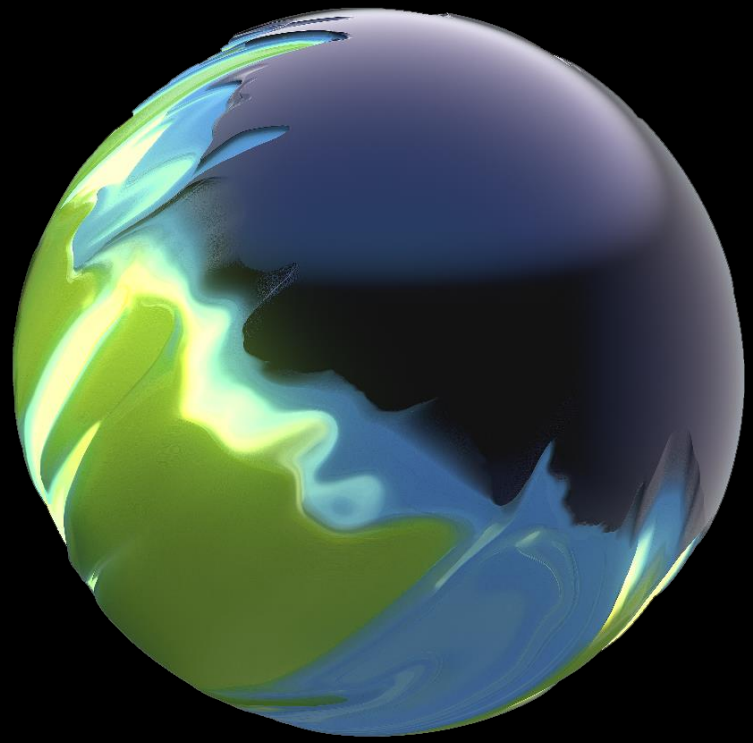
Deloitte.



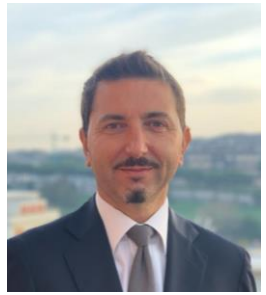
CERT – Key Team for Enhancing Resilience

Meeting with Università Roma2 - Tor Vergata

December 2021

Cyber

Il Team



Lorenzo Russo

Partner | Deloitte Risk Advisory

lorusso@deloitte.it

Bio

Partner di Deloitte Risk Advisory con esperienza di oltre 20 anni in ambito Cyber Security Strategy, Governance & Risk Management, maturata in progetti con governi, organizzazioni internazionali e aziende Fortune 500. Co-autore del Framework Nazionale per la Cyber Security e del NATO Next Generation CERTs Handbook e Advisor delle UN per temi di National Cyber Strategy e Capacity Building

Francesco Tozzi

Director| Deloitte Risk Advisory

ftozzi@deloitte.it

Bio

Francesco has 10+ years of experience in Cyber Security for IT and ICS fields. Specialized in Governance, Cyber Security strategies and Cyber Security risk management.

His main experiences come from the definition of strategies for the management of Cyber Security and from the design of operational models of multinationals in different sectors, such as Oil & Gas, Manufacturing, Food & Beverage.

Agenda

- CERT OVERVIEW
- CERT PROCESSES
- CERT CAPABILITIES
- CERT ENABLERS
- CERT IMPLEMENTATION PROJECT

Deloitte Cyber Presentation

Deloitte presentation

Our service areas

Deloitte's people are dedicated to providing confidence in markets and finding innovative solutions that contribute to a stronger economy and healthier society. Enabled by a global network of strong businesses and valued services—built on decades of insight and experience—they solve tough problems, build trust and help clients achieve transformative results.

Consulting

Human Capital Strategy and Operations Technology

Audit & Assurance

Audit Assurance

Financial Advisory

Financial Crisis Mergers and Acquisitions

Tax & Legal

Global Business Tax Services Global Employer Services Indirect Tax Legal

Risk Advisory

Strategic and Reputation Risk Regulatory Risk Financial Risk Operational Risk Cyber Risk

Note: *The above list of services is a representative sampling of Deloitte's cross-business capabilities. Deloitte offers many services, not all of which are available from every Deloitte member firm and not all of which are permissible for audit clients under various professional and regulatory standards*

Deloitte Cyber Risk Services – Our presence in Italy

Deloitte Risk Advisory includes Cyber Security services through a local footprint of over 300 Cyber Security professionals in 5 cities

300 +

Cyber risk practitioners serving Italian clients

Our consultants hold **key professional and industry certifications**, such as CISSP, CISM, ISO 27001, COBIT, ITIL

Our heritage, combined with **deep technology expertise and broad industry experience**, means we're prepared for every scenario across the cyber risk landscape

Collaborating with leading government agencies and industry associations on Cyber Security standards, advanced threat solutions, and cyber resilience practices

Deloitte Presence in Italy

Deloitte Cyber Risk Services – Our Global Presence

Deloitte currently serves 70% of the Fortune 500 companies through a global footprint of over 8,600 Cyber Security professionals in 46 countries

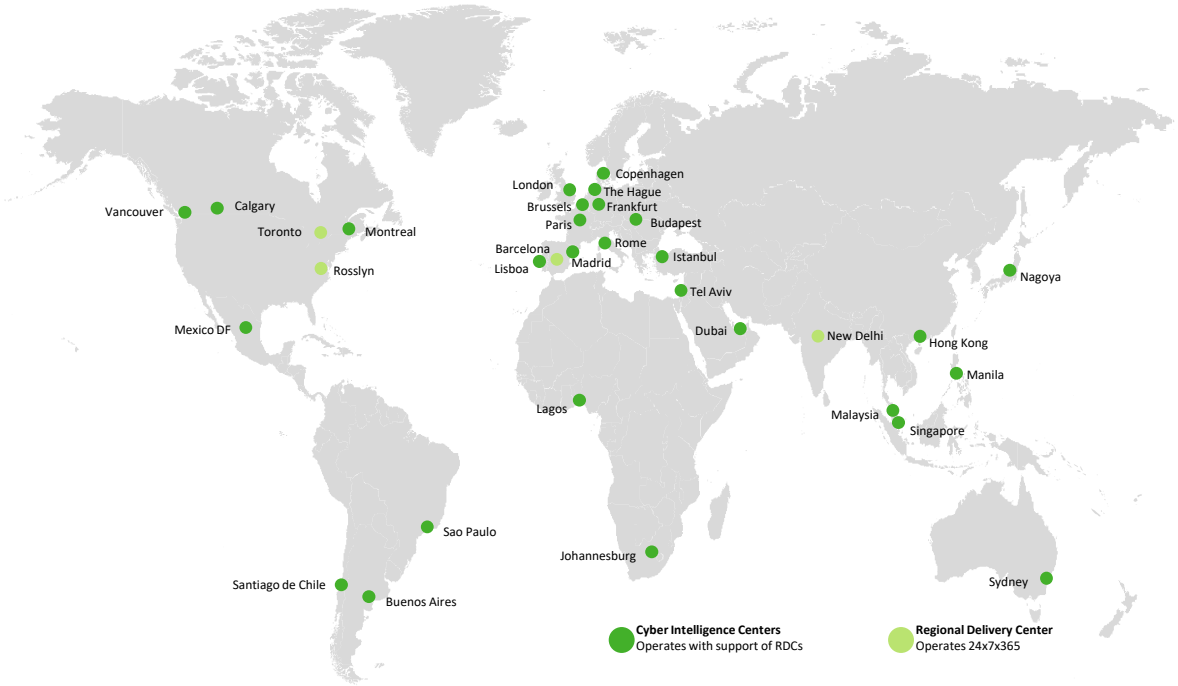
Deloitte Global Footprint

Our history…

Our **heritage**, combined with **deep tech expertise** and **broad industry experience**, means we're prepared for every scenario across the **cyber risk landscape** and we have gained **multidisciplinary experience**

27+ **years** in providing cyber services

20% Deloitte North South Europe[1] / Middle East **Cyber growth** YTD



Built by our people…

Deloitte's Cyber business is built around a diverse **global network** of cyber professionals with:

8,600+ dedicated cyber risk service **practitioners worldwide**

Of which, **1,300+** specifically **dedicated** to **North South Europe** and **Middle East**

Backed by **10,000+** **practitioners** with a **security focus** in other supporting areas

30+ **Cyber Intelligence Centers** provide advisory **SOC-related services**, fully customizable managed **security solutions** including advanced security monitoring, threat analytics, cyber threat management, and incident response for businesses

For our clients

Largest professional services **network** in the world…

70% of the **Fortune 500 companies** benefit from Deloitte cyber expertise

Alliances with **cyber vendors** globally provide our clients with access to a wide range of cyber risk technologies and the latest in technology innovation

Deloitte's delivery centers showcase our capabilities to meet the increasing **market demand** in cyber security services. Through our Regional Delivery Centers (RDC) we are able to provide 24x7 **support** to our **clients** with our multi-lingual teams of cyber specialists

Notes: 1) NSE: North South Europe (UK, Belgium, Switzerland, Netherland, Italy, Greece)

Deloitte’s Cyber Security Services

Deloitte’s Cyber Security portfolio covers all aspects related to reducing cyber risk through prevention, detection, and response services…

Deloitte Services Portfolio

Cyber Strategy

- Cyber strategy, transformation, and assessments
- Cyber risk management and compliance
- Cyber training education and awareness

Detect and Respond

- Monitoring and Management
- Threat Intelligence and analysis
- Operations management and Support
- Advanced Research
- Content Development

Application Security

- Digital technologies for innovation delivery encompassing (robotics and cognitive and mobile apps, ERP process systems)
- Integrity controls (SAP S4/HANA and Oracle, GRC, CRM and HR security controls, and SecDevOps lifecycle)

Cyber Cloud

- Cloud security and governance
- Cloud security orchestration and automation
- Cloud incident response
- Strategy and planning
- Workload migration and protection
- Micro service and container security
- DevSecOps

Infrastructure Security

- Threat and vulnerability management
- Core infrastructure security
- Asset management
- Mobile and endpoint security
- Technical resilience

Emerging Technologies

- OT Security
- Connected Products
- Smart Cities

Data & Privacy

- Data Risk Technologies
- Cloud Access Security Broker
- Data Access Governance Encryption/Tokenization
- Rights, Certificate, Consent, Cookie Management
- Retention & Destruction
- Payment & Database Security

Identity

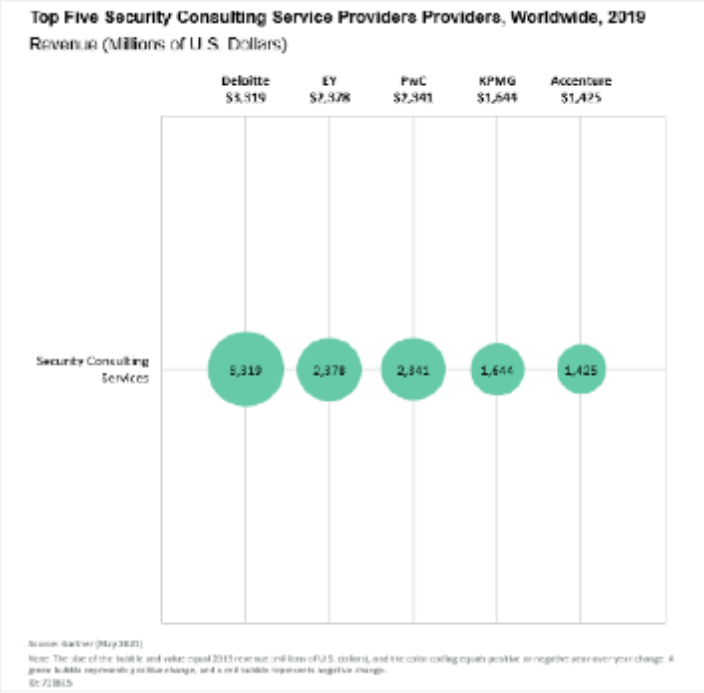
- Digital Identity platform
- Global Delivery Model
- Deloitte's IAM program - governance, people, process, and technology

Deloitte's Awards

…and to gain different important recognitions and awards

Deloitte Recognitions

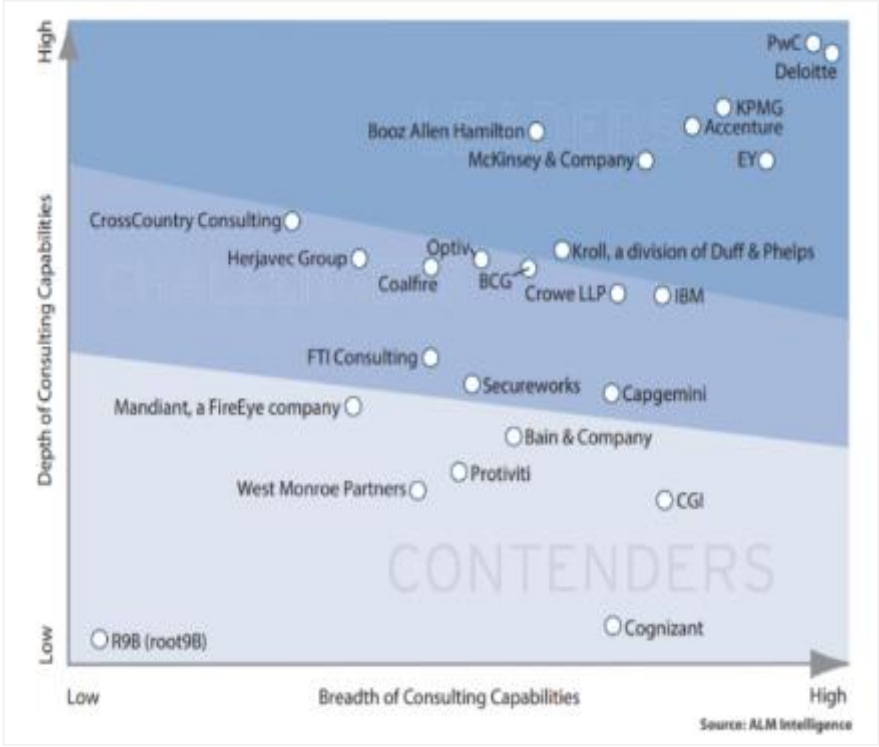
Security Consulting Services Worldwide Gartner, 2019/2020



*"Deloitte ranked #1 globally in Security Consulting by Gartner (**9th consecutive year**)"*

Global Cyber Security Consulting Providers, Forrester Q2 2019

Cyber Security Consulting Vanguard, 2019



Deloitte presentation

Our shared value

Integrity

At Deloitte, everything we do starts with integrity. In our marketplace nothing is more important than our reputation and, accordingly, we commit to conducting business with **honesty**, **distinctive quality, and high levels of professional behavior**. Ambition for excellence in customer service

Value

We play a critical role in helping both the capital markets and our member firm clients operate more effectively.

We consider this **role** a **privilege** and we know it requires constant vigilance and unrelenting commitment.

Dedication

We are proud of our culture of borderless collegiality and work hard to support our people.

We strive to create an **inclusive environment** that reflects our strong, clear expectations about diversity, respect and fair treatment.

Diversity

Our member firm clients' business challenges are complex and benefit from the innovation and **varied perspectives** that our practitioners bring.

We understand that working with people of different backgrounds, cultures and thinking styles helps our people to grow into better professionals and leaders.

The right approach

Lean.

Practical.

Hands-on.

Accessible.

Buy-in from day 1.

Deloitte presentation

Our commitment and knowledge with International Organization

ESTABLISHMENT OF NATIONAL CIRT

Deloitte assisted Burundi and the Republic of Botswana in establishing a Computer Incident Response Team

Deloitte's project team:

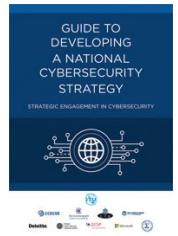
- Created a functioning national CIRT able to provide its constituents with a basic set of services
- Built human capacity at the national level in the field of cybersecurity and trained the future CIRT staff on CIRT operations and incident response
- Assisted the country with the development of awareness programs to improve cybersecurity posture of the identified constituents

CYBER DRILLS

Deloitte supported 17 cyber exercises initiatives of United Nation Agency ITU to enhance cyber security capabilities of CERTs worldwide

In the last six years ITU has organized multiple events in different regions completing training and exercise sessions with delegates mainly belonging to national CERTs/CSIRTs

Deloitte conducted the interactive cyber drill exercise. This type of drill immerses potential cyber incident responders in a simulated cyber scenario to help participants evaluate their cyber incident response preparedness

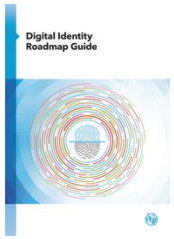


GUIDE TO DEVELOPING A NATIONAL CYBERSECURITY STRATEGY

Deloitte was a major contributor in the drafting of the ITU Guide to developing a National Cybersecurity Strategy

The purpose of the Guide is to steer national leaders and policy-makers in the development of a National Cybersecurity Strategy, and in thinking strategically about cybersecurity, cyber-preparedness and resilience

Deloitte attempted to address, organize and prioritize many of the aspects related to cybersecurity, based on existing and well-recognised models, frameworks and other references



DIGITAL IDENTITY ROADMAP GUIDE

Deloitte supported the ITU for drafting the Digital Identity Roadmap Guide

Deloitte leveraged on its experience in the implementation of digital identity systems to support the ITU in drafting the Digital Identity Roadmap Guide.

This guide introduces the main aspects to be considered by national leaders and policy makers in developing a National Digital Identity Framework, and should be considered a practical tool to guide stakeholders rather than an academic study on the topic of National Digital Identity Frameworks.

