Catalogue of EATM-CERT Services

Edition: 2.0
Edition date: 13-03-2020
Classification: WHITE
Reference nr: SRV00-Catalogue of EATM-CERT Services

DOCUMENT CONTROL

Document Title	Catalogue of EATM-CERT Services
Document Subtitle	This field is automatically updated
Document Reference	SRV00-Catalogue of EATM-CERT Services
Edition Number	2.0
Edition Validity Date	13-03-2020
Classification	WHITE
Status	Released Issue
Author(s)	Patrick MANA NMD/INF/IAC
Contact Person(s)	Patrick MANA NMD/INF/IAC

APPROVAL TABLE

Authority	Date	Signature
Prepared by: EATM-CERT Team	13/03/2020	
Reviewed and endorsed by: Patrick MANA	13/03/2020	
Approved by: Iacopo PRISSINOTTI	17/03/2020	

EDITION HISTORY

Edition No.	Validity Date	Author(s)	Reason
1.0	11/09/2017	Patrick MANA	First Version
2.0	13/03/2020	Patrick MANA	Update of EATM-CERT services

TABLE OF CONTENT

TABLE OF FIGURES

No table of figures entries found.

TABLE OF TABLES

INTRODUCTION

This Service Catalogue sets out core services available to the European ATM Stakeholders (the EATM-CERT constituents). It provides an overview of EATM-CERT services and specifies information to be shared between EATM-CERT and the 'User' to start operational cooperation. Where appropriate, it provides links or references for useful documents and webpages. The services are based on the typical CERT services as documented by ENISA[1] and CERT Coordination Center[2].

For each service / product, constituents will find:

- Summary description: a few words describing the service / product;
- Service access: key information for accessing or triggering the service.

Cooperation: Constituents are encouraged to notify EATM-CERT with feedback on the services to improve them and to feed in information about supplementary areas of interest.

Background

EUROCONTROL has set up the European Air Traffic Management Computer Emergency Response Team (EATM-CERT) early 2017. Its constituency is composed of EUROCONTROL services, systems and products as well as, on a voluntary basis, ATM/aviation Stakeholders (Air Navigation Service Providers (ANSPs), Airport Operators (AOs) and Airspace Users (AUs)) of the EUROCONTROL Member and comprehensive agreement States.

EATM-CERT's mission is to support the European ATM/aviation Stakeholders to protect themselves against intentional and malicious cyber-attacks that would hamper the integrity of their IT assets and harm ATM service provision. The scope of EATM-CERT's activities covers prevention, detection, response and recovery.

General information

Contact

EATM-CERT

Address: EUROCONTROL EATM-CERT –

Rue de la Fusée, 96 - 1130 Bruxelles

Phone: +32.2.729.46.55

Website:
https://www.eurocontrol.int/service/european-air-

Constituent (info required)

- ✓ Physical/postal address
- ✓ Contact person name / phone / email
- ✓ Functional mailbox for alerts and incident response

[1] https://www.enisa.europa.eu/activities/cert/support/guide2/introduction/possible-services

[2] http://www.cert.org/incident-management/services.cfm

traffic-management-computer-emergency-response-team

Email: eatm-cert@eurocontrol.int

Security & Privacy

EATM-CERT	Constituent (info required)
PGP KeyID: 0xADCE88E4	✓ PGP KeyID
PGP FP: 1AEC 6983 1356 472E 422A 2BC2 B4BA B640 ADCE 88E4	✓ PGP FP

For information about EATM-CERT, how to become a constituent, how to work with EATM-CERT, you can also contact:

Patrick MANA

patrick.mana@eurocontol.int

Tel: +32.2.729.30.56

Mobile: +32.499.94.23.93

1 Services categories

EATM-CERT services are grouped into four categories:

- **Intelligence services**: These services help constituents improve their (cyber) security posture thanks to lessons learned from others, strategic, operational, tactical information collected about threats and potential or actual incidents or attacks. Performance of these services will directly reduce the number of incidents in the future.

- **Incident Response services**: These services are triggered by an event or request, such as a report of a compromised host, widespread malicious code, software vulnerability, or something that was identified by an intrusion detection or logging system. Reactive services are the core component of CERT activities.

