PEMERINTAH KABUPATEN MIMIKA

INOVASI WARGA MIMIKA

Kategori Anugerah

Inovasi Warga Mimika

Inovator

Judul Inovasi

SIJAGA — Sistem Intelijen Jaringan dan Aset Digital Pemerintah

Tanggal Pengembangan Inovasi

Latar Belakang Permasalahan

Pemerintah Kabupaten Mimika mengoperasikan banyak situs web dan aplikasi yang sebagian besar dikelola sendiri oleh masing-masing OPD, tanpa pemantauan terpusat:

- Situs web sering tidak dapat diakses (down) tanpa diketahui pengelola hingga dilaporkan masyarakat;
- Sertifikat SSL kedaluwarsa dan masa aktif domain habis tanpa peringatan, membuat layanan tiba-tiba tidak dapat diakses atau ditandai tidak aman;
- Banyak CMS dan plugin tidak diperbarui sehingga memiliki celah keamanan yang diketahui publik;
- Situs pemerintah pernah disusupi malware, diretas, bahkan berubah menampilkan konten judi daring (defacement) tanpa terdeteksi dini;
- Tidak ada inventaris aset digital: Diskominfo tidak memiliki daftar lengkap situs, subdomain, server, dan aplikasi yang harus dilindungi;
- Tidak ada dasbor pemantauan, sistem peringatan dini, maupun pemantauan cadangan data (backup);
- Pemantauan manual membuat laporan kondisi SPBE dan audit keamanan sulit, lambat, dan tidak menyeluruh.

Akibatnya pelayanan publik terganggu, risiko kebocoran data meningkat, indeks SPBE dan keamanan informasi menurun, serta biaya pemeliharaan membengkak. Kondisi tersebut mendorong lahirnya gagasan **SIJAGA (Sistem Intelijen Jaringan dan Aset Digital Pemerintah)**: platform pemantauan seluruh aset digital pemerintah daerah dalam satu dasbor waktu nyata dengan peringatan dini dan kecerdasan artifisial.

Tujuan Melakukan Inovasi

1. Meningkatkan keamanan seluruh aset digital Pemerintah Kabupaten Mimika melalui pemantauan terpusat dan peringatan dini ancaman siber;
2. Membangun inventaris aset digital pemerintah daerah (situs, aplikasi, API, server, domain, SSL, basis data, backup) yang lengkap dan selalu mutakhir;
3. Menurunkan waktu henti (downtime) layanan digital dengan deteksi gangguan dalam hitungan menit, bukan setelah dilaporkan masyarakat;
4. Mencegah insiden memalukan dan merugikan — sertifikat/domain kedaluwarsa, peretasan, malware, dan perubahan situs menjadi konten judi — melalui deteksi dini otomatis;
5. Menyediakan skor keamanan dan kesehatan per aset dan per OPD sebagai dasar pembinaan serta prioritas perbaikan;
6. Mempermudah audit keamanan dan pelaporan kondisi SPBE/indeks KAMI melalui laporan otomatis dan jejak audit;
7. Menyediakan dasbor eksekutif bagi Bupati dan Sekretaris Daerah sebagai dasar kebijakan tata kelola TI berbasis data.

Manfaat

Outcome yang ditargetkan dan indikator pengukurannya (mohon dilengkapi dengan angka aktual saat implementasi):

- **Downtime layanan menurun** — indikator: waktu rata-rata deteksi dan pemulihan gangguan; persentase uptime layanan publik digital;
- **Insiden keamanan dicegah lebih dini** — indikator: jumlah SSL/domain diperpanjang sebelum kedaluwarsa; jumlah indikasi malware/defacement terdeteksi dan ditangani sebelum viral;
- **Tata kelola terukur** — indikator: skor keamanan/kesehatan per OPD dan trennya; jumlah OPD yang menindaklanjuti pembinaan;
- **Audit dan SPBE lebih mudah** — indikator: waktu penyusunan laporan kondisi TI (dari minggu menjadi seketika); kontribusi pada kenaikan indeks SPBE dan indeks KAMI;
- **Efisiensi anggaran** — indikator: penurunan biaya pemulihan insiden dan pemeliharaan reaktif;
- **Kepercayaan publik meningkat** — indikator: berkurangnya insiden situs pemerintah bermasalah yang menjadi sorotan publik.

