FIRST & AfricaCERT Virtual Symposium for Africa and Arab Regions

SAHER
Cyberthreat supervision platform based on open source tools

Mariem Mahjoub

TLP:WHITE

○○○

FIRST Improving Security Together

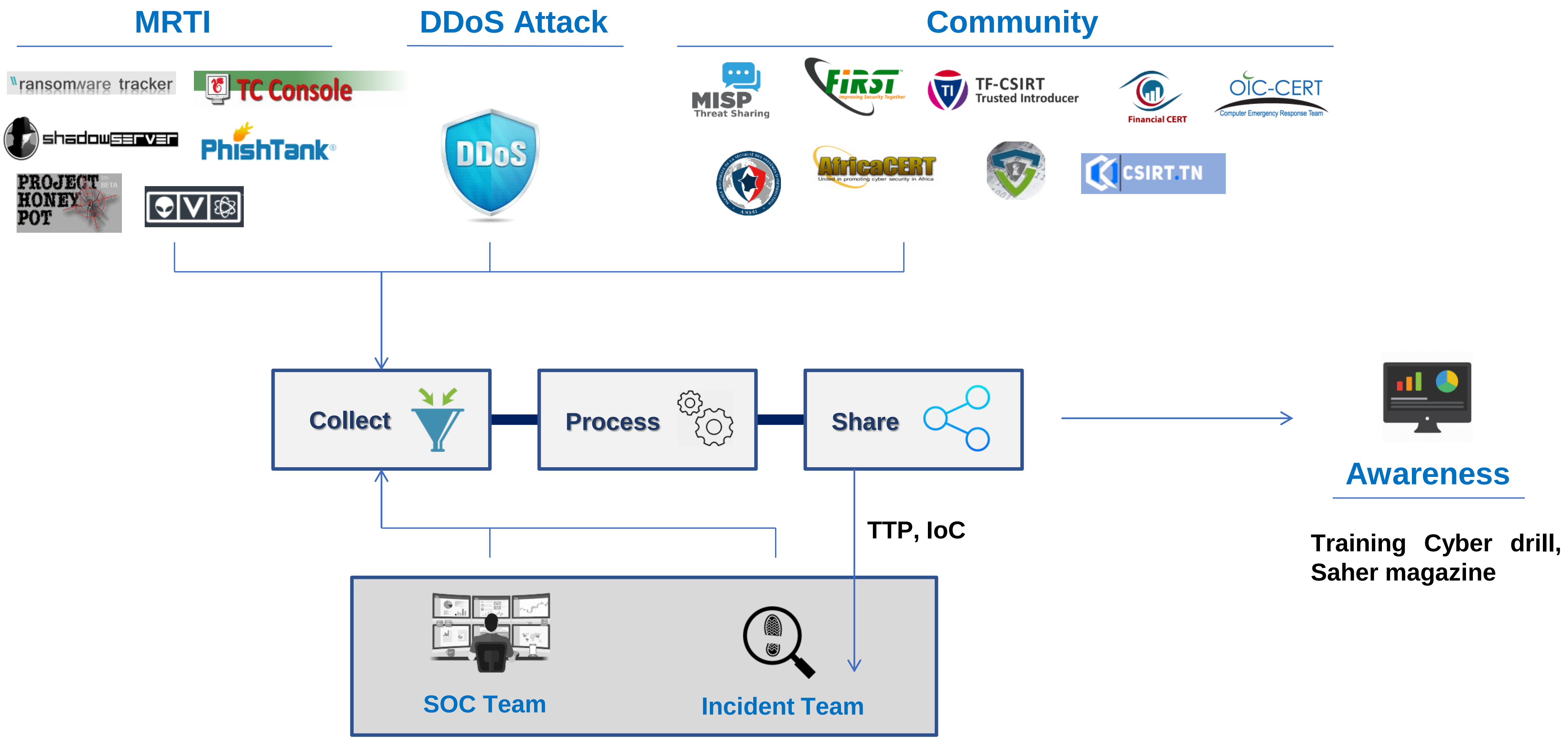
AfricaCERT

الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

SAHER

- Technical Plateform
- Open Source tools
- Developed by the ISAC team
- Real-time cyber attack monitoring

SAHER architecture



ransomware tracker
TC Console
shadowserver
PhishTank
PROJECT HONEY POT
DDoS
MISP Threat Sharing
FIRST Improving Security Together
TF-CSIRT Trusted Introducer
Financial CERT
OIC-CERT Computer Emergency Response Team
ANSSI
AfricaCERT United in promoting cyber security in Africa
CSIRT.TN

MRTI

DDoS Attack

Community

Collect

Process

Share

TTP, IoC

SOC Team

Incident Team

Awareness

Training Cyber drill, Saher magazine

SAHER

- Services’s availability supervision (POP, SMTP, DNS, HTTP…)
- IP REPUTATION
- Detection of massive attacks (DDoS, Mining, IoT, …)
- Behaviour study of attackers
- DDoS Attack