- **Proactive services**: These services provide assistance and information to help prepare, protect, and secure constituent systems in anticipation of attacks, problems, or events. These services augment existing and well-established services that are independent of incident handling and are traditionally performed by other areas of an organization such as the IT, audit, or training departments. If the CERT/CSIRT performs or assists with these services, the CSIRT's point of view and expertise can provide insight to help improve the overall security of the organization and identify risks, threats, and system weaknesses. Performance of these services will directly reduce the number of incidents in the future.

- **Competence services**: These services increase staff awareness and understanding of cyber security best practices, challenges, … . Performance of these services will indirectly contribute to improve the cyber security posture.

EATM-CERT services, though free of charge for its constituents, can be subject to an Agreement.

- Minimum requirement: conditions and mutual obligations of 'Service provider' (EATM-CERT) and 'User' as described in the Agreement;
- General access conditions: as described in the Agreement.

The following services of common interest are provided to all ANSPs, AOs and AUs of EUROCONTROL Member and comprehensive agreement States at no extra cost:

Intelligence services:

- Announcements and Advisories;
- Alerts and warnings;
- Cyber Threat Intelligence and feeds;
  - Aviation Quarterly Cyber Threat landscape report for senior management;
  - EATM-CERT map of publicly reported cyber events impacting aviation;
  - Fraudulent websites impersonating aviation stakeholders;

  - CTI and feeds distributed via Announcements, Advisories, Alerts and Warnings;
  - MISP (Malware Information Sharing Platform);
  - Dark/Deep Web researches;
- Credential leaks detection.

Incident Response services:

- Artefact analysis and actions;
- Scams impersonating EUROCONTROL staff;
- Incident response support and coordination (remote);
- Incident response and analysis (remote):
  - Forensic evidence collection;
  - Tracking or tracing;

Proactive services:

- Security assessments:
  - Infrastructure & Best Practices review;
  - Penetration testing;
  - Vulnerability watch;
  - Vulnerability scanning;

Competence services:

- Phishing awareness campaigns;
- Awareness building.

✓ General access conditions: functional mailbox (FMB), PGP key, IP/ASN range.

Other services can be provided by EATM-CERT to its constituents under specific agreements captured in an Agreement and not free of charge:

Competence services:

- Education/Training (others than IANS training).

2 Intelligence services

2.1 Announcements and Advisories

This service includes, but is not limited to, vulnerability warnings and security advisories. Such announcements inform constituents about new developments with medium to long-term impact, such as newly found vulnerabilities or intruder tools/tactics. Announcements enable constituents to protect their systems and networks against newly found problems before they can be exploited.

This service also includes reports (including White papers) to take stock of lessons learnt in past cyber-security events or incidents and to recommend approaches to prevent future problems.

Finally, this service also provides constituents with a comprehensive and easy-to-find collection of useful information that aids in improving security. Such information might include:

- reporting guidelines and contact information for EATM-CERT;
- archives of announcements;
- documentation about best practices;
- general cyber-security guidance and checklists;
- information that can improve overall security practices.

Purpose: This service aims to raise awareness and improve the preventive security controls as well as the cyber resilience of the constituent in order to protect their systems and networks against cyber-attacks. Intended use of this information is for medium to long term actions.

Service access

- Specific products: Advisories, EATM-CERT reports (including White papers) and web portal (https://www.eurocontrol.int/service/european-air-traffic-management-computer-emergency-response-team).
- Channel: EATM-CERT Web Portal, EATM-CERT Sharepoint (OneSKy), Email distribution, MISP.
- Information required: Email address (access to Web Portal and recipient of email reports).

2.2 Alerts and Warnings

This service involves disseminating information that describes an imminent or on-going cyber threat targeting the User and includes, but is not limited to, information about a threat actor, threat campaign, malware, high impact vulnerability specific to your infrastructure as well as any short-term recommended course of action for dealing with the resulting problem. The alert or warning is sent as a reaction to the identified cyber threat to notify constituents of the activity and to provide specific guidance for protecting their systems or recovering any systems that were affected. Information may be created by EATM-CERT or may be redistributed from vendors, other CERTs or security experts, or other parts of the constituency.

