

# CDEF BULETIN

CYBER DEFENSE COMMUNITY INDONESIA

EDISI 01 TAHUN 2022

## MITRE ATT&CK FOR BETTER DETECTION AND PREVENTION

| Ewaldo Simon Hiras

## PROGRAM PERLINDUNGAN DATA PRIBADI UNTUK MENYELARASKAN KEAMANAN INFORMASI DAN PRIVASI

| Eryk Budi Pratama dan Ardhanti Nurwidya

## PENERAPAN SISTEM MONITORING 24/7 DAN AGENTLESS MONITORING MENGUNAKAN RASPBERRY PI

| Ramadhan Hidayat

## MENGUNAKAN LINKEDIN UNTUK “MENDARATKAN” PEKERJAAN DI CYBER SECURITY

| Mangatas Tondang

---

Atas berkat rahmat Allah Yang Maha Kuasa akhirnya CDEF Bulletin edisi terbaru berhasil dirilis. Atas nama tim Redaksi, kami mengucapkan terima kasih yang sebesar-besarnya kepada seluruh kontributor yang telah meluangkan waktu dan tenaganya untuk menyumbangkan ide dan pemikirannya melalui tulisan untuk CDEF buletin edisi kali ini.

Besar harapan kami bahwa tulisan-tulisan yang ada pada setiap edisi CDEF Buletin dapat ikut berkontribusi dalam membangun kemandirian bangsa terutama pada ranah keamanan siber. Harapan besar itulah yang kemudian selalu menggerakkan kami untuk terus berkontribusi dan menjaga konsistensi untuk merilis CDEF Buletin secara berkala.

Pada edisi kali ini terdapat begitu banyak informasi dan hal-hal menarik untuk dipelajari dan didiskusikan lebih lanjut. Mulai dari tips dan trik untuk memanfaatkan media sosial LinkedIn untuk mendapatkan pekerjaan idaman di bidang keamanan siber. Kemudian ada juga analisis mendalam terkait program Perlindungan Data Pribadi dan manajemen keamanan siber pada lingkungan yang berbasis Cloud.

Beberapa topik lain yang tidak kalah serunya juga ada seperti penggunaan Raspberry Pi sebagai Sistem Monitoring Keamanan, penggunaan Scoutsuite untuk keamanan Cloud, optimalisasi penggunaan framework MITRE ATT&CK, dan informasi mendalam terkait proses-proses yang berjalan pada sistem operasi Windows.

Semoga tulisan-tulisan tersebut dapat membawa manfaat bagi para pembaca sekalian dan amal yang terus mengalir bagi para penulisnya. Akhir kata, terima kasih untuk semua pembaca CDEF Buletin yang terus setia membaca dan menunggu edisi terbaru dari CDEF Buletin.

Selamat membaca, tetap jaga kesehatan dan keamanan dimanapun kita berada.

Salam Hangat,

Tim Redaksi CDEF Buletin

KATA PENGANTAR

05

## MENGGUNAKAN LINKEDIN UNTUK "MENDARATKAN" PEKERJAAN DI CYBER SECURITY

oleh Mangatas Tondang

21

## PROGRAM KEAMANAN INFORMASI SEBAGAI LANGKAH PENCEGAHAN KEBOCORAN DATA

oleh Eryk Budi Pratama dan Ardhanti Nurwidya

36

## MANAJEMEN KEAMANAN MULTI CLOUD

oleh Eryk Budi Pratama dan Novita Handayani Koswara

54

## PENERAPAN SISTEM MONITORING 24/7 DAN AGENTLESS MONITORING MENGGUNAKAN RASPBERRY PI

oleh Ramadhan Hidayat

62

## SCOUTSUITE "SURVEY CORPS" PENJAGA DINDING LAYANAN CLOUD DARI BERBAGAI ANCAMAN "TITAN"

oleh Muhammad Fajar Masputra

71

## MITRE ATT&CK FOR BETTER DETECTION AND PREVENTION

oleh Ewaldo Simon Hiras

83

## WINDOWS CORE PROCESS

oleh Ewaldo Simon Hiras

93

## SECURITY ALERT

oleh Tim Redaksi

DAFTAR ISI

# JOIN US! CYBER DEFENSE COMMUNITY INDONESIA



**WWW.CDEF.ID**

| Kunjungi situs/website resmi komunitas CDEF



**HTTPS://S.ID/CDEF-SPOTIFY**

| Ikuti diskusi streaming kami di Spotify



**HTTPS://TWITTER.COM/CDEF\_ID**

| Follow twitter akun resmi komunitas CDEF



**HTTPS://GITHUB.COM/CDEFID**

| Bergabung dan berkontribusi bersama kami melalui Github resmi komunitas CDEF



**REDAKSI@CDEF.ID**

| Info lebih lanjut silahkan kirim e-mail melalui alamat resmi e-mail kami



**HTTPS://CDEF.ID/GABUNG-DISKUSI-CDEF**

| bergabunglah dalam forum diskusi kami di Discord CDEF



**HTTPS://S.ID/CDEF-LINKEDIN**

| Follow akun LinkedIn komunitas CDEF



**HTTPS://S.ID/CDEF-YOUTUBE**

| Subscribe channel Youtube resmi komunitas CDEF





# MENGGUNAKAN LINKEDIN UNTUK “MENDARATKAN” PEKERJAAN DI CYBER SECURITY

oleh Mangatas Tondang



LinkedIn adalah platform media sosial terbesar di dunia dengan fokus kepada pasar pekerja profesional. Tujuan utama dari situs ini adalah untuk menghubungkan kalangan profesional dengan satu sama lain, dengan pekerjaan dan posisi yang tepat serta mempelajari keterampilan yang dibutuhkan untuk kesuksesan karir setiap penggunanya. Sekarang LinkedIn sudah menambahkan banyak fitur untuk memperkuat hubungan profesional, contohnya adalah alat untuk menyelenggarakan acara *offline*, kelompok atau grup untuk membahas topik tertentu, atau alat untuk mengunggah artikel, foto dan video.

Jika Anda adalah seseorang yang sedang mencari pekerjaan di dunia *Cyber Security* atau seorang pelajar yang baru saja tamat dari universitas dan mencari pekerjaan di bidang tersebut, LinkedIn merupakan solusinya karena dapat digunakan secara strategis untuk membangun jaringan yang kompeten, menambah ilmu, bahkan bisa digunakan untuk mencari langkah selanjutnya pada karir Anda. Artikel ini akan membahas tentang hal-hal apa saja yang bisa Anda lakukan untuk “mendaratkan” pekerjaan *Cyber Security* dengan bantuan dari LinkedIn. Semua fitur yang dibahas adalah gratis, dimulai dengan bagaimana membangun *Complete Profile* yang tepat agar *Recruiter* bisa memberikan kita dengan tawaran pekerjaan yang tepat dan bagaimana kita bisa memperkenalkan diri kita dan berinteraksi dengan pengguna LinkedIn, termasuk *Recruiter* melalui *Meaningful Connection*. Lalu membahas tentang bagaimana caranya menggunakan “LinkedIn Jobs” serta menempah **LinkedIn Job Search**. Fitur yang terakhir adalah mendalami komponen-komponen dari “LinkedIn Job Post” dan apa saja *Job Description* seperti kemampuan dan skill yang diperlukan untuk pekerjaan-pekerjaan di dalam dunia *Cyber Security*.

#### Disclaimer

Artikel ini bukanlah garansi untuk mendapatkan pekerjaan dan harap digunakan hanya sebatas referensi dan bukan menjadi petunjuk mutlak. LinkedIn Premium tidak diperlukan untuk menerapkan hal-hal yang dijelaskan pada artikel ini.

## MEMBANTU RECRUITER MENEMUKAN PROFILE ANDA

### #1 - MEMBANGUN PROFIL LINKEDIN

LinkedIn, pada intinya, adalah sebuah platform media sosial dan pada *platform* tersebut, membangun Profil adalah tugas pertama dari setiap pengguna. Perbedaan LinkedIn dengan media sosial lainnya adalah LinkedIn tidak menambahkan informasi seperti film favorit atau foto liburan Anda namun membutuhkan informasi terkait dunia profesional Anda. Ada 3 level informasi yang dapat ditambahkan ke LinkedIn, yaitu *Core*, *Recommended* dan *Additional*.

#1 - CORE	<b>#1 - Edukasi</b>
	<ul style="list-style-type: none"> <li>• Utamakan untuk menambah informasi dari SMA/SMK dan tingkatan di atasnya.</li> <li>• Ada baiknya menambahkan satu paragraf tentang material yang Anda pelajari di institusi tersebut.</li> <li>• Anda bisa menambahkan kelas-kelas yang Anda ambil di bagian "<i>Recommended</i> - Kelas"</li> </ul>
	<b>#2 - Posisi</b>
	<ul style="list-style-type: none"> <li>• Utamakan posisi pekerjaan yang bersangkutan dengan pekerjaan Anda yang sekarang atau yang Anda cari, di contoh ini kita menggunakan <i>Cyber Security</i>.</li> <li>• Sertakan informasi pendukung seperti tanggal, lokasi dan sedikit informasi mengenai tugas Anda. Harap berhati-hati untuk tidak melanggar perjanjian privasi dan rahasia dengan perusahaan yang Anda tuliskan, seperti NDA (<i>Non Disclosure Agreement</i>) atau perjanjian lainnya.</li> <li>• Gunakan kalimat penuh menjelaskan apa yang Anda lakukan dan dampak apa yang Anda berikan terhadap perusahaan. Contohnya, "Melakukan revisi terhadap dokumentasi pekerja baru dan meningkatkan efisiensi pelatihan dari 4 minggu menjadi 2 minggu."</li> </ul>
	<b>#3 - Keterampilan (Skill)</b>

	<ul style="list-style-type: none"> <li>• LinkedIn hanya memperbolehkan maksimal 50 <i>skills</i> untuk ditambahkan ke profil Anda.</li> <li>• Pastikan bahwa kemampuan terbaik dan kemampuan yang sesuai dengan pekerjaan yang Anda mau atau cari sudah Anda tambahkan ke dalam bagian ini.</li> <li>• Anda bisa mengombinasikan beberapa <i>skill</i> menjadi satu, misalnya Microsoft Excel, Microsoft Words dan Microsoft PowerPoint dapat disatukan menjadi <i>Microsoft Office Suite</i>.</li> </ul>
--	---

	<b>Fitur - 1#</b>	#2 - RECOMENDED
<ul style="list-style-type: none"> <li>• Fitur adalah tempat dimana Anda bisa menunjukkan hal-hal menarik yang sedang Anda lakukan atau telah Anda lakukan.</li> <li>• Bisa berupa artikel, <i>post</i>, tautan ke situs lainya seperti situs video, dokumen dan lain-lain.</li> </ul>		
	<b>Lisensi dan sertifikasi - 2#</b>	
<ul style="list-style-type: none"> <li>• <i>Cyber Security</i> adalah salah satu dunia perkerjaan yang memiliki banyak sertifikasi, berbayar ataupun gratis. LinkedIn dapat digunakan untuk memaparkan sertifikasi tersebut terhadap pengguna lain.</li> <li>• Anda bisa menambahkan ID dari sertifikasi tersebut atau menambahkan tautan ke situs verifikasi seperti <i>Cred.ly</i> dan lainnya</li> </ul>		
	<b>Kelas - 3#</b>	
Anda bisa menambahkan kelas-kelas apa saja yang sudah Anda ambil, baik di dalam edukasi formal seperti universitas atau edukasi informal seperti <i>bootcamp</i> atau pelatihan khusus.		
	<b>Rekomendasi - 4#</b>	
<ul style="list-style-type: none"> <li>• Rekomendasi adalah fitur yang sangat berguna untuk menunjukkan kualitas anda di pekerjaan anda sebelumnya.</li> <li>• Sebelum meninggalkan pekerjaan lama, ada baiknya agar Anda meminta kolega dan atasan Anda untuk meninggalkan rekomendasi di LinkedIn Anda.</li> </ul>		

### #3 - ADDITIONAL

Bagian dibawah ini bisa ditambahkan jika Anda memilikinya dan informasi ini bisa membantu Anda menemukan komunitas yang sesuai dengan pandangan Anda.

- Pengalaman sukarelawan
- Publikasi dan paten
- Proyek
- Honor, penghargaan dan nilai tes
- Bahasa
- Organisasi
- Kausa (*Causes*)
- Kontak Informasi

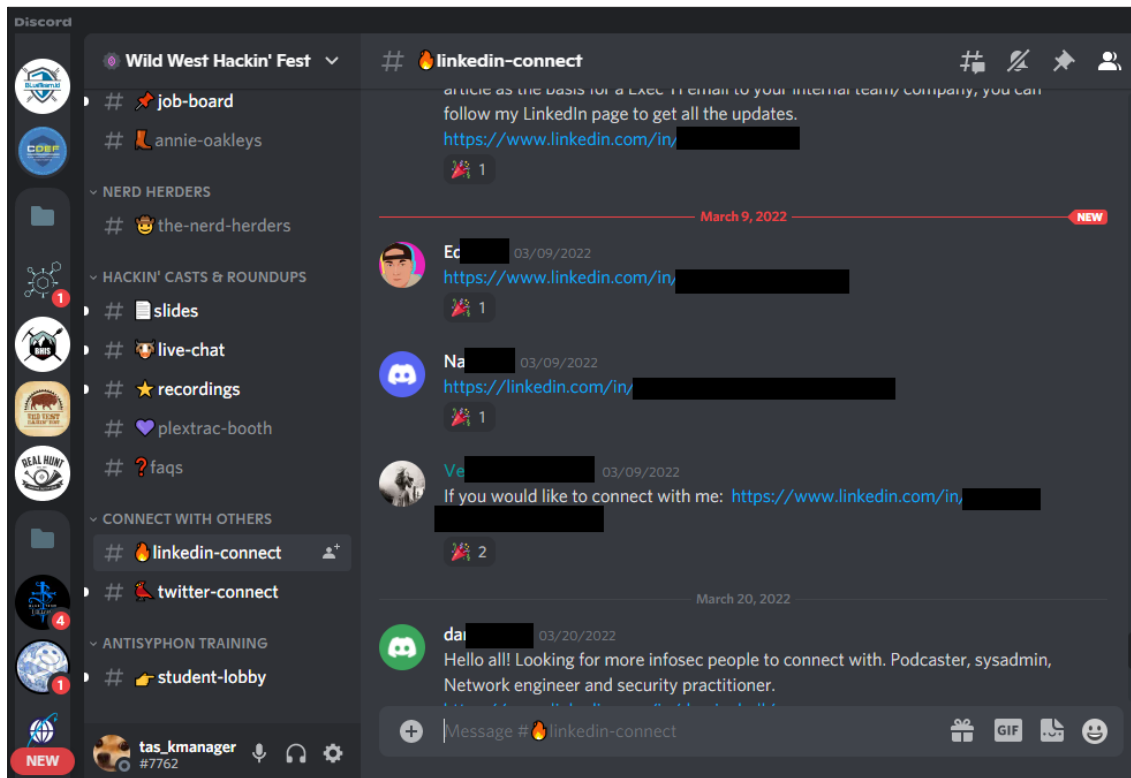
## #2 - MEANINGFUL CONNECTIONS

Seperti dunia nyata, berkoneksi di dunia maya melalui LinkedIn juga membutuhkan sedikit tenaga dan usaha. Apabila Anda ingin menambah koneksi di LinkedIn ada baiknya sebelum mengirim permintaan koneksi, Anda sudah pernah berinteraksi dengan orang tersebut, baik di dunia nyata atau di dunia maya. Berikut adalah hal-hal yang bisa Anda lakukan untuk membuka koneksi di dunia maya:

- Bergabung di dalam satu grup terkait dengan *cyber security* dan berinteraksi melalui chat pribadi atau diskusi grup, contohnya adalah grup CDEF.ID Discord atau WhatsApp.
- Bekerja sama di kompetisi Cyber Security online seperti *Capture The Flag* atau Hackaton. Contohnya adalah **Splunk Boss of the SOC**.
- Berinteraksi dengan koneksi tingkat kedua dan ketiga di LinkedIn, contohnya merespon *poll*, memberikan komentar di artikel koneksi tersebut atau dengan menyukai artikel dari koneksi Anda.
- Mengikuti konferensi *online* dan melakukan interaksi melalui *platform chat*, seperti Discord dan Slack. Beberapa konferensi bahkan memiliki ruangan khusus untuk mencantumkan LinkedIn Anda. Contohnya konferensi “Wild West Hackin’ Fest” .

Berikut adalah hal-hal yang bisa anda lakukan untuk membuka koneksi di dunia nyata, yaitu:

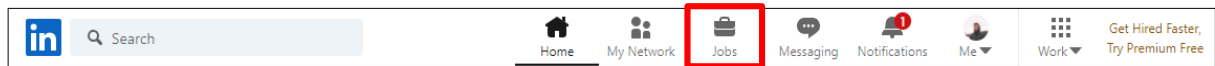
- Mengundang teman-teman di kantor atau sekolah untuk berkoneksi di LinkedIn. Banyak potensi yang Anda bisa lakukan disini, seperti saling memberikan rekomendasi.



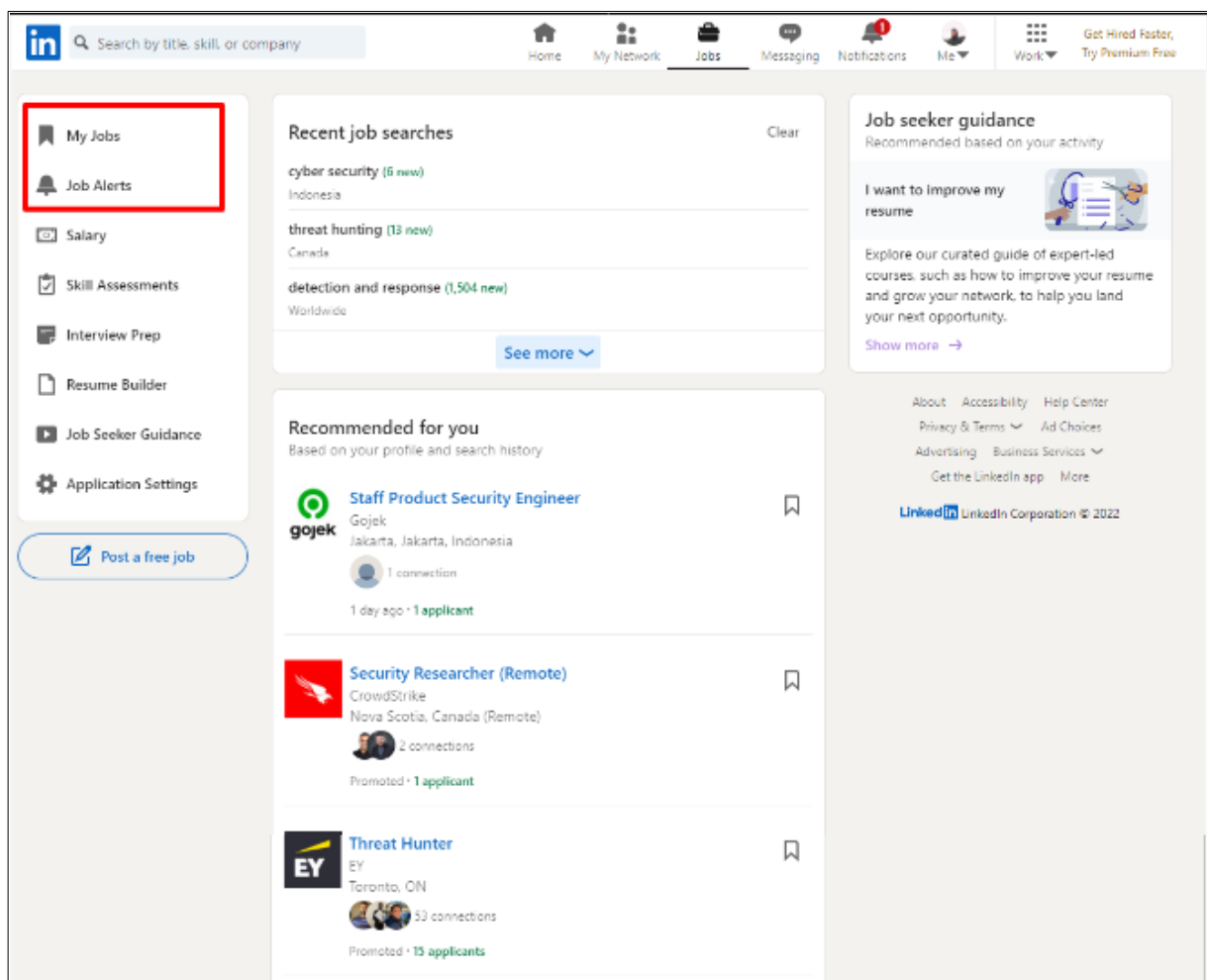
- Mendatangi program *open house* atau *career fair* dari perusahaan-perusahaan teknologi dan berinteraksi dengan *recruiter* dan *hiring manager*. Disini anda bisa lebih dalam lagi mengenal perusahaan dan pekerjaan *Cyber Security* apa saja yang tersedia. Jangan lupa untuk meminta kartu nama dan izin untuk menambahkan mereka ke dalam koneksi Anda.
- Mendatangi *meetup* seperti *meetup* komunitas CDEF dan berpartisipasi dengan sungguh-sungguh. Berinteraksi dengan peserta meetup pada saat istirahat atau sesi diskusi.



