Workshop on Cooperation with Stakeholders during Cyber Crisis

Regional Forum on Cyber security for the Americas Region

Bogotà – August 4 2015

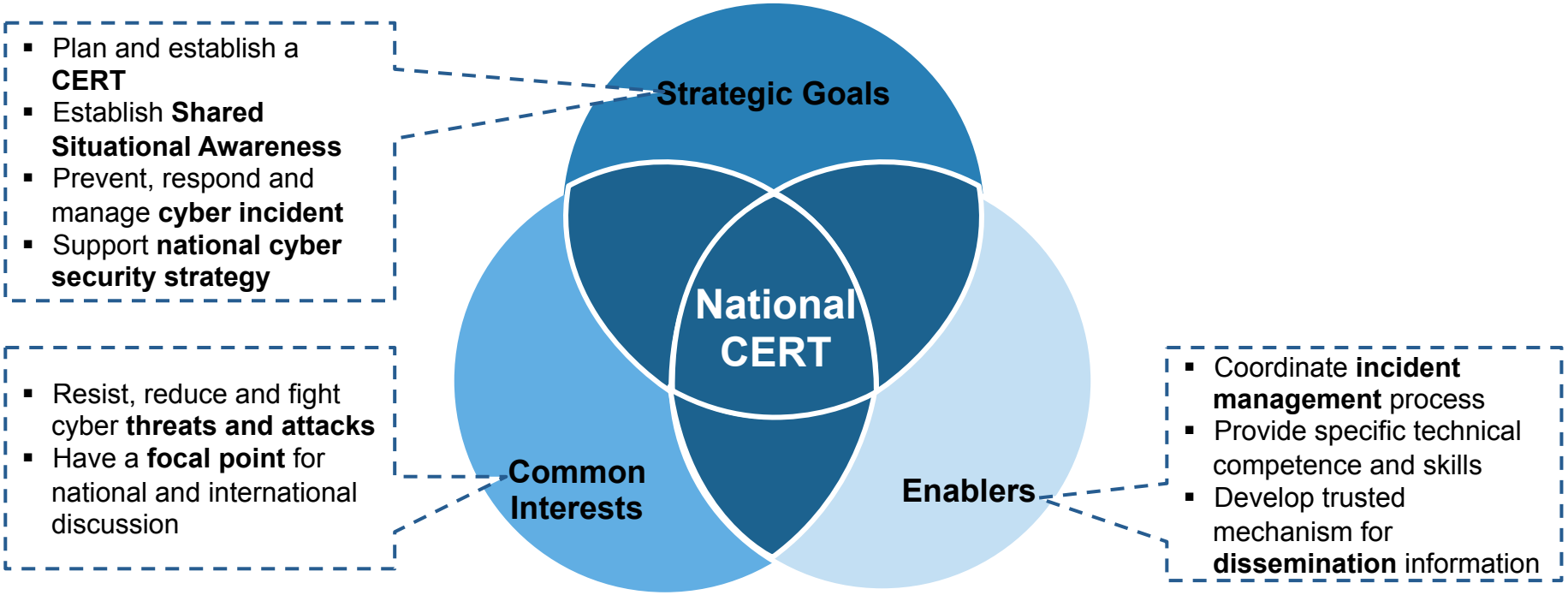
Workshop Objectives

Objectives

- **Provide an overview on typical CERT framework**
- Present communication tools and techniques to enable CERT services
- Introduce main topics of Intellium cyber drill

CERT is a core component of nation's strategy to secure critical information infrastructures vital to national security

Why build a National CERT



MISSION

- Act as a reliable and trusted, single **point of contact** for emergencies
- Facilitate **communication** among Constituency, other CERTs and experts working to solve security problems
- Maintain close ties with research activities and conduct **research** to improve the security of existing systems
- Initiate proactive measures to increase **awareness** on information security and computer security issues

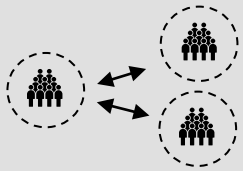
CERT framework is built on stakeholders that interact according to their specific roles and responsibilities…

