e-ISSN 2962-3626

JURNAL KOMPUTER INDONESIA

Cyber Security In 2023: The Latest Challenges And Solutions

Keamanan Siber Di Tahun 2023: Tantangan Dan Solusi Terbaru

Ahmad Doni Wiratama [1)]
[1)] ***Universitas Bengkulu***
Email: [1)] wiratamadoni@gmail.com

How to Cite :
Wiratama, D,A. (2023). Cyber Security in 2023: The Latest Challenges and Solutions. Jurnal Komputer Indonesia, 2(1). Doi:

ARTICLE HISTORY
Received [8 Mei 2023]
Revised [10 Juni 2023]
Accepted [12 Juni 2023]

KEYWORDS
Cyber Security , Latest Challenges And Solutions

ABSTRAK

Keamanan siber telah menjadi isu krusial di era digital, khususnya di tahun 2023 di mana teknologi terus berkembang pesat. Artikel ini membahas berbagai tantangan yang dihadapi dalam menjaga keamanan siber, seperti meningkatnya serangan siber yang semakin canggih, dan solusi terbaru yang ditawarkan untuk menghadapinya. Penelitian ini dilakukan melalui analisis literatur serta studi kasus yang relevan. Hasil dari penelitian ini menunjukkan bahwa pendekatan baru seperti Zero Trust, kecerdasan buatan dalam deteksi ancaman, dan kolaborasi antar entitas menjadi kunci utama dalam memperkuat keamanan siber di tahun 2023.

ABSTRACT

Cybersecurity has become a crucial issue in the digital age, especially in 2023 where technology continues to evolve rapidly. This article discusses the challenges faced in maintaining cybersecurity, such as the rise of increasingly sophisticated cyberattacks, and the latest solutions offered to deal with them. The research was conducted through literature analysis as well as relevant case studies. The results show that new approaches such as Zero Trust, artificial intelligence in threat detection, and collaboration between entities are key to strengthening cybersecurity in 2023.

PENDAHULUAN

Keamanan siber adalah salah satu aspek paling penting dalam teknologi informasi di era modern. Dengan pesatnya pertumbuhan dunia digital pada tahun 2023, tantangan dalam keamanan siber semakin kompleks. Dunia digital yang terus berkembang membawa serta ancaman siber yang semakin canggih dan sulit dideteksi. Ancaman seperti ransomware, phishing, dan Advanced Persistent Threats (APT) tidak hanya menargetkan individu, tetapi juga organisasi besar dan pemerintah. Serangan-serangan ini mengancam keamanan data dan integritas sistem, yang dapat mengakibatkan kerugian signifikan jika tidak ditangani dengan baik.

Keamanan siber tidak hanya penting untuk melindungi data pribadi dan organisasi, tetapi juga untuk menjaga kelangsungan operasi bisnis dan kepercayaan publik. Setiap organisasi, baik besar maupun kecil, bergantung pada sistem informasi untuk operasi sehari-hari, dan kerusakan atau pencurian data dapat memiliki konsekuensi yang merugikan. Serangan siber dapat mengakibatkan kerugian finansial yang signifikan, kerusakan reputasi, dan gangguan operasional yang dapat berdampak pada stabilitas bisnis.

Selain itu, dengan meningkatnya kesadaran akan pentingnya data pribadi, perlindungan data menjadi prioritas utama. Regulasi seperti GDPR (General Data Protection Regulation) di Uni Eropa dan CCPA (California Consumer Privacy Act) di Amerika Serikat menegaskan bahwa perlindungan data tidak hanya merupakan kewajiban hukum tetapi juga tanggung jawab etis bagi organisasi. Dengan serangan yang semakin kompleks, kepercayaan publik terhadap organisasi dapat dipertaruhkan jika data tidak dilindungi dengan baik

Ransomware telah menjadi salah satu ancaman siber paling dominan dan merusak. Serangan ransomware mengenkripsi data korban dan meminta tebusan untuk kunci dekripsi. Meskipun bukan ancaman baru, ransomware terus berkembang dengan metode yang lebih canggih dan target yang lebih besar, termasuk organisasi besar dan infrastruktur kritis. Serangan seperti ini dapat mengakibatkan gangguan operasional yang parah dan kerugian finansial yang besar.

