Mutiara : Jurnal Penelitian dan Karya Ilmiah
Volume 4, Nomor 2, April 2026
e-ISSN :2988-3148; p-ISSN :2988-313X, Hal 67-84
DOI: https://doi.org/10.59059/mutiara.v4i2.3264
Tersedia: https://journal.staiypiqbaubau.ac.id/index.php/Mutiara

Penerapan Extended Detection and Response (XDR) Platform di Pelanggan PT Neotech Cakrawala Indonesia

Ika Yulistiyah[1], Anwar T. Sitoroes[2*], Samroh[3], Ahmad Soderi[4], Juwari[5]
[1-5]Teknologi Informasi, Sekolah Tinggi Manajemen Informatika dan Komputer Mercusuar, Bekasi, Indonesia
Email: ikayulistia19@gmail.com[1], anwar@mercusuar.ac.id[2], samroh74@gmail.com[3], ahmad@mercusuar.ac.id[4], joe.marada1@gmail.com[5]
[*]*Penulis korespondensi: anwar@mercusuar.ac.id*

Abstract. *The growing dependence on web-based systems has increased exposure to cybersecurity threats, particularly web defacement attacks that compromise system integrity, organizational reputation, and public trust. Conventional security approaches such as Endpoint Detection and Response (EDR) and Security Information and Event Management (SIEM) are frequently implemented in fragmented ways, limiting comprehensive threat visibility and slowing incident response. This study examines the implementation of Extended Detection and Response (XDR) integrated with an Agile approach to enhance early detection and response to web defacement attacks. Employing a qualitative case study design, data were collected through semi-structured interviews, observation, and document analysis involving cybersecurity analysts, system administrators, and IT managers. The findings reveal that XDR improves cross-domain threat visibility through integrated data correlation, enabling faster anomaly detection and more efficient incident handling. The Agile approach supports adaptive implementation, iterative evaluation, and cross-functional collaboration, strengthening organizational responsiveness to evolving cyber threats. The study contributes theoretically by reinforcing a holistic cybersecurity framework integrating technological and organizational dimensions, and practically by offering strategic insights for organizations seeking to enhance web security resilience.*

Keywords: *Agile; Cyber; Extended Detection Response; Security; Web Defacement.*

Abstrak. Ketergantungan yang semakin besar pada sistem berbasis web telah meningkatkan paparan terhadap ancaman keamanan siber, khususnya serangan defacement web yang mengorbankan integritas sistem, reputasi organisasi, dan kepercayaan publik. Pendekatan keamanan konvensional seperti Endpoint Detection and Response (EDR) dan Security Information and Event Management (SIEM) sering diterapkan secara terfragmentasi, membatasi visibilitas ancaman yang komprehensif dan memperlambat respons insiden. Studi ini meneliti implementasi Extended Detection and Response (XDR) yang terintegrasi dengan pendekatan Agile untuk meningkatkan deteksi dini dan respons terhadap serangan web defacement. Dengan menggunakan desain studi kasus kualitatif, data dikumpulkan melalui wawancara semi-terstruktur, observasi, dan analisis dokumen yang melibatkan analis keamanan siber, administrator sistem, dan manajer TI. Temuan tersebut mengungkapkan bahwa XDR meningkatkan visibilitas ancaman lintas domain melalui korelasi data terintegrasi, memungkinkan deteksi anomali yang lebih cepat dan penanganan insiden yang lebih efisien. Pendekatan Agile mendukung implementasi adaptif, evaluasi iteratif, dan kolaborasi lintas fungsi, memperkuat responsivitas organisasi terhadap ancaman siber yang terus berkembang. Studi ini berkontribusi secara teoretis dengan memperkuat kerangka kerja keamanan siber holistik yang mengintegrasikan dimensi teknologi dan organisasi, serta secara praktis dengan menawarkan wawasan strategis bagi organisasi yang ingin meningkatkan ketahanan keamanan web.

Kata kunci: Agile; Deteksi Respons Yang Diperluas; Keamanan; Siber; Web Defacement.

1. LATAR BELAKANG

Kemajuan pesat teknologi informasi telah membawa perubahan signifikan dalam pengelolaan sistem digital di berbagai sektor, termasuk pemerintahan, pendidikan, dan industri (Williams, 2021). Transformasi digital ini telah meningkatkan ketergantungan organisasi pada aplikasi berbasis web sebagai media utama untuk penyampaian informasi dan aktivitas operasional. Namun, selain manfaat ini, muncul ancaman keamanan siber yang semakin kompleks dan dinamis, salah satunya adalah serangan *defacement web*. Serangan semacam ini

Naskah Masuk: 27 Februari 2026; Revisi: 24 Maret 2026; Diterima: 27 April 2026; Terbit: 30 April 2026

tidak hanya memengaruhi tampilan situs web, tetapi juga mencerminkan kelemahan dalam sistem keamanan dan dapat mengurangi kepercayaan publik terhadap organisasi yang bertanggung jawab mengelola sistem informasi.

Secara global, *defacement web* tetap menjadi salah satu bentuk serangan siber yang paling sering terjadi, terutama yang menargetkan institusi publik dan situs web organisasi pendidikan (Albalawi et al., 2022). Laporan keamanan siber internasional menunjukkan bahwa ribuan situs web mengalami insiden defacement setiap tahun, biasanya melalui eksploitasi kerentanan aplikasi web, kredensial yang lemah, atau konfigurasi server yang salah (Kumar et al., 2021). Di Indonesia, Badan Siber dan Kripto Nasional (BSSN) juga melaporkan bahwa serangan siber terhadap situs web pemerintah lokal dan institusi pendidikan masih didominasi oleh insiden defacement, yang sering dilakukan untuk tujuan vandalisme digital atau pesan ideologis (Ukas et al., 2025).

Fenomena *defacement web* tidak boleh dipandang hanya sebagai masalah teknis, tetapi juga sebagai perhatian sosial dan kelembagaan. Perubahan tidak sah pada konten situs resmi dapat memicu kecemasan publik, merusak reputasi organisasi, dan merusak legitimasi institusional. Dalam konteks organisasi layanan publik, gangguan semacam itu dapat menghambat akses ke informasi dan layanan digital yang merupakan hak publik. Oleh karena itu, upaya untuk mencegah dan memungkinkan deteksi dini serangan kerusakan web merupakan isu strategis yang memerlukan penyelidikan ilmiah mendalam.

PT Neotech Cakrawala Indonesia adalah perusahaan yang bergerak di bidang solusi keamanan Teknologi Informasi (TI) dan data center, yang berlokasi di Jakarta Barat. Perusahaan ini menyediakan layanan komprehensif mulai dari perencanaan, implementasi, pemeliharaan sistem keamanan, hingga pelatihan teknis bagi klien. Neotech memiliki spesialisasi dalam layanan seperti penetration *Testing* (*black box, white box, grey box*), *Security Operations Center as a Service* (SOCaaS), serta solusi keamanan aplikasi termasuk *Web Application Firewall* (WAF), *Dynamic Application Security Testing* (DAST), dan *Static Application Security Testing* (SAST). Dengan tim bersertifikasi dan pengalaman melayani berbagai sektor seperti pemerintahan, perbankan, manufaktur, dan rumah sakit, PT Neotech Cakrawala Indonesia berkomitmen untuk membantu klien menjaga keamanan siber secara real-time dan meningkatkan efisiensi operasional teknologi mereka, dengan menyediakan solusi keamanan *Extended Detection And Response* (XDR).