Manfaat dirasakan berlapis: masyarakat memperoleh layanan digital yang andal dan aman; admin OPD terbantu peringatan otomatis; Diskominfo memiliki alat pembinaan; pimpinan daerah memperoleh visibilitas penuh; Tim SPBE dan Inspektorat memperoleh data audit yang siap pakai.

Rancang Bangun atau Desain Inovasi

a. Permasalahan yang melatarbelakangi munculnya ide inovasi
Pemerintah Kabupaten Mimika mengoperasikan banyak situs web dan aplikasi yang sebagian besar dikelola sendiri oleh masing-masing OPD, tanpa pemantauan terpusat:

- Situs web sering tidak dapat diakses (down) tanpa diketahui pengelola hingga dilaporkan masyarakat;
- Sertifikat SSL kedaluwarsa dan masa aktif domain habis tanpa peringatan, membuat layanan tiba-tiba tidak dapat diakses atau ditandai tidak aman;
- Banyak CMS dan plugin tidak diperbarui sehingga memiliki celah keamanan yang diketahui publik;
- Situs pemerintah pernah disusupi malware, diretas, bahkan berubah menampilkan konten judi daring (defacement) tanpa terdeteksi dini;
- Tidak ada inventaris aset digital: Diskominfo tidak memiliki daftar lengkap situs, subdomain, server, dan aplikasi yang harus dilindungi;
- Tidak ada dasbor pemantauan, sistem peringatan dini, maupun pemantauan cadangan data (backup);
- Pemantauan manual membuat laporan kondisi SPBE dan audit keamanan sulit, lambat, dan tidak menyeluruh.

Akibatnya pelayanan publik terganggu, risiko kebocoran data meningkat, indeks SPBE dan keamanan informasi menurun, serta biaya pemeliharaan membengkak. Kondisi tersebut mendorong lahirnya gagasan **SIJAGA (Sistem Intelijen Jaringan dan Aset Digital Pemerintah)**: platform pemantauan seluruh aset digital pemerintah daerah dalam satu dasbor waktu nyata dengan peringatan dini dan kecerdasan artifisial.

b. Gagasan utama/ide inovasi
SIJAGA (Sistem Intelijen Jaringan dan Aset Digital Pemerintah) adalah platform terpadu yang memantau kesehatan, keamanan, kinerja, dan kepatuhan seluruh aset digital Pemerintah Kabupaten Mimika — situs web, aplikasi, API, server/VM/cloud, basis data, domain, DNS, sertifikat SSL, email, subdomain, hingga status backup — dalam satu dasbor waktu nyata, dirancang untuk diterapkan bersama Dinas Komunikasi dan Informatika.

SIJAGA bekerja dalam tiga lapisan:

1. **Lapisan inventaris:** penemuan aset otomatis (asset discovery, termasuk pemetaan subdomain) membentuk inventaris aset digital yang selalu mutakhir beserta penanggung jawab tiap OPD — fondasi tata kelola yang selama ini tidak ada;

2. **Lapisan pemantauan & peringatan dini:** pemeriksaan berkala tanpa agen (agentless) atas ketersediaan (uptime), kinerja, masa aktif SSL/domain, konfigurasi keamanan (security header), versi CMS/plugin, indikasi malware dan defacement (termasuk perubahan menjadi konten judi), serta status backup; setiap temuan kritis memicu peringatan otomatis ke WhatsApp/Telegram/email pengelola OPD dan operator Diskominfo;
3. **Lapisan kecerdasan:** AI menilai skor keamanan dan kesehatan tiap aset, memprediksi potensi gangguan dan kebutuhan kapasitas, memprioritaskan kerentanan yang harus ditambal, merangkum kondisi dalam narasi eksekutif otomatis bagi pimpinan, dan menyusun laporan kepatuhan pendukung penilaian SPBE dan indeks KAMI — dengan tindak lanjut selalu diputuskan manusia (human in the loop).