SAHER Tools

Threat intel

Firewall

Web SSO

VPN

IP Manager

Monitoring

Request Tracker

Dashboard

Mattermost

MISP

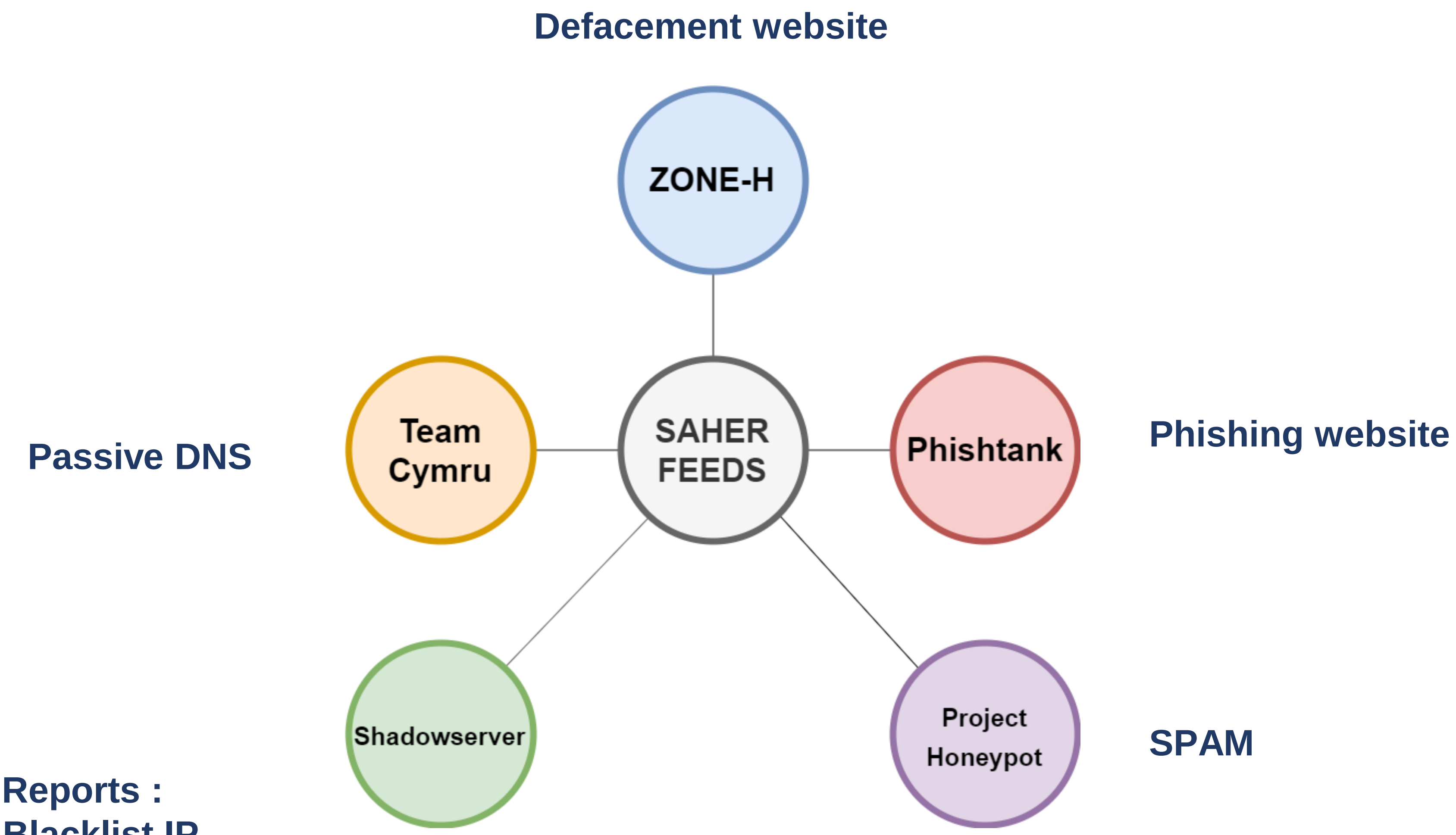
IDS

Case Manager

Elastic stack

Doc Sharing

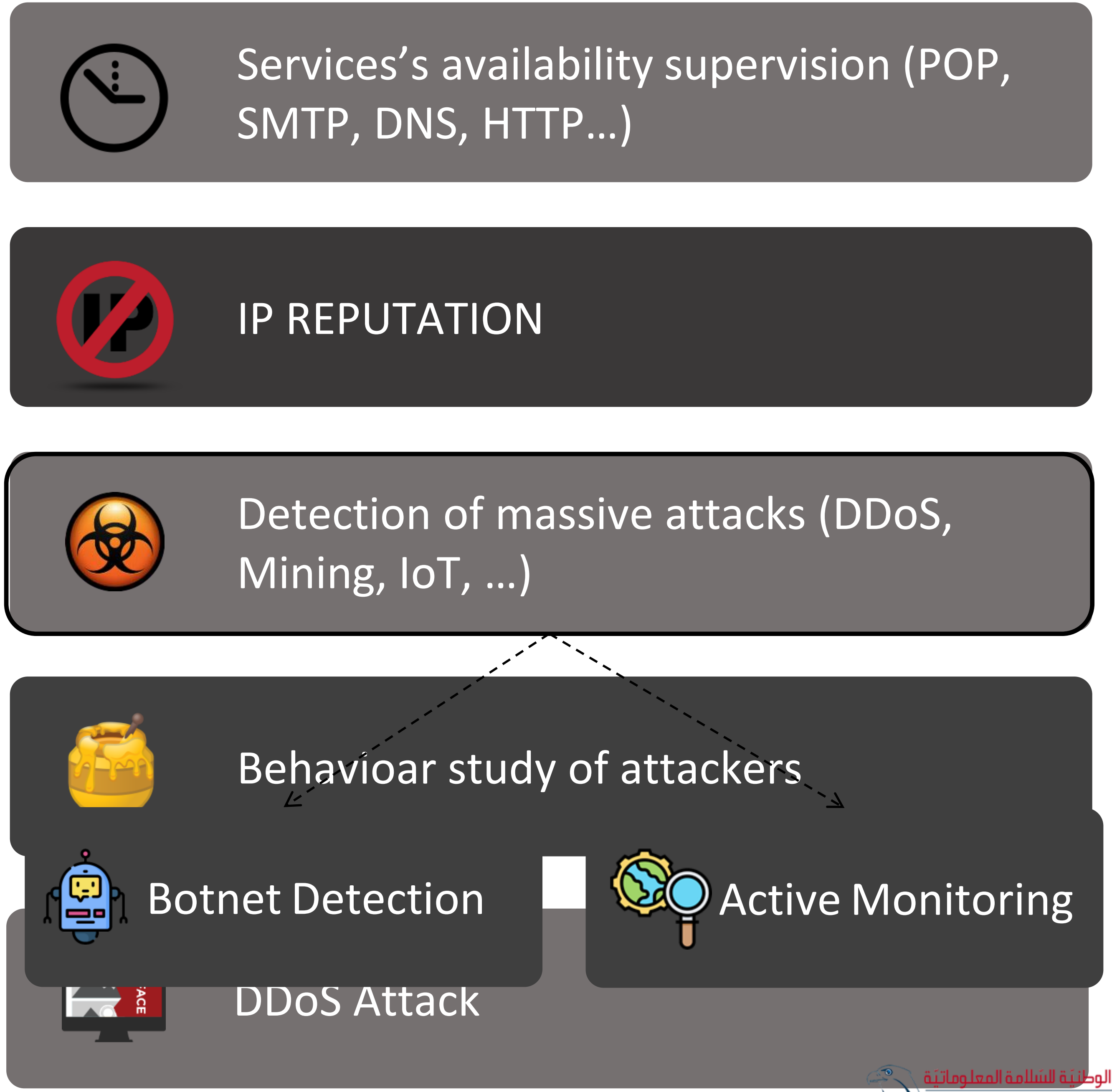
SAHER Feeds



76 Reports :

- Blacklist IP
- Accessible RDP, SMB, SSH, FTP, Hadoop
- …

SAHER



Services’s availability supervision (POP, SMTP, DNS, HTTP…)

IP REPUTATION

Detection of massive attacks (DDoS, Mining, IoT, …)

