RFC 2350 CyberArmyID-CSIRT

1. Informasi Mengenai Dokumen

Dokumen ini berisi deskripsi CyberArmyID-CSIRT berdasarkan RFC 2350, yaitu informasi dasar mengenai CyberArmyID-CSIRT, menjelaskan tanggung jawab, layanan yang diberikan, dan cara untuk menghubungi CyberArmyID-CSIRT.

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 16 Agustus 2024.

1.2. Daftar Distribusi untuk Pemberitahuan

Tidak ada daftar distribusi untuk pemberitahuan pembaharuan dokumen.

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada :
https://csirt.cyberarmy.id/rfc-2350 (versi Bahasa Indonesia)

1.4. Keaslian Dokumen

Kedua dokumen telah ditanda tangani dengan PGP *Key* milik CyberArmyID-CSIRT. Untuk lebih jelas dapat dilihat pada Subbab 2.8.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :
Judul : RFC 2350 CyberArmyID-CSIRT;
Versi : 1.0;
Tanggal Publikasi : 13 Agustus 2024;
Kedaluwarsa : Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

PT Global Inovasi Siber Indonesia (Cyber Army Indonesia) - Computer Security Incident Response Team
Disingkat : CyberArmyID-CSIRT.

2.2. Alamat

Jalan Pariwisata No.4, Sukawarna, Kec. Sukajadi, Kota Bandung, Jawa Barat 40164.

2.3. Zona Waktu

Indonesia (GMT+7)

2.4. Nomor Telepon

+62 822 9888 1337
+62 812 1337 5559

2.5. Nomor Fax

Tidak ada

2.6. Telekomunikasi Lain

N/A.

2.7. Alamat Surat Elektronik (*E-mail*)

csirt@cyberarmy.id

2.8. Kunci Publik (*Public Key*) dan Informasi/Data Enkripsi lain

-----BEGIN PGP PUBLIC KEY BLOCK-----

xsDNBGa6EGkBDAC5n9bDXQenvbniH2REXVa9ltz2FR1l+1faVjApEJpmTyNCQk92
iVwpNOWDiNfR6Jc9uUMaPWTnZhvpoA0E3OUD94rO1uL5eK30ykwDD2ie2Jd4TjpA
MpnhjDLTwO4QpW3ZDRYGSapkEj6YcSGHjBeKgZd9C+fFKWOs85N/fcd9Sg2ZmpLI
iQpsvxaqV5EFWuyzJ4bty1TYDTYlmsOAGJWNOT7Yq73MOoGqWSfutoNHrn8DAHpR
6A9lfnzSu2/Bk4Pgy1v3ob6yWZGCV1zmXr4ArCq6Vmyci5YMhWHpysAq1N1BnsQh
Cl1geapMQjtsEgoFjOdlzmOAtqWXqV37EOvSwClWgB51oJjrvpGWPovwt9HvMyho
7pNcerNZpWKqdnapwelMn/Zpr5dEvl87IKboKaZgI252cRqDYhoWJQ7A8iyCs1cN
5wR9bvbuZ1eE1sAfguCQ88w33GwMJrERVnMuzr6hqxCqRUJ5oDuy5rarAKeT596z
ojlHZMjTlxJwSEsAEQEAAc0mQ3liZXJBcm15SUQgQ1NJUlQgPGNzaXJ0QGN5YmVy
YXJteS5pZD7CwQ0EEwEIADcWIQTTF7yDn4A0ozXZrKmAobY0OvgSAgUCZroQaQUJ
CWYBgAIbAwQLCQgHBRUICQoLBRYCAwEAAAoJEIChtjQ6+BICFjcL/2A5ht8VasmM
sZHgkVIr+o8Goz6X72EbklzzQmdCW3rVVdK1RCk2AEOx47G7QHhxR3bSYlZ2RI1w
P4XND5pCJ0bRF3ADFVJhuQDUvjHQHLJQjosLE59YcEWXKNpy/36QcNw4AsxSdBYq
CMty/O7bCF/C4uaTrVMAPqbuhT/R1eJjmqplloe2PCHNjct1TzDxru1YeQzorRBY
N53dNwcdAhuW//sqSbbQhyUFx5SiBfgFYtflKX19tMQOrZZAWw7P2JLyMhFb632U
Cc98STsAJMaxqg083MuWgo8i9oY8p6GEdjmSvhIEwiwU/BR3EQQkyXKKay0FaMe2
pYcsaEJ/RgDV3LVHyOI7w62c7magrIXvlmRfsXqxWX/z+FCtqnbwTAZ3ZA2waJvJ

