GEBYAR

BULETIN EDISI 62/MARET 2023

AUTO-ID

UNTUK KALANGAN SENDIRI

THE EMERGENCE OF OPERATIONAL TECHNOLOGY SECURITY

ACSCare

Tips & Info:
PING dari Source Address tertentu pada perangkat NGFW FortiGate

[-] E-Buletin

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

EDITORIAL

Para insan IT dan OT yang kami banggakan,

Edisi kali ini akan membahas keamanan di sektor *Operational Technology* (OT), alias konsekuensi resiko yang kita hadapi dengan kapabilitas otomatisasi kontrol dari mesin-mesin di pabrik.

Why bother? Dengan keterbukaan informasi dan kemungkinan akses secara jarak jauh yang semakin tersedia oleh perkembangan teknologi, *attack surface* semakin melebar jika tidak diamankan secara serius. Dalam pembahasan ini kita akan menguak kesulitan awal yang kemudian melandasi keharusan identifikasi aset dan juga kerjasama yang mutlak diperlukan antara dua pihak yang pada esensinya berbeda prinsip kerja.

Solusi principal kami mengkategorikan sertifikasi teknis OT pada layar tertinggi. Hal ini mengindikasikan kerumitan yang memerlukan ketelitian dan investasi yang tidak sedikit.

So how is it worth it, to invest not only considerable time, but also potentially substantial funds to secure machines that we bought (might have been) a decade ago? Jawabannya karena OT berhubungan secara langsung dengan kelangsungan bisnis. Kehilangan data dapat dimitigasi dengan DRC (*Disaster Recovery Center*) yang mumpuni, meski begitu berhentinya produksi adalah sesuatu yang kritis, bahkan fatal, terhadap keberlangsungan perusahaan dan semua insan yang bekerja di dalamnya.

Selain OT, kami juga akan membahas kerangka *Managed Service* yang disusun berdasarkan spesialisasi kami yang telah dibangun selama ini, beserta tentunya *latest product update*, serta berbagai infomasi lainnya seperti *corporate Info*, *Product Highlight*, Tips & Info dan lain-lain. *Enjoy the read.*

Salam Hangat,

Ken Looho
Professional Services, NSE3
PT. Autojaya Idetech | PT. Solusi Periferal

PEMIMPIN REDAKSI
Andre S.Kouanak

SEKRETARIS REDAKSI
Listya Kartikasari (Jakarta)
Indah Widiyanti (Cikarang)
Luh Wayan Sumariani (Denpasar)
Herdina Septiyaningrum (Semarang)
Sari Wilujeng (Surabaya)

EDITOR
Nuning Kustiawita
Chandra Sari

DESAINER
Oscar Budi Trianto

KONTRIBUTOR (PENULIS)
Ken Looho
Ihdi Arwan
Irvan Kurniawan

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

2 Editorial - **Ken Looho**
3 The Emergence of Operational Technology Security
16 News & Event
20 ACSCare
22 Product Highlight
26 Corporate & Principal Info
30 Tips & Info PING dari Source Address tertentu pada perangkat NGFW FortiGate

THE EMERGENCE OF OPERATIONAL TECHNOLOGY SECURITY

by **Ken Looho** & **Ihdi Arwan**, Professional Services ACS Group

TECHNOLOGY PARADOX

Kemudahan koneksi antarmuka dan antar lokasi yang semakin hari semakin seakan tanpa batas dan semakin "*seamless*" tidak dapat kita terima begitu saja. Seiring dengan kemudahan ini, terdapat potensi penyusupan yang juga paralel semakin besar dengan lebarnya celah *attack surface*.

Teknologi saat ini mengharuskan kita tidak hanya meningkatkan fokus tersendiri pada *cyber security*, tapi juga memperdalam wawasan agar *bad actors* tidak memanfaatkan kerentanan jaringan yang mungkin ada.

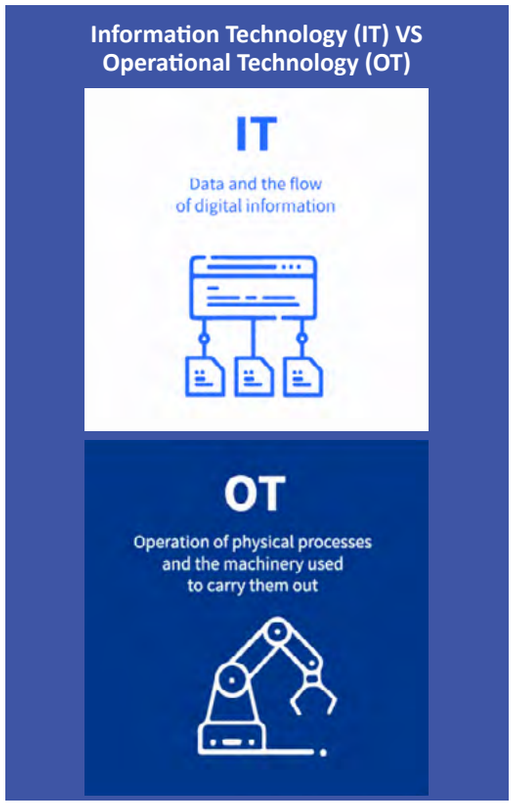
Terbukanya tirai *Operational Technology* (OT) dalam ketersediaannya koneksi ini menimbulkan problema yang tidak mudah dimitigasi, karena berbagai perbedaan yang signifikan dengan sistem IT pada umumnya. Perlakuan khusus perlu ditindaklanjuti dengan kerjasama yang baik antara pihak IT dengan pihak OT.

STATE OF THE WORLD

Sebelum isu keamanan OT muncul, terdapat pemisahan/gap yang cukup besar antara pihak IT dan pihak OT soal pengembangan teknologi. Kedua pihak biasanya bekerja secara terpisah. Salah satu penyebab hal ini terjadi adalah ketentuan untuk *update software/firmware*.

Pada dunia IT, sudahlah sebuah kelaziman dan *best practice* untuk melakukan *update/patching* dari *system*. Hal ini mutlak diperlukan dengan cepat berkembangnya ancaman-ancaman siber yang terus berevolusi, sehingga kita memerlukan system versi terkini yang dapat melakukan mitigasi. Jika terjadi hal yang tidak diinginkan, terdapat resiko data hilang ketika proses *update* tidak sempurna.

Pendekatan tersebut bertolak belakang dengan OT, dimana tradisionalnya *system* OT akan memilih untuk tidak pernah melalui siklus *update*, karena resiko *downtime* yang tidak sepadan dengan kehilangan kemampuan produksi yang merupakan KPI utama dari pihak OT. Resiko yang diemban ketika *update* terjadi tidaklah hanya data, tapi jauh lebih kritis, yaitu *patching* yang tidak *compatible* sehingga menyebabkan *downtime*.



VS

Operational Technology	Information Technology
Does Things *Controls Things* *Monitors Things*	*Protects Data* *Stores Data* *Manupulates Data*
PERFORMANCE PRIORITIES	
Low Bandwidth Real-Time	High Bandwidth Delay Tolerant
AVAILABILITY	
Outages: not acceptable Redundancy Required	Rebooting: bad but doable Retriavable Back-up Acceptable
RISK	
Human Safety Property Safety	Data Integrity Data Security
OPERATORS	
Control Engineers with content skills Network Design by Process Engineers	IT Staff with systems skills Dedicated Networks Designers
CONSTRAINTS	
More Specific Hardware Security not Primary Specialized Communications Protocols	Flexible Hardware Easy Security updates Industry Standard - TCP/IP
MAINTENANCE	
Single Vendor Support 10 to 15 year Component Life Remote Components, Hidden Access Updates Carefully Planned and Tested No Full-Time Dedicated IT Staff	Multiple Support Sources 3 to 5 year Component Life Modular, Accessible Components Frequent Patches and Updates IT Staff or Service Contract in place
SECURITY PRIORITY	
Availability, Integrity, Confidentiality	Confidentialitym Integrity Availability

IT VS OT

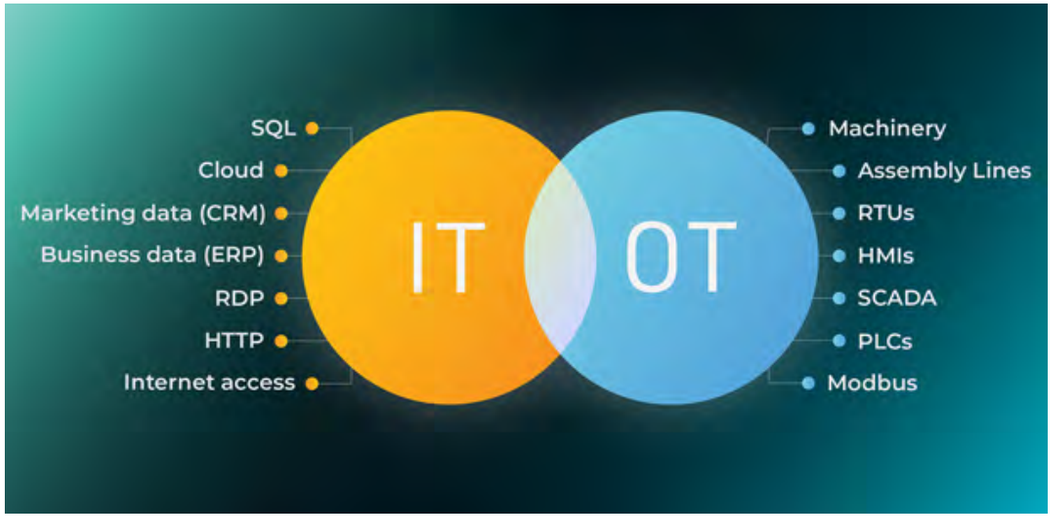
Kondisi ini tidak jarang menimbulkan perselisihan antara pihak IT dan pihak OT, yang pada puncaknya dapat mengakibatkan pihak IT seringkali tidak mengurusi keamanan system OT sama sekali.

Tentunya dengan tren transformasi perusahaan yang berlomba-lomba mengarah ke digitalisasi *industry* 4.0 hal ini tidaklah mungkin dibiarkan. Kemudahan akses secara *remote* dari jarak jauh dengan koneksi yang tersedia adalah salah satu alasan pentingnya keamanan di sisi OT bekerjasama dengan pihak IT.

