RFC 2350

CIRT-SH R&P

1. Informasi Mengenai Dokumen

Dokumen ini berisi deskripsi CIRT-SH R&P berdasarkan RFC 2350, yaitu informasi dasar mengenai Cyber Incident Response Team Subholding R&P, menjelaskan tanggung jawab, layanan yang diberikan, dan cara untuk menghubungi Cyber Incident Response Team Subholding R&P.

1.1. Tanggal Update Terakhir

Dokumen merupakan dokumen versi 1.0 yang diterbitkan pada tanggal 25 August 2023.

1.2. Daftar Distribusi untuk Pemberitahuan

Tidak ada daftar distribusi untuk pemberitahuan mengenai pembaharuan dokumen.

1.3. Lokasi dimana Dokumen ini bisa didapat

Dokumen ini tersedia pada :
kpi.pertamina.com/Tim_Keamanan_Siber/rfc2350.pdf (versi Bahasa Indonesia)

1.4. Keaslian Dokumen

Kedua dokumen telah ditandatangani dengan PGP *Key* milik CIRT-SH R&P. Untuk lebih jelas dapat dilihat pada Subbab 2.8.

1.5 Identifikasi Dokumen

Dokumen memiliki atribut, yaitu:
Judul : RFC 2350 CIRT-SH R&P;
Versi : 1.0;
Tanggal Publikasi : 25 August 2023;
Kedaluwarsa : 03 Juli 2025.

2. Informasi Data/Kontak

2.1. Nama Tim

Kepanjangan dari CYBER INCIDENT RESPONSE TEAM Subholding R&P
Disingkat : CIRT-SH R&P.

2.2. Alamat

Patrajasa Tower Lantai 9
Jl. Jend. Gatot Subroto Kav. 32-34 Jakarta Selatan 12950

2.3. Zona Waktu

Jakarta (GMT+07:00 Jakarta)

2.4. Nomor Telepon

021 135

2.5. Nomor Fax

-

2.6. Telekomunikasi Lain

021 - 3815111 ext 2580

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

kpi.cyber.security@pertamina.com

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

Bits: 2048

ID: A942 D7DA 1EFF 23D3

Fingerprint: A69F2A925D51829A1BDD4D3EA942D7DA1EFF23D3

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

mQENBGTUiSMBCACoNHSXC3CHnM3ujWBuBE6c0pVQlJwa23xSoadIDEm/hWPdJ/gJ
ud/wTGMMU0zcnCokNKo7RBtnjstRJfyKTv3iCP0Bo0nPImQYJURL+Vqeux/XzZ8+
kwgzO5m9wXAEwNgdIOHFjKXtMxo9JsuV1yO3wyko6pc0WJk7rA20XmJVt/BMYEMO
MlhOTqPEo7M+dhmDosjRCOPVyppioDQmxUBw8alja/ccg4U2R28BIpYHhsHos9bA
qu2psU1/TLNq3BlR+rW7VSLq1wXWC77XhwiSl66AwXoH0jY+548D782RVzGOmGxf
FRUu1lifT/6FBZlRhtDANOtGgZaCaQHbflGlABEBAAG0NWtwaS5jeWJlci5zZWN1
cml0eSA8a3BpLmN5YmVyLnNlY3VyaXR5QHBlcnRhbWluYS5jb20+iQFXBBMBCAA
BBQJUiEEpp8qkl1Rgpob3U0+qULX2h7/I9MFAmTUiSMCGwMFCQWk0a0FCwkIBwICIgIG
FQoJCAsCBBYCAwECHgcCF4AACgkQqULX2h7/I9ODxAgAoieF3QHhrGFBQRyvLCgb
5witSwqB5iPrsSqyhw9nrNyFvOCWEE65yKIY/zH1pyA+xwvbGbwaxjfBykn6z6rX
AkNPnCVSvnPfQdYsL245C6jucFC7X4RTzaYa3Gz/io/3M8Xra5NMei2c4VUEPR8T
V1bYv9LEDxcd7RLLsRRx5WhUBgkSx87CwqDDB2sTdy2XCV1oPLF3u55EKjXnsmrV
Rnc53nOgAqv5zjzQcs+2VkdrJ+oR82MsDXlvt6/ROX/fPKSeuS3k7IWv0tKJ/zGH
6IL9novZfjespNLI6eky4QZliKM3b0Kj7IcxatI34tnxbKIPNUPadLsneUB9uB7IL
K7kBDQRk1IkjAQgAsdios/frN6xbCmDO+YfNq623wNE9qNF3mbgKgxCOWuk0DQEf
oddtHHGiwLBOn194tvDktH3+gSs63SbACz9JXOVnHGeM7EV4q7qbfBzQn7Z+FGDW
+D/EJMhUYGIRQYmx5+iPsxVQiCpzF/vCRjlGFi2DnDbof5BPCI2YC3ImSsobCTMy

