GEBYAR

BULETIN EDISI 40/SEPTEMBER 2017

AUTO-ID

UNTUK KALANGAN SENDIRI

Advanced Threats, Advanced Solutions:
Mengintegrasikan Sandbox Ke Dalam Infrastruktur Anda

Analisa Log & Report Perangkat Fortinet Secara Terpusat

Menyambut
HUT ke 10 Tahun
Gebyar AUTO-ID

Tips & Info :
Tips dalam mengantisipasi Web Defacement

MEDIA KOMUNIKASI
PELANGGAN

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

PEMIMPIN REDAKSI
Andre S.Kouanak

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

EDITOR
Usadi Sastra Atmadja

DESAINER
Oscar Budi Trianto

KONTRIBUTOR (PENULIS)
Dasa Aprily Ardy
Maulana Ibrahim
Irvan Kurniawan

ALAMAT REDAKSI
Jakarta
Perkantoran Gunung Sahari Permai
#C03-05, Jl. Gunung Sahari Raya
No 60-63 Jakarta 10610.
Telp : +6221-4208221(H), 4205187(H)
Fax : +6221-4207903, 4207904,
4205853

CONTENT

3 Editorial - **Dasa Aprily Ardy**
4 Advanced Threats, Advanced Solutions:
Mengintegrasikan Sandbox Ke Dalam Infrastruktur Anda
10 News & Event
12 Analisa Log & Report Perangkat Fortinet Secara Terpusat
16 Menyambut 10 thn Buletin
18 Product Highlight
20 Corporate & Principal Info
22 Tips & Info : Tips dalam mengantisipasi web defacement

EDITORIAL

Cara yang paling efektif untuk melindungi organisasi Anda adalah dengan segera memblokir berbagai known threats tanpa mempengaruhi kinerja jaringan secara keseluruhan, baik dari sisi jaringannya itu sendiri, aplikasi maupun di sisi endpoint-nya. Hal ini biasanya dapat dilakukan dengan mengimplementasi solusi next generation firewall, secure email gateways, web application firewall, endpoint security client untuk menghentikan malware, gangguan keamanan, botnets dan lainnya pada infrastruktur jaringan.

Namun, serangan zero-day (unknown threats) dan ancaman malware dengan level tingkat lanjut seringkali direkayasa untuk menghindari solusi keamanan tradisional. Teknologi advanced threat detection harus ditambahkan untuk secara otomatis mendeteksi ancaman yang sebelumnya tidak diketahui dan menciptakan basis data penilaian untuk dapat ditindaklanjuti. Sandboxing dikenal karena fungsinya dalam menguji item yang asalnya tidak diketahui, pada satu lingkungan yang aman dan dijalankan untuk melihat bagaimana perilakunya, dalam mengubah hal yang tadinya tidak diketahui menjadi diketahui. Ketika teridentifikasi sebagai sebuah bentuk ancaman yang baru, hal ini perlu dengan segera untuk diatasi. Dapat ditangani secara otomatis dengan menggunakan intelligence sharing antara perangkat keamanan detection maupun prevention secara langsung, diakhiri dengan teknik mitigasi, kombinasi antara manusia dan teknologi yang bekerja sama.

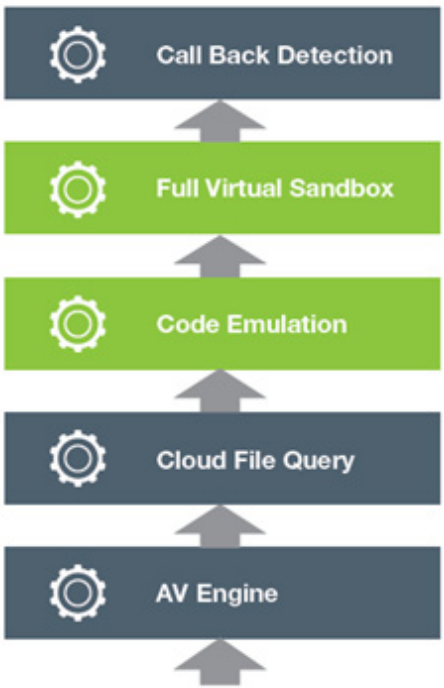
Menyambung bahasan keamanan jaringan pada bulletin terdahulu (Edisi 39) tentang “Mengatasi Perkembangan Cyber Threats dengan Advanced Threat Protection System”, di bulletin edisi kali ini yang kami beri judul “Advanced Threats, Advanced Solutions: Mengintegrasikan Sandbox Ke Dalam Infrastruktur Anda” mencoba untuk menjelaskan betapa pentingnya elemen teknologi threat detection Sandbox sebagai puzzle yang melengkapi infrastruktur perangkat keamanan jaringan dalam melindungi organisasi Anda terhadap serangan-serangan cyber baru di masa yang akan datang.

Dasa Aprily Ardy
Technology Development Supervisor

PT. Autojaya Idetech
PT. Solusi Periferal

Advanced Threats, Advanced Solutions: Mengintegrasikan Sandbox Ke Dalam Infrastruktur Anda

Di dunia komputer, istilah sandboxing umum diartikan sebagai sebuah lingkungan dimana selain sifatnya yang aman dan terisolasi, merupakan lingkungan bagi tim peneliti dalam menjalankan berbagai macam malicious code yang ada dan melakukan analisa lanjutan terhadapnya.



Gambar 1. FortiSandbox Technologies

Konsep inilah yang umum diterapkan pada perangkat-perangkat keamanan jaringan dewasa ini, mereka dapat mengeksekusi dan memeriksa lalu lintas jaringan terhadap kemungkinan adanya malicious code yang tidak mampu dideteksi oleh perangkat keamanan jaringan tradisional. Dengan kemampuannya meniru sistem operasi end-user secara virtual, perangkat sandbox mengeksekusi malicious code tersebut dan mengamati aktivitas yang terjadi. Apabila dalam aktivitas-aktivitas tersebut ada yang membahayakan terhadap konfigurasi sistem operasi, sandbox dapat mengambil keputusan untuk tidak melewatkan malicious code tersebut ke jaringan.

Teknologi awal perangkat sandbox hanya dapat memindai file-file yang bersifat executable (.exe & .dll), tetapi dengan pesatnya perkembangan teknologi sandboxing hingga saat ini mampu memindai bermacam file extension tambahan, seperti Adobe Flash, JavaScript, Microsoft Office dan lainnya.

Solusi mutakhir sandboxing dewasa ini memungkinkan kemudahan integrasi ke dalam infrastruktur perangkat keamanan jaringan yang sudah ada, dengan mekanisme otomasi terhadap malicious code dan melakukan proteksi yang diperlukan di titik awal malicious code tersebut terdeteksi.

Mengapa Sandboxing Penting?

Jika teknologi sandboxing sudah ada sejak lama, kenapa baru sekarang dianggap menjadi satu bagian penting dalam infrastruktur keamanan jaringan? Jawabannya cukup mudah, para penjahat dunia maya tidak akan pernah puas dengan satu dua kemenangan teror cyber yang ada, mereka terus mengasah kemampuan dan berinvestasi dalam mengembangkan teknik dan tools-tools baru untuk menyebarkan malicious wares. Dengan tujuan tertentu, mereka akan terus menemukan cara-cara

baru dalam mengeksploitasi kelemahan yang ada, baik di sisi pengguna maupun di sisi perangkat lunak. Solusi sandboxing saat ini, dapat membantu anda tidak hanya menemukan ancaman-ancaman tersebut dengan cepat, namun juga meminimalisir dan bahkan mengatasinya.

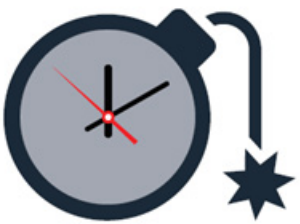
Advanced Persistent Threats (APT)

APT dikembangkan secara spesifik dan terstruktur, dengan target serangan yang jelas. Mereka dapat menghindari teknik deteksi tradisional dengan memanfaatkan kerentanan (lubang keamanan yang tidak di-patch), malware yang sebelumnya tidak dikenal (zero-day threats), maupun URL hosting dan IP address yang sebelumnya tidak terdata mengimplikasikan serangan-serangan cyber. Dengan teknik coding yang mutakhir, mempunyai tujuan untuk mengacaukan sistem target serangan mereka dengan menghindari radar keamanan jaringan selama mungkin. Mereka juga mempunyai teknik rekayasa sosial tingkat tinggi untuk mengelabui pengguna, bahkan untuk pengguna yang paling sadar akan keamanan jaringan sekalipun.

Beberapa APT mempunyai teknik untuk menghindari deteksi keamanan (Advanced Evasion Techniques) seperti sandboxing, diantaranya:

- **Logic Bombs**

  Merupakan code yang tidak aktif setelah terinstalasi sampai adanya action tertentu yang memicunya untuk aktif.

