GEBYAR

AUTO-ID

BULETIN EDISI 66
MARET 2024

E-Buletin

UNTUK KALANGAN SENDIRI

EDR

XDR

SENJATA RAHASIA UNTUK KEAMANAN SIBER DI ERA DIGITAL

MANAGED SERVICE: SOLUSI TEPAT UNTUK KEBUTUHAN TI ANDA

WAVE PTX: RADIO PTT BROADBAND TANGGUH DARI MOTOROLA

TIPS UNTUK MENJAGA KEAMANAN KATA SANDI

MEDIA KOMUNIKASI PELANGGAN

ACS GROUP

PT. AUTOJAYA IDETECH
PT. SOLUSI PERIFERAL
www.acsgroup.co.id

EDITORIAL

Para Pembaca yang Budiman,

Puji syukur kehadirat Tuhan Yang Maha Esa, kita telah memasuki awal tahun 2024. Semoga segala pencapaian dan hambatan yang telah kita lalui di tahun sebelumnya dapat menjadi pengalaman yang berharga sebagai bekal menghadapi tantangan baru di tahun ini.

Dunia teknologi terus mengalami kemajuan yang begitu cepat sehingga memaksa kita untuk terus beradaptasi terhadap perubahan tersebut. Perkembangan dunia teknologi yang pesat, terutama di bidang keamanan siber, membawa berbagai tantangan baru. Kejahatan siber semakin berkembang dan masif, menuntut perusahaan dan organisasi untuk lebih waspada dan peduli terhadap keamanan jaringan dan data.

Kita harus terus siaga dalam menjaga keamanan data demi keberlangsungan bisnis. Saat ini, semua perusahaan atau organisasi harus mulai menyadari pentingnya keamanan jaringan dan data.

Buletin edisi kali ini mengangkat topik utama mengenai solusi pencegahan kejahatan siber dengan **EDR** (*Endpoint Detection and Response*) dan **XDR** (*Extended Detection and Response*). Solusi ini telah banyak digunakan di tingkat *enterprise* untuk meningkatkan keamanan siber.

Selain topik utama, buletin ini juga menghadirkan berbagai informasi menarik dan bermanfaat, seperti *Product Highlight* (Zebra, SEUIC, Sangfor, dan Fortinet), Tips dan Trik, serta *Corporate* dan *Principal Info*.

Semoga Buletin edisi awal tahun ini bermanfaat dan inspirasi bagi rekan-rekan bisnis sekalian dalam menghadapi tantangan di tahun 2024 ini.

Maulana Ibrahim

Professional Services Supervisor

PT. Autojaya Idetech

PT. Solusi Periferal

PEMIMPIN REDAKSI
Andre S.Kouanak

SEKRETARIS REDAKSI
Listya Kartikasari (Jakarta)
Indah Widiyanti (Cikarang)
A.A. Ayu Isna Surya Dewi (Denpasar)
Herdina Septiyaningrum (Semarang)
Sari Wilujeng (Surabaya)

EDITOR
Nuning Kustiawita
Chandra Sari

DESAINER
Oscar Budi Trianto

KONTRIBUTOR (PENULIS)
Maulana Ibrahim
Boedijanto
Ardy
Taufiq Rahman
Arijanto Hartanto
Angelina Rasta Perbina Ginting
Richard Andrian
Irvan Kurniawan Jong, PMP

ALAMAT REDAKSI
Jakarta (HO)
Perkantoran Gunung Sahari Permai
#C03-05, Jl. Gunung Sahari Raya
No 60-63 Jakarta 10610.
T : +6221-4208221, 4205187
E : acs.marcom@acsgroup.co.id

CONTENT

EDR DAN XDR: SENJATA RAHASIA UNTUK KEAMANAN SIBER DI ERA DIGITAL

by **Maulana Ibrahim**, Professional Services Supervisor | ACS Group

Di era digital, ancaman siber kian canggih. Untuk mengatasinya, solusi Endpoint Detection and Response (EDR) dan Extended Detection and Response (XDR) menjadi semakin penting.

EDR (*Endpoint Detection and Response*)

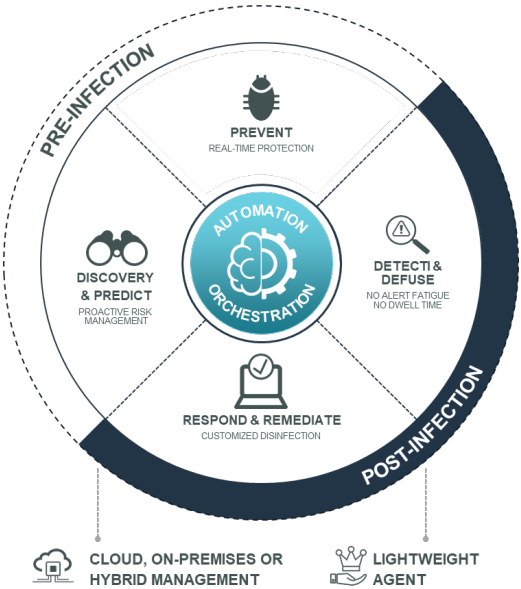
Perkembangan teknologi informasi saat ini mengalami banyak perubahan konseptual. Teknologi tidak lagi hanya tentang konektivitas dan saling terkoneksi. Keamanan data dan lalu lintas dalam jaringan menjadi bagian terpenting yang harus selalu dijaga.

Semakin berkembang kemudahan teknologi, semakin terbuka pula celah kejahatan terhadap data dan berbagai objek serangan lainnya.

Seiring meningkatnya ancaman dunia maya, langkah-langkah defensif perlu dipersiapkan untuk menangkalnya. Salah satu komponen penting dalam bidang keamanan siber adalah *Endpoint Detection and Response* (EDR).

Endpoint Detection and Response (EDR) adalah solusi keamanan berkelanjutan dan terintegrasi yang menggabungkan pemantauan dan pengumpulan data secara *real-time* dan terus menerus pada *endpoint*. EDR bekerja berdasarkan kebijakan dan aturan yang diterapkan, serta memiliki kemampuan respons dan analisis otomatis.

EDR adalah solusi keamanan siber yang dirancang untuk melindungi perangkat *endpoint*. Solusi ini bekerja dengan cara mendeteksi dan merespon setiap ancaman, berbeda dengan perangkat lunak atau antivirus tradisional yang fokus utamanya hanya pada *signature* virus yang sudah diketahui.



Apa perbedaan EDR dengan Antivirus?

EDR terus memantau aktivitas setiap perangkat atau *endpoint* dengan mengumpulkan data dari setiap *endpoint*, memeriksa data tersebut untuk menganalisis pola dan perilaku anomali secara *real-time*, dan melakukan respons dengan cepat terhadap potensi insiden serangan.

Antivirus berfokus pada pengecekan file yang berpotensi terinfeksi virus. Secara tradisional, antivirus menggunakan database yang terdiri dari *signature* virus yang sudah dikenali sebelumnya.

Berikut adalah perbedaan antara Antivirus Tradisional, *Next-Generation Antivirus* (NGAV), dan hubungannya dengan solusi EDR:

1. **Antivirus Tradisional:**
   - **Pendekatan *Signature-Based***

     Antivirus tradisional menggunakan pendekatan berbasis *signature*. Antivirus tradisional mengidentifikasi ancaman berdasarkan pola atau *signature* yang telah diketahui sebelumnya.
   - **Terbatas pada Ancaman yang Dikenal**

     Antivirus tradisional efektif dalam mendeteksi ancaman yang sudah diketahui, tetapi kurang efektif dalam mendeteksi ancaman baru atau yang belum diketahui.
   - **Fokus pada Pencegahan**

     Antivirus tradisional lebih fokus pada pencegahan dan memiliki keterbatasan dalam mendeteksi ancaman lanjutan.

