The organization should leverage a continuous CTI lifecycle that consistently maintains his awareness positioning

- Share actionable intelligence information with **relevant stakeholders** (internal actors, national organizations, …)

- Clearly define what organization **need to protect** and why
- Allocate necessary **budget** to execute the plan

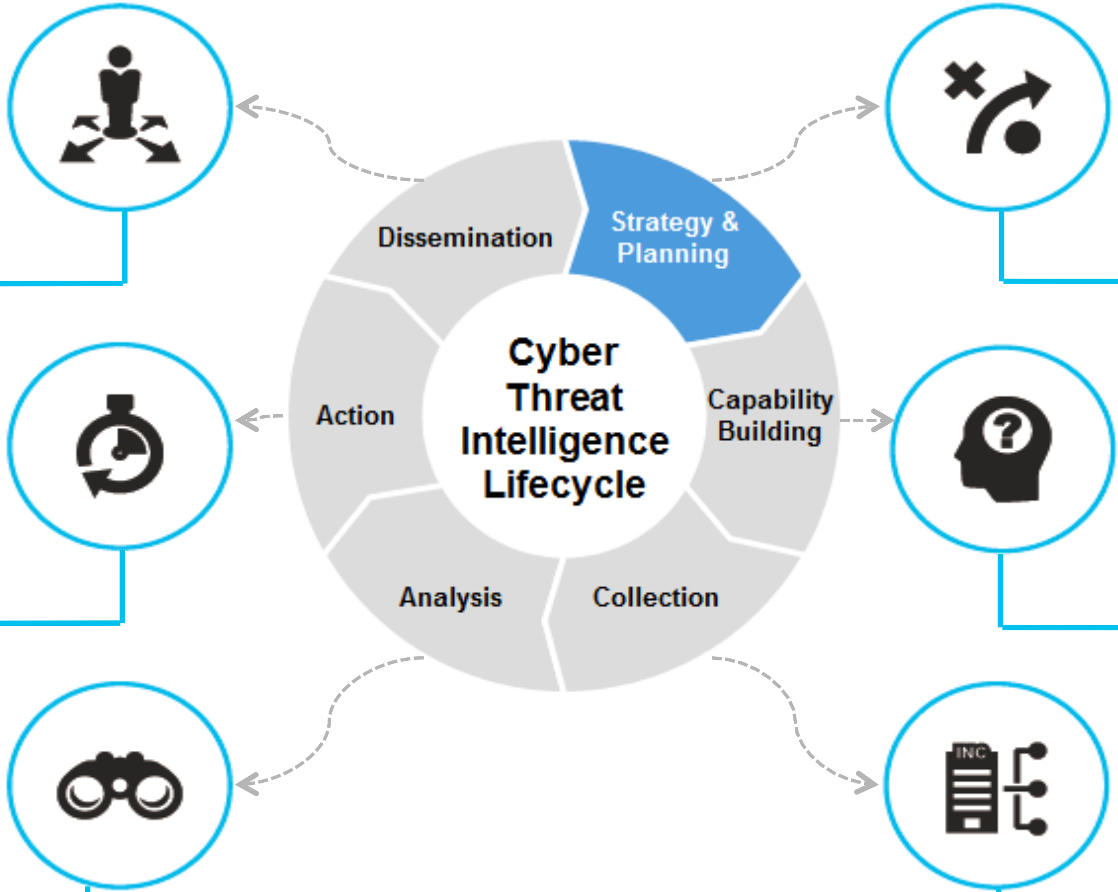
- Dedicate unit (CERT and/ or SOC) take or direct **actions** to prevent a cyber attack or to disrupt an attack in progress

- Staff appropriate positions - **internal and/ or external resources -** to implement the CTI program
- Special **training** for analysts

- Transform collected data into **actionable intelligence** in the context of the specific entity

