Journal of Applied Informatics and Computing (JAIC)
Vol.x, No.x, Juli 201x, pp. xx~xx
e-ISSN: 2548-6861

Evaluasi Kebijakan Keamanan Active Directory berdasarkan CIS Controls pada PT. XYZ Indonesia

Rachmat Maulana[1], Andy Triwinarko[2]
* Teknik Informatika, Politeknik Negeri Batam
** Rekayasa Keamanan Siber, Politeknik Negeri Batam
rachmat.maulana4@students.polibatam.ac.id [1], andy@polibatam.ac.id[2]

Article Info

Article history:

Received …
Revised …
Accepted …

Keyword:

Active Directory, CIS Benchmarks, CIS Controls, Group Policy Object.

ABSTRACT

Active Directory (AD) plays an important role in identity management and authentication in Windows-based enterprise environments, where security policies applied through Group Policy Objects (GPOs) directly affect system security and operational resilience. This study evaluates Active Directory security policy compliance with CIS Microsoft Windows Server 2022 Benchmark v4.0.0 and maps its implementation to CIS Controls v8. This evaluation focuses on seven GPOs, namely Default Domain Policy, Sysmon Enrollment, PowerShell 7 Enrollment, Python Enrollment, C++ Enrollment, Wazuh Enrollment, and Wazuh Activation, using direct configuration observation, document analysis, and descriptive evaluation. The results show varying levels of compliance with CIS recommendations, highlighting gaps between operational requirements and secure configuration principles, particularly in access control and script execution policies. These findings indicate that the CIS Benchmark provides a structured and effective framework for evaluating GPO-based security configurations, while the resulting recommendations are expected to support improvements to Active Directory security policies aligned with CIS Controls v8 and enhance the overall security posture of the environment.

I. PENDAHULUAN

A. Pendahuluan Penelitian

Keamanan data dan manajemen sumber daya informasi merupakan faktor krusial yang memengaruhi kinerja operasional suatu bisnis di era digital saat ini. Sebagai komponen penting dalam arsitektur IT modern, *Active Directory Domain Services* (AD DS) membantu bisnis mengorganisir dan melindungi data serta sumber daya mereka secara efektif. Sistem manajemen terpadu dan efektif untuk mengawasi pengguna dan kebijakan kini menjadi hal yang esensial akibat pengaruh teknologi yang semakin besar di tempat kerja. Active Directory muncul sebagai solusi yang komprehensif untuk mengelola hak akses pengguna dan kebijakan keamanan secara terpusat. Dengan AD, *administrator* dapat mengatur dan mengelola akses pengguna ke sumber daya jaringan, yang sangat penting untuk menjaga integritas dan kerahasiaan data [1].

Active Directory tidak hanya berfungsi sebagai layanan direktori, tetapi juga sebagai mekanisme pengendali autentikasi, otorisasi, dan konfigurasi sistem melalui *Group Policy Object* (GPO). Melalui GPO, *administrator* dapat menerapkan kebijakan keamanan dan konfigurasi teknis secara terpusat ke seluruh endpoint dalam domain. Oleh karena itu, konfigurasi Active Directory memiliki pengaruh langsung terhadap postur keamanan sistem secara keseluruhan [2]. Standar keamanan industri seperti CIS Controls dan CIS Benchmark menekankan pentingnya penerapan prinsip keamanan siber pada layanan direktori untuk mengurangi risiko eskalasi hak akses dan penyalahgunaan kredensial [3].

PT. XYZ Indonesia sedang mendirikan *Security Operations Center* (SOC) sebagai tim operasional dan fungsi

e-ISSN: 2548-6861

keamanan yang bertugas memantau, mengevaluasi, dan merespons insiden siber. Tim SOC telah mengembangkan sistem *Security Information and Event Management* (SIEM) sebagai metode utama untuk mengumpulkan, mengkorelasikan, dan menganalisis log keamanan dari berbagai perangkat di lingkungan kerja guna mendukung aktivitas tersebut.

Active Directory digunakan sebagai mekanisme manajemen terpusat untuk endpoint berbasis Windows dalam implementasi SIEM, terutama dalam hal deployment agen SIEM, otomatisasi respons aktif, dan instalasi perangkat lunak tambahan melalui *Group Policy Object* (GPO). Menurut metode ini, Active Directory merupakan elemen teknis yang krusial dan diperlukan agar implementasi dan operasional SIEM tim SOC dapat berjalan dengan sukses.

Namun, berdasarkan pengamatan awal terhadap lingkungan uji (*staging*), penggunaan Active Directory di perusahaan lebih difokuskan pada memenuhi kebutuhan operasional distribusi agen dan perangkat lunak dukungan SIEM. Evaluasi konfigurasi keamanan Active Directory itu sendiri, khususnya kebijakan GPO yang diterapkan, belum dilakukan secara sistematis menggunakan standar keamanan yang diakui. Beberapa kebijakan masih menggunakan konfigurasi *default*, dan ada kebijakan yang memerlukan hak administratif dalam proses instalasi perangkat lunak. Kondisi ini menunjukkan bahwa ada konfigurasi yang memiliki karakteristik serupa dengan praktik yang berpotensi tidak sesuai dengan prinsip *least privilege* dan *secure configuration*.

Laporan resmi dari *National Security Agency* (NSA) dan *Cybersecurity and Infrastructure Security Agency* (CISA) tahun 2023 menyatakan bahwa penggunaan konfigurasi bawaan serta pengelolaan hak istimewa yang tidak dibatasi merupakan dua dari sepuluh praktik *misconfiguration* yang paling umum ditemukan [4]. Kesamaan karakteristik tersebut menunjukkan pentingnya dilakukan evaluasi formal terhadap konfigurasi Active Directory, terutama ketika layanan direktori tersebut digunakan sebagai mekanisme pendukung utama dalam implementasi sistem keamanan seperti SIEM.

Berdasarkan kondisi tersebut, penelitian ini dilakukan untuk mengevaluasi konfigurasi kebijakan keamanan Active Directory yang diterapkan melalui *Group Policy Object* (GPO) pada PT. XYZ Indonesia. Evaluasi dilakukan tersebut untuk menilai tingkat kesesuaian terhadap CIS Benchmark sebagai acuan teknis serta menganalisis tingkat kepatuhannya terhadap CIS Controls v8 sebagai kerangka kerja pengendalian keamanan siber. Selain itu, penelitian ini bertujuan mengidentifikasi kesenjangan konfigurasi kebijakan keamanan yang ada dan menganalisis dampak rekomendasi perbaikan yang dirumuskan terhadap tingkat kepatuhan CIS Controls v8 berdasarkan analisis kesenjangan.

Penelitian ini dibatasi pada evaluasi konfigurasi Active Directory melalui GPO pada lingkungan uji (*staging*) dan tidak mencakup evaluasi arsitektur SIEM, pengujian penetrasi, maupun simulasi serangan. Rekomendasi perbaikan yang dihasilkan disusun secara konseptual berdasarkan standar CIS tanpa melakukan implementasi langsung pada sistem produksi. Dengan pendekatan evaluatif berbasis standar, penelitian ini diharapkan dapat memberikan gambaran objektif mengenai kondisi konfigurasi keamanan Active Directory pada tahap awal implementasi SIEM, sekaligus menjadi referensi dalam upaya penguatan konfigurasi keamanan yang selaras dengan praktik terbaik industri.

B. Landasan Teori

1. *Windows*

Windows adalah sistem operasi yang dikembangkan oleh Microsoft, yang dirancang untuk memberikan antarmuka pengguna grafis (GUI) yang intuitif dan kemudahan dalam pengelolaan sumber daya komputer.

Windows Server, sebagai varian khusus untuk lingkungan server, menyediakan berbagai layanan penting seperti Active Directory, yang memungkinkan pengelolaan identitas dan akses pengguna secara terpusat dalam jaringan. Fitur ini sangat penting untuk organisasi yang memerlukan kontrol yang ketat terhadap hak akses pengguna dan keamanan data [5].

Windows juga dikenal karena kemampuannya dalam mengelola hak akses pengguna melalui kebijakan keamanan yang dapat disesuaikan, yang membantu dalam mencegah akses tidak sah dan melindungi informasi sensitif [6].

2. *Active Directory (AD)*

Active Directory (AD) adalah layanan direktori yang dikembangkan oleh Microsoft untuk mengelola keamanan dan otorisasi dalam jaringan domain, memungkinkan administrator untuk mengelola hak akses pengguna dan sumber daya secara terpusat [7]. AD berfungsi sebagai basis data terdistribusi yang menyimpan informasi tentang objek-objek dalam jaringan, termasuk pengguna, grup, dan computer [8]. Active Directory memfasilitasi pengelolaan kebijakan grup yang dapat diterapkan secara lokal maupun melalui jaringan, sehingga memudahkan pengaturan hak akses dan keamanan data [9].

3. *Policy-Based Security Model*

Model keamanan berbasis kebijakan *(Policy-Based Security Model*) merujuk pada pendekatan keamanan yang bergantung pada kebijakan yang ditetapkan oleh organisasi untuk mengatur akses dan kontrol terhadap sumber daya dalam jaringan. Dalam konteks ini, kebijakan tersebut diimplementasikan melalui berbagai komponen seperti mesin kebijakan, *administrator* kebijakan, dan titik

penegakan kebijakan, yang semuanya berfungsi untuk memverifikasi dan menentukan konteks akses ke sumber daya [10]. Di lingkungan Windows, pendekatan ini diimplementasikan melalui *Group Policy Object* (GPO) yang dikelola menggunakan Active Directory.

4. *Group Policy Object (GPO)*

Group Policy Object (GPO) adalah sekumpulan pengaturan yang digunakan untuk mengelola dan mengonfigurasi sistem operasi, aplikasi, dan pengaturan keamanan di lingkungan jaringan berbasis Windows [11]. GPO memungkinkan administrator untuk menerapkan kebijakan secara terpusat kepada pengguna dan komputer dalam domain, sehingga memudahkan pengelolaan dan pengaturan keamanan di seluruh jaringan.

GPO berfungsi untuk mengatur berbagai aspek dari pengalaman pengguna dan keamanan sistem, termasuk pengaturan desktop, kebijakan kata sandi, dan pengaturan perangkat keras. Dengan GPO, *administrator* dapat memastikan bahwa semua pengguna dan komputer dalam domain mematuhi kebijakan yang telah ditetapkan, sehingga meningkatkan keamanan dan efisiensi operasional jaringan [1].

5. *Kerangka Kerja Keamanan Siber*

Untuk menghadapi meningkatnya ancaman serangan siber, organisasi perlu menerapkan kerangka kerja keamanan siber sebagai acuan dalam mengelola risiko dan menjaga integritas aset informasi. Beberapa kerangka kerja yang umum digunakan adalah ISO/IEC 27001, NIST *Cybersecurity Framework* (CSF), dan CIS Controls. Setiap kerangka memiliki fokus dan keunggulan masing-masing.

NIST CSF merupakan kerangka kerja berbasis risiko yang digunakan secara luas di berbagai sektor. Kerangka ini terdiri dari lima fungsi inti: *Identify*, *Protect*, *Detect*, *Respond*, dan *Recover*, yang diuraikan menjadi 23 kategori dan 108 subkategori. NIST CSF cocok untuk organisasi berskala besar karena fleksibel dan menyeluruh [12]. Namun, karena sifatnya yang luas dan konseptual, NIST CSF lebih bersifat strategis dan kurang rinci dalam hal implementasi teknis, sehingga membutuhkan pemetaan tambahan [13].

ISO/IEC 27001 merupakan standar internasional untuk membangun Sistem Manajemen Keamanan Informasi (SMKI). Sementara ISO/IEC 27001 berfungsi sebagai panduan implementasi kontrol dalam ISO 27001 [12]. Meski cocok untuk organisasi yang sudah matang dalam tata kelola, standar ini dianggap kurang efisien diterapkan di organisasi kecil/baru yang sedang berkembang, karena kompleksitas dokumen dan persyaratan sertifikasinya [13].

CIS Controls adalah kerangka kerja teknis yang dikembangkan oleh *Center for Internet Security* (CIS). Versi ke-8 berisi 18 kontrol utama dan 153 subkontrol yang berorientasi pada pencegahan serangan siber secara praktis dan dapat diukur. CIS Controls membagi kontrol ke dalam tiga *Implementation Group* (IG) sesuai dengan ukuran, risiko, dan sumber daya organisasi. IG1 untuk organisasi kecil, IG2 untuk organisasi menengah, IG3 untuk organisasi besar dan kompleks.[14].