Kesenjangan keterampilan dalam keamanan siber adalah masalah global yang semakin mendalam. Dengan berkembangnya ancaman dan teknologi, permintaan untuk profesional keamanan siber yang terampil meningkat pesat. Namun, kekurangan tenaga kerja yang terlatih menyebabkan kesulitan dalam mengelola dan mengatasi ancaman dengan efektif. Hal ini mengharuskan organisasi untuk terus memperbarui keterampilan dan pengetahuan staf mereka.

Di tahun 2023, pendekatan terhadap keamanan siber perlu ditingkatkan untuk menghadapi ancaman yang terus berkembang. Artikel ini bertujuan untuk mengidentifikasi tantangan utama yang dihadapi dalam keamanan siber tahun ini, serta mengeksplorasi solusi terbaru yang dapat diterapkan untuk mengatasi ancaman-ancaman tersebut. Dengan memahami lanskap ancaman yang berkembang dan teknologi terbaru dalam keamanan siber, diharapkan artikel ini dapat memberikan wawasan yang berharga bagi individu dan organisasi dalam melindungi diri mereka dari serangan yang semakin canggih dan merugikan.

LANDASAN TEORI

Keamanan Siber

Keamanan siber adalah cabang dari ilmu komputer yang fokus pada perlindungan sistem komputer, jaringan, perangkat, dan data dari ancaman atau serangan yang dapat merusak integritas, kerahasiaan, dan ketersediaan informasi. Keamanan siber mencakup berbagai praktik dan teknologi yang dirancang untuk melindungi sistem dan data dari akses yang tidak sah, kerusakan, dan gangguan. Konsep dasar keamanan siber melibatkan beberapa elemen penting, termasuk:

1. Kerahasiaan (Confidentiality): Melindungi informasi dari akses yang tidak sah. Ini biasanya dicapai melalui teknik enkripsi dan kontrol akses yang ketat.
2. Integritas (Integrity): Memastikan bahwa data tidak diubah atau dimodifikasi tanpa izin. Teknik seperti hashing dan kontrol versi digunakan untuk menjaga integritas data.
3. Ketersediaan (Availability): Menjamin bahwa sistem dan data tersedia bagi pengguna yang sah ketika dibutuhkan. Ini melibatkan pengelolaan cadangan, pemulihan bencana, dan perlindungan terhadap serangan yang dapat menyebabkan downtime.

Ancaman dan Kerentanan dalam Keamanan Siber

Ancaman dan kerentanan adalah dua konsep yang mendasar dalam keamanan siber. Ancaman adalah potensi bahaya yang dapat mengeksploitasi kerentanan, sedangkan kerentanan adalah kelemahan dalam sistem yang dapat dimanfaatkan oleh ancaman. Beberapa ancaman utama yang dihadapi pada tahun 2023 meliputi:

1. Ransomware: Jenis malware yang mengenkripsi data korban dan meminta tebusan untuk kunci dekripsi. Ransomware sering kali menargetkan organisasi besar dan infrastruktur kritis, menyebabkan kerugian finansial dan gangguan operasional.

2. Phishing: Teknik penipuan yang digunakan untuk memperoleh informasi sensitif, seperti kredensial login, dengan menyamar sebagai entitas yang tepercaya. Phishing sering dilakukan melalui email, pesan teks, atau media sosial.
3. Advanced Persistent Threats (APT): Serangan yang dilakukan oleh aktor yang sangat terampil dan sering kali didukung oleh negara atau kelompok dengan sumber daya besar. APT dirancang untuk mendapatkan akses yang berkelanjutan dan mencuri informasi berharga secara bertahap.

