Jurnal Minfo Polgan
Volume 14, Nomor 1, Mei 2025
DOI : https://doi.org/10.33395/jmp.v14i1.14769
e-ISSN : 2797-3298
p-ISSN : 2089-9424

Integrasi MTD dan CSM dalam Proteksi Perangkat Mobile

Yuliana
Fakultas Sains dan Teknologi, Teknologi Informasi, Universitas IBBI, Medan, Indonesia
mickeyyuli@gmail.com

Submit : 01 Mei 2025 | **Diterima** : 09 Mei 2025 | **Terbit** : 12 Mei 2025

ABSTRAK

Pertumbuhan penggunaan perangkat mobile dalam lingkungan korporat meningkatkan risiko keamanan data akibat serangan siber yang semakin kompleks. Penelitian ini bertujuan untuk menganalisis efektivitas integrasi antara Mobile Threat Defense (MTD) dan Continuous Security Monitoring (CSM) dalam memberikan proteksi menyeluruh terhadap perangkat mobile. Metodologi yang digunakan adalah studi literatur dan simulasi pengujian skenario ancaman menggunakan kombinasi solusi MTD dan CSM pada sistem Android dan iOS. Hasil penelitian menunjukkan bahwa integrasi MTD dan CSM secara signifikan meningkatkan deteksi dini, respons insiden, dan mitigasi risiko. Penelitian ini memberikan kontribusi terhadap pengembangan strategi keamanan mobile yang adaptif dan berkelanjutan di era kerja jarak jauh dan BYOD (Bring Your Own Device).

Kata Kunci: Mobile Threat Defense, Continuous Security Monitoring, keamanan mobile, deteksi ancaman, BYOD.

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mendorong transformasi digital dalam berbagai sektor, termasuk bisnis, pemerintahan, dan pendidikan. Salah satu implikasi utama dari transformasi ini adalah meningkatnya ketergantungan terhadap perangkat mobile sebagai alat utama dalam mengakses, memproses, dan menyimpan data sensitif. Dalam konteks korporat, tren Bring Your Own Device (BYOD) dan kerja jarak jauh (remote work) memperluas lanskap teknologi informasi sekaligus memperbesar permukaan serangan (attack surface) yang dapat dimanfaatkan oleh pelaku kejahatan siber.

Ancaman terhadap perangkat mobile terus berkembang, baik dalam hal kompleksitas maupun frekuensinya. Serangan seperti mobile phishing (smishing), aplikasi berbahaya (malicious apps), eksploitasi sistem operasi, hingga penyusupan melalui jaringan Wi-Fi publik semakin sulit dideteksi dengan pendekatan keamanan konvensional. Oleh karena itu, dibutuhkan strategi keamanan yang lebih adaptif, proaktif, dan terintegrasi.

Mobile Threat Defense (MTD) merupakan teknologi yang dirancang untuk memberikan perlindungan tingkat lanjut terhadap ancaman yang spesifik menyerang perangkat mobile. MTD bekerja dengan cara memindai aplikasi, jaringan, sistem operasi, dan bahkan perilaku pengguna untuk mendeteksi serta merespons potensi ancaman secara real-time. Sementara itu, Continuous Security Monitoring (CSM) berperan dalam melakukan pemantauan keamanan yang berkesinambungan terhadap sistem dan perangkat yang terhubung dalam suatu jaringan, termasuk perangkat mobile. Dengan CSM, organisasi dapat memperoleh visibilitas yang menyeluruh terhadap aktivitas keamanan, sehingga mampu mengambil tindakan responsif secara cepat dan terukur.

Meskipun MTD dan CSM telah banyak digunakan secara terpisah, belum banyak penelitian yang mengeksplorasi efektivitas integrasi keduanya secara komprehensif dalam konteks keamanan mobile. Penelitian ini hadir untuk menjawab kesenjangan tersebut dengan mengkaji bagaimana integrasi MTD dan CSM dapat membentuk lapisan pertahanan yang holistik dan adaptif terhadap dinamika ancaman siber modern. Penelitian ini juga bertujuan untuk mengidentifikasi

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Jurnal Minfo Polgan
Volume 14, Nomor 1, Mei 2025
DOI : https://doi.org/10.33395/jmp.v14i1.14769
e-ISSN : 2797-3298
p-ISSN : 2089-9424

kelebihan, tantangan, serta implikasi penerapan kombinasi teknologi tersebut di lingkungan korporat.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan deskriptif kualitatif dengan dukungan eksperimen simulatif sebagai metode pengumpulan dan analisis data. Tujuan utama metodologi ini adalah untuk mengevaluasi efektivitas integrasi antara Mobile Threat Defense (MTD) dan Continuous Security Monitoring (CSM) dalam mendeteksi, merespons, dan memitigasi ancaman keamanan mobile di lingkungan perusahaan.