6. *Center for Internet Security (CIS)*

Center for Internet Security (CIS) bertujuan untuk menjadikan dunia yang terhubung menjadi tempat yang lebih aman bagi individu, organisasi, dan pemerintah dengan memanfaatkan keahlian inti dalam kolaborasi dan inovasi. CIS adalah organisasi nirlaba yang didorong oleh komunitas, yang mengembangkan CIS Controls dan CIS Benchmarks, yang diakui secara global sebagai praktik terbaik untuk mengamankan sistem dan data IT. CIS memimpin komunitas global profesional IT dalam terus meningkatkan standar ini dan menyediakan alat serta layanan untuk melindungi secara proaktif terhadap ancaman yang muncul.

CIS Controls adalah seperangkat tindakan yang diprioritaskan dan dirancang untuk memberikan praktik terbaik dalam pertahanan siber, bertujuan untuk mengurangi risiko serangan siber yang paling umum dan berbahaya. Kerangka kerja ini membantu organisasi dalam mengidentifikasi dan mengatasi celah keamanan dengan cara yang terstruktur dan terukur, sehingga meningkatkan kemampuan mereka untuk melindungi aset informasi dan infrastruktur TI [14].

CIS Benchmark adalah panduan konfigurasi dasar dan praktik terbaik untuk pengaturan sistem yang aman, yang menekankan pentingnya mematuhi pedoman spesifik yang merujuk pada berbagai CIS Controls. Kontrol-kontrol ini dirancang untuk meningkatkan kemampuan keamanan siber suatu organisasi. Dikembangkan oleh *Center for Internet Security* (CIS), CIS Benchmark merupakan hasil dari proses konsensus kolaboratif yang melibatkan para profesional dan ahli keamanan siber dari seluruh dunia. Komunitas ini secara terus-menerus bekerja untuk mengidentifikasi, menyempurnakan, dan memvalidasi praktik terbaik dalam mengamankan sistem IT, perangkat lunak, dan jaringan [15].

Penelitian ini memilih CIS Controls v8 dan CIS Benchmarks Windows Server 2022 sebagai acuan evaluasi utama karena pedoman teknis operasionalnya yang dapat diterapkan langsung pada konfigurasi sistem. Berbeda dengan NIST *Cybersecurity Framework* (CSF), CIS Benchmarks menawarkan parameter konfigurasi yang spesifik, terukur, dan dapat diverifikasi. Hal ini membuatnya sangat berguna untuk evaluasi teknis dalam lingkungan Active Directory. Selain itu, CIS Controls dipilih karena aspek teknisnya, fleksibilitasnya, dan orientasinya pada pencegahan insiden. Mereka juga memperkenalkan pendekatan bertahap melalui *Implementation Groups* (IGs), memungkinkan organisasi untuk mengadopsi kontrol keamanan sesuai dengan kapasitas sumber daya mereka, sehingga meningkatkan keterapanannya dalam skenario praktis.

e-ISSN: 2548-6861

7. *Security Hardening*

Security hardening adalah proses yang bertujuan untuk meningkatkan keamanan sistem komputer atau jaringan dengan mengurangi kerentanan terhadap serangan dan ancaman [16]. Teknik *hardening* bertujuan untuk menambah tingkat keamanan pada server dengan mengurangi tingkat kerawanan di dalamnya terhadap serangan peretas [17]. Proses ini mencakup pengurangan permukaan serangan dengan cara menonaktifkan layanan yang tidak diperlukan, membatasi akses hanya untuk pengguna yang berwenang, serta menerapkan kebijakan keamanan yang lebih ketat [3].

C. Kajian Pustaka

Penelitian ini merujuk pada beberapa penelitian sebelumnya yang berkaitan sebagai referensi yang dapat membedakan penelitian ini dengan penelitian yang telah didapati sebelumnya dan juga digunakan sebagai referensi acuan dari penelitian ini. Berikut beberap peneltian yang berkaitan disajikan pada Tabel 1:

TABEL 1. TABEL RINGKASAN KAJIAN PUSTAKA

Nama Peneliti	Judul Penelitian	Metode Penelitian	Hasil Penelitian
Rajeshkumar Sasidharan	*A Case Study to Implement Windows System Hardening using CIS Controls*	Studi Kasus	Penerapan CIS Controls dan GPO pada lingkungan Windows meningkatkan skor keamanan sistem dari 28% menjadi lebih dari 98%. Implementasi terbukti efektif melalui pengujian bertahap di testbed.
Mohammad Afdhal Jauhari	Pengukuran Kematangan Keamanan Siber pada Perusahaan Teknologi Informasi dengan *Framework* CIS Controls	Kualitatif	Menggunakan CIS Controls IG1. Ditemukan tingkat kematangan sangat rendah (skor 0,41). Rekomendasi diberikan berupa peningkatan kebijakan keamanan, kontrol teknis, dan pelatihan karyawan.
Muhammad Najib, Bambang Purnomosidi, Muhammad A. Nugroho	Implementasi *Security Auditor* untuk Standardisasi Instalasi Server pada Layanan SaaS Menggunakan CIS Benchmark	Pengembangan Aplikasi	Sistem *auditor* berhasil melakukan audit server CentOS berbasis CIS Benchmark secara otomatis dan memberikan visualisasi nilai kepatuhan, membantu admin dalam evaluasi keamanan.
Nanang Sadikin & Marliana Sari	Implementasi *Password Policy* pada *Domain Security Policy* GPO Active Directory untuk Keamanan Jaringan	Studi Pustaka dan Observasi	Konfigurasi *password policy* melalui GPO meningkatkan keamanan jaringan, mengurangi risiko *password attack*, dan memudahkan administrasi keamanan.
Glen M. Taberima & Desi Ramayanti	Mengoptimalkan Manajemen dan Keamanan TI melalui Implementasi Layanan Domain Active Directory	Studi Kasus dengan pendekatan PPDIOO	Implementasi AD DS berhasil meningkatkan efisiensi manajemen TI, kontrol akses pengguna, dan keamanan jaringan melalui penerapan kebijakan terpusat menggunakan GPO.
Rachmat Maulana	Evaluasi Kebijakan Keamanan Active Directory berdasarkan CIS Controls pada PT. XYZ Indonesia	Studi kasus	Penilaian terhadap aturan keamanan Active Directory berdasarkan CIS Controls v8 menunjukkan tingkat kepatuhan awal sebesar 15% untuk kontrol yang relevan. Kepatuhan diperkirakan akan meningkat lebih dari 30% jika rekomendasi perbaikan yang mengacu CIS Benchmark diikuti.

Berdasarkan kajian terhadap penelitian terdahulu, sebagian besar penelitian yang membahas Active Directory berfokus pada implementasi kebijakan tertentu atau pengujian hasil tanpa mengaitkannya secara sistematis dengan kerangka pengendalian keamanan siber yang lebih luas. Penelitian ini berbeda karena tidak hanya mengevaluasi kesesuaian konfigurasi teknis Active Directory menggunakan CIS Benchmark, tetapi juga memetakan hasil evaluasi tersebut ke CIS Controls v8 untuk menunjukkan kontribusi setiap kebijakan GPO terhadap kontrol keamanan strategis. Dengan demikian, penelitian ini menjembatani evaluasi teknis dan pengendalian keamanan tingkat *enterprise*.

II. METODE

A. Metode Penelitian

Penelitian ini menggunakan metode kualitatif dengan pendekatan studi kasus. Metode ini digunakan karena peneliti ingin mengevaluasi dan memahami secara mendalam konfigurasi kebijakan keamanan yang diterapkan dalam Active Directory pada lingkungan SOC PT. XYZ Indonesia.

Penelitian kualitatif dimaksudkan untuk memahami fenomena secara holistik dan kontekstual melalui pengumpulan data secara alamiah. Pengetahuan dibangun melalui interpretasi peneliti terhadap data yang diperoleh [18].

Pendekatan studi kasus memungkinkan peneliti untuk mengkaji fenomena dalam konteks nyata dan mendalam dengan fokus pada makna dan proses. Studi kasus ini tidak hanya bertujuan untuk mengevaluasi, tetapi juga merancang perbaikan kebijakan keamanan berbasis standar CIS Benchmark

B. Objek Penelitian & Ruang Lingkup

Objek penelitian ini adalah lingkungan aktual infrastruktur uji coba (*staging*) Active Directory yang digunakan oleh Perusahaan XYZ Indonesia, yang terdiri dari satu *server domain controller* yang berbasis Windows Server 2022 dan 2 perangkat klien yang berbasis Windows 10 yang bergabung kedalam *domain* tersebut.

Objek evaluasi difokuskan GPO yang aktif diterapkan dan digunakan pada lingkungan Active Directory tersebut.

Penelitian ini mengkaji konfigurasi kebijakan keamanan Active Directory yang diterapkan melalui *Group Policy Objects* (GPO). Penelitian ini mengevaluasi kepatuhan terhadap CIS Benchmark Microsoft Windows Server 2022 dan menyelaraskan hasil evaluasi tersebut dengan CIS Controls versi 8.

Penelitian ini secara khusus terbatas pada lingkungan *staging* yang digunakan untuk pengujian, dengan fokus utama pada aspek teknis konfigurasi sistem serta analisis yang didasarkan pada dokumentasi. Perlu dicatat bahwa ruang lingkup penelitian ini secara sengaja tidak mencakup komponen seperti simulasi serangan atau pengujian penetrasi, evaluasi komprehensif terhadap arsitektur SIEM, serta implementasi langsung rekomendasi di lingkungan produksi.

C. Jenis dan Sumber Data

Data yang digunakan dalam penelitian ini bersifat kualitatif, terdiri dari:

- Data primer: diperoleh melalui observasi langsung terhadap sistem Active Directory yang dikonfigurasi oleh kebijakan domain dan dokumentasi hasil dari "gpresult" dan "gpreport" dari sisi *domain controller* untuk mengidentifikasi kebijakan keamanannya.
- Data sekunder: Berasal dari dokumen CIS Benchmark Microsoft Windows Server 2022, CIS Controls v8, Dokumentasi Microsoft terkait Active Directory dan GPO, dan literatur ilmiah dan hasil penelitian terdahulu yang relevan.

D. Teknik Pengumpulan Data

Teknik pengumpulan data dalam penelitian kualitatif dapat berupa observasi, wawancara, dan studi dokumentasi [18]. Penelitian ini menggunakan dua teknik: observasi langsung dan studi dokumen, yang dipilih karena sesuai untuk mengevaluasi objek teknis berupa konfigurasi sistem informasi. Berikut pengumpulan data yang digunakan dalam penelitian ini meliputi:

1. Observasi

Observasi dilakukan dengan pendekatan partisipatif, di mana peneliti mengakses langsung sistem Active Directory dan melakukan pemeriksaan terhadap kebijakan yang diterapkan melalui *Group Policy Object* (GPO). Adapun tahapan observasi adalah sebagai berikut:

- Mengakses langsung *Group Policy Management Console* (GPMC) pada *domain controller*.
- Menggunakan perintah "gpreport" untuk membuat laporan terperinci dari GPO yang digunakan.
- Menginventarisasi kebijakan yang aktif dan relevan dengan aspek keamanan (misalnya: *account policy*, *script execution*, *user rights*).
- Mendokumentasikan temuan dalam bentuk tabel observasi, *screenshot*, dan catatan konfigurasi.

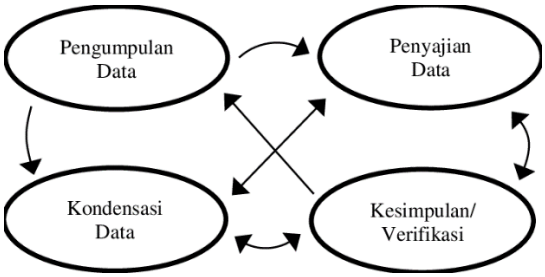
2. Studi Dokumen

Studi dokumen dilakukan untuk membandingkan konfigurasi aktual dengan acuan dari CIS Benchmark for Windows Server 2022 dan memetakan hasil evaluasi kedalam CIS Controls v8 yang relevan. Data dikumpulkan dari dokumen konfigurasi AD, referensi CIS Controls v8, dan CIS Benchmark for Windows Server 2022.

