DEFEND IT360

Inovasi Untuk Solusi

Defend IT360 SOC Report

Daily Report Hutama Karya
27 - 28 Oktober 2025

08:00 – 08:00 (GMT+7)
01:00 – 01:00 (UTC)

Document

Report ver1.0

Release Date
28/10/2025

DEFEND IT360 SECURITY OPERATION CENTER

Head Office
Sudirman 7.8
Tower 1, Lantai 27
Jakarta Pusat, DKI Jakarta - 10220

Executive Summary

Berdasarkan data yang diambil dalam periode 27 – 28 Oktober pukul 08.00 – 08.00, saat ini User yang terdaftar sebagai pengguna aktif adalah 2.824 dengan 3.304 pengguna tidak kadaluarsa, menunjukkan keberlanjutan akses yang stabil. Selain itu, terdapat 15 akun admin yang memiliki kontrol penuh atas sistem. Saat ini, tidak ada akun yang masuk dalam daftar pantauan dan 3 akun digunakan bersama, yang berisiko terhadap keamanan. 60 akun terhubung dengan akun lainnya, sementara 469 akun telah dinonaktifkan dan tidak dapat mengakses sistem.

Terdapat lima pengguna dengan angka Notable Behavior yang berbeda, Notable Behavior adalah perilaku mencurigakan atau tidak biasa yang terdeteksi dari aktivitas pengguna. Meskipun tidak selalu berarti berbahaya, perilaku ini cukup signifikan untuk dianalisis lebih lanjut karena bisa menjadi indikator awal dari aktivitas berbahaya. Pengguna Timbul Martua memiliki jumlah terbanyak yaitu 389, diikuti oleh pengguna Fasya Dibyana Prakasita HK SIS dengan 349 kemudian untuk Aprizal, Bambang Eko dan Bagian Manajemen Kontrak EPC memiliki angka yang lebih rendah, yakni 266, 241 dan 218.

Dalam hal pengumpulan data, terdapat 28 *event sources* yang semuanya berstatus "*running*", menunjukkan pengelolaan data yang berjalan lancar dan efektif. Namun, terdapat 4 *event source* dalam status "*Warning*", dengan tidak ada pembaruan dalam 120 menit terakhir, yang mengindikasikan potensi masalah pada *event sources* tersebut. Pengawasan lebih lanjut sangat dianjurkan untuk mencegah gangguan pada keseluruhan sistem.

Untuk memitigasi risiko ini, diperlukan langkah-langkah seperti verifikasi aktivitas login dan proses sistem, penerapan autentikasi multifaktor, penegakan kebijakan penggunaan aplikasi, peningkatan kesadaran keamanan bagi pengguna, serta penerapan kontrol teknis untuk membatasi instalasi dan eksekusi aplikasi yang tidak terotorisasi. Temuan ini menegaskan pentingnya monitoring berkelanjutan dan evaluasi terhadap pola autentikasi, perilaku pengguna, proses sistem, serta penggunaan aplikasi

di lingkungan organisasi guna mencegah potensi insiden yang dapat berdampak pada integritas dan kerahasiaan data.

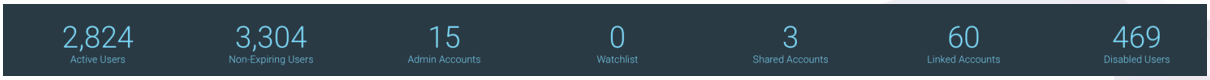
Berdasarkan hasil monitoring sistem keamanan oleh tim SOC, teridentifikasi empat alert yang memerlukan perhatian lebih lanjut, yaitu: *Suspicious Process – Malicious Hash On Asset, Suspicious Authentication – DataCamp Limited, User Behavior – Account Password Reset (Others), dan Non-Approved Application – File Transfer Tools*. Temuan ini menunjukkan adanya aktivitas proses mencurigakan yang terdeteksi melalui hash berbahaya pada aset, autentikasi mencurigakan terhadap layanan eksternal, perubahan kata sandi akun yang berpotensi mengindikasikan percobaan pengambilalihan akun, serta penggunaan aplikasi transfer file yang tidak terotorisasi oleh organisasi. Keempat aktivitas tersebut berpotensi menimbulkan risiko serius, termasuk eksekusi malware, kompromi kredensial, kebocoran data, komunikasi non-resmi, dan akses tidak sah di luar pengawasan sistem keamanan.

