.
- Severity ***: A dropdown menu with options L, M, and H. The 'M' option is currently selected.
- Tags**: A text input field with the placeholder 'Tags'.
- Date ***: A date and time picker showing '14-03-2017 09:07' and a 'now' button.
- TLP ***: A dropdown menu with options WHITE, GREEN, AMBER, and RED. The 'AMBER' option is currently selected.
- Description ***: A large text area with the placeholder 'Case description'.

Case tasks:

- Task title**: A text input field with the placeholder 'Task title'.
- Add task**: A blue button to add a new task.
- No tasks have been specified**: A message indicating that no tasks have been added yet.

Footer:

- Cancel**: A button to cancel the case creation.
- * Required field**: A legend indicating that fields with an asterisk are required.
- + Create case**: A blue button to create the new case.

Case Templates

Case Templates are present to automatically add tasks, description, metrics and custom fields while creating a new case. A user can choose to create an empty case or based on a registered template. You can create custom templates to which you add tasks as shown below.

The screenshot displays the 'Case template management' interface. On the left, a sidebar contains a '+ New template' button and a list of 'Current templates' including 'MISP' and 'Demo'. The main area is titled 'Case basic information' and contains several fields: 'Template name' (set to 'MISP' with a note 'This name should be unique'), 'Title prefix' (set to '[MISP]' with a note 'This is used to prefix the case name'), 'Severity' (set to 'M' with a note 'This will be the details case's severity'), 'TLP' (set to 'TLP:AMBER' with a note 'This will be the default case TLP'), 'Tags' (set to 'misp' and 'ioc' with a note 'These will be the default cases' tags'), and 'Description' (set to 'Imported from MISP Event.'). Below these fields, there are two sections: 'Case tasks (5)' and 'Case metrics (1)'. The 'Case tasks' section lists three tasks: '1-Identification', '2-Containment', and '3-Eradication', each with 'Edit' and 'Delete' options. The 'Case metrics' section lists one metric: 'Unique & successful C2 calls', also with 'Edit' and 'Delete' options.

Case template management

+ New template

Current templates

MISP

Demo

Case basic information

Template name * MISP
This name should be unique

Title prefix [MISP]
This is used to prefix the case name

Severity M
This will be the details case's severity

TLP TLP:AMBER
This will be the default case TLP

Tags misp ioc Tags
These will be the default cases' tags

Description * Imported from MISP Event.

