# KEAMANAN INFORMASI

## KEAMANAN SISTEM OPERASI & ENDPOINT


**Disusun oleh:**

Akxel Brian Nirwana

2344390009



**Program Studi Sistem Informasi**

**Fakultas Teknik**

**UNIVERSITAS PERSADA INDONESIA**

**2025**

# KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa, sebab atas rahmat dan karunia-Nya penulis dapat menyelesaikan penulisan makalah individu dengan judul **"Keamanan Sistem Operasi & Endpoint: Hardening, Patch Management, Antivirus/EDR"** ini dengan baik dan tepat waktu.

Makalah ini disusun sebagai bentuk dari pemenuhan tugas mata kuliah Keamanan Informasi dan secara spesifik membahas mengenai strategi pertahanan berlapis untuk mengamankan fondasi infrastruktur digital, yaitu sistem operasi dan perangkat *endpoint*, dari berbagai ancaman siber yang terus berevolusi. Pembahasan difokuskan pada tiga pilar utama keamanan *endpoint* modern: Hardening Sistem Operasi untuk meminimalkan celah kerentanan sejak awal, Patch Management yang sistematis untuk penutupan lubang keamanan secara proaktif, dan implementasi solusi canggih Endpoint Detection and Response (EDR) sebagai mekanisme deteksi dan respons *real time*.

Penulis juga mengucapkan terima kasih yang sebesar-besarnya kepada dosen pengampu mata kuliah Keamanan Informasi, Bapak Jhonny Z.A, Ir., M.M., atas bimbingan dan arahan yang telah diberikan selama proses penyusunan makalah ini. Bimbingan beliau sangat membantu penulis dalam menyajikan pemahaman yang komprehensif mengenai pentingnya pendekatan proaktif, preventif, dan responsif dalam mengamankan *endpoint*, serta bagaimana integrasi ketiga teknik ini menjadi kunci utama dalam menjaga Triad CIA (Kerahasiaan, Integritas, dan Ketersediaan) aset digital di lingkungan korporat.

Penulis menyadari penyusunan makalah ini jauh dari sempurna dan berharap dapat menerima kritik serta saran yang membangun demi perbaikan di masa mendatang.

Akhir kata, penulis berharap semoga tulisan ini dapat memberikan pemahaman serta wawasan yang lebih baik mengenai prosedur keamanan sistem operasi, pentingnya pemeliharaan rutin, serta urgensi adopsi teknologi pertahanan canggih dalam menghadapi tantangan keamanan siber di dunia digital yang terus berkembang. Semoga makalah ini bermanfaat bagi para pembaca dan memberikan kontribusi kecil terhadap upaya membangun pertahanan *endpoint* yang tangguh.

# DAFTAR ISI

# BAB I

# PENDAHULUAN

## 1.1 Latar Belakang Masalah

Di era digital yang didominasi oleh mobilitas dan komputasi awan, sistem operasi (OS) dan perangkat endpoint seperti laptop, desktop, dan server telah menjadi inti dari operasional bisnis dan titik akses utama ke data sensitif. Seiring dengan peningkatan kompleksitas infrastruktur TI, endpoint juga menjadi target utama serangan siber. Berbagai laporan keamanan menunjukkan bahwa mayoritas pelanggaran data (*data breaches*) dimulai dari eksploitasi kerentanan pada perangkat endpoint yang tidak terkelola dengan baik.

Ancaman siber modern tidak lagi terbatas pada malware berbasis tanda tangan (*signature based*) yang dapat diatasi oleh Antivirus tradisional, melainkan telah berevolusi menjadi serangan canggih dan tidak terdeteksi (*Zero Day, Fileless Malware*). Tantangan ini diperburuk oleh dua faktor utama: kerentanan bawaan sistem yang sering kali muncul dari konfigurasi default yang longgar, dan kerentanan yang tercipta seiring waktu akibat kurangnya pembaruan keamanan.