SIJAGA diposisikan sebagai cikal bakal *Government Security Operation Center* (SOC) daerah dan dirancang replikabel bagi pemerintah daerah lain.

c. Metode Pembaharuan (upaya yang akan dilakukan sebelum dan sesudah inovasi)
Sebelum adanya inovasi:

- Tidak ada inventaris aset digital; situs dan aplikasi tersebar tanpa daftar induk.
- Gangguan diketahui setelah dilaporkan masyarakat; SSL/domain kedaluwarsa tanpa peringatan.
- Peretasan, malware, dan defacement (termasuk konten judi) terdeteksi terlambat.
- Kondisi keamanan tiap OPD tidak terukur; laporan SPBE dan audit disusun manual.

Sesudah adanya inovasi:

- Inventaris aset digital otomatis dan selalu mutakhir dengan penanggung jawab jelas per OPD.
- Seluruh aset dipantau waktu nyata dari satu dasbor; gangguan diketahui dalam hitungan menit.
- Peringatan dini otomatis (WhatsApp/Telegram/email) sebelum SSL/domain kedaluwarsa dan saat terdeteksi anomali, malware, atau defacement.
- Skor keamanan dan kesehatan per aset/per OPD menjadi dasar pembinaan dan prioritas penambalan.
- Laporan kondisi SPBE, keamanan, dan aset dihasilkan otomatis untuk pimpinan, Tim SPBE, dan Inspektorat.

d. Keterlibatan aktor inovasi: stakeholder pentahelix yang perlu dilibatkan dan perannya
- **Pemerintah:** Diskominfo sebagai pengelola platform dan pembina keamanan informasi; admin OPD sebagai penanggung jawab aset dan penindak lanjut peringatan; Bupati/Sekretaris Daerah sebagai pengguna dasbor eksekutif; Tim SPBE dan Inspektorat sebagai pengguna laporan kepatuhan dan audit; BSSN (Gov-CSIRT) sebagai mitra rujukan penanganan insiden dan intelijen ancaman.
- **Akademisi:** perguruan tinggi sebagai mitra kajian keamanan, audit metodologi penilaian skor, dan penyiapan talenta keamanan siber lokal.
- **Dunia Usaha/Swasta:** penyedia hosting/cloud dan registrar domain sebagai sumber data melalui API; mitra teknologi keamanan sebagai pendukung pengembangan.
- **Ormas/Masyarakat:** penerima manfaat layanan digital yang andal; kanal pelaporan publik bila menemukan situs pemerintah bermasalah.
- **Media Massa:** mendorong transparansi kualitas layanan digital pemerintah dan edukasi keamanan informasi.

e. Keunggulan/Kebaharuan inovasi
Kebaruan SIJAGA terletak pada perubahan tata kelola aset digital dari reaktif-tersebar menjadi proaktif-terpusat:

Aspek	Kondisi Saat Ini	Dengan SIJAGA
Inventaris aset digital	Tidak ada daftar induk	Asset discovery otomatis, inventaris selalu mutakhir + penanggung jawab per OPD
Deteksi gangguan	Setelah dilaporkan masyarakat	Pemantauan waktu nyata, peringatan dalam hitungan menit
SSL/domain kedaluwarsa	Layanan mati mendadak	Peringatan dini bertingkat jauh sebelum jatuh tempo