Case tasks (5) + Add task

1-Identification Edit Delete

2-Containment Edit Delete

3-Eradication Edit Delete

Case metrics (1) + Add metric

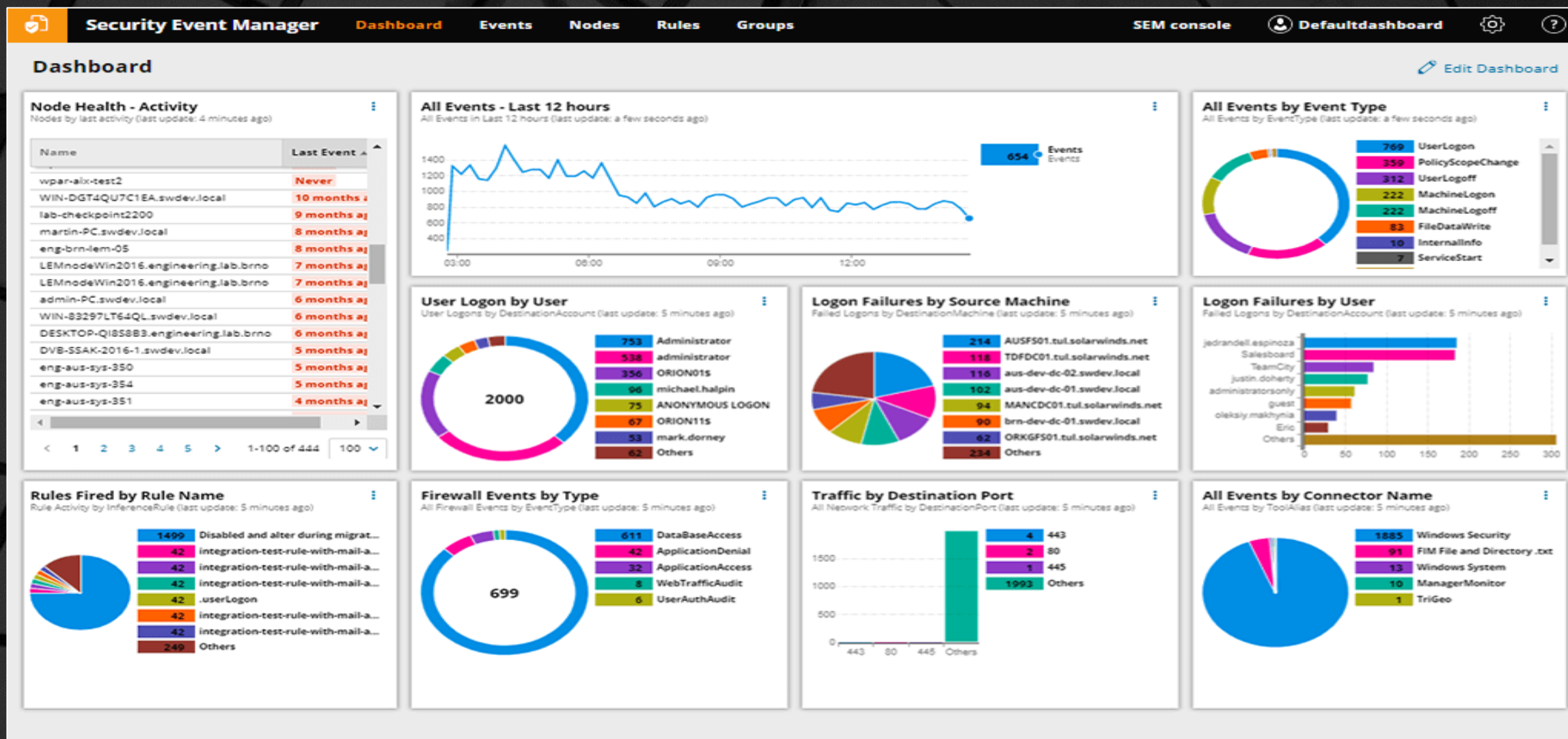
Unique & successful C2 calls Delete

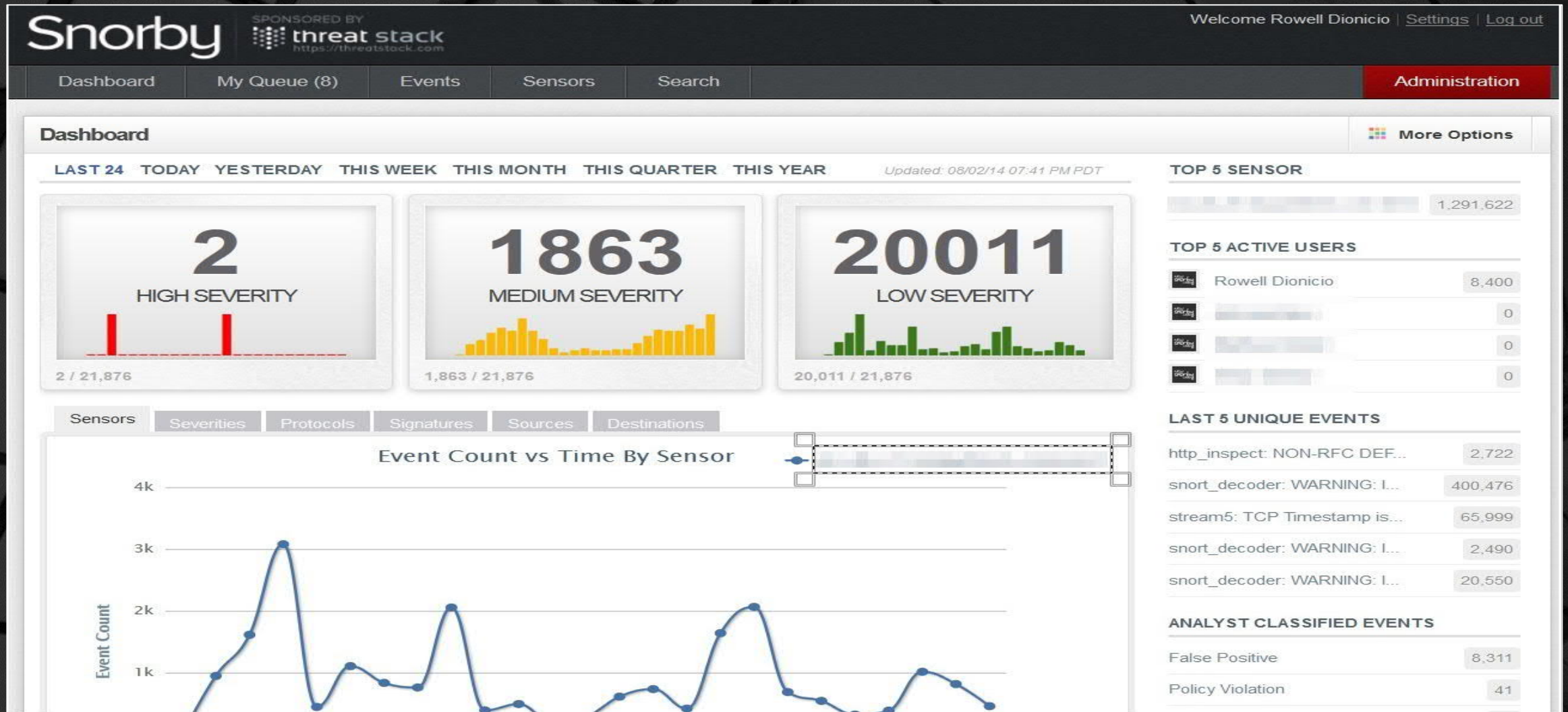
Case Templates

The user can change values defined in template. A template contains:

- ▶ default severity
- ▶ default tags
- ▶ title prefix (can be changed by user at case creation)
- ▶ default TLP
- ▶ task list (title and description)
- ▶ metrics
- ▶ custom fields

Snort





Nagios

Browser window: <http://localhost/nagios/>

Nagios

General

- Home
- Documentation

Current Status

- Tactical Overview
- Map
- Hosts
- Services
- Host Groups
 - Summary
 - Grid
- Service Groups**
 - Summary
 - Grid
- Problems
 - Services (Unhandled)
 - Hosts (Unhandled)
 - Network Outages

Quick Search:

Reports

- Availability
- Trends
- Alerts
 - History
 - Summary
 - Histogram
- Notifications
- Event Log

Current Network Status
Last Updated: Fri Sep 30 14:53:06 PDT 2011
Updated every 90 seconds
Nagios® Core™ 3.2.1 - www.nagios.org
Logged in as nagiosadmin

[View Service Status Detail For All Service Groups](#)
[View Status Summary For All Service Groups](#)
[View Service Status Grid For All Service Groups](#)

Host Status Totals




Up	Down	Unreachable	Pending
15	0	0	0

Service Status Totals






















Ok	Warning	Unknown	Critical	Pending
77	3	14	1	0

Service Overview For All Service Groups




CC (CC-Cluster)