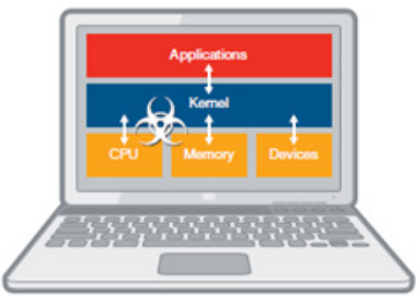


Gambar 2. Logic Bombs

  Logic bombs yang paling umum dikenal adalah time bombs, dan satu teknik logic bombs ini telah digunakan dalam serangan-serangan high-profile cyber yang terjadi di masa lalu. Dalam time bomb, bagian paling berbahaya dari code akan tetap tersembunyi hingga jangka waktu yang telah ditentukan. Sang penyerang menginstall malware di banyak sistem, dengan berharap agar tidak ketahuan sampai waktu tertentu, waktu dimana malware tersebut "meledak" secara bersama-sama. Teknik logic bombs lain membutuhkan interaksi manusia agar dapat berjalan, seperti mengklik mouse ataupun proses reboot untuk menunjukkan bahwa code benar-benar berada pada komputer pengguna, bukan di lokasi inspeksi virtual seperti sandbox. Dengan teknik logika seperti di atas, logic bombs bisa sulit terdeteksi, karena kondisi logika seperti itu tidak mungkin terpenuhi oleh teknologi sandbox di masa lalu.

- **Rootkit dan Bootkits**

  Malware dengan level tingkat lanjut sering mengandung komponen rootkit yang menumbangkan sistem operasi dengan kernel-level code untuk mengendalikan sistem secara penuh. Sandbox berpotensi rentan terhadap teknik penghindaran ini karena fitur monitor perilaku dari sandbox akhirnya juga dapat ditumbangkan. Lebih jauh, rootkit dapat menginfeksi sistem dengan malware saat boot-up, sesuatu yang biasanya tidak diamati oleh sandbox.

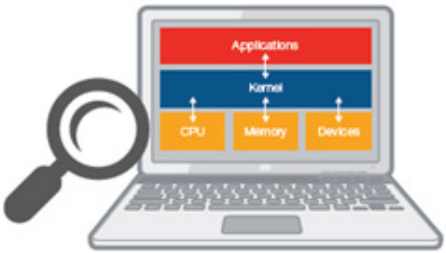


Gambar 3. Rootkit

- **Sandbox Detection**

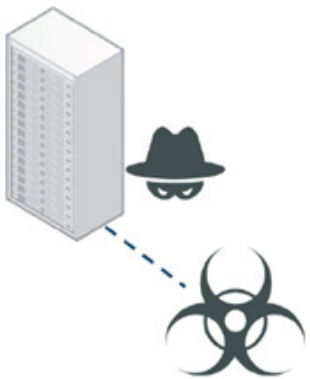
  Teknik penghindaran tingkat lanjut lainnya adalah kesadaran akan lingkungan sandbox itu sendiri. Beberapa APT mempunyai code berisi rutinitas yang mencoba untuk menentukan apakah ia berjalan di lingkungan virtual (sandbox) atau mungkin memeriksa fingerprints dari lingkungan virtual yang ada terhadap vendor-vendor sandbox tertentu. Jika code mendeteksi bahwa ia berada

di sandbox, tahapan eksekusi malicious code tersebut tidak akan dijalankan.



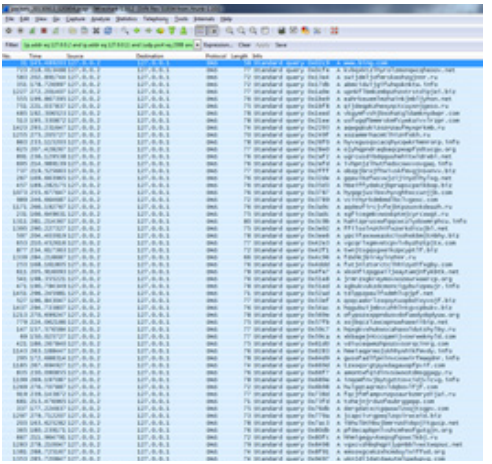
Gambar 4. Sandbox Detection

- **Botnet Command dan Control Window**
  Aktivitas botnet command & control (botnet C&C) biasa dimulai dengan sebuah dropper. Dropper merupakan code yang benar-benar bersih dalam struktur coding-nya, namun mempunyai rutinitas terhubung ke URL atau alamat IP tertentu untuk mengunduh file yang berisi perintah. Apabila server yang dituju oleh dropper tidak tersedia atau tidak aktif selama analisis yang dilakukan oleh sandbox, sandbox menganggap tidak ada aktivitas berbahaya untuk diamati.



Gambar 5. Botnet C&C

- **Network Fast Flux**
  Malware dengan level tingkat lanjut dapat menggunakan teknik fast flux atau domain generation algorithm (DGA) untuk mengubah alamat URL maupun IP yang akan digunakan oleh host yang terinfeksi dalam menghindari fitur identifikasi berbasis reputasi server botnet c&c. Ketika dalam observasi sandbox, host yang terinfeksi terlihat hanya menuju satu alamat tujuan, tetapi dalam waktu yang berbeda, host tersebut akan mencoba untuk berkomunikasi ke beberapa alamat yang berbeda untuk mengirim trafik malicious yang ada.



Gambar 6. Domain Generation Algorithm (DGA)

- **Encrypted Archives**
  Satu trik yang ketinggalan jaman metodenya namun masih sangat efektif adalah menyembunyikan malware ke dalam arsip yang terenkripsi, yang berarti file tidak dapat dibuka tanpa kata sandi yang diperlukan. Dengan sedikit social engineering, penyerang meyakinkan target untuk membuka arsip dan meluncurkan malware dengan memasukkan kata sandi yang dimaksud. Sandbox tidak dapat memasukkan kata sandi secara otomatis, yang berarti malware tidak akan berjalan selama pengamatan dan analisa sandbox berjalan.

Gambar 7. Encrypted Archives

Sandbox Replication

Begitu teknik-teknik penghindaran deteksi sandbox diatas dapat ditangani, barulah nilai dari sebuah sandbox dapat terlihat. Tujuan utama dari sandboxing adalah untuk sepenuhnya meniru perilaku dan bagaimana kode-kode berbahaya tersebut mencari jalan untuk masuk ke dalam organisasi. Idealnya, keluaran yang dihasilkan oleh sandbox harus identik dengan keluaran yang dihasilkan oleh kode-kode berbahaya tersebut ketika dijalankan di lingkungan pengguna akhir. Dalam prakteknya, menghasilkan keluaran yang identik sangat sulit dicapai karena banyaknya variabel yang terlibat. Seperti mencoba untuk menumbuhkan dua tanaman dengan benih biji yg sama variabel dalam jumlah komposisi air, cahaya, suhu dan tanah dapat menghasilkan keluaran yang berbeda.

- **Exploits dan Aplikasi**
  Advanced threat dapat disamarkan ke dalam bentuk file dokumen yang mengelabui aplikasi pengguna (Microsoft Word, Microsoft Excel atau Adobe Reader) untuk menjalankan kode berbahaya. Untuk meniru perilaku ini dengan handal, sandbox harus dijalankan melalui berbagai macam sistem operasi, yang masing-masing menjalankan beberapa versi aplikasi-aplikasi. Ini adalah proses trial-and-error yang banyak membutuhkan waktu dan biaya. Banyak vendor solusi sandbox mencoba mengatasi ini dengan menambahkan tenaga lebih ke dalam perangkat sandbox mereka, CPU yang lebih besar, lebih banyak RAM dan lebih banyak virtual machine agar proses trial-and-error tersebut dapat dipersingkat waktunya, namun langkah tersebut dinilai tidak efisien dan membutuhkan biaya yang lebih mahal. Langkah yang paling baik adalah menyeimbangkan sistem operasi dan aplikasi berdasarkan seberapa sering pengunaannya serta memilih lingkungan sistem operasi yang paling rentan terhadap ancaman serangan-serangan berbahaya.

- **32- vs. 64-bit, Windows XP vs. Windows 7/8/10**
  Kode 32-bit dapat berjalan baik di lingkungan sistem operasi 32-bit maupun 64-bit, sehingga para pembuat malware terus menggunakan 32-bit untuk memaksimalkan penyebaran infeksi mereka. Mayoritas malware saat ini masih dalam file .exe (executable), khususnya format Portable Executable 32-bit atau PE32. File PE32 dapat dijalankan di lingkungan Windows XP maupun Windows 7/8/10, sehingga sebagian besar perilaku berbahaya dapat diamati pada Windows XP (dimana XP tidak mendukung kode 64-bit) saja, tanpa perlu pengujian lebih lanjut pada Windows 7/8/10.
  Selain itu, kecuali dalam kasus tertentu yang sangat terbatas, Microsoft tidak lagi mendukung Windows XP. Ini berarti bahwa Windows XP akan berhenti menerima update patch keamanan, yang berarti semakin banyak lubang-lubang keamanan yang akan terbuka. Menjadikan Windows XP sebagai ladang subur untuk infeksi malware. Kabar baiknya, hampir semua teknik penghindaran malware yang menyerang Windows XP dapat dipicu untuk dideteksi dan di analisa oleh sandbox. Kabar buruknya, pengguna yang masih menggunakan Windows XP sebagai sistem operasinya menjadi rentan akan serangan-serangan yang khusus ditargetkan oleh si penyerang. Anda bisa yakin bahwa malware akan terus dikembangkan untuk menargetkan para pengguna yang belum beralih ke Windows 7/8/10, dengan data yang menunjukkan banyaknya pengguna Windows XP yang masih ada saat ini.