Untuk mengatasi tantangan ini, diperlukan strategi keamanan yang komprehensif dan berlapis pada tingkat fundamental OS dan endpoint. Strategi tersebut mencakup tiga pilar kritis: *Hardening* Sistem Operasi untuk meminimalkan permukaan serangan sejak awal; *Patch Management* yang sistematis untuk secara proaktif menutup celah keamanan yang ditemukan; dan adopsi solusi *Endpoint Detection* and *Response* (EDR) yang mampu mendeteksi dan merespons ancaman real-time yang telah melewati pertahanan pencegahan. Kesenjangan antara ancaman yang semakin canggih dan metode perlindungan tradisional inilah yang melatarbelakangi pentingnya analisis mendalam terhadap ketiga pilar keamanan endpoint ini dalam rangka melindungi integritas dan ketersediaan aset informasi.

## 1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan, rumusan masalah dalam penulisan makalah ini adalah sebagai berikut:

1. Bagaimana Hardening Sistem Operasi dapat meminimalkan permukaan serangan *endpoint* dan apa saja langkah-langkah kritis yang harus diterapkan untuk mencapai konfigurasi keamanan optimal?
2. Mengapa Patch Management menjadi komponen esensial dalam mengurangi risiko kerentanan yang dieksploitasi, dan bagaimana siklus manajemen penambalan yang efektif dapat diimplementasikan pada lingkungan *endpoint*?
3. Apa perbedaan mendasar antara solusi Antivirus (AV) tradisional dengan Endpoint Detection and Response (EDR), dan bagaimana adopsi EDR dapat meningkatkan kemampuan deteksi dan respons terhadap ancaman siber canggih pada *endpoint*?
4. Bagaimana integrasi antara *Hardening*, *Patch Management*, dan solusi keamanan (*Antivirus/EDR*) dapat membentuk strategi pertahanan *endpoint* yang berlapis dan efektif dalam menjaga CIA Triad?

### 1.3 Tujuan Penulisan

Tujuan penulisan makalah ini adalah untuk:

1. Menganalisis konsep dan metodologi Hardening Sistem Operasi serta mengidentifikasi praktik terbaik yang direkomendasikan untuk pengerasan sistem.
2. Mengeksplorasi pentingnya dan siklus implementasi Patch Management yang efisien sebagai alat pencegahan utama terhadap eksploitasi kerentanan perangkat lunak.
3. Membandingkan fitur dan kapabilitas antara Antivirus tradisional dan Endpoint Detection and Response (EDR), serta menjelaskan peran EDR sebagai solusi keamanan responsif modern.
4. Merumuskan model strategis yang mengintegrasikan *Hardening*, *Patch Management*, dan *Antivirus/EDR* untuk mencapai keamanan sistem operasi dan *endpoint* yang komprehensif.

# BAB II

# PEMBAHASAN

## 2.1 Konsep Dasar Keamanan Informasi

Keamanan informasi merupakan disiplin ilmu dan praktik yang bertujuan melindungi informasi dari berbagai ancaman untuk memastikan kelangsungan bisnis serta meminimalkan risiko bisnis (Aplikas Servis Pesona, 2024). Landasan fundamental dari semua kebijakan dan teknologi keamanan informasi dikenal sebagai CIA Triad (Course-Net, 2024), yang terdiri dari tiga pilar utama:

### 2.1.1 Kerahasiaan (*Confidentiality*)

Kerahasiaan adalah prinsip yang memastikan bahwa informasi hanya dapat diakses oleh individu, entitas, atau proses yang telah diberi otorisasi (Batang Kab. CSIRT, 2023). Pelanggaran terhadap pilar ini dapat berupa kebocoran data sensitif, seperti data pelanggan, rahasia dagang, atau informasi keuangan perusahaan.

Mekanisme untuk menegakkan kerahasiaan meliputi:

- Enkripsi: Mengubah data menjadi kode yang tidak dapat dibaca tanpa kunci.
- Kontrol Akses: Menggunakan otentikasi ketat (seperti otentikasi multi-faktor) untuk membatasi siapa yang dapat melihat data.
- Akses Berbasis Kebutuhan (Need to Know Basis): Menerapkan prinsip *Least Privilege* (hak akses paling minimum).

