Mentimeter

Octopus Conference 2019

Cooperation against Cybercrime

20-22 November 2019

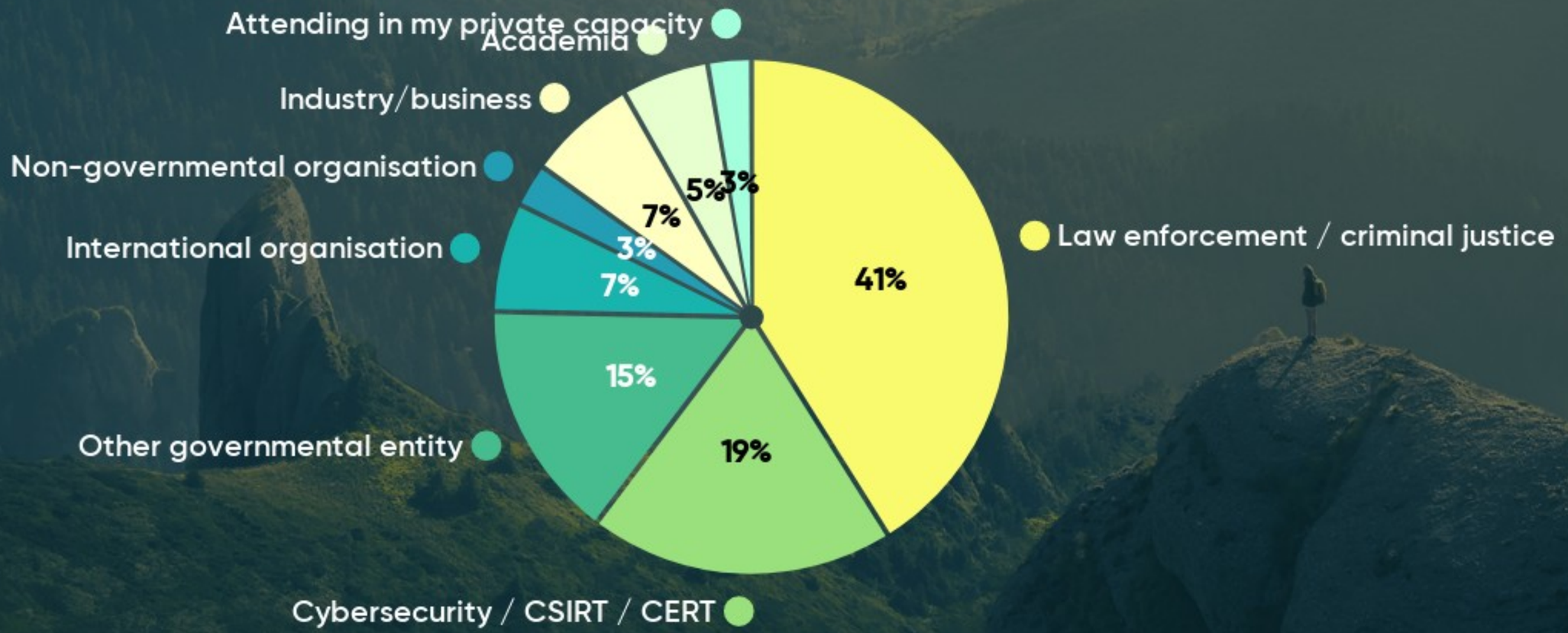
Palais de l'Europe, Council of Europe, Strasbourg, France

Workshop 3


Mentimeter
COOPERATION ON CYBERCRIME AND CYBERSECURITY
FROM INCIDENTS RESPONSE TO CRIMINAL JUSTICE
4
1

What is your background?

Mentimeter



58

What are your expectations from this Workshop?