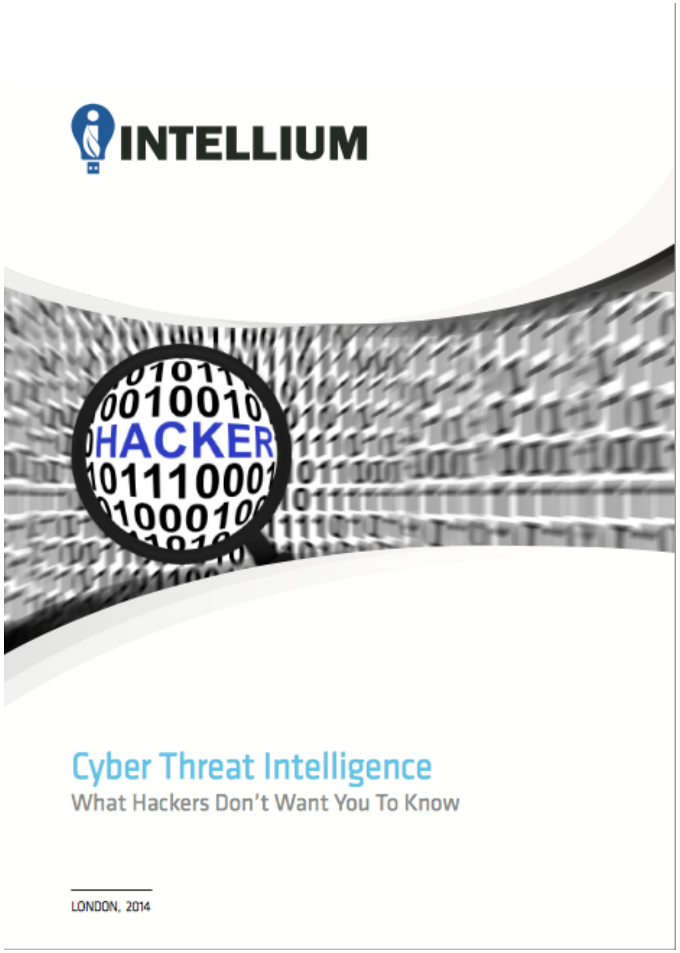
- Collect relevant threat information from **internal and external sources** (employees, OSINT, fee-based services, …)

Threat Intelligence Lifecycle



Intellium produced a viewpoint on Cyber Threat Intelligence, available on our website

Cyber Threat Intelligence report



INTELLIUM

Cyber Threat Intelligence

What Hackers Don't Want You To Know

LONDON, 2014

Topics covered
▪ What is Cyber Threat Intelligence ▪ The attacker's inherent advantage ▪ Building a CTI capability ▪ Why CTI programs fails ▪ Conclusions

More info on

http://www.intelliumgroup.com

Session Objectives

Objectives

- Present **main topics, objectives** and **tools** for CERT cooperation and coordination

We have selected three relevant topics, related to CERT capabilities, that will be addressed during the drill

Cyber drill topics

Topics	Description	Objectives
1 Information Sharing	One of the CERT role **is to enable the communication** between members of the same and different Constituency	• **Gain information** on vulnerabilities and threat that otherwise not have access to • Through vulnerability and threat intelligence, **prevent and reduce** the occurrence / impacts of cyber incidents
2 Reporting Threats/ Vulnerabilities / Incidents	**Analysis conducted by CERT** in order to restore / sanitize the situation. This will be the starting point to report the event, including **mitigation guidance, recommendation and best practices**	• **Be alerted** to threats and potential vulnerabilities experienced by others, therefore be better prepared themselves • **Learn** from others and adopt best practice
2 Cooperation with LEAs	Establishment of **cooperation mechanism** to coordinate in case of cyber incidents	• **Tackle** security issues collectively so as to generate a “public good”

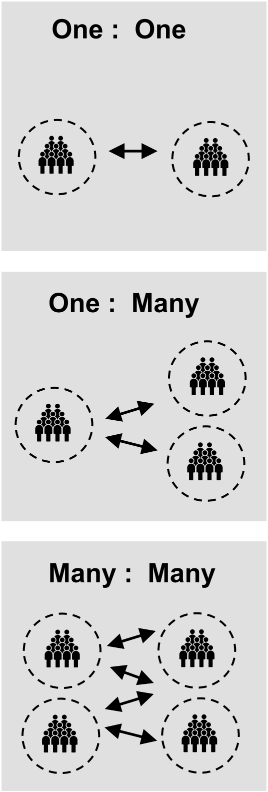
Objective of this Cyber Drill is to improve CERT capability to coordinate and communicate with relevant stakeholders in order to manage cyber incidents

One of the crucial aspects of CERT work consists of the exchange of information and communication

