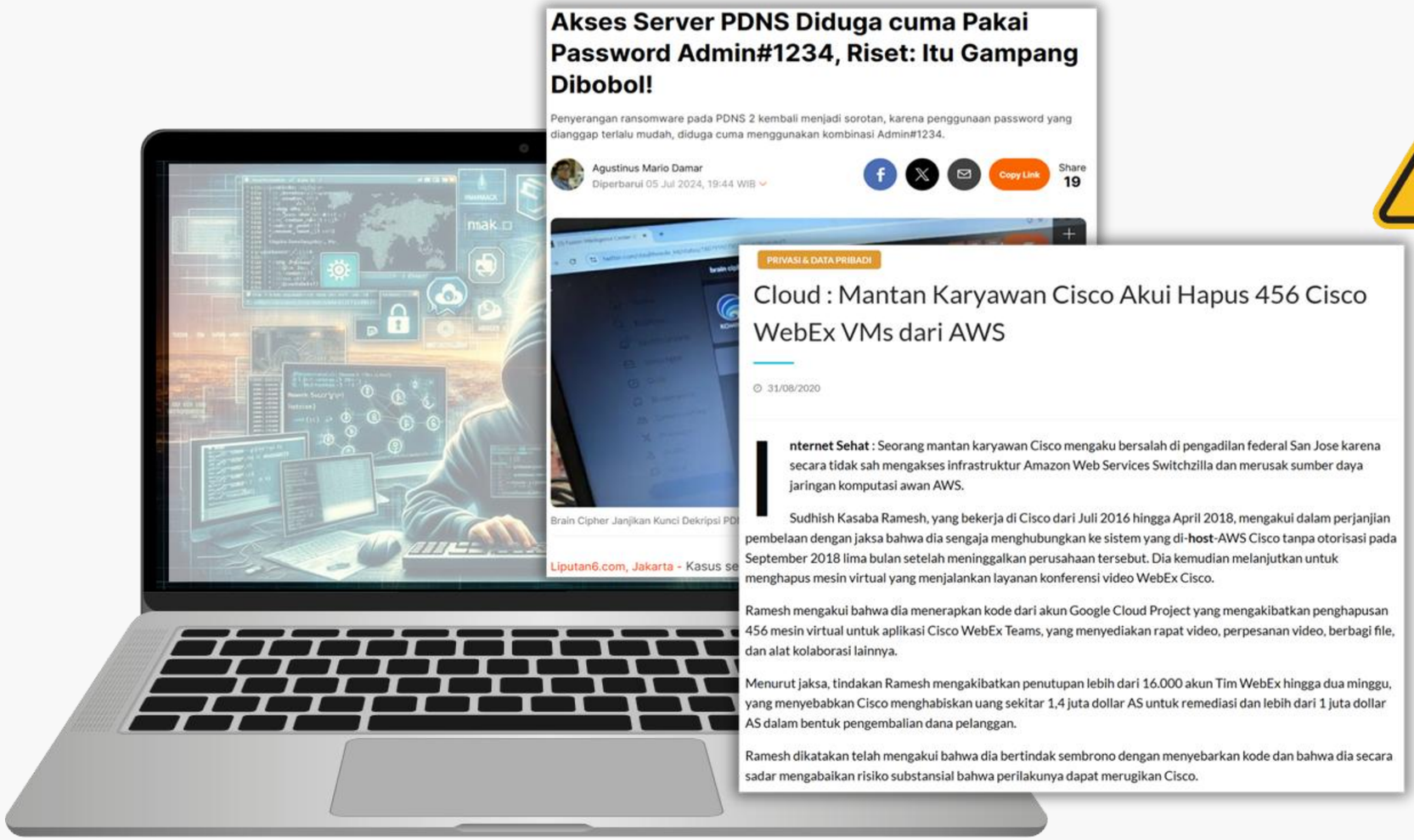
ALTOS SECURITY

Powered by TKMT Risk Management

CYBER RESILIENCE FOR THE DIGITAL ENTERPRISE

Real-World Cyber Attack Case Study



DAMPAK:
KERUGIAN FINANSIAL, REPUTASI & HUKUMAN PIDANA

ALTOS SECURITY

ALTOS
an Acer Group Company

TKMT
PT. Tri Kreasi Mandiri Teknologi

1 PRIVILEGED ACCESSS MANAGEMENT

2 DATA LOSS PREVENTION

3 NEXT GENERATION FIREWALL

4 CYBER THREAT INTELEGENCE

REGULATION COMPLIANCE

UU PDP, SEOJK 29 & ISO 27001/2 COMPLIANCE

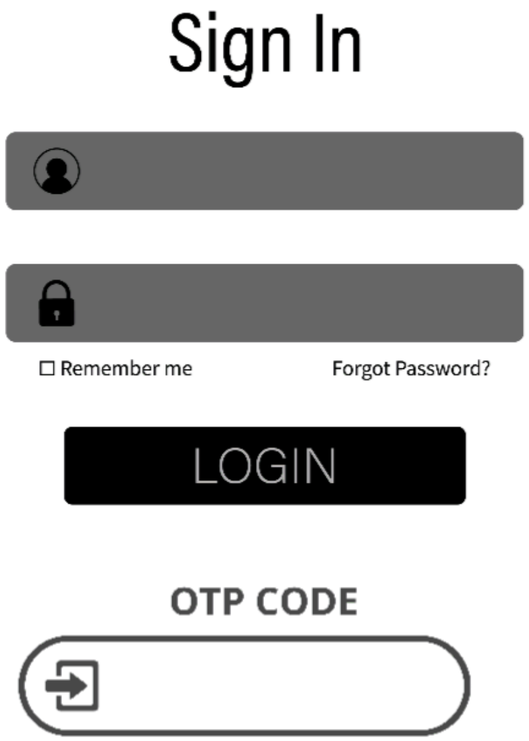
Sebagai dari pemenuhan syarat-syarat Infosec yang ditentukan dalam ISO 27001/27002, UU ITE, SEOJK, dan UU PDP bagi semua sektor industri.