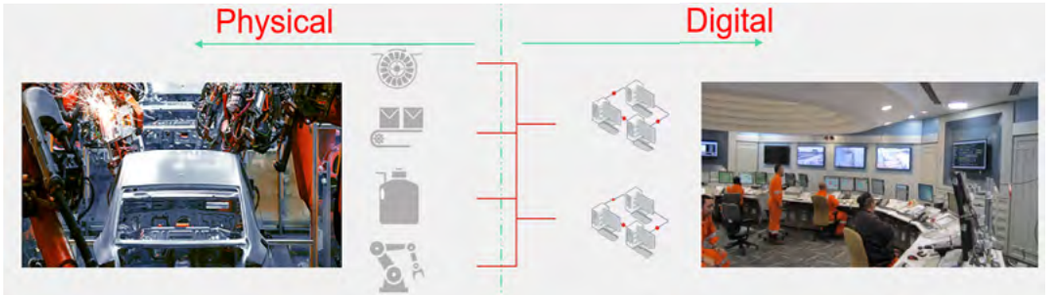
Pemerintah Indonesia dengan INDI 4.0 bermaksud untuk memberikan gambaran global dan suatu arahan yang pada dasarnya logis untuk diikuti. Keamanan siber menjadi salah satu *highlight* dan jika arahan ini bergerak menjadi regulasi nantinya, pentinglah suatu konvergensi keamanan bisa diciptakan antara IT dan OT.

Sebelum kita membahas keamanan OT lebih dalam, perlu ada penyelarasan pemahaman tentang apa itu OT sendiri?

Gambar 1. INDI 4.0 Sebagai Arahan Kepatuhan Pengembangan Teknologi



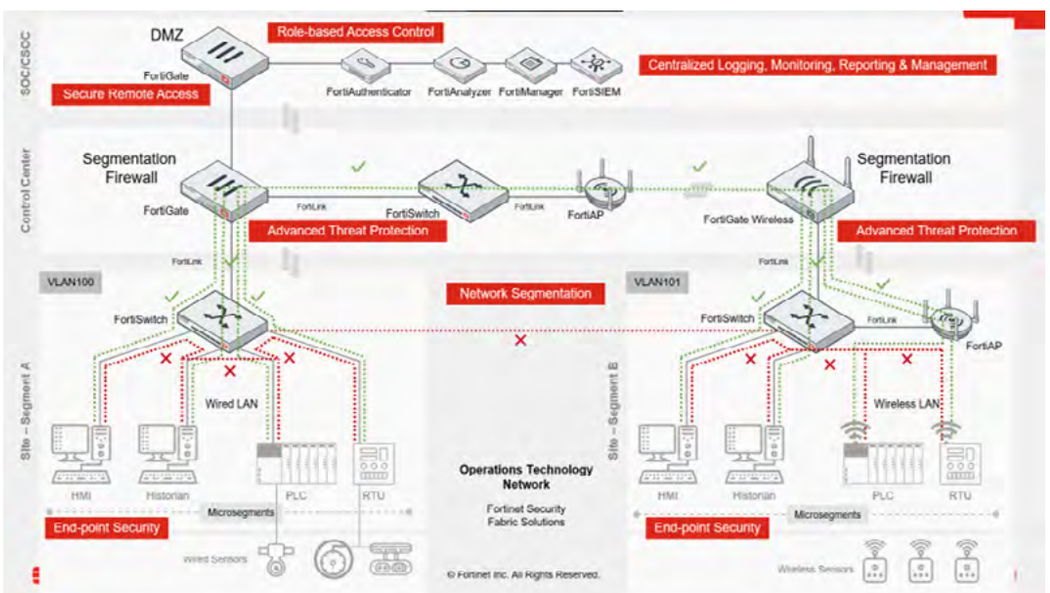
Gambar 2. IT & OT, Simplified



Gambar 3. Digitalisasi Operational Technology

OPERATIONAL TECHNOLOGY IN A GLANCE

Secara umum, OT adalah praktik penggunaan perangkat keras (*hardware*) dan perangkat lunak (*software*) yang secara eksklusif melakukan pemantauan, memproses, dan juga mengontrol industrial *equipment* secara fisik. OT menggunakan *hardware* dan *software* secara eksklusif untuk menampilkan dan mengatur *industrial equipment*, atau lebih sederhananya: mesin-mesin dalam suatu pabrik. Terdapat berbagai fasilitas yang memudahkan interaksi manusia dengan mesin produksi, seperti: system HMI (*Human Machine Interface*), SCADA (*Supervisory Control and Data Acquisition*), *Programmable Logic Controllers* (PLC), *Distributed Control Systems* (DCS) yang semuanya ini masuk dalam kategori bernama ICS (*Industrial Control System*).



Gambar 4. Digitalisasi Keamanan Best Practice Untuk OT

Berbagai perangkat ICS ini sangat memudahkan operator mesin, karena selain menampilkan informasi soal status mesin, juga dapat melakukan kontrol langsung untuk penyesuaian kinerja.

Analogi sederhananya: Anda tinggal menekan tombol di layar komputer pada suatu lokasi terpusat, dibanding memutar sekrup secara manual di lokasi mesin berada.

CIRI KHAS OT & TANTANGANNYA

Challenges of securing OT

The difficulties in security OT systems include:

Rising ransomware attacks
Ransomware accounted for **33%** of attacks against OT in 2020[1]

Exploding ICS vulnerabilities
ICS related attacks in 2020 were up **49%** from the prior year[1]

Insider threats
Insider incidents made up **13%** of all OT-related incidents in 2020, with **60%** involving malicious insiders[1]

Out-of-date tools
OT environments rely on legacy devices and servers that are harder to update and protect

Expanding surface of attack
Introducing **5G** to factory floors expands the attack surface. Organizations are allowing other technologies to connect to their networks, which adds a new potential attack vector and source of malware.

Lack of security expertise
Companies do not have the cybersecurity talent or skills to defend their organizations.

Source:

1: IBM Security 2021. "X-Force Threat Intelligence Index 2021."

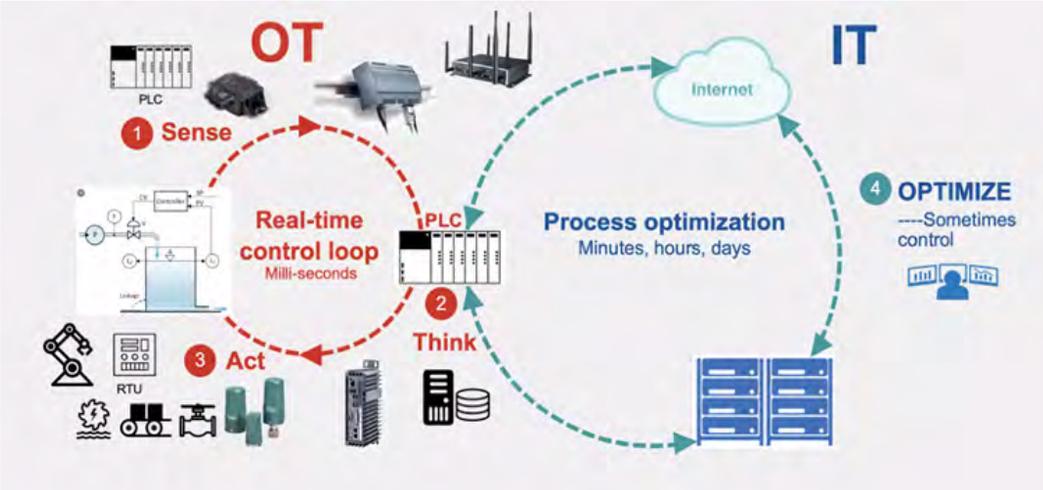
LALU DIMANA LETAK KESULITAN UNTUK KEAMANANNYA?

1. Secure Access & Remote Session

Kembali ke kisah tradisional dimana OT dulunya tidak diakses secara *remote*. Jika perangkat pabrik memerlukan pemeliharaan, teknisi dari pemilik *brand* tersebut (contoh: ABB, Schneider, Siemens, Yokogawa, Rockwell, Emerson) akan datang langsung ke pabrik tersebut, diawasi oleh PIC pabrik, melakukan perawatan yang diperlukan ke suatu mesin spesifik.

Di era ini, teknisi ini bisa berasal dari mana saja di belahan dunia, dimana dengan fasilitas *remote access* mereka dapat melakukan konfigurasi secara langsung. Letak permasalahannya adalah, apakah kedua *endpoint device* dan jaringan yang dibangun diantaranya sudah aman dari penyusup? Jika dahulu kala kondisi "*Air Gap*" yang tidak terhubung ke jaringan eksternal atau teknologi digital bisa dijaga, saat ini hal itu seringkali hanyalah sebatas mitos.

Perkembangan *industry* 4.0 menuntut perusahaan dan organisasi untuk lebih produktif dan efisien. Mengharuskan kedua *system* tradisional IT dan OT yang sebelumnya terpisah agar dapat terintegrasi dan saling terhubung satu sama lain. Banyak industri mulai tumbuh dengan transformasi digital yang mengintegrasikan jaringan dan komunikasi digital ke dalam *system* OT dengan menerapkan inovasi teknologi terbaru seperti industri *Internet of Things* (IoT). Solusi ini bertujuan untuk meningkatkan otomatisasi, menambahkan "*smart devices*", menghubungkan perangkat ke jaringan demi kenyamanan dan kemudahan serta membuat data lebih efisien dan selalu tersedia.



Gambar 4. Digitalisasi Keamanan Best Practice Untuk OT

Konvergensi antara IT dan OT bukan berarti tanpa resiko. Menghubungkan antara operasional dengan teknologi informasi membuka pintu besar peluang baru para penjahat siber untuk mengincar OT ICS ini sebagai target serangan siber dan mendapatkan kendali pada *system* operasional dan bahkan semua perangkat yang terkoneksi di dalamnya.