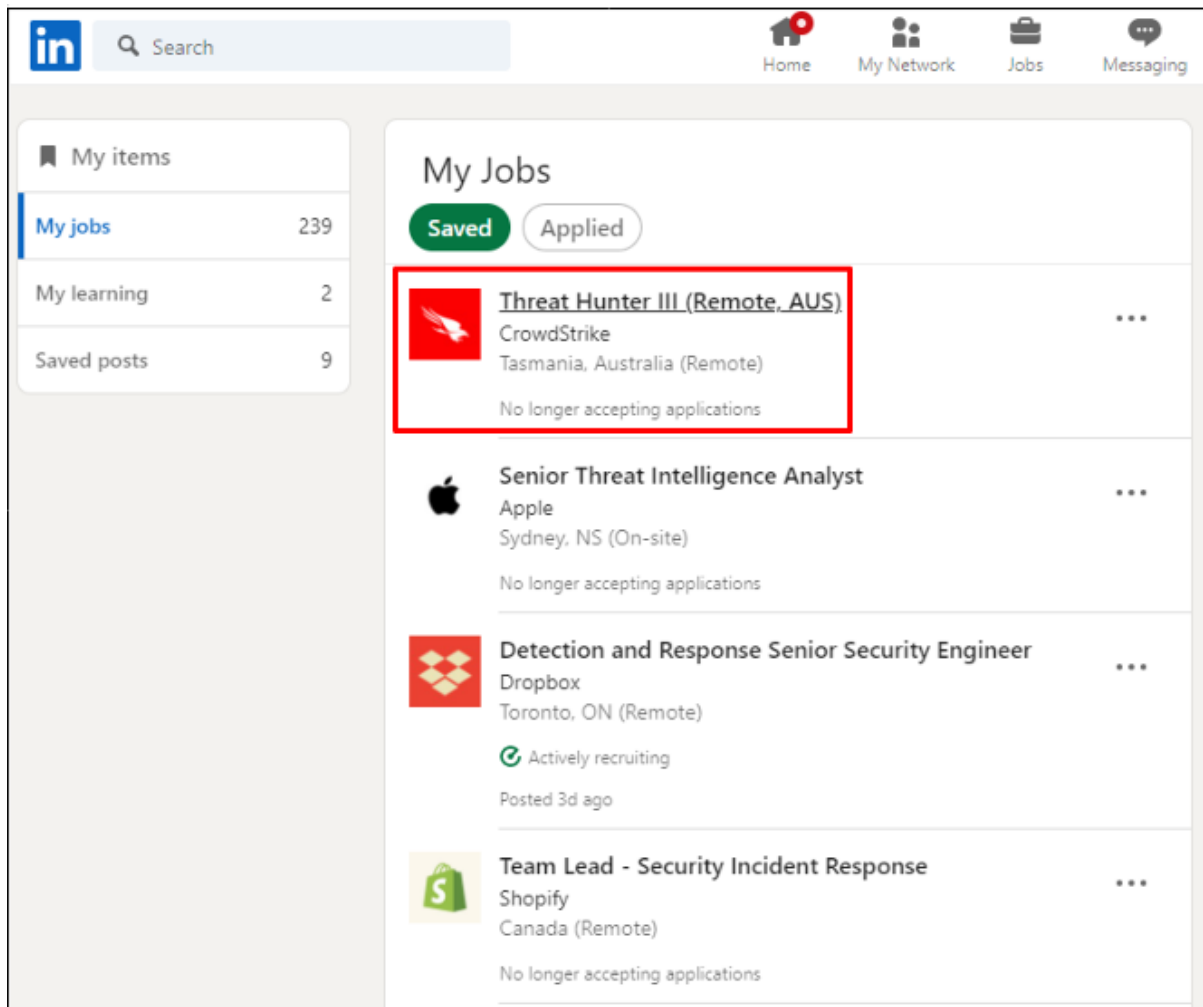
### #3 - LINKEDIN JOBS



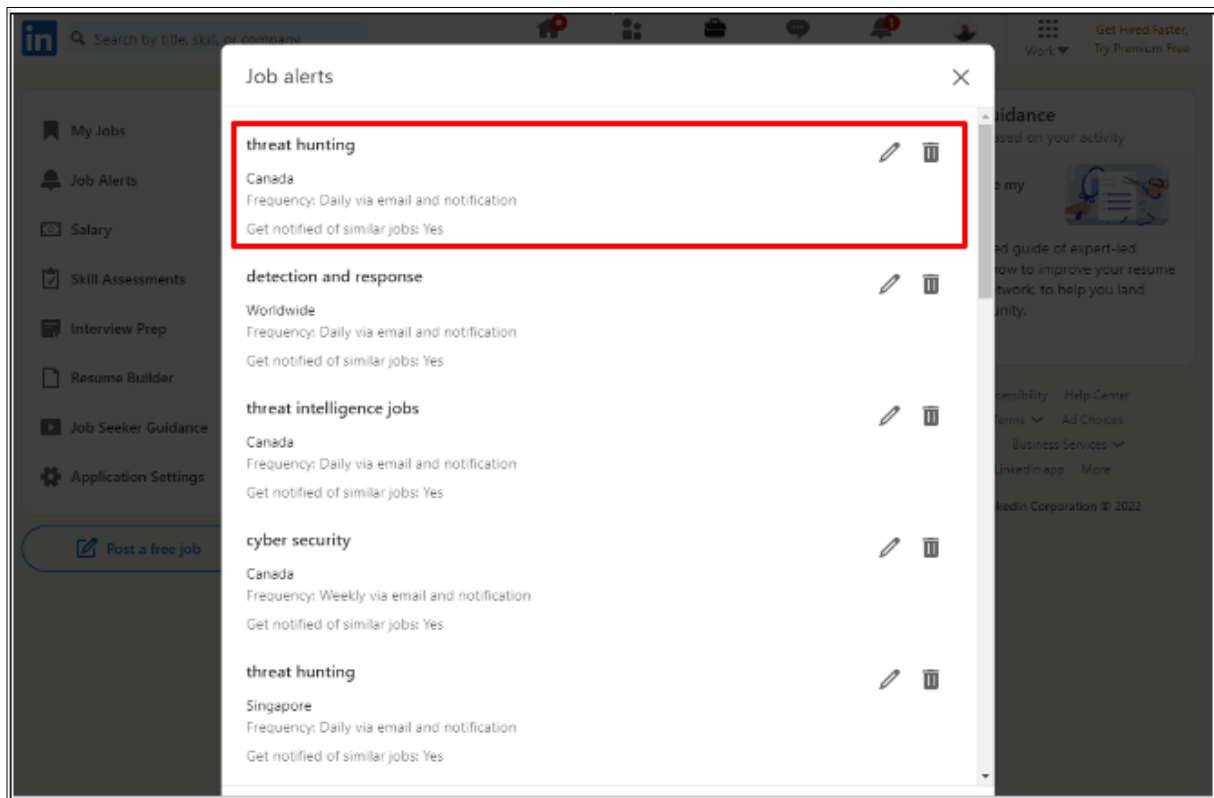
Anda dapat dengan mudah menemukan **LinkedIn Jobs** di sisi kanan atas halaman utama. Berikut adalah tampilan **LinkedIn Jobs**. Kita akan fokus ke dua bagian dari **LinkedIn Jobs**, **My Jobs** dan **Job Alerts**. Bagian-bagian ini sangat kritikal bagi Anda pencari pekerjaan. Anda boleh mengeksplorasi bagian lainnya. Di bawah ini adalah tampilan **LinkedIn Jobs**.



**My Jobs** adalah tempat Anda akan menemukan pekerjaan-pekerjaan yang Anda sudah cari, kumpulkan atau lamar. Anda dapat melihat informasi seperti nama pekerjaan tersebut, perusahaan yang mencari pekerjaan tersebut, logo perusahaan tersebut, lokasi dari pekerjaan tersebut dan apakah mereka masih menerima lamaran atau tidak. Di bawah ini adalah tampilan **My Jobs**.

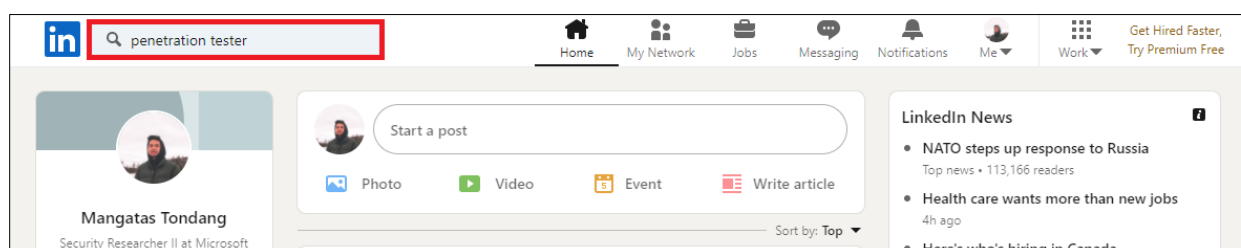


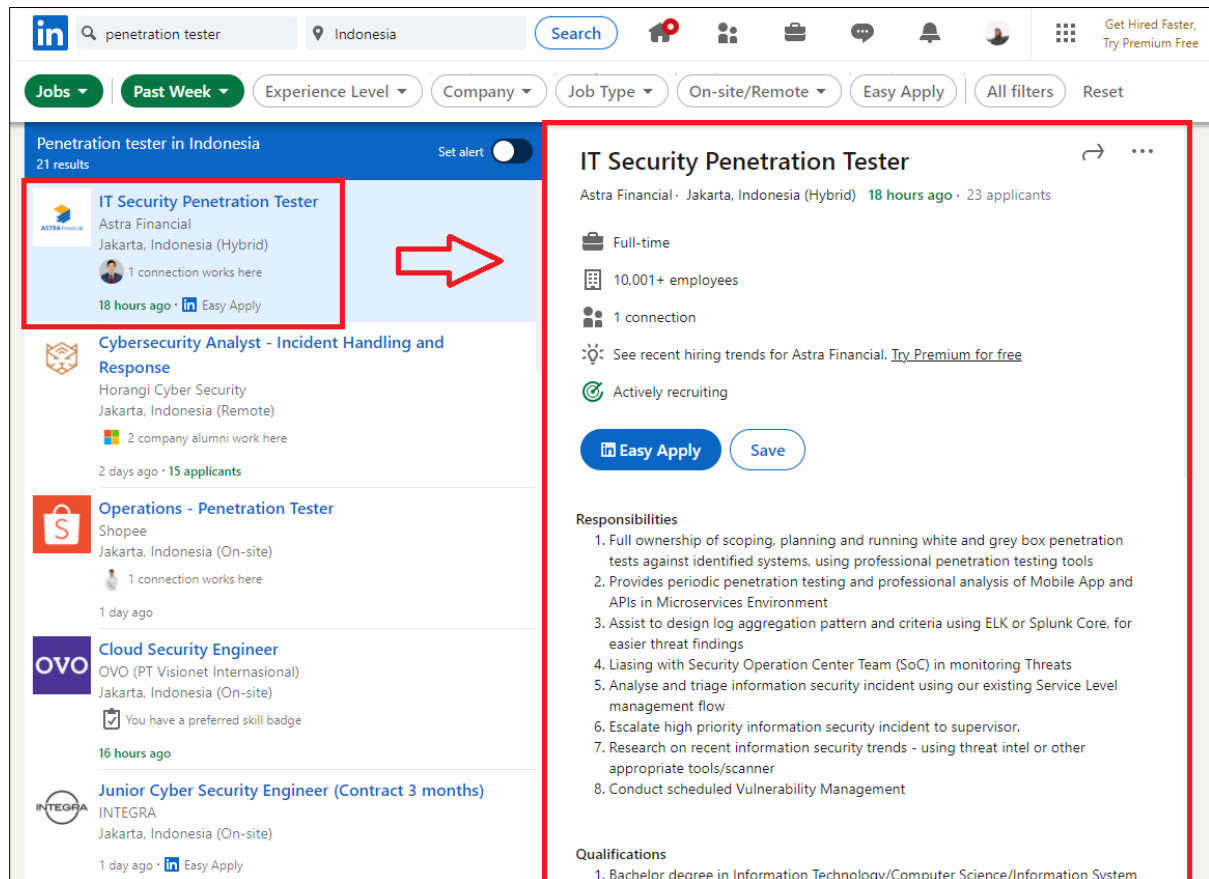
Bagian yang paling penting dalam pencarian pekerjaan dengan LinkedIn adalah **Job Alerts**. Disini Anda bisa menemukan semua **Job Alerts** yang Anda sudah buat sebelumnya. Berikut adalah contoh **Job Alerts** dari akun Saya. Anda dapat melihat informasi mengenai **Job Alerts** yang telah saya buat, contohnya adalah pekerjaan **Threat Hunting** di Kanada, setiap hari saya akan menerima update tentang pekerjaan yang sesuai dengan kriteria melalui email dan notifikasi. Saya juga mengizinkan LinkedIn mengirimkan pekerjaan yang mirip dengan kriteria Saya. Hal ini dilakukan oleh *Process Big Data* dan *Machine Learning* yang dimiliki oleh LinkedIn.



#### #4 - MENEMPAH LINKEDIN JOB SEARCH

Hal yang pertama dilakukan ialah Anda harus memberikan kriteria kepada LinkedIn agar mereka bisa membantu mencari pekerjaan bagi. Semua dimulai dari **search bar** di sisi kiri atas halaman LinkedIn. Pada contoh kali ini, kita akan mencari *role Penetration Tester* di Indonesia. Ketik ketentuan yang anda inginkan di *search bar* dan tekan enter.





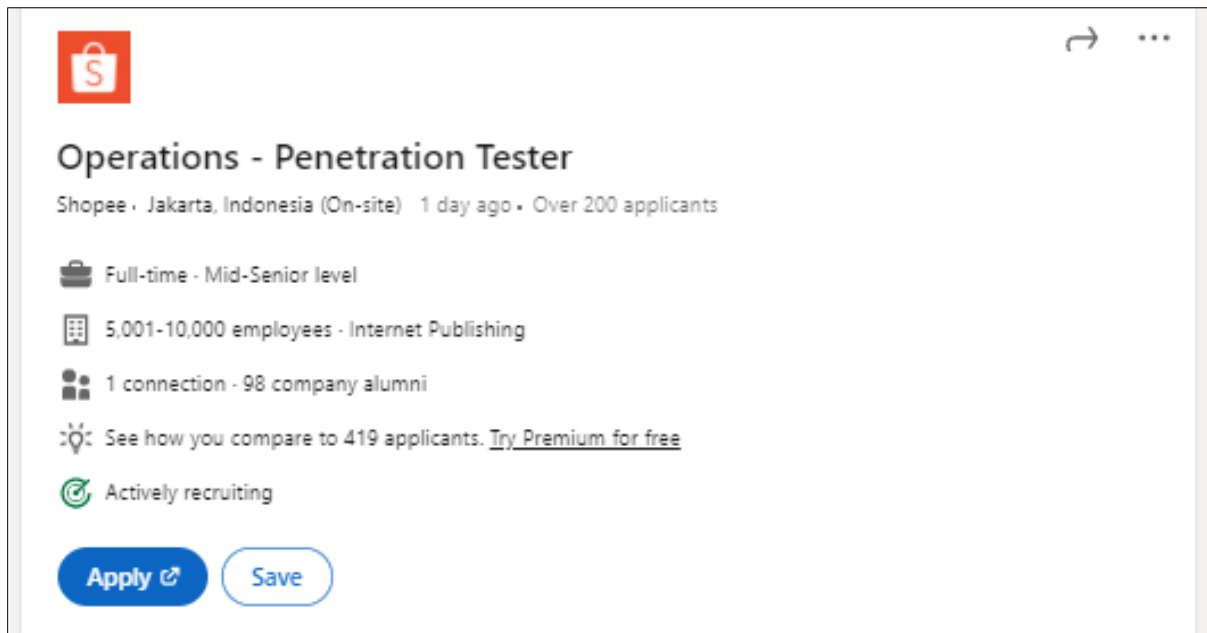
Setelah halaman dimuat, tambahkan Indonesia di lokasi. Di atas Anda bisa melihat bagian Filter, diikuti dengan bagian utama. Di bagian utama, di sebelah kiri Anda bisa melihat pekerjaan yang sesuai dengan kondisi Anda, dalam contoh ini Penetration Tester. Di sisi kanan Anda bisa melihat bagian dari sebuah LinkedIn Job Posting.

Ada beberapa bagian yang bisa dispesifikasikan pada **LinkedIn Job Search** seperti:

- Waktu unggah pekerjaan tersebut ditampilkan (Seminggu yang lalu, Sebulan yang lalu, dan lainnya).
- Tingkat pengalaman yang diperlukan untuk pekerjaan tersebut (Magang, Awal, Senior, dan lainnya).
- Perusahaan yang mencari pekerja.
- Tipe pekerjaan (*part-time*, *full-time*, kontrak, magang, dan lainnya).
- Lokasi pekerjaan tersebut (di kantor, *Remote* atau WFH, dan campuran).

- **Fitur Easy Apply**, dimana kita tidak perlu memasukkan banyak informasi ke dalam sistem HR perusahaan tersebut. Semua proses dilakukan melalui LinkedIn.

## #5 - KOMPONEN LINKEDIN JOB POST



Kita akan membahas bagian **LinkedIn Job Posting** dengan lebih jelas di bagian ini. Dibagian kepala, kita bisa melihat informasi seperti pekerjaan apa yang dicari, nama dan logo perusahaan, dan lokasi dari pekerjaan tersebut. Kita juga bisa melihat kapan pekerjaan tersebut di unggah ke LinkedIn dan jumlah orang yang sudah melamar ke pekerjaan tersebut. Pada contoh di atas Anda dapat melihat lebih dari 200 orang sudah melamar (lebih tepatnya 419 pelamar) ke pekerjaan tersebut melalui LinkedIn. Anda juga dapat melihat jenis dan tingkat dari pekerjaan tersebut. Dari situ Anda tahu bahwa ada satu orang koneksi kita yang bekerja di perusahaan tersebut dan perusahaan ini masih aktif mencari calon pekerja untuk pekerjaan tersebut. Kita punya dua opsi, antara untuk melakukan proses aplikasi atau menyimpan pekerjaan tersebut ke **My Jobs**.

## About the job

### Job Description

- Perform penetrations tests of infrastructure, wireless, web applications, mobile application, API, IoT, and also have experiences in social engineering and physical attack
- Work with teams to communicate findings and recommendations
- Monitor progress, manage risk and ensure key stakeholders are kept informed about progress and expected outcomes

### Requirements

- Minimum 1-year experience in related fields
- Have passion and curiosity to explore new techniques and attack vectors
- Strong communication skills and the ability to provide technical guidance to both technical and non-technical audiences
- Deep knowledge in industry security best practices/standards/policies such as NIST, OWASP, CIS, MITRE&ATT@CK
- Have experience in penetration test projects
- A self-motivated learner that continuously wants to share knowledge to improve others
- Have experience in the Red Teaming project is an advantage
- Offensive Security certification is an advantage

Di bagian **About the Job** perusahaan tersebut akan berusaha untuk menjelaskan hal seperti deskripsi dari pekerjaan tersebut, skill yang harus dimiliki oleh pelamar dan terkadang hal lainnya seperti bagaimanakah hari-hari pekerja di perusahaan tersebut dan kultur dari perusahaan tersebut.

### Set alert for similar jobs

Penetration Tester, Jakarta, Indonesia

[Set alert](#)

### Pay range unavailable

Salary information is not available at the moment.

Are you interested in salary information for this job? Yes / No

### About the company



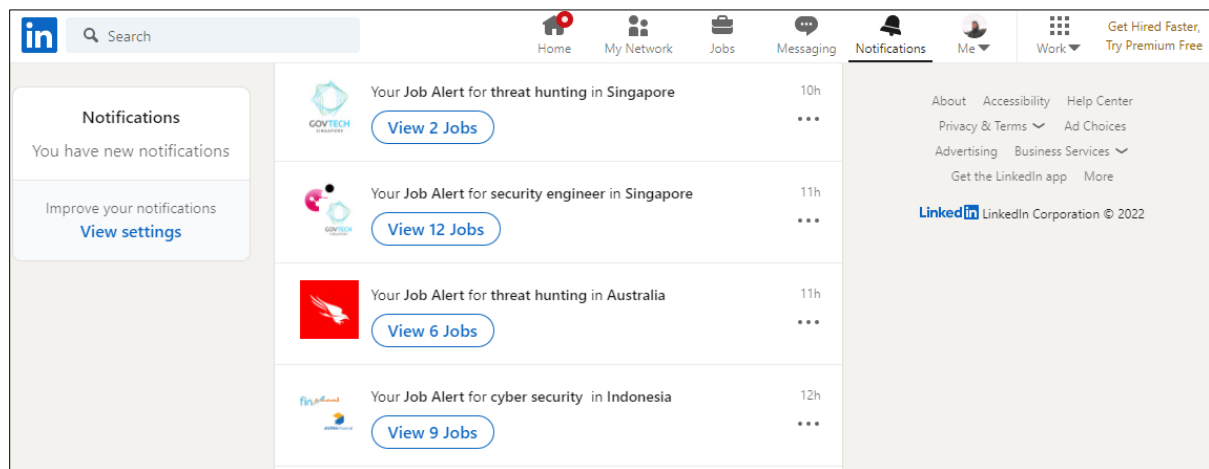
Shopee  
1,406,433 followers

[+ Follow](#)

Di bagian selanjutnya Anda bisa dengan gampang menghidupkan **LinkedIn Job Alert** untuk pekerjaan yang mirip dengan pekerjaan di atas. Informasi tentang gaji dan



keuntungan tidak tersedia untuk **Job Posting** ini. Anda juga bisa mempelajari informasi tentang perusahaan dengan mengikuti perusahaan tersebut di LinkedIn.



Setelah menambah **Job Alerts** Anda akan menerima notifikasi dari LinkedIn sesuai dengan periode yang Anda telah setuju. Dari sini Anda akan menjadi orang pertama yang tahu mengenai **Job Posting** baru dari perusahaan di lokasi yang Anda tentukan dengan pekerjaan yang anda tentukan. Langkah selanjutnya adalah untuk melamar pekerjaan tersebut, Happy Hunting!

## JOB DESCRIPTION DI DUNIA CYBER SECURITY

Sebagai bonus dari artikel ini, saya akan membagikan dua peran umum di dalam *Cyber Security* dan *skill* apa saja yang dibutuhkan agar menjadi sukses di dalam pekerjaan tersebut.

Red Team Operator
Peran serupa
<i>Penetration Tester, Offensive Security Engineer, Offensive Security Researcher, Vulnerability Researcher, Exploit Developer</i>
Tugas utama
Melakukan serangan terhadap jaringan dan komponen teknologi dari perusahaan tersebut. Bisa dimulai dari aktivitas mudah seperti NMAP <i>scanning</i> , Enumerasi

## Red Team Operator

direktori dan aktivitas Recon lainnya. Biasanya diakhiri dengan mengambil alih *Domain Controller* dari perusahaan tersebut atau mengeluarkan informasi sensitif dari server tertentu.

### Kemampuan Teknikal

- Pengertian dan pengalaman yang dalam di Sistem Operasi (Windows, Linux, Mac, Mobile, Cloud, dan lainnya).
- Pengertian dan pengalaman yang dalam di protokol jaringan dan penggunaan alat bantu seperti WireShark dan analisis data dari PCAP.
- *Social Engineering* melalui media telepon, email atau fisik.
- Membangun dan menggunakan alat-alat *Offensive Security* seperti NMAP, BurpSuite, Mimikatz, CobaltStrike.
- Automasi menggunakan *Scripting Language* seperti Python atau Perl.
- Pengertian tentang Application Development atau Programming seperti C#, Golang, Java, dan lainnya.

### Kemampuan Non Teknikal

- Membuat dan menjelaskan dokumen untuk tim teknis atau eksekutif C-Level
- Melakukan presentasi dari hasil temuan selama masa proyek atau tugas
- Manajemen waktu dan orang (tim)

## Blue Team Analyst

### Peran serupa

Security Analyst, Security Specialist, Triage Analyst, SIEM Analyst

### Tugas utama

Melakukan eskalasi terhadap alert dari serangan terhadap jaringan dan komponen teknologi dari perusahaan tersebut. Dimulai dengan membuka tiket dan melanjutkan investigasi ke alat-alat seperti EDR atau AV, SIEM dan perangkat Network.

Blue Team Analyst
Kemampuan Teknikal
<ul style="list-style-type: none"> <li>• Pengertian dan pengalaman di Sistem Operasi (Windows, Linux, Mac, Mobile, Cloud, dan lainnya).</li> <li>• Pengertian dan pengalaman di protokol Network dan penggunaan alat bantu seperti WireShark dan analisis data dari PCAP.</li> <li>• Pengertian dalam hal <i>Events</i> dan <i>Alerts</i> dari vendor EDR atau AV.</li> <li>• Pengalaman investigasi dengan menggunakan SIEM. Familiar dengan query language seperti KQL, SPQL atau EQL.</li> <li>• Menggunakan OSINT baik yang gratis atau berbayar, seperti VirusTotal, Greynoise, dan lainnya.</li> <li>• Pengertian dari penggunaan alat-alat Offensive Security seperti NMAP, BurpSuite, Mimikatz, CobaltStrike</li> <li>• Automasi menggunakan Scripting Language seperti Python atau Perl</li> <li>• Pengertian tentang Application Development atau Programming seperti C#, Golang, Java, dan lainnya.</li> </ul>
Kemampuan Non Teknikal
<ul style="list-style-type: none"> <li>• Membuat dan melaksanakan dokumentasi untuk eskalasi di dalam waktu SLA (<i>Service Level Agreement</i>)</li> <li>• Melakukan dokumentasi tentang temuan di dalam periode waktu tertentu</li> </ul>

Anda bisa mengunjungi situs GitHub pribadi Saya dan membaca presentasi **“The Job Seeker of InfoSec”** dimana Saya membahas peran diatas lebih dalam dan juga membahas peran-peran yang lain seperti GRC, *Application Security* dan *Infrastructure Security*.

## REFERENSI

[https://github.com/tas-kmanager/SecurityPresentation/blob/master/JobSeekerOfInfoSec/JSOIS\\_ISSessions.pdf](https://github.com/tas-kmanager/SecurityPresentation/blob/master/JobSeekerOfInfoSec/JSOIS_ISSessions.pdf)

## TENTANG PENULIS



Mangatas Tondang adalah seorang penggiat Cyber Security asal Indonesia yang tinggal dan bekerja di Toronto, Canada. Sekarang ini Mangatas bekerja sebagai Security Researcher II di Microsoft, dengan fokus utama untuk melakukan penelitian lanjutan tentang serangan cyber dan menemukan metodologi baru di bagian deteksi dan respon. Pengalaman Mangatas sangat beragam, dimulai dari Incident Response, Threat Hunting hingga Detection Engineering. Mangatas sangat aktif di dunia Cyber Security dimana sudah pernah menyampaikan presentasi di DEF CON, SANS Summit dan beragam konferensi lainnya.

# PROGRAM KEAMANAN INFORMASI SEBAGAI LANGKAH PENCEGAHAN KEBOCORAN DATA

oleh Eryk Budi Pratama dan Ardhanti Nurwidya



Masyarakat Indonesia baru saja dibuat kecewa dengan adanya insiden kebocoran data pribadi yang terjadi secara berentet. Insiden ini terjadi di beberapa instansi pemerintah yang mengelola data pribadi masyarakat secara masif. Tahun 2022 ini dibuka dengan adanya kebocoran data di server Kementerian Kesehatan yang membuat data riwayat kesehatan pasien dapat diakses oleh publik. Hal ini cukup miris mengingat bahwa data kesehatan merupakan data pribadi spesifik (atau sering juga disebut sebagai data sensitif) yang pemrosesannya harus dilakukan dengan proteksi berlapis. Kebocoran ini pada umumnya disebabkan karena adanya kelemahan pada penerapan kontrol

keamanan informasi. Rancangan UU Perlindungan Data Pribadi ( "**RUU PDP**" ) menjadi topik yang hangat dan kerap diperbincangkan oleh berbagai praktisi. Apakah RUU PDP dapat menjadi acuan untuk penerapan kontrol keamanan informasi yang baik?