ALTOS
an Acer Group Company

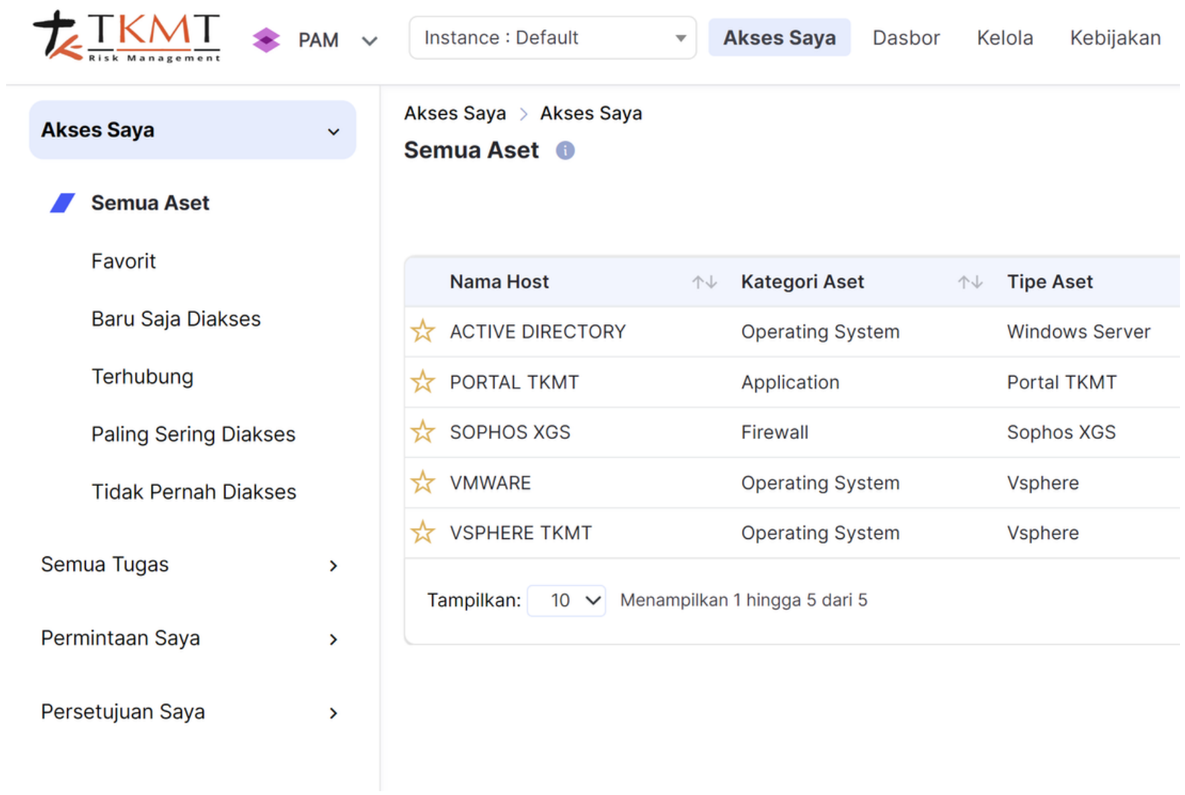
TKMT
PT. Tri Kreasi Mandiri Teknologi

MODUL PRIVILEGED ACCESS MANAGEMENT

Modul - Privileged Access Management



Modul - Privileged Access Management



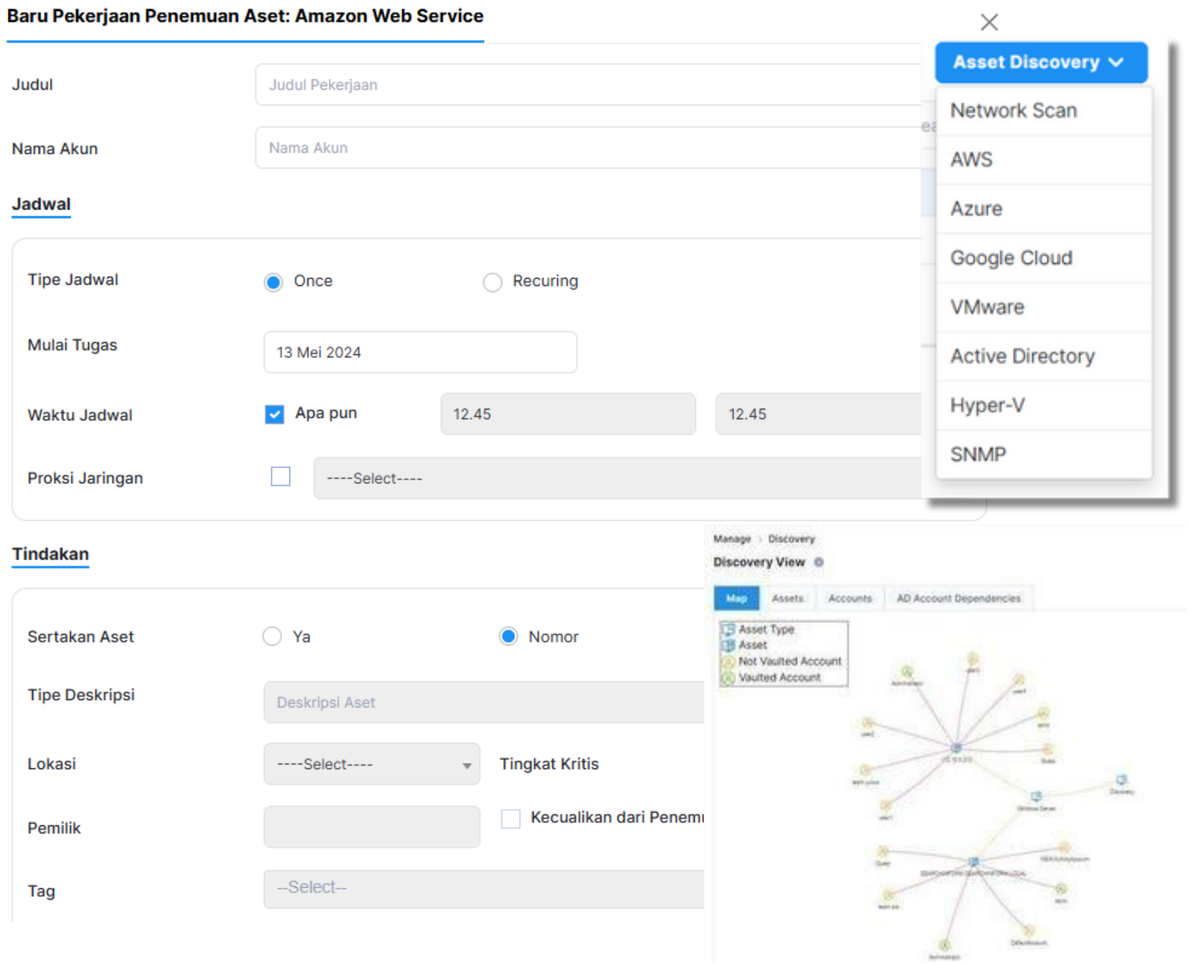
AKTIFKAN AKSES SATU KLIK

KLIK Ke server Anda, perangkat jaringan, aplikasi dan lainnya.