E. Teknik Analisis Data

Miles dan Hubberman menganjurkan agar aktivitas analisis data kualitatif dilakukan secara interaktif dan berlangsung secara terus menerus pada setiap level atau tahapan penelitian sehingga datanya bersifat jenuh berkelanjutan antara pengumpulan, kondensasi, penyajian, dan penarikan kesimpulan data, [18]. Gambar 1 berikut ini proses model analisis data yang berlangsung secara bersamaan:

e-ISSN: 2548-6861



Gambar 1. Komponen Analisis Data

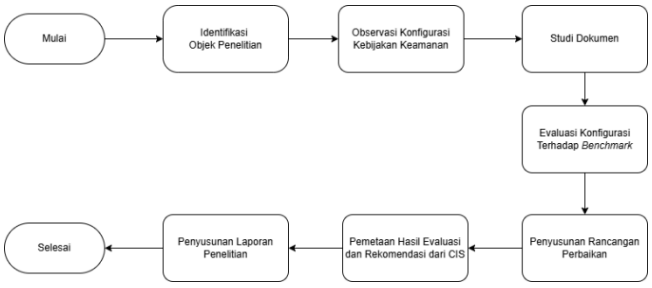
Dalam penerapannya, analisis difokuskan pada proses kondensasi data, penyajian data, dan penarikan kesimpulan, yang dilakukan secara interaktif dan berulang berikut penjelasan lebih lanjut setiap prosesnya:

1. Kondensasi Data
   Kondensasi dilakukan pada data observasi konfigurasi *Group Policy Object* (GPO) terkait keamanan Active Directory dengan acuan CIS Benchmark.
2. Penyajian Data
   Data yang dikondensasikan disajikan dalam tabel evaluasi kesesuaian konfigurasi, pemetaan CIS Benchmark terhadap CIS Controls v8, dan gap analysis.
3. Penarikan Kesimpulan
   Penarikan kesimpulan menafsirkan pola kesesuaian dan ketidaksesuaian, serta merumuskan rekomendasi perbaikan kebijakan keamanan.

Proses ini berlangsung secara berulang hingga diperoleh pemahaman yang komprehensif terhadap kondisi keamanan Active Directory pada lingkungan penelitian.

F. Alur Kerja Penelitian

Untuk mencapai tujuan penelitian, peneliti menyusun alur kerja sistematis yang mencerminkan proses evaluasi sekaligus perancangan perbaikan kebijakan keamanan. Berikut Gambar 2 menampilkan 7 alur kerja penelitian ini secara ringkas:

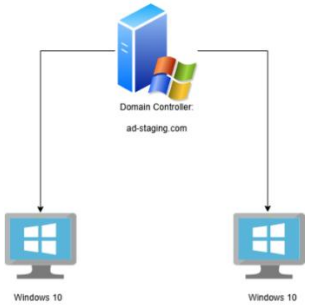


Gambar 2. Alur Kerja Penelitian

Berdasarkan Gambar 2, berikut penjelasan lebih lanjut untuk alur yang terdiri dari tujuh tahap utama sebagai berikut:

1. Identifikasi Objek Penelitian

   Pada tahap awal, peneliti menetapkan bahwa objek penelitian adalah sistem Active Directory yang dibangun dalam lingkungan uji coba (*staging*) oleh PT. XYZ Indonesia. Gambar 3 menunjukkan desain sistem objek penelitian yang menjadi dasar evaluasi kebijakan keamanan Active Directory



Gambar 3.Topologi Infrastruktur Objek Penelitian

   Fokus observasi diarahkan pada kebijakan yang diterapkan melalui *Group Policy Object* (GPO).
2. Observasi Konfigurasi GPO

   Peneliti melakukan observasi langsung terhadap konfigurasi yang ada melalui *Group Policy Management Console* (GPMC) serta melakukan pengecekan di sisi klien menggunakan perintah seperti "gpresult". Peneliti mendokumentasikan seluruh GPO yang aktif.
3. Studi Dokumen

   Dokumen acuan yang digunakan adalah CIS Benchmark for Microsoft Windows Server dan CIS Controls v8. CIS Benchmark digunakan untuk melihat konfigurasi yang direkomendasikan secara teknis, sementara CIS Controls digunakan sebagai kerangka kerja keamanan siber yang bersifat konseptual untuk memetakan setiap temuan konfigurasi terhadap kontrol keamanan tingkat organisasi.
4. Evaluasi Kesesuaian Konfigurasi terhadap *Benchmark*

   Data observasi yang berupa konfigurasi akan dibandingkan satu per satu dengan item dalam CIS Benchmark. Hasil evaluasi ini disusun dalam bentuk tabel evaluasi yang mencantumkan:
   - Nama kebijakan
   - Tujuan kebijakan
   - Rekomendasi CIS
   - Status kesesuaian
   - Potensi risiko dari ketidaksesuaian.
5. Penyusunan Rancangan Perbaikan Kebijakan Keamanan

   Berdasarkan item-item yang dinyatakan tidak sesuai, peneliti menyusun rancangan perbaikan.

Rancangan ini mengacu pada bagian "*Remediation Procedure*" dari CIS Benchmark, yang berisi langkah-langkah teknis untuk memperbaiki konfigurasi.

Tujuan dari tahap ini adalah menghasilkan *output* yang aplikatif, yaitu dokumen perbaikan yang siap diterapkan pada lingkungan AD uji coba.

6. Pemetaan Hasil Evaluasi dan Rekomendasi terhadap CIS Controls v8

   Setelah evaluasi dan rancangan perbaikan selesai, setiap hasil dikaitkan kembali ke kontrol-kontrol dalam CIS Controls v8. Pemetaan ini bertujuan untuk menunjukkan bahwa setiap kebijakan yang diperbaiki berkontribusi terhadap kontrol keamanan tingkat organisasi/*enterprise.*

7. Penyusunan Laporan Penelitian

   Tahap akhir adalah menyusun seluruh temuan, evaluasi, dan rancangan perbaikan ke dalam bentuk laporan tugas akhir. Laporan mencakup:

   - Tabel hasil evaluasi.
   - Rekomendasi perbaikan teknis.
   - Pemetaan kontrol ke CIS.

   Laporan ini dapat dijadikan dasar implementasi kebijakan keamanan oleh perusahaan.

III. HASIL DAN PEMBAHASAN

Penelitian ini dilakukan pada lingkungan Active Directory berbasis Windows Server 2022 yang berfungsi sebagai *domain controller* utama dan 2 perangkat *client workstation* Windows 10 yang tergabung ke domain. Objek utama penelitian mencakup tujuh kebijakan *Group Policy Object* (GPO) yang mengatur aspek autentikasi dan distribusi distribusi kebutuhan SIEM.

Data penelitian diperoleh melalui hasil observasi konfigurasi GPO secara langsung, dokumentasi laporan kebijakan GPO dalam format HTML, dan Dokumentasi konfigurasi GPO, kemudian dibandingkan dengan acuan CIS Microsoft Windows Server 2022 Benchmark v4.0.0 untuk menentukan tingkat kepatuhan terhadap standar keamanan.

A. Kebijakan Keamanan Active Directory yang Diterapkan

Untuk memberikan gambaran yang sistematis mengenai kebijakan *Group Policy Object* (GPO) yang diterapkan di lingkungan uji coba PT. XYZ Indonesia, Gambar 4 merupakan hasil observasi visual dari GPO yang aktif pada *Group Policy Mangement Console* (GPMC) di lingkungan Active Directory.

Gambar 4. Hasil observasi konfigurasi GPO aktif pada GPMC

Berdasarkan hasil observasi terhadap GPO yang aktif tersebut, dilakukan identifikasi kebijakan yang diterapkan pada lingkungan Active Directory beserta cakupan penerapannya. Setiap GPO dianalisis untuk mengetahui fungsi dan keterkaitannya dengan pengaturan keamanan yang relevan. Hasil identifikasi ini selanjutnya dirangkum dalam tabel observasi sebagai dasar evaluasi kesesuaian kebijakan terhadap standar CIS

Tabel 2 berikut ini menyajikan ringkasan GPO aktif beserta tujuannya. Penyajian dalam bentuk tabel ini dimaksudkan untuk membantu dalam mengklasifikasikan dan memahami fungsi kebijakan secara operasional.

TABEL 2. TEMUAN GPO YANG DITERAPKAN

No	Nama GPO	Fungsi / Tujuan Umum	Deskripsi Singkat
1	*Default Domain Policy*	Kebijakan keamanan bawaan Active Directory	Mengatur *password policy*, *account lockout*, dan autentikasi Kerberos.
2	*Sysmon Enrollment*	Monitoring dan audit aktivitas sistem	Menginstal serta mengonfigurasi Sysmon untuk *logging* forensik.
3	*PowerShell 7 Enrollment*	Distribusi PowerShell versi terbaru	Menyediakan PowerShell 7 secara otomatis bagi seluruh *host* domain.
4	*Python Enrollment*	Instalasi *interpreter* Python	Menyediakan Python *runtime* untuk agen *monitoring* dan otomasi skrip.
5	*C++ Enrollment*	Instalasi Visual C++ Runtime Libraries	Menjamin dependensi aplikasi berbasis C++ tersedia di setiap *host*.
6	*Wazuh Enrollment*	Penerapan agen keamanan Wazuh	Menghubungkan *endpoint* ke sistem SIEM (*Security Information and Event Management*).
7	*Wazuh Activation*	Aktivasi agen Wazuh	Mengaktifkan agen agar terhubung ke Wazuh Manager.

Secara keseluruhan, implementasi GPO pada PT. XYZ Indonesia saat ini menunjukkan pendekatan yang berfokus pada automasi instalasi dan penyebaran perangkat lunak pendukung sistem keamanan. PowerShell, Python, dan Visual C++ Redistributable digunakan sebagai dependensi utama untuk eksekusi skrip serta kompatibilitas aplikasi monitoring. Adapun Sysmon dan Wazuh adalah dua komponen penting dalam ekosistem deteksi dan respons insiden.

Dari ketujuh GPO tersebut, enam merupakan *custom policies* hasil konfigurasi tambahan, dan satu yaitu *Default Domain Policy* merupakan kebijakan bawaan (*built-in policy*) Active Directory.

B. Evaluasi Kesesuaian Kebijakan dengan CIS Benchmark

Evaluasi dilakukan dengan membandingkan parameter konfigurasi pada setiap GPO dengan kontrol yang relevan

e-ISSN: 2548-6861

dalam *CIS Microsoft Windows Server 2022 Benchmark v4.0.0*. Mengingat hanya *Default Domain Policy* yang memiliki aturan parameter yang tertulis secara eksplisit dalam CIS Benchmark, evaluasi terhadap enam GPO lainnya dilakukan melalui pendekatan analisis aspek fungsional dan keamanan. Setiap konfigurasi yang terdapat dalam GPO kustom tersebut diperiksa secara menyeluruh, dan jumlah aspek yang dievaluasi mencerminkan konfigurasi aktual yang memang ada pada masing-masing GPO. Karena GPO kustom tidak memiliki padanan parameter langsung dalam CIS Benchmark dan hanya memuat pengaturan operasional tertentu, pemetaan dilakukan secara kategorikal terhadap prinsip keamanan yang relevan dalam sub-bagian CIS Benchmark, seperti pengaturan layanan, hak akses, eksekusi skrip, kebijakan *installer*, atau pemrosesan sumber file. Dengan demikian, evaluasi tetap mengikuti struktur pengendalian CIS meskipun lingkupnya berbeda antara GPO bawaan dan GPO kustom. Berikut merupakan hasil evaluasi kesesuaian kebijakan pada GPO yang diterapkan:

1. *Default Domain Policy:* GPO *Default Domain Policy* merupakan *baseline policy* bawaan Active Directory yang mengatur parameter inti keamanan autentikasi. Gambar 5 merupakan hasil observasi kebijakan yang diterapkan pada GPO *Default Domain Policy*.

Gambar 5. Dokumentasi konfigurasi Kebijakan pada GPO *Default Domain Policy*

Berdasarkan hasil observasi tersebut, dilakukan analisis terhadap parameter kebijakan yang dikonfigurasi pada GPO Default Domain Policy. Setiap pengaturan yang teridentifikasi kemudian dibandingkan dengan rekomendasi yang tercantum dalam CIS Microsoft Windows Server 2022 Benchmark, khususnya pada bagian *Account Policies* dan *Account Lockout Policies*. Hasil perbandingan ini selanjutnya disajikan dalam tabel evaluasi untuk menunjukkan tingkat kesesuaian konfigurasi yang diterapkan. Tabel 3 dibawah ini merupakan hasil evaluasi kebijakan yang ada pada GPO *Default Domain Policy*.