CERT Overview

CERT AT A Glance

A National CERT is a core element of a strategy to protect critical infrastructure vital to national security

- Detect, respond and prevent **threats**
- Manage **cyber incidents**
- Establish **Shared Situational Awareness**

- Coordinate **incident management** process
- Act as **focal point** for national and international discussions

- Provide specific **technical competence and skills**
- Develop trusted mechanism for information **dissemination**

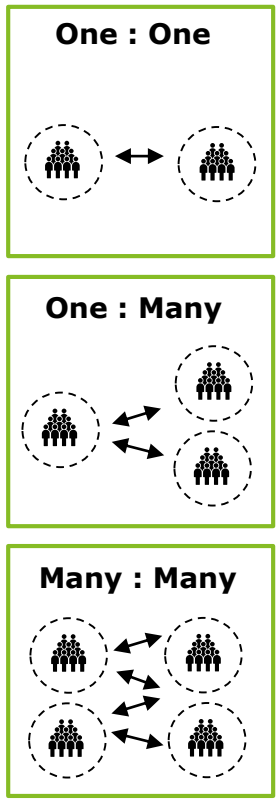
TYPICAL CERT MISSION

- 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 AT A Glance

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

Sharing approach



Stakeholders

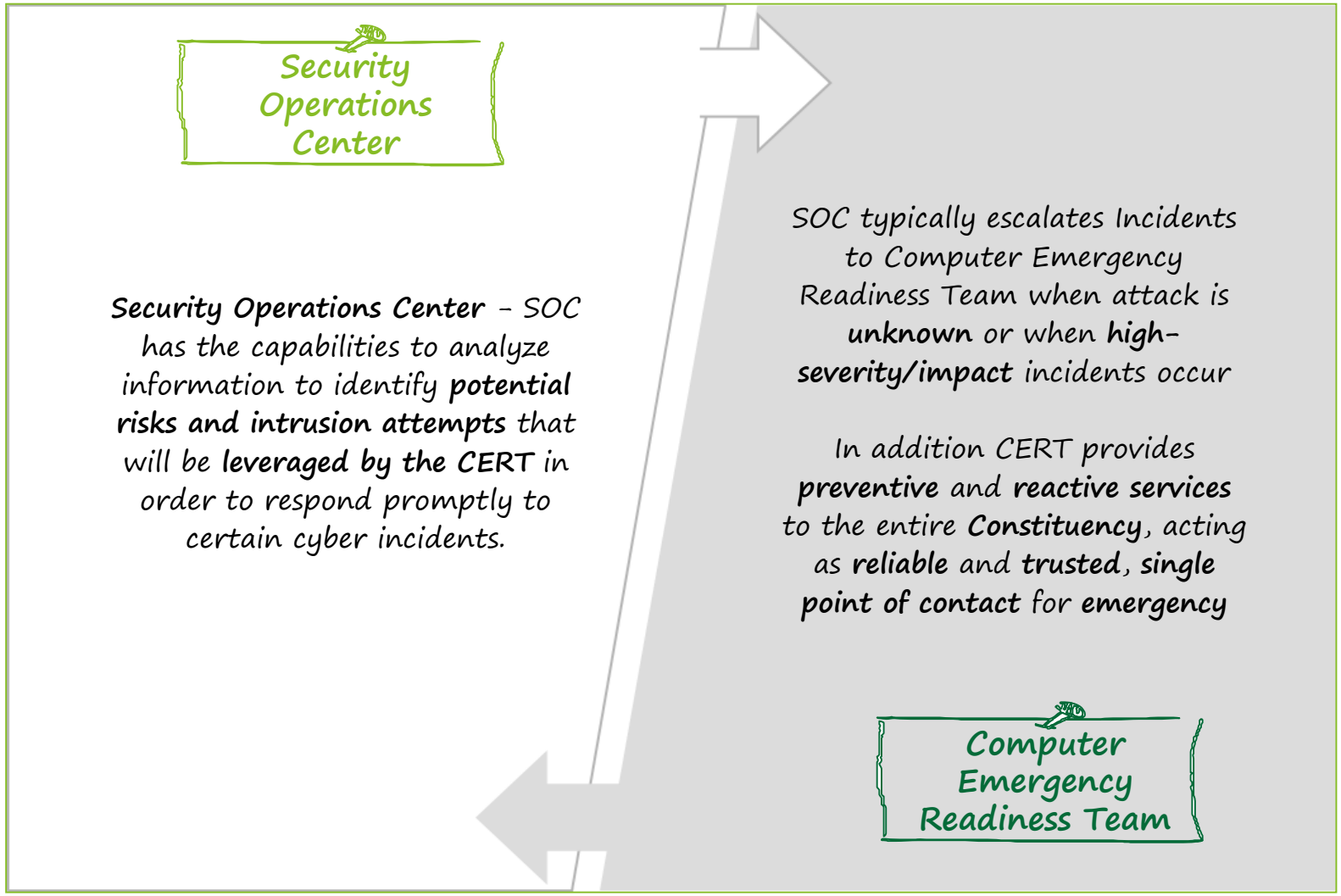
Enablers for interactions

- 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 (i.e. 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 prevented and/or mitigated, and less damage occurs.*

CERT AT A Glance

…with a strictly cooperation between SOC and CERT toward advanced and modern Cyber Defence capabilities



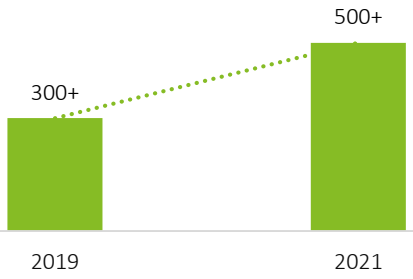
CERT AT A Glance

Different external and internal needs drive the request of new or redefined CERT at European level

Needs for CERT Development

- ***Regulation***
- ***National Cybersecurity Strategy pressure***
- ***Leading Practice***
- ***Intelligence and infosharing initiatives driven by governments and industry***
- ***Threats landscape evolution***

Europe is the region in the world with the **highest presence of national, government and sectoral CERTs** counting more than **500+** CERTs.



The last **two years** have seen an **increase** of more than **200 CERTs** around Europe, but they are still **not enough** compared to the threat landscape.

CERTs in Europe

NOT EXHAUSTIVE

Sources: ENISA, FIRST, TF-CSIRT, Carnegie Mellon, OAS, Deloitte Analysis

Sources: www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map; https://www.first.org/members/map

Note:
(*) taking into account only the accredited members

CERT AT A Glance

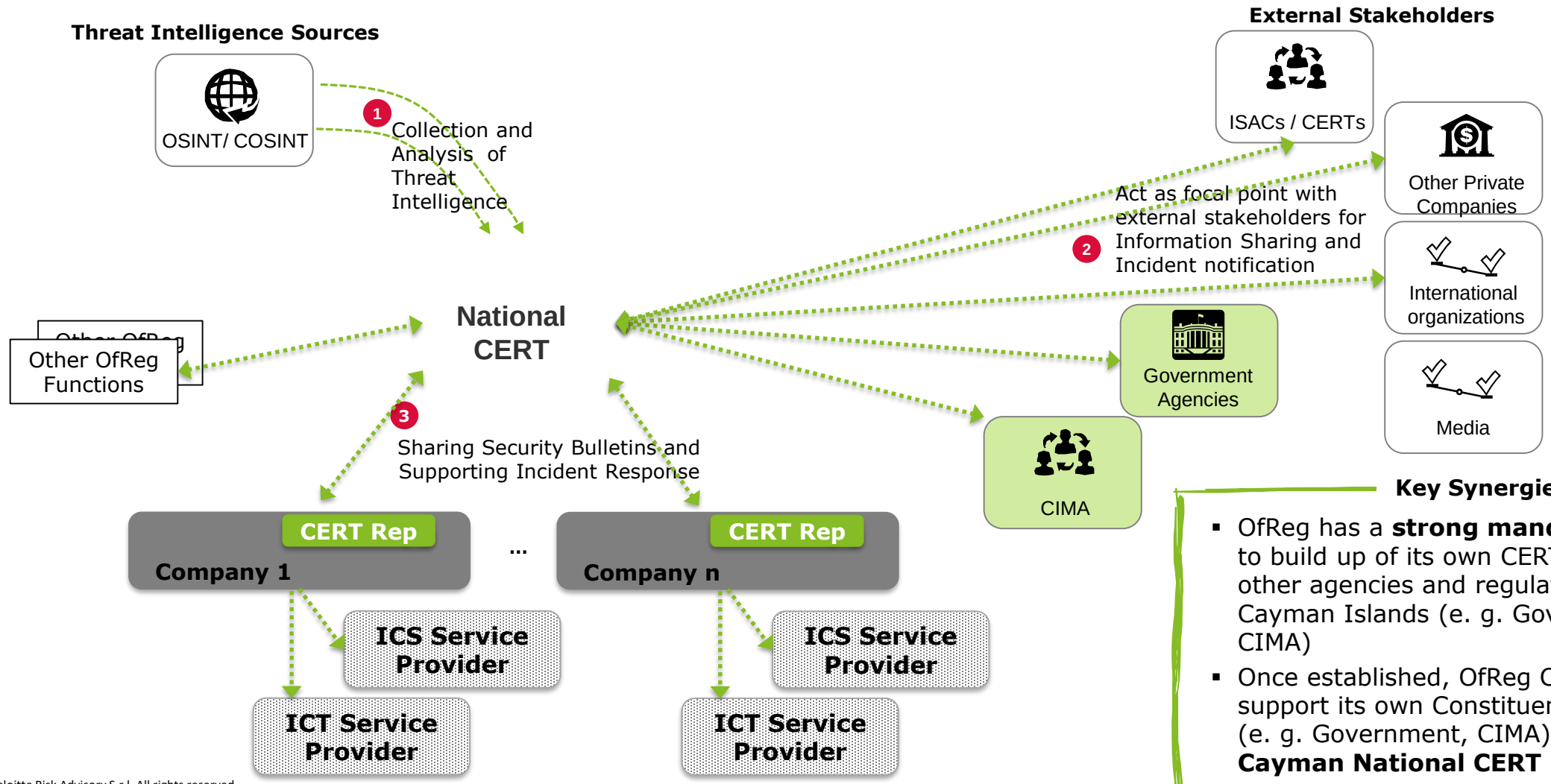
CERT's mission and role might be significantly different according to the Constituency

	Corporate CERT	Sectorial CERT	National CERT
Primary Mission	• Prevention and cyber incident response • Corporate Situational Awareness • Point of Contact for Cyber Incidents and Crisis	• Prevention and Incident Response coordination • Sectorial Shared Situational Awareness • Point of Contact for Industry/Sector cyber incidents	• Prevention and coordination of critical cyber incidents • National Shared Situational Awareness • Point of Contact at National level
Constituency	• Employees, customers and third parties	• Users and customers belong to organizations in the same sector/industry	• Citizens and organizations (mainly private)
Authority on Incident Response	• Distributed or Centralized	• No or limited authority (only coordination and structured information sharing)	• Depending on national strategy (typically limited)
Relationship focus	• Internal / external	• Internal / external	• External
Primary communication tools	• Phone, secure corporate mail / secure mail, web portal, Instant Messaging	• Phone, secure mail / web portal	• Phone, secure mail, web portal

Sources: ENISA, Esri, DeLorme Publishing, Deloitte Analysis

National CERT Operational Relations

National CERT shall interact with its own Constituency and other external stakeholders as other sector organizations, acting likely as a Cayman National CERT



Key Synergies

- OfReg has a **strong mandate** related to build up of its own CERT more than other agencies and regulators in Cayman Islands (e. g. Government, CIMA)
- Once established, OfReg CERT might support its own Constituency as others (e. g. Government, CIMA) **acting** as **Cayman National CERT**

CERT Processes

CERT - Cyber Security Services Portfolio

CERT intends to deliver a complete set of Cyber security services covering the prevention of Cyber Threats to protection and response of Incidents

Security Services Portfolio

A – Threat Prevention

Service that manages the ever changing threat landscape to OfReg Constituency by identifying and analyzing external threats and vulnerabilities

- **A1** Early Warning
- **A2** Information Sharing
- **A3** Artifact Analysis
- **A4** Threat Intelligence
- **A5** Exercise / Red Teaming

B – Threat Protection

Service that supports in the developing of safeguards, based on the OfReg Constituency threat landscape, to ensure protection of critical applications and infrastructure services

- **B1** Cyber Security Advisory
- **B2** Cyber Security Awareness
- **B3** Critical Vulnerability Management

C – Threat Detection

Service that identifies occurrences (pro-actively and retrospectively) of cyber security events based on the OfReg Constituency threat landscape

- **C1** Threat Hunting
- **C2** Cyber Security Event Monitoring
- **C3** Cyber Security Analytics

D – Incident Response & Crisis Management

Service that develops and implements appropriate activities and technology to respond to cyber security events, ranging from small incidents to attacks by professional adversaries

- **D1** Incident Response
- **D2** Crisis Management
- **D3** Digital Forensics

Provided by OfReG CERT

Provided only by Constituency Members

Note: (1) Services are described in the Appendix

CERT Core Processes – Incident Response

The Incident Response Process consists of 5 phases in which stakeholders are continuously communicating with each other

5

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

4

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

1

- **Incidents detection** through information sharing, notification from users, analysis of events from the security systems / SOCs, OSINT
- Development of **indicators and specific metrics** for early incidents detection

2

- **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

3

- **Support 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

CERT Core Processes – Incident Response

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

1 Preparedness and prevention

	DEFINITION OF CERT OPERATING STRATEGY	DEFINITION OF GUIDELINES AND CONTROLS	IMPLEMENTATION OF INFORMATION SHARING TOOLS	PLANNING OF CYBER SECURITY PROGRAMS
SUB-PHASE DESCRIPTION	**Establish** an **incident response capability** and process to be ready to respond to threats and recover from incidents	**Define rules**, **guidelines** and **procedures** for systems, networks and applications	Engage, communicate and **interact with** relevant **stakeholders**	**Promote** cyber security **awareness** that includes seminars, conferences, exercises
COMMUNICATIONS ACTIVITIES	Establish **CERT communication** approach and **strategy**, including roles and responsibilities of CERT communication staff members.	Define and **disseminate** rules, guidelines and procedures **to communicate**, cooperate and share information **with** CERT **stakeholders**	**Implement information sharing protocol**, **tools** and **techniques** to communicate and facilitate cooperation	**Plan** communication **activities**, including periodic events (e.g. training) to **foster** 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.

CERT Core Processes – Incident Response

In the Detection phase, effective communications facilitate proactive and reactive threat information gathering

2 Detection

COMMUNICATION
Leverage multiple sources to gather / share data and information

INTERNAL SOURCES

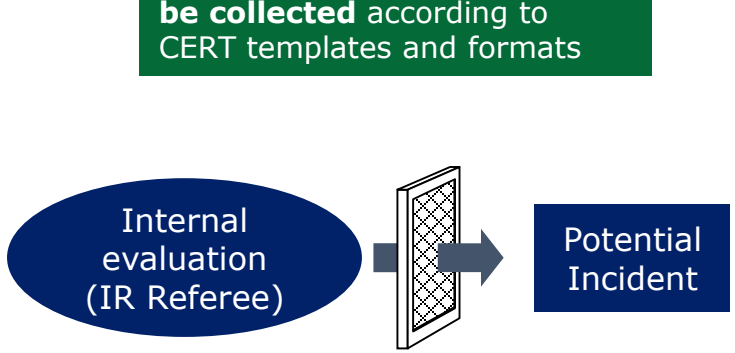
EXTERNAL SOURCES

Data from automated systems (i.e. SIEM)

Notification from users

Notification / reports from entities

Notification from other CERTs, organization



Evidences, coming from automated (i.e. Log, consoles) and human sources, **have to be collected** according to CERT templates and formats

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

CERT Core Processes – Incident Response

Effective classification of events requires stakeholders to communicate in common impact evaluation terms

ILLUSTRATIVE

3 Analysis and Triage

Impact 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

Normality → **Emergency**

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

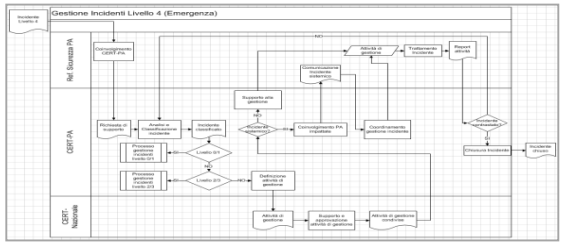
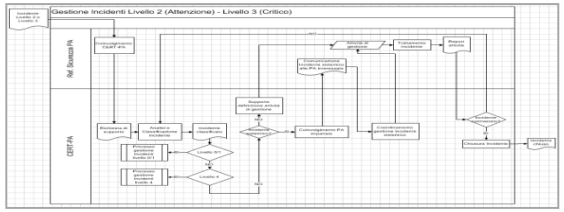
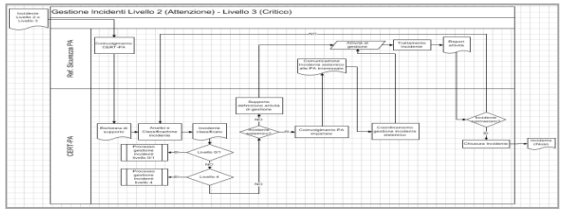
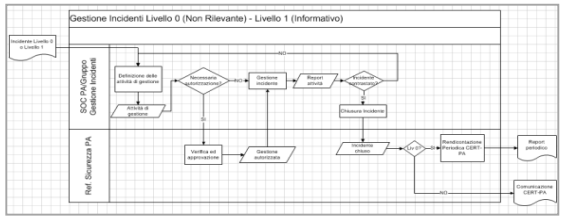
Level 0 Not relevant
- CERT is not informed, the incident is directly managed by the involved entity

CERT Core Processes – Incident Response

The Response phase should then include pre-defined processes to mitigate the incident based on its classification

ILLUSTRATIVE

4 Response

Level of emergency	Workflow diagram
Level 4 Emergency	
Level 3 Critical	
Level 2 Attention	
Level 1 Informative	