Host	Status	Services	Actions
CC-Cluster	UP	2 OK 1 WARNING	  

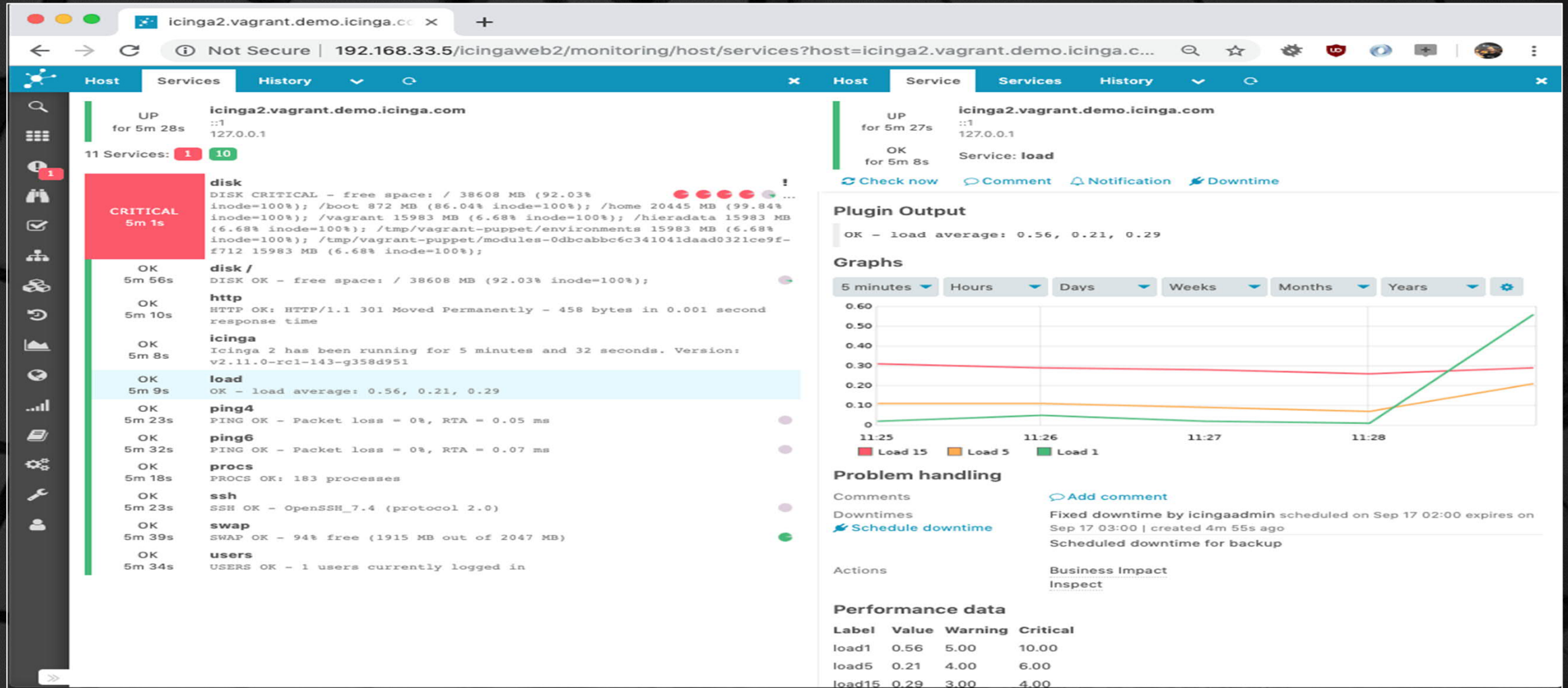
CC (CC-Databases)

Host	Status	Services	Actions
CC-App-Services	UP	13 OK	  
CC-Documents	UP	13 OK 2 UNKNOWN	  
CC-Fab	UP	13 OK	  
CC-Last-Login	UP	2 OK	  
CC-Modules	UP	2 OK	  
CC-Schemas	UP	2 OK	  
CC-Security	UP	2 OK	  