Mentimeter

67

Your view on current level of cooperation between law enforcement and CSIRT/CERT

Mentimeter

70


Mentimeter
"INCIDENTS" VERSUS "CRIME"
DEFINING THE TERMS AND RESPONSE

Mentimeter

COMMON TAXONOMY FOR LAW ENFORCEMENT AND THE NATIONAL NETWORK OF CSIRTS

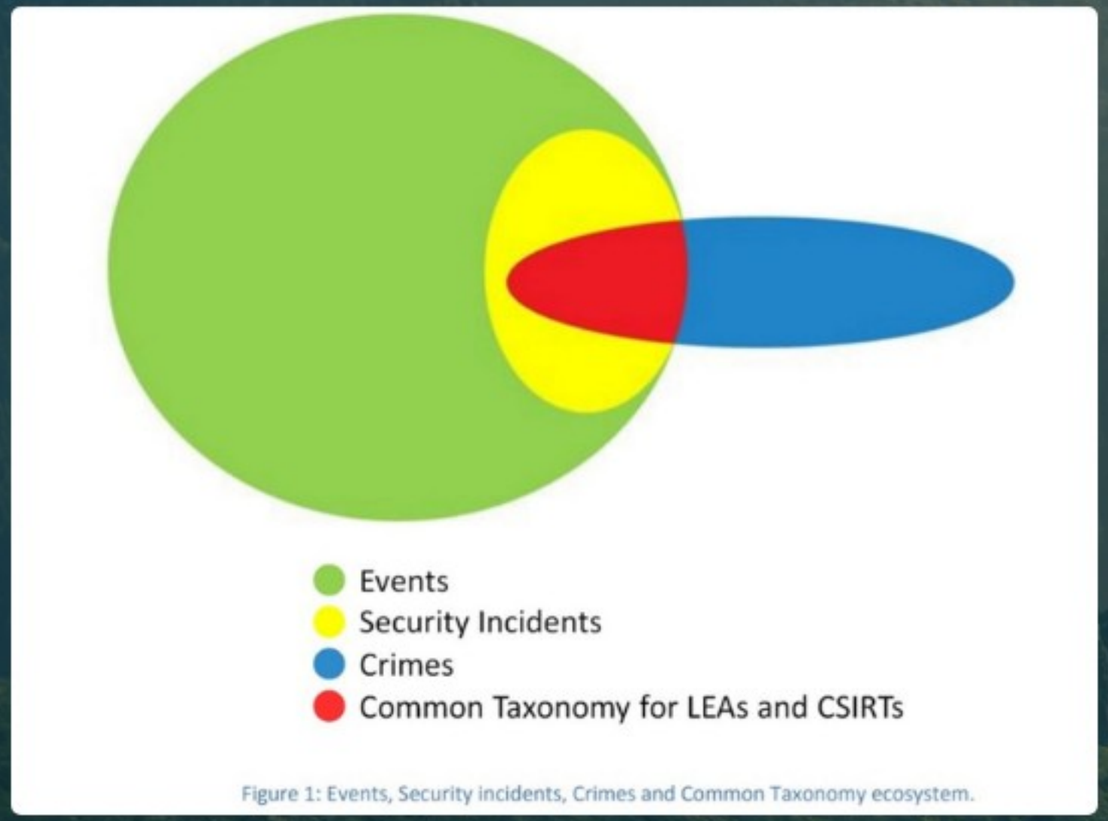


Figure 1: Events, Security incidents, Crimes and Common Taxonomy ecosystem.

- Produced jointly by ENISA / Europol
- Actual version 1.3 of December 2017
- Mapping each type of cyber incident with relevant international legal framework

Mentimeter

A FEW CONSIDERATIONS

- Define what is the scope of incident handling: prevention, report, management, corrective action
- Applicable framework can often dictate the fate of the incident or case
- Time of discovery/first response route is important
- One incident, several paths to follow (internal, CSIRT/CERT, law enforcement, other agency, etc.)
- Who is entitled to define the act as "incident" or "crime"

Malware attached to a message or email message containing link to malicious URL or IP.

Mentimeter

65

Single system scan searching for open ports or services using these ports for responding.

Mentimeter

57

Interception of communications without authorisation of subjects or not on the grounds prescribed by law.