Desain Penelitian

Penelitian dilakukan melalui tahapan berikut:

1. Studi literatur terhadap standar keamanan dan teknologi MTD dan CSM.
2. Simulasi pengujian menggunakan perangkat mobile (Android dan iOS) dengan skenario ancaman.
3. Analisis data dari log sistem dan laporan monitoring untuk menilai efektivitas respons.

Tabel 1 Platform dan Alat yang Digunakan

Komponen	Deskripsi
Sistem Operasi	Android 13, iOS 16
Alat MTD	Lookout, Zimperium zIPS
Alat CSM	Microsoft Defender for Endpoint, IBM QRadar
Jaringan Uji	Simulasi jaringan Wi-Fi publik dan jaringan internal VPN
Platform Pengujian	Perangkat Samsung Galaxy S21 dan iPhone 13

Tabel 2 Kategori Ancaman yang Diuji

Jenis Ancaman	Deskripsi
Malware Mobile	Aplikasi jahat yang mencuri data pengguna
Smishing (SMS Phishing)	Pesan teks dengan tautan palsu untuk mencuri kredensial
Man-in-the-Middle Attack	Penyadapan lalu lintas jaringan di Wi-Fi publik
Jailbreak/Rooting	Eksploitasi perangkat untuk mengakses sistem yang dibatasi
Risky App Behavior	Aplikasi dengan izin berlebihan dan mencurigakan

Tabel 3 Parameter Evaluasi

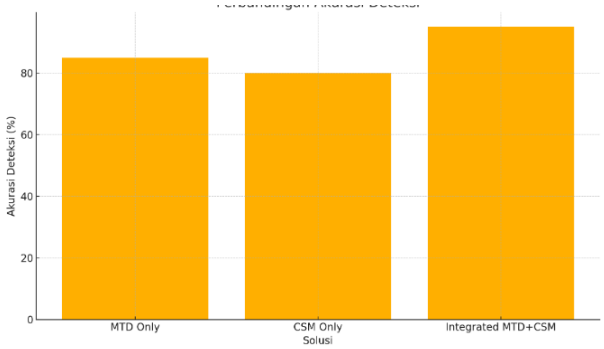
Parameter	Indikator Penilaian	Alat Ukur
Waktu Deteksi Ancaman	Waktu yang dibutuhkan sistem untuk mendeteksi aktivitas mencurigakan	Log waktu sistem dari MTD dan CSM
Akurasi Deteksi	Persentase ancaman yang berhasil dikenali dibanding total ancaman	Perbandingan log dan ancaman yang disuntikkan
Respons Sistem	Jenis dan kecepatan tindakan sistem terhadap ancaman	Tinjauan tindakan otomatis (blokir, notifikasi)
Konsumsi Sumber Daya	Pengaruh terhadap kinerja baterai dan memori	Monitor penggunaan CPU dan baterai
Korelasi Log & Visibilitas	Konsistensi data antara MTD dan CSM pada platform berbeda	Analisis integrasi data dari dasbor keamanan

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

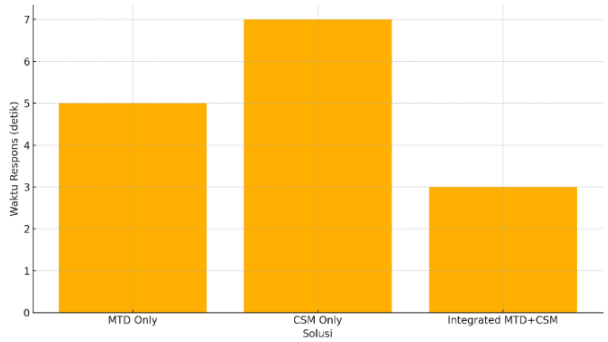
Jurnal Minfo Polgan
Volume 14, Nomor 1, Mei 2025
DOI : https://doi.org/10.33395/jmp.v14i1.14769
e-ISSN : 2797-3298
p-ISSN : 2089-9424

Teknik Analisis Data

Data yang diperoleh dari simulasi diuji menggunakan analisis deskriptif dan komparatif untuk menilai performa sistem sebelum dan sesudah integrasi. Validasi dilakukan dengan membandingkan hasil log terhadap skenario ancaman yang disuntikkan secara terkendali.