PujZkN8xT9lyJZEI1nBb0xRffsvGb0XPgLNBGJ7X78DNgSUqlVQXF8ZLMv68TZsi
nvDsvn8T2tByLfAV2rFkxs3QHoRpaZYGAYudcGnvV6GjMs7xZid6czzTcEFQfHNQ
Kw05j6et0C644TzheK7gp2QC6L4NxdV44aqpgwARAQABiQE8BBgBCAAmFiEEpp
8q
kl1Rgpob3U0+qULX2h7/I9MFAmTUiSMCGwwFCQWk0a0ACgkQqULX2h7/I9PYdA
f/
VZhaLfOWdhV9u5i1qLTXLkHUZq7Uu4OwaUC3dtX68KPPUuqR8Sh4t4SWZu6tl4F
C
0BdmAlxyvJhEUruDFFCPbL1u5TCejRf8hEGo36saRfR3fRNV9K3DTaPed3OETY+
X
C7Oav3J4WshTYO7h8SLzKnczuqqQYAKoQy2D9gs9tpslzPLxZIvl/uGtkDza/QtA
N0ViRdxvl/aLhhDcEUGFlp+1sv6osJeJerhvvVjUwgsiSpA0jxu5mC58HsdFHeyH
fOV8actjXuXA/FrxUZo+NdNor1y5/1SOJSbsi2DQwJjuJzDA+HMV6By4X6VBGJEo
p917wEh9VISLaCA8Nfzcng==
=R1u8
-----END PGP PUBLIC KEY BLOCK-----

File PGP *key* ini tersedia pada :
kpi.pertamina.com/Tim_Keamanan_Siber/kunci-public.asc

2.9. Anggota Tim

Isnanto Nugroho S selaku Head of Steering Committee CIRT-SH R&P. Nur Rachmawati, selaku Team Lead CIRT-SH R&P .

2.10. Informasi/Data lain

-.

2.11. Catatan-catatan pada Kontak CIRT-SH R&P

Metode yang disarankan untuk menghubungi CIRT-SH R&P adalah melalui *e-mail* pada alamat kpi.cyber.security@pertamina.com atau melalui nomor telepon 021 - 3815111 ext 2580 pada hari kerja jam 07.00 - 16.00.

3. Mengenai CIRT-SH R&P

3.1. Visi

Visi CIRT-SH R&P adalah World Best Class Cyber Security In Refinery

3.2. Misi

Misi dari CIRT-SH R&P, yaitu :

a. mendeteksi dini ancaman keamanan siber dan merespons dengan cepat terhadap insiden yang terjadi
b. menerapkan langkah-langkah pencegahan keamanan siber yang aktif dan pasif
c. melakukan penyelidikan mendalam untuk memahami sumber, metode, dan dampak dari insiden keamanan siber
d. berfokus pada pemulihan sistem dan data yang terpengaruh.
e. meningkatkan kesadaran tentang keamanan siber

f. berkolaborasi dengan departemen internal dan pihak eksternal untuk merespons insiden
g. meningkatkan kemampuan dengan melakukan evaluasi pasca-insiden
h. melakukan keamanan proaktif untuk mengidentifikasi kerentanan sebelum menjadi ancaman nyata
i. mengembangkan dan menguji rencana respons darurat untuk berbagai jenis insiden, memastikan bahwa tim siap untuk bertindak dalam situasi kritis.

3.3. Konstituen

Konstituen CIRT-SH R&P meliputi Seluruh Stakeholder PT Pertamina Subholding R&P seperti pekerja, direksi, vendor dan customer

3.4. Sponsorship dan/atau Afiliasi

Pendanaan CIRT-SH R&P bersumber dari Anggaran Biaya Operasional Perusahaan

3.5. Otoritas

Otoritas yang mungkin dimiliki oleh CIRT:

a. mengambil keputusan sehubungan dengan penanganan insiden keamanan siber
b. mengakses sistem, jaringan, atau data yang terkait dengan insiden
c. mengisolasi sistem atau jaringan yang terinfeksi atau terdampak oleh insiden keamanan
d. berkomunikasi dan berkoordinasi dengan pihak eksternal
e. menyampaikan informasi kepada manajemen, fungsi terkait, atau pihak eksternal, tergantung pada kebijakan dan tingkat eskalasi yang ditetapkan
f. mengembangkan dan merevisi kebijakan keamanan siber, panduan tindakan darurat, atau pedoman operasional lainnya
g. melaporkan hasil penyelidikan, tindakan yang diambil, dan hasil pemulihan kepada pihak terkait dan manajemen
h. mengadakan pelatihan keamanan siber dan kesadaran bagi pekerja dan stakeholder perusahaan lainnya

4. Kebijakan – Kebijakan

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

CIRT-SH R&P melayani penanganan insiden siber dengan jenis berikut:

a. Malware dan Serangan Virus
b. Serangan DDoS (Distributed Denial of Service)
c. Penyusupan dan Pengambilan Akun
d. Pencurian Data dan Pelanggaran Keamanan
e. Penyalahgunaan Sistem dan Jaringan
f. Eksploitasi Kerentanan
g. Insiden Fisik terkait Teknologi IT dan OT
h. Kehilangan atau Pencurian Perangkat
i. Serangan Phishing dan Spear Phishing

4.2. Kerja sama, Interaksi dan Pengungkapan Informasi/ data

Berikut adalah beberapa cara untuk melakukan kerjasama dan berbagi informasi dalam lingkup keamanan siber:

1. Pembentukan Kemitraan: Pertama-tama, identifikasi CSIRT atau perusahaan lain yang relevan dengan sektor industri atau lingkungan yang sama. Pembentukan kemitraan formal atau informal memungkinkan pertukaran informasi yang lebih efisien.
2. Perjanjian Kerahasiaan (Non-Disclosure Agreement): Sebelum berbagi informasi sensitif, pastikan untuk menandatangani perjanjian kerahasiaan atau kesepakatan bersama untuk melindungi informasi yang dibagikan.
3. Forum dan Grup Diskusi: Mengikuti forum atau grup diskusi di bidang keamanan siber di mana para profesional dapat berinteraksi, bertukar pengalaman, dan berbagi informasi terkini tentang ancaman siber.
4. Mitra Intelijen Keamanan: Berkolaborasilah dengan mitra intelijen keamanan yang menyediakan informasi tentang ancaman terbaru, malware, dan metode serangan yang mungkin mempengaruhi Perusahan.
5. Pemantauan Bersama (Joint Monitoring): Lakukan pemantauan bersama terhadap aktivitas jaringan dan sistem untuk mendeteksi dini ancaman dan insiden. Ini dapat membantu memperoleh wawasan yang lebih luas tentang tren serangan.
6. Scanning Bersama: Lakukan pemindaian sistem dan aplikasi bersama dengan CSIRT lain untuk mengidentifikasi kerentanan dan mendapatkan pemahaman yang lebih baik tentang risiko.
7. Laporan Insiden Bersama: Jika terjadi insiden, berbagi informasi tentang insiden dengan CSIRT atau perusahaan lain untuk mendapatkan wawasan lebih lanjut tentang teknik serangan, dampak, dan cara merespons.
8. Latihan dan Simulasi Bersama: melakukan latihan dan simulasi respons insiden bersama dengan CSIRT lain untuk menguji rencana dan kesiapan dalam menghadapi skenario insiden yang kompleks.
9. Pertukaran Pengetahuan: Berbagi laporan dan analisis tentang insiden yang terjadi, termasuk cara penanganan dan tindakan perbaikan yang diambil, sehingga dapat menjadi pembelajaran bagi pihak lain.
10. Pertemuan dan Konferensi: menghadiri pertemuan, konferensi, atau lokakarya tentang keamanan siber di mana kita dapat berinteraksi langsung dengan para profesional dari perusahaan lain.
11. Pusat Informasi Keamanan: Ikuti atau berkontribusi pada pusat informasi keamanan yang menyediakan wawasan dan solusi tentang ancaman dan kerentanan terkini.
12. Laporan Kejahatan Siber: Jika insiden melibatkan kejahatan siber atau pelanggaran hukum lainnya, kolaborasi dengan lembaga penegak hukum atau agen penegak hukum untuk memberikan informasi yang relevan.

4.3. Komunikasi dan Autentikasi

Informasi Biasa:

Untuk berbagi informasi biasa yang tidak memiliki sensitivitas tinggi, CIRT dapat menggunakan media komunikasi yang lebih umum dan mudah diakses, seperti:

1. Email: Email adalah saluran komunikasi standar yang dapat digunakan untuk pertukaran informasi rutin, pemantauan, dan koordinasi antara anggota tim dan pihak terkait.
2. Grup Pesan Instan: Aplikasi pesan instan atau alat kolaborasi seperti Whats up, Microsoft Teams dapat digunakan untuk percakapan real-time, berbagi berita terbaru, dan memberikan pembaruan berkala.
3. Laporan: CIRT membuat buletin keamanan atau laporan berkala yang memuat ringkasan tentang ancaman terbaru, tren, atau perkembangan penting dalam keamanan siber.

Informasi Terbatas/Rahasia:

Untuk informasi yang memiliki tingkat keamanan atau kerahasiaan lebih tinggi, CIRT harus menggunakan media komunikasi yang lebih aman dan terenkripsi untuk melindungi informasi sensitif, seperti:

1. Aplikasi Pesan Terenkripsi: Gunakan aplikasi pesan yang menawarkan enkripsi end-to-end, seperti WhatsApp, untuk berbicara tentang informasi rahasia.
2. Pusat Kontrol Keamanan: Perusahaan dapat memiliki pusat kontrol keamanan yang aman dan terenkripsi di mana CIRT dapat berkomunikasi dan berbagi informasi sensitif.
3. Jaringan Virtual Pribadi (VPN): CIRT dapat menggunakan VPN untuk mengamankan komunikasi dan mengakses jaringan internal secara aman dari lokasi yang berbeda.
4. Ruang Rapat Virtual Terenkripsi: Platform rapat virtual yang menyediakan enkripsi dan pengendalian akses dapat digunakan untuk diskusi rahasia antara anggota tim.
5. Instrumen Pengarsipan Terenkripsi: Bagi dokumen atau informasi yang harus diarsipkan, pastikan menggunakan instrumen pengarsipan yang terenkripsi.
6. Kriptografi: Menggunakan alat kriptografi seperti kunci enkripsi untuk mengamankan konten yang dikirim dan diterima.
7. Pertemuan Tatap Muka: Untuk informasi yang sangat rahasia, pertemuan tatap muka dalam ruangan yang aman dan terjaga dapat digunakan