2. ***Next-Generation Antivirus* (NGAV)**
   - **Pendekatan Berbasis Perilaku dan *Machine Learning***

     NGAV memonitor perilaku dan aktivitas di *endpoint* untuk mendeteksi ancaman berdasarkan pola yang mencurigakan atau perilaku yang tidak biasa. Kemudian, NGAV menganalisis data dan mengidentifikasi pola yang menunjukkan adanya ancaman menggunakan *machine learning*.
   - **Deteksi yang Lebih Canggih**

     NGAV lebih mampu mendeteksi ancaman yang tidak dapat diidentifikasi oleh metode *signature* tradisional.
   - **Fokus pada Deteksi dan Respons**

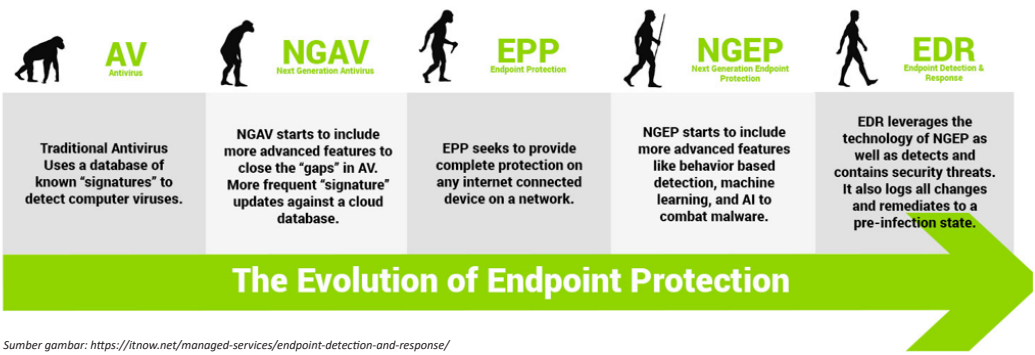
     NGAV tidak hanya fokus pada pencegahan, tetapi juga pada deteksi dan respon cepat terhadap ancaman yang terdeteksi.

Hubungan dengan EDR

NGAV dan EDR sering kali terkait erat. EDR memperluas konsep NGAV dengan menyediakan kemampuan deteksi dan respons yang lebih lanjut dan alat untuk melakukan investigasi forensik dan analisis lebih mendalam pada tingkat *endpoint*.

Banyak solusi EDR juga mencakup fitur-fitur NGAV. Integrasi NGAV dan EDR memberikan visibilitas yang lebih besar dan kemampuan respons yang lebih canggih terhadap ancaman siber

NGAV merupakan evolusi dari antivirus tradisional dengan pendekatan yang lebih mutakhir dalam mendeteksi ancaman. Pendekatan ini berfokus pada perilaku (*behavior-based*) dan bukan hanya pada *signature* virus yang sudah diketahui.



Sumber gambar: https://itnow.net/managed-services/endpoint-detection-and-response/

Solusi keamanan EDR membawa konsep NGAV lebih jauh dengan menyediakan alat dan fungsi yang lebih lengkap. EDR memungkinkan Anda untuk mendeteksi ancaman dengan lebih efektif, merespons ancaman dengan cepat dan tepat, menyelidiki asal-usul dan dampak ancaman di tingkat *endpoint*.

Solusi yang efektif untuk melindungi perangkat Anda dari ancaman siber sering kali mencakup kombinasi dari NGAV dan EDR. Kombinasi ini memberikan perlindungan yang lebih komprehensif, visibilitas yang lebih luas terhadap potensi ancaman, dan kemampuan respons yang lebih cepat.

Implementasi EDR yang efektif melibatkan beberapa komponen utama untuk memastikan perlindungan yang optimal dan respons yang cepat terhadap insiden keamanan. Berikut adalah beberapa komponen kunci dalam implementasi EDR:

1. **Agen EDR**

   Merupakan sebuah perangkat lunak yang diinstal pada setiap *endpoint* yang akan dimonitor dan dilindungi. Berfungsi untuk mengumpulkan data aktivitas *endpoint*, mendeteksi ancaman, dan merespons jika diperlukan.

2. ***Server* Manajemen EDR**

   Berfungsi untuk mengelola dan mengkoordinasikan aktivitas agen di berbagai *endpoint*. *Server* ini juga berfungsi untuk menyimpan dan menganalisis data yang dikumpulkan untuk laporan dan investigasi.

3. **Deteksi Anomali dan Analisis Perilaku**

   Mengidentifikasi pola aktivitas mencurigakan atau tidak biasa di *endpoint*. Fitur ini melibatkan algoritma *machine learning* dan kecerdasan buatan untuk meningkatkan deteksi ancaman.

4. **Manajemen Kejadian dan Respon**

   Integrasi dengan Sistem Security Incidents and Events Management (SIEM) membantu dalam mengelola, menganalisis, dan merespon kejadian keamanan. Dengan begitu, tim keamanan dapat melacak aktivitas, menganalisis log, dan memberikan respon yang cepat terhadap ancaman.

5. **Integrasi *Threat Intelligence***

   Komponen ini mengintegrasikan sumber *Threat Intelligence* eksternal untuk memperbarui basis data ancaman dan memberikan informasi kontekstual tentang ancaman yang baru dan berkembang.

6. **Modul Forensik dan Investigasi**

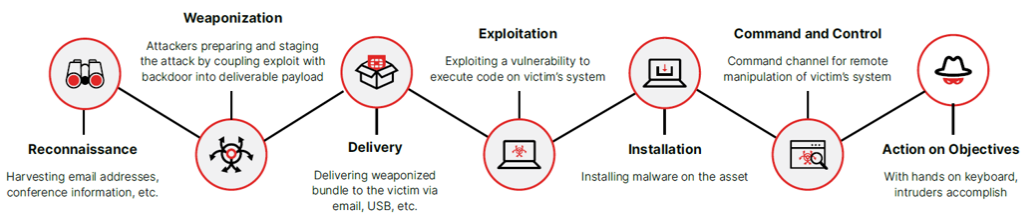
   Modul ini memfasilitasi investigasi forensik untuk memahami sumber dan dampak ancaman. Hal ini mencakup pemantauan aktivitas, analisis file, dan pemulihan pasca insiden.

7. **Fungsi Respon dan Isolasi *Endpoint***

   Fungsi ini memungkinkan tim keamanan untuk memberikan respon cepat terhadap ancaman dengan mengisolasi *endpoint* yang terinfeksi atau menghentikan proses berbahaya.

8. **Antivirus dan Proteksi *Endpoint***

   Meskipun EDR bukanlah pengganti antivirus tradisional, beberapa solusi EDR menyertakan fungsi proteksi *endpoint* tambahan termasuk pencegahan malware dan ancaman *signature* yang dikenal.



Gambar the Cyber Kill Chain® - developed by Lockheed Martin

9. *Dashboard* dan Laporan

Sistem EDR menyediakan user *interface*/ antarmuka pengguna yang intuitif dengan *dashboard* dan laporan yang mudah dimengerti. Hal ini mempermudah tim keamanan untuk memantau aktivitas, menganalisis hasil deteksi, dan melaporkan insiden.

10. Integrasi dengan Perangkat Keamanan Lainnya

Penting untuk memastikan integrasi yang baik dengan perangkat keamanan lainnya di lingkungan IT, seperti *firewall*, perangkat deteksi intrusi, dan solusi keamanan lainnya. Visibilitas jadi lebih komprehensif.

Penting untuk diingat bahwa implementasi EDR lebih dari sekadar memasang perangkat lunak. EDR dapat mengoptimalkan pengaturan yang tepat, mengatur kebijakan keamanan yang baik, serta melatih dan melibatkan tim keamanan untuk memastikan efektivitas deteksi dan respons ancaman siber.