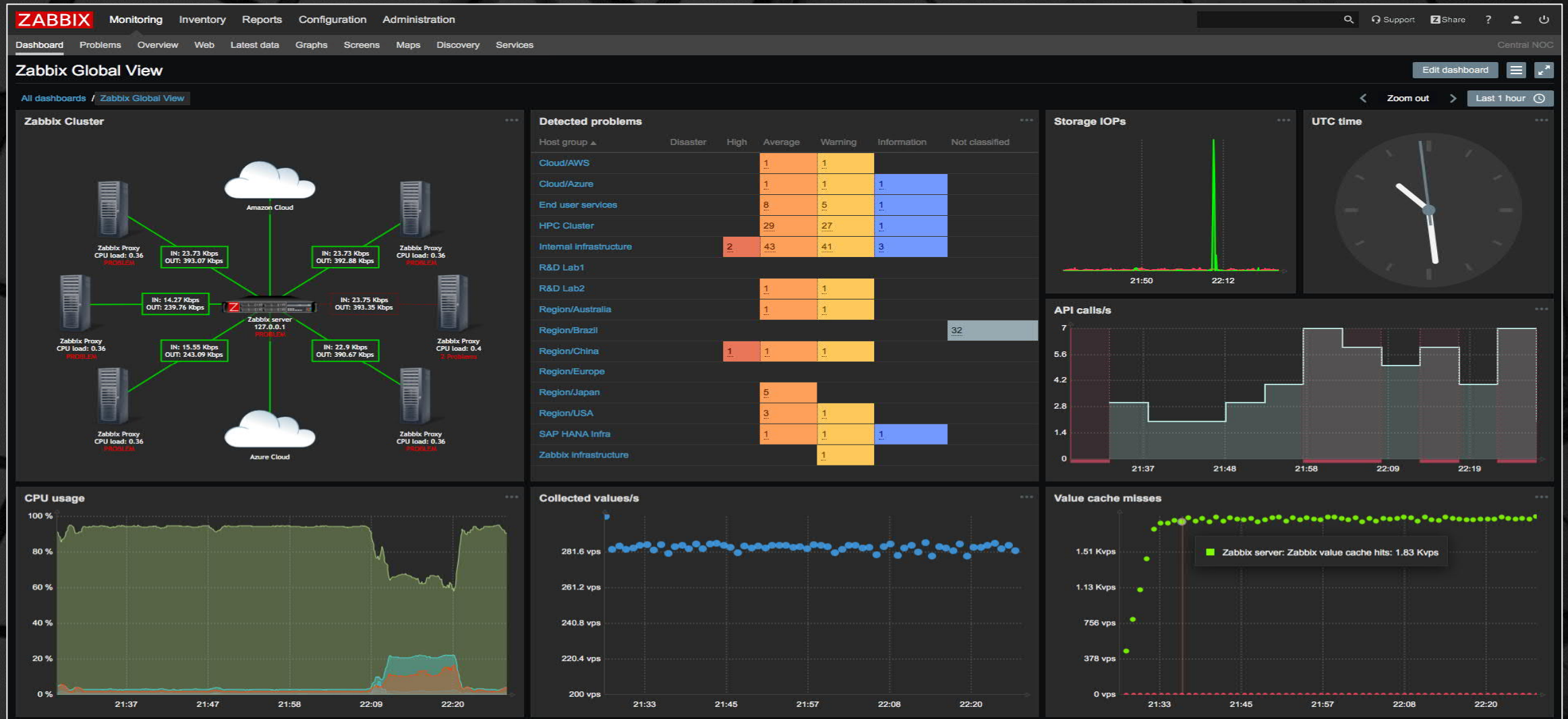
CC (CC-Hosts)

Host	Status	Services	Actions
colleen-laptop.marklogic.com	UP	9 OK	  

<http://localhost/nagios/cgi-bin/status.cgi?servicegroup=all&style=overview>



Zabbix



PhishTank

[Sign In](#)[Register](#) | [Forgot Password](#)[Home](#) [Add A Phish](#) [Verify A Phish](#) [Phish Search](#) [Stats](#) [FAQ](#) [Developers](#) [Mailing Lists](#) [My Account](#)

Join the fight against phishing

[Submit](#) suspected phishes. [Track](#) the status of your submissions.
[Verify](#) other users' submissions. [Develop](#) software with our free API.

