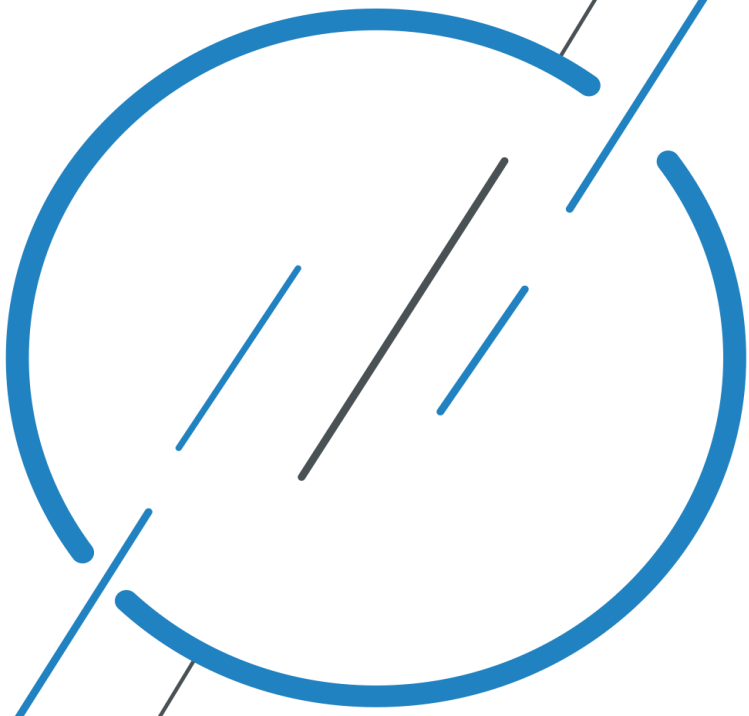
SysDream
Cybersécurité Hub One



RFC 2350
CERT SysDream

TLP : WHITE

Update history

Version	Date (MM/DD/YYYY)	Author	Object
1.0	11/10/2021	CERT-SYSDREAM	Creation
1.0	01/15/2022	Serge Carpentier	Approbation
1.1	03/10/2022	CERT-SYSDREAM	Translation to english
1.1	03/10/2022	Serge Carpentier	Approbation
1.2	03/16/2022	CERT-SYSDREAM	Modification affiliation section
1.2	03/16/2022	Serge Carpentier	Approbation
1.3	03/21/2022	CERT-SYSDREAM	Modification 4.1,5 and 5.1 Section, URL location and authenticating document
1.3	03/21/2022	Serge Carpentier	Approbation
1.4	03/29/2022	CERT-SYSDREAM	Minor correction (Document Identification)
1.4	03/29/2022	Serge Carpentier	Approbation
1.5	07/06/2022	CERT-SYSDREAM	Update 3.3 Affiliation
1.5	07/06/2022	Serge Carpentier	Approbation

Document classification

Entities	Recipient list	Diffusion object
	Not Applicable	
	Public classification	
	TLP : WHITE	

Documents reference

Reference	Title of document	Version
[1]	IETF RFC 2350	June 1998

SUMMARY

1 Document information

This document contains a description of the SysDream Cybercrime Center, and hereinafter called "CERT SysDream", as recommended by RFC2350 [1]. It provides the essential information of CERT SysDream, its responsibilities as well as the services provided to its sponsors.

1.1 Document review / Date of last update

The current version of this document is indicated in the update history (**see Page 2 – Update history**)

1.2 Distribution List for Notifications

No contact list is defined for notification of changes to this document at this time.