TABEL 3. EVALUASI GPO DEFAULT DOMAIN POLICY

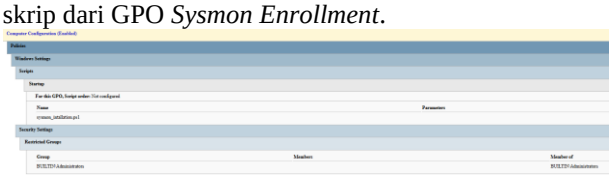
ID Benchmark	Kebijakan	Rekomendasi CIS	Temuan	Status
1.1.1	*Enforce Password History*	≥ 24 Password	24 Password	Sesuai
1.1.2	*Maximum Password Age*	≤ 365 days	42 days	Sesuai
1.1.3	*Minimum Password Age*	≥ 1 days	1 days	Sesuai
1.1.4	*Minimum password length*	≥ 14 characters	7 characters	Tidak Sesuai
1.1.5	*Password must meet complexity requirements*	Enabled	Enabled	Sesuai
1.1.6	*Relax minimum password length limits*	Enabled	Not set	Tidak Sesuai
1.1.7	*Store passwords using reversible encryption*	Disabled	Disabled	Sesuai
1.2.1	*Account lockout Duration*	≥ 15 minutes	Not set	Tidak Sesuai
1.2.2	*Account lockout threshold*	≤ 5 attempts ≠ 0	0 attempt	Tidak Sesuai
1.2.3	*Allow Administrator account lockout*	Enabled	Not set	Tidak Sesuai
1.2.4	*Reset account lockout counter after*	≥ 15 minutes	Not set	Tidak Sesuai

GPO ini sebagian kebijakan sudah sesuai dengan CIS Benchmark. Risiko yang ditimbulkan akibat ketidaksesuain pada *password policy* dapat menimbulkan risiko *brute-force attack* dan *password spraying*, karena pengguna masih dapat menggunakan sandi yang terlalu pendek dan sistem menoleransi terlalu banyak percobaan gagal sebelum mengunci akun

2. *Sysmon Enrollment*: GPO ini bertujuan untuk menggelar utilitas *System Monitor* (Sysmon) guna memperkaya kapabilitas pencatatan *log* sistem (*logging*) yang lebih rinci dibandingkan *Event Log* standar Windows, yang esensial untuk deteksi anomali.

   Metode yang digunakan pada GPO ini adalah *Startup Script* berbasis PowerShell. Skrip tersebut diprogram untuk mengunduh *Sysinternals Suite* dan berkas konfigurasi XML (sysmonconfig-export.xml) dari repositori eksternal secara dinamis, lalu mengeksekusi instalasi Sysmon. Karena instalasi membutuhkan privilese tinggi, konfigurasi tambahan dilakukan melalui *Restricted Groups*, di mana grup khusus tersebut ditambahkan sementara ke dalam grup *administrator* lokal (*Administrators*) pada mesin target. Gambar 6

merupakan hasil observasi konfigurasi kebijakan *Restricted Groups* yang digunakan untuk proses eksekusi skrip dari GPO *Sysmon Enrollment*.



Gambar 6. Dokumentasi konfigurasi penerapan *Restricted Group* pada GPO Sysmon

Skrip dieksekusi oleh sistem pada fase *startup* sebelum pengguna melakukan *login*. Skrip akan memeriksa konektivitas jaringan, mengunduh komponen yang diperlukan, dan menginstal Sysmon. Keberhasilan eksekusi dapat diverifikasi melalui kemunculan *log* operasional Sysmon pada *Event Viewer* di sisi klien. Tabel 4 menyajikan hasil evaluasi dari beberapa aspek yang mewakili proses eksekusi GPO ini.

TABEL 4. EVALUASI GPO SYMON ENROLLMENT

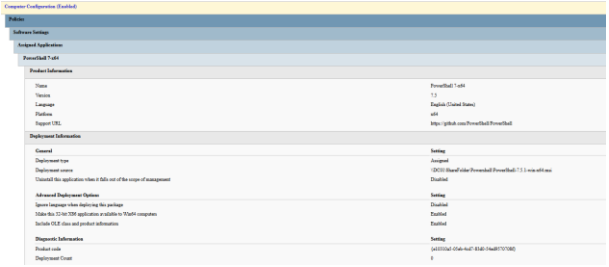
Aspek	Relevansi CIS Benchmark	ID Benchmark	Status
Eksekusi skrip	Administrative Template (Scripts)	18.9.38	Sesuai
Hak akses Admin	User Right Assignment	2.2.4	Tidak sesuai

Penggunaan *Startup Script* dinilai sesuai dengan prinsip manajemen sistem yang aman sebagaimana diatur dalam CIS 18.9.38. Namun, konfigurasi *Restricted Groups* menjadi temuan utama yang bersifat tidak sesuai. Penambahan grup kustom "*Software-Install*" ke dalam grup *Administrators* lokal secara otomatis memberikan hak istimewa penuh, termasuk hak-hak sensitif yang dibatasi ketat oleh CIS 2.2.4: "*Act as part of the operating system is set to 'No One'*". Konfigurasi ini melanggar prinsip *Least Privilege*.

Risiko yang ditimbulkan jika salah satu akun dalam grup "*Software-Install*" dikompromikan, penyerang langsung mendapatkan akses penuh ke seluruh sistem, memungkinkan mereka untuk menanamkan *rootkit*, mematikan kontrol keamanan, atau melakukan pergerakan lateral (*lateral movement*) ke server lain dengan mudah. GPO ini direkomendasikan untuk diperketat dengan menghapus penambahan hak admin yang tidak diperlukan

3. *Powershell 7 Enrollment*: GPO ini mendistribusikan PowerShell 7 melalui kebijakan *Software Installation* (*Computer Configuration*) menggunakan paket MSI Powershell 7 yang tersimpan di jaringan. Sistem operasi akan menginstal PowerShell 7 sebelum antarmuka pengguna dimuat. Tujuan PowerShell 7 ini memungkinkan agen Wazuh untuk mengeksekusi perintah-perintah *Active Response* tingkat lanjut yang tidak didukung oleh PowerShell versi lama bawaan Windows.

Konfigurasi GPO ini menggunakan mekanisme standar *Software Installation* pada *Computer Configuration*. Paket MSI PowerShell 7 ditambahkan sebagai paket yang ditugaskan (*Assigned package*). Gambar 7 merupakan hasil observasi penerapan kebijakan instalasi perangkat lunak Powershell 7 melalui GPO.



Gambar 7. Dokumentasi konfigurasi Instalasi Powershell 7 dari GPO

Berdasarkan dokumentasi konfigurasi tersebut, dilakukan analisis terhadap metode instalasi PowerShell 7 yang diterapkan melalui kebijakan *Software Installation* pada *Computer Configuration*. Mekanisme ini memastikan proses instalasi berjalan secara terpusat dan dieksekusi oleh sistem sebelum antarmuka pengguna dimuat. Tabel 5 menyajikan hasil evaluasi berdasarkan beberapa aspek terkait proses eksekusi dari GPO tersebut.

TABEL 5. EVALUASI GPO POWERSHELL ENROLLMENT

Aspek	Relevansi CIS Benchmark	ID Benchmark	Status
Metode Instalasi	Windows Installer	18.10.81.2	Sesuai
Log Audit	Windows Powershell	18.10.87.1	Tidak sesuai

Metode instalasi *Assigned* pada level komputer dinilai ***sesuai*** karena proses instalasi berjalan menggunakan hak akses *SYSTEM*. Hal ini mematuhi rekomendasi CIS 18.10.81.2: *"Ensure 'Always install with elevated privileges' is set to 'Disabled'."* Dengan metode ini, administrator tidak perlu memberikan hak elevasi berbahaya kepada pengguna biasa untuk menginstal perangkat lunak.

e-ISSN: 2548-6861

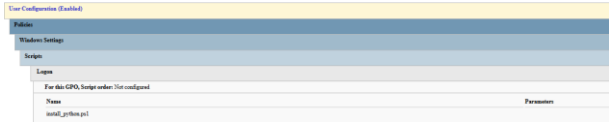
Meskipun instalasinya aman, CIS sangat fokus pada keamanan PowerShell seperti yang terterta pada CIS 18.10.87: "*Ensure 'Turn on PowerShell Script Block Logging' is set to 'Enabled'*"

Evaluasi menunjukkan bahwa keberadaan Powershell7 harus diikuti oleh penyesuaian kebijakan *logging* agar aktivitas skrip tetap dapat dipantau. Tanpa penyesuaian ini, konsistensi kontrol audit antara PowerShell versi lama dan baru tidak dapat terjamin

4. *Python Enrollment*: GPO ini menyediakan *runtime* bahasa pemrograman Python di seluruh *endpoint* target sebagai prasyarat lingkungan (*dependency management*) untuk fitur *Active Response* Wazuh, khususnya integrasi Yara yang berbasis Python.

   Proses instalasi ini dikonfigurasi sebagai *Logon Script* pada *User Configuration* > *Windows Settings* > *LogOn* > *PowerShell Scripts*. Skrip instalasi berisi perintah untuk menjalankan *installer* Python secara diam-diam (*quiet mode*) dari direktori jaringan.

   Jadi skrip berjalan saat pengguna melakukan otentikasi masuk (*login*) ke sistem, memastikan pustaka Python tersedia di profil pengguna untuk skrip keamanan yang membutuhkannya. Gambar 8 merupakan hasil observasi konfigurasi kebijakan instalasi Python yang diterapkan melalui GPO.



Gambar 8. Dokumentasi konfigurasi instalasi python dengan metode *User Configuration* pada GPO

   Berdasarkan hasil observasi konfigurasi tersebut, dilakukan analisis terhadap mekanisme instalasi Python yang diterapkan melalui kebijakan pada konteks pengguna. Evaluasi difokuskan pada metode eksekusi skrip untuk menjalankan perintah instalasi melalui GPO. Hasil evaluasi ini kemudian dirangkum dalam tabel evaluasi untuk menilai kesesuaian kebijakan instalasi Python terhadap rekomendasi CIS Benchmark yang relevan. Tabel 6 dibawah ini merupakan hasil evaluasi dari proses eksekusi GPO ini.

TABEL 6. EVALUASI GPO PYTHON ENROLLMENT

Aspek	Relevansi CIS Benchmark	ID Benchmark	Status
Eksekusi Skrip	User Account Control (UAC)	2.3.17.3	Tidak sesuai
User Config	Windows Installer	18.10.81.1	Tidak sesuai

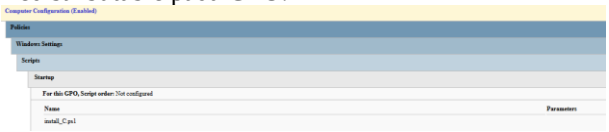
   GPO ini menerapkan *Logon Script* pada konfigurasi pengguna (*User Configuration*), yang berarti instalasi berjalan saat pengguna masuk ke sistem.

   CIS mewajibkan agar *Standard User* langsung ditolak jika meminta akses admin seperti yang tertulis di CIS 2.3.17.3 (L1) "*Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests*'". Seperti yang tertulis juga pada CIS 18.10.81.1 (L1) "*Ensure 'Allow user control over installs' is set to 'Disabled*'" bahwa user biasa tidak boleh memiliki kendali untuk mengubah opsi instalasi

   Dengan menaruh script di sisi *User Configuration*, seolah-olah memberikan beban instalasi kepada user. Berdasarkan hasil evaluasi, mekanisme ini dinilai tidak optimal, mekanisme instalasi perlu dialihkan ke *Computer configuration* agar fungsional dan aman.

5. *C++ Enrollment:* Sama seperti *Python Enrollment*, GPO ini bertujuan memenuhi dependensi pustaka sistem. Pustaka Visual C++ Redistributable diperlukan agar biner eksekusi Yara dapat berjalan tanpa kesalahan kompatibilitas.

   Konfigurasi menggunakan *Startup Script PowerShell* pada *Computer Configuration*. Skrip ini memanggil installer dengan parameter "`/install /passive /norestart`" untuk mencegah interaksi pengguna atau reboot mendadak. Instalasi dieksekusi di latar belakang saat sistem dimulai (*startup*), memastikan pustaka C++ siap digunakan sebelum layanan keamanan lainnya mencoba beroperasi. Gambar 9 merupakan hasil observasi konfigurasi kebijakan instalasi Visual C++ Redistributable pada GPO.