Aspek	Kondisi Saat Ini	Dengan SIJAGA
Peretasan/defacement/judi	Terdeteksi terlambat, viral lebih dulu	Deteksi perubahan konten dan indikasi malware otomatis oleh AI
Keamanan per OPD	Tidak terukur	Skor keamanan & kesehatan per aset/OPD sebagai dasar pembinaan
Laporan SPBE/audit	Manual, lambat, parsial	Laporan kepatuhan otomatis pendukung penilaian SPBE/indeks KAMI
Pimpinan daerah	Tidak ada visibilitas	Dasbor eksekutif + narasi otomatis AI yang mudah dipahami non-teknis

Sepanjang penelusuran, belum terdapat pemerintah kabupaten/kota di Tanah Papua yang mengoperasikan platform pemantauan aset digital terpadu dengan peringatan dini dan penilaian keamanan berbasis kecerdasan artifisial. Pembeda SIJAGA dari perangkat monitoring komersial: (1) dibangun untuk konteks tata kelola pemerintahan — terhubung ke struktur OPD, penilaian SPBE/indeks KAMI, dan alur pembinaan Diskominfo; (2) pemantauan tanpa agen sehingga OPD tidak perlu mengubah sistemnya; (3) seluruh temuan dikelola dengan prinsip human in the loop dan menjadi cikal bakal SOC pemerintah daerah.

f. Tahapan kerja inovasi atau spesifikasi produk

1. Inventarisasi: penemuan aset otomatis (situs, subdomain, IP publik, server, aplikasi) dan registrasi penanggung jawab tiap OPD.
2. Pemantauan berkala tanpa agen: ketersediaan dan waktu respons, masa aktif SSL/domain/DNS, security header, versi CMS/plugin, indikasi malware dan perubahan konten (defacement/judi), kesehatan server (CPU, memori, penyimpanan), API, basis data, dan status backup.
3. Peringatan dini: temuan kritis memicu notifikasi otomatis bertingkat (WhatsApp, Telegram, email, dasbor) ke admin OPD dan operator Diskominfo sesuai eskalasi.
4. Analisis AI: penilaian skor keamanan/kesehatan per aset dan per OPD, prioritas kerentanan, prediksi gangguan dan kapasitas, intelijen ancaman, serta narasi eksekutif otomatis.
5. Tindak lanjut: operator memverifikasi temuan (human in the loop), berkoordinasi dengan OPD untuk perbaikan/penambalan, dan mencatat insiden hingga tuntas; insiden signifikan dirujuk ke Gov-CSIRT/BSSN.
6. Pelaporan: laporan berkala kondisi aset, keamanan, dan kepatuhan SPBE untuk pimpinan, Tim SPBE, dan Inspektorat; jejak audit lengkap.

Spesifikasi produk: platform web dengan dasbor operasional dan dasbor eksekutif; mesin pemeriksa terdistribusi (uptime, SSL, DNS, header, konten) tanpa agen; pemindai kerentanan dan deteksi perubahan konten; integrasi API penyedia cloud/registrar; notifikasi multi-kanal; peta GIS sebaran aset; modul AI penilaian skor, prediksi, dan peringkas naratif; kontrol akses berjenjang (Diskominfo, OPD, pimpinan, auditor); seluruhnya selaras arsitektur SPBE, standar keamanan informasi (SNI ISO/IEC 27001, indeks KAMI), dan Undang-Undang Pelindungan Data Pribadi.