1.3 Locations where this document may be found

The current version of this document is available at the following address:

- https://sysdream.com/files/cert/CERT-SysDream-RFC2350.pdf

1.4 Authenticating this Document

This document has been signed with the CERT SysDream PGP key and the signature file is available at the following address:

- https://sysdream.com/files/cert/CERT-SysDream-RFC2350.pdf.sig

1.5 Document Identification

Title: **CERT-SysDream-RFC2350.pdf**
Version: **1.5**
Document Date: **2022-06-07 (YYYY-MM-DD)**
SHA-256 Expiration: this document is valid until superseded by a later version

2 Contact Information

2.1 Name of Team

Official name : **Centre de Lutte Contre la Cybercriminalité SysDream**
Short name : **CERT SysDream**

2.2 Address

SYSDREAM
CLCCS - Centre de Lutte Contre la Cybercriminalité SysDream
14, Place Marie-Jeanne Bassot
92300 LEVALLOIS-PERRET

2.3 Time Zone

CET/CEST : **Paris (GMT+01:00, et GMT+02:00 Summer time)**

2.4 Telephone Number

+33 (0) 1 83 07 00 06

2.5 Facsimile Number

Not applicable

2.6 Other Telecommunication

Not applicable

2.7 Electronic Mail Address

If you need to notify us about an information security incident or a cyber-threat targeting or involving CERT SysDream, please contact us at: cert@sysdream.com

2.8 Public Keys and Encryption Information

PGP is used for functional exchanges with CERT SysDream.

- User ID: **CERT-SYSDREAM – 2k22**
- Key ID : **0x109652FC**
- Key Type: **RSA**
- Key Size: **4096**
- Expires: **21/02/2030**
- Empreinte : **527A 82E4 5ECE 100B 569B 2C9E 1C26 0B3F 1096 52FC**

The public PGP key is available at: https://sysdream.com/files/cert/cert-sysdream-public_key.asc It can be retrieved from one of the usual public key servers.

2.9 Team Members

The list of team members is not published. It is made up of experts in Information Systems Security (ISS) whose expertise is as follows :

- Risk and compliance analysis
- Analysis of vulnerabilities
- Threat analysis
- Digital investigation
- Penetration testing
- Incident & crisis management

The identity of one of the CERT SysDream members may be disclosed on a case-by-case basis on a need-to-know basis.

2.10 Other Information

See our web site at https://sysdream.com for additional information about CERT-SysDream.

2.11 Points of Customer Contact

2.11.1 Sponsor external to GROUPE ADP (Aéroports de Paris)

The preferred communication channel with CERT SysDream is the email mentioned in point 2.7.

In the event of an emergency, please specify the tag **[URGENT/EMERGENCY]** in the subject field of your email (see 2.7 Email address) or call the contact number in point 2.4 during working hours (9am-6pm non-stop).

Outside working hours and in the event of a suspected critical incident, the CERT SysDream office can be contacted at the telephone number mentioned in point 2.4 but an email must be sent if possible, to the email address mentioned in point 2.7

2.11.2 GROUPE ADP (Aéroports de Paris) and its subsidiaries

The preferred communication channel with CERT SysDream is the email mentioned in point 2.7.

In case of emergency, please specify the tag **[HUB - URGENT/EMERGENCY]** in the subject field of your email (see 2.7 Email address) or call the contact number in point 2.4 during working hours (9am-6pm non-stop).

Outside working hours and in the event of a suspected critical incident, the CERT SysDream office can be contacted at the telephone number mentioned in point 2.4 but an email must be sent if possible to the email address mentioned in point 2.7

3 Charter

3.1 Mission Statement

The CERT SysDream's mission with regard to its sponsors according to the defined service agreement is to:

- Fight against Cybercrime;
- Monitor Information Systems in Cyberspace;
- Detect vulnerabilities on networks and systems;
- Coordinate and investigate the response to Cybersecurity incidents;

CERT SysDream will investigate any Cybersecurity incident that may implicate its sponsors as the source or target of an attack or any cyber threats.

3.2 Constituency

GROUPE ADP (Aéroports de Paris), its subsidiaries as well as customers who have subscribed to CERT SysDream services.

3.3 Affiliation

The CERT SysDream has relationships with the following organization:

CAMPUS CYBER	*https://campuscyber.fr/acteurs/ - via Hub One*
TF-CSIRT	*https://www.trusted-introducer.org/directory/teams/cert-sysdream-fr.html*
InterCERT FRANCE	*https://www.cert.ssi.gouv.fr/csirt/intercert-fr/*

3.4 Authority

The CERT SysDream is owned by SysDream, a subsidiary of the Hub One Group (GROUPE ADP - Aéroport de Paris) and is under the authority of the Director of the SysDream Security Incident Response Business Line.