Dalam penelitiannya, *The Fortinet 2019 Operational Technology Security Trends Report* menemukan bahwa resiko ancaman serangan siber terhadap sector OT ini meningkat seiring dengan berkembangnya transformasi digital *industry* 4.0 yang saling terkoneksi internet dan menghubungkan *system* OT dengan *system* IT.

Pada kerangka IT, *remote access* adalah sebuah hal lazim yang dilakukan sehari-hari. Pengamanan *endpoint* dapat dilakukan dengan berbagai fitur *firewall*, *antivirus*, dan EDR. Namun infrastruktur OT seringkali tidak terjamah atau bahkan tidak terkoneksi ke pengamanan IT, sehingga jalur *bypass* seringkali menjadi solusi yang dapat menjadi pedang bermata dua. Kelancaran akses langsung ke mesin sangat berbahaya jika tidak ada layer yang melakukan inspeksi paket.

2. Endpoint Vulnerability

Pada mesin-mesin itu sendiri, seringkali yang dilakukan oleh pihak *maintenance* adalah *plugin* laptop via kabel atau *plugin* USB *Stick* ke perangkat HMI secara langsung. Apa yang terjadi jika laptop sudah terkandung *sleeper modbus/malware* lainnya yang aktif hanya ketika terkoneksi ke perangkat lainnya? Mesin bisa langsung terinfeksi. Apa yang terjadi jika ada 100 mesin yang di-*maintain* pada periode tersebut? Bagaimana cara melacak mesin spesifik yang terkena *malware* di rentetan *supply chain*, tanpa mengganggu proses produksi secara keseluruhan?

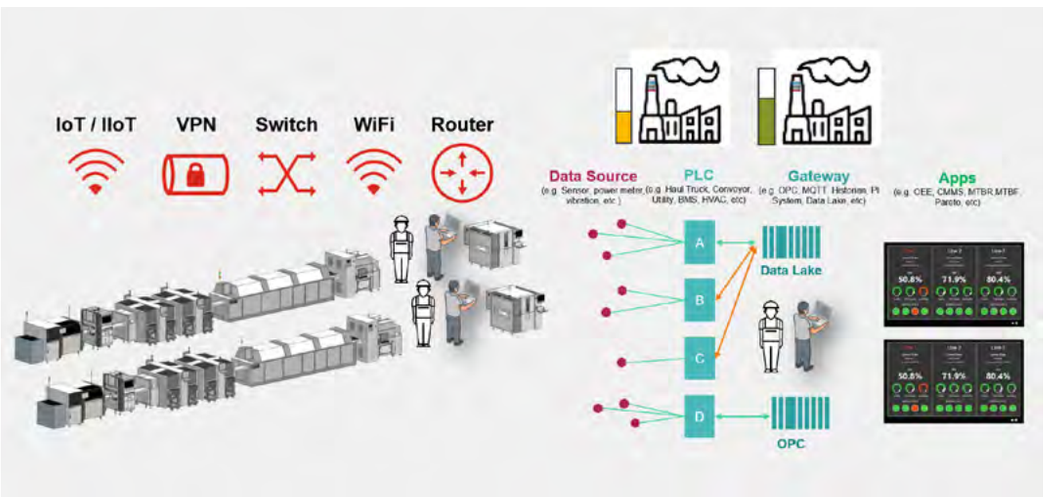
3. Different line, different system

ABB, Schneider, Siemens, Yokogawa, Rockwell, Emerson adalah beberapa contoh brand OT yang mengisi *production line*. Masing-masing memiliki *proprietary protocol*. Dengan banyaknya *system* yang pada kondisi normalnya cukup beragam bahkan di satu *production line*, muncul tantangan dimana masing-masing *system* memiliki keunikan tersendiri untuk konfigurasinya. Ini dapat menimbulkan waktu yang substansial untuk melakukan *security hardening* dimana *protocol* yang dimiliki setiap OT cenderung memiliki *proprietary* sendiri-sendiri. Kondisi ini menyebabkan desentralisasi *system* yang menimbulkan kompleksitas tersendiri.

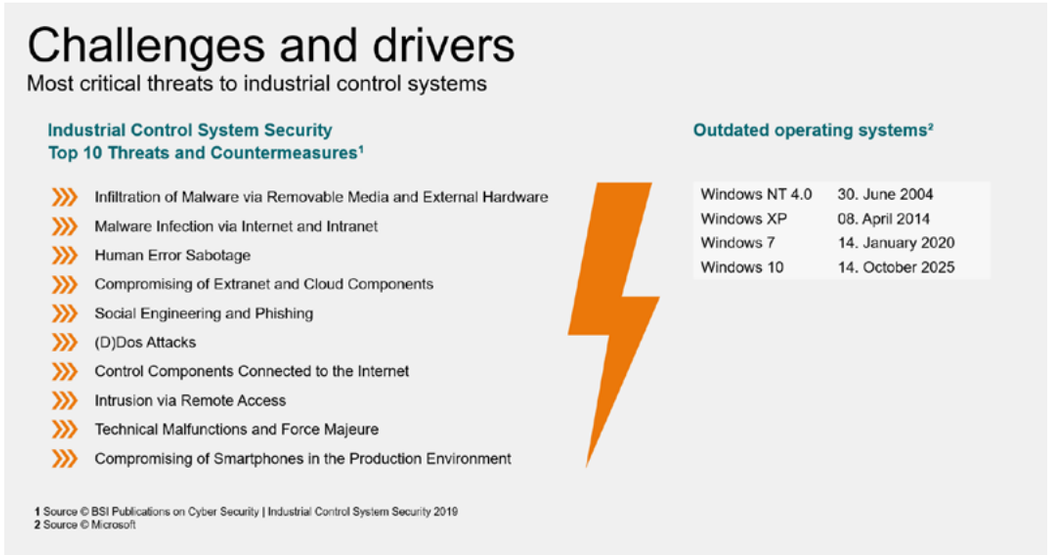
4. Aset OT

Aset OT seringkali tidak terindifikasi dengan benar, sehingga IT seringkali tidak familiar dengan aset yang ada di lantai produksi.

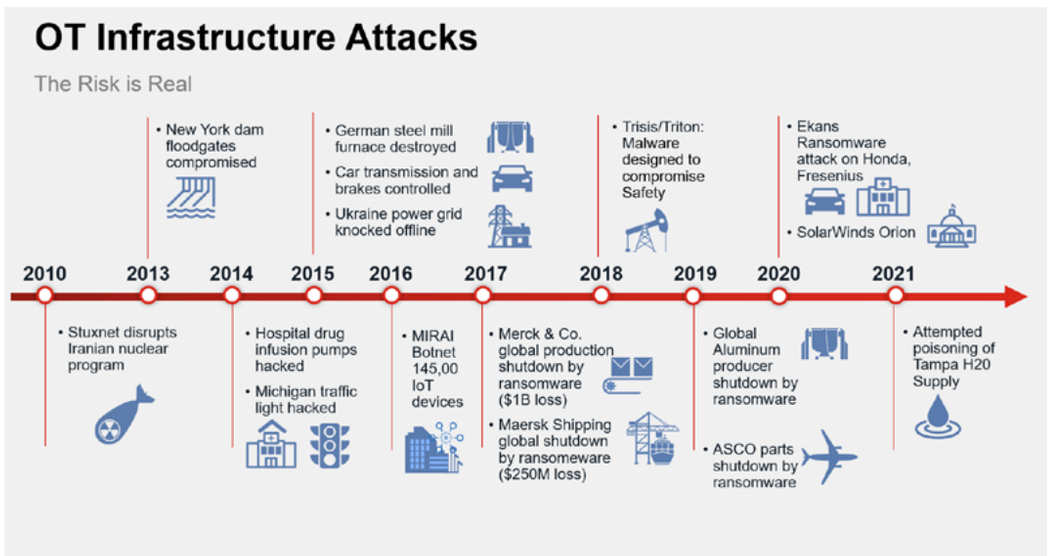
Gambar 5. Pengamanan FortiGuard Terhadap Protocol OT



Gambar 6. Asset OT dan Keutamaannya



Gambar 7. Ancaman Paling Umum Pada ICS



Gambar 8. OT Infrastructure Attacks

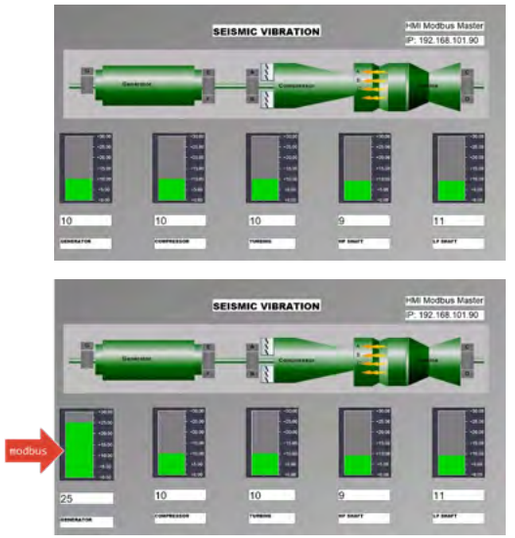
5. Outdated Patch + No Audit

Secara prinsip keamanan siber hal inilah yang paling fatal. Sayangnya hal ini sangat lazim di OT, karena kesulitan poin-poin di atas maka *update session* seringkali menjadi terbengkalai dan bahkan menjadi momok karena resiko *downtime* yang tidak sepadan dengan KPI produksi jika terjadi sesuatu yang tidak diinginkan pada proses *patching*.