Found a phishing site? Get started now — see if it's in the Tank:

[Is it a phish?](#)

Recent Submissions

You can help! [Sign in](#) or [register](#) (free! fast!) to verify these suspected phishes.

ID	URL	Submitted by
7310261	https://esl-playglobal.net	CyberSt0rm1
7310260	https://values.rubberduckcars.com/02834992/am_bin/...	ymst
7310259	https://nobleinstall.com/service/hosting/mail?uid=	ymst
7310258	https://mochkin.xyz/pge/891241974/1274917/index.ph...	NIRT
7310256	https://veriizonaoll.weebly.com/	j4232l
7310254	https://www.sky-bt.com/index.html	verifrom
7310253	https://santanderclient.com/	paulch

What is phishing?

Phishing is a fraudulent attempt, usually made through email, to steal your personal information.

[Learn more...](#)

What is PhishTank?

PhishTank is a collaborative clearing house for data and information about phishing on the Internet. Also, PhishTank provides an open API for developers and researchers to integrate anti-phishing data into their applications at no charge.

[Read the FAQ...](#)

[Home](#) [News](#) [Events](#) [Archive](#) [Archive ★](#) [Onhold](#) [Notify](#) [Stats](#) [Register](#) [Login](#)

NOTIFIER DOMAIN

Special defacements only ☐ Fulltext/Wildcard ☐ Onhold (Unpublished) only ☐

Date :

Total notifications: **3,339** of which **715** single ip and **2,624** 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
2019/03/21	ProtoWave Reloaded					biblioteca.ifnmg.edu.br/93.htm	Linux	mirror
2019/03/21	ProtoWave Reloaded				★	www.biblioteca.pm.go.gov.br/93...	Linux	mirror
2019/03/21	ProtoWave Reloaded				★	www.biblioteca.al.rs.gov.br/93...	Linux	mirror
2019/03/04	ProtoWave Reloaded			R	★	kenya.iom.int/nev.jpg	Linux	mirror
2019/03/04	ProtoWave Reloaded			R	★	acuna.gob.mx/nev.jpg	Linux	mirror
2019/03/04	ProtoWave Reloaded				★	mahaiwmp.gov.in/sites/nev.jpg	Unknown	mirror
2019/02/26	ProtoWave Reloaded			R	★	www.maderasdelorinoco.gob.ve/9...	Linux	mirror
2019/02/06	ProtoWave Reloaded					solosagrado.com.br/1.txt	Linux	mirror
2019/02/06	ProtoWave Reloaded					yugioh.com.br/1.txt	Linux	mirror
2018/11/30	ProtoWave Reloaded				★	ps.tjac.jus.br/93.htm	Unknown	mirror
2018/11/30	ProtoWave Reloaded				★	simba.se.gov.br/93.htm	Linux	mirror
2018/11/29	ProtoWave Reloaded				★	monitoramento.seplan.mt.gov.br...	Linux	mirror
2018/11/29	ProtoWave Reloaded				★	transitolandia.der.df.gov.br/9...	Unknown	mirror
2018/11/29	ProtoWave Reloaded				★	colegio.pm.df.gov.br/93.htm	Win 2008	mirror
2018/11/29	ProtoWave Reloaded				★	transparencia.caetite.ba.gov.b...	Unknown	mirror
2018/11/29	ProtoWave Reloaded				★	tributos.alagoinhas.ba.gov.br/...	Unknown	mirror
2018/11/29	ProtoWave Reloaded		M		★	colegio.pmdf.df.gov.br/93.htm	Win 2008	mirror
2018/11/29	ProtoWave Reloaded				★	transparencia.arapongas.pr.gov...	Win 2008	mirror
2018/11/29	ProtoWave Reloaded				★	tributosweb.petropolis.rj.gov...	Win 2012	mirror
2018/11/29	ProtoWave Reloaded				★	intranet.pedreira.sp.gov.br/93...	Win 2008	mirror
2018/11/29	ProtoWave Reloaded				★	sistemas.cbpm.ba.gov.br/93.htm	Win 2003	mirror
2018/11/29	ProtoWave Reloaded				★	transservprev.sjpatrocinio.pr...	Win 2016	mirror
2018/11/29	ProtoWave Reloaded				★	sistemas.rionegro.pr.gov.br/93...	Win 2008	mirror
2018/11/29	ProtoWave Reloaded				★	transpref.sjpatrocinio.pr.gov...	Win 2016	mirror
2018/11/29	ProtoWave Reloaded				★	sistemas2.portovelho.ro.gov.br...	Linux	mirror

