

ALTOS SECURITY



Powered by  TKMT
Risk Management

CYBER RESILIENCE FOR THE DIGITAL ENTERPRISE

Real-World Cyber Attack Case Study

Akses Server PDNS Diduga cuma Pakai Password Admin#1234, Riset: Itu Gampang Dibobol!

Penyerangan ransomware pada PDNS 2 kembali menjadi sorotan, karena penggunaan password yang dianggap terlalu mudah, diduga cuma menggunakan kombinasi Admin#1234.

Agustinus Mario Damar
Diperbarui 05 Jul 2024, 19:44 WIB



Cloud : Mantan Karyawan Cisco Akui Hapus 456 Cisco WebEx VMs dari AWS

31/08/2020

Internet Sehat : Seorang mantan karyawan Cisco mengaku bersalah di pengadilan federal San Jose karena secara tidak sah mengakses infrastruktur Amazon Web Services Switchzilla dan merusak sumber daya jaringan komputasi awan AWS.

Sudhish Kasaba Ramesh, yang bekerja di Cisco dari Juli 2016 hingga April 2018, mengakui dalam perjanjian pembelaan dengan jaksa bahwa dia sengaja menghubungkan ke sistem yang di-host-AWS Cisco tanpa otorisasi pada September 2018 lima bulan setelah meninggalkan perusahaan tersebut. Dia kemudian melanjutkan untuk menghapus mesin virtual yang menjalankan layanan konferensi video WebEx Cisco.

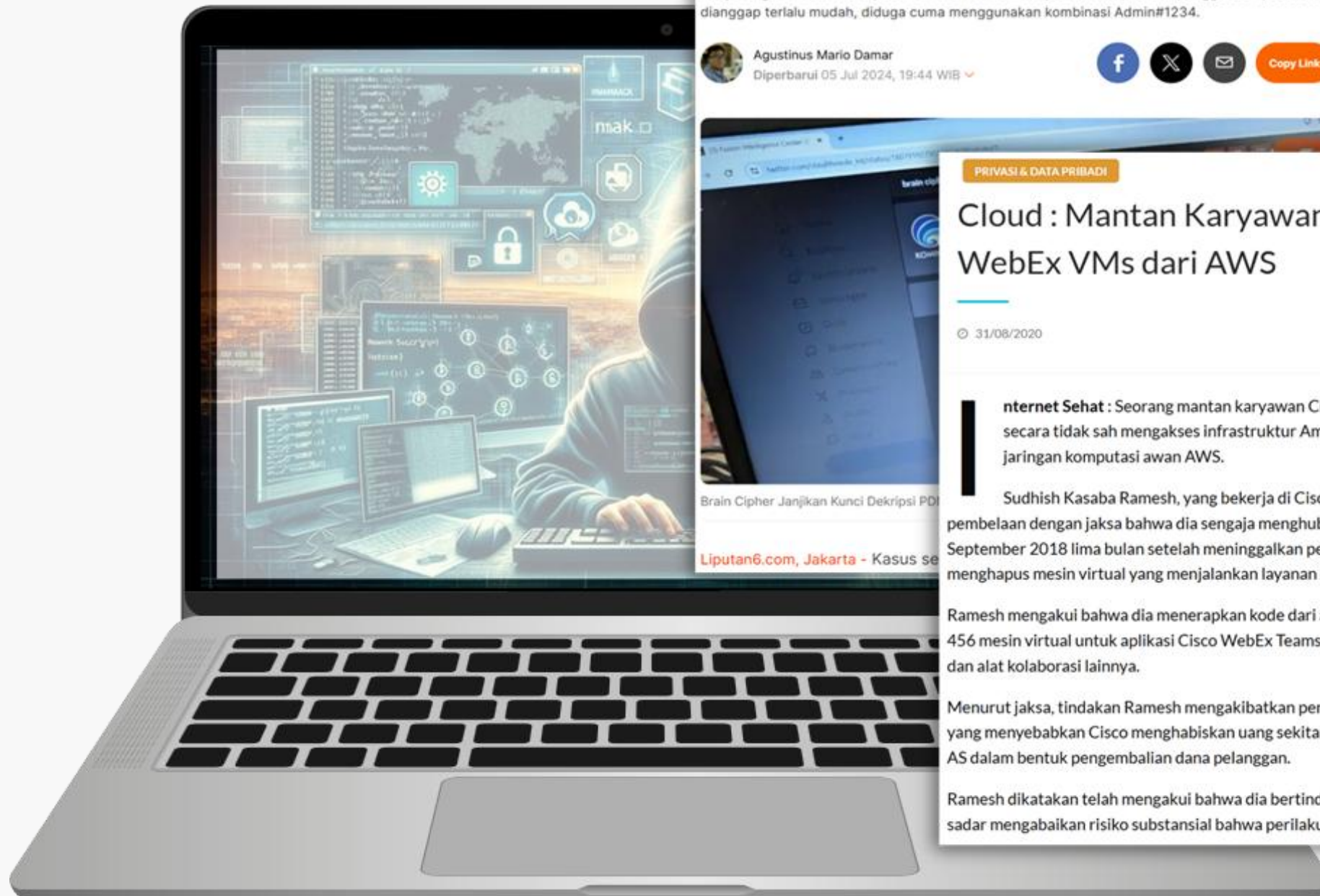
Ramesh mengakui bahwa dia menerapkan kode dari akun Google Cloud Project yang mengakibatkan penghapusan 456 mesin virtual untuk aplikasi Cisco WebEx Teams, yang menyediakan rapat video, perpesanan video, berbagi file, dan alat kolaborasi lainnya.