Behavioar study of attackers

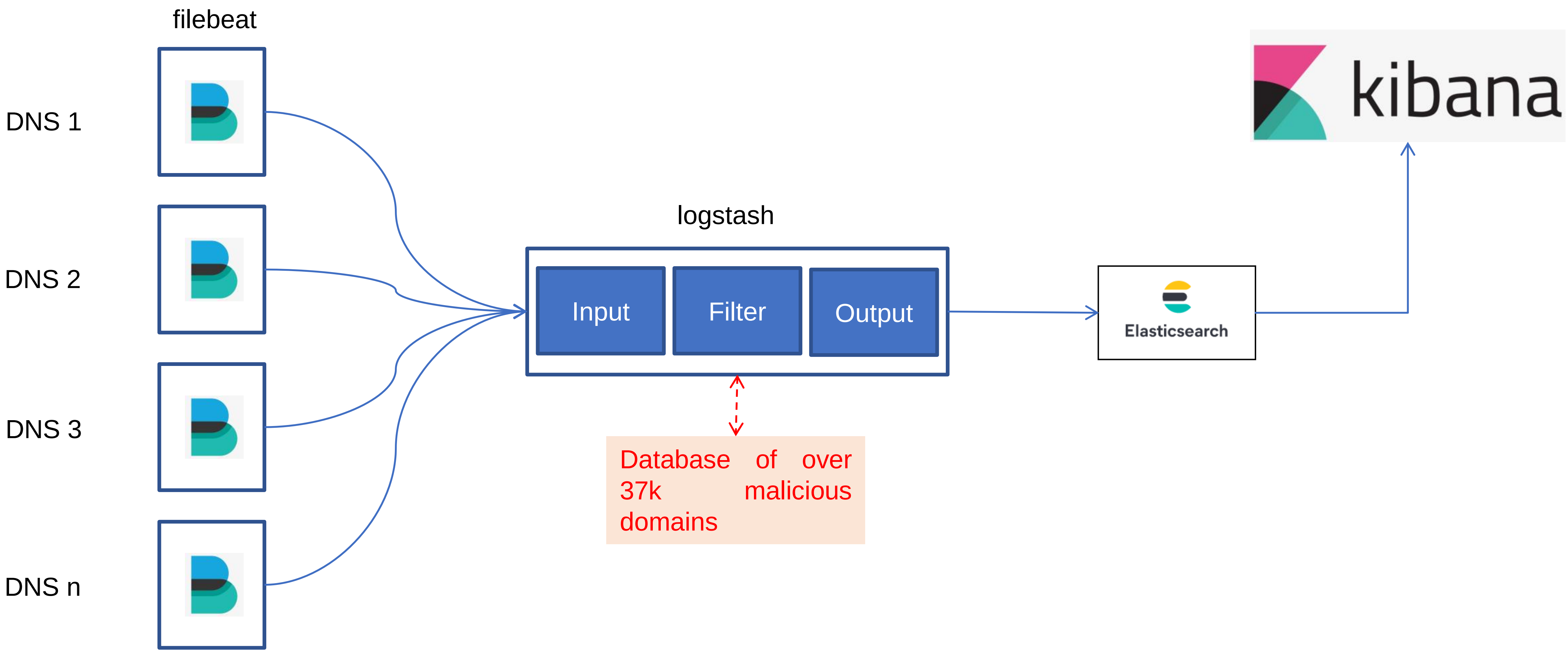
Botnet Detection

Active Monitoring

DDoS Attack

الوكالة الوطنية للسلامة المعلوماتية
Agence Nationale de la Sécurité Informatique

SAHER :: Botnet detection



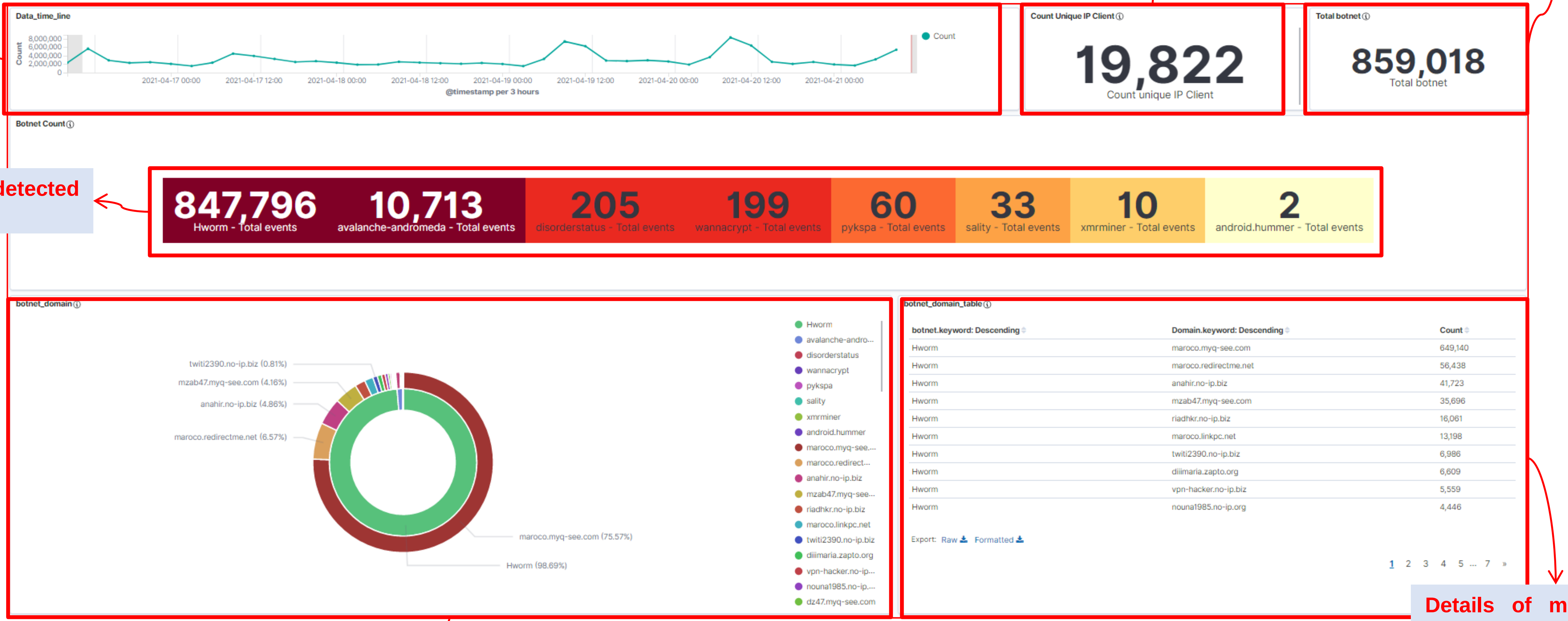
Database of over 37k malicious domains

Screenshot dashboard

Number of botnet per day

Number of unique IP addresses

Total Botnet



Data_time_line

Count Unique IP Client ⓘ

19,822
Count unique IP Client

Total botnet ⓘ

859,018
Total botnet

Botnet Count ⓘ

847,796	10,713	205	199	60	33	10	2
Hworm - Total events	avalanche-andromeda - Total events	disorderstatus - Total events	wannacrypt - Total events	pykspa - Total events	sality - Total events	xmrminer - Total events	android.hummer - Total events