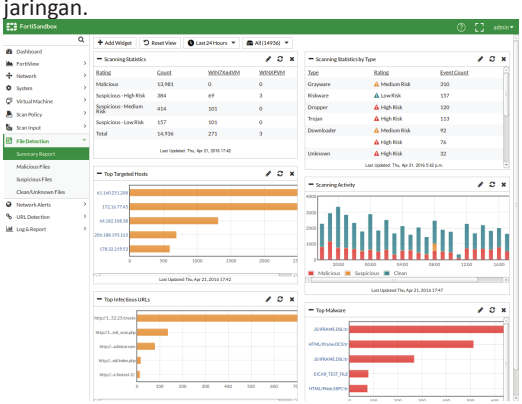
- **Android**
  Mobile malware berkembang dengan pesat dewasa ini, terutama di lingkungan Android yang sistem operasinya relative terbuka dan terfragmentasi. Meskipun insiden keamanan yang terjadi pada mobile hanya berdampak kecil sejauh ini, tetapi resikonya terus berkembang, terutama di beberapa wilayah negara tertentu di dunia. Seiring waktu, ancaman keamanan melalui smartphone dan tablet yang sudah menjadi bagian dari kehidupan sehari-hari akan semakin canggih dan kompleks.

- **Lebih dari Windows dan Android**
  Selanjutnya, dibutuhkan perangkat sandbox yang tidak hanya mendukung sepenuhnya kode 32-bit dan 64-bit, namun juga beberapa platform dari sistem operasi seperti Windows, Mac OS X, Linux,

Android, Windows Mobile, iOS, Blackberry dan Symbian.

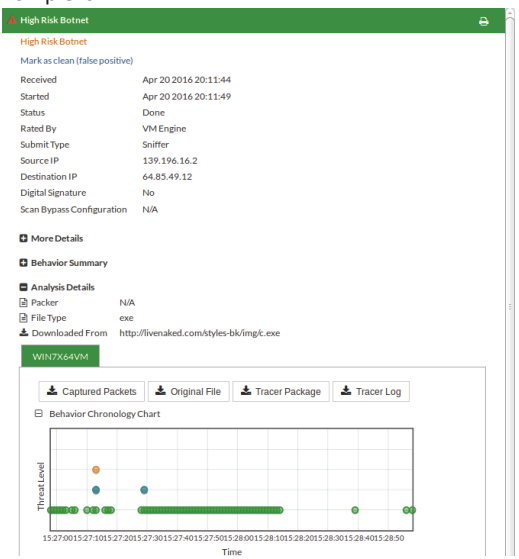
Advanced Integration-Solusi dari Fortinet

FortiSandbox dari Fortinet memberi penggunanya kemampuan untuk sepenuhnya mengintegrasikan teknologi sandbox ke dalam infrastruktur perangkat keamanan yang ada. FortiSandbox merupakan perangkat multi-layer sandbox dengan fitur-fitur pre-filtering seperti antivirus yang sangat komprehensif, proses CPRL, dan akses cloud terhadap FortiGuard Labs, lembaga riset global untuk ancaman keamanan jaringan.



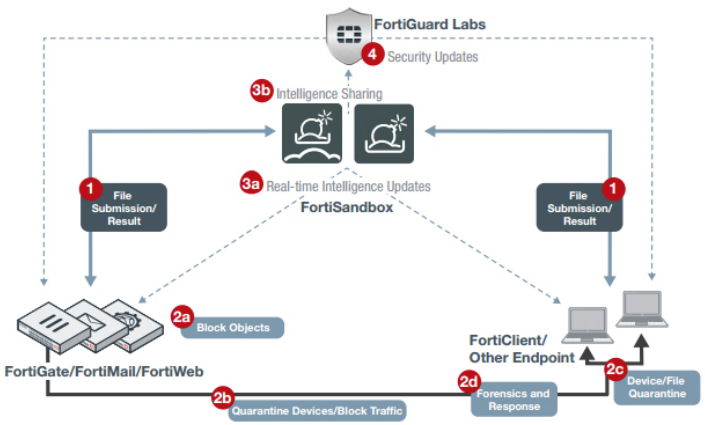
Gambar 8. Real-time Threat Status Dashboard

CPRL, kepanjangan dari Compact Pattern Recognition Language merupakan paten yang dimiliki oleh Fortinet dimana teknologi ini berkerja secara proaktif mendeteksi signature threat melalui metode deep inspection, yang caranya jauh melebihi pendeteksian secara konvensional. Hasil dari proses CPRL ini dapat mendeteksi 50000 lebih varian malware baik known maupun unknown. CPRL yang ada pada FortiSandbox secara proaktif mendeteksi signature baik APT (Advanced Persistent Threat) maupun teknik-teknik AET (Advanced Evasion Techniques) yang sudah kita bahas sebelumya, memfungsikan FortiSandbox untuk lebih fokus menganalisa threat yang jauh lebih kompleks.



Gambar 9. Detailed Malware Report

Dengan konfigurasi minimal, Fortisandbox dapat sepenuhnya berintegrasi dengan perangkat FortiGate,



Gambar 10. FortiSandbox Threat Mitigation Workflow

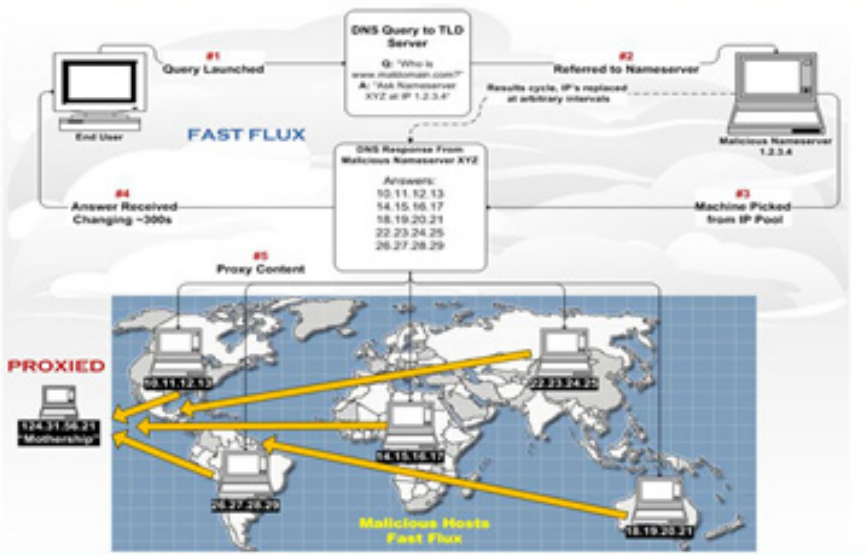
FortiMail, FortiWeb dan FortiClient Anda. Anda dapat mengkonfigurasi perangkat-perangkat ini untuk mengirim file (atau sekumpulan file) ke FortiSandbox untuk dianalisa, dan jika FortiSandbox menemukan file yang dianggap berbahaya atau berisiko, penilaian tersebut akan dikembalikan ke perangkat pengirim untuk dilakukan tindakan sesuai dengan kebijakan yang telah ditentukan.

Kesimpulan

Kenyataannya pada saat ini bahwa para pencipta malware sangat menyadari akan semua bentuk teknologi perangkat keamaan yang ada saat ini, dengan terus mengembangkan Advanced Persistent Threat yang bersifat kompleks serta menggunakan teknik-teknik penghindaran (Advanced Evasion Techniques) dengan harapan dapat melewati deteksi maupun mitigasi dari perangkat keamanan yang ada, agar berhasil mengirimkan malware-malware buatannya. Dengan begitu, proses deteksi pada perangkat keamanan haruslah bersifat inspeksi secara menyeluruh ke dalam bagian-bagian maupun perilaku jaringan yang potensial terhadap serangan.

Pendekatan terbaiknya adalah dengan teknologi kombinasi deteksi pencegahan malware secara proaktif (seperti Fortinet CPRL) untuk menghentikan sebanyak mungkin Advanced Persistent Threat termasuk yang dirancang menggunakan Advanced Evasion Techniques untuk mengelabui teknologi deteksi tingkat lanjut yang mutakhir sekalipun seperti sandboxing, dengan tetap memfungsikannya sebagai teknologi dalam menemukan serangan-serangan custom threat yang lebih kompleks lagi.

