RFC 2350

Cyber Incident Response Team (CIRT) PERTAMINA

1. Informasi Dokumen

Dokumen ini berisi deskripsi CIRT Pertamina menurut RFC 2350. Diantaranya berisi informasi dasar tentang CIRT Pertamina, tanggung jawab dan layanan yang ditawarkan, serta narahubung.

1.1. Tanggal Pembaruan Terakhir

Ini adalah versi 1.1 pada 22/10/2024. Format tanggal Indonesia adalah DD/MM/YYYY.

1.2. Daftar Distribusi Notifikasi

Tidak ada daftar distribusi notifikasi per 22/10/2024.

1.3. Lokasi Dokumen

Versi terbaru dari dokumen ini selalu dapat ditemukan di:
https://cirt.pertamina.com/rfc-2350/

Untuk tujuan validasi, versi ASCII yang ditandatangani GPG dari dokumen ini ada di:
https://cirt.pertamina.com/pgp-public-key/

Kunci yang digunakan untuk penandatanganan adalah kunci CIRT Pertamina sebagaimana tercantum pada bagian 2.8. Kunci Publik dan Informasi Enkripsi.

2. Informasi Kontak

2.1. Nama Tim

Cyber Incident Response Team (CIRT) Pertamina.

2.2. Alamat

Jalan Medan Merdeka Timur 1A
Jakarta Pusat, 10110
Indonesia

2.3. Zona Waktu

Kami berlokasi di Asia, Jakarta - Indonesia Waktu Barat yaitu GMT+07:00.

Format waktu Indonesia adalah HH:MM:SS dalam notasi 24 jam – tanpa AM/PM.

2.4. Nomor Telepon

Telp. 1500234

2.5. Nomor Faksimili

-

2.6. Telekomunikasi Lainnya

-

2.7. Alamat Surat Elektronik

Mohon kirimkan laporan insiden keamanan informasi ke infosec[at]pertamina[dot]com

2.8. Kunci Publik dan Informasi Enkripsi

CIRT Pertamina menggunakan kunci penandatanganan untuk tujuan operasional. Harap enkripsi email sensitif dengan kunci publik CIRT Pertamina dan kirim ke infosec@pertamina.com.

Kunci PGP CIRT Pertamina adalah:

Bit: 4096

ID: 0x57C659DE

Fingerprint: 32B6DCAD6E327FFE6E8AA4709046A1E957C659DE

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

mQINBGcXS+kBEAC0Ple/Jto6TqCHlGaGAzWCFOmjuS2+3gt0ZewE5ijS+js5HXAj
u250z+8hYCqqhUZ7e43SsxU4fRdf3wWYMVY8KjBmF6kqpss9iV1eDoxWephnhlFm
/fUZCtQTSuT1Q5yI8dL/T0wyfobrPfXGZQWPJtcxsHoQeSV8ayHRFXJI+tF+4hlj
IZYNQD2uLffDexBAir9JxryZiu2eeRMGBuaIsqcFCNUhDM7F58yU3g0KfiEUEFaR
BcOW1hHqvy4DuU78c+vfcKlCJtbQoPYHDo1a3lUIuHcoqD8AH7p965X5+7WRG/K8
vGbgAFPcb2rW1h4dIG6w8Hkoc71yPwRsLdZsk1RtCCT5NRriruqcHVxybJ2184c5
baY0M2L4NPJHF81TsjMXhRhH12VK5ZoVHQlaCuKuogWzE6v/z5rFiiMjaaAGEbqX
+ypUjureZg77VTcm6UZqQFN3kd3VKZqtutmhUN/z+3FUXRm8vyhy/H7oOsb+4i0g
Y2IEAYgsTPBSFYjEt/FrfB93BUN2JPNG+rrvaE/Dcdp9yo0gTcH6LmPhure5CTyZ