Purpose: This service aims to inform the constituent about an imminent or on-going cyber threat in order to minimize reaction and recovery time and ultimately reduce or eliminate any impact. Intended use of this information is for short term actions.

Service access

- Specific products: Alerts and Warnings
- Channel: Email distribution, Phone communication
- Information required: FMB (where alerts should be forwarded to), emergency phone number, PGP key, ASN/IP range, Internet domains owned, Technologies employed, email address domain.

2.3 Cyber Threat Intelligence and feeds

EATM-CERT provides various types of Cyber Threat Intelligence (CTI) and feeds in real-time to its constituents. CTI and feeds help constituents better learning from attacks experimenting by other organisations from aviation as well as other domains of activity.

There are various types of information that will be shared:

- **Cyber-intelligence** - (threat landscape, intelligence about cyber threat actors' capability and intent): this can be sensitive and there can be restrictions (Traffic Light Protocol (TLP) [3] markings can help with sharing to some extent).
- **Indicators of Compromise (IoCs)** - these can be shared as they are not related to individual systems/services (TLP (Traffic Light Protocol) still to be used). IOCs are e.g. malicious IP@, malicious URL, Malware hash. Sharing this information will help others protect themselves; similarly, receiving this information from others will help entities better protect their systems/services. There is no need to further disclose who has discovered them (be it ANSP A or ANSP B or Airport Operator C or Airport Operator D or Airspace User E or Airspace User F, etc…) as it does not add any value.
- **Tactics, Techniques and Procedures (TTPs)** - (scenarios of attacks, preferred methods used by hackers): this information can be shared (TLP still to be used) as it is usually not related to particular systems/services.
- **Vulnerabilities:**
  - As user of an item: the only interesting information to be shared is about the item (HW, SW, service, protocol, standard, etc.) for which the vulnerability was found, not about who is using it. Therefore, this information can be shared with others to help them protect themselves. The owner of the item has to propose a patch/fix. No need to further disclose who has discovered the vulnerability.
  - As an owner/manufacturer of an item: if an entity produces software systems, then usually item owners share the vulnerabilities with the users of this item. Best practices are to share these vulnerabilities with CERTs (National or sectorial) to allow CERTs to better manage incident response where the item is involved.
- **Incident reports** - TLP and de-identification can be used to share some aspects of incidents, while some incidents may be excluded from sharing.
  - serious incidents: National/Regional mandatory reporting to Competent Authorities applies to this category of incidents e.g. as per general cybersecurity and data protection regulations such as the European Union General Data Protection Regulation (GDPR) or Critical Infrastructures National or Regional regulations (e.g. NIS Directive for the European Union). Consequently, there can be some restrictions in sharing reports about those incidents. However, some aspects e.g. IOCs can be shared (de-identified); and
  - non-serious incidents: can be shared (de-identified).

The products of this Service are:

- Aviation quarterly cyber threat landscape report for senior management;
- EATM-CERT map of publicly reported cyber events impacting aviation: here;
- Fraudulent websites impersonating aviation stakeholders (airlines, airports);
- EATM-CERT Twitter account: @EATMCERT;
- CTI and feeds (vulnerabilities; Indicators of Compromise (IoCs); Tactics, Techniques and Procedures (TTPs));
- Information collected on the Dark/Deep web– examples are:
  - Compromised accounts;
  - Vulnerabilities of aviation systems known to attackers and potential intent to exploit them;
  - Sensitive documents leaks;
  - Fraudulent information e.g. frequent flyer miles for sale;
  - Activities and developments (e.g. new TTPs, new targets) of APTs (Advanced Persistent Threats), cyber-crime, hacktivists, …

These CTI and feeds are obtained by a mix of:

- EATM-CERT intelligence capabilities based on:
  - OSINT (Open Source Intelligence);
  - searches on Dark/Deep web);
- Aviation stakeholders sharing their CTI and feeds (directly or through aviation related ISACs (Information Sharing and Analysis Centres) or equivalent);
- National cyber security centres;
- Non-aviation sectorial CERTs or ISACs;
- CTI vendors feeds purchased by EATM-CERT via contractual relationships.