Teknologi Keamanan Siber

Teknologi keamanan siber merupakan alat dan metode yang digunakan untuk melindungi sistem dan data dari ancaman. Beberapa teknologi utama meliputi:

1. Enkripsi: Teknik yang digunakan untuk mengamankan data dengan mengubahnya menjadi format yang tidak dapat dibaca tanpa kunci dekripsi. Enkripsi digunakan dalam komunikasi data, penyimpanan data, dan perlindungan data pribadi.
2. Firewall: Sistem yang mengontrol lalu lintas jaringan berdasarkan aturan yang telah ditentukan, mencegah akses tidak sah ke atau dari jaringan internal.
3. Antivirus dan Antimalware: Program yang dirancang untuk mendeteksi, mencegah, dan menghapus perangkat lunak berbahaya dari sistem. Ini termasuk pemantauan real-time dan pemindaian berkala.

Pendekatan dan Strategi Keamanan Siber

Untuk mengelola ancaman dan kerentanan, organisasi perlu mengadopsi pendekatan dan strategi yang komprehensif. Beberapa pendekatan utama meliputi:

1. Zero Trust Architecture: Pendekatan keamanan yang mengadopsi prinsip "tidak pernah percayai, selalu verifikasi." Dalam model ini, akses ke sistem dan data diberikan hanya setelah verifikasi identitas pengguna dan perangkat yang ketat.
2. Keamanan Berbasis Cloud: Dengan adopsi luas layanan cloud, pendekatan ini fokus pada melindungi data dan aplikasi yang disimpan di cloud, termasuk penggunaan teknologi seperti enkripsi dan kontrol akses berbasis kebijakan.
3. Pemantauan dan Respon Keamanan: Teknologi seperti SIEM (Security Information and Event Management) dan SOAR (Security Orchestration, Automation, and Response) digunakan untuk mengumpulkan, menganalisis, dan merespons data keamanan secara real-time. Ini membantu dalam mendeteksi ancaman lebih awal dan merespons secara otomatis.

Kecerdasan Buatan (AI) dan Pembelajaran Mesin dalam Keamanan Siber

AI dan pembelajaran mesin memainkan peran yang semakin penting dalam keamanan siber. Keduanya digunakan untuk meningkatkan deteksi ancaman dan respons secara otomatis. AI dapat menganalisis data dalam jumlah besar untuk mengidentifikasi pola dan anomali yang menandakan serangan siber. Pembelajaran mesin memungkinkan sistem untuk belajar dari data sebelumnya dan meningkatkan akurasi deteksi ancaman seiring waktu.

1. Deteksi Anomali: AI dapat mengidentifikasi perilaku yang tidak biasa dalam sistem yang mungkin menunjukkan adanya serangan. Ini termasuk analisis lalu lintas jaringan dan aktivitas pengguna.
2. Otomatisasi Respon: Pembelajaran mesin dapat digunakan untuk mengotomatisasi respons terhadap ancaman, seperti memblokir IP yang mencurigakan atau mengisolasi sistem yang terinfeksi.

Regulasi dan Kepatuhan dalam Keamanan Siber

Regulasi dan kepatuhan merupakan aspek penting dalam pengelolaan keamanan siber. Regulasi seperti GDPR (General Data Protection Regulation) dan CCPA (California Consumer Privacy Act) menetapkan standar untuk perlindungan data dan privasi. Kepatuhan terhadap regulasi ini tidak hanya membantu dalam menghindari denda hukum tetapi juga membangun kepercayaan dengan pelanggan dan mitra bisnis.

Kesenjangan Keterampilan dalam Keamanan Siber

Kesenjangan keterampilan adalah masalah yang signifikan dalam keamanan siber, dengan permintaan yang tinggi untuk profesional yang terampil dan kekurangan tenaga kerja yang memenuhi syarat. Pendidikan dan pelatihan berkelanjutan, serta inisiatif untuk meningkatkan kesadaran tentang karir di bidang keamanan siber, sangat penting untuk mengatasi kekurangan ini.

METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif dengan pendekatan deskriptif. Sumber data utama berasal dari analisis literatur yang mencakup artikel jurnal, buku, laporan industri, serta studi kasus yang relevan mengenai keamanan siber. Selain itu, wawancara dengan pakar keamanan siber juga dilakukan untuk mendapatkan wawasan mendalam mengenai tantangan dan solusi terbaru yang diterapkan pada tahun 2023. Data yang diperoleh dianalisis menggunakan teknik analisis isi untuk mengidentifikasi tema-tema utama dan tren yang relevan.

Pengumpulan Data Sekunder

Analisis data sekunder dilakukan dengan menggunakan data dari sumber eksternal yang relevan. Data ini mencakup:

1. Statistik dan Laporan Penelitian: Data yang dikumpulkan dari studi dan survei yang dilakukan oleh lembaga penelitian keamanan siber dan organisasi industri.
2. Studi Kasus: Menganalisis studi kasus yang menunjukkan implementasi solusi keamanan siber di berbagai organisasi dan sektor.

Analisis Kualitatif dan Kuantitatif

Metode analisis data melibatkan pendekatan kualitatif dan kuantitatif:

1. Analisis Kualitatif: Mengkaji deskripsi dan narasi dari laporan dan artikel untuk memahami konteks dan efek dari berbagai ancaman serta solusi. Ini termasuk analisis mendalam tentang bagaimana ancaman baru berkembang dan solusi yang diterapkan.
2. Analisis Kuantitatif: Menggunakan data numerik dari laporan dan survei untuk mengukur frekuensi, prevalensi, dan dampak dari ancaman siber. Ini juga mencakup analisis tren statistik untuk memahami pola serangan dan efektivitas solusi.

Studi Kasus Implementasi

Penelitian ini juga mencakup studi kasus dari organisasi yang telah menerapkan solusi keamanan siber terbaru. Studi kasus ini melibatkan:

1. Deskripsi Implementasi: Menjelaskan bagaimana solusi diterapkan di berbagai organisasi, termasuk teknologi yang digunakan, perubahan kebijakan, dan prosedur operasional.
2. Evaluasi Efektivitas: Menilai keberhasilan solusi dalam mengatasi ancaman siber, termasuk dampak pada keamanan sistem, operasi bisnis, dan kepuasan pengguna.

Wawancara dan Survei

Untuk melengkapi analisis, wawancara dan survei dilakukan dengan para ahli keamanan siber, praktisi industri, dan pengambil keputusan dari berbagai organisasi. Tujuan wawancara dan survei adalah:

1. Mengumpulkan Perspektif: Mendapatkan pandangan dan pengalaman praktis tentang tantangan yang dihadapi dan solusi yang diterapkan.
2. Evaluasi Tren: Mengidentifikasi tren terbaru dalam keamanan siber dan mendapatkan wawasan tentang praktik terbaik dan inovasi yang sedang berkembang.

Pengolahan Data

Data yang diperoleh dari studi literatur, analisis data, dan wawancara diproses dan disusun untuk menyusun laporan yang komprehensif. Laporan ini mencakup:

1. Ringkasan Temuan: Menyajikan temuan utama dari analisis dan studi kasus, termasuk tantangan yang dihadapi dan solusi yang diterapkan.
2. Rekomendasi: Memberikan rekomendasi berbasis data untuk menghadapi tantangan keamanan siber di masa depan.

Penyajian dan Diskusi

Laporan akhir disusun untuk menyajikan hasil penelitian dalam format yang jelas dan terstruktur. Diskusi akan mencakup analisis mendalam mengenai temuan, implikasi bagi industri, dan arah penelitian di masa depan.

