PERANCANGAN SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE UNTUK RESPONS INSIDEN SEMI-OTOMATIS (STUDI KASUS: UPA TIK UPN VETERAN JAKARTA)

BAYU ERIK WIBISONO
NIM.2010511056

PROGRAM STUDI S1 INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN"
JAKARTA
2026

PERANCANGAN SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE UNTUK RESPONS INSIDEN SEMI-OTOMATIS(STUDI KASUS: UPA TIK UPN VETERAN JAKARTA)

BAYU ERIK WIBISONO
NIM. 2010511056

SKRIPSI
Sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer

PROGRAM STUDI S1 INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN" JAKARTA
2026

LEMBAR PENGESAHAN

Judul	:	Perancangan Security Orchestration, Automation, and Response untuk Respons Insiden Semi-Otomatis (Studi Kasus: UPA TIK UPN Veteran Jakarta)
Nama	:	Bayu Erik Wibisono
NIM	:	2010511056
Program Studi	:	S1 Informatika

Disetujui oleh:

Penguji 1:
Dr. Ridwan Raafi'Udin, S.Kom., M.Kom.

Penguji 2:
Nurhuda Maulana, S.T., M.T.

Pembimbing 1:
Henki Bayu Seta, S.Kom, M.TI.

Pembimbing 2:
Hamonangan Kinantan Prabu, S.T, M.T.

Diketahui oleh:

Koordinator Program Studi:
Dr. Ridwan Raafi'udin, S.Kom., M.Kom.
NIP. 198805022021211001

Dekan Fakultas Ilmu Komputer:
Prof. Dr. Ir. Supriyanto, ST., M.Sc., IPM.
NIP. 197605082003121002

Tanggal Ujian Tugas Akhir:
12 Januari 2026

PERNYATAAN ORISINALITAS

Tugas akhir ini adalah hasil karya mandiri dan semua sumber yang dikutip maupun yang dirujuk telah saya nyatakan benar.

Nama	:	Bayu Erik Wibisono
NIM	:	2010511056
Tanggal	:	22 Januari 2026
Judul Skripsi	:	**PERANCANGAN SECURITY ORCHESTRATION, AUTOMATION, AND RESPONS UNTUK RESPONS INSIDEN SEMI-OTOMATIS (STUDI KASUS: UPA TIK UPN VETERAN JAKARTA)**

Bilamana pada kemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, maka saya besedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 22 Januari 2026

Yang menyatakan,

Bayu Erik Wibisono

PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR
UNTUK KEPENTINGAN AKADEMIS

Sebagai civitas akademika Universitas Pembangunan Nasional "Veteran" Jakarta, saya yang bertanda tangan di bawah ini:

Nama	: Bayu Erik Wibisono
NIM	: 2010511056
Fakultas	: Ilmu Komputer
Program Studi	: S-1 Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikakn kepada Universitas Pembangunan Nasional "Veteran" Jakarta Hak Bebas Royalti Non eksklusif (*Non – exclusive Royalty Free Right*) atas skripsi saya yang berjudul:

Perancangan Security Orchestration, Automation, and Response untuk Respons Insiden Semi-Otomatis (Studi Kasus: UPA TIK UPN Veteran Jakarta)

Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional "Veteran" Jakarta berhak menyimpan, mengalih media atau memformatkan, mengelola dalam bentuk pangkalan data (basis data), merawat, dan mempublikasikan skripsi saya selama tetap mencantumkan nama saya sebagai penulis dan sebagai pemilik Hak Cipta. Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di: Jakarta
Pada Tanggal: 30 Agustus 2025
Yang menyatakan,

Bayu Erik Wibisono

PERANCANGAN SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE UNTUK RESPONS INSIDEN SEMI-OTOMATIS (STUDI KASUS: UPA TIK UPN VETERAN JAKARTA)