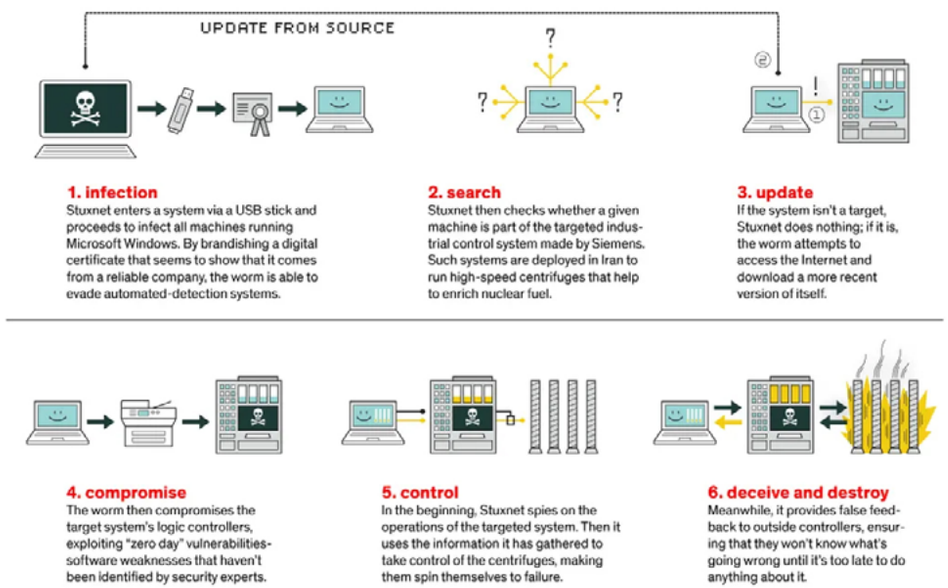
FACT OF THE MATTER/USE CASES

OT mencakup hal-hal yang bersifat "dapur" dan karenanya rahasia seringkali dijaga ketat. Walaupun kondisi ini menyebabkan banyak kejadian *ransomware* yang tidak terkuak, beberapa kasus karena sudah menjadi kasus besar sudah menjadi berita konsumsi *public*.

Hal yang kelihatannya simple seperti nilai meteran yang berubah pada HMI karena *Modbus Spoofing*, jika tidak disadari dapat menyebabkan operator melakukan penyesuaian manual langsung yang pada jangka waktu tertentu dapat menyebabkan kerusakan mesin produksi.



Gambar 9. Efek Modbus Spoofing

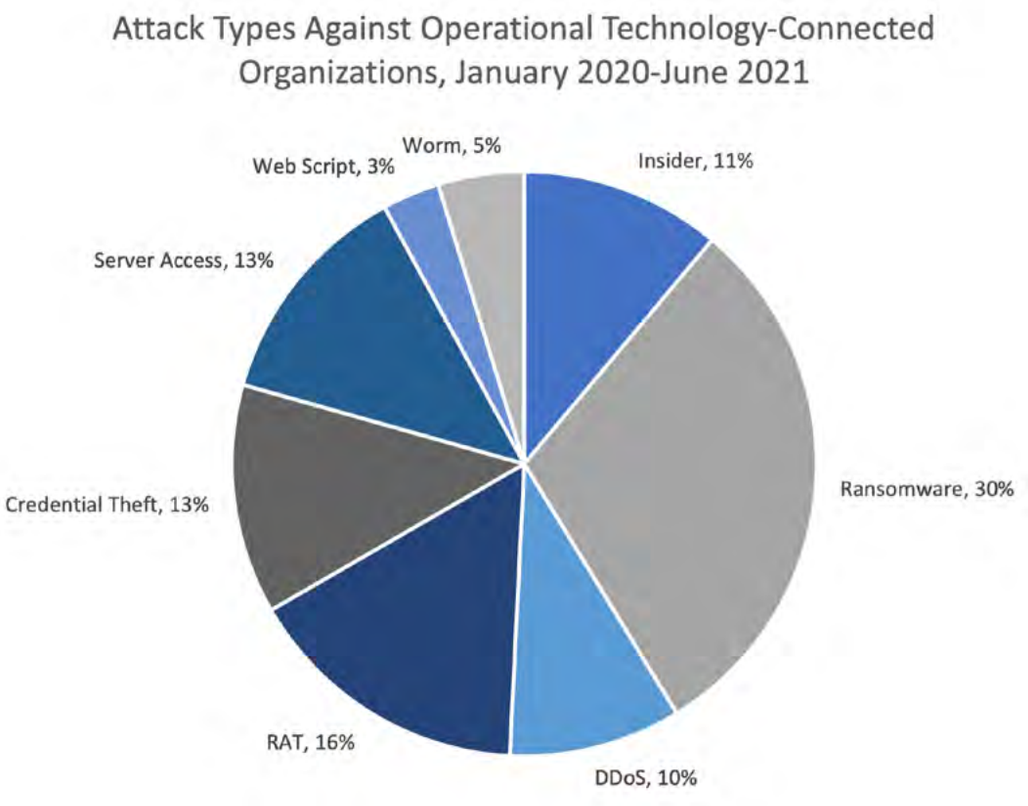


Gambar 10. Serangan Malware di Lingkungan OT

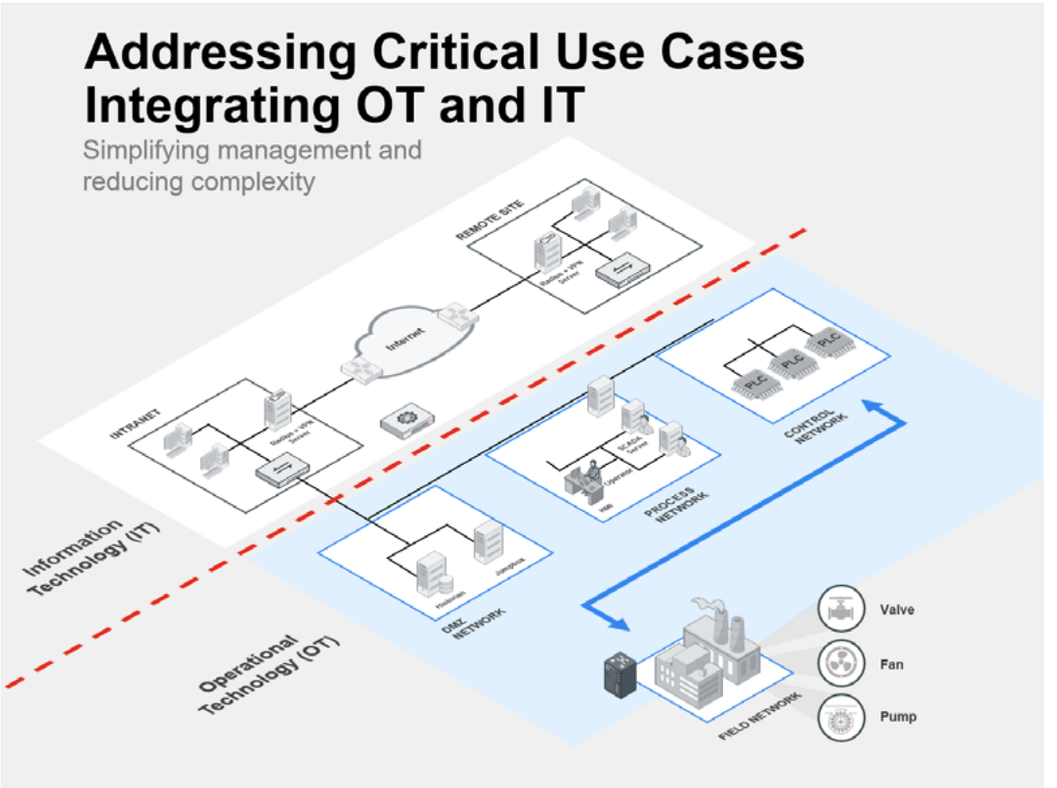
Sebuah survey di tahun 2017 dimana 82% praktisi keamanan data memperkirakan bahwa perangkat IoT yang tidak aman kemungkinan besar akan menyebabkan "*Data Breach*" di organisasi atau perusahaan mereka. Sebagai contoh insiden seperti serangan *malware* NotPetya di tahun 2017 menunjukkan bahwa sistem IT dan OT yang kompleks dan saling terhubung menyebabkan kehancuran yang tersebar luas dan cepat sehingga mengakibatkan gangguan di segala aspek mulai dari pengembangan produk, proses produksi dan pengiriman.

#WHOIS RESPONSIBLE

Perusahaan yang sudah mengedepankan keamanan siber dan mendirikan divisi sendiri untuknya biasanya cukup familiar dengan CISO (*Chief Information Security Officer*) dan BISO (*Business Information Security Officer*). CISO menangani keamanan dan strategi IT, sedangkan OT ditangani oleh BISO karena berhubungan langsung dengan proses produksi/*value creation*. CISO lebih berinteraksi dengan manajemen pada level strategis dan BISO berkutat pada level operasional dan taktis.



Gambar 11. Prosentase Berbagai Macam Tipe Serangan Siber



Gambar 12. Addressing Critical Use Cases Integrating OT and IT

IT X OT | STEP BY STEP, BIT BY BIT, STONE BY STONE, BRICK BY BRICK.

Konvergensi IT/OT adalah pendukung bisnis yang sangat penting, tetapi harus disertai dengan keamanan siber terintegrasi di seluruh perusahaan. Berikut ini adalah beberapa rekomendasi tindakan untuk membantu mengatasi serangan siber di OT:

1. **Segmentation - The establishment of DMZ/ Layer 3.5**

Pertama, dokumentasikan dan pahami lingkungan operasional perusahaan Anda, termasuk jaringan, data *flow* dan detail perangkat apa saja yang terhubung, serta titik akses fisik yang dapat dieksploitasi, seperti sensor atau *switches*. Segmentasikan sistem berdasarkan klasifikasinya dengan melihat variasi data dan *operational flows*-nya, bukan hanya di lingkungan OT tetapi juga dipengaruhi *system* dan protokol di lingkungan IT.

Sesuai namanya *Demilitarized Zone*(DMZ) adalah sebuah pembatas antara segmen IT dan segmen OT, yang akan mengandung pertahanan pertama pada serangan ke segmen OT. DMZ ini akan berperan sebagai "pemisah" antara *environment* IT dan OT, agar *treatment* yang berbeda dapat diimplementasikan secara efektif

Sebagai bagian dari *assessment*, Fortinet menyediakan OT *Security Posture* yang merupakan sebuah rangkaian kuisoner, dimana bersama partner seperti ACS Group, kita dapat bersama-sama melakukan penilaian yang *objective*, agar tahap selanjutnya, OT-specific CTAP, dapat

YouTube

Scan this QRcode

Gambar 13. "Apa itu CTAP" (Fortinet) Youtube (link QR Code)

dilakukan dengan tepat sasaran. Perlu kita sadari, kerentanan jaringan keamanan yang dapat diekploitasi dari luar, tidak kalah krusialnya dari internal.

