RFC 2350 CSIRT Telkomsigma

1. Informasi Mengenai Dokumen

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

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 12 Desember 2023.

1.2. Daftar Distribusi untuk Pemberitahuan

Satuan Kerja di Lingkungan PT Sigma Cipta Caraka (Telkomsigma).

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada :
https://www.telkomsigma.co.id/csirt/ (versi Bahasa Indonesia)

1.4. Keaslian Dokumen

Dokumen telah ditandatangani dengan PGP *Key* milik Tim CSIRT Telkomsigma – PT Sigma Cipta Caraka. Untuk lebih jelas dapat dilihat pada Subbab 2.8.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu :

Judul	: RFC 2350 Tim CSIRT Telkomsigma
Versi	: 1.0
Tanggal Publikasi	: 12 Desember 2023
Kedaluwarsa	: Dokumen ini valid hingga dokumen terbaru dipublikasikan.

2. Informasi Data/Kontak

2.1. Nama Tim

Cyber Security Incident Response Team PT Sigma Cipta Caraka
Disingkat : CSIRT Telkomsigma

2.2. Alamat

Graha Telkomsigma II
Jl. CBD lot VIII Nomor 8,
kelurahan lengkong gudang,
Tangerang 15321, Indonesia

2.3. Zona Waktu

Jakarta (GMT +07:00)

2.4. Nomor Telepon

(021) 5389186

2.5. Nomor Fax

Tidak Ada

2.6. Telekomunikasi Lain

Tidak Ada

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

csirt@sigma.co.id

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

Bits : 4096 Bits
ID : 0x3F63BCBA
Key Fingerprint : D20C C2DE 774C C6D7 6702 50FE D588 0FA8 3F63 BCBA

Blok PGP Public Key :

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: Encryptomatic OpenPGP for Windows 2.7.17.0

mQINBGXoGN8BEACLJqLM1F54Tv2/ykpffT77ToCidzrZRDGSrevL9vQxtYnw21nt
EY47Tvd0uATkbQd9QsbtA5sTUAF5fC8kLU8+qu6T4Id201JnRcqGWWcHx9JYhU7W
Iofo1BoDlVjgx6LDgZOeIGMOoTKkUOFcKkGpH/mAfT/SE9NVevF/urNv8GsSu5Uy
KphzDL2HLGd43GQtwMQV3whWq+OzhXWIh1/Esrw9UvYLmVBiTgfJLsqC/KnklgwW
qfRwp7UwME5C/BMfzKRyHlraybiii1yQgCPzyX9ZOT+l914vZ9hSAWiPHOP0RmuJ
wPwRvkuLtMs1ZrKMrjgNAqWprBGmru8cyJF07okVXpA6g/2iHOPDeH3YZH7J2jl2
9+/Kg+qmVl7NpoXFRuJYLqPfFqkbfDsFQcwN9VRxmKKC+64Q5KHFdhvvdQ7QR/7q
fh+DMkbf/fbgAhxKv6cIF2X4Jgm8G5EDjWXe6IsJ3gV/y1LguVbAcWfT9Sgn8SGp
Wa1BKfvxA13QarRo70qIUPyGILw16S5suA5t6ERgQ2gXNaVKmncFMP80tnnHDwJc
88Jkv2Iwx+HZ0o+FsEJKBCPLou4fWJY5qERKJ679pUjig83sZbyyqixOXp94mMcN
8oM0+FnyaZLgZmdoMi7pLlN6b7P5+pd4lRDe30ofD3BeZy5NQ9bGTAaE/QARAQAB
tBFjc2lydEBzaWdtYS5jby5pZlkClgQTAQoADAUCZegY3wKZAQIbAwAKCRByApkx
m2W3WZSwD/42zZK18MOQjhNh+OIvhXFdKLyBb/kasI5Ol01DNalc6VdepW2wCFk3
Vb369kJc2UAK3djPxCcPQaRkj2+91PAgTD/sV7jerHunK/kJL/ZkAcBfzvbd0vB7
LLh91Ivha4ltgD+L2eOi1G5Hf/dIb6u5vpdS1DNo6Oaz2XFBmQRWK50dRMUb/sKN
0YIZNA1fG25eIlF3fpwrtjcYh1XyhJQwPIyOBszQ8ncO8hsh+hSfcQ5LVzZPOGtb
+ysjXwC1ckIdqmbW1cwsWES1HdrgpEIkuixA2OUruzm5oWsDr1iHjJAr4kHYH7ZH
kFQfzySznEmGy+SbjW0dL4fbGWsdjGsum4iLRKE3Iov6AkJiBv4zE2yDAkRpqb4s
6XRuHOutN2FB9osBT1rl4JjuJ5YurwQ67F+NT8U9spytNTfYrLXbTcW/8JOMopxd
wyMd6hB3hbydSQco9S79Tgp2ZA0hN5LEUJW0CAHPW94mdqIMZOiL0blnFxs35kWd
kRoQHvQJmU/qr6TkNBACjqQEtKm6iR788NUEcTsNSOyR0Z8SBb5H8MayVjyvVf7C
O+1SlcnMGJ2TMj5A+ggeLt2jL87yBOOw7QNa11QKJ0Xh17NxT+TcSXKHLpbWQgy9
aaH02EOp8SBvuF+1WxrkITxFR6iPX4KR26ZHzj0OfWrH7vbjadpC+bkBDQRl6Bjf
AQgAmGDNKuK03KoV9lbEjJNaKKO4NpajWLljNv/d9zdIxMje+Y5KFNZranor/Xi5
4TSVzG2aCtQw1PxIuZiXUnCluII1UC1JOqxIDOG1qm63SOV4M8nsHiAeqLMgCXOj
FhPisyju4z74T/NT2RDUtq3C/OLP1KJXyiFqd3H0JqUkUQEfakOBCVuaq7N0I7x3
oR0xWgGJ3cgeJLxznfOMasUd75ptYBZqu9roWciu0dmg80zJUaffQVTOL6Xqu7Eq
8+jcUOeJm4G1zfT5AhODIHGoWC5mc30ZstunhJq4LiBWGD6WtlFhm4j4RMc62Ylj