CERT stakeholders' interaction

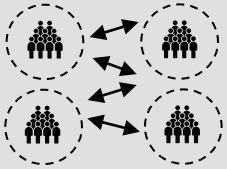
Sharing approach

One : One

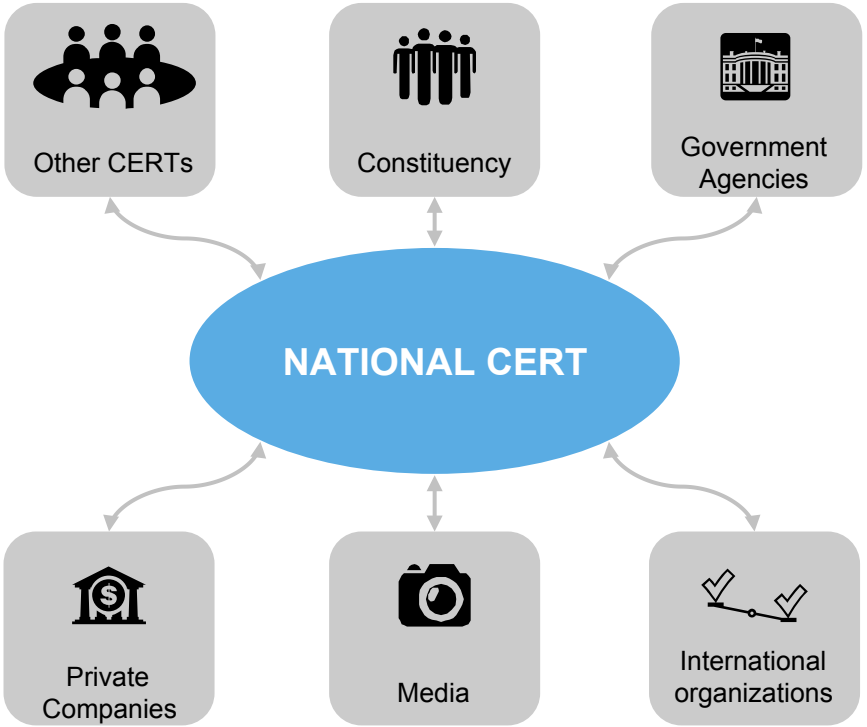
One : Many



Many : Many



Stakeholders



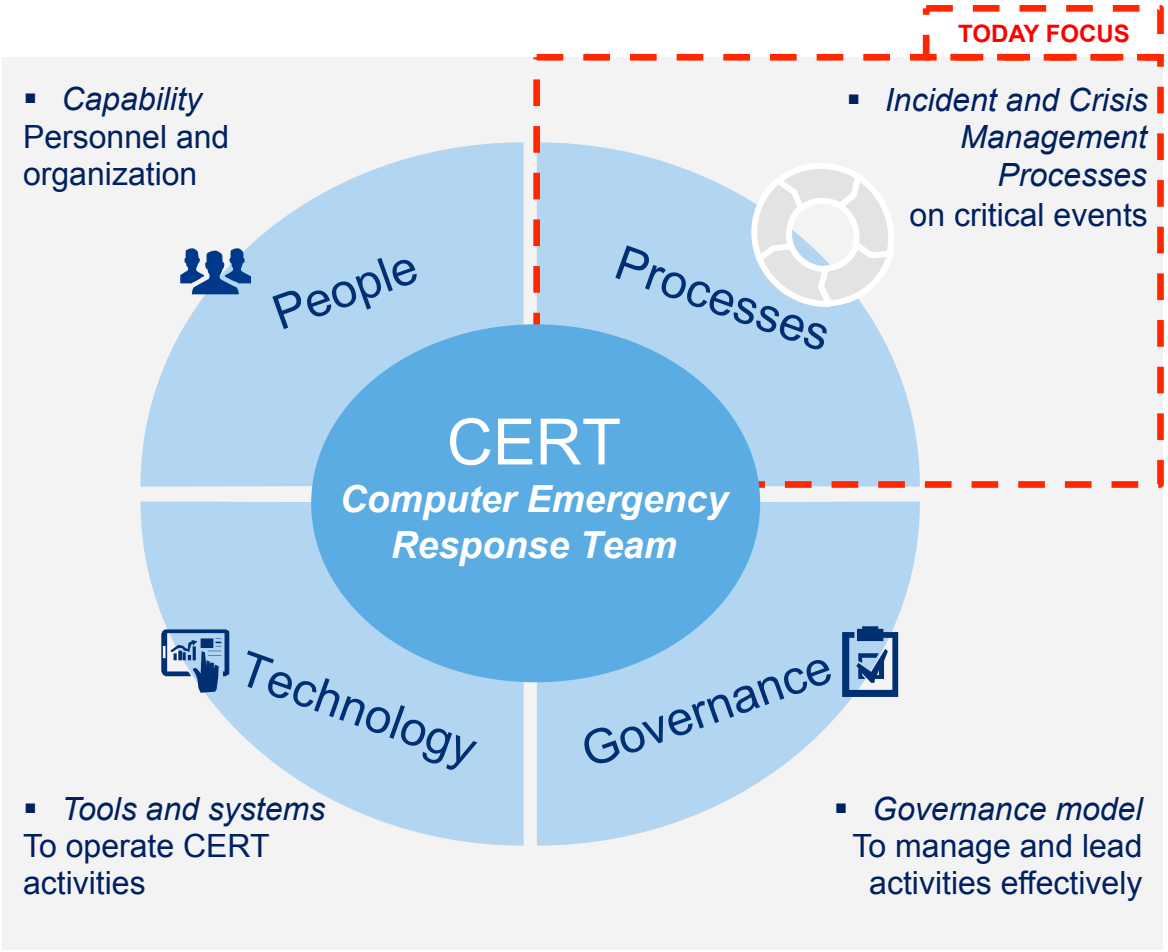
Enablers for interactions

- Conferences/Seminars
- Standards/Good Practices
- Social networking tools
- Blogs
- Wikis
- Forums
- Infrastructure tools (Email / PGP / RTIR)
- 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 fundamental mutual value proposition: the more effectively information is shared and exchanged between interested parties, the faster cyber incidents can be mitigated and less damage occurs.

…and specific components that allow to respond and manage cyber security emergencies and incidents

CERT components[1]



CERT Incident Response

- CERT allows structured **exchange of information** to prevent and respond against cyber events
- CERT is an enabler to establish **trusted relationships** with stakeholders:
  - Constituency and other CERTs
  - Government and institutional agencies / entities
  - Private companies
  - National, regional and International organizations
- CERT coordinates and fosters **communication** among several actors in case of threats, vulnerabilities and incident

[1] Source: Carnagie Mellon University, 1988

The Incident Response process requires an adequate organizational structure to provide CERT services

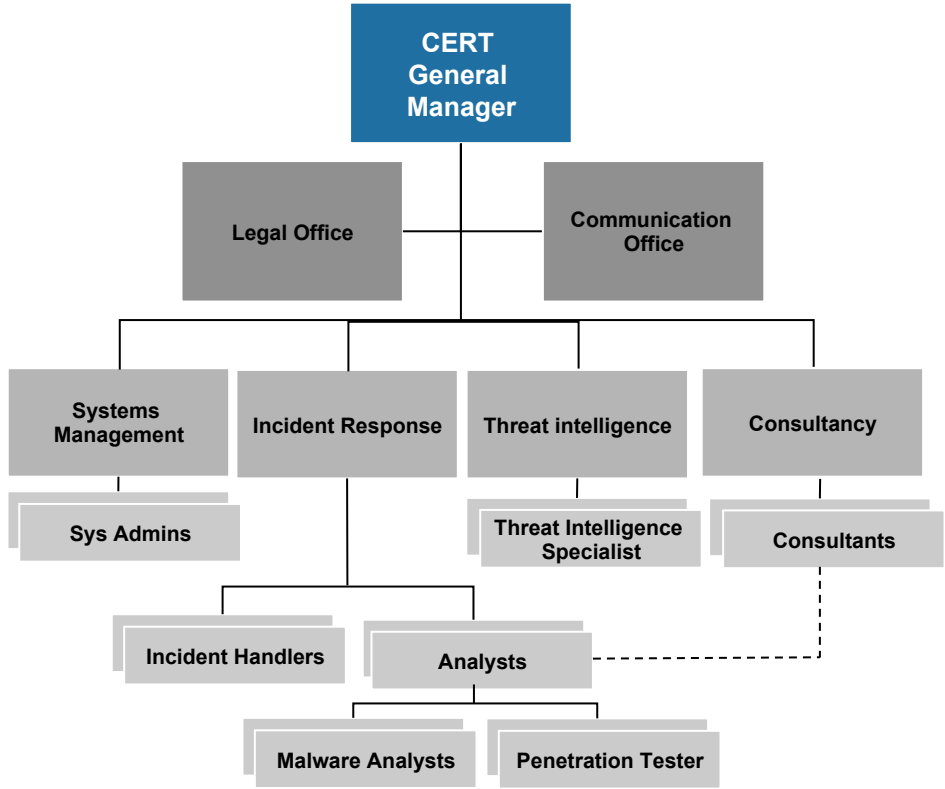
CERT Organizational Structure

ILLUSTRATIVE

CERT Staff

Main Role	Main tasks
General Manager	▪ Provide strategic direction ▪ Represent and supervise the team
Legal Officer	▪ Support the legal aspects of incidents both at national and international level
Communication Officer	▪ Manage communication with CERT Stakeholders, media, press
Sys Admins	▪ Perform systems management
Analyst	▪ Identify information and potential incident ▪ Support on tecnhical issues
Malware Analyst	▪ Analyse malicious software
Penetration Tester	▪ Perform penetration testing
Incident Handler	▪ Support and coordinate how to respond to incidents
Threat Intelligence Specialist	▪ Gather information from multiple feeds and correlate the events
Consultants	▪ Hired when needed for specific activities

Organizational Chart



The Organizational Structure has to be in line with CERT mission, activities and services provisioning

The Incident Response Process is composed by 5 phases in which involved actors have defined roles and responsibilities

Incident response process lifecycle

- **Drafting of constituency rules** on cyber security based on national and international standards, best practices, lessons learned
- **Monitoring the Constituency** by implementing a set of controls based on guidelines
- **Dissemination** activities

- **Incidents detection** through information sharing, notification from users, analysis of events from the security systems, Open & Closed Source Intelligence, ...
- Development of **indicators and specific metrics** for early incidents detection

- **Identification of measures** to restore services once the threat has been neutralized
- **Design and control of the recovery plan,** with engagement of any resource needed to restore standard levels of service
- **Enrichment of the Knowledge Base** in order to learn from the incident and disseminate the knowledge towards Constituency and stakeholders

- **Incident analysis and classification**, collection, correlation and in-depth analysis of the evidences (Data -> Information)
- **Triage and activation of response** process to incident and related impacts
- Definition of **escalation measures** to respond timely

- **Execution of response** activities
- **Communication** towards relevant stakeholders by means of resilient channels or standard channels, depending on the stakeholder
- **Coordination and cooperation** with Constituency and stakeholders

First phase consists of methodologies to establish incident response capabilities and prevent incidents

Preparedness and prevention phase

Main activities
▪ **Definition of CERT approach**: establish an incident response capability and process, so organization is ready to respond to threats and incidents ▪ **Definition of rules / guidelines / controls**: ensure that systems, networks and applications are known and prepared ▪ **Identification of information sharing tools and techniques:** engage, communicate and interact with relevant stakeholders ▪ **Planning of Cyber Security Programs**: promote cyber security awareness

This phase involves establishing and training an incident response team, acquiring the necessary tools and resources. The organization attempts to limit preventively the number of incidents by implementing controls based on risk assessments results.