2. Tegakkan SOP

Peran dan tanggung jawab seputar keamanan siber di perusahaan atau organisasi harus dipahami dengan jelas. Formalisasikan keamanan data dengan mengembangkan kebijakan, rencana dan prosedur yang diperlukan untuk mengelola dan mempertahankan keamanan dunia maya. Tata Kelola program ini harus di dukung oleh kepemimpinan eksekutif sehingga memungkinkan transformasi yang berkelanjutan dari waktu ke waktu.

3. Sustainable Development with continuous awareness training and regular audit

Dorong dan arahkan organisasi atau perusahaan Anda dengan menyediakan program Pendidikan dan kesadaran yang disesuaikan dengan peran. Contoh, operator lapangan berbeda wawasan dengan manajer pabrik dan sebagainya. Mendidik operator dan administrator tentang resiko dunia maya yang relevan dapat menumbuhkan budaya atau kesadaran pribadi yang memprioritaskan dunia maya sebagai keamanan-keselamatan, perolehan pendapatan, bisnis operasi dan stabilitas bisnis. Saat ini keterlambatan produksi dapat sangat mempengaruhi kontrak kerja, pendapatan dan reputasi perusahaan serta pertumbuhan jangka panjang.

4. Visibilitas lebih dalam untuk mengidentifikasi dan menanggapi resiko serangan

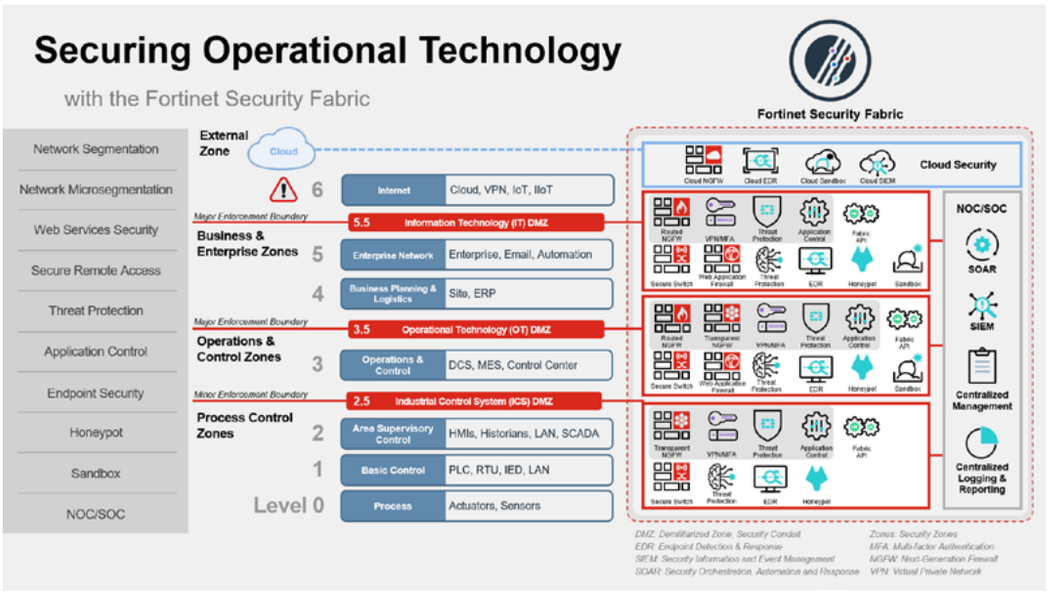
Terapkan sensor deteksi, pencatatan dan pengumpulan log yang terpusat dan kemampuan pemantauan serangan siber di perusahaan Anda. Sinkronkan upaya respons dengan menetapkan pendekatan yang terkoordinasi untuk mengelola OT/IT dan insiden di perusahaan. Tidak hanya untuk modul-modul laporannya, Anda juga dapat memanfaatkan *rule creation* dan *automation action* yang sudah disediakan FortiAnalyzer.

5. Virtual Patching

Fortinet menyediakan *tools Virtual Patching* yang khusus dibuat untuk perangkat-perangkat OT yang ketinggalan versi OS, yang akan sekaligus menjawab pertanyaan "apakah ada resiko *downtime*?"

6. NGFW Placement

Tentunya kita sadari investasi OT tidaklah kecil. Selain *firewall*, kita bisa mengutilisasikan *Secure Switch* dan *Secure* AP yang baiknya dari merk yang sama untuk memudahkan proses konfigurasi yang seragam. Berbagai *brand* saat ini berlomba-lomba, tak terkecuali FORTINET, untuk menyediakan tenunan produk-produk/Product



Gambar 14. Securing Operational Technology

Fabrics yang saling mendukung kelangsungan satu perangkat dengan lainnya dengan *seamlessness of policy making*. Sebaiknya kita juga menanamkan EDR pada *device* yang kebiasaannya langsung dikonfigurasi di tempat agar memitigasi *security bypassing* secara internal.

Perlu juga dipertimbangkan kondisi perangkat-perangkat ini saat ditempatkan secara fisik. Apakah ada *dedicated server room* atau dibutuhkan *equipment* yang *rugged*.

Selamat memperingati hari

Jumat Agung & Paskah

Kiranya cinta kasih dari Tuhan melalui Jumat Agung dan Paskah akan meningkatkan iman dan keyakinan umatNYA serta menghadirkan kedamaian, kebahagiaan dan cinta kasih dalam keluarga bahkan di antara sesama. Tuhan memberkati.

#CLOUDYDAY

Alibaba Cloud Hand's-On with ACS Group

Pada tanggal 13 Desember yang lalu bertempat di Barley & Barrel-Artotel Suites Bianti Hotel-Yogyakarta, ACS Group menyelenggarakan *event Hands-On Lab* yang dibawakan secara langsung oleh Eggy Tanuwijaya, Head of Solution Architect dari Alibaba Cloud Indonesia. Selain principal, acara ini juga didukung oleh tim distributor dari Blue Power Technology.

Hadirin bersumber dari *customer base* kami di *industry* edukasi dan *hospitality* yang berlokasi di kota Yogyakarta dan sekitarnya. Dalam sesi interaktif yang berdurasi 3 jam ini, para peserta masing-masing mempraktekkan *deployment* berbagai *instances* secara langsung pada infrastruktur Alibaba Cloud dan juga melakukan eksplorasi dari *troubleshooting* umum.

Tujuan event ini memberikan pemaparan dan pengalaman praktis yang dapat digunakan untuk mengeksekusi implementasi dari fasilitas-fasilitas

pada *Public Cloud*, dan bagaimana kita perlu menyadari model *shared-responsibility* dalam perjalanan pengadopsian *cloud* pada keseharian perusahaan. Fleksibilitas yang tersedia bagi pengguna *cloud* untuk menkonfigurasi *resources* yang tepat guna dan tepat waktu sesuai spesifikasi menjadi keunggulan utama dari *Public Cloud*. *Support* yang juga tersedia secara *one-to-one* termasuk tatap muka dengan tim *engineer* secara langsung merupakan satu dari banyak alasan dari kolaborasi ACS Group dengan Alibaba Cloud, *as a global initiative needs local action as part of their market availability.*

Joint Event ACE Lombok | 6th Gathering 2022

MENUJU ENGINEER LOMBOK YANG KOMPETEN

Pada tanggal 10 Desember 2022, Asosiasi Chief Engineer-Lombok (ACE Lombok) kembali diselenggarakan di Golden Palace Hotel. Acara yang dihadiri para anggota ACE Lombok, Bali dan daerah lainnya ini mengusung tema "Menuju Engineer Lombok Yang Kompeten".

Pada acara ini kata sambutan disampaikan oleh Ketua FKLPIDI (Forum Komunikasi Lembaga Pelatihan Kerja dan Industri Daerah) NTB, I Ketut Sarta dan sebagai *keynote speaker* oleh Made Sumantra - Deputy GM Development (PT. Jakarta Setiabudi International, Tbk).

Sama seperti *event* ACE di Bali di bulan November 2022 yang lalu, ACS Group bersama dengan Hytera POC *Solution* ikut berpartisipasi dengan membuka *booth* dimana para *engineer* yang hadir di *booth* mendapatkan penjelasan mengenai teknologi Hytera POC.

Hytera POC telah mengeluarkan berbagai produk *Private Mobile Radio* (PMR), *Handheld Radio*, *Mobile Radio Device*, *Repeater* & *System Modular Radio*, *Handset*, dan berbagai sistem komunikasi yang berkualitas tinggi.

Joint Event Alibaba Cloud

ALIBABA CLOUD DEVELOPER SUMMIT

Mendukung Kiprah Perkembangan Teknologi

ACS Group ikut berpartisipasi dalam acara yang kembali digelar oleh Alibaba Cloud Indonesia dengan mengusung tema "Tech for Innovation 2023 Alibaba Cloud Developer Summit". Acara ini diselenggarakan pada hari Selasa, 10 Januari 2023 yang dilaksanakan di Hotel The Ritz - Carlton, Pacific Place, Jakarta.

Saat ini, Alibaba Cloud meluncurkan komunitas pengembang atau *developer* Apsara berskala tingkat internasional, dikenal sebagai *Apsara Developer Community,* yang dibentuk sebagai penghubung untuk membantu dan mendukung *developer* di seluruh dunia juga untuk memfasilitasi kemajuan ekonomi digital.

Partisipan yang sebagian besar adalah *IT Developer* dan mahasiswa mencermati apa yang disampaikan pendiri Alibaba Cloud, Dr. Wang Jian, yang meng-*highlight* bahwa 1 Watt di era digitalisasi ini sama seperti 10 Watt di era elektrifikasi sebelumnya.

ACS Group mengisi sesi "Revolution of Traditional Business Becomes Smart Business in Indonesia" yang dibawakan oleh Ken Looho - Professional Services, menyoroti langkah dan tantangan organisasi bisnis *non-digital* dalam mengadopsi teknologi terkini dan bagaimana *cloud computing* dapat menjadi solusinya.