Macro – Processes Benefit

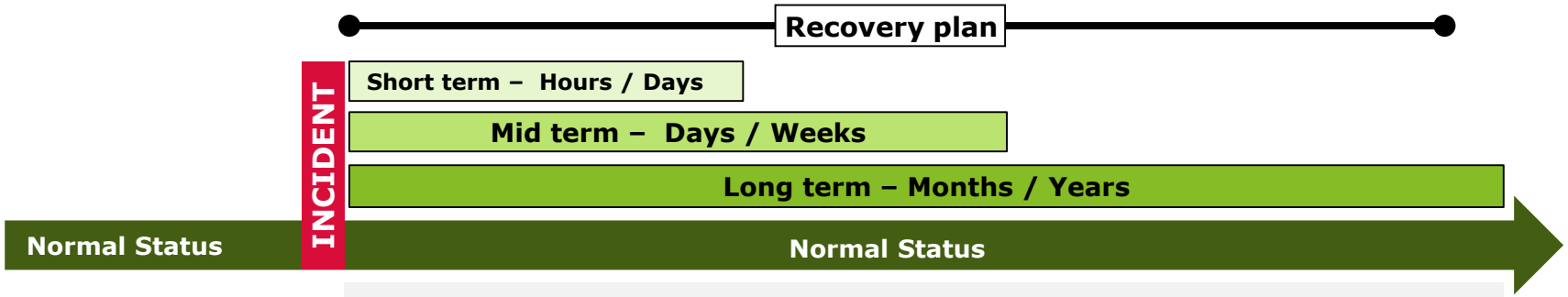
- **Definition of communication procedures** for each level of emergency including point of contacts. It ensures that required stakeholders will be proactively involved
- **Improvement of coordination** activities according to information sharing protocol
- **Definition of roles and responsibilities** 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

CERT Core Processes – Incident Response

Once the immediate emergency has been resolved, CERTs must communicate short, medium, and long terms plans

ILLUSTRATIVE

5 Recovery



TYPICAL MODEL TO RESTORE NORMAL OPERATIONS

- **Communicate short/mid/long terms messages** according to defined procedures and tools
- **Gather of lessons learned** on the incident and **share them** with CERT Constituency / stakeholders
- Confirm that expected results and **response activities have been successful**.
- 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)

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

CERT Core Processes - Information Sharing

The Information Sharing process consists of four consequential phases, ranging from gathering to information dissemination

1

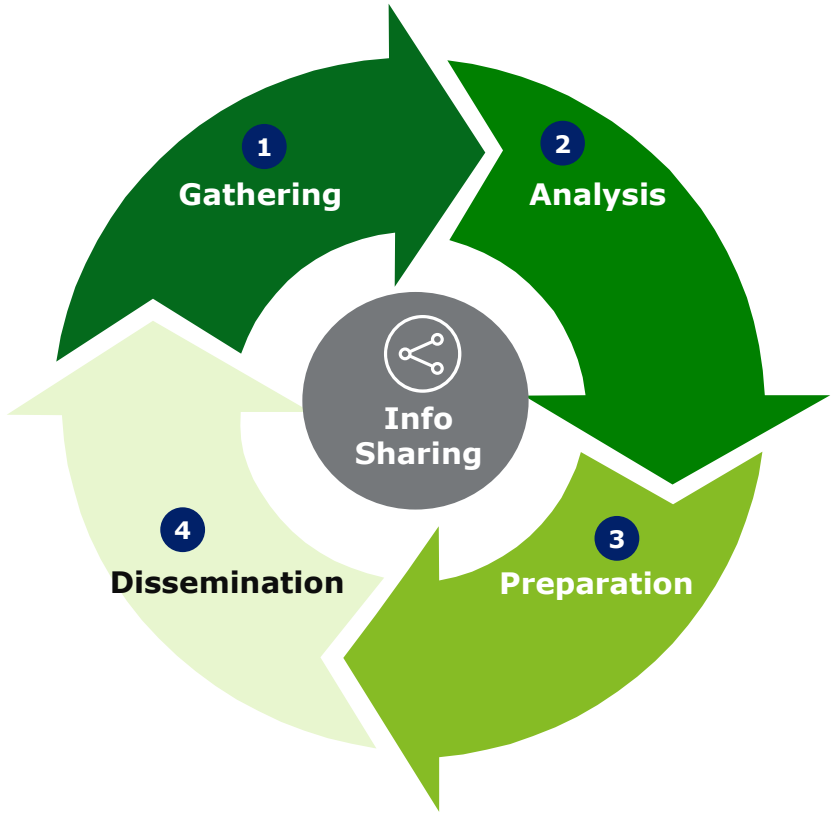
- Information is gathered through several sources (e.g. threats, vulnerabilities, incident responses process)

INFORMATION

2

- Analysis and correlation of information is performed

ANALYSIS



4

- Information is quickly shared with stakeholders in order to take appropriate actions to respond to the event

SHARING

3

- Definition of format, target and channel for each type of information
- Identification of the communication protocol to share information

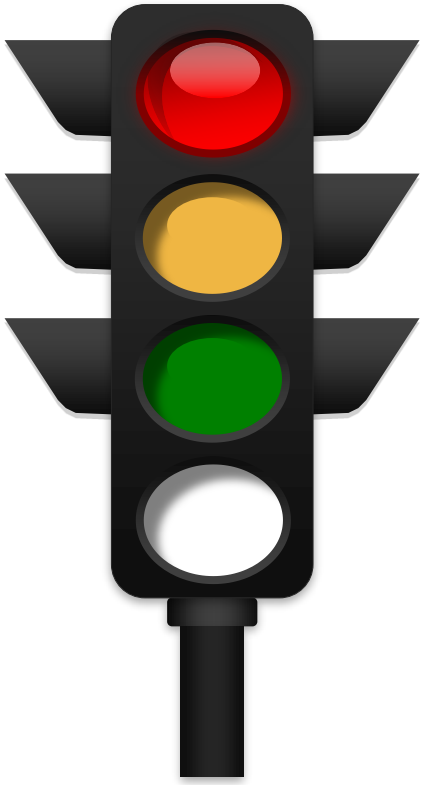
FORMAT

Process Phase

Output

CERT Core Processes - Information Sharing

All shared information should be classified according to an information confidentiality protocol, such as the Traffic Light Protocol



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.

CERT Core Processes - Information Sharing

An example of operational working method on Information Sharing is the Classification of Threats used by US-CERT

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

CATEGORY	THREAT	DESCRIPTION
CAT 0	**Exercise/Network Defense Testing**	This category is used during state, federal, national, international exercises and approved activity testing of internal/external network defenses or responses.
CAT 1	**Unauthorized Access**	In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource.
CAT 2	**Denial of Service (DoS)**	An attack that successfully prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.
CAT 3	**Malicious Code**	Successful installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are NOT required to report malicious logic that has been successfully quarantined by antivirus (AV) software.
CAT 4	**Improper Usage**	A person violates acceptable computing use policies.
CAT 5	**Scans/Probes/Attempted Access**	This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.
CAT 6	**Investigation**	Unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.

The classification provides seven Threat Categories from CAT 0 to CAT 6.
The first one of them (CAT 0) is for managing test activities only.

CERT Core Processes - Information Sharing

The Information Sharing initiative comprises four main activities

1 **Information Gathering from multiple sources**

2 **Dissemination of alerts, bulletin, advisor**

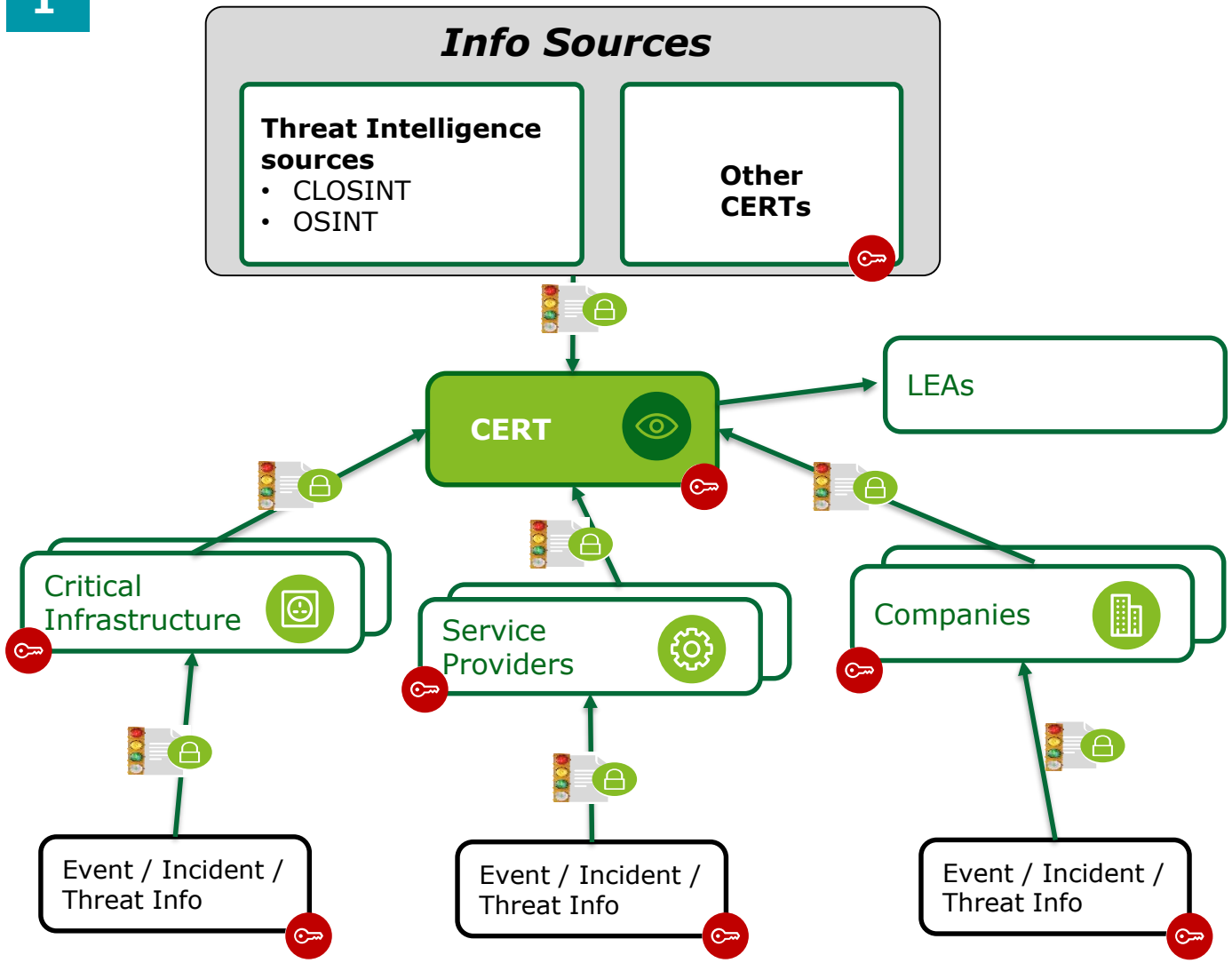
3 **Periodic communication: meetings and workshop**

4 **Reports and awareness**

CERT Core Processes - Information Sharing

Initiative in action - Information Gathering from multiple sources

1



Source of information

- **External:** for instance Threat Intelligence, other CERTs;
- **Alerts** coming form **Constituency's Members** classified according to TLP;
- In case the information is an **IoC,** CERT can use the **format shared in the Constituency** (e.g. CSV).

Cyphred Information

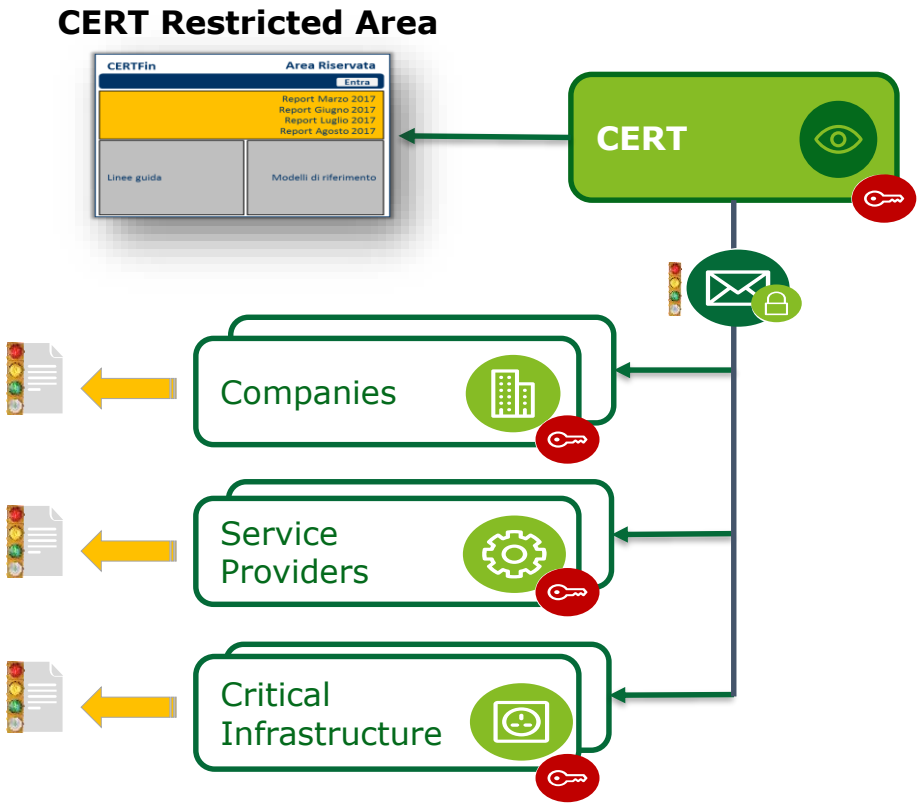
Limited Access

TLP Protocol

CERT Core Processes - Information Sharing

Initiative in action - Dissemination of alerts, bulletin, advisor

2



Constituency's Member which has a PGP key can receive information classified under TLP: RED sent by CERTs in a secure mode.

Comments

- **CERT sends information** within the Constituency including **description** and **technical details** (e.g. IoC) on new **threats** and **vulnerability** using appropriate format;
- CERT uses **TLP protocol** to classify the information;
- In case of **TLP:RED, CERT can** use tools such as **PGP** key to communicate with Constituency.

Cyphred Information

Limited Access

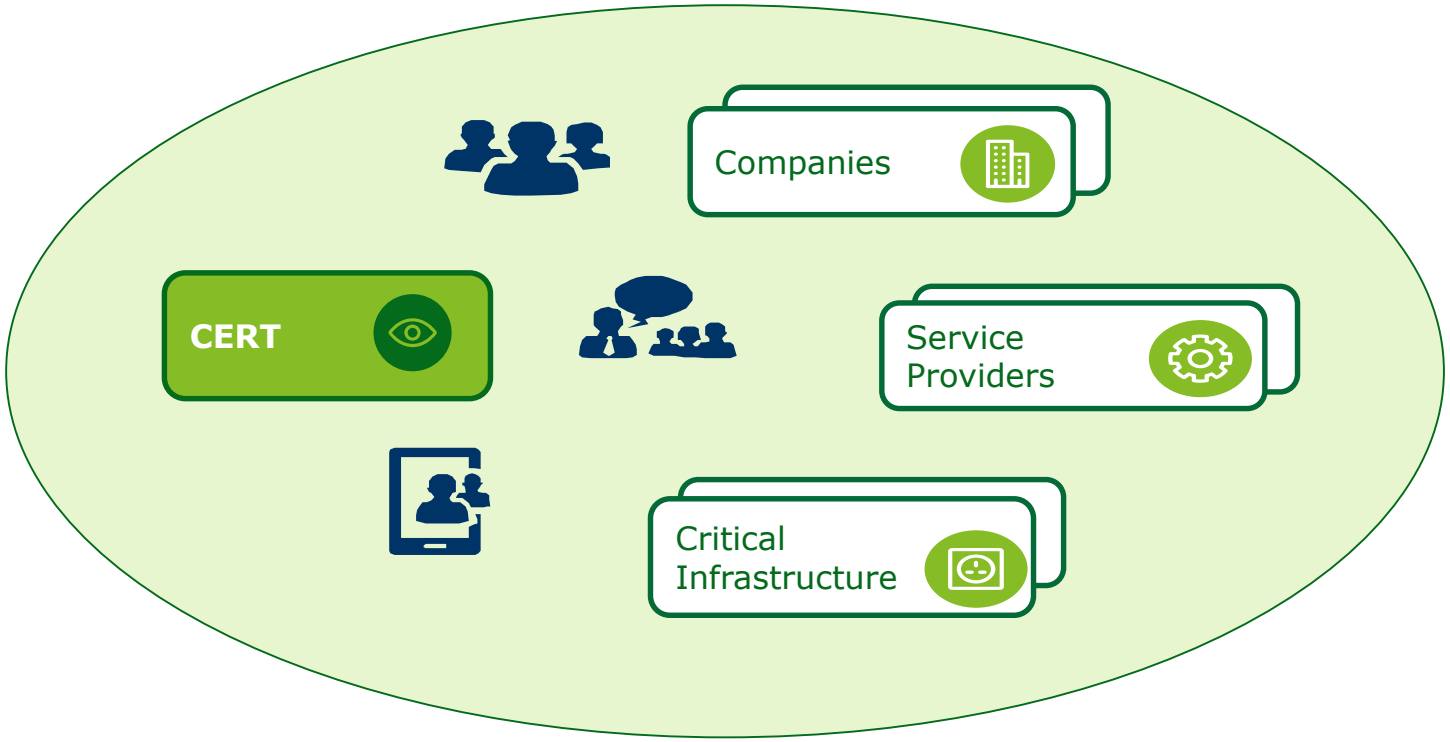
TLP Protocol

E-mail

CERT Core Processes - Information Sharing

Initiative in action - Periodic communication (meetings and workshop)

