Monas: Jurnal Inovasi Aparatur
Vol. 5 No. 1 (2023): 56-67
e-ISSN 2656-0194

STRATEGI PEMIMPIN GENERASI Z DALAM MENGELOLA ETHICAL HACKER PADA COMMUNITY META4SEC DI INDONESIA

THE STRATEGY OF GENERATION Z LEADERS IN MANAGING ETHICAL HACKER IN THE META4SEC COMMUNITY IN INDONESIA

Ratih Damayanti[1,*], Andrie Yuswanto[2,*], Farras Givari[3]
[1]Akademi Televisi Indonesia, Jl Daan Mogot No.11 Kedoya Utara Kb. Jeruk Jakarta Barat, 11520
[2]Institut Teknologi Budi Utomo, Jl. Mawar Merah No.23 Pd. KopiDuren Sawit Jakarta Timur, 13460
[3]Redlimit.id, Jl Rawakuning No.7 Pulogebang Jakarta Timur, 13950

*ratileea@gmail.com

ABSTRAK

Penelitian ini bertujuan untuk mengetahui bagaimana strategi seorang Pemimpin muda Generasi Z (Gen-Z) dapat membantu mewujudkan tujuan komunitas yang mengacu pada visi misi organisasi, serta didapatkan informasi bagaimana semua unsur dalam komunitas dapat bersinergi, berkolaborasi dalam mengembangkan ethical hacker pada komunitas hacker. Metode penelitian dilakukan dengan menggunakan metode kualitatif, yaitu in depth interview yang merupakan wawancara mendalam yang melibatkan interaksi satu lawan satu antara peneliti dan responden. Wawancara dilakukan terhadap satu orang manajer komunitas, satu orang pendiri, dan tiga orang member komunitas, pada unit analisis komunitas Meta4sec. Penelitian ini menemukan bahwa kepemimpinan karakter Gen-Z merupakan generasi yang memiliki kesenangan untuk bekerja secara kolaboratif dan menghargai pendekatan tim dalam menyelesaikan masalah dan mendapatkan solusi. Gaya kepemimpinan kolaboratif ini meliputi kemampuan mendengarkan, mengajak anggota tim terlibat, menstimulasi kontribusi dari semua anggota yang aktif, dan membangun lingkungan komunitas yang positif dan inklusif dan menjawab masalah terkait kurangnya pengalaman manajemen, perbedaan generasi, kesulitan dalam berkomunikasi dan bekerja sama, sehingga terbukti efektif membuat komunitas ini semakin hari semakin berkembang. Melalui penelitian ini, terlihat bahwa manajemen dan strategi yang di lakukan komunitas Meta4sec mampu bertahan dan menarik banyak member baru untuk belajar dan konsultasi terkait ethical hacker secara mudah.

Kata kunci: *kepemimpinan, ethical hacker, komunitas, manajemen*

ABSTRACT

This study aims to find out how the strategies of a young Generation Z (Gen-Z) leader can help realize community goals that refer to the vision and mission of the organization, as well as obtain information on how all elements in the community can work together and collaborate in developing ethical hackers in the hacker community. The research method was carried out using qualitative methods, namely in-depth interviews which are in-depth interviews involving one on one interaction between the researcher and the respondent. Interviews were conducted with one community manager, one founder, and three community members, in the Meta4sec community analysis unit. This research found that Gen-Z character leadership is a generation that has the pleasure to work collaboratively and appreciates a team approach in solving problems and getting solutions. This collaborative leadership style includes the ability to listen, get team members involved, stimulate contributions from all active members, and build a positive and inclusive community environment and answer problems related to lack of management experience, generational differences, difficulties in communicating and working together, so that it proves to be effective make this community growing day by day. Through this research, it can be seen that the management and strategies carried out by the Meta4sec community are able to survive and attract many new members to easily learn and consult regarding ethical hackers.

***Keywords**: leadership, ethical hacker, community, management*

PENDAHULUAN

Pemimpin muda di bidang keamanan siber dapat memainkan peran penting dalam membentuk masa depan keamanan digital, karena pemimpin muda dalam keamanan siber harus memiliki dasar yang kuat dalam keterampilan teknis. Ini termasuk pengetahuan tentang bahasa pemrograman, jaringan, algoritma enkripsi, kerentanan sistem, dan teknologi baru. Penelitian Ojogiwa (2021) menunjukan bahwa kepemimpinan strategis merupakan dimensi manajemen strategis yang memiliki hubungan positif dengan efektivitas organisasi /komunitas. Tetap mengikuti tren dan ancaman keamanan siber terbaru sangat penting. Penelitian Kohnová et al. (2021) menemukan bahwa anak muda Generasi Z dinilai sangat baik, terutama dalam kemampuan mereka mempelajari hal-hal baru, kreativitas mereka, dan tingkat keterampilan mereka dalam aplikasi / layanan online, karena kemampuan ini penting untuk kesuksesan bisnis di masa depan. Generasi Z, lahir 1996-2010 atau iGeneration selalu memiliki akses instan ke internet, Ipod, dan iPhone untuk mengambil dan mengirimkan informasi yang dapat memberikan pengaruh kuat pada gaya belajar mereka (Nicholas, 2020). Pada organisasi keamanan sangat mengandalkan kerja tim para ahli dan mereka bekerja sama di bawah tekanan tinggi, harus bereaksi secepat mungkin untuk melindungi aset dan data organisasi (Hámornik & Krasznay, 2017).

Pemanfaatan teknologi informasi, media dan komunikasi menjadi salah satu faktor yang mendorong perubahan perilaku masyarakat maupun peradaban manusia dalam menumbuhkan inovasi disruptif. Kemajuan teknologi, secara tidak langsung memberikan gambaran bahwa era Society 5.0 era akan menggantikan Industry 4.0 yang akan segera berakhir, cyber crime atau kejahatan siber telah ikut berevolusi dengan menggunakan pola pendekatan interaksi social engineering yang akan berpotensi merugikan banyak pihak. Society 5.0 adalah era teknologi modern dengan mengandalkan manusia sebagai komponen utamanya (Widmann & Mulder, 2020). Sehingga, konsekuensi logis dari kondisi ini menempatkan teknologi informasi menjadi "pedang bermata dua." Karena selain memberikan kontribusi bagi peningkatan proses bisnis dan kemajuan dalam memberikan pelayanan buat masyarakat, teknologi informasi juga menjadi sarana yang efektif bagi perbuatan melawan hukum di dunia maya yang termasuk dalam *cyber crime*.