Untuk memitigasi risiko ini, diperlukan langkah-langkah seperti verifikasi aktivitas login dan proses sistem, penerapan autentikasi multifaktor, penegakan kebijakan penggunaan aplikasi, peningkatan kesadaran keamanan bagi pengguna, serta penerapan kontrol teknis untuk membatasi instalasi dan eksekusi aplikasi yang tidak terotorisasi. Temuan ini menegaskan pentingnya monitoring berkelanjutan dan evaluasi terhadap pola autentikasi, perilaku pengguna, proses sistem, serta penggunaan aplikasi di lingkungan organisasi guna mencegah potensi insiden yang dapat berdampak pada integritas dan kerahasiaan data.

Untuk memitigasi risiko ini, diperlukan langkah-langkah seperti verifikasi aktivitas login dan proses sistem, penerapan autentikasi multifaktor, penegakan kebijakan penggunaan aplikasi, peningkatan kesadaran keamanan bagi pengguna, serta penerapan kontrol teknis untuk membatasi instalasi dan eksekusi aplikasi yang tidak terotorisasi. Temuan ini menegaskan pentingnya monitoring berkelanjutan dan evaluasi terhadap pola autentikasi, perilaku pengguna, proses sistem, serta penggunaan aplikasi di lingkungan organisasi guna mencegah potensi insiden yang dapat berdampak pada integritas dan kerahasiaan data.

User and Account Information

User and Account



Saat ini *User* yang terdaftar sebagai pengguna aktif terdapat 2.824 yang terus menggunakan layanan dan menunjukkan bahwa sebagian besar pengguna masih berinteraksi dengan sistem. Di sisi lain, terdapat 3.304 akun pengguna yang tidak memiliki tanggal kadaluarsa, artinya akun-akun ini tetap aktif tanpa batas waktu yang jelas.

Hal ini dapat dilihat sebagai indikasi bahwa pengguna tersebut berkomitmen untuk terus menggunakan sistem dalam jangka panjang. Terkait dengan manajemen akun, ada 15 akun admin yang memiliki hak administratif penuh untuk mengakses, mengelola, dan memantau sistem, memberikan mereka kontrol total atas operasional dan 59 akun terhubung dengan akun lainnya.

Namun, terdapat 469 akun pengguna yang dinonaktifkan. Akun-akun yang dinonaktifkan ini tidak dapat lagi mengakses sistem, menunjukkan adanya pemeliharaan dan pembersihan akun yang tidak aktif atau bermasalah. Selain itu, ada 3 akun yang digunakan bersama oleh lebih dari satu orang, yang dapat berisiko terhadap potensi masalah keamanan, mengingat adanya kemungkinan penggunaan yang tidak sah atau berbagi akses yang tidak terkontrol.

Saat ini, tidak ada akun yang masuk dalam daftar pantauan, yang menunjukkan bahwa tidak ada akun yang dianggap mencurigakan atau berisiko tinggi untuk keamanan. Meski demikian, pemantauan berkelanjutan terhadap akun-akun ini tetap diperlukan untuk memastikan sistem tetap aman.

Top 5 Risky Users

User	Notable Behavior	Open Incident
Timbul Martua	389	2360
Fasya Dibyana Prakasita HK SIS	349	2452
Bambang Eko	266	1299
Aprizal.	241	1495
Bagian Manajemen Kontrak EPC	218	1383

Berdasarkan data diatas, terdapat lima pengguna dengan angka Notable Behavior yang berbeda, Notable Behavior adalah perilaku mencurigakan atau tidak biasa yang terdeteksi dari aktivitas pengguna. Meskipun tidak selalu berarti berbahaya, perilaku ini cukup signifikan untuk dianalisis lebih lanjut karena bisa menjadi indikator awal dari aktivitas berbahaya. Pengguna Timbul Martua memiliki jumlah terbanyak yaitu 389, diikuti oleh pengguna Fasya Dibyana Prakasita dengan 349 kemudian untuk Aprizal, Bambang Eko dan Bagian Manajemen Kontrak EPC. memiliki angka yang lebih rendah, yakni 266, 241 dan 218. Hal ini menunjukkan bahwa meskipun pengguna Timbul Martua dan Fasya Dibyana Prakasita lebih sering terdeteksi, frekuensi pada pengguna lainnya cukup seragam, dengan sedikit perbedaan antara Aprizal, Bambang Eko dan Bagian Manajemen Kontrak EPC.