Satu identitas untuk login ke semua pemanfaatan cloud dan aplikasi lokal standar SSO

SINGLE SIGN-ON

Modul - Privileged Access Management



TEMUKAN ASET DAN AKUN

Melindungi aset dan perkuat keamanan akses

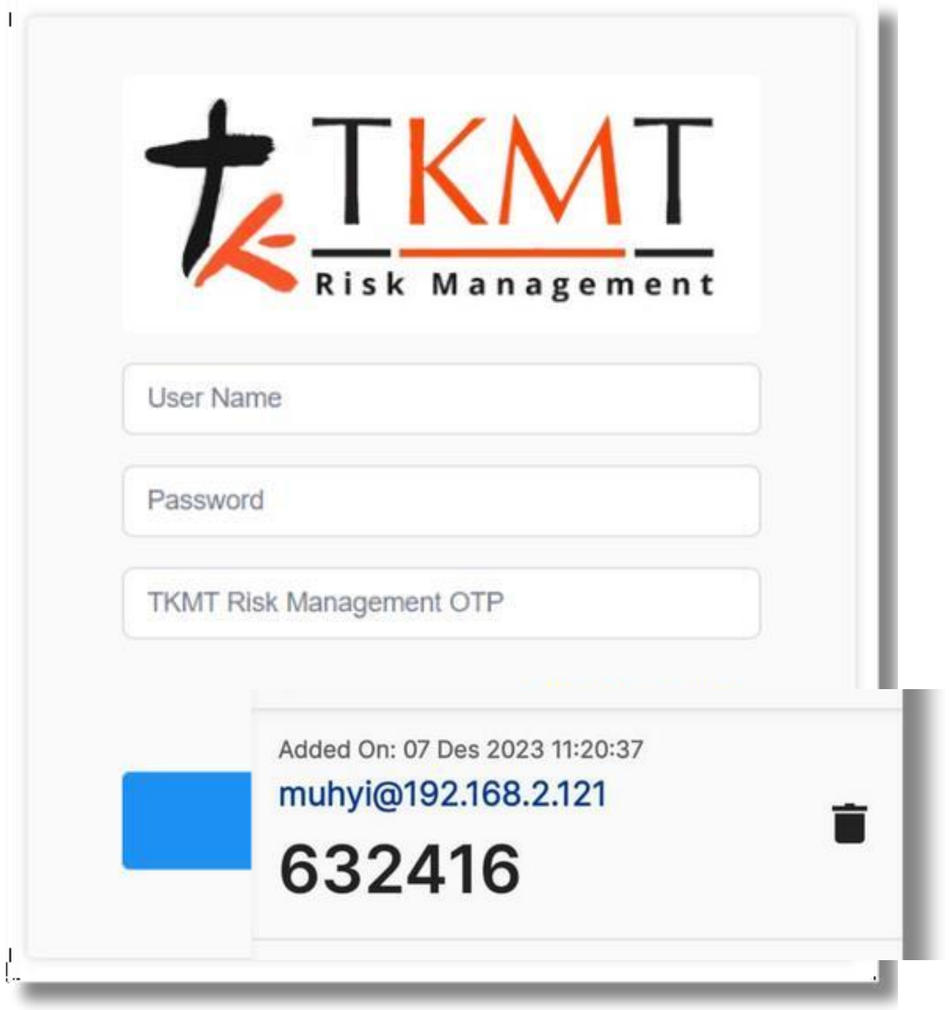
TEMUKAN ASET

Temukan aset dalam perusahaan untuk ditambahkan ke Aset Akses, menggunakan banyak metode, seperti pemindaian jaringan, direktori aktif, snmp,cloud, hyper-v dan lain-lain.