Selanjutnya, menyatukan metode pencegahan ke dalam proses deteksi lanjutan sebagai solusi menyeluruh yang mencakup semua vector potensial terjadinya serangan dan memfasilitasinya dengan respon tindakan kejadian adalah kuncinya. Dan ketika komponen solusi semacam itu diberikan oleh kelompok riset akan keamanan global seperti FortiGuard Labs, respon dan pembaharuan signature threats baik yang bersifat known maupun unknown akan menjadi jaminan perangkat keamanan, bahkan dengan potensi malware yang akan terus berkembang nantinya. Paling tidak, carilah vendor perangkat keamanan yang tidak hanya memberikan solusi, namun juga menyediakan laboratorium riset threats yang secara rutin berbagi informasi dan bisa berkolaborasi untuk memastikan bahwa infrastruktur perangkat keamanan yang bersifat heterogen pun dapat diperkuat tanpa meninggalkan celah yang dapat menimbulkan potensi serangan keamanan.



Gambar 6. Komponen Kunci dari FortiSandbox

*/ Penulis : Dasa Aprily Ardy (ardy@acsgroup.co.id)
Maulana Ibrahim (taufik.maulana@acsgroup.co.id)

Workshop

Integrator Hospitality Solution Day with Hikvision

Profit IT merupakan wadah/perkumpulan dari para Professional IT se Bali, kembali bersama ACS Group pada tanggal 12 Agustus 2017 lalu mengadakan acara Solution Day bersama HIKVISION dengan thema "INTEGRATOR HOSPITALITY"

Hikvision merupakan brand CCTV atau video surveillance terbesar di dunia dan Hikvision tetap fokus dalam bidang CCTV/ Video Surveillance. Dan pada. kesempatan yang baik ini Hikvison memperkenalkan Solusi Keamanan dan Pengawasan di bidang perhotelan/sektor Pariwisata kepada Profesional IT Bali. Keamanan dan kenyamanan merupakan syarat mutlak untuk sektor pariwisata sehingga pelancong bisa berlibur dengan tenang. Untuk itu Hikvision membeberkan solusi apa saja dari Hikvision yang bisa diterapkan pada sektor Pariwisata.

Pembahasan pada workshop ini meliputi :

- **Face Recognition (Pengenalan Wajah)**
  Dengan penggunaaan CCTV HIKVISION tidak hanya sekedar bisa memantau, dengan teknologi Face Recognition ini kamera Hikvision dapat mengenali wajah secara akurat, dan menangkap gambaran wajah secara jelas dan sekaligus memicu alarm, bila wajah yang dipantau merupakan wajah orang yang ada dalam daftar blacklist/pencarian.

- **License Plate Reconition**
  (Pengenalan plat kendaraan)
  Solusi Pengenalan plat kendaraan ini sangatlah cocok untuk kebutuhan manajemen parkir kendaraan. Dengan kemampuan membaca plat kendaraan, solusi ini mempermudah pihak manajemen mencatat secara otomatis plat nomer kendaraan yang masuk, beserta dengan waktunya. Disamping itu dapat juga mem-blacklist plat nomer tertentu dilengkapi dengan pemicu alarm. Dengan smart search dan Smart back up memudahkan untuk investigasi bila terjadi suatu perkara di wilayah parkir.

- **Under Vehicle Screening System (Pengamanan di bawah kendaraan)**
  Setiap tempat umum, seperti hotel, gedung perkantoran melakukan pemeriksaan kendaraan, baik di bagian bawah kendaraan. Dengan solusi pemindai dari Hikvision, dapat menangkap gambar dari bawah kendaraan. "Hal ini sangatlah membantu untuk pemeriksaan lebih cepat dan akurat." Ujar Robert Ridwan, Sales Manager Hikvision Indonesia

  Selain tiga solusi di atas Hikvision juga menjelaskan Solusi Panovie Multi lens Camera, Smart analytic Camera, Central Monitoring & Central Storage System, access Control dan juga Video Intercom. Yang akan menjadi pilihan solusi untuk industri pariwisata di Bali.

- **Hardisk Seagate Skyhawk**
  "Skyhawk menjadi pilihan yang tepat untuk media penyimpanan video, dengan penyimpanan maksimal 10TB" jelas Randu Atmaja, Product Specialist Seagate Indonesia.

Workshop

INDUSTRIAL MANUFACTURING Solution Day 2017

Wacana Solusi untuk Industrial Manufacturing di Surabaya dan sekitarnya

Surabaya, 23 Agustus 2017 bertempat di Hotel Swizz Beliin Manyar Surabaya, ACS Group dalam presentasinya di hadapan para peserta workshop kembali memaparkan Empat Pilar solusi Produk antara lain Automated Identification and Data Capture (AIDC), Information and Communication Technolongy (ICT), Surveliance and Security System, dan Profesional Services (Integration Service, Software Development, R n D).

Workshop kali ini, ACS Group menggunakan metode baru pada penyampaian materi dan peserta dibagi empat kelompok seperti kelas. Dalam waktu bersamaan, para pembicara langsung dibagi empat untuk memberikan materinya di setiap kelompok dan bergilir selama 30 menit waktu yang telah disiapkan.

Adapun pembicara dalam workshop ini antara lain perwakilan dari Zebra Technologies, Hikvision, Brother, Fortinet, dan team ACS Group.

Pembahasan setiap pembicara antara lain dari perwakilan Zebra Technologies dan team ACS Group memaparkan bahwa dengan hadirnya teknologi RFID ini sama sekali bukan untuk menggantikan teknologi Barcode. Dalam proses bisnis tertentu, penerapan Label/Tag RFID akan jauh lebih ekonomis dibandingkan dengan menggunakan teknologi barcode, terutama jika digunakan dalam proses close loop, dalam arti tag RFID ini dapat digunakan secara berulang kali dengan proses scanning yang cepat dan sekaligus berbeda dengan proses scanning barcode yang umumnya dilakukan secara satu persatu.

Dari perwakilan Hikvision dan team ACS Group mempresentasikan perangkat pengawasan dan keamanan yang canggih seperti kamera CCTV, speed domes, sistem kontrol akses dan alarm, serta lainnya. Beberapa keunggulan dari Hikvision diantaranya Face Recognition, (Pengenalan Wajah), Central Monitoring & Central Storage System, Smart Analytic Camera, Under Vehicle Screening Sytem (Pengamanan bawah kendaraan), dan License Plate Recognition (Pengenalan plat kendaraan). Solusi kamera Hikvison ini merupakan bagian yang mendukung solusi aplikasi yang telah dikembangkan oleh ACS Group. Aplikasi tersebut adalah GAS-V : Gate Access System – Vehicle. Aplikasi ini sudah diterapkan di salah satu perusahaan industri otomotif atau sejenisnya untuk melindungi kendaraan-kendaraan hasil produksi di area distribution center atau area QC pada saat keluar-masuk di area-area tersebut terhadap personal yang tidak memiliki otoritas.

Dari perwakilan Brother dan team ACS Group hadir dengan P-Touch labeling, solusi produk Printer label yang sangat durable include dengan pemotong otomatis. Brother memiliki Laminate Label khusus yang digunakan untuk pelabelan aset yang tahan terhadap gesekan, bahan chemical, sinar ultra violet, abrasi dan lain-lain. Solusi P-Touch dari Brother ini merupakan bagian dalam penerapan aplikasi Asset Management and Tracking System (AMTS), aplikasi ini dikembangkan sendiri oleh ACS Group. Dimana beberapa label aset diharuskan tahan terhadap lingkungan yang menatang tersebut.

Dari perwakilan Fortinet menyampaikan tentang Industri Manufaktur bergantung kepada apa yang umumnya disebut Industrial Control System (ICS). Dampak pelanggaran keamanan terhadap kebanyakan sistem teknologi informasi umumnya hanya terbatas pada kerugian finansial. ICS baru-baru ini menjadi sasaran menarik bagi terorisme dan perang cyber. Sumber keuangan dan sumber daya manusia yang tersedia bagi pelakunya bisa menjadi lebih besar dari pada Penjahat cyber konvensional. Bagaimana sekarang, terlepas dari tantangan ini dan banyak tantangan lainnya, Solusi Fortinet dapat membantu memastikan Keamanan dan keandalan ICS, dan khususnya mereka yang menggunakan Supervisory Control and Data Acquisition (SCADA) System.