DEFEND IT360

Data Collection Health

1. Healthy Condition

Data Collection	Address/Port	Status
AD-LDAP-DC INDONET	192.168.15.13	Running
AD-LDAP-HO PRIMARY	10.10.40.11	Running
AD-LDAP-HO SECONDARY	10.10.40.12	Running
AD - SEC LOGS - DC INDONET	192.168.15.13	Running
AD - SEC LOGS - HO PRIMARY	10.10.40.11	Running
AD - SEC LOGS - HO SECONDARY	10.10.40.12	Running
ARUBA - NAC – HO	Port: 1037	Running
ARUBA - NAC – HO 02	Port: 1037	Running
ARUBA – WLC – HO	Port: 1038	Running
BIND - DNS01 - DRC	Port: 1048	Running
BIND - DNS01 - DC INDONET	Port:1046	Running
BIND - DNS01 – HO	Port: 1032	Running
BIND - DNS02 - DC INDONET	Port: 1047	Running
BIND - DNS02 - HO	Port:1052	Running
BIND - DNS03 - HO	Port:1032	Running
DHCPD - DHCP01 - HO	Port:1053	Running

DHCPD - DHCP02 - HO	Port: 1054	Running
FORTIGATE - FIREWALL - DC INDONET	Port: 1039	Running
FORTIGATE - FIREWALL - DRC	Port:1027	Running
FORTIGATE - FIREWALL - HO	Port:1025	Running
FORTIGATE - FIREWALL VM - DC INDONET	Port: 1049	Running
GCP - DEV - DC INDONET	-	Running
GCP - PROD - DC INDONET	-	Running
OFFICE 365 - WORKSPACE - SAAS	-	Running
RAPID7 - INSIGHTVM - DC INDONET	Nexpose Host: 46.51.266.179:443	Running
SOPHOS - AV - DC INDONET	Port: 1028	Running
vCenter - VMWARE - DC INDONET	Port: 1514	Running
vCenter - VMWARE - DRC	Port: 1514	Running

Berdasarkan informasi yang ditunjukkan, data collection terdapat total 28 sources yang semuanya berstatus running. Hal ini menunjukkan bahwa sistem atau proses yang mengelola data tersebut berjalan dengan lancar dan tidak mengalami gangguan. Semua sumber yang terlibat aktif dalam mengumpulkan data, yang dapat mengindikasikan bahwa pengumpulan informasi terkait kondisi kesehatan berlangsung secara efektif dan tanpa hambatan. Keberhasilan status "*running*" pada seluruh sumber ini dapat dianggap sebagai tanda bahwa proses pengolahan dan pengumpulan data berjalan dengan stabil dan dapat diandalkan.