Gambar 9. Dokumentasi konfigurasi onstalasi C++ dengan metode *Computer Configuration* pada GPO

   Berdasarkan hasil observasi konfigurasi tersebut, dilakukan analisis terhadap kebijakan instalasi *Visual C++ Redistributable*. Evaluasi difokuskan pada metode eksekusi skrip yang menjalankan perintah paket instalasi melalui GPO. Hasil evaluasi ini selanjutnya dirangkum dalam tabel evaluasi untuk menilai kesesuaian kebijakan

instalasi terhadap rekomendasi CIS Benchmark yang relevan. Tabel 7 merupakan hasil evaluasi GPO ini berdasarkan aspek eksekusinya.

TABEL 7. EVALUASI GPO C++ ENROLLMENT

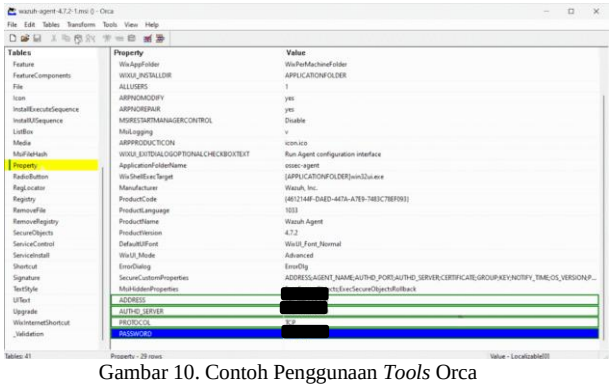
Aspek	Relevansi CIS Benchmark	ID Benchmark	Status
Eksekusi Skrip	Scripts	18.9.38	Sesuai

Penggunaan skrip *startup* yang berjalan secara asinkron mematuhi panduan pada CIS 18.9.38 (*Scripts*), yang memastikan pustaka sistem terpasang secara global pada mesin sebelum interaksi pengguna terjadi.

Dengan distribusi melalui *Startup Script* sudah sesuai, tetapi integritas *installer* dan perlindungan akses skrip perlu dipastikan lagi agar tidak menjadi penyebab serangan.

6. *Wazuh Enrollment*: GPO ini berfungsi sebagai mekanisme distribusi utama untuk agen Wazuh. Tujuannya adalah memastikan seluruh *endpoint* terinstalasi agen keamanan yang terkonfigurasi secara seragam untuk terhubung ke manajemen pusat tanpa intervensi manual.

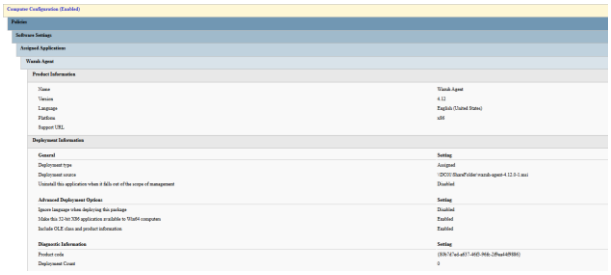
Konfigurasi melibatkan modifikasi paket instalasi MSI menggunakan perangkat lunak *Orca*. Parameter vital seperti alamat IP manajer (WAZUH_MANAGER) dan kunci autentikasi disisipkan ke dalam tabel properti MSI. Modifikasi ini disimpan sebagai file transformasi (.mst). Gambar 10 ini contoh modifikasi yang dilakukan pada file *installer* Wazuh.



Gambar 10. Contoh Penggunaan *Tools* Orca

Dalam GPO, paket didistribusikan melalui *Computer Configuration* > *Policies* > *Software Settings* > *Software installation* dengan metode *Advanced* untuk menerapkan file transformasi tersebut saat instalasi.

Kebijakan dieksekusi oleh layanan *Group Policy Client* pada saat *booting* sistem. Sistem akan mendeteksi paket MSI yang ditugaskan (*assigned*) dan melakukan instalasi senyap (*silent installation*) sebelum layar *login* muncul. Gambar 11 merupakan hasil observasi konfigurasi kebijakan instalasi Wazuh Agent yang dilakukan melalui GPO.



Gambar 11. Dokumentasi konfigurasi Instalasi Wazuh Agent

Berdasarkan hasil observasi konfigurasi tersebut, dilakukan analisis terhadap kebijakan instalasi Wazuh Agent. Evaluasi difokuskan pada mekanisme instalasai agen melalui GPO serta temuan adanya penyisipan kredensial pada *file installer*. Hasil evaluasi ini selanjutnya dirangkum dalam tabel evaluasi untuk menilai kesesuaian terhadap rekomendasi CIS Benchmark yang relevan. Tabel 8 merupakan hasil evaluasi dari beberapa aspek terkait proses konfigurasi dan eksekusi GPO tersebut.

TABEL 8. EVALUASI GPO WAZUH ENROLLMENT

Aspek	Relevansi CIS Benchmark	ID Benchmark	Status
Manajemen Kredensial	Security Options	2.3.10.4	Tidak sesuai
Metode Instalasi	Windows Installer	18.10.81.2	Sesuai
Sumber File	Hardened UNC Paths	18.6.14.1	Tidak sesuai

Penyimpanan kata sandi registrasi dalam format *cleartext* di dalam file .mst yang dapat diakses melalui jaringan mengekspos kredensial tersebut terhadap risiko pencurian. CIS 2.3.10.4 (L2) "*Ensure 'Network access: Do not allow storage of passwords and credentials for network authentication' is set to 'Enabled'*". Prinsip ini menegaskan bahwa penyimpanan kredensial dalam bentuk yang dapat diretrievasi tanpa enkripsi yang memadai adalah kerentanan.

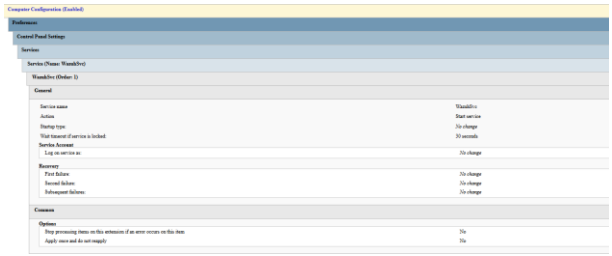
Distribusi melalui jaringan memerlukan pengamanan jalur UNC. CIS 18.6.14.1 (L1) "*Ensure 'Hardened UNC Paths' is set to 'Enabled...'*". Tanpa pengerasan jalur UNC (*Mutual Authentication*, *Integrity*), proses pengambilan installer rentan terhadap serangan *spoofing* atau *tampering*.

e-ISSN: 2548-6861

Instalasi terpusat melalui Assigned MSI sudah sesuai, tetapi penyimpanan parameter sensitif dan penggunaan UNC path tanpa penguatan menimbulkan risiko keamanan. Pengamanan jalur distribusi dan proteksi parameter perlu perbaikan

7. *Wazuh Activation*: GPO ini menggunakan *Group Policy Preferences* (GPP) untuk mengatur status layanan "*WazuhSvc*" menjadi "*Automatic*" dan memaksakan tindakan "*Start service*".

   Implementasi dilakukan melalui *Group Policy Preferences*. Pada jalur *Computer Configuration* > *Preferences* > *Control Panel Settings* > *Services*, sebuah objek layanan baru didefinisikan untuk layanan bernama "*WazuhSvc*". Gambar 12 merupakan hasil observasi konfigurasi kebijakan aktivasi layanan Wazuh melaui GPO.



Gambar 12. Dokumentasi konfigurasi aktivasi layanan Wazuh melalui GPO

Berdasarkan hasil observasi konfigurasi tersebut dilakukan analisis terhadap penerapa kebijakan aktivasi layanan Wazuh. Evaluasi difokuskan pada mekanisme aktivasi agen Wazuh melalui GPO. Hasil evaluasi ini selanjutnya dirangkum dalam tabel evaluasi untuk menilai kesesuaian terhadap rekomendasi CIS Benchmark yang relevan. Tabel 9 menyajikan hasil evaluasi berdasarkan aspek eksekusi dari GPO tersebut.

TABEL 9. EVALUASI GPO WAZUH ACTIVATION

Aspek	Relevansi CIS Benchmark	ID Benchmark	Status
Layanan Sistem	System services	5	Sesuai

Fokus utama CIS 5 (*System Services*) adalah menonaktifkan layanan yang tidak aman. Dengan ini, memastikan ketersediaan (*Availability*) layanan kontrol keamanan dinilai sesuai.

Secara keseluruhan, evaluasi menunjukkan bahwa *Default Domain Policy* merupakan satu-satunya GPO yang memiliki padanan parameter eksplisit dalam CIS Benchmark, sementara enam GPO lainnya dipetakan secara kategorikal berdasarkan aspek fungsionalnya. Temuan utama mencakup ketidaksesuaian pada parameter autentikasi, hak akses yang tidak sesuai pada *Sysmon Enrollment*, serta desain instalasi *Python Enrollment* dan *Wazuh Enrollment* yang menimbulkan risiko operasional.

Konfigurasi pada GPO lain umumnya sudah sesuai, dengan beberapa dependensi seperti *logging* PowerShell dan keamanan UNC path yang perlu dipastikan penerapannya. Temuan ini menjadi dasar bagi penyusunan rekomendasi perbaikan berikutnya

Seluruh hasil evaluasi pada bagian ini diperoleh melalui observasi langsung terhadap konfigurasi GPO pada lingkungan uji (*staging*) dan dievaluasi secara deskriptif berdasarkan acuan CIS Benchmark.

C. Rekomendasi Perbaikan Konfigurasi Keamanan Active Directory

Berdasarkan hasil evaluasi yang telah dipaparkan sebelumnya, teridentifikasi sejumlah konfigurasi GPO yang belum memenuhi standar keamanan CIS Microsoft Windows Server 2022 Benchmark v4.0.0. Ketidaksesuaian ini mencakup aspek krusial seperti manajemen identitas, hak akses administratif, arsitektur distribusi perangkat lunak, serta keamanan jaringan.

Untuk meningkatkan status kepatuhan, disusun rekomendasi perbaikan teknis yang diklasifikasikan berdasarkan area risiko. Implementasi rekomendasi ini bertujuan untuk menutup celah keamanan (*security hardening*) dan memastikan integritas lingkungan Active Directory.

1. Penguatan Kebijakan Akun (*Account Policy Hardening*): Evaluasi pada *Default Domain Policy* menunjukkan adanya risiko tinggi terhadap serangan berbasis identitas akibat konfigurasi panjang kata sandi yang tidak memadai dan non-aktifnya fitur penguncian akun. Diperlukan peningkatan entropi kata sandi dan pengaktifan mekanisme pertahanan aktif untuk memitigasi serangan *brute-force* dan *credential stuffing*.

   Upaya yang dapat dilakukan *administrator* adalah dengan melakukan perubahan pada *path* `Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies`. Lalu ubah nila kebijakan yang ada sesuai dengan rekomendasi CIS Benchmark. Tabel 10 dibawah ini dapat membantu proses perbaikan yang dibutuhkan untuk penguatan kebijakan akun.

TABEL 10. REKOMENDASI PERBAIKAN CIS BENCHMARK

ID Benchmark	Kebijakan	Rekomendasi CIS
1.1.4	*Minimum password length*	≥ 14 characters

1.1.6	*Relax minimum password length limits*	Enabled
1.2.1	*Account lockout Duration*	≥ 15 minutes
1.2.2	*Account lockout threshold*	≤ 5 attempts ≠ 0
1.2.3	*Allow Administrator account lockout*	Enabled
1.2.4	*Reset account lockout counter after*	≥ 15 minutes

2. Perbaikan pada Hak Akses Administratif (*Privilege Management*): Pada GPO *Sysmon Enrollment*, praktik penambahan grup instalasi ke dalam grup Administrator lokal melalui *Restricted Groups* dinilai melanggar prinsip keamanan fundamental.

   Pencabutan hak akses administratif permanen dari grup "*Software-Install*" mutlak diperlukan untuk mematuhi prinsip *Least Privilege* sesuai CIS Section 2.2. Mengingat skrip instalasi Sysmon dijalankan menggunakan *Startup Script* (yang berjalan dengan hak akses *SYSTEM*), elevasi hak akses pengguna tidak diperlukan untuk keberhasilan instalasi.