Bayu Erik Wibisono

ABSTRAK

Kompleksitas serangan siber yang semakin meningkat menuntut sistem deteksi dan respons cepat yang terintegrasi. Penelitian ini merancang sistem Security Orchestration, Automation, and Response (SOAR) melalui pendekatan semi-otomatis dengan memanfaatkan Wazuh sebagai Security Information and Event Management (SIEM), MISP sebagai Threat Intelligence, IRIS untuk manajemen insiden, serta Shuffle sebagai SOAR. Sistem juga dilengkapi notifikasi Google Chat untuk peringatan dini serta kontrol atas sistem. Pengujian dilakukan terhadap serangan aplikasi web seperti SQL Injection, File Inclusion, serta deteksi *malware*. Hasilnya, Wazuh berhasil mendeteksi serangan yang diujikan. Nilai kinerja menunjukkan waktu Mean Time to Detect (MTTD) sebesar 6.66 detik, Mean Time to Acknowledge (MTTA) sebesar 18 detik, dan Mean Time to Respond (MTTR) sebesar 10 detik, serta setiap *workflow* dapat dijalankan dalam waktu kurang dari 35 detik menandakan proses deteksi dan respons berjalan cepat. Secara keseluruhan, sistem SOAR yang dibangun meningkatkan visibilitas keamanan, otomatisasi respons, serta efektivitas penanganan insiden.

Kata Kunci: SOAR, SIEM, CTI, Manajemen Kasus, Semi-Otomatisasi

DESIGN OF SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE FOR SEMI-AUTOMATED INCIDENT RESPONSE (CASE STUDY: UPA TIK UPN VETERAN JAKARTA)

Bayu Erik Wibisono

ABSTRACT

The increasing complexity of cyberattacks demands an integrated system capable of rapid detection and response. This study designs a semi-automated Security Orchestration, Automation, and Response (SOAR) system by utilizing Wazuh as Security Information and Event Management (SIEM), MISP as Threat Intelligence platform, IRIS for incident management, and Shuffle as SOAR. The system is also equipped with Google Chat notifications for early warnings and system control. Testing was conducted against web application attacks such as SQL Injection, File Inclusion, and malware detection. The results show that Wazuh successfully detected the tested attacks. The performance metrics show a Mean Time to Detect (MTTD) of 6.66 seconds, a Mean Time to Acknowledge (MTTA) of 18 seconds, and a Mean Time to Respond (MTTR) of 10 seconds, with each workflow executed in under 35 seconds, demonstrating a fast detection and response process. Overall, the implemented SOAR system enhances security visibility, response automation, and the effectiveness of incident handling.

Keywords: SOAR, SIEM, CTI, Case Management, Semi-Automation

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Allah SWT atas segala rahmat, hidayah, dan taufik-Nya sehingga penulis dapat menyelesaikan Tugas Akhir yang berjudul "Perancangan Security Orchestration, Automation, and Response untuk Respons Insiden Semi-Otomatis (Studi Kasus: UPA TIK UPN Veteran Jakarta)" dengan baik dan tepat waktu.

Tugas Akhir ini merupakan salah satu syarat untuk menyelesaikan studi pada Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta. Penulis menyadari sepenuhnya bahwa terselesaikannya Tugas Akhir ini tidak terlepas dari bantuan, bimbingan, dan dukungan dari berbagai pihak, baik secara langsung maupun tidak langsung.

Dengan rasa syukur dan hormat, penulis menyampaikan terima kasih yang tulus dan sebesar-besarnya kepada:

1. Allah SWT, Tuhan Yang Maha Esa, atas limpahan rahmat, karunia, dan kekuatan yang senantiasa menyertai selama proses penyusunan Tugas Akhir ini. Segala capaian hingga saat ini tidak akan pernah terwujud tanpa izin serta pertolongan-Nya.
2. Prof. Dr. Ir. Supriyanto, ST., M.Sc., IPM, selaku Dekan Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta, yang telah menghadirkan dukungan, fasilitas, dan lingkungan belajar yang produktif dan kondusif sehingga mendorong mahasiswa untuk terus berkembang dan berprestasi.
3. Ibu Dr. Widya Cholil, S.Kom., M.I.T., selaku Ketua Program Studi S1 Informatika, yang senantiasa memberikan arahan, perhatian, serta kebijakan yang memudahkan mahasiswa dalam menempuh dan menyelesaikan studinya dengan baik.
4. Bapak Henki Bayu Seta, S.Kom., M.TI., selaku Dosen Pembimbing I, yang dengan sabar telah memberikan arahan, masukan ilmiah, serta sudut pandang yang luas dalam menyempurnakan penelitian ini, sehingga karya ini dapat terselesaikan dengan lebih baik.