botnet_domain ⓘ

botnet_domain_table ⓘ

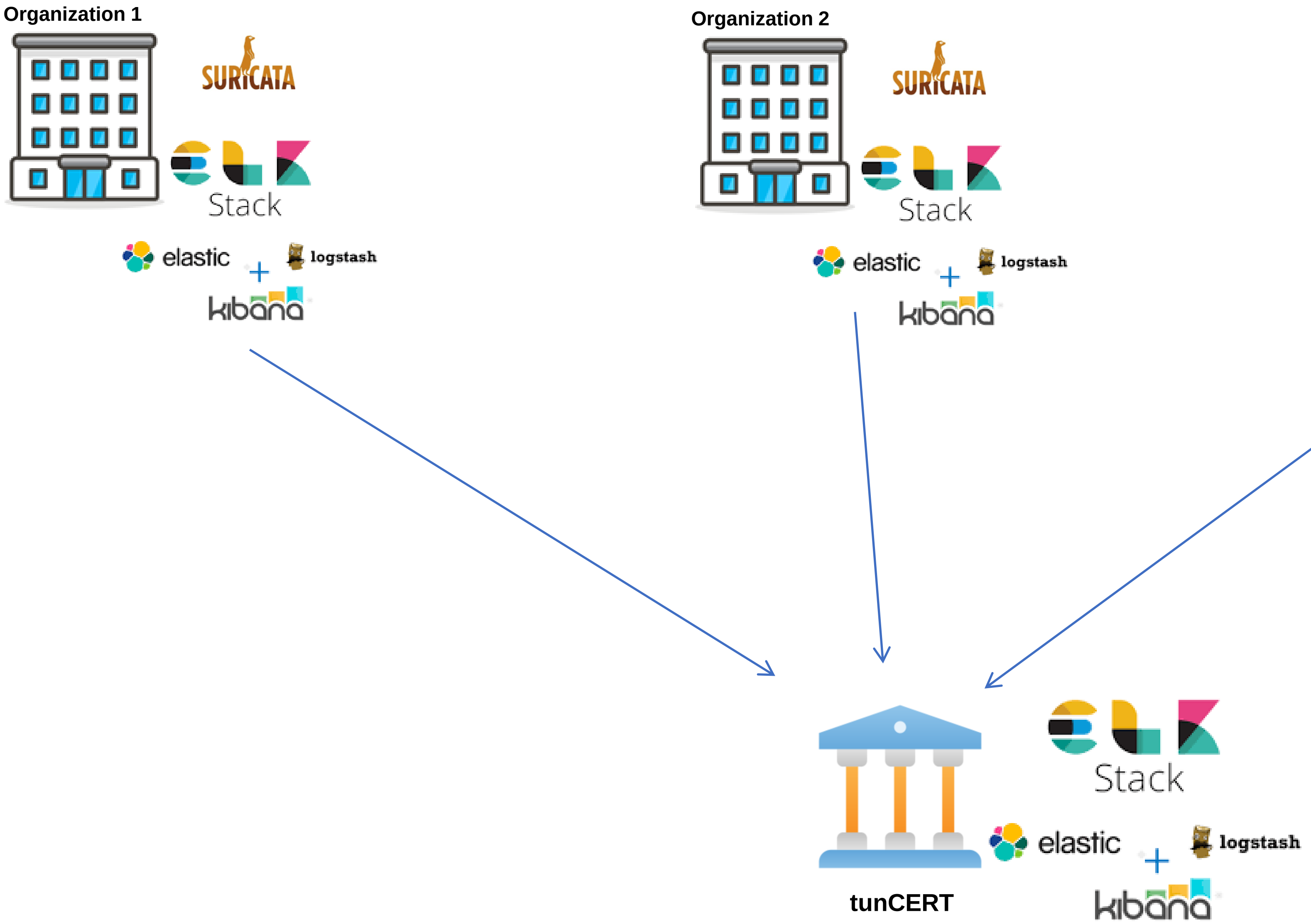
botnet.keyword: Descending	Domain.keyword: Descending	Count
Hworm	maroco.myq-see.com	649,140
Hworm	maroco.redirectme.net	56,438
Hworm	anahir.no-ip.biz	41,723
Hworm	mzab47.myq-see.com	35,696
Hworm	riadhkr.no-ip.biz	16,061
Hworm	maroco.linkpc.net	13,198
Hworm	twiti2390.no-ip.biz	6,986
Hworm	diiimaria.zapto.org	6,609
Hworm	vpn-hacker.no-ip.biz	5,559
Hworm	nouna1985.no-ip.org	4,446