Kemajuan besar dari *cloud computing* memberikan banyak alternatif dalam sisi IT DevOps untuk menangani transisi yang lebih efektif menuju pembangunan berkelanjutan tanpa menghambat proses bisnis. Pemilihan *Managed Service Provider* yang tepat juga merupakan faktor penting dalam proses ini sehingga memungkinkan perusahaan untuk fokus pada elemen penting keberlangsungan bisnis mereka.

ACS Group mengedepankan pentingnya *Managed Service Provider* memahami *business process* secara detail dari end-user agar dapat merekomendasikan solusi teknologi yang tepat guna.

Joint Event Profit Bali | 13th Annual Gathering 2023

HOSPITALITY 5.0
GROW UP TOGETHER

ACS Group bersama Hytera & Zebra Technologies hadir kembali menyapa ratusan personel IT yang hadir pada pertemuan tahunan (*annual gathering*) Profesional IT (ProfIT) ke-13 dengan mengusung tema "Hospitality 5.0 Grow Up Together" yang diselenggarakan di HARRIS Hotel and Residences Sunset Road, Kuta, Sabtu (25/2/2023).

Dalam sambutannya, Chief Executive Office Professional IT Bali, Armika Jaya, mengatakan harapan ke depan bagaimana membuat IT ini lebih mudah diterima dan diterapkan.

Chairman Professional IT Bali, Eka Kunindra Jaya, menambahkan acara kali ini tercatat 500 orang melakukan registrasi yang berasal dari pekerja IT berbagai sektor industri, meliputi perhotelan, pemerintah, rumah sakit, sekolah, universitas, dan profesional lainnya.

Eric Ananda, MBA
Country Channel Manager, Zebra Technologies Indonesia

Api Agape Paradisa Budi
Sr. Sales Engineer, Zebra Technologies Indonesia

Zebra Technologies pada acara ini memperkenalkan lini teknologi baru dengan mengusung tema "Smart Hospitality" yang dapat meningkatkan pengalaman *customer*/para tamu hotel untuk melakukan proses *check-in* dan *check-out*. Adapun teknologi yang dilahirkan Zebra untuk menjawab kebutuhan tersebut, seperti: *Laundry Tracking System – Powered by* RFID; *Food Safety Supply Chain*; *Inventory Management*; *Mobile POS and Communication Tool Powered by Workforce Connect*.

Krisna Dhian Wahyudi
Country Channel Manager, Hytera Indonesia

Sementara itu, Hytera memperkenalkan lini teknologi baru yaitu *Push to Talk Over Cellular* (PoC) guna menjawab ketidakmampuan dari HT (*Handy Talkie*) konvensional yaitu, suara yang dihasilkan kurang jernih, hingga kebutuhan *data-intensive multimedia services* yang semakin tinggi, seperti gambar dan video. Melalui booth yang dibuka oleh Hytera, terdapat beberapa barang demo unit, seperti: Hytera PoC PNC380 & PNC360S; Hytera PoC MNC360; dan Hytera Body-Worn Camera (BWC) VM580D. PoC Hytera dilengkapi dengan teknologi kemampuan audio yang jernih, video, tombol navigasi, standar IP militer, sampai GPS Tracker.

Hytera dan Zebra Technologies mengharapkan dengan kemajuan teknologi yang dikembangkan ini dapat memberikan solusi kepada setiap permasalahan di berbagai sektor industri, khususnya perhotelan.

ANAK YANG CERDIK/BODOH?

KOLOM KETAWA

Menjelang petang datanglah seorang anak perempuan mendatangi sebuah warung makan. Melihat sang anak datang, sang pelayan yang biasa melayani berbisik kepada pelanggan yang saat itu sedang melihat-lihat makanan yang akan dipilihnya, "Bu... Bu... Anda tahu tidak? Anak yang baru masuk ini adalah anak terbodoh di dunia"... "Percaya ga Bu?". "Ah masa sih" sahut si pelangan... "Saya membuktikannya bu... Lihat ya".

Sang pelayan mengambil uang dua puluh ribu rupiah di satu tangan dan lima ribu rupiah di tangan lainnya. Kemudian, pelayan tersebut memanggil anak perempuan itu "De... de sini deh" lalu sang anak menghampirinya. Sang pelayan bertanya, "Kamu mau pilih yang mana, de?"

Anak perempuan tersebut tanpa berpikir panjang, lalu meraih uang lima ribu rupiah, sambil mengucapkan terima kasih, lalu pergi keluar.

"Tuhhh benarkan bu? Aku sudah pernah melakukan ini beberapa kali dan anak itu selalu memilih uang lima ribu!" kata sang pelayan. "Dia itu tidak pernah belajar!".. keduanya pun tertawa.

Setelah pelanggan keluar dari warung makan, dia melihat anak perempuan tersebut baru saja selesai membeli makanan ringan. "Hei de sini deh, ibu mau tanya? tadi saat kamu disodorin uang kenapa kamu memilih uang yang lima ribu bukan yang dua puluh ribu?".

Sambil menikmati makanan ringannya Anak perempuan itu menjawab, "Kalau aku ambil uang dua puluh ribu, tuh ibu ga akan pernah nawarin uang ke aku lagi bu!"... "ooohhhh !@#%%**&&"

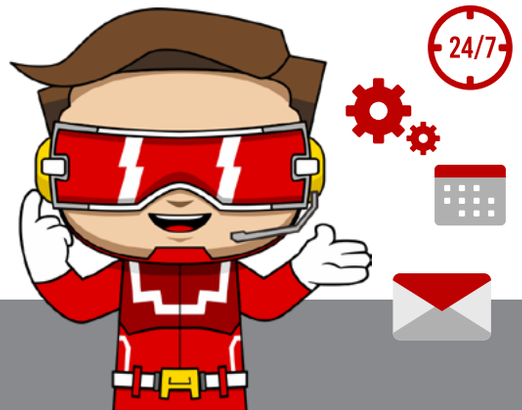
ACSCare
BY ACS GROUP

Kebutuhan operasional dapat terhambat secara signifikan dengan *downtime* yang disebabkan malfungsi dari beberapa perangkat keras (*hardware*) IT. Tentunya hal yang tidak diinginkan ini dan secara langsung akan mengganggu kinerja serta memakan waktu tambahan dari tim IT dan *Procurement*. Diperlukan solusi yang secara komprehensif dan ekonomis dapat dilakukan tanpa menambah beban dan budget yang tak terduga dari personil IT.

ACS Group menawarkan ACSCare untuk beberapa perangkat yang telah menjadi spesialisasi kami, agar tim Anda dapat bekerja dengan optimal tanpa mengalokasikan *resource* berlebih untuk menganalisa kemudian melakukan tindakan perbaikan perangkat.

Extended Manufacturing Defect Coverage

Standard Warranty pada *hardware* menjamin ketersediaan *spare-part* untuk kasus *manufacturing defect* selama 1-tahun pertama sejak pembelian. Dengan ACSCare, periode ini diperpanjang sampai 3-tahun, mencakup berbagai produk antara lain *Label Printer*, *Regional Mobile Computer* dan *Access Point*.



Critical Spare-Part Backup

Printhead & *platen roll* adalah salah satu contoh *spare-part* dari *printer* yang paling penting, dimana ketersediaannya adalah esensial. Cakupan juga termasuk untuk Hytera *PTT-over-Cellular* dan *Mobile Terminal*.

Unit Backup

Tidak hanya *spare-part*, ACSCare juga menyediakan berbagai unit *ready-to-deploy* tertentu, termasuk perangkat RFID, untuk mengantisipasi kejadian tidak terduga yang menyebabkan unit operasional tidak dapat dipakai atau diperbaiki secara cepat.

Remote Support

Case yang banyak kami alami adalah kebutuhan konfigurasi sederhana yang dapat terakomodasi dengan *remote support*, baik melalui komunikasi telepon atau dengan kontrol secara *remote*. ACSCare menyediakan *hotline support* yang dapat dihubungi pada jam kerja.

Pickup & Delivery

Hilangkan kerisauan ekspedisi dan serahkan pada ACSCare untuk melakukan P&D yang secara langsung memastikan unit anda dapat diterima kembali dengan kondisi aman.

TAT Commitment

Berfungsi layaknya seperti asuransi, ACSCare mendukung kontinuitas bisnis anda dengan komitmen *Turn Around Time* (TAT) yang terukur.

Further Managed Service

Tentunya kemampuan *Managed Service* ACS Group tidak berhenti sampai disitu. Kami juga menyediakan layanan untuk kebutuhan *Mobile Device Management* [MDM], *Cyber Security* & *Wireless LAN Remote Support*, *Wireless LAN Coverage Site Survey*, *Cyber Threat Assessment*, 24x7 *Support Availability*, serta *Preventive & Corrective Maintenance.*

"Mari sambut Cahaya Ramadhan dengan embun suka cita, mohon dimaafkan dari segala khilaf yang pernah ada, mari kita sucikan diri perbanyak ibadah dan raup pahala sebanyak-banyaknya. Marhaban ya Ramadhan, Barokallahu lana".

Seluruh staf dan Management **ACS GROUP** mengucapkan

Semoga Allah memberikan rahmat kepada semua para pelanggan yang beragama Muslim untuk menyongsong hari yang Fitri, damai dan membahagiakan. Kiranya kegembiraan Idulfitri berlipat beribu kali dan tetap bersamamu selamanya.

Selamat menunaikan **IBADAH PUASA**, dan Selamat menyongsong **HARI RAYA IDUL FITRI 1444 H**, kami mohon maaf lahir batin. Semoga amal kita diterima di sisi Alllah SWT. Aamiin

ZEBRA

TC78 Ultra-Rugged Mobile Computer

Industri : Transportation, Field Mobility & Location Solutions.