3



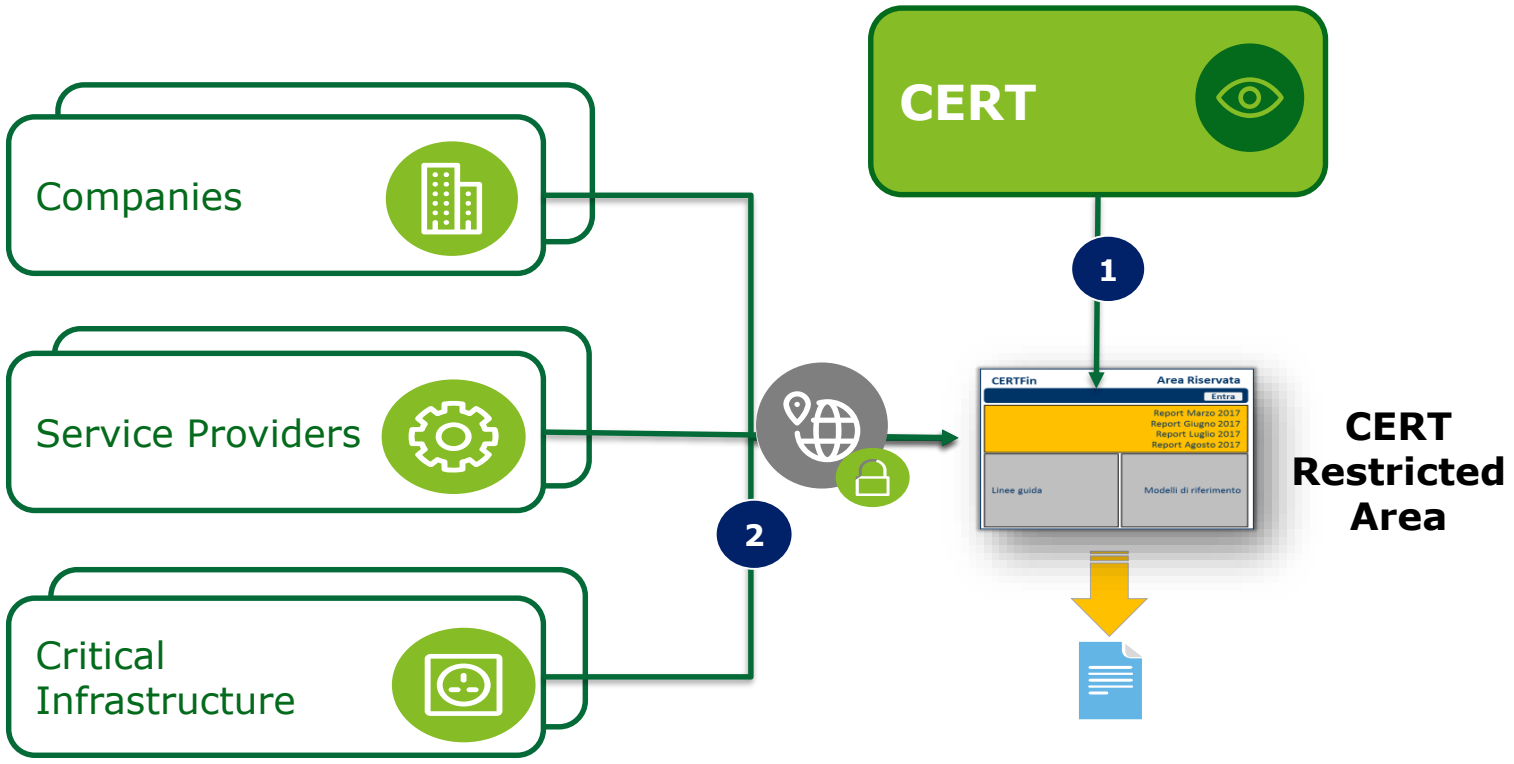
Comments

- **CERT** organize periodic meetings, workshops, and calls to share information
- Meetings and workshop can be **limited to a subgroup of the Constituency** / relevant stakeholders based on confidentiality of topics

CERT Core Processes - Information Sharing

Initiative in action - Reports and awareness

4



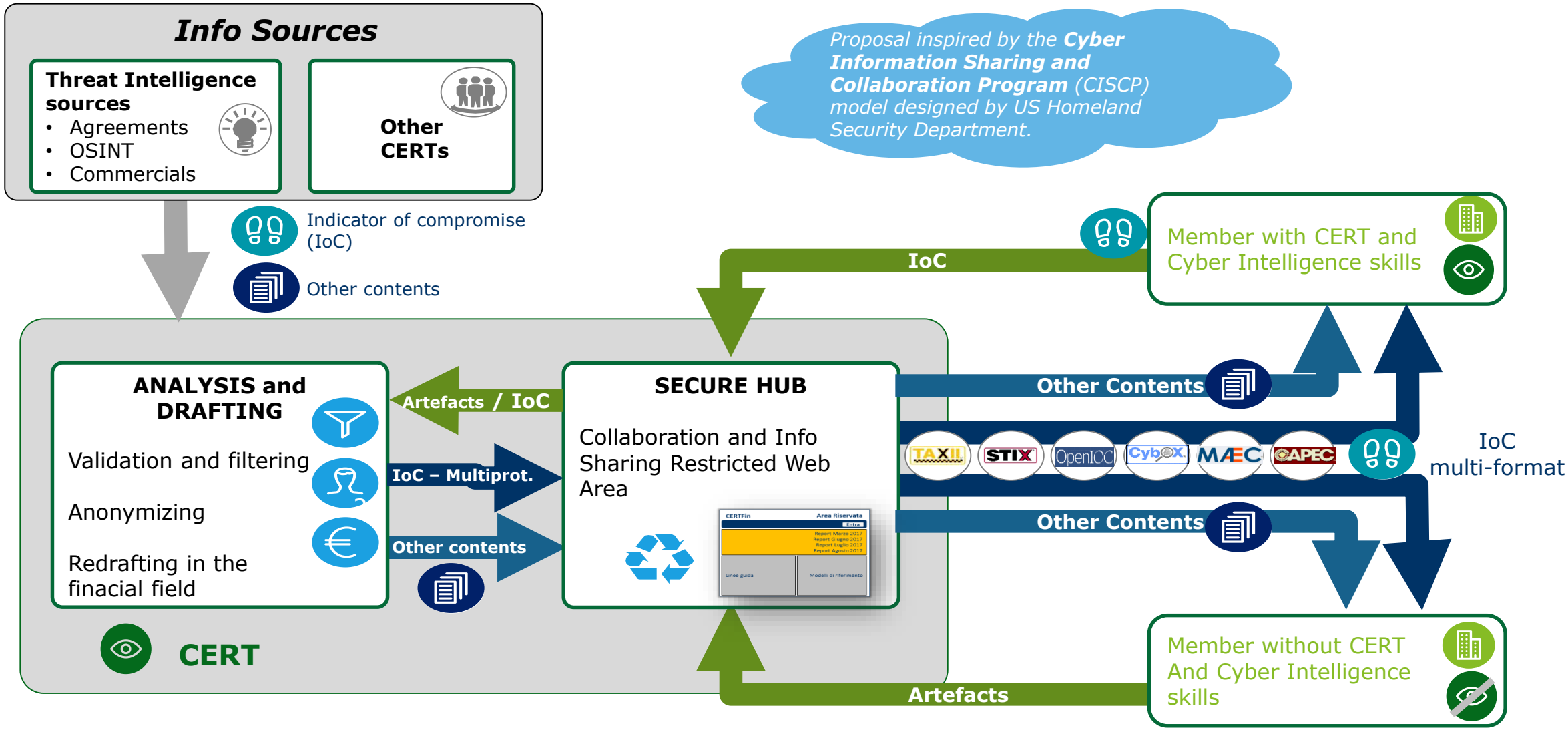
Comments

1. CERT uses Restricted Area for:
   - Reports and alerts;
   - Guidelines.

2. Constituency's Member can log in CERT Restricted Area to read uploaded material.

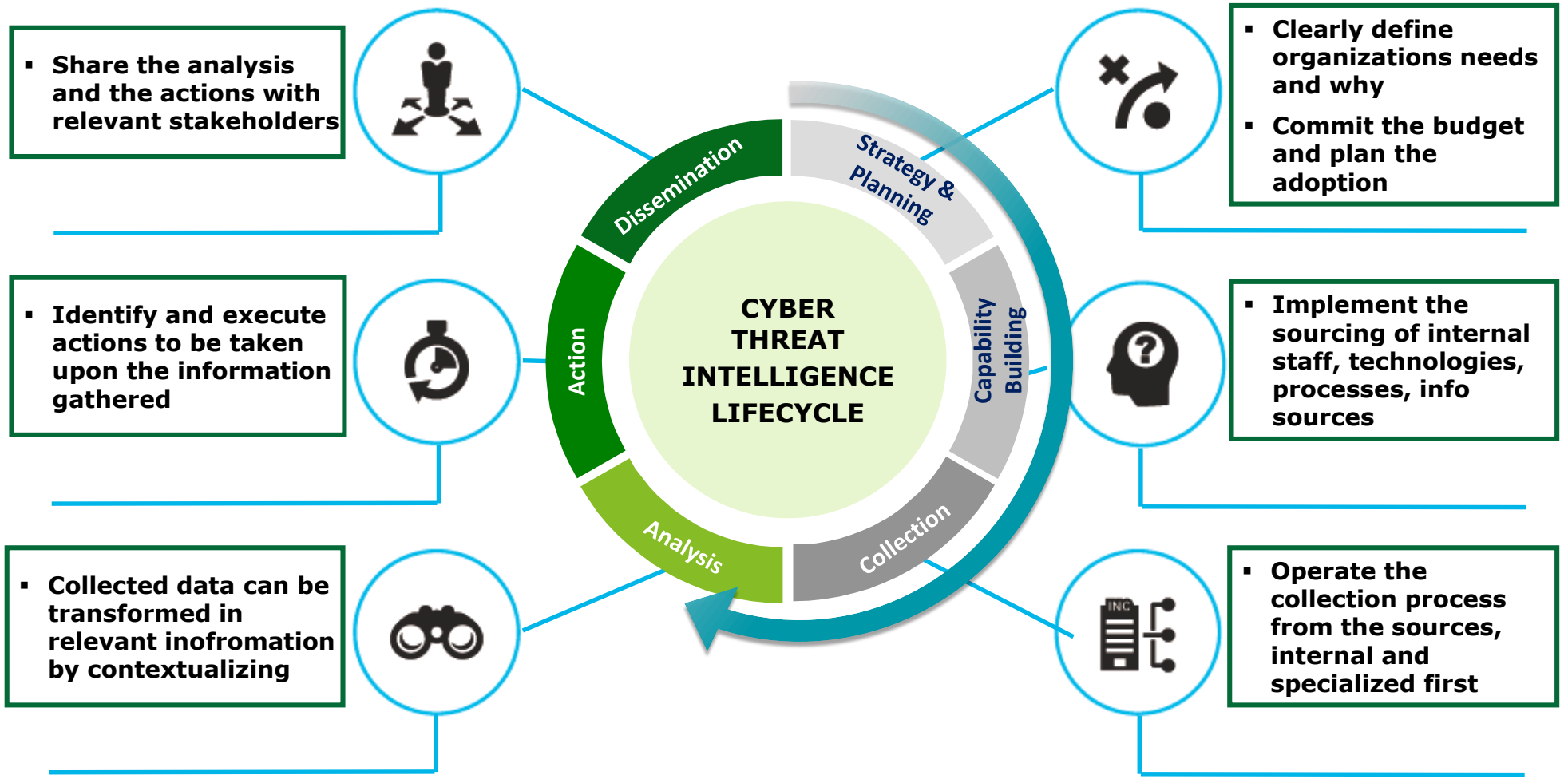
CERT Core Processes - Information Sharing

Information Flow



CERT Core Processes – Cyber Threat Intelligence

One other core process is the Cyber Threat Intelligence, which is based upon the CTI Lifecycle, derived from FBI Intelligence model



CERT Core Processes - Cyber Threat Intelligence

The cycle begins with the acquisition of three types of Intelligence that differ by scope and mode of collection…

Types of CTI

SOURCES OF INFORMATION

Threat Intelligence Providers

OSINT/ CLOSINT

External Stakeholders

Government Agencies

ISACs / CERTs

Other Private Companies

International organizations

Web / Deep Web / Dark Web[1]

OSINT / CLOSINT

FIELD

Give/Share Intelligence information and feed which could be relevant for the Constituency

These are divided into two types

CERT Conducts extensive / targeted searches in the Web to identify **potential violations** perpetrated **outside** the Constituency's perimeter

TYPE OF INFORMATION

1 **Human Readable Intelligence**

2 **Machine Readable Intelligence**

3 **Intelligence Acquired Through Active Research**

DESCRIPTION AND FORMAT

Description

New vulnerabilities, threats, malware, but also attack modes with impact on assets. They require **analysts to identifies preventive and monitoring measures**

Format

Bulletin, Alert, Advisory, Report

Description

New vulnerabilities, threats, malware with elementary feed (IP, URL, IoC) that can impact on assets ICT/ICS. They can be **acquired from security solutions automatically**

Format

Proprietary or open as STIX, Open IoC, Alert, Report

Description

Violations linked to Information Leakeage, Phishing, e-Fraud, Brand Abuse, ecc.
They require analysis for validation and subsequent response and / or containment action

Format
Alert, Report

CERT Core Processes - Cyber Threat Intelligence

... and by different operating levels of Intelligence to handle

Focus on Human Readable Intelligence

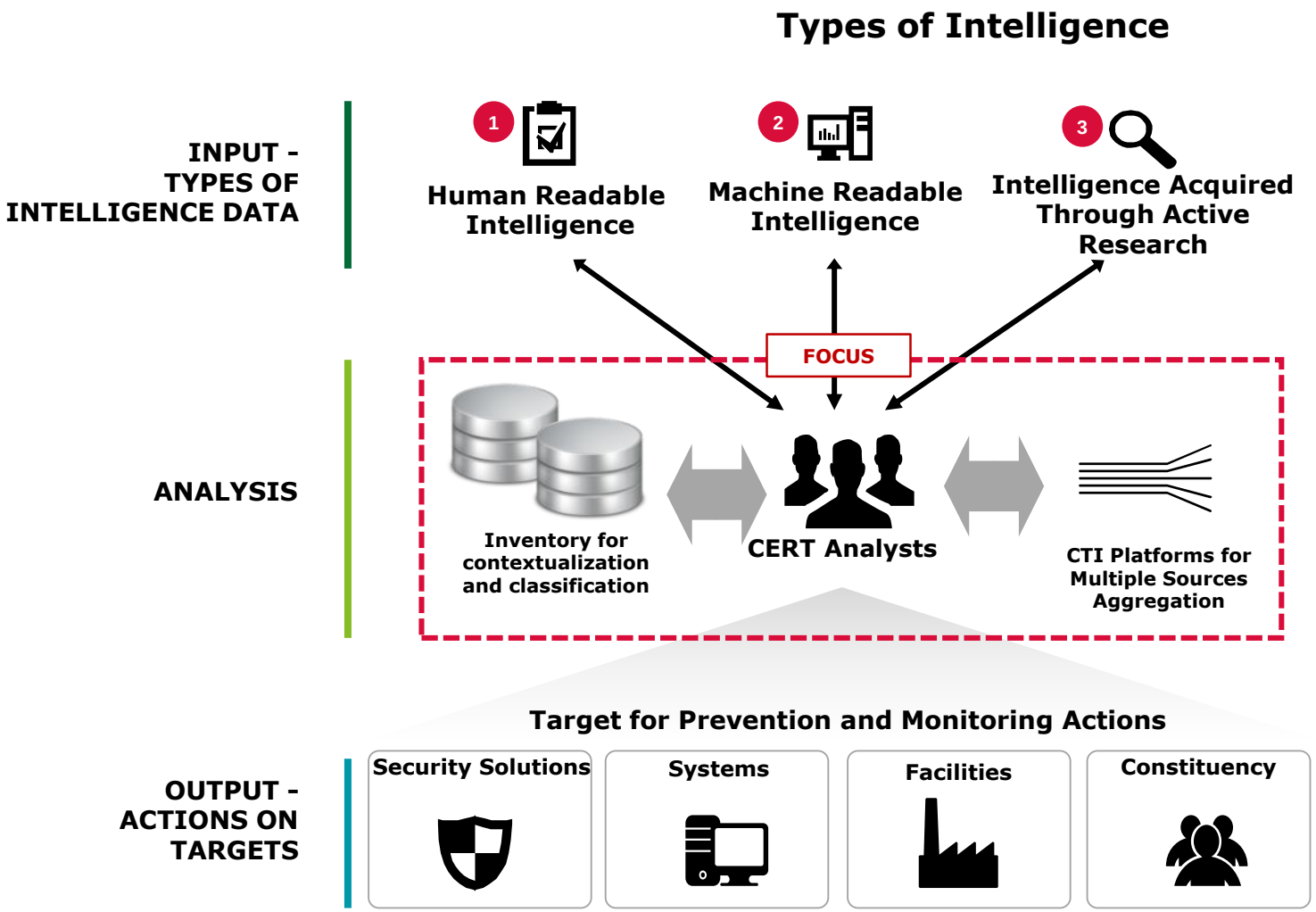
HUMAN READABLE INTELLIGENCE

Operational Levels of Cyber Intelligence[1]	CERT Responsibilities	Intelligence Examples
Strategic	▪ Collection and analysis of **Strategic Intelligence information** to identify initiatives and prevention/defense programs	▪ Strategic assessments, including long-term forecasts ▪ Annual Intelligence Reports ▪ Evaluation of risk profiles ▪ Geopolitical analysis ▪ Check of the risks for the adoption of new technologies
Operational / Adversary	▪ Identification of **reliable sources** and **information sharing** ▪ The analyzes are conducted in collaboration to identify actions, prevention and defense interventions	▪ Assessment on threat actors ▪ Vulnerabilities analysis ▪ Weekly / Monthly / Quarterly Intelligence Reports ▪ Technical reports with detailed analysis and descriptions of possible actions to be taken
Tactical	▪ Collection and analysis of **Tactical Intelligence information** to identify actions, prevention/defense interventions	▪ Daily Analysis ▪ Short reports to disseminate ▪ Malware Analysis Report ▪ Raw information reports ▪ Raw feeds (IP, domain, URL)