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30

Malware Domain List

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

Search

Page 0 1 ... 1814

Date (UTC)	Domain	IP	Reverse Lookup	Description	ASN	
⬆ ⬇	⬆ ⬇	⬆ ⬇	⬆ ⬇	⬆ ⬇	⬆ ⬇	
2017/12/04_18:50	textspeier.de	104.27.163.228	-	phishing/fraud	13335	
2017/10/26_13:48	photoscape.ch/Setup.exe	31.148.219.11	knigazdorovya.com.	trojan	14576	
2017/09/28_08:11	izeselet.hu/wp-content/uploads/2016/03/ch.js	87.229.63.171	s3.abplusz.hu.	coin mining	62292	
2017/06/02_08:38	sarahdaniella.com/swift/SWIFT%20\$.pdf.ace	63.247.140.224	coriandertest.hmdnsgroup.com.	trojan	19271	
2017/05/01_16:22	amazon-sicherheit.kunden-ueberpruefung.xyz	185.61.138.74	hosted-by.blazingfast.io.	phishing	49349	
2017/03/20_10:13	dieutribenhkhop.com/parking/pay/rd.php?id=10	84.200.4.125	125.0-255.4.200.84.in-addr.arpa.	Ransom, Fake.PCN, Malspam	31400	
2017/03/20_10:13	dieutribenhkhop.com/parking/	84.200.4.125	125.0-255.4.200.84.in-addr.arpa.	Ransom, Fake.PCN, Malspam	31400	
2017/03/20_10:13	fourthgate.org/Yryzvt	104.200.67.194	-	Ransom, Fake.PCN, Malspam	8100	
2017/03/20_10:13	alegroup.info/ntnrhst	194.87.217.87	mccfortwayne.org.	Ransom, Fake.PCN, Malspam	197695	
2017/03/14_23:02	privatkunden.datapipe9271.com/	104.31.75.147	-	Paypal phishing	13335	
2017/03/14_23:02	ssl-6582datamanager.de/	54.72.9.51	ec2-54-72-9-51.eu-we st-1.compute.amazonaws.com.	redirects to Paypal phishing	16509	
2017/03/06_21:09	down.mykings.pw:8888/ups.rar	60.250.76.52	60-250-76-52.HINET-IP.hinet.net.	related to a Mirai windows spreader trojan	3462	
				related to a Mirai windows		

TPOT



[Home](#) [Search](#) [Articles](#) [Tools](#) [Admin](#) [RTIR](#) [Logged in as root](#)

RTIR for aperturescience42.local

RTIR

Lookup '192.168.1.2'

New ticket in Incident R 192.168.1.2

^ Current Incident: #5

#	Subject	Status Owner	Last Updated Told	Created Due	Priority Time Left
5	Possible DoS	open root	1 minute ago	6 weeks ago 2 days	50