TC78 dirancang untuk pekerja yang menghabiskan pekerjaan mereka di luar ruangan. Perangkat ini memiliki jaringan nirkabel yang komprehensif untuk kinerja dan keandalan yang tak tertandingi — Wi-Fi 6E, 5G, dan CBRS 1, termasuk *streaming* video dan panggilan video; Bluetooth 5.2 untuk kinerja aksesori yang unggul serta layar Full HD 6 inci yang cerah mudah dilihat sekalipun berada di bawah sinar matahari secara langsung. Produk yang dirancang tahan terhadap benturan saat jatuh di atas beton dengan ketinggian 3.05 meter ini, siap untuk operasional di lapangan. Lebih ringan, dan hampir 20% lebih tipis, mudah untuk digenggam dan digunakan oleh tangan dengan berbagai ukuran.

ZEBRA

TC58 Mobile Computer

Industri : Transportation, Field Mobility & Location Solutions.

Mobile Computer TC58 yang tangguh, dilengkapi dengan teknologi Wi-Fi yang lebih cepat dan hemat daya (Wi-Fi 6, Wi-Fi 6E, CBRS (khusus AS), 5G); dukungan lokasi yang kaya; suara berkualitas tinggi; dan kamera belakang berwarna berkualitas tinggi untuk foto dan video beresolusi tinggi. Produk ini memiliki *scan engine* pilihan yaitu SE4720 1D/2D atau *scan engine* SE55 1D/2D *Advanced Range* dengan teknologi IntelliFocus™, *Device Tracker*, Zebra's *Dimensioning™ Certified Mobile Parcel* dan alat *Mobility* DNA, menjadikan TC58 sebagai generasi baru pengumpulan data *the four walls* untuk operasional di area luar. Produk ini sudah divalidasi oleh Microsoft Teams untuk menjalankan aplikasi *Walkie Talkie* serta memiliki standard IP68 dan IP65 dengan baterai sesuai spesifikasi penyegelan IEC yang berlaku.

ZEBRA

ZQ320 Mobile Printer

Industri : Transportation, Retail, Manufacturing & Hospitality.

Mobile Printer ZQ320 memungkinkan para pekerja ritel dan pekerja lapangan mencetak struk/kuitansi atau label dengan kualitas tinggi di manapun produk ini digunakan. *Mobile printer* ini ringan, cepat, fleksibel, andal, lebih produktif dan mampu memenuhi kebutuhan pelanggan serta proses bisnis dengan lebih baik. *Printer* seluler ini juga memiliki standard IP54, dapat diberdayakan secara terus menerus dan dilengkapi dengan solusi manajemen jarak jauh bluetooth yang siap pakai.

ARUBA HPE

AP-535 Internal Antenna Models

Industri : All Industries

Perangkat Aruba AP-535 *internal antenna* adalah perangkat *access point indoor* standar **802.11ax (Wi-Fi 6)**, yang dirancang untuk konektivitas dengan kinerja tinggi dalam *deployment* perangkat mobile dan perangkat IoT di lingkungan jaringan *wireless high density* seperti lingkungan perkantoran dimana jumlah perangkat klien yang besar secara simultan terhubung.

Dengan *built-on* Wi-Fi 6 standard, Aruba AP-535 hadir dengan fitur-fitur seperti OFDMA, *bidirectional uplink/downlink* MU-MIMO, dan *Target Wake Time* (TWT) untuk menciptakan kinerja *multi-user* yang terbaik dan meningkatkan efisiensi. Dengan kecepatan koneksi maksimum hingga 2.97 Gbps dan maksimum jumlah *associated clients per radio*-nya hingga 1024 *clients*.

Aruba AP-535, seperti perangkat Aruba AP Wi-Fi 6 lainnya, mendukung teknologi Zigbee, Bluetooth 5, dan *third-party overlays* untuk kemudahan dalam *deployment* dan manajemen layanan IoT serta menyediakan *telemetry* untuk *contact-tracing dashboards* yang terdapat pada Aruba Central.

Dalam hal keamanan, Aruba AP-535 tentunya sudah dilengkapi perlindungan terhadap jaringan dengan *encryption* dan *authentication* yang kuat, pengamanan *credentials/keys storage*, dan kebijakan akses (*access policy enforcement firewalls*) terhadap *user* dan perangkat-perangkat IoT.

ARUBA HPE

AP-555 Internal Antenna Models

Industri : All Industries

Perangkat *access point* Aruba AP-555 internal antenna dirancang untuk melayani koneksi nirkabel pada *multiple clients* secara simultan dengan dual radio MIMO 8x8 + 4x4 sangat cocok diterapkan pada ruang *indoor* yang luas dan *high-density* karena mampu memberikan kecepatan koneksi *wireless* hingga 5.37 Gbps.

Dengan fitur Wi-Fi 6 OFDMA, MU-MIMO dan ClientMatch, perangkat ini mampu menangani *multiple clients* pada setiap channel, apa pun jenis perangkat atau *traffic*-nya, perangkat ini juga didukung teknologi AI-*powered* RF untuk menghilangkan masalah *sticky client*.

Pada level keamanan Aruba AP-555 semakin ditingkatkan dengan standar WPA3 dan *Enhanced Open security* tanpa meningkatkan kompleksitas serta memastikan perlindungan *guest access* yang kuat. Seperti perangkat Aruba AP Wi-Fi 6 lainnya, AP-555 juga sudah dilengkapi dengan fitur *Air Slice* untuk *SLA-grade performance* dalam memantau *latency-sensitive*, *high-bandwidth*, dan *IoT services*.

Keunggulan tambahan lainnya dari teknologi 802.11ax, pada perangkat access point Aruba, termasuk AP-555, memiliki kapabilitas seperti dalam hal *AI-powered RF optimization*, *always-on connectivity*, serta *Green* AP *mode* yang AI-*powered energy* menghemat energi hingga 70%.

ZKTECO

RevFace15 [TI]

Industri : Healthcare, Retail & Hospitality.

RevFace15 [TI] dirancang berdasarkan algoritma pengenalan wajah terbaru dan CPU khusus ZKTeco untuk menjalankan algoritma pengenalan wajah.

Dengan dukungan daya komputasi dan algoritma pengenalan wajah yang luar biasa, terminal ini juga mengintegrasikan modul *thermal imaging* beresolusi besar dengan sistem pengenalan wajah *Computer Vision*.

RevFace15 [TI] dapat mewujudkan otentikasi biometrik yang cepat dan akurat ditambah lagi dengan deteksi dan peringatan bagi pengguna yang tidak mengenakan masker dan mereka yang memiliki suhu tubuh tidak normal. Ini juga meningkatkan efisiensi penyaringan kerumunan di tempat-tempat umum.

Fiturnya sebagai berikut:

- Pengenalan wajah dan deteksi suhu beberapa orang sekaligus (hingga 4 orang).
- Kecepatan pengenalan wajah kurang dari 0,2 detik per wajah
- Kamera sensor CMOS *starlight* 2MP dengan fungsi WDR, mendukung penyesuaian otomatis sesuai dengan kondisi pencahayaan untuk memberikan gambar yang akurat dan detail di area dengan intensitas cahaya yang kontras
- Rentang suhu kerja yang luas: 16°C hingga 35°C (60,8°F hingga 95°F)
- Algoritme *anti-spoong* terhadap media cetak (Foto Laser, berwarna dan B/W), video, dan topeng 3D
- Deteksi masker; verifikasi wajah tersedia dengan masker.

Saksikan Podcast ACS Group yang membahas Produk Hytera POC di channel Youtube kami.

Scan this QRcode

SUBSCRIBE ACS Group Youtube Channel

SEUIC

AUTOID UTouch

Industri : Retail, Warehouse Management & Power Inspection field.

AUTOID UTouch adalah *mobile terminal* RFID untuk pengambilan data di lapangan, dapat digunakan secara bebas baik untuk di area industri seperti ritel, pergudangan, manajemen aset publik, logistik dan lain-lain, untuk membantu pelanggan mengoptimalkan serta melancarkan bisnis dan manajemen aset mereka. Produk ini mampu memindai 200 tag RFID/detik dan memiliki jarak pindai sejauh 15 meter, sekaligus dapat digunakan untuk membaca barcode 1D & 2D.

AUTOID UTouch ini memiliki Wi-Fi 4G/Dual-band dan standard IP65 yang tahan benturan saat jatuh pada jarak 1.5 meter, dibangun dengan bentuk slim dan bobot yang ringan, hanya 465g, sehingga memudahkan pengguna untuk menggunakannya dalam waktu yang lama dan tidak melelahkan.

HYTERA

PNC380 PoC Radio

Industri : Traffic Police, Property Security, Logistics, Airports, Major Events, & Industrial Parks.

PNC380 merupakan *All Rounded Device* digunakan oleh setiap petugas lapangan. Bentuknya yang ringkas dan kemudahan dalam pengoperasian menjadi favorit bagi bagi seluruh pengguna PoC di setiap lini bisnis. Didukung sinyal seluler dari GSM SIM Card dan wi-fi, pengguna dapat berkoordinasi dengan lainnya tanpa batasan jarak lagi. Lalu, Mic PNC380 telah dilengkapi *noise cancellation* membuatnya semakin fokus pada suara pengguna yang berkirim pesan suara ke pengguna lainnya. Selain itu, PoC ini juga telah dilengkapi NFC, Bluetooth 4.1, dan standar ketahanan IP67 dan MIL-STD-810G

Melalui fitur *dispatcher* (optional) dari aplikasi Hytalk, Anda dapat mengetahui perpindahan lokasi *realtime* dari seluruh pengguna melalui GPS *tracker* yang terpasang & dan kondisi terkini di sekitarnya melalui kamera beresolusi 5MP. Kamera ini juga berfungsi untuk live video report ke semua pengguna. Hytera PoC PNC380 sangat ideal untuk berbagai skenario lapangan seperti warehouse & factory complex, security & facility support, logistic, event organizer, healthcare, hospitality dan beragam area kerja lainnya.

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

#ACSforIndonesia

Solusi Teknologi Bangsa

Kick Off ACS Group

Pada tanggal 16 Januari 2023, seluruh karyawan ACS Group, baik yang ada di pusat maupun seluruh cabang, mengadakan acara bersama *Kick Off* #ACSForIndonesia "Solusi Teknologi Bangsa". Acara ini diadakan sebagai awal kegiatan dan ucapan syukur kepada Tuhan Yang Maha Kuasa atas berkahNya di sepanjang tahun 2023. Pada acara ini seluruh peserta mendapatkan pengarahan-pengarahan untuk siap bahu membahu melaksanakan tugas sesuai visi dan misi perusahaan.