Mentimeter

51

Mass mailing of requests (network packets, emails, etc.) from one single source to a specific service, aimed at affecting its normal functioning.

Mentimeter

54

Mass emailing aimed at collecting data for phishing purposes with regard to the victims.

Mentimeter

46

Unauthorised manipulation or reading of information contained in a database by using the SQL injection technique.

Mentimeter

42

Unauthorised access to a system or component by using credentials found in open access.

Mentimeter

41

Unsuccessful login by using sequential credentials for gaining access to the system.

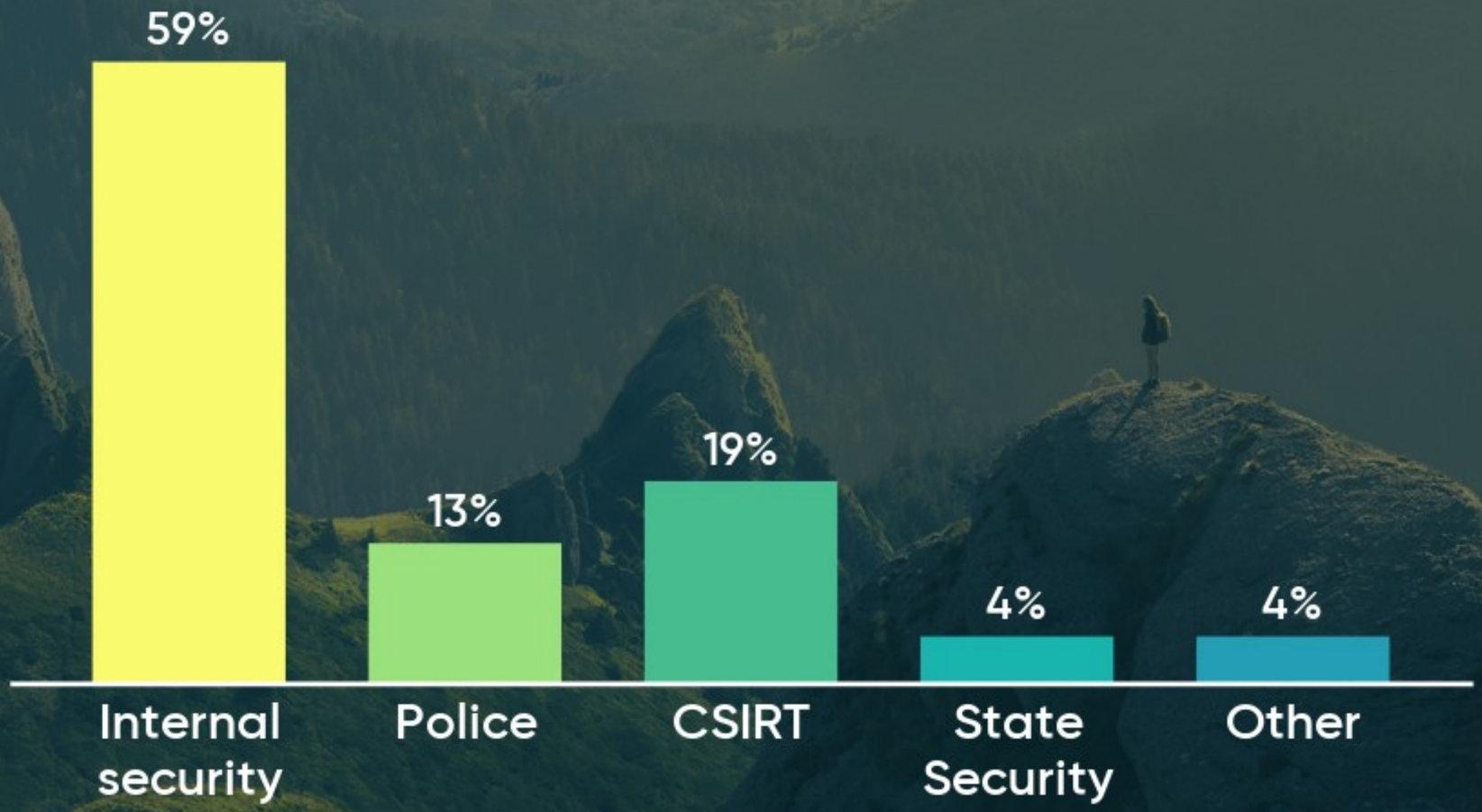
Mentimeter

38


Mentimeter
ONE INCIDENT, TWO PATHS?
DIFFERENCES BETWEEN INCIDENT HANDLING AND CRIMINAL INVESTIGATIONS

Whenever there is a minor cyber incident in your institution (breach of data, port scan, etc.), it is usually reported to:

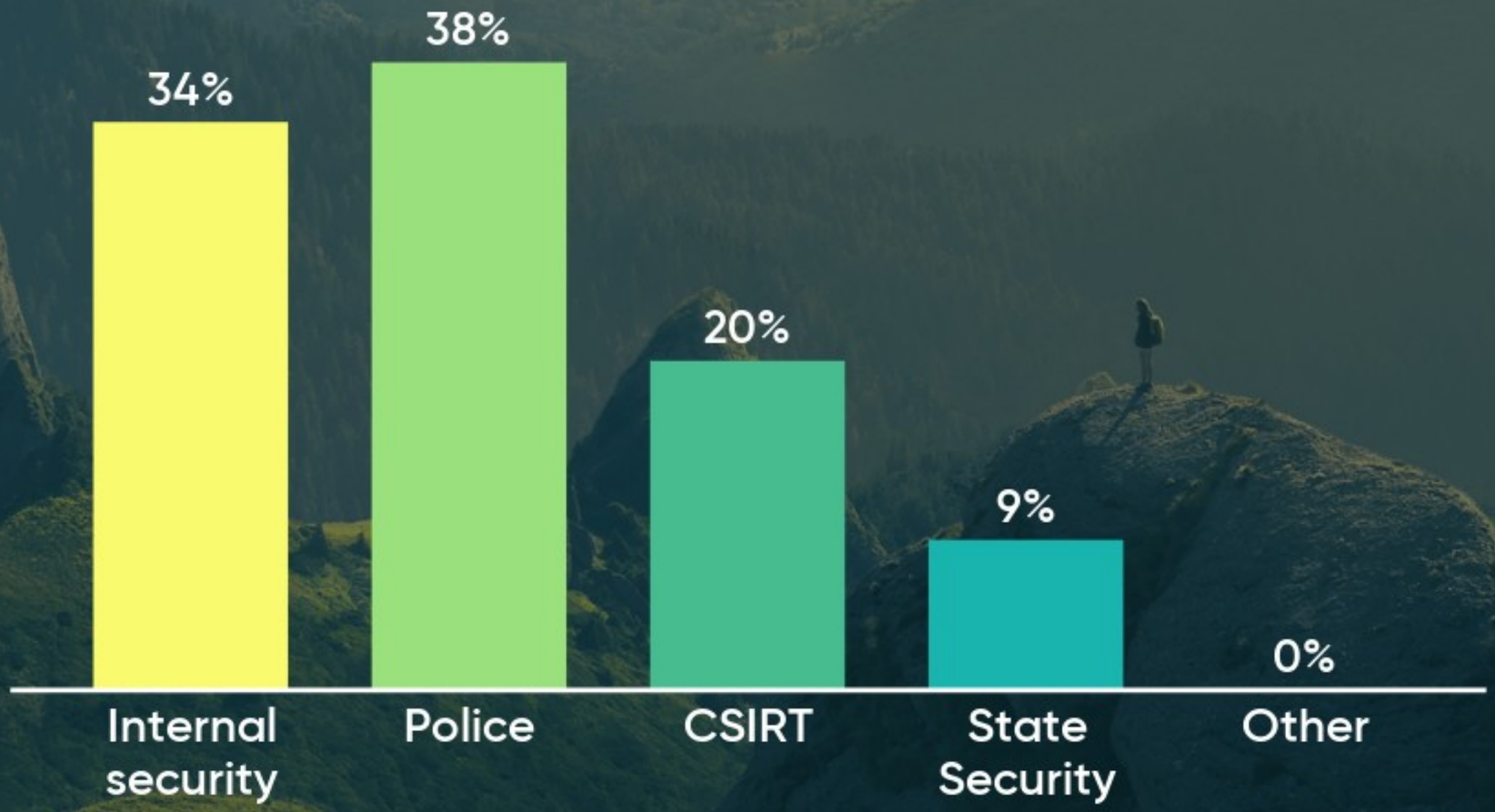
Mentimeter



57

Whenever there is a major cyber incident in your institution (DDos, defacement, etc.), it is usually reported to:

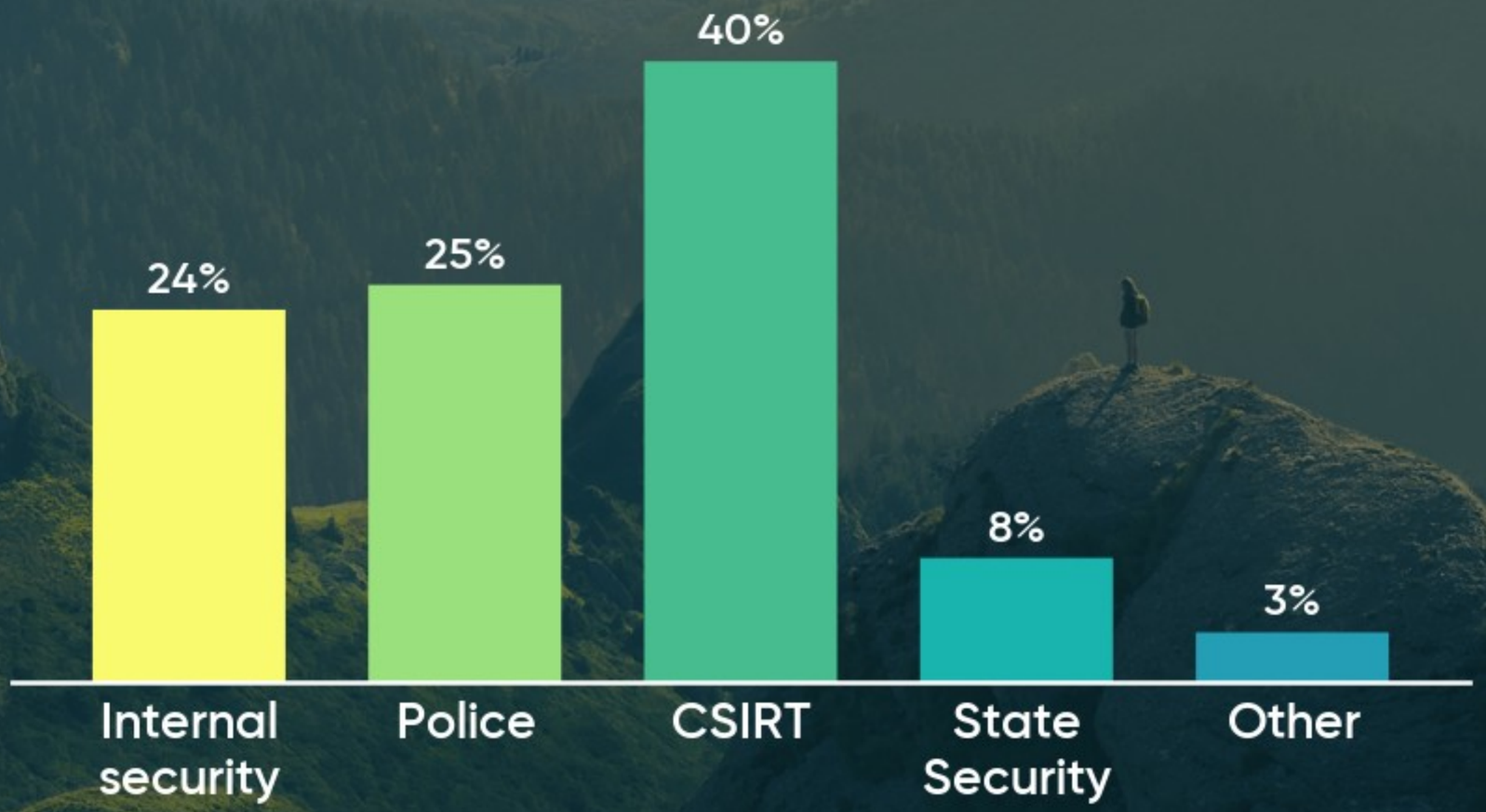
Mentimeter



38

The most efficient handling of cyber incidents, irrespective of scope and gravity, is performed by:

Mentimeter