EDR juga dilengkapi dengan fitur *Cyber threat hunting* yang merupakan praktik proaktif (*tactics, techniques, and procedures* - MITRE ATT & CK) dalam mencari dan mengidentifikasi ancaman potensial yang lolos dari deteksi otomatis keamanan siber.

Cyber threat hunting melibatkan pencarian manual dan analisis data untuk menemukan tanda-tanda serangan yang lolos dari deteksi otomatis. Fitur *threat hunting* memungkinkan analis keamanan untuk melakukan penyelidikan aktif dan menganalisis data lebih mendalam. EDR memberikan visibilitas dan alat untuk mendukung praktik *cyber threat hunting*.

Mengatasi Tantangan Keamanan Siber Modern dengan EDR

EDR (*Endpoint Detection and Response*) membantu organisasi mengatasi berbagai tantangan keamanan siber modern, termasuk:

1. Zero-Day Exploits

Zero-day menargetkan atau mengincar celah dan kerentanan yang tidak diketahui oleh vendor perangkat lunak atau komunitas keamanan siber. Analisis dan integrasi intelijen EDR membantu melawan ancaman baru ini.

2. Insider Threats

EDR memitigasi ancaman dari dalam dengan memantau dan menganalisa perilaku setiap pengguna. Anomali atau aktivitas yang tidak biasa dapat diidentifikasi dan diatasi dengan cepat.

***3. Advanced Presistent Therats* (APTs)**

Merupakan jenis serangan siber yang dilakukan secara terus menerus dan sangat terarah. Seringkali tidak terdeteksi oleh metode pengamanan tradisional. EDR dapat mendeteksi dan menggagalkan serangan APTs.

***4. Integration with Security Operations* (SecOps)**

EDR tidak beroperasi secara terpisah. EDR terintegrasi dengan *Secure Operation Center* (SOC) dan *incident Response* (IR). Hal ini merupakan strategi untuk meningkatkan strategi keamanan siber.

5. Collaboration With SOCs

EDR dapat menangkap data terkait aktivitas pengguna atau *endpoint*. EDR juga berkolaborasi dengan SOC untuk menganalisis data dengan efektif. Kolaborasi ini juga mengatasi potensi serangan keamanan secara terkoordinasi.

6. Incident Response Enhancement

EDR memberikan informasi secara detail mengenai sifat insiden keamanan sebagai respon insiden. Dengan begini, pengambilan keputusan dapat difasilitasi dengan lebih cepat dan tepat.

Implementasi *Endpoint Detection and Response* (EDR) di perusahaan dan organisasi merupakan langkah penting dalam membangun pertahanan siber yang kuat. Proses ini melibatkan

beberapa tahapan yang perlu dilakukan secara berkelanjutan, yaitu perencanaan, penerapan, dan pengelolaan. Berikut adalah penjelasan lebih detail mengenai tahapan-tahapan tersebut:

1. **Penilaian dan Perencanaan**
   - **Identifikasi Tujuan dan Kebutuhan**

     Tentukan tujuan implementasi EDR, seperti meningkatkan deteksi dan respons terhadap ancaman, mempercepat investigasi insiden, atau meningkatkan visibilitas keamanan.
   - **Evaluasi Lingkungan IT**

     Analisis lingkungan IT perusahaan, termasuk jumlah *endpoint*, sistem operasi yang digunakan, arsitektur jaringan, dan kebijakan keamanan yang sudah ada.
   - **Pemilihan Vendor EDR**

     Evaluasi solusi EDR dari vendor yang berbeda. Pilihlah solusi yang sesuai dengan kebutuhan dan anggaran perusahaan.
2. **Pengujian dan Pemilihan Perangkat/Alat**
   - **Pengujian *Proof of Concept* (PoC)**

     Lakukan uji coba PoC untuk memastikan bahwa solusi EDR dapat diintegrasikan dengan lingkungan perusahaan dan memenuhi kebutuhan keamanan.
   - **Pemilihan Peralatan Berdasarkan hasil PoC**

     Pilih solusi EDR yang paling sesuai dengan kebutuhan dan kompatibel dengan lingkungan perusahaan.
3. **Perencanaan Arsitektur dan Konfigurasi**
   - **Perencanaan Arsitektur**

     Rencanakan arsitektur implementasi EDR yang meliputi penempatan *server*, konfigurasi agen pada *endpoint*, dan integrasi dengan sistem keamanan yang sudah ada.
   - **Konfigurasi**

     Lakukan konfigurasi awal untuk mengaktifkan deteksi dan respons dasar sesuai dengan kebijakan keamanan perusahaan.
4. **Penerapan dan Pengujian**
   - **Uji Coba Implementasi**

     Terapkan EDR pada sebagian kecil dari *endpoint* untuk memastikan integrasi yang lancar dan menghindari gangguan operasional.
   - **Pengujian Keamanan**

     Lakukan pengujian keamanan menyeluruh untuk memastikan solusi EDR berfungsi optimal dan dapat mendeteksi dan merespons ancaman.
5. **Penggantian dan Penerapan Penuh**
   - **Penggantian Penuh**

     Jika pengujian fase pertama berhasil, terapkan EDR secara menyeluruh pada semua *endpoint* dalam lingkungan perusahaan.
   - **Pemantauan dan Pemeliharaan**

     Lakukan pemantauan dan pemeliharaan rutin untuk memastikan keefektivan EDR dan mendeteksi potensi masalah dengan cepat.
6. **Pelatihan Tim dan Keterlibatan Pengguna**
   - **Pelatihan Tim Keamanan**

     Berikan pelatihan kepada tim keamanan tentang cara menggunakan dan memanfaatkan fitur EDR dengan efektif.
   - **Keterlibatan Pengguna**

     Libatkan pengguna akhir untuk memahami pentingnya keamanan *endpoint* dan memberikan pelatihan tentang cara melaporkan aktivitas mencurigakan.
7. **Integrasi dengan Solusi Lain**

   Pastikan EDR terintegrasi dengan solusi

keamanan lain di perusahaan, seperti SIEM, *firewall*, dan solusi keamanan lainnya, untuk mendapatkan visibilitas yang lebih komprehensif.

8. **Pengelolaan Keamanan dan Pemantauan Berkelanjutan**
   - **Pengelolaan Keamanan**

     Libatkan tim keamanan dalam pengelolaan dan pemeliharaan rutin EDR. Lakukan update perangkat lunak secara berkala dan terapkan perubahan kebijakan keamanan sesuai kebutuhan.
   - **Pemantauan dan Respons**

     Terus pantau aktivitas keamanan menggunakan EDR dan lakukan respons cepat terhadap ancaman yang terdeteksi.
9. **Evaluasi dan Peningkatan**
   - **Evaluasi Rutin**

     Lakukan evaluasi rutin terhadap efektivitas EDR dengan mengukur kinerja, deteksi, dan respons terhadap ancaman.
   - **Peningkatan Berkelanjutan**

     Terus tingkatkan solusi EDR secara berkala sesuai dengan perkembangan terbaru dalam keamanan siber dan tren serangan yang baru.
10. **Keterlibatan dengan Komunitas Keamanan**
    - **Keterlibatan Eksternal**

      Ikuti perkembangan terbaru dalam keamanan siber dan libatkan diri dengan komunitas keamanan untuk tetap mendapatkan wawasan terkini dan berbagi pengalaman praktik terbaik.
    - **Ingat bahwa implementasi EDR bukan sebuah proyek sekali jadi**

      Implementasi ini adalah sebuah proses berkelanjutan yang memerlukan pemantauan dan peningkatan secara konsisten. Hal ini penting untuk memastikan bahwa sistem EDR mampu menghadapi ancaman siber yang terus berkembang.