## Program Keamanan Informasi

---

Program keamanan informasi atau yang sering lebih dikenal dengan *Information Security Programs* atau *Infosec Programs* adalah serangkaian kegiatan untuk yang dilakukan untuk melindungi proses bisnis, data dan aset IT dengan mengidentifikasi *people, process, and technology* yang dapat berdampak kepada *security, confidentiality* dan *integrity* dari aset IT.

Guna mencapai kesuksesan dari Program Keamanan Informasi membutuhkan kerjasama tim dari berbagai keahlian, bukan hanya ahli dengan latar belakang IT Security, namun juga latar belakang hukum. Hal ini juga tercermin dalam komposisi anggota di berbagai asosiasi terkait dengan privasi, seperti *International Association of Privacy Professionals (iapp.org)* serta dibentuknya Asosiasi Praktisi Pelindungan Data Indonesia ([appdi.org.id](http://appdi.org.id)) yang beranggotakan ahli dengan latar belakang yang berbeda-beda.

Program Keamanan Informasi juga sangat penting untuk mencegah adanya kebocoran data karena dengan adanya program yang jelas dan didukung oleh berbagai pihak di dalam suatu organisasi, maka kontrol keamanan informasi dapat diterapkan di inisiatif-inisiatif yang lebih riskan. Faktor pendorong lainnya bagi suatu organisasi untuk menerapkan Program Keamanan Informasi adalah:

- a. **Adanya risiko kebocoran data pribadi.** Dalam tiga tahun terakhir, kita bisa melihat bahwa kebocoran data pribadi terjadi baik di sektor public maupun privat. Penyebab utama (*root cause*) dari berbagai kebocoran tidak dipublikasikan, namun salah satu unsur yang rentan adalah *People*. Maka, program ini dapat membantu organisasi dalam meningkatkan kompetensi dari orang-orang yang terlibat dalam pemrosesan data pribadi di suatu organisasi dengan menerapkan *Privacy Awareness Training* secara berkelanjutan.



- b. **Regulasi perlindungan data pribadi.** Meski RUU PDP belum disahkan, tetapi sudah ada lebih dari 30 regulasi yang mengatur tentang data pribadi. Dalam regulasi ini, program pencegahan merupakan hal yang dapat menjadi faktor yang menunjukkan kepatuhan organisasi terhadap prinsip perlindungan data pribadi.
- o **Perkominfo No. 20/2016** mewajibkan pengendali data untuk memiliki berbagai aturan internal terkait dengan perlindungan data pribadi sesuai dengan peraturan perundang-undangan. Berbagai aturan internal inilah yang merupakan "*game plan*" yang mencakup Program Keamanan Informasi, utamanya terkait dengan pemrosesan data pribadi.
  - o **RUU PDP** juga mengatur bahwa pengendali data pribadi wajib bertanggung jawab atas pemrosesan data pribadi dan menunjukkan pertanggungjawabannya dalam pemenuhan kewajiban pelaksanaan prinsip perlindungan data pribadi. Artinya, dalam hal terjadi kegagalan pemrosesan data pribadi, pengendali data akan dituntut untuk membuktikan bahwa pengendali data tersebut telah memproses data pribadi sesuai dengan prinsip-prinsip perlindungan data pribadi.
- c. **Peningkatan kepercayaan investor dan pelanggan.** Trust dari pelanggan adalah kunci keberlangsungan bisnis. Komitmen organisasi dalam perlindungan data pribadi membuat pelanggan akan semakin percaya untuk memberikan data dan melakukan transaksi. Sama halnya dalam perspektif investor. Saat ini isu *sustainability* atau keberlanjutan semakin menjadi semakin penting. Hal tersebut dibuktikan dengan mulai banyaknya organisasi yang ingin meningkatkan kapabilitas manajemen *Environment, Social, dan Governance (ESG)*, yang mana isu privasi merupakan salah satu elemen dalam laporan ESG tersebut.

Violation	Number of Fines
Insufficient legal basis for data processing	355 (with total € 435,458,731)
Non-compliance with general data processing principles	226 (with total € 810,768,644)
Insufficient technical and organisational measures to ensure information security	207 (with total € 97,756,619)
Insufficient fulfilment of data subjects rights	99 (with total € 17,665,170)
Insufficient fulfilment of information obligations	87 (with total € 235,052,795)
Insufficient cooperation with supervisory authority	41 (with total € 239,929)
Insufficient fulfilment of data breach notification obligations	22 (with total € 1,479,091)
Insufficient involvement of data protection officer	12 (with total € 350,600)
Insufficient data processing agreement	6 (with total € 1,006,580)
Unknown	6 (with total € 22,704,400)

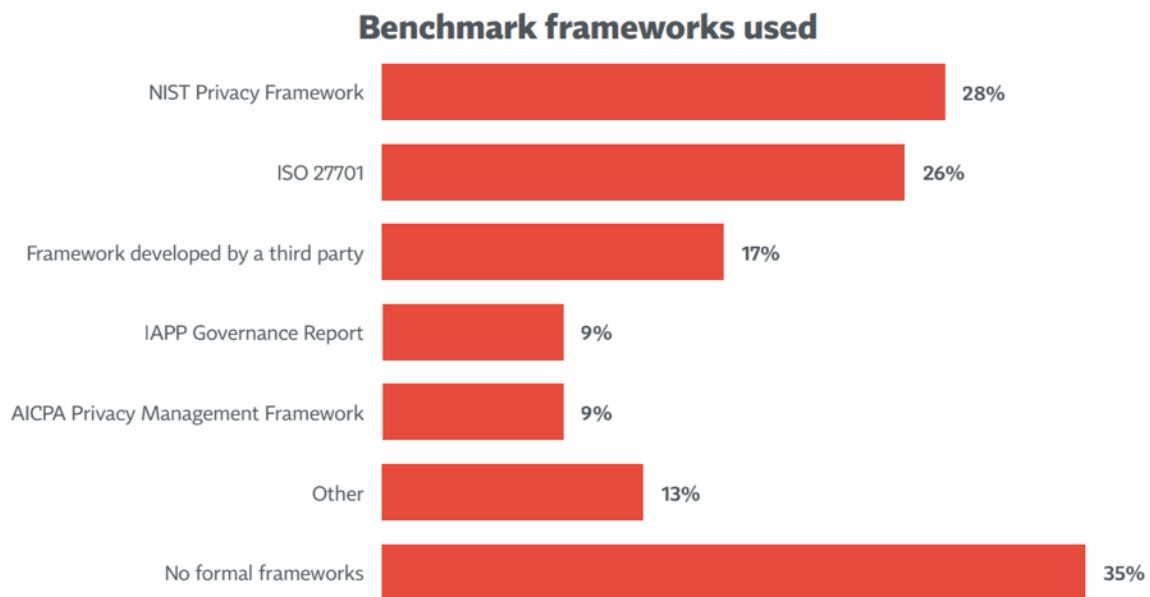
**Gambar 1 - Statistik pelanggaran data pribadi yang terjadi di Eropa (Sumber: <https://www.enforcementtracker.com/?insights>)**

Berdasarkan statistik General Data Protection Regulation atau GDPR *Enforcement Tracker* [1], justru aspek keamanan informasi menempati urutan ketiga (*Insufficient technical and organizational measures to ensure information security*) dengan banyak pelanggaran mencapai 355 dan total denda mencapai lebih dari 400 juta euro. Sedangkan, urutan pertama dan kedua adalah terkait dengan penggunaan dasar / landasan hukum yang sesuai dan pemenuhan terhadap prinsip-prinsip pemrosesan data pribadi yang diatur dalam GDPR. Hal ini juga diamini oleh tim perumus RUU PDP yang mengatur bahwa pelanggaran dapat berupa ketidaksesuaian pemrosesan data pribadi dengan prinsip-prinsip perlindungan data pribadi serta penggunaan dasar hukum yang tepat (*legal basis*). Artinya, tidak perlu menunggu sampai sebuah kegagalan data pribadi terjadi untuk dapat memberikan teguran atau bahkan sanksi terhadap organisasi yang memproses data pribadi dengan tidak tepat. Contohnya, Google didenda sebesar 50 juta euro karena tidak secara jelas menyampaikan bagaimana data pengguna diproses melalui berbagai platform yang dimiliki – termasuk dalam layanan search engine, Maps, YouTube – dalam hal untuk menyajikan *personalized advertisements*.

## Privacy Framework

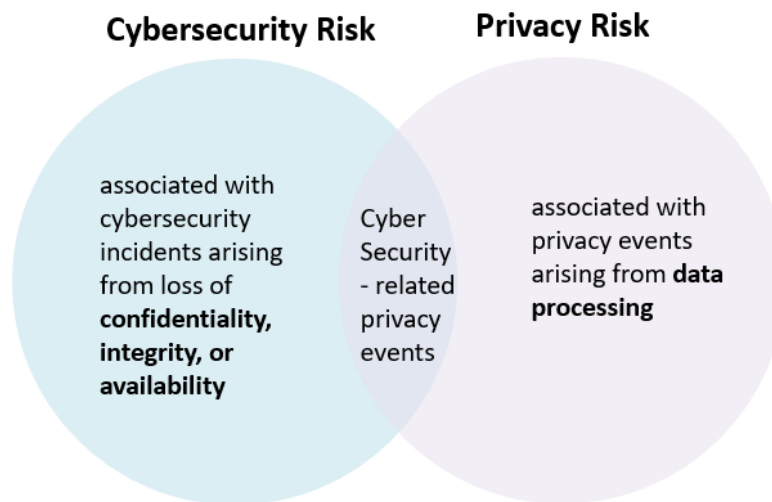
---

Berdasarkan survei IAPP [3], 48% dari organisasi telah memiliki rencana dan program untuk *Privacy*, dimana **NIST Privacy Framework** dan ISO 27701:2019 dijadikan sebagai *framework* utama dalam penyusunan program.



**Gambar 2 - Statistik Privacy Framework (Sumber: IAPP Annual Privacy Governance Report 2021)**

*Risk based approach* merupakan cara yang umum digunakan organisasi dalam memitigasi dan meminimalisasi risiko. Meskipun pengelolaan risiko siber dapat berkontribusi terhadap pengelolaan risiko privasi, namun hal tersebut belum cukup karena risiko privasi juga dapat muncul dengan cara yang tidak sama sekali terkait dengan insiden keamanan siber, seperti yang telah dicatat oleh GDPR *Enforcement Tracker* [2]



**Gambar 3. Risiko Cybersecurity vs Privacy (Sumber: NIST Privacy Framework)**

Dalam keamanan siber, khususnya dalam konteks NIST Cybersecurity Framework, area utama yang harus kita identifikasi adalah Aset, terutama aset kritikal atau istilah umum yang digunakan adalah **Crown Jewels Asset**. Dalam konteks *privacy*, identifikasi aset yang harus diproteksi direpresentasikan dalam bentuk pemrosesan data (personal data *processing activities*). Jika dalam menyusun strategi keamanan informasi kita harus melakukan identifikasi **Crown Jewels Asset** di awal, maka dalam *privacy*, yang harus diidentifikasi di awal adalah aktivitas pemrosesan apa saja yang melibatkan data pribadi. RUU PDP telah mendefinisikan arti dan jenis data pribadi.

Salah satu *framework* keamanan informasi yang sering digunakan adalah **NIST Cybersecurity Framework**, yang dimana memiliki lima domain, yaitu **Identify, Protect, Detect, Respond, dan Recover**. Mengingat **NIST Privacy Framework** adalah ekstensi dari **NIST Cybersecurity Framework**, maka kelima domain **NIST Cybersecurity Framework** tetap ada, namun dengan tambahan tiga domain baru, yaitu: **Govern, Control, dan Communicate**. Terdapat dua domain yang terintegrasi dengan keamanan informasi, yaitu **Identify-P** dan **Protect-P**.

Sebagai contoh, untuk domain **Identify**, pada NIST Cybersecurity Framework, kategori kontrol yang paling awal muncul adalah **Asset Management**. Dalam **NIST**

**Privacy Framework**, kategori kontrol yang muncul paling awal adalah *Inventory and Mapping*, yaitu dengan melakukan identifikasi pemrosesan data pribadi (*Record of Processing Activities - ROPA*), pencarian data pribadi pada sistem (*Data Discovery*), dan/atau pembaruan metadata. ROPA dapat dilakukan secara manual (disimpan dalam spreadsheet) maupun menggunakan *privacy management tools*. *Data Discovery* dapat dilakukan dengan *privacy management tools* atau memanfaatkan solusi *Data Loss/Leakage Prevention* (DLP) yang saat ini dimiliki organisasi. Sedangkan untuk pembaruan metadata, dapat dilakukan secara manual atau memanfaatkan solusi *Data Management* yang saat ini dimiliki.

Function Unique Identifier	Function	Category Unique Identifier	Category
ID-P	Identify-P	ID.IM-P	Inventory and Mapping
		ID.BE-P	Business Environment
		ID.RA-P	Risk Assessment
		ID.DE-P	Data Processing Ecosystem Risk Management
GV-P	Govern-P	GV.PO-P	Governance Policies, Processes, and Procedures
		GV.RM-P	Risk Management Strategy
		GV.AT-P	Awareness and Training
		GV.MT-P	Monitoring and Review
CT-P	Control-P	CT.PO-P	Data Processing Policies, Processes, and Procedures
		CT.DM-P	Data Processing Management
		CT.DP-P	Disassociated Processing
CM-P	Communicate-P	CM.PO-P	Communication Policies, Processes, and Procedures
		CM.AW-P	Data Processing Awareness
PR-P	Protect-P	PR.PO-P	Data Protection Policies, Processes, and Procedures
		PR.AC-P	Identity Management, Authentication, and Access Control
		PR.DS-P	Data Security
		PR.MA-P	Maintenance
		PR.PT-P	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

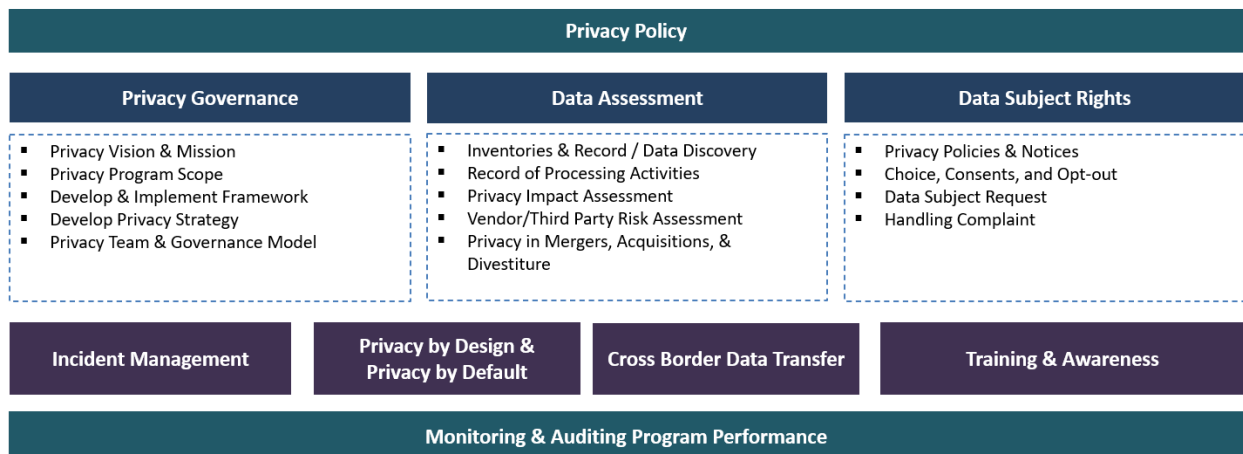
**Gambar 4 - Domain Privacy sebagai ekstensi dari domain Security di NIST Cybersecurity Framework (Sumber: NIST Privacy Framework)**

## APAKAH NIST PRIVACY FRAMEWORK SUDAH CUKUP UNTUK MENJADI PANDUAN BAGI ORGANISASI DALAM MERENCANAKAN PROGRAM PERLINDUNGAN DATA PRIBADI DAN PRIVASI?

Untuk panduan dasar, framework ini sudah cukup menjawab bagaimana menyusun rencana program keamanan informasi dan privasi yang selaras.

### Program Perlindungan Data dan Privasi - Domain

Berdasarkan buku *Privacy Program Management* yang dirilis oleh IAPP, *Data Privacy Program* merupakan pendekatan terstruktur yang menggabungkan beberapa disiplin ilmu ke dalam kerangka kerja (*framework*) yang memungkinkan organisasi memenuhi persyaratan kepatuhan hukum dan ekspektasi klien bisnis atau pelanggan dengan mempertimbangkan mitigasi risiko atas pelanggaran data. *Framework* ini dituangkan dalam rangkaian kebijakan privasi internal atau *privacy policy*. Berikut adalah rangkuman area yang dapat menjadi bahan pertimbangan dalam menyusun rencana program privasi.



**Gambar 5. Data Privacy Framework**

**Sumber: Hasil Analisis Penulis dari buku IAPP Privacy Program Management**

*Privacy Policy* harus memiliki kekuatan yang cukup tinggi di level kebijakan organisasi untuk memastikan bahwa seluruh unit kerja mematuhi apa yang telah diatur dalam



*Privacy Policy*. Selayaknya kebijakan pada umumnya, perlu dilakukan *review* dan pembaruan secara berkala, sehingga dibutuhkan aktivitas pemantauan dan audit (sebagaimana diperlukan) untuk memastikan bahwa program privasi termasuk *privacy policy* yang ada di dalamnya selalu menyesuaikan dengan konteks organisasi, rencana dan operasional bisnis, serta regulasi yang berlaku.

Pertanyaannya, apabila organisasi memiliki cabang perusahaan di berbagai negara, maka regulasi mana yang harus menjadi acuan bagi pembentukan suatu kebijakan privasi? Idealnya, *privacy policy* suatu organisasi harus mencakup ketentuan-ketentuan dan sesuai dengan seluruh peraturan perundang-undangan yang berdampak kepada organisasi tersebut. Maka, dibutuhkan suatu tim yang bertugas untuk menganalisis seluruh regulasi yang berlaku. Namun, organisasi dapat juga dapat mengacu kepada regulasi yang dianggap sebagai “*good practice*” dan memastikan bahwa seluruh kebijakan privasi telah menganut prinsip-prinsip perlindungan data pribadi.

Untuk memastikan bahwa program perlindungan data pribadi dan privasi dijalankan secara efektif, maka perlu ditentukan pengukuran dan metrik yang jelas bisa dalam bentuk KPI, KRI, dan/atau OKR. Berdasarkan survei IAPP [2], tanggap insiden menjadi metrik yang paling banyak dilaporkan kepada Manajemen, dimana hal ini sangat selaras dengan metrik keamanan informasi yang juga dilaporkan ke Manajemen. DPIA / PIA menempati posisi berikutnya mengingat pentingnya aktivitas ini dalam mengidentifikasi dan menentukan rencana mitigasi risiko-risiko privasi. Dalam keamanan informasi “*human is the weakest link in cybersecurity*” , hal tersebut berlaku dalam praktik privasi juga sehingga training dan awareness harus menjadi metrik wajib dalam program perlindungan data pribadi dan privasi.

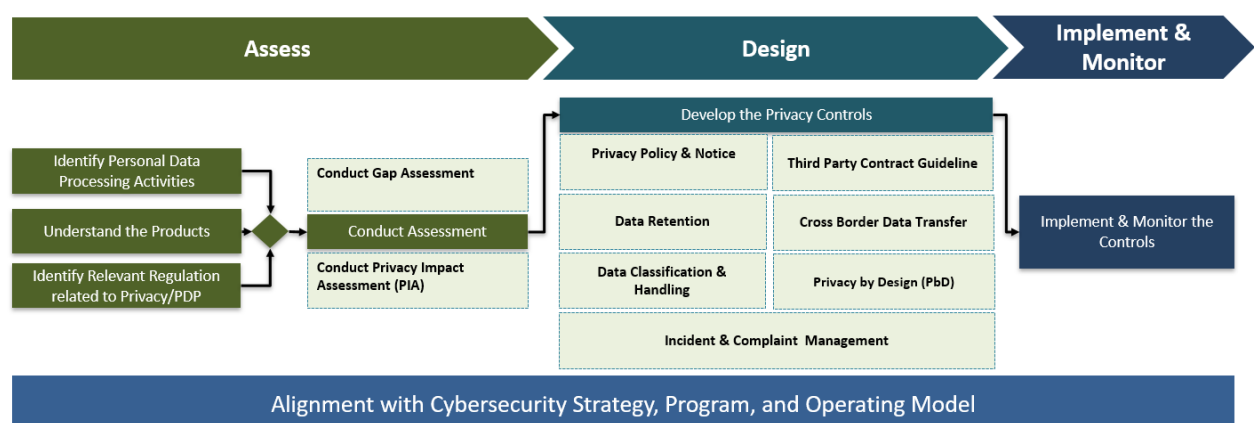
## Program Perlindungan Data dan Privasi - Process

---

Bagaimana cara menyusun dan mengimplementasikan program perlindungan data pribadi? Secara umum, kita dapat melakukan penilaian (*assessment*) terlebih dahulu terkait dengan kesiapan kita dalam mengidentifikasi tiga hal, yaitu:

- a. Proses bisnis yang melibatkan pemrosesan data pribadi;
- b. Produk dan/atau layanan yang diberikan organisasi kepada penggunanya; dan
- c. Regulasi terkait perlindungan data pribadi yang relevan dengan organisasi.

Ketika sudah dapat mengidentifikasi ketiga hal tersebut, maka organisasi dapat mempertimbangan untuk menyusun *framework* perlindungan data pribadi yang dapat diadopsi sesuai dengan nature of business serta kapasitas dari organisasi. Umumnya, organisasi akan membentuk ***framework* berbasis NIST Privacy Framework, ISO 27701 dan custom framework** baik yang dikembangkan internal maupun dibantu oleh pihak eksternal / konsultan. Jika organisasi telah memiliki *framework* yang jelas, maka aktivitas berikutnya adalah melakukan penilaian kesenjangan dan/atau kematangan dari organisasi terhadap *framework* yang telah diadopsi tersebut. Kesenjangan yang ditemukan dalam penilaian kesenjangan dan/atau kematangan dapat menjadi landasan organisasi dalam menyusun inisiatif-inisiatif di masa depan. Penilaian lain yang sangat penting dilakukan organisasi adalah *Privacy Impact Assessment* ( "**PIA**" ). Penilaian risiko privasi akan menghasilkan kontrol untuk melakukan mitigasi risiko-risiko privasi.



**Gambar 6. Proses penilaian, perencanaan, penerapan, dan pemantauan program perlindungan data pribadi (Sumber: Hasil Analisis Penulis)**

Setelah mengetahui kesenjangan dan risiko privasi, maka organisasi harus menentukan bentuk implementasi dari kontrol, baik dalam bentuk penyusunan kebijakan dan prosedur, manajemen insiden dan komplain, serta **Privacy by Design**. Pada saat mengembangkan kontrol, organisasi perlu memperhatikan kontrol-kontrol yang sifatnya teknis dan organisasi. Pada tahap implementasi dan pemantuan kontrol, hal-hal yang harus diperhatikan adalah:

- Melakukan review dan pembaruan RoPA (*Record of Processing Activities*) dan PIA (*Privacy Impact Assessment*);
- Melakukan review dan pembaruan kebijakan dan prosedur terkait perlindungan data pribadi dan privasi;
- Melakukan *training* dan *awareness* kepada karyawan serta ekosistem secara berkala;
- Melakukan penyelarasan (*alignment*) antara program perlindungan data pribadi dan privasi dengan program keamanan informasi yang sudah ada di organisasi;
- Melakukan penilaian kapabilitas dan/atau audit secara berkala;
- Meningkatkan kapabilitas organisasi dalam menerapkan pengelolaan data (*data management*).

Dari aspek teknologi, memang disarankan organisasi untuk menggunakan **privacy management tools** untuk memudahkan pengelolaan program perlindungan data pribadi. Namun, organisasi perlu memperimbangkan beberapa hal, misalnya besar data pribadi yang diproses, seberapa banyak kerja sama dengan pihak ketiga, ketersediaan sumber daya internal, dan anggaran. Beberapa solusi keamanan informasi yang dapat mendukung implementasi program perlindungan data pribadi dan privasi adalah *Data Discovery, Encryption, Tokenization, Database Security, Key and Certificate Management, Digital Rights Management, dan/atau Data Loss/Leakage Prevention (DLP)*.