In the Detection phase, information on current threats and events is gathered both proactively and reactively

Detection phase

Internal Sources

ICT components

- Network
- Data Center
- Desktop comp.
- Mobile devices
- Application Mng
- ICT Security
- DataBase
- …

Data from automated systems (ex. SIEM)

Notification from users / citizens

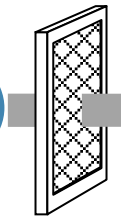
External Sources

Notification / reports from entities

Notification from CERTs and/or Intelligence

Evidences, coming from digital (ex. Log, consoles) and human sources, have to be collected according to CERT templates and formats

Internal evaluation (IR Referee)



Potential Incident

Within this phase, it is mandatory that Incident Response referee has an up-to-date expertise and knowledge on cyber threats and vulnerabilities

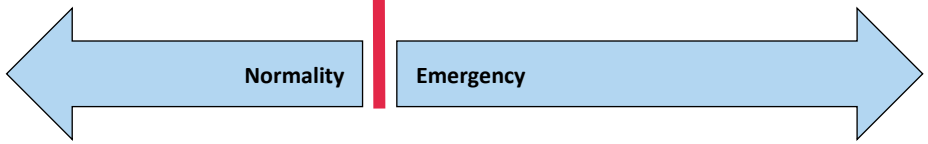
During third phase, analysis of events is conducted in order to classify potential incidents through a shared impact matrix

Analysis and triage phase

ILLUSTRATIVE

Impacts Matrix

Criteria	Level 0	Level 1	Level 2	Level 3	Level 4
People	No impacts	Limited impacts	Low – Medium impacts	Medium – high impacts (1 or 2 life at risk)	High impacts on citizens' safety
Economy	No impacts	Limited impacts, without damages on citizens	Low – Medium economic impact, but no risks on CERT operations	Relevant economic impact, risks on CERT operations	Relevant economic impact and risks at national level
CERT services	No impacts	Limited impacts on services provisioning	Low – Medium impacts on services provisioning	Relevant impacts on services provisioning	Critical services are affected; no guarantee on basic services
Reputation	No impacts	Local visibility of the incident	Low – Medium visibility of the incident	National visibility of the incident	International visibility of the incident
Social	No impacts	The incident generates uncertainty	The incident generates uncertainty, people behavior changes in short term	The incident generates uncertainty, people behavior changes in mid term	The incident generates panic among citizens



Level of emergency

Level 4 Emergency
- All CERT resources are involved to respond to incident and restore normal situation
- CERT coordinates activities on constituency / institutions / stakeholders

Level 3 Critical
- The majority of CERT resources are involved to respond to incident and restore normal situation
- CERT coordinates activities on constituency / institutions / stakeholders

Level 2 Attention
- CERT supports the entity to solve the incident
- Lessons learned process is activated

Level 1 Informative
- CERT is informed on the events, generally after the incident
- CERT can support on gathering evidences

Level 0 Not relevant
- CERT is not informed, the incident is directly managed by the involved entity

The Respond phase includes pre-defined and tested processes to mitigate and solve the incident

Respond and mitigate phase

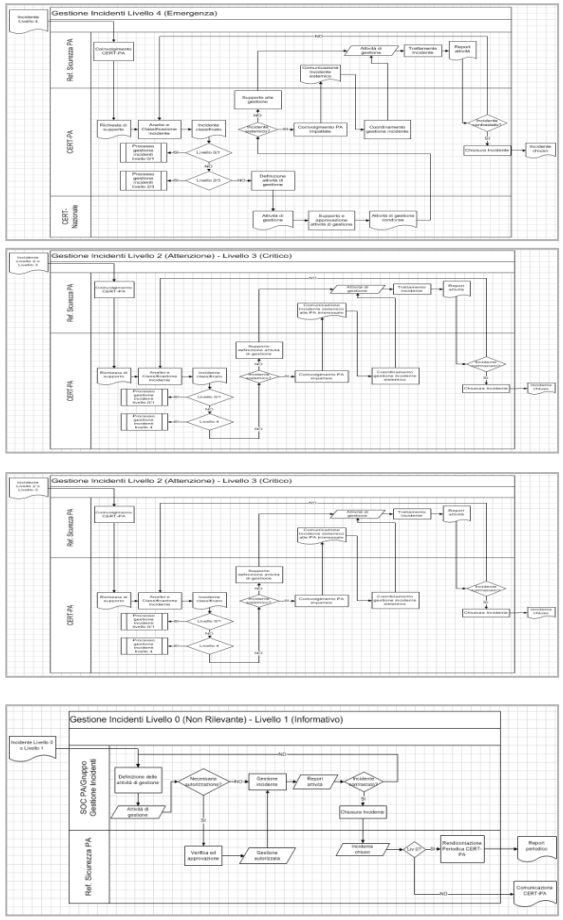
ILLUSTRATIVE

Level 4 Emergency

Level 3 Critical

Level 2 Attention

Level 1 Informative



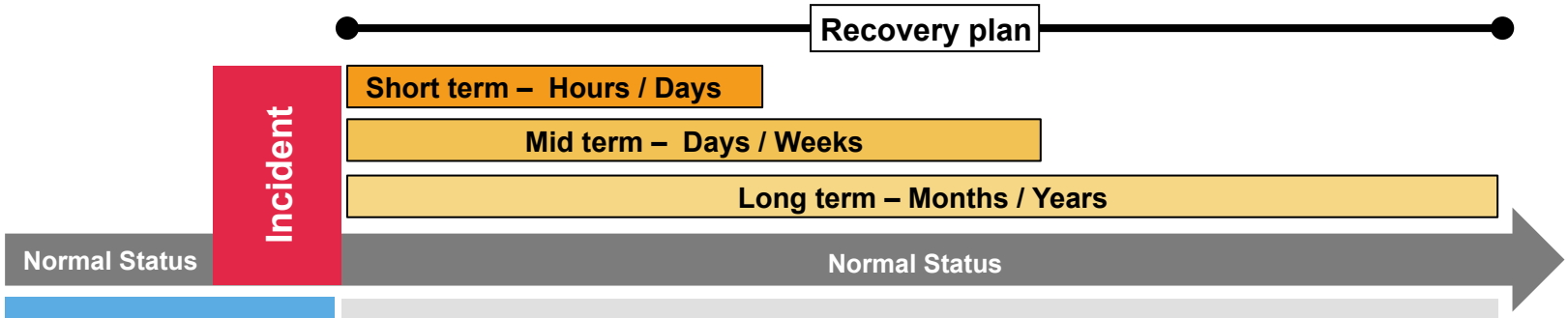
Macro – Processes Benefit

- **Definition of roles and responsibilities** of involved actors during the respond phase. It guarantees that the team works together to pursue a common goal
- **Decrease of probability of mistakes** during the critical steps of the respond phase, clearly stating the workflow and criteria to take decisions
- **Improvement of coordination** activities according to information sharing protocol

As soon as the emergency is over, the recovery of normal operations, investigation and learning phase is activated

Recovery phase

ILLUSTRATIVE



Typical model to restore normal operations

- Confirm that expected results and response activities have been successful. The situation is under control, no need for more emergency coordination
- Communicate with appropriate tools, such as reports, forensic data
- Gather of lessons learned on the incident and sharing with CERT Constituency / stakeholders
- Coordinate short / mid / long term activities and check corrective measure effectiveness through monitoring activities
- Review the performance of the whole process, in terms of efficiency and effectiveness to identify improvements (performance management)