Cybersecurity adalah bidang yang berkembang pesat, dengan ancaman baru muncul secara teratur. *Cyber Security* mencakup perlindungan sistem, program, data, dan jaringan dari ancaman cyber-crime dan *cyber defence* sangat mengandalkan performan tim (Yuswanto, 2023). Insiden keamanan informasi semakin meningkat jumlahnya dan semakin beragam dan merusak serta mengganggu ketersediaan layanan (Firmansyah & Yuswanto, 2022). Seorang pemimpin muda harus memiliki hasrat untuk belajar dan terbuka untuk perbaikan diri terus menerus. Mengejar sertifikasi, menghadiri konferensi, dan berpartisipasi dalam komunitas keamanan siber dapat membantu meningkatkan pengetahuan dan keahlian. *Cybersecurity* adalah perhatian global, dan para pemimpin muda di bidang ini harus memiliki perspektif yang luas. Keamanan dunia maya telah menjadi salah satu prioritas terbesar bagi bisnis dan pemerintah, memperkuat kepemimpinan strategis adalah aspek kunci dalam memastikan visi keamanan siber tercapai (Lehto & Limnéll, 2021). Mereka harus mengetahui kebijakan, peraturan, dan standar keamanan dunia maya internasional. Berkolaborasi dengan pakar dari berbagai negara dan memahami tantangan keamanan siber global dapat menghasilkan solusi yang lebih efektif.

Memahami risiko merupakan hal mendasar dalam kepemimpinan keamanan siber. Pemimpin muda harus terampil dalam penilaian risiko, pemodelan ancaman, dan menerapkan kontrol keamanan yang sesuai. Mereka harus dapat menyeimbangkan kebutuhan keamanan dengan tujuan bisnis dan memberikan panduan tentang strategi mitigasi risiko. Meskipun keahlian teknis itu penting, keterampilan kepemimpinan dan manajemen sama pentingnya bagi seorang pemimpin muda. Ini termasuk pengambilan keputusan yang efektif, pemecahan masalah, pemikiran strategis, pembangunan tim, dan pendampingan. Seorang pemimpin yang kuat

menginspirasi dan memotivasi timnya untuk mencapai tujuan keamanan siber bersama.

Lanskap keamanan siber terus berkembang, menuntut para pemimpin untuk menjadi inovatif dan mudah beradaptasi. Merangkul teknologi baru, seperti kecerdasan buatan, pembelajaran mesin, dan blockchain, dapat membantu menciptakan solusi keamanan tingkat lanjut. Seorang pemimpin muda harus terbuka terhadap ide dan pendekatan baru sambil tetap memperhatikan tren masa depan. Pemimpin muda dalam keamanan siber dapat membuat perbedaan dengan mengadvokasi praktik keamanan siber yang kuat dan meningkatkan kesadaran di antara individu, organisasi, dan pembuat kebijakan. Mendidik orang lain tentang keamanan online, ancaman dunia maya, dan praktik terbaik dapat berkontribusi pada lingkungan digital yang lebih aman. Integritas pribadi, menunjukkan standar etika yang tinggi, kepercayaan dan kredibilitas sangat penting dalam bidang ini, dan pemimpin harus bertindak secara bertanggung jawab, menjaga kerahasiaan, dan memprioritaskan kesejahteraan tim dan pemangku kepentingan mereka. Dengan mewujudkan kualitas-kualitas ini, seorang pemimpin muda dapat memberikan kontribusi yang signifikan di bidang keamanan siber dan membantu membentuk masa depan digital yang aman dan tangguh.

Dalam buku *The Ethics of Cybersecurity*, Christen et al. (2020) menye butkan bahwa pemimpin keamanan siber harus mematuhi kerangka etika yang kuat karena menjadi sangat diperlukan untuk melindungi kepercayaan dan keyakinan dalam infrastruktur digital sebagai nilai-nilai fundamental, kebebasan, atau privasi. Mereka harus memprioritaskan melindungi privasi data, menghormati hak pengguna, dan mempromosikan praktik yang bertanggung jawab. Pengambilan keputusan yang etis sangat penting saat menangani kerentanan, pengungkapan insiden keamanan, dan menangani informasi sensitif. Hasil penelitian Yuswanto et al. (Yuswanto et al., 2023) menemukan bahwa gaya kepemimpinan berpengaruh langsung signifikan terhadap *Persistence* dan *Integrity*, Komunikasi yang efektif sangat penting bagi seorang pemimpin di bidang apa pun. Pemimpin keamanan siber harus mampu menyampaikan konsep teknis yang kompleks dengan cara yang jelas dan mudah dipahami kepada pemangku kepentingan teknis dan non-teknis. Kolaborasi dengan tim lain, seperti TI, hukum, dan manajemen, sangat penting untuk menerapkan strategi keamanan siber yang efektif. Pemimpin Generasi Z tumbuh di era di mana kemajuan teknologi dimulai, dan mereka dapat mengakses informasi yang mudah dan cepat melalui alat teknologi, seperti Internet dan smartphone. Generasi Z adalah ahli teknologi yang dibentuk oleh puncak teknologi, dan individualistis, bisnis online, dan multitasker. Mereka suka bekerja secara kolaboratif dengan otonomi pribadi di tempat kerja yang fleksibel yang memungkinkan keseimbangan kehidupan kerja dan kerja etis, dan mereka membutuhkan pemantauan dan umpan balik di tempat kerja (Bulut & Maraba, 2021)

Ethical hacker atau peretas etis' sering diidentikkan dengan peretas yang mematuhi kode etik yang mengutamakan nilai-nilai ramah bisnis (Jaquet-Chiffelle & Loi, 2020). Fungsi komunitas *ethical hacker* adalah menggunakan keterampilan dan pengetahuan mereka tentang sistem komputer dan keamanan jaringan untuk membantu melindungi dan meningkatkan keamanan komunitas atau organisasi. Pentingnya *cybersecurity* dan penggunaan teknik hacking etis untuk perlindungan data pengguna melalui karakterisasi standar dan teknik yang ditetapkan secara global dapat diterapkan pada organisasi untuk meminimalisir kemungkinan ancaman dunia maya sambil memastikan perlindungan data pengguna (Hawamleh et al., 2020). *Ethical hacker*, juga dikenal sebagai peretas "*white hat*", adalah individu yang diberi wewenang dan dipercaya untuk mengidentifikasi kerentanan dalam sistem komputer, jaringan, dan aplikasi perangkat lunak, dengan tujuan membantu mencegah akses tidak sah, pelanggaran data, dan insiden keamanan lainnya. Komunitas *ethical hacker* biasanya terlibat dalam berbagai aktivitas untuk memenuhi fungsinya, antara lain : (1) Penilaian Kerentanan: Mereka menilai sistem dan jaringan komputer untuk mengidentifikasi potensi kelemahan dan kerentanan keamanan. Ini mungkin melibatkan melakukan audit keamanan menyeluruh, pengujian penetrasi, dan pemindaian kerentanan. (2) Pengujian