XDR (*Extended Detection and Response*)

XDR, singkatan dari *Extended Detection and Response*, merupakan sebuah sistem keamanan siber yang menawarkan solusi menyeluruh dan optimal. Berbeda dengan EDR yang fokus pada *endpoint*, XDR mengintegrasikan data dari berbagai sumber, termasuk data, produk, aplikasi *cloud*, email, dan lainnya.

XDR merupakan salah satu inovasi terbaru dalam menangani ancaman kejahatan siber yang dapat mengendalikan berbagai jenis kejahatan siber. Berbeda dengan EDR, XDR tidak hanya fokus pada *endpoint*, tetapi juga mencakup deteksi dan respons terhadap ancaman di berbagai lapisan teknologi keamanan, seperti jaringan (*Network*), *cloud*, dan email. XDR mengintegrasikan data dari berbagai sumber untuk memberikan pemahaman yang lebih luas tentang serangan dan memungkinkan respons yang holistik.

XDR juga memiliki konektivitas *inter-layer* yang memungkinkan Anda melihat bagaimana serangan berkembang di berbagai aspek lingkungan keamanan.

Mengapa Sistem Keamanan XDR Penting?

Menurut data dari McAfee Corp, terdapat peningkatan signifikan dalam serangan siber di berbagai belahan dunia. Serangan ini menargetkan layanan *cloud* dan teknologi kolaborasi yang semakin sering digunakan dengan maraknya sistem kerja jarak jauh (WFH).

Data menunjukkan peningkatan sekitar 63% dalam serangan siber pada layanan *cloud*

dan teknologi kolaborasi. Hal ini sejalan dengan semakin banyaknya perusahaan yang menerapkan WFH, di mana karyawan mengakses data dan aplikasi perusahaan melalui internet.

Meningkatnya serangan siber menunjukkan pentingnya keamanan sistem *cloud* bagi perusahaan. Serangan siber dapat mengakibatkan penyalahgunaan data perusahaan atau data konsumen, yang dapat membawa dampak negatif bagi perusahaan.

Untuk meningkatkan keamanan sistem *cloud* dan teknologi kolaborasi, perusahaan perlu menerapkan sistem keamanan XDR (*Extended Detection and Response*).

Bagaimana XDR bekerja?

Sistem keamanan XDR memiliki tiga kemampuan utama, yaitu:

1. **Analisis dan Deteksi**

   XDR menggunakan rangkaian analitik canggih untuk mendeteksi berbagai jenis serangan siber. Kemampuan analisis dan deteksi XDR meliputi:

   - **Analisis *Traffic* Internal dan Eksternal**

     XDR menganalisis lalu lintas jaringan internal dan eksternal untuk mendeteksi aktivitas mencurigakan yang mungkin mengindikasikan serangan siber.

   - ***Integrated Threat Intelligence***

     XDR memanfaatkan informasi intelijen ancaman terbaru untuk melacak metode, alat, sumber, dan strategi yang digunakan oleh para penyerang siber.

   - ***Machine Learning-Based Detection***

     XDR mengidentifikasi pola serangan siber, sehingga memungkinkan deteksi dini dan pencegahan proaktif.

2. **Investigasi dan Respon**

   Setelah mendeteksi ancaman, XDR membantu Anda untuk mengetahui tingkat keparahan dari ancaman dan meresponsnya sesuai dengan informasi tersebut melalui beberapa fitur di bawah ini:

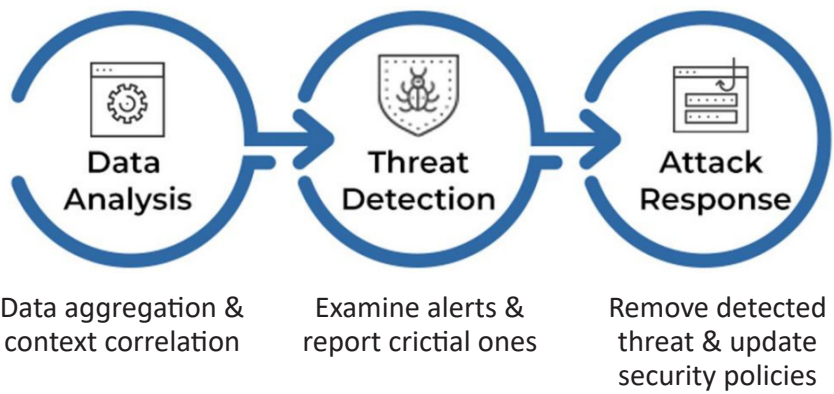
   - ***Correlation of related alerts and data***

     XDR secara otomatis mengumpulkan peringatan dari berbagai sumber dan kemudian membuat *timeline* serangan dari log aktivitas. XDR kemudian memprioritaskan peristiwa serangan dan memprediksi jenis serangan selanjutnya.

   - ***Centralized User Interface (UI)***

     XDR menyediakan konsol untuk menyelidiki dan merespons semua peristiwa serangan sehingga meningkatkan efisiensi dan mempercepat waktu respons.

BAGAIMANA XDR BEKERJA?



- ***Response Orchestration Capabilities***

  XDR memungkinkan Anda untuk mengambil tindakan respons secara langsung melalui antarmuka XDR, menghemat waktu dan sumber daya.

3. Penerapan yang Dinamis dan Fleksibel

XDR dirancang secara dinamis untuk memberikan manfaat berkelanjutan dalam memerangi ancaman siber yang terus berkembang. Berikut adalah beberapa fitur utama yang mendukung kemampuan XDR:

- ***Security Orchestration***

  XDR terintegrasi dengan berbagai kontrol keamanan yang ada sehingga insiden siber dapat direspons secara *real-time*.

- ***Scalable Storage and Compute***

  XDR menggunakan sumber daya *cloud* untuk memenuhi kebutuhan data dan analisis data. XDR juga meningkatkan visibilitas seluruh infrastruktur anda untuk mengidentifikasi dan menginvestigasi ancaman.

- ***Improvement Overtime***

  XDR menggunakan *machine learning* untuk mempertajam kemampuannya dalam mendeteksi dan merespons ancaman siber.

XDR (*Extended Detection and Response*) merupakan pengembangan teknologi dari solusi EDR (*Endpoint Detection and Response*). EDR memang berguna dalam mendeteksi, menganalisis, menginvestigasi, dan merespons ancaman pada *endpoint*. Namun, fokusnya terbatas pada *endpoint* saja.

XDR mampu melakukan semua fungsi EDR pada setiap layer proteksi lainnya, mulai dari email, *network*, *endpoint*, *server*, hingga jaringan *cloud*.

XDR memungkinkan tim SOC (*Security Operations Center*) untuk mengelola semua layer proteksi dalam satu platform, meningkatkan efisiensi dan efektivitas dalam menangani ancaman siber. XDR juga dapat mendeteksi dan merespons ancaman siber secara lebih cepat dan tepat sehingga meminimalkan dampak negatif pada organisasi.

GAYA HIDUP YANG SALAH

KOLOM KETAWA

Beberapa pria sedang berada di ruang ganti gym ketika sebuah telepon seluler di bangku berdering. Seorang pria mengangkatnya dan menyalakan speaker sebelum menjawab. Semua orang di ruangan itu berhenti untuk mendengarkan.

“Halo?”

“Hai papa, ini adek. Papa lagi di gym, ya?” seorang remaja menjawab sambil bertanya.

“Iya, ada apa dek?”

“Aku lagi belanja dan ketemu kemeja dan jas satu set yang bagus banget untuk pesta ulang tahun Mira. Pacarku yang aku kenalin minggu lalu ke papa sama mama, ingatkan, Pa?”

“Tentu saja papa ingat...”

