PEDOMAN TEKNIS

LADA (LAYANAN ANALITIK DETEKSI ANCAMAN)

DINKOMINFOTIK KABUPATEN BANGKA

PEDOMAN TEKNIS INOVASI LADA

(LAYANAN ANALITIK DETEKSI ANCAMAN)

BAB I

PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi informasi dan komunikasi telah mendorong percepatan transformasi digital dalam penyelenggaraan pemerintahan. Pemanfaatan sistem elektronik, aplikasi layanan publik, pusat data, jaringan komputer, dan layanan berbasis internet menjadi bagian yang tidak terpisahkan dari penyelenggaraan pemerintahan modern.

Di sisi lain, meningkatnya ketergantungan terhadap teknologi informasi turut meningkatkan risiko ancaman keamanan siber yang dapat mengganggu ketersediaan, integritas, dan kerahasiaan informasi. Ancaman tersebut dapat berupa serangan malware, ransomware, brute force attack, unauthorized access, eksploitasi kerentanan sistem, hingga berbagai bentuk serangan siber lainnya yang berpotensi mengganggu layanan pemerintahan dan pelayanan publik.

Dalam pelaksanaannya, pengelolaan keamanan informasi di lingkungan Pemerintah Kabupaten Bangka masih menghadapi tantangan berupa keterbatasan sistem pemantauan terintegrasi, belum optimalnya konsolidasi log keamanan, keterbatasan data untuk analisis ancaman secara cepat, serta belum tersedianya mekanisme evaluasi keamanan yang terstruktur dan berkelanjutan.

Untuk menjawab tantangan tersebut, Pemerintah Kabupaten Bangka melalui Dinas Komunikasi, Informatika dan Statistik mengembangkan inovasi **LADA (Layanan Analitik Deteksi Ancaman)** sebagai sistem monitoring keamanan informasi yang terintegrasi dan berbasis sumber terbuka (open source). Sistem ini memanfaatkan platform Wazuh untuk melakukan pemantauan keamanan siber secara real-time, mendeteksi ancaman secara dini, mengonsolidasikan log dari berbagai server, serta mendukung respons insiden yang lebih cepat, tepat, dan terukur.

Melalui implementasi LADA, diharapkan terwujud penguatan tata kelola keamanan informasi, peningkatan ketahanan siber pemerintah daerah, serta peningkatan kepercayaan masyarakat terhadap layanan digital Pemerintah Kabupaten Bangka.

B. Dasar Hukum

1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024.
2. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
3. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah.
4. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
5. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.
6. Peraturan Badan Siber dan Sandi Negara tentang Penyelenggaraan Keamanan Siber dan Pembentukan CSIRT.
7. Peraturan perundang-undangan lainnya yang berkaitan dengan keamanan informasi dan keamanan siber.

C. Maksud

Pedoman teknis ini disusun sebagai acuan dalam pelaksanaan Inovasi LADA guna mendukung pengelolaan keamanan informasi yang efektif, terintegrasi, terukur, dan berkelanjutan di lingkungan Pemerintah Kabupaten Bangka.

D. Tujuan

Sistem LADA ini dikembangkan dengan maksud dan tujuan sebagai berikut:

1. Membangun sistem monitoring keamanan informasi yang terintegrasi dan beroperasi secara *real-time* di lingkungan Pemerintah Kabupaten Bangka.

2. Menyediakan data pemantauan keamanan informasi yang valid, terpusat, dan mudah dianalisis sebagai dasar pengambilan keputusan strategis pimpinan.

3. Meningkatkan kecepatan dan ketepatan deteksi dini serta respons terhadap ancaman dan insiden keamanan siber.

4. Mewujudkan standar prosedur kerja (SOP) monitoring keamanan informasi yang baku dan dapat diterapkan secara konsisten di seluruh unit kerja.

5. Memperkuat sinergi dan kolaborasi lintas bidang dalam pengelolaan keamanan informasi daerah melalui forum evaluasi yang terstruktur.

6. Meningkatkan ketahanan siber Pemerintah Kabupaten Bangka dan kepercayaan masyarakat terhadap keamanan layanan digital pemerintah.

E. Sasaran

1. Dinas Komunikasi, Informatika dan Statistik Kabupaten Bangka.
2. Tim Tanggap Insiden Siber (TTIS)/CSIRT Kabupaten Bangka.
3. Administrator sistem dan jaringan.
4. Pengelola aplikasi dan website pemerintah daerah.
5. Seluruh perangkat daerah yang menggunakan infrastruktur teknologi informasi pemerintah daerah.