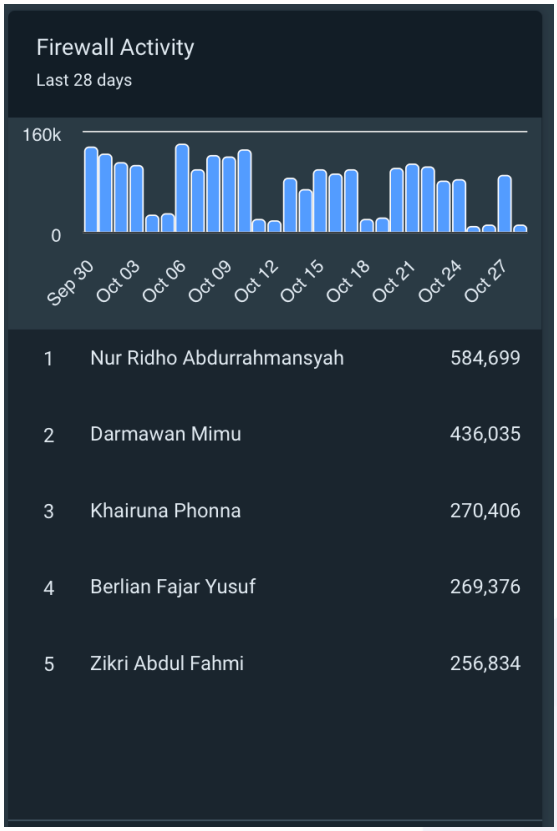
2. Warning Condition

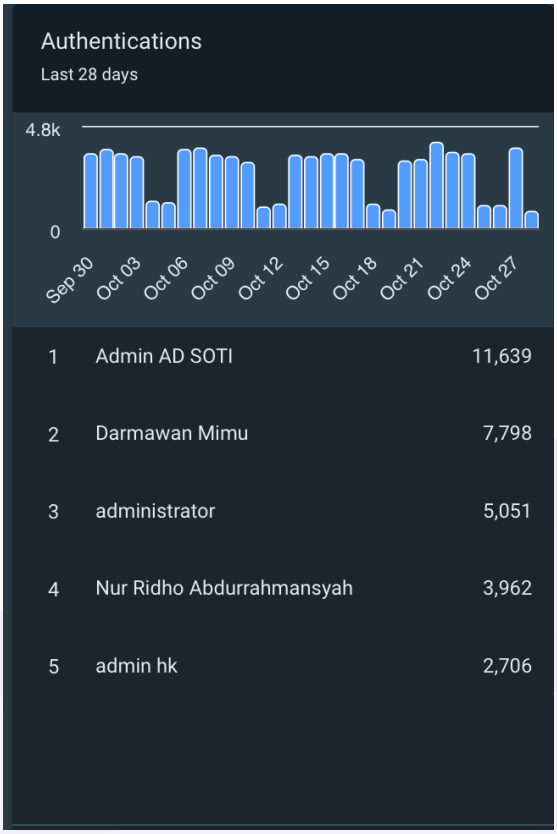
Data Collection	Address/Port	Status
AKAMAI - WAF - DC INDONET	Port: 1029	Last Detected 120 Minutes Since the Last Event
AKAMAI - ZTNA - DC INDONET	Port: 1030	Last Detected 120 Minutes Since the Last Event
GCP - NETWORK - DC INDONET	-	Last Detected 120 Minutes Since the Last Event

Berdasarkan data diatas, terdapat 3 sumber (event source) yang statusnya berada dalam kondisi peringatan "*Warning*", dengan catatan bahwa "*Last Detected 120 Minutes Since the Last Event*". Hal ini menunjukkan bahwa tidak ada peristiwa atau pembaruan yang terdeteksi dalam 120 menit terakhir untuk setiap *event source* tersebut. Meskipun statusnya "W*arning*" ketidakaktifan ini mungkin menunjukkan adanya potensi masalah atau penurunan kinerja pada *event sources* tersebut yang perlu segera ditangani agar tidak memengaruhi kelancaran sistem secara keseluruhan. Adanya peringatan ini dapat menjadi indikasi bahwa pengawasan lebih lanjut diperlukan untuk memastikan sistem tetap berjalan dengan baik.

Activity Record

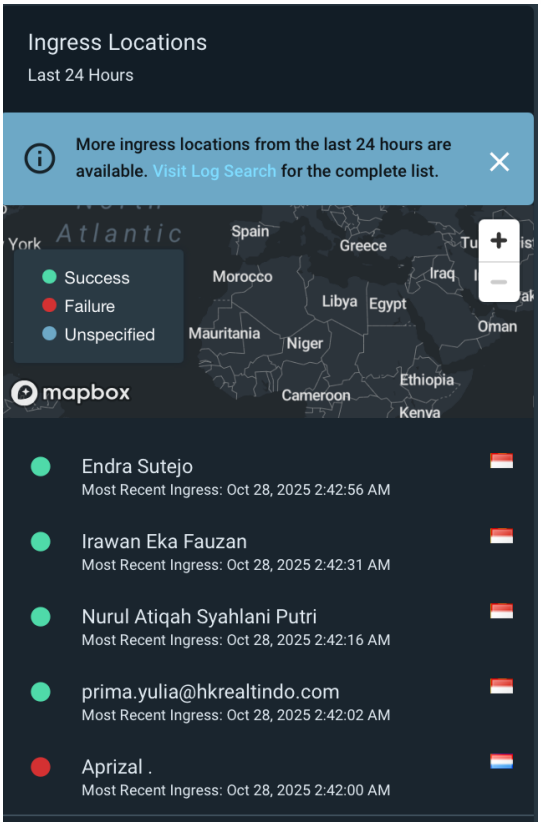
Top 5 Firewall Activity and Top 5 Authentications