TEMUKAN AKUN

Temukan akun di aset Perusahaan dengan menggunakan akun administrator di aset.

Modul - Privileged Access Management



TAMBAHKAN LAPISAN LAYER SECURITY EXTRA

Perkuat keamanan melalui jaminan autentikasi yang tinggi, dorong pengguna MFA yang unggul pengalaman

MULTI FACTOR AUTHENTICATION

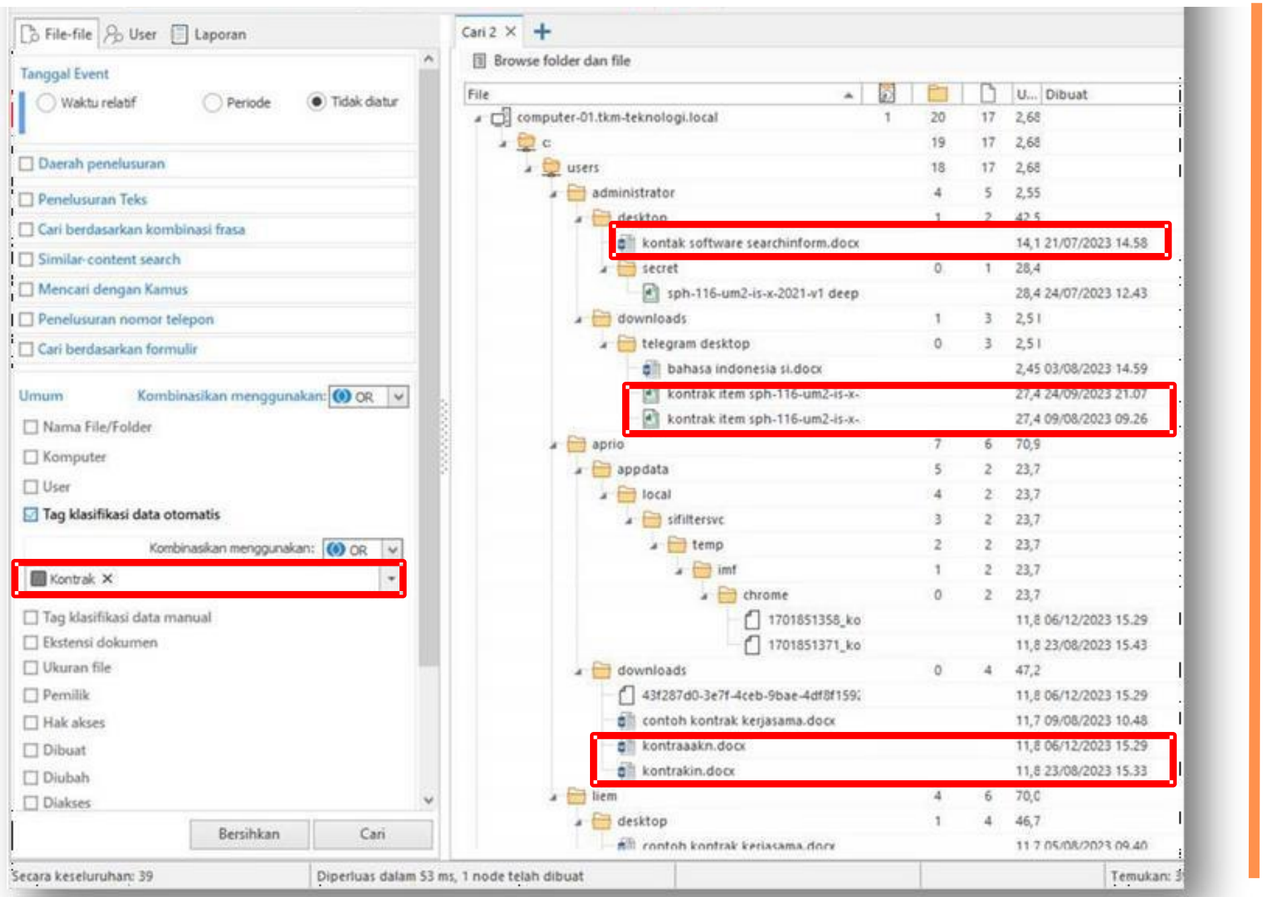
BROAD AUTHENTICATION METHODS

RISK AWARE

STANDARD BASED

MODUL DATA LOSS PREVENTION

Modul - Data Loss Prevention



TEMUKAN DATA AUDIT

Temukan data penting dan lakukan klasifikasi.