1

Information Sharing

Ways to share

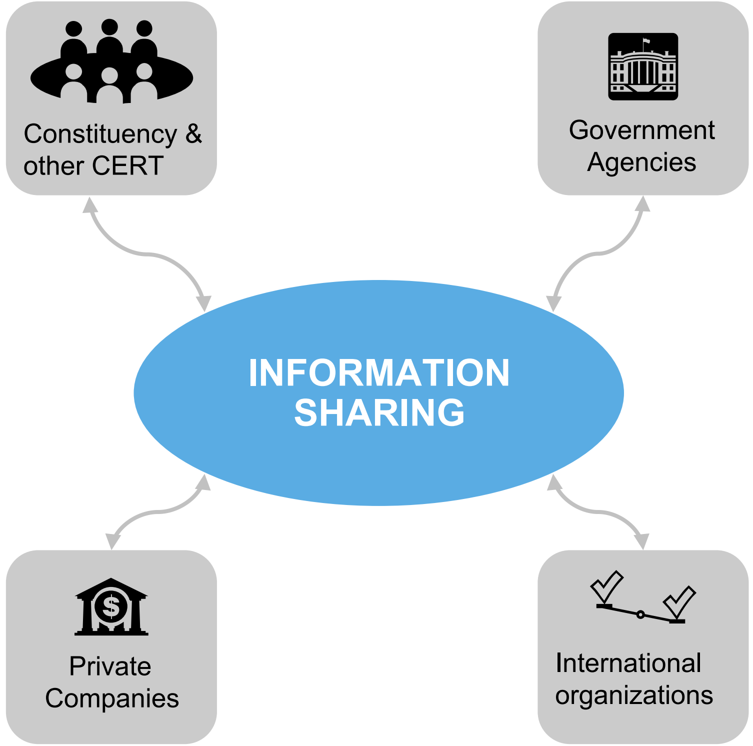


One : One

One : Many

Many : Many

Involved actors



Constituency & other CERT

Government Agencies

INFORMATION SHARING

Private Companies

International organizations

Enablers

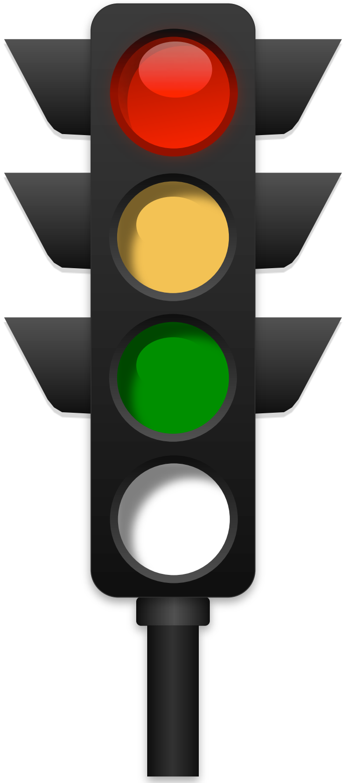
- Conferences/Seminars
- Standards/Good Practices
- Social networking tools
- Blogs
- Wikis
- Forums
- Working groups
- Professional groups
- Binding rules of behaviour:
  - – NDAs
  - – Chatham House
  - – Information sharing protocol (ex. Traffic Light Protocol – TLP)

Final goal is to derive a <u>fundamental mutual value proposition</u>: the more effectively information is shared and exchanged between interested parties, the faster cyber incidents can be mitigated and less damage occurs.

In particular, sensitive information should be classified and shared according to information sharing protocol, such as TLP