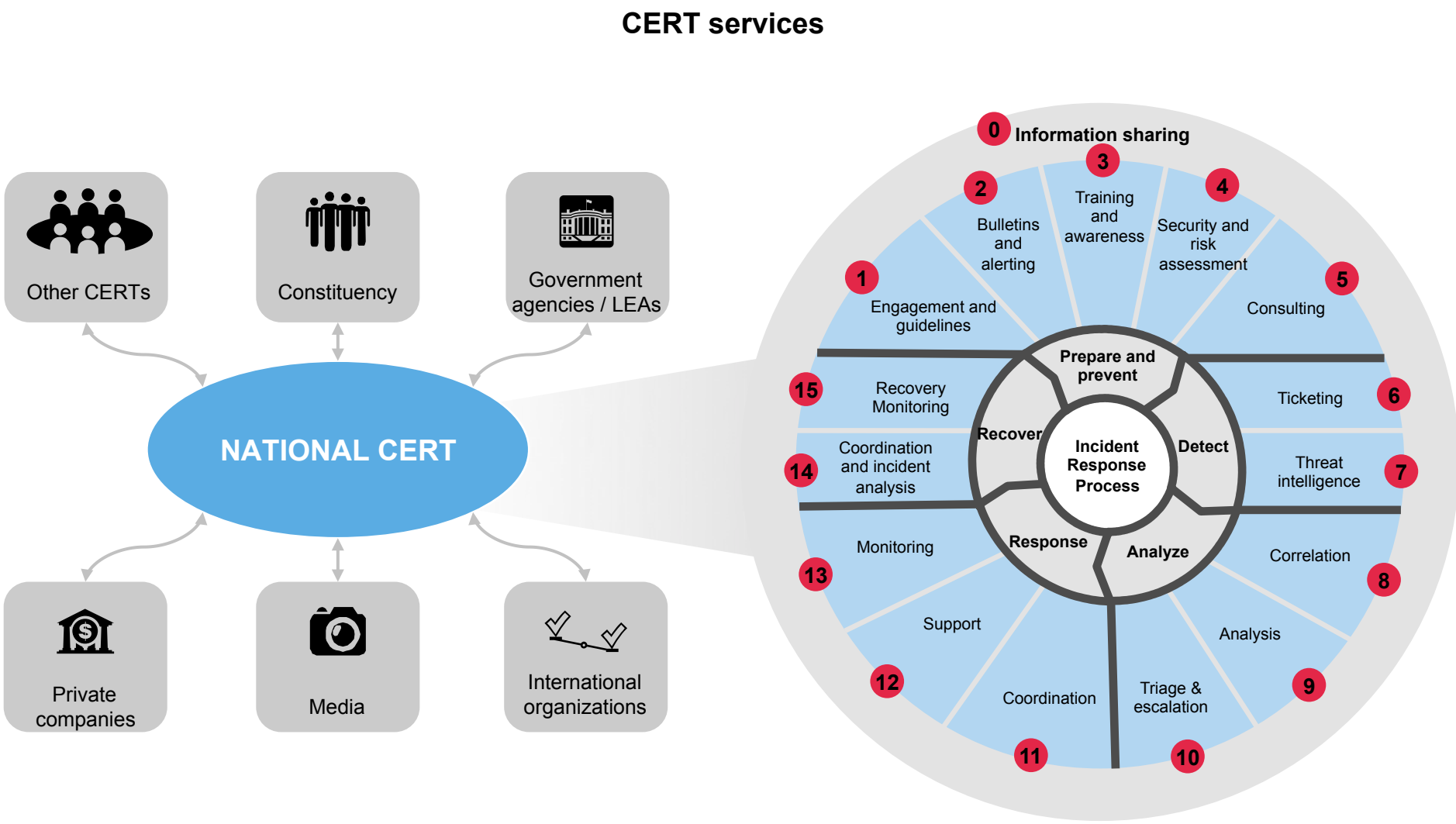
Procedures to restore normal operations rely on incident type and involved stakeholders (i.e. LEAs, institutions, private companies, …)

Workshop Objectives

Objectives

- Provide an overview on typical CERT framework
- **Present communication tools and techniques to enable CERT services**
- Introduce main topics of Intellium cyber drill

CERT provides several services to its stakeholders



Service 0 – Information sharing – CERT as data flux facilitator

Information sharing

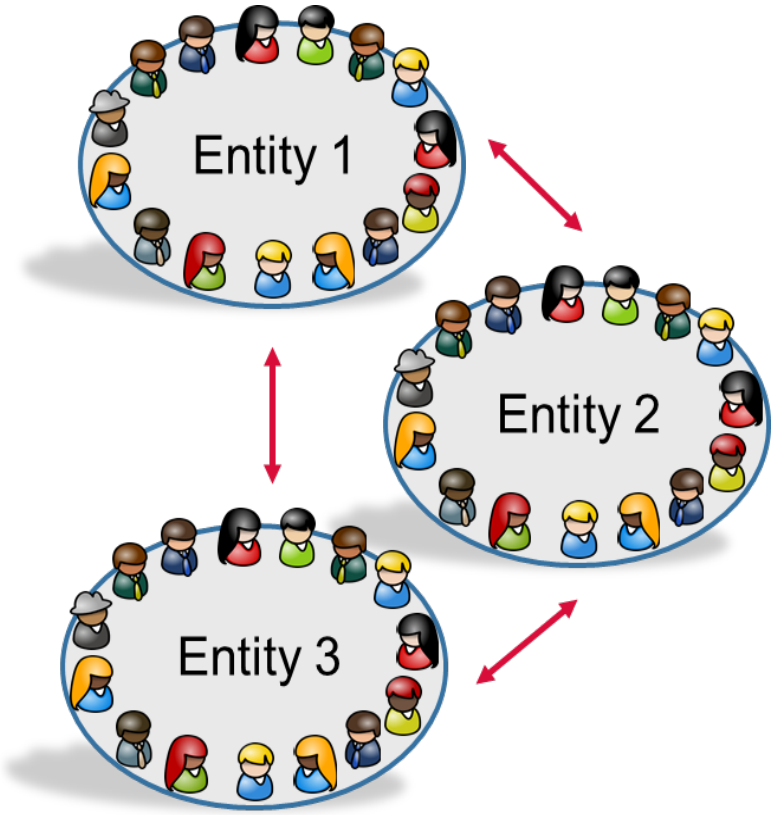
Typical TLP - all

Service Description
▪ Information sharing service is the skeleton to provide CERT's services and defines the standard approach to share information (both input and output) for each CERT stakeholder

Communication trigger	▪ None	**Communication class**	▪ Depending on the environment – must be capable to pass through white to red information
Responsibility	▪ Depending on the environment – usually CERT leader	**Actors**	▪ All the stakeholders / actors / Constituency user
Tools	▪ Sharing platform ▪ Infrastructure tools (email, PGP, RTIR, …)		

Information sharing is the transversal tool that enables communication among stakeholders…