Menurut jaksa, tindakan Ramesh mengakibatkan penutupan lebih dari 16.000 akun Tim WebEx hingga dua minggu, yang menyebabkan Cisco menghabiskan uang sekitar 1,4 juta dollar AS untuk remediasi dan lebih dari 1 juta dollar AS dalam bentuk pengembalian dana pelanggan.

Ramesh dikatakan telah mengakui bahwa dia bertindak sembrono dengan menyebarkan kode dan bahwa dia secara sadar mengabaikan risiko substansial bahwa perilakunya dapat merugikan Cisco.



DAMPAK:
KERUGIAN FINANSIAL,
REPUTASI & HUKUMAN
PIDANA





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.





 **MODUL PRIVILEGED ACCESS MANAGEMENT**



Modul - Privileged Access Management



Sign In

Remember me

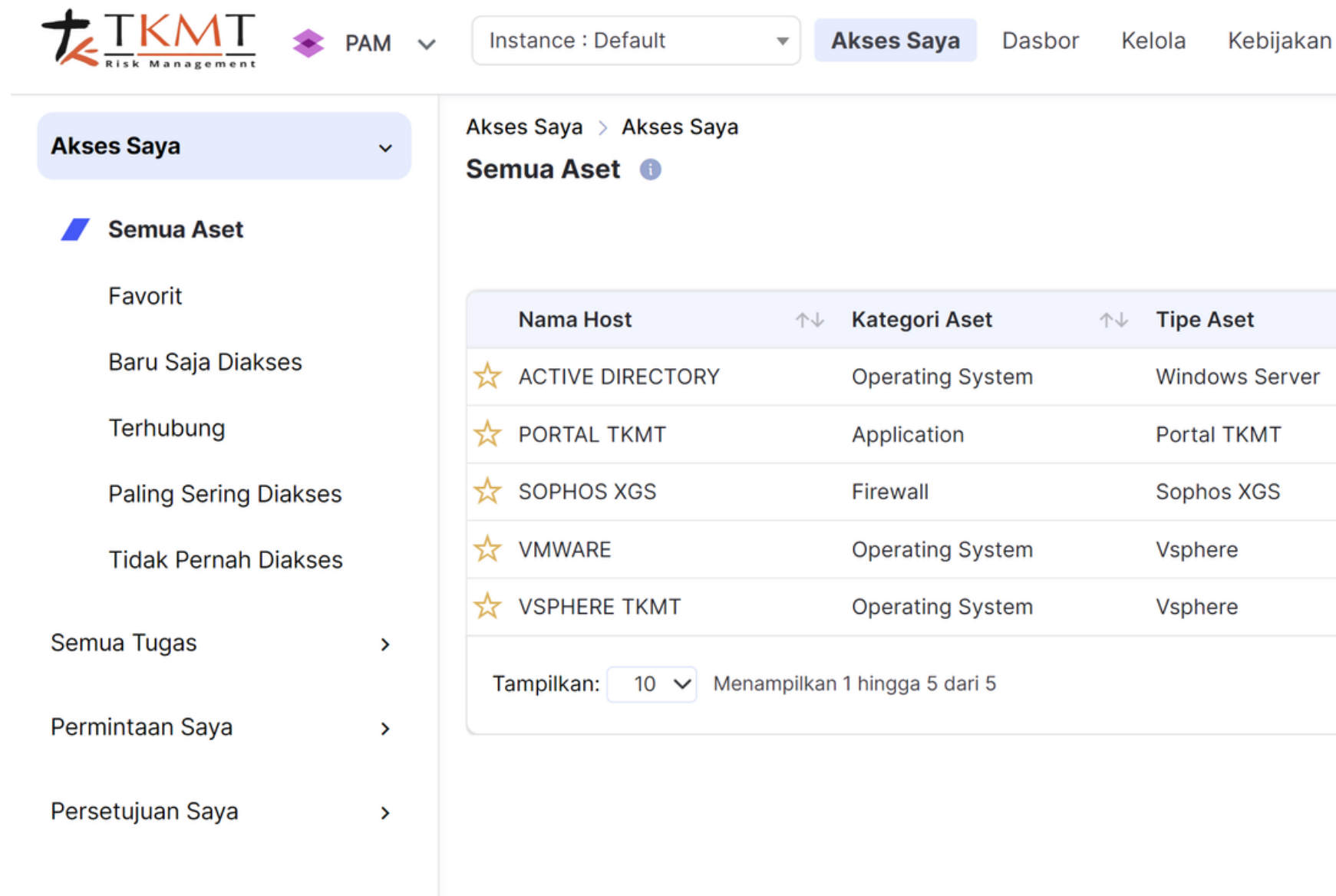
[Forgot Password?](#)