HASIL DAN PEMBAHASAN

Hasil

Hasil penelitian menunjukkan bahwa tantangan terbesar dalam keamanan siber di tahun 2023 meliputi peningkatan serangan siber yang lebih kompleks, seperti serangan berbasis AI yang mampu menyesuaikan diri dengan sistem keamanan yang ada, serta kebocoran data akibat human error. Selain itu, pemanfaatan teknologi Internet of Things (IoT) yang luas tanpa keamanan yang memadai juga menambah risiko serangan. Dalam menghadapi tantangan ini, beberapa solusi terbaru telah diadopsi. Pendekatan Zero Trust mulai diterapkan secara luas, dengan perusahaan-perusahaan besar yang mengimplementasikan kebijakan akses minimal dan verifikasi terus-menerus. AI dan ML juga memainkan peran penting dalam deteksi ancaman yang lebih proaktif. Penggunaan teknologi enkripsi yang lebih kuat dan teknik pemulihan data yang lebih cepat menjadi aspek penting dalam meningkatkan keamanan data. Kerjasama antara sektor publik dan swasta dalam pertukaran informasi tentang ancaman siber juga menjadi langkah yang signifikan dalam memperkuat keamanan.

Pembahasan

1) Ransomware

Ransomware tetap menjadi salah satu ancaman terbesar dalam keamanan siber pada tahun 2023. Serangan ransomware telah berkembang dari serangan yang hanya mengenkripsi data menjadi ancaman yang lebih kompleks yang juga mencuri data dan mengancam publikasi data sensitif. Teknik seperti double extortion semakin umum, di mana pelaku ancaman tidak hanya mengenkripsi data tetapi juga mengancam untuk membocorkan data yang dicuri jika tebusan tidak dibayar. Menurut laporan terbaru, sekitar 70% organisasi mengalami serangan ransomware yang melibatkan ancaman kebocoran data pada tahun 2023, menunjukkan peningkatan signifikan dibandingkan tahun-tahun sebelumnya.

2)Phishing dan Spear Phishing

Serangan phishing dan spear phishing semakin canggih, menggunakan teknik manipulasi psikologis untuk menargetkan individu dan organisasi. Pada tahun 2023, pelaku ancaman menggunakan email yang lebih meyakinkan dan teknik social engineering untuk mencuri kredensial dan informasi pribadi. Data menunjukkan bahwa sekitar 60% serangan phishing berhasil mengecoh pengguna karena kurangnya kesadaran dan pelatihan. Phishing juga semakin sering dilakukan melalui saluran komunikasi baru, seperti media sosial dan aplikasi perpesanan.

3)Advanced Persistent Threats (APT)

APT adalah ancaman yang terus-menerus menargetkan organisasi dengan tujuan jangka panjang untuk mencuri data sensitif atau merusak sistem. Serangan APT pada tahun 2023 telah menunjukkan peningkatan dalam kompleksitas dan ketahanan. APT menggunakan teknik seperti

lateral movement dan credential dumping untuk mengeksploitasi kelemahan dalam jaringan dan memperoleh akses ke informasi berharga secara bertahap. Laporan menunjukkan bahwa 50% dari serangan APT baru-baru ini memanfaatkan kerentanan perangkat lunak yang belum diperbarui.

4)Kelemahan dalam Internet of Things (IoT)

Peningkatan perangkat IoT yang terhubung ke jaringan juga menambah tantangan keamanan siber. Banyak perangkat IoT memiliki kelemahan dalam hal keamanan, seperti default credentials dan enkripsi yang lemah. Pada tahun 2023, serangan terhadap perangkat IoT telah meningkat, dengan pelaku ancaman memanfaatkan kerentanan ini untuk mendapatkan akses ke jaringan internal. Sekitar 40% serangan terhadap perangkat IoT berhasil karena kurangnya perlindungan yang memadai.