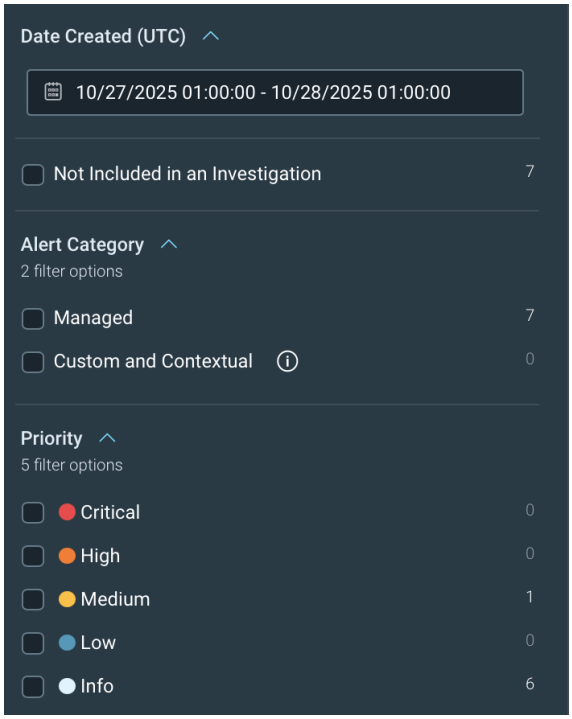
Kedua grafik ini memberikan gambaran tentang keamanan jaringan selama 28 hari terakhir. Aktivitas firewall menunjukkan fluktuasi yang signifikan terutama di sekitar tanggal 06 Oktober yang memerlukan pemantauan dan analisis lebih lanjut. Sementara itu, autentikasi grafik menunjukkan tren jumlah otentikasi selama 28 hari terakhir. Terdapat lonjakan Autentikasi yang signifikan pada 07 Oktober.

1. Ingress Locations



Ingress Location tersebut memberitahukan aktivitas login ke dalam sistem dalam 24 jam terakhir, berasal dari negara apa dan status login tersebut apakah berhasil (ditandai dengan warna hijau), gagal (ditandai dengan warna merah), dan belum ditentukan (ditandai dengan warna biru).

2. Total Alert



Severity	Count
Critical	0
High	0
Medium	1
Low	0
Info	6

Notes: Penarikan data Alerts Rapid7 diambil pada pukul 01.00 – 01.00 dengan alasan perbedaan konfigurasi waktu yang diterapkan pada tools Rapid7 (UTC) dan Indonesia(GMT+7).

Alert Analytic

1. Suspicious Process - Malicious Hash On Asset

Alert Name	Suspicious Process - Malicious Hash On Asset
Severity	**Medium**
Time Detection	27 Oktober 2025, 07:37:09 (UTC) 27 Oktober 2025, 14:37:09 (GMT+7)
Description	Process Behavior – Suspicious Process - Malicious Hash On Asset mengacu pada deteksi aktivitas proses mencurigakan di mana sebuah file yang dijalankan pada aset memiliki hash yang cocok dengan indikator malware yang telah diketahui. Hal ini dapat menunjukkan adanya upaya eksekusi kode berbahaya di sistem, yang berpotensi menjadi bagian dari serangan siber atau infeksi malware yang lebih luas
Hostname	DESKTOP-9J0BPJ8
Username	ENG_DIV
Process Name	gSteelCal.exe
Exe path	***D:\\F_My Self\\Software\\gSteelCal\\gSteelCal.exe***
Command Line	\"D:\\F_My Self\\Software\\gSteelCal\\gSteelCal.exe\"
Exe File Owner	DESKTOP-9J0BPJ8\\ENG_DIV
Hashes	**MD5:** ee30f649186ae76fdef3c0ad1a0220a2 **SHA256:** f4ac0dc215a31ee48c561b9341b50ea0e635c48b0dc383016cab010777e3dd7b