Dalam praktiknya, banyak organisasi masih mengandalkan pendekatan keamanan tradisional seperti *Endpoint Detection and Response* (EDR) atau *Security Information and Event Management* (SIEM). Meskipun pendekatan-pendekatan ini memainkan peran penting,

pelaksanaannya seringkali bersifat parsial dan terfragmentasi. EDR terutama berfokus pada aktivitas tingkat endpoint, sementara SIEM menekankan pengumpulan dan analisis log tanpa kemampuan respons yang sepenuhnya terintegrasi (Yusof, 2024). Kondisi ini menyulitkan organisasi untuk mencapai visibilitas ancaman yang komprehensif, terutama untuk serangan lintas lapisan seperti defasemen web.

Keterbatasan pendekatan keamanan tradisional semakin didukung oleh temuan empiris dari studi sebelumnya yang menunjukkan keterlambatan dalam deteksi ancaman dan respons insiden. Beberapa studi mengungkapkan bahwa sistem keamanan yang tidak terintegrasi cenderung menghasilkan peringatan terisolasi, sehingga analis keamanan harus meluangkan waktu tambahan untuk mengkorelasikan data dan membuat keputusan (Islam et al., 2019). Situasi ini menjadi semakin kritis ketika organisasi menghadapi keterbatasan dalam sumber daya manusia keamanan siber.

Sebagai respons terhadap kompleksitas ancaman siber modern, konsep *Extended Detection and Response* (XDR) telah dikembangkan dan diadopsi oleh berbagai organisasi. XDR menawarkan pendekatan keamanan yang lebih terintegrasi dengan mengonsolidasikan data dari berbagai sumber seperti *endpoint*, jaringan, server, dan aplikasi ke dalam satu platform analitis. Pendekatan ini memungkinkan deteksi ancaman yang lebih kontekstual dan respons insiden yang lebih cepat serta terkoordinasi (Aminu et al., 2024).

Dalam konteks *defasemen web*, XDR memiliki potensi signifikan untuk meningkatkan kemampuan deteksi dini dan respons insiden. Dengan mengkorelasikan aktivitas mencurigakan di berbagai lapisan sistem, XDR dapat mengidentifikasi pola serangan yang mungkin tidak terdeteksi oleh sistem keamanan konvensional. Studi terbaru menunjukkan bahwa implementasi XDR meningkatkan efektivitas deteksi serangan berbasis web dan secara signifikan mengurangi waktu respons insiden (Chung et al., 2023).

Namun demikian, penerapan XDR tidak tanpa tantangan, terutama terkait kompleksitas sistem dan kebutuhan adaptasi terhadap lingkungan organisasi yang dinamis. Banyak organisasi menghadapi kesulitan dalam menerapkan solusi keamanan yang kaku dan linier, mengingat sifat ancaman siber yang berkembang pesat. Oleh karena itu, pendekatan implementasi yang adaptif dan fleksibel diperlukan untuk memastikan sistem keamanan berkembang sesuai dengan ancaman yang muncul dan kebutuhan organisasi.

Pendekatan Agile menjadi sangat relevan dalam penerapan sistem keamanan siber modern. Agile menekankan iterasi berkelanjutan, kolaborasi tim, dan responsivitas terhadap perubahan. Dalam pengembangan dan penerapan sistem keamanan, Agile memungkinkan organisasi melakukan evaluasi dan perbaikan bertahap berdasarkan temuan nyata dan umpan

balik pengguna (Marçal et al., 2025). Pendekatan ini dianggap lebih cocok untuk menangani ancaman siber yang tidak dapat diprediksi dan terus berkembang.

Beberapa studi sebelumnya telah meneliti penerapan *Agile* dalam pengembangan perangkat lunak; namun, penelitian yang secara khusus mengintegrasikan Agile dengan implementasi XDR untuk deteksi defacement web masih terbatas. Sebagian besar studi yang ada berfokus pada aspek teknis XDR atau efektivitas Agile dalam pengembangan aplikasi secara umum, tanpa menelaah secara mendalam proses implementasi keamanan siber adaptif (Handri et al., 2024). Kesenjangan ini menyoroti perlunya penyelidikan lebih lanjut.

Selain itu, penelitian sebelumnya cenderung mengandalkan pengukuran kinerja kuantitatif, sementara eksplorasi mendalam tentang proses implementasi, pengalaman, dan dinamika organisasi dalam konteks keamanan siber masih terbatas. Oleh karena itu, pendekatan kualitatif diperlukan untuk memahami bagaimana XDR diimplementasikan, tantangan yang dihadapi, dan bagaimana Agile mendukung praktik keamanan siber yang sukses dalam lingkungan organisasi.

2. KAJIAN TEORITIS

Keamanan siber merupakan serangkaian tindakan dan praktik yang bertujuan melindungi sistem, jaringan, aplikasi, dan data dari akses tidak sah maupun serangan digital (Irawan et al., 2024). Keamanan siber didasarkan pada tiga prinsip utama yang dikenal sebagai *CIA Triad*, yaitu *confidentiality*, *integrity*, dan *availability* (D. Kurniawan, 2025). Kerahasiaan berkaitan dengan pembatasan akses terhadap informasi, integritas menjaga agar data tidak diubah secara ilegal, sedangkan ketersediaan memastikan sistem dapat digunakan oleh pihak yang berhak. Ketiga prinsip tersebut menjadi dasar dalam membangun sistem pertahanan siber pada organisasi.

Ancaman siber merupakan berbagai kondisi atau aktivitas yang dapat memanfaatkan kelemahan sistem digital untuk menimbulkan kerugian. Perkembangan teknologi membuat ancaman siber semakin kompleks dan tidak hanya bertujuan merusak sistem, tetapi juga dapat digunakan untuk pencurian data, pemerasan, spionase, dan aktivitas ilegal lainnya (Harahap et al., 2025). Karena itu, organisasi membutuhkan pendekatan keamanan yang tidak hanya mengandalkan pertahanan tradisional, tetapi juga mampu mengenali pola perilaku dan karakteristik ancaman yang terus berubah.

Serangan siber merupakan tindakan yang dilakukan secara sengaja untuk memperoleh akses tidak sah, merusak, mengubah, atau mengganggu sistem komputer, jaringan, maupun data (Suharto & Apriyani, 2021). Serangan dapat dilakukan melalui berbagai teknik dan

memanfaatkan kelemahan pada sistem atau aplikasi. Dalam menghadapi serangan, pemahaman terhadap taktik, teknik, dan prosedur penyerang menjadi penting karena dapat membantu organisasi mengenali pola serangan dan menentukan langkah pencegahan maupun penanganan yang sesuai.