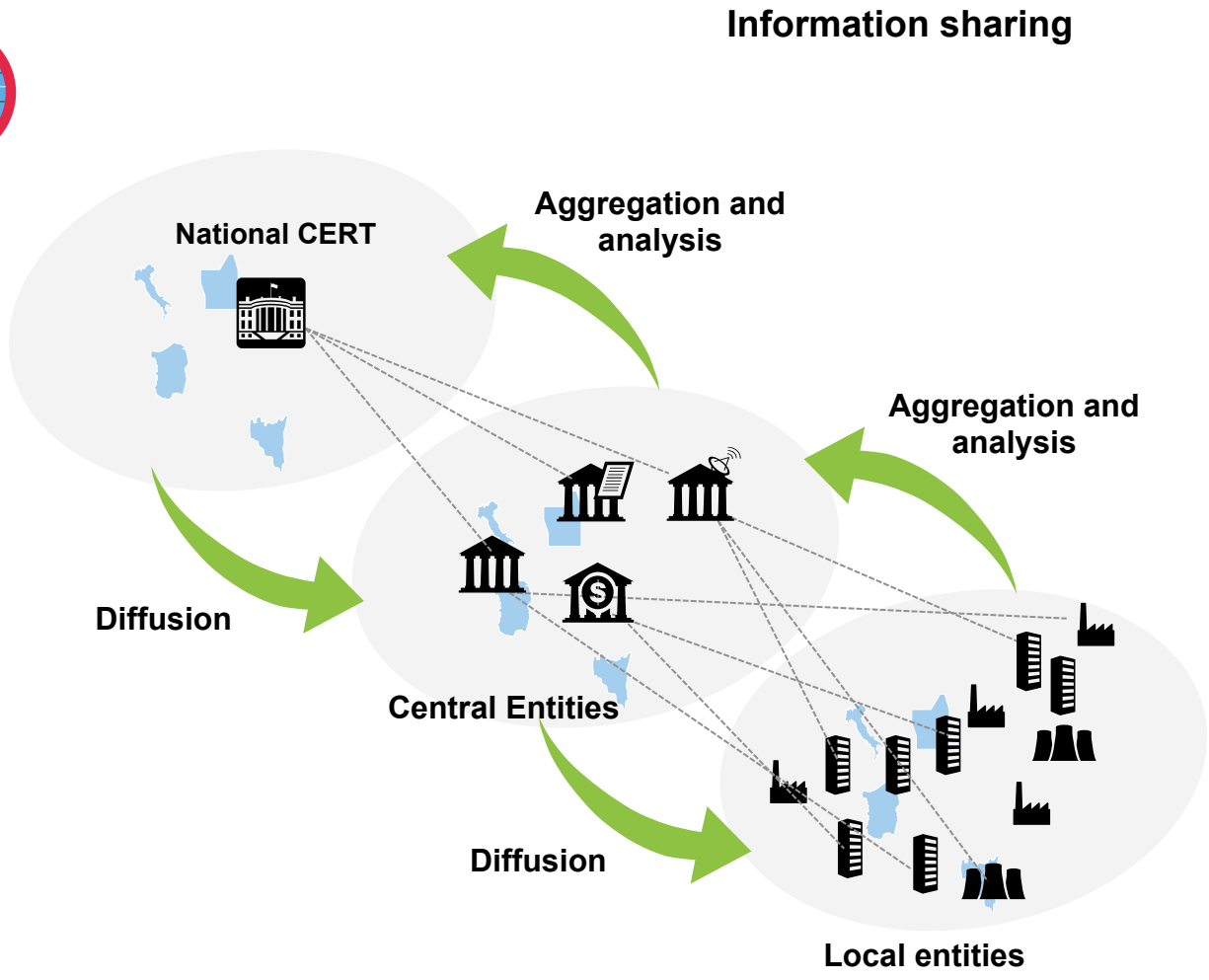
Information sharing



Information Sharing among entities

	Typical process
Gathering	▪ Information gathering through different sources (other stakeholders, Open or Closed Source Intelligence (OSINT/CSINT), whistleblowers, sensors, honeypots, other trusted sources, …
Analysis	▪ Analysis if threats, vulnerabilities, incidents, either with data coming from the start than during the investigation; technology analysis; geo-political analysis, … ▪ Trend analysis and scouting/Analysis of any possible counterpart/relevant parties
Dissemination	▪ Alarms, bulletins or indicators (KPI, IoA, IoC, …) shared to relevant (trusted) parties ▪ Public dissemination on new potential vulnerabilities; information sharing with relevant communities (i.e. FIRST, Trusted Introducer, ITU, …)

…and CERT is the focal point for incident detection, response and recovery

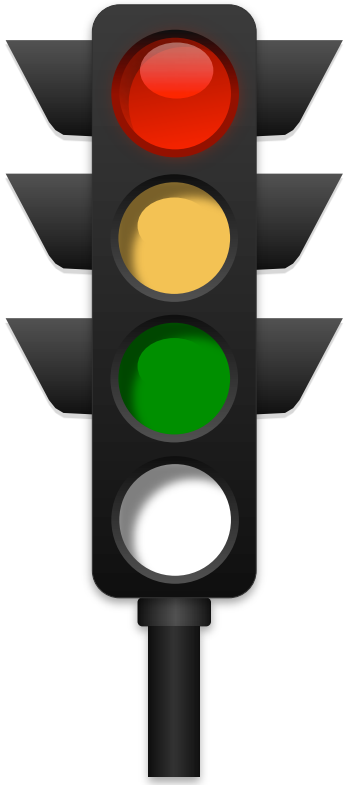


Key Principles

- Shared information is a national resource
- Shared Information is structured and flagged with a shared format
- The consumer (and not the producer) should input the information (i.e. hint of an attack)
- Shared interest communities can make information available to the whole constituency/stakeholders group
- Information should be shared in a timely manner, with coherent channels, in order to promote the Shared Situational Awareness
- Data quality should span the whole life of the information
- Information must be protected with suitable countermeasure, for every access

Any shared information has to be classified according to an information confidentiality protocol, such as TLP

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.

Service 1 – Engagement and guidelines – "nosci te ipsum" (know yourself)

Engagement and guidelines

Typical TLP AMBER

Service Description
▪ Engagement service is the tool to start the relationship with Constituency in order to provide incident response and restore services ▪ A guideline, inspired by standards and best practices, is used to clearly define CERT services and expected behavior/technologies/rules from the counter-part

Communication trigger	▪ Engagement request from CERT to constituency ▪ Request from the entity in the constituency to be relevant for the CERT	**Communication class**	▪ Availability: Standard ▪ Confidentiality: High ▪ Integrity: High ▪ Speed: Standard
Responsibility	▪ CERT General Manager	**Actors**	▪ Constituency Representative ▪ CERT Top Management
Tools	▪ Guidelines ▪ Formal Agreement		

Service 2 – Bulletins and alerts – the «ordinary marketing» of the CERT

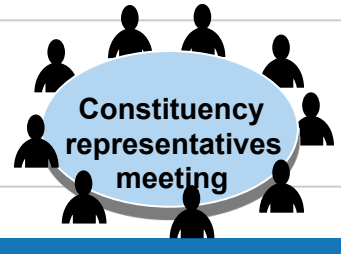
Bulletins and alerts

Typical TLP GREEN

Service Description

- Day-by-day alerts or periodic bulletins are one of the cornerstone of prevention phase: they share information gained by CERT through the communication with specific counterparts (Constituency, International Organizations, Law Enforcement Agencies, Vendors/Service Providers, …) with Constituency and other CERTs

Communication trigger	▪ New events related to vulnerabilities ▪ Periodic statistical/update communication
Communication class	▪ Availability: Standard ▪ Confidentiality: Medium ▪ Integrity: High ▪ Speed: Standard/Periodic
Responsibility	▪ CERT Communication Manager
Actors / Target Audience	▪ Constituency ▪ Other CERTs
Tools	▪ Email + PGP (signature / encryption) ▪ Web Portal



Service 3 – Training and awareness – level services capabilities within CERT Constituency

Training and awareness

Typical TLP WHITE

Service Description

- This service is mandatory to align all skills of Constituency according to CERT's needs, by balancing capabilities between the central coordinator (CERT) and the local action team (actors)
- It is important to train constituency representatives to use the CERT correctly in terms of engagement, communication, TLP, processes of Incident Management (Detection, Response, Recovery)

Communication trigger	▪ At each new engagement ▪ Periodic campaign ▪ On demand
Communication class	▪ Availability: Standard ▪ Confidentiality: Low ▪ Integrity: Medium ▪ Speed: Standard/Periodic
Responsibility	▪ CERT Communication Manager
Actors / Target Audience	▪ Constituency Security group ▪ Other Stakeholders
Tools	▪ Books / Manual / Guidelines / E-Learning courses ▪ Presentation / Training program

Service 4 – Security and risk assessment – monitor the readiness of Constituency

Security and risk assessment

Typical TLP **RED**

Service Description

- Security Assessment is useful to define security baseline of each entity of Constituency, helping CERT to understand strengths and weaknesses of the environment they are protecting
- A broader approach to the risk assessment can be used in order to link the weaknesses to the real losses suffered from the entity business/interests – allowing a more effective approach to the Incident Management

Communication trigger	▪ By request ▪ Periodic campaign
Communication class	▪ Availability: Standard ▪ Confidentiality: High ▪ Integrity: High ▪ Speed: standard/periodic
Responsibility	▪ CERT General Manager
Actors / Target Audience	▪ Constituency Representatives
Tools	▪ Risk management framework and tools ▪ Vulnerability Assessment / Management tools