5. Bapak Hamonangan Kinantan Prabu, S.T., M.T., selaku Dosen Pembimbing II, yang senantiasa membantu, membimbing, serta memberikan arahan dengan penuh kesabaran. Dengan ketulusan, Bapak selalu memberikan waktu, kesempatan, dan dukungan yang berharga sehingga penulis dapat berkembang dan menyelesaikan penelitian ini dengan sebaik-baiknya.
6. Bapak Muhammad Adrezo, S.Kom., M.Sc., selaku Dosen Pembimbing Akademik. Bapak senantiasa memberikan semangat dan motivasi, khususnya di masa-masa sulit yang pernah peneliti hadapi selama menempuh pendidikan. Dukungan Bapak menjadi salah satu faktor penting yang membuat peneliti dapat bertahan dan menyelesaikan studi hingga tahap ini.
7. Seluruh dosen dan staf Fakultas Ilmu Komputer. Melalui ilmu bermanfaat yang diberikan serta bimbingan yang berharga, penulis memperoleh banyak pengetahuan dan pengalaman yang bermanfaat, serta bantuan dan dukungan yang diberikan dalam berbagai keperluan akademik sangat membantu kelancaran penyelesaian studi.
8. Keluarga tercinta yang selalu mendukung peneliti sepenuhnya, baik dalam doa, moral, maupun materi. Dengan penuh kasih sayang, keluarga senantiasa memberikan arahan, mengingatkan, dan membimbing. Dukungan yang tiada henti dari keluarga menjadi kekuatan terbesar peneliti dalam menyelesaikan studi ini.
9. Teman-teman seperjuangan di Program Studi Informatika angkatan 2022, yang telah menjadi bagian penting dalam perjalanan penulis selama menempuh perkuliahan. Kehadiran teman-teman yang selalu dapat diandalkan menjadi sumber semangat dan motivasi bagi peneliti.
10. Diri sendiri, yang telah berjuang dan berusaha sebaik mungkin meskipun sempat menghadapi masa-masa sulit di awal perkuliahan..

Penulis menyadari bahwa penulisan Tugas Akhir ini masih jauh dari kata sempurna, baik dari segi materi maupun penyajian, mengingat keterbatasan kemampuan dan pengetahuan yang dimiliki. Oleh karena itu, penulis dengan rendah hati mengharapkan kritik dan saran yang membangun demi penyempurnaan Tugas

Akhir ini di masa mendatang. Semoga karya ini dapat memberikan manfaat, baik bagi penulis sendiri maupun bagi pihak lain yang membutuhkan.

Akhir kata, penulis mengucapkan terima kasih yang sebesar-besarnya kepada semua pihak yang telah memberikan dukungan, serta berharap semoga segala bantuan dan kebaikan yang diberikan mendapatkan balasan yang setimpal dari Tuhan Yang Maha Esa.

Jakarta, 4 Agustus 2025

Penulis

DAFTAR ISI

DAFTAR GAMBAR

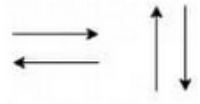
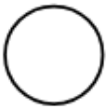
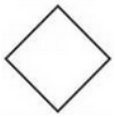
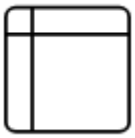
DAFTAR TABEL

DAFTAR PERSAMAAN

DAFTAR SKRIP

DAFTAR LAMPIRAN

DAFTAR SIMBOL

No.	Simbol	Nama Simbol	Fungsi
1.		Terminator	Simbol ini menandakan titik awal atau akhir dari sebuah program atau proses.
2.		Flow	Simbol ini menghubungkan antara satu simbol dengan simbol lainnya dalam alur.
3.		On-Page Reference	Simbol ini menunjukan keluar-masuknya aliran proses atau penyambungan langkah pada lembar kerja yang sama.
4.		Process	Simbol ini melambangkan suatu aktivitas atau tindakan yang dilaksanakan dalam sebuah alur proses.
5.		Decision	Simbol ini menggambarkan kondisi tertentu, menghasilkan dua kemungkinan keputusan, yaitu “Ya” atau “Tidak”.
6.		Input/Output	Simbol ini menunjukkan kegiatan menerima masukan (*input*) atau menghasilkan keluaran (*output*).
7.		Predefined Process	Simbol ini menggambarkan proses yang sudah ditentukan sebelumnya dan dapat dipanggil kembali (subproses).
8.		Internal Storage	Simbol ini menyatakan penyimpanan data internal atau sementara, misalnya memori komputer.