Salah satu bentuk serangan yang menjadi fokus penelitian adalah *Web Defacement*. *Web Defacement* merupakan serangan ketika pelaku mengubah tampilan atau isi halaman situs secara ilegal (Jumaryadi et al., 2024). Serangan tersebut dapat dilakukan dengan memanfaatkan kelemahan pada aplikasi web, konfigurasi server, sistem manajemen konten, atau mekanisme keamanan lainnya. Walaupun tidak selalu bertujuan mencuri data, perubahan tidak sah pada situs dapat mengganggu layanan, menurunkan kredibilitas, dan merusak reputasi organisasi di mata pengguna.

Deteksi dan respons ancaman siber merupakan bagian penting dalam sistem pertahanan digital. Deteksi berfungsi mengidentifikasi aktivitas atau pola yang menunjukkan adanya ancaman, sedangkan respons bertujuan mengurangi atau menghentikan dampak setelah ancaman ditemukan (Slamet, 2025). Proses respons dapat mencakup isolasi sistem yang terdampak, penghilangan ancaman, serta pemulihan sistem. Oleh karena itu, sistem keamanan membutuhkan kemampuan deteksi yang cepat dan mekanisme respons yang terkoordinasi agar dampak serangan dapat diminimalkan.

Extended Detection and Response (XDR) merupakan pendekatan keamanan yang mengintegrasikan data dan kemampuan deteksi dari berbagai sumber dalam satu lingkungan keamanan (Risyani et al., 2025). XDR dapat menggabungkan informasi dari endpoint, jaringan, aplikasi, cloud, dan sumber keamanan lainnya sehingga organisasi memperoleh visibilitas ancaman yang lebih luas. Melalui korelasi berbagai data tersebut, XDR dapat membantu mengidentifikasi hubungan antara aktivitas yang sebelumnya terlihat sebagai peristiwa terpisah dan mempercepat proses investigasi serta respons terhadap insiden.

XDR memiliki cakupan yang lebih luas dibandingkan solusi keamanan yang hanya berfokus pada satu lapisan. EDR terutama berfokus pada perlindungan endpoint, sedangkan XDR mengintegrasikan informasi dari berbagai lingkungan teknologi informasi. Dalam penerapannya, XDR juga dapat berhubungan dengan SIEM, SOAR, UEBA, firewall, dan berbagai sumber log lainnya. Integrasi tersebut bertujuan menciptakan visibilitas keamanan yang lebih komprehensif dan mendukung respons yang lebih terkoordinasi.

Dalam penelitian ini, penerapan XDR menggunakan Stellar Cyber Open XDR sebagai platform utama. Platform tersebut berfungsi sebagai pusat pengumpulan, analisis, dan korelasi data keamanan dari berbagai sumber. Arsitekturnya mencakup *Sensor Data Collector*, platform

XDR, analitik berbasis *machine learning*, UEBA, *threat intelligence*, modul respons otomatis melalui SOAR, *security data lake*, dan *unified dashboard*. Integrasi tersebut memungkinkan aktivitas keamanan dipantau dalam satu tampilan dan mendukung proses deteksi, investigasi, serta respons terhadap ancaman.

Metodologi Agile merupakan pendekatan implementasi yang menekankan proses bertahap, adaptif, kolaboratif, dan terbuka terhadap umpan balik. Dalam penerapan XDR pada penelitian ini, Agile dilakukan melalui tahapan *Plan, Design, Develop, Test, Deploy, Review,* dan *Launch*. Setiap tahap memungkinkan sistem dievaluasi dan disempurnakan berdasarkan kebutuhan serta hasil implementasi sebelumnya. Pendekatan ini sesuai untuk lingkungan keamanan siber yang menghadapi ancaman dinamis karena memungkinkan perubahan dan perbaikan dilakukan secara berkelanjutan. Dengan demikian, kombinasi XDR dan Agile menjadi dasar teoritis penting dalam membangun sistem keamanan yang lebih terintegrasi, adaptif, dan mampu mendukung deteksi serta respons terhadap Web Defacement secara lebih cepat.

3. METODE PENELITIAN

Studi ini menggunakan pendekatan penelitian kualitatif menggunakan desain studi kasus. Pendekatan ini dipilih karena studi ini bertujuan untuk memperoleh pemahaman mendalam tentang proses implementasi *Extended Detection and Response* (XDR) dalam mendeteksi dan merespons serangan *defacement web*, serta peran pendekatan Agile dalam mendukung adaptabilitas sistem keamanan siber dalam konteks organisasi. Pendekatan studi kasus memungkinkan eksplorasi fenomena secara mendalam dan holistik, terutama ketika batas antara fenomena dan konteksnya tidak didefinisikan dengan jelas (Yin, 2017). Pendekatan ini dianggap tepat untuk menelaah dinamika, pengalaman, dan praktik nyata dalam implementasi keamanan siber yang tidak dapat ditangkap secara memadai melalui metode kuantitatif.

Penelitian ini dilakukan di sebuah organisasi yang beroperasi di bidang teknologi informasi dan manajemen sistem berbasis web, dengan fokus pada lingkungan operasional yang telah mengalami atau berisiko tinggi terhadap serangan defacement web. Studi ini dilakukan dari Januari hingga April 2025, mencakup tahapan perencanaan penelitian, pengumpulan data, analisis, dan validasi. Pemilihan lokasi penelitian didasarkan pada ketersediaan sistem XDR yang telah diterapkan dan akses peneliti terhadap informan utama yang terlibat langsung dalam manajemen keamanan siber.

Karakteristik pelanggan yang menjadi objek penelitian perlu dipahami dalam kaitannya dengan lingkungan sistem yang dilindungi oleh PT Neotech Cakrawala Indonesia. Pelanggan dalam penelitian ini merupakan organisasi yang menggunakan layanan dan sistem berbasis web sebagai bagian dari kegiatan operasional dan penyampaian informasi. Lingkungan pelanggan memiliki kebutuhan keamanan yang berbeda-beda sesuai dengan karakteristik infrastruktur, aplikasi, jaringan, dan tingkat paparan terhadap ancaman siber. Oleh karena itu, penerapan XDR tidak diposisikan sebagai proses yang sepenuhnya seragam, tetapi disesuaikan dengan kondisi keamanan dan kebutuhan operasional masing-masing lingkungan pelanggan. Fokus penelitian diarahkan pada pengalaman penerapan XDR dalam lingkungan pelanggan yang memiliki risiko terhadap gangguan keamanan aplikasi dan potensi serangan web defacement.

Informan dalam penelitian memiliki peran yang berbeda sesuai dengan keterlibatannya dalam proses penerapan dan pengelolaan keamanan. Analis keamanan siber memberikan informasi mengenai proses pemantauan peringatan, analisis korelasi data, identifikasi pola ancaman, dan penanganan insiden. Administrator sistem berperan memberikan informasi mengenai kondisi infrastruktur, proses integrasi sumber data, konfigurasi sistem, serta perubahan teknis yang diperlukan selama penerapan XDR. Sementara itu, manajer teknologi informasi memberikan perspektif mengenai kebutuhan organisasi, koordinasi antarunit, pengambilan keputusan, serta evaluasi penerapan sistem. Perbedaan peran tersebut memungkinkan penelitian memperoleh gambaran penerapan XDR dari aspek operasional, teknis, dan manajerial.