“Harganya cuma 10 jutaan loh, Pa. Boleh nggak aku beli pakai uang papa?”

“Oh, boleh saja kalau kamu suka banget sama jas itu”

“Yessss, makasih papa. Aku juga perlu jam tangan, Pa. Biar nanti di pesta kelihatan macho, Pa”

“Berapa tuh jamnya?”

“Murah kok, Pa, 30 juta aja. Aku suka banget dan warnanya cocok sama jas yang tadi”

“Ya sudah, tapi itu yang branded kan?”

“Oh, iya. Sudah pasti”

“Kamu bayar pakai kartu kredit papa saja”

“Yeeeiii! Papa memang yang terbaik! Satu lagi boleh ga, Pa? Aku mau beliin Mira hadiah spesial nih... Aku tadi minta tolong Santi bantuin cari gaun untuk Mira, harganya 25 juta. Boleh ya, Pah?”

“Boleh, apa sih yang nggak buat kamu? Yang penting kamu happy. Charge saja ke kartu papa ya, oke?”

“Oke, makasih banyak papa! Aku sayang papa, dah!”

“Dahhh, papa juga sayang kamu.”

Pria itu menutup telepon. Laki-laki lain di ruang ganti menatapnya dengan heran, mulut terbuka lebar. Salah satu pria berkomentar “Wah, mas sayang banget ya sama anaknya? Sampai dibolehin belanja sebanyak itu.”

Si pria yang menjawab telepon itu berbalik dan bertanya, “Ada yang tahu ga ini HP siapa?”

&%%$#@^*&%%$#@^*

MANAGED SERVICE: SOLUSI TEPAT UNTUK KEBUTUHAN TI ANDA

Mencakup Hardware, Software, Support, Reporting, Instalasi dan Implementasi

by **Boedijanto**, Branch Manager ACS Group Surabaya

Di era digital ini, perkembangan Teknologi Informasi (TI) semakin pesat. Bisnis pun dituntut untuk lebih fleksibel dan efisien. Hal ini mendorong kebutuhan akan *Managed Service*, khususnya di bidang TI.

Managed Service menawarkan solusi bagi perusahaan yang ingin fokus pada bisnis utamanya tanpa harus terbebani dengan pengelolaan TI.

Pengelolaan TI yang kompleks dapat menghambat fokus perusahaan pada bisnis utamanya. *Managed Service* hadir sebagai solusi yang menawarkan berbagai manfaat, di antaranya:

1. Mengubah belanja modal (*Capex*) menjadi biaya operasional (*Opex*) yang lebih mudah diprediksi. Biaya TI menjadi lebih terkontrol dan stabil.
2. Membebaskan tim TI internal untuk fokus pada pengembangan bisnis dan strategi TI jangka panjang.
3. Mendapatkan akses ke teknologi terbaru dan terkini tanpa perlu investasi besar. Teknologi ini juga akan didukung oleh tim yang memang fokus di solusi TI tersebut.
4. Meringankan beban pemeliharaan sebab vendor *Managed Service* bertanggung jawab penuh atas pemeliharaan dan perawatan infrastruktur TI.
5. Menghilangkan risiko biaya tak terduga untuk perbaikan atau penggantian infrastruktur TI karena biaya sudah di atur secara berkala (*Opex*).
6. Perusahaan dapat berdiskusi dengan vendor *Managed Service* untuk menentukan SLA yang sesuai dengan kebutuhan dan ekspektasi.
7. Layanan dan *supports* dapat ditingkatkan atau dikurangi dengan mudah sesuai dengan pertumbuhan bisnis.
8. *Managed Service* memiliki tim ahli yang berpengalaman untuk memantau dan memelihara infrastruktur TI, sehingga meminimalkan *downtime* dan meningkatkan *uptime* sistem.

ACS Group Vendor Teknologi Informasi Terpercaya

ACS Group adalah perusahaan yang bergerak di bidang Teknologi Informasi (TI) dengan berbagai layanan dan solusi untuk mendukung kebutuhan bisnis Anda. Kami menawarkan solusi *Managed Service* yang profesional dan terpercaya untuk AIDC (*Automatic Identifier Data Collection*), *Wired* dan *Wireless Infrastructure*, *Cyber Security*, juga Security *Access Control System*. Kunjungi website kami di www.acsgroup.co.id.

Ruang Lingkup ACS *Managed Service*

ACS *Managed Service* menawarkan solusi komprehensif untuk kebutuhan TI Anda, dengan beberapa parameter yang menjadi standar kebutuhan di berbagai perusahaan:

a. Fleksibilitas Solusi Produk

Pilih solusi produk yang sesuai dengan kebutuhan Anda, baik sewa saja maupun sewa dengan opsi hak milik. Sesuaikan dengan anggaran dan strategi jangka panjang Anda.

b. Skema Pembiayaan yang Beragam

Pilih pembayaran tahunan atau bulanan dengan minimum kontrak 2 tahun. Anda juga bisa mendiskusikan skema pembiayaan yang paling sesuai untuk kebutuhan Anda dengan kami.

c. Jaringan *Service Center* yang Luas

Dapatkan akses ke *Service Center* yang tersebar di kota-kota besar di Indonesia, yaitu Jakarta, Cikarang, Surabaya, Semarang, dan Bali.

***d. Call Center* 24/7**

Hubungi *Call Center* yang menjadi single contact point untuk semua permasalahan TI Anda. Anda dapat memilih layanan 8x5 atau 24/7 sesuai dengan kebutuhan operasional Anda.

***e. Service Hub* di Seluruh Indonesia**

Dapatkan akses ke *Service Hub* yang tersebar di berbagai daerah di Indonesia, mendekati lokasi operasional Anda.

***f. Back Up Unit* Produk**

Kelancaran operasional Anda akan lebih pasti dengan *Back Up Unit* produk yang kami sediakan.

***g. Pick Up* dan *Delivery* Perangkat**

Hemat waktu dan tenaga dengan layanan *Pick Up* dan *Delivery* untuk perangkat yang rusak.

Support yang Tepat untuk Operasional Anda dengan ACS *Managed Service*

ACS *Managed Service* berkomitmen untuk memberikan dukungan Teknologi Informasi yang optimal bagi kelancaran operasional di perusahaan Anda. Berikut beberapa layanan yang kami tawarkan:

i. Proactive Monitoring

Sistem peringatan proaktif yang akan memberikan rekomendasi kepada pelanggan sebelum terjadi permasalahan.

***ii. Problem Handling* yang Sistematis**

Penanganan masalah akan di proses menggunakan sistem *ticketing* yang terstruktur. Anda mendapatkan informasi dan *log* yang akurat dan mudah dipahami.

iii. Preventive Maintenance

Pemeliharaan berkala akan dilakukan oleh tim engineer yang berpengalaman. Pemeliharan ini minimalkan kerusakan pada perangkat dan meningkatkan usia pakainya.

iv. Patch Management

Patch terbaru akan dipantau dan diterapkan secara berkala.

v. SLA yang Disesuaikan

Service Level Agreement (SLA) yang didiskusikan dan disesuaikan dengan kebutuhan Anda. *Response Time, Resolution Time,* dan *Turn Around Time* dari perbaikan perangkat yang mengalami kerusakan dapat dimodifikasi dalam SLA.

vi. Report dan Rekomendasi

Kami akan melaporan kegiatan *Managed Service* setiap bulan/kuartal yang berisi detail *support* yang telah dilakukan. Kami juga akan mengajukan rekomendasi untuk meningkatkan kelancaran operasional perusahaan.