(1) Source: Intelligence and National Security Alliance (INSA) produced a document titled "Operational Levels of Cyber Intelligence" that expands on traditional tiers of intelligence and extends them to the cyber domain

CERT Core Processes - Cyber Threat Intelligence

To support CTI process, there are specifics enabling tools for analysts, such as inventory and CTI platforms

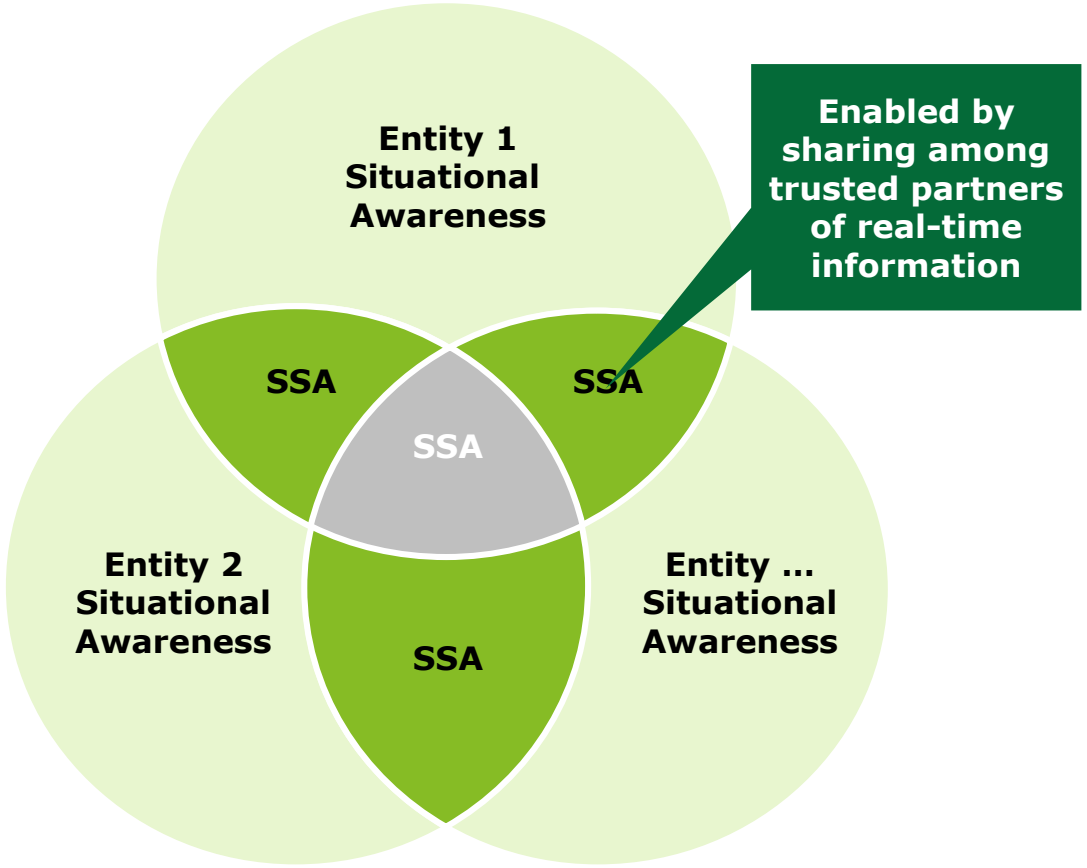


Analysis Activities

- The **contextualization** of intelligence **requires** a deep **knowledge** of the Constituency assets
- **Evaluations** (included in the inventory) performed on assets allow to **understand** what **priority** must be assigned to prevention and monitoring **actions**
- The **analyzes** are **enabled by CTI Platform**, tools designed to aggregate data from multiple sources and that put them into security solutions

CERT Core Processes - Shared Situational Awareness

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

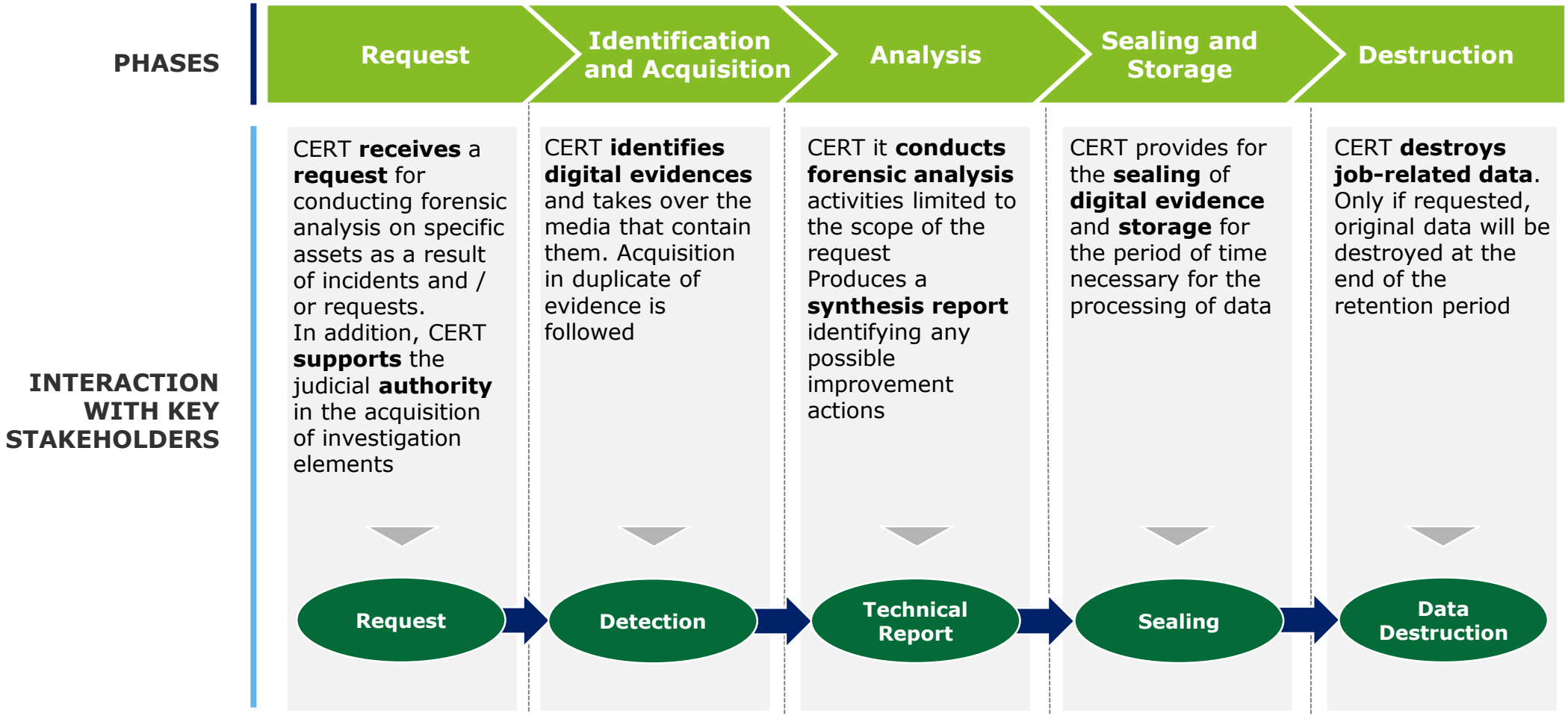


SSA Key Considerations

- 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
- The Shared Situational Awareness (SSA) 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

CERT Processes - Cyber Forensic

The Cyber Digital Forensics process supports the acquisition, analysis, preservation and destruction of computer artifacts



CERT Processes – Red Teaming

Red Teaming Operations Services can be used to significantly raise the overall level of CERT cyber awareness

Red Teaming Operations **assesses** the **cyber readiness** and **awareness** the CERT based on cyber threat scenarios derived from IT security assessment.

With Red Teaming Operations it is possible to validate the materialization of the cyber threat scenarios on a operational level. Controlled incidents are executed based on **predefined scenarios**, **like spear phishing** and **social engineering**.

Red Teaming Operations is about

Resilience

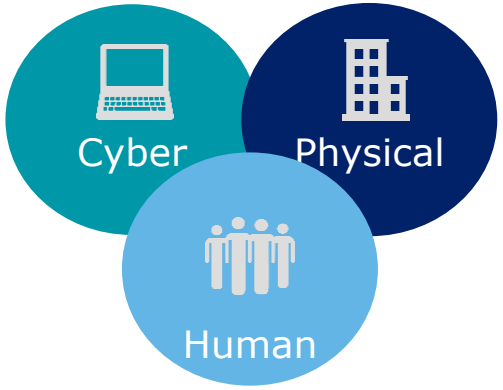
Cyber Awareness

Planning & Response

Red Teaming Operations focusses on **three core elements** of Information Security:

- **Cyber**: this represents the **online world**, the Internet as well as corporate Intranets and all other computer networks.
- **Physical**: this is the buildings, the desks, the safes and the IT **physical infrastructure**.
- **The Human**: this represents the employees, customers, clients, third parties that binds the cyber and physical world **together**.

The Information Security elements



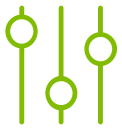
-- EXAMPLE -- **Combined scenarios flow** – EXAMPLE --

1	Attackers perform target reconnaissance and gather information required for the next stages of the attack. Such information might contain: employee and third party data, technical or physical aspects. **(Physical, Cyber and Human – Intelligence gathering)**	
2	Attackers break the physical perimeter and gain physical access to the target location. ***(Physical + Human – Physical entry via social engineering)***	Attackers trick employees into installing malware via an targeted email phishing attack. ***(Human – Mail phishing via social engineering)***
3	Taking advantage of the physical access priory obtained, attackers install a hardware implant in the target office building. ***(Physical – Hardware implant)***	The malware installed as a result of the phishing attack is used by attackers to implant other software necessary for remote access to the network. ***(Cyber – Software implant)***
4	Attackers gain remote access to the internal network via the implanted hardware and software. Further, attackers use this as a stepping stone to gain access to critical systems and data. ***(Cyber – Tactical network exploitation)***	

CERT Processes – Red Teaming

Red Teaming exercises are a cornerstone to build effective cyber defensive capabilities, so they are essential for CERT a complete services portfolio

Red Teaming Key Success Factors



Right business and technical mixture. Red teaming exercises need to combine the right amount of technical and business understanding to become useful and representative.

Improvement of defensive capabilities. Through Red Teaming exercises, the CERT Team can **develop** and **improve expertise**, training at the same time not only their technical **skills**, but also their ability to work with Incident Response and Info Sharing **tools**, following the pre-defined **processes** (CTI, IS, IR)

Thorough understanding of the context. For a red teaming exercise to be successful, a thorough understanding is necessary of the actor being simulated. The **objectives of** this **actor need** to **match** the **risks** of the **CERT** and will thus be incorporated in the defined scenarios driving all the exercise.

Tailored threat driven scenario selection and execution. Not some random attacks to random objectives. The best planning comes from **in depth understanding** of the **constituency** and of its **risks**, in order to **translate** them into **scenarios** that matter, combining risk and threat management approaches.

CERT Processes – Red Teaming

Each Exercise can be delivered through a four-phases specific approach

Planning

Phase 1

- Determine **final** scope and **objectives** of the exercises
- Create **unique scenarios** of controlled incidents tailored to CERT's situation
- Determine **start** and **end times** of execution phase and GO/NO-GO parameters

Execution

Phase 2

- **Execute scenarios** to achieve pre-agreed objectives
- Consists of **tactical network exploitation** activities
- **Record observations** of problem areas and evidence of the objectives achieved

Reporting

Phase 3

- **Document** observations in a final **report** together with management summary
- **Document issues** identified for each observation, **provide** importance **rating** and **recommendations**
- **Demonstrate** how each objective was accomplished

Remediation

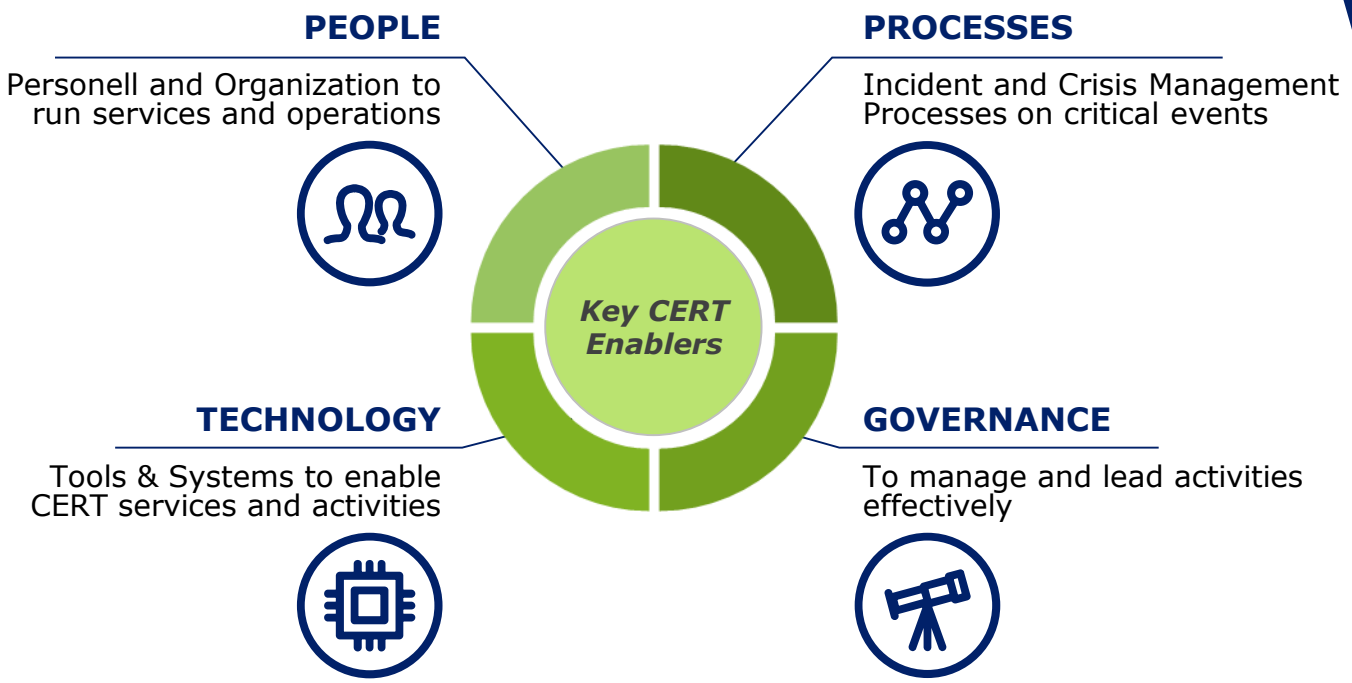
Phase 4 (optional)

- Create **remediation plan** based on recommendations
- **Prioritizing** actions and create rough short-, mid- and long-term **planning**
- **Aligning** actions to applicable security **roadmaps**

CERT Capabilities

CERT Methodology & Vision

Four components are vital to build a first-in-class National CERT which is able to effectively prevent, respond and manage cyber security incidents and emergencies



Main Objectives

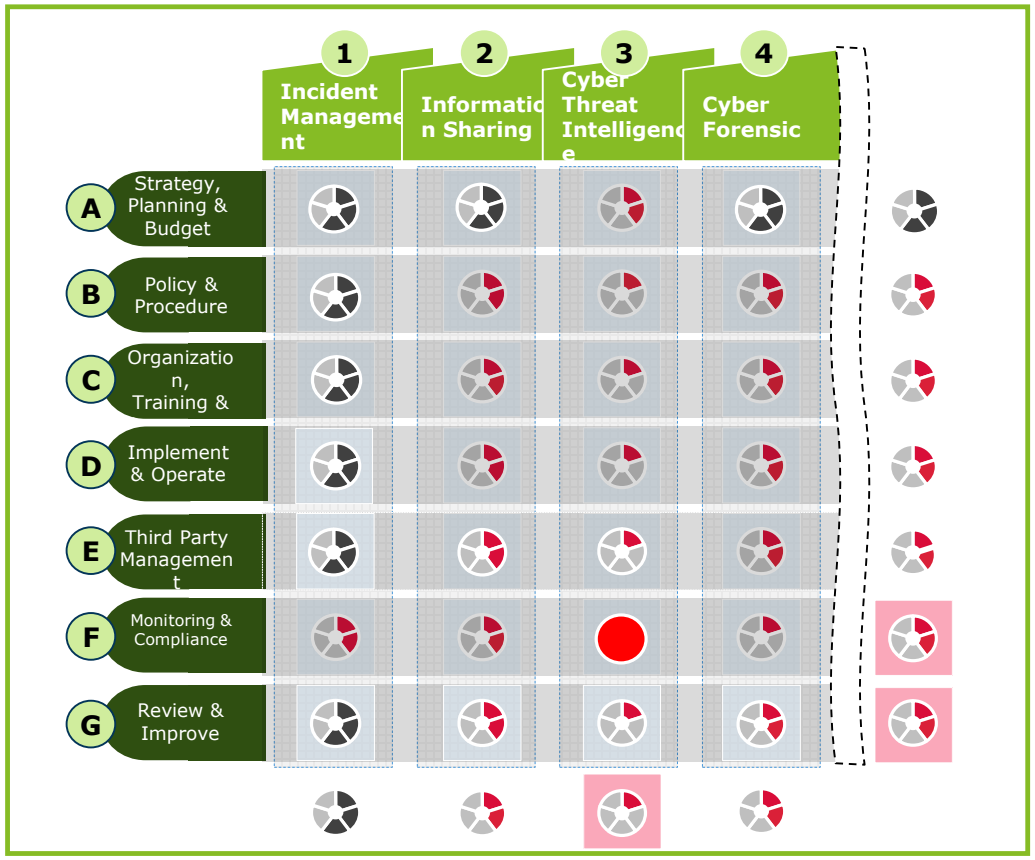
- CERTs allow structured **exchange of information** to prevent and respond against cyber events
- CERTs are enablers for establishing **trusted relationships** with stakeholders:
  - Constituency and other CERTs
  - Government and institutional agencies / entities
  - Private companies
  - National, regional and International organizations
- CERTs coordinate and foster **communication** among several actors in case of threats, vulnerabilities and incidents