45


Mentimeter
CRITICAL INFRASTRUCTURE PROTECTION
A MAJOR CASE FOR COOPERATION ?

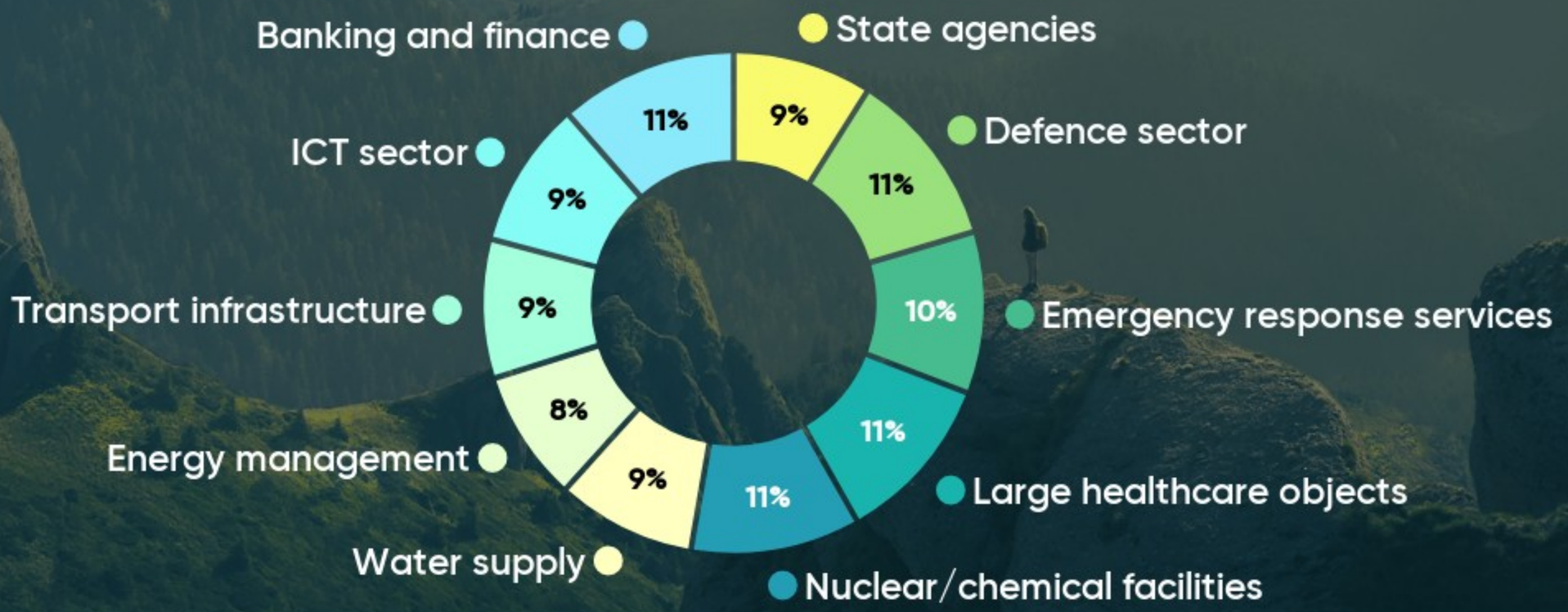
Which is the stomgest defining criterion for CII?