3. Standarisasi Arsitektur Distribusi Perangkat Lunak: Pada GPO *Python Enrollment* dinilai tidak sesuai dikarenakan penggunaan *Logon Script* yang rentan konflik dengan *User Account Control* (UAC) serta lokasi instalasi yang tidak standar.

   Diperlukan migrasi metode eksekusi dari konteks pengguna (*User Context*) ke konteks sistem (*System Context*). Hal ini bertujuan menjamin konsistensi instalasi tanpa bergantung pada sesi pengguna dan memastikan aset perangkat lunak dapat diakses oleh agen keamanan lainnya.

   Proses remediasi dilakukan dengan memindahkan skrip instalasi dari *User Configuration (Logon)* ke *Computer Configuration (Startup)*.

4. Penguatan Jalur Distribusi Jaringan (*Network Integrity*): Evaluasi pada GPO *Wazuh Enrollment*, *C++ Enrollment*, dan *PowerShell 7 Enrollment* menunjukkan adanya ketergantungan keamanan pada jalur jaringan yang belum diamankan, hal ini berpotensi dimanipulasi melalui serangan *spoofing*.

   Implementasikan GPO baru pada level domain untuk mengaktifkan *Hardened UNC Paths* sesuai CIS 18.6.14.1. Konfigurasikan nilai yang di rekomendasikan CIS Benchmark. Konfigurasi tersebut diterapkan untuk jalur (*path*) `\\*\SYSVOL` dan `\\*\NETLOGON` serta *share folder* distribusi perangkat lunak. Konfigurasi ini menjamin bahwa paket *installer* yang diterima klien adalah autentik dan tidak dimodifikasi di tengah jalan.

5. Peningkatan Visibilitas Audit (*Logging Enhancement*): Meskipun instalasi *PowerShell 7* telah berjalan dengan baik, kehadiran *shell* baru ini menciptakan celah audit jika tidak disertai kebijakan pencatatan yang sesuai. Lakukan perluasan cakupan kebijakan audit untuk meliputi seluruh mesin eksekusi PowerShell guna mencegah *blind spot* dalam forensik digital.

   Administrator harus memastikan GPO *Administrative Templates* untuk PowerShell dikonfigurasi untuk mengaktifkan "*Turn on PowerShell Script Block Logging*" (CIS 18.10.87.1). Kebijakan ini harus diterapkan pada level komputer agar efektif mencakup aktivitas pada `pwsh.exe` (PowerShell 7) maupun `powershell.exe` (Legacy).

6. Kontrol Aset dan Keamanan Instalasi Perangkat Lunak (*Software Inventory & Secure Installation*): Rekomendasi ini dibuat karena proses instalasi *software* sebelumnya dilakukan tanpa validasi digital dan tanpa *Software Restriction Policy* (SRP). Untuk meningkatkan keamanan, GPO harus dikonfigurasi agar sistem hanya mengizinkan instalasi dari *trusted publisher* atau *signed binaries*, dan menerapkan *AppLocker* atau SRP untuk mencegah eksekusi file instalasi dari sumber tidak sah.

   Kebijakan ini mematuhi mendukung CIS Control 2 – *Inventory and Control of Software Assets*, yang memastikan bahwa perangkat lunak yang dijalankan di domain telah diverifikasi.

   Harapannya dapat menutup potensi *malware injection* dalam proses instalasi, memastikan setiap instalasi terekam dan tervalidasi, dan meningkatkan keandalan rantai distribusi *software* (*software supply chain security*).

Rekomendasi di atas tidak hanya bersifat korektif, namun juga preventif, karena dirancang untuk menutup celah eksploitasi yang mungkin terjadi di lingkungan Active Directory. Penerapannya secara bertahap dan terstruktur dapat membantu perusahaan meningkatkan kematangan keamanan informasi secara menyeluruh.

D. Pemetaan terhadap kebijakan keamanan Active Directory terkait relevansinya dengan CIS Controls v8

Pada tahap ini, tujuan utamanya adalah mengintegrasikan hasil evaluasi konfigurasi *Group Policy Object* (GPO) berdasarkan CIS Benchmark dengan kerangka kerja kontrol keamanan tingkat organisasi yaitu CIS Controls v8. Pemetaan dilakukan pada dua tingkat analisis. Langkah pertama adalah melakukan pemetaan konseptual antara

e-ISSN: 2548-6861

bagian-bagian relevan dari CIS Benchmark dan kontrol utama dalam CIS Controls v8 untuk menunjukkan hubungan antara standar konfigurasi teknis dan tujuan kontrol keamanan yang diatur dalam CIS Controls v8. Kedua, pemetaan operasional dilakukan antara GPO yang diimplementasikan di lingkungan Active Directory dan kontrol CIS Controls v8 untuk menunjukkan kontribusi teknis masing-masing kebijakan terhadap kontrol keaaman yang diatur dalam CIS Controls v8.

Pendekatan berlapis ini memungkinkan analisis kepatuhan Active Directory tidak hanya dilihat dari perspektif konfigurasi teknis, tetapi juga dari perspektif kontrol keamanan tingkat organisasi. Berikut Tabel 11 yang menjelaskan terkait pemetaan CIS Benchmark dan CIS controls v8 yang mengatur Active Directory.

TABEL 11. PEMETAAN CIS BENCHMARK DAN CIS CONTROLS YANG MENGATUR ACTIVE DIRECTORY

Section CIS Benchmark	**Fokus Konfigurasi CIS Benchmark**	**CIS Control (v8)**	**Relevansi terhadap Active Directory**
1. *Account Policies*	Kebijakan kata sandi (panjang, kompleksitas, masa berlaku) dan penguncian akun pengguna.	5 – *Account Management*	Mengatur autentikasi pengguna domain agar kredensial AD kuat, mencegah *brute-force* dan *reuse password*.
2. *Local Policies*	Kebijakan keamanan dan hak pengguna, termasuk pengaturan *Domain Controller*, *Domain Member*, LDAP, dan Kerberos.	5 – *Account Management* 6 – *Access Control Management*	Mengamankan komunikasi LDAP/Kerberos antar domain, membatasi hak administratif, dan menjaga integritas data AD.
3. *Event Log*	Pengaturan ukuran, retensi, dan izin akses terhadap log keamanan.	8 – *Audit Log Management*	Merekam aktivitas otentikasi, modifikasi objek AD, dan kejadian administratif untuk keperluan audit dan forensik.
4. *Restricted Groups*	Pengaturan keanggotaan grup administratif (mis. *Domain Admins*, *Enterprise Admins*).	6 – *Access Control Management*	Melindungi grup administratif AD agar tidak dapat diubah oleh akun tidak sah.
5. *System Services*	Pengelolaan layanan sistem penting pada DC, seperti menonaktifkan *Print Spooler* untuk mencegah eksploitasi.	4 – *Secure Configuration Management*	Mengurangi permukaan serangan pada Domain Controller dengan menonaktifkan layanan tidak diperlukan.
17. *Advanced Audit Policy Configuration*	Audit aktivitas autentikasi (Kerberos, *logon/logoff*), manajemen akun, perubahan direktori, dan penggunaan hak istimewa.	8 – *Audit Log Management*	Memberikan visibilitas penuh terhadap aktivitas AD, mendukung deteksi insiden dan pelacakan akses administratif.
18. *Administrative Templates (Computer Configuration)*	Kebijakan tambahan terkait keamanan AD seperti LAPS, *Group Policy* refresh, Netlogon, dan LDAP/Kerberos signing.	5 – *Account Management* 6 – *Access Control Management* 4 – *Secure Configuration Management*	Meningkatkan keamanan AD dengan enkripsi komunikasi, rotasi password lokal terkelola (LAPS), serta penerapan GPO yang konsisten.

Hasil pemetaan di atas menunjukkan bahwa sebagian besar aspek keamanan Active Directory yang diatur dalam CIS Benchmark secara langsung beririsan dengan CIS Controls v8, khususnya *Control* 4 (*Secure Configuration Management*), *Control* 5 (*Account Management*), Control 6 (*Access Control Management*), dan *Control* 8 (*Audit Log Management*). Pemetaan ini menegaskan bahwa konfigurasi teknis yang dievaluasi melalui CIS Benchmark memiliki implikasi langsung terhadap kepatuhan terhadap kontrol keamanan inti dalam CIS Controls.

Namun, perlu dicatat bahwa pemetaan pada tahap ini bersifat konseptual dan tidak semua rekomendasi CIS Benchmark dapat diterapkan secara langsung melalui mekanisme GPO. Beberapa rekomendasi memerlukan dukungan kebijakan organisasi tambahan dan prosedur operasional, sehingga efektivitas keamanan Active Directory tidak hanya ditentukan oleh konfigurasi teknis, tetapi juga oleh praktik manajemen keamanan yang berkelanjutan.

Untuk mengaitkan pemetaan konseptual dengan implementasi teknis dalam lingkungan penelitian, pemetaan lebih lanjut dilakukan antara GPOs yang diterapkan dan CIS Controls v8. Pemetaan ini berfokus pada hubungan fungsional antara keluaran kebijakan GPO dan tujuan keamanan yang diwakili oleh kontrol dalam CIS Controls v8. Dengan pendekatan ini, kontribusi masing-masing GPO dalam memperkuat keamanan Active Directory dapat dianalisis secara lebih operasional dan terukur.

Pemetaan yang dilakukan pada Tabel 12 menunjukkan relasi fungsional antara setiap GPO dengan kontrol dan *safeguard* yang relevan dalam CIS Controls v8 yang memiliki dampak teknis terhadap penguatan konfigurasi Active Directory. Prinsip pemetaan mempertimbangkan kesesuaian fungsional antara *output* GPO dan tujuan keamanan yang disampaikan oleh setiap *safeguard*.

TABEL 12. RELEVANSI GPO YANG DITERAPKAN DENGAN CIS CONTROLS v8

No	Nama GPO	CIS Controls v8	Alasan Relevansi
1	*Default Domain Policy*	Control 4, 5, 6	Mengatur *baseline* konfigurasi, manajemen akun, dan hak akses administratif
2	*C++ Enrollment*	Control 2	Mengontrol perangkat lunak dan keamanan aplikasi
3	*PowerShell 7 Enrollment*	Control 4	Mengatur keamanan eksekusi skrip
4	*Python Enrollment*	Control 2	Membatasi interpreter dan modul aplikasi
5	*Sysmon Enrollment*	Control 8, 13	Memantau aktivitas endpoint dan proses
6	*Wazuh Activation*	Control 8, 13	Mengirim log keamanan ke server SIEM
7	*Wazuh Enrollment*	Control 8, 13	Sentralisasi pengumpulan event keamanan

Hasil pemetaan pada Tabel 12 menunjukkan bahwa implementasi GPO berkontribusi langsung terhadap sejumlah kontrol utama dalam CIS Controls v8, terutama *Control* 2 (*Inventory and Control of Software Assets*), *Control* 4 (*Secure Configuration Management*), *Control* 5 (*Account Management*), *Control* 8 (*Audit Log Management*), dan *Control* 13 (*Network Monitoring and Defense*). Kontribusi ini terlihat dari fungsi teknis GPO dalam mengatur instalasi perangkat lunak, penguatan kebijakan autentikasi, pencatatan aktivitas sistem, serta pengiriman log keamanan ke sistem terpusat.

Berdasarkan pemetaan konseptual pada Tabel 11 dan Tabel 12, dapat disimpulkan bahwa kebijakan *Group Policy Object* (GPO) yang diterapkan dalam lingkungan Active Directory secara langsung terkait dengan sejumlah kontrol kunci dalam CIS Controls v8. Namun, pemetaan tersebut juga menunjukkan bahwa hubungan yang ada tidak sepenuhnya mewakili pemenuhan semua langkah pengamanan yang dibutuhkan oleh setiap kontrol.

Beberapa GPO secara fungsional mendukung tujuan keamanan tertentu, tetapi implementasinya masih terbatas atau tidak sepenuhnya selaras dengan rekomendasi CIS Benchmark. Kondisi ini menyebabkan beberapa pengamanan dalam CIS Controls v8 tidak sepenuhnya terpenuhi, meskipun kontrol yang relevan telah diidentifikasi sebagai relevan pada tahap pemetaan.