CERT Capabilities - Governance

CERT Governance should respond to specific metrics in order to be effective and continuously improved

ILLUSTRATIVE

Governance Maturity Model



Key data sources

	Objectives	Content
Internal Policies	▪ Provide CERT and Incident Response Model, internal operating procedure aligned with CERT Community recommendations	▪ Information Management ▪ Operating procedures and metrics ▪ Roles and responsibilities ▪ Incident Response templates and guidelines
Key Indicators	▪ Represent in a simple and synthetic form CERT Services metrics and managed incident (KPI – Key Performance Indicator)	▪ Identified key indicator for all the CERT Services
Executive Dashboard	▪ Adopt a straight forward interface to inform stakeholder and support the resolution of potential deviation from objectives	▪ Represent all the identified key indicator both from Incident Response and CERT execution perspective

Not Applicable · Not Implemented · Initial / Ad Hoc · Repitable and · Process Defined · Managed and Measurable · Optimized · Key Finding

CERT Capabilities - People

The organizational structure of the CERT is a critical aspect to support effective operations and proactivity

ILLUSTRATIVE

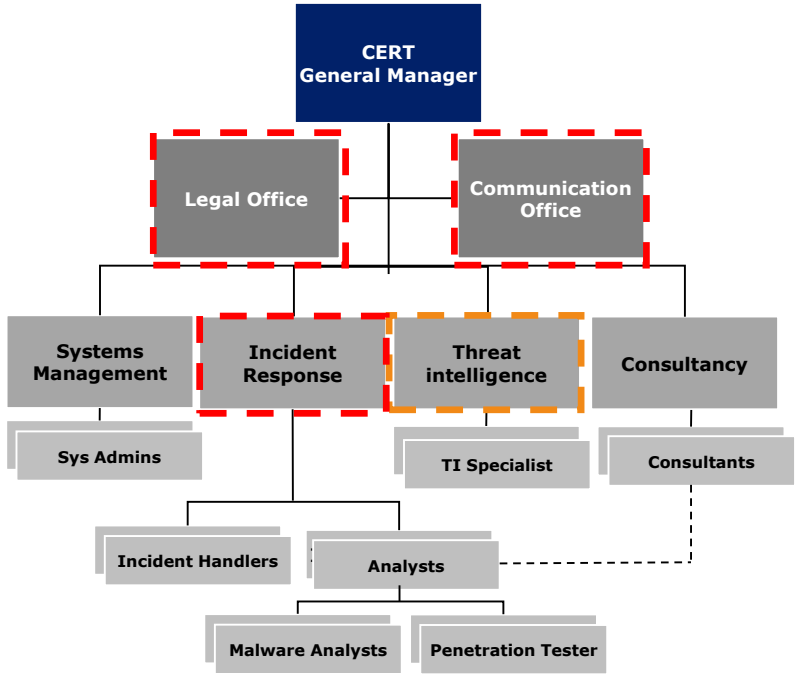
CERT services

ROLE	MAIN TASKS
General Manager	▪ Provide strategic direction ▪ Represent and supervise the team
Legal Officer	▪ Manage legal issues related to CERT
Communication Officer	▪ Manage communication activities related to CERT
Sys Admins	▪ Perform systems management
Analyst	▪ Identify information and potential incident
Malware Analyst	▪ Analyse malicious software
Penetration Tester	▪ Perform penetration testing
Incident Handler	▪ Support and coordinate incident response
TI Specialist	▪ Gather and correlate data and information
Consultants	▪ Hired when needed for specific activities

REACTIVE CAPABILITIES

PROACTIVE CAPABILITIES

Organizational Chart



Communication Key staffing

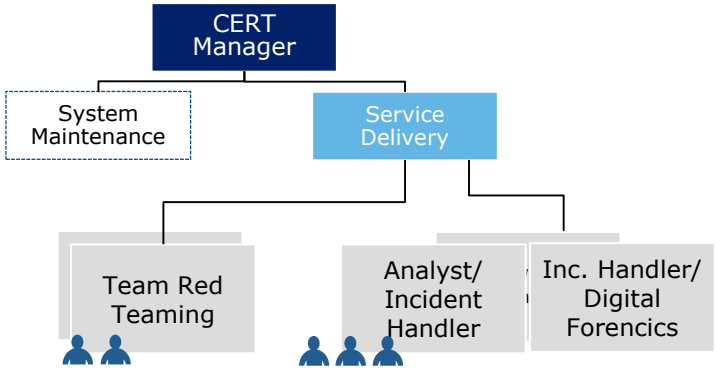
- ✓ **Communication Officer:**
  Acts as interface with CERT stakeholders and organizations. Maintains and constantly update internal and external list of point of contacts
- ✓ **Legal Officer:**
  Advises on information disclosure according to CERT policy and national laws and regulations
- ✓ **Threat Analysts:**
  Support on technical description related to threat/incident

CERT should have a **Communication Office**, including media policy and established associated procedures, to provide information

CERT Capabilities - People

The tipical internal organization is defined considering the number of critical events, analyzed sources and Info Sharing relationships

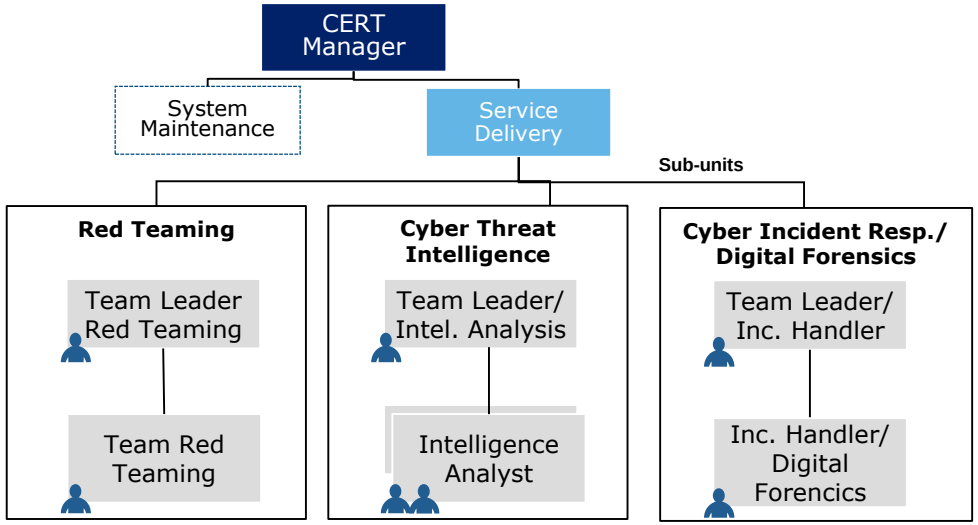
Internal Organization – Standard



Features:

- CERT is composed by a **Manager** with technical skills and at least **3 incident Management** - **Cyber Threat Intelligence** figures, with **2** figures for **Red Teaming** activities
- Communication with external entities is a manager responsibility. Communications and legal skills are borrowed from the responsible offices
- Working hours are the office ones, but maximum availability is required for Analysts/Incident Handler

Internal Organization – Best in Class

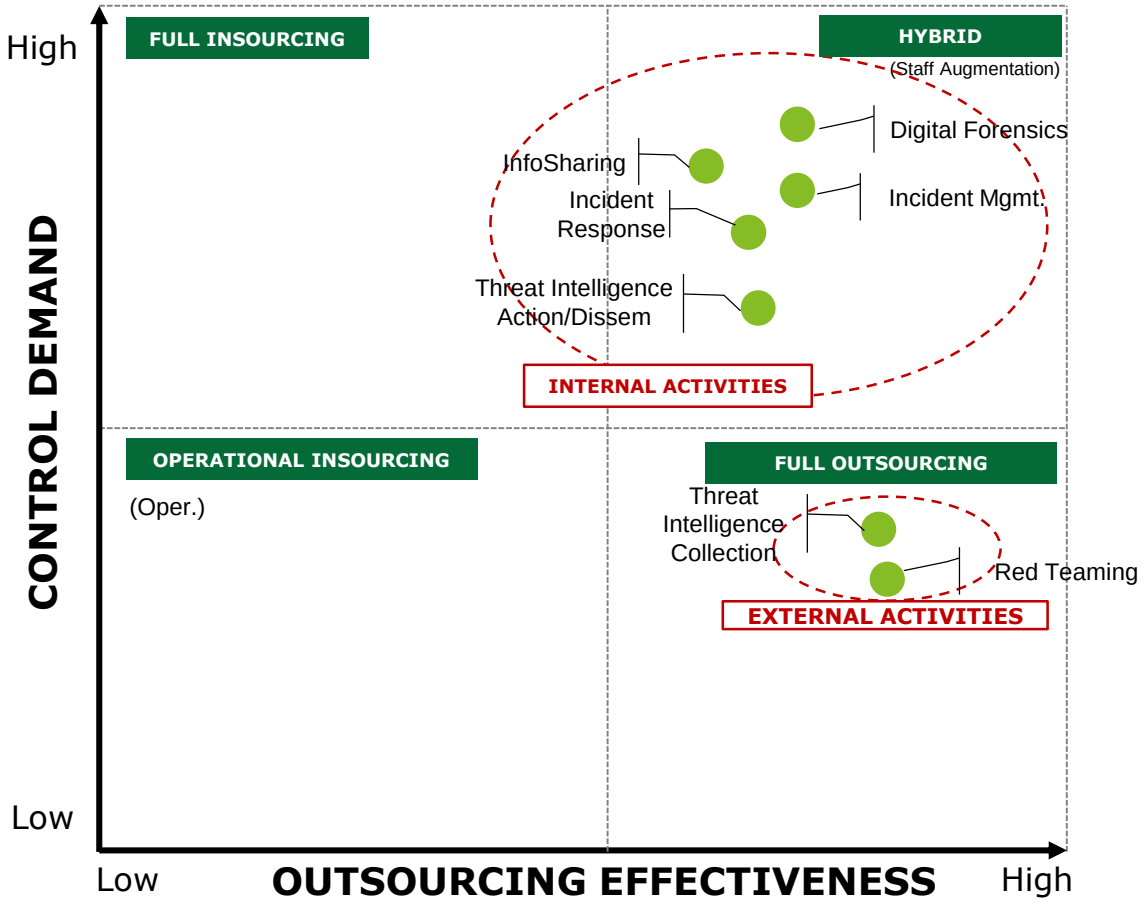


Features:

- The CERT team is progressively increased with introduction of **units** and their respective **Team Leaders**
- Communication with external entities is a manager responsibility. For accreditation processes there is additional support, not represented. Communications and legal skills are borrowed from the responsible offices.
- Working hours are the office ones, but maximum availability is required for Analysts/Incident Handler

CERT Capabilities – Sourcing Model

To provide its services to the Constituency the National CERT must adopt a specific sourcing model



High control by the CERT supported by important skills and experiences of external personnel

Internal Activities

Cyber Incident Response, Digital Forensics, Info Sharing and **Threat Intelligence** (i.e. for analysis and communication) activities require high control but benefit from specialized third-party staff to integrate CERT internal staff.

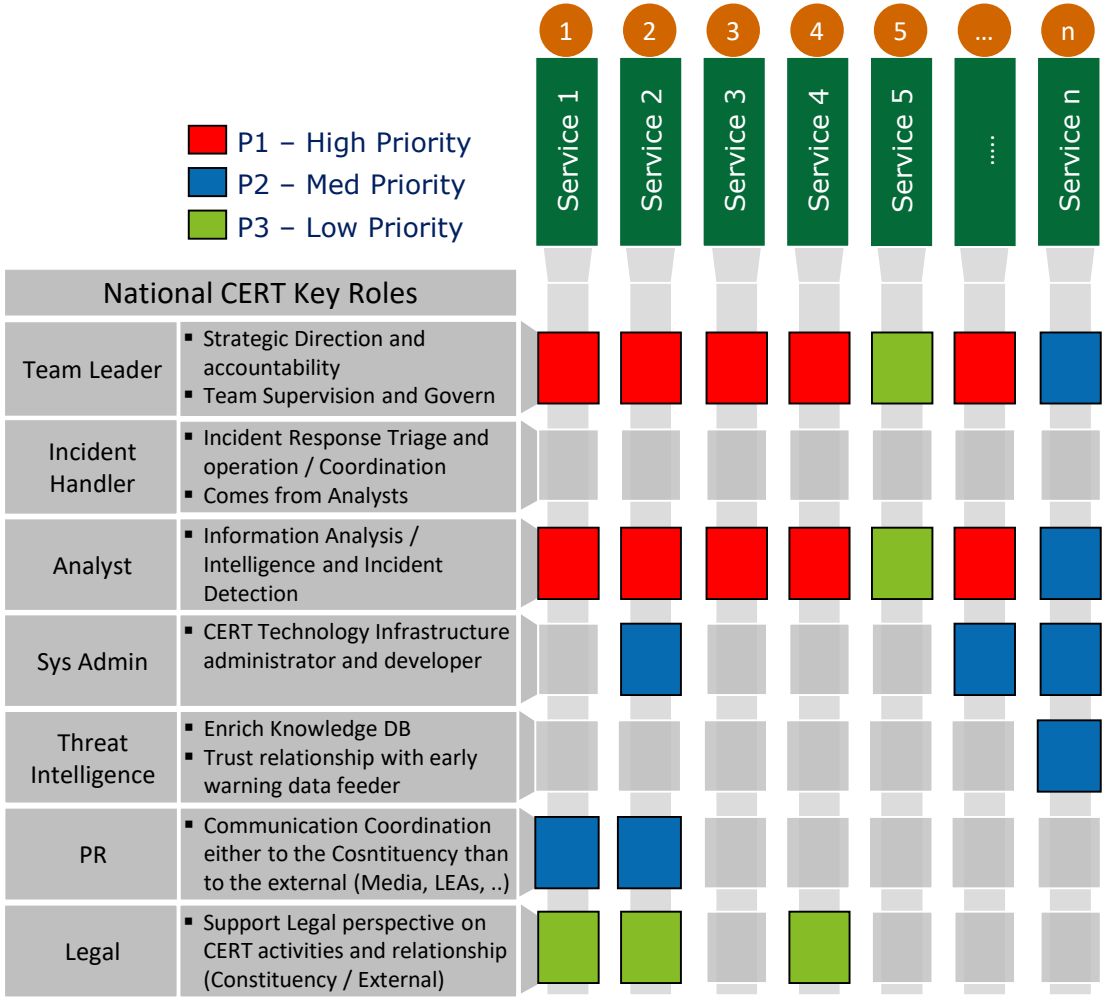
Outsourceable Activities

Cyber Threat Intelligence (data gathering and analysis) and **Red Teaming** require analysts with very specific skills. Conversely they do not require high control. It is therefore possible **to use third parties** to:

- collect information from intelligence sources for preliminary analysis;
- Perform red teaming exercises.

CERT Capabilities – Skills

One of the key pillars for CERT operation is the recruiting of dedicated people with the correct skillset

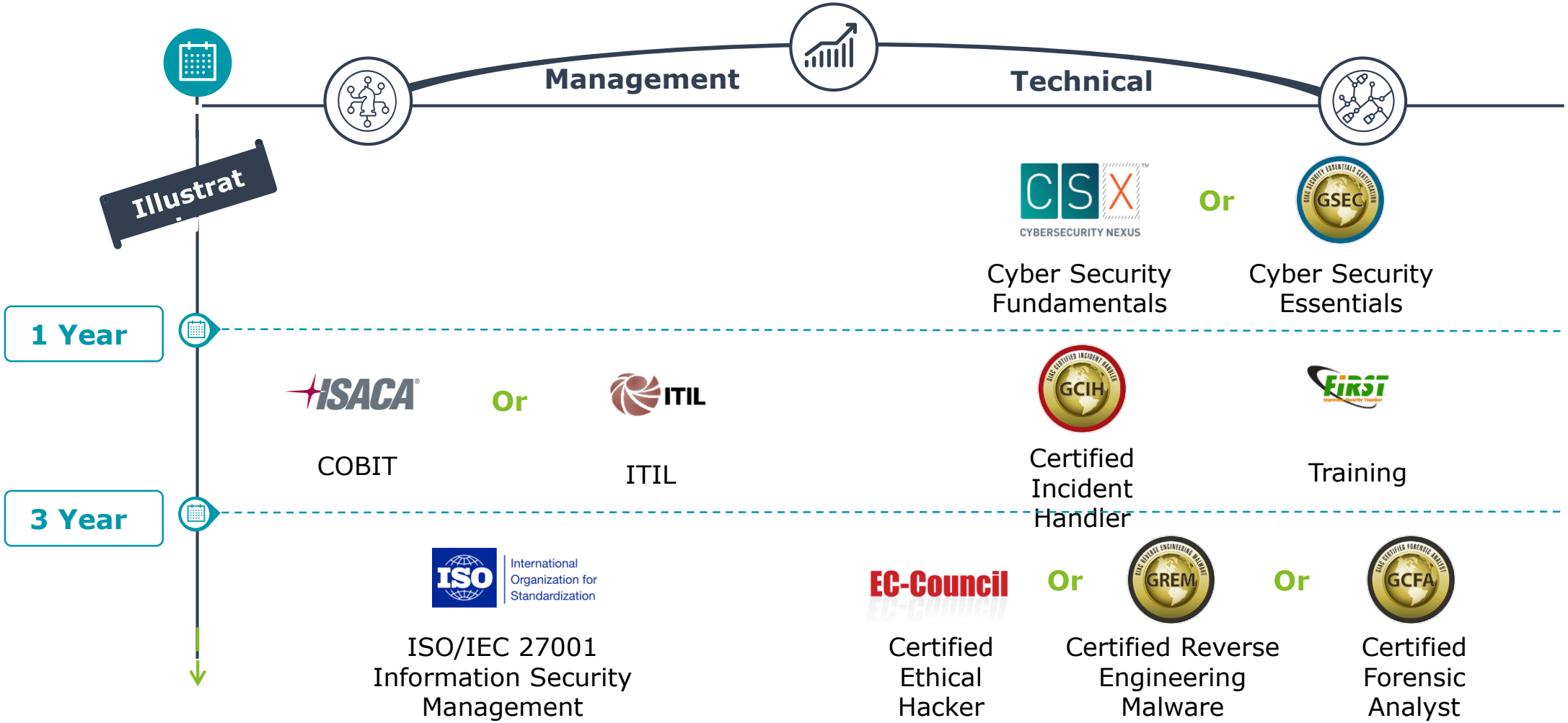


Key People Skillset

- Integrity
- Good Communication
- Diplomacy
- Team builder
- Capability to work under tight schedules
- Problem solving
- Time Management
- Sensitive to weak signals
- Good knowledge of ICT
- Good knowledge of Cyber Security
- Understanding of vulnerabilities (hw/sw/human)
- Network protocols and services
- Cyber Security Countermeasures
- Some skill in software development