### 2.1.2 Integritas (Integrity)

Integritas menjamin bahwa informasi akurat, lengkap, dan belum dimodifikasi oleh pihak yang tidak berwenang. Ini memastikan bahwa informasi yang diterima atau disimpan adalah representasi yang benar dari data aslinya. Pelanggaran integritas, seperti malware yang memodifikasi konfigurasi sistem atau data di database, dapat merusak kepercayaan dan operasional bisnis.

Mekanisme yang digunakan untuk menjaga integritas meliputi:

- Fungsi *Hashing* dan Tanda Tangan Digital: Untuk memverifikasi keaslian dan mendeteksi perubahan data.

- Kontrol Versi: Melacak perubahan pada data untuk memungkinkan pemulihan ke keadaan yang valid.
- Validasi *Input*: Memastikan data yang dimasukkan ke dalam sistem sesuai dengan aturan yang ditetapkan.

### 2.1.3 Ketersediaan (Availability)

Ketersediaan memastikan bahwa pengguna yang sah dapat mengakses sistem dan sumber daya informasi ketika dibutuhkan tanpa gangguan signifikan. Ketersediaan tidak hanya tentang sistem yang up and running, tetapi juga tentang kinerja yang optimal (Aplikas Servis Pesona, 2024). Serangan yang paling sering mengancam ketersediaan adalah Denial of Service (DoS) atau kegagalan perangkat keras.

Mekanisme untuk meningkatkan ketersediaan meliputi:

- Redundansi dan *Failover*: Menggunakan sistem atau komponen cadangan untuk mengambil alih fungsi jika sistem utama gagal.
- Pencadangan (*Backup*) dan Pemulihan Bencana (*Disaster Recovery*): Prosedur untuk memastikan data dapat dikembalikan setelah insiden besar.

## 2.2 Keamanan Sistem Operasi (OS)

Sistem Operasi (OS) adalah perangkat lunak dasar yang mengelola sumber daya perangkat keras dan menyediakan layanan umum untuk program aplikasi. Dalam arsitektur keamanan, OS bertindak sebagai lapisan pertahanan pertama dan terpenting, karena mengontrol semua akses ke memori, proses, file, dan jaringan. Keamanan Sistem Operasi adalah serangkaian prosedur kontrol preventif yang melindungi aset sistem apa pun dari pencurian, modifikasi, atau penghapusan akibat pelanggaran OS (Hafiz, 2022).

### 2.2.1 Peran Sentral OS dalam Keamanan

OS bertanggung jawab atas implementasi mekanisme keamanan mendasar, termasuk:

1. Otentikasi dan Otorisasi: Mengelola akun pengguna dan memastikan hanya pengguna dengan hak akses yang tepat yang dapat melakukan perubahan signifikan (ITBOX, 2024).

2. Manajemen Memori dan Proses: Mengisolasi proses aplikasi untuk mencegah satu program yang terinfeksi memengaruhi program lain atau kernel OS.
3. Pengendalian *Input/Output*: Mengontrol akses ke perangkat periferal dan komunikasi jaringan.

### 2.2.2 Ancaman Umum terhadap Sistem Operasi

Kerentanan dalam OS sering menjadi sasaran karena akses ke OS berarti akses ke seluruh sumber daya sistem dan data sensitif yang ada di dalamnya. Ancaman-ancaman umum meliputi:

- *Malware* (Virus, Trojan, Worm): Perangkat lunak berbahaya yang dirancang untuk merusak atau mencuri data (Hafiz, 2022).
- *Eksploitasi Kerentanan (Vulnerability Exploits)*: Serangan yang memanfaatkan celah keamanan yang belum ditambal pada kode OS.
- *Buffer Overflow*: Serangan di mana penyerang membanjiri buffer penyimpanan data sementara dengan data berlebihan, yang dapat menyebabkan eksekusi kode berbahaya.
- *Denial of Service (DDoS)*: Serangan yang bertujuan membuat sumber daya sistem tidak dapat diakses oleh pengguna yang sah.
- Pencurian Data Pribadi dan Identitas: Berakibat dari kerentanan OS yang memungkinkan penyerang mendapatkan data login atau informasi kartu kredit (DomaiNesia, 2025).