DAFTAR ISTILAH

No.	Istilah	Kepanjangan	Deskripsi
1.	API	Application Programming Interface	Mekanisme yang memungkinkan dua komponen perangkat lunak saling berkomunikasi dan bertukar informasi. API bertindak sebagai perantara, yang memungkinkan untuk integrasi berbagai platform atau layanan.
2.	APT	Advanced Persistent Threat	Serangan siber, di mana penyerang memperoleh akses tidak sah ke sistem atau jaringan dan mempertahankan akses tersebut dalam jangka waktu yang panjang untuk mengumpulkan informasi.
3.	Cache	-	Tempat penyimpanan sementara yang digunakan untuk menyimpan data atau informasi sehingga dapat digunakan kembali dengan cepat.
4.	CDB	Constant Database	Mekanisme Wazuh yang membandingkan data masuk dengan daftar yang telah ditetapkan.
5.	CIA Triad	Confidentiality, Integrity, Availability	CIA Triad adalah konsep dasar dalam keamanan informasi. Confidentiality menjamin bahwa informasi hanya dapat diakses oleh pihak yang berwenang. Integrity memastikan data tetap akurat, utuh, dan bebas dari perubahan yang tidak sah. Availability menjamin data dan sistem selalu dapat diakses oleh pihak yang berwenang.

6.	CLM	Centralized Log Management	Proses pengumpulan log dari berbagai sistem ke satu lokasi untuk disimpan dan dianalisis.
7.	Cloudflare	-	Layanan internet yang berfungsi sebagai pengaman web dan dapat bertindak sebagai VPN.
8.	Container	-	Paket dari perangkat lunak yang berisi seluruh komponen dan dependensi yang dibutuhkan agar dapat dijalankan di berbagai *environment*.
9.	CRI	Cyber Risk Index	Metrik penilaian dengan skala 0 - 100 yang menunjukkan tingkat risiko keamanan siber, semakin tinggi nilainya, semakin besar kemungkinan terjadinya serangan. Kategori *low risk* (0-30), *medium risk* (31-69), dan *high risk* (70-100).
10.	CREM	Cyber Risk Exposure Management	Metode untuk menghitung nilai CRI dengan mengidentifikasi semua aset, menilai risiko secara *real-time*, dan dapat memberikan rekomendasi mitigasi.
11.	CTI	Cyber Threat Intelligence	Proses pengumpulan dan analisis informasi tentang ancaman siber yang sedang terjadi, untuk membantu tim keamanan dalam memahami dan merespons serangan siber.
12.	CVE	Common Vulnerabilities and Exposures	Daftar standar yang berisi identitas unik setiap kerentanan atau celah keamanan

			yang diketahui dalam perangkat lunak atau sistem.
13.	CVSS	Common Vulnerability Scoring System	Standar kerangka kerja yang digunakan untuk menilai tingkat keparahan dalam suatu sistem.
14.	Daemon	-	Layanan yang aktif berjalan di *background*.
15.	DFIR-IRIS	Digital Forensic and Incident Response - Incident Response Information Sharing	Platform yang digunakan untuk berkolaborasi antar tim keamanan dalam mengidentifikasi dan investigasi insiden keamanan. Platform ini dapat menerima *alert*, eskalasi kasus, membuat catatan dan penugasan, serta mengumpulkan bukti.
16.	Docker	-	Platform yang menyediakan virtualisasi pada tingkat sistem operasi untuk menjalankan aplikasi di dalam paket yang disebut *container*.
17.	DVWA	Damn Vulnerable Web Application	Aplikasi web yang sengaja dibuat rentan terhadap berbagai jenis serangan keamanan web untuk tujuan pendidikan dan pengujian sistem.
18.	Endpoint	-	Perangkat keras yang terhubung ke dalam jaringan serta berfungsi untuk berkomunikasi dan bertukar informasi di dalam jaringan tersebut.
19.	Firewall	-	Sistem keamanan jaringan yang memantau dan menyaring trafik masuk maupun keluar berdasarkan aturan yang diterapkan. Fungsinya termasuk