## **Peran Pejabat Perlindungan Data Pribadi (PPDP) / DPO**

---

Berdasarkan banyak regulasi yang telah dikeluarkan oleh berbagai negara, PPDP/DPO harus memiliki posisi yang independent, dimana PPDP/DPO dapat memberikan nasihat/anjuran terkait dengan pemrosesan data kepada manajemen perusahaan atau petinggi organisasi tanpa adanya tekanan. Sebagai contoh GDPR, juga memberikan keleluasaan kepada perusahaan atau organisasi untuk memenuhi kewajiban penunjukan PPDP/DPO melalui metode outsource. Dalam hal ini, suatu perusahaan dan organisasi dapat memiliki kebebasan untuk menentukan posisi PPDP/DPO, apakah ditempatkan di suatu departemen tertentu (misalnya: departemen legal,

departemen IT), merupakan gabungan dari berbagai departemen, atau diberikan kepada pihak ketiga. Kita harus memahami bahwa tidak ada kebijakan **“one fits all”** terkait dengan bentuk dan posisi PPDP/DPO karena setiap perusahaan atau organisasi memiliki skala yang berbeda, baik dari jumlah sumber daya manusia yang dapat menangani isu perlindungan data pribadi maupun volume data yang dikelola. Sehingga, selama fungsi PPDP/DPO dapat dijalankan dengan baik, dimana tim memiliki akses langsung ke manajemen dan dapat memberikan nasihat tanpa adanya tekanan, maka hal tersebut dapat telah dianggap memenuhi ketentuan terkait dengan PPDP/DPO.

Kesuksesan sebuah program ditentukan juga berdasarkan kompetensi tim yang mengelola program tersebut. Pelindungan data pribadi merupakan topik yang cukup baru, apalagi di Indonesia yang belum memiliki regulasi komprehensif terkait dengan pelindungan data pribadi. Untuk menerapkan suatu kompetensi tertentu dengan kewajiban sertifikasi yang berat tentu membutuhkan waktu untuk dapat diterima oleh masyarakat dan industri. Di banyak negara, ekosistem PPDP/DPO juga berjalan secara alami, dimana semakin banyak organisasi yang menerapkan praktik pelindungan data pribadi yang mutakhir, maka praktisi juga akan semakin termotivasi untuk meningkatkan kapabilitasnya agar diterima oleh pasar. Oleh sebab itu, kami menyarankan bahwa PPDP/DPO sebaiknya berlatar belakang hukum dan/atau IT, serta memiliki edukasi dan pengalaman kerja menangani isu data pribadi.

Keselarasan program, dalam hal ini perlindungan data pribadi dan keamanan informasi, ditentukan juga oleh kolaborasi dengan *key partners* yang terkait dengan perencanaan dan penerapan praktik perlindungan data pribadi. Berbagai program terkait dengan perlindungan data pribadi harus memperoleh persetujuan dan dukungan dari manajemen, sehingga, ini adalah suatu hal yang penting untuk dapat meyakinkan pemilik perusahaan dan/ atau petinggi organisasi terkait dengan pentingnya perlindungan data pribadi untuk keberlanjutan suatu usaha. Dalam menjalankan program perlindungan data pribadi, dibutuhkan dukungan dari berbagai departemen. **“It takes a village to create a sustainable privacy program”** . Tim legal untuk membentuk kebijakan internal dan perjanjian *transfer* data dengan pihak ketiga,

tim kebijakan publik dan hubungan pemerintah untuk memastikan keterlibatan pemerintah dalam program dan apakah program tersebut sudah sesuai dengan regulasi serta program pemerintah, tim humas untuk memastikan keterlibatan masyarakat, tim IT untuk menerapkan kontrol atas data pribadi yang dikelola oleh perusahaan dan masih banyak tim lainnya yang harus dilibatkan sesuai dengan bentuk dan skala program yang akan dijalankan.

## Penutup

---

Dalam tulisan ini, penulis ingin menyampaikan pentingnya pembentukan Program Keamanan Informasi guna menunjang tata Kelola perlindungan data pribadi yang baik. Keamanan informasi dan perlindungan data pribadi merupakan dua hal yang saling terkait dan tidak dapat dipisahkan. Maka, suatu organisasi yang memproses data pribadi dan ingin memulai membentuk Program Keamanan Informasi dapat melakukan hal sebagai berikut:

- Melakukan investasi pada sumber daya manusia yang mumpuni dan memiliki pengetahuan serta pengalaman di bidang keamanan informasi dan perlindungan data pribadi;
- Membentuk tim yang terdiri dari praktisi yang memiliki pengalaman di bidang hukum, keamanan informasi, manajemen data, dan/atau manajemen risiko;
- Membentuk *privacy policy* dan *privacy notice* sesuai dengan pemrosesan data yang dilakukan oleh internal perusahaan, contohnya: kebijakan manajemen insiden kebocoran data. *Privacy policy* juga harus diumumkan kepada karyawan dan direvisi dari waktu ke waktu sesuai dengan perkembangan pemrosesan data serta peraturan perundang-undangan; dan
- Membentuk program perlindungan data pribadi yang berkelanjutan mencakup pelatihan bagi pegawai maupun ekosistem pihak ketiga yang terkait, misalnya: pengguna aplikasi. Sehingga baik karyawan dan pengguna memahami kebijakan serta fitur yang digunakan oleh organisasi untuk meningkatkan keamanan informasi dan melindungi data pribadi.

## Referensi

---

- [1]. <https://www.enforcementtracker.com/?insights>
- [2]. <https://iapp.org/resources/article/privacy-governance-report/>
- [3]. <https://iapp.org/resources/article/privacy-program-management/>

### TENTANG PENULIS



#### **Eryk Budi Pratama**

M.Kom, M.M., CIPM, CIPP/E, FIP

<https://www.linkedin.com/in/erykbudipratama/>

Eryk merupakan praktisi dan konsultan di bidang Keamanan Informasi, Perlindungan Data, dan Privasi Data di salah satu organisasi global ternama, serta **Chapter Chair** untuk **International Association of Privacy Professionals** (IAPP) Jakarta. Memiliki pengalaman dalam memberikan konsultansi dan implementasi kontrol keamanan informasi di berbagai jenis organisasi dan industri, baik dalam maupun luar negeri. Eryk banyak membantu organisasi mulai dari tahap perencanaan, penyusunan strategi, penilaian kapabilitas dan maturity, penyusunan framework, penyusunan dokumentasi, pengujian teknis, dan penilaian non-teknis terhadap penerapakan keamanan informasi, keamanan siber, dan perlindungan serta privasi data.



#### **Ardhanti Nurwidya**

S.H., L.L.M, CIPP/E

<https://www.linkedin.com/in/ardhanti-nurwidya-9a466245/>

Ardhanti merupakan praktisi perlindungan data pribadi yang saat ini berprofesi sebagai VP Public Policy and Government Relation di salah satu grup teknologi besar di Indonesia dan pengurus dari Asosiasi Praktisi Perlindungan Data Indonesia (APPDI). Ardhanti memiliki pengalaman sebagai legal counsel

dan memiliki lisensi PERADI. Ardhanti memiliki pengalaman membangun kolaborasi dan kerja sama dengan berbagai institusi pemerintah di Indonesia maupun Regional.



# MANAJEMEN KEAMANAN MULTI CLOUD

oleh Eryk Budi Pratama dan Novita Handayani Koswara



## Transformasi ke Cloud

---

Saat ini adopsi *cloud* bukanlah hal baru, terutama bagi organisasi yang memang *cloud-native* atau *technology company* yang umumnya menggunakan pendekatan *agile* dalam pengembangan produk berbasis *cloud*. Menurut survei Gartner [1], pada tahun 2025 lebih dari 50% organisasi akan beralih atau memindahkan aplikasi, sistem, dan/atau infrastrukturnya ke *cloud*, tergantung dari *cloud service* model yang diadopsi. Berdasarkan pengalaman penulis, untuk organisasi yang memiliki banyak infrastruktur di *on-premises*, atau yang umum dikenal sebagai “non-cloud-native”, umumnya akan mempertimbangkan aspek biaya dan risiko ketika ingin melakukan migrasi ke *cloud*. Aspek biaya tentu menjadi prioritas pertimbangan dalam menentukan sejauh apa adopsi dan/atau migrasi *cloud* dilakukan. Hal ini tentu juga tergantung pada sejauh apa kebutuhan bisnis terhadap penggunaan *cloud*. Aspek risiko (terutama isu keamanan siber) dan kesiapan sumber daya manusia internal tentu



menjadi pertimbangan dalam menentukan penggunaan *cloud*. Risiko terkait pemenuhan regulasi yang mengatur penyimpanan dan perlindungan data juga menjadi perhatian utama untuk saat ini, mengingat banyaknya kasus kebocoran data dan akan adanya RUU yang mengatur perlindungan data pribadi.

Setidaknya ada dua pertimbangan dalam menentukan adopsi dan/atau migrasi *cloud*, yaitu aspek komersial dan teknis. Aspek komersial cukup jelas, yaitu mempertimbangkan berbagai skenario adopsi *cloud*, misalnya bagaimana kombinasi terbaik (*hybrid cloud*) untuk penggunaan DC/DRC berbasis *public cloud*, *private cloud*, atau *on-premises*. Dari aspek teknis, beberapa hal yang dipertimbangkan mencakup kebutuhan keamanan (*security requirements*), kinerja (*performance*), *performance availability*, skalabilitas, *technology support*, dan lain-lain. Dengan asumsi organisasi akan mengadopsi *public cloud*, ada satu hal yang ingin dihindari yaitu ketergantungan terhadap satu penyedia (*vendor lock-in*). Hal tersebut menjadi pertimbangan juga untuk mengadopsi lebih dari satu *public Cloud Service Provider* (CSP). Survei dari Tripwire and Dimensional Research [2] pada tahun 2021 menunjukkan bahwa 73% dari responden saat ini beroperasi di *multi-cloud environment*. Pro dan kontra tentunya ada, ditinjau dari sisi ketersediaan dan kapabilitas SDM internal, teknologi yang tersentral untuk mengelola keamanan cloud, dan tata kelola keamanan *multi-cloud*.

## Tata Kelola Keamanan Multi Cloud

---

Keamanan multi-cloud menjadi hal yang penting bagi organisasi yang mempunyai atau mengadopsi infrastruktur *multi-cloud*. Data yang berpindah dari satu *Cloud Service Provider* (CSP) ke CSP yang lain dapat menjadi kerentanan sistem (*system vulnerability*). Untuk memastikan sistem keamanan dari infrastruktur *multi-cloud*, organisasi dapat memilih untuk mengadopsi *framework* dan/atau standar keamanan cloud yang tersedia seperti *Cloud Security Alliance* (CSA) *Cloud Control Matrix* (CCM), ISO 27017, NIST *Guideline on Security and Privacy in Public Cloud Computing*, dan lain-lain sesuai dengan kebutuhan. Dari pengalaman dalam implementasi *multi-cloud*, penulis menggunakan *customized framework* yang umumnya berasal dari gabungan beberapa *framework* dan standar.

[illegible]

CSA sudah menyusun *Critical Areas of Focus* atau area utama yang dapat diprioritaskan organisasi dalam melakukan penilaian kapabilitas dan implementasi tata kelola dan manajemen keamanan *cloud*. Kami setuju bahwa cara efektif penerapan kontrol keamanan *cloud* adalah dengan menerapkan kontrol teknis / konfigurasi terhadap

*cloud platform* dan *instances / resources* di atasnya. Namun, dalam konteks tata kelola dan manajemen keamanan *cloud* untuk organisasi, dengan mempertimbangkan beberapa hal berikut:

- Jumlah *cloud services* dan *computing resources* yang digunakan,
- Integrasi *on-premises* dan *cloud (hybrid cloud)*,
- Letak geografis kantor cabang atau perwakilan organisasi (jika ada)
- Letak penyimpanan data sensitif dan data pribadi (hal ini berhubungan dengan kepatuhan terhadap regulasi yang berlaku),
- Jumlah *public cloud provider* yang digunakan, dan
- Jumlah organisasi yang *cloud resources*-nya dikelola secara tersentral,

maka perencanaan, tata kelola, dan manajemen keamanan *cloud* perlu dilakukan secara efektif dan efisien. Beberapa area utama yang perlu diperhatikan untuk keamanan *cloud* mencakup namun tidak terbatas pada arsitektur, tata kelola, manajemen risiko, aspek hukum, tata kelola informasi, keamanan infrastruktur, keamanan aplikasi, keamanan data, manajemen insiden, manajemen identitas dan akses, dan integrasi antar CSP.

	Architectural Relevance						Corp Gov Relevance	Cloud Service Delivery Model Applicability			Supplier Relationship		AICPA 2009 TSC Map	AICPA Trust S
	Phys	Network	Compute	Storage	App	Data		SaaS	PaaS	IaaS	Service Provider	Tenant / Consumer		
m,ols		X	X	X	X	X		X	X	X	X	X	S3.2.g	(S3.2.g superu: and ser
ering stability /or file re	X	X	X	X	X	X	X	X	X	X	X		S3.7	(S3.7) I system

Gambar 2. Kertas Kerja CSA CCM (Sumber: CSA CCM)

Sebagai tambahan informasi, CSA CCM ini cukup memudahkan organisasi baik yang bertindak sebagai *Service Provider* maupun *Tenant / Pengguna cloud* karena pada kertas kerja CSA CCM karena terdapat informasi kontrol-kontrol terkait yang juga dapat diterapkan untuk *Service Provider*, *Tenant*, atau keduanya. Selain itu terdapat

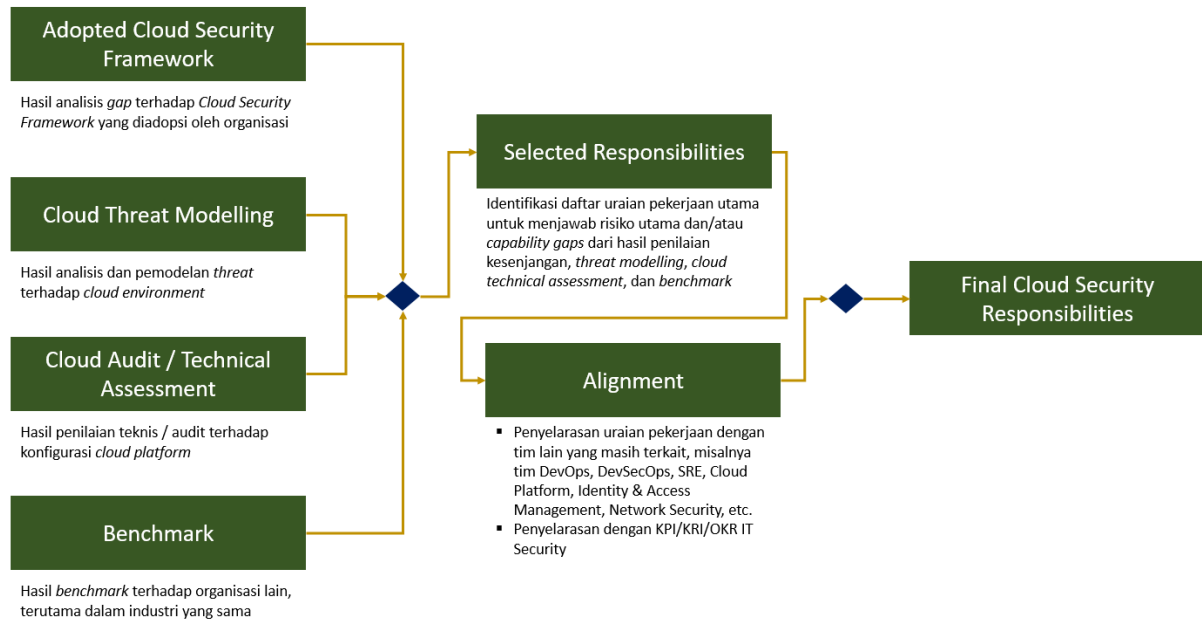
informasi *applicability* terhadap jenis layanan cloud yang digunakan, apakah IaaS (*Infrastructure as a Service*), PaaS, dan/atau SaaS (*Security as a Service*). Mengingat terdapat pemetaan terhadap berbagai *framework*, standar, dan *common practice*, maka organisasi dapat melakukan kustomisasi CSA CCM sesuai kebutuhan.

## Kompetensi Tim Cloud Security

---

Kemampuan dan kompetensi SDM internal dalam mengelola keamanan cloud, menjadi salah satu kunci keberhasilan pelaksanaan tata kelola keamanan *multi-cloud*, terlepas semua uraian pekerjaan dilakukan internal maupun ada sebagian yang diserahkan ke MSSP. Pertanyaannya, bagaimana mekanisme penyusunan kompetensi minimal tim *cloud security* yang sesuai dengan organisasi? Apa saja uraian pekerjaannya?

Pendekatan yang digunakan organisasi bisa berbeda dalam menentukan kompetensi dan uraian pekerjaan tim *cloud security*. Secara sederhana, organisasi dapat melakukan *benchmark* langsung dari organisasi lain yang telah atau akan memiliki tim *cloud security*. Standar kompetensi yang bersifat nasional maupun internasional (misalnya NIST *Cybersecurity Workforce* - NICE) pun juga dapat digunakan. Dari pengalaman kami, berikut adalah ilustrasi penyusunan kompetensi dan uraian pekerjaan dari tim *cloud security*.



Gambar 3 - Mekanisme penyusunan kompetensi tim cloud security (Sumber: Hasil Analisis Penulis)

Masukan awal atas kebutuhan terhadap keamanan *cloud* diidentifikasi dari beberapa aktivitas, yang mencakup namun tidak terbatas pada:

- Hasil analisis kesenjangan terhadap *framework* keamanan siber dan/atau *cloud security* yang diadopsi oleh organisasi, baik yang *customized* maupun *off-the shelf* (misalnya CSA Cloud Control Matrix – CSA CCM);
- Hasil pemodelan ancaman cloud (*threat modeling*);
- Hasil penilaian dan pengujian teknis atas penerapan kontrol *cloud security* yang dapat mengacu pada *common practice* seperti CIS Benchmark; dan
- Hasil *benchmark* terhadap organisasi lain.

Hasil penilaian di atas tentunya akan menghasilkan sedikit atau banyak *area of improvement* yang untuk selanjutnya akan diprioritaskan berdasarkan beberapa pertimbangan, misalnya terhadap aspek risiko, biaya, kemudahan implementasi, ketersediaan sumber daya, dan lain-lain. Prioritas inisiatif yang telah ditentukan, nantinya akan diselaraskan dengan uraian pekerjaan dari tim lain yang masih terkait dengan cloud. Hal ini untuk memastikan tidak ada pekerjaan yang timpang tindih dan akuntabilitas yang jelas. Selanjutnya organisasi dapat menentukan kriteria penilaian kinerja karyawan, dalam hal ini tim *cloud security*. Beberapa contoh uraian pekerjaan

dari *cloud security* yang kami ambil dari beberapa sumber website penyedia lowongan kerja.

- Menyusun rencana dan strategi implementasi kontrol keamanan *multi-cloud*
- Merancang dan mengembangkan arsitektur keamanan *multi-cloud*
- Implementasi kontrol keamanan *multi-cloud*
- Menerapkan otomatisasi solusi dan proses keamanan untuk *multi-cloud*
- Terlibat dalam proses manajemen insiden keamanan informasi yang melibatkan *cloud environment*
- Melakukan *vulnerability assessment* secara rutin terhadap *multi-cloud platform*
- Mendukung tim DevOps dalam melakukan otomatisasi proses deployment di cloud
- Melakukan pemetaan dan pemodelan ancaman (*threat*) di cloud
- Melakukan *hardening* dan *patching* secara rutin
- dan lain-lain

Untuk menjalankan uraian pekerjaan tersebut, tentunya tim *cloud security* dituntut untuk menguasai lebih dari satu cloud platform yang digunakan oleh organisasi, *automation tools*, dan tentunya menerapkan *automation* terhadap *security tools*. Sebagai tambahan saja, jika organisasi anda memiliki tim IT GRC, maka pekerjaan yang berkaitan dengan penyusunan *framework*, kebijakan, dan prosedur dapat diserahkan ke tim tersebut. Untuk hal yang lebih teknis, misalnya petunjuk teknis dan petunjuk pelaksanaan, tim *cloud security* dapat berkontribusi lebih banyak dalam proses penyusunannya.

## Pengujian dan Pemantauan Keamanan Cloud

---

Pengujian keamanan dan kerentanan pada suatu sistem umumnya dilakukan dengan dua cara, yaitu *Vulnerability Assessment & Penetration Testing* (VAPT) dan *hardening/configuration review*. Dari pengalaman kami, VAPT di cloud tidak jauh berbeda dengan VAPT pada umumnya yang dilakukan terhadap aplikasi, infrastruktur (*server*), dan perangkat network. Namun, setidaknya ada dua hal yang perlu diperhatikan dan menjadi tantangan bagi para *pentester*.

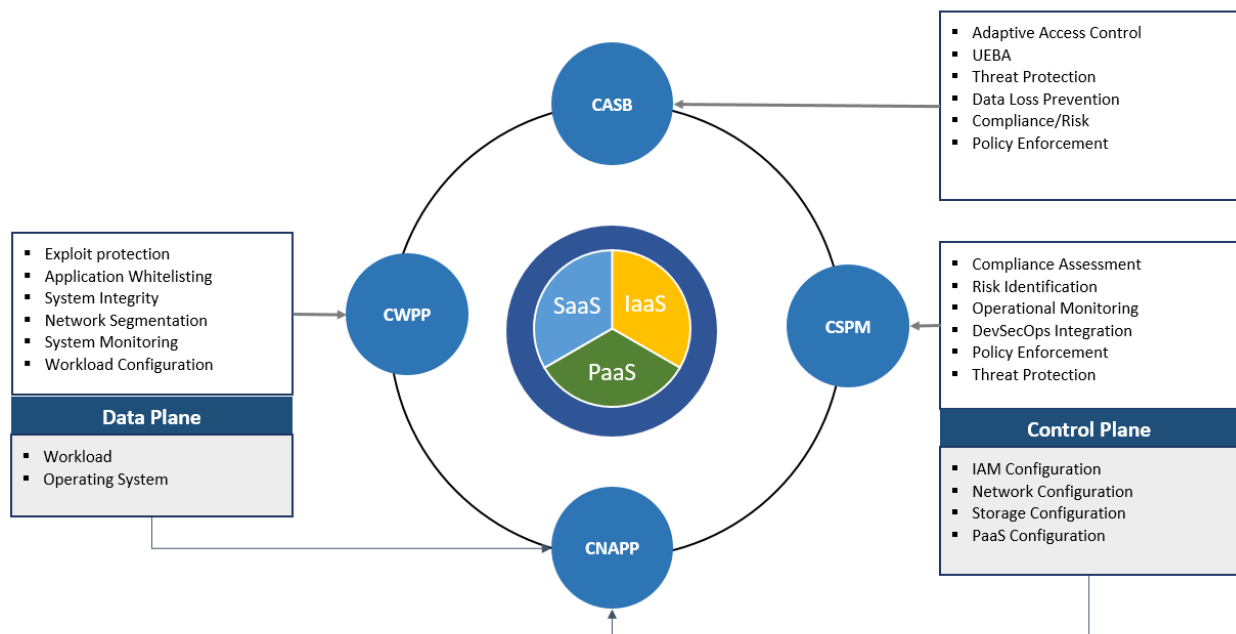
- **Perizinan.** Jika melakukan VAPT di *on-premises environment*, jika dilakukan oleh pihak eksternal, maka diperlukan dokumen legal seperti perjanjian kerja sama/kontrak kerja dan NDA. Namun jika dilakukan di *cloud*, maka kita perlu mendapatkan izin dari CSP juga. Tentunya hal ini tergantung dari kebijakan masing-masing CSP dan target VAPT-nya, apakah SaaS, PaaS, dan IaaS.
- **Network Protection-by-default.** Dengan adanya *shared responsibilities* antara CSP dan tenant, hal tersebut membuat adanya distribusi kontrol keamanan, yang dalam hal ini tentunya tenant tidak akan bisa mengakses sumber daya komputasi sampai ke layer paling bawah. Sebagai contoh, anggap saja kita whitelist IP *address pentester* dan semua protection rules kita bypass. Ketika terdapat suatu aktivitas pengujian tertentu, masih memungkinkan untuk dideteksi dan diblokir oleh CSP (misalnya DDoS), meskipun semua proteksi di sisi kita telah ditanggalkan.

Cukup banyak referensi yang dapat dicari untuk melakukan pengujian keamanan pada cloud, salah satunya repo Github <https://github.com/4AndersonLin/awesome-cloud-security>. CSP yang umumnya diulas adalah AWS, GCP, dan Azure. Dari pengalaman kami melakukan pengujian keamanan multi-cloud, baik dengan bantuan *Cloud Security Posture Management (CSPM) tools* maupun manual, berikut adalah daftar kerentanan yang umumnya ada.