BAB II

TAHAPAN INOVASI

No.	Tahapan Inovasi	Deskripsi Kegiatan	Output	Waktu
1	Identifikasi Masalah dan Analisis Kebutuhan	Melakukan kajian mendalam terhadap kondisi keamanan informasi yang ada, pemetaan potensi ancaman siber, serta analisis kesenjangan (gap analysis) antara kondisi nyata dengan standar keamanan yang diharapkan.	Dokumen analisis kebutuhan sistem monitoring keamanan informasi	Agustus 2025

No.	Tahapan Inovasi	Deskripsi Kegiatan	Output	Waktu
2 3	Perancangan Arsitektur Sistem SIEM Pembangunan dan Konfigurasi Sistem	Merancang arsitektur teknis sistem SIEM Wazuh, menyusun SOP Monitoring Keamanan Informasi, serta menetapkan pembagian peran antara Bidang Persandian dan Bidang e-Government dalam operasional sistem monitoring. Melakukan instalasi Wazuh Manager dan konfigurasi dashboard pemantauan, pemasangan agent Wazuh pada server-server utama Dinkominfotik Bangka, serta pengaturan rule deteksi ancaman sesuai kebutuhan instansi.	Rancangan teknis sistem dan SOP Monitoring Keamanan Informasi Sistem Wazuh SIEM aktif dengan dashboard dan agent terpasang	Agustus – September 2025 September 2025
4	Uji Coba dan Validasi Sistem	Menjalankan simulasi insiden keamanan untuk menguji akurasi deteksi Wazuh, memverifikasi kelengkapan data log yang terekam, serta melakukan kalibrasi rule dan konfigurasi sistem berdasarkan hasil evaluasi teknis bersama Tim Tanggap Insiden Siber (TTIS).	Laporan uji coba dan berita acara validasi sistem bersama TTIS	September – Oktober 2025

No.	Tahapan Inovasi	Deskripsi Kegiatan	Output	Waktu
5	Implementasi dan Operasionalisasi	Mengoperasikan sistem SIEM secara penuh dengan pembentukan mekanisme monitoring rutin, pelaksanaan forum diskusi bulanan bersama TTIS untuk evaluasi hasil monitoring, serta penyampaian laporan keamanan berkala kepada pimpinan.	Sistem beroperasi penuh, laporan monitoring berkala tersedia	Oktober 2025
6	Evaluasi Efektivitas dan Pengembangan Lanjutan	Mengukur efektivitas sistem SIEM melalui indikator kinerja yang telah ditetapkan, menyusun rekomendasi peningkatan cakupan monitoring ke perangkat daerah lain, serta merencanakan integrasi dengan sistem keamanan daerah yang lebih luas.	Laporan evaluasi efektivitas dan roadmap pengembangan sistem	Oktober 2025 – Berkelanjutan

BAB III

RANCANG BANGUN INOVASI

A. Gambaran Umum

LADA (Layanan Analitik Deteksi Ancaman) merupakan sistem monitoring keamanan informasi yang dibangun dengan memanfaatkan platform sumber terbuka Wazuh sebagai pusat pengumpulan, analisis, dan pemantauan log keamanan dari berbagai aset teknologi informasi Pemerintah Kabupaten Bangka.

Sistem ini dirancang untuk memberikan kemampuan deteksi dini terhadap ancaman keamanan siber melalui pengumpulan log secara terpusat, analisis otomatis, visualisasi data keamanan secara real-time, serta dukungan prosedur operasional yang terstandarisasi.

B. Komponen Utama Sistem

1. LADA Manager (Wazuh Manager)

Merupakan pusat pengelolaan dan analisis log keamanan yang berfungsi sebagai inti sistem. Komponen ini menerima data dari seluruh agen, melakukan korelasi log, mendeteksi ancaman secara otomatis, dan menghasilkan notifikasi atau peringatan keamanan.

2. LADA Agent (Wazuh Agent)

Agen yang dipasang pada server atau perangkat yang dipantau. Agen bertugas mengumpulkan log aktivitas sistem dan mengirimkannya secara real-time melalui saluran komunikasi terenkripsi ke LADA Manager.

3. LADA Dashboard

Antarmuka berbasis web yang menampilkan visualisasi kondisi keamanan informasi secara real-time, meliputi indikator ancaman, status server, aktivitas sistem, dan laporan keamanan yang dapat diakses oleh administrator dan tim pengelola.

4. SOP Monitoring Keamanan Informasi

Dokumen prosedur operasional standar yang mengatur mekanisme monitoring, klasifikasi insiden, eskalasi penanganan, pelaporan, dan tindak lanjut terhadap ancaman keamanan informasi.