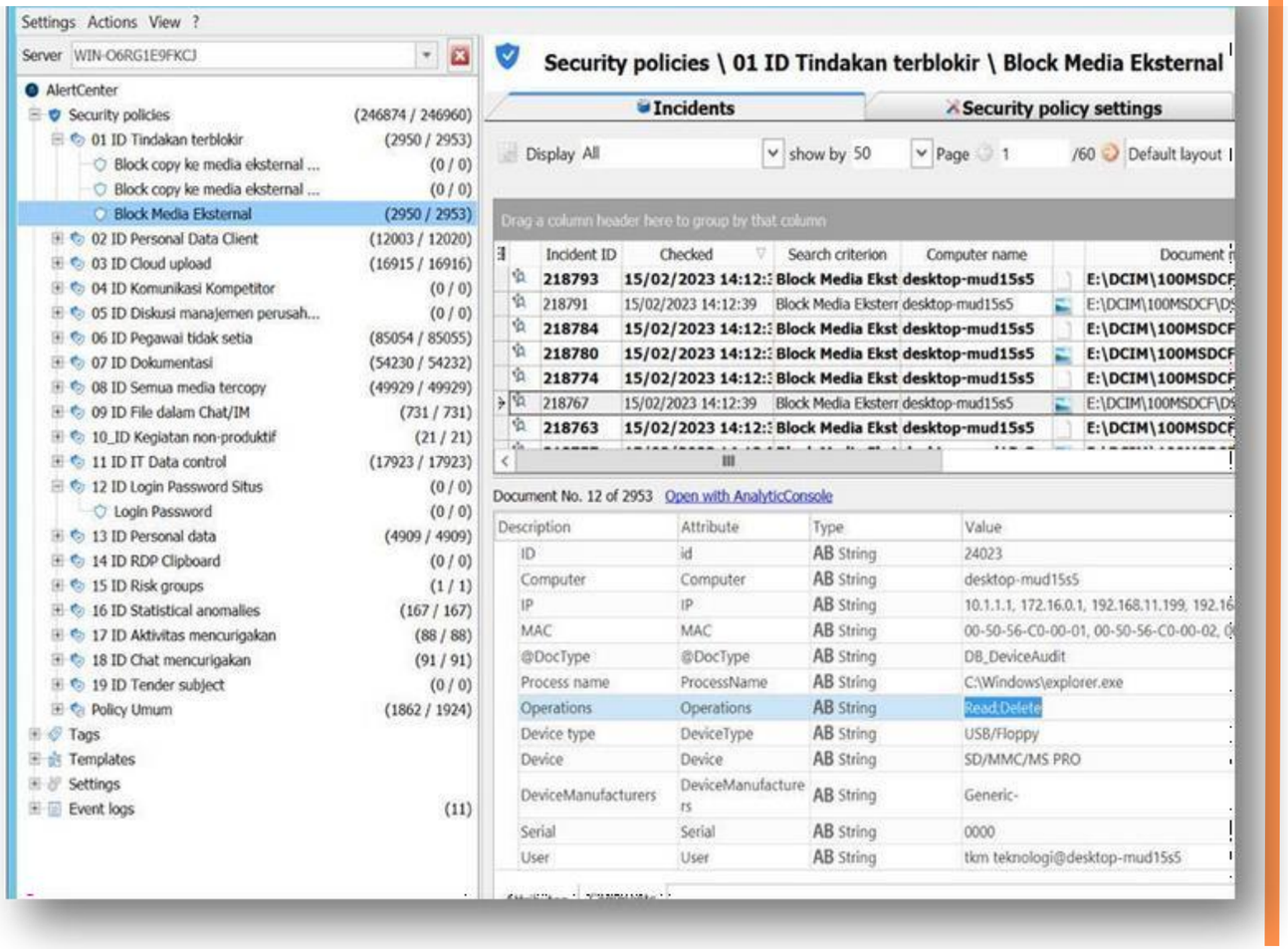
KLASIFIKASI DATA

Klasifikasikan data berdasarkan tingkatan data, apakah data kritis, tinggi, sedang, rendah atau klasifikasi data otomatis

TEMUKAN DATA AUDIT

melakukan penemuan tentang data-data penting dalam suatu perusahaan untuk mencegah kebocoran data