## 2.3 Keamanan Endpoint

Endpoint adalah perangkat komputasi apa pun yang terhubung ke jaringan dan bertindak sebagai titik akhir (terminal) komunikasi data (UTI-TTIS, 2024). Dalam lingkungan perusahaan modern, endpoint telah meluas dari sekadar desktop dan server menjadi laptop, smartphone (melalui kebijakan BYOD), dan perangkat IoT.

### 2.3.1 Definisi dan Pentingnya Keamanan Endpoint

Keamanan Endpoint (Endpoint Security) adalah strategi dan solusi teknologi yang bertujuan mengamankan perangkat endpoint ini dari ancaman digital dan akses tidak sah (Intel, 2023). Endpoint sering dianggap sebagai titik masuk jaringan perusahaan utama untuk serangan siber, karena diperkirakan sebanyak 70% pelanggaran data yang berhasil berasal dari perangkat endpoint (IBM, t.t.).

Pentingnya Keamanan Endpoint didorong oleh beberapa faktor:

- **Akses ke Data Sensitif**: *Endpoint* adalah jalur utama bagi karyawan untuk mengakses data dan aplikasi perusahaan (UTI-TTIS, 2024).
- **Pergeseran Model Kerja**: Peningkatan pekerjaan jarak jauh dan perangkat pribadi (*BYOD*) melipatgandakan jumlah *endpoint* yang harus dilindungi (IBM, t.t.).
- **Mitigasi Ancaman Lanjutan**: *Endpoint* menjadi target utama untuk serangan canggih seperti *Ransomware* dan *Cryptojacking*.

### 2.3.2 Kerentanan Endpoint

Kerentanan utama pada endpoint seringkali melibatkan faktor manusia dan konfigurasi yang longgar:

- Perangkat Lunak Usang: *Endpoint* yang tidak menerima *patch* rutin menjadi target empuk.
- Kesalahan Pengguna: Serangan *phishing* atau *social engineering* yang berhasil memanipulasi pengguna di *endpoint*.
- Konfigurasi Default: Menggunakan pengaturan standar pabrik yang rentan terhadap eksploitasi yang sudah diketahui.

## 2.4 Teknik Pengamanan Sistem Operasi dan Endpoint

Pengamanan sistem operasi dan endpoint membutuhkan pendekatan berlapis yang mencakup tindakan pencegahan proaktif, pemeliharaan rutin, dan kemampuan deteksi/respons canggih.

### 2.4.1 Hardening Sistem Operasi

Hardening (Pengerasan Sistem) adalah praktik keamanan untuk mengurangi permukaan serangan (attack surface) dengan mematikan layanan, fitur, atau fungsi yang tidak perlu dan mengkonfigurasi sistem dengan pengaturan yang paling aman. Ini merupakan tindakan proaktif yang dilakukan sebelum sistem digunakan dalam lingkungan produksi (i-3.co.id, t.t.; Robere & Associates, t.t.).

#### 2.4.1.1 Tujuan Hardening

Tujuan utama hardening adalah mengeliminasi attack vectors dan memperkecil attack surface (hanjuan.net, t.t.; Robere & Associates, t.t.). Dengan menghapus atau menonaktifkan komponen yang tidak kritis, kerentanan yang tidak diketahui atau yang ada pada komponen tersebut dapat dihilangkan.