LOGIN

OTP CODE



Modul - Privileged Access Management



The screenshot shows the TKMT PAM dashboard. The top navigation bar includes the TKMT logo, 'PAM', 'Instance : Default', and 'Akses Saya' (highlighted), along with links for 'Dasbor', 'Kelola', and 'Kebijakan'. The left sidebar contains navigation options: 'Akses Saya', 'Semua Aset' (selected), 'Favorit', 'Baru Saja Diakses', 'Terhubung', 'Paling Sering Diakses', 'Tidak Pernah Diakses', 'Semua Tugas', 'Permintaan Saya', and 'Persetujuan Saya'. The main content area displays 'Akses Saya > Akses Saya' and 'Semua Aset'. A table lists assets with columns for 'Nama Host', 'Kategori Aset', and 'Tipe Aset'. Below the table is a 'Tampilkan: 10' dropdown and the text 'Menampilkan 1 hingga 5 dari 5'.

Nama Host	Kategori Aset	Tipe Aset
★ ACTIVE DIRECTORY	Operating System	Windows Server
★ PORTAL TKMT	Application	Portal TKMT
★ SOPHOS XGS	Firewall	Sophos XGS
★ VMWARE	Operating System	Vsphere
★ VSPHERE TKMT	Operating System	Vsphere

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

Baru Pekerjaan Penemuan Aset: Amazon Web Service

Judul:

Nama Akun:

Jadwal

Tipe Jadwal: Once Recuring

Mulai Tugas:

Waktu Jadwal: Apa pun

Proksi Jaringan:

Tindakan

Sertakan Aset: Ya Nomor

Tipe Deskripsi:

Lokasi: Tingkat Kritis

Pemilik: Kecualikan dari Penem.

Tag:


Asset Discovery

- Network Scan
- AWS
- Azure
- Google Cloud
- VMware
- Active Directory
- Hyper-V
- SNMP

Discovery View

Map Assets Accounts AD Account Dependencies

Asset Type
Asset
Not Vaulted Account
Vaulted Account



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.