			melakukan pemblokiran terhadap alamat IP yang berpotensi membahayakan sistem.
20.	EWS	Early Warning Systems	Sistem deteksi yang dirancang untuk memberikan peringatan dini (bisa dalam bentuk notifikasi) tentang potensi bahaya atau kejadian yang dapat membahayakan sistem.
21.	HIPAA	Health Insurance Portability and Accountability Act	Regulasi di Amerika Serikat yang mengatur perlindungan privasi dan keamanan data kesehatan pribadi.
22.	HTTP	Hypertext Transfer Protocol	Protokol komunikasi untuk transfer data antar klien (browser) dengan server.
23.	IDS	Intrusion Detection System	Sistem keamanan yang berfungsi untuk mendeteksi aktivitas mencurigakan atau serangan di dalam jaringan maupun *host* dengan cara memantau trafik dan log.
24.	IH&R	Incident Handling and Response	Proses mendeteksi, menangani, dan merespons dari ancaman yang mengganggu ketersediaan sistem atau kerahasisaan data.
25.	IoC	Indicator of Compromise	Sebuah informasi (Seperti IP, domain, hash, *file*) yang dapat menjadi petunjuk adanya serangan siber yang sedang atau telah terjadi.
26.	IP	Internet Protocol	Protokol yang digunakan untuk melakukan *routing* dan *addressing* paket data sehingga paket dapat dikirim

			dan diterima dengan sesuai di dalam jaringan.
27.	JSON	JavaScript Object Notation	Format standar untuk merepresentasikan data dalam bentuk *key-value.* JSON umumnya digunakan untuk menyimpan dan mentransmisikan data antar aplikasi web, terutama dalam komunikasi melalui API atau integrasi sistem.
28.	GDPR	General Data Protection Regulation	Regulasi privasi dan keamanan data di Uni Eropa yang mengatur perlindungan data pribadi individu dan cara organisasi mengumpulkan, menyimpan, serta memproses data tersebut.
29	Groq	-	Layanan kecerdasan buatan daring yang dapat digunakan untuk LLM.
30.	LLM	Large Language Model	Model pembelajaran mesin untuk memahami, memprediksi, dan menghasilkan teks dalam bahasa alami.
31.	MITRE ATT&CK	MITRE Adversarial Tactics, Techniques, and Common Knowledge	Kerangka yang digunakan untuk memetakan TTP pelaku ancaman dan dapat diakses secara global. Kerangka ini sebagai referensi dalam pemodelan dan kontrol ancaman.
32.	Malware	Malicious Software	Perangkat lunak berbahaya yang dibuat untuk merusak, mencuri informasi, atau mengambil kendali tanpa izin pengguna.

33.	MISP	Malware Information Sharing Platform	Platform *open-source* yang digunakan untuk menyimpan dan membagikan indikator serta ancaman keamanan siber guna mendukung analisis insiden keamanan siber dan *malware*.
34.	MTTA	Mean Time to Acknowledge	Waktu rata-rata yang dibutuhkan tim dalam mengakui dan mengonfirmasi keberadaan insiden yang terjadi.
35.	MTTD	Mean Time to Detect	Waktu rata-rata yang dibutuhkan sistem dalam mendeteksi insiden sejak pertama kali terjadi.
36.	MTTR	Mean Time to Respond	Waktu rata-rata yang dibutuhkan untuk mulai melakukan respons setelah insiden diakui.
37.	NIST	National Institute of Standards and Technology	Lembaga standar dan teknologi di Amerika Serikat yang mengeluarkan kerangka kerja, pedoman, serta standar keamanan informasi.
38.	Node	-	Komponen atau blok yang merepresentasikan fungsi tertentu dalam alur kerja.
39.	PCI DSS	Payment Card Industry Data Security Standard	Regulasi standar keamanan global yang ditetapkan untuk melindungi data pemegang kartu serta mengoptimakan transaksi kartu kredit dan debit.
40.	Phishing	-	Kejahatan siber dengan memancing korban untuk memberikan data atau informasi sensitif melalui pesan atau web.