#### 2.4.1.2 Standar dan Pedoman Hardening

Banyak organisasi menggunakan kerangka kerja internasional untuk memandu proses hardening, seperti:

- NIST SP 800-123: Publikasi dari *National Institute of Standards and Technology* (NIST) yang memberikan panduan terperinci untuk pengamanan *server* umum, termasuk *checklist* konfigurasi keamanan (Telkom University, 2024).
- ISO/IEC 27001:2013: Standar ini menekankan pentingnya pengamanan sistem dan aplikasi dari potensi serangan, termasuk melalui proses *security hardening* (Robere & Associates, t.t.).

#### 2.4.1.3 Area Fokus Hardening OS

Proses hardening sistem operasi mencakup beberapa area utama (Madhava, t.t.):

1. Pengerasan Jaringan (*Network Hardening*): Menghapus protokol lama (misalnya, telnet) dan menerapkan aturan *firewall* OS yang ketat, hanya mengizinkan *port* yang benar-benar esensial.
2. Manajemen Akun dan Hak Akses: Menghapus akun *default* (administrator/guest) dan menerapkan prinsip *Least Privilege*, di mana pengguna hanya diberikan izin minimum untuk menjalankan tugas mereka.
3. Pengerasan Layanan (*Service Hardening*): Menyetel atau menonaktifkan layanan sistem yang tidak digunakan, seperti layanan *file sharing* yang tidak relevan atau *daemon* lama.
4. Konfigurasi *Logging* dan Audit: Mengaktifkan *logging* peristiwa keamanan secara komprehensif untuk mempermudah deteksi anomali dan investigasi insiden di masa mendatang.
5. Pengerasan *Filesystem*: Menerapkan izin *file* dan direktori yang ketat untuk mencegah perubahan pada *file* sistem penting oleh pengguna biasa atau *malware*.

Proses hardening harus diulang secara berkala karena lingkungan sistem terus berubah, dan ancaman baru terus muncul (Widyasecurity, 2025).

### 2.4.2 Patch Management (Manajemen Penambalan)

Patch Management adalah proses sistematis dan berkelanjutan dalam mengidentifikasi, memperoleh, menguji, dan menerapkan pembaruan perangkat lunak (patch) atau hotfix pada sistem operasi dan aplikasi untuk memperbaiki kerentanan atau bug (Intel, 2023). Ini adalah tindakan preventif kritis, karena kerentanan yang tidak ditambal (unpatched

vulnerabilities) merupakan vektor serangan paling umum yang dieksploitasi oleh peretas (CyberHub Indonesia, 2024).

#### 2.4.2.1 Tujuan dan Manfaat Patching

Pentingnya patch management terletak pada kemampuannya untuk:

- **Meningkatkan Keamanan Sistem**: Menutup celah-celah keamanan yang rentan dimanfaatkan oleh peretas, mencegah *malware*, *ransomware*, dan ancaman siber lainnya (CyberHub Indonesia, 2024).
- **Kepatuhan dan Audit**: Memenuhi persyaratan regulasi dan standar keamanan (seperti PCI DSS atau ISO 27001) yang mengharuskan pembaruan sistem yang tepat waktu (Scalefusion Blog, 2025).
- **Stabilitas dan Kinerja**: Selain keamanan, *patch* sering kali memperbaiki *bug*, meningkatkan stabilitas, dan mengoptimalkan kinerja sistem (i-3.co.id, t.t.; CyberHub Indonesia, 2024).

#### 2.4.2.2 Siklus Manajemen Patch

Manajemen patch yang efektif mengikuti siklus terstruktur (Intel, 2023):

1. **Inventarisasi**: Memelihara daftar semua *endpoint* dan perangkat lunak yang ada untuk menentukan cakupan *patching*.
2. **Penilaian dan Prioritas**: Mengidentifikasi *patch* yang diperlukan dan memprioritaskan yang menambal kerentanan kritis atau yang sedang dieksploitasi (*Zero Day*).
3. **Pengujian (*Testing*)**: Menerapkan *patch* di lingkungan non produksi (*staging environment*) untuk memastikan tidak ada konflik atau gangguan yang terjadi.
4. **Penyebaran (*Deployment*)**: Menerapkan *patch* pada *endpoint* produksi, seringkali di luar jam kerja untuk meminimalkan dampak operasional.
5. **Verifikasi dan Dokumentasi**: Memastikan *patch* telah terpasang dengan benar dan mendokumentasikan proses untuk keperluan audit.

