DEFEND IT360

Inovasi Untuk Solusi

Defend IT360 SOC Report

Daily Report Hutama Karya
24 - 25 Oktober 2025

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

Document

Report ver1.0

Release Date
25/10/2025

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 24 – 25 Oktober pukul 08.00 – 08.00, saat ini User yang terdaftar sebagai pengguna aktif adalah 2.823 dengan 3.303 pengguna tidak kadaluarsa, menunjukkan keberlanjutan akses yang stabil. Selain itu, terdapat 14 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. 59 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 380, diikuti oleh pengguna Fasya Dibyana Prakasita HK SIS dengan 354 kemudian untuk Bambang Eko, Aprizal dan Daniel Erlanda memiliki angka yang lebih rendah, yakni 250, 242 dan 215.

Dalam hal pengumpulan data, terdapat 28 *event sources* yang semuanya berstatus "*running*", menunjukkan pengelolaan data yang berjalan lancar dan efektif. Namun, terdapat 3 *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.

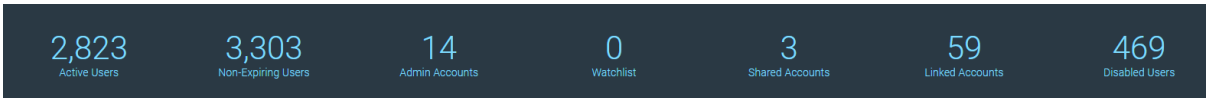
Berdasarkan hasil analisis, teridentifikasi tiga temuan yang perlu mendapat perhatian lebih lanjut. Temuan pertama adalah *User Behavior – Account Password Reset (Others)*, yang menunjukkan adanya pola aktivitas reset akun dengan karakteristik tidak lazim. Meskipun aktivitas ini berpotensi merupakan tindakan sah, pola yang teridentifikasi dapat mengindikasikan kemungkinan penyalahgunaan kredensial atau upaya eskalasi akses oleh pihak yang tidak berwenang. Kondisi ini menegaskan perlunya analisis konteks lebih lanjut untuk memastikan legitimasi aktivitas serta penerapan langkah mitigasi yang tepat guna mencegah potensi kompromi akun.

Temuan kedua adalah *Non-Approved Application – File Transfer Tools*, di mana terdeteksi penggunaan aplikasi transfer file yang tidak termasuk dalam daftar resmi organisasi. Aktivitas ini berpotensi meningkatkan risiko kebocoran data serta membuka jalur komunikasi non-resmi yang dapat dimanfaatkan untuk aktivitas tidak sah. Untuk meminimalisir risiko tersebut, diperlukan penegakan kebijakan penggunaan aplikasi, peningkatan kesadaran keamanan bagi pengguna, serta penerapan kontrol teknis untuk membatasi instalasi atau eksekusi aplikasi tidak terotorisasi.

Secara keseluruhan, kedua temuan ini menyoroti adanya risiko signifikan yang berkaitan dengan potensi penyalahgunaan kredensial dan kebocoran data akibat penggunaan aplikasi tidak terotorisasi. Organisasi perlu melakukan monitoring berkelanjutan, investigasi mendalam terhadap pola aktivitas pengguna, serta penegakan kebijakan keamanan yang lebih ketat untuk memastikan setiap aktivitas abnormal dapat terdeteksi dan ditindaklanjuti sebelum menimbulkan dampak yang lebih besar terhadap sistem maupun data organisasi.

User and Account Information

User and Account



Saat ini *User* yang terdaftar sebagai pengguna aktif terdapat 2.823 yang terus menggunakan layanan dan menunjukkan bahwa sebagian besar pengguna masih berinteraksi dengan sistem. Di sisi lain, terdapat 3.303 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 14 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	380	2347
Fasya Dibyana Prakasita HK SIS	354	2449
Bambang Eko	250	1489
Aprizal.	242	1292
Daniel Erlanda	215	1376

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 380, diikuti oleh pengguna Fasya Dibyana Prakasita dengan 354 kemudian untuk Bambang Eko, Aprizal dan Daniel Erlanda. memiliki angka yang lebih rendah, yakni 250, 242 dan 215. 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 Bambang Eko, Aprizal dan Daniel Erlanda.

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: 46.51.248.179:443	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.