- Penggunaan *Multi Factor Authentication* untuk akun dengan *privilege* tinggi/tertinggi (misalnya *root*)
- *Cloud storage* yang dapat diakses secara publik
- Enkripsi pada *cloud disk/storage* tidak diaktifkan
- *Firewall rules* di *cloud platform* mengizinkan beberapa port dapat diakses publik, misalnya HTTP, SSH, Database, RDP, dan lain-lain. (Kami menyarankan port tersebut dapat diakses jika sudah terkoneksi dengan VPN)
- "ANY-ANY" pada konfigurasi *firewall rules* (untuk hal ini perlu validasi secara manual)
- Konfigurasi *password policy* yang tidak sesuai kebijakan/standar organisasi
- *Dormant account* atau akun yang sudah tidak aktif digunakan melebihi jangka waktu tertentu yang ditentukan oleh organisasi
- dan lain-lain.

## Tentang Cloud Security Posture Management (CSPM)

Sebelum kami menjelaskan tentang salah satu jenis solusi untuk menilai dan memantau kerentanan *multi-cloud*, kami ingin memberikan gambaran bahwa terdapat beberapa jenis solusi keamanan *multi-cloud* yang umumnya diadopsi oleh organisasi berdasarkan dari penelitian Gartner.



Gambar 4 - Beberapa solusi keamanan cloud (Sumber: Penelitian Gartner yang dirangkum oleh Penulis)

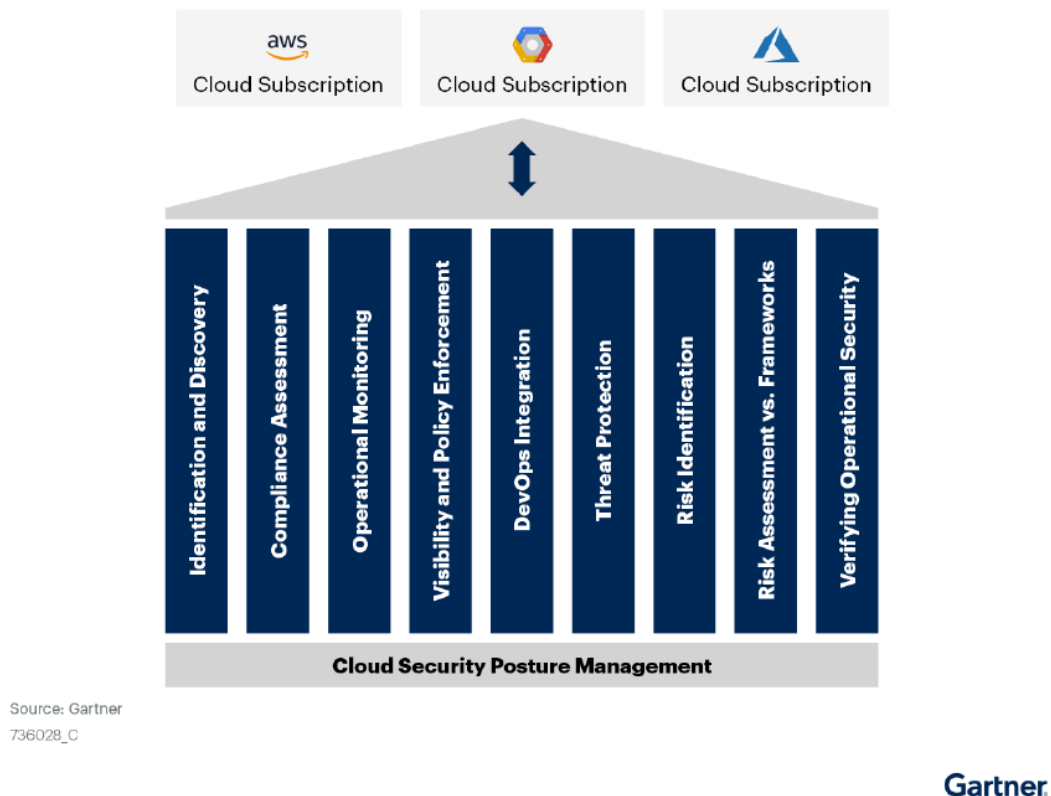
Beberapa solusi yang umumnya dapat diadopsi organisasi dalam menerapkan kontrol keamanan multi-cloud.

- *Cloud Access Security Brokers (CASB)*
- *Cloud-Native Application Protection Platforms (CNAPP)*
- *Cloud Workload Protection Platforms (CWPP)*
- *Cloud Security Posture Management (CSPM)*

Pada tulisan ini, kami hanya membahas secara singkat tentang CSPM. Secara sederhana, CSPM dapat diibaratkan seperti *vulnerability management tools*, namun spesifik untuk cloud dan dapat terintegrasi dengan proses DevSecOps. Menurut Gartner [4], CSPM merupakan solusi yang secara berkelanjutan dapat mengelola



postur keamanan cloud melalui pencegahan, deteksi, respons, dan identifikasi proaktif dari risiko infrastruktur *cloud*. Seperti yang kita ketahui bahwa kontrol keamanan *cloud* dapat diterapkan terhadap dua komponen, yaitu *Data Plane* dan *Control Plane*. Fungsi dari CSPM adalah untuk memproteksi *control plane*, yang dalam hal ini mencakup konfigurasi IAM, *storage*, *network*, dan *cloud-native function*. Jika ingin melakukan proteksi terhadap workload, maka CWPP tools dapat digunakan. Berikut adalah beberapa kapabilitas CSPM.



Gambar 5 Kapabilitas CSPM

Sumber: Gartner - How to Protect Your Clouds With CSPM, CWPP, CNAPP and CASB

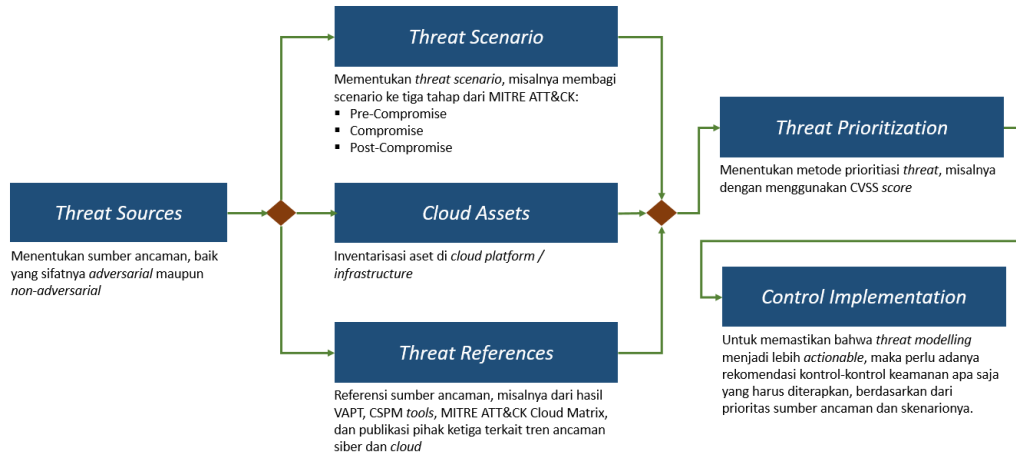
Apakah semua fitur CSPM perlu digunakan? Belum tentu. Tergantung dari kebutuhan organisasi, terutama jika menggunakan solusi CSPM yang berbayar, bisa saja ada biaya lisensi tersendiri untuk masing-masing fitur. Kemudian, seberapa efektif CSPM dalam mendeteksi kerentanan di cloud? Berdasarkan pengalaman penulis, hal tersebut tergantung dari seberapa banyak jumlah aset yang didaftarkan di dalam CSPM dan juga *detection rules/policy* yang digunakan. Kelebihan tools berbayar memang umumnya sudah menyediakan *out-of-the-box rules/policy* yang tinggal digunakan. Untuk *use cases* tertentu, pastinya kita perlu untuk membuat *custom rules/policy*.

## Pemodelan Ancaman Cloud (Cloud Threat Modeling)

---

Melakukan pemodelan ancaman (*threat modeling*) atau penilaian ancaman (*threat assessment*) itu antara tidak terlalu penting dan penting, tergantung kebutuhan organisasi. *Threat modeling* bisa jadi tidak terlalu penting, karena organisasi mengharapkan "*current real threat*", yaitu ancaman yang memang benar-benar telah terdeteksi dan relevan dengan organisasi, bukan yang "berpotensi" akan terjadi. Misalnya ancaman yang berhasil terdeteksi dari perangkat keamanan (EDR, IDS/IPS, SIEM, dan lainnya). Untuk mendapatkan ancaman yang nyata saat ini, tidak perlu harus membuat suatu pemodelan. Cukup minimal dari perangkat SIEM akan dapat informasinya. Informasi dari *threat intelligence feed* pun tidak terlalu bernilai jika tidak dikorelasi dengan informasi internal yang dimiliki oleh organisasi. *Threat modeling* bisa menjadi penting, jika pemodelan ancaman ini menjadi konsumsi tidak hanya tim *IT Security*, namun juga tim lain yang terkait, misalnya tim Manajemen Risiko, Audit Internal, atau tim produk. Pada suatu kasus, bahkan aktivitas yang dibantu *tools* khusus *threat modeling* ini terintegrasi dengan *ticketing system* yang digunakan oleh seluruh tim, sehingga munculnya suatu *security requirements* pada produk dan *deployment* memiliki landasan dan sudah selaras dengan ancaman saat ini maupun potensi ancaman yang dihadapi oleh organisasi.

Terdapat beberapa metode yang umum digunakan untuk *threat modeling*, yaitu STRIDE, PASTA, Attack Trees, VAST, OCTAVE, dan lain-lain. Kemudian, bagaimana untuk cloud? Pada dasarnya menggunakan metode yang paling umum digunakan seperti STRIDE masih dimungkinkan. Namun, mempertimbangkan tren ancaman yang semakin "*advanced / sophisticated*", maka berdasarkan pengalaman kami, dapat menggunakan pendekatan berbasis MITRE ATT&CK. MITRE memiliki Cloud Matrix [5] yang dapat memudahkan kita untuk menentukan *threat actor* TTPs terhadap cloud. Pendekatan *cloud threat modeling* yang dapat digunakan sebagaimana pada Gambar 6.



Gambar 6. Mekanisme penyusunan *cloud threat modeling* (Sumber: Hasil Analisis Penulis)

Menurut penulis, secara praktikal, kita dapat fokus langsung ke *threat references*. Sebagai contoh, kita menentukan referensi utama adalah MITRE ATT&CK Cloud Matrix. Kemudian setelah menentukan daftar *cloud assets* yang menjadi ruang lingkup, selanjutnya kita dapat membagi dulu taktik menjadi tiga bagian, yaitu *Pre-Compromise*, *Compromise*, dan *Post Compromise*.

Pre-Compromise	Compromise								Post-Compromise	
Initial Access 5 techniques	Execution 1 techniques	Persistence 5 techniques	Privilege Escalation 2 techniques	Defense Evasion 7 techniques	Credential Access 5 techniques	Discovery 12 techniques	Lateral Movement 3 techniques	Collection 4 techniques	Exfiltration 1 techniques	Impact 6 techniques
Drive-by Compromise Exploit Public-Facing Application Phishing (1) Trusted Relationship Valid Accounts (2)	User Execution (1)	Account Manipulation (2) Create Account (1) Implant Internal Image Office Application Startup (6) Valid Accounts (2)	Domain Policy Modification (1) Valid Accounts (2)	Domain Policy Modification (1) Hide Artifacts (1) Impair Defenses (3) Modify Cloud Compute Infrastructure (4) Unused/Unsupported Cloud Regions Use Alternate Authentication Material (2) Valid Accounts (2)	Brute Force (4) Forge Web Credentials (2) Steal Application Access Token Steal Web Session Cookie Unsecured Credentials (2)	Account Discovery (2) Cloud Infrastructure Discovery Cloud Service Dashboard Cloud Service Discovery Cloud Storage Object Discovery Network Service Scanning Password Policy Discovery Permission Groups Discovery (1) Software Discovery (1) System Information Discovery System Location Discovery System Network Connections Discovery	Internal Spearphishing Taint Shared Content Use Alternate Authentication Material (2)	Data from Cloud Storage Object Data from Information Repositories (3) Data Staged (1) Email Collection (2)	Transfer Data to Cloud Account	Data Destruction Data Encrypted for Impact Defacement (1) Endpoint Denial of Service (3) Network Denial of Service (2) Resource Hijacking

Gambar 7. Mekanisme penyusunan cloud threat modeling (sumber: MITRE ATT&CK Cloud Matrix dan Hasil Analisis Penulis)

Dalam menentukan potensi ancaman, pertama kita tentukan dulu daftar aset yang terdampak. Pendekatannya bisa per jenis aset (misalnya *cloud firewall*), maupun gabungan dari beberapa jenis aset yang dimiliki organisasi (misalnya perangkat keamanan – *cloud firewall* dan WAF, infrastruktur aplikasi – API *Gateway* dan *load balancer*). Setelah aset teridentifikasi, kemudian kita dapat menentukan potensi ancaman, misalnya *misconfiguration*, *unauthorized changes*, *account hijacking*, *missing MFA*, dan lain-lain. Sebagai pelengkap, kita bisa menambahkan pemetaan ancaman ke komponen STRIDE yang relevan, CVE, CWE, dan sejenisnya. Untuk menentukan tingkat risiko dari ancaman, dapat ditambahkan juga CVSS score atau metode pengukuran risiko lainnya yang digunakan oleh organisasi. Agar potensi ancaman mendekati apa yang memang sedang dihadapi oleh organisasi, maka kita dapat menyertakan hasil VAPT, *configuration review*, temuan CSPM tools, informasi dari *threat intelligence feeds*, maupun sumber data kerentanan yang lainnya. Seperti yang telah kami sebutkan bahwa *threat modeling* ini sebaiknya *actionable*, sehingga dalam laporan pemodelan ancaman, kita dapat menambahkan informasi terkait kontrol keamanan apa saja yang saat ini telah diimplementasikan oleh organisasi. Kita perlu mencari *benchmark* juga terkait *common practice* apa saja yang dapat diterapkan untuk potensi ancaman yang sedang dianalisis. Kontrol keamanan dapat bersifat pencegahan (*preventive*), deteksi (*detection*), dan/atau perbaikan (*corrective*), disesuaikan dengan kebutuhan masing-masing organisasi. Kesenjangan (*gap*) dari kontrol saat ini dan *common practice* dapat dijadikan rekomendasi untuk target peningkatan kontrol keamanan terhadap potensi ancaman terkait.

Dalam menyusun skenario serangan, kita dapat menentukan dulu daftar kategori taktik, nama taktik, dan teknik yang akan digunakan. Sebagai contoh dalam tahap *Pre-Compromise untuk Initial Access* (TA0001), kita tentukan dulu teknik dan subtekniknya yang ingin disertakan, misalnya *Phishing* (T1566), *Spear Phishing Attachment* (T1566.001), dan *Spear Phishing Link* (T1566.002). Deskripsi yang ringkas dan jelas terkait TTP yang digunakan juga penting agar pihak terkait yang membutuhkan informasi threat modeling ini memahami lebih jelas skenario yang akan digunakan. Pembuatan diagram proses untuk menunjukkan langkah-langkah serangan juga akan sangat membantu, karena umumnya pembaca akan lebih menyukai diagram daripada

teks saja. Hal yang cukup penting adalah memahami kontrol yang ada saat ini apa saja untuk dapat mengurangi risiko skenario serangan tersebut. Referensi kontrol yang dapat digunakan cukup banyak, misal mengacu ke MITRE Shiled, MITRE D3FEND, CIS *Benchmark*, atau sumber yang lain.

## Implementasi Tata Kelola Multi Cloud

---

Selain *framework*, tata kelola sangat berkaitan dengan pembuatan kebijakan, prosedur, dan petunjuk teknis untuk memastikan bahwa kontrol keamanan dapat diterapkan secara standar dan kontekstual, sesuai dengan kebutuhan dan risiko yang dihadapi oleh organisasi. Biasanya muncul pertanyaan, apakah harus ada kebijakan yang spesifik mengatur keamanan cloud? Dari beberapa pengalaman penulis, tidak harus ada kebijakan spesifik yang mengatur keamanan cloud. Banyak dari area-area keamanan cloud yang masih bersinggungan dan relevan terhadap kontrol keamanan informasi pada umumnya, sehingga jika konteksnya adalah kebijakan, maka hal-hal yang spesifik ke tata kelola keamanan cloud dapat disertakan ke kebijakan keamanan informasi yang ada saat ini. Jika memang organisasi butuh yang sedikit lebih detil, maka dapat disusun suatu standar keamanan cloud. Hal ini tentunya tergantung dari hierarki penyusunan kebijakan di organisasi masing-masing. Bisa jadi di level kebijakan, ada yang sangat umum, ada yang sedikit detil. Bahkan di level standar, ada yang pada praktiknya sangat detil seperti petunjuk teknis.

Dari pengalaman penulis, umumnya organisasi telah memiliki suatu kebijakan Keamanan Informasi yang kontennya sangat umum. Kebijakan Keamanan Informasi hanya berisi beberapa lembar karena memang tujuannya untuk seluruh karyawan. Untuk organisasi yang telah menerapkan ISO 27001, biasanya membuat satu dokumen lagi terkait *Information Security Management System* (ISMS). Untuk organisasi yang menerapkan *cloud-native*, biasanya membutuhkan suatu dokumen yang lebih teknis dari kebijakan dan spesifik membahas keamanan cloud. Dalam menyusun kebijakan teknis terkait keamanan cloud, wajib hukumnya kita memahami seluruh kebijakan dan prosedur yang ada di organisasi agar tidak tumpang tindih dan lebih selaras. Dalam penyusunan kebijakan seperti ini, tim *cloud security* dapat dibantu oleh tim IT GRC.

Dalam konteks petunjuk teknis dan prosedur teknis, secara sederhana organisasi dapat mengacu ke CIS Benchmark, sesuai dengan public *cloud service provider* yang digunakan. Tentunya kita perlu sesuaikan lagi *checklist* yang ada karena belum tentu semuanya dapat diterapkan bagi organisasi.

Tantangan yang umumnya ditemui dalam melakukan penilaian dan implementasi keamanan multi-cloud salah satunya berkaitan juga dengan arsitektur. Memang dalam menyusun arsitektur, tim *cloud security* atau *security architect* kadang punya pendekatan yang berbeda. Perspektif arsitektur ada yang hanya terbatas pada diagram jaringan secara high level, ada yang sampai ke low level (termasuk services yang digunakan), ada yang diagramnya sudah detil tapi tidak menunjukkan integrasi antar *cloud platform (multi-cloud)*, dan ada juga yang "TOGAF-banget" (kami belum menemukan yang "SABSA-banget"). Namun, kembali lagi ke *appetite* bagi organisasi, sejauh apa visibilitas yang diharapkan dari suatu arsitektur, karena memang menurut kami, arsitektur tidak hanya sebatas gambar diagram jaringan saja.

## Metriks Penilaian Keamanan Cloud

---

Peter Drucker pernah mengatakan **"You cannot manage what you cannot measure"**, sehingga adanya *Key Performance Indicator* (KPI), *Key Risk Indicator* (KRI), dan/atau *Objectives & Key Results* (OKR) menjadi sangat penting untuk memastikan bahwa kontrol keamanan cloud dapat diterapkan secara maksimal. Metriks tersebut juga tentunya akan berpengaruh ke penilaian kinerja karyawan, dalam hal ini tim IT Security secara umum dan **Tim Cloud Security** secara khusus. Mengingat kami membantu klien baik yang "*traditional enterprise*" maupun "*cloud native / tech-company*", maka bisa jadi organisasi lebih memilih pengukuran dengan konsep KPI atau OKR. Terlepas dari itu, kami biasanya juga mengusulkan penggunaan pengukuran kinerja berbasis KRI. Jika KPI dan OKR berfokus pada nilai / hasil tertentu yang harus dicapai, maka KRI berfokus pada risiko utama yang harus dimitigasi. Kemudian, apa saja metrik untuk keamanan cloud? Penyusunan metrik untuk keamanan cloud umumnya mengacu pada metrik yang dimiliki oleh organisasi karena pastinya seluruh metrik harus selaras untuk mendukung strategi organisasi. Pendekatan sederhana

yang penulis gunakan dalam penyusunan metrik untuk keamanan cloud adalah sebagai berikut:

1. **Menentukan risiko-risiko utama dari area keamanan cloud.** Risiko ini bisa diperoleh dari hasil analisis kesenjangan atau maturitas terhadap *cloud security framework* yang digunakan.
2. **Menentukan kategori metrik, misalnya Manajemen atau Operasional.** Hal ini dilakukan untuk mengakomodasi stakeholder yang lebih luas, setidaknya di level manajerial ke atas dan operasional.
3. **Menentukan KPI/OKR/KRI beserta deskripsi singkat** yang menjelaskan KPI/OKR/KRI tersebut beserta kategorinya (apakah KPI, OKR, atau KRI).
4. **Menentukan rumus atau indikator perhitungan metrik** yang dapat berupa persentase (%), jumlah/kuantitas, atau rata-rata.
5. **Menentukan frekuensi,** misalnya harian, mingguan, bulanan, kuartal, atau tahunan.
6. **Menentukan sumber data,** misalnya dari perangkat, laporan, atau kegiatan tertentu.
7. **Menentukan pihak-pihak yang relevan,** misalnya metrik terkait *Identity & Access Management* bisa jadi tim *cloud security* harus bekerja sama dengan tim IAM (jika memang terpisah).

Contoh dari KPI/OKR yang bersifat Manajemen misalnya jumlah inisiatif *cloud security roadmap* yang telah dikerjakan, persentase temuan *audit cloud* yang telah diremediasi, dan lain-lain. Contoh dari KPI/OKR yang bersifat Operasional misalnya jumlah *Cloud DLP rule/policy* yang dibuat, jumlah temuan dari CSPM tools yang telah diremediasi, persentase jumlah *encryption key* yang dirotasi, dan lain-lain. Contoh dari KRI misalnya persentase jumlah *dormant account*, jumlah requests yang berasal dari *blacklisted IP*, persentase jumlah *cloud assets* yang telah diperkuat / *harden*, dan lain-lain.

## Kesimpulan

---

Menerapkan kontrol keamanan pada cloud tidak terlalu berbeda dengan penerapan kontrol keamanan informasi pada umumnya. Perbedaannya hanya pada area fokusnya

yang lebih spesifik untuk ke perlindungan terhadap *cloud environment*. Dari pengalaman penulis, hal-hal yang sifatnya tata kelola masih relevan untuk dipertimbangkan secara serius untuk organisasi tertentu. Untuk organisasi yang bertransformasi digital, umumnya fokus utama di awal adalah bagaimana melakukan *cloud migration* dan/atau *cloud adoption* yang efektif dan efisien. Kata efektif, berarti sesuai dengan target migrasi dari berbagai aspek, misalnya perihal kinerja, risiko, regulasi, dukungan layanan dan teknologi, dan lain-lain. Efisien berarti biaya yang dikeluarkan untuk migrasi dan/atau adopsi *hybrid cloud* sesuai dengan perencanaan dan anggaran yang dimiliki organisasi. Ketika analisis dari aspek komersil dan teknikal telah dilakukan, kemudian *hybrid cloud* telah diterapkan, baru aspek keamanan cloud mulai diterapkan. Meskipun pada praktiknya sering seperti itu, namun menurut kami sebaiknya keamanan cloud dipertimbangkan sejak awal, ketika organisasi menyusun rencana transformasi digital, khususnya cloud transformation.

*Last but not least*, tidak ada *best practice* dalam penerapan keamanan *multi-cloud*, namun risiko keamanan cloud dapat dimitigasi dengan penerapan *customized practice* yang sesuai dengan masing-masing organisasi, dengan mempertimbangkan aspek *governance, people, process*, dan *technology*.

## Referensi

---

- [1]. <https://www.gartner.com/en/newsroom/press-releases/2022-02-09-gartner-says-more-than-half-of-enterprise-it-spending>
- [2]. <https://www.tripwire.com/misc/securing-public-cloud-infrastructure-survey>
- [3]. <https://cloudsecurityalliance.org/research/cloud-controls-matrix/>
- [4]. <https://www.gartner.com/en/documents/3899373/innovation-insight-for-cloud-security-posture-management>
- [5]. <https://attack.mitre.org/matrices/enterprise/cloud>



## TENTANG PENULIS



### Eryk Budi Pratama

M.Kom, M.M., CIPM, CIPP/E, FIP, Certified Cloud Security (CCSK)

<https://www.linkedin.com/in/erykbudipratama/>

Eryk merupakan praktisi dan konsultan di bidang Keamanan Informasi, Perlindungan Data, dan Privasi Data di salah satu organisasi global ternama, serta **Chapter Chair** untuk **International Association of Privacy Professionals** (IAPP) Jakarta. Memiliki pengalaman dalam memberikan konsultansi dan implementasi kontrol keamanan informasi di berbagai jenis organisasi dan industri, baik dalam maupun luar negeri. Eryk banyak membantu organisasi mulai dari tahap perencanaan, penyusunan strategi, penilaian kapabilitas dan maturity, penyusunan framework, penyusunan dokumentasi, pengujian teknis, dan penilaian non-teknis terhadap penerapakan keamanan informasi, keamanan siber, dan perlindungan serta privasi data.