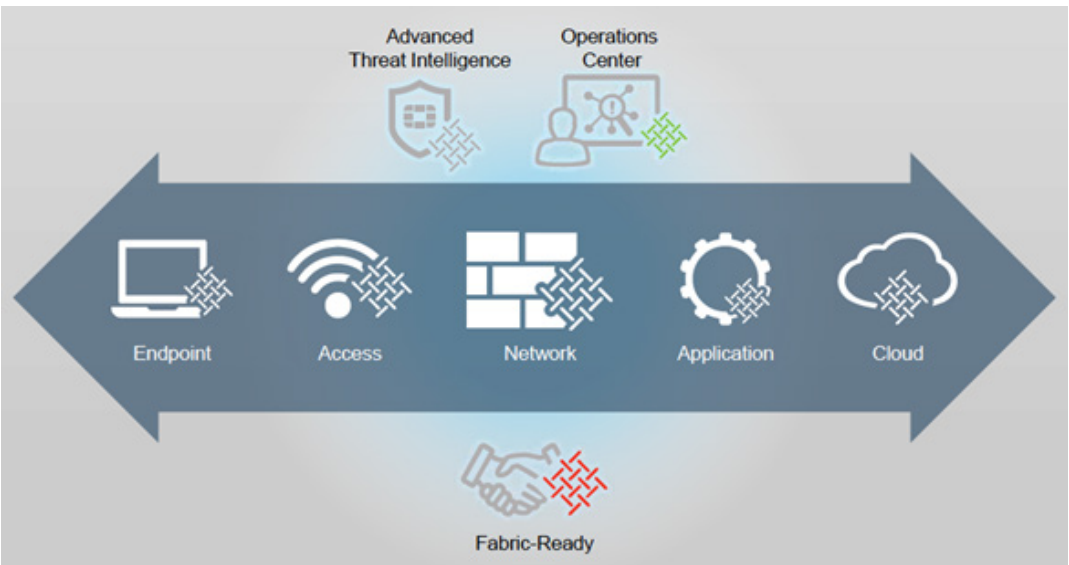
Analisa Log & Report Perangkat Fortinet Secara Terpusat

Di era sekarang ini dimana teknologi semakin berkembang pesat membuat jaringan perusahaan juga tumbuh pesat dan alur bisnis harus tetap dijaga supaya tetap berjalan dan terkontrol, hal ini yang membuat berbagai vendor keamanan jaringan berpikir dalam memberikan kemudahan melakukan kelola log dan report serta analisa data, selain tujuan utamanya adalah memberikan perlindungan jaringan atau network security yang komprehensif.

Fortinet sebagai vendor keamanan jaringan mempunyai solusi yang dikenal dengan "The Fortinet Security Fabric" dimana seluruh kebutuhan akan keamanan jaringan sudah disediakan oleh Fortinet sesuai dengan porsi dan kebutuhannya, dirancang khusus untuk menyesuaikan kebutuhan infrastruktur jaringan dalam menangkal pola serangan keamanan yang begitu cepat dan dinamis. Dengan Fortinet Security Fabric dapat meningkatkan performa dari setiap perangkat, karena dengan kolaborasi yang ada dari masing-masing perangkat Fortinet ini dapat memberikan respon dan waktu yang lebih cepat dalam mendeteksi ancaman yang ada.

Konsolidasi perangkat dalam sebuah jaringan sangat berdampak positif terhadap keamanan jaringan itu sendiri tapi ada yang perlu juga diperhatikan, yaitu kemudahan dalam mengatur dan mengakses log dan report dari setiap perangkat yang ada dalam infrastruktur jaringan kita, karena jika tidak kita akan kesulitan dalam mencari log dan report, hal ini akan menghambat kecepatan kita dalam melakukan investigasi setiap serangan dan mengambil tindakan terhadap jaringan kita secara cepat.

Dengan semakin bertambahnya infrastruktur



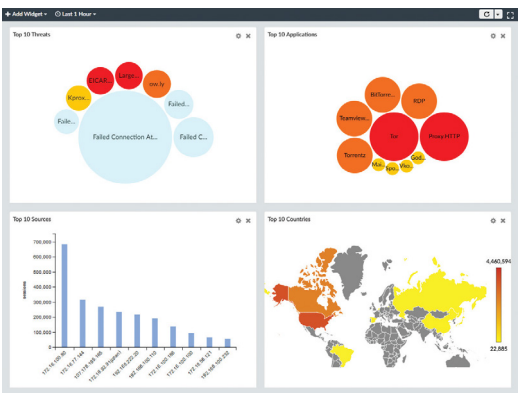
Gambar 1. Fortinet Security Fabric

Gambar 2. Konsolidasi Perangkat Fortinet dalam "Security Fabric"

perangkat jaringan, membuat kita berpikir lagi bagaimana caranya memanajemen atau mengelola log dan report dari perangkat-perangkat yang digunakan. Hal yang tentunya akan merepotkan ketika kita harus mengelola log atau report secara satu persatu di setiap perangkat, selain tidak efisien hal ini juga dapat menyebabkan menurunnya performa dari perangkat jaringan yang ada. Log dan report sudah menjadi bagian yang sangat penting yang dibutuhkan untuk melakukan analisa dalam permasalahan ancaman kemanan jaringan yang sedang terjadi, serta data yang realtime juga sangat diperlukan sebagai bahan analisa dalam melakukan investigasi terhadap permasalahan atau ancaman jaringan yang terjadi.

Di Fortinet kita mengenal yang namanya FortiAnalyzer, FortiAnalyzer adalah salah satu solusi produk dari Fortinet yang dapat melakukan penarikan data log (network security logging) dan report (reporting appliances) yang terintegrasi dengan semua produk Fortinet. Dengan adanya FortiAnalyzer kita dapat mengelola log dan report antar perangkat jaringan dengan begitu mudah, serta melakukan analisa dari apa yang sedang terjadi dalam suatu jaringan.

Selain dalam bentuk appliance, FortiAnalyzer juga tersedia dalam bentuk virtual machine. Untuk versi virtual-nya FortiAnalyzer dapat berjalan pada platform VMware vSphere, Xen, KVM maupun Hyper-V. Dengan tidak adanya perbedaan dan kemampuan antara versi appliance maupun versi virtual, FortiAnalyzer memberikan pengawasan monitoring yang lengkap dengan hasil report yang dapat disesuaikan dengan kebutuhan.



Gambar 3. FortiAnalyzer Dashboard

FortiAnalyzer dengan sistem log dan report terpusat

atau tersentralisasi, memberikan alert secara realtime serta investigasi dan response terhadap event dari apa yang sedang terjadi, serta kemudahan dalam mereview log yang sudah dapat dikonversi dalam bentuk dokumen HTML/CSV/XML/PDF.

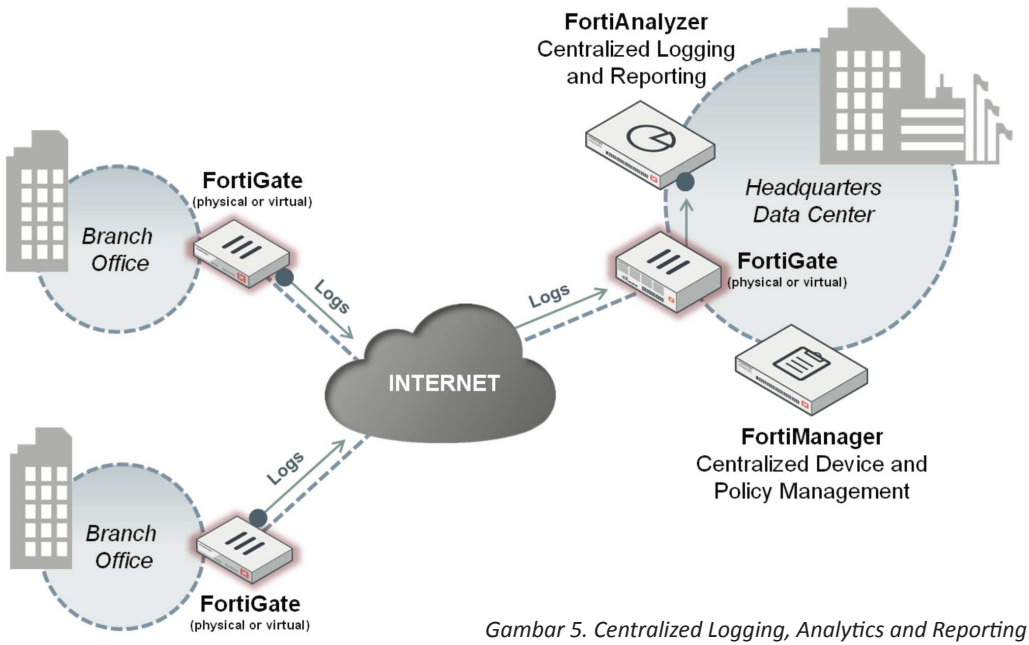
Gambar 4. FortiAnalyzer Threats Statistics

Dengan system log yang terpusat FortiAnalyzer mampu memberikan log dan analisa report dari masing-masing perangkat jaringan terhadap ancaman yang terjadi secara global, tentunya hal ini akan memberikan kemudahan bagi seorang IT administrator dalam melakukan pemeliharaan perangkat jaringan, terlebih perusahaannya memiliki banyak cabang di masing-masing tempat yang berbeda.