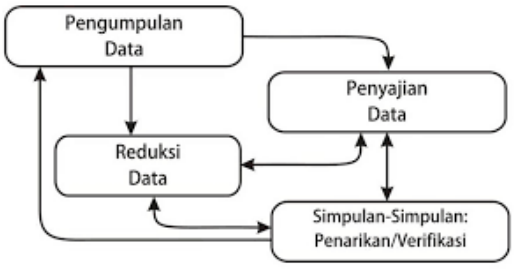
Penetrasi: Mereka mencoba untuk mengeksploitasi kerentanan yang teridentifikasi dalam lingkungan yang terkendali untuk menentukan sejauh mana potensi kerusakan yang dapat ditimbulkan oleh penyerang. Ini membantu organisasi memahami celah keamanan mereka dan memprioritaskan upaya perbaikan. (3) Konsultasi Keamanan: Mereka memberikan saran dan panduan ahli kepada organisasi untuk meningkatkan postur keamanan mereka secara keseluruhan. Ini mungkin termasuk merekomendasikan praktik terbaik keamanan, menerapkan kontrol dan kebijakan keamanan, dan melakukan program pelatihan kesadaran karyawan. (4) Tanggapan Insiden: Jika terjadi insiden atau pelanggaran keamanan, peretas etis dapat terlibat dalam menyelidiki pelanggaran, menganalisis dampaknya, dan membantu dalam proses pemulihan. Mereka bekerja sama dengan tim tanggap insiden untuk menahan dan mengurangi kerusakan yang disebabkan oleh insiden tersebut. (5) Kesadaran dan Pendidikan Keamanan: Peretas etis memainkan peran penting dalam meningkatkan kesadaran tentang keamanan dunia maya di kalangan masyarakat. Mereka sering mengadakan lokakarya, sesi pelatihan, dan kampanye kesadaran untuk mendidik individu dan organisasi tentang ancaman keamanan umum, praktik online yang aman, dan pentingnya tindakan keamanan yang kuat. (6) Pengungkapan yang Bertanggung Jawab: Ketika peretas etis menemukan kerentanan keamanan, mereka mengikuti praktik pengungkapan yang bertanggung jawab dengan melaporkan temuan tersebut ke organisasi atau vendor perangkat lunak yang terpengaruh. Ini memungkinkan organisasi untuk mengatasi kerentanan dan merilis tambalan atau pembaruan untuk melindungi penggunanya. Secara keseluruhan, peretas etis komunitas berkontribusi pada ekosistem keamanan siber dengan mengidentifikasi kerentanan secara proaktif, membantu organisasi memperkuat pertahanan keamanan mereka, dan mempromosikan lingkungan digital yang lebih aman bagi komunitas.

Objek Penelitian ini adalah Pemimpin sekaligus *community manager* dari komunitas Meta4sec yang keseluruhan aktivitas manajemen komunikasinya dikelola dan dipimpinnya, *Founder* atau Pendiri komuniti Meta4sec dan 3 anggota komunitas yang aktif. Gen-Z memiliki pemahaman teknologi yang lebih baik, mereka mungkin menghadapi beberapa tantangan dalam mengelola ethical hacker dalam komunitas. Berikut adalah beberapa masalah yang mungkin muncul, antara lain : Bebeberapa masalah terjadi antara lain kurangnya pengalaman manajemen, perbedaan generasi, kesulitan dalam berkomunikasi dan bekerja sama serta cara mengelola komunitas ethical hacker dengan efektif.

Penelitian ini bertujuan untuk mengetahui bagaimana strategi Pemimpin muda Generasi Z untuk dapat membantu mewujudkan tujuan komunitas Meta4sec yang mengacu pada visi misi organisasi, dengan cara mencari informasi bagaimana semua unsur dalam komunitas dapat bersinergi, berkolaborasi dalam mengembangkan komunitas ethical hacker community melalui Meta4sec.

METODOLOGI

Penelitian dilakukan dengan menggunakan metode kualitatif, yaitu *in depth interview*. *In depth interview* adalah wawancara mendalam yang melibatkan interaksi satu lawan satu antara peneliti dan responden. Penelitian dilakukan dengan wawancara yang panjang dan mendalam dengan responden secara rinci pengalaman, pandangan, persepsi, makna yang terkait dengan topik penelitian dan interaksi langsung antara peneliti dengan respoden melalui pertanyaan dan jawaban yang lebih terbuka.



Gambar 1. Teknik Analisi Data Kualitatif

(Felinda & Sugiyono, 2018)

Teknik analisis data penelitian dalam analisis kualitatif memiliki empat tahap yaitu pengumpulan data, reduksi data, penyajian data dan langkah terakhir adalah penarikan kesimpulan dan verifikasi.

Objek wawancara dalam penelitian ini adalah satu orang *Community Manager* Meta4sec, satu orang pendiri Pendiri dan tiga

orang member dari komunitas Meta4sec. Pertanyaan disusun untuk terkait kepemimpinan terhadap visi dan misinya serta dan bagaimana strategi yang dilakukan untuk mensinergikan semua unsur di dalam komunitas agar mampu berkolaborasi. Komunitas Meta4sec dipimpin oleh Generasi (Gen Z) anak muda yang memiliki ketertarikan terhadap *Cybersecurity*.

Perencanaan awal dilakukan yakni menentukan tujuan penelitian, mengidentifikasi responden yang tepat sesuai karakteristik dan tujuan penelitian kemudian menentukan metode wawancara yang sesuai. Pertanyaan disusun secara terstruktur berdasarkan kerangka konseptual dari beberapa teori yang relevan dan tinjauan dari literatur sebelumnya untuk dikembangkan sehingga memperoleh kebaruan.

Dalam buku "*Qualitative Interviewing: The Art of Hearing Data*" Rubin, (2011) membahas tentang teknik wawancara sebagai metode bagi peneliti untuk memperoleh informasi yang lebih mendalam dan holistik dari responden melalui proses pendengaran yang cermat.