List of detected botnets

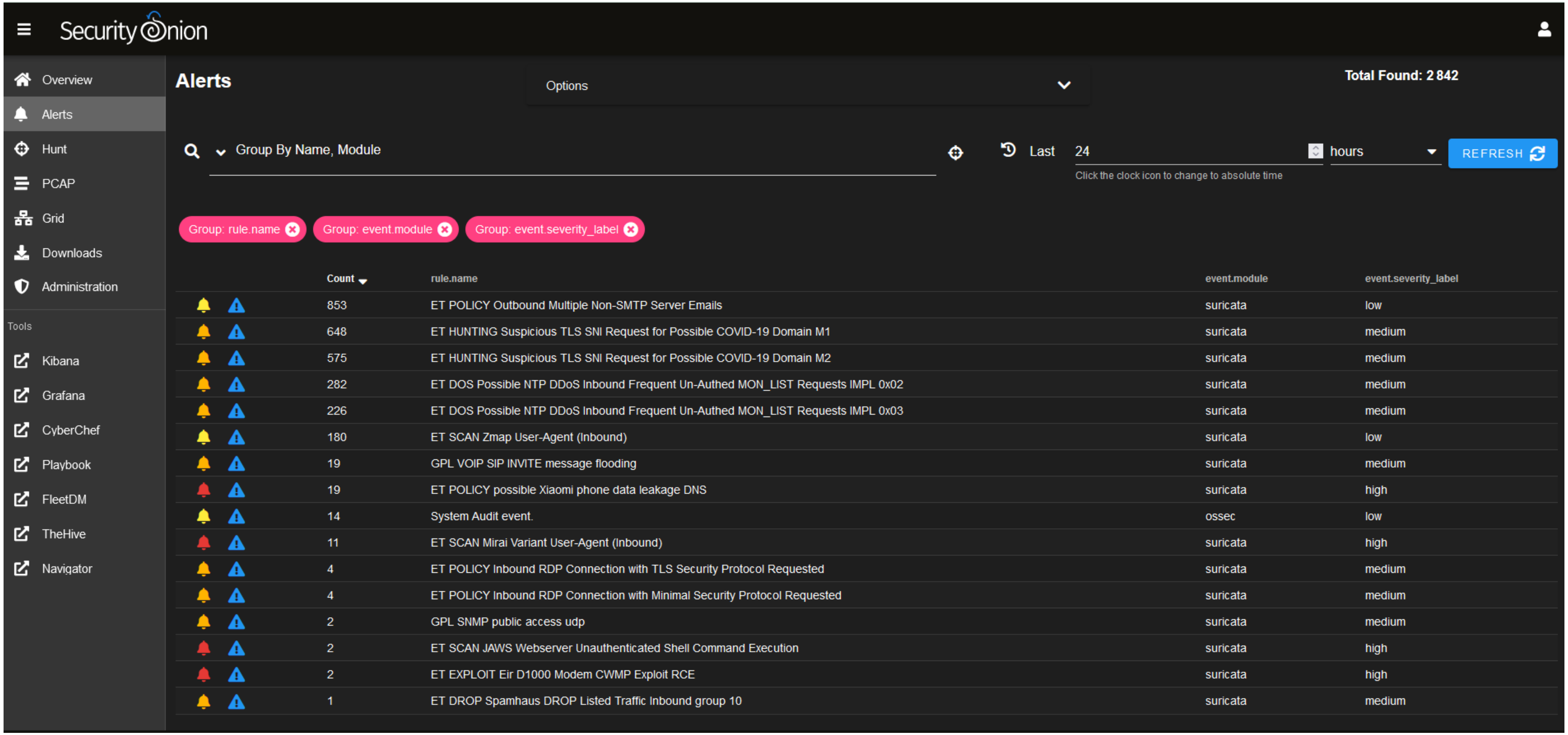
Details of malicious domains / botnets

Malicious domains

SAHER::Active Monitoring



SAHER::Active Monitoring



Alerts

Total Found: 2 842

Group By Name, Module

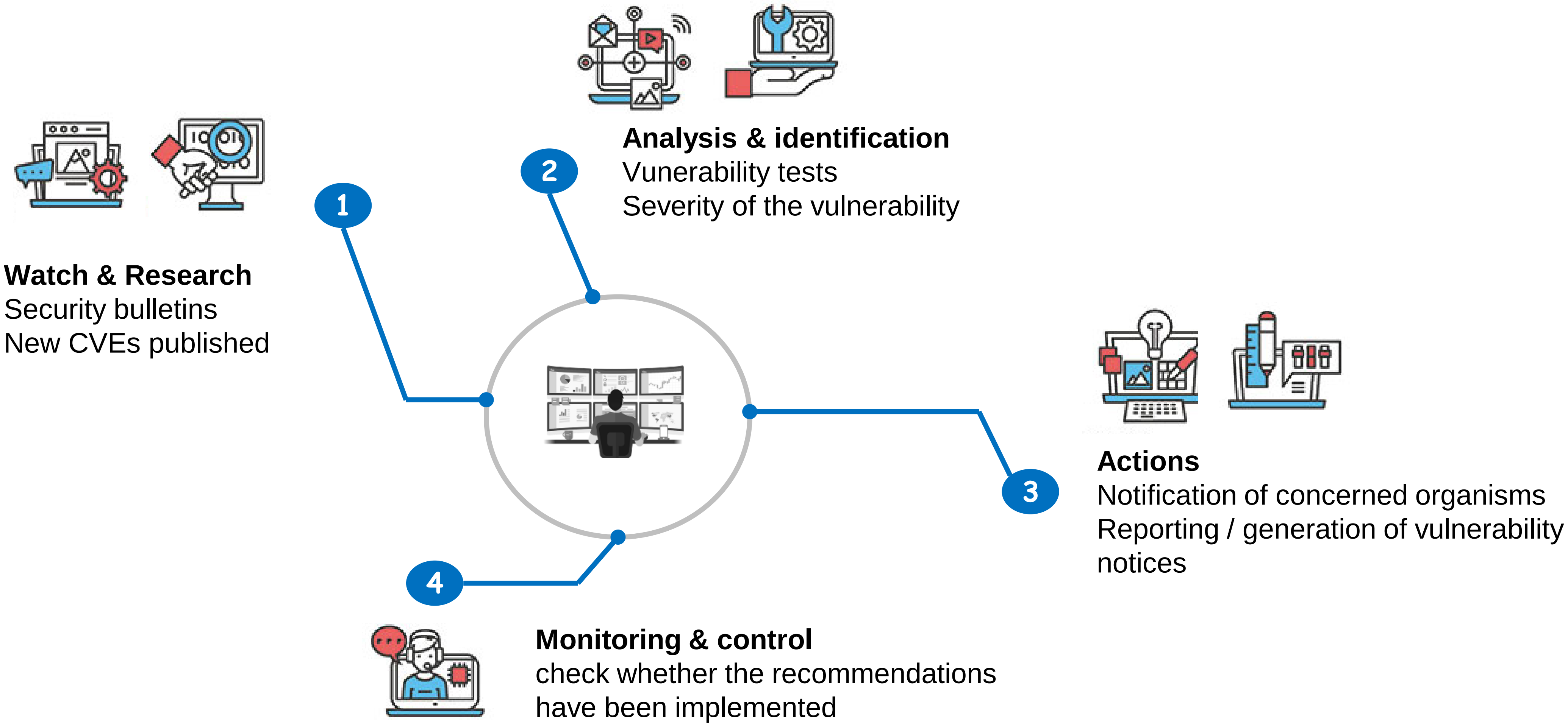
Last 24 hours

Click the clock icon to change to absolute time

Group: rule.name ⊗ Group: event.module ⊗ Group: event.severity_label ⊗

		Count	rule.name	event.module	event.severity_label
🔔	⚠	853	ET POLICY Outbound Multiple Non-SMTP Server Emails	suricata	low
🔔	⚠	648	ET HUNTING Suspicious TLS SNI Request for Possible COVID-19 Domain M1	suricata	medium
🔔	⚠	575	ET HUNTING Suspicious TLS SNI Request for Possible COVID-19 Domain M2	suricata	medium
🔔	⚠	282	ET DOS Possible NTP DDoS Inbound Frequent Un-Authed MON_LIST Requests IMPL 0x02	suricata	medium
🔔	⚠	226	ET DOS Possible NTP DDoS Inbound Frequent Un-Authed MON_LIST Requests IMPL 0x03	suricata	medium
🔔	⚠	180	ET SCAN Zmap User-Agent (Inbound)	suricata	low