Para peserta penelitian dipilih menggunakan sampling bertujuan, dengan kriteria yang memerlukan keterlibatan langsung dalam perencanaan, implementasi, atau pengelolaan sistem keamanan siber. Peserta termasuk analis keamanan siber, administrator sistem, dan manajer teknologi informasi. Selain itu, pengambilan sampel bola salju digunakan untuk mengidentifikasi informan tambahan yang direkomendasikan oleh peserta awal yang memiliki pengetahuan dan pengalaman relevan. Pendekatan ini memungkinkan peneliti memperoleh perspektif yang lebih kaya dan komprehensif tentang implementasi XDR dan penerapan pendekatan *Agile* dalam organisasi (Pissanidis & Demertzis, 2024).

Teknik pengumpulan data terdiri dari wawancara semi-terstruktur, observasi non-peserta, dan analisis dokumen. Wawancara semi-terstruktur digunakan untuk mengeksplorasi pengalaman, persepsi, dan praktik peserta terkait implementasi XDR dan proses Agile. Observasi dilakukan untuk memahami alur kerja keamanan dan respons terhadap potensi serangan *defacement web*. Analisis dokumen mencakup peninjauan kebijakan keamanan, laporan insiden, dan dokumentasi teknis sistem. Penggunaan berbagai teknik pengumpulan

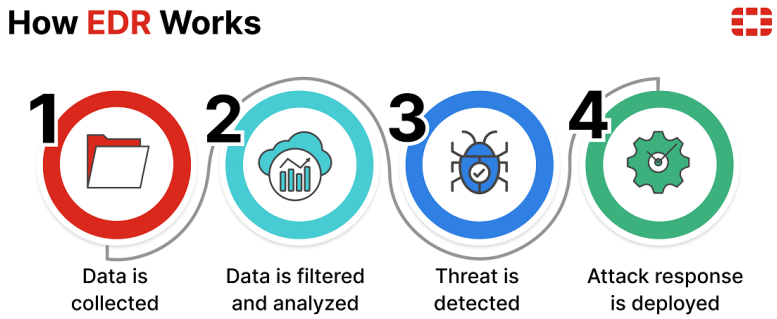
data bertujuan meningkatkan kedalaman data dan memungkinkan triangulasi metodologis (Creswell & Poth, 2017).

Data yang dikumpulkan dalam penelitian tidak hanya berupa informasi hasil wawancara, tetapi juga mencakup bukti dan informasi yang berkaitan dengan aktivitas keamanan sistem. Bentuk data tersebut meliputi log aktivitas aplikasi web, informasi aktivitas jaringan, data dari endpoint, peringatan keamanan, catatan insiden, dokumentasi konfigurasi, serta hasil pengamatan terhadap proses pemantauan dan respons. Data wawancara digunakan untuk menjelaskan pengalaman dan penilaian informan terhadap proses penerapan XDR, sedangkan data observasi dan dokumen digunakan untuk memahami bagaimana informasi keamanan dikumpulkan, dikorelasikan, dan digunakan dalam proses investigasi.

Dalam proses analisis ancaman, data dari berbagai sumber digunakan untuk mengidentifikasi keterkaitan antara aktivitas yang pada awalnya terlihat terpisah. Misalnya, aktivitas yang muncul pada aplikasi web dibandingkan dengan perubahan aktivitas endpoint, pola akses jaringan, atau peringatan keamanan lain yang terjadi dalam periode yang berkaitan. Korelasi tersebut memungkinkan peneliti dan tim keamanan mengidentifikasi pola anomali secara lebih kontekstual, sehingga suatu kejadian tidak hanya dinilai berdasarkan satu indikator. Dengan demikian, penggunaan data lintas sumber menjadi bagian penting dalam menemukan hubungan aktivitas yang berpotensi menunjukkan adanya percobaan serangan atau gangguan terhadap sistem pelanggan.

Validasi data dilakukan menggunakan beberapa strategi untuk memastikan kredibilitas dan kepercayaan temuan penelitian. Triangulasi sumber dan metode diterapkan dengan membandingkan data yang diperoleh dari wawancara, pengamatan, dan dokumentasi. Selain itu, pemeriksaan anggota dilakukan dengan mengonfirmasi temuan awal bersama peserta kunci untuk memastikan keselarasan antara interpretasi peneliti dan pengalaman peserta. Jejak audit juga dijaga dengan mendokumentasikan seluruh proses penelitian secara sistematis untuk meningkatkan transparansi dan keandalan (Ahmed, 2024).

Analisis data mengikuti model interaktif yang diusulkan oleh Miles, Huberman, dan Saldaña, yang melibatkan kondensasi data, tampilan data, serta pengambilan dan verifikasi kesimpulan. Data wawancara ditranskripsi dan dianalisis secara tematik untuk mengidentifikasi pola, tema, dan hubungan antara konsep yang terkait dengan implementasi XDR dan pendekatan Agile. Proses analisis bersifat iteratif dan berkelanjutan bersamaan dengan pengumpulan data, memungkinkan peneliti menangkap dinamika dan perubahan yang muncul sepanjang proses penelitian (Miles et al., 2013).



Gambar 1. Cara Kerja EDR.

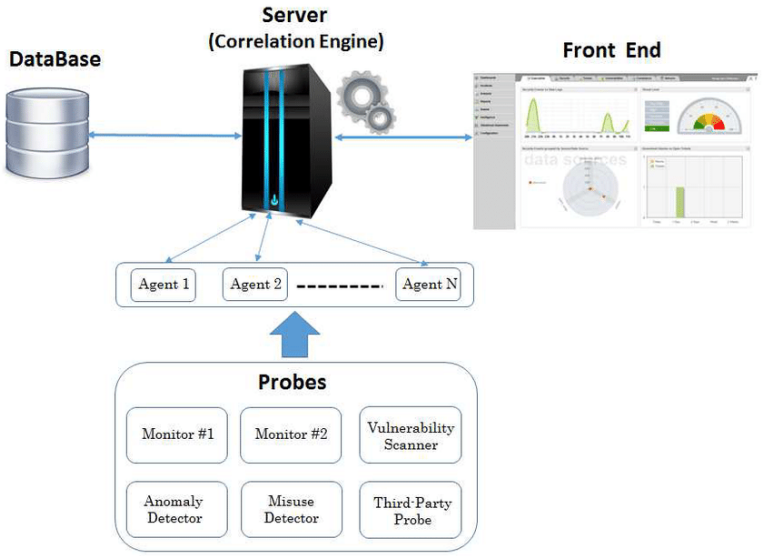
4. HASIL DAN PEMBAHASAN

Keamanan siber secara luas didefinisikan sebagai seperangkat teknologi, proses, dan mekanisme tata kelola yang komprehensif yang dirancang untuk melindungi sistem digital, jaringan, dan data dari akses tidak sah dan serangan berbahaya. Penelitian keamanan siber kontemporer menekankan bahwa perlindungan yang efektif tidak hanya membutuhkan perlindungan teknis tetapi juga penyelarasan organisasi dan manajemen strategis (Alam et al., 2025). Seiring organisasi semakin bergantung pada platform berbasis web untuk layanan operasional dan publik, keamanan aplikasi web telah menjadi domain penting dalam studi keamanan siber. Integritas, ketersediaan, dan kerahasiaan sistem web kini menjadi kunci untuk menjaga kredibilitas institusional dan kepercayaan digital.