Desain penelitian kuantitatif dan kualitatif untuk menyelidiki fenomena yang menarik yang tujuannya adalah untuk memberikan gambaran umum tentang penelitian kualitatif dan penjelasan analisis isi yang akurat dan dapat dipahami serta aplikasi potensialnya, misalnya, dalam tinjauan literatur sistematis dan pengembangan teori (Kyngäs, 2020),

Pertanyaan untuk *Community Manager* adalah sebagai berikut :

1. Bagaimana anda mendeskripsikan tugas anda sebagai *Community Manager*?
2. Apa tanggung jawab utama anda dalam tugas ini?
3. Bagaimana cara Anda membangun dan memelihara komunitas *online* yang aktif dan terlibat?
4. Apa strategi atau taktik yang akan Anda gunakan?
5. Bagaimana Anda akan mengukur keberhasilan atau dampak dari upaya Anda dalam mengelola komunitas?
6. Apa indikator yang akan Anda gunakan untuk keberhasilan Anda sebagai *community manager*?
7. Bagaimana Anda akan menangani konflik atau masalah dalam komunitas?
8. Apa pendekatan Anda dalam mengelola situasi yang mungkin kontroversial atau memicu perselisihan jika terjadi diskusi online?
9. Bagaimana Anda akan berinteraksi dengan anggota komunitas secara individu?
10. Bagaimana Anda akan merespons pertanyaan, umpan balik, atau keluhan yang diajukan oleh anggota komunitas?
11. Bagaimana Anda akan mempromosikan kolaborasi dan keterlibatan anggota komunitas?
12. Apa langkah-langkah konkret yang Anda ambil untuk mendorong partisipasi aktif dari anggota komunitas?
13. Bagaimana cara Anda menggunakan media sosial dan platform lainnya untuk memperluas jangkauan komunitas?
14. Apa strategi Anda dalam membangun dan mempertahankan kehadiran yang kuat di platform-platform tersebut?
15. Bagaimana Anda akan mengelola konten yang dibagikan oleh anggota komunitas?
16. Apakah ada kebijakan atau pedoman yang akan Anda terapkan dalam hal ini?
17. Bagaimana Anda akan berkolaborasi dengan tim internal?
18. Bagaimana Anda akan terus memperbarui pengetahuan Anda tentang tren, perubahan, atau inovasi terbaru?
19. Apa langkah-langkah yang Anda ambil untuk tetap diperbarui dengan praktik terbaik dalam bidang ini?

Pertanyaan untuk Pendiri komunitas adalah sebagai berikut :

1. Bagaimana ide awal Anda untuk memulai komunitas *Hacker* ini?
2. Apa yang memotivasi Anda dalam memulai komunitas *Hacker* ini?
3. Bagaimana Anda mendefinisikan "*Hacker*" ?
4. Apa saja aktivitas dan acara yang sering diadakan oleh komunitas *Hacker*?
5. Bagaimana komunitas *Hacker* membantu anggotanya dalam pengembangan keterampilan dan pengetahuan?

6. Motivasi apa yang anda berikan terhadap kepemimpinan *manager community*?
7. Ketrampilan manajerial apa yang anda bekali untuk memberikan kepercayaan diri pemimpin *manager community* ini?
9. Apa yang menjadi pertimbangan anda untuk memilih pemimpin muda sebagai *manager community*?
10. Bagaimana Anda mencari dan merekrut anggota baru untuk bergabung dengan komunitas *Hacker*?
11. Bagaimana Anda memastikan bahwa anggota komunitas *Hacker* tetap aktif dan terlibat dalam kegiatan komunitas?

Pertanyaan untuk anggota komunitas adalah sebagai berikut :

1. Bagaimana anda menemukan komunitas Meta4sec?
2. Darimana Anda mendapatkan informasi tentang komunitas ini?
3. Apakah Anda selalu mengikuti setiap kegiatan *online* dan *offline* yang diadakan oleh komunitas ini?
4. Bagaimana cara kepemimpinan anak muda dalam komunitas ini?
5. Apa yang membuat Anda merasa yakin dengan kapabilitas *community manager* di komunitas ini?
6. Apa yang Anda harapkan dari komunitas ini ke depan?
7. Apa yang membuat Anda tertarik dengan konsep "*Hacker"*, dan bagaimana Anda mendefinisikan hal itu?
8. Apakah Anda akan menginformasikan *community* ini kepada teman atau rekanan anda yang memiliki ketertarikan yang sama?
9. Bagaimana Anda memandang peran dan kontribusi komunitas *Hacker* terhadap masyarakat luas?
10. Bagaimana mengukur keberhasilan komunitas menurut Anda?

Pertanyaan akan disampaikan dalam bentuk wawancara atau interview selama 1 (satu) bulan dari tanggal 22 Mei 2023 sampai dengan 22 Juni 2023. Selanjutnya ditranskripsikan dalam bentuk teks tertulis. Selanjutnya akan didefinisikan dengan mengekstraksi dari tema, tren dan perspektif yang didapat dari hasil wawancara tersebut.

HASIL DAN PEMBAHASAN

Analisis kualitatif dilakukan berdasarkan empat tahap yaitu pengumpulan data, reduksi data, penyajian data dan langkah terakhir adalah penarikan kesimpulan dan verifikasi. Berdasarkan hasil dari data yang dipeloleh diketahui bahwa komunitas ini berdiri pada 17 Agustus 2000 yang digeraki oleh sekelompok anak muda millenial yang memiliki peminatan sama, yaitu bidang *Cybersecurity* dan *ethical hacking*. Meta adalah sebuah kata yang berasal dari bahasa Yunani kuno yang berarti melebihi (*beyond),* dan Meta juga merupakan singkatan dari "*Most Effective Tactics Available*" merupakan istilah yang kerap digunakan dalam dunia game, terutama game yang memiliki element kompetitif, dimana seorang pemain akan menggunakan strategi terbaik untuk menang. Sedangkan angka 4 (empat) merupakan jumlah pendiri dan *Sec* merupakan kepanjangan dari *Security*. *Tagline* ini menyesuaikan dengan semangat yang ada dalam diri pengelola komunitas ini untuk menjadi media komunikasi, media belajar media bertukar informasi dan berbagi informasi seputar *ethical hacking.*

Meta4sec memiliki misi, Mengelola komunitas dalam media digital dengan anggota yang beragam karakter namun didominasi oleh *millenial* dan dipimpin pula oleh millenial menjadi sesuatu yang menarik. Penelitian ini akan menjelaskan tentang kepemimpinan millenial Gen-Z dalam mengelola komunitas virtual pada platform media digital berdasarkan hasil wawancara.