5)Solusi Terbaru dalam Keamanan Siber

Teknologi Deteksi dan Respons yang Ditingkatkan

Untuk menghadapi ancaman siber yang semakin kompleks, teknologi deteksi dan respons telah mengalami kemajuan signifikan. Sistem SIEM (Security Information and Event Management) dan EDR (Endpoint Detection and Response) kini menggunakan kecerdasan buatan (AI) dan pembelajaran mesin (machine learning) untuk mengidentifikasi dan merespons ancaman secara lebih cepat dan akurat. Teknologi ini memungkinkan pemantauan real-time dan analisis data yang lebih baik untuk mendeteksi pola ancaman dan aktivitas yang mencurigakan. Penggunaan AI dalam deteksi ancaman telah meningkatkan efisiensi dan efektivitas respons terhadap insiden siber.

6)Enkripsi dan Perlindungan Data yang Ditingkatkan

Peningkatan enkripsi dan perlindungan data menjadi prioritas utama dalam strategi keamanan siber. Teknologi enkripsi end-to-end, seperti Quantum Cryptography dan Homomorphic Encryption, semakin diterapkan untuk melindungi data sensitif dari akses yang tidak sah. Solusi ini memastikan bahwa data tetap aman meskipun terjadi pelanggaran keamanan. Selain itu, pendekatan seperti Zero Trust Architecture (ZTA) menjadi semakin populer, yang memastikan bahwa setiap permintaan akses diperiksa secara independen tanpa menganggap kepercayaan internal.

7)Pelatihan dan Kesadaran Pengguna

Mengurangi risiko serangan phishing dan social engineering memerlukan peningkatan kesadaran dan pelatihan pengguna. Program pelatihan keamanan yang berkelanjutan dan simulasi serangan phishing membantu meningkatkan kesadaran pengguna dan kemampuan mereka untuk mengenali ancaman. Data menunjukkan bahwa organisasi yang menerapkan pelatihan keamanan yang konsisten mengalami penurunan insiden phishing sebesar 30% dibandingkan dengan yang tidak menerapkan pelatihan.

8)Kebijakan dan Regulasi Bar

Kebijakan dan regulasi baru juga memainkan peran penting dalam meningkatkan keamanan siber. Regulasi seperti GDPR di Eropa dan CCPA di California menetapkan standar untuk perlindungan data dan privasi. Pada tahun 2023, terdapat peningkatan dalam penerapan regulasi global yang mengharuskan organisasi untuk melaporkan insiden keamanan dan melindungi data pribadi. Penerapan kebijakan ini membantu mendorong praktik keamanan yang lebih baik dan memastikan akuntabilitas dalam pengelolaan data.

9)Penggunaan Teknologi Blockchain

Blockchain telah diterapkan sebagai solusi untuk meningkatkan keamanan data dan integritas transaksi. Teknologi blockchain menyediakan ledger yang tidak dapat diubah dan transaksi yang dapat diverifikasi yang membantu dalam mengamankan data dan mencegah

pemalsuan. Penerapan blockchain dalam keamanan siber semakin berkembang, terutama dalam konteks identitas digital dan keamanan transaksi.

10)Evaluasi dan Diskusi

Hasil penelitian menunjukkan bahwa tantangan dalam keamanan siber tahun 2023 semakin kompleks dan memerlukan pendekatan yang multifaset. Serangan ransomware, phishing, APT, dan kerentanan IoT menunjukkan bahwa pelaku ancaman semakin canggih dan inovatif. Untuk mengatasi tantangan ini, solusi terbaru seperti teknologi deteksi berbasis AI, enkripsi canggih, pelatihan pengguna, kebijakan regulasi, dan blockchain telah diterapkan secara luas. Meskipun solusi ini menawarkan kemajuan signifikan dalam mengatasi ancaman, masih ada tantangan dalam implementasinya. Misalnya, penerapan enkripsi dan Zero Trust Architecture dapat menambah kompleksitas dan biaya operasional. Pelatihan pengguna juga memerlukan sumber daya dan komitmen yang berkelanjutan. Oleh karena itu, organisasi perlu mengevaluasi solusi yang paling sesuai dengan kebutuhan mereka dan memastikan bahwa pendekatan keamanan mereka dapat beradaptasi dengan ancaman yang terus berkembang.