	SHA1: 79850b4519060db407bcea458b09f2d2624adf43
Source Reputation	***Malware*** VirusTotal - File - f4ac0dc215a31ee48c561b9341b50ea0e635c48b0dc383016cab010777e3dd7b
Recommendations	1. Gunakan autentikasi 2FA untuk menambah lapisan keamanan 2. Memastikan perangkat lunak dan system selalu diperbarui untuk mengurangi kerentanannya 3. Menerapkan kebijakan kuat untuk kata sandi dan Batasan percobaan login 4. Melakukan audit dan Penetration Testing secara berkala untuk mengevaluasi celah keamanan

2. Suspicious Authentication - DataCamp Limited

Alert Name	Suspicious Authentication - DataCamp Limited
Severity	**INFO**
Time Detection	27 Oktober 2025, 02:14:11 (UTC) 27 Oktober 2025, 09:14:11 (GMT+7)
Description	Alert ini mendeteksi adanya autentikasi yang berhasil dengan menggunakan VPN. Deteksi ini digunakan untuk mengawasi aktivitas yang tidak biasa yang mungkin menunjukkan penyalahgunaan kredensial atau akses yang tidak sah.
User	Muhammad Imi
Email	muhammad.imi@hutamakarya.com
Resul	***Success***
Source IP	212.97.69.35 (Kazakhstan)
Source Reputation	***0/95 security vendor flagged this IP address as malicious*** *Source:* VirusTotal - IP address - 212.97.69.35
Recommendations	1. Validasi aktivitas dari user tersebut, apakah legitimate atau tidak. 2. Kunci akun yang terdampak Security Operation Center Defend IT360 3. Reset Password 4. Blokir akses VPN yang tidak digunakan 5. Pastikan MFA diaktifkan dan diterapkan untuk semua pengguna

	6. Berikan edukasi pengguna

3. User Behavior - Account Password Reset - (Others)

Alert Name	User Behavior - Account Password Reset - (Others)
Severity	INFO
Time Detection	27 Oktober 2025, 03:29:44 (UTC) 27 Oktober 2025, 10:29:44 (GMT+7)
Description	User Behavior – Account Passwor Reset – (Others) mengacu pada deteksi aktivitas mencurigakan di mana seseorang mencoba mereset kata sandi akun, yang bisa menunjukkan upaya penyusupan atau percakapan ilegal untuk mengakses akun pengguna.
Source User	Zikri Abdul Fahmi
Target User	Ivan Hermawan
Action	PASSWORD_RESET
Computer Name	SERVHK-AD2.hutamakarya.co
OS Version	Microsoft Windows Server 2019 Standard
Recommendations	1. Verifikasi Identitas 2. Pemberitahuan Pengguna jika reset passwor terjadi 3. Penggunaan Otentikasi Dua Faktor (2FA) 4. Membatasi Akses Reset Kata Sandi 5. Audit dan Tinjau Aktivitas Pengguna

4. User Behavior - Account Password Reset - (Others)

Alert Name	User Behavior - Account Password Reset - (Others)
Severity	INFO
Time Detection	27 Oktober 2025, 03:29:44 (UTC) 27 Oktober 2025, 10:29:44 (GMT+7)
Description	User Behavior – Account Passwor Reset – (Others) mengacu pada deteksi aktivitas mencurigakan di mana seseorang mencoba mereset kata sandi akun, yang bisa menunjukkan upaya penyusupan atau percakapan ilegal untuk mengakses akun pengguna.
Source User	Khairuna.ponna
Target User	Alra.fakhira
Action	PASSWORD_RESET
Computer Name	SERVHK-AD2.hutamakarya.co
OS Version	Microsoft Windows Server 2019 Standard
Recommendations	1. Verifikasi Identitas 2. Pemberitahuan Pengguna jika reset passwor terjadi 3. Penggunaan Otentikasi Dua Faktor (2FA) 4. Membatasi Akses Reset Kata Sandi 5. Audit dan Tinjau Aktivitas Pengguna