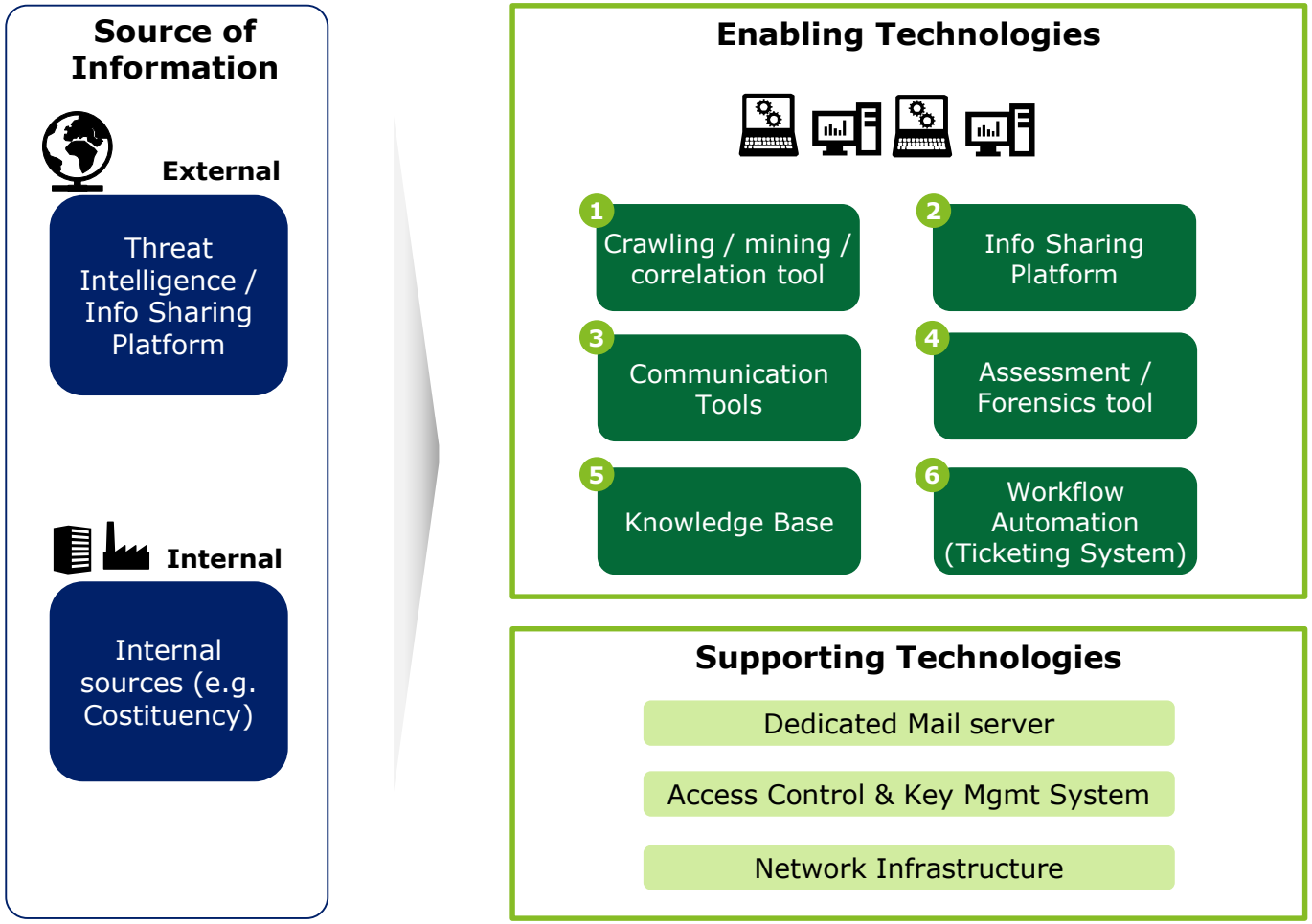
CERT Capabilities – Skills

One of the key pillars for CERT operation is the training the team



CERT Capabilities - Technologies

Likewise, the technologies in use are a fundamental element for a CERT, each component should be easy to use and resilient



Detail

1. **Crawling / mining / correlation tool**
   - Threat Intelligence enabling technologies for Collecting, Searching, and Analyzing Information on Threats, Violations, etc
2. **Dedicated info-sharing Plaforms**
   - Technologies dedicated to the acquisition / exchange of information and their propagation towards security solutions aimed at prevention and monitoring
3. **Secure Communication Tools**
   - Coordination and communication tools with adequate security levels (eg authenticated / encrypted communications)
4. **Assessment / Forensics tools**
   - Technologies supporting investigative activities and Digital Forensic
5. **Knowledge Base**
   - Tools to support analysis and definition of a standard modus operandi
6. **Workflow Automation (Ticketing System)**
   - Technologies to automate and track activities in particular Incident Response ones

CERT Capabilities - Technologies

Likewise, the technologies in use are a fundamental element for a CERT, each component should be easy to use and resilient

The CIRT (Computer Incident Response Team) has sufficient capabilities to respond to incidents. Its main goal is to handle incidents and keep contacts with the constituencies. It acts as main point of contact for all the security-related communications.

CIRT Website

WordPress CMS

- Full-fledged installation with **responsive design,** , SSL certificates, **SEO optimization**
- **Enhanced security** through Fail2ban, bot/hotlink protection,
- **phpList integration**, full analytics, RSS, graphic customization, etc.

Threats and Vulnerability Management

Taranis threat management platform

- Specifically **designed for CERT operations**
- **scans the internet** for texts about digital threats and vulnerabilities
- Designed for **collecting, analyzing, and publishing**

Newsletter Management System

PHPList, open source marketing and mass-mailing platform

- Full, **native integration** with WordPress
- detailed bounce analytics and **automatic throttle calibration** for massive emailing
- **secure authentication** and delivery managed by default

Security Incident Response Platform

Open source incident response automation

- Able to **receive alerts** from multiple sources (SIEM, IDS, MISP),
- **Integration** with other CSOC Tools
- Designed for Cortex tool which gives **increased analysis automation**

CERT Enablers

CERT Enablers

CERTs are supported by three specific communication enablers for ensuring trust, resilience and smoothness under pressure

1 AFFILIATION

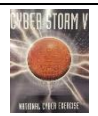
Trusted relationship benefits of the active affiliation to international groups, for leveraging tools, best practices and information

AGENCY	TARGET RECOGNITION LEVEL
enisa	Inclusion in ENISA CERT Inventory
FIRST	Full-Member Affiliation
TI	Trusted Introducer Accreditation
AUTHORIZED TO USE CERT	"Authorized to use CERT" endorsement
OIC-CERT Computer Emergency Response Team	General or Full-Member Affiliation
APCERT Asia Pacific Computer Emergency Response Team	Operational Member

TARGET.

2 EXERCISES

Exercises / Cyber drills are important to define and test communication and its tools and channels

YEAR	E.G. CYBER US EXERCISES
	CS I (2006)
	CS II (2008)
	CS III (2010)
	CS IV (2012)
	CS V (2015)

3 PLATFORMS & STANDARDS

Centralized systems that allow to collect, manage and share data and information. Information need to be formatted according to standards

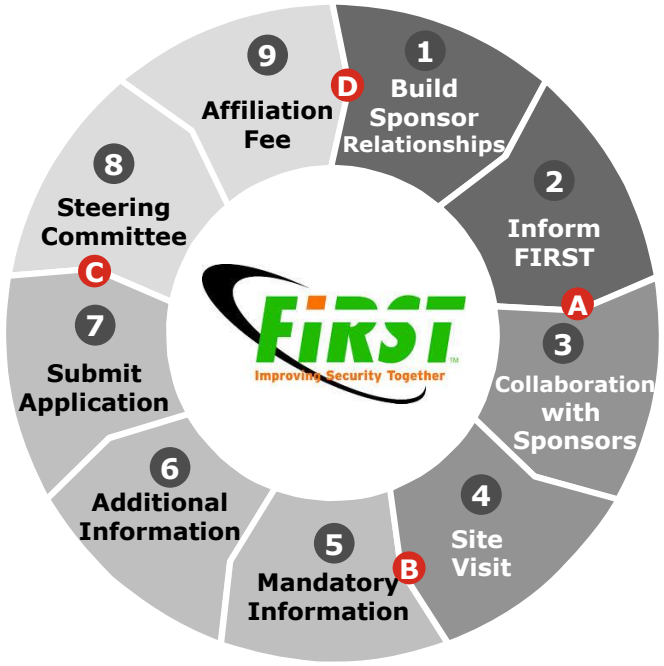
EXAMPLE	DESCRIPTION
STIX	Structured Threat Information eXpression (STIX™)
TAXII	Trusted Automated eXchange of Indicator Information (TAXII™)
CIRCL Computer Incident Response Center Luxembourg	Malware Information Sharing Platform (MISP)
CiSP A CATALYST FOR COLLABORATION	Cyber-security Information Sharing Partnership (CiSP), part of CERT-UK

CERT Enablers - Affiliation

In order to be recognized as a center of excellence, a new National CERT must be accredited to international recognized bodies like FIRST …

1 Affiliation

FIRST Affiliation Process



Process Steps	Key Milestones
1 **Build relationships** with two existing Full Members for nominating your team ("sponsors")	First Informed A
2 **Inform FIRST** Secretariat (FSS) that your team wants to join FIRST. (6-month limit starts here)	
3 **Work with your sponsors** so they have a thorough understanding of your team	Site Visit Completed B
4 **Arrange for a site visit** by at least one sponsor	
5 **Provide all the mandatory information** requested in support to your nomination	Application Submitted C
6 **Provide any additional information** requested by FIRST	
7 Your sponsor will **submit your application** (after a 6-month period, at most).	
8 **Steering Committee** will deliver on your specific nomination	Affiliation Complete D
9 If application is approved, **pay the membership affiliation fee**	

Key Takeaways

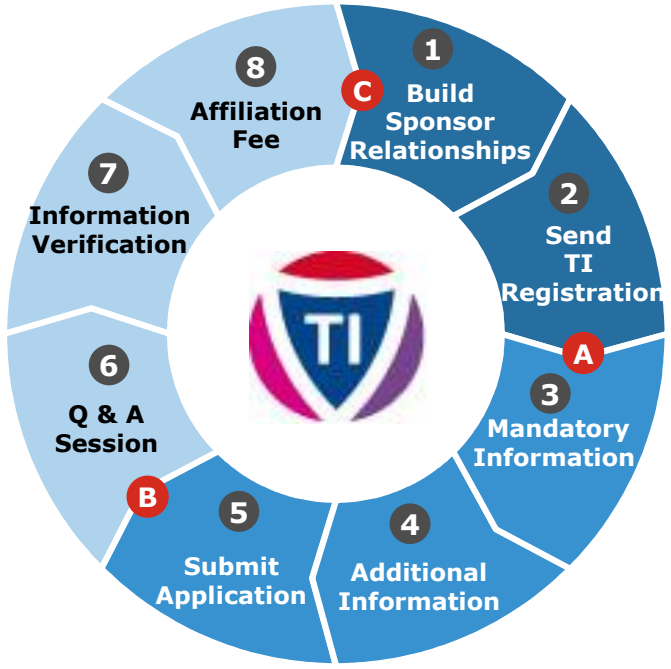
- Provides **instant credibility** to a new CERT
- Allows the new CERT to distinguish its services and to position itself as one of the **firsts CERT in Caribbean area** to achieve FIRST affiliation
- Gives new CERT access to the largest **international information sharing platform** for CERTs
- **Increase new CERT capabilities** to its constituency

Sources: FIRST

CERT Enablers - Affiliation
… and Trusted Introducer (TI)

1 Affiliation

TI Accreditation Process



Process Steps	Key Milestones
1 **Build relationships** with two TI-Accredited Members for nominating your team ("sponsors")	TI-Listing A
2 **Fill out the TI-list** (v23) and send it to TI committee through ti@trusted-introducer.org)	
3 **Provide** all **mandatory information** requested (see Appendix B, Appendix C and RFC2350 document for details)	Application Submitted B
4 **Provide** any additional **information requested** by TI (see Appendix C document)	
5 **Submit** the **application** with all the documents requested	
6 **Support Q&A sessions** with the TI team to discuss issues or questions arising with regards to the provided information, its authenticity or its actuality	TI-Accredited C
7 The **TI team will verify and assess** all the materials that have been sent by the candidate	
8 If the application is approved, **pay the membership affiliation fee**	

Key Takeaways

- Based on lack of site visit and Board Review requirements, the **TI Accreditation process can be accomplished in less time than the FIRST Affiliation process**
- **Strengthens ties** with TI member CERTs
- Access to the **internal knowledge** and to the **out-of-band warning system** of member CERTs of the community

Sources: TI

CERT Enablers - Exercises

In order to enhance its resiliency, a national CERT should define several Cyber Exercises with the aim to test its core processes, tools and resources

2 Exercises

Cyber Wargaming

Cyber Wargaming is an ***interactive technique*** that ***immerses*** potential cyber-incident responders in a ***simulated cyber scenario*** to help CERTs evaluate their ***cyber incident response preparedness***

Cyber wargames drive improvements in cyber resiliency, including:

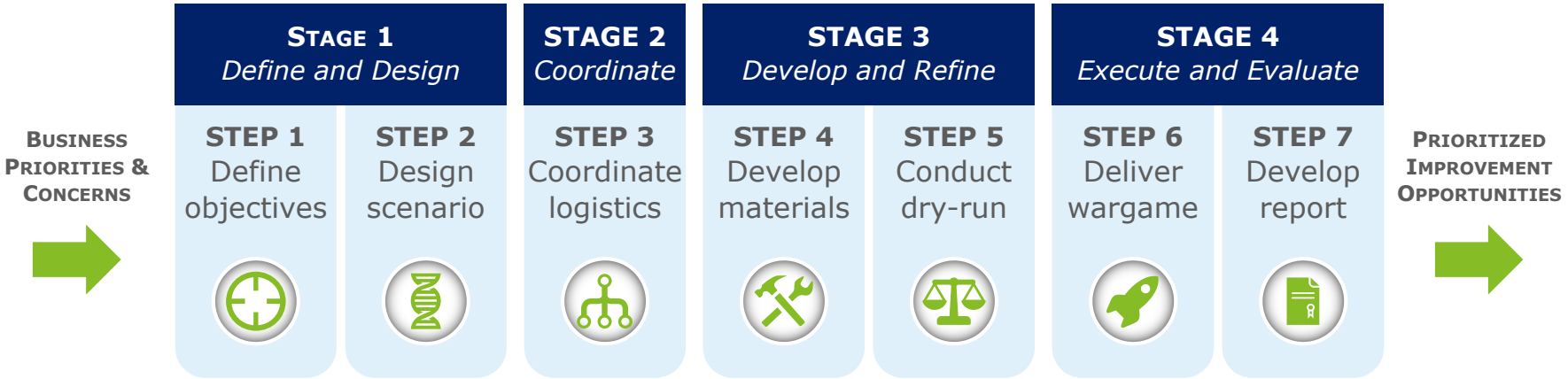
- **Stronger response capabilities** aligned towards mitigating the highest impact risks of a cyber incident
- **Broader consensus** on the appropriate strategies and activities to execute cyber incident response
- **Improved understanding** of the people, processes, data, and tools needed to respond to a cyber incident
- **Better identification of gaps** in cyber incident response people, processes, and tools
- **Enhanced awareness** of the downstream impacts of cyber incident response decisions and actions
- **Tighter integration** between parties likely to be collectively involved in the response to a cyber incident
- **Improved clarity** regarding ownership of authority related to certain key cyber incident response decisions
- **Reduced time-to-response** through the development of cyber incident response "muscle memory"

CERT Enablers - Exercises

Effective Cyber Wargames require precise planning, structured execution, and comprehensive post exercise analysis

2 Exercises

Cyber Wargaming



Cyber Wargaming Toolkit

Methodology	A wargame design and engagement execution methodology informed by military practices, educational research, and experience	**Scenario and Inject Inventories**	An inventory of scenarios, ranging from basic to complex; and inventory of injects including CERT alerts, news articles, social media feeds, news clips, etc.	**Delivery Tools**	Customized tools to enable realistic exercises – including a secure player communications platform, electronic player status placards, and participant polling system
Engagement Artifacts	A library of sample artifacts and templates – including activity checklists, design workbooks, facilitator guides, etc.	**Training Material**	Materials to train cyber wargame facilitators, players, and observers on how to participate effectively in a cyber wargame	**Production Team**	An experienced roster of printers, video producers, etc. to support efficient, secure, and quality production of wargame materials

CERT Enablers - Exercises

The predisposition of a Cyber Range represents a further initiative to enhance national Cyber Security

2 Exercises

Similarities Between Physical and Digital World

Physical Cyber Range

Physical environment where is possible to:

- Test Weapons
- Complete Live Attack and Defense Exercises
- Develop War Tactics, Techniques and Procedures (TTPs)

Digital environment where is possible to:

- Assess Cyber Response Effectiveness
- Assess Cyber Attacks Effectiveness
- Complete Cyber Warfighters Training
- Develop Tactics, Techniques and Procedures (TTPs)

Digital Cyber Range

Cyber Range

Why a Cyber Range?