Ternyata dalam pengelolaan komunitas Meta4sec dibutuhkan manajemen yang sesuai dengan selera dari anak muda yang berada dalam komunitas tersebut. Millenial dalam kelompok discord ternyata rata-rata berusia sekitar 16 sd 30 tahun dan komunitas ini di manajeri oleh anak muda berusia 15 tahun. Pengelolaan manajemen komunikasi melalui discord (chat group) dilakukan dengan cara, menyusun jadwal virtual meeting yang dibuat dengan rentang waktu 1 kali dalam seminggu. Pertemuan dilakukan dengan mengangkat berbagai isu menarik seputar IT Security. Memilih discord

karena aktivitas yang multitasking dan fleksibel, membuat discord dapat menjadi pilihan yang paling fleksibel. Didukung oleh hasil penelitian Arifianto & Izzudin (2021) menunjukkan bahwa sebagian besar peserta mengkonfirmasi bahwa Discord adalah media alternatif yang disukai karena antarmuka pengguna yang menarik, kelengkapan fitur, dan kemudahan penggunaan. Keterbaruan dalam mencari dan mendapatkan topik juga memiliki pengaruh besar terhadap intensitas dan loyalitas para membernya. Dengan jumlah member 2200 (Update tanggal 19 Juni 2022) personil tentunya komunitas ini harus dapat dikelola secara stratejik. Manajer Komunitas dalam discord meta4sec dipimpin oleh Gen-Z yang memiiliki talenta besar di bidang security, namun dalam mengelola komunitas juga diperlukan kemahiran memilih topik dan memberikan tawaran menarik yang memberikan manfaat dan keuntungan bagi membernya.

Berdasarkan hasil wawancara dengan *Community Manager* Meta4sec, yang dilakukan, terdapat beberapa langkah konkrit yang dilakukan tara lain rutin mengadakan pertemuan secara online maupun offline. Mengadakan pertemuan offline melalui aktivitas meet up yang dilakukan secara continuity, dengan menawarkan tema yang menarik yang berkenaan dengan topik *ethical hacker, cyber security* dan isu nyata yang sedang berkembang melalui diskusi dengan mengundang narasumber praktisi bidang yang relevan, dan memberikan kuis dengan *gift away* dan souvenir yang tematik untuk dapat mempererat relasi komunitas. Bina komunitas djuga dilakukan dengan diskusi yang dilakukan harian maupun mingguan lewat acara live streaming. Diskusi yang berjalan dikondisikan sangat informal dan akrab oleh manajer discord Meta4sec yang juga berperan menjadi moderator. Terkadang aktivitas ethical hacking dari member yang telah berhasil menemukan bug bounty menjadi diskusi yang bermanfaat bagi para member lain yang rata-rata dari Gen-Z, hal ini merupakan bentuk sebagai ruang berbagi informasi untuk member yang lain. Disini terlihat betapa Gen-Z dalam berkomuniti mereka menumbuhkan sikap keterbukaan dalam proses transfer knowledge yang berjalan alamiah. Biasanya para member juga akan saling memberikan info atau melaporkan keberhasilan mereka lewat sosial media pertemanan, seperti Instagram dan reposting dari para member lainnya dengan men tagline Meta4sec. Publikasi yang legal secara internal dan eksternal ternyata memberikan dampak signifikan bagi penambahan member dalam *community* discord Meta4sec. *Community Manager* juga selalu mempromosikan komunitasnya dalam berbagai event yang diikutinya, baik saat menjadi narasumber maupun saat menjadi peserta dalam event penyelenggaraan pelatihan *cyber security*. Membangun jaringan dan kepercayaan menjadi salah satu tugas dari *community manager* untuk memperluas popularitas komunitas dan mendapatkan peluang baru.

Hasil dari wawancaran dengan founder Meta4sec, dikethuia bahwa ide awal komunitas ini dibuat untuk mewadahi seluruh lapisan masyarakat untuk dapat dengan mudah mempelajari IT security khususnya *ethical hacker (white hacker/hacker* baik). Motivasi dalam membuat komunitas hacker baik ini adalah ikut berperan serta dan membantu pemerintah mengenalkan ilmu IT dengan mudah dan murah melalui komunitas Hacker selama ini dikonotasikan sebagai penjahat, tetapi ada hacker baik yang membantu pengelola IT jika ada kerentanan. Untuk update informasi dan menguatkan komunitas dilakukan kegiatan rutin antara lain meet up/pertemuan rutin setahun 2 kali, discord sebagai alat untuk konsultasi dan sharing antar anggota, update video terbaru di youtube channel terkait pembalajaran baru. Kemudian terhadap pengurus komunitas, founder selalu tanamkan untuk selalu semangat untuk berbagi ilmu, karena dengan berbagi kita menjadi bermanfaat dan ilmu yang kita miliki akan bertambah. Ketrampilan manajerial juga ditanamkan kepada *manager community* dengan memberikan arahan dan bimbingan terkait perencanaan, monitoring dan evaluasi terkait komunitas. Dipilihnya pemimpin muda Gen-Z sebagai manager community untuk dijadikan contoh dan merupakan salah satu daya tarik dan masih memiliki jalan yang panjang dalam mempelajari bidang IT security ini. Merekrut anggota baru untuk bergabung dengan komunitas Hacker di lakukan secara holistil/alamiah sehingga member masuk karena merasa nyaman dan manfaat. Untuk memastikan bahwa anggota komunitas

Hacker tetap aktif dan terlibat dalam kegiatan komunitas dengan cara monitoring evaluasi kegiatan yang sudah ditentukan harus berjalan.

Wawancara dengan anggota Komunitas Meta4sec, yang menanamkan diri mereka adalah *ethical hacking* yaitu peretas yang memiliki etika atau disebut white hacker, karena tujuan peretasan yang mereka lakukan adalah untuk kebaikan dengan memberikan laporan kepada pemilik *website* bahwa aplikasi website yang mereka buat memiliki kerentanan dan ini akan berbahaya bagi keamanan data yang mereka miliki. Komunitas ini sering juga menyebut diri mereka sebagai *cyber army* atau penjaga keamanan siber. Banyak komunitas serupa yang ada dan tumbuh massif berkembang di Indonesia, tetapi mereka ebih nyaman bergabung di komunitas Meta4sec yang rata-rata masih berusia muda. Ketertarikan mereka terhadap dunia siber biasanya muncul karena antusiasme dan hobi mereka terhadap dunia siber. Kebanyakan dari aktivitas *hacking* yang resmi, mereka akan mendapatkan temuan untuk kemudian dilaporkan kepada pengelola platform *bug bounty*, bahkan mereka menawarkan program tersebut dengan imbalan yang cukup signifikan bagi individu yang berhasil menemukan kerentanan dalam sistem yang mereka buat dalam level mayor maupun minor.