Modul - Data Loss Prevention



PERLINDUNGAN DATA PENTING

Melindungi data penting dalam suatu perusahaan

DATA LOSS PREVENTION

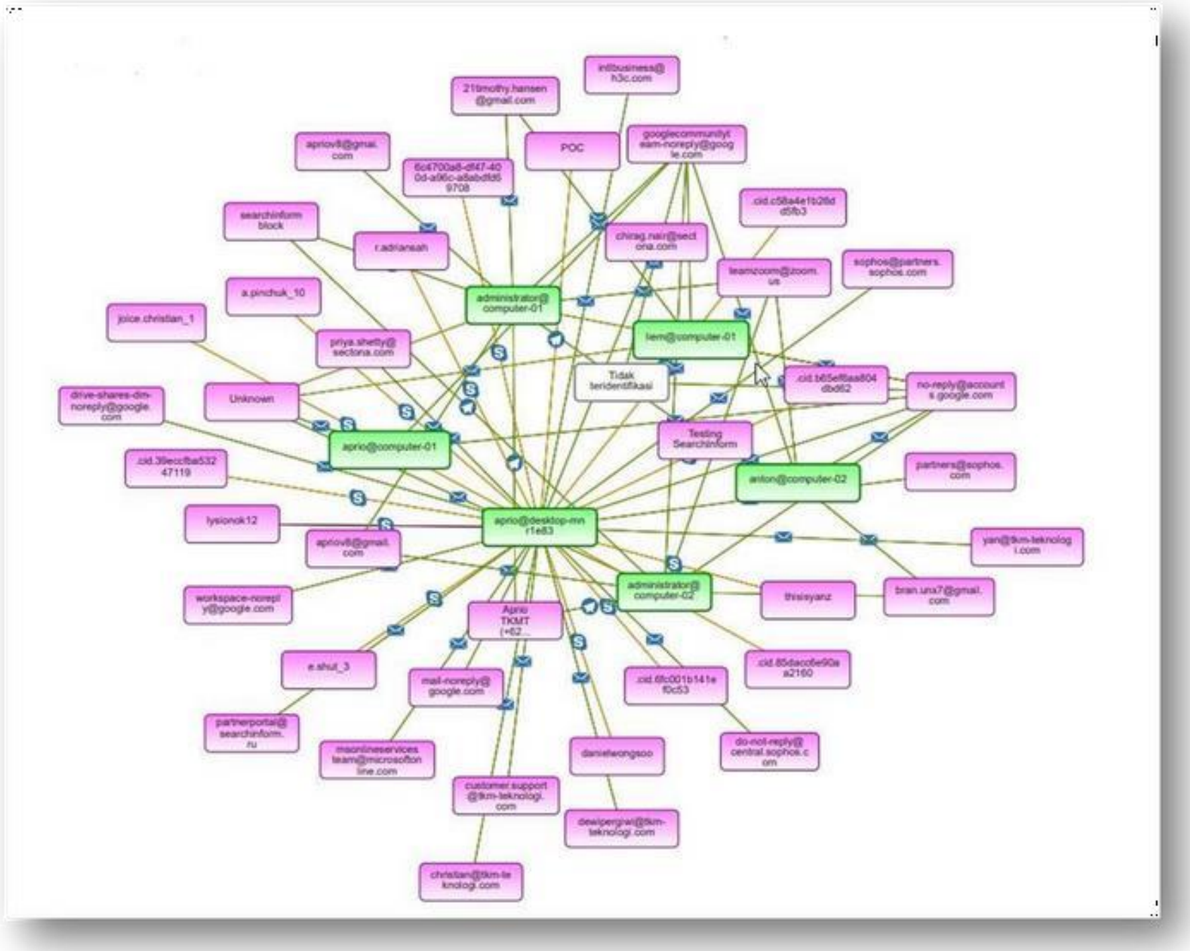
Melindungi data-data penting perusahaan dari berbagai media yang bisa menjadi pusat kebocoran data seperti:

- E-mail
- InstantMessenger
- Cloud
- ExternalDrives

CONTROLLING DATA

Dapat mengontrol data penting dari berbagai platform

Modul - Data Loss Prevention



USER INTERAKSI DIAGRAM

Membantu aktivitas forensik digital dengan grafik interaksi pengguna

KOMUNIKASI USER

Dapat melihat komunikasi dan menganalisis antar pengguna, baik pengguna internal maupun eksternal serta platform komunikasi yang digunakan.

FORENSIK DIGITAL

Dapat membantu aktivitas forensik digital terhadap aktivitas mencurigakan

ALTOS
an Acer Group Company

TKMT
PT. Tri Kreasi Mandiri Teknologi

MODUL NEXT GENERATION FIREWALL

Modul - Next Generation Firewall

ALTOS an Acer Group Company

TKMT PT. Tri Kreasi Mandiri Teknologi

NEXT GENERATION FIREWALL

Untuk perusahaan publik dan komersial dengan ukuran berapa pun dengan 100 sd tak terhingga pengguna Internet yang menggunakan sistem operasi seluler dan desktop apa pun.

VPN SERVER

Untuk koneksi kantor dan pengguna jarak jauh yang aman dan andal melalui VPN. Klien VPN WireGuard Asli, mendukung protokol asli IKEv2/IPsec, L2TP/IPsec, SSTP. Biaya administrasi dan keamanan minimum untuk organisasi mandiri.

USER AUTHORIZATION

Gunakan otorisasi tunggal Kerberos atau otorisasi berdasarkan log keamanan pengontrol domain untuk kontrol akses ke situs web dan sumber daya internet yang transparan dan mudah

EMAIL SERVER AND RELAY

Sebagai perantara yang mengatur pengiriman, penerimaan, dan penerusan pesan email antara pengirim dan penerima.

PROXY SERVER AND WEB FILTER

Pemfilteran lalu lintas web berdasarkan 145 kategori. Inspeksi SSL. Streaming pemeriksaan virus.

INTEGRATION INTO NETWORK INFRASTRUCTURE

Konfigurasi integrasi yang mudah dengan Microsoft Active Directory, FreeIPA (akan datang), SIEM (via syslog), sistem pemantauan (agen Zabbix, SNMP), DLP (via ICAP). Protokol perutean dinamis BGP, OSPF.

MONITORING AND REPORTING

Laporan penggunaan web yang dikategorikan. Pelaporan situs web yang diizinkan atau diblokir. Log waktu sesi web terperinci.

CENTER CONSOLE

Pusat kendali Server NGFW. Kebijakan keamanan umum diterapkan pada firewall, filter konten, kontrol aplikasi, batasan kecepatan.

Modul - Next Generation Firewall

ALTOS an Acer Group Company

TKMT PT. Tri Kreasi Mandiri Teknologi

DEEP PACKET INSPECTION

FILTERING NGFW SUPPORT SAMPAI LAYER 7

CONTENT FILTERING

Kontrol akses jaringan dengan pemblokiran 500 juta alamat dalam 145 kategori seperti phishing/penipuan, pusat distribusi malware, botnet, pengumpulan data rahasia, spam, iklan/spanduk, dll.