jzkj0kiFCg17Mf2/b2O26Qm+4yLY9x9vhOXAKL1phUIWLxVFO4+FAzTHrzB2+Tq6
LFqe75xqK1GZJB+VTHImYthBBdxjUtalLm8ao6r3xXnW2LOPXAES6trLSQARAQAB
tClJbmZvc2VjIFBlcnRhbWluYSA8aW5mb3NlY0BwZXJ0YW1pbmEuY29tPokCVwQT
AQgAQRYhBDK23K1uMn/+boqkcJBGoelXxlneBQJnF0vpAhsPBQkFo3/nBQsJCAcC
AiICBhUKCQgLAgQWAgMBAh4HAheAAAoJEJBGoelXxlneDZMP/Aj4CcYVyFzbG4i
a
eLs0tOkP1Wv6Wqj+8JArR+y9xgVSumQajvgemhK9bl3ATpUWrlwqI/PbGaAzV6k8
rabriFtmnH4+DDemGNpUQ09vv2Mz0HBF7E73IIrlLqgDBQkU+b1xBB0U8xIIwFDe
ihQmhRnUCD+wLj1v2rPMNGnd7DlaBIO/DqkKL24Y/Dh/ULdVeiQseVaFYLrTJ+3M
HTqCilXuo3eTkTm6YwXRM2E+cnw6bbl1aKoKaCpt0Qwrf7ZUNEAJujEHBJQi54MX
2fgwzImxlJX8aJdSjTtnHdQYthyfvRaAp+QKyS52uJ+ipCzEBiC1UfHsPZfd1HYn
sJXWsSES8CqNSUiMm7ehfruO97VNnACW935l0qne9UcKitMB5onGfqUavwZG+pI
R
B+M1MJpRuC7DfpzvElNt82biYGmysUNiFVLm8h12wjarnz0VHqazACugs9AJrYBe
f+KPBDfRZOglrz7wzDiTmOtagTJ9wRFYlGP1WAEXZj05UnW22uYkTsflxPpgvx2J
HdUv6jzFZZibZoPOk+5DE9aMJ3sLWqxv8RKOhE/F91e7pee0kKTKJ7kDtDCIJQbb
C611ph6UwQ2hOarSOSMQaCLf+J+bU0ULRdu7+gRQS1CGaIq4rQ5BnTFCNWNKk
qIz
+V4DrT9CntSUht4+V/Nl3MKtUm4V
=xGLg
-----END PGP PUBLIC KEY BLOCK-----

2.9. Anggota Tim

Hananto Susilo, selaku Team Lead CIRT Pertamina.

2.10. Informasi Lainnya

Informasi lebih lanjut mengenai CIRT Pertamina dapat dilihat di: https://cirt.pertamina.com/

2.11. Titik Kontak Pelanggan

Metode yang dipilih untuk menghubungi CIRT Pertamina adalah melalui e-mail. Untuk laporan insiden dan masalah terkait keamanan informasi, silakan langsung email ke infosec@pertamina.com

Jika tidak memungkinkan – atau karena alasan keamanan tidak dapat menggunakan email, Anda dapat menghubungi atau menghubungi kami melalui saluran tetap – telepon di 1500234.

Operasi CIRT PERTAMINA pada umumnya dibatasi pada jam kerja biasa:
Dari jam 8:00 pagi sampai jam 5:00 sore yaitu GMT +07:00
Time Zone Asia, Jakarta – Waktu Indonesia Barat
Senin sampai Jumat, tidak termasuk Hari Libur Nasional.
Perhatian: Kami akan merespon HANYA SELAMA JAM TERSEBUT.

3. Piagam

3.1. Informasi Organisasi

CIRT Pertamina merupakan organisasi ad-hoc yang terdiri dari fungsi ICT terkait cyber security di seluruh Pertamina Group yang ditandatangani oleh Direktur Penunjang Bisnis, PT Pertamina (Persero).

3.2. Pernyataan Misi

Tujuan utama CIRT Pertamina adalah sebagai tim penanganan insiden siber pada level korporat, untuk mengkoordinasikan dan menangani insiden di seluruh Pertamina Group.

3.3. Konstituen

Konstituen CIRT Pertamina adalah:

- Dewan Komisaris dan Direksi PT Pertamina (Persero);
- Enterprise IT, Direktorat Penunjang Bisnis, PT Pertamina (Persero);
- Shared Service ICT, Direktorat Penunjang Bisnis, PT Pertamina (Persero);
- Sub Holding CIRT Sektoral (Gas, Upstream, Commercial & Trading, Refinery & Petrochemical, Power New & Renewable Energy, Integrated Marine Logistics);
- IT Anak Perusahaan dan departemen yang terkait dengan organisasi CIRT Pertamina;
- IDSIRTII/CC sebagai CSIRT Nasional Indonesia.

3.4. Sponsor dan/atau Afiliasi

CIRT Pertamina dibentuk oleh internal Pertamina. Artinya, sepenuhnya hanya dibiayai oleh PT Pertamina (Persero).