### Novita Handayani Koswara

Certified AWS Developer

<https://www.linkedin.com/in/novitakoswara/>

Novita merupakan praktisi Cloud-Engineering yang memiliki pengalaman di berbagai platform berbasis cloud. Menguasai beberapa bahasa pemrograman dan berpengalaman menangani berbagai jenis aplikasi pendukung cloud. Saat ini bekerja di salah satu organisasi global ternama sebagai konsultan senior di bidang keamanan siber.

# PENERAPAN SISTEM MONITORING 24/7 DAN AGENTLESS MONITORING MENGGUNAKAN RASPBERRY PI

oleh Ramadhan Hidayat



Raspberry Pi memiliki keunggulan konsumsi listrik yang rendah, dan meskipun kemampuan pemrosesannya terbatas, Sistem Monitoring juga dapat diterapkan di Raspberry Pi cara ini cukup untuk memantau satu atau dua perangkat tertentu. Dalam kesempatan kali ini, penulis mencoba berbagi pengalaman terkait penerapan Raspberry Pi sebagai Sistem Monitoring yang memantau OpenWRT sebagai sistem operasi pada router dan AdGuardHome sebagai *DNS Server* yang dipasang di perangkat yang sama.

Sebelum melanjutkan, jika rekan-rekan hanya ingin sekedar memantau DNS Server seperti AdGuardHome dari Raspberry Pi menggunakan Sistem Monitoring, sudah ada tutorial yang lebih mudah karena hanya menggunakan satu Raspberry Pi saja

(<https://github.com/nin9s/elk-hole>). Namun, karena penulis ingin memantau perangkat lain dan perangkat tersebut tidak mendukung pemasangan HIDS seperti wazuh-agent, penulis mencoba cara yang agak berbeda.

## Memonitor Aktivitas OpenWRT

---

Untuk merakit Sistem Monitoring, saya mengikuti cara yang tersedia pada halaman tautan berikut <https://jacobriggs.io/blog/posts/how-to-install-a-wazuh-siem-server-on-a-raspberry-pi-4b-26.html>. Selanjutnya, kita perlu menambahkan konfigurasi yang membuat sistem monitoring keamanan untuk menerima log dari perangkat lain. Yang paling mudah adalah dengan menerima data melalui syslog. Untuk melakukan konfigurasi ini dapat dilakukan dengan membuka file `/var/ossec/etc/ossec.conf` dan tambahkan konfigurasi berikut di dalam `<ossec_config>`.

```
<remote>
  <connection>syslog</connection>
  <port>514</port>
  <protocol>udp</protocol>
  <allowed-ips>0.0.0.0/24</allowed-ips>
  <local_ip>[ip raspberry pi]</local_ip>
</remote>
```

Silakan ubah parameter `[ip raspberry pi]` sesuai alamat IP Raspberry Pi yang digunakan. Kemudian lakukan restart wazuh-manager, dengan menjalankan perintah berikut:

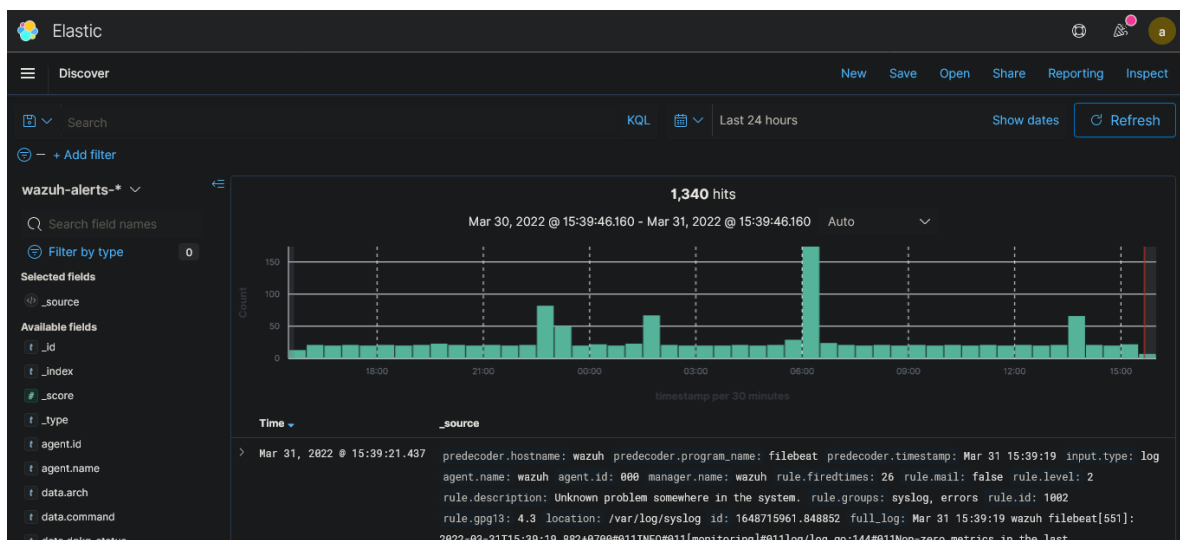
```
systemctl restart wazuh-manager
```

Selanjutnya, buka *web interface* OpenWRT dan masuk ke dalam menu System -> Logging dan masukan konfigurasi data parameter seperti pada Gambar 1 berikut.

System Properties	
Logging	
System log buffer size	64 kiB
External system log server	192.168.16.111
External system log server port	514
External system log server protocol	UDP
Write system log to file	/tmp/system.log
Log output level	Debug
Cron Log Level	Debug

Gambar 1 – Konfigurasi Pengiriman System Logging pada OpenWRT

Ubah alamat IP pada parameter “**External system log server**” sesuai dengan alamat IP Raspberry Pi yang digunakan. Untuk memastikan data yang dikirimkan, anda dapat mengakses Elastic, pada bagian menu **Discover**, data syslog OpenWRT akan muncul di bagian index pattern dengan nama **wazuh-alerts-\*** sebagaimana pada Gambar 2.



Gambar 2 – Data Syslog OpenWRT yang diterima

Jika data belum masuk, lakukan perubahan konfigurasi pada file `/var/ossec/etc/ossec.conf`, khususnya di bagian `<remote>` kemudian di parameter `<protocol>` ubah menjadi **tcp**, kemudian lakukan perubahan pada `<port>` yang digunakan misalnya menjadi 513. Setelah itu lakukan restart wazuh-manager dengan menggunakan perintah “`systemctl restart wazuh-manager`” melalui terminal. Pastikan anda melakukan penyesuaian parameter “**External system log server**” pada konfigurasi OpenWRT yang digunakan, misal ubah port logging OpenWRT ke 513 juga.

## Memonitor Aktifitas AdGuardhome

Dikarenakan log AdGuardhome memiliki format json serta keterbatasan OpenWRT dalam menambah repositori, maka cara syslog tidak cocok untuk mengirim log ini. Dengan demikian OpenWRT tidak dapat menggunakan Filebeat ataupun Logstash, maka penulis menggunakan Log Courier sebagai media pengirim log dari OpenWRT, dan menggunakan **Log Carver** sebagai penerima log dari OpenWRT dan melempar lognya ke elasticsearch. Caranya adalah sebagai berikut:

### Langkah Konfigurasi Log Courier

1. Download Golang, dengan menggunakan baris perintah berikut

```
sudo apt install golang
```

2. Download Log Courier, dengan menggunakan baris perintah berikut

```
curl -so log-courier-v2.9.0.tar.gz https://github.com/driskell/log-courier/archive/refs/tags/v2.9.0.tar.gz  
tar xzvf log-courier-v2.9.0.tar.gz
```

3. Lakukan Compile aplikasi Log Courier

```
cd log-courier-2.9.0  
go generate .  
go install .
```

4. Lakukan perubahan konfigurasi pada Log Courier, dengan menggunakan perintah berikut

```
cd ~/go/bin
vi adguardhome-logcourier.yaml
```

masukkan konfigurasi berikut pada file tersebut

```
files:
  - paths:
      - /root/go/bin/querylog.log
    reader: json
    fields:
      type: adguardhome
      add host field: true
general:
  persist directory: /var/lib/log-courier
network:
  servers:
    - [ip raspberry pi]:12345
transport: tcp
```

5. Jika dilihat di path file, yang kita kirim adalah file **querylog.log**, yang mana file tersebut tidak ada. Maka langkah selanjutnya adalah membuat file tersebut, kita perlu membuat *symlink* terlebih dahulu

```
ln -s /opt/AdGuardHome/data/querylog.json querylog.log
```

6. Lakukan verifikasi apakah konfigurasi yang dilakuakn sudah benar, dengan menjalankan perintah berikut

```
./log-courier -config-test -config AdGuardHome-Elastic.yaml
```

Log courier saat ini belum dapat berjalan, oleh karena kita butuh mengaktifkan **Log Carver** terlebih dahulu

## Langkah Konfigurasi Log Carver pada Raspberry Pi

1. Download Golang

```
sudo apt install golang
```

## 2. Download Log Courier

```
curl -so log-courier-v2.9.0.tar.gz https://github.com/driskell/log-courier/archive/refs/tags/v2.9.0.tar.gz

tar xzvf log-courier-v2.9.0.tar.gz
```

## 3. Kemudian lakukan Compile Log Carver, dengan baris perintah berikut

```
cd log-courier-2.9.0/log-carver
go generate .
go install .
```

## 4. Kemudian buat konfigurasi Log Carver pada **log-carver.yaml**, dengan langkah berikut

```
cd ~/go/bin
vi log-carver.yaml
```

## 7. Lakukan konfigurasi Log Carver, dengan menggunakan konfigurasi berikut

```
receivers:
- listen:
  - 0.0.0.0:12345
  transport: tcp
pipelines:
- if: >-
  event.type == "json"
  then:
  - name: add_tag
    tag: adguardhome
- else:
  - name: add_tag
    tag: unknown_event
network:
  transport: es-https
  index pattern: >-
    adguardhome-%{+2006.01.02}
  servers:
  - 127.0.0.1:9200
  ssl ca: /etc/filebeat/certs/root-ca.pem
  username: [username elastic]
  password: [password elastic]
```

8. Lakukan verifikasi apakah konfigurasi yang dilakukan sudah benar, dengan menjalankan perintah berikut

```
./log-carver -config-test -config log-carver.yaml
```

9. Jalankan program **Log Carver**, dengan perintah berikut

```
./log-carver -config-debug -config log-carver.yaml
```

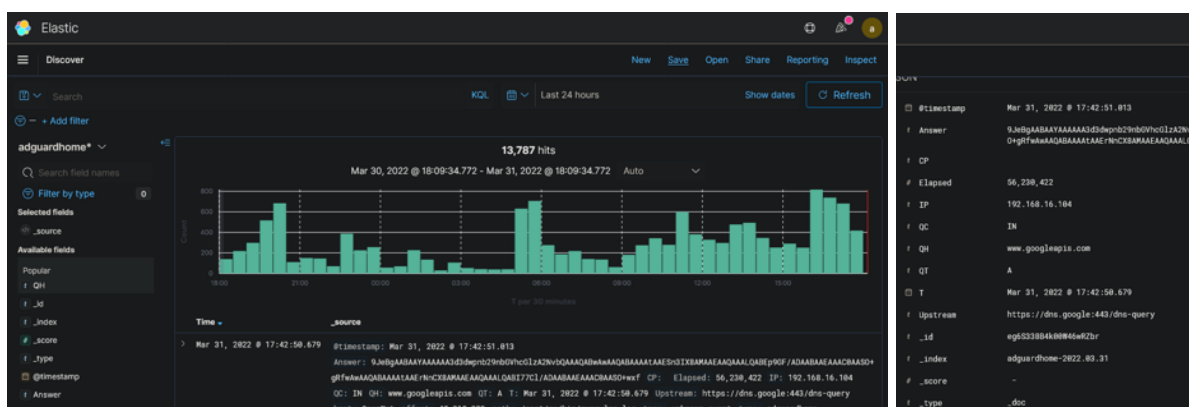
10. Jalankan program **Log Courier** di OpenWRT

```
./log-courier -config-debug -config log-carver.yaml
```

Buka ELK melalui browser, kemudian masuk ke dalam Menu Management -> Stack Management -> Index Pattern, kemudian pilih **Create index pattern**

Pada bagian **Step 1**, masukkan **adguardhome\***, kemudian pada **Step 2** pilih "time field T", setelah itu pilih **Create indeks pattern**.

Setelah itu buka Menu Kibana -> Discover, setelah itu pilih Index Pattern **wazuh-alerts-\*** ke **adguardhome\***. Data Adguardhome akan muncul seperti pada Gambar 3.



Gambar 3 – Data **adguardhome** yang diterima



## Referensi

---

- [1]. <https://jacobriggs.io/blog/posts/how-to-install-a-wazuh-siem-server-on-a-raspberry-pi-4b-26.html>
- [2]. <https://documentation.wazuh.com/current/user-manual/capabilities/log-data-collection/how-it-works.html#remote-syslog>
- [3]. <https://github.com/driskell/log-courier/blob/main/docs/log-courier/Configuration.md>
- [4]. <https://github.com/driskell/log-courier/blob/main/docs/log-carver/Configuration.md>
- [5]. <https://github.com/nin9s/elk-hole>
- [6]. <https://github.com/AdguardTeam/AdGuardHome>
- [7]. <https://openwrt.org/packages/table/start>

### TENTANG PENULIS



#### **Ramadhan Hidayat**

Mahasiswa UIN Syarif Hidayatullah Jakarta

# SCOUTSUITE “SURVEY CORPS” PENJAGA DINDING LAYANAN CLOUD DARI BERBAGAI ANCAMAN “TITAN”

oleh Muhammad Fajar Masputra



Era digital saat ini sudah semakin berkembang, baik secara teknologi, pendidikan, bisnis, ekonomi dan bidang lainnya. Perkembangan teknologi menjadi salah satu hal yang cukup menyita perhatian belakangan ini semenjak mulai mewabahnya pandemi COVID-19. Tagar-tagar seperti digitalisasi atau kerja dari rumah (WFH – *Work From Home*) menjadi semboyan baru yang disampaikan para ahli/praktisi dalam berbagai kesempatan. Perkembangan teknologi yang cukup masif diimplementasikan sejak mewabahnya Pandemi COVID-19 ini adalah teknologi komputasi awan (*cloud*).

Cloud menjadi solusi sebuah perusahaan dapat tetap produktif dan bisnis tetap berjalan di-era Pandemi. Tidak sedikit pastinya perusahaan yang memanfaatkan cloud di era pandemi ini, dan pastinya tidak sedikit pula yang akhirnya menyandarkan kegiatan operasional bisnis mereka kepada cloud. Cloud sudah menjadi nyawa dan tulang punggung berbagai lini bisnis saat ini terutama di era pandemi. Cloud saat ini sudah menyentuh berbagai aspek di sebuah perusahaan mulai dari *product, people, process* dan *business* saat ini sudah bergantung pada ketersediaan layanan cloud.

Cloud sendiri bukan teknologi yang benar-benar baru. Implementasi cloud dalam berbagai sebuah produk sendiri juga bukan hal yang baru. Namun, sejauh apa implementasi keamanan cloud yang dalam produk kita? Sesering apa kita dalam melakukan pengecekan atas konfigurasi keamanan layanan cloud kita? Ini yang masih sering menjadi Pekerjaan Rumah (PR) besar bagi pemilik produk yang menggantungkan bisnisnya pada layanan cloud.

Solusi atas keamanan layanan cloud sudah banyak tersedia, mulai dari yang sumber terbuka (*open source*) hingga berbayar (*commercial*). Dalam artikel ini, saya akan membahas salah satu *tools* yang bertujuan untuk melakukan *automatic-audit* atas kerentanan konfigurasi layanan cloud kita dari berbagai aspek yang bersifat *open source*.

Tools tersebut bernama ScoutSuite (source: <https://github.com/nccgroup/ScoutSuite>). ScoutSuite sendiri merupakan *tools* yang digunakan untuk melakukan audit secara otomatis ke berbagai layanan cloud (*multi-provider*), proyek ini dibawah riset NCCGroup (source: <https://research.nccgroup.com/2020/10/01/tool-release-scoutsuite-5-10/>) dan bersifat *open-source*.

## Bagaimana Cara Kerja Scout Suite ?

---

**ScoutSuite** sendiri menggunakan API yang disediakan oleh layanan cloud, setelah itu ScoutSuite akan mengumpulkan seluruh informasi yang dibutuhkan, dan memberikan *highlight* pada bagian dari layanan cloud kita yang memiliki celah kerentanan. ScoutSuite juga menyediakan hasil yang menampilkan secara jelas kemungkinan dari *attack surface* yang bisa menyerang layanan cloud kita.



Sebenarnya, jika dilihat penjelasan di atas, ScoutSuite serupa dengan fungsi Survey Corps dalam Serial Attack on Titan. Squad yang dipimpin Erwin Smith ini merupakan satu-satunya pasukan yang melakukan perburuan Titan, analisa terhadap Titan dan melakukan eksplorasi terhadap dunia di luar dinding. Dua orang prajurit yang berperan besar dalam Survey Corps tersebut adalah Levi Ackerman dan Hange Zoe. Levi Ackerman adalah prajurit yang mempunyai kemampuan bertarung diatas rata-rata, pengalamannya dalam membunuh titan telah teruji selama dia bergabung dengan Pasukan Survey Corps. Hange Zoe sendiri merupakan anggota survey corps yang bertugas dan terobsesi melakukan penelitian terkait titan. Jika kita ibaratkan dengan fungsinya, kemampuan dari Levi dan Hange pendekatannya sama dengan ScoutSuite ketika melakukan audit atas layanan cloud kita yaitu mengumpulkan seluruh potensi ancaman yang muncul dilayanan cloud kita dengan cepat dan tepat serta melakukan penilaian risiko atas potensi ancaman tersebut dan memberikan analisa.

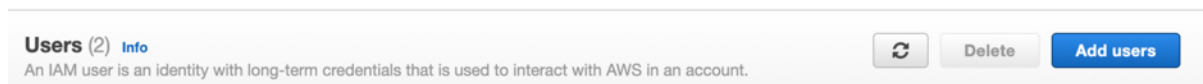
# Instalasi ScoutSuite

Pada pembahasan kali ini akan dijelaskan juga bagaimana penggunaan dari ScoutSuite pada salah satu penyedia layanan cloud **Amazon Web Services (AWS)**.

## # 1 - Proses Instalasi

Lakukan konfigurasi User pada AWS Console, dengan langkah-langkah sebagai berikut

1. Masuk ke dalam AWS Console
2. Pilih menu **IAM**, lalu pilih tab **Users**
3. Klik **Add Users** untuk menambahkan **User** baru khusus untuk ScoutSuite, seperti Gambar di bawah ini



Gambar 1 – Penambahan User baru

4. Berikan nama pada User tersebut dan pastikan melakukan *tick* pada bagian **“AccessKey - Programmatic Access”** seperti Gambar di bawah ini:

Gambar 2 – Konfigurasi Access Key – Programmatic Access

5. Pada bagian **Permission** pastikan bahwa User tersebut memiliki akses untuk melakukan **SecurityAudit** dan **ViewOnlyAccess** (Lihat Gambar berikut)

Add user 1 2 3 4 5

▼ Set permissions

Add user to group

Copy permissions from existing user

Attach existing policies directly

Create policy ↺

Filter policies  Showing 4 results

	Policy name	Type	Used as
<input type="checkbox"/>	AWSSecurityHubFullAccess	AWS managed	None
<input type="checkbox"/>	AWSSecurityHubOrganizationsAccess	AWS managed	None
<input type="checkbox"/>	AWSSecurityHubReadOnlyAccess	AWS managed	None
<input checked="" type="checkbox"/>	SecurityAudit	Job function	Permissions policy (1)

► Set permissions boundary

Gambar 3 – Penambahan Permission pada User

6. Klik **Next** hingga muncul tampilan dibawah ini, lalu klik **Create User**

Add user 1 2 3 4 5

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name	ScoutSuite
AWS access type	Programmatic access - with an access key
Permissions boundary	Permissions boundary is not set

Permissions summary

The following policies will be attached to the user shown above.

Type	Name
Managed policy	SecurityAudit
Managed policy	ViewOnlyAccess

Tags

No tags were added.

Gambar 4 – Penambahan User berhasil Dibuat

7. Terakhir jangan lupa untuk **mendownload** file csv yang berisi key yang akan **setup** di host dari ScoutSuite.

Add user 1 2 3 4 5

✓ Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: <https://718376853120.signin.aws.amazon.com/console>

Download .csv

Gambar 5 – Download File untuk Konfigurasi di Host ScoutSuite

## #2 - Konfigurasi AWS

1. Download **AWS CLI** melalui situs  
(<https://docs.aws.amazon.com/cli/latest/userguide/getting-started-install.html>)  
Lakukan instalasi sesuai dengan operating sistem yang Anda gunakan.
2. Setelah itu masuk kedalam terminal klik **aws configure**
3. Masukkan **Access Key** dan **Secret Key** dari User yang sudah Anda buat dilangkah sebelumnya (pada file csv yang telah Anda download)

## #3 - Konfigurasi ScoutSuite

1. Clone ScoutSuite dengan perintah berikut di dalam host yang telah dibuat  

```
//melakukan clone atas repo ScoutSuite kedalam host kita  
git clone https://github.com/nccgroup/ScoutSuite.git
```
2. Masuk ke dalam folder ScoutSuite yang telah di clone dengan menjalankan perintah berikut di terminal  

```
//masuk kedalam folder ScoudSuite  
cd ScoutSuite
```
3. Lakukan instalasi ScoutSuite dengan perintah berikut  

```
//melakukan installasi library yang dibutuhkan  
pip install -r requirements.txt
```
4. Lakukan instalasi modul coloredlogs, cherrypy dan cherrypy (dalam kasus ini menggunakan MacOS), dengan perintah berikut  

```
pip install coloredlogs  
pip install cherrypy  
pip install cherrypy_cors
```
5. Jalankan ScoutSuite dari terminal dengan menjalankan perintah berikut  

```
python3 scout.py aws
```