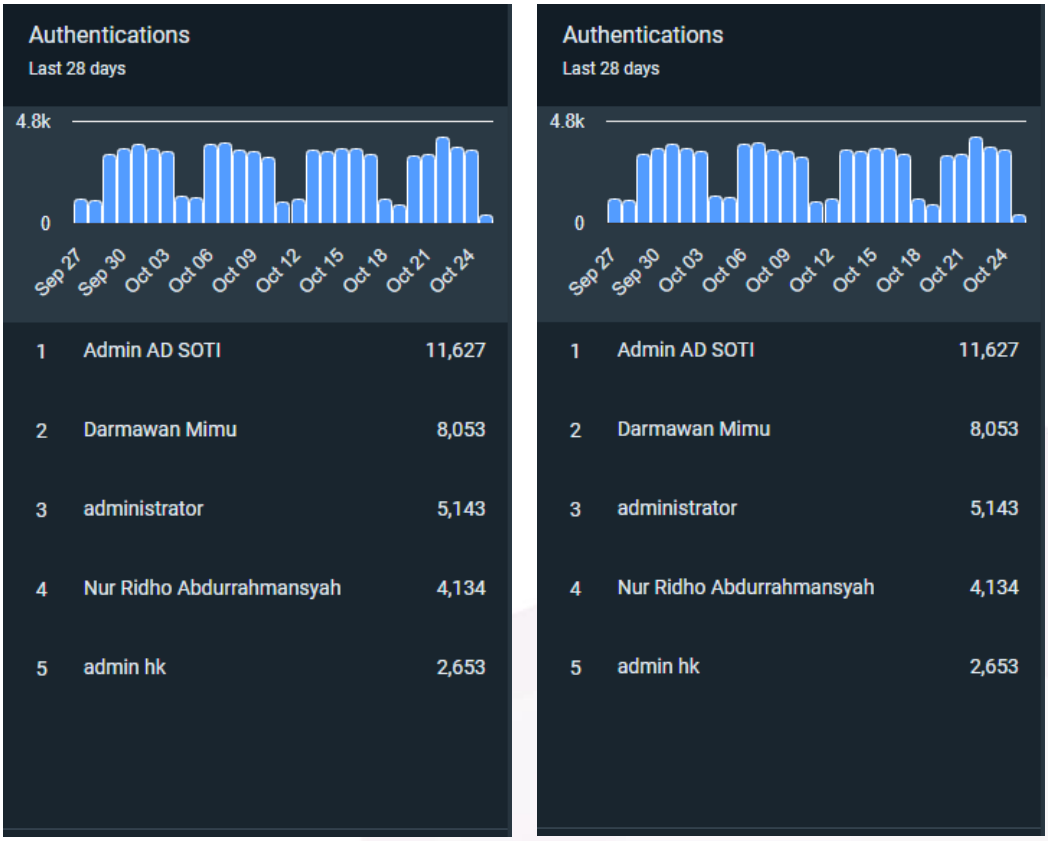
2. Warning Condition

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.