5. Layanan

5.1. Layanan Utama

Layanan utama dari CIRT-SH R&P yaitu :

5.1.1. Pemberian Peringatan Terkait Keamanan Siber

Pemberian peringatan terkait keamanan siber adalah langkah proaktif untuk mengidentifikasi, menganalisis, dan mengkomunikasikan ancaman atau risiko keamanan siber kepada entitas yang relevan. Berikut adalah beberapa komponen yang mungkin termasuk dalam layanan ini

1. **Pemantauan Ancaman**: CIRT melakukan pemantauan terus-menerus terhadap lingkungan keamanan siber, termasuk mengidentifikasi tren terbaru dalam ancaman siber, serangan yang sedang berlangsung, dan metode baru yang digunakan oleh penjahat siber.
2. **Analisis Ancaman**: Tim melakukan analisis mendalam terhadap informasi tentang ancaman siber yang ditemukan. Mereka memahami metode serangan, sasaran yang mungkin, dan dampak potensial yang dapat terjadi.
3. **Pengklasifikasian Risiko**: Berdasarkan analisis, CIRT mengklasifikasikan risiko dan ancaman berdasarkan tingkat keparahan, potensi dampak, dan probabilitas terjadinya. Ini membantu dalam menentukan prioritas tindakan yang harus diambil.
4. **Pemberian Peringatan Dini**: Tim memberikan peringatan dini tentang ancaman yang sedang berlangsung atau potensi ancaman di masa depan kepada pihak-pihak yang terkait, seperti manajemen senior, departemen terkait, dan entitas lain dalam perusahaan.
5. **Pemberitahuan Eksternal**: Selain pemberitahuan internal, CIRT juga dapat berkomunikasi dengan mitra bisnis, lembaga penegak hukum, atau penyedia layanan keamanan eksternal untuk membagikan informasi terkait ancaman siber yang relevan.
6. **Rekomendasi Tindakan**: Tim memberikan rekomendasi tentang langkah-langkah yang dapat diambil untuk mengurangi risiko atau menghadapi ancaman siber. Ini mungkin melibatkan tindakan pencegahan, perbaikan keamanan, atau penyesuaian taktik pertahanan.
7. **Pembaruan Teratur**: CIRT dapat menyediakan pembaruan berkala tentang tren ancaman siber, perubahan dalam lingkungan keamanan, atau ancaman baru yang muncul.
8. **Kesadaran Keamanan**: Layanan ini juga dapat mencakup upaya untuk meningkatkan kesadaran keamanan siber di seluruh perusahaan melalui pelatihan, kampanye informasi, atau sumber daya edukatif.
9. **Kolaborasi Industri**: Tim dapat berkolaborasi dengan entitas lain di sektor industri untuk berbagi informasi tentang ancaman yang bersifat sektoral atau umum.

5.1.2. Penanganan Insiden Siber

Penanganan Insiden Siber merupakan proses merespons dan mengatasi berbagai jenis insiden keamanan siber yang dapat terjadi dalam lingkungan teknologi informasi dan komunikasi perusahaan. Berikut adalah beberapa komponen yang mungkin termasuk dalam layanan ini:

1. **Deteksi dan Identifikasi**: CIRT akan mendeteksi dan mengidentifikasi insiden keamanan siber dengan memantau aktivitas jaringan, sistem, dan aplikasi secara aktif. CIRT akan menggunakan alat dan teknik khusus untuk mengidentifikasi anomali dan tanda-tanda serangan.

2. **Evaluasi Dampak**: Setelah insiden teridentifikasi, tim akan melakukan evaluasi dampak insiden terhadap sistem, data, operasional, dan reputasi perusahaan. Ini membantu dalam menentukan skala dan prioritas respons.
3. **Isolasi dan Pengendalian**: Jika diperlukan, CIRT dapat mengambil tindakan untuk mengisolasi atau membatasi dampak insiden dengan memutuskan sementara akses ke sistem yang terdampak.
4. **Analisis Teknis**: Tim akan melakukan analisis teknis mendalam terhadap serangan atau insiden untuk memahami metode yang digunakan oleh penyerang, eksploitasi kerentanan, dan jalur pergerakan dalam jaringan.
5. **Pembersihan dan Pemulihan**: CIRT akan membersihkan sistem dari malware atau ancaman lain yang terlibat dalam insiden. Setelah itu, mereka akan memulihkan sistem ke kondisi normal dan memastikan data tidak terkompromi.
6. **Pemantauan Lanjutan**: Setelah insiden ditangani, CIRT akan terus memantau situasi untuk memastikan tidak ada aktivitas mencurigakan atau ulang serangan.
7. **Pelaporan dan Dokumentasi**: CIRT akan membuat laporan insiden yang mencakup detail analisis, langkah-langkah respons yang diambil, dan rekomendasi perbaikan keamanan. Dokumentasi ini dapat digunakan untuk pembelajaran di masa depan dan kepatuhan regulasi.
8. **Koordinasi dengan Pihak Terkait**: CIRT akan berkoordinasi dengan departemen terkait, manajemen senior, dan pihak eksternal seperti penyedia layanan keamanan, jika diperlukan.
9. **Pemberitahuan Hukum dan Regulasi**: Jika insiden melibatkan pelanggaran data atau kejahatan siber lainnya, CIRT akan mengikuti prosedur hukum dan regulasi yang berlaku untuk pemberitahuan dan pelaporan.
10. **Pemulihan Bisnis**: Jika insiden berdampak pada kelangsungan operasional, CIRT akan membantu dalam upaya pemulihan bisnis dan pemulihan operasional normal.