Uz0UhrQM/NKXHIMY4MbJOp+BZG9HAxkZzWwO9GDaPycdyAU0mNqZa4+H/3VCXRCi
+ZxdRMFt3NJr3aAB9Q5xJR3+3Bu+KuD+08PdH6PBpBfGuTqCqdqlBs7AzQRmuhBq
AQwAzwxgKmEbQ8kx0bwBGPKaoBigESmOMrW3H34SWz9dodQlFwmDlk2WHYVtj74j
lzhKm/j8HXV7YNVyoE0EN92XBchp0AVQBJ1RBJPwFmFB/kwtQ4oyD2kDWiQ9qTHg
s58u1qlSWZsj5vfGox/Pgh1gPS3R304Up0cZyFxLwGyzTKHB4Hp56BTd9pSFC0px
ZwTdk7HEGr8rN5CDDFY89jVpzAPRlK5vkz9c30fC31jmUOvGX19LcDqav5rmd2uG
7vP08SnwB4thRKvOHOdRrtGmfdwgHCr7BIP4G2DcVECq57mSfKOeAnpnmgWoXTmX
5Ht8GIqcDuPnbQ6ezO3Ha+iOwT/2P/2mFgEqsHmUZy9IGEttoTztA10eDdgSK8t1
IPvjrlJX8T73PkckVAubSHg2wi6eqimbLJwXDeWHIoNcmrzx5tJG6/ThNPCQ4hLb
wyFDn9yAQ98b9zmcCGO1a//Ox5myxhMJdkO5IvvRMET2XOzbV4N08AisLSKaQBeL
S1DtABEBAAHCwPwEGAEIACYWIQTTF7yDn4A0ozXZrKmAobY0OvgSAgUCZroQagUJ
CWYBgAIbDAAKCRCAobY0OvgSAI8dDACSkfLizxAm5KxaG1wxAyJk/h3hI7K+E+/j
K3rof/+W8pvAdawNcOOS2xSWDnEpX5Q3ujBzQ1tE3w+FwS6qgpzFZfXYAwLJ9rzT
DznVaS1RarDf3IGYAgIlcDQUaKymnhkZtWMHfnL2s7oX0suzgXAMls5qQla0kQ6S
XH/MsWuI+r/Y6X3+Ahw3TvgO6Q9NCNlq25iiPyWzTG1nZJFoF53Xzh/hd0BkviK2
eiOsTZhz0oFuX07FOczyMYB55ZggbOEk9UqnNQd0zOhpW/0X8mS4OZgeO7eBMO72
KSaALoooDhenR1W06R7h6nxAsyepx1H3jnQYioc0q8uLrWIHUWBwDGBNT9X4KAq8
ugS3ROe0r4GDVQ3pUjeln/1J19y3gM118/PXUnduPdmwDEL+j9p1OaW8NhDbchgZ
00ldvugEqC/8oRXAcD49/tSZoRlV0Yp39c3bpFMypJ3BpkBVmw/1asg2DVhakD+V
uoHNFNu1jDciP2wLqy3Ibny+edXFtKI=
=K6u+
-----END PGP PUBLIC KEY BLOCK-----

File PGP key ini tersedia pada:
https://csirt.cyberarmy.id/CyberArmyIDCSIRT_pubkey.asc

2.9. Anggota Tim

Ketua CyberArmyID-CSIRT adalah CEO Cyber Army Indonesia.
Yang termasuk anggota tim adalah seluruh anggota tim DevSecOps Cyber Army Indonesia.

2.10. Informasi/Data lain

N/A.

2.11. Catatan-catatan pada Kontak CyberArmyID-CSIRT

Metode yang disarankan untuk menghubungi CyberArmyID-CSIRT adalah melalui *e-mail* pada alamat csirt@cyberarmy.id atau melalui nomor telepon yang tercantum pada Informasi Data/Kontak, pada hari Senin-Minggu pada pukul 08.00-17.00 WIB dan jika terdapat hal-hal yang mendesak di luar jam tersebut dapat dilakukan penanganan.

3. Mengenai CyberArmyID-CSIRT

3.1. Visi

Terwujudnya pengelolaan sistem keamanan informasi yang aman di Cyber Army Indonesia.

3.2. Misi

Perwujudan visi sebagaimana dituangkan di atas akan dicapai melalui upaya-upaya yang terkandung dalam misi CyberArmyID-CSIRT, yaitu :

a. Mengkoordinasikan dan mengkolaborasikan layanan keamanan siber di lingkungan perusahaan dan pemangku kepentingan.
b. Membangun kemampuan dan kapasitas sumber daya keamanan siber.
c. Membangun kerjasama dalam rangka penanggulangan dan pemulihan insiden keamanan siber.

3.3. Konstituen

Konstituen CyberArmyID-CSIRT meliputi meliputi seluruh karyawan CyberArmyID.