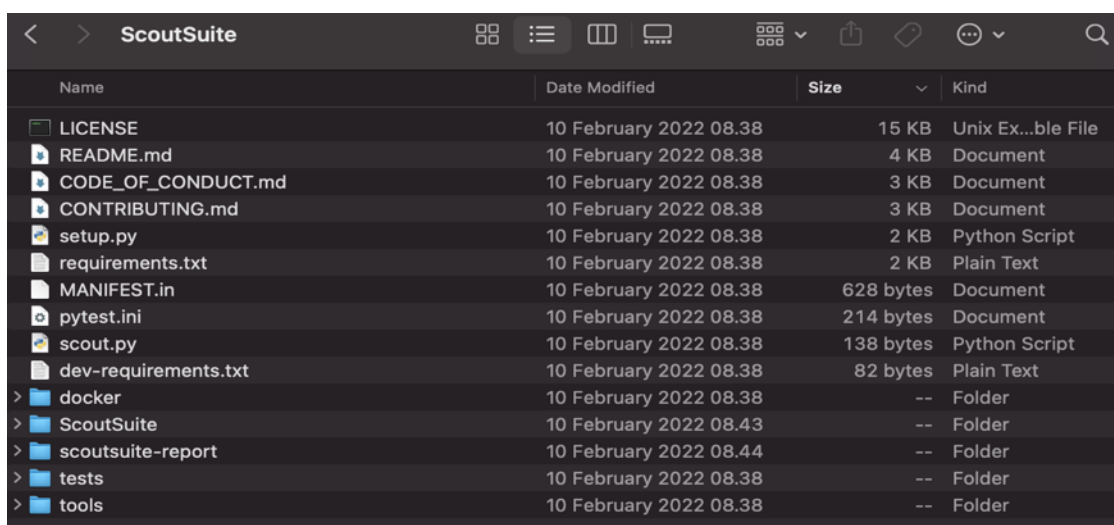
Setelah melakukan running maka ScoutSuite akan berjalan seperti gambar dibawah ini:

```
2022-02-10 08:40:52 fntmac-028.local scout[5645] INFO Launching Scout
2022-02-10 08:40:52 fntmac-028.local scout[5645] INFO Authenticating to cloud provider
2022-02-10 08:40:58 fntmac-028.local scout[5645] INFO Gathering data from APIs
2022-02-10 08:40:58 fntmac-028.local scout[5645] INFO Fetching resources for the ACM service
2022-02-10 08:40:59 fntmac-028.local scout[5645] INFO Fetching resources for the Lambda service
2022-02-10 08:41:00 fntmac-028.local scout[5645] INFO Fetching resources for the CloudFormation service
2022-02-10 08:41:01 fntmac-028.local scout[5645] INFO Fetching resources for the CloudTrail service
2022-02-10 08:41:03 fntmac-028.local scout[5645] INFO Fetching resources for the CloudWatch service
2022-02-10 08:41:04 fntmac-028.local scout[5645] INFO Fetching resources for the Config service
2022-02-10 08:41:05 fntmac-028.local scout[5645] INFO Fetching resources for the Direct Connect service
2022-02-10 08:41:06 fntmac-028.local scout[5645] INFO Fetching resources for the DynamoDB service
2022-02-10 08:41:07 fntmac-028.local scout[5645] INFO Fetching resources for the EC2 service
2022-02-10 08:41:09 fntmac-028.local scout[5645] INFO Fetching resources for the EFS service
2022-02-10 08:41:10 fntmac-028.local scout[5645] INFO Fetching resources for the ElastiCache service
2022-02-10 08:41:11 fntmac-028.local scout[5645] INFO Fetching resources for the ELB service
2022-02-10 08:41:12 fntmac-028.local scout[5645] INFO Fetching resources for the ELBv2 service
2022-02-10 08:41:13 fntmac-028.local scout[5645] INFO Fetching resources for the EMR service
2022-02-10 08:41:15 fntmac-028.local scout[5645] INFO Fetching resources for the IAM service
2022-02-10 08:41:15 fntmac-028.local scout[5645] INFO Fetching resources for the KMS service
2022-02-10 08:41:16 fntmac-028.local scout[5645] INFO Fetching resources for the RDS service
2022-02-10 08:41:17 fntmac-028.local scout[5645] INFO Fetching resources for the RedShift service
2022-02-10 08:41:18 fntmac-028.local scout[5645] INFO Fetching resources for the Route53 service
2022-02-10 08:41:19 fntmac-028.local scout[5645] INFO Fetching resources for the S3 service
2022-02-10 08:41:23 fntmac-028.local scout[5645] INFO Fetching resources for the SES service
2022-02-10 08:41:24 fntmac-028.local scout[5645] INFO Fetching resources for the SNS service
2022-02-10 08:41:25 fntmac-028.local scout[5645] INFO Fetching resources for the SQS service
2022-02-10 08:41:27 fntmac-028.local scout[5645] INFO Fetching resources for the VPC service
2022-02-10 08:41:28 fntmac-028.local scout[5645] INFO Fetching resources for the Secrets Manager service
2022-02-10 08:44:05 fntmac-028.local scout[5645] INFO Running pre-processing engine
2022-02-10 08:44:05 fntmac-028.local scout[5645] INFO Running rule engine
2022-02-10 08:44:06 fntmac-028.local scout[5645] INFO Applying display filters
2022-02-10 08:44:06 fntmac-028.local scout[5645] INFO Running post-processing engine
2022-02-10 08:44:06 fntmac-028.local scout[5645] INFO Saving data to scoutsuite-report/scoutsuite-results/scoutsuite_results_aws-718376853120.js
2022-02-10 08:44:06 fntmac-028.local scout[5645] INFO Saving data to scoutsuite-report/scoutsuite-results/scoutsuite_exceptions_aws-718376853120.js
2022-02-10 08:44:06 fntmac-028.local scout[5645] INFO Creating scoutsuite-report/aws-718376853120.html
2022-02-10 08:44:07 fntmac-028.local scout[5645] INFO Opening the HTML report
```

Gambar 6 – ScoutSuite berhasil dijalankan

## Hasil Laporan

Laporan hasil analisa dan audit dari ScoutSuite akan muncul pada folder scoutsuite\_report seperti dibawah ini:

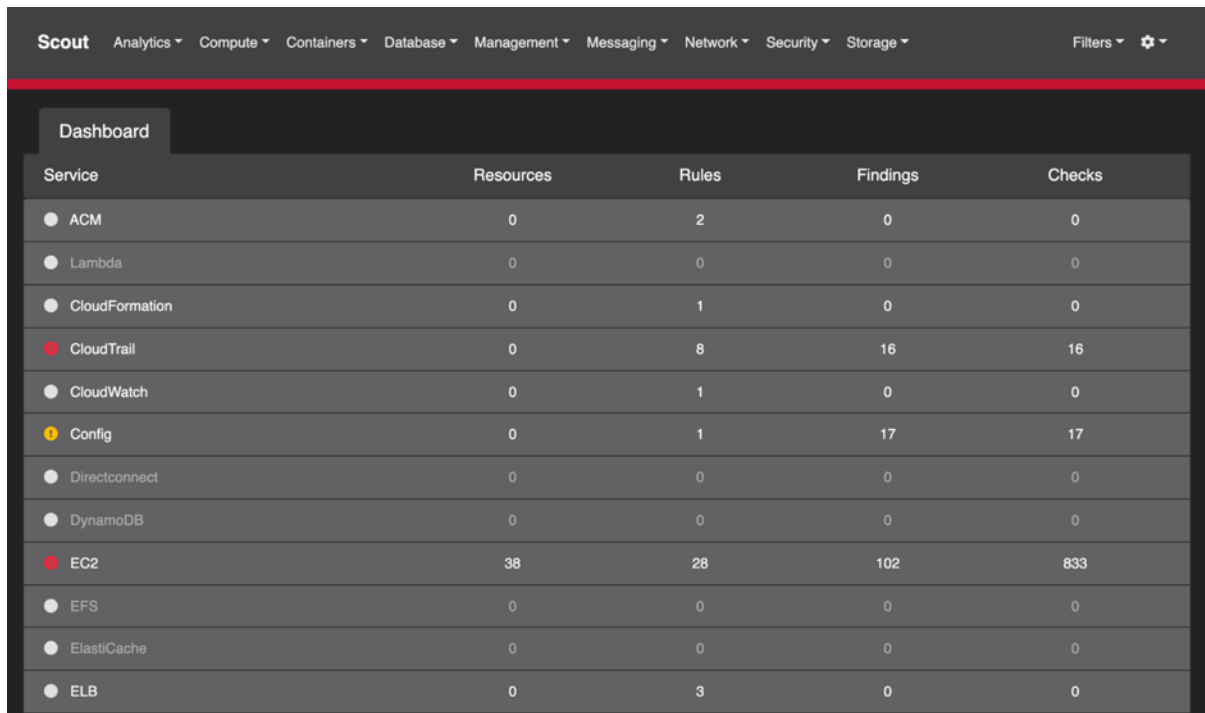


Name	Date Modified	Size	Kind
LICENSE	10 February 2022 08:38	15 KB	Unix Ex...ble File
README.md	10 February 2022 08:38	4 KB	Document
CODE_OF_CONDUCT.md	10 February 2022 08:38	3 KB	Document
CONTRIBUTING.md	10 February 2022 08:38	3 KB	Document
setup.py	10 February 2022 08:38	2 KB	Python Script
requirements.txt	10 February 2022 08:38	2 KB	Plain Text
MANIFEST.in	10 February 2022 08:38	628 bytes	Document
pytest.ini	10 February 2022 08:38	214 bytes	Document
scout.py	10 February 2022 08:38	138 bytes	Python Script
dev-requirements.txt	10 February 2022 08:38	82 bytes	Plain Text
> docker	10 February 2022 08:38	--	Folder
> ScoutSuite	10 February 2022 08:43	--	Folder
> scoutsuite-report	10 February 2022 08:44	--	Folder
> tests	10 February 2022 08:38	--	Folder
> tools	10 February 2022 08:38	--	Folder

Gambar 7 – Tampilan Folder Report pada ScoutSuite

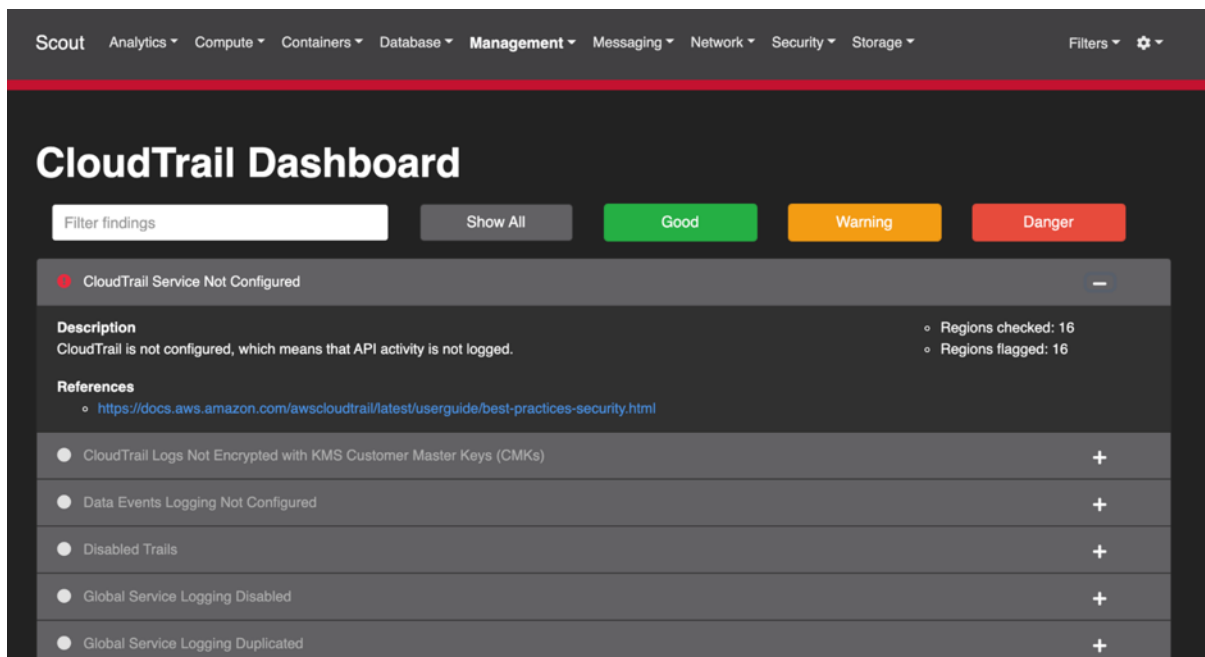


Laporan berformat html dan dapat dibuka dengan menggunakan browser. Laporan tersebut berisi kerentanan yang ada di seluruh aset layanan cloud kita. ScoutSuite juga memberikan referensi atas kerentanan tersebut dan remediasi yang dapat dilakukan untuk menutup kerentanan tersebut.



Service	Resources	Rules	Findings	Checks
ACM	0	2	0	0
Lambda	0	0	0	0
CloudFormation	0	1	0	0
CloudTrail	0	8	16	16
CloudWatch	0	1	0	0
Config	0	1	17	17
Directconnect	0	0	0	0
DynamoDB	0	0	0	0
EC2	38	28	102	833
EFS	0	0	0	0
ElastiCache	0	0	0	0
ELB	0	3	0	0

Gambar 8 – Tampilan Laporan Kerentanan yang Ditemukan oleh ScoutSuite



**CloudTrail Dashboard**

Filter findings: [ ] Show All [ ] Good [ ] Warning [ ] Danger

**CloudTrail Service Not Configured**

**Description**  
CloudTrail is not configured, which means that API activity is not logged.

**References**  

- <https://docs.aws.amazon.com/awscloudtrail/latest/userguide/best-practices-security.html>

- CloudTrail Logs Not Encrypted with KMS Customer Master Keys (CMKs) +
- Data Events Logging Not Configured +
- Disabled Trails +
- Global Service Logging Disabled +
- Global Service Logging Duplicated +

Gambar 9 – Rekomendasi Perbaikan Kerentanan yang dihasilkan oleh ScoutSuite

#### Tips & Trik

Lebih baik apabila instalasi mengikuti dokumentasi yang ada di github, menggunakan virtual environment dari Python supaya terisolasi lingkungan instalasi dari ScoutSuite.

ScoutSuite merupakan aplikasi yang lebih optimal digunakan sebagai bentuk evaluasi, artinya lebih baik digunakan ketika infrastruktur cloud kita sudah mulai terbentuk. ScoutSuite kurang maksimal ketika kita gunakan sebagai tools yang sifatnya pencegahan. Maka dari itu, langkah terbaik dalam penerapan keamanan dalam penggunaan layanan cloud adalah memberikan *security awareness* terkait bagaimana tim terkait melakukan konfigurasi yang aman.

#### TENTANG PENULIS



#### **Muhammad Fajar Masputra**

Security Engineer at Finantier

Powering the next generation of Financial Services across SEA

# MITRE ATT&CK FOR BETTER DETECTION AND PREVENTION

oleh Ewaldo Simon Hiras



## Pengantar

---

ATT&CK (*Adversarial Tactics, Techniques, and Common Knowledge*) Framework adalah sebuah *knowledge base* yang berisi Taktik, Teknik, dan Prosedur (TTP) yang digunakan oleh *adversary* (musuh) dalam melakukan penyerangan. ATT&CK memberikan sebuah kerangka bagi *defender* untuk mengerti bagaimana perilaku *attacker* ketika menyerang.



## Pengantar Tools: ATT&CK Navigator dan DETTECT

Untuk lebih memahami tulisan ini, disarankan agar pembaca mengakrabkan diri dengan beberapa *tools* yang akan menjadi alat bantu. Berikut beberapa panduan sangat singkat penggunaan perangkat dimaksud. Secara umum alur kerja ATT&CK dan DETTECT adalah ATT&CK atau DETTECT digunakan untuk membuat layer, sedangkan ATT&CK digunakan untuk visualisasi layernya.

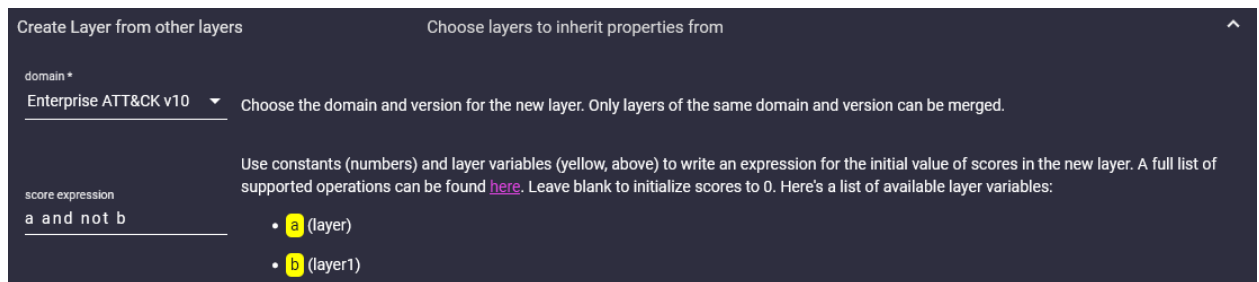
### Panduan singkat ATT&CK

#### 1. Membuat layer

Membuat layer dapat dilakukan menggunakan *web based interface* lokal atau melalui *interface online*<sup>3</sup>. Selanjutnya kita dapat memilih layer yang sudah tersedia di ATT&CK melalui menu selection control dan mengetik di kotak pencarian.

#### 2. Membandingkan layer

Membandingkan dua layer dilakukan dengan terlebih dahulu membuat dua layer, kemudian membuat layer baru dari layer yang sudah ada sebelumnya. Pada contoh di bawah, terlihat bahwa kita akan menciptakan sebuah layer baru yang berisi teknik yang ada pada **layer a**, namun tidak ada pada **layer b**.



Gambar 2 - Create layer from other layer

### Panduan singkat DETTECT

#### 1. Melakukan instalasi DETTECT

Penggunaan DETTECT dimulai dengan instalasi, saya sendiri menggunakan python dengan venv, namun tersedia juga versi *docker* nya<sup>4</sup>. Tanpa melakukan instalasi

<sup>3</sup> <https://mitre-attack.github.io/attack-navigator>

<sup>4</sup> <https://github.com/rabobank-cdc/DeTTect/wiki/Installation-and-requirements>

DETTECT versi web bisa diakses, namun untuk melakukan konversi yaml ke format json harus dilakukan di lokal.

## 2. Memilih data source DETTECT

Dapat dilakukan melalui *web based interface* lokal setelah instalasi, atau melalui *interface online*<sup>5</sup>.

## 3. Melakukan konversi yaml ke format json

Langkah ini dilakukan setelah user menggunakan web based DETTECT dan mengunduh yaml-nya, dan perlu dilakukan konversi ke json sebelum diunggah ke ATT&CK platform berbasis web. Langkah ini dilakukan dengan perintah:

```
python dettect.py d -ft sample-data/techniques-administration-endpoints.yaml -l
```

# Improve Detection & Prevention

ATT&CK dapat digunakan untuk melakukan penilaian, memprioritaskan dan pada akhirnya meningkatkan kemampuan deteksi maupun pencegahan. Kita akan menggunakan **ATT&CK Navigator** dan **DETTECT** dan secara sederhana dengan langkah-langkah yang dilakukan adalah sebagai berikut:

1. Melakukan penilaian/*assessment* sumber data yang dimiliki.
2. Menggunakan DETTECT untuk mengetahui *coverage data sources* yang dimiliki
3. Melakukan *gap analysis* untuk memfokuskan ruang perbaikan. Hal ini dapat dilakukan dengan beberapa cara, antara lain:
  - a. *Gap analysis* antara cakupan yang saat ini ada dengan TTP *threat actor/software* tertentu; atau
  - b. *Gap analysis* antara *current prevention/security control* dengan TTP *threat actor/software* tertentu.
  - c. *Gap analysis* antara *detection rules* dan *data source*.
4. Melakukan langkah perbaikan berdasarkan langkah 3.

Untuk membantu pembaca memahami secara utuh langkah-langkah tersebut, maka penulis akan menyajikan penggunaannya dalam sebuah case study berikut.

---

<sup>5</sup> <https://rabobank-cdc.github.io/detectect-editor/#/datasources>

## Case study PT X

Sebagai contoh case study ini, PT X, sebuah perusahaan yang memonitor *data sources* berupa *windows event log* hanya atas *event ID* 4624, 4625, 4648, 4672, dan 4698. Dengan maraknya pemberitaan mengenai serangan Conti Ransomware, maka PT X berusaha untuk memperbaiki deteksi yang dimiliki dengan menggunakan ATT&CK. Sebagai bagian dari Tim Keamanan PT X maka kita akan melakukan perbaikan dengan mengikuti langkah yang disampaikan sebelumnya, sebagai berikut:

### 1. Melakukan asesmen *data sources* yang dimiliki.

PT X memiliki *data sources* yang bersumber dari *windows event log*. Pertama kita perlu mengetahui mapping antara *data sources* yang dimiliki dengan *data sources* ATT&CK<sup>6</sup> setelah itu melihat seberapa besar *coverage* dari *data sources* tersebut dengan menggunakan DETTECT, dan kemudian dijadikan layer di ATT&CK Navigator. Sebagai bagian dari skenario ini, berikut beberapa event id beserta mapping dengan ATT&CK yang menjadi data source bagi PT X.

Event ID	Description	Mapping Data Source ATT&CK
4624	Account successfully logged on	Logon Session
4625	Account failed to log on	Logon Session
4648	A logon was attempted using explicit credentials	Logon Session
4672	Special privileges assigned to new logon	Logon Session
4698/ 4700	Scheduled task created	Scheduled Job
5140/ 5145	A network share object was accessed	Network Share Access

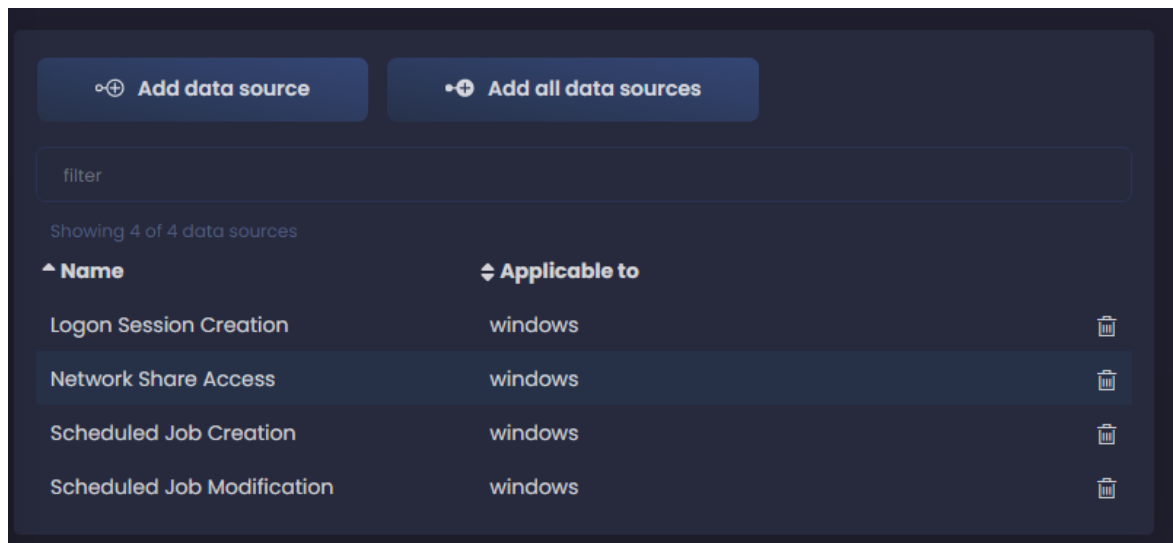
### 2. Menggunakan DETTECT untuk mengetahui *coverage data sources* yang dimiliki

Setelah itu DETTECT digunakan untuk melihat *coverage* dari *data sources* tersebut, jangan lupa melakukan *tuning* pada beberapa *field* (*applicable to, available for analysis and detection*, dan *field kualitas data*<sup>7</sup>). Lakukan download YAML dari

<sup>6</sup> A little bit of guess work involved

<sup>7</sup> hanya sebagai bagian dari dokumentasi

DETTECT, ubah menjadi bentuk json<sup>89</sup> sehingga bisa diunggah ke ATT&CK Navigator menjadi sebuah layer baru.