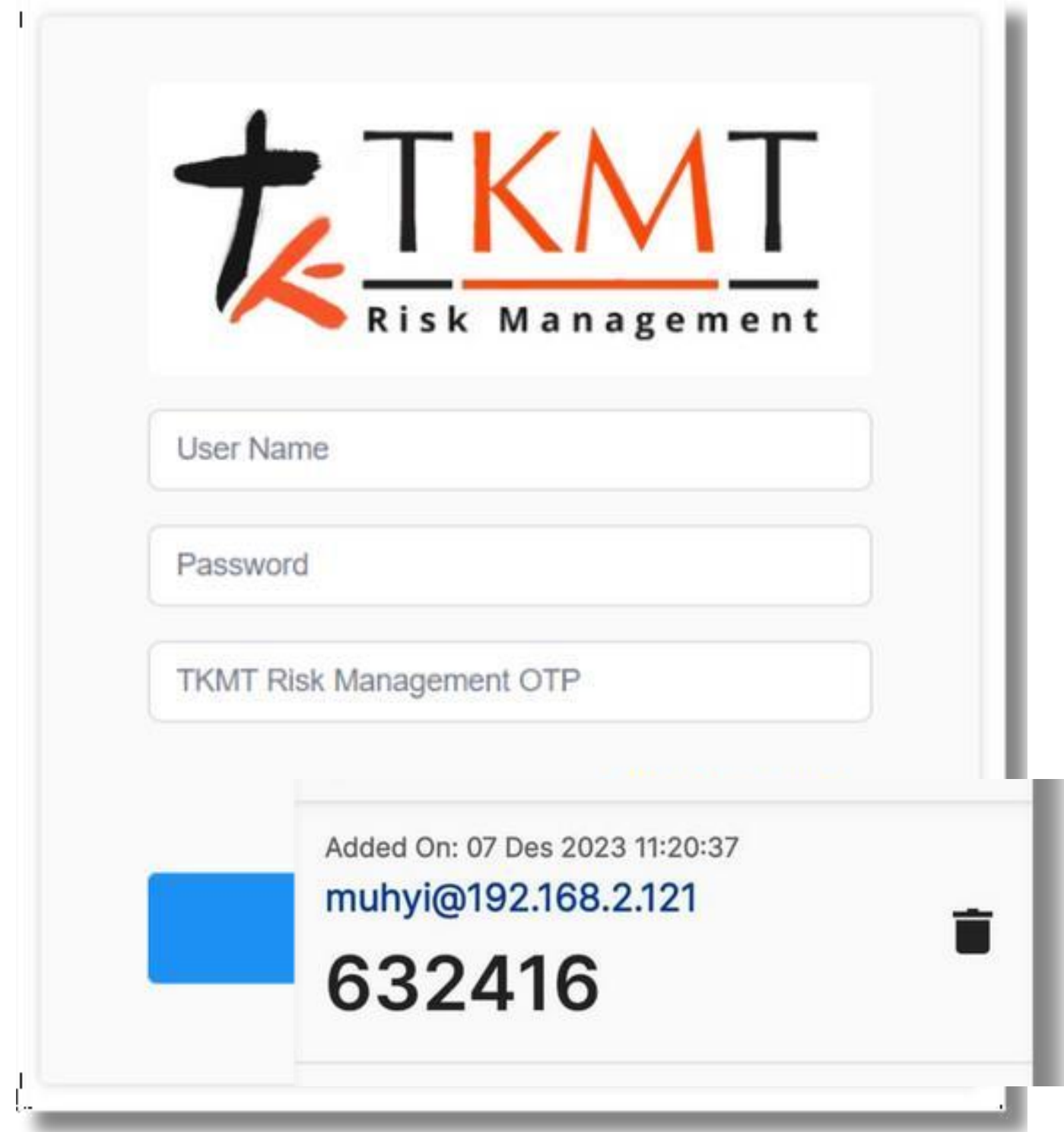
TEMUKAN AKUN

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



TKMT Risk Management

User Name

Password

TKMT Risk Management OTP

Added On: 07 Des 2023 11:20:37
muhyi@192.168.2.121
632416



**MULTI FACTOR
AUTHENTICATION**



**BROAD AUTHENTICATION
METHODS**



RISK AWARE

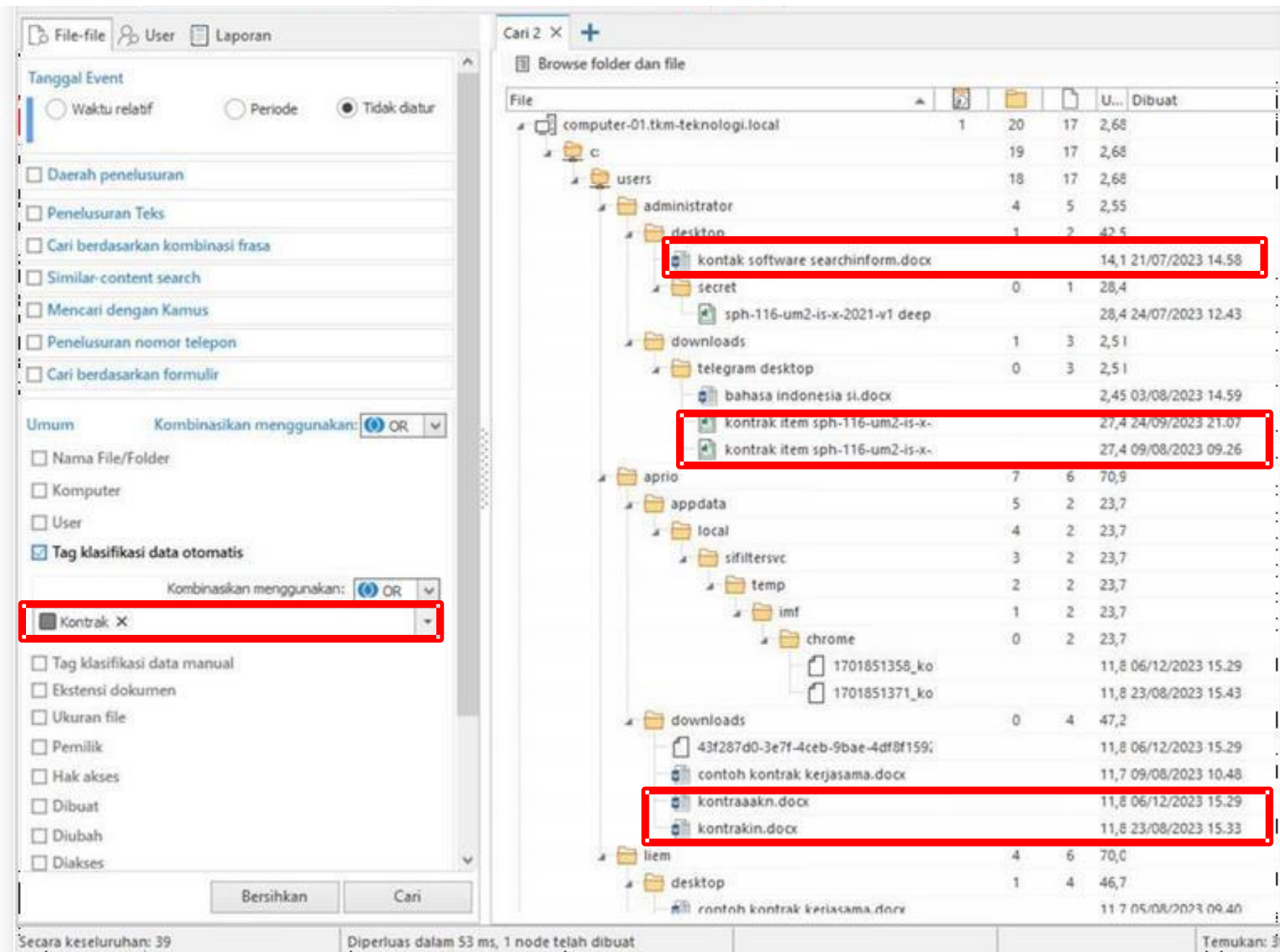


STANDARD BASED



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

The screenshot displays the Microsoft Security Center interface. On the left, a tree view shows 'Security policies' with '01 ID Tindakan terblokir' expanded to 'Block Media Eksternal'. The main pane shows 'Security policies \ 01 ID Tindakan terblokir \ Block Media Eksternal' with an 'Incidents' tab. A table lists several incidents, all dated 15/02/2023 14:12:39, with the search criterion 'Block Media Ekst' and computer name 'desktop-mud15s5'. Below the incidents, a 'Document No. 12 of 2953' is shown with a table of attributes and values.

Incident ID	Checked	Search criterion	Computer name	Document
218793	15/02/2023 14:12:39	Block Media Ekst	desktop-mud15s5	E:\DCIM\100MSDCF
218791	15/02/2023 14:12:39	Block Media Eksterr	desktop-mud15s5	E:\DCIM\100MSDCF\DS
218784	15/02/2023 14:12:39	Block Media Ekst	desktop-mud15s5	E:\DCIM\100MSDCF
218780	15/02/2023 14:12:39	Block Media Ekst	desktop-mud15s5	E:\DCIM\100MSDCF
218774	15/02/2023 14:12:39	Block Media Ekst	desktop-mud15s5	E:\DCIM\100MSDCF
218767	15/02/2023 14:12:39	Block Media Eksterr	desktop-mud15s5	E:\DCIM\100MSDCF\DS
218763	15/02/2023 14:12:39	Block Media Ekst	desktop-mud15s5	E:\DCIM\100MSDCF