Service 5 – Consulting – to help Constituency to be aligned to standards and solve issues slowing down CERT support

Consulting

Typical TLP AMBER

Service Description
▪ Consulting is the service needed from CERT to better understand and cope with weaknesses and specific characteristic of each entity of Constituency

Communication trigger	▪ By request	**Communication class**	▪ Availability: Standard ▪ Confidentiality: High ▪ Integrity: Medium / High ▪ Speed: standard/periodic
Responsibility	▪ CERT General Manager	**Actors / Target Audience**	▪ Constituency Security group ▪ Other Stakeholders
Tools	▪ Specific tools for CERT capabilities		

Service 6 – Ticketing & knowledge DB – the «timing machine» of information sharing

Ticketing and knowledge DB

Typical TLP AMBER

Service Description

- Ticketing service is the entry point of the Incident Response process and is intended to trace, both content and time, all potential events that can generate an incident, including related information either before an incident occurs and during and after response and recovery from an occurred incident.
- Those information create the knowledge DB of CERT that have to be shared within CERT Team to improve day-by-day operation

Communication trigger	▪ continuous
Communication class	▪ Availability: High ▪ Confidentiality: Medium/High ▪ Integrity: Medium/High ▪ Speed: continuous
Responsibility	▪ CERT Analysts
Actors / Target Audience	▪ CERT ▪ InfoSharing partners (case-by-case)
Tools	▪ RTIR or similar tools ▪ Knowledge DB tools (linked to the tickets)

Service 7 – Threat intelligence

Threat intelligence

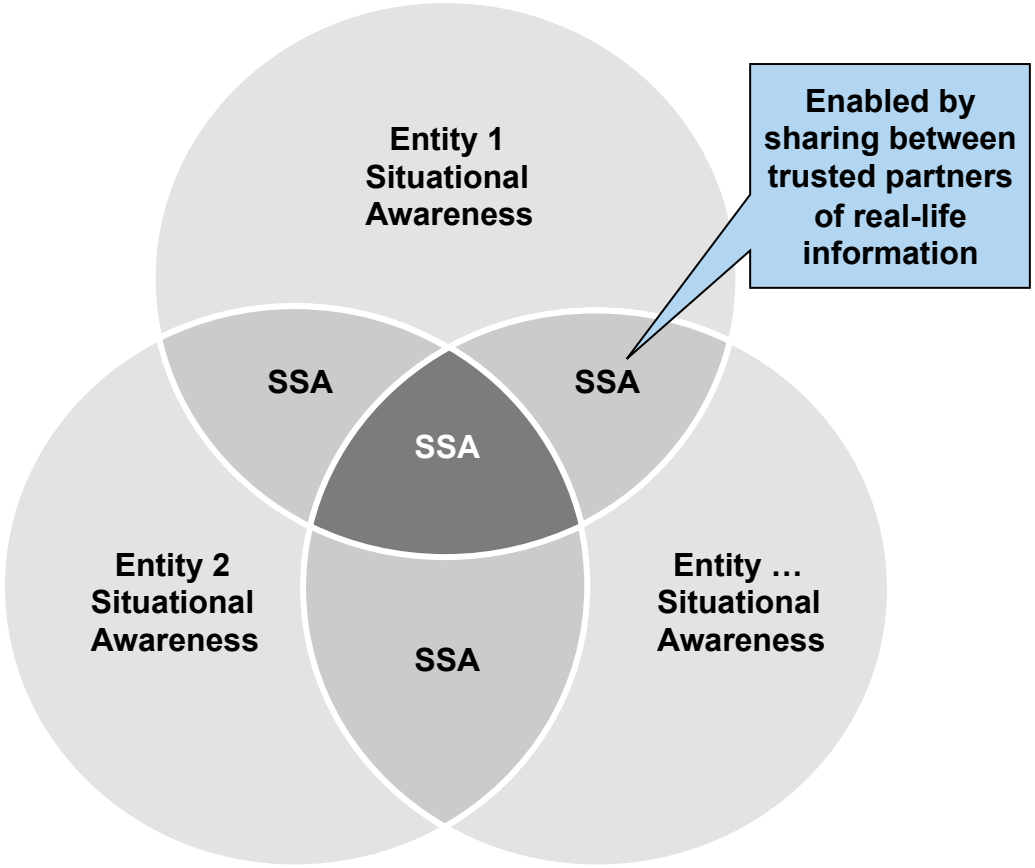
Typical TLP RED

Service Description
▪ The goal of threat intelligence is to find/detect preventive information and transform them into actionable information, aiming at collecting all relevant threats related to Constituency, technology (i.e. vulnerabilities, patches, tools, data services, …) and geo-political issues (i.e. attack sources, motivation, black market, underground information, information from other CERTs and/or Governments, …)

Communication trigger	▪ At each new engagement ▪ Periodic campaign	**Communication class**	▪ Availability: Continuous ▪ Confidentiality: Amber/Red ▪ Integrity: Low/Medium ▪ Speed: Continuous
Responsibility	▪ CERT General Manager supported by Threat Intelligence Specialists	**Actors / Target Audience**	▪ CERT Intelligence Analyst
Tools	▪ Intelligence Sources (structured/unstructured) ▪ OSINT/CSINT and Knowledge DB		

The convergence of information sharing and threat intelligence brings to the Shared Situational Awareness

Shared situational awareness



SSA Key Considerations

- The Situational Awareness (SA) gives **awareness of the surrounding actions/information to the entity**, helping to understand how information, events and impacts are evolving in the future
- Shared SA gives **the ability** to every trusted partner **to have a thoughtful vision of the threats,** to prevent and respond to incidents timely and efficiently
- SSA is directly linked to the Threat Intelligence capability: having accurate information on Constituency and their «surroundings» (at large) gives the **ability to evaluate the risk** that a specific event can trigger an incident

The rise of major adversaries is the most relevant trend in 2014, targeting governments and critical services

Major trends of 2014

And relevant changes in threat scenario

Government Top Target

Government is the most direct attacked sector of 2014. This does not exclude collateral damage (private sector). Attacks to private companies related to political tensions are on the rise (i.e. Sony Attack)

Banks still a relevant target

Financial Trojans grew in both complexity and penetration. Two major banking botnets – Gameover Zeus (GOZ) and Shylock targetted two-factor authentication and online banking security.

China and Russia

China-based adversaries continued to be the most prolific in the targeted intrusion space, but public reporting on a number of actors linked to Iran and Russia show the breadth of the threat from targeted intrusion operators.