Exploring Edge to Cloud: Mendalami Transformasi IT bersama HPE di PROFIT Bali 2024

Professional IT Bali tahunan mengangkat topik "Techno Break" yang diadakan pada Sabtu, 24 Februari 2024, di HARRIS Hotel & Residences Sunset Road - Bali. ACS Group berkolaborasi dengan Hewlett Packard Enterprise (HPE) dengan dukungan dari Sistech Kharisma untuk memperkenalkan solusi server terbaru dalam acara tersebut. Kolaborasi ini memberikan nilai tambah yang signifikan pada diskusi dan memperkaya pengetahuan para peserta mengenai teknologi server.

Nuki Nugroho selaku Distributor Business Manager membahas tentang "Unlock Your Data's Potential with Edge to Cloud" yang di dalamnya menekankan 3 poin penting HPE Proliant, yaitu: *Intuitive* (*Simple, Unified, Automated*), *Trusted* (*Fundamental, Uncompromising, Protected*), dan *Optimized*.

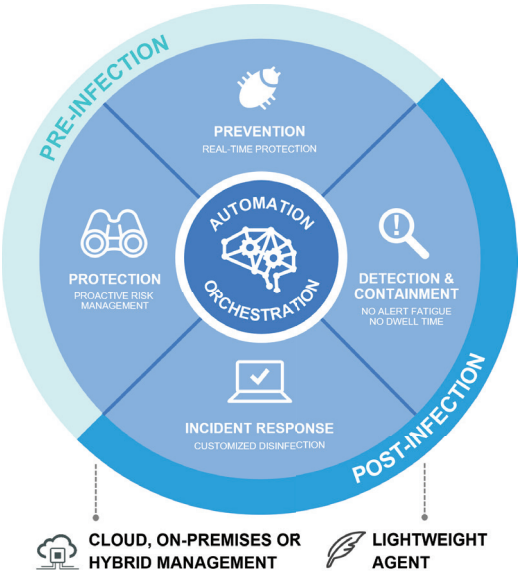
Acara tersebut memberikan platform bagi para profesional IT di Bali untuk berbagi pengetahuan, pengalaman, dan wawasan terbaru dalam industri teknologi informasi. Kesempatan ini juga memungkinkan terbentuknya kolaborasi yang saling menguntungkan antara para pemangku kepentingan di bidang teknologi informasi di Bali dan sekitarnya, yang pada akhirnya memperkaya pemahaman akan perkembangan terkini dalam industri tersebut.

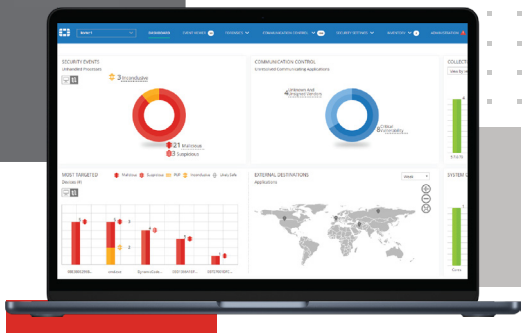
FORTINET

FortiEDR™

Real Time Endpoint Protection, Detection, and Automated Response

Industri : Semua Industri





FortiEDR adalah solusi keamanan *endpoint* yang mendeteksi ancaman tingkat lanjut serta menghentikan *data breaching* dan *ransomware* secara ***real-time***. Solusi ini dapat mengurangi *surface attack* melalui *vulnerability assessments* dan *risk mitigation policies.* FortiEDR memberikan lapisan pertahanan pertama dengan *next-generation antivirus* (NGAV) *engine* berbasis *machine-learning.* Solusi ini juga dapat melindungi *endpoint* dari *data-breach* atau *data-loss*, mengeliminasi *dwell-time,* dan menghadirkan solusi perlindungan *endpoint detection and response* (EDR) dengan fitur otomasi untuk mendeteksi, meredakan, menyelidiki, merespons, dan memulihkan insiden.

POINT MOBILE

PM451 Handheld Terminal

Industri : Manufaktur, WMS, Logistik & Transportasi.

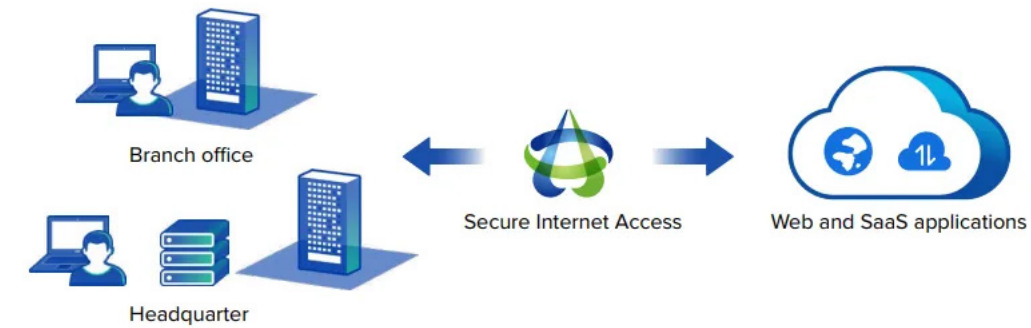
PM451 adalah penerus kesuksesan Point Mobile PM450. *Operation system* perangkat ini adalah Android 11 terkini yang dapat di-*upgrade* sampai dengan Android 14. PM451 dapat terkoneksi dengan WiFi terbaru serta dilengkapi prosesor Octa-core 2.2GHz dengan RAM 4GB dan ROM 64GB. Produk ini juga memiliki rating IP65 sehingga tahan terhadap debu dan cipratan air. Perangkat ini dilengkapi dengan *scanner* yang mampu membaca semua simbologi GS1 bahkan barcode label yang tercetak dengan buruk dengan pilihan versi *imager* yang mampu membaca jarak jauh hingga 29 meter. PM451 memiliki 3 opsi pilihan *keypad* serta pegangan (*gun*) yang menjadikan PM451 ini pilihan sempurna untuk operasional gudang Anda. Kami siap membantu Anda untuk mendapatkan penjelasan lebih lanjut.

SANGFOR

Sangfor IAG – Internet Access Gateway & Solusi Web Filtering

Industri : Semua Industri

Sangfor IAG adalah solusi keamanan *gateway internet* yang membantu organisasi melindungi produktivitas pengguna dan kepatuhan terhadap kebijakan internet. Sangfor IAG bekerja sama dengan *Endpoint Secure* dalam mencegah pengguna yang menggunakan aplikasi *proxy avoidance* untuk melewati batas keamanan. Solusi ini juga dapat menyesuaikan kebijakan kontrol lalu lintas jaringan secara dinamis dan mengelola *bandwidth* untuk setiap pengguna. Sangfor IAG menawarkan dekripsi *gateway* dan dekripsi klien dalam meningkatkan fleksibilitas organisasi untuk menjalankan salah satu atau keduanya secara paralel sesuai dengan kebijakan perusahaan.



ZEBRA

FXR90 Ultra-Rugged Fixed RFID Readers

Industri : Manufaktur, Pergudangan, Logistik & Transportasi.

Dengan Kecepatan baca yang kuat pesat 1.300+ tag per detik, maksimalkan kemampuan pelacakan aset di lingkungan yang menantang dengan Zebra FXR90 Ultra-Rugged Fixed RFID Reader. Produk yang dirancang dengan penyegelan IP65/67 kelas industri dan rentang suhu pengoperasian yang luas, alat ini dapat diandalkan di lingkungan industri maupun luar ruangan. Dilengkapi dengan Wi-Fi 6, Bluetooth®, dan antena RFID internal opsional, FXR90 juga mudah digunakan serta dikelola di jaringan mana pun. Anda akan mendapatkan konektivitas dan visibilitas yang tak tertandingi dengan 5G, GPS, dan seluler pribadi (opsional).

POINT MOBILE

PM84 Mobile Computers

Industri : Layanan Lapangan, Transportasi & Logistik, Manajemen Gudang, Ritel, dan Perhotelan.