g. Keberlanjutan inovasi: potensi pengembangan dan replikasi inovasi

- **Pendanaan:** tahap rintisan melalui APBD (Diskominfo); efisiensi dari penurunan insiden, penghematan biaya pemulihan, dan perbaikan indeks SPBE menjadi justifikasi anggaran berkelanjutan;
- **Regulasi:** diusulkan Peraturan Bupati tata kelola aset digital dan keamanan informasi — kewajiban registrasi aset OPD ke SIJAGA, standar minimal keamanan, dan prosedur tindak lanjut peringatan;
- **Sumber daya manusia:** tim pengelola pada Diskominfo (embrio SOC daerah), pelatihan admin OPD, dan kemitraan perguruan tinggi untuk talenta keamanan siber;
- **Infrastruktur dan pemeliharaan:** arsitektur modular dengan pemeriksa terdistribusi; pembaruan tanda tangan ancaman dan pemeliharaan rutin; cadangan data platform terjadwal;
- **Peta jalan lima tahun:** Tahun 1 — inventaris aset, pemantauan situs/server/SSL/domain, peringatan dini; Tahun 2 — pemantauan API, basis data, cloud, dan backup; Tahun 3 — AI keamanan penuh (skor, prediksi, intelijen ancaman); Tahun 4 — Government Security Operation Center daerah; Tahun 5 — Regional Government Digital Intelligence Platform yang direplikasi pemerintah daerah lain;
- **Pengembangan AI:** evaluasi akurasi deteksi berkala, audit metodologi skor, dan human in the loop pada seluruh tindak lanjut;

- **Integrasi SPBE:** keluaran laporan diselaraskan dengan instrumen penilaian SPBE dan indeks KAMI; koordinasi insiden dengan Gov-CSIRT/BSSN;
- **Replikasi:** desain multi-tenant dan standar terbuka memungkinkan adopsi kabupaten/kota lain dengan biaya rendah — menjawab masalah yang sama di hampir semua daerah.

Kebaruan, Keunikan atau Keaslian

Kebaruan SIJAGA terletak pada perubahan tata kelola aset digital dari reaktif-tersebar menjadi proaktif-terpusat:

Aspek	Kondisi Saat Ini	Dengan SIJAGA
Inventaris aset digital	Tidak ada daftar induk	Asset discovery otomatis, inventaris selalu mutakhir + penanggung jawab per OPD
Deteksi gangguan	Setelah dilaporkan masyarakat	Pemantauan waktu nyata, peringatan dalam hitungan menit
SSL/domain kedaluwarsa	Layanan mati mendadak	Peringatan dini bertingkat jauh sebelum jatuh tempo
Peretasan/defacement/judi	Terdeteksi terlambat, viral lebih dulu	Deteksi perubahan konten dan indikasi malware otomatis oleh AI
Keamanan per OPD	Tidak terukur	Skor keamanan & kesehatan per aset/OPD sebagai dasar pembinaan
Laporan SPBE/audit	Manual, lambat, parsial	Laporan kepatuhan otomatis pendukung penilaian SPBE/indeks KAMI
Pimpinan daerah	Tidak ada visibilitas	Dasbor eksekutif + narasi otomatis AI yang mudah dipahami non-teknis

Sepanjang penelusuran, belum terdapat pemerintah kabupaten/kota di Tanah Papua yang mengoperasikan platform pemantauan aset digital terpadu dengan peringatan dini dan penilaian keamanan berbasis kecerdasan artifisial. Pembeda SIJAGA dari perangkat monitoring komersial: (1) dibangun untuk konteks tata kelola pemerintahan — terhubung ke struktur OPD, penilaian SPBE/indeks KAMI, dan alur pembinaan Diskominfo; (2) pemantauan tanpa agen sehingga OPD tidak perlu mengubah sistemnya; (3) seluruh temuan dikelola dengan prinsip human in the loop dan menjadi cikal bakal SOC pemerintah daerah.

Tingkat Kesiapterapan atau Keunggulan Produk

SIJAGA saat ini berada pada tahap **rancangan siap bangun menuju prototipe**: arsitektur, modul pemantauan, alur peringatan dini, dan pemilihan teknologi telah selesai dirancang; pembangunan purwarupa inventaris aset dan pemantauan situs/SSL/domain merupakan tahap pertama peta jalan.

Output terukur yang ditargetkan pada tahun pertama penerapan (mohon dilengkapi dengan angka aktual saat implementasi):

- Purwarupa beroperasi memantau aset digital Pemkab Mimika pada dasbor tunggal;
- Jumlah aset digital terinventarisasi (situs, subdomain, server, aplikasi) beserta penanggung jawab OPD;
- Persentase situs pemerintah yang terpantau uptime, SSL, dan domainnya;
- Jumlah peringatan dini terkirim dan ditindaklanjuti (SSL/domain diperpanjang sebelum kedaluwarsa, gangguan dipulihkan);
- Waktu rata-rata deteksi gangguan (dari hari menjadi menit).