5. Non-Approved Application - File Transfer Tools

Alert Name	Non-Approved Application - File Transfer Tools
Severity	**INFO**
Time Detection	27 Oktober 2025, 08:33:13 (UTC) 27 Oktober 2025, 15:33:13 (GMT+7)
Description	ini merujuk pada penggunaan perangkat lunak atau alat transfer file yang tidak sah atau tidak disetujui untuk mentransfer file dalam jaringan atau sistem. Alat ini mungkin tidak memenuhi standar keamanan atau kepatuhan yang ditetapkan oleh organisasi, yang dapat menimbulkan risiko terhadap data dan sistem yang ada
Hostname	KS190078-Hendra
Username	KS190078-HENDRA
File Owner	KS190078-HENDRA\\Hendra Satrya
File Name	Filezilla.exe
Command Line	\"C:\\Program Files\\FileZilla FTP Client\\filezilla.exe\"
More Information	
Recommendations	1. Membuat kebijakan yang jelas mengenai alat transfer file 2. Menyediakan alternatif yang aman seperti SFTP, FTPS

	3. Menerapkan kontrol akses

6. Non-Approved Application - File Transfer Tools

Alert Name	Non-Approved Application - File Transfer Tools
Severity	**INFO**
Time Detection	27 Oktober 2025, 08:26:13 (UTC) 27 Oktober 2025, 15:26:13 (GMT+7)
Description	ini merujuk pada penggunaan perangkat lunak atau alat transfer file yang tidak sah atau tidak disetujui untuk mentransfer file dalam jaringan atau sistem. Alat ini mungkin tidak memenuhi standar keamanan atau kepatuhan yang ditetapkan oleh organisasi, yang dapat menimbulkan risiko terhadap data dan sistem yang ada
Hostname	25914339-Nurindra
Username	25914339-NURIND
File Owner	25914339-NURIND\\Nurindra Notarianto
File Name	Filezilla.exe
Command Line	\"C:\\Program Files\\FileZilla FTP Client\\filezilla.exe\"

More Information	"exe_file": {
	"owner": "BUILTIN\\Administrators",
	"orig_filename": "filezilla.exe",
	"description": "FileZilla FTP Client",
	"product_name": "FileZilla",
	"version": "3, 67, 1, 0",
	"created": "2024-07-15T08:02:54.000Z",
	"last_modified": "2024-07-15T08:02:54.000Z",
	"size": 4237896,
	"internal_name": "FileZilla 3",
	"hashes": {
	"md5": "71e87d8f4ab33dd57bff41f76c339e64",
	"sha256": "96816c715a54e596a9d12527d9bb0d2dbcbc02d2a73ce72a1fd36d634d3587cd",
	"sha1": "d202fea4df82d26fabbfe3bdb9515a08d021cd09",
	"imphash": "3ff9474b5c787c02fd263fe738f178eb"
	},
	"signing_status": "SIGNED_VALID",

Recommendations	1. Membuat kebijakan yang jelas mengenai alat transfer file 2. Menyediakan alternatif yang aman seperti SFTP, FTPS 3. Menerapkan kontrol akses

7. Non-Approved Application - File Transfer Tools

Alert Name	Non-Approved Application - File Transfer Tools
Severity	**INFO**
Time Detection	27 Oktober 2025, 08:26:13 (UTC) 27 Oktober 2025, 15:26:13 (GMT+7)
Description	User Behavior – Account Passwor Reset – (Others) mengacu pada deteksi aktivitas mencurigakan di mana seseorang mencoba mereset kata sandi akun, yang bisa menunjukkan upaya penyusupan atau percakapan ilegal untuk mengakses akun pengguna.
Hostname	21964137-ZainM
Username	21964137-ZAINM
File Owner	21964137-ZAINM\\Zain Maulana Azmi
File Name	Putty.exe
Command Line	\"C:\\Users\\SIT\\AppData\\Local\\Google\\Cloud SDK\\google-cloud-sdk\\bin\\sdk\\putty.exe\" -t -i

More Information	
Recommendations	1. Membuat kebijakan yang jelas mengenai alat transfer file 2. Menyediakan alternatif yang aman seperti SFTP, FTPS 3. Menerapkan kontrol akses