Tujuan bug *bounty* bagi sebagian anggota komunitas meta4sec adalah meningkatkan keamanan sistem dengan memanfaatkan keahlian dan pengetahuan dari para ahli keamanan. Dengan membuka peluang bagi peneliti keamanan untuk menemukan dan melaporkan kerentanan, organisasi dapat mengidentifikasi dan memperbaiki celah keamanan sebelum para *black hacker* menemukannya dan mengeksploitasinya. *Bug bounty* saat ini menjadi sebuah ajang pembuktian kekuatan sebuah sistem di industri teknologi dan banyak ditawarkan oleh para perusahaan besar, seperti Microsoft, Apple, Google. Awalnya member komunitas menemukan Meta4sec dalam kanal *Youtube* yang berupa video pembelajaran pendek namun lengkap seputar *ethical hacking*. Mereka mendapatkan banyak *insight* yang menyeluruh dan lengkap serta terbuka tentang pembelajaran dan langkah penting untuk menjadi *Hacker*. Menurut mereka, tidak banyak konten dalam internet yang menjelaskan perihal *hacking* tips dengan lengkap seperti yang mereka temukan dalam kanal video Meta4sec. Hal ini jelas terlihat dalam *comment* yang diberikan dalam konten yang membuat video berikutnya selalu ditunggu.

Community manager menurut hasil wawancara kepada member dianggap mampu memberikan penjelasan yang mereka butuhkan dan selalu membagi informasi yang bermanfaat seputar *ethical hacking*. Meskipun masih berusia muda, menurut para anggota komunitas, ternyata *community manager* mampu menjelaskan dengan detail dan memberikan jawaban yang solutif seputar aktivitas *hacking/bug bounty* sekaligus memberikan pembelajaran dengan metode yang aplikatif dengan memberikan demo praktik yang mudah untuk dipahami. *Community manager* juga dianggap mampu mengelola diskusi dengan baik, menyapa anggota yang aktif dan bertanya tentang hal-hal ringan yang memunculkan keakraban dalam kelompok. Para narasumber dalam sesi sharing juga adalah personil yang memiliki kapabilitas baik dalam keilmuannya dibidang *cyber security* dengan kompetensi yang dibuktikan dengan sertifikat internasional yang dimiliki. Para anggota komunitas tidak dikenakan biaya ketika mereka belajar juga menjadi daya tarik bagi mereka karena pelatihan seperti ini umumnya berbayar dan Komunitas ini pun masih jarang ditemukan di Indonesia. Menurut mereka peran dan kontributor white hacker seperti mereka saat ini sangat dibutuhkan untuk membantu pemerintah dalam mengendalikan kejahatan siber di Indonesia. Perkembangan penambahan anggota di discord dan keaktifan dalam aktivitas sharing season dalam bentuk online dan offline menjadi salah satu indikator keberhasilan Meta4sec sebagai komunitas ethical *hacker community* di Indonesia sebagai wadah untuk belajar dan mengembangkan kewaspadaan akan pentingnya menjaga keamanan siber untuk kepentingan masyarakat secara khusus dan kedaulatan negara. Sektor keamanan nasional juga diperluas dari dunia nyata ke dunia maya sehingga hasil dari analisis kebijakan standarisasi keamanan perangkat telekomunikasi untuk menunjang kebijakan pertahanan dan diharapkan komunitas *ethical*

hacker yang ada dapat berperan aktif (Yuswanto & Wibowo, 2020).

Tantangan dalam komunitas meta4sec berdasarkan penelitian unutk menjadikan perhatian, antara lain: (1) Bidang keamanan siber terus berkembang, dengan kerentanan baru, teknik serangan, dan teknologi yang muncul secara teratur. Peretas etis perlu tetap diperbarui dan terus meningkatkan keterampilan dan pengetahuan mereka untuk mengimbangi lanskap ancaman yang terus berubah. Seluruh member meta4sec harus beroperasi dalam batas-batas hukum dan mematuhi pedoman etika. Menavigasi kerangka hukum dan memastikan bahwa aktivitas mereka sah dan sesuai hukum dapat menjadi tantangan. Mereka perlu mempertahankan moral yang kuat dan membuat keputusan etis saat melakukan penilaian keamanan. White hacker terkadang menghadapi skeptisisme dan kurangnya kepercayaan dari individu dan organisasi. Beberapa orang mungkin memandang mereka dengan curiga, menganggap mereka memiliki niat jahat. Ini bisa menjadi tantangan bagi peretas etis untuk mendapatkan pengakuan atas kontribusi dan upaya mereka dalam mengamankan sistem dan jaringan. Komunitas sering beroperasi dengan sumber daya terbatas, seperti waktu, dana, dan akses ke alat khusus. Mereka mungkin menghadapi tantangan dalam memperoleh sumber daya dan dukungan yang diperlukan untuk secara efektif melakukan penilaian keamanan dan mengatasi kerentanan. Meskipun kolaborasi dan berbagi informasi sangat penting dalam komunitas keamanan dunia maya, mungkin ada tantangan dalam membina kepercayaan dan kerja sama di antara para peretas etis. Berbagi detail, alat, dan teknik kerentanan yang sensitif dapat menjadi keseimbangan yang rumit, karena beberapa individu mungkin menyalahgunakan atau mengeksploitasi informasi tersebut. Beradaptasi dengan Teknologi Baru untuk memahami teknologi yang muncul seperti kecerdasan buatan, Internet of Things (IoT), komputasi awan, dan blockchain. Mengikuti perkembangan ini dapat menuntut dan membutuhkan pembelajaran berkelanjutan. Etika di Area Abu-Abu yaitu menyeimbangkan kebutuhan untuk mengungkap kerentanan dengan dampak potensial pada sistem dan individu dapat menimbulkan dilema etika. Untuk mengatasi semua tantangan ini memerlukan komitmen untuk terus belajar, pengembangan profesional, kolaborasi, dan kepatuhan terhadap standar etika. Peretas etis dapat mengambil manfaat dari berpartisipasi dalam konferensi, program pelatihan, dan terlibat dengan komunitas keamanan siber untuk mengatasi tantangan ini secara kolektif.