"Menjadi *leader* di bidang IT solution provider harus selalu dapat mengikuti perkembangan teknologi yang bergerak sangat cepat dan dinamis. Memanfaatkan segala macam *platform* baik itu *website*, *social media*, atau media lainnya sebagai alat yang paling *actual* agar dapat terus menjual.

Tetapi kerja yang sebenar-benarnya membutuhkan pembuktian, menghasilkan karya nyata yang bukan hanya sekedar duduk manis di belakang meja.

Di awal tahun ini patut kita bertanya pada diri kita sendiri, apa perubahan yang bisa kita lakukan, untuk diri kita sendiri, untuk keluarga, untuk orang sekitar, untuk perusahaan, dan juga untuk negara.

Apakah perubahan tersebut akan menjadi lebih baik, lebih besar atau kemungkinan akan sama saja karena zona nyaman yang sedang kita nikmati sekarang?

Menjadi *millenial* saja tidak cukup, pemimpin harus bergerak maju, tahan banting dan siap menghadapi badai." Itulah narasi dari acara *Kick Off* tersebut.

Acara *Kick off* ACS Group ini dibuka oleh Indra Tjahjadi[1] selaku Managing Director, dilanjutkan dengan "Success Spirit" yang disampaikan oleh Arijanto Hartanto[2] - Sales & Marketing Director.

Pada acara ini beberapa karyawan ACS Group mendapatkan apresiasi sebagai *TOP PERFORMER'S* 2022 dan terpilih 5 orang karyawan antara lain:

1. Adrian Dewantoro - Branch Manager, Semarang
2. Liana Andari - Senior Account Executive, Jakarta
3. Ridwan David Deden - Enterprise IT Engineer, Jakarta
4. Bimo Jati Utomo - Service Center Engineer, Jakarta
5. Ahmad Deden Pramana, Office Support, Jakarta

Dalam acara ini juga ACS Group memberikan penghargaan kesetiaan sebagai karyawan ACS Group berupa sertifikat dan pin emas kepada beberapa karyawan antara lain kepada:

Tiga karyawan dengan masa jabatan 15 tahun yaitu:

1. Dasa Aprily Ardy, Jakarta
2. Deni Sutiharyanto, Jakarta
3. Satria Ardhi Bramana, Jakarta

Lima karyawan dengan masa jabatan 20 tahun yaitu:

1. Irvan Kurniawan, Jakarta
2. Liana Andari, Jakarta
3. Endah Novita Anggraini, Jakarta
4. A A Ngurah Mahendra, Denpasar
5. Moh Gufron, Surabaya

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

BEING CERTIFIED MEANS WE ARE QUALIFIED TO RUN HIGHER-QUALITY JOB FOR YOU AS OUR VALUED CUSTOMER.

and many more...

Training Update Product HPE Aruba

Pada tanggal 10 Februari 2023 lalu, seluruh sales dan beberapa engineer kembali mendapatkan update produk dari HPE Aruba yang dibawakan oleh Krisanti Pramono, Partner Business Manager at Aruba, a Hewlett Packard.

Update produk yang diberikan antara lain Aruba Central (Cloud Based Controller), Edge connect (Aruba SD WAN/SD Branch Solution), Aruba Instan On (SMB Ap), Aruba CX+Pensando Series dan Appliance for Data Center

Training Certified Digital Marketing Communication

ACS Group terus meningkatkan pengetahuan bagi para stafnya untuk menunjang operasional perusahaan dalam membangun komunikasi dengan para pelanggan. Tanggal 13 - 15 Februari yang lalu tiga staf dari departemen marketing communication Oscar Budi Trianto, Achmad Mustakhin dan Chandra Sari telah mengikuti training Certified Digital Marketing Communication. Dari training ini ke tiga staf kami mendapatkan sertifikasi CDMC serta pengetahuan tentang marketing communcation strategy, content marketing dan lead management, ecommerce, web analitics, SEM, social media marketing dan lain-lain.

2022 Shaping Intelligence Summit

ACS Group bersama lebih dari 400 mitra Hikvision dari seluruh dunia ikut berpartisipasi dalam pertemuan puncak “2022 Shaping Intelligence Summit” di Bali, pada tanggal 29-30 November 2022. Para peserta saling bertukar ide, wawasan, pengalaman, dan praktik dalam megatren teknologi AIoT.

Selama pertemuan tersebut, Hikvision, pelanggan, mitra teknologi dan solusi, serta pemimpin industri lainnya berkumpul untuk melihat masa depan AIoT dan menjelajahi jalan menuju kesuksesan bersama.

“Tepat berada di garis depan AI, IoT, dan teknologi lainnya, memiliki peluang besar untuk melakukan inovasi dan kolaborasi AIoT dengan para partner untuk membantu organisasi layanan publik dan perusahaan dengan solusi yang dapat mengoptimalkan pengambilan keputusan dan meningkatkan efisiensi operasional,” kata Keen Yao, Vice President dari Hikvision, dalam pidato pembukaannya untuk KTT tersebut.

Pada pertemuan ini, beberapa mitra teknologi dan pelanggan mempresentasikan bagaimana mereka memanfaatkan teknologi dan solusi AIoT Hikvision untuk mendorong peningkatan keamanan dan efisiensi di industri mereka.

Dalam acara ini, Hikvision juga meluncurkan program STAR, yang bertujuan untuk bermitra dengan organisasi nirlaba di seluruh dunia dan mengeksplorasi cara-cara inovatif untuk meningkatkan pelestarian lingkungan dan pelestarian budaya melalui teknologi canggih Hikvision.

42Gears Menjalin Kerjasama Dengan ACS Group

Pada tanggal 17 Januari 2023 ACS Group menerima kunjungan partner 42Gears di kantor pusat ACS Group, yang berada di Jl. Gunung Sahari Raya, Jakarta.

Kunjungan tersebut membahas kerjasama antara ACS Group dan 42Gears. 42Gears yang diwakili oleh Vikram Varakhedi sebagai Manager Strategic Partnerships APAC & ME serta Rohit Kumar sebagai Head Sales APAC & ME menyerahkan Partner Certificate kepada ACS Group yang diwakili oleh Arijanto Hartanto - Sales & Marketing Director.

42Gears adalah aplikasi solusi manajemen perangkat seluler multi platform yang mengamankan, memonitor dan mengelola dari jarak jauh seluruh armada perangkat mobile operasional anda di lapangan (Mobile Komputer, tablet, desktop dan device smart lainnya). Administrator dapat melihat layar perangkat dan dapat menggunakan mouse dan keyboard desktop untuk berinteraksi dengan perangkat seluler tersebut.

TIPS & INFO

PING DARI SOURCE ADDRESS TERTENTU PADA PERANGKAT NGFW FORTIGATE

Pada saat melakukan perintah ping dari perangkat NGFW FortiGate, perangkat yang biasanya memiliki banyak interface, secara default ping akan bersumber dari interface terdekat ke tujuan.

Sebagai contoh, perangkat dengan interface 'inside'-nya adalah IP 10.1.1.1 dan interface 'outside'-nya adalah IP '12.34.22.122' serta gateway default IP '12.34.22.121'. Dengan tidak adanya route statik, maka ketika mencoba melakukan ping ke IP 4.2.2.2 dari perangkat, ping akan bersumber dari source IP '12.34.22.122'.

Berikut tip untuk mengatur **source address** pada perangkat FortiGate dengan CLI, jalankan perintah execute ping-options view-settings. Yang mana secara 'default' Source Address-nya adalah auto.

```
LABFW-01 # execute ping-options view-settings
Ping Options:
        Repeat Count: 5
        Data Size: 56
        Timeout: 2
        Interval: 1
        TTL: 64
        TOS: 0
        DF bit: unset
        Source Address: auto
        Pattern:
        Pattern Size in Bytes: 0
        Validate Reply: no
        Adaptive Ping: disable
```

Berikut beberapa settings lainnya yang perlu diperhatikan, seperti:

- 5 packets yang akan di-sent
- Dengan Data Size 56 bytes
- Timeout value: 2

Rubah parameter Ping Option source address-nya dengan menjalankan perintah command berikut, dalam contoh kali ini dengan Source Address-nya adalah IP 1.1.20.225:

execute ping-options source 1.1.20.225

```
LABFW-01 # execute ping-options view-settings
Ping Options:
        Repeat Count: 5
        Data Size: 56
        Timeout: 2
        Interval: 1
        TTL: 64
        TOS: 0
        DF bit: unset
        Source Address: 1.1.20.225
        Pattern:
        Pattern Size in Bytes: 0
        Validate Reply: no
        Adaptive Ping: disable
```

Jangan lupa ketik command exit atau <ctrl-d> untuk keluar/exit dan commit terhadap perubahan setting yang telah dilakukan. Selamat mencoba!

Sumber: https://infosecmonkey.com/fortigate-cli-tips-and-tricks/
*/ Penulis : Irvan Kurniawan (irvan.kurniawan@acsgroup.co.id)

ZEBRA CAPTURE YOUR EDGE

We give you the performance edge to go above and beyond.

At Zebra, we're committed to empowering teams with the mobility and insight to deliver at the cutting edge of excellence. More than just providing intelligent hardware, we offer solutions that give organisations complete visibility to make smart, nimble decisions about what action to take now, and how to plan for tomorrow.

RETAIL SCANNER

INDUSTRIAL SCANNER

MOBILE COMPUTER

MOBILE PRINTER

INDUSTRIAL PRINTER

DESKTOP PRINTER

RFID SOLUTION PRODUCTS

www.zebra.com

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
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.

BUSINESS PARTNERS

Alibaba Cloud · aruba a Hewlett Packard Enterprise company · BarTender by SEAGULL SCIENTIFIC · BOSCH Invented for life · brother at your side
Extreme Connect Beyond the Network · FORTINET · Hewlett Packard Enterprise · HID · HIKVISION
HUAWEI · Hytera · ivanti · JANZ · POINT Mobile
SAMSUNG · Seuic · 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