Approach Cyber CSIRT - RFC2350

Document Version 1.0 - 13th March 2024

Contents

1 Document Information

This document, prepared following RFC2350 guidelines, provides a comprehensive description of the Approach Cyber Computer Security Incident Response Team (CSIRT). It outlines the team's mission, policies, services, and contact information.

1.1 Date of last update

Version 1.0, created 13th March 2024

1.2 Locations where this document may be found

This document is available at https://www.approach-cyber.com/en/rfc2350.html

1.3 Authenticating this Document

Signed with Adobe PDF using the company's official digital signature.

1.4 Document Identification

- Title: rfc2350-Approach
- Version: 1
- Document Date: 2024-03-13
- Expiration: This document is valid until superseded by a later version.

2 Contact Information

This section describes how to contact Approach Cyber CSIRT.

2.1 Name of the Team

- Full Name: APPROACH-CYBER-CSIRT
- Short Name: AC.CSIRT

Approach Cyber CSIRT is Approach Cyber’s commercial CERT/CSIRT team (Computer Emergency Response Team / Computer Security Incident Response Team).

2.2 Address

Approach Cyber CSIRT
Rue Edouard Belin 7, 1435 Mont-Saint-Guibert, Belgium

2.3 Time Zone

GMT+1 (with Daylight Saving Time or Summer Time, which starts on the last Sunday in March and ends on the last Sunday in October). Also known as CET/CEST.

2.4 Telephone Numbers

- +32 10 83 21 06 (Belgian Business hours)
- +41 21 561 16 44 (Swiss Business hours)

2.5 Facsimile Number

None available.

2.6 Other Telecommunication

None available.

2.7 Electronic Mail Address

If you need to notify us about an information security incident or a cyber-threat targeting or involving Approach Cyber or one of its customers, please contact us at:

csirt@approach-cyber.com

2.8 Public Keys and Encryption Information

PGP/GnuPG is supported to secure communication.

Consequently, the APPROACH-CYBER-CSIRT has a PGP key:

- KeyID: 0x7FB7FCEF17F319A1
- Fingerprint: 6294 AC41 F73E 7E6F 9C16 E146 7FB7 FCEF 17F3 19A1

The key can be retrieved from one of the usual public key servers such as http://pgp.mit.edu/.

The key shall be used whenever information must be sent to APPROACH-CYBER-CSIRT in a secure manner.

- Please use this key when you want/need to encrypt messages that you send to APPROACH-CYBER-CSIRT.
- When due, APPROACH-CYBER-CSIRT will sign messages.
- When due, sign your messages using your own key please. It helps when that key is verifiable (for instance, using the public key servers).

2.9 Team Members

APPROACH-CYBER-CSIRT's acting team leader is Jean-François Stenuit.

The team consists of at least 6 security analysts. It is internally supported by the other teams of Approach Cyber (governance and privacy specialists, secure software development, penetration testers).

2.10 Other Information

General information about APPROACH-CYBER-CSIRT can be found at the following URL:

https://www.approach-cyber.com/en/cyber-emergency-services.html

2.11 Points of Customer Contact

The preferred method to contact Approach Cyber CSIRT is to use our JIRA service portal available at:

https://approach-cyber.atlassian.net/jira/servicedesk/

Alternatively, the following e-mail address can be used:

csirt@approach-cyber.com

Depending on their service contract, customers may have access to a 24/7 hotline number.

3 Charter

3.1 Mission Statement

Approach Cyber CSIRT is dedicated to offering "Detect & Response" services as part of the Approach Cyber suite, focusing on aiding customers during cybersecurity incidents.

3.2 Constituency

Serving customers in Belgium and Switzerland, Approach Cyber CSIRT operates under service contracts with clients, ensuring tailored cybersecurity assistance.

3.3 Sponsorship/Affiliation

Operated by Approach-Cyber, a leader in cybersecurity and privacy. APPROACH-CYBER-CSIRT maintains contact with various national and international CSIRT and CERT teams.

3.4 Authority

Approach Cyber CSIRT manages security incidents exclusively at the behest of its client base, operating within the mandate provided by these clients. The team's function is anchored in the authorization granted by its clientele.

In its capacity, Approach Cyber CSIRT primarily serves as a consultative entity to internal security divisions, offering strategic operational advice. It is crucial to note that Approach Cyber CSIRT does not possess the jurisdiction to mandate specific remedial actions. The onus of implementing any proposed measures rests entirely with the recipients of such advice.

In essence, Approach Cyber CSIRT anticipates a collaborative relationship with its clients' system administrators and users, facilitating a synergistic approach to cybersecurity incident management.

4 Policies

4.1 Types of Incidents and Level of Support

Approach Cyber CSIRT addresses a broad spectrum of cybersecurity incidents, including but not limited to malware infections, intrusions, DDoS attacks, data leaks, phishing, and ransomware.

The support provided by Approach Cyber CSIRT is tailored according to the nature and criticality of the incident, its impact, the category of the client, the extent of the user community involved, and the available resources of Approach Cyber CSIRT at that moment. Approach Cyber CSIRT's response, including incident management and digital forensics, will be methodically deployed based on the specifics of each security incident.

It's important to note that Approach Cyber CSIRT does not offer direct assistance to end-users. Instead, end-users should seek help from their Security Operation Centre (SOC) or internal CSIRT. In instances where clients lack a specialized security team, Approach Cyber collaborates closely with local IT teams or operators to ensure effective incident response. Support from Approach Cyber CSIRT is primarily aimed at these groups, ensuring they have the necessary assistance to address and mitigate security incidents effectively.

4.2 Cooperation, Interaction, and Disclosure of Information

Approach Cyber CSIRT is committed to fostering a robust network of collaboration and information sharing, both within its immediate constituency and with other certified CSIRTs globally. Central to our operations is the principle of maintaining confidentiality while ensuring that critical security information is exchanged efficiently to prevent and respond to cybersecurity threats.

Our policy embraces open communication channels, particularly leveraging platforms like MISP for the dynamic exchange of threat intelligence and incident data.

We prioritize transparency with our clients, advising them of our cooperative endeavours while strictly adhering to data protection laws and their privacy needs.

4.3 Communication and Authentication

Preferring PGP-encrypted email for secure and authenticated communication.

5 Services

Approach Cyber CSIRT offers an extensive range of services aligned with the FIRST Service Framework 2.1.0, covering event and incident management, vulnerability management, situational awareness, and knowledge transfer.

6 Incident Reporting

Incidents can be reported through our JIRA portal, with email and telephone as alternatives.

7 Disclaimers and Legal Notices

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

Signed of

This document is electronically signed by Jean-Christophe Wilski, CFO of Approach Belgium

Digitally signed by Wilski Jean-Christophe Jean-Pierre J
Date: 23/04/2024 10:08:06