Description	Attribute	Type	Value
ID	id	AB String	24023
Computer	Computer	AB String	desktop-mud15s5
IP	IP	AB String	10.1.1.1, 172.16.0.1, 192.168.11.199, 192.168.11.199
MAC	MAC	AB String	00-50-56-C0-00-01, 00-50-56-C0-00-02, 00-50-56-C0-00-03
@DocType	@DocType	AB String	DB_DeviceAudit
Process name	ProcessName	AB String	C:\Windows\explorer.exe
Operations	Operations	AB String	Read, Delete
Device type	DeviceType	AB String	USB/Floppy
Device	Device	AB String	SD/MMC/MS PRO
DeviceManufacturers	DeviceManufacturers	AB String	Generic-
Serial	Serial	AB String	0000
User	User	AB String	tkm teknologi@desktop-mud15s5

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



**ALTOS SECURITY
CYBER SECURITY
SOLUTIONS**



MODUL NEXT GENERATION FIREWALL

NGFW - Pengamanan Gerbang Lalu Lintas Data Anda



Modul - Next Generation Firewall

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.



ALTOS NGFW

Powered by TKMT
Risk Management



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.



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

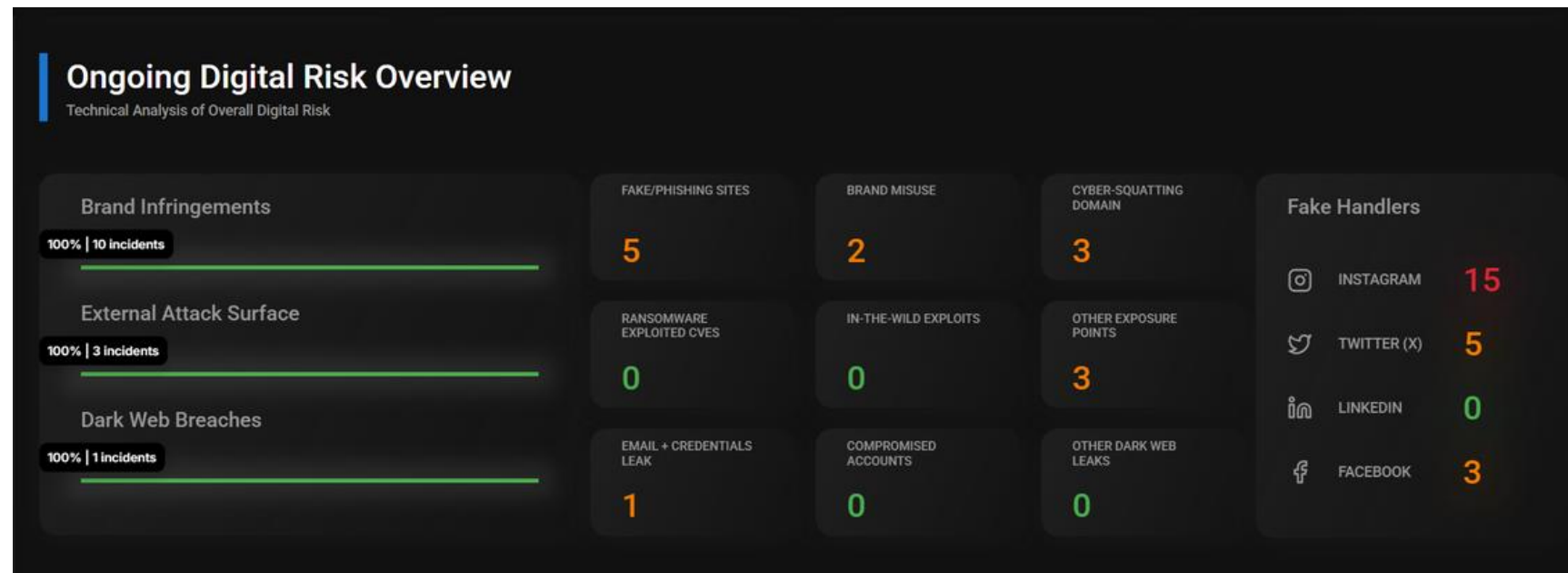
Pemindaian streaming file dan skrip yang diunduh menggunakan perangkat lunak anti-virus. Memblokir virus sebelum masuk ke jaringan lokal.