5.2. Layanan Tambahan

Layanan tambahan dari CIRT-SH R&P yaitu :

5.2.1. Penanganan Kerawanan Sistem Elektronik

Penanganan Kerawanan Sistem Elektronik merupakan serangkaian tindakan untuk mengidentifikasi, mengatasi, dan mengurangi risiko dari kerawanan atau celah keamanan yang dapat dieksploitasi oleh penyerang. Berikut adalah beberapa langkah umum yang dilakukan oleh CIRT dalam penanganan kerawanan sistem elektronik:

1. Pengidentifikasian Kerawanan: CIRT akan melakukan analisis dan evaluasi sistem elektronik untuk mengidentifikasi kerawanan yang ada. Ini bisa melibatkan pemeriksaan terhadap perangkat keras, perangkat lunak, konfigurasi, dan infrastruktur teknologi yang digunakan dalam perusahaan.

2. Penilaian Risiko: CIRT akan menilai risiko yang terkait dengan kerawanan tersebut, termasuk potensi dampak dan kemungkinan eksploitasi oleh penyerang. Dari sini, tim akan menentukan prioritas tindakan yang harus diambil.
3. Pengembangan dan Implementasi Tindakan Pencegahan: CIRT akan merancang dan menerapkan langkah-langkah pencegahan untuk mengurangi risiko dari kerawanan tersebut. Ini bisa termasuk konfigurasi ulang sistem, pembaruan perangkat lunak, penambahan lapisan keamanan, dan tindakan lainnya untuk mengurangi peluang eksploitasi.
4. Pemantauan dan Deteksi: Setelah langkah-langkah pencegahan diimplementasikan, CIRT akan terus memantau sistem elektronik untuk mendeteksi aktivitas yang mencurigakan atau tanda-tanda serangan yang potensial.
5. Respons Terhadap Ancaman Aktif: Jika CIRT mendeteksi ancaman atau serangan yang aktif, tim akan segera merespons dengan mengambil langkah-langkah untuk menghentikan serangan, mengisolasi kerawanan, dan memulihkan sistem ke keadaan yang aman.
6. Analisis Pasca-Kejadian: Setelah insiden ditangani, CIRT akan melakukan analisis mendalam terhadap kejadian tersebut untuk memahami bagaimana kerawanan dapat dieksploitasi dan bagaimana respons dapat ditingkatkan di masa depan.
7. Pelaporan dan Rekomendasi: CIRT akan menyusun laporan tentang insiden keamanan, tindakan yang diambil, dan rekomendasi untuk perbaikan lebih lanjut dalam sistem dan kebijakan keamanan.

5.2.2. Penanganan Artefak Digital

Artefak digital merujuk pada berbagai jenis data dan informasi yang dapat ditemukan dan diekstraksi dari sistem yang terlibat dalam suatu insiden keamanan. Layanan ini melibatkan identifikasi, analisis, dan pemrosesan artefak digital untuk membantu mengungkap sumber dan dampak insiden serta mendukung investigasi lebih lanjut:

Berikut adalah beberapa langkah yang mungkin dilakukan oleh CIRT dalam penanganan artefak digital:

1. Pengumpulan Data: Tim CIRT akan mengumpulkan berbagai jenis data dan artefak digital yang terkait dengan insiden, termasuk log sistem, jejak aktivitas, file sistem, dan informasi lain yang dapat memberikan wawasan tentang cara insiden terjadi.
2. Analisis Data: Tim akan menganalisis data yang dikumpulkan untuk mengidentifikasi pola dan tanda-tanda aktivitas yang mencurigakan. Analisis ini dapat membantu mengungkap bagaimana serangan dilakukan, alat yang digunakan, dan dampaknya terhadap sistem.
3. Pemulihan Artefak: Artefak digital yang diidentifikasi dapat meliputi file yang dikompromikan, jejak serangan, kode berbahaya, atau komunikasi jaringan yang mencurigakan. Tim akan berusaha untuk memulihkan dan memeriksa artefak ini dengan hati-hati untuk memahami mekanisme serangan.