Beberapa fitur yang dimiliki oleh FortiAnalyzer :

- **Sentralisasi Log & Report Perangkat**
  Log dan report dari perangkat-perangkat Fortinet yang terpusat dengan kemudahan mengakses hanya melalui satu manajemen konsol. Termasuk didalamnya aktivitas trafik jaringan, system event, viruses, attacks dan web filtering events. Hal ini dapat memudahkan seorang IT administrator dalam memonitor setiap lalu lintas jaringan yang ada di perangkatnya.

- **Otomasi Indicators of Compromise (IOC)**
  Melakukan scanning log keamanan pada FortiGate untuk mengidentifikasi trafik dengan pola yang mencurigakan. Dengan proses deteksinya yang akurat, terus menjaga dan memonitor akan kemungkinan serangan Advanced Persistent Threat (APT) yang ada.



Gambar 5. Centralized Logging, Analytics and Reporting

- **Tampilan Aktivitas Jaringan Secara Realtime Maupun Historis**
  Menampilkan summary dari aktivitas jaringan yang terjadi, baik dari sisi aplikasi, alamat asal, alamat tujuan, alamat website, ancaman keamanan, hingga sistem dan administrative events.

- **Integrasi Dengan Fortinet Security Fabric**
  Berkorelasi dengan log-log pada setiap perangkat Fortinet seperti FortiGate, FortiSandbox, FortiMail dan lainnya untuk analisa log dan visibilitas yang lebih dalam.

- **Custom Report**
  Dengan 28+ lebih template contoh report yang langsung dapat digunakan, kustomisasi report juga dapat dibuat berdasarkan 300+ lebih chart yang sudah ada. Tipe report bisa dalam bentuk HTML/CSV/XML/PDF yang fleksibel sesuai kebutuhan.

- **Pencarian Log Untuk Analisa Forensik**
  Dapat melakukan pencarian arsip log untuk kebutuhan analisa forensik secara historis

- **Monitoring & Alert**
  FortiAnalyzer secara proaktif memonitor aktivitas jaringan secara realtime untuk mengidentifikasi issue, masalah, maupun serangan jaringan. Monitoring tersebut didukung dengan notifikasi alert secara otomatis, agar dapat dilakukan respon tindakan yang diperlukan.

*/ Penulis : Dasa Aprily Ardy (ardy@acsgroup.co.id)
Maulana Ibrahim (taufik.maulana@acsgroup.co.id)

KOLOM KETAWA

MEMBELI ALAT PANCING

Di suatu sore yang cerah, ada seorang wanita yang bernama Bu Arsi. Bu Arsi disuruh oleh suaminya untuk membeli alat pancing dan senarnya. Sebenarnya, Bu Arsi sama sekali tidak tahu banyak tentang alat-alat pancing. Jadi, dia hanya mengambil satu buah pancing dan senar yang terlihat menarik baginya.

Setelah itu, dia membayar semua barang yang dibelinya di loket kasir. Di belakang meja, terdapat seorang karyawan laki-laki yang sedang mengenakan kacamata hitam. Pak Joyo namanya. Karena Bu Arsi tidak mengetahui kualitas pancing dan senar yang dibelinya, dia bertanya kepada Pak Joyo.

Bu Arsi : "Maaf, Pak. Saya ingin membeli pancing dan senar yang bagus. Apakah yang saya ambil ini sudah berkualitas bagus?" (Bu Arsi bertanya sambil menyodorkan pancing dan senar yang dibelinya.)

Pak Joyo : "Maaf, Bu. Saya seorang tunanetra. Namun, saya bisa mengetahui merek dan kualitas barang jika Anda menjatuhkan barang tersebut ke atas meja kasir ini."

Bu Arsi : "Ah, masa sih, Pak? Saya coba, ya." (Bu Arsi langsung menjatuhkan pancing dan senar pancing yang dipilihnya ke atas meja kasir.)

Pak Joyo : "Dari suaranya, ini adalah joran pancing grafit dan senar gulungan Zebco 202. Kualitasnya bagus, Bu."

Bu Arsi : "Wah, hebat sekali, Anda. Baiklah, saya akan membelinya. Berapa harga totalnya?"

Pak Joyo : "Totalnya Rp300.000,00 saja, Bu."

Sembari mengeluarkan uang, Bu Arsi tidak sengaja kentut. Bunyinya sangat nyaring dan baunya cukup menyengat. Namun, dia malu untuk mengatakannya kepada Pak Joyo. Akhirnya, Bu Arsi memilih untuk diam saja.

Pak Joyo : "Maaf, Bu. Keseluruhan harganya menjadi Rp400.000,00."

Bu Arsi : "Lo, kok harganya naik, Pak?"

Pak Joyo : "Iya, Bu. Selain membeli pancing dan senarnya, Anda ternyata juga baru saja mengambil sebuah peluit pemanggil ikan yang harganya Rp50.000,00 dan sebuah umpan bau pemanggil ikan yang harganya Rp50.000,00. Jadi totalnya Rp400.000,00."

Bu Arsi : @#$#%$^^%

MENYAMBUT HUT KE 10th GEBYAR AUTO-ID

Setelah melalui masa yang panjang dan telah berhasil melewati berbagai kesulitan GEBYAR AUTO-ID pada bulan Desember yang akan datang akan memasuki usia yang ke 10. Dalam rangka menyambut hari ulang tahun yang ke 10 ini GEBYAR AUTO-ID akan membagikan hadiah yang menarik bagi pembaca setia di seluruh Indonesia

2 Hadiah Utama yaitu **2 Smartphone** serta **50 souvenir** yang menarik yang dapat anda menangkan secara mudah.

Anda cukup mengisi quiz yang telah kita sediakan serta mengisi quetioner dari kami, dan jangan lupa tuliskan data anda secara jelas, seperti nama, company, jabatan, no. HP, dan e-mail. Foto/scan halaman yang sudah anda jawab ini secara baik dan kirim by email ke **acs.marcom@acsgroup.co.id** paling lambat tanggal **25 Oktober 2017**. Jawaban yang **TEPAT** dan **TERBAIK** akan kami kumpulkan serta kami undi. Keputusan panitia untuk pemenang tidak dapat diganggu gugat.

QUETIONER

Pilih jawaban anda dan lingkari serta isilah pertanyaan di bawah ini,

1. Menurut Anda apakah isi dari Bulletin kami sudah informatif ?
   A. Sangat Dimengerti
   B. Dimengerti
   C. Biasa Saja
   D. Sulit Dimengerti

2. Dari Buletin kami ini, Apakah Anda mendapatkan informasi-informasi yang bermanfaat bagi Anda dan Perusahaan ?
   A. Sangat Bermanfaat
   B. Bermanfaat
   C. Biasa Saja
   D. Tidak Bermanfaat

3. Infomasi apa yang menurut Anda cukup menarik di Bulletin kami ?
   .....
   .....

4. Mohon saran/masukkan dari Anda mengenai Bulletin kami ?
   .....
   .....
   .....

QUIZ CARI KATA

Cari kata-kata di samping yang ada di kolom bawah. Anda dapat melingkari/stabilo kata yang sesuai secara vertikal, horisontal maupun diagonal.

FORTISANDBOX
SCANNERS
BARCODE
CAMERA CCTV
ACCESS POINT
RFID SYSTEMS
RUGGEDNESS
LABEL PRINTERS
WIRELESS NETWORKS
MOBILE COMPUTER

M	Q	J	R	K	A	I	S	C	C	T	X	B	A	N	T	A	W	V	B
O	J	O	F	U	F	U	K	Y	U	L	M	B	A	K	Y	C	K	H	F
B	M	B	F	Z	R	O	R	O	K	I	D	U	N	G	A	C	O	Q	S
A	J	A	D	U	F	M	O	B	I	L	E	C	O	M	P	U	T	E	R
N	T	Y	J	X	I	C	W	B	B	C	S	L	E	K	L	A	U	I	E
K	S	K	V	C	D	L	T	J	K	L	R	R	W	R	H	K	L	C	T
U	T	U	I	A	S	O	E	D	O	C	R	A	B	A	V	C	C	T	N
S	N	R	A	S	Y	Y	N	A	O	A	N	A	M	X	T	R	J	H	I
M	I	E	V	F	S	O	S	I	C	A	L	I	O	T	C	Y	J	A	R
A	O	T	A	H	T	P	S	C	H	J	P	B	B	Y	C	R	E	W	P
K	P	A	L	A	E	D	E	R	E	T	D	S	I	A	A	D	H	B	L
O	S	D	L	D	M	S	L	M	E	N	D	O	L	E	R	O	S	X	E
F	S	G	E	R	S	F	E	K	A	N	T	O	E	Z	E	X	V	R	B
J	E	H	N	U	S	A	R	S	E	N	N	A	L	T	M	S	S	C	A
W	C	J	J	R	F	S	I	T	U	O	L	E	S	C	A	G	S	G	L
X	C	C	O	O	R	T	W	U	I	O	P	U	R	T	C	B	A	Q	W
V	A	S	X	C	R	U	O	P	R	E	W	C	X	S	Z	B	G	W	T
Z	C	Z	G	O	P	Y	A	C	A	S	W	F	T	V	B	N	R	T	E
A	G	A	F	B	U	L	Y	A	B	T	L	I	R	Z	Q	X	G	M	V
Q	L	A	U	J	A	J	E	S	S	E	N	D	E	G	G	U	R	D	D

Nama : .....
Perusahaan : .....
Jabatan : .....
No. Hp : .....
Email : .....