High Profile events

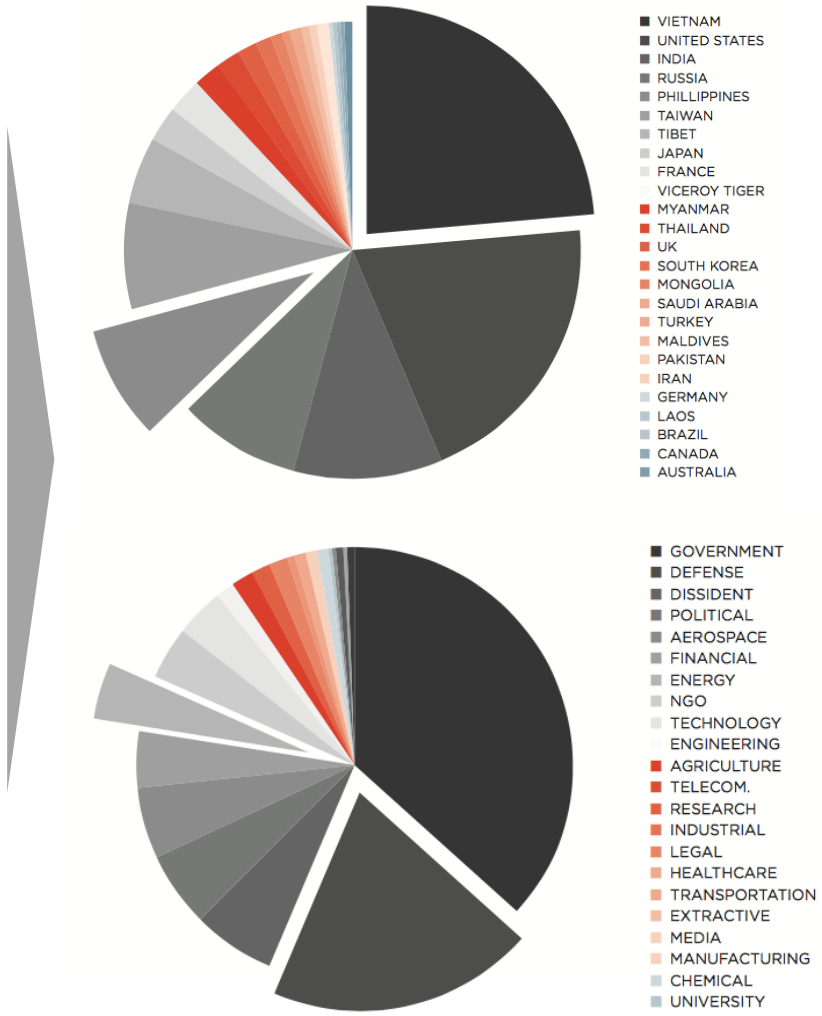
High-profile events continued to drive a significant number of targeted intrusion campaigns. In 2014, unpredictable events such as the Malaysia Airlines incidents and increased unrest in Ukraine drove campaigns more than planned events such as the World Cup or the G20 Summit.

Emerging Actors

In 2014 new actors emerged in the Adversary scenario: North Korea, Iran, India.

Target countries and sectors of 2014

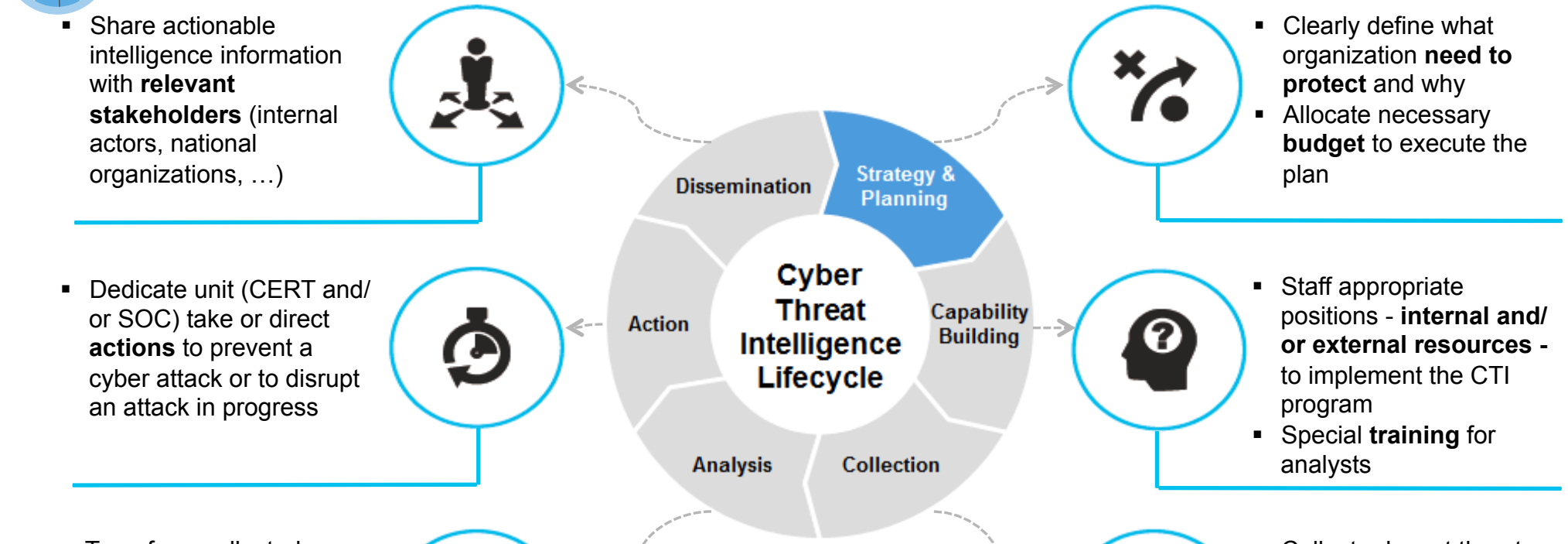
by state-sponsored adversaries



Source: Crowdstrike Global Threat Report 2014; Intellium Analysis

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

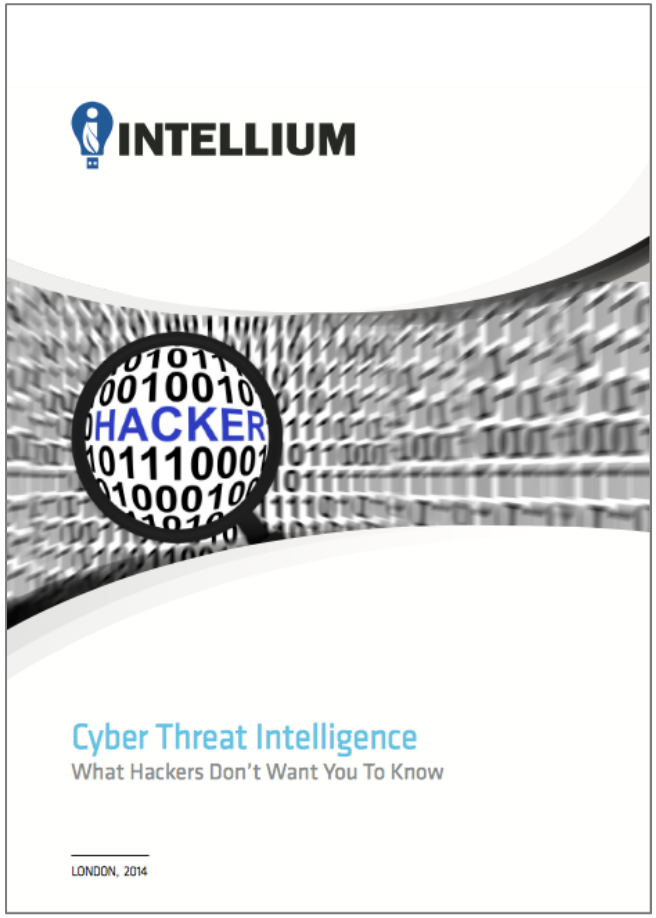
Cyber threat intelligence lifecycle



- 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, …)

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

Cyber threat intelligence report



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

More information are available on:
www.intelliumgroup.com

Service 8 – Correlation – how to link data and information

Correlation

Typical TLP RED

Service Description
▪ Correlation service will get information from «Detect» phase in order to evaluate real impacts and outcomes of each event, trying to give an overall vision on what is happening to Constituency ▪ Main goal is to find correlation schemas on different tickets, indicating some events that have a transversal impact

Communication trigger	▪ Tickets	**Communication class**	▪ Availability: Medium/High ▪ Confidentiality: High ▪ Integrity: High ▪ Speed: Fast
Responsibility	▪ CERT General Manager	**Actors / Target Audience**	▪ CERT Analysts
Tools	▪ SIEM / Ticketing / Knowledge DB ▪ OSINT / CSINT / TI		

Service 9 – Analysis – what has been detected and correlated has to be analyzed in the Constituency context

Analysis

Typical TLP RED

Service Description
▪ Event, Information, Signal Analysis are the main components of this service. The goal is to evaluate in the specific context of the Constituency. If the analyzed ticket is an incident, it requires further investigations on causes, behavior, time of diffusion, related parties and (potential or real) impact