🔔	⚠	19	GPL VOIP SIP INVITE message flooding	suricata	medium
🔔	⚠	19	ET POLICY possible Xiaomi phone data leakage DNS	suricata	high
🔔	⚠	14	System Audit event.	ossec	low
🔔	⚠	11	ET SCAN Mirai Variant User-Agent (Inbound)	suricata	high
🔔	⚠	4	ET POLICY Inbound RDP Connection with TLS Security Protocol Requested	suricata	medium
🔔	⚠	4	ET POLICY Inbound RDP Connection with Minimal Security Protocol Requested	suricata	medium
🔔	⚠	2	GPL SNMP public access udp	suricata	medium
🔔	⚠	2	ET SCAN JAWS Webserver Unauthenticated Shell Command Execution	suricata	high
🔔	⚠	2	ET EXPLOIT Eir D1000 Modem CWMP Exploit RCE	suricata	high
🔔	⚠	1	ET DROP Spamhaus DROP Listed Traffic Inbound group 10	suricata	medium

SAHER :: continuous supervision..



1

Watch & Research
Security bulletins
New CVEs published

2

Analysis & identification
Vunerability tests
Severity of the vulnerability

3

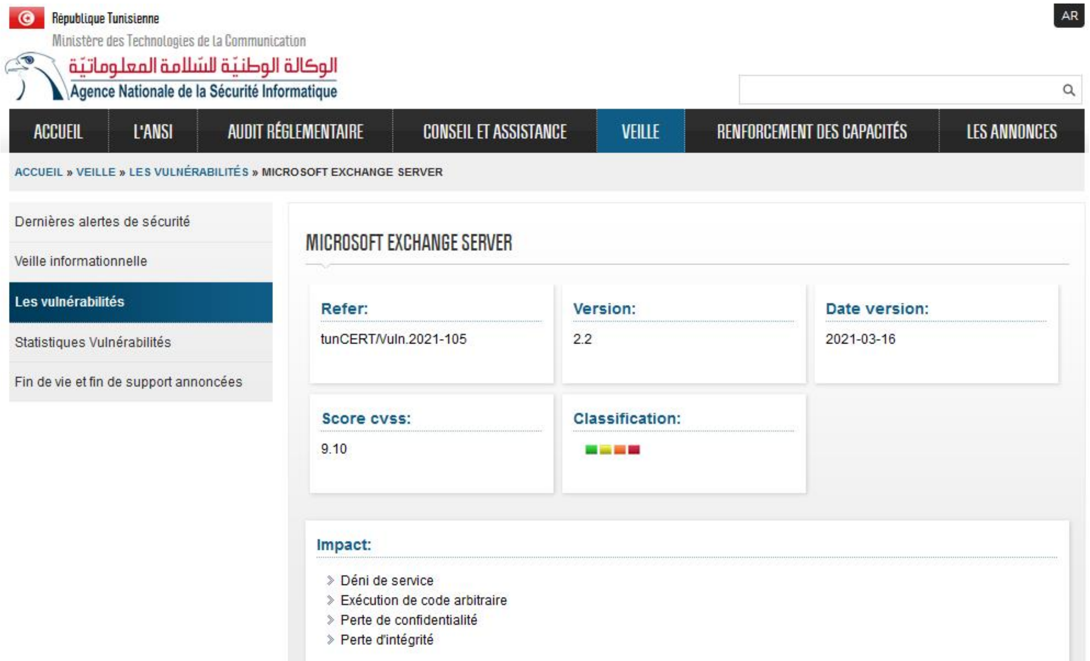
Actions
Notification of concerned organisms
Reporting / generation of vulnerability notices