Kesiapterapan didukung oleh: pendekatan pemantauan tanpa agen sehingga tidak mengubah sistem OPD yang ada, teknologi pemantauan yang telah matang, kebutuhan infrastruktur ringan pada tahap awal, dan model rintisan bertahap per modul sesuai peta jalan.

Kemanfaatan Produk Inovasi

Outcome yang ditargetkan dan indikator pengukurannya (mohon dilengkapi dengan angka aktual saat implementasi):

- **Downtime layanan menurun** — indikator: waktu rata-rata deteksi dan pemulihan gangguan; persentase uptime layanan publik digital;
- **Insiden keamanan dicegah lebih dini** — indikator: jumlah SSL/domain diperpanjang sebelum kedaluwarsa; jumlah indikasi malware/defacement terdeteksi dan ditangani sebelum viral;
- **Tata kelola terukur** — indikator: skor keamanan/kesehatan per OPD dan trennya; jumlah OPD yang menindaklanjuti pembinaan;
- **Audit dan SPBE lebih mudah** — indikator: waktu penyusunan laporan kondisi TI (dari minggu menjadi seketika); kontribusi pada kenaikan indeks SPBE dan indeks KAMI;
- **Efisiensi anggaran** — indikator: penurunan biaya pemulihan insiden dan pemeliharaan reaktif;
- **Kepercayaan publik meningkat** — indikator: berkurangnya insiden situs pemerintah bermasalah yang menjadi sorotan publik.

Manfaat dirasakan berlapis: masyarakat memperoleh layanan digital yang andal dan aman; admin OPD terbantu peringatan otomatis; Diskominfo memiliki alat pembinaan; pimpinan daerah memperoleh visibilitas penuh; Tim SPBE dan Inspektorat memperoleh data audit yang siap pakai.

Tingkat Keberlanjutan

- **Pendanaan:** tahap rintisan melalui APBD (Diskominfo); efisiensi dari penurunan insiden, penghematan biaya pemulihan, dan perbaikan indeks SPBE menjadi justifikasi anggaran berkelanjutan;
- **Regulasi:** diusulkan Peraturan Bupati tata kelola aset digital dan keamanan informasi — kewajiban registrasi aset OPD ke SIJAGA, standar minimal keamanan, dan prosedur tindak lanjut peringatan;
- **Sumber daya manusia:** tim pengelola pada Diskominfo (embrio SOC daerah), pelatihan admin OPD, dan kemitraan perguruan tinggi untuk talenta keamanan siber;
- **Infrastruktur dan pemeliharaan:** arsitektur modular dengan pemeriksa terdistribusi; pembaruan tanda tangan ancaman dan pemeliharaan rutin; cadangan data platform terjadwal;
- **Peta jalan lima tahun:** Tahun 1 — inventaris aset, pemantauan situs/server/SSL/domain, peringatan dini; Tahun 2 — pemantauan API, basis data, cloud, dan backup; Tahun 3 — AI keamanan penuh (skor, prediksi, intelijen ancaman); Tahun 4 — Government Security Operation Center daerah; Tahun 5 — Regional Government Digital Intelligence Platform yang direplikasi pemerintah daerah lain;
- **Pengembangan AI:** evaluasi akurasi deteksi berkala, audit metodologi skor, dan human in the loop pada seluruh tindak lanjut;
- **Integrasi SPBE:** keluaran laporan diselaraskan dengan instrumen penilaian SPBE dan indeks KAMI; koordinasi insiden dengan Gov-CSIRT/BSSN;
- **Replikasi:** desain multi-tenant dan standar terbuka memungkinkan adopsi kabupaten/kota lain dengan biaya rendah — menjawab masalah yang sama di hampir semua daerah.