^ Incidents: 192.168.1.2

Search

#	Subject	Status	Priority	Actions
2	a problem!	resolved	50	[Merge][Investigate]
5	Possible DoS	open	50	[Investigate]

^ Investigations: 192.168.1.2

Search

Link

#	Subject	Status	Priority	Actions
10	Possible DoS	open	0	[Link]

^ Incident Reports: 192.168.1.2

Search

Link

#	Subject	Status	Priority	Actions
1	a problem!	resolved	0	[Link]
4	Possible DoS	resolved	0	[Link]

^ Blocks: 192.168.1.2

Search

Link

Create

#	Subject	Status	Priority	Actions
3	a problem!	removed	0	[Link]
6	Possible DoS	post incident	0	[Link]

Look Up Information

Traceroute to: 192.168.1.2

Go

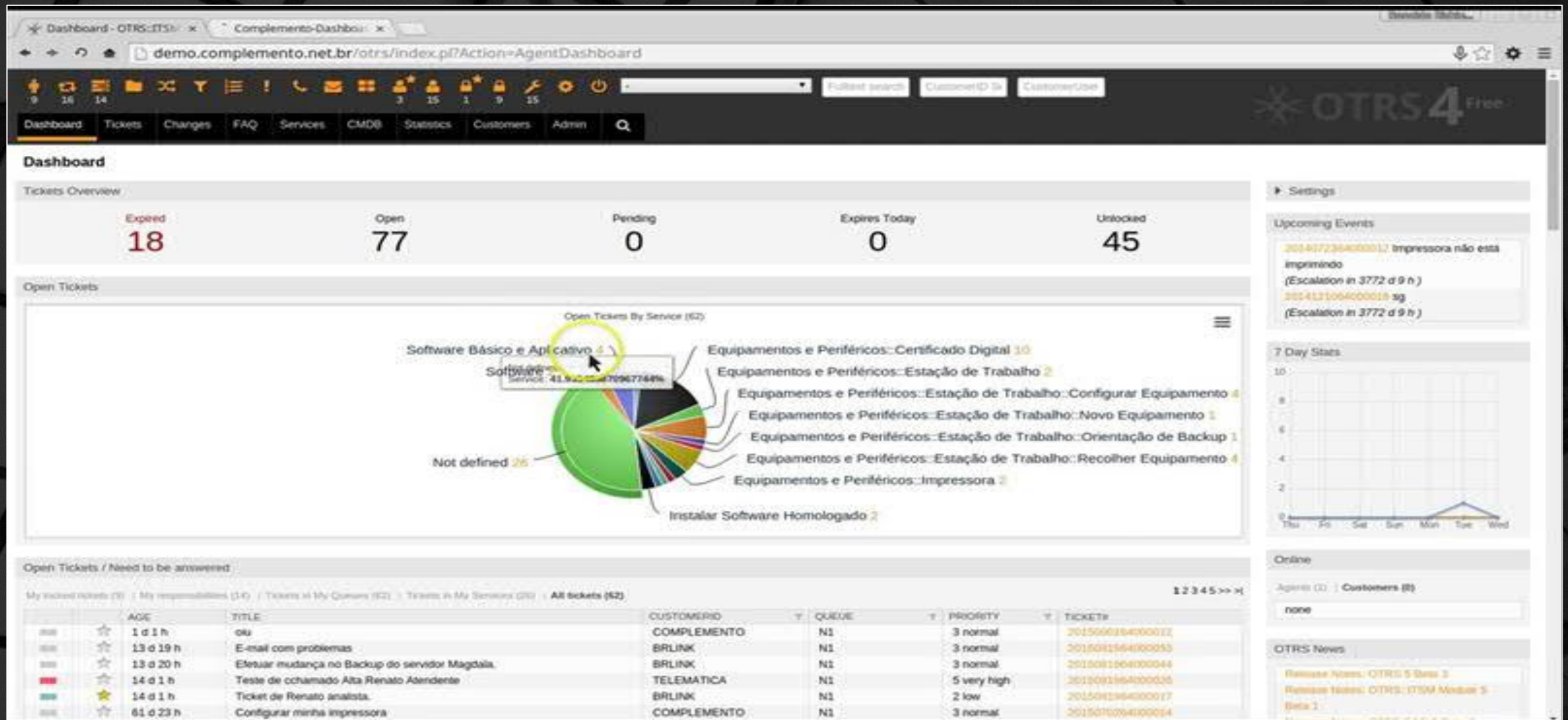
WHOIS: 192.168.1.2 at VERISIGN

Go

Research Tool: 192.168.1.2 at CVE

Go

OTRS





Questions



Thank You