- Have **highly qualified staff** able to make advanced threats
- Have **environments** to **perform exercises** with potentially catastrophic effects (eg running a malware)
- Have **realistic** environments, that may:
  - Be returned to the baseline for test repetition;
  - Allow configuration changes to test different scenarios.
- Have environments where it's possible to **test TTPs**

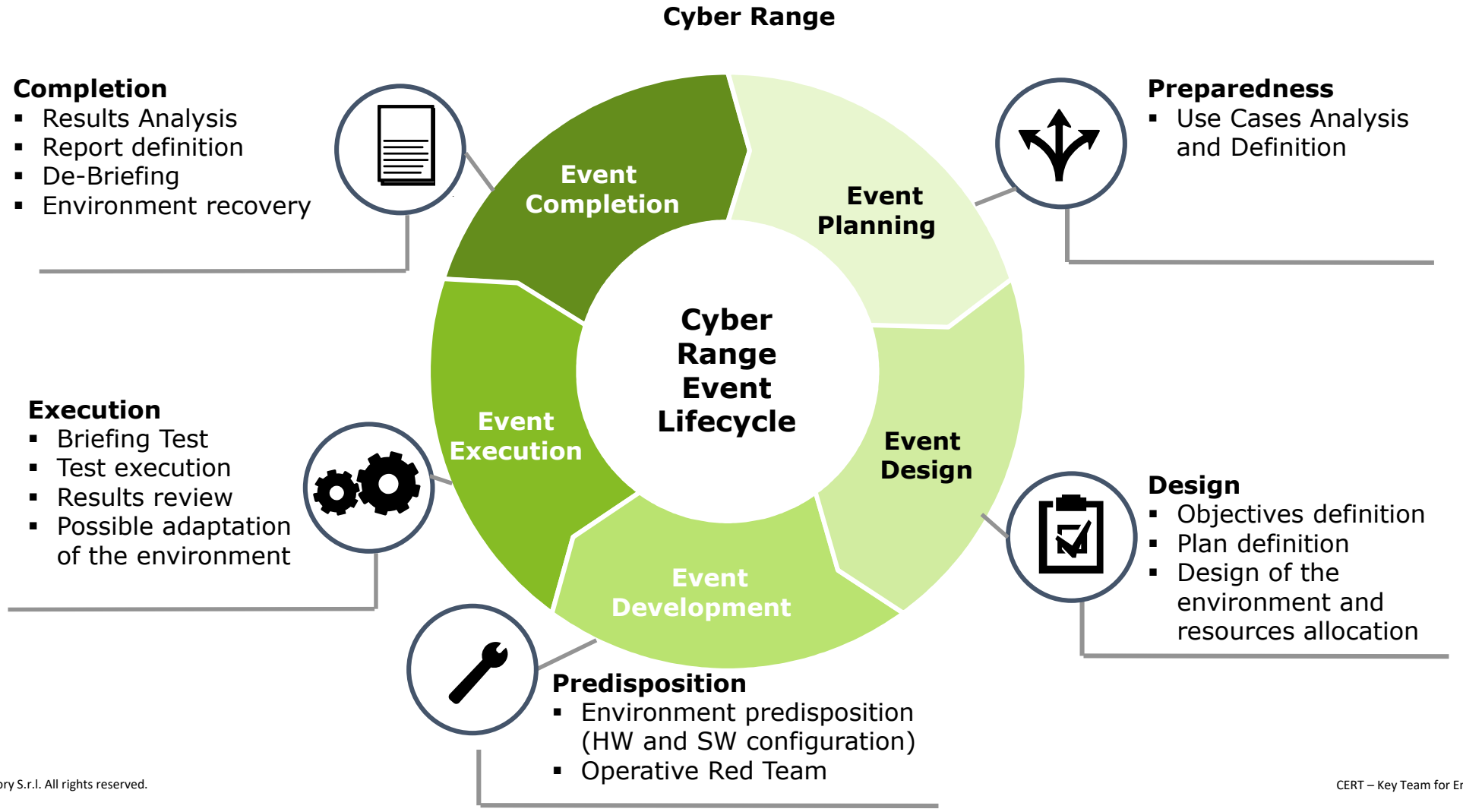
Cyber Range Main Features

- **Rapid emulation** of complex networks and operative environments, to be used by:
  - **Blue force** = Friendly
  - **Red Force** = Adversary
  - Grey Network = Neutral
- Possibility to **complete simultaneous tests** at different levels of classification
- **Improve efficiency** in terms of time:
  - Rapid predisposition of environments
  - Recovery of the environments to their initial state
  - Simple variation of configurations
- **Meeting the needs of different types of users** (Operational Test and Evaluation OT & E, R & D, Solutions and Products Testers ...)

CERT Enablers - Exercises

Each cyber range exercise / test foresees the completion of a predetermined set of five phases

2 Exercises



CERT Enablers – Platforms and Standards

Reporting to international recognized standards facilitates the development of CERT capabilities and credibility

3 Platforms and Standards

Examples of Cyber Security Standards

Typical Domains

1. Information Security Risk Management
2. Software Development and Maintenance
3. Infrastructure Design and Operations
4. HR / Physical Security
5. Identity and Access Management
6. Incident Management
7. Business Continuity Management

CERT Enablers – Platforms and Standards

Deloitte is highly focused in finding the best technologies to support CERT Info Sharing process

Source: Study on European Commision SMART 2014/1079 project performed by Deloitte (2015).

Infosharing Tools	Level of spread (*)
Malware Information Sharing Platform (MISP)	**95,65%**
Request Tracker (RT) – RTIR, AIRT	86,96%
IntelMQ	**42,48%**
Taranis	34,78%
Megatron	26,09%
AbuseHelper	21,74%
Trusted Introducer DB	21,74%
MANTIS Cyber Threat Intelligence Management Framework	8,7%
Information Feed Analysis System (IFAS)	4,35%
N6 – Network Security Incident eXchange	4,35%
Cybergreen Platform	4,35%
Warden	0%
Malware Communications Analyzer (MalCom)	0%
Collective Intelligence Framework (CIF)	0%
Collaborative Research into Threats (CRIT)	0%

(*) Percentage of sample considered.

Comments

- **MISP** (Malware Information Sharing Platform) is the common information sharing platform within CERTs Community;
- Before using an information sharing platform it is paramount to analyse technical and operational requirements.

CERT Implementation Project

CERT Implementation Project

In order to design and implement a CERT, it is required to answer different key questions for each element

CERT SOLUTION

Vertical Capabilities and Expertise

STRATEGY & REFERENCE MODEL

Define overall strategy and direction for CERT development and growing. Planning and design of CERT structure and related capabilities. Ensure alignment with standard and leading practices

Advise

- Vision and Strategy
- Benchmarking and leading practices
- Reference Model and Framework
- Processes and procedures
- Implementation masterplan
- Accreditation and certification
- Tools, software and services selection

TECHNOLOGY ENABLEMENT

Design and implement core technology solutions and platform in order to enable services delivery and capabilities, in alignment with the reference model and overall strategy

Implement

- Info-sharing and communications platforms
- Cyber intelligence and analytics platforms
- Orchestration and service automation
- Detection systems and architectures
- Threat mitigation systems
- Cyber Range

OPERATING SERVICES

Ensuring readiness and timely responses, supporting day-to-day operations, facilitating sourcing of high-specialized components mainly in threat intelligence, incident response and simulation areas

Manage

- Incident Response
- Cyber Threat Intelligence
- Hunting services
- Managed Exercises and Periodic Simulations
- Managed CERT platforms (for smaller CERTs)

Our Credentials

Deloitte delivered multiple capabilities across industries

National CERT – EMEA Region

CLIENT CHALLENGE – The project focused on assisting a State in EMEA Region with a capability to respond to cyber threats. The **establishment** of a **Computer Emergency Response Team** ensured the protection of the government infrastructures, assist in drafting the overall plan on the country's approach to cybersecurity related issues, and thus served as a **focal point** for further **building and implementing** the national culture of cybersecurity

DELOITTE IMPACT

Deloitte achieved the following objectives:

- Improved **national preparedness** on the identification, response and resolution of cybersecurity incidents at identified constituents of the CIRT
- Creation of an **effective and efficient** capability ready to respond to cyber threats
- Increased ability to enact **security measures** and **deploy effective responses** when security incidents occur.

Sectorial CERT – Energy Sector

CLIENT CHALLENGE – Deloitte worked to design and implement the **Global CERT Team**, with the mission to prevent the occurrence of **Cyber Incidents** improving **security controls** and **countermeasures**; detect and analyze incidents to mitigate the impact and reduce/limit future occurrences; coordinate response to incidents engaging both Internal Stakeholder and their related External Counterparties

DELOITTE IMPACT

Deloitte achieved the following objectives:

- Led the **definition** of the **Operating Model** that includes: mission and objectives, services portfolio, organization structure, processes and procedure, team member profile, training program, supporting technologies and tools.
- Define **rolling-out processes** and **technologies** (dealing with more than 60 different stakeholders of 8 countries), **training on the job**, international **affiliations** with 8 National CERTs of the countries where the Group has business operations and with Trusted Communities
- Deliver **managed security services** to support the CERT mission

Corporate CERT – Oil & Gas Sector

CLIENT CHALLENGE – Deloitte worked to **enhance** the Global Cyber Intelligence capabilities of the client, to effectively prevent and respond to cyberattacks to the Oil & Gas sector by **identifying strategy** and **operating models** and **methodologies** to identify threat scenarios and carry out red teaming and cyber tabletop exercises

DELOITTE IMPACT

Deloitte achieved the following objectives:

- Assessment of **security capabilities** of Cyber Intelligence, Incident Response, Information Sharing and Cyber Forensic team
- **Strategy definition** for building the capabilities in term of process, people and technologies and **plan and budget estimation** for the implementation
- Support for the **preparation of playbooks** to support cyber threat intelligence analysis
- **Identification** and **formalization** of interaction criteria and **communication models** with internal and external Stakeholders

Deloitte.

Important notice

This document has been prepared by Deloitte Risk Advisory S.r.l. (as defined below) for the sole purpose of providing a proposal to the parties to whom it is addressed in order that they may evaluate the capabilities of Deloitte RA to supply the proposed services.

The information contained in this document has been compiled by Deloitte RA and includes material which may have been obtained from information provided by various sources and discussions with management but has not been verified or audited. This document also contains confidential material proprietary to Deloitte RA. Except in the general context of evaluating our capabilities, no reliance may be placed for any purposes whatsoever on the contents of this document or on its completeness. No representation or warranty, express or implied, is given and no responsibility or liability is or will be accepted by or on behalf of Deloitte RA or by any of its partners, members, employees, agents or any other person as to the accuracy, completeness or correctness of the information contained in this document or any other oral information made available and any such liability is expressly disclaimed.

This document and its contents are confidential and may not be reproduced, redistributed or passed on, directly or indirectly, to any other person in whole or in part without our prior written consent.

This document is not an offer and is not intended to be contractually binding. Should this proposal be acceptable to you, and following the conclusion of our internal acceptance procedures, we would be pleased to discuss terms and conditions with you prior to our appointment.

CERT Capabilities – Technologies Detail Cards (1/6)

It is necessary to adopt solutions that support the collection and analysis of intelligence data

1 Crawling / mining / correlation tool

Key Technology

Description

- **Data collection** on hosts, compromised domains and websites, malicious payloads, and IP addresses associated with malicious activity
- Ability to **collect** and **aggregate** data from different sources and formats (CSV, STIX, Custom XML.JSON, IODEK, OpenIOC, email)
- Ability to **correlate** the collected data
- Support the threat indicator **content analysis** and the evaluation of the contents' relationships
- Standard support like STIX TAXII

Enabled / Supported Processes

	Process		Reason
1	CYBER THREAT INTELLIGENCE	✓	Crawling / mining / correlation solutions allow to gather and correlate information from multiple sources
2	CYBER INCIDENT RESPONSE	✓	Violations identified on the Internet are an input to the Incident Response process
3	DIGITAL FORENSICS		
4	INFORMATION SHARING	✓	The information obtained about threats and vulnerabilities is shared with the internal functions for prevention and monitoring action

Main Vendors

- Symantec. – Threat Intel
- LOOKINGGLASS – X-Force
- IBM – OTX
- ALIEN VAULT – Threat Intell + ISight
- FireEye – idefence
- VERISIGN – First Watch
- RSA – CIC - TIA
- Deloitte. – Falcon Intelligence
- CROWDSTRIKE

CERT Capabilities – Technologies Detail Cards (2/6)

Info-sharing platforms allow to promptly receive / exchange information on threats and vulnerabilities …

2 Info-sharing Platforms

Key Technology

Description

- Information sharing on threats like botnet, DoS/DDoS attacks, malware types, 0-days
- **IOC database** with examples of IOC for malware, incidents, threat-actors, intelligence
- **Automatic correlation** between attributes and indicators for malware, attack campaigns, events and known incidents
- **Storing events** and **attributes / indicators** in structured formats (STIX TAXII)
- Injection directly into security solutions for readable machine data

Enabled / Supported Processes

	Process		Reason
1	CYBER THREAT INTELLIGENCE	✓	The info-sharing platforms constitute a valid source of information for the CTI process
2	CYBER INCIDENT RESPONSE	✓	Among shared information there is the one related to the incident. The goal is to respond quickly to that incident
3	DIGITAL FORENSICS		
4	INFORMATION SHARING	✓	Info-sharing platforms are a support tool to increase the effectiveness of the information shared

Main Vendors

MISP Threat Sharing

IT ISAC Information Sharing and Analysis Center

CSP A CATALYST FOR COLLABORATION

US-CERT UNITED STATES COMPUTER EMERGENCY READINESS TEAM AIS Platform

CERT Capabilities – Technologies Detail Cards (3/6)

... and the adoption of secure communication mechanisms reduces the risk of information disclosure

3 Secure Communication Tools

Key Technology

Description

- **Encryption** of **communication channels**
  - Instant Messaging
  - Calls,
  - Video Calls
  - Video Conference
  - Email
- **Encryption** of **attachments**
- Document Sharing Systems

Enabled / Supported Processes

	Process		Reason
1	CYBER THREAT INTELLIGENCE		
2	CYBER INCIDENT RESPONSE	✓	The availability of secure communication channels allows to exchange information by reducing the risk of information leakage
3	DIGITAL FORENSICS		
4	INFORMATION SHARING	✓	The availability of secure communication channels allows to exchange information by reducing the risk of information leakage

Main Vendors

OpenPGP, Cisco webex, BlueJeans VIDEO CONFERENCING, WhatsApp, GoToMeeting by CITRIX, privatewave secure communication solutions, silent circle, Signal

CERT Capabilities – Technologies Detail Cards (4/6)

The tools for performing assessments and forensics support the development of CERT's investigative capabilities

4 Assessment / Forensics tool

Key Technology

Description

- **Information management**: data identification, preservation
- **Data collection**, processing, review
- **Text-based** researches
- Identifying potential **custodians** and **sources** of information
- **Integration** with e-mail, ECM and cloud based storage
- **Data analytics**

Enabled / Supported Processes

	Process		Reason
1	CYBER THREAT INTELLIGENCE		
2	CYBER INCIDENT RESPONSE	✓	Forensic analysis tools help to improve the effectiveness of incidents post-mortem analysis
3	DIGITAL FORENSICS	✓	Forensic analysis tools allow you to complete collection and acquisition activities keeping safeguarding the integrity
4	INFORMATION SHARING		

Main Vendors

GUIDANCE SOFTWARE, RECOMMIND, Kroll Ontrack, CounterTack, LogRhythm, exterro, FTI CONSULTING TECHNOLOGY, ZyLAB

CERT Capabilities – Technologies Detail Cards (5/6)

CERT must also have a repository that contains information about threats, incidents and related solutions

5 Knowledge Base

Key Technology

Description

- **Access** to content based on roles and principles of **"need-to-know" and "least-privilege"**
- Highly **agile** search for content
- **Ready-to-use** content
- **Work instructions** and **how-to guide** to handle incidents
- Tracking of **Techniques**, **Tactics** and **procedures**

Enabled / Supported Processes

	Process		Reason
1	CYBER THREAT INTELLIGENCE	✓	KB is supporting the CTI process to quickly store and retrieve information
2	CYBER INCIDENT RESPONSE	✓	The KB constitutes the archive of past events and the repository for the documentation required to handle incidents
3	DIGITAL FORENSICS	✓	The availability of a readily obtainable information store facilitates and supports investigative activities
4	INFORMATION SHARING	✓	The availability of easily obtainable information facilitates analysis activities and correlations with historical data

Main Vendors

IBM, Microsoft, MediaWiki, tiki, Alfresco, DokuWiki, OpenText, BlueSpice for MediaWiki

CERT Capabilities – Technologies Detail Cards (6/6)

The adoption of an automation workflow tool then increases CERT incident handling capabilities

6 Workflow Automation (Ticketing System)

Key Technology

Description

- Support for **automation of process workflows**, actors, and tasks
- **Templates** for the management of known incidents based on past occurrences
- Support for **custom play-book** definition for incident response activities
- **Integration** with threat intelligence, forensic and SIEM solutions
- Event **historicization**

Enabled / Supported Processes

	Process		Reason
1	CYBER THREAT INTELLIGENCE		
2	CYBER INCIDENT RESPONSE	✓	The workflow automation tool supports Incident Response management effectively and efficiently
3	DIGITAL FORENSICS	✓	The workflow tool is an activity tracing tool
4	INFORMATION SHARING	✓	The workflow tool is an activities tracing tool

Main Vendors

DFLABS, RSA SecOps, HEXADITE, resilient an IBM Company, CYBERSPONSE, RESOLUTION1 SECURITY