3.4. Sponsorship dan/atau Afiliasi

Pendanaan CyberArmyID-CSIRT bersumber dari anggaran pendapatan komersial dari produk dan layanan CyberArmyID.

3.5. Otoritas

Berdasarkan Kebijakan Pengelolaan Sistem dan Teknologi Informasi dan Kebijakan Pengelolaan Keamanan Informasi, CyberArmyID-CSIRT memiliki kewenangan untuk melakukan penanggulangan insiden, mitigasi insiden, investigasi, dan analisis dampak insiden, serta pemulihan pasca insiden keamanan siber.

4. Kebijakan – Kebijakan

4.1. Jenis-jenis Insiden dan Tingkat/*Level* Dukungan

CyberArmyID-CSIRT memiliki otoritas untuk menangani insiden yaitu:

a. Web Defacement;
b. DDOS;
c. Malware;
d. Phishing;
e. Advanced Persistent Threats (APT)
f. Vulnerability Report

Dukungan yang diberikan oleh CyberArmyID-CSIRT kepada konstituen dapat bervariasi bergantung dari jenis dan dampak insiden.

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

CyberArmyID-CSIRT akan melakukan kerjasama dan berbagi informasi dengan CSIRT atau organisasi lainnya dalam lingkup keamanan siber. Seluruh informasi yang diterima oleh CyberArmyID-CSIRT Indonesia akan dirahasiakan.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa CyberArmyID-CSIRT Indonesia dapat menggunakan alamat e-mail tanpa enkripsi data (e-mail konvensional) dan telepon. Namun, untuk komunikasi yang memuat informasi sensitif/terbatas/rahasia dapat menggunakan enkripsi PGP pada e-mail.

5. Layanan

5.1. Layanan Utama

Layanan utama dari CyberArmyID-CSIRT yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Layanan ini dilaksanakan oleh CyberArmyID-CSIRT berupa pemberian peringatan adanya insiden siber kepada pemilik sistem elektronik dan informasi statistik terkait layanan ini diberikan oleh konstituen.

5.1.2. Penanganan Insiden Siber

Layanan ini diberikan berupa kegiatan menerima, menanggapi, dan menganalisis Insiden Siber.

5.2. Layanan Tambahan

Layanan tambahan dari CyberArmyID-CSIRT yaitu :

5.2.1. Penanganan Kerawanan Sistem Elektronik

Layanan ini berupa koordinasi, analisis dan rekomendasi teknis dalam rangka penguatan aspek kendali keamanan (security control) baik dalam lingkup teknis ataupun non-teknis (Policy/Governance).

Secara umum penanganan ini dibagi menjadi :

1. Pelaporan kerawanan yang bersifat sewaktu oleh pemilik/penyelenggara sistem elektronik milik konstituen.
2. Layanan penanganan kerawanan sebagai tindak lanjut dari kegiatan audit atau vulnerability assessment

5.2.2. Pemberitahuan Hasil Pengamatan Potensi Ancaman

Layanan ini diberikan berupa penyampaian kepada konstituen terkait ancaman terhadap Sistem Elektronik yang dapat muncul akibat perkembangan teknologi, politik, ekonomi, dan perkembangan lainnya.

5.2.3. Pendeteksian Serangan

Tim CyberArmyID-CSIRT memiliki beberapa sistem untuk mendeteksi apakah sistem pada perusahaan yang bersangkutan dengan stakeholder aman atau memiliki risiko, sehingga dapat dilakukan penanggulangan sedini mungkin.

5.2.4. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Tim CyberArmyID-CSIRT melakukan webinar mengenai isu sistem keamanan informasi.

6. Pelaporan Insiden

Laporan insiden keamanan siber memilii 2 mekanisme:

a. Internal

Melalui grup yang telah dibuat untuk koordinasi dengan melampirkan sekurang-kurangnya memuat:

i. Identitas Pelapor (username pengguna);
ii. Waktu Terjadinya Insiden;
iii. Deskripsi Insiden disertai Bukti (screenshoot, domain name, URL, email, log file, dan lainnya).
iv. Atau sesuai dengan ketentuan lain yang berlaku

b. Eksternal

Melalui email yang dapat dikirimkan ke csirt@cyberarmy.id dengan melampirkan Formulir Aduan Insiden Siber yang sekurang-kurangnya memuat:

i. Identitas Pelapor (foto/scan kartu identitas);
ii. Waktu Terjadinya Insiden;
iii. Deskripsi Insiden disertai Bukti (screenshoot, domain name, URL, email, log file, dan lainnya).
iv. Atau sesuai dengan ketentuan lain yang berlaku

7. *Disclaimer*

Tidak ada