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.



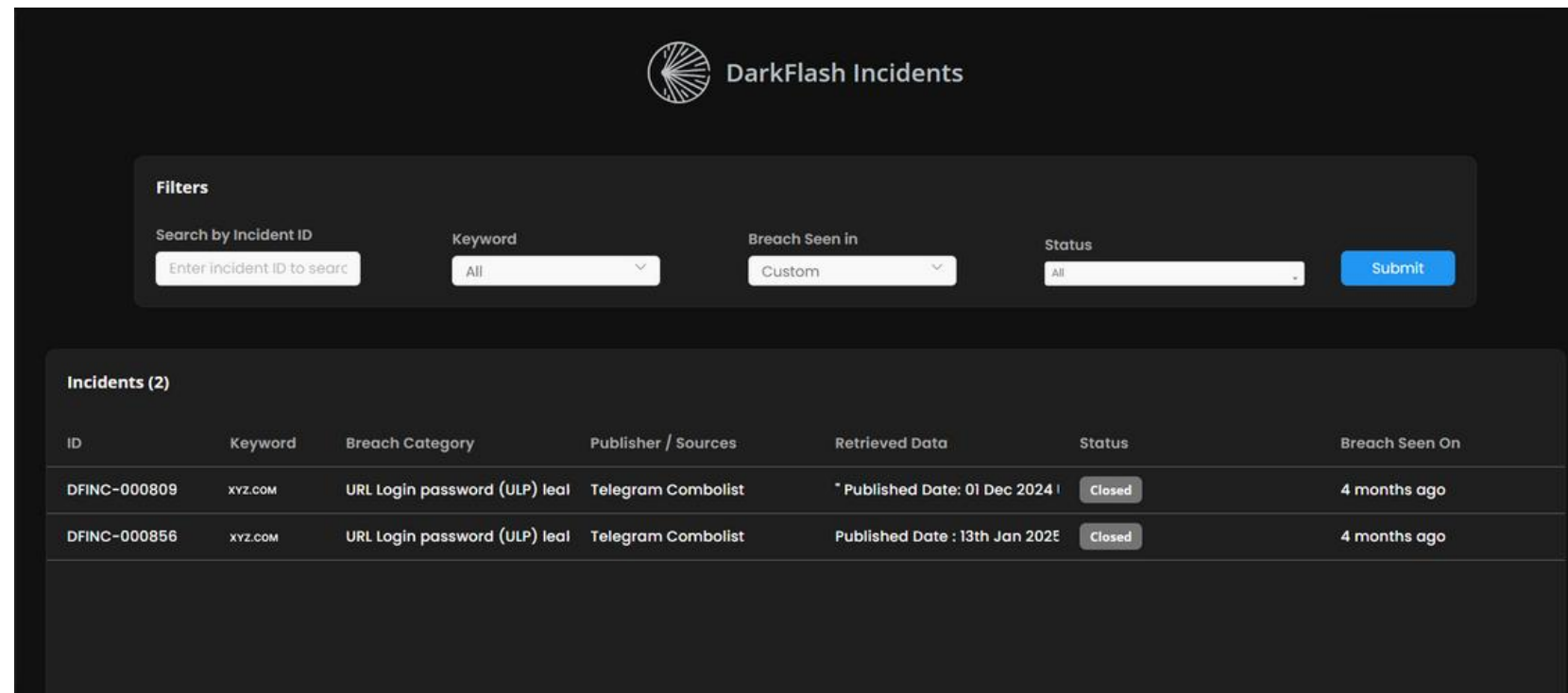
TAKEDOWN FAKE APPLICATION

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

Modul – Cyber Threat Intelligence

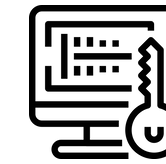
DARKFLASH

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



The screenshot shows the DarkFlash Incidents interface. At the top, there's a search bar with filters for Incident ID, Keyword, Breach Seen in, and Status. Below the filters, a table lists two incidents. The table has columns for ID, Keyword, Breach Category, Publisher / Sources, Retrieved Data, Status, and Breach Seen On.