Gambar 3 - Menambahkan data sources pada DETTECT

Setelah melakukan upload ke ATT&CK navigator, maka pada gambar di bawah, kita dapat melihat beberapa teknik yang ter-cover oleh *data source* yang dimiliki oleh PT X.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise Exploit Public-Facing Application External Remote Services Hardware Additions Phishing Spearfishing Link Spearfishing via Service Replication Through Removable Media Supply Chain Compromise Compromise Hardware Supply Chain Compromise Dependencies and Development Tools Compromise Software Supply Chain Trusted Relationship Valid Accounts Default Accounts Domain Accounts Local Accounts	Command and Scripting Interpreter JavaScript PowerShell Python Visual Basic Windows Command Shell Exploitation for Client Execution Inter-Process Communication Component Object Model Dynamic Data Exchange Native API Scheduled Task/Job AT (Windows) Scheduled Task Shared Modules Software Deployment Tools System Services Service Execution User Execution Malicious File Malicious Link Windows Management Instrumentation	Account Manipulation Exchange Email Delegate Permissions BITS Jobs Boot or Logon Autostart Active Setup LSASS Driver Port Monitors Print Processors Registry Run Keys / Startup Folder Security Support Provider Shortcut Modification Time Providers Winlogon Helper DLL Logon Script (Windows) Network Logon Script User Execution Browser Extensions Compromise Client Software Binary Create Account	Bypass User Account Control Access Token Manipulation Create Process with Token Make and Impersonate Token Parent PID Spoofing SID-History Injection Token Impersonation/Theft BITS Jobs Declassify/Decode Files or Information Direct Volume Access Domain Policy Modification Domain Trust Modification Group Policy Modification Execution Guardrails Security Support Provider Shortcut Modification Time Providers Winlogon Helper DLL Boot or Logon Initialization Scripts Logon Script (Windows)	Abuse Elevation Control Mechanism Bypass User Account Control Access Token Manipulation Create Process with Token Make and Impersonate Token Parent PID Spoofing SID-History Injection Token Impersonation/Theft BITS Jobs Declassify/Decode Files or Information Direct Volume Access Domain Policy Modification Domain Trust Modification Group Policy Modification Execution Guardrails Exploitation for Defense Evasion File and Directory Permissions Modification Windows File and Directory Permissions Modification Hide Artifacts Email Action Rules	Adversary-in-the-Middle ARP Cache Poisoning LLMNR/NBT-NS Poisoning and SMB Relay Brute Force Credential Stuffing Password Cracking Password Guessing Password Spraying Credentials from Password Stores Credentials from Web Browsers Password Managers Windows Credential Manager Web Cookies Input Capture Credential API Hooking C2 Host Capture	Account Discovery Domain Account Email Account Local Account Application Window Discovery Browser Bookmark Discovery Domain Trust Discovery File and Directory Discovery Group Policy Discovery Network Service Scanning Network Share Discovery Network Sniffing Password Policy Discovery Peripheral Device Discovery Permissions Groups Software Discovery Query Registry Remote System Discovery Software Discovery Security Software Discovery System Information Discovery System Location	Exploitation of Remote Services Internal Spearfishing Lateral Tool Transfer Remote Service Session Hijacking RDP Hijacking Remote Services Distributed Component Object Model Remote Desktop Protocol SMB/Windows Admin Shares VNC Windows Remote Management Replication Through Removable Media Software Deployment Tools Taint Shared Content Use Alternate Authentication Material Pass the Hash Pass the Ticket	Adversary-in-the-Middle ARP Cache Poisoning File Transfer Protocols Mail Protocols Web Protocols Exfiltration Through Removable Media Archive via Custom Method Archive via Library Archive via Utility Audio Capture Automated Collection Browser Session Hijacking Clipboard Data Data from Information Repositories Sharepoint Data from Local System Data from Network Shared Drive Data from Removable Media Data Staged Local Data Staging Remote Data Staging File and Directory	Application Layer Protocol DNS File Transfer Protocols Mail Protocols Web Protocols Exfiltration Over Symmetric Encrypted Non-C2 Protocol Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol Data Encoding Non-Standard Encoding Standard Encoding Data Obfuscation Junk Data Protocol Impersonation Steganography Dynamic Resolution DNS Calculation Domain Generation Algorithms Fast Flux DNS Encrypted Channel Asymmetric Cryptography Symmetric Cryptography	Automated Exfiltration Data Transfer Size Limits Exfiltration Over Alternative Protocol Exfiltration Over Asymmetric Encrypted Non-C2 Protocol Exfiltration Over Symmetric Encrypted Non-C2 Protocol Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol Exfiltration Over C2 Channel Exfiltration Over Other Network Medium Exfiltration Over Bluetooth Exfiltration Over Physical Medium Exfiltration Over USB Exfiltration Over Web Service Exfiltration to Cloud Storage Exfiltration to Code Repository Scheduled Transfer	Account Access Removal Data Destruction Data Encrypted for Impact Data Manipulation Runtime Data Manipulation Stored Data Manipulation Transmitted Data Manipulation Defacement External Defacement Internal Defacement Disk Wipe Disk Content Wipe Disk Structure Wipe Endpoint Denial of Service Application Exhaustion Flood Application or System Exploitation OS Exhaustion Flood Service Exhaustion Flood Firmware Corruption Inhibit System Recovery Network Denial of Service

Gambar 4 - Coverage data sources default PT X

<sup>8</sup> python dettect.py ds -fd ../c/shared/x\_default.yaml -l

<sup>9</sup> <https://github.com/rabobank-cdc/DeTTect/wiki/How-to-use-the-framework>



3. Melakukan gap analysis untuk memfokuskan ruang perbaikan. Hal ini dapat dilakukan dengan beberapa cara, antara lain:

a. Gap analysis antara current coverage dengan TTP threat actor/software tertentu;

Sesuai dengan skenario awal kita, PT X mengetahui mengenai serangan Conti pada sebuah PT Z dan berusaha menyiapkan *detection* yang lebih baik dengan menggunakan ATT&CK. Untuk melakukan hal ini, maka kita perlu mengetahui TTP yang dimiliki Conti kemudian *coverage data source* PT X sekarang, dan kemudian menggabungkan dua layer tersebut untuk melihat TTP conti yang tidak tercover oleh PT X sekarang.

Membuat *layer* TTP Conti tidak menjadi bahasan utama, namun secara umum dilakukan dengan menggunakan menu *selection control* kemudian mencari Conti di search box. Untuk membandingkan layer TTP Conti dan layer data sources PT X sekarang, maka kita perlu membuat layer baru yang menggabungkan antara TTP Conti (Gambar 5) dengan coverage yang dimiliki PT X sekarang (Gambar 4).

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Active Scanning	Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interface	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Adversary in-the-Middle	Account Discovery	Exploitation of Remote Services	Adversary in-the-Middle	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Gather Victim Host Information	Compromise Accounts	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution	Access Token Manipulation	Access Token Manipulation	Brute Force	Browser Bookmark Discovery	Intercept Spearphishing	Archive Collected Data	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information	Compromise Infrastructure	External Remote Services	Deploy Container	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	Credentials from Password Stores	Browser Bookmark Discovery	Automated Collection	Audio Capture	Data Encoding	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Gather Victim Network Information	Develop Capabilities	Hardware Additions	Exploitation for Client Execution	Boot or Logon Autostart Execution	Build Image on Host	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking	Clipboard Data	Dynamic Resolution	Exfiltration Over C2 Channel	Data Manipulation
Gather Victim Org Information	Establish Accounts	Pushing	Inter-Process Communication	Browser Extensions	Direct Volume Access	Direct Volume Access	Domain Policy Modification	Cloud Service Dashboard	Replication Through Removable Media	Data from Cloud Storage Object	Encrypted Channel	Defacement	Disk Wipe
Phishing for Information	Obtain Capabilities	Replication Through Removable Media	Native API	Compromise Client Software Binary	Create or Modify System Process	Create or Modify System Process	Domain Policy Modification	Cloud Storage Object Discovery	Software Deployment Tools	Data from Configuration Repositories	Ingress Tool Transfer	Endpoint Denial of Service	Firmware Corruption
Search Closed Sources	Stage Capabilities	Supply Chain Compromise	Scheduled Task/Job	Create Account	Domain Policy Modification	Domain Policy Modification	Input Capture	Container and Resource Discovery	File and Directory Discovery	Data from Information Repositories	Multi-Stage Channels	Exfiltration Over Physical Medium	Resource Hijacking
Search Open Technical Databases	Trusted Relationship	Valid Accounts	Software Deployment Tools	Create or Modify System Process	Event Triggered Execution	Event Triggered Execution	Network Sniffing	Group Policy Discovery	Use Alternate Authentication Material	Data from Local System	Non-Application Layer Protocol	Scheduled Transfer	System Shutdown/Reboot
Search Open Websites/Domains	User Execution	Windows Management Instrumentation	System Services	External Remote Services	Hijack Execution Flow	Hijack Execution Flow	OS Credential Dumping	Network Service Scanning	Network Share Discovery	Data from Removable Media	Protocol Tunneling	Service Stop	
Search Victim-Owned Websites	Implant Internal Image	Modify Authentication Process	Scheduled Task/Job	Process Injection	Process Injection	Process Injection	Steal Application Access Token	Network Sniffing	Network Sniffing	Data Staged	Remote Access Software	Traffic Signaling	
	Modify Authentication Process	Office Application Startup	Pre-OS Boot	Scheduled Task/Job	Indirect Command Execution	Indirect Command Execution	Two-Factor Authentication Interception	Permission Groups Discovery	Process Discovery	Input Capture	Screen Capture	Web Service	
	Scheduled Task/Job				Masquerading	Masquerading	Unsecured Credentials	Query Registry	Remote System	Video Capture			

Gambar 5 - Conti TTP

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 9 techniques	Privilege Escalation 13 techniques	Defense Evasion 40 techniques	Credential Access 13 techniques	Discovery 29 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 10 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning [10]	Acquire Infrastructure [7]	Drive-by Compromise [9]	Command and Control Scripting [12]	Account Manipulation [9]	Abuse Elevation Control Mechanism [13]	Abuse Elevation Control Mechanism [40]	Adversary-in-the-Middle [13]	Account Discovery [29]	Exploitation of Remote Services [9]	Adversary-in-the-Middle [17]	Application Layer Protocol [10]	Automated Exfiltration [9]	Account Access Removal [13]
Gather Victim Host Information [10]	Compromise Accounts [7]	Exploit Public-Facing Application [9]	Container Administration Command [12]	BITS Jobs [9]	Access Token Manipulation [13]	Access Token Manipulation [40]	Brute Force [13]	Application Window Discovery [29]	Internal Spearphishing [9]	Archive Collected Data [17]	Communication State Limits [10]	Data Transfer Size Limits [9]	Data Destruction [13]
Gather Victim Identity Information [10]	Compromise Remote Services [7]	External Remote Services [9]	Deploy Container [12]	Boot or Logon Automated Execution [9]	Boot or Logon Automated Execution [13]	Boot or Logon Automated Execution [40]	Browser Bookmark Discovery [13]	Browser Bookmark Discovery [29]	Lateral Tool Transfer [9]	Audio Capture [17]	Data Encoding [10]	Exfiltration Over Alternative Protocol [9]	Data Encrypted for Impact [13]
Gather Victim Network Information [10]	Develop Capabilities [7]	Hardware Additions [9]	Exploitation for Client Execution [12]	Boot or Logon Manipulation Scripts [9]	Boot or Logon Manipulation Scripts [13]	Boot or Logon Manipulation Scripts [40]	Build Image on Host [13]	Cloud Infrastructure Discovery [29]	Remote Service Session Hijacking [9]	Automated Collection [17]	Dynamic Resolution [10]	Exfiltration Over C2 Channel [9]	Data Manipulation [13]
Gather Victim Org Information [10]	Establish Accounts [7]	Phishing [9]	Inter-Process Communication [12]	Compromise Client Software [9]	Create or Modify System Process [13]	Create or Modify System Process [40]	Deepfuscate/Decode Files or Information [13]	Cloud Service Dashboard [29]	Remote Service Session Hijacking [9]	Browser Session Hijacking [17]	Data Obfuscation [10]	Defacement [9]	Disk Wipe [13]
Phishing for Information [10]	Obtain Capabilities [7]	Replication Through Removable Media [9]	Naïve API [12]	Scheduled Task/Job [9]	Domain Policy Modification [13]	Domain Policy Modification [40]	Direct Volume Access [13]	Cloud Storage Object Discovery [29]	Software Deployment Tools [9]	Clipboard Data [17]	Dynamic Resolution [10]	Exfiltration Over Other Network Protocol [9]	Endpoint Denial of Service [13]
Search Closed Sources [10]	Stage Capabilities [7]	Supply Chain Compromise [9]	Trusted Relationship [12]	Create Account [9]	Event Triggered Execution [13]	Event Triggered Execution [40]	Execution Guardrails [13]	Container and Resource Discovery [29]	Replication Through Removable Media [9]	Data from Cloud Storage Object [17]	Encrypted Channel [10]	Exfiltration Over Physical Medium [9]	Firmware Corruption [13]
Search Open Technical Databases [10]	Search Open Websites/Domains [7]	Valid Accounts [9]	Software Deployment Tools [12]	Create or Modify System Process [9]	Escape to Host [13]	Escape to Host [40]	File and Directory Permissions Modification [13]	Domain Trust Discovery [29]	Software Deployment Tools [9]	Data from Information Repository [17]	Fallback Channels [10]	Exfiltration Over Physical Medium [9]	Inhibit System Recovery [13]
Search Victim-Owned Websites [10]			User Execution [12]	External Remote Services [9]	Hide Artifacts [13]	Hide Artifacts [40]	Network Stalling [13]	File and Directory Discovery [29]	Use Appropriate Authentication Material [9]	Data from Local System [17]	Ingress Tool Transfer [10]	Exfiltration Over Web Service [9]	Network Denial of Service [13]
			Windows Management Instrumentation [12]	Hijack Execution Flow [9]	Hijack Execution Flow [13]	Hijack Execution Flow [40]	OS Credential Dumping [13]	Group Policy Discovery [29]	Use Appropriate Authentication Material [9]	Data from Network Shared Drive [17]	Multi-Stage Channels [10]	Exfiltration Over Web Service [9]	Resource Hijacking [13]
			Implement Internal Image [12]	Scheduled Task/Job [9]	Indirect Command Execution [13]	Indirect Command Execution [40]	Steal Application Access Token [13]	Network Service Discovery [29]	Use Appropriate Authentication Material [9]	Data from Removable Media [17]	Non-Application Layer Protocol [10]	Scheduled Transfer [9]	Service Stop [13]
			Modify Authentication Process [12]	Valid Accounts [9]	Process Injection [13]	Process Injection [40]	Steal or Forge Kerberos Tickets [13]	Network Stalling [29]	Use Appropriate Authentication Material [9]	Data from Removable Media [17]	Protocol Tunneling [10]	Transfer Data to Cloud Account [9]	System Shutdown/Reboot [13]
			Office Application Startup [12]	Pre-OS Boot [9]	Pre-OS Boot [13]	Pre-OS Boot [40]	Two-Factor Authentication Interception [13]	Peripheral Device Discovery [29]	Use Appropriate Authentication Material [9]	Data Staged [17]	Proxy [10]		
			Pre-OS Boot [12]	Scheduled Task/Job [9]	Scheduled Task/Job [13]	Scheduled Task/Job [40]	Unsecured Credentials [13]	Permission Groups Discovery [29]	Use Appropriate Authentication Material [9]	Email Collection [17]	Remote Access Software [10]		
							Unsecured Credentials [13]	Process Discovery [29]	Use Appropriate Authentication Material [9]	Input Capture [17]	Traffic Signaling [10]		
							Unsecured Credentials [13]	Query Registry [29]	Use Appropriate Authentication Material [9]	Screen Capture [17]	Web Service [10]		
							Unsecured Credentials [13]	Remote System [29]	Use Appropriate Authentication Material [9]	Video Capture [17]			

Gambar - 6 TTP Conti yang tidak dicakup oleh Data yang Dimiliki

Pada gambar di atas, terlihat bahwa hanya terdapat satu teknik yang digunakan Conti dan sudah di-cover oleh *data source* yang dimiliki oleh PT X, yaitu **taint shared content**, sedangkan sisanya tidak tercover.

**b. Gap analysis antara current prevention/security control dengan TTP threat actor/software tertentu.**

*Gap analysis* dengan *security control* dilakukan dengan membuat layer baru yang berasal dari controls yang diterapkan perusahaan. Sebagai contoh penulis akan menggunakan mapping NIST 800-53 dengan ATT&CK karena mapping tersebut sudah tersedia<sup>10</sup>. Mungkin tidak banyak perusahaan Indonesia yang menggunakan NIST 800-53 sebagai *control*, namun NIST 800-53 cukup banyak digunakan, sehingga terdapat banyak sumber mapping NIST 800-53 ke security control lainnya seperti ISO 27001<sup>11</sup>, CIS<sup>12</sup> atau *security control* lain yang dimiliki perusahaan. Apabila *security control* yang digunakan perusahaan tidak ditemukan dalam *mapping* tersebut, maka harus dilakukan kegiatan manual, seperti yang kita lakukan pada langkah 1.

Sama seperti yang sebelumnya, kita akan membuat layer baru dengan menggunakan NIST 800-53. Artinya terhadap teknik yang sudah memiliki warna terdapat paling tidak *prevention* yang disediakan NIST 800-53 dan implementasinya dalam perusahaan. Gambar dibawah memperlihatkan

<sup>10</sup> <https://ctid.mitre-engenuity.org/our-work/nist-800-53-control-mappings/>

<sup>11</sup> <https://csrc.nist.gov/CSRC/media/Publications/sp/800-53/rev-5/final/documents/sp800-53r5-to-iso-27001-mapping.docx>

<sup>12</sup> <https://www.cisecurity.org/insights/white-papers/cis-controls-v8-mapping-to-nist-csf>

*coverage prevention* yang dimiliki NIST 800-53. Secara umum *coverage* NIST 800-53 sangat baik, tentu saja sedikit *fine tuning* tetap diperlukan untuk memastikan bagaimana implementasi kontrol tersebut pada perusahaan anda. Sebagai pembanding maka dapat dibuat *layer* baru antara NIST 800-53 dengan Conti TTP, sehingga kita dapat melihat bagian conti TTP yang memiliki kekurangan *prevention/ controls* atau bahkan tidak dicover oleh NIST 800-53.

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 40 techniques	Credential Access 15 techniques	Discovery 29 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Phishing for Information (a1)	Acquire Infrastructure (a11)	Exploit Public-Facing Application (a18)	Command and Control (a29)	Server Software Compromise (a44)	Exploitation for Privilege Escalation (a63)	Modify System Image (a78)	Unsecured Credentials (a97)	Network Service Scanning (a112)	Exploitation of Remote Services (a132)	Data from Cloud Storage Object (a151)	Application Layer Protocol (a151)	Exfiltration Over Alternative Protocol (a167)	Data Manipulation (a182)
Active Scanning (a2)	Compromise Accounts (a12)	Valid Accounts (a19)	Software Deployment Tools (a30)	Valid Accounts (a45)	Valid Accounts (a45)	Exploitation for Defense Evasion (a79)	Adversary-Provided Credentials (a98)	Network Sniffing (a113)	Software Deployment Tools (a133)	Data from Cloud Storage Object (a152)	Remote Access Software (a152)	Firmware Corruption (a183)	
Gather Victim Host Information (a3)	Compromise Infrastructure (a13)	Drive-by Compromise (a20)	Inter-Process Communication (a31)	Create or Modify System Process (a46)	Abuse Elevation Control Mechanism (a47)	Abuse Elevation Control Mechanism (a47)	Exploitation for Credential Access (a99)	Container and Resource Discovery (a114)	Remote Service Session Hijacking (a134)	Data from Information Repositories (a153)	Transfer Data to Cloud Account (a168)	Service Stop (a184)	
Gather Victim Identity Information (a4)	Develop Capabilities (a14)	External Remote Services (a21)	Windows Management Instrumentation (a32)	High Execution Flow (a111)	Create or Modify System Process (a66)	Indicator Removal on Host (a82)	OS Credential Dumping (a100)	Domain Trust Discovery (a115)	Adversary-in-the-Middle (a135)	Data from Information Repositories (a154)	Encrypted Channel (a153)	Exfiltration Over Physical Medium (a169)	Inhibit System Recovery (a185)
Gather Victim Network Information (a5)	Establish Accounts (a15)	Phishing (a22)	Replication Through Removable Media (a23)	External Remote Services (a50)	Escape to Host (a67)	High Execution Flow (a111)	Stall Application Access Token (a101)	Cloud Service Dashboard (a117)	Remote Services (a135)	Automated Collection (a155)	Protocol Tunneling (a171)	Data Encrypted for Impact (a186)	
Gather Victim Org Information (a6)	Obtain Capabilities (a16)	Stage Capabilities (a17)	Scheduled Task/Job (a34)	Implant Internal Image (a51)	High Execution Flow (a111)	Pre-OS Boot (a49)	Stall or Forge Kerberos Tickets (a102)	Cloud Infrastructure Discovery (a118)	Lateral Tool Transfer (a136)	Data from Removable Media (a156)	Traffic Signaling (a172)	Exfiltration Over Network (a170)	Data Destruction (a187)
Search Closed Sources (a7)	Supply Chain Compromise (a24)	Trusted Relationship (a25)	System Services (a35)	Modify Authentication Process (a52)	Scheduled Task/Job (a68)	Domain Policy Modification (a69)	Modify Authentication Process (a103)	Password Policy Discovery (a119)	Replication Through Removable Media (a137)	Browser Session Hijacking (a157)	Communication Through Removable Media (a173)	Data Transfer Size Limits (a190)	Defacement (a188)
Search Open Technical Databases (a8)	Hardware Additions (a26)	Container Administration Command (a36)	User Execution (a37)	Browser Extensions (a37)	Process Injection (a54)	Signed Binary/Proxy Execution (a87)	Brute Force (a104)	Account Discovery (a120)	Network Share Discovery (a121)	Email Collection (a158)	Dynamic Resolution (a174)	Scheduled Transfer (a192)	Endpoint Denial of Service (a190)
Search Open Websites/Domains (a9)	Native API (a27)	Deploy Container (a38)	Modify Authentication Process (a39)	Create account (a40)	Boot or Logon Initialization Scripts (a55)	Impair Defenses (a88)	Network Sniffing (a105)	Application Window Discovery (a122)	Use alternate Authentication Material (a139)	Data from Local System (a159)	Fallback Channels (a175)	Exfiltration Over Other Network Medium (a193)	Account Access Removal (a195)
Search Victim-Owned Websites (a10)	Shared Modules (a28)	BITS Jobs (a57)	Access Token Manipulation (a57)	Event Triggered Execution (a58)	Account Manipulation (a74)	Root or Logon Initialization Scripts (a75)	Forced Authentication (a106)	Browser Bookmark Discovery (a123)	Internal Spearphishing (a140)	Archive Collected Data (a144)	Ingress Tool Transfer (a176)	Resource Hijacking (a196)	System Shutdown/Reboot (a197)

Gambar 7 - NIST 800-53 mapping to ATT&CK

Sama dengan langkah sebelumnya, maka kita dapat membandingkan NIST 800-53 (Gambar 7) dengan TTP Conti (Gambar 5), seperti yang bisa kita perhatikan pada gambar selanjutnya. Terlihat bahwa terdapat beberapa TTP yang tidak memiliki *security control* sama sekali pada NIST 800-53.

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 40 techniques	Credential Access 15 techniques	Discovery 29 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (1/2)	Acquire Infrastructure (4/4)	Drive-by Compromise (4/4)	Command and Scripting Interpreter (4/4)	Account Manipulation (4/4)	Abuse Elevation Control Mechanism (4/4)	Abuse Elevation Control Mechanism (4/4)	Adversary-in-the-Middle (2/2)	Account Discovery (3/4)	Exploitation of Remote Services (2/2)	Adversary-in-the-Middle (2/2)	Application Layer Protocol (4/4)	Automated Exfiltration (1/1)	Account Access Removal (4/4)
Gather Victim Host Information (1/1)	Compromise Accounts (1/1)	Exploit Public-Facing Application (4/4)	Container Administration Command (4/4)	BITS Jobs (4/4)	Access Token Manipulation (4/4)	Access Token Manipulation (4/4)	Brute Force (4/4)	Application Window Discovery (1/1)	Internal Spearphishing (2/2)	Archive Collected Data (1/1)	Communication Through Removable Media (4/4)	Data Transfer Size Limits (4/4)	Data Destruction (4/4)
Gather Victim Identity Information (1/1)	Compromise Infrastructure (2/2)	External Remote Services (4/4)	Deploy Container (4/4)	Boot or Logon Autostart Execution (11/15)	Boot or Logon Autostart Execution (11/15)	Boot or Logon Autostart Execution (11/15)	Credentials from Password Stores (4/4)	Browser Bookmark Discovery (1/1)	Lateral Tool Transfer (2/2)	Audio Capture (4/4)	Automated Collection (4/4)	Exfiltration Over Alternative Protocol (3/3)	Data Encrypted for Impact (4/4)
Gather Victim Network Information (1/1)	Develop Capabilities (2/2)	Hardware Additions (4/4)	Exploitation for Client Execution (4/4)	Boot or Logon Initialization Scripts (4/4)	Boot or Logon Initialization Scripts (4/4)	Boot or Logon Initialization Scripts (4/4)	Exploitation for Credential Access (4/4)	Cloud Infrastructure Discovery (1/1)	Remote Service Hijacking (2/2)	Automated Collection (4/4)	Data Obfuscation (2/2)	Exfiltration Over C2 Channel (4/4)	Data Manipulation (3/3)
Gather Victim Org Information (1/1)	Establish Accounts (2/2)	Phishing (4/4)	Inter-Process Communication (2/2)	Browser Extensions (4/4)	Create or Modify System Process (4/4)	Create or Modify System Process (4/4)	Forced Authentication (4/4)	Cloud Service Dashboard (1/1)	Remote Services (4/4)	Browser Session Hijacking (2/2)	Data Defacement (4/4)	Exfiltration Over Other Network Channel (4/4)	Defacement (2/2)
Phishing for Information (3/3)	Obtain Capabilities (2/2)	Replication Through Removable Media (4/4)	Native API (4/4)	Domain Policy Modification (2/2)	Domain Policy Modification (2/2)	Domain Policy Modification (2/2)	Input Capture (2/4)	Cloud Service Discovery (1/1)	Replication Through Removable Media (4/4)	Clipboard Data (4/4)	Dynamic Resolution (4/4)	Exfiltration Over Other Network Channel (4/4)	Disk Wipe (2/2)
Search Closed Sources (2/2)	Stage Capabilities (2/2)	Supply Chain Compromise (4/4)	Scheduled Task/Job (4/4)	Event Triggered Process (4/4)	Event Triggered Process (4/4)	Event Triggered Process (4/4)	Forge Web Credentials (2/2)	Cloud Storage Object Discovery (1/1)	Replication Through Removable Media (4/4)	Data from Cloud Storage Object (4/4)	Encrypted Channel (2/2)	Exfiltration Over Physical Medium (1/1)	Endpoint Denial of Service (