BLOCKING ANONYMIZERS

Pemblokiran berupaya melewati sistem pemfilteran konten menggunakan server proxy, plugin browser, TOR, dan VPN.

APPLICATION CONTROL (DPI)

Memungkinkan Anda memblokir lalu lintas dari skype, WhatsApp, BitTorrent, Youtube, Steam, TikTok, dll. untuk pengguna dan grup tertentu.

INTRUSION PREVENTION SYSTEM (IPS)

Memblokir serangan, DoS, spyware, telemetri windows, pusat C&C botnet, penambang kripto berbahaya. Aktivitas pencegahan virus dalam jaringan. Memblokir wilayah yang tidak dapat diandalkan berdasarkan reputasi GeoIP dan IP.

WEB APPLICATION FIREWALL (WAF)

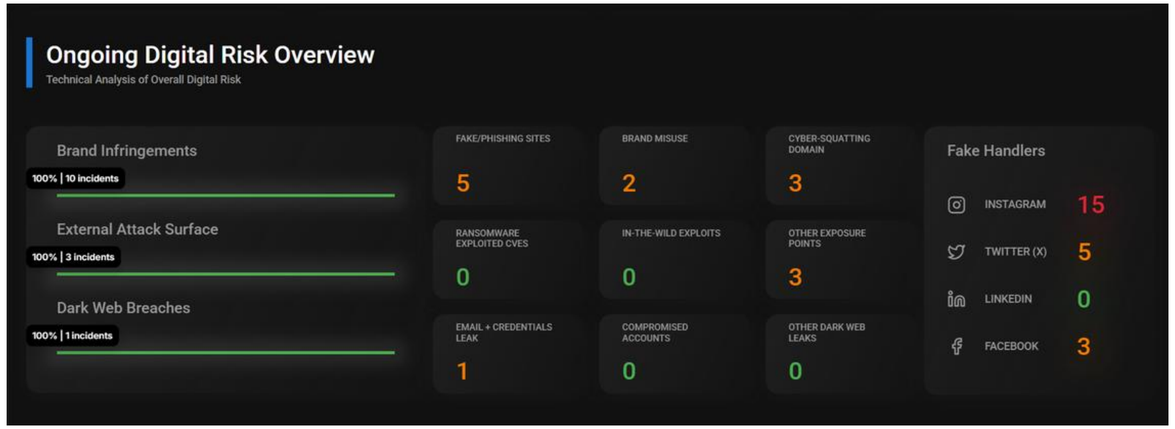
Melindungi sumber daya web internal menggunakan firewall aplikasi web saat mempublikasikannya di internet. Pemfilteran dan perlindungan lalu lintas email untuk server email yang dipublikasikan.

ANTIVIRUS TRAFFIC SCANNING

Pemindaian streaming file dan skrip yang diunduh menggunakan perangkat lunak anti-virus. Memblokir virus sebelum masuk ke jaringan lokal.

MODUL CYBER THREAT INTELLIGENCE

Modul – Cyber Threat Intelligence



BRANDSAFE

Lindungi brand anda dari pemalsuan di internet

BRAND IMPOSTOR TAKEDOWN

Melindungi merek Anda dari afiliasi yang menyesatkan atau tidak sah yang berpotensi merusak reputasi.

PHISHING DETECTION

Melindungi merek Anda dari afiliasi yang menyesatkan atau tidak sah yang berpotensi merusak reputasi.

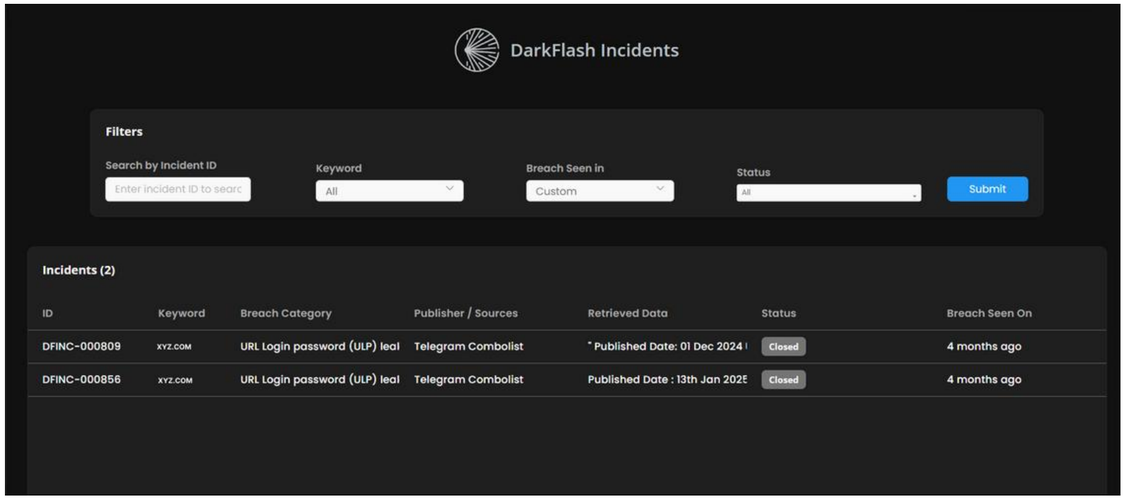
BANNED FAKE ACCOUNT

Mendeteksi dan menghapus akun media sosial palsu yang menyamar sebagai perwakilan resmi merek Anda.

TAKEDOWN FAKE APPLICATION

Mengidentifikasi dan menghapus aplikasi palsu yang menyamar sebagai aplikasi resmi milik Anda.