fGwNRb/+wkRGV26awq3aTUpDcQARAQABiQIfBBgBCgAJBQJl6BjfAhsMAAoJEHIC
mTGbZbdZAG4P/2QpQvztvhTwYgIjEM0E22D7LyddypxbVWRcjdrs/2xFp+EYL1TI
UAwV98eXz3aFrDZK9GMkXDXUeTDfl9zck7LYLauI/izXLWSHYOOjeiRcquzByroK
dd945xBeVu6BXrmMVzaEasbe1URLOCfpdUPG8ioIXJK8le29jTJSPo8psejPi4k4
2y0c3GJO/yS7pimjgsf0W/Jr0HnG3Vkgrbwn4USjYfuHmXP3eC4OSpSd/o2z9UJY
f4HubPRLQJGkrrrBg6H8UclHtihZ9S1BfL55unqPZfIhfQlh1dzyRNALMzkgP9oa
8Of9KQxXId5hcMVoAfQIk/sYy6D1+RuNQBNboZCuLof1rMpiHyJ7+ykaaFDsfF0/
vS2rcl8nqZwbAyWlxK+5fmCgOnIFO50xA4t/0aVAWG/QYxBEP84Wn6wAnMKqoh+U
g1rFmPUy4eMQkkEiRd0x7hZ2xqUf5uok7up2L/ivkAXfUCi+hdrxzMkE7JvilJPu
7WsB+9ZxIdtBzBwpccXrZXVXcMRcOHPjRWWJcDY22baCQVmFLYCeGYZ9PItNuEgb
XkOaPWuQYTY+qJqWmTtfkBuy9YEcMSo0YX0CQN1tX5YdOClEUBV47FE24xwKYJQ1
KscaNIx17POoG2HD3S2yVsu+Mng+/pxOyIRHdcgj2ejwLAnb6FUeTkyj
=u/3T
-----END PGP PUBLIC KEY BLOCK-----

File PGP *key* ini tersedia pada :
https://www.telkomsigma.co.id/csirt/publickey.asc

2.9. Anggota Tim

Ketua CSIRT Telkomsigma (CSIRT Coordinator) dijabat oleh General Manager Cyber Security Delivery and Operation PT Sigma Cipta Caraka. Susunan anggota Tim CSIRT Telkomsigma merupakan karyawan dari PT Sigma Cipta Caraka.

2.10. Informasi/Data lain

Tidak ada.

2.11. Catatan-catatan pada Kontak Tim CSIRT Telkomsigma

Metode yang disarankan untuk menghubungi Tim CSIRT Telkomsigma adalah melalui *e-mail* pada alamat csirt[at]sigma[dot]co[dot]id atau melalui nomor telepon (021) 5389186 ke Garuda Cyber Security Operation Center yang siaga selama 24/7.

3. Mengenai Gov-CSIRT

3.1. Visi

Visi Tim CSIRT Telkomsigma adalah menjadi pusat keunggulan dalam pengelolaan insiden keamanan komputer di Lingkungan PT Sigma Cipta Caraka dan mampu melindungi aset informasi yang dimiliki oleh PT Sigma Cipta Caraka, serta berkontribusi pada lingkungan siber yang lebih aman dan andal.

3.2. Misi

Misi dari Tim CSIRT Telkomsigma, yaitu :

a. Melakukan deteksi aktif dan pemantauan berkelanjutan terhadap ancaman keamanan komputer dan jaringan untuk mengidentifikasi potensi insiden keamanan.
b. Memberikan respons cepat terhadap insiden keamanan yang teridentifikasi untuk meminimalkan dampaknya dan memulihkan sistem yang terpengaruh.
c. Melakukan investigasi dan analisis menyeluruh terhadap insiden keamanan untuk mengidentifikasi penyebabnya, mengumpulkan bukti digital, dan mengembangkan pemahaman yang mendalam tentang insiden tersebut.