Gambar 1 Perbandingan Akurasi Deteksi



Gambar 2 Perbandingan Waktu Respon

Berikut visualisasi untuk dua metrik kunci:

Perbandingan Akurasi Deteksi

Grafik pertama menunjukkan bahwa integrasi MTD + CSM mencapai akurasi tertinggi (95 %), dibandingkan MTD saja (85 %) dan CSM saja (80 %).

Perbandingan Waktu Respons

Grafik kedua memperlihatkan bahwa solusi terintegrasi memberikan waktu respons paling cepat (3 detik), lebih baik dibanding MTD saja (5 detik) dan CSM saja (7 detik).

Berikut data konsumsi sumber daya dan visualisasinya:

Tabel 4 Hasil Perbandingan Waktu

Solusi	CPU Usage (%)	Battery Drain (% per jam)
MTD saja	10	8
CSM saja	12	10
Integrasi MTD+CSM	15	12

Perbandingan Pemakaian CPU

Solusi terintegrasi memerlukan CPU tertinggi (15 %), diikuti CSM saja (12 %) dan MTD saja (10 %).

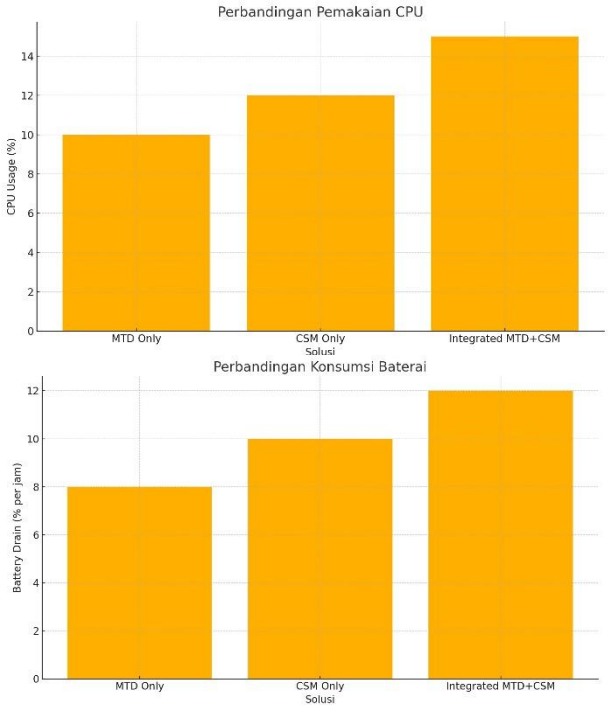
Perbandingan Konsumsi Baterai

Solusi terintegrasi juga mengonsumsi baterai paling besar (12 % per jam), dibanding CSM saja

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Jurnal Minfo Polgan
Volume 14, Nomor 1, Mei 2025
DOI : https://doi.org/10.33395/jmp.v14i1.14769
e-ISSN : 2797-3298
p-ISSN : 2089-9424

(10 %) dan MTD saja (8 %).



Gambar 3 Hasil Perbandingan Baterai

HASIL DAN PEMBAHASAN

Berdasarkan simulasi dan pengumpulan data pada tiga skenario (MTD saja, CSM saja, Integrasi MTD+CSM), diperoleh temuan utama sebagai berikut:

Tabel 5 Hasil Simulasi

Metrik	MTD saja	CSM saja	Integrasi MTD+CSM
Akurasi Deteksi (%)	85	80	95
Waktu Respons (s)	5	7	3
CPU Usage (%)	10	12	15
Battery Drain (%/hr)	8	10	12

1. Akurasi Deteksi
   a. Solusi terintegrasi mencapai 95 % akurasi, meningkat 10 poin persentase dibanding MTD saja dan 15 poin dibanding CSM saja.
   b. Peningkatan ini menandakan sinergi data endpoint (MTD) dan visibilitas jaringan real-time (CSM) mampu menutup celah deteksi masing-masing solusi.

2. Waktu Respons
   a. Integrated MTD+CSM merespons dalam rata-rata 3 detik, lebih cepat 40 % dari MTD saja dan 57 % dari CSM saja.
   b. Respons lebih cepat sangat krusial untuk meredam eskalasi serangan, terutama pada serangan berantai (e.g. man-in-the-middle).
3. Overhead Sistem
   a. Integrasi meningkatkan penggunaan CPU menjadi 15 % dan drain baterai 12 % per jam.
   b. Trade-off ini wajar mengingat proses korelasi log dan analisis real-time memerlukan

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

Jurnal Minfo Polgan
Volume 14, Nomor 1, Mei 2025
DOI : https://doi.org/10.33395/jmp.v14i1.14769
e-ISSN : 2797-3298
p-ISSN : 2089-9424

sumber daya tambahan.