Dilengkapi prosesor Octa-Core @ 2.0 GHz, RAM 4 GB, dan ROM 64 GB, PM84 menangani berbagai aplikasi dengan lancar. Baterai 4.950 mAh (opsi 7.020 mAh) yang mudah diganti, menunjang operasional seharian.

Kamera belakang 13 MP (Auto Focus) menghasilkan gambar tajam dan jelas untuk dokumentasi di lapangan. Kamera depan 5 MP mendukung panggilan video untuk komunikasi real-time yang efektif.

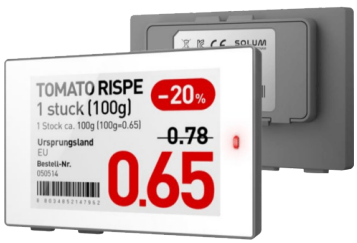
PM84 memiliki daya tahan luar biasa dengan rating IP65 (opsi IP67) yang tahan air dan debu. Dilengkapi karet pengaman, PM84 mampu menahan benturan dari ketinggian 1,8 m (6 kaki) dan 1,5 m (5 kaki) tanpa karet pengaman. PM84 juga mampu beroperasi pada suhu ekstrem antara -20 °C dan 60 °C (-4 °F ~ 140 °F).

*** Produk ini sedang dalam pengurusan Type Approval (Postel)*

SOLUM

Electronic Shelf Labels (ESL) SOLUM

Industri : Ritel & Pergudangan.



ESL (*Electronic Shelf Label*) atau sistem label rak elektronik digunakan oleh toko untuk menampilkan harga, barcode, produk, serta promo yang diletakan biasanya diletakkan di depan atau tepi rak ritel. Label ini dapat diperbarui atau diubah secara otomatis di bawah kendali *server* terpusat. Selain pada ritel, label elektronik ini juga cocok untuk di aplikasikan di manufaktur untuk identitas rak yang dinamis.

ESL menggunakan kertas elektronik (*E-paper*) atau layar kristal cair (LCD) untuk menunjukkan informasi yang dapat disesuaikan. *E-paper* banyak digunakan pada industri ritel atau manufaktur karena memberikan tampilan yang tajam dan mendukung pencitraan grafis yang baik karena hanya memerlukan daya selama pembaruan. Baterai yang digunakan dapat bertahan selama 10 tahun. Jaringan komunikasi lewat nirkabel dari server pusat memungkinkan tampilan yang ada di ESL diperbarui secara otomatis setiap kali ingin dirubah, berbeda dengan label kertas yang sekali pakai dibuang.

ESL memiliki fitur:

- Memiliki 7 warna.
- Efisiensi energi lebih tinggi. *Lifecycle* baterai dapat bertahan hingga 10 tahun.
- Kecepatan *update* 45,000 ESL per *gateway*.
- Resolusi hingga 144 dpi.
- Tampilan dan bezel yang lebih dinamis.
- Rating IP67. Dapat digunakan dalam *freezer*.

Untuk penjelasan lebih detail lagi, Anda dapat menghubungi fitur chat kami di www.acsgroup.co.id.

Scan this QRcode

ACS GROUP
PT. AUTOJAYA IDETECH
PT. SOLUSI PERIFERAL
www.acsgroup.co.id

• ACS Group mengucapkan •

Selamat Hari Raya

Nyepi

11 Maret 2024

Selamat Merayakan

Hari Jum'at Agung & Minggu Paskah

29 & 31 Maret 2024

Selamat Hari Raya

Idul Fitri

10 & 11 April 2024

Minal 'Aidin wal-Faizin

Mohon Maaf Lahir & Bathin

WAVE PTX: RADIO PTT BROADBAND TANGGUH DARI MOTOROLA

Motorola Solutions adalah pemimpin global dalam peralatan penunjang keamanan dan keselamatan bagi publik dan perusahaan. Motorola Solutions dikenal di Indonesia sebagai penyedia teknologi nirkabel berkualitas tinggi, termasuk smartphone dan PTT (Handy-Talkie).

Pada 2018, Motorola Solutions meluncurkan Wave PTX, sebuah inovasi terbaru dalam komunikasi PTT yang menggunakan jaringan broadband (internet) sebagai sumbernya. Hadir di Indonesia pada 2023 lalu, solusi ini siap menunjang kegiatan operasional di ruang-ruang publik, manufaktur, hingga berbagai industri lainnya.

Solusi Wave PTX dari Motorola Solutions terdiri dari tiga komponen utama, yaitu:

Motorola TLK with Wave PTX

Motorola TLK adalah radio yang dirancang untuk berkomunikasi melalui jaringan *broadband* (GSM 4G / Wi-Fi). Perangkat ini tangguh di segala kondisi dengan desain sederhana bersertifikat IP54 dan MIL-STD. Wave PTX pada setiap perangkat memungkinkan komunikasi tanpa batas, kapanpun dan dimanapun Anda berada.

Wave PTX for Mobile Apps

Wave PTX dapat diunduh dan diinstal langsung pada *smartphone* Android maupun iOS. Tidak hanya fungsi PTT, aplikasi ini juga dapat mengirim pesan dan membagikan file multimedia lainnya.

Wave PTX Dispatch

Wave PTX Dispatch adalah aplikasi web yang memungkinkan Anda mengontrol dan mengelola tim Anda dengan mudah, di mana pun mereka berada. Dapatkan kemudahan tambahan melalui Wave PTX Dispatch, seperti:

- Pemantauan posisi via GPS.
- Berkirim pesan dan data multimedia.
- Perekaman suara percakapan.
- Fitur-fitur menarik lainnya.

Hubungi ACS Group di *official* WhatsApp kami 081-1194-4534 (*chat only*) untuk mendapatkan penjelasan lebih detail tentang produk yang kami tawarkan.

Dari Manual ke Digital: ACS Group Optimalkan Manajemen Toko dengan Label Elektronik dari SOLUM

Pada tanggal 18 Januari 2024, ACS Group mengikuti pelatihan online mengenai Label Elektronik (*Electronic Shelf Label* atau ESL) yang diselenggarakan oleh SOLUM dan dibawakan oleh Mr. Rakesh Sakamuri. Pelatihan ini fokus pada cara-cara berikut:

- Menginstalasi *Software* AISM/*Dashboard* pada laptop.
- Menginstalasi dan mengkonfigurasi *Gateway Launcher*.
- Merancang label menggunakan *Software Layout Designer*.
- Melakukan *Deploy Label* yang sudah dirancang ke Label ESL.

Berikut adalah beberapa label elektronik yang dirancang saat pelatihan dan setelah pelatihan:

Meningkatkan Keamanan dan Efisiensi Jaringan dengan HPE Aruba Networking

Tim sales dan pre-sales ACS Group mengikuti *product update* dari HPE Aruba Network pada 19 Februari 2024. Acara ini bertujuan untuk mempelajari solusi jaringan inovatif terbaru dari HPE Aruba Network.

Salah satu fokus utama workshop ini adalah HPE Aruba Networking Edge Services Platform (ESP). Tim ACS Group mempelajari bagaimana ESP menjaga keamanan konektivitas dari *edge* hingga *cloud* dengan memanfaatkan keamanan Zero Trust dan SASE.

Workshop ini juga membahas Secure Access Service Edge (SASE), arsitektur yang menggabungkan kemampuan WAN komprehensif (SD-WAN, routing, optimalisasi WAN) dengan layanan keamanan berbasis cloud (SWG, CASB, ZTNA). Tim ACS Group mendapatkan pemahaman yang lebih baik tentang bagaimana SASE dapat

membantu meningkatkan keamanan dan kinerja jaringan.