Mentimeter

24

Please rate these services in terms of critical value and effect on cybersecurity

Mentimeter



30

How would you rate the following statements?

Mentimeter

17


Mentimeter
WHAT COULD BE DONE TO IMPROVE COOPERATION?
PLEASE SHARE YOUR IDEAS

What could be done to improve cooperation?

Mentimeter

In order to increase efficiency and productivity need more human and financial resources.

Showing different governments how effective domestic justice is when there is multilateral cooperation.

Exchange Human Resources among the institutions involved

COMPLETE MERGE/FUSION OF THE CSIRT/LA

Harmonization of standards, establishment of cooperation networks, information sharing in relation to multi-jurisdictional attacks, collaboration between law enforcement agencies within different states

Il faut une legislation forte qui precise les roles des parties afin d'etablir la confiance et legitimer les actions qui pourrons etre posees. creer une unite de police speciale qui comprendra aisement l'interet de travailler avec le CIRTS.

Better sharing of information, talking the same language, improved frameworks for cooperation, increased trust

Secondment of personnel (for specific periods) from the national csirt to law enforcement and vice versa

political will/awarenessemphasize the importance in the National Cyber Security Strategydefine scope and responsibilitiessecondment

17

What could be done to improve cooperation?

Mentimeter

Capacity building, awareness and sharing of information among all stake holders is key

Harmonization of standards, establishment of cooperation networks, information sharing in relation to mult- jurisdictional attacks, collaboration btn law enforcement agencies within different states

Better understanding of the issues and continuous collaboration amongst member countries in the way forward in fighting this cybercrime issues.

Des approches innovantes voient le jour : elles sont basées sur un renforcement de la capacité de défense et le développement de schémas de coopération entre les différents acteurs impliqués.

Share information, more practices on using informal channels but within the legal boarders or frameworks. Establishing a good relationship to have better outcomes. Relatiinship first, outcome second.

Clear roles and responsibilities defined in a Standard Operating Procedure

La mise en place d'agents de liaison est un levier majeur. Having Law Enforcements detached agents in CSIRT.

Having relationship with most all law enforcement agencies, organisations,individual and nationa & Internation will ease to sharing information to solve the issues.

17

What are your main takeaways from this Workshop?

Mentimeter

A clear outline of ways to foster great and more integrated coordination between Law Enforcement and National CSIRT Agencies

Atelier tres interessant, peut etre qu'il faudra integrer des simulation d'attaques pour des exercices pratiques a temps reel. Merci pour le partage d'experience on a beaucoup appris

La coopération entre les différents acteurs impliqués sont encore à developper. Il ne faut pas s'arrêter dans notre lancée et cette atelier étaient très enrichissant

A clear outline of ways to foster great

The important of establishing a strong effective network to share information between agenices either domestic agencies and international agemcies.

Excellent workshop and panel has been the best!

The importance of public and private partnership and also international cooperation with dealing in incident responses at a national and international level

We have to contribute to built up/reinforce the bridges/channels of communications among the institutions involved

8

Did we miss anything important? Please tell us

Mentimeter

Pas exeactement, les cas souleves etaient tres interessants merci pour le partage d'experience

The role of artificial intelligence

We does not discuss about the private sector (critical infrastructure) obligation/necessity to report cyberattacks or cybersecurity incidents

It looks solid for me if these recommendations willbe implemented

4

Mentimeter

Octopus Conference 2019

Cooperation against Cybercrime

20-22 November 2019

Palais de l'Europe, Council of Europe, Strasbourg, France

THANK YOU FOR YOUR PARTICIPATION!

8 11 5