4

Monitoring & control
check whether the recommendations have been implemented

SAHER : : Use Case proxy logon

- 200 Exchange Servers
- Several vulnerable servers
- Several compromised servers (with webshell)
- https://www.ansi.tn/fr/tuncert/les-vulnerabiltes/microsoft-exchange-server-11


République Tunisienne
Ministère des Technologies de la Communication
الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique
AR
ACCUEIL
L'ANSI
AUDIT RÉGLEMENTAIRE
CONSEIL ET ASSISTANCE
VEILLE
RENFORCEMENT DES CAPACITÉS
LES ANNONCES
ACCUEIL » VEILLE » LES VULNÉRABILITÉS » MICROSOFT EXCHANGE SERVER
Dernières alertes de sécurité
Veille informationnelle
Les vulnérabilités
Statistiques Vulnérabilités
Fin de vie et fin de support annoncées

MICROSOFT EXCHANGE SERVER

Refer:
tunCERT/Vuln.2021-105

Version:
2.2

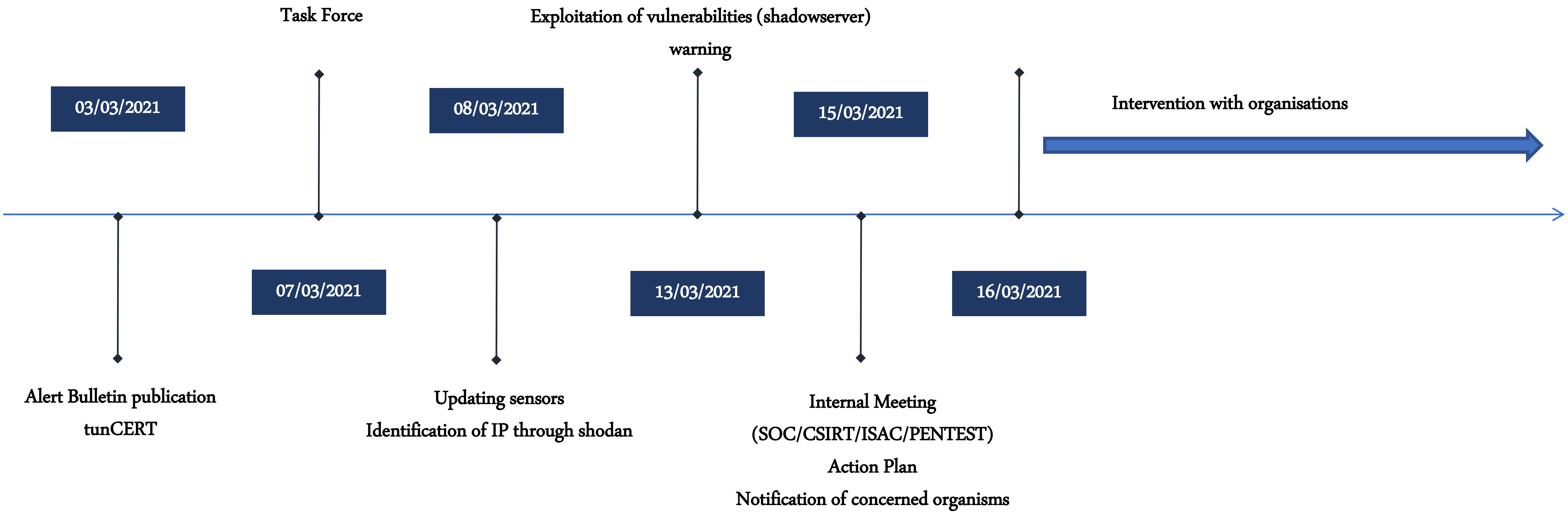
Date version:
2021-03-16

Score cvss:
9.10

Classification:
🟩🟨🟧🟥

Impact:
- Déni de service
- Exécution de code arbitraire
- Perte de confidentialité
- Perte d'intégrité

Timeline ProxyLogon/Microsoft Exchange



03/03/2021

Alert Bulletin publication
tunCERT

07/03/2021

Task Force

08/03/2021

Updating sensors
Identification of IP through shodan

13/03/2021

Exploitation of vulnerabilities (shadowserver)
warning

15/03/2021

Internal Meeting
(SOC/CSIRT/ISAC/PENTEST)
Action Plan
Notification of concerned organisms

16/03/2021

Intervention with organisations

A continuous work…

Thank you

saher@ansi.tn