Dalam kepemimpinan, menurut Putrawan (2020, p. 9) konsep kepemimpinan merupakan komponen fundamental di dalam menganalis proses dan dinamika di dalam organisasi yang di kaitkan dengan sifat (strait), perilaku (behaviors), pengaruh (influence), pola interaksi (interaction patterns), dan hubungan peran (role reation ship). Salah satu gaya atau tipe kepemimpinan yang populer hingga sekarang adalah kepemimpinan transformasional. Menurut Ivancevich *et all* (2014, p. 460), "*transformational leader are able to influence others by using charisma, paying attention, to followers, and stimulating others."* pemimpin transformasional mampu memengaruhi orang lain dengan menggunakan karisma, memperhatikan, ke pengikut, dan merangsang orang lain, hal ini sesuai dengan kebutuhan kepemimpinan pada komunitas Meta4sec pada penelitian ini. Sejalan dengan Hughes, Ginnet, dan Churphy (2015, p. 579) kepemimpinan transformasional mengubah status quo dengan menarik pengikut nilai, rasa, tujuan yang lebih tinggi. Diperkuat temuan Bateman dan Snell (2015, p. 425), kepemimpinan transformasional adalah "*is leaders who motivate people to transcend their personal interests for the good of the group*." Artinya adalah pemimpin yang memotivasi orang untuk mengatasi kepentingan pribadi mereka untuk kebaikan kelompok. Sedangkan Bryman sebagaimana dikutip Aamodt (2013, p. 450) menyatakan, "*transformational leaders are confidence, have a need to influence others, and hold strong attitude that their beliefs and ideas are correct*." Pemimpin transformasional adalah yakin, memiliki kebutuhan untuk mempengaruhi orang lain, dan memiliki sikap yang kuat bahwa keyakinan dan ide-ide mereka benar. Penelitian Luo et al. (2019) memberikan perluasan penting dari kepemimpinan transformasional, dan dengan kepemimpinan bersama, bagaimana memilih

mentor tim terbaik dan lebih banyak lagi untuk memfasilitasi tim kepemimpinan yang efektif (Luo et al., 2019). Penelitian ini menemukan bahwa kepemimpinan karakter Gen-Z merupakan Generasi yang memiliki kesenangan untuk bekerja secara kolaboratif dan menghargai pendekatan tim dalam menyelesaikan masalah dan mendapatkan solusi dan harus dapat mengikuti perkembangan jaman (trasformasional).

Manajemen Meta4sec juga memiliki strategi dalam mengembangkan kelompok komunitasnya dengan cara membangun komunikasi yang baik dengan kelompoknya yaitu dengan cara melibatkan para anggota yang aktif untuk berkontribusi hasil temuan dan pembelajaran yang mereka dapat. *Community manager* Meta4sec juga intensif memberikan video pembelajaran secara rutin dan membuka ruang diskusi yang luas dengan para anggotanya melalui discord maupun media komunikasi yang lain. Di University of Alaska Anchorage (UAA) Discord sebagai platform untuk bimbingan belajar online dengan sistem obrolan online gratis yang dapat diakses melalui browser web, program komputer, atau aplikasi seluler dan merupakan pesaing aplikasi termasuk Skype, Slack, dan TeamSpeak (Mock, 2019). *Community manager* juga selalu merespon cepat terhadap kasus–kasus yang didiskusikan seputar ethical hacking. Metode penyampaian yang menarik dan mudah untuk dipahami menjadi kelebihan yang dimiliki oleh *Community manager*. Meskipun masih berusia muda, pengalaman, ketrampilan dan reputasi keberhasilan dalam menemukan kerentanan terbukti memunculkan kepercayaan para anggota komunitas terhadap Meta4sec. Keterbaruan ilmu dan metode *hacking* yang mudah dipahami dalam video pembelajaran yang dibawakan oleh *community manager* memunculkan minat dan keinginan untuk belajar yang lebih intensif dalam ruang-ruang diskusi melalui platform media komunikasi yang digunakan , seperti discord, wa grup atau *direct contact* yang direspon dengan cepat oleh *community manager* meta4sec.

Solidaritas dan loyalitas para anggota komunitas terlihat dari antusiasme mereka dalam berbagi ilmu dalam virtual classroom di discord maupun dalam pertemuan secara luring. Keterlibatan dalam diskusi yang memegang etika aturan komunitas yang telah disclaimer oleh *community manager* menjadi indikasi bahwa para anggota ingin mempertahankan eksistensi komunitas. Peningkatan kemampuan para komunitas melalui penawaran pelatihan bebas biaya selalu memenuhi *quota* dan ini menunjukkan bahwa komunitas ini memiliki animo belajar yang tinggi. Jumlah anggota yang bertambah menunjukkan popularitas komunitas Meta4sec dikalangan *ethical hacker enthusiastic* semakin dikenal dan ini menjadi indikator keberhasilan *community manager.* Selain itu kepemimpinan dengan usia muda tidak menjadi sebuah *gap* atau memunculkan keraguan dari para member karena mereka lebih mengedepankan profesionalitas dan pembuktian kemampuan dan prestasi serta karakter yang tergambar dari gaya komunikasi yang dilakukan oleh community manager saat menjadi pimpinan maupun moderator dalam diskusi

Integritas pimpinan komunitas/ organisasi diperlukan untuk mencapai tujuan (Codreanu, 2019) dan budaya integritas memungkinkan eksekutif SDM untuk mempengaruhi integritas dan perilaku etis dalam tim manajemen puncak (Tasoulis et al., 2019). Menurut Tasoulis (2019) Faktor-faktor yang mempengaruhi integritas pemimpin meliputi: karakteristik individu (pola pikir altruistik, keaslian, harga diri berbasis organisasi, nilai-nilai pribadi yang memberikan integritas, Machiavellianisme), Dalam penelitiannya Dahlan dan Fatmawada (2020) menyebutkan untuk meningkatkan kualitas pengelolaan sumber daya manusia pengaruhi oleh kompetensi dan integritas, serta didukung pula oleh penelitian Leicht-Deobald (2019) mengidentifikasi tantangan penting terkait integritas. Etika, moral dan legalitas harus sejalan dengan hati nurani. Integritas akan menyesuaikan kenyataan dengan ucapan kita yang berarti tepat janji dan sesuai harapan (Covey, 2016). Integritas sebagai komitmen individu untuk positif nilai-nilai sehingga mampu bertindak dan berperilaku sesuai dalam menciptakan situasi yang baik (Ramdani, 2018). Berdasarkan hasil penelitian dapat disintesiskan bahwa integritas wajib dimiliki oleh seorang pemimpin termasuk Gen-Z.

SIMPULAN DAN SARAN

Berdasarkan hasil penelitian dapat disintesiskan bahwa integritas wajib dimiliki oleh seorang pemimpin pada Gen-Z dan gaya kepemimpinan kolaboratif meliputi kemampuan mendengarkan, mengajak anggota tim terlibat, menstimulasi kontribusi dari semua anggota yang aktif, dan membangun lingkungan komunitas yang positif dan inklusif dan sebagai strategi untuk menjawab masalah terkait kurangnya pengalaman manajemen, perbedaan generasi, kesulitan dalam berkomunikasi dan bekerja sama, sehingga terbukti efektif membuat komunitas ini semakin hari semakin berkembang, dan harus dapat mengikuti perkembangan jaman (transformasional).