ID	Keyword	Breach Category	Publisher / Sources	Retrieved Data	Status	Breach Seen On
DFINC-000809	xyz.com	URL Login password (ULP) leak	Telegram Combolist	Published Date: 01 Dec 2024	Closed	4 months ago
DFINC-000856	xyz.com	URL Login password (ULP) leak	Telegram Combolist	Published Date: 13th Jan 2025	Closed	4 months ago



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 KEBOCOROAN DOKUMEN PRIBADI

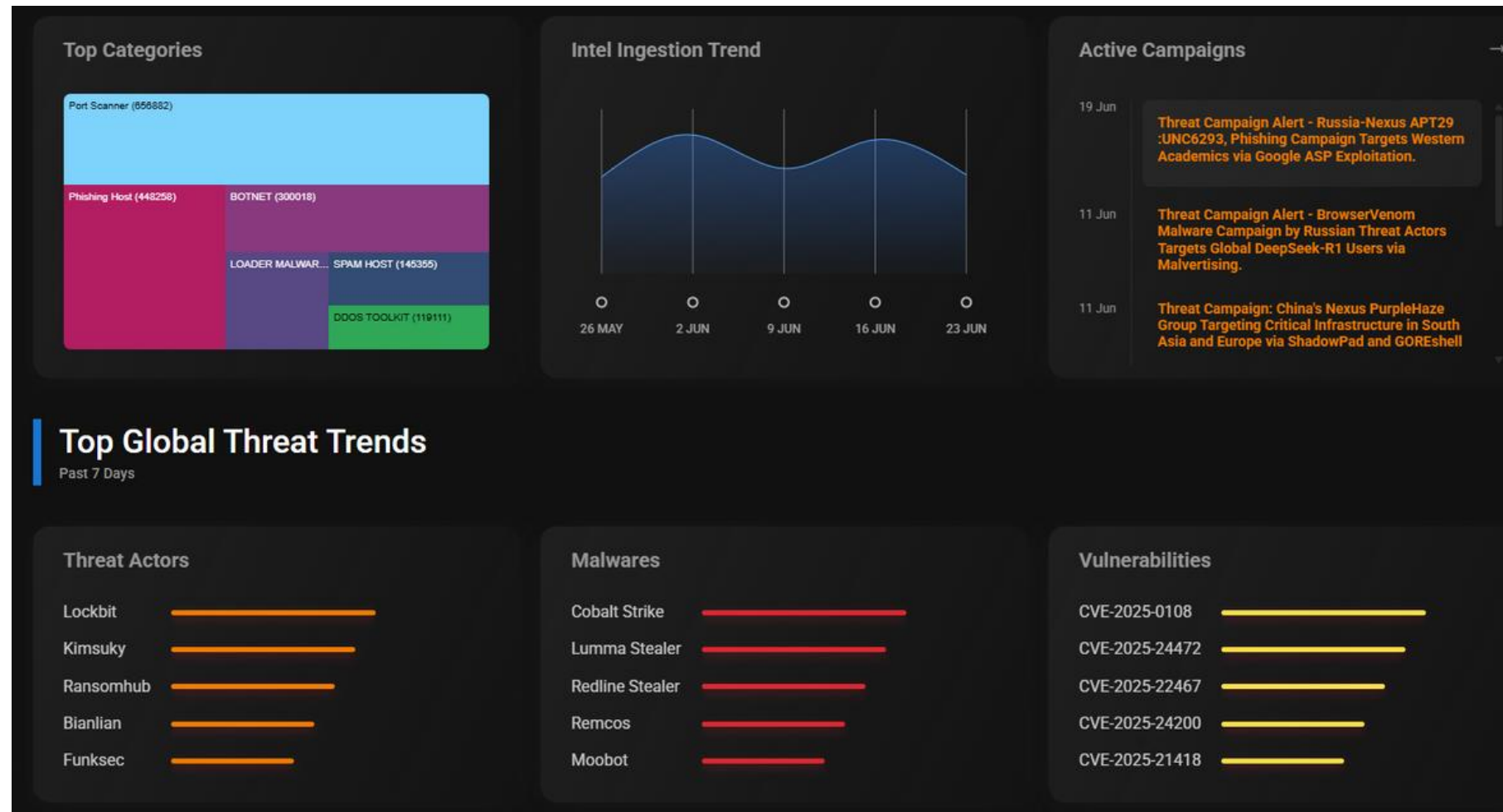
Mengidentifikasi kredensial yang telah bocor dan digunakan oleh pihak tidak sah.



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.

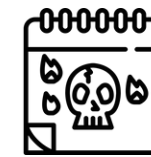
Modul – Cyber Threat Intelligence



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 ALERTING



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