Oleh karena itu, analisis selisih (*gap analysis*) lebih lanjut diperlukan untuk secara sistematis mengidentifikasi perbedaan antara konfigurasi kebijakan keamanan Active Directory saat ini dan kondisi yang direkomendasikan oleh CIS Benchmark dan CIS Controls v8. Analisis selisih ini bertujuan untuk mengukur tingkat kepatuhan awal, mengidentifikasi area kelemahan spesifik, dan mengevaluasi potensi peningkatan kepatuhan setelah menerapkan rekomendasi perbaikan yang diformulasikan.

E. Gap Analysis Kepatuhan Active Directory dengan CIS Controls v8

Analisis kesenjangan (*gap analysis*) dilakukan untuk mengidentifikasi perbedaan antara kondisi konfigurasi kebijakan keamanan yang diterapkan saat ini dengan kondisi yang direkomendasikan berdasarkan CIS Benchmark dan CIS Controls. Analisis ini bertujuan untuk memberikan gambaran tingkat kepatuhan awal terhadap standar keamanan, sekaligus mengidentifikasi area konfigurasi yang memerlukan perbaikan pada kebijakan *Group Policy Object* (GPO) yang diterapkan.

Pada penelitian ini, penilaian kondisi setelah perbaikan dilakukan secara konseptual dengan mengasumsikan bahwa seluruh rekomendasi perbaikan telah diterapkan sesuai rekomendasi perbaikan yang diberikan sebelumnya. Pendekatan ini digunakan untuk menggambarkan potensi peningkatan tingkat kepatuhan terhadap CIS Controls serta sebagai dasar perencanaan implementasi rancangan *hardening* kebijakan keamanan Active Directory di masa mendatang, tanpa melakukan perubahan langsung pada sistem yang menjadi objek penelitian. Berikut Tabel 13 yang menyajikan hasil dari analisis kesenjangan antara dua kondisi konfigurasi:

TABEL 13. GAP ANALYSIS KEPATUHAN ACTIVE DIRECTORY TERHADAP CIS CONTROLS V8

CIS Safeguard	Asset Type	Security Function	Title	Description	Before	After
			Inventory and Control of Software Assets			
2,3	Applications	Respond	Address Unauthorized Software	Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	x	✓

e-ISSN: 2548-6861

2,5	Applications	**Protect**	Allowlist Authorized Software	Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.	x	✓
2,6	Applications	**Protect**	Allowlist Authorized Libraries	Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.	x	✓
2,7	Applications	**Protect**	Allowlist Authorized Scripts	Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.	x	✓
			Secure Configuration of Enterprise Assets and Software			
4,1	Applications	**Protect**	Establish and Maintain a Secure Configuration Process	Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	x	✓
4,3	Users	**Protect**	Configure Automatic Session Locking on Enterprise Assets	Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	✓	✓
4,7	Users	**Protect**	Manage Default Accounts on Enterprise Assets and Software	Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.	✓	✓
4,10	Devices	**Respond**	Enforce Automatic Device Lockout on Portable End-User Devices	Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.	x	✓
			Account Management			
5,1	Users	**Identify**	Establish and Maintain an Inventory of Accounts	Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	x	✓
5,2	Users	**Protect**	Use Unique Passwords	Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	x	✓
5,4	Users	**Protect**	Restrict Administrator Privileges to Dedicated Administrator Accounts	Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	x	✓
5,6	Users	**Protect**	Centralize Account Management	Centralize account management through a directory or identity service.	✓	✓
			Access Control Management			
6,1	Users	**Protect**	Establish an Access Granting Process	Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.	x	✓
6,2	Users	**Protect**	Establish an Access Revoking Process	Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.	x	✓
6,7	Users	**Protect**	Centralize Access Control	Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.	x	✓
			Audit Log Management			
8,1	Network	**Protect**	Establish and Maintain an Audit Log Management Process	Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	✓	✓

8,2	Network	Detect	Collect Audit Logs	Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	x	✓
8,3	Network	Protect	Ensure Adequate Audit Log Storage	Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	✓	✓
8,4	Network	Protect	Standardize Time Synchronization	Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.	✓	✓
8,5	Network	Detect	Collect Detailed Audit Logs	Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.	x	✓
8,9	Network	Detect	Centralize Audit Logs	Centralize, to the extent possible, audit log collection and retention across enterprise assets.	✓	✓
8,11	Network	Detect	Conduct Audit Log Reviews	Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.	✓	✓
			Network Monitoring and Defense			
13,1	Network	Detect	Centralize Security Event Alerting	Centralize security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard.	✓	✓
13,2	Devices	Detect	Deploy a Host-Based Intrusion Detection Solution	Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.	✓	✓
13,7	Devices	Protect	Deploy a Host-Based Intrusion Prevention Solution	Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.	x	✓
13,11	Network	Detect	Tune Security Event Alerting Thresholds	Tune security event alerting thresholds monthly, or more frequently.	x	✓

Berdasarkan hasil analisis kesenjangan, sebelum proses penguatan, kepatuhan terhadap sejumlah kontrol dasar, khususnya *Contro*l 2 (*Inventory and Control of Software Assests*), *Control* 5 (*Account Management*), dan *Control* 8 (*Audit Log Management*), masih rendah. Pada tahap awal ini, berbagai langkah pengamanan terkait validasi perangkat lunak, penguatan pengaturan otentikasi, dan cakupan catatan audit baru diterapkan secara parsial, sehingga tidak memenuhi standar CIS Controls v8. Setelah proses *hardening* secara konseptual, ketiga kontrol ini menunjukkan peningkatan yang paling signifikan. Persentase kepatuhan untuk *Control* 2, *Control* 5, dan *Control* 8 meningkat secara signifikan dalam tabel setelah penguatan, menunjukkan bahwa lebih banyak CIS Safeguard berhasil dipenuhi, terutama yang terkait dengan mekanisme manajemen kredensial, perluasan cakupan pengumpulan log, dan kontrol eksekusi untuk perangkat lunak dan skrip di lingkungan domain. Beberapa CIS Safeguard lainnya untuk validasi perangkat lunak, penguatan pengaturan otentikasi, dan cakupan *log audit* hanya diterapkan sebagian, sehingga tidak memenuhi standar CIS Controls v8.

Peningkatan terkait dengan perbaikan konfigurasi yang diterapkan melalui kebijakan GPO yang ditingkatkan. Kebijakan kata sandi dan parameter penguncian akun diperketat dalam kebijakan *Domain Default*, yang secara langsung berkontribusi pada peningkatan kepatuhan terhadap *Control* 5. Pembatasan hak administratif melalui pengaturan Grup Terbatas yang ditingkatkan mendukung kinerja *Control* 6 (*Access Control Management*). Penggunaan metode audit lanjutan seperti Sysmon dan *PowerShell Script Block Logging*, serta integrasi agen Wazuh sebagai sistem pemantauan terpusat, meningkatkan penerapan pengamanan dalam *Control* 8 (*Audit Log Mangement*) dan 13 (*Network Monitoring and Defense*). Selain itu, penerapan kebijakan eksekusi berbasis tanda tangan digital dan pembatasan sumber instalasi perangkat lunak melalui Applocker menghasilkan peningkatan kepatuhan terhadap Control 2, karena proses verifikasi skrip dan installer menjadi lebih konsisten.

Secara garis besar, hasil analisis kesenjangan menunjukkan bahwa kontrol perangkat lunak, manajemen akun, dan catatan audit mengalami peningkatan paling signifikan setelah proses penguatan konseptual. Serangkaian peningkatan ini berhasil memperbaiki implementasi langkah-langkah pengamanan yang sebelumnya hanya diterapkan secara parsial, sehingga menghasilkan perbaikan yang dapat diukur dan lebih sesuai dengan spesifikasi CIS Controls v8. Meskipun beberapa kebijakan masih memerlukan penyempurnaan lebih lanjut untuk mencapai kepatuhan optimal, hasil menunjukkan bahwa langkah-langkah penguatan tersebut efektif dan memiliki pengaruh positif terhadap postur keamanan Active Directory secara keseluruhan.

Status kepatuhan setiap CIS Control v8 ditentukan berdasarkan hasil evaluasi kebijakan keamanan Active Directory yang relevan. Suatu CIS Control dinyatakan

e-ISSN: 2548-6861

terpenuhi apabila seluruh parameter kebijakan yang menjadi ruang lingkup evaluasi menunjukkan status sesuai terhadap rekomendasi CIS Benchmark.Sebaliknya, apabila terdapat satu atau lebih parameter kebijakan yang tidak sesuai, maka CIS Control tersebut dinyatakan tidak terpenuhi. Penilaian persentase kepatuhan dilakukan dengan menghitung jumlah pengamanan yang terpenuhi dalam setiap kontrol, kemudian membaginya dengan jumlah total pengamanan yang dievaluasi dengan rumus seperti ini:

$$\text{Persentase Kepatuhan Control} = \frac{\text{Jumlah Safeguard Dipenuhi}}{\text{Jumlah Total Safeguard}} \times 100\%$$

Penggunaan persentase dan skor dalam penelitian ini bersifat deskriptif untuk menggambarkan tingkat pemenuhan kontrol, bukan sebagai analisis statistik.

Berdasarkan hasil *gap analysis* pada Tabel 13 dan aturan penentuan status kepatuhan yang telah dijelaskan sebelumnya, dilakukan perhitungan tingkat kepatuhan CIS Controls v8 pada dua kondisi, yaitu sebelum dan setelah penerapan rekomendasi hardening secara konseptual. Tabel 14 menunjukkan kondisi kepatuhan CIS Controls v8 sebelum penerapan rekomendasi *hardening* keamanan. Dari seluruh CIS Control yang relevan terhadap lingkungan Active Directory, hanya sebagian kecil kontrol yang dinyatakan terpenuhi berdasarkan hasil evaluasi kebijakan keamanan yang diterapkan. Kondisi ini menunjukkan bahwa kebijakan keamanan yang ada masih bersifat operasional dan belum sepenuhnya mengacu pada praktik terbaik keamanan sistem yang direkomendasikan oleh CIS.

TABEL 14. TABEL SKOR KEPATUHAN AWAL CIS CONTROLS V8 YANG MENGATUR ACTIVE DIRECTORY

CIS Control v8	***Poin Kepatuhan***	***Skor (%)***
Control 2 Inventory and Control of Software Assets	0/7	0%
Control 4 Secure Configuration of Enterprise Assets and Software	2/12	16.67%
Control 5 Account Management	1/6	16.67%
Control 6 Access Control Management	0/8	0%
Control 8 Audit Log Management	5/12	41.67%
Control 13 Network Monitoring and Defense	2/11	18.18%
	Rata-rata	15.53%

Pada temuan awal, tingkat kepatuhan saat berada di kisaran rendah. *Control* 2 (*Inventory and Control of Software Assets*) dan *Control* 6 (*Access Control Management*) masing-masing memiliki tingkat kepatuhan 0%. Hal ini menunjukkan bahwa mekanisme pengendalian perangkat lunak, termasuk pembatasan eksekusi skrip dan validasi instalasi, serta pengelolaan hak akses administratif belum diterapkan secara memadai. Hanya sebagian kecil dari langkah-langkah pengamanan yang dipenuhi oleh *Control* 4 dan 5, dengan skor masing-masing 16,67% dan 18,18%. Kontrol 8 memiliki skor tertinggi (41,67%), tetapi masih jauh di bawah tingkat ideal. Standar keamanan dasar sebelum perbaikan belum memenuhi standar CIS, seperti yang ditunjukkan oleh rata-rata keseluruhan sebesar 15,53%.

Tabel 15 menunjukkan kondisi kepatuhan CIS Controls v8 setelah penerapan konseptual rekomendasi *hardening* keamanan. Hasil evaluasi menunjukkan adanya peningkatan jumlah CIS Control yang terpenuhi dibandingkan dengan kondisi awal. Peningkatan ini menunjukkan bahwa penerapan rekomendasi kebijakan keamanan berdasarkan CIS Benchmark berpotensi meningkatkan tingkat kepatuhan dan memperkuat postur keamanan Active Directory.