Terakhir, tim ACS Group mempelajari solusi Aruba Instant On, solusi *deployment* dan manajemen Wi-Fi yang mudah digunakan. Solusi ini menyediakan koneksi Wi-Fi yang aman, andal, stabil, dan cepat.

Bergerak Maju dengan Semangat 'Teamwork Makes the Dream Work': Kisah Inspiratif ACS Group di Tahun 2024

Semangat "Teamwork Makes the Dream Work" menjadi pendorong bagi ACS Group pada tahun 2024. Menurut Indra Tjahjadi, Managing Director ACS Group, *tagline* ini mencerminkan pentingnya figur yang memiliki mindset proaktif dan siap menghadapi perubahan. Pemikiran ini mendorong kolaborasi, ketegasan, keberanian menghadapi tantangan, dan kegembiraan dalam menghadapi ketidakpastian. Semua nilai ini menekankan pentingnya kerja sama yang cerdas dan produktif.

Rapat kerja ACS Group di Taman Bukit Palem Resort, Bogor, pada 29 Februari - 2 Maret 2024, tidak hanya bertujuan untuk mengevaluasi kinerja tahun sebelumnya, tetapi juga untuk merencanakan strategi dan program tahun berjalan. Seluruh cabang ACS Group, termasuk Jakarta, Cikarang, Semarang, Surabaya, dan Denpasar, turut serta dalam acara ini.

Selamat kepada Iwan - Senior Account Executive (kiri), Ihdi Arwan - Engineer Supervisor ACS Group Semarang (tengah) dan Julian Antono - Service Center Engineer ACS Group (kanan) atas prestasi sebagai *Best Performers* tahun 2023. Dedikasi mereka diharapkan dapat terus menginspirasi dan memberikan kontribusi positif bagi ACS Group di masa depan. Semoga semangat dan kesuksesan senantiasa mengiringi ACS Group dalam perjalanan ke depan.

• BEST PERFORMERS 2023 •

ACS GROUP
PT. AUTOJAYA IDETECH
PT. SOLUSI PERIFERAL
www.acsgroup.co.id

SERTIFIKASI MENANDAKAN KOMPETENSI KAMI DALAM MENANGANI TUGAS BERKUALITAS TINGGI UNTUK ANDA SEBAGAI PELANGGAN TERHORMAT KAMI

and many more...

TIPS UNTUK MENJAGA KEAMANAN KATA SANDI

by **Irvan Kurniawan Jong, PMP**, Enterprise IT Solutions General Manager ACS Group

Menjaga keamanan kata sandi (*password*) sangat penting untuk melindungi akun dan data pribadi Anda. Berikut adalah beberapa tips untuk membantu Anda menjaga keamanan kata sandi:

1. **Gunakan kata sandi yang kuat**
   - Buat kata sandi yang panjang, minimal 12 karakter.
   - Gunakan kombinasi huruf besar, huruf kecil, angka, dan simbol.
   - Hindari menggunakan kata-kata yang mudah ditebak atau informasi pribadi seperti nama atau tanggal lahir.
2. **Jangan menggunakan kata sandi yang sama**
   - Gunakan kata sandi yang berbeda untuk setiap akun yang Anda miliki.
   - Jika salah satu akun diretas, akun lainnya tetap aman.
3. **Perbarui kata sandi secara berkala**
   - Ganti kata sandi secara berkala, minimal setiap enam bulan sekali.
   - Jangan menggunakan kata sandi yang sama untuk waktu yang lama.
4. **Gunakan autentikasi dua faktor (2FA)**
   - Aktifkan autentikasi dua faktor jika tersedia.
   - Ini memberikan lapisan tambahan keamanan dengan meminta verifikasi melalui perangkat lain seperti ponsel.

5. **Hati-hati dengan phishing**
   - Hindari mengklik tautan atau membuka lampiran dari email yang mencurigakan.
   - Pastikan situs web yang Anda kunjungi aman sebelum memasukkan kata sandi.
6. **Gunakan aplikasi *Password Manager***
   - Pertimbangkan untuk menggunakan aplikasi *Password Manager* untuk menghasilkan dan menyimpan kata sandi secara aman.
   - Aplikasi *Password Manager* dapat membuat kata sandi unik dan kompleks untuk setiap akun.
7. **Jangan simpan kata sandi pada perangkat umum**
   - Hindari menyimpan kata sandi pada perangkat umum atau menggunakan komputer bersama.
   - Jika Anda harus menyimpannya, pastikan perangkat tersebut terlindungi dengan kata sandi atau PIN.
8. **Waspadai *Keylogger***
   - *Install* dan perbarui perangkat lunak keamanan untuk melindungi diri dari *keylogger* yang dapat mencatat ketikan Anda.
9. **Selalu *logout***
   - Selalu keluar dari akun Anda setelah selesai menggunakan perangkat, terutama pada perangkat bersama atau umum.

Dengan mengikuti tips ini, Anda dapat meningkatkan keamanan kata sandi Anda dan melindungi akun-akun online Anda dari ancaman keamanan.

ACS GROUP PT. AUTOJAYA IDETECH PT. SOLUSI PERIFERAL

CORE BUSINESS SOLUTIONS: 4 PILLARS

1 Automatic Identification & Data Capture (AIDC)
IT peripherals such as: Barcode/RFID printers, Barcode/RFID readers or scanners, enterprise mobile printers, enterprise mobile computer (handheld, vehicle mount, tablet, wearable).

2 IT Infrastructure & Cyber Security
Network Devices (Access Point, Controller, Wired/Wireless), Hyper Converge Data Center, Public & Private Cloud, Cyber Security (Next-Gen Firewall, Network Access Control, Endpoint protection, OT).

3 Enterprise Security System
Access Control (+Turnstile, Barrier Gate), Surveillance (Enterprise IP Cam), Alarm system, Unified Command & Control Center.

4 Enterprise Business Solution
Software Package, Managed and Professional Services.

Alibaba Cloud · Allied Telesis · BarTender · brother at your side · eG Innovations · Extreme · FORTINET · HID · Hewlett Packard Enterprise · HIKROBOT · HIKVISION · HPE aruba networking · HUAWEI · Hytera · ivanti · JANZ · OPT Machine Vision · POINT Mobile · SAMSUNG · Seuic · tp-link · ZEBRA · ZKTeco Indonesia

Jakarta (Head Office)
Perkantoran Gunung Sahari Permai #C03-05
Jl. Gunung Sahari Raya No 60-63 Jakarta 10610
Telp : +6221 - 4208221, 4205187
Email : sales.admin@acsgroup.co.id

Jakarta (Service Center)
Perkantoran Gunung Sahari Permai Blok E No. 3
Jl. Gunung Sahari No. 60 - 63, Kemayoran, Kota Administrasi Jakarta Pusat, DKI Jakarta - 10610
Telp : +6221 - 4208221, 4205187

Cikarang
Cikarang Square Blok E No 62, Jl. Raya Cikarang, Cibarusah Km 40, Cikarang Barat, Bekasi
Telp : +6221 - 29612366, 29612367
Email : adminckg@acsgroup.co.id

Semarang
Grand Ngaliyan Square Blok B No.18, Ngaliyan 50181, Semarang
Telp : +6224 - 76638092, 76638093
Email : adminsmg@acsgroup.co.id

Surabaya
Komplek Ruko Gateway Blok D-27
Jl. Raya Waru, Sidoarjo 61254
Telp : +6231 - 8556277, 8556278
Email : adminsby@acsgroup.co.id

Denpasar
Ruko Grand Sudirman Agung Blok B No.29,
Jl. PB Sudirman, Dauh Puri Kelod,
Denpasar Barat, Denpasar - Bali 80114
Telp : +62361 - 4457859
Email : admindps@acsgroup.co.id