This non-intrusive Service does not require modifications to the EUROCONTROL or constituents IT infrastructure.

Some products of the Service needs a contribution of constituents as a list of information (e.g. IP@s, URLs, domain names, brands, Hardware and Software technologies) is needed to filter and sort out CTI being relevant to a constituent.

MISP: The distribution of some CTI and feeds can be supported by automated means such as MISP (Malware Information Sharing Platform). The procedure to connect EATM-CERT MISP is described in EATM-CERT document "GDL05-MispConnectionGuideline".

The information provided by this Service will be primarily in English. However, EATM-CERT provides also some CTI, especially OSINT, in other languages.

Purpose: This service aims to inform constituents about relevant Cyber Threat Intelligence and feeds.

Service access

- Agreement for some aspects
- Channel: MISP, Email distribution, Phone communication, Twitter
- Information required: FMB (where alerts should be forwarded to), email address, key assets.
- Systematic use and conformance to TLP marking

2.4 Credential leaks detection

EATM-CERT provides to its constituents a service to detect leaks of credentials associated to domain name(s) as well as IP address ranges and personal email addresses.

These leaks are obtained by continuously monitoring the Surface Web, Deep Web and Dark Web in order to identify public or private information about leaks of credentials used to access any kind of website.

The Service will need a contribution of constituents as a list of domain names to be monitored is needed to filter and sort out leaks relevant to a constituent.

EATM-CERT manages this service but each constituent has full access to its own leaks via a user account. Information access can be automated through the use of an API.

The procedure to benefit from this Service is described in EATM-CERT document "GDL06-SpyCloud LeakDetectionServiceGuideline".

Purpose: This service aims to inform a constituent about credential leaks related to its domain name(s).

Service access

- Agreement
- Specific products: Alerts
- Channel: User account, email
- Information required: FMB (where alerts should be forwarded to), email address, domain name(s).

3 Incident Response services

3.1 Artefact analysis and actions

EATM-CERT performs or supervises the performance of a technical examination and analysis of artefacts found on a compromised system. The analysis might include identifying the file type and structure of the artefact, comparing a new artefact against existing artefacts or other versions of the same artefact to see similarities and differences, or reverse engineering or disassembling code to determine the purpose and function of the artefact. This service also involves sharing and synthesizing analysis results and response strategies pertaining to an artefact with other researchers, CERTs, vendors, and other security experts. Activities also include maintaining a constituent archive of known artefacts and their impact and corresponding response strategies. EATM-CERT determines the appropriate actions to detect and remove malware from a system based on identified malware, as well as actions to prevent malware from being installed. This may involve creating signatures that can be added to antivirus software, IDS etc. or security controls to prevent similar cyber incidents.

Purpose: This service aims to provide technical expertise and experience in the identification of a potentially malicious artefact in order to offer recommendations for prevention and detection.

Service access

- Agreement
- Channel: EATM-CERT Web Portal, Email
- Data protection notification and privacy statement.

3.2 Protect constituents against scams impersonating EUROCONTROL staff

EATM-CERT is supporting aviation stakeholders to fight fraudulent emails impersonating EUROCONTROL staff requesting to pay undue invoices.

The main actions consist in:

- Collecting the original email received by the stakeholder as evidence required to further proceed;
- Requesting the suspension of the fraudulent domain names to ensure that they cannot be used anymore by the fraudsters;
- Communicating the fraud cases to Europol; and
- Contacting the banks that are being used by the fraudsters.

Purpose: This Service aims to protect aviation stakeholders from scams impersonating EUROCONTROL staff.

Service access

- Specific products: domain take down, report
- Channel: Email distribution, Phone communication, MISP (fraudulent domains)
- Information required: FMB (where alerts should be forwarded to), email address.

3.3 Incident response support and coordination (remote)

EATM-CERT assists and guides the victim(s) of the attack in recovering from an incident via virtual crisis room, phone, email, fax, or documentation on a best effort basis. This can involve technical assistance in the interpretation of data collected, providing contact information, or relaying guidance on mitigation and recovery strategies. It does not involve direct, on-site incident response actions. EATM-CERT provides guidance remotely so that site personnel can perform the recovery themselves.