1

Traffic Light Protocol - TLP



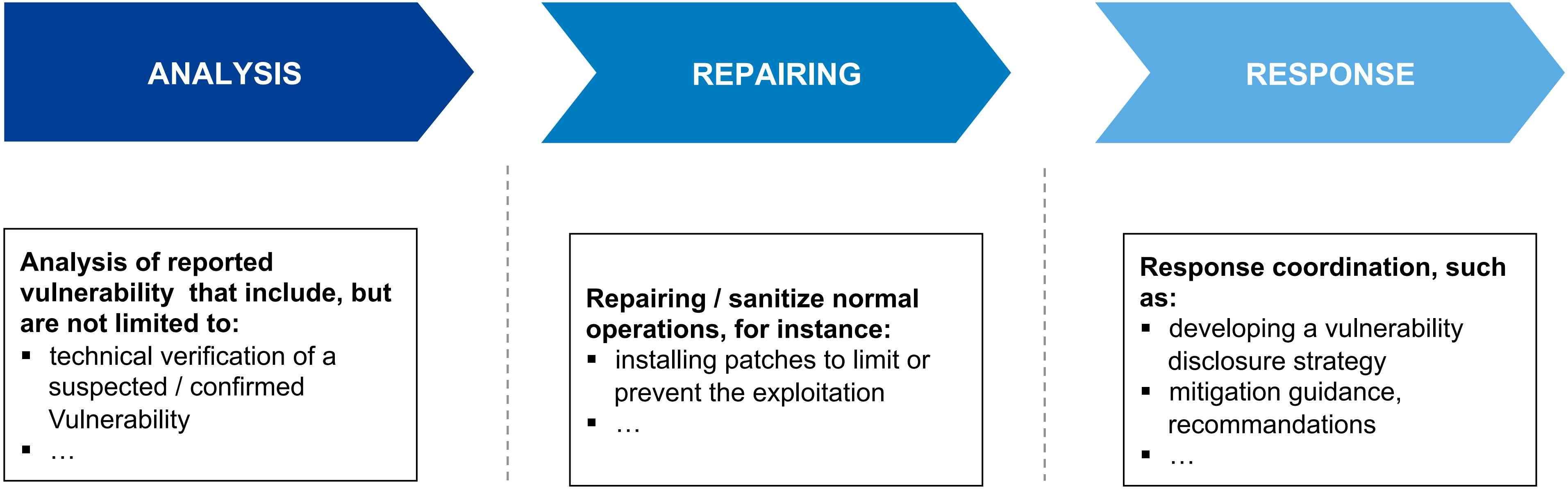
Color	Type of information	Sharing
RED	Information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Information exclusively intended for direct recipients
AMBER	Information requires support to be effectively acted upon, but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Information for an organisation, possibly limited to certain persons in the organisation
GREEN	information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Peers and partner organizations within their sector or community, but not via publicly accessible channels.
WHITE	information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	information may be distributed without restriction, subject to copyright controls.

TLP provides a simple and intuitive schema for indicating when and how sensitive cybersecurity information can be shared within the global cybersecurity community of practice.

An important role of the CERT embraces the incident handling process and related activities

2

Report Threats / Vulnerabilities / Incidents



ANALYSIS

Analysis of reported vulnerability that include, but are not limited to:

- technical verification of a suspected / confirmed Vulnerability
- …

REPAIRING

Repairing / sanitize normal operations, for instance:

- installing patches to limit or prevent the exploitation
- …

RESPONSE

Response coordination, such as:

- developing a vulnerability disclosure strategy
- mitigation guidance, recommandations
- …

The CERT will act in order to establish and maintain the communication among several actors, such as other involved CERT, vendors.
The main role of CERT is to advise in case of threats, vulnerabilities and cyber incidents

In order to create an effective cooperation among CERT and LEAs/Institutions, an adequate agreement has to be identified

3

Cooperation with LEAs/Institutions

Aspects to be addressed

- Definition of dedicated **information sharing protocols** and classification of information
- Increase the **communication**, for instance in terms of consultations, when CERT receives a request from LEAs
- **Periodic Training** activities
- …

Actors to be involved

- **Local enforcement Agencies** at national (ex. Police Forces) and international level (ex. Interpol)
- **National Institutions** with dedicated units for cybersecurity (ex. National Intelligence)
- **International Organizations** (ex. ITU-IMPACT, Africa CERT, FIRST)
- …

The combination of these two components is the key element to create the framework for cooperation mechanism

Therefore, our session is structured into four main parts, three for the exercises and one for the wrap-up

Time Schedule

#	Item	Time	Duration
1	Introduction to the exercise	14:00 – 14:10	10 minutes
2	Task 1: Information Sharing	14:10 – 14:35	25 minutes
3	Task 2: Early Warning	14:35 – 15:00	25 minutes
Coffee Break		*15:00 – 15:15*	*15 minutes*
4	Task 3: Cooperation with LEAs / Institutions	15:15 – 15:45	30 minutes
5	Exercise summary and wrap-up	15:50 – 16:00	10 minutes
		Total duration	**1 hour, 45 minutes**

A “conductor” from Intellium will coordinate the drill by providing the teams instructions. Moreover, he will be available to answer any questions that may arise and will evaluate final results by giving useful feedback to improve CERT functionalities.

As you have been informed, we are conducting a questionnaire to collect useful information for the cyber drill

Cyber drill questionnaire

https://www.surveymonkey.com/s/Intellium

INTELLIUM

Focusing on cyber security
for critical infrastructures.

Intellium LTD | Charles House, 108-110, Finchley Road - NW3 5JJ LONDON | Tel: +44 20 3290 4911 - E-mail: contact@intelliumgroup.com | Copyright © 2015