BARIKAT CSIRT RFC 2350 Profile

1. Document Information

This document contains a description of BARIKAT CSIRT in accordance with RFC 2350(RFC 2350 (https://www.rfc-editor.org/info/rfc2350). It provides basic information about BARIKAT CSIRT, its channels of communication, and its roles.

1.1. Date of Last Update

This is version 1.0 – 2021/11/10

1.2. Distribution List for Notifications

There is no distribution list for notifications. Our customers are notified via e-mail when necessary.

1.3. Locations where this Document May Be Found

The current version of this document is always available at:

https://www.barikat.com.tr/barikat-csirt-rfc-2350-profile.pdf

2. Contact Information

2.1. Name of the Team

Official Name: BARIKAT CSIRT
Short Name: BARIKAT-CSIRT

2.2. Address

BARIKAT Internet Guvenligi Bilisim Tic. A.S.,
Mustafa Kemal Mahallesi,
Dumlupinar Bulvari No:164,
Kentpark Ofis, Kat:4 Daire:06,
Cankaya, 06510 Ankara
Turkey

2.3. Time Zone

+03:00 – Europe/Istanbul

2.4. Telephone Number

+90 312 235 44 41

2.5. Facsimile Number

+90 312 235 44 51

2.6. Other Telecommunication

Not applicable

2.7. Electronic Mail Address

csirt@barikat.com.tr

2.8. Public Keys and Encryption Information

Please encrypt any sensitive e-mail with the BARIKAT CSIRT’s PGP key:

PGP Key ID: C486FDD9
PGP Fingerprint: CE9A 11BA D5AB 1765 8A41 AD7F E884 6ADA C486 FDD9

2.9. Team Members

This information is not publicly available.

2.10. Other Information

Further information about the BARIKAT CSIRT can be found at:

https://www.barikat.com.tr/en/

BARIKAT CSIRT is member of TF-CSIRT (Trusted Introducer). See https://www.trusted-introducer.org/directory/teams/barikat-csirt.html for more information.

2.11. Points of Contact

The preferred method to contact BARIKAT CSIRT is by sending an email to the following address: csirt@barikat.com.tr

A security analyst can be contacted at this email address during hours of operation. Urgent cases can be reported by phone (+90 531 221 22 81) on 7/24 basis.

3. Charter

3.1. Mission Statement

BARIKAT has been established in 2008 and only deals with cyber security. Our main goal is to increase level of our customers cyber security maturity. Our solutions to current security problems are based on sound methodologies practiced worldwide.

Our technical staff provides many services and consultancies needed to create a solid security posture for any modern organization.

BARIKAT holds NATO grade security clearance for premises and National Defense Ministry level for whole staff.

Organizations require a wide range of trainings to create and enhance their cyber security workforce. BARIKAT Academy can provide trainings for such organizations and help them create a top-notch Security Operation Center (SOC).

Our security services and consultancies cover organizations gaps or enhance existing teams' capabilities. Our teams can transfer their knowledge to newly created security teams as well.

Our R&D department researches technologies and methodologies needed to increase cyber security level and develops products, services and methodologies needed in a modern organization to increase it as well.

Customers can benefit from our experience, professionalism and reliability in the auditing, consultation, architecture and integration of leading network and security solutions. We deliver state-of-the-art cloud, managed and SOC services from our ISO 27001-certified Cyber Security Monitoring Center.

Our mission is to explain, advise and provide the needs of people, processes and technologies that customers know or do not know in order to maintain and increase their cyber security levels.

3.2. Constituency

With more than 260 personnel, it operates in Ankara/Turkey, Istanbul/Turkey, Doha/Qatar and Amsterdam/Netherlands. BARIKAT is working with more than 200 organizations and representing more than 40 technology partners.
The constituency of BARIKAT-CSIRT is composed of all users, systems, and networks in all offices explained above.

3.3. Sponsorship and/or Affiliation

BARIKAT-CSIRT operates with the authority delegated by BARIKAT Private Company.

3.4. Authority

BARIKAT-CSIRT operates as a unit under the Technical Operations Directorate of BARİKAT.