PRODUCT HIGHLIGHT

Aruba
Access Point 300 Series

Produk solusi untuk sektor industri : Semua industri.

Access Point Aruba 300 series Wave 2 merupakan access point indoor yang memiliki performa yang tinggi untuk lingkungan medium density.
Jalur akses Wave 2 ini memberikan multi-user MIMO (MU-MIMO) aware ClientMatch yang berguna untuk meningkatkan efisiensi pada jaringan dan men-support kebutuhan penanganan dari kepadatan perangkat-perngkat yang terus meningkat pada jaringan Anda.
Access Point dengan Dual Radio 802.11ac dan sudah Built-in Bluetooth Low-Energy (BLE) radio.

Fortinet Advanced Threat Protection Framework

memberikan end-to end perlindungan di seluruh rantai serangan, untuk keamanan tanpa ada kompromi. Fortinet terdiri dari tiga elemen, bekerja secara bergandengan tangan yaitu :

- Mencegah Serangan
- Mendeteksi dan Menganalisis Ancaman
- Mengurangi Dampak dan Meningkatkan Perlindungan

Terbagi menjadi:

1. FortiGate
2. FortiSandbox
3. FortiMail
4. FortiClient
5. FortiSwiitch
6. Dan lain-lain

Aruba
Switch 2540 Series

Produk solusi untuk sektor industri : Semua industri.

Aruba 2540 Switch series dioptimalkan untuk me-manage pengguna ponsel. Dilengkapi dengan manajemen keamanan dan jaringan yang canggih-Aruba ClearPass Policy Manager dan Aruba AirWave - Layer 2 access switch ini mudah digunakan dan dikelola. Dengan dukungan dari cloud-based central Aruba, Anda dapat dengan cepat mengatur situs cabang pada jarak jauh dengan sedikit atau tanpa dukungan IT. Aruba 2540 memberikan fitur entry level untuk kampus perusahaan, SMB dan kantor cabang. Produk ini menyediakan uplink built-in 10GbE, model QoS, static dan RIP routing, IPv6, PoE+ yang kuat dan tidak memerlukan lisensi perangkat lunak.

Aruba
Switch 2530 Series

Produk solusi untuk sektor industri : Semua industri.

Aruba Switch 2530 series merupakan switch yang menyediakan keamanan, keandalan, dan memiliki kemudahan dalam penggunaannya untuk perusahaan, kantor cabang, dan UKM.
Rangkaian switch ini menghadirkan kemampuan Layer 2 penuh dengan peningkatan access security, ACLs, traffic priority, sFlow, dan dukungan host IPv6 yang optimal.
The Aruba 2530 Switch Series menawarkan fleksibilitas uplink dengan empat Gigabit atau dua 10 Gigabit Ethernet uplinks pada beberapa model 24 dan 48-port.

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

Business WiFi
MADE SIMPLE
Through Your Smartphone

OfficeConnect OC20

GET IT ON Google play

Download on the App Store

OfficeConnect Mobile Apps

Hewlett Packard Enterprise

SiS SiSTECH KHARISMA

FAREWELL

Pak Acksan 27 Tahun

mengabdi bersama ACS Group

Salah satu bagian dari keluarga besar ACS Group yaitu Bapak Acksan kini telah memasuki masa pensiun dan berhenti dari tugas beliau sebagai salah satu staff gudang. Masa pengabdian beliau selama 27 tahun telah dilakukan dengan setia, jujur dan loyal terhadap perusahaan dan beliau merupakan pegawai yang pertama dari ACS Group yang memasuki masa pensiun di bulan Agustus 2017. Selamat menikmati masa pensiun bersama keluarga tercinta dan sehat selalu.

Kunjungi kami
di **booth I02** ACS GROUP
dalam event
B2C commerce INDONESIA
yang diselenggarakan pada tanggal
10-11 Oktober 2017
di Balai Kartini Jakarta, Indonesia

TRAINING
Product Update Hikvision

Pada tanggal 1 Agustus 2017 bertempat di Gedung ACS Group Jl. Gunung Sahari Raya, seluruh Sales, staf Marketing dan beberapa Engineer ACS Group mendapatkan training product update dari Hikvision. Hikvision merupakan perusahaan penyedia produk dan solusi keamanan terkemuka di dunia. Produk-produk Hikvision diantaranya adalah kamera CCTV analog , kamera IP , kamera Analog HD, Alarm dan lain-lain. Para sales dibekali berbagai info produk baru, spesifikasi serta penerapan solusinya di lapangan. Training seperti ini juga diberikan kepada para sales dan engineer di cabang Denpasar - Bali yang berlangsung pada tanggal 12 Agustus 2017.

Training ini disampaikan oleh Eko Purnomo - Hikvision Pre- Sales Manager.

SHARING KNOWLEDGE
Product Aruba

ACS Group melakukan sharing product knowledge produk Aruba kepada para staff di salah satu perusahaan cigarete terbesar di Indonesia pada tanggal 15-16 Agustus 2017. Sharing knowledge ini membahas tentang Aruba Wireless Controller, Access Point, AirWave Management Platform beserta fitur-fiturnya dalam rangka professional services di tempat mereka.

Tea Walk PHRI 2017
Gunung Mas Puncak Jawa Barat

PHR(Perhimpunan Hotel dan Restoran Indonesia) merupakan asosiasi non-profit dari pemilik hotel dan restoran serta para profesional yang memfokuskan kegiatannya untuk pengembangan dan pertumbuhan sektor-sektor penting industri pariwisata di Indonesia.

Pada tanggal 13 Agustus 2017 PHRI bersama seluruh anggotanya se Jabodetabek mengadakan acara TEA WALK PHRI bertempat di Gunung Mas Puncak - Jawa Barat. Acar ini diikuti kurang lebih 600 peserta dan ACS Group sebagai mitra dari PHRI ikut berpartisipasi sebagai salah satu sponsor pada acara ini.

Acara ini diawali dengan sambutan dari Ketua umum PHRI yang diwakili oleh Ketua PHRI DKI Jakarta Khrisnadi dan dibuka oleh Gumilar Ekalaya dari Dinas Pariwisata dan Kebudayaan DKI Jakarta.

Para peserta mendaftarkan diri di booth ACS untuk mendapatkan goodie bag yang diberikan oleh beberapa vendor ACS yang turut berpartisipasi pada acara ini diantaranya TechData/Fortinet, Hikvision, Brother, Honeywell, Noah Arkindo dan Helios.

Tips dalam mengantisipasi Web Defacement

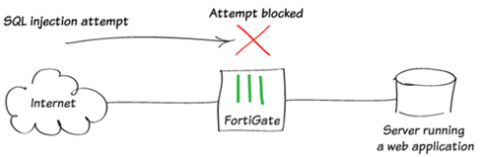
Web defacement adalah salah satu tantangan keamanan terbesar bagi setiap organisasi yang terkait dengan bisnis online. Web defacement biasanya dilakukan oleh hacker yang masuk ke server web dan mengganti sebagian halaman situs web khususnya main page ataupun merubah secara keseluruhannya. Sasaran umum dari serangan web defacement dan telah terjadi adalah pada situs web pemerintahan, situs web perbankan dan situs web perusahaan bahkan situs web perusahaan telekomunikasi yang terbesar di Indonesia dapat terkena serangan Web defacement.

Berikut adalah sedikit tips dalam mengantisipasi web defacement:

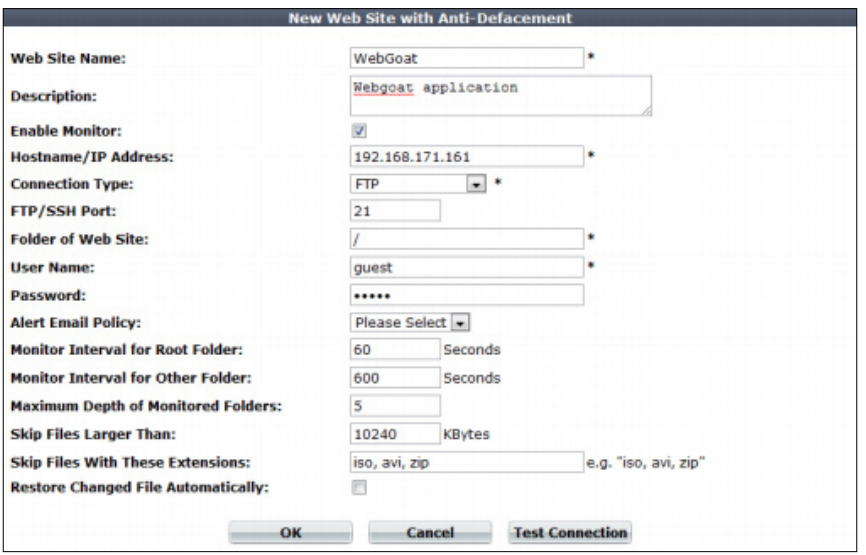
1. Lakukan Audit keamanan jaringan data secara berkala.