4. Pengklasifikasian Data: Data dan artefak yang dikumpulkan akan dianalisis dan diklasifikasikan sesuai dengan tingkat sensitivitas dan relevansinya terhadap insiden. Ini membantu dalam memprioritaskan tindakan dan menyelidiki dampak lebih lanjut.
5. Rekonstruksi Insiden: Berdasarkan artefak digital dan data yang dianalisis, CIRT akan mencoba merekonstruksi kronologi insiden dan alur serangan. Hal ini membantu memahami langkah-langkah yang diambil oleh penyerang dan merespons dengan tepat.
6. Eksplorasi Jejak: Tim akan mencari tahu apakah ada jejak-jejak tambahan dari serangan atau pelanggaran lain yang mungkin tidak terdeteksi sebelumnya.
7. Kolaborasi dengan Penegak Hukum: Jika insiden melibatkan aktivitas ilegal atau pelanggaran hukum, tim CIRT dapat bekerja sama dengan otoritas penegak hukum untuk memberikan bukti dan dukungan dalam penyelidikan lebih lanjut.
8. Pelaporan dan Rekomendasi: Hasil dari analisis artefak digital akan digunakan untuk menyusun laporan yang memberikan pemahaman mendalam tentang insiden dan memberikan rekomendasi untuk perbaikan keamanan di masa depan.

5.2.3. Pemberitahuan Hasil Pengamatan Potensi Ancaman

Tujuan pemberitahuan Hasil Pengamatan Potensi Ancaman adalah untuk memberikan informasi tentang ancaman potensial yang dapat mempengaruhi perusahaan, sehingga perusahaan dapat mengambil langkah-langkah proaktif dalam mengatasi risiko keamanan yang mungkin timbul. Berikut adalah beberapa aspek penting dari layanan Pemberitahuan Hasil Pengamatan Potensi Ancaman yang dapat disediakan oleh CIRT:

1. Pemantauan Aktif: Tim CIRT akan secara aktif memantau lingkungan siber untuk mendeteksi tren dan perubahan dalam ancaman keamanan. Ini melibatkan pemantauan sumber-sumber informasi seperti berita keamanan, laporan industri, dan pemberitahuan dari lembaga keamanan siber lainnya.
2. Analisis Ancaman: Tim akan menganalisis informasi yang diperoleh dari pemantauan untuk mengidentifikasi ancaman potensial yang dapat berdampak pada perusahaan. Analisis ini melibatkan pemahaman mendalam tentang sifat ancaman, teknik penyerangan, dan kelompok penyerang yang mungkin terlibat.
3. Pemeringkatan Risiko: Berdasarkan analisis, CIRT akan memberikan pemeringkatan risiko kepada perusahaan tentang ancaman yang diidentifikasi. Pemeringkatan ini dapat mencakup informasi tentang tingkat risiko, potensi dampak, dan urgensi tindakan yang perlu diambil.
4. Pemberitahuan: Tim CIRT akan menghasilkan pemberitahuan resmi kepada pihak yang bertanggung jawab di dalam perusahaan, termasuk manajemen senior dan tim keamanan siber internal. Pemberitahuan ini berisi detail tentang ancaman yang diidentifikasi, serta rekomendasi untuk mengurangi risiko.

5. Rekomendasi Tindakan: Pemberitahuan tersebut juga akan mencakup rekomendasi konkret mengenai tindakan yang sebaiknya diambil oleh perusahaan. Ini dapat termasuk langkah-langkah pencegahan, pembaruan perangkat lunak, atau perubahan konfigurasi yang dapat membantu melindungi perusahaan dari ancaman tersebut.
6. Pembaruan Berkala: Tim CIRT akan terus memantau perkembangan ancaman dan memberikan pembaruan berkala kepada perusahaan jika ada perubahan atau perkembangan baru dalam situasi keamanan.
7. Pelaporan dan Analisis: CIRT akan mencatat hasil pemberitahuan, tindakan yang diambil oleh perusahaan, dan hasil dari langkah-langkah yang telah diimplementasikan. Analisis ini dapat membantu perusahaan dalam memahami dampak dari layanan ini dan mengevaluasi efektivitas tanggapan mereka terhadap ancaman.

5.2.4. Pendeteksian Serangan

Pendeteksian Serangan merupakan upaya untuk mendeteksi aktivitas atau serangan yang mencurigakan atau tidak sah pada infrastruktur dan sistem perusahaan, sehingga dapat diambil tindakan secara cepat untuk mencegah dampak yang lebih besar. Berikut adalah aspek penting dari layanan Pendeteksian Serangan yang dapat dilakukan oleh CIRT:

1. Pemantauan Aktivitas: Tim CIRT akan melakukan pemantauan aktif terhadap lalu lintas jaringan, log aktivitas, dan jejak keamanan dalam lingkungan siber perusahaan. Pemantauan ini bertujuan untuk mengidentifikasi aktivitas yang mencurigakan, termasuk perilaku yang tidak biasa atau tanda-tanda serangan.
2. Analisis Pola: CIRT akan menganalisis pola lalu lintas dan aktivitas untuk mengidentifikasi anomali yang mungkin menunjukkan adanya serangan atau eksploitasi. Ini melibatkan pemahaman tentang bagaimana serangan biasanya terjadi dan bagaimana penyerang dapat mencoba menyelinap dalam jaringan.
3. Deteksi Intrusi: Tim akan menggunakan alat-alat dan teknik deteksi intrusi untuk mengidentifikasi upaya masuk yang tidak sah ke dalam sistem atau jaringan. Ini termasuk deteksi usaha menerobos password, upaya eksploitasi kerentanan, dan perilaku mencurigakan lainnya.
4. Penggunaan Teknologi Deteksi: CIRT akan menggunakan perangkat lunak dan solusi deteksi canggih untuk memantau aktivitas jaringan, lalu lintas, dan aplikasi. Ini dapat melibatkan penggunaan alat-alat seperti Sistem Deteksi Intrusi (IDS), Sistem Deteksi Serangan (IPS), serta analisis malware dan perilaku jaringan yang mencurigakan.
5. Penelusuran Jejak: Setelah aktivitas mencurigakan terdeteksi, CIRT akan melakukan penelusuran jejak untuk memahami bagaimana serangan dilakukan, sumbernya, dan bagaimana penyerang berinteraksi dengan lingkungan.
6. Peringatan dan Tanggapan Cepat: Jika serangan atau aktivitas mencurigakan terdeteksi, tim akan memberikan peringatan kepada