Web defacement merupakan bentuk serangan siber yang persisten dan terlihat di mana penyerang mengubah konten situs web tanpa izin. Meskipun kadang dianggap sebagai serangan dengan kompleksitas rendah, *defacement web* dapat menandakan kerentanan sistemik yang lebih dalam dan menyebabkan kerusakan reputasi serta gangguan layanan. Studi menunjukkan bahwa defacement web sering mengeksploitasi kelemahan dalam sistem manajemen konten, konfigurasi server, atau mekanisme autentikasi (C. Kurniawan & Triayudi, 2024). Sifat berulang dari insiden semacam ini menyoroti perlunya mekanisme deteksi proaktif yang mampu mengidentifikasi anomali sebelum terjadi kerusakan signifikan.

Solusi keamanan tradisional, termasuk *Endpoint Detection and Response* (EDR) dan *Security Information and Event Management* (SIEM), telah lama diterapkan untuk memantau dan menganalisis kejadian keamanan. Namun, sistem-sistem ini sering beroperasi secara terpisah, membatasi visibilitas ancaman yang komprehensif dan memperlambat koordinasi respons (Paidy, 2025). Kerangka pemantauan yang terfragmentasi dapat menghasilkan peringatan terisolasi yang memerlukan korelasi manual, sehingga meningkatkan waktu yang

dibutuhkan untuk mendeteksi dan mengurangi serangan multi-vektor seperti penghancuran web. Keterbatasan ini mendorong pengembangan kerangka deteksi yang lebih terintegrasi.



Gambar 2. Arsitektur SIEM.

Sebelum penerapan XDR, kondisi pemantauan keamanan pada lingkungan pelanggan masih ditandai oleh penggunaan sumber informasi yang tersebar pada beberapa sistem. Informasi mengenai aktivitas aplikasi web, jaringan, dan endpoint belum selalu dapat dilihat secara bersamaan dalam satu konteks investigasi. Ketika muncul aktivitas mencurigakan, proses identifikasi membutuhkan pemeriksaan terhadap beberapa sumber informasi sebelum tim keamanan dapat menentukan hubungan antarperistiwa. Kondisi tersebut berpotensi menyebabkan waktu analisis menjadi lebih panjang, terutama apabila indikasi ancaman muncul secara bertahap dan tersebar pada lebih dari satu komponen sistem.

Dalam kondisi sebelum penerapan XDR, penanganan gangguan juga lebih bergantung pada proses pemeriksaan dan korelasi yang dilakukan secara manual oleh personel keamanan. Peringatan yang muncul dari satu sistem belum secara otomatis memberikan gambaran mengenai aktivitas lain yang berkaitan. Oleh sebab itu, kebutuhan untuk mengintegrasikan berbagai sumber telemetri keamanan menjadi salah satu alasan utama penerapan XDR pada lingkungan pelanggan.

Extended Detection and Response (XDR) telah muncul sebagai model keamanan canggih yang dirancang untuk mengintegrasikan data telemetri di seluruh titik akhir, jaringan, server, dan aplikasi ke dalam lingkungan analitik yang terpadu. Dengan mengkorelasikan data keamanan berlapis-lapis, XDR meningkatkan pemahaman ancaman kontekstual dan mempercepat respons insiden (Abd Rahman Wahid et al., 2025). Temuan empiris menunjukkan bahwa sistem deteksi terintegrasi secara signifikan mengurangi waktu rata-rata

untuk mendeteksi (MTTD) dan waktu rata-rata untuk merespons (MTTR) dibandingkan dengan pendekatan konvensional (Arifiansyah, 2025). Kemampuan ini menempatkan XDR sebagai solusi yang menjanjikan untuk mengurangi serangan berbasis web yang kompleks.

Meskipun ada kemajuan teknologi, efektivitas sistem keamanan siber juga dipengaruhi oleh strategi implementasi. Metodologi *Agile*, yang ditandai dengan pengembangan iteratif, kolaborasi, dan adaptabilitas, semakin diterapkan melampaui pengembangan perangkat lunak ke manajemen keamanan siber (Maidin et al., 2025). Mengintegrasikan prinsip *Agile* ke dalam implementasi XDR memungkinkan organisasi untuk terus menyesuaikan konfigurasi keamanan sebagai respons terhadap ancaman yang terus berkembang. Namun, penelitian terbatas secara eksplisit meneliti aplikasi gabungan XDR dan Agile dalam mengatasi defasemen web, menunjukkan adanya kesenjangan teoretis dan empiris yang ingin diatasi oleh studi ini.

Hasil studi ini menunjukkan bahwa penerapan *Extended Detection and Response* (XDR) secara signifikan meningkatkan kemampuan organisasi untuk mendeteksi dan merespons serangan defacement web. Berdasarkan wawancara dengan informan kunci, sistem XDR mampu mengintegrasikan berbagai sumber data keamanan seperti log aplikasi web, aktivitas jaringan, dan data endpoint ke dalam satu platform terpadu. Integrasi ini memungkinkan tim keamanan memperoleh pandangan yang lebih komprehensif tentang ancaman potensial dibandingkan pendekatan sebelumnya yang mengandalkan sistem keamanan yang terfragmentasi.

Proses penerapan XDR dilakukan secara bertahap agar integrasi sistem dapat disesuaikan dengan kondisi lingkungan pelanggan. Tahap awal dilakukan melalui identifikasi kebutuhan keamanan dan pemetaan sumber data yang tersedia, termasuk sumber log dan aktivitas dari aplikasi web, jaringan, serta endpoint. Tahap berikutnya adalah integrasi sumber-sumber tersebut ke dalam platform XDR agar informasi keamanan dapat dikumpulkan dalam lingkungan analisis yang lebih terpadu. Setelah integrasi dilakukan, konfigurasi sistem disesuaikan dengan kebutuhan pemantauan dan karakteristik aktivitas yang terdapat pada lingkungan pelanggan.

Tahap selanjutnya berfokus pada pengujian kemampuan sistem dalam menerima data, menghubungkan peristiwa, dan menghasilkan peringatan terhadap aktivitas yang tidak sesuai dengan pola normal. Hasil pengujian digunakan untuk menilai apakah terdapat sumber data yang belum terintegrasi secara optimal, peringatan yang memerlukan penyesuaian, atau proses respons yang perlu diperbaiki. Setelah tahap pengujian, sistem diterapkan secara operasional dan terus dievaluasi berdasarkan aktivitas keamanan yang terdeteksi. Dengan proses tersebut,

penerapan XDR tidak hanya berupa pemasangan platform, tetapi merupakan rangkaian kegiatan mulai dari pemetaan kondisi awal, integrasi, konfigurasi, pengujian, hingga evaluasi operasional.