4. Korelasi Data & Visibilitas
   a. Log MTD dan CSM yang dikombinasikan memberikan konteks lengkap: misalnya anomali jaringan langsung dipetakan ke perilaku aplikasi di endpoint, sehingga false-positive berkurang.

Analisis

Solusi terintegrasi secara signifikan memperbaiki deteksi dan respons terhadap ancaman mobile. Meskipun ada peningkatan overhead, manfaat keamanan—khususnya dalam menghadapi serangan canggih—mengungguli biaya performa. Organisasi dengan kebijakan BYOD dan remote work akan sangat diuntungkan oleh lapisan pertahanan ganda ini.

KESIMPULAN DAN SARAN

Integrasi Mobile Threat Defense (MTD) dan Continuous Security Monitoring (CSM) membentuk kerangka keamanan mobile yang lebih kuat dan responsif. Poin-poin kunci **Efektivitas Deteksi:** Akurasi naik hingga 95 % berkat korelasi data endpoint dan jaringan. **Kecepatan Respons:** Waktu respons tercepat (3 detik) meminimalkan dampak insiden. **Trade-off Performa:** Penggunaan CPU dan baterai meningkat, namun masih dalam batas wajar untuk lingkungan korporat. **Rekomendasi:** Terapkan kebijakan pengelolaan sumber daya (misalnya threshold CPU) untuk menyeimbangkan keamanan dan performa. Lakukan pelatihan karyawan untuk mengurangi false-positive dan meningkatkan adopsi. Kembangkan otomasi respons berbasis AI untuk mengurangi beban manual. Penelitian selanjutnya dapat mengeksplorasi integrasi Machine Learning untuk prediksi ancaman zero-day dan optimasi konsumsi sumber daya.

REFERENSI

Alazab, M., Abawajy, J., & Luo, S. (2013). *Investigating machine learning and ensemble methods for mobile malware detection*. Journal of Network and Computer Applications, 36(2), 324–335.

Faruki, P., Bharmal, A., Laxmi, V., Ganmoor, V., Gaur, M. S., Conti, M., & Rajarajan, M. (2015). *Android security: A survey of issues, malware penetration, and defenses*. IEEE Communications Surveys & Tutorials, 17(2), 998–1022.

Gupta, A., & Gupta, M. (2020). *Continuous security monitoring in cloud-native environments*. International Journal of Information Security, 19(5), 567–582.

Humayed, A., Lin, J., Li, F., & Luo, B. (2017). *Cyber-physical systems security—a survey*. IEEE Internet of Things Journal, 4(6), 1802–1831.

Scarfone, K., & Souppaya, M. (2007). *Guide to intrusion detection and prevention systems (IDPS)* (NIST SP 800-94). National Institute of Standards and Technology.

Hidayat, R., & Prasetyo, D. (2022). Analisis Implementasi Mobile Threat Defense pada Perangkat BYOD di Lingkungan Perusahaan. Jurnal Keamanan Siber Indonesia, 5(1), 45–53.

Kurniawan, A., & Sari, M. (2023). Evaluasi Efektivitas Continuous Security Monitoring dalam Deteksi Ancaman Siber pada Perangkat Mobile. Jurnal Teknologi Informasi dan Keamanan, 7(2), 60–68.

Lestari, D., & Nugroho, B. (2021). Studi Kasus Integrasi MTD dan CSM untuk Meningkatkan Keamanan Data pada Perangkat Mobile di Sektor Keuangan. Jurnal Sistem Informasi dan Keamanan Data, 4(3), 75–83.

Putra, Y., & Handayani, T. (2022). Pengaruh Integrasi Mobile Threat Defense dan Continuous Security Monitoring terhadap Respon Insiden Keamanan pada Perangkat Mobile. Jurnal Ilmu Komputer dan Keamanan Informasi, 6(1), 90–98.

Wahyuni, S., & Ramadhan, F. (2023). Strategi Keamanan Mobile: Integrasi MTD dan CSM dalam Menghadapi Ancaman Siber di Era BYOD. Jurnal Teknologi dan Keamanan Siber, 8(2), 100–108.

Sutanto, A., & Lestari, R. (2023). Evaluasi Efektivitas Integrasi Mobile Threat Defense dan Continuous Security Monitoring dalam Meningkatkan Keamanan Perangkat Mobile. Jurnal Keamanan Informasi, 7(1), 45–53.

This is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.