5. Forum Evaluasi TTIS

Forum evaluasi bulanan yang melibatkan Tim Tanggap Insiden Siber untuk melakukan kajian terhadap insiden yang terjadi, mengevaluasi efektivitas pengendalian, serta menyusun rekomendasi peningkatan keamanan informasi.

C. Metode Pembaharuan

1. Implementasi platform monitoring keamanan berbasis Wazuh.
2. Integrasi log keamanan dari seluruh server ke dalam satu sistem.

3. Penyediaan dashboard monitoring real-time.
4. Otomatisasi deteksi ancaman dan notifikasi insiden.
5. Penerapan SOP monitoring keamanan informasi.
6. Pelaksanaan evaluasi berkala melalui Forum TTIS.

D. Keunggulan Inovasi

1. Menggunakan platform open source tanpa biaya lisensi.
2. Monitoring keamanan dilakukan secara real-time.
3. Konsolidasi log dari berbagai aset teknologi informasi.
4. Deteksi dini ancaman secara otomatis.
5. Dashboard keamanan yang mudah dipahami.
6. Mendukung tata kelola keamanan informasi yang terukur.
7. Skalabel dan dapat dikembangkan sesuai kebutuhan organisasi.
8. Efisien dari sisi biaya implementasi dan operasional.

BAB IV

PEDOMAN TEKNIS INOVASI

A. Arsitektur Sistem LADA

Sistem LADA dibangun dengan arsitektur terdistribusi. Wazuh Manager dipasang pada server dedicated yang berfungsi sebagai pusat pemrosesan data keamanan. Agent Wazuh dipasang pada setiap server yang dikelola Dinkominfotik Bangka dan mengirimkan data log secara terenkripsi ke Manager. Dashboard terpusat dapat diakses melalui browser oleh seluruh anggota tim monitoring dari jaringan internal pemerintah.

B. Mekanisme Deteksi dan Alert

Wazuh secara otomatis menganalisis log yang masuk menggunakan rule-set bawaan yang dapat dikustomisasi sesuai kebutuhan instansi. Setiap temuan dikategorikan berdasarkan tingkat keparahan: Critical (ancaman kritis yang memerlukan penanganan segera), High (ancaman tinggi), Medium (anomali yang

perlu diinvestigasi), dan Low (informasi pemantauan umum). Alert otomatis dikirimkan kepada petugas monitoring saat threshold tertentu terlampaui.

C. Manajemen Log Terpusat

Seluruh log dari server dan perangkat yang terhubung diagregasi dalam satu repositori terpusat di Wazuh Manager. Data log dapat diakses, dicari, dan dianalisis

melalui dashboard dengan fitur filter berdasarkan waktu, sumber, jenis event, dan tingkat keparahan. Sistem juga mendukung retensi log jangka panjang untuk keperluan forensik dan audit keamanan.

D. Pemantauan Integritas File dan Kerentanan

Wazuh secara aktif memantau perubahan pada file-file kritis di sistem (File Integrity Monitoring/FIM), memberikan peringatan dini jika terjadi modifikasi yang tidak sah. Selain itu, sistem secara berkala melakukan pemindaian kerentanan (vulnerability assessment) pada seluruh server yang terhubung dan menampilkan hasilnya di dashboard untuk ditindaklanjuti tim teknis.

E. Pelaporan dan Dokumentasi Berkala

Dashboard Wazuh dilengkapi fitur pembuatan laporan yang dapat dikonfigurasi sesuai kebutuhan. Laporan monitoring mencakup ringkasan ancaman, statistik insiden, status keamanan per server, dan tren dalam periode tertentu. Laporan ini menjadi dokumen resmi yang disampaikan kepada Kepala Dinas sebagai bahan evaluasi dan pengambilan keputusan strategis terkait keamanan informasi daerah.

BAB V

MONITORING DAN EVALUASI

Monitoring dan evaluasi dilakukan secara berkala terhadap:

1. Jumlah ancaman yang terdeteksi.
2. Waktu respons penanganan insiden.
3. Ketersediaan dan keandalan sistem monitoring.
4. Tingkat kepatuhan pelaksanaan SOP.

5. Efektivitas mitigasi ancaman keamanan informasi.
6. Hasil evaluasi Forum TTIS.

BAB VI

PENUTUP

Pedoman Teknis Inovasi LADA (Layanan Analitik Deteksi Ancaman) ini menjadi acuan dalam penyelenggaraan monitoring keamanan informasi secara terintegrasi di lingkungan Pemerintah Kabupaten Bangka. Melalui penerapan sistem ini diharapkan terwujud pengelolaan keamanan informasi yang efektif, responsif, terukur, dan berkelanjutan guna mendukung tata kelola pemerintahan digital yang aman, andal, dan terpercaya.