Salah satu temuan utama adalah peningkatan kecepatan deteksi anomali dalam sistem web. Informan melaporkan bahwa sebelum implementasi XDR, perubahan tidak sah pada file web atau aktivitas mencurigakan sering kali hanya diidentifikasi setelah terjadi gangguan layanan. Setelah penerapan XDR, sistem ini mampu mengeluarkan peringatan dini berdasarkan korelasi aktivitas lintas sistem, memungkinkan kemungkinan serangan defacement web terdeteksi sejak dini. Temuan ini menunjukkan bahwa integrasi data lintas domain merupakan faktor krusial dalam meningkatkan efektivitas deteksi ancaman.

Selain peningkatan deteksi, studi ini juga mengungkapkan peningkatan dalam proses respons insiden. Sistem XDR memungkinkan tim keamanan melakukan analisis insiden dengan lebih efisien, karena informasi terkait ancaman disajikan dalam satu tampilan yang dikontekstualisasikan. Informan menunjukkan bahwa waktu yang dibutuhkan untuk mengidentifikasi sumber serangan dan menentukan langkah-langkah mitigasi secara signifikan berkurang dibandingkan saat EDR dan SIEM digunakan secara terpisah. Hal ini menunjukkan bahwa XDR berfungsi tidak hanya sebagai alat deteksi tetapi juga sebagai mekanisme pendukung keputusan dalam mengelola insiden kerusakan di web.

Perbandingan kondisi sebelum dan sesudah penerapan menunjukkan perubahan terutama pada proses deteksi dan penanganan gangguan. Sebelum penerapan XDR, identifikasi ancaman lebih banyak dilakukan melalui pemeriksaan terhadap informasi dari sistem yang terpisah, sehingga proses menentukan hubungan antarperistiwa membutuhkan waktu analisis yang lebih panjang. Setelah XDR digunakan, data dari beberapa sumber dapat dikorelasikan dalam satu lingkungan pemantauan, sehingga analis memperoleh konteks ancaman yang lebih lengkap dalam proses investigasi. Perubahan tersebut memungkinkan proses pendeteksian dan penentuan langkah mitigasi dilakukan secara lebih terarah dibandingkan dengan kondisi sebelumnya.

Perbedaan lain terlihat pada proses penanganan gangguan. Sebelum integrasi XDR, tim keamanan perlu mengumpulkan informasi dari beberapa sistem untuk memahami sumber dan dampak suatu kejadian. Setelah penerapan XDR, informasi yang berkaitan dengan suatu peringatan dapat dianalisis melalui hubungan data lintas domain, sehingga proses investigasi dapat dilakukan dengan langkah yang lebih terstruktur. Dalam penelitian ini, perbandingan tersebut ditunjukkan secara kualitatif berdasarkan pengalaman informan dan hasil pengamatan

terhadap perubahan proses kerja, karena fokus penelitian adalah memahami proses dan dampak implementasi, bukan melakukan pengukuran kuantitatif eksperimental terhadap kinerja sistem.

Untuk memberikan gambaran yang lebih konkret mengenai manfaat sistem, hasil penerapan dapat dilihat melalui kemampuan XDR dalam mengidentifikasi rangkaian aktivitas yang berpotensi berkaitan dengan gangguan keamanan aplikasi web. Sebagai contoh, suatu aktivitas mencurigakan dapat ditandai melalui munculnya perubahan atau aktivitas yang tidak sesuai dengan pola normal pada lingkungan aplikasi, kemudian dianalisis bersama informasi aktivitas jaringan dan data endpoint yang berkaitan. Dalam kondisi seperti ini, nilai utama XDR terletak pada kemampuan untuk tidak hanya menampilkan satu peringatan secara terpisah, tetapi membantu menghubungkan beberapa indikasi agar analis memperoleh konteks yang lebih lengkap mengenai kemungkinan sumber gangguan.

Temuan tersebut menunjukkan bahwa proses deteksi ancaman menjadi lebih bermakna ketika suatu indikasi diperiksa berdasarkan hubungan dengan aktivitas lain dalam lingkungan sistem. Dalam konteks ancaman web defacement, informasi mengenai aktivitas yang tidak biasa dapat menjadi dasar untuk melakukan pemeriksaan lebih lanjut sebelum gangguan berkembang menjadi perubahan tidak sah yang terlihat pada layanan web. Dengan demikian, penerapan XDR memberikan manfaat tidak hanya pada kemampuan menghasilkan peringatan, tetapi juga pada kemampuan mendukung proses investigasi dan pengambilan keputusan respons secara lebih cepat dan terkoordinasi.

Dari perspektif implementasi, pendekatan *Agile* memainkan peran penting dalam mendukung keberhasilan penerapan XDR. Berdasarkan pengamatan dan wawancara, praktik Agile memungkinkan proses implementasi dilakukan secara bertahap dan adaptif sesuai kebutuhan organisasi. Setiap iterasi implementasi dievaluasi dan disempurnakan berdasarkan temuan lapangan, memungkinkan peningkatan sistem secara berkelanjutan tanpa mengganggu aktivitas operasional inti. Pendekatan ini dianggap lebih fleksibel dibandingkan model implementasi linier tradisional.

Proses kerja bertahap dalam penerapan XDR dilakukan melalui siklus evaluasi dan perbaikan pada setiap tahapan implementasi. Setelah suatu tahap dilakukan, tim mengevaluasi hasil integrasi, kualitas data yang diterima, kemampuan sistem dalam menghasilkan peringatan, serta kesesuaian proses respons dengan kebutuhan operasional. Hasil evaluasi tersebut menjadi masukan untuk menentukan perubahan yang diperlukan pada tahap berikutnya. Dengan demikian, evaluasi tidak hanya dilakukan setelah seluruh sistem selesai diterapkan, tetapi berlangsung selama proses implementasi.

Mekanisme perbaikan dilakukan berdasarkan temuan yang muncul pada setiap iterasi. Apabila ditemukan sumber data yang belum memberikan informasi secara optimal, konfigurasi dan proses integrasinya dapat diperbaiki. Apabila peringatan belum memberikan konteks yang cukup bagi proses investigasi, tim dapat melakukan penyesuaian terhadap pengaturan dan alur analisis. Hasil pengamatan terhadap penggunaan sistem dan masukan dari pihak yang terlibat kemudian digunakan sebagai dasar evaluasi berikutnya. Pola tersebut menunjukkan bahwa pendekatan Agile berfungsi sebagai mekanisme pembelajaran berkelanjutan yang memungkinkan penerapan XDR disesuaikan secara bertahap dengan kondisi operasional dan perubahan ancaman.