### 2.4.3 Antivirus dan Endpoint Detection and Response (EDR)

Antivirus (AV) dan Endpoint Detection and Response (EDR) adalah alat utama yang digunakan pada endpoint untuk mendeteksi dan merespons ancaman, meskipun keduanya beroperasi dengan filosofi yang berbeda

#### 2.4.3.1 Antivirus (AV) Tradisional

Antivirus Tradisional adalah garis pertahanan dasar yang berfokus pada pencegahan malware yang sudah dikenal.

- Metode Deteksi: AV bekerja secara reaktif dengan memindai *file* dan mencocokkannya dengan basis data tanda tangan (*signature based*) ancaman yang sudah diketahui (CyberHub Indonesia, 2024).
- Kemampuan: Hanya dapat menghapus atau mengkarantina *malware* yang terdeteksi, tetapi kurang efektif terhadap ancaman baru (*Zero Day*) atau *fileless malware* (SentinelOne, 2025).

#### 2.4.3.2 Endpoint Detection and Response (EDR)

EDR adalah solusi keamanan modern yang menawarkan kemampuan deteksi, analisis, dan respons yang jauh lebih canggih daripada AV tradisional. EDR merupakan evolusi dari Next-Generation Antivirus (NGAV) yang menggabungkan kemampuan pencegahan dengan pemantauan berkelanjutan (SentinelOne, 2025).

| Fitur | Antivirus (AV) Tradisional | Endpoint Detection and Response (EDR) |
|---|---|---|
| **Fokus Utama** | Pencegahan *malware* yang dikenal (*Signature based*). | Deteksi, investigasi, dan respons terhadap ancaman lanjutan. |
| **Sifat Operasi** | Reaktif (Bereaksi terhadap ancaman yang sudah ada). | Proaktif dan Detektif (Memantau perilaku *real time*). |
| **Visibilitas** | Terbatas pada pemindaian *file* dan aplikasi (Primacs, 2023). | Pemantauan seluruh aktivitas perangkat, proses, dan interaksi sistem secara *real time* (CyberHub Indonesia, 2024). |
| **Respon** | Karantina/Penghapusan *malware*. | Isolasi perangkat dari jaringan, menghentikan proses berbahaya, *threat hunting*, dan pemulihan sistem otomatis (Primacs, 2023). |
| **Ancaman** | Efektif melawan ancaman umum. | Efektif melawan ancaman *Zero Day*, *Ransomware*, dan *Fileless Malware*. |

#### 2.4.3.3 Sinergi AV dan EDR

Dalam praktik keamanan siber kontemporer, EDR tidak sepenuhnya menggantikan AV, melainkan melengkapi dan memperluas fungsinya. Banyak solusi EDR modern menyertakan fungsionalitas AV yang ditingkatkan (Next Generation AV) sebagai lapisan pencegahan awal, sementara kemampuan deteksi perilaku dan respons otomatis EDR

menangani ancaman kompleks yang berhasil lolos dari pertahanan awal (CyberHub Indonesia, 2024).