EATM-CERT also provides advisory support to better coordinate the response effort among parties involved in an incident. This usually includes the victim of the attack, other sites involved in the attack, and any sites requiring assistance in the analysis of the attack. It may also include the parties that provide IT support to the victim, such as Internet service providers, other CERTs, and system and network administrators at the site. The coordination support may involve collecting contact information, notifying sites of their potential involvement (as victim or source of an attack), collecting statistics about the number of sites involved, and facilitating information exchange and analysis. The support work may involve notification and collaboration with an organization's legal counsel, human resources or public relations departments. It could also include, with the consent of the affected party, engaging with law enforcement.

Purpose: This service aims to assist the constituent when faced with a cyber incident by providing response and recovery procedures as well as contacts for quicker and more efficient resolution.

Service access

- Agreement
- Alerts/Incidents should be reported to eatm-cert@eurocontrol.int
- The following minimum information should be provided in the initial message: name of victim organisation, local cyber-security incident response contact details (email address, phone), date/time of detection, type of cyber-security incident, actions taken.
- Further information may be asked during the procedure.

3.4 Incident response and analysis (remote)

The purpose of the analysis is to identify the scope of the cyber-security incident, the extent of damage caused by the cyber-security incident, the nature of the incident, and available response strategies or workarounds. EATM-CERT helps to analyse the affected systems and conduct the acquisition of the systems. Incident response support can be provided by telephone or email.

In case of a request coming from the affected ATM Stakeholder, EATM-CERT team members would travel to the site and perform the response activities in alongside the local team (the context of such intervention will be defined as part of the Agreement between EATM-CERT and its constituents on an ad-hoc individual basis).

EATM-CERT may use the results of vulnerability and artefact analysis to understand and provide the most complete and up-to-date analysis of what has happened on a specific system. EATM-CERT correlates activity across incidents to determine any interrelations, trends, patterns, or intruder signatures. Sub-services that may be offered as part of incident analysis are:

- **Forensic evidence collection**: EATM-CERT supports the local team or carries out the collection, preservation, documentation, and analysis of evidence from a compromised computer system to determine changes to the system and to assist in the reconstruction of events leading to the compromise. Tasks involved in forensic evidence collection include (but are not limited to):
    - Making a bit-image copy of the affected system's hard drive; gathering volatile data of affected system (RAM image, running processes, open network connections etc.),
    - Checking for changes to the system such as new programs, files, services, and users;
    - Looking at running processes and open ports via memory forensic analysis; and
    - Checking for Trojan horse programs and toolkits.
- **Tracking or tracing**: EATM-CERT supports the tracing of the origins of an intrusion or identifying systems to which the intruder had access. This activity might involve tracking or tracing how the intruder entered the affected systems and related networks, which systems were used to gain that access, and what other systems and networks were used as part of the attack. This work might be done alone but usually involves working with relevant public authorities, Internet service providers, or other involved organisations.

Purpose: This service aims to assist the constituent when faced with a cyber incident by actively engaging in the response and recovery process.

Service access

- Agreement
- Channel: EATM-CERT Web Portal, Email, Phone
- Data protection notification and privacy statement.

4 Proactive services

4.1 Security Assessments

This service provides a detailed review and analysis of an organization's security based on industry standards or using tools and techniques to identify cyber-security vulnerabilities. This service may use ethical hacking techniques to test selected information systems and networks of the constituent to assess vulnerabilities. Depending on the needs and preferences of the constituent, this service can be limited to the internet accessible parts of the constituent's information systems, or include all or part of the constituent's information systems and networks. This service requires a thorough and rigorous synchronisation/planning of activities as well as a strictly defined scope.

There are many different types of security assessments that can be provided, including the following:

- **Infrastructure & Best practices review**—manually reviewing the hardware and software configurations, routers, firewalls, servers, and desktop devices to ensure that they match the organizational or industry best practices security policies and standard configurations. Interviewing employees and system and network administrators to determine if their security practices match the defined organizational security policy or some specific industry standards.
- **Penetration testing**—testing the security of a site by purposefully attacking its systems and networks. Constituents can benefit from this Service in accordance with the following steps:
  - Joint Agreement (e.g. NDA);
  - Scoping (formalised by the joint approval of the scoping document);
  - On-site pentest (standard duration: 1 week);
  - Findings Report (formalised by the joint approval of the final report).