Temuan juga menunjukkan bahwa kolaborasi pemangku kepentingan meningkat setelah adopsi pendekatan *Agile*. Tim keamanan, administrator sistem, dan manajer teknologi informasi aktif terlibat dalam proses evaluasi dan pengambilan keputusan. Kolaborasi ini memperkuat pemahaman bersama tentang risiko dan strategi mitigasi kerusakan web. Secara konseptual, hasil ini mendukung pandangan bahwa keamanan siber bukan sekadar masalah teknis tetapi proses organisasi yang membutuhkan koordinasi lintas fungsi.

Dalam konteks teori keamanan siber, hasilnya selaras dengan pendekatan keamanan terintegrasi yang menekankan visibilitas komprehensif dan respons insiden yang dikontekstualisasikan. XDR terbukti efektif mengatasi keterbatasan sistem keamanan tradisional yang terfragmentasi. Dengan mengkorelasikan data dari berbagai sumber, XDR memberikan nilai tambah dalam bentuk pemahaman ancaman yang lebih dalam, terutama untuk serangan web defacement yang melibatkan beberapa vektor serangan secara bersamaan.

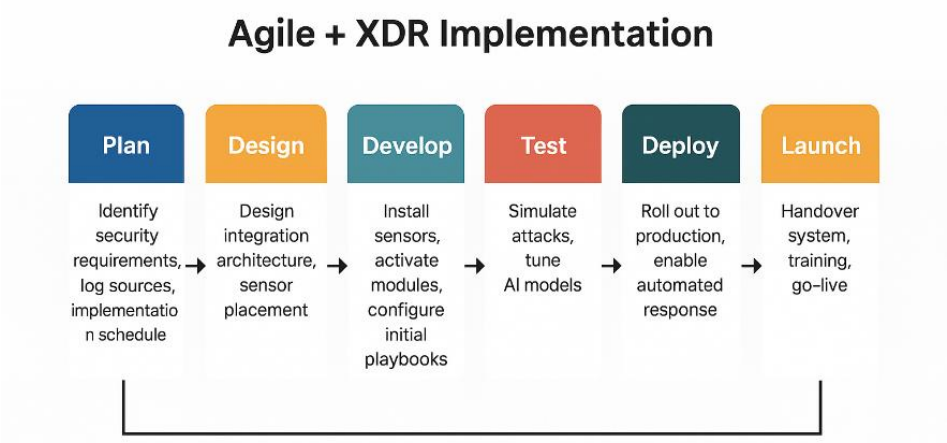
Diskusi temuan juga menyoroti tantangan dalam pelaksanaan XDR, khususnya terkait kebutuhan untuk meningkatkan kapasitas sumber daya manusia. Para informan mencatat bahwa memahami dan mengoperasikan sistem XDR membutuhkan pembelajaran berkelanjutan, terutama dalam menganalisis data yang berkorelasi dan menafsirkan peringatan keamanan. Namun, pendekatan *Agile* membantu mengurangi tantangan ini melalui proses pembelajaran iteratif dan evaluasi berkelanjutan, memungkinkan adaptasi bertahap terhadap sistem baru.

Selain kesiapan sumber daya manusia, penerapan XDR juga menghadapi tantangan yang berkaitan dengan kesiapan infrastruktur. Integrasi berbagai sumber data membutuhkan konektivitas dan konfigurasi yang sesuai agar informasi dari aplikasi, jaringan, endpoint, dan sumber keamanan lainnya dapat dikumpulkan secara konsisten. Perbedaan konfigurasi antarlingkungan dapat menyebabkan proses integrasi membutuhkan penyesuaian tambahan.

Oleh karena itu, kesiapan infrastruktur menjadi salah satu faktor yang memengaruhi kelancaran implementasi dan kualitas data yang dapat dianalisis oleh platform XDR.

Kendala lain berkaitan dengan proses menggabungkan berbagai sistem keamanan yang sebelumnya digunakan secara terpisah. Setiap sistem dapat menghasilkan format data, tingkat detail, dan karakteristik peringatan yang berbeda. Kondisi tersebut menuntut proses penyesuaian agar data dapat digunakan secara efektif dalam proses korelasi. Selain itu, tim keamanan perlu menyesuaikan alur kerja karena penggunaan XDR mengubah cara informasi keamanan dikumpulkan dan dianalisis. Oleh sebab itu, keberhasilan penerapan tidak hanya ditentukan oleh kemampuan teknologi, tetapi juga oleh kesiapan personel, kesesuaian infrastruktur, dan kemampuan organisasi dalam mengelola perubahan proses kerja.

Secara keseluruhan, hasil dan diskusi menunjukkan bahwa mengintegrasikan XDR dengan pendekatan Agile secara signifikan meningkatkan efektivitas dalam mendeteksi dan merespons serangan *defacement web*. Temuan ini mengatasi kekurangan dalam penelitian sebelumnya yang cenderung memisahkan mekanisme deteksi teknologi dari strategi implementasi. Oleh karena itu, studi ini memperkuat gagasan bahwa sistem keamanan siber yang sukses tidak hanya bergantung pada teknologi canggih tetapi juga pada pendekatan implementasi yang adaptif dan sadar konteks.



Gambar 3. Implementasi Agile dan XDR.

5. KESIMPULAN DAN SARAN

Studi ini menyimpulkan bahwa integrasi *Extended Detection and Response* (XDR) dengan pendekatan Agile secara signifikan meningkatkan efektivitas dalam mendeteksi dan merespons serangan *defacement web* dalam lingkungan organisasi. Temuan ini menunjukkan bahwa XDR memberikan visibilitas ancaman yang komprehensif melalui korelasi data lintas domain, memungkinkan deteksi anomali lebih awal dan respons insiden yang lebih cepat serta lebih terinformasi. Metodologi *Agile* mendukung implementasi yang adaptif dan iteratif serta

mendorong kolaborasi lintas fungsi, memungkinkan sistem keamanan berkembang sesuai dengan ancaman siber dinamis tanpa mengganggu stabilitas operasional. Secara teori, studi ini memperkuat perspektif keamanan siber holistik yang menekankan ketergantungan antara kemampuan teknologi dan proses organisasi. Secara praktis, ini menawarkan wawasan yang dapat ditindaklanjuti bagi organisasi yang ingin memperkuat keamanan berbasis web melalui strategi yang terintegrasi dan fleksibel. Dari sudut pandang kebijakan, hasilnya menyoroti pentingnya mengadopsi kerangka kerja keamanan siber yang menggabungkan teknologi deteksi canggih dengan model implementasi adaptif untuk meningkatkan ketahanan siber organisasi jangka panjang..

DAFTAR REFERENSI

Abd Rahman Wahid, D. A., Hayat, M. A. M., Abd Rahman, A., & Faisal, M. (2025). Stacking architecture-endpoint detection: a hybrid multi-layered architecture for endpoint threat detection. *Int J Adv Appl Sci*, *14*(4), 1263–1280.