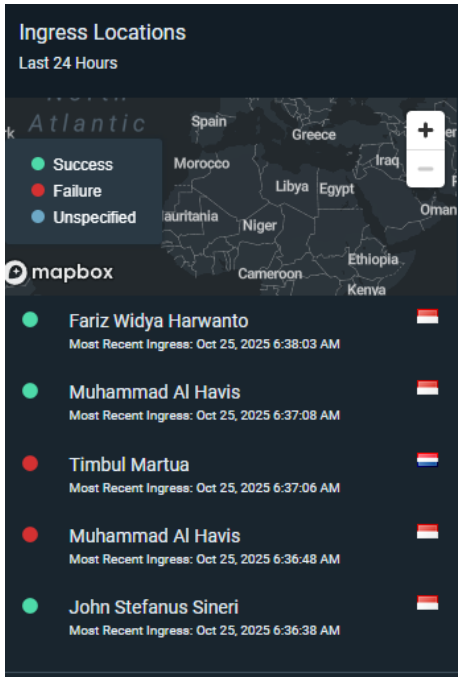
Activity Record

Top 5 Firewall Activity and Top 5 Authentications



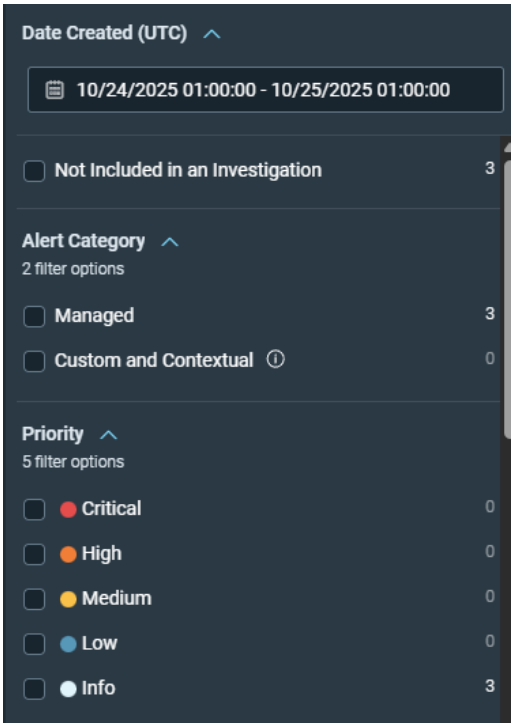
Kedua grafik ini memberikan gambaran tentang keamanan jaringan selama 28 hari terakhir. Aktivitas firewall menunjukkan fluktuasi yang signifikan terutama di sekitar tanggal 06 Oktober yang memerlukan pemantauan dan analisis lebih lanjut. Sementara itu, autentikasi grafik menunjukkan tren jumlah otentikasi 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	0
Low	0
Info	3

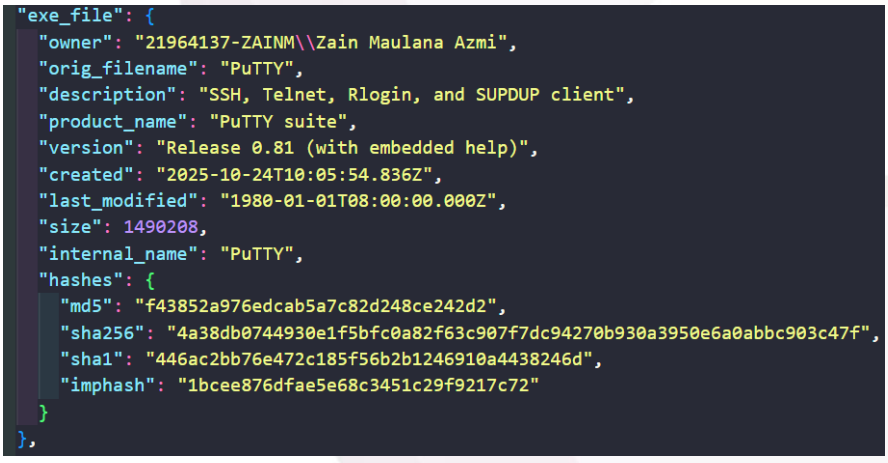
Notes: Penarikan data Alerts Rapid7 diambil pada pukul 01.00 – 01.00 dengan alasan perbedaan konfigurasi waktu yang diterapkan pada tools Rapid7 (UTC) dan Indonesia(GMT+7).

Alert Analytic

1. User Behavior – Account Password Reset – (Others)

Alert Name	User Behavior - Account Password Reset - (Others)
Severity	**INFO**
Time Detection	24 Oktober 2025, 10:32:22 (UTC) 24 Oktober 2025, 17:32:22 (GMT+7)
Description	User Behavior – Account Password Reset – (Others) mengacu pada deteksi aktivitas mencurigakan dimana seseorang mencoba reset kata sandi akun, yang bisa menunjukan Upaya penyusupan atau percakapan ilegal untuk mengakses akun pengguna.
Source User	Khairuna Phonna
Target User	edy.kusnendar gantri.radimas
Action	***PASSWORD_RESET***
Computer Name	SERVHK-AD2.hutamakarya.com
OS Version	Microsoft Windows Server 2019 Standard
Recommendations	1. Verifikasi Identitas 2. Pemberitahuan Pengguna jika reset password terjadi 3. Penggunaan Otentikasi Dua Faktor 4. Membatasi Akses Reset Kata Sandi 5. Audit dan Tinjau Aktivitas Pengguna

2. Non-Approved Application – File Transfer Tools

Alert Name	Non-Approved Application - File Transfer Tools
Severity	**INFO**
Time Detection	24 Oktober 2025, 10:10:39 (UTC) 24 Oktober 2025, 17:10:39 (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, yang dapat menimbulkan risiko terhadap data dan system.
Hostname	21964137-ZainM
Username	21964137-ZAINM\\Zain Maulana Azmi
File Owner	BUILTIN\\Administrators
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