pihak yang berwenang dalam perusahaan dan segera mengambil tindakan untuk mencegah eskalasi lebih lanjut. Ini mungkin melibatkan isolasi sistem, penghentian aktivitas yang mencurigakan, atau respons lainnya.

7. Analisis Pasca-Kejadian: Setelah serangan terdeteksi dan ditangani, CIRT akan melakukan analisis mendalam terhadap serangan tersebut untuk memahami sifatnya, alat yang digunakan, dan kerentanannya.

5.2.5. Analisis Risiko Keamanan Siber

Analisis Risiko Keamanan Siber bertujuan untuk memberikan pemahaman yang lebih baik tentang risiko yang mungkin dihadapi oleh perusahaan dan membantu mereka mengambil tindakan yang tepat guna mengurangi risiko tersebut,. Berikut adalah langkah-langkah yang mungkin dilakukan oleh CIRT dalam layanan Analisis Risiko Keamanan Siber:

1. Identifikasi Aset dan Ancaman: CIRT akan bekerja sama dengan perusahaan untuk mengidentifikasi aset digital yang kritis dan berharga, seperti data sensitif, sistem, aplikasi, dan infrastruktur jaringan. Selain itu, tim juga akan menganalisis ancaman potensial yang dapat mempengaruhi aset tersebut, termasuk ancaman internal dan eksternal.
2. Penilaian Ranah Ancaman: CIRT akan menganalisis ranah ancaman untuk mengidentifikasi jenis ancaman yang mungkin terjadi, seperti malware, serangan phishing, penolakan layanan (DoS), dan lain-lain. Tim akan mencoba memahami bagaimana ancaman-ancaman ini dapat mempengaruhi aset dan operasi perusahaan.
3. Pengukuran Kerentanan: CIRT akan melakukan penilaian kerentanan terhadap sistem dan aplikasi perusahaan untuk mengidentifikasi celah keamanan yang mungkin dapat dimanfaatkan oleh penyerang. Ini dapat melibatkan pemindaian keamanan, analisis kode, dan pengujian penetrasi.
4. Penilaian Dampak: Tim akan menilai potensi dampak dari serangan terhadap aset perusahaan, termasuk dampak finansial, reputasi, operasional, dan kepatuhan. Ini membantu perusahaan dalam memahami konsekuensi potensial dari serangan dan mengalokasikan sumber daya dengan bijaksana.
5. Penilaian Kemungkinan: CIRT akan menilai kemungkinan terjadinya serangan berdasarkan faktor-faktor seperti keberhasilan serangan serupa di masa lalu, tingkat keamanan saat ini, dan tren ancaman siber saat ini.
6. Peringkat Risiko: Berdasarkan penilaian dampak dan kemungkinan, CIRT akan memberikan peringkat risiko untuk masing-masing ancaman. Ini membantu perusahaan dalam memprioritaskan langkah-langkah pencegahan dan respons.
7. Rekomendasi Pengurangan Risiko: CIRT akan memberikan rekomendasi konkret mengenai langkah-langkah yang dapat diambil oleh perusahaan untuk mengurangi risiko yang diidentifikasi. Ini mungkin termasuk tindakan teknis, pelatihan keamanan, perbaikan kebijakan, dan praktik terbaik dalam keamanan siber.

8. Pemantauan dan Pembaruan: CIRT akan terus memantau perubahan dalam ancaman dan risiko serta memberikan pembaruan berkala kepada perusahaan untuk membantu mereka tetap mengelola risiko secara efektif.