Modul – Cyber Threat Intelligence



DARKFLASH

Deteksi & Monitor Pelanggaran Data Secara Instan dengan Solusi Pemantauan Dark/Deep Web

MONITOR KEBOCORAN KREDENSIAL

Melindungi merek Anda dari afiliasi yang menyesatkan atau tidak sah yang berpotensi merusak reputasi.

DETEKSI KEBOCOROAN SOURCE-CODE DI REPOSITORY KODE

Mengawasi platform seperti GitHub dan GitLab untuk mencegah kebocoran kode sumber

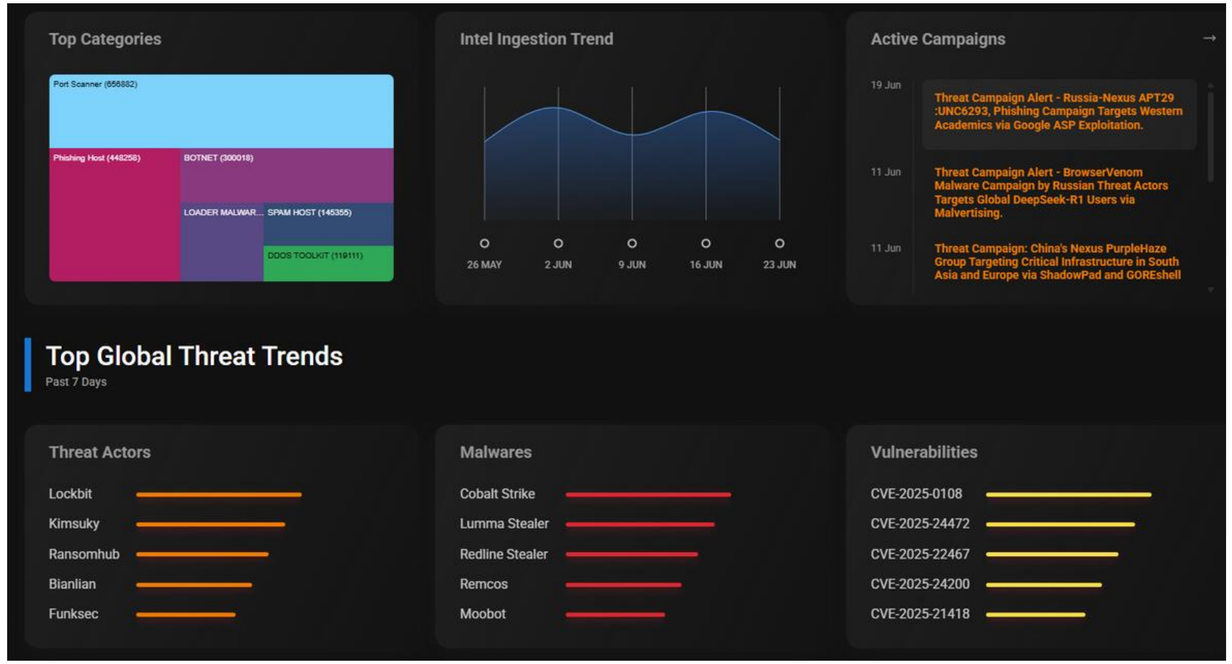
IDENTIFIKASI KEBCOROAN DOKUMEN PRIBADI

Mengidentifikasi kredensial yang telah bocor dan digunakan oleh pihak tidak sah.

DETEKSI PELANGGRAN IDENTITAS PRIBADI

Memantau dan mendeteksi penyebaran data pribadi seperti KTP, alamat, atau nomor kontak

Modul – Cyber Threat Intelligence



THREATBOLT INTELLIGENCE

Deteksi & Monitor Pelanggaran Data Secara Instan dengan Solusi Pemantauan Dark/Deep Web

ANALISIS TREND ANCAMAN SIBER

Menyediakan data tren ancaman siber guna membantu tim memahami jenis dan pola serangan yang sedang marak terjadi.

LIVE-MAP ANCAMAN SIBER

Visualisasi kampanye APT/Ransomware secara real-time yang menargetkan jaringan Anda.

NOTIFIKASI EXPLOITASI CVE

Notifikasi instan terkait eksploitasi CVE yang berdampak pada organisasi Anda.

ANALISA KAMPANYE ANCAMAN SIBER

Analisa kampanye ancaman siber bertujuan mengungkap pola dan tujuan serangan agar dapat dilakukan pencegahan dan respons yang tepat.

Modul – Cyber Threat Intelligence

SHADOWSPOT

Identifikasi celah dari sudut pandang penyerang dengan ShadowSpot External Attack Surface Management.

DETEKSI KELEMAHAN ZERO DAY

Dengan pemahaman terhadap aset dan jalur eksposurnya, pelanggan dapat segera melakukan mitigasi terhadap kerentanan zero-day.

LIVE-MAP ASSET TEREKSPOS

memetakan aset-aset digital yang terekspos secara global berdasarkan lokasi geografis

PEMINDAIAN KELEMAHAN OTOMATIS

Melakukan pemindaian rutin untuk mendeteksi kerentanan, kesalahan konfigurasi yang berpotensi dimanfaatkan oleh penyerang.

PROACTIVE ALLERTING

Notifikasi instan atas temuan kritis yang berpotensi menjadi titik masuk bagi penyerang ke dalam sistem.

Thank You!

ALTOS
an Acer Group Company

TKMT
PT. Tri Kreasi Mandiri Teknologi