Para hacker selalu mencoba untuk mengeksploitasi kerentanan atau celah keamanan yang tidak ditambal dengan benar. Bentuk kerentanan yang paling sering terjadi dan menjadi kesalahan yang paling mendasar adalah penggunaan port yang terbuka untuk terhubung ke server tanpa log on, dan salah satu implikasi terjadinya serangan Remote code execution dimana penyerang menjalankan kode berbahaya melalui koneksi yang terbuka.

Remote Code Execution adalah kemampuan penyerang untuk mengeksekusi kode mereka di server lain, dengan cara yang tidak dimaksudkan oleh pemilik aplikasi. Eksploitasi yang berhasil terhadap kerentanan ini memungkinkan penyerang mengirimkan muatan berbahaya (malicious), yang bervariasi. Temuan awal menunjukkan bahwa penyerang secara aktif menargetkan kerentanan ini untuk tujuan penyelidikan, dan dalam beberapa kasus untuk penyebaran malware.



Pemeriksaan rutin dan pengujian penetrasi sangat membantu dalam mengevaluasi keamanan infrastruktur IT mulai dari kelemahan sistem operasi, layanan dan aplikasi, konfigurasi yang tidak tepat, atau perilaku end user yang berisiko guna melindungi sistem dengan lebih baik.



Sudah seharusnya melakukan Review, Testing, Simulasi secara berkala terhadap keamanan pada Server yang dikelola. Bahkan bisa bekerja sama dengan Hacker (White Hacker yang dapat dipercaya reputasinya) untuk melakukan Audit terhadap implementasi Security Web Server yang kritikal.

2. Proteksi terhadap serangan injeksi SQL.

Injeksi SQL adalah pendekatan yang sangat klasik namun masih populer di kalangan penyerang. Teknik ini memungkinkan penyerang untuk mengambil informasi penting dari database Web server. Dengan pernyataan SQL yang dimodifikasi, penyerang mungkin dapat merusak data yang ada, menghancurkan data di sistem, atau bahkan mengekstrak keseluruhan database sistem.

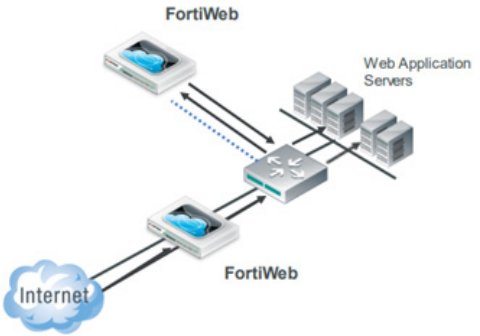
Banyak aplikasi web mengambil data masukan pengguna dari sebuah formulir, dan data masukan pengguna dimasukkan langsung ke dalam pernyataan SQL di dalam aplikasi Web.

Tapi metode terbaik untuk mencegah injeksi SQL adalah dengan menghindari penggunaan SQL yang dihasilkan secara dinamis dalam kode. Sebagai gantinya, gunakan prosedur tersimpan atau stored procedures.

3. Proteksi terhadap serangan Cross-Site Scripting (XSS).

Serangan Cross site scripting adalah ketika penyerang mencoba untuk melewatkan kode script ke dalam isibentuk web untuk mencoba menjalankan kode yang tidak seharusnya di situs web. Hal ini memungkinkan penyerang untuk menyematkan kode script di halaman web yang dapat melakukan berbagai tindakan yang tidak sah termasuk: mengubah tampilan halaman web, mencuri cookie session dari pengguna lain dari situs web atau bahkan sebagai sarana untuk membentuk serangan XSS di situs-situs lain.

Untuk mencegah serangan XSS dengan mencegah pengguna menyuntikkan kode melalui formulir web. Salah satu praktik terbaik untuk mencegah serangan cross site scripting adalah dengan Encode Output yang benar.



Salah satu serangan XSS yang paling umum adalah mencuri cookies. Skrip berbahaya yang dibuat menyebabkan browser mengirim semua cookie ke setiap pengunjung domain situs web Anda ke penyerang. Hal ini dapat mengakibatkan penyerang dapat mencuri kredensial semua pengguna.

Pencegahan yang bagus untuk melawan serangan ini adalah dengan menggunakan Cookie HTTP-Only. Dengan ini, cookie yang dikirim melalui HTTP tidak dapat diakses oleh Javascript melalui document.cookie, sehingga mencegah pencurian cookie melalui XSS.

Pencegahan terbaik lainnya adalah menggunakan Web Application Firewalls (WAF). Dengan WAF maka dapat memeriksa nilai masukan parameter yang berbahaya, modifikasi parameter Read-only, menyaring output yang berbahaya dan memblokir permintaan yang dicurigai.

4. Gunakan alat pemantauan dan pendeteksian Keamanan Data.

Menggunakan perangkat keamanan data yang handal yang diantaranya yang memiliki fitur Firewall, IDS (Intrusion Detection System) dan IPS (Intrusion Prevention System). Contohnya adalah dengan menggunakan perangkat keamanan data yang terpercaya dari vendor Fortinet. Perangkat ini tersedia dalam bentuk software, hardware security serta cloud base ini bisa secara otomatis mengirimkan email alert bahkan bisa mengirimkan alert via SMS jika sistem mendeteksi adanya serangan dari hacker.

Dengan Web Vulnerability Scanner dapat melakukan pemindaian atau scan tingkat kerentanan aplikasi web, melakukan analisa terhadap kemungkinan potensi serangan dan mendeteksi web application vulnerabilities. Dengan pemantauan dan pendeteksian yang baik akan tercapai Application Delivery terhadap ketersediaan dan akselerasi akan kinerja dari situs web aplikasi yang kritikal.

*/ Penulis : Irvan Kurniawan (irvan.kurniawan@acsgroup.co.id)

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

PRODUCT

- Bar Code (Label) Printers
- Bar Code Scanners
- Rugged Mobile Computers
- RFID Tags and RFID Readers
- Enterprise Wireless LAN
- Enterprise Wireless Broadband
- Security Networks
- Security System (CCTV, Access Control, Alarm System)
- Consumable: Customize Label and various Thermal Ribbon

PROFESSIONAL SERVICES

- Wireless RF Site Survey and Wireless RF Performance Audit
- Installation and Commissioning
- Hardware Repair (On Call) and Maintenance Contract
- 24 x 7 Support Ready (with SLA and annual contract)
- Manage Services
- Application Software Package, such as:
  - Asset Management and Tracking System (AMTS)
  - Document Asset and Tracking System (DATS)
  - Mobile Meter Reading Solution (MMR)
  - Agro Data Integration System (ADIS)
  - Stability Program System (Stab-Pro)
  - Gate Access System - Vehicle(GAS-V)
  - STOCK KEEPER
  - PRODUCTION TRACKING

INDUSTRY SOLUTION

- Manufacturing
- Transportation & Logistics
- Retail & E-commerce
- Fast Moving Consumer Goods
- Hospitality
- Financial Services
- Education & Healthcare
- Agriculture & Mining

BUSINESS PARTNERS

ZEBRA PREMIER SOLUTION PARTNER
Honeywell PLATINUM PLUS PERFORMANCE PARTNER Printer Specialist
POINTMobile
brother at your side
aruba a Hewlett Packard Enterprise company
Seuic
FORTINET
Cambium Networks
Extreme Connect Beyond the Network
HIKVISION
AXIS COMMUNICATIONS
TelView CCTV SYSTEM
FARGO
BarTender BY SEAGULL SCIENTIFIC
ivanti

Jakarta (HO)
Perkantoran Gunung Sahari Permai #C03-05
Jl. Gunung Sahari Raya No 60-63 Jakarta 10610
Telp : +6221-4208221(H), 4205187(H)
Fax : +6221-4207903, 4207904, 4205853

Cikarang
Cikarang Square Blok E No 62, Jl. Raya Cikarang,
Cibarusah Km 40, Cikarang Barat, Bekasi
Telp : +6221.29612366, 29612367
Fax : +6221.29612368

Semarang
Grand Ngaliyan Square Blok B No.18,
Ngaliyan 50181, Semarang
Telp : +6224.76638092, 76638093
Fax : +6224.76638096

Surabaya
Komplek Ruko Gateway Blok D-27
Jl. Raya Waru, Sidoarjo 61254
Telp : +6231-8556277(H); 8556278
Fax : +6231-8556279

Denpasar
Jl. Gatot Subroto I – XI, No 18
Denpasar Bali 80239
Telp : +62361-419284 (H)
Fax : +62361-424775