KESIMPULAN DAN SARAN

Kesimpulan

Keamanan siber di tahun 2023 menghadapi tantangan yang semakin kompleks seiring dengan berkembangnya teknologi. Serangan siber yang lebih canggih memerlukan pendekatan baru dalam melindungi data dan sistem. Pendekatan Zero Trust, pemanfaatan AI untuk deteksi ancaman, serta kerjasama antar entitas menjadi solusi utama yang diidentifikasi dalam penelitian ini. Implementasi solusi-solusi ini secara tepat dapat membantu mengurangi risiko serangan siber dan melindungi data serta sistem dari ancaman yang ada

Saran

Berdasarkan hasil penelitian, disarankan agar organisasi dan pemerintah lebih proaktif dalam mengadopsi pendekatan Zero Trust dan memanfaatkan teknologi AI dalam deteksi ancaman. Selain itu, pelatihan dan kesadaran keamanan siber bagi karyawan harus ditingkatkan untuk meminimalisir human error yang dapat menyebabkan kebocoran data. Kerjasama yang lebih erat antara sektor publik dan swasta juga diperlukan untuk berbagi informasi dan strategi dalam menghadapi ancaman siber.

DAFTAR PUSTAKA

BleepingComputer. (2023). Top Cybersecurity Threats and Trends of 2023. Retrieved from https://www.bleepingcomputer.com

Check Point. (2023). Check Point Cyber Security Report 2023. Retrieved from https://www.checkpoint.com

Cisco. (2023). Cisco Annual Cybersecurity Report 2023. Retrieved from https://www.cisco.com

CISA. (2023). CISA Insights: Ransomware. Retrieved from https://www.cisa.gov

Cloud Security Alliance. (2023). Cloud Security Trends 2023. Retrieved from https://cloudsecurityalliance.org

CrowdStrike. (2023). CrowdStrike Global Threat Report 2023. Retrieved from https://www.crowdstrike.com

ENISA. (2023). ENISA Threat Landscape Report 2023. Retrieved from https://www.enisa.europa.eu

Europol. (2023). Internet Organised Crime Threat Assessment (IOCTA) 2023. Retrieved from https://www.europol.europa.eu

FireEye. (2023). M-Trends 2023: A View from the Front Lines of Cybersecurity. Retrieved from https://www.mandiant.com

Forrester. (2023). Forrester Wave™: Endpoint Security Software, Q1 2023. Retrieved from https://go.forrester.com

Gartner. (2023). Market Guide for Endpoint Detection and Response Solutions. Retrieved from https://www.gartner.com

IBM. (2023). IBM X-Force Threat Intelligence Index 2023. Retrieved from https://www.ibm.com/security

IEEE. (2023). IEEE Transactions on Information Forensics and Security. Retrieved from https://ieeexplore.ieee.org

Kaspersky Lab. (2023). The State of Ransomware 2023: Attacks, Trends, and Solutions. Retrieved from https://www.kaspersky.com

McAfee. (2023). McAfee Labs Threats Report: August 2023. Retrieved from https://www.mcafee.com

NIST. (2023). NIST Cybersecurity Framework: A Guide to Managing Cybersecurity Risk. Retrieved from https://www.nist.gov/cyberframework

Palo Alto Networks. (2023). Unit 42 Threat Report 2023. Retrieved from https://www.paloaltonetworks.com

SANS Institute. (2023). SANS 2023 Cybersecurity Trends. Retrieved from https://www.sans.org

Symantec. (2023). Internet Security Threat Report 2023. Retrieved from https://www.broadcom.com/company/newsroom/press-releases/2023/

Trend Micro. (2023). Trend Micro Security Roundup Report 2023. Retrieved from https://www.trendmicro.com