Keterbatasan penelitian ini pada komunitas Meta4sec yang berdomisili di Jakarta, secara fasilitas dan teknologi terpenuhi tetapi belum tentu di kota lain. Masukan untuk penelitian selanjutnya perlu di lakukan selain terkait regenerasi kepemimpinan kedepan sesuai dengan perkembangan zaman, dan pengembangan terkait metode pembelajaran dan *sharing knowledge* seperti *blended learning* dan penemuan-penemuan baru dalam bidang *cybersecurity* yang berkembang secara massif menarik untuk di kaji lebih dalam.

UCAPAN TERIMA KASIH

Ucapan terima kasih kepada *founder* dan anggota *Ethical Hacker Community* Meta4sec atas semua waktu dan kerjasamanya sehingga penelitian ini selesai, dan seluruh pihak yang mendukung penelitian ini.

DAFTAR PUSTAKA

Aamodt, M. A. (2013). *Industrial/Organizational Psychology: An Applied Approach* (8th editon). Cengage learning.

Arifianto, M., & Izzudin, I. (2021). Students' acceptance of discord as an alternative online learning media. *International Journal of Emerging Technologies in Learning (IJET)*, *16*(20), 179–195.

Bulut, S., & Maraba, D. (2021). Generation Z and its perception of work through habits, motivations, expectations preferences, and work ethics. *Psychology and Psychotherapy Research Study*.

Christen, M., Gordijn, B., & Loi, M. (2020). *The ethics of cybersecurity*. Springer Nature.

Codreanu, A. (2019). Strategic human resource management. A milestone for integrity building in public administration. *Redefining Community in Intercultural Context*, *8*(1), 267–274.

Covey, S. R. (2016). *The 7 habits of highly effective people: Powerful lessons in personal change*. Simon and Schuster.

Dahlan, D., & Fatmawada, F. (2020). The fusion of competence and integrity problems in transformation of public human resources management model. *Jurnal Ilmiah Ilmu Administrasi Publik*, *9*(2), 185–190.

Felinda, I., & Sugiyono, S. (2018). Pembelajaran Sejarah Yang Efektif Di Sma Negeri 1 Mlati Sleman. *ISTORIA: Jurnal Pendidikan Dan Ilmu Sejarah*, *14*. https://doi.org/10.21831/istoria.v14i1.19426

Firmansyah, M., & Yuswanto, A. (2022). Knowledge management for information security incident handling at Security Operation Center of Jakarta Provincial Government. *Monas: Jurnal Inovasi Aparatur*, *4*(2), 441–452.

Hámornik, B. P., & Krasznay, C. (2017). A team-level perspective of human factors in cyber security: security operations centers. *International Conference on Applied Human Factors and Ergonomics*, 224–236.

Hawamleh, A. M. A., Alorfi, A. S. M., Al-Gasawneh, J. A., & Al-Rawashdeh, G. (2020). Cyber security and ethical hacking: The importance of protecting user data. *Solid State Technology*, *63*(5), 7894–7899.

Jaquet-Chiffelle, D.-O., & Loi, M. (2020). Ethical and unethical hacking. *The Ethics of Cybersecurity*, 179–204.

John M. Ivancevich, Robert Kanopaske, M. T. M. (2014). Organizational Behavior and Management. In *Organizational Behavior & Management*. New York: McGraw-Hill.

Kohnová, L., Papula, J., & Salajová, N. (2021). Generation Z: Education In The World Of Digitization For The Future Of Organizations. *INTED2021 Proceedings*, *1*, 10199–10208. https://doi.org/10.21125/INTED.2021.2126

Kyngäs, H. (2020). Qualitative research and content analysis. *The Application of Content Analysis in Nursing Science Research*, 3–11.

Lehto, M., & Limnéll, J. (2021). Strategic leadership in cyber security, case Finland. *Information Security Journal: A Global Perspective*, *30*(3), 139–148.

Leicht-Deobald, U., Busch, T., Schank, C., Weibel, A., Schafheitle, S., Wildhaber, I., & Kasper, G. (2019). The challenges of algorithm-based HR decision-making for personal integrity. *Journal of Business Ethics*, *160*(2), 377–392.

Luo, A., Guchait, P., Lee, L., & Madera, J. M. (2019). Transformational leadership and service recovery performance: The mediating effect of emotional labor and the influence of culture. *International Journal of Hospitality Management*, *77*, 31–39.

Mock, K. (2019). Experiences using Discord as platform for online tutoring and building a CS community. *Proceedings of the 50th ACM Technical Symposium on Computer Science Education*, 1284.

Nicholas, A. (2020). Preferred Learning Methods of Generation Z. *Faculty and Staff - Articles & Papers*. https://digitalcommons.salve.edu/fac_staff_pub/74

Ojogiwa, O. T. (2021). The crux of strategic leadership for a transformed public sector management in Nigeria. *International Journal of Business and Management Studies*, *13*(1), 83–96.

Putrawan, I. M. (2020). *Kepemimpinan Guru Dalam Perilaku Organisasi : Beberapa konsep dan langkah-langkah pengukurannya* (1st ed.). Alfabeta.

Ramdani, Z. (2018). Construction of academic integrity scale. *International Journal of Research Studies in Psychology, 7(1), 87-97.*

Richard L. Hughes, R. C. G. and G. J. C. (2015). *Leadership: Enhancing the lessons of experience* (eight edit). McGraw-Hill Education.

Rubin, H. J., & Rubin, I. S. (2011). *Qualitative interviewing: The art of hearing data*. sage.

Snell, T. S. B. and S. A. (2015). *Management* (eleventh e). McGraww-Hill.

Tasoulis, K., Krepapa, A., & Stewart, M. M. (2019). Leadership integrity and the role of human resource management in Greece: gatekeeper or bystander? *Thunderbird International Business Review*, *61*(3), 491–503.

Widmann, A., & Mulder, R. H. (2020). The effect of team learning behaviours and team mental models on teacher team performance. *Instructional Science*, *48*(1), 1–21.

Yuswanto, A. (2023). Pengaruh Leadership Style Terhadap Task Performance Melalui Persistence, Procedural Justice Dan Integrity Pada Security Operation Center (Soc) Di Indonesia . *UNIVERSITAS NEGERI JAKARTA*.

Yuswanto, A., Putrawan, I. M., & Eryanto, H. (2023). Cyber Security Strategy: Factors Affecting Performance at Security Operation Center (SOC) In Indonesia. *Resmilitaris*, *13*(1), 3110–3127.

Yuswanto, A., & Wibowo, B. (2020). Pembangunan Pusat Pengendalian Operasional Keamanan Informasi (Pusdalops Kami) guna Meningkatkan Pelayanan E-Gov dari Ancaman Kejahatan Siber. *Academia. Edu*.