41.	Playbook	-	Panduan terstruktur yang berisi langkah-langkah penanganan insiden dalam keamanan siber.
42.	Plugin	-	Komponen perangkat lunak tambahan yang dipasang pada aplikasi utama untuk menambah fungsionalitas tanpa memodifikasi kode inti.
43.	Port	-	Nomor yang digunakan oleh protokol jaringan untuk membedakan jenis layanan pada sebuah perangkat. *Port* sebagai gerbang komunikasi antar aplikasi.
44.	PVE	Proxmox Virtual Environment	Platform virtualisasi *open-source* berbasis Linux yang digunakan untuk mengelola *virtual machine* dan *container* dengan antarmuka web.
45.	Ransomware	-	Jenis *malware* yang dapat mengenkripsi *file* atau sistem, kemudian menuntut tebusan untuk memulihkanya kembali.
46.	RBAC	Role-Based Access Control	Model kontrol akses yang memberikan izin berdasarkan peran (*role*) yang dimiliki pengguna dalam suatu sistem.
47.	SIEM	System Information and Event Management	Solusi keamanan siber yang memungkinkan organisasi mendeteksi, menganalisis, dan merespons ancaman dengan mengumpulkan serta mengelola log dari berbagai sumber.
48.	SOAR	Security Orchestration,	Solusi keamanan siber yang dirancang untuk mengintegrasikan berbagai alat keamanan, mengotomatiskan tugas-

		Automation, and Response	tugas berulang, serta mengoordinasikan respons insiden keamanan.
49.	SSH	Secure Shell	Protokol jaringan yang digunakan untuk akses jarak jauh secara aman ke server atau perangkat melalui koneksi terenkripsi.
50.	SSO	Single Sign-On	Mekanisme autentikasi terpusat yang memungkinkan pengguna *login* sekali untuk mengakses banyak aplikasi terintegrasi.
51.	Syslog	System Log	Protokol standar untuk mencatat, menyimpan, dan mengirim log dari perangkat jaringan, sistem operasi, maupun aplikasi ke server log terpusat.
52.	TCP	Transmission Control Protocol	Protokol komunikasi standar yang digunakan untuk bertukar informasi secara andal, berurutan, serta memastikan data terkirim secara lengkap.
53.	TTP	Tactic, Technique, and Procedure	Metode yang digunakan pelaku ancaman dalam merencanakan serangan. Tactic, tujuan yang ingin dicapai pelaku. Technique, metode yang ingin digunakan. Procedure, langkah dan detail teknis dalam melakukan teknik tersebut.
54.	UDP	User Datagram Protocol	Protokol komunikasi ringan yang digunakan untuk mengirim pesan secara cepat, namun tanpa jaminan keandalan.

55.	URL	Uniform Resource Locator	Alamat unik yang digunakan untuk mengakses dan menemukan berbagai sumber daya, seperti halaman web, dokumen, atau gambar.
56.	VM	Virtual Machine	Virtualisasi dari komputer yang mampu menjalankan hampir semua fungsi komputer fisik, termasuk aplikasi dan sistem operasi.
57.	VPN	Virtual Private Network	Teknologi yang mengenkripsi koneksi internet, serta dapat digunakan untuk membuat koneksi secara *private*.
58.	Webhook	-	Metode otomatis yang memungkinkan aplikasi mengirim data ke aplikasi lain saat suatu peristiwa terjadi.
59.	Workflow	-	Langkah kerja yang tersusun secara sistematis untuk menyelesaikan suatu tugas atau mencapai tujuan tertentu.
60.	XDR	Extended Detection and Response	Solusi keamanan yang menggabungkan data dan sumber deteksi baik *endpoint* maupun jaringan untuk mendeteksi dan merespons ancaman.