5.2.6. Konsultasi Terkait Kesiapan Penanganan Insiden Siber

Konsultasi Terkait Kesiapan Penanganan Insiden Siber bertujuan untuk membantu perusahaan mengembangkan rencana dan strategi yang efektif untuk menangani insiden keamanan dan meminimalkan dampak yang mungkin terjadi. Berikut adalah beberapa aspek penting dari layanan Konsultasi Terkait Kesiapan Penanganan Insiden Siber yang dapat dilakukan oleh CIRT:

1. Evaluasi Kesiapan Saat Ini: CIRT akan melakukan evaluasi terhadap kemampuan dan kesiapan perusahaan dalam menghadapi insiden keamanan siber. Ini mencakup tinjauan terhadap kebijakan dan prosedur yang ada, infrastruktur keamanan, pelatihan pekerja, serta alat dan teknologi yang digunakan.
2. Pemetaan Ancaman dan Skenario: Tim akan membantu perusahaan dalam memetakan ancaman yang paling mungkin terjadi dan mengembangkan skenario insiden yang mungkin terjadi. Hal ini membantu perusahaan untuk lebih siap dan dapat merespons secara cepat dan efektif.
3. Pengembangan Rencana Respons Insiden: Berdasarkan pemetaan ancaman dan skenario, CIRT akan membantu perusahaan dalam mengembangkan rencana respons insiden yang jelas dan terstruktur. Rencana ini mencakup langkah-langkah yang harus diambil saat terjadi insiden, serta peran dan tanggung jawab tim respons insiden.
4. Pelatihan dan Latihan: CIRT akan menyediakan pelatihan kepada pekerja perusahaan mengenai tindakan yang harus diambil selama insiden. Selain itu, tim juga dapat mengadakan latihan simulasi insiden untuk menguji efektivitas rencana respons dan melatih tim respons insiden.
5. Pemilihan Alat dan Teknologi: CIRT akan memberikan saran mengenai alat dan teknologi yang dapat membantu dalam pendeteksian, pemantauan, dan penanganan insiden keamanan siber. Hal ini termasuk pemilihan dan konfigurasi perangkat lunak deteksi intrusi, sistem manajemen insiden, dan alat lain yang mendukung respons insiden.
6. Peninjauan Kebijakan dan Prosedur: Tim akan membantu perusahaan dalam meninjau dan memperbarui kebijakan dan prosedur keamanan yang ada untuk memastikan kesesuaian dengan praktik terbaru dan ancaman terkini.
7. Berkolaborasi dengan Tim Internal: CIRT akan berkolaborasi dengan tim keamanan siber internal dan manajemen untuk memastikan bahwa rencana dan strategi yang dikembangkan sesuai dengan kebutuhan dan tujuan perusahaan.
8. Pembaruan dan Perbaikan: CIRT akan membantu perusahaan dalam melakukan pembaruan berkala terhadap rencana respons dan strategi

kesiapan insiden, sejalan dengan perkembangan keamanan siber dan perubahan lingkungan perusahaan.

5.2.7. Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber

Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber bertujuan untuk membantu perusahaan meningkatkan tingkat kesadaran dan pemahaman tentang ancaman keamanan siber serta mengajarkan praktik-praktik yang aman kepada para pengguna dan pekerja perusahaan. Berikut adalah beberapa aspek penting dari layanan Pembangunan Kesadaran dan Kepedulian Terhadap Keamanan Siber yang dapat dilakukan oleh CIRT:

1. Pelatihan Keamanan: CIRT akan memberikan pelatihan kepada pekerja tentang ancaman keamanan siber, teknik serangan umum, dan praktik terbaik untuk melindungi informasi dan sistem. Pelatihan ini dapat mencakup topik seperti phishing, malware, penggunaan kata sandi yang kuat, dan langkah-langkah pencegahan lainnya.
2. Pengembangan Materi Edukasi: CIRT akan membantu mengembangkan materi edukasi dan sumber daya yang dapat digunakan oleh perusahaan, seperti presentasi, video, dan panduan keamanan. Materi ini dapat membantu dalam menyebarkan informasi tentang keamanan siber kepada semua lapisan pekerja.
3. Kampanye Kesadaran: Tim dapat merancang kampanye kesadaran keamanan siber yang kreatif dan menarik, termasuk penggunaan poster, pengumuman, dan penghargaan untuk pengguna yang aktif dalam mengamankan informasi.
4. Uji Kesadaran: CIRT dapat melakukan uji kesadaran (awareness testing) dengan mengirimkan email palsu (phishing simulation) kepada pekerja untuk mengukur sejauh mana mereka dapat mengenali upaya serangan phishing. Ini membantu mengidentifikasi area di mana tingkat kesadaran perlu ditingkatkan.
5. Workshop dan Sesi Edukasi: CIRT dapat mengadakan workshop dan sesi edukasi secara berkala untuk membahas isu-isu keamanan siber terbaru, berbagi kisah sukses atau insiden, dan menjawab pertanyaan peserta.
6. Kampanye Perilaku Aman: Tim dapat merancang kampanye yang mendorong perilaku aman dalam penggunaan teknologi dan informasi. Ini termasuk memastikan penggunaan kata sandi yang kuat, menghindari mengklik tautan yang mencurigakan, dan menjaga keamanan perangkat.
7. Pemantauan dan Evaluasi: CIRT akan terus memantau efektivitas kampanye dan pelatihan kesadaran serta melakukan evaluasi untuk mengukur perubahan dalam perilaku dan peningkatan kesadaran keamanan.
8. Kustomisasi dan Penyesuaian: Layanan ini akan disesuaikan dengan kebutuhan dan budaya perusahaan, sehingga materi dan pendekatan yang digunakan relevan dan efektif.

6. Pelaporan Insiden

Laporan insiden keamanan siber dapat dikirimkan ke kpi.cyber.security@pertamina.com 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*

-