4. Policies

4.1. Types of Incidents and Level of Support

Incident Types are categorized as below:

- Data Loss
- Confidentiality Breach
- Social Engineering
- Physical Security Breach, theft, etc.
- Unauthorized Access
- Suspicious logs
- Denial of Service
- Other

The level of support given by BARİKAT-CSIRT will vary depending on the type and severity of the incident or issue and the level of the agreement signed with the client.

4.2. Co-operation, Interaction and Disclosure of Information

BARIKAT-CSIRT highly regards the importance of operational cooperation and information sharing between CERTs and also with other organizations which may contribute towards or make use of their services.

All information is handled according to its classification level. Classification levels in use are;

- TOP SECRET
- SECRET
- PRIVATE
- RESTRICTED
- UNCLASSIFIED

BARIKAT-CSIRT supports the Information Sharing Traffic Light Protocol (ISTLP; see https://www.trusted-introducer.org/links/ISTLP-v1.1-approved.pdf) as well; information that arrives with the tags WHITE, GREEN, AMBER, or RED will be handled appropriately.

4.3. Communication and Authentication

Telephones will not be considered sufficiently secure to be used even unencrypted. Unencrypted email will not be considered particularly secure, but will be sufficient for the transmission of low-sensitivity data. If it is necessary to send highly sensitive data by email, PGP or one-time-use symmetric keys will be used. Network file transfers will be considered to be similar to e-mail for these purposes: sensitive data should be encrypted for transmission. All encryptions' keys should be transmitted over a separate communication channel (one-time readable password, Signal, Telegram messages, etc.).

Referrals from known trusted people will be sufficient to identify someone. Otherwise, appropriate methods will be used, such as a search of memberships, the use of WHOIS and other Internet registration information, etc, along with telephone call-back or e-mail mail-back to ensure that the party is not an impostor. Incoming e-mail whose data must be trusted will be checked with the originator personally, or by means of digital signatures

5. Services

5.1. Reactive Services:

Response part of CSIRT services are triggered by an event or request, such as a report of a compromised host, widespread malicious code or defaced web site. After the detection of an incident, BARIKAT's incident respond team starts acting properly and timely manner.

The BARIKAT Incident Response team shaped according to the type and scope of the event.

5.2. Readiness

BARIKAT's CSIRT Services that relate to Readiness can be grouped into two categories; Proactive Services and Security Quality Management Services.

Proactive services provide assistance and information to help prepare, protect, and secure systems. Proactive services will directly reduce the number of incidents in the future.

Security quality management services augment existing and well-established services that are independent of incident handling and are performed by other departments such as the IT, audit, or training departments. These services are generally proactive but contribute indirectly to reducing the number of incidents.

5.2.1. BARIKAT's Proactive CSIRT Services:

- Announcements
  - Intrusion Alerts
  - Vulnerability Warnings
  - Security Advisories
- Technology Watch
- Penetration Tests
- Configuration and Maintenance of Security Tools, Applications, and Infrastructures
- Development of Security Tools by R&D Department
  - ASMA (Asset Manager)
  - LoDDoS (DDOS Automation Tool)
- 7x24 Central Monitoring (SOC) Services
  - Level-1 Security Analyst
  - Level-2 Security Analyst
- Security-Related Information Dissemination
- Cyber Threat Information Gathering and Sharing
- Managed Security Services
- On-site Security Services Support

5.2.2. BARIKAT's Security Quality Management Services:

- Risk Analysis
- Business Continuity and Disaster Recovery Planning
- Compliance Audits or Assessments,
- SOC Analysis
- Security Architecture Analysis
- Effective Security Controls Analysis
- Security Consulting
- Awareness Building
- Education/Training by Barikat Academy
  - Hacker School
  - Role Based Courses
  - Job Based Courses
  - CSIRT Personnel Training

6. Incident Reporting Forms

There are no local forms developed yet for reporting incidents to BARIKAT-CSIRT. Incident reports can be sent to csirt@barikat.com.tr.

7. Disclaimers

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