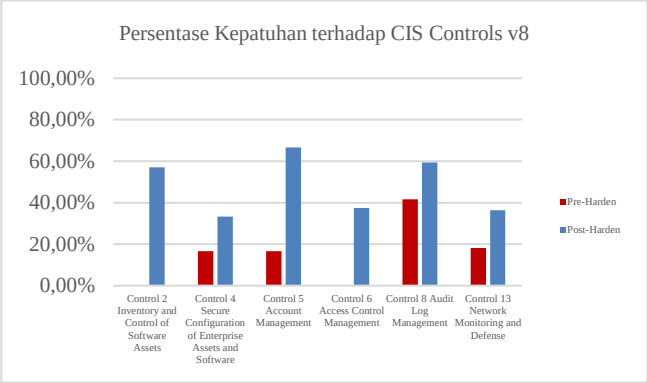
TABEL 15. TABEL SKOR KEPATUHAN CIS CONTROLS V8 PASCA-PENGUATAN

CIS Control v8	***Poin Kepatuhan***	***Skor (%)***
Control 2 Inventory and Control of Software Assets	4/7	57.14%
Control 4 Secure Configuration of Enterprise Assets and Software	4/12	33.33%
Control 5 Account Management	4/6	66.67%
Control 6 Access Control Management	3/8	37.50%
Control 8 Audit Log Management	7/12	58.33%
Control 13 Network Monitoring and Defense	4/11	36.36%
	Rata-rata	48.22%

Dari penialaian kepatuhan pada kondisi pasca-pernguatan, semua kontrol menunjukkan peningkatan kepatuhan. Setelah penerapan konseptual pembatasan instalasi perangkat lunak dan penguatan kebijakan eksekusi, *Control* 2 meningkat menjadi 57,14%. Berdasarkan simulasi penerapan rekomendasi dalam pengelolaan akun administratif dan kebijakan kata sandi, *Control* 5 meningkat menjadi 66,67%. Selain itu, *Control* 6 (37,50%), *Control* 8 (58,33%), dan *Control* 13 (36,36%) juga menunjukkan peningkatan. Konfigurasi kebijakan keamanan Active Directory telah mengalami peningkatan signifikan berdasarkan asumsi penerapan penuh rekomendasi, sebagaimana terlihat dari rata-rata keseluruhan yang naik menjadi 48,22% pada Tabel 15 berikut:

Interpretasi angka-angka diatas menunjukkan bahwa pengaturan Active Directory pertama tidak mengikuti CIS

Controls v8 dengan baik dan masih memiliki banyak celah keamanan. Namun, setelah mengikuti saran penguatan, tingkat kepatuhan meningkat secara signifikan, dengan peningkatan rata-rata lebih dari 30%. Gambar 13 dibawah ini menunjukkan grafik perbandingan antara sebelum dilakukan proses rancangan *hardening* dan setelahnya:



Gambar 13. Grafik Kepatuhan Active Directory terhadap CIS Controls v8

Hal ini menunjukkan bahwa perubahan yang dilakukan telah secara signifikan meningkatkan keamanan sistem, membuat pengelolaan akun lebih efektif, menambah jumlah informasi dalam log audit, dan membuat alat pemantauan keamanan bekerja lebih baik. Namun, beberapa langkah pengamanan belum terpenuhi, sehingga perlu diperkuat secara terus-menerus untuk mencapai tingkat kepatuhan yang lebih tinggi pada evaluasi berikutnya.

IV. KESIMPULAN

Berdasarkan hasil evaluasi kebijakan keamanan Active Directory yang dilakukan di lingkungan staging PT. XYZ Indonesia, dapat disimpulkan bahwa Active Directory telah dimanfaatkan untuk mendukung kebutuhan operasional *Security Operation Centre* (SOC) dan implementasi *Security Information and Event Mangement* (SIEM), khususnya melalui penerapan kebijakan terpusat menggunakan *Group Policy Object* (GPO) untuk distribusi agen, dukungan instalasi perangkat lunak, dan manajemen konfigurasi sistem. Namun, hasil evaluasi kepatuhan terhadap CIS Benchmark dan CIS Controls v8 menunjukkan bahwa tidak semua kebijakan keamanan yang diterapkan telah memenuhi rekomendasi standar yang ditetapkan. Beberapa konfigurasi masih menggunakan pengaturan *default* atau memberikan fleksibilitas yang signifikan untuk mendukung kebutuhan operasional, yang mengakibatkan celah dalam prinsip konfigurasi aman dan prinsip hak akses minimalis.

Pemetaan kebijakan keamanan Active Directory terhadap CIS Controls v8 menunjukkan bahwa beberapa kebijakan yang diterapkan telah berkontribusi dalam mendukung beberapa kontrol keamanan, terutama yang terkait dengan manajemen akses, konfigurasi sistem, dan audit aktivitas. Namun, masih ada kontrol CIS yang belum sepenuhnya dipenuhi akibat keterbatasan dalam implementasi konfigurasi teknis melalui GPO. Selain itu, mekanisme implementasi agen keamanan Wazuh dan perangkat lunak pendukung secara terpusat melalui GPO dianggap efektif dalam mendukung operasi sistem, tetapi berpotensi menimbulkan risiko keamanan jika tidak disertai dengan hak akses yang memadai dan pengaturan audit yang tepat.

Berdasarkan temuan ini, studi ini menghasilkan rekomendasi untuk meningkatkan kebijakan keamanan Active Directory, yang disusun dengan merujuk pada prosedur remediasi CIS Benchmark, dengan tujuan meningkatkan tingkat kepatuhan konfigurasi keamanan tanpa mengganggu kebutuhan operasional sistem yang ada. Secara keseluruhan, studi ini menunjukkan bahwa pendekatan evaluasi kebijakan keamanan Active Directory berdasarkan CIS Benchmark dan CIS Controls v8 dapat digunakan sebagai metode sistematis dan terukur untuk menilai kesiapan konfigurasi keamanan layanan direktori, sekaligus membantu organisasi mengidentifikasi risiko potensial dan merencanakan perbaikan keamanan sistem yang lebih terarah.

Hasil analisis kesenjangan menunjukkan bahwa rekomendasi perbaikan yang dirumuskan berdasarkan, berpotensi meningkatkan tingkat kepatuhan Active Directory terhadap CIS Controls v8 secara signifikan. Perbandingan antara kondisi awal dan kondisi setelah perbaikan secara konseptual memperlihatkan peningkatan rata-rata kepatuhan dari 15,53% menjadi 48,22%, yang menunjukkan bahwa pendekatan evaluatif berbasis standar mampu memberikan dampak positif terhadap postur keamanan Active Directory.

UCAPAN TERIMA KASIH

Penulis ingin mengucapkan terima kasih kepada bapak Andy Triwinarko selaku pembimbing. Terima kasih banyak atas bimbingan, arahan, dan masukan yang diberikan selama proses penelitian dan penulisan. Ucapan terima kasih juga disampaikan kepada para penguji atas saran dan kritik yang membangun, serta kepada PT. XYZ Indonesia atas dukungan dan penyediaan lingkungan penelitian yang diperlukan. Ucapan terima kasih juga disampaikan kepada semua pihak yang telah membantu secara langsung maupun tidak langsung sehingga penelitian ini dapat diselesaikan dengan baik dan diharapkan dapat berkontribusi pada pengembangan kebijakan keamanan sistem informasi, khususnya dalam lingkungan Active Directory.

e-ISSN: 2548-6861

DAFTAR PUSTAKA

[1] G. M. Taberima and D. Ramayanti, "MENGOPTIMALKAN MANAJEMEN DAN KEAMANAN TI MELALUI IMPLEMENTASI LAYANAN DOMAIN ACTIVE DIRECTORY: STUDI KASUS PADA INFRASTRUKTUR TI PERUSAHAAN," vol. 6, no. 1, 2024.

[2] A. Nabillah, M. Rifqi, and S. Maesaroh, "IMPLEMENTASI KEBIJAKAN GRUP POLICY UNTUK MITIGASI RISIKO KEAMANAN PADA SERVER DI PT XYZ," vol. 9, no. 1, 2025.

[3] R. Sasidharan, "A Case Study to Implement Windows System Hardening using CIS Controls," *Int. J. Comput. Trends Technol.*, vol. 70, no. 7, pp. 1–7, Jul. 2022, doi: 10.14445/22312803/IJCTT-V70I7P101.

[4] NSA and CISA, "NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations," Cybersecurity and Infrastructure Security Agency, Oct. 2023. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-278a

[5] I. Tyshyk, "ENSURING THE SECURITY OF CORPORATE USERS ACCOUNTS," *Cybersecurity Educ. Sci. Tech.*, pp. 214–225, 2023, doi: 10.28925/2663-4023.2023.22.214225.

[6] A. W. Firmansyah, R. D. Marcus, A. S. Ilmananda, and F. Y. Pamuji, "Manajemen Akun Pengguna Berbasis Roaming Profile untuk Memperkuat Perlindungan Data di Laboratorium Komputer," *SMATIKA J.*, vol. 12, no. 02, pp. 255–264, Dec. 2022, doi: 10.32664/smatika.v12i02.688.

[7] N. C. Iyer, A. M. Kabbur, and H. G. Wali, "Implementation of Active Directory for efficient management of networks," *Procedia Comput. Sci.*, vol. 172, pp. 112–114, 2020, doi: 10.1016/j.procs.2020.05.016.

[8] D. Goel, M. Ward, A. Neumann, F. Neumann, H. Nguyen, and M. Guo, "Hardening Active Directory Graphs via Evolutionary Diversity Optimization based Policies," *ACM Trans. Evol. Learn. Optim.*, p. 3688401, Aug. 2024, doi: 10.1145/3688401.

[9] R. Mahajan, D. M. Mahajan, and D. D. Singh, "Window azure Active Directory Services for Maintaining Security & Access Control".

[10] F. Raheman, "From Standard Policy-Based Zero Trust to Absolute Zero Trust (AZT): A Quantum Leap to Q-Day Security," *J. Comput. Commun.*, vol. 12, no. 03, pp. 252–282, 2024, doi: 10.4236/jcc.2024.123016.

[11] N. Sadikin and M. Sari, "Implementasi Password Policy pada Domain Security Policy Group Policy Object (GPO) Active Directory Domain Services untuk Keamanan Jaringan di Windows Server," *Jurnal Maklumatika*, vol. 10, no. 1, pp. 1–9, Jan. 2023.

[12] T. S. Putri, N. M. Mutiah, and D. P. Prawira, "ANALISIS MANAJEMEN RISIKO KEAMANAN INFORMASI MENGGUNAKAN NIST CYBERSECURITY FRAMEWORK DAN ISO/IEC 27001:2013 (Studi Kasus: Badan Pusat Statistik Kalimantan Barat)," *Coding J. Komput. Dan Apl.*, vol. 10, no. 02, p. 237, Oct. 2022, doi: 10.26418/coding.v10i02.54972.

[13] V. Mahendra and B. Soewito, "Penerapan Kerangka Kerja NIST Cybersecurity dan CIS Controls sebagai Manajemen Risiko Keamanan Siber," *Techno.Com*, vol. 22, no. 3, pp. 527–538, Aug. 2023, doi: 10.33633/tc.v22i3.8491.

[14] M. A. Jauhari, B. A. Wardijono, and E. Hegarini, "Pengukuran Kematangan Keamanan Siber pada Perusahaan Teknologi Informasi dengan Framework Center for Internet Security Controls," *J. SAINTEKOM*, vol. 14, no. 1, pp. 72–83, Mar. 2024, doi: 10.33020/saintekom.v14i1.610.

[15] M. Najib, B. Purnomosidi D.P, and M. A. Nugroho, "IMPLEMENTASI SECURITY AUDITOR UNTUK STANDARDISASI INSTALASI SERVER PADA LAYANAN SAAS MENGGUNAKAN CIS BENCHMARK," *Cyber Secur. Dan Forensik Digit.*, vol. 5, no. 2, pp. 83–88, Jan. 2023, doi: 10.14421/csecurity.2022.5.2.3929.

[16] M. A. Zein, U. Y. K. S. Hediyanto, and A. Almaarif, "HARDENING SISTEM OPERASI VIRTUAL PRIVATE SERVER FAKULTAS REKAYASA INDUSTRI BERDASARKAN NIST SP 800- 123," *JIPI J. Ilm. Penelit. Dan Pembelajaran Inform.*, vol. 8, no. 1, pp. 230–241, Feb. 2023, doi: 10.29100/jipi.v8i1.3438.

[17] R. R. Fakhry, "Penerapan Keamanan Server dengan Teknik Hardening pada Sistem Operasi Ubuntu Server," Apr. 2021, [Online]. Available: http://eprints.ums.ac.id/id/eprint/90707

[18] F. Fiantika *et al.*, *Metodologi Penelitian Kualitatif*. PT. GLOBAL EKSEKUTIF TEKNOLOGI, 2022.