  The procedure to benefit from this Service is described in EATM-CERT document "SRV01-SecurityAssessment".

- **Vulnerability scanning**—using vulnerability scanning infrastructure or application scanners to determine which systems and networks are vulnerable.

  The procedure to benefit from this Service is described in EATM-CERT document "SRV04-VulnerabilityScanning".

- **Vulnerability watch**—informing about public announcement of vulnerabilities related to some specific assets.

  The procedure to benefit from this Service is described in EATM-CERT document "SRV03-VulnerabilityWatch".

A security assessment report is provided to the constituent that reviews, classifies and prioritizes the vulnerabilities and makes suggestions for effective countermeasures and, upon request, makes suggestions for improved objectives for the cyber security infrastructure.

EATM-CERT can also support cyber-security awareness sessions at senior management level by presenting the security assessment report, in order to improve prevention and to obtain support (buy-in) for the improvement plan resulting from the review.

Purpose: This service aims to identify vulnerabilities and weak points in the cyber posture of the constituent in order to mitigate them and improve its cyber resilience.

Service access

- Agreement.
- Channel: EATM-CERT Web Portal, Email
- Technical information and defined scope
- Accepted risk assessment of the security assessments
- Data protection notification and privacy statement.

5 Competence services

5.1 Phishing awareness campaign

This Service consists of preparing the campaign, sending emails, monitoring the behaviours of targeted individuals and reporting about findings, lessons learned and recommendations. It aims to raise awareness about correct and inappropriate behaviours when receiving and processing a phishing email. It trains individuals to receiving and processing suspicious emails as phishing is a very much used and successful method to attack organisations.

EATM-CERT produces and launches phishing awareness campaigns:

- Targeting EUROCONTROL staff;
- Targeting aviation stakeholder staff in charge of accounting and payments (see 8);
- Constituent staff upon the specific request of this constituent.

Purpose: This Service aims to raise awareness of aviation stakeholders about phishing risks and proceedings.

Service access

- Agreement for ad-hoc constituent campaigns
- Specific products: Phishing awareness report
- Channel: Email distribution
- Information required: FMB (where report should be forwarded to), email address.

5.2 Awareness building

EATM-CERT is able to identify where constituents require more information and guidance to better conform to accepted security practices and organisational security policies.

Increasing the general security awareness of the constituent population not only improves their understanding of security issues but also helps them perform their day-to day operations in a more secure manner. This can reduce the occurrence of successful attacks and increase the probability that constituents will detect and report attacks, thereby decreasing recovery times and eliminating or minimising losses.

EATM-CERT will seek opportunities to increase cyber-security awareness through developing articles, posters, newsletters, web sites, or other informational resources that explain security best practices and provide advice on precautions to take.

It also includes organising Table Top Exercises, Capture The Flag, Red Team/Blue Team exercises as well as supporting workshops, conferences, shows … .

Activities may also include scheduling meetings and seminars to keep constituents up to date with ongoing security procedures and potential threats to organisational systems.

Purpose: This service aims to offer practical advice to the constituent's people in order to improve the cyber practices employed.

Service access

- Agreement.
- Channel: EATM-CERT Web Portal, Email, Reports, conferences, workshops

5.3 Education/Training

This service involves providing information to constituents about cyber-security issues through seminars, workshops, courses, and tutorials. Topics might include cyber-security incident reporting guidelines, appropriate response methods, cyber-security incident response tools, cyber-security incident prevention methods, and other information necessary to protect, detect, report, and respond to cyber-security incidents.

This service does not include the cyber-security training courses as provided by EUROCONTROL Institute of Air Navigation Services (IANS).

The constituent will pay for such ad-hoc/ education/training service.

Purpose: This Service aims to increase cybersecurity competence and skills of aviation stakeholders.