d. Memberikan edukasi dan pelatihan kepada anggota organisasi dan masyarakat terkait praktik keamanan yang lebih baik untuk mencegah insiden keamanan komputer.
e. Berkolaborasi dengan entitas internal dan eksternal, termasuk lembaga penegak hukum, vendor keamanan, dan Tim CSIRT lainnya, untuk meningkatkan pertukaran informasi dan koordinasi tanggapan.
f. Membantu dalam pengembangan kebijakan keamanan komputer dan prosedur respons keamanan yang efektif.
g. Melakukan pemantauan lingkungan siber secara aktif untuk mendeteksi ancaman yang berkembang dan mengidentifikasi kerentanannya yang mungkin ada.
h. Melakukan riset keamanan untuk memahami tren dan perkembangan terbaru dalam ancaman keamanan dan teknik serangan.
i. Mengembangkan atau menggunakan alat keamanan yang diperlukan untuk mendukung deteksi, pemantauan, dan respons insiden keamanan.

3.3. Konstituen

Konstituen Tim CSIRT Telkomsigma meliputi :

a. Pengguna sistem elektronik di lingkungan PT Sigma Cipta Caraka.
b. Seluruh konstituen Tim CSIRT Telkomsigma melaksanakan rekomendasi dan/atau imbauan yang dikeluarkan oleh CSIRT Coordinator dari Tim CSIRT Telkomsigma.

3.4. Sponsorship dan/atau Afiliasi

Tim CSIRT Telkomsigma merupakan bagian dari PT Sigma Cipta Caraka sehingga seluruh pendanaan untuk penyelenggaraan bersumber dari:

a. Anggaran operasional PT Sigma Cipta Caraka.
b. Sumber pendapatan lainnya yang sah.

3.5. Otoritas

Berdasarkan Surat Keputusan Direktur Delivery and Operation PT Sigma Cipta Caraka Nomor: SK.142/DVR/CPDS/2023 Tentang Pembentukan Cyber Security Incident Response Team (CSIRT) Telkomsigma yang disahkan pada 31 Oktober 2023, Tim CSIRT Telkomsigma adalah Tim yang bertugas atas penanganan insiden siber yang terjadi di sistem informasi internal Telkomsigma yang berdampak atau mempengaruhi sistem keuangan atau merusak reputasi Telkomsigma, atau merupakan pelanggaran terhadap hukum negara yang berlaku.

4. Kebijakan – Kebijakan

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

Tim CSIRT Telkomsigma melayani penanganan insiden siber dengan jenis berikut :

a. *Service Interrupt.*
    1) *Denial of Service*
    2) *Mail Bomb*
    3) *Ping Attacks*
    4) *Multiple Request Attack*

5) *Root Compromise*
6) *Packet Floods*
7) *RC Bots*
8) *Virus Infection*
9) *Brute force*

b. *Malicious Communication.*
   1) *Threats*
   2) *Hate Mail*
   3) *Harassment Mail*
   4) *IRC Abuse*
   5) *Flaming directly to Individual*

c. *Unsolicited Bulk Email.*
   1) *Spam*
   2) *Chain Mail*
   3) *Mass Mail*

d. *Application (SQL Injection).*

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

a. Kerja sama antar Organisasi atau Instansi dapat dilaksanakan dengan tujuan untuk saling berbagi sumber daya pengetahuan, keterampilan dan informasi mengenai keamanan Siber.
b. Kerja sama antar Organisasi atau Instansi dilakukan dengan tetap memperhatikan kebijakan, sistem prosedur dan perlindungan kepentingan PT Sigma Cipta Caraka.

4.3. Komunikasi dan Autentikasi

Untuk komunikasi biasa Tim CSIRT Telkomsigma 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

Layanan tanggap insiden siber dari CSIRT Telkomsigma berupa:

a. Layanan Reaktif adalah layanan yang terkait dengan kebutuhan melakukan respons terhadap insiden siber termasuk penangkalan, penindakan dan pemulihan siber, meliputi tugas peringatan, penanganan insiden, kerentanan, artefak, dukungan teknis, koordinasi dan respons, analisis kerentanan dan layanan interaksi (help desk).
b. Layanan Proaktif adalah layanan yang mendeteksi dan mencegah serangan siber sebelum ada dampak nyata, meliputi tugas pengumuman, pengawasan teknologi, uji kesesuaian, konfigurasi perangkat dan infrastruktur, layanan deteksi ancaman dan diseminasi informasi.
c. Layanan Manajemen Kualitas Keamanan adalah layanan yang mendukung kegiatan reaktif dan proaktif, meliputi tugas kebijakan dan pelatihan analisis risiko, perencanaan pemulihan bencana, kelangsungan kegiatan, konsultasi keamanan, peningkatan kewaspadaan, dan pengelolaan infrastruktur CSIRT.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke cisrt[at]sigma[dot]co[dot]id dengan melampirkan sekurang-kurangnya :

a. Foto/*scan* kartu identitas
b. Bukti insiden berupa foto atau *screenshoot* atau *log file* yang ditemukan
c. Atau sesuai dengan ketentuan lain yang berlaku

7. *Disclaimer*

Tidak ada.