Communication trigger	▪ Tickets	**Communication class**	▪ Availability: Medium/High ▪ Confidentiality: High ▪ Integrity: High ▪ Speed: Fast
Responsibility	▪ CERT General Manager	**Actors / Target Audience**	▪ CERT Analysts
Tools	▪ SIEM / Ticketing / Knowledge DB ▪ OSINT / CSINT / TI		

Service 10 – Triage & escalation - choose the correct level of emergency and act

Triage & escalation

Typical TLP RED

Service Description

- During this phase, CERT defines officially if an event has to be considered an incident and, if so, what are expected impacts and relevant parties to be alerted and supported
- This service defines the level of each incident

Communication trigger	▪ Incident Tickets
Communication class	▪ Availability: High ▪ Confidentiality: Typically High ▪ Integrity: High ▪ Speed: Fast
Responsibility	▪ CERT General Manager
Actors / Target Audience	▪ Constituency Security groups ▪ Other Stakeholders
Tools	▪ Information gathered from the other services/stakeholders

Service 11 – Response coordination – when trust increases speed and effectiveness in the response

Response coordination

Typical TLP RED

Service Description
▪ This service aims at coordinating each stakeholder involved in the incident, directly impacted or be able to help in the response (i.e. ISP)

Communication trigger	▪ Incident (level 2,3,4)	**Communication class**	▪ Availability: High ▪ Confidentiality: High ▪ Integrity: High ▪ Speed: Fast
Responsibility	▪ Incident Manager	**Actors / Target Audience**	▪ Constituency Security groups ▪ Other Stakeholders
Tools	▪ Telephone / email / PGP / Video Conferencing / by-person meetings		

Service 12 – Support to incident response – share knowledge and resources with Constituency and stakeholders

Support to incident response

Typical TLP RED

Service Description

- CERT will support all stakeholders and Constituency in order to solve the emergency in the shortest time, giving the availability of procedures, knowledgeable people, technical resources and connections to other stakeholders (i.e. international relations, political support, …)
- During this phase it is paramount to balance practical activities with ticketing and timing of the actions, in order to comply with service 11 and, if incurring in legal actions, being prepared to demonstrate the flow of activities

Communication trigger	▪ Incident (level 2,3,4)	**Communication class**	▪ Availability: High ▪ Confidentiality: High ▪ Integrity: Medium ▪ Speed: Fast
Responsibility	▪ CERT General Manager	**Actors / Target Audience**	▪ CERT Communication Manager ▪ Constituency Security group ▪ Other Stakeholders
Tools	▪ CERT knowledge and relations ▪ Media & Communication tools		

Service 13 – Response monitoring – a third party eye on what is happening during incident response

Response monitoring

Typical TLP RED

Service Description

- This service enables Performance Management control of the Incident Response process, paying attention as a third party to the actions suggested by CERT and implemented by Constituency/Stakeholder

Communication trigger	▪ Incident (level 2,3,4) ▪ Coordination (11) and Support (12) Services
Communication class	▪ Availability: Standard ▪ Confidentiality: High ▪ Integrity: High ▪ Speed: standard/periodic
Responsibility	▪ CERT General Manager
Actors / Target Audience	▪ CERT Team ▪ Constituency Security group ▪ Other Stakeholders
Tools	▪ Incident Management workflow diagrams and monitoring facilities

Service 14 – Recovery coordination and post-incident analysis – back to ordinary status

Coordination and incident analysis

Typical TLP AMBER

Service Description

- When an incident is declared closed by CERT Leader and Heads of the Constituency, the activities will move on the recovering of the service level as before the incident occurred
- CERT coordinates different actions to be implemented by Constituency and other interested stakeholders
- Information that remains and that has been gathered during previous phases have to be analyzed with relevant stakeholders in order to understands weaknesses, mistakes and improvement areas: this process has to be structured in the Knowledge DB in order to be used in the future (*Lessons Learned*)

Communication trigger	▪ Closing incident declaration	**Communication class**	▪ Availability: Standard ▪ Confidentiality: Medium ▪ Integrity: High ▪ Speed: standard/periodic
Responsibility	▪ Incident Manager	**Actors / Target Audience**	▪ CERT Team ▪ Constituency Security group ▪ Other Stakeholders
Tools	▪ Knowledge DB ▪ Ticketing System		

Service 15 – Monitoring of recovery actions – has the recover completed correctly?

Recovery monitoring

Typical TLP AMBER

Service Description

- This service, parallel to Recovery Coordination and Incident Analysis, gives CERT the status update on the recovering activities of each actor involved, to:
  - Keep update Constituency representatives and Top Management
  - Keep the pressure on Constituency / stakeholders involved in the recovery activities
  - Support legal activities on the long term

Communication trigger	▪ Closing incident declaration
Communication class	▪ Availability: Standard ▪ Confidentiality: Medium ▪ Integrity: Medium ▪ Speed: Standard
Responsibility	▪ CERT General Manager
Actors / Target Audience	▪ Constituency Representatives ▪ Other Stakeholders Representatives
Tools	▪ Communication tools ▪ Ticketing system ▪ Knowledge DB

Workshop Objectives

Objectives

- Provide an overview on typical CERT framework
- Present communication tools and techniques to enable CERT services
- **Introduce main topics of Intellium cyber drill**

We have selected three relevant topics that will be addressed as examples of approach for stakeholder communication

Relevant topics

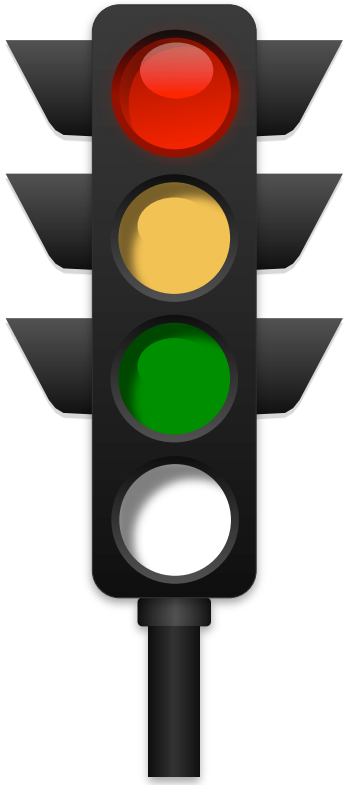
Topic	Description	Objectives
1 **Information Sharing**	One of CERT role **is to enable the communication** between members of the same and different Constituency	• **Gain information** on vulnerabilities and threat that otherwise not have access to • Through vulnerability and threat intelligence, **prevent and reduce** the occurrence / impacts of cyber incidents
2 **Incident Handling Reporting**	**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
3 **Communication and Cooperation**	Establishment of **cooperation mechanism** to coordinate in case of cyber incidents with stakeholders	• **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

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.

One of the most relevant component of the incident handling process is the reporting activities of security events

2

Incident handling reporting

ANALYSIS → **RESPONSE** → **RESTORE**

Analysis of vulnerabilities that include, but are not limited to:

- technical verification of a suspected / confirmed Vulnerability
- …

Response coordination, such as:

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

Restoring / sanitize normal operations, for instance:

- installing patches to limit or prevent the exploitation
- …

The CERT will act in order to establish and maintain the communication among several actors (Costituency, other CERTs, vendors, …). The main role of CERT is to advise and report in case of threats, vulnerabilities and cyber incidents

In order to create an effective cooperation among stakeholders an adequate agreement has to be identified

3

Cooperation among CERT stakeholders

Aspects to be addressed	Actors to be involved
• Definition of dedicated **information sharing protocols** including classification of information and tools to communicate • Increase the **communication**, for instance with Law Enforcement Agencies (LEAs) • **Periodic Training** activities • …	• **Law Enforcement Agencies** at national (ex. Police Forces) and international level (ex. Interpol) • **National Institutions** and dedicated units for cybersecurity (ex. National Intelligence) • **International Organizations** (ex. ITU, FIRST) • …

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

INTELLIUM

Intellium Italia Srl| via Sommarive, 18 - 38123 Trento | E-mail: contact@intelliumgroup.com |