3.5. Wewenang

CIRT Pertamina memiliki tujuan utama untuk menangani segala jenis insiden keamanan siber dan mengkoordinasikan inisiatif keamanan siber lainnya di seluruh Pertamina Group.

4. Kebijakan

4.1. Jenis Insiden dan Tingkat Dukungan

CIRT Pertamina berwenang untuk menangani segala jenis insiden keamanan siber, yang terjadi atau mengancam konstituen kami (lihat bagian 3.3 Konstituen) dan kepentingan strategis siber, yang memerlukan koordinasi lintas organisasi, terutama di tingkat korporasi. Kami akan memberlakukan tindakan pencegahan apa pun yang diperlukan dan berkomitmen untuk memberi informasi kepada konstituen kami tentang potensi kerentanan apa pun. Perhatian khusus akan diberikan pada isu-isu yang secara langsung mempengaruhi infrastruktur kritis.

4.2. Kerjasama, Interaksi dan Keterbukaan Informasi

CIRT Pertamina akan bekerjasama dengan organisasi lain di bidang keamanan siber dan infrastruktur Internet. Keterlibatan tersebut sering membutuhkan pertukaran data atau informasi mengenai insiden dan masalah. Namun demikian CIRT Pertamina berkomitmen untuk melindungi privasi para konstituennya dan oleh karena itu (dalam keadaan normal) hanya menyampaikan informasi terbatas dan anonim kepada pihak lain, kecuali beberapa perjanjian kontrak berlaku, misalnya Non Disclosure Agreement (NDA) atau Pernyataan Kerahasiaan.

4.3. Komunikasi dan Otentikasi

Untuk komunikasi biasa, yang tidak mengandung informasi sensitif, CIRT Pertamina akan menggunakan metode konvensional seperti e-mail yang tidak terenkripsi.

Untuk komunikasi yang aman, email atau telepon terenkripsi PGP akan digunakan. Jika perlu untuk mengautentikasi seseorang sebelum berkomunikasi, ini dapat dilakukan baik melalui rekan kepercayaan yang ada atau bahkan pertemuan tatap muka jika perlu.

5. Layanan

5.1. Tanggapan Insiden

5.1.1. Triase Insiden

Menentukan apakah insiden dan pelapornya valid dan otentik. Menilai informasi terkait dan memprioritaskan insiden.

5.1.2. Koordinasi Insiden

Menentukan organisasi yang terlibat. Menghubungi orang yang bertanggung jawab untuk menyelidiki dan mengambil tindakan yang tepat. Memfasilitasi kontak dengan pihak lain yang dapat membantu menyelesaikan insiden tersebut. Kirim laporan ke Tim CSIRT terkait lainnya, seperti IDSIRTII/CC jika diperlukan.

5.1.3. Penyelesaian & Pemulihan Insiden

Menginfokan tim keamanan informasi lain yang terlibat untuk mengambil tindakan yang tepat. Menindaklanjuti kemajuan, meminta laporan, melaporkan kembali dan eskalasi ke otoritas/manajemen yang lebih tinggi. CIRT Pertamina membantu tim keamanan lainnya dalam aspek teknis dan manajemen insiden sesuai kebutuhan. Kami terlibat dalam segala jenis proses mitigasi dan remediasi atas permintaan konstituen.

5.2. Kegiatan Proaktif

Melakukan monitoring Security Operation Center level korporat– untuk mendeteksi ancaman yang diketahui, anomali dan segala jenis potensi masalah keamanan di dalam Infrastruktur IT Pertamina. Menyediakan informasi terkait keamanan informasi, intelijensi ancaman, pemantauan aktual dan hasil analisis insiden. Mengelola sosialisasi untuk meningkatkan kesadaran keamanan informasi kepada konstituen, pihak terkait dan memberikan pelatihan keamanan siber secara berkala.

6. Formulir Pelaporan Insiden

Silakan kirim informasi laporan insiden keamanan ke infosec[at]pertamina[dot]com dengan disertai ID dan bukti insiden (log atau file) dalam lampiran.

7. Penyangkalan

Setiap tindakan pencegahan yang akan diambil dalam persiapan informasi, termasuk peringatan dan pemberitahuan, CIRT Pertamina mengasumsikan tidak akan

bertanggung jawab atas kesalahan, kelalaian atau kerusakan akibat penggunaan informasi yang terkandung di dalamnya.

Informasi ini harus digunakan hanya seperti yang telah disebutkan.