4 Policies

4.1 Types of Incidents and Level of Support

CERT SysDream is the central point of contact for the declaration of all Cybersecurity incidents for the GROUPE ADP (Aéroports de Paris) as well as the clients who have subscribed to the security incident response offers. CERT SysDream deals with all types of Cybersecurity incidents that occur or threaten to occur within the perimeter defined with its sponsors. The level of assistance may vary according to the mission orders and the SLA's defined in the service agreements established between the stakeholders. Services provided by CERT SysDream are listed in section (5. Services)

4.2 Co-operation, Interaction and Disclosure of Information

The CERT SysDream will exchange all necessary information with other CSIRT's/CERT's as well as with other affected parties if they are involved in a security incident or incident response and according to the classification of the information.

No incident or vulnerability information will be passed on to anyone other than the relevant stakeholders. French law enforcement agencies requesting information in the context of a criminal investigation will receive the information requested within the limits of the court decision and the criminal investigation, if they present a valid court decision from a jurisdiction French.

All incoming information within the CERT SysDream is categorized as "INTERNAL" by default. If a specific agreement exists, the information is treated in accordance with that agreement and classified as "RESTRICTED" or "CONFIDENTIAL". "RESTRICTED" or "CONFIDENTIAL" information may only be made public with the consent of the parties involved, or on a need-to-know basis.

The CERT SysDream respects and applies the TLP (Traffic Light Protocol) information exchange classification protocol.

4.3 Communication and Authentication

The preferred means of communication with CERT SysDream is email. Sensitive information will be encrypted before being transmitted. It is recommended to encrypt and sign the security incident report information sent to the CERT SysDream. Depending on the stakeholders, the CERT SysDream will use PGP or Zed! container to guarantee the confidentiality and integrity of the documents exchanged. PGP can be used to authenticate the files exchanged.

Authorizations to access information classified as "RESTRICTED" or "CONFIDENTIAL" are subject to a non-disclosure agreement (NDA) for all members of CERT SysDream and by a specific agreement signed between the commendatory and the Director of CERT. Information classified as "INTERNAL", "RESTRICTED" or "CONFIDENTIAL" may not be disclosed without the authorization of the CERT SysDream Director.

5 Services

5.1 Reactive activities

5.1.1 Incident Response

CERT SysDream offers the following responsive services:

- Alerts and warnings
- Incident analysis, coordination, and response
- Vulnerability analysis, coordination, and response
- Forensic analysis

5.1.2 Security incident report service

The security incident report reception service is available 24/7. Activities for the service is the reception reports of adverse events and notification to the declarant that they have been considered within 2 hours in open hours and 4 hours in non-working hours, excluding specific contracts; An incident number will be communicated to the declarant.

5.1.3 Incident Triage

The triage actions carried out are as follows:

- Analysis and qualification of reports on behalf of the sponsor
- Escalation to the perimeter mission head, who manages the processing in the event of a major security incident ("significant" level incident) in order to allocate adequate resources and define an initial containment position
- If necessary, issue an alert to the competent authorities of the State or contact in charge of the ISS depending on the nature of the incident and the procedures in place, such as:
    - To the Information Systems Security Director/Manager/Contact of the commendatory when the latter is identified
    - To the french National Information Systems Security Agency (ANSSI) in the event of a major cybersecurity incident that may impact other sectors
    - To the National Commission for Computing and Liberties (CNIL) in the event of a personal data breach;

5.1.4 Incident Coordination

The coordination actions carried out are as follows:

- If necessary, support the structure concerned in the treatment of the information systems security incident and coordinate the first operations with the internal teams of the commendatory such as:

- Assessment of the perimeter impacted by the security incident
- The establishment of crisis cells (Operational and Managerial)
- The collection of any digital evidence as well as the Indicators of Attacks (IoA)
- Analysis by the CERT SysDream digital investigation teams for confirmation of the malicious act
- Definition and proposal of provisional and/or corrective measures
- In-depth analysis of the incident to identify the root causes of the incident and the extent of the impacts

All of these operations will be formalized by a preliminary analysis report including:

- The first results of the evaluations
- Urgent containment actions implemented
- The key stages of the incident and remediation
- The digital investigations report
- The detailed chronology of the events of the incident
- Indicators of compromise related to the incident
- Cyber intelligence elements related to the group(s) of attacker(s)
- The strategy for restoring services in a nominal situation
- A managerial report mentioning the key assessments for the contextualization of the incident
- digital evidence

Throughout the incident, progress points will be organized and the commendatory can add new elements to the incident for analysis.

5.1.5 Incident Resolution

The security incident resolution actions taken are as follows:

- Analyze artefacts and respond, on a case-by-case basis
- Advise the structure(s) concerned on the appropriate measures to be implemented
- Follow the security incident resolution process (Destruction of data held by CERT SysDream, perimeter monitoring, Feedback)

5.2 Proactive activities

5.2.1 Informations and alerts

The CERT SysDream monitors current information security news and threats specific to the business sectors of GROUPE ADP and its sponsors. It informs and alerts its sponsors through security bulletins communicated by email. In some cases, the information will be classified "CONFIDENTIAL" and encrypted before distribution to the parties concerned. The information provided is as follows:

- Security bulletins on standard technologies (emergence of threats, innovative attack methodologies, new vulnerabilities) and specific to the sectors of sponsors (security incidents, new vulnerabilities)
- Security alerts and recommendations to protect against current threats
- Security and incident management support documents (reflex sheets, practical sheets, good practice guides). CISO's (Chief Information Security Officer) sponsors and the CERT SysDream have a mailing list that also allows players to be alerted about a critical threat.

CERT SysDream develops vulnerability testing tools for its sponsors.

5.2.2 Information systems security audit and assessment

The CERT SysDream carries out automatic security audits (DAST), excluded intrusion tests. This is an information system security diagnostic service concerning the exposure of the services of the sponsors in cyberspace or in uncontrolled type networks.

The following activities are carried out as part of these audits:

- Search for data leaks (source code leak, user data leak...) and assessment of their relevance
- Realization of a mapping of the exposed assets (technologies and servers used, cryptographic configuration...) in order to determine the surface and the vectors of attacks
- Search for vulnerabilities (unmanaged "shadow it" type machines or misconfigured servers), weak/default identifiers, Web vulnerabilities (SQL injections, XSS, LFI, RFI...) and evaluation of their exploitability.

At the end of the audit, the CERT SysDream issues a report intended for management and/or the Head of Information Systems Security. It introduce :

- Identified vulnerabilities and their level of criticality
- Exploitation impact
- Recommendations aimed at reducing the identified risks.

5.2.3 Threat Status

As part of the reinforcement of the security of its sponsors, CERT SysDream assesses the risks of the business context with the internal services of its sponsors in order to improve the means of detection, defense and awareness. The steps implemented are as follows:

- Analysis of the business context
- Research and gathering of information (Assets/Threats)
- Reports and preparation of awareness reports
- Restitution with the sponsor's teams

The objectives for sponsors are:

- Considering events, activities and tendencies that could generate a dysfunction of the activity
- Measure to be implemented to detect, prevent and mitigate malicious activities against the sponsor
- Implementation of good security and operating practices

6 Incident Reporting Forms

Incidents that must be declared to CERT SysDream must contain at least the following information:

- The declarant's contact details
- The contact details referent person
- Date and time of the incident as well as the Time Zone
- Is the incident still ongoing?
- The findings of the incident
- Impacts of the incident
- Source IP addresses, network ports, protocols
- Destination IP addresses, network ports, protocols
- And all information relating to the security incident

7 Disclamers

While every precaution will be taken in the preparation of information, notifications and alerts, CERT SysDream assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.