Ahmed, S. K. (2024). The pillars of trustworthiness in qualitative research. *Journal of Medicine, Surgery, and Public Health*, *2*, 100051. https://doi.org/https://doi.org/10.1016/j.glmedi.2024.100051

Alam, R. G. G., Faruq, A., & Effendy, M. (2025). Cybersecurity Management Strategies for Smart Cities in Indonesia: Cultural Factors and Implementation Challenges. *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, *10*(3), 319–328. https://doi.org/https://doi.org/10.22219/kinetik.v10i3.2226

Albalawi, M., Aloufi, R., Alamrani, N., Albalawi, N., Aljaedi, A., & Alharbi, A. R. (2022). Website defacement detection and monitoring methods: A review. *Electronics*, *11*(21), 3573. https://doi.org/https://doi.org/10.3390/electronics11213573

Aminu, M., Akinsanya, A., Dako, D. A., & Oyedokun, O. (2024). Enhancing cyber threat detection through real-time threat intelligence and adaptive defense mechanisms. *International Journal of Computer Applications Technology and Research*, *13*(8), 11–27. https://doi.org/10.7753/IJCATR1308.1002

Arifiansyah, F. (2025). Analyzing Systemic Failures in IT Incident Management: Insights from Post-Mortem Analysis. *Eduvest-Journal of Universal Studies*, *5*(5), 5522–5535. https://doi.org/https://doi.org/10.59188/eduvest.v5i5.51192

Chung, M.-H., Yang, Y., Wang, L., Cento, G., Jerath, K., Raman, A., Lie, D., & Chignell, M. H. (2023). Implementing data exfiltration defense in situ: a survey of countermeasures and human involvement. *Acm Computing Surveys*, *55*(14s), 1–37. https://doi.org/https://doi.org/10.1145/3582077

Creswell, J. W., & Poth, C. N. (2017). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*. SAGE Publications.

Handri, E. Y., Sensuse, D. I., & Tarigan, A. (2024). Developing an agile cybersecurity framework with organizational culture approach using Q methodology. *IEEE Access*, *12*, 108835–108850.

Harahap, S. S., Halkis, M., & Sutanto, R. (2025). Advanced Persistent Threat (APT) sebagai Ancaman Perang Siber Asimetris Terhadap Pemerintah Indonesia. *Innovative: Journal Of Social Science Research*, *5*(3 SE-Articles), 4465–4485. https://doi.org/10.31004/innovative.v5i3.19091

Irawan, A., Fadholi, W. H. N., Erikamaretha, Z., & Sinlae, F. (2024). Tantangan dan Strategi Manajemen Keamanan Siber di Indonesia berbasis IoT. *Journal Zetroem*, *6*(1 SE-Article), 114–119. https://doi.org/10.36526/ztr.v6i1.3376

Islam, C., Babar, M. A., & Nepal, S. (2019). A multi-vocal review of security orchestration. *ACM Computing Surveys (CSUR)*, *52*(2), 1–45. https://doi.org/https://doi.org/10.1145/3305268

Jumaryadi, Y., Desmon, J., & Hidayatulloh, S. (2024). Systematic Literature Review: Serangan Deface Website sebagai Bentuk Kejahatan Siber. *Jurnal Sistem Informasi, Teknologi Informatika Dan Komputer*, *14*(2), 106–112. https://doi.org/10.24853/justit.14.2.106-112

Kumar, A., Chandran, S., & Somani, A. (2021). Conducting online web-based surveys at the time of COVID-19 pandemic: A short report. *Archives of Mental Health*, *22*(2), 158–161.

Kurniawan, C., & Triayudi, A. (2024). File integrity monitoring as a method for detecting and preventing web defacement attacks. *Jurnal Online Informatika*, *9*(2), 276–285. https://doi.org/https://doi.org/10.15575/join.v9i2.1326

Kurniawan, D. (2025). Kebijakan Dan Prosedur Keamanan Teknologi Informasi : Studi Literatur. *Jurnal Ilmu Komputer Dan Sistem Informasi |JIKSI|*, *2*(3 SE-Articles), 121–125. https://doi.org/10.61346/jiksi.v2i3.115

Maidin, S. S., Yahya, N., bin Fauri Fauzi, M. A., & Bakar, N. S. A. A. (2025). Current and future trends for sustainable software development: Software security in agile and hybrid agile through bibliometric analysis. *Journal of Applied Data Sciences*, *6*(1), 311–324. https://doi.org/https://doi.org/10.47738/jads.v6i1.473

Marçal, D., Metrôlho, J., & Ribeiro, F. (2025). Integrating Sentiment Analysis into Agile Feedback Loops for Continuous Improvement. In *Applied Sciences* (Vol. 15, Issue 22, p. 12329). https://doi.org/10.3390/app152212329

Miles, M. B., Huberman, A. M., & Saldana, J. (2013). *Qualitative Data Analysis: An Expanded Sourcebook*. SAGE Publications.

Paidy, P. (2025). Unified Threat Detection Platform With AI, SIEM, and XDR. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *6*(1), 95–104. https://doi.org/https://doi.org/10.63282/3050-9262.IJAIDSML-V6I1P111

Pissanidis, D. L., & Demertzis, K. (2024). Integrating AI/ML in cybersecurity: An analysis of open XDR technology and its application in intrusion detection and system log management. *Computer Science and Mathematics*. https://doi.org/https://doi.org/10.20944/preprints202312.0205.v2

Risyani, Y., Japit, S., Bombongan, C., Selamat, T., & Yuliana, Y. (2025). Sistem Keamanan Siber Adaptif Berbasis AI: Analisis Kinerja, Arsitektur, dan Penerapannya pada Organisasi Modern. *Jurnal Minfo Polgan*, *14*(2 SE-), 2999–3006. https://doi.org/10.33395/jmp.v14i2.15630

Slamet, S. (2025). Smishing Guard: Strategi Pengembangan Sistem Deteksi Dan Respons

Ancaman SMS Phising. *SPIRIT*, *17*(1). https://doi.org/10.53567/spirit.v17i1.380

Suharto, M. A., & Apriyani, M. N. (2021). Konsep Cyber Attack, Cyber Crime, Dan Cyber Warfare Dalam Aspek Hukum Internasional. *Risalah Hukum*, *17*(2 SE-Articles), 98–107. https://doi.org/10.30872/risalah.v17i2.705

Ukas, R. J., Sembiring, B. R., Wenas, N. C., & Alverdian, I. (2025). Data Breaches in Government Institutions and Society and Their Impacts on National Security in Indonesia. *AEGIS: Journal of International Relations*, *9*(1). https://doi.org/http://dx.doi.org/10.33021/aegis.v9i1.5735

Williams, L. D. (2021). Concepts of Digital Economy and Industry 4.0 in Intelligent and information systems. *International Journal of Intelligent Networks*, *2*, 122–129. https://doi.org/https://doi.org/10.1016/j.ijin.2021.09.002

Yin, R. K. (2017). *Case Study Research and Applications: Design and Methods*. SAGE Publications.

Yusof, Z. Bin. (2024). Effectiveness of endpoint detection and response solutions in combating modern cyber threats. *Journal of Advances in Cybersecurity Science, Threat Intelligence, and Countermeasures*, *8*(12), 1–9.