Service access

- Agreement.
- Channel: On-site, on-line

Appendices

A. Summary of access to Services – Channels of delivery

	Request & Access	Agreement	Public website	Service Portal	MISP	Email	Phone	Twitter
Intelligence	Announcements and Advisories			Y	Y	Y	Y	
	Alerts and Warnings				Y		Y	TLP:WHITE only
	CTI and feeds				Y	Y	Y	
	CTI - Aviation quarterly cyber threat landscape report for senior management					Y		
	CTI - EATM-CERT map		Y					TLP:WHITE only
	CTI - Fraudulent websites					Y		
	CTI - Info on Dark/Deep web	Y				Y	Y	
Response	Credential leaks detection	Y		Y		Y		
	Artefact analysis and actions	Y				Y		
	Scams impersonating EUROCONTROL staff				Y	Y	Y	
	Incident response support and coordination (remote)	Y				Y	Y	
	Incident response and analysis (remote)			Y		Y	Y	
Proactive	Infrastructure & Best practices review	Y		Y		Y		
	Penetration testing	Y		Y		Y		
	Vulnerability scanning	Y		Y		Y		
	Vulnerability watch	Y		Y		Y		
Competence	Phishing awareness campaign	Y*				Y		
	Awareness building		Y	Y		Y		TLP:WHITE only
	Education/Training	Y						

*: for ad-hoc constituent campaigns

Table 1: Channels of Service delivery

B. SRV01-SecurityAssessment

SRV01-SecurityAssessment_v.1.0.docx

C. SRV03-VulnerabilityWatch

SRV03-VulnerabilityWatch_v.1.0.docx

D. SRV04-VulnerabilityScanning

SRV04-VulnerabilityScanning_v.1.0.docx

E. GDL05-MispConnectionGuideline

GDL05-MispConnectionGuideline V1.1.docx

F. GDL06-SpyCloud LeakDetectionServiceGuideline

GDL06-SpyCloud LeakDetectionServiceG

References

[1] https://www.enisa.europa.eu/activities/cert/support/guide2/introduction/possible-services

[2] http://www.cert.org/incident-management/services.cfm

[3] https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/considerations-on-the-traffic-light-protocol

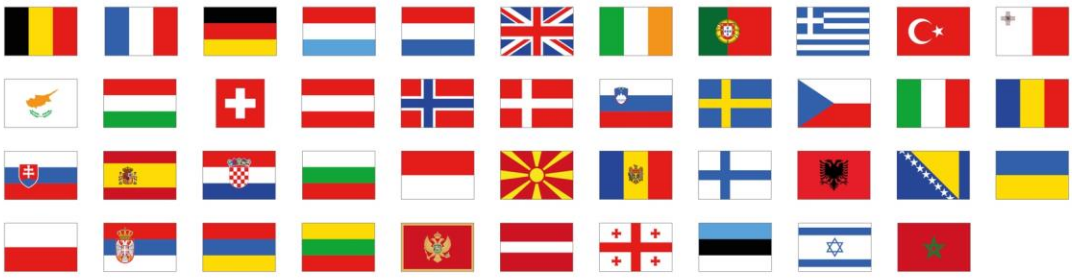
Abbreviations

Term	Definition
ANSP	Air Navigation Service Provider
AO	Airport Operator
AU	Airspace User
APT	Advanced Persistent Threat
ASN	Abstract Syntax Notation
ATM	Air Traffic Management
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
CTI	Cyber Threat Intelligence
EATM-CERT	European Air Traffic Management Computer Emergency Response Team
FMB	Functional Mail Box
GDPR	General Data Protection Rule
IANS	Institute of Air Navigation Service
IDS	Intrusion Detection System
IP	Internet Protocol
IoC	Indicator of Compromise
ISAC	Information Sharing and Analysis Center
IT	Information Technology
MISP	Malware Information Sharing Platform
NDA	Non Disclosure Agreement
NIS	Network and Information Security
OSINT	Open Source Intelligence
PGP	Pretty Good Privacy
TLP	Traffic Light Protocol
TTPs	Tactics, Techniques and Procedures
URL	Uniform Resource Locator

Table 2 - Abbreviations table

EUROCONTROL

SUPPORTING EUROPEAN AVIATION



www.eurocontrol.int