# BAB III

# PENUTUP

## 3.1 Kesimpulan

Keamanan sistem operasi dan endpoint merupakan lapisan pertahanan paling krusial dalam arsitektur keamanan informasi sebuah organisasi, yang secara langsung mendukung terpenuhinya prinsip CIA Triad Kerahasiaan, Integritas, dan Ketersediaan. Kegagalan untuk mengamankan endpoint dapat menciptakan titik masuk utama bagi serangan siber canggih, mengingat perangkat ini adalah pintu gerbang bagi karyawan menuju data dan jaringan perusahaan. Terdapat tiga pilar utama yang harus diimplementasikan secara terintegrasi untuk mencapai postur keamanan endpoint yang tangguh: Hardening Sistem Operasi, Patch Management, dan implementasi solusi Antivirus/EDR. Hardening berfungsi sebagai tindakan proaktif untuk mengurangi permukaan serangan secara mendasar, dengan menghilangkan konfigurasi dan layanan yang tidak perlu. Sementara itu, *Patch Management* adalah proses preventif dan berkelanjutan yang menutup celah kerentanan (yang menjadi vektor serangan paling umum) melalui pembaruan rutin. Terakhir, solusi Antivirus yang diperkuat dengan teknologi EDR bertindak sebagai lapisan deteksi dan respons lanjutan, mampu mengidentifikasi dan mengisolasi ancaman canggih (*Zero Day* atau *Fileless Malware*) yang berhasil melewati kontrol pencegahan awal, memastikan visibilitas dan waktu respons yang cepat terhadap insiden keamanan. Dengan demikian, keamanan endpoint bukanlah tugas yang ad-hoc, melainkan harus dipertahankan melalui siklus kebijakan, pemeliharaan rutin, dan teknologi respons modern.

## 3.2 Saran

Berdasarkan kesimpulan mengenai pentingnya pendekatan keamanan endpoint yang berlapis, diajukan beberapa saran praktis untuk implementasi dan penelitian di masa depan. Pertama, organisasi sangat disarankan untuk menggeser fokus dari Antivirus tradisional ke solusi EDR atau NGAV yang memiliki kemampuan analisis perilaku real time dan fitur threat hunting. Langkah ini penting untuk mengatasi ancaman modern yang semakin canggih dan mampu menghindari deteksi berbasis tanda tangan. Kedua, manajemen patch harus diubah dari tugas teknis menjadi proses

manajemen risiko yang diprioritaskan, di mana patch untuk kerentanan kritis atau yang sedang dieksploitasi harus diterapkan dengan segera setelah pengujian yang memadai. Organisasi perlu berinvestasi dalam alat otomatisasi *patch management* untuk memastikan cakupan endpoint yang konsisten. Ketiga, pelatihan kesadaran keamanan (*security awareness training*) harus secara rutin diberikan kepada pengguna endpoint, karena faktor manusia tetap menjadi mata rantai terlemah. Penelitian selanjutnya disarankan untuk menganalisis efektivitas biaya antara Hardening manual berbasis checklist (seperti NIST) dibandingkan dengan penggunaan otomatisasi konfigurasi (Configuration Management Tools) dalam lingkungan cloud atau hybrid, untuk mengukur seberapa jauh otomatisasi dapat meningkatkan konsistensi dan kecepatan hardening tanpa mengorbankan fungsionalitas sistem.

## DAFTAR PUSTAKA


Admin. (2024, January 03). *EDR vs Antivirus: Mana yang Paling Efisien Untuk Melindungi Endpoint?* Diambil kembali dari Prima Cyber Solusi: https://www.primacs.co.id/post/edr-vs-antivirus-mana-yang-paling-efisien-untuk-melindungi-endpoint

Admin. (2025, July 01). *What Is Patch Management?* Retrieved from Intel: https://www.intel.com/content/www/us/en/learn/what-is-patch-management.html

admin, i. (2022, Oktober 05). *Apa Itu Patch Management dan Mengapa Harus Dilakukan Secara Berkala?* Diambil kembali dari Inovasi Informatika Indonesia: https://i-3.co.id/apa-itu-patch-management-dan-mengapa-harus-dilakukan-secara-berkala/

Dani. (2025, July 16). *Hardening dalam Cybersecurity: Studi Kasus yang Efektif*. Diambil kembali dari Widya Security: https://widyasecurity.com/2025/07/17/hardening-dalam-cybersecurity-studi-kasus-yang-efektif/

Redaksi. (2024, Oktober 04). *System Hardening*. Diambil kembali dari Hanjuan's Services: https://hanjuan.net/system-hardening/

Redaksi. (2025, 05 21). *System Hardening*. Diambil kembali dari Madhava: https://madhava.id/system-hardening/