LAPORAN EVALUASI PENYELENGGARAAN TIM TANGGAP INSIDEN SIBER (TTIS)

KABUPATEN BANYUWANGI
TAHUN ANGGARAN 2024

DAFTAR ISI

BAB I
PENDAHULUAN

A. Latar Belakang

TTIS merupakan pilar penting keamanan siber. Hal ini disebabkan TTIS menjalankan peran tanggap insiden siber untuk meminimalisir dan mengontrol cakupan eskalasi yang terdampak insiden siber serta memulihkan Sistem dan Infrastruktur Teknologi Informasi dan Komunikasi pada kondisi normal sehingga Proses Kerja dan Layanan dapat berjalan normal kembali. Pada praktiknya, TTIS menyelenggarakan 3 (tiga) area layanan berupa Reaktif, Proaktif dan Manajamen Kualitas Keamanan untuk mendukung tata kelola keamanan siber yang mana, "Reaktif" dalam tanggap insiden siber terhadap pendampingan dan penanganan insiden siber pada konstituen dan "Aktif" dalam meningkatkan keamanan sistem dan infrastruktur sebelum insiden siber terjadi dan/ atau sebuah kondisi anomali terdeteksi serta "*lesson learned*" atas upaya penanganan insiden siber yang telah dilakukan dalam rangka perbaikan kebijakan keamanan siber.

Berdasarkan Peraturan Presiden nomor 18 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, diamanahkan kepada instansi pemerintah penyelenggara sistem pemerintahan berbasis elektronik (SPBE) untuk menyelenggarakan penanganan insiden keamanan SPBE. Adapun dalam praktiknya, penanganan insiden keamanan SPBE dilaksanakan oleh sebuah tim khusus yang disebut *Computer Security Incident Response Team* (TTIS). Dalam rangka Penyelenggaraan TTIS, setiap organisasi atau instansi pemerintah dapat mengacu pada Peraturan Badan Siber dan Sandi Negara (BSSN) Nomor 1 tahun 2024 tentang Pengelolaan Insiden Siber yang mana TTIS dikategorisasikan menjadi 3 (tiga) yaitu TTIS Nasional, TTIS Sektor, dan TTIS Organisasi. Masing-masing TTIS memiliki hak dan kewajiban sesuai dengan kategorisasinya.

Pemerintah *Kabupaten Banyuwangi* telah membentuk Tim Tanggap Insiden Siber yang diberi nama ***Banyuwangi-CSIRT*** pada ***28 Oktober 2022*** berdasarkan Keputusan Bupati Banyuwangi Nomor: 188/456/KEP/429.011/2022**.** TTIS merupakan TTIS Organisasi yang menginduk TTIS Sektor Pemerintah yang dilaksanakan oleh BSSN melalui Gov-TTIS Indonesia. BSSN sebagai pengampu TTIS Sektor Administrasi Pemerintahan memiliki tugas melakukan pembinaan dan penguatan TTIS Sektor

Administrasi Pemerintahan sehingga nantinya masing-masing TTIS organisasi Instansi Pemerintah mampu melakukan pengelolaan insiden siber secara mandiri dan profesional.

Guna mewujudkan TTIS Organisasi yang mampu merespon insiden siber secara mandiri maka dilakukan Evaluasi Penyelenggaraan TTIS *Kabupaten Banyuwangi* untuk mengukur kematangan TTIS dalam melaksanakan layanan TTIS sesuai dengan RFC-2350 yang telah dideklarasikan. Adapun hasil evaluasi TTIS tersebut akan menjadi bahan masukan bagi Bupati Banyuwangi dan BSSN dalam menentukan kebijakan dan penguatan *Banyuwangi-CSIRT*.

B. Dasar

1. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik;
2. Peraturan Presiden Nomor 18 Tahun 2020 tentang Rencana Pembangunan Jangka Menengah Nasional Tahun 2020-2024
3. Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital;
4. Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber;
5. Peraturan Deputi Bidang Keamanan Siber dan Sandi Pemerintahan dan Pembangunan Manusia Nomor 1 Tentang Pedoman Pembentukan Tim Tanggap Insiden Siber Sektor pemerintahan;
6. Keputusan Bupati Banyuwangi Nomor : 188/456/Kep/429.011/2022 Tentang Tim Tanggap Insiden Siber (Computer Security Incident Response Team) Kabupaten Banyuwangi;
7. Surat Tanda Registrasi Tim Tanggap Insiden Siber atau Computer Security Incident Response Team Kabupaten Banyuwangi Nomor Registrasi 122/CSIRT.01.02.01/BSSN/11/2022**.**

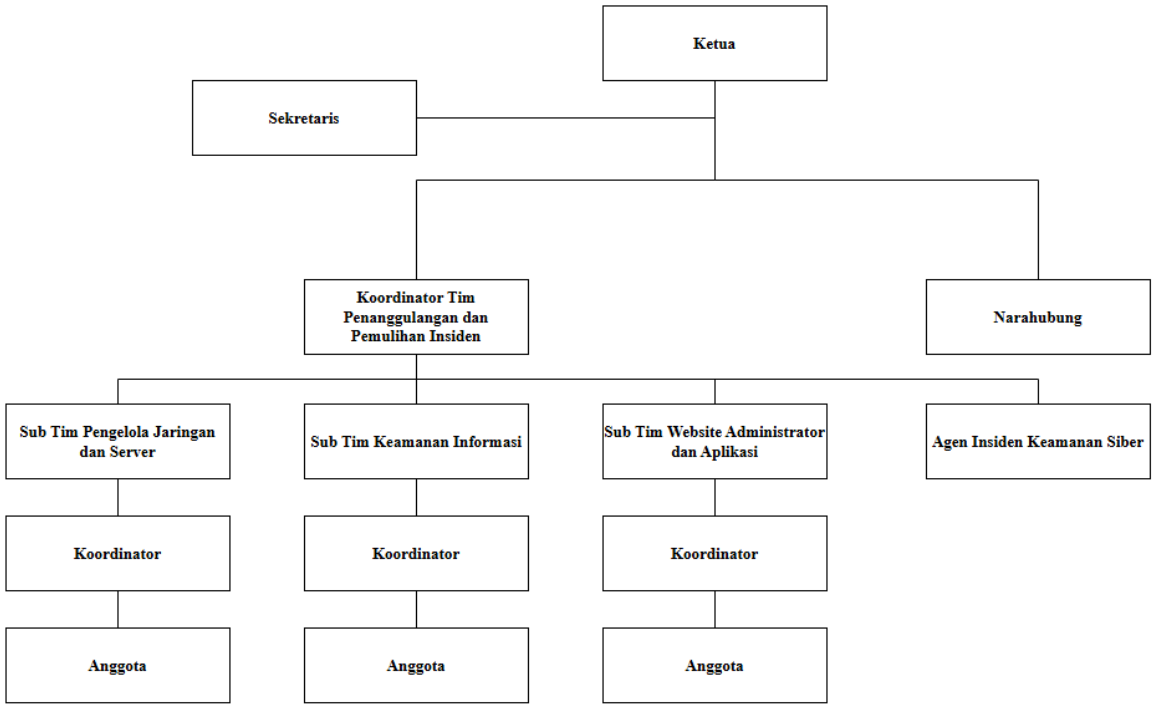
C. Tujuan

Evaluasi Penyelenggaraan TTIS bertujuan untuk mengukur efektivitas penyelenggaraan TTIS dalam pengelolaan insiden siber di internal Pemerintah Kabupaten Banyuwangi serta menjaga keamanan layanan sistem elektornik milik Pemerintah Kabupaten Banyuwangi.

BAB II
TTIS BANYUWANGI-CSIRT

Merujuk pada Keputusan Bupati Banyuwangi Nomor : 188/456/Kep/429.011/2022 Tentang Tim Tanggap Insiden Siber (Computer Security Incident Response Team) Kabupaten Banyuwangi**.** TTIS menyelenggarakan 2 (dua) fungsi yaitu fungsi utama dan fungsi tambahan. Fungsi Utama terdiri dari pemberian peringatan terkait keamanan siber; perumusan panduan teknis penganan insiden siber; pencatatan setiap laporan/aduan yang dilaporkan, pemberian rekomendasi langkah penanganan awal kepada pihak terdampak; pemilihan (*triage)* insiden siber sesuai dengan kriteria yang ditetapkan dalam rangka memprioritaskan insiden siber yang akan ditangani; penyelenggaraan koordinasi penanganan insiden siber kepada pihak yang berkepentingan; dan pengelenggaraan fungsi lainnya sesuai kebutuhan. Adapun fungsi tambahan berupa penanganan kerentanan sistem elektronik, sosialiasi kesadaran keamanan informasi, dan lain sebagainya.

Dalam rangka menyelenggarakan layanan tersebut, Pemerintah Kabupaten Banyuwangi**.** menyusun struktur TTIS yang terdiri dari :



Gambar 1 Struktur Organisasi TTIS Banyuwangi-CSIRT

Ketua, mempunyai tugas dan tanggung jawab yaitu:

a. Memimpin pelaksanaan tugas dan bertanggung jawab atas kegiatan Banyuwangi-CSIRT;
b. Bertanggung jawab dalam pengalokasian sumber daya yang dibutuhkan untuk mengoperasionalkan layanan Banyuwangi-CSIRT;
c. Mengkoordinasikan Banyuwangi-CSIRT dengan instansi dan pihak-pihak terkait lainnya dalam rangka pelaksanaan tugas dan fungsi Banyuwangi-CSIRT, serta menjalin kerja sama antar CSIRT;
d. Memantau operasional dan kinerja Banyuwangi-CSIRT;
e. Membuat perencanaan operasional dan strategis mengenai Banyuwangi-CSIRT;
f. Mengkoordinasikan edukasi dan pelatihan mengenai keamanan siber di lingkungan Kabupaten Banyuwangi;
g. Dalam melaksanakan tugas, Ketua Banyuwangi-CSIRT bertanggung jawab serta menyusun dan menyampaikan laporan kepada Bupati.

Sekretaris, mempunyai tugas dan tanggung jawab yaitu

a. Melaksanakan fungsi kesekretariatan/ ketatausahaan meliputi administrasi dan dokumentasi pada operasional layanan Banyuwangi-CSIRT;
b. Membantu Ketua dalam menjalankan tugas dan tanggung jawabnya;
c. Menyelenggarakan rapat-rapat koordinasi.

Narahubung mempunyai tugas dan tanggung jawab yaitu:

a. Menyediakan Point Of Contact (POC) untuk Banyuwangi-CSIRT, berupa alamat email, nomor telepon, dan komunikasi lainnya;
b. Menerima peringatan siber yang ditujukan untuk Banyuwangi-CSIRT dan memberikan peringatan siber ke CSIRT lainnya; dan
c. Memberikan laporan penanganan insiden Siber yang telah terjadi kepada Tim Tanggap Siber Nasional.

Koordinator Tim Penanggulangan dan Pemulihan Insiden, memiliki tugas dan tanggung jawab:

a. Melakukan koordinasi apabila terjadi insiden siber;
b. Melakukan penanggulangan dan pemulihan insiden secara cepat dan tepat;
c. Melakukan tindakan korektif atas celah kerawanan (vulnerability) yang ditemukan;
d. Melakukan pemeriksaan dan analisis terhadap artifak yang ditemukan;

e. Melakukan analisis risiko;
f. Melakukan audit atau penilaian keamanan;
g. Menjadi tim teknis yang memberikan edukasi dan pelatihan.

Sub Tim Pengelola Jaringan dan Server, mempunyai tugas dan tanggung jawab yaitu:

a. Membuat dokumentasi jaringan yang beroperasional, berupa dokumentasi konfigurasi, dokumentasi lalu lintas normal (baseline) jaringan, dan dokumentasi performa jaringan;
b. Menyiapkan perangkat jaringan yang diperlukan untuk melakukan deteksi intrusi di jaringan dan analisa log di server;
c. Melakukan analisa log dan rekam digital lainnya pada jaringan dan server;
d. Menerapkan konsep keamanan pada konfigurasi jaringan dan meminimalisir celah keamanan di jaringan;
e. Melakukan pemantauan lalu lintas jaringan dan memeriksa apabila terdapat anomali di jaringan;
f. Melakukan tindakan korektif pada jaringan dan server sebagai solusi atas insiden siber maupun temuan celah keamanan;
g. Berkoordinasi dengan Internet Service Provider (ISP), jika diperlukan;
h. Menjadi tim teknis yang memberikan edukasi dan pelatihan.

Sub Tim Keamanan Informasi, mempunyai tugas dan tanggung jawab yaitu:

a. Melakukan deteksi dan identifikasi serangan siber;
b. Melakukan triase insiden meliputi penilaian dampak dan prioritas insiden;
c. Melakukan analisis dan menemukan celah keamanan yang menjadi penyebab insiden siber;
d. Melakukan tindakan korektif untuk menanggulangi insiden siber;
e. Melakukan tindakan korektif berupa perbaikan celah keamanan (hardening) untuk mencegah insiden terulang kembali;
f. Melakukan pemeriksaan dan analisis terhadap artifak yang ditemukan;
g. Melakukan audit atau penilaian keamanan;
h. Melakukan analisis risiko;
i. Menjadi tim teknis yang memberikan edukasi dan pelatihan.

Sub Tim Website Administrator dan Aplikasi, mempunyai tugas dan tanggung jawab yaitu:

a. Melakukan pengelolaan terhadap content website atau sistem informasi dan komunikasi lainnya;
b. Melakukan backup data secara berkala dan menyiapkan website cadangan sebagai solusi sementara apabila terjadi insiden siber;
c. Berkoordinasi dengan pengguna sistem informasi ketika insiden;
d. Melakukan tindakan korektif pada aplikasi sebagai solusi atas insiden siber maupun temuan celah keamanan.

Agen Insiden Keamanan Siber, mempunyai tugas dan tanggung jawab yaitu :

a. Melakukan monitoring keamanan informasi yang terjadi pada masing-masing Organisasi Perangkat Daerah di Pemerintah Kabupaten Banyuwangi;
b. Melaporkan kejadian Insiden Siber yang terjadi kepada Tim Penanggulangan dan Pemulihan Insiden.

BAB III
PENYELENGGARAAN TTIS KABUPATEN BANYUWANGI

Pemerintah Kabupaten Banyuwangi menyelenggarakan layanan TTIS terhadap seluruh konstituen sesuai dengan RFC-2350 yang meliputi Perangkat Daerah di Lingkungan Pemerintah Kabupaten Banyuwangi guna terwujudnya ketahanan siber pada Pemerintah Kabupaten Banyuwangi yang handal dan profesional untuk mewujudkan Banyuwangi Semakin Digital. Adapun dalam penyelenggaraannya, TTIS berkolaborasi dengan seluruh Organisasi Perangkat Daerah melalui agen siber yang tergabung dalam Tim TTIS. TTIS membuka layanan portal aduan siber dan menghimbau baik kepada pegawai internal maupun masyarakat luar untuk dapat melaporkan insiden siber jika terdapat gangguan atau tidak berjalannya sistem elektronik milik Pemerintah Kabupaten Banyuwangi ke alamat https://csirt.banyuwangikab.go.id.

Selama dalam penyelenggaraan TTIS dalam 2 tahun**,** Pemerintah Kabupaten Banyuwangi melalui Dinas Komunikasi, Informatika dan Persandian melaksanakan evaluasi penyelenggaraan TTIS dan kematangan penanganan insiden siber dengan hasil sebagai berikut:

A. Fungsi TTIS

Fungsi Utama yang diselenggarakan berupa :

1. Pemberian peringatan terkait keamanan siber

   Fungsi ini berupa pemberian peringatan terkait informasi anomali atau ancaman siber kepada seluruh konstituen. Peringatan ini diharapkan dapat mendorong langkah-langkah mitigasi dan pencegahan secara cepat untuk meminimalkan risiko insiden keamanan siber. Peringatan ini mencakup informasi mengenai anomali atau potensi ancaman siber yang terdeteksi melalui sistem monitoring keamanan siber terintegrasi, seperti Fortinet yang telah dipasang pada seluruh aset teknologi informasi milik OPD. Selain itu, informasi ancaman juga diterima dari sumber eksternal, seperti platform Cyber Threat Intelligence, laporan dari BSSN, dan pengaduan masyarakat melalui website Banyuwangi-CSIRT. Setiap informasi yang diterima dianalisis dan divalidasi untuk menentukan tingkat kritikalnya sebelum disampaikan kepada OPD terkait.

   Laporan tersebut berisi informasi terperinci, termasuk jenis ancaman, aset yang terdampak, rekomendasi langkah mitigasi, dan batas waktu untuk menindaklanjuti peringatan. OPD diwajibkan memberikan umpan balik berupa laporan tindak lanjut atas rekomendasi yang diberikan. Jika OPD menghadapi kendala teknis dalam proses

mitigasi, TTIS Banyuwangi-CSIRT menyediakan pendampingan, meliputi pembaruan keamanan, konfigurasi ulang perangkat, atau langkah forensik sesuai kebutuhan hingga status ancaman dapat diatasi sepenuhnya.

2. Perumusan panduan teknis penanganan Insiden Siber

   Fungsi ini berupa perumusan panduan teknis penanganan insiden siber.

   TTIS Banyuwangi-CSIRT telah melakukan identifikasi dan perumusan panduan teknis yang disesuaikan dengan kondisi saat ini, adapun hasil identifikasi panduan teknis diperoleh 3 panduan teknis yang harus dibuat yaitu, panduan teknis penanganan insiden Web Defacement dan Malware. Hal ini dilandasi karena seringnya terjadi insiden siber web Defacement, Ransomware, maupun DDOS pada server. Dari hasil identifikasi tersebut, untuk Panduan Teknis Penanganan Insiden Siber Web Defacement dan Ransomware sudah disahkan, sedangkan untuk Panduan Teknis Penanganan Insiden Siber DDOS masih dalam bentuk draft.

3. Pencatatan setiap laporan/aduan yang dilaporkan, pemberian rekomendasi langkah penanganan awal kepada pihak terdampak;

   TTIS telah menerima aduan insiden siber di tahun 2024. Aduan siber ini dikelompokkan menjadi sebagai berikut :

   a. Aduan insiden siber

      Aduan insiden siber sebanyak 8 Aduan dengan keberhasilan penanganan insiden siber sebanyak 8 Aduan sebagaimana ditunjukkan pada tabel 1.

Tabel 1. Penanganan peretasan situs web Kab. Banyuwangi

No	Alamat url yang ternotifikasi/ dilaporkan	Tanggal Kejadian	Sumber Laporan	Status Penanganan	Lama Waktu Penanganan	SLA	Temuan Hasil Investigasi/ Penyelidikan	Keterangan
1.	https://bipafour.banyuwangikab.go.id/	5 Agustus 2024	Laporan internal TTIS	Tertangani	1 hari	1x24 jam	Terindikasi ditemukan Penghapusan data pada sistem, penyerang teridentifikasi dapat masuk dikarenakan password yang digunakan terlalu mudah / tidak standar.	Insiden ditangani oleh Banyuwangi-CSIRT dan data dapat duplihkan menggunakan data backup.
2.	https://mawasdiri.banyuwangikab.go.id/	17 Juli 2024	Laporan internal TTIS	Tertangani	14 hari	1x24 jam	Terindikasi ditemukan beberapa hal sebagai berikut: a. webshell b. script deface slot gacor	insiden berhasil ditangani oleh pengembang dan dilakukan

								perubahan password user dengan menggunakan password yang standar
3.	https://dlh.banyuwangikab.go.id	8 Juli 2024	Laporan internal TTIS	Tertangani	30 hari	1x24 jam	Terindikasi ditemukan webshell pada server dan halaman terindeks oleh mensin pencari	Dilakukan instalasi ulang pada server dan dilakukan pembaruan dengan website terbaru
4	https://inspektorat.banyuwangikab.go.id	7 Juni 2024	Laporan internal TTIS	Tertangani	3 hari	1x24 jam	Terindinkasi ditemukan web defacement judi online slot gacor dan beberapa webshell pada server	insiden berhasil ditangani oleh pengembang dan Banyuwangi-CSIRT
5	https://sidenistam.banyuwangikab.go.id/	22 Mei 2024	Laporan Internal TTIS	Tertangani	1 hari	1x24 jam	Terindinkasi ditemukan web defacement judi online slot gacor dan beberapa webshell pada server	insiden berhasil ditangani oleh pengembang dan Banyuwangi-CSIRT
6	https://wiki.banyuwangikab.go.id	13 Mei 2024	Laporan Internal TTIS	Tertangani	2 hari	1x24 jam	Terindinkasi ditemukan web defacement judi online slot gacor dan beberapa webshell / malicious code pada server	Insiden ditangani oleh Banyuwangi-CSIRT
7.	https://rsudblambangan.banyuwangikab.go.id/	8 Mei 2024	Laporan Internal TTIS	Tertangani	8 hari	1x24 jam	Terindinkasi ditemukan web defacement judi online slot gacor	Dilakukan instalasi ulang server dan dilakukan pembaruan dengan website terbaru
8	https://pbb.banyuwangikab.go.id	16 Maret 2024	Laporan Internal TTIS	Tertangani	14 hari	1x24 jam	Terindinkasi ditemukan web defacement judi online slot gacor dan beberapa webshell pada server	insiden berhasil ditangani oleh pengembang dan Banyuwangi-CSIRT

Sebagai tindak lanjut untuk mencegah insiden siber agar tidak terulang kembali, dilakukan beberapa langkah strategis, antara lain: Melakukan pembaruan sistem untuk menutup celah kerentanan yang ditemukan, mengganti seluruh kredensial server, database, serta pengguna sistem aplikasi dengan kombinasi password yang sesuai standar keamanan siber, melakukan Information Technology Security Assessment (ITSA) secara mandiri oleh Dinas Komunikasi, Informatika, dan Persandian Kabupaten Banyuwangi terhadap beberapa aplikasi setelah

insiden tertangani untuk memastikan tidak ada kerentanan lain pada sistem terdampak.

Adapun dalam proses penanganan insiden siber ditemukan kendala sebagai berikut :

1) Kurangnya komunikasi yang efektif dengan pemilik sistem elektronik, baik dalam hal respons cepat maupun koordinasi untuk langkah perbaikan, menghambat percepatan penanganan insiden.
2) OPD pemilik sistem belum memahami pentingnya langkah mitigasi pasca-insiden sebagai upaya pencegahan berulangnya insiden.
3) Keterbatasan jumlah atau kompetensi SDM yang menangani keamanan sistem elektronik.
4) Beberapa aplikasi yang dikembangkan oleh pihak ketiga sehingga terjadi keterbatasan akses atau ketergantungan pada pihak eksternal untuk melakukan perbaikan, sehingga proses pemulihan menjadi terhambat.

Sebagai upaya yang dilakukan untuk mengatasi kendala tersebut, Dinas Komunikasi dan Informatika *Kabupaten Banyuwangi* sebagai Unit Kerja pengampu TTIS melakukan langkah-langkah sebagai berikut : .

1) Penunjukan contact person dari setiap OPD pemilik sistem untuk mempermudah komunikasi dengan TTIS Banyuwangi-CSIRT;
2) Mengadakan pelatihan atau workshop terkait keamanan siber kepada pemilik sistem elektronik;
3) Melakukan pengawasan rutin terhadap implementasi rekomendasi perbaikan serta memberikan laporan evaluasi kepada pimpinan;
4) Menerapkan kebijakan terkait dokumentasi teknis lengkap dari pihak ketiga sebagai referensi untuk perbaikan mandiri jika diperlukan;
5) Mengembangkan dan menerapkan kebijakan teknis terkait standar keamanan siber yang wajib diikuti oleh seluruh pemilik sistem elektronik di lingkungan Pemerintah Kabupaten Banyuwangi.

b. Perangkat Lunak Berbahaya (Malware)

Aduan siber terhadap serangan atau infeksi malware sebanyak 2 aduan dengan keberhasilan penanganan malware sebanyak 2 aduan sebagaimana ditunjukkan

pada tabel 2. Peretasan ini terjadi pada Sistem Elektronik dan/atau komputer pada Organisasi Perangkat Daerah *Kabupaten Banyuwangi***.**

Tabel 2. Penanganan *Malware* Kab. Banyuwangi

No	Jenis Malware	Tanggal Kejadian	Sumber Laporan	Jumlah Perangkat yang Terdampak	Metode Penanganan	Status Penanganan	Investigasi/ Penyelidikan	Keterangan
1.	Spyware, Trojan	25 Juni 2024	Notifikasi Insiden	2 Komputer	a. Isolasi komputer dan jaringan b. Pemindaian Anti Malware c. Pengembalian data yang disembunyikan / diubah oleh malware	Tertangani	Terindikasi : a. Terdampak karena menginstal aplikasi dari sumber tidak resmi b. Versi Operating Sistem yang digunakan sudah usang	File data telah berhasil dikembalikan dan dilakukan instalasi OS versi terbaru
2.	Trojan	15 Juli 2024	Laporan Internal TTIS	1 Komputer	a. Isolasi komputer dan jaringan b. Pemindaian Anti Malware	Tertangani	Terindikasi : a. akses url yang mengandung malware b. instal aplikasi bajakan / bukan dari sumber resmi	Insiden telah berhasil ditangani dengan melakukan pembersihan malware serta menginstal FortiClient pada komputer

Sebagai upaya perbaikan dan untuk mencegah agar tidak terulang insiden siber tersebut maka dilakukan langkah-langkah sebagai berikut:

1) Menerbitkan Surat Edaran Sekretaris Daerah terkait Pedoman Keamanan Siber bagi pegawai di Lingkungan Pemerintah Kabupaten Banyuwangi.
2) Menerapkan kebijakan keamanan endpoint, seperti pembaruan sistem secara rutin, pengaturan firewall, dan pengelolaan hak akses pengguna.
3) Menginstal perangkat lunak keamanan FortiClient pada perangkat pengguna dan memastikan pengguna mematuhi kebijakan penggunaan yang aman.
4) Memberikan pelatihan kepada pengguna akhir tentang kesadaran keamanan siber

Adapun dalam upaya penanganan insiden sber dan upaya pencegahannya ditemukan kendala sebagai berikut :

1) Pengguna akhir tidak menjalankan kebijakan keamanan seperti penggunaan antivirus atau pembaruan perangkat lunak secara rutin.
2) Menggunakan aplikasi atau software bajakan yang diunduh dari sumber tidak terpercaya ada kemungkinan telah disusupi malware.
3) Banyak pengguna akhir yang belum memahami pentingnya keamanan siber, sehingga sering mengabaikan langkah-langkah perlindungan.
4) Beberapa perangkat keras dan perangkat lunak yang digunakan tidak kompatibel dengan teknologi keamanan terbaru.

4. Pemilahan (triage) Insiden Siber sesuai dengan kriteria yang ditetapkan dalam rangka memprioritaskan Insiden Siber yang akan ditangani

   TTIS Banyuwangi-CSIRT dalam pemilahan Insiden Siber dilakukan dengan memperhatikan dampak dan tingkat keparahan insiden siber terhadap organisasi maupun stakeholder yang ada. Adapun kategori dampak dan tingkat keparahan dibagi menjadi 3 yaitu, Tinggi, Sedang, dan Rendah. Pemilihan kategori didasarkan pada besarnya dampak yang ditimbulkan maupun kemungkinan seringnya hal tersebut terjadi.

5. Penyelenggaraan koordinasi penanganan Insiden Siber kepada pihak yang berkepentingan

   Untuk penyelenggaraan koordinasi penanganan insiden siber, TTIS Banyuwangi-CSIRT sudah memiliki SOP Penanganan Insiden dengan alur sebagai berikut.

Fungsi Tambahan meliputi :

1. Penanganan Kerentanan Sistem Elektronik

   Penanganan Kerentanan Sistem Elektroniok yang dilakukan berupa identifikasi kerentanan, penilaian risiko atas kerentanan yang ditemukan, serta tindak lanjut untuk memperbaiki kerentanan. Upaya identifikasi dan penilaian keamanan dilakukan melalui kegiatan *IT Security Assessment* yang dilakukan oleh TTIS terhadap sistem elektronik yang memiliki profil risiko yang tinggi. Jumlah aset yang telah dilakukan *IT Security Assessment* sebanyak 6 sistem elektronik, perbaikan telah selesai dilakukan pada 4 sistem, sementara 2 sistem lainnya masih dalam proses perbaikan, sebagaimana ditunjukkan pada tabel 3.

   Tabel 3. Penanganan Kerentanan Sistem Elektronik

No	Nama Sistem Elektronik	Link url Sistem Elektronik	Tanggal Pelaksanaan	Pelaksana ITSA	Status Kerentanan	Status Perbaikan/ Tindak Lanjut	Keterangan
1	Aplikasi PBB P-2	https://pbb.banyuwangikab.go.id/	30 April s.d 04 Mei 2024	Dinas Komunikasi, Informatika dan Persandian Kab. Banyuwangi	- Ditemukan kerentanan dengan rincian: - Level low sebanyak 2 informational - Level low sebanyak 1 temuan - Level high sebanyak 1 temuan	Termuan kerentanan telah diperbaiki	
2	Aplikasi Go-KerWangi	https://goker.banyuwangikab.go.id/	12 s.d 14 Agustus 2024	Dinas Komunikasi, Informatika dan Persandian Kab. Banyuwangi	- Ditemukan kerentanan dengan rincian: - Level low sebanyak 1 temuan - Level medium sebanyak 1 temuan	temuan kerentanan sudah diperbaiki dan telah diverifikasi	
3	Aplikasi Tiketing Banyuwangi Festival	https://bfest.banyuwangikab.go.id/	29 s.d 31 Agustus 2024	Dinas Komunikasi, Informatika dan Persandian Kab. Banyuwangi	Ditemukan kerentanan dengan rincian: - Level low sebanyak 1 temuan - Level medium sebanyak 1 temuan	temuan kerentanan sudah diperbaiki dan telah diverifikasi	
4	Aplikasi SSO Banyuwangi	https://sso.banyuwangikab.go.id/	17 s.d 19 September 2024	Dinas Komunikasi, Informatika dan Persandian Kab. Banyuwangi	Ditemukan kerentanan dengan rincian: - Level low sebanyak 1 temuan - Level medium sebanyak 1 temuan	temuan kerentanan sudah diperbaiki dan telah diverifikasi	
5	E-Audit Kabupaten Banyuwangi	https://e-audit.banyuwangikab.go.id/	25 s.d 29 November 2024	BSSN	Ditemukan kerentanan dengan rincian:	proses perbaikan	

					- Level medium sebanyak 2 temuan		
6	JDIH Kabupaten Banyuwangi	https://jdih.banyuwangikab.go.id/	25 s.d 29 November 2024	BSSN	Ditemukan kerentanan dengan rincian: - Level low sebanyak 3 temuan - Level medium sebanyak 3 temuan - Level high sebanyak 1 temuan	proses perbaikan	

Sebagai tindak lanjut atas rekomendasi hasil IT Security Assesment, Dinas Komunikasi, Informatika dan Persandian Kabupaten Banyuwangi melakukan hal – hal sebagai berikut :

a. Mengirimakan pemberitahuan kepada dinas terkait untuk dilakukan perbaikan terhadap temuan kerentanan hasil IT Security Assesment, khususnya bagi sistem elektronik yang dikembangkan oleh pihak ketiga.
b. Melakukan pembaruan sistem untuk menutup celah kerentanan yang ditemukan hasil IT Security Assesment untuk sistem elektronik yang dikembangkan oleh Dinas Komunikasi, Informatika dan Persandian Kabupaten Banyuwangi.
c. Mengimplementasikan mekanisme keamanan tambahan, termasuk penguatan konfigurasi firewall serta penerapan Web Application Firewall (WAF).

2. Pembangunan Kesadaran dan Kepedulian terhadap Keamanan Siber

   Fungsi Pembangunan Kesadaran dan Kepedulian terhadap Keamanan Siber bertujuan untuk membangun kesadaran dan kepedulian pegawai Pemerintah *Kabupaten Banyuwangi* terhadap keamanan siber serta untuk meningkatkan kompetensi di bidang keamanan siber dan sandi. Program kegiatan Edukasi dan Pelatihan yang diselenggarakan berupa :

   a. Literasi Digital terkait keamanan siber yang dipublikasikan melalui media situs Website TTIS Kabupaten Banyuwangi yang dapat diakses melalui tautan https://csirt.banyuwangikab.go.id/;

b. Surat Edaran berupa himbauan keamanan siber yang didistribusikan melalui email dinas;
c. Webinar dengan berbagai pihak khususnya BSSN juga dilakukan untuk menambah pengetahuan dan wawasan serta berbagi pengalaman terkait penanganan insiden siber yang sedang tren terjadi.
d. Bimbingan Teknis terkait keamanan siber dilakukan Pemerintah Kabupaten Banyuwangi rutin dilakukan setiap tahun, pada tahun 2024 ini Kabupaten Banyuwangi menggelar Hacking Day 5.0 bekerja sama dengan BSSN membekali kapasitas dasar cyber security bagi pengguna teknologi digital kepada ASN dan operator pendidikan.

Adapun rincian layanan Edukasi dan Pelatihan ditunjukkan pada tabel 4.

Tabel 4. Edukasi dan Pelatihan

No	Kegiatan	Tanggal Pelaksanaan	Penyelenggara Kegiatan	Bentuk Kegiatan	Target/Peserta Kegiatan	Keterangan
1	Literasi Digital Keamanan Informasi	2 Februari 2024	Pemerintah Kabupaten Banyuwangi	Publikasi keamanan informasi melalui https://csirt.banyuwangikab.go.id/	Seluruh Pegawai Kabupaten Banyuwangi	Informasi berupa keamanan data pada perangkat ponsel
2.	Bimbingan Teknis	29 s.d 31 Mei 2024	BSSN	Kesiapsiagaan Insiden Siber pada CSIRT Sektor Pemerintah Daerah Tahun 2024 Tahap II	TTIS Daerah	
3.	Bimbingan Teknis	20 s.d 22 Agustus 2024	BSSN	Cross Sectoral Cyber Exercise #6 Penanganan Insiden Siber	TTIS daerah Jawa Timur	
4.	Webinar	2 September 2024	BSSN	Manajemen Risiko Keamanan Siber Pemerintah Daerah Tahun 2024	TTIS Daerah	
5.	Bimbingan Teknis	30 s.d 31 Oktober 2024	Pemerintah Kabupaten Banyuwangi	Banyuwangi Hacking Day 5.0 : Pembinaan Kapasitas Keamanan Siber Bagi Apatur Sipil	Aparatur Sipil Negara Kabupaten Banyuwangi dan Operator Pendidikan	

				Negara Kabupaten Banyuwangi		
6	Webinar	22 November 2024	BSSN	Sharing Session Penanganan Web Defacement Judi Online	TTIS Pusat dan Daerah	Pengenalan dan simulasi tools investigasi dan penyampaian lesson learned penanganan insiden web defacement perjudian daring

B. Sumber Daya Penyelenggara TTIS

Sumber Daya Penyelenggara TTIS dilakukan pembaruan setiap tahun guna mengetahui kekuatan sumber daya TTIS dalam menyelenggarakan layanan terhadap konstituen.

1. Sumber Daya Manusia TTIS

Tabel 5. Sumber Daya Manusia TTIS

No	Nama	Jabatan	Kompetensi	Pelatihan/ Sertifikasi	Unit Kerja
1.	SYAIFUDDIN YULIANSYAH, S.Kom	Anggota Sub Tim Keamanan Informasi	Keamanan Siber	CEH	Dinas Komunikasi, Informatika dan Persandian
2.	ARIF FAUZI, S.Kom	Koordinator Sub Tim Pengelola Jaringan dan Server	Keamanan Siber	CEH	Dinas Komunikasi, Informatika dan Persandian
3.	ANANG VIDHIANTO, A.Md.Kom	Anggota Sub Tim Pengelola Jaringan dan Server	Keamanan Siber	CEH	Dinas Komunikasi, Informatika dan Persandian
4.	DENDI AKHMAN WAHYU ARDANU, A.Md	Anggota Sub Tim Pengelola Jaringan dan Server	Keamanan Siber	CEH	Dinas Komunikasi, Informatika dan Persandian

5.	FAHMI MAS'UL UN ZELLYA N, A.Md	Anggota Sub Tim Website Administrator dan Aplikasi	Keamanan Siber	CEH	Dinas Komunikasi, Informatika dan Persandian

Pada Tahun 2024, Pemerintah Kabupaten Banyuwangi menyelenggarakan program peningkatan kompetensi berupa pelatihan dan sertifikasi *Certified Etichal Hacker* (CEH) yang diikuti sebanyak 5 (lima) orang pegawai Dinas Komunikasi Informatika dan Persandian Kabupaten Banyuwangi. Adapun program peningkatan kompetensi lainnya berupa Bimbingan Teknis *Cyber Drill* yang dilaksanakan dengan mengikutsertakan pegawai Dinas Komunikasi, Informatika dan Persandian. Selain itu, Pemerintah *Kabupaten Banyuwangi* turut serta mengikuti kegiatan Pertemuan Tahunan TTIS dan *Workshop* Pengelolaan TTIS yang membahas isu keamanan siber serta penyelenggaraan dan evaluasi sebuah TTIS Organisasi.

Atas capaian tersebut, Kompetensi Sumber Daya Manusia TTIS mengalami peningkatan khususnya terkait dengan pengelolaan insiden siber dan keamanan siber pada Sistem Elektronik. Namun mengingat metode serangan siber juga mengalami perkembangan seiring perkembangan teknologi informasi maka Pemerintah Kabupaten Banyuwangi akan menyelenggarakan program peningkatan kompetensi TTIS di Tahun selanjutnya berupa :

a. Pelatihan dan Sertifikasi;
b. Bimbingan Teknis;
c. Webinar.

2. Sumber Daya Perangkat TTIS

Tabel 6. Sumber Daya Perangkat TTIS

No	Nama	Spesifikasi	Jumlah	Unit Kerja/ Bidang Pengelola
1.	FORTINET Fortigate FG-1500D	Network Firewall. 2x 240GB SSD onboard storage	1 (satu)	Dinas Komunikasi, Informatika dan Persandian
2.	Website TTIS Banyuwangi-CSIRT	Ubuntu	1 (satu)	Dinas Komunikasi, Informatika dan Persandian

Pemerintah *Kabupaten Banyuwangi* diberikan alokasi dana untuk penambahan perangkat keras yang diperuntukan untuk *Kabupaten Banyuwangi*. Perangkat keras ini dioptimalkan untuk penambahan Sistem Elektronik yang dimonitor oleh sistem firewall fotigate.

3. Kebijakan, Peraturan serta Norma, Standar Prosedur dan Kriteria

Tabel 7. Kebijakan, Peraturan dan NSPK

No	Nama	Nomor	Keterangan D=Draft, R=Rilis, P=Publikasi (D/R/P, Tahun)
1.	Peraturan Bupati Banyuwangi Nomor 5 Tahun 2023 Tentang Pelaksanaan Dan Pengelolaan Sistem Keamanan Informasi Di Lingkungan Pemerintah Kabupaten Banyuwangi	Nomor 5 Tahun 2023	P, 2023
2.	Surat Edaran Sekretaris Daerah Tentang Pedoman Keamanan Siber Bagi Pegawai di Lingkungan Pemerintah Kabupaten Banyuwangi	Nomor 046/2522/429.116/2023	P, 2023
3.	Pedoman Penyelenggaraan Manajemen Keamanan Sistem Pemerintahan Berbasis Elektronik Pemerintah Kabupaten Banyuwangi	-	P, 2023
4.	Pedoman Penyelenggaraan Manajemen Keamanan Informasi Berdasarkan Iso/Iec 27001:2022	-	P, 2024

	Dalam Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik Pemerintah Kabupaten Banyuwangi		
5.	SOP Penanganan Insiden	Nomor 188/49/KEP/429.116/2024	P, 2024
6.	SOP Penanganan Insiden Virus/Malware	Nomor 188/49/KEP/429.116/2024	P, 2024
7.	SOP Penanganan Insiden Kerentanan	Nomor 188/49/KEP/429.116/2024	P, 2024
8.	SOP Penanganan Insiden DDOS	Nomor 188/49/KEP/429.116/2024	P, 2024
9.	SOP Penanganan Insiden Phising	Nomor 188/49/KEP/429.116/2024	P, 2024

Pemerintah Kabupaten Banyuwangi telah memiliki kebijakan tentang pelaksanaan persandian untuk pengamanan informasi yang ditetapkan melalui Peraturan. Kebijakan ini menjadi landasan hukum bagi Dinas Komunikasi, Informatika dan Persandian Kabupaten Banyuwangi dalam menyelenggarakan keamanan siber di lingkungan Pemerintah Kabupaten Banyuwangi.

Adapun Kebijakan tentang Standar Manajemen Keamanan Informasi menjadi standar yang harus dipatuhi oleh seluruh Organisasi Perangkat Daerah Pemerintah Kabupaten Banyuwangi dalam pengembangan dan pengelolaan Sistem Elektronik.

C. Kematangan Penanganan Insiden Siber

Pemerintah Kabupaten Banyuwangi melalui Dinas Komunikasi, Informatika dan Persandian melaksanakan kegiatan pengukuran tingkat maturitas penanganan insiber siber dengan menggunakan instrumen Tingkat Maturitas Penanganan Insiden Siber (TMPI) sebagai upaya profiling terhadap kematangan Tim Tanggap Insiden Siber dan Organisasi Dinas Komunikasi, Informatika dan Persandian dalam menerapkan keamanan siber di lingkungan Pemerintah Kabupaten Banyuwangi.

TMPI merupakan instrumen yang digunakan untuk mengukur tingkat kematangan tim tanggap insiden siber dalam melakukan pengelolaan insiden siber di internal instansi. Ruang Instrumen TMPI terdiri dari 3 (tiga) fase yaitu Persiapan, Respon dan Tindak Lanjut. Adapun masing-masing ruang lingkup memberikan gambaran secara nyata atas kondisi TTIS dalam menjalankan proses bisnis pengelolaan insiden siber.

Hasil pengukuran TMPI TTIS pada tahun 2024 diperoleh skor *2,95* atau level 3 yang menunjukkan bahwa pengelolaan insiden siber di organisasi sudah memiliki prosedur yang terdefinisi dan terstruktur. Kekuatan utama terletak pada pendataan aset yang baik, penerapan kontrol keamanan teknis seperti firewall dan IDS/IPS, serta keberadaan tim TTIS yang beroperasi dengan dukungan SOP dan pelatihan berkala. Namun, terdapat

beberapa kelemahan yang perlu diperbaiki, seperti keterbatasan dalam kemampuan deteksi insiden tingkat lanjut, dokumentasi kerugian finansial, serta pemanfaatan data insiden untuk analisis tren dan pembelajaran jangka panjang.

Upaya yang dilakukan oleh TTIS dalam meningkatkan skor TMPI berupa:

1. Penyusunan Kebijakan penanganan insiden siber;
2. Inventarisasi aset dan analisa dampak risiko, bisnis dan hukum;
3. Penyusunan skenario penanganan insiden siber serta mekakukan simulasi;

BAB IV
PENUTUP

Laporan Evaluasi Penyelenggaraan TTIS disusun berdasarkan atas capaian penyelenggaran TTIS selama 1 (satu) tahun. Hasil capaian ini merupakan wujud komitmen pimpinan Pemerintah Kabupaten Banyuwangi dalam menjaga keamanan siber terhadap sistem elektronik yang dikelola baik oleh Dinas Komunikasi Informatika dan Persandian maupun Organisasi Perangkat Daerah.

Demikian Laporan Evaluasi Penyelenggaraan TTIS disusun sebagai bahan pertimbangan Bupati Banyuwangi dan Kepala Badan Siber dan Sandi Negara dalam menentukan kebijakan dan penguatan TTIS sehingga mampu melakukan pengelolaan insiden siber secara mandiri dan profesional.

Banyuwangi , 18 Desember 2024
Kepala Dinas Komunikasi, Informatika dan Persandian
Kabupaten Banyuwangi

BUDI SANTOSO, S.Sos., M.Si
197406191993021002

LAMPIRAN

DOKUMENTASI KEGIATAN

A. Launching TTIS

Gambar 2 Peresmian TTIS Kabupaten Banyuwangi

BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA

Memberikan Surat Tanda Registrasi Tim Tanggap Insiden Siber atau Computer Security Incident Response Team (CSIRT)
Kepada :

Kabupaten Banyuwangi
Provinsi Jawa Timur

Atas terbentuknya

Banyuwangi-CSIRT

Sebagai Tim Tanggap Insiden Siber Organisasi pada Sektor Pemerintah
dengan Nomor Registrasi : **122/CSIRT.01.02.01/BSSN/11/2022**

Ditetapkan di Jakarta
pada tanggal 10 November 2022
KEPALA BADAN SIBER DAN SANDI NEGARA,

LETJEN TNI (PURN) HINSA SIBURIAN

Gambar 3 Tanda Registrasi Banyuwangi-CSIRT

B. Penyelenggaraan Layanan TTIS

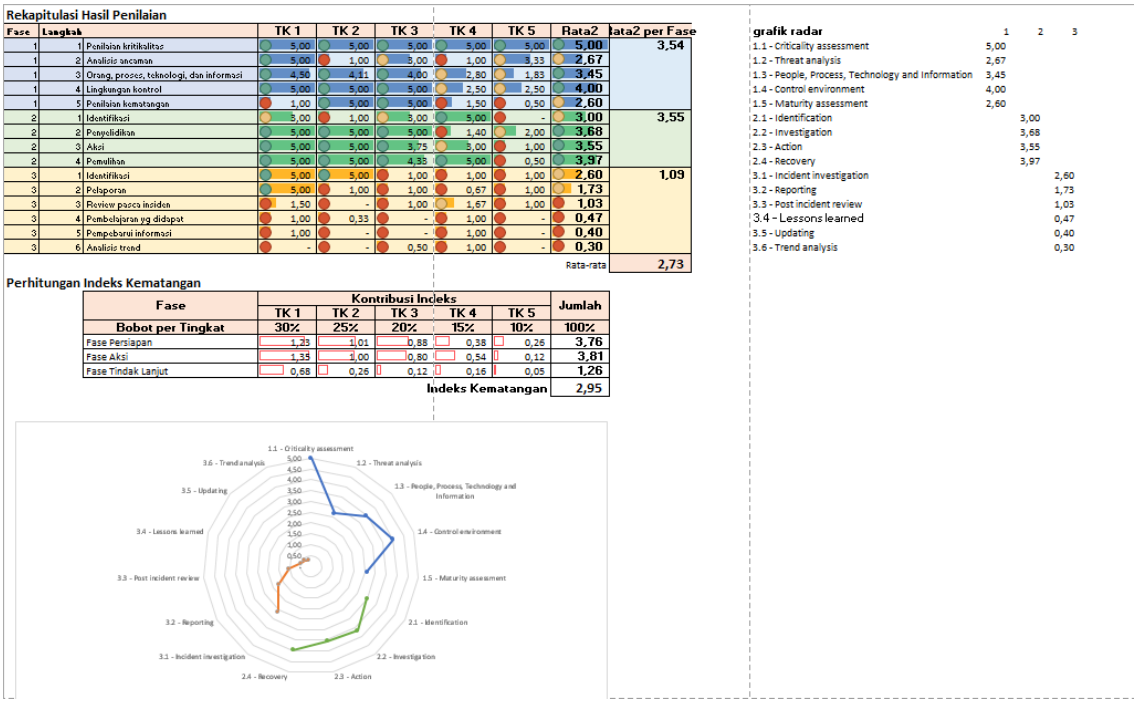
Gambar 4 Kegiatan Penanganan insiden siber malware pada perangkat komputer OPD

Gambar 5 Kegiatan Penanganan insiden siber malware pada perangkat komputer Perpustakaan JDIH

Gambar 6 Kegiatan Bimtek Hacking Day bagi Aparatur Sipil Negera Kabupaten Banyuwangi

Gambar 7 Kegiatan Bimtek Hacking Day bagi Operator Pendidikan

C. Pengukuran Kematangan Penanganan Insiden Siber



Rekapitulasi Hasil Penilaian

Fase	Langkah		TK 1	TK 2	TK 3	TK 4	TK 5	Rata2	Rata2 per Fase
1	1	Penilaian kritikalitas	5,00	5,00	5,00	5,00	5,00	5,00	3,54
1	2	Analisis ancaman	5,00	1,00	5,00	1,00	3,33	2,67	
1	3	Orang, proses, teknologi, dan informasi	4,56	4,11	4,00	2,80	1,83	3,45	
1	4	Lingkungan kontrol	5,00	5,00	5,00	2,50	2,50	4,00	
1	5	Penilaian kematangan	1,00	5,00	5,00	1,50	0,50	2,60	
2	1	Identifikasi	3,00	1,00	3,00	5,00	-	3,00	3,55
2	2	Penyelidikan	5,00	5,00	5,00	1,40	2,00	3,68	
2	3	Aksi	5,00	5,00	3,75	3,00	1,00	3,55	
2	4	Pemulihan	5,00	5,00	4,33	5,00	0,50	3,97	
3	1	Identifikasi	5,00	5,00	1,00	1,00	1,00	2,60	1,09
3	2	Pelaporan	5,00	1,00	1,00	0,67	1,00	1,73	
3	3	Review pasca insiden	1,50	-	1,00	1,67	1,00	1,03	
3	4	Pembelajaran yg didapat	1,00	0,33	-	1,00	-	0,47	
3	5	Pembaharui informasi	1,00	-	-	1,00	-	0,40	
3	6	Analisis trend	-	-	0,50	1,00	-	0,30	
								Rata-rata	2,73

Perhitungan Indeks Kematangan

Fase	Kontribusi Indeks					Jumlah
	TK 1	TK 2	TK 3	TK 4	TK 5	
Bobot per Tingkat	30%	25%	20%	15%	10%	100%
Fase Persiapan	1,23	1,01	0,88	0,38	0,26	3,76
Fase Aksi	1,35	1,00	0,80	0,54	0,12	3,81
Fase Tindak Lanjut	0,68	0,26	0,12	0,16	0,05	1,26
					Indeks Kematangan	2,95

grafik radar	1	2	3
1.1 - Criticality assessment	5,00		
1.2 - Threat analysis	2,67		
1.3 - People, Process, Technology and Information	3,45		
1.4 - Control environment	4,00		
1.5 - Maturity assessment	2,60		
2.1 - Identification		3,00	
2.2 - Investigation		3,68	
2.3 - Action		3,55	
2.4 - Recovery		3,97	
3.1 - Incident investigation			2,60
3.2 - Reporting			1,73
3.3 - Post incident review			1,03
3.4 - Lessons learned			0,47
3.5 - Updating			0,40
3.6 - Trend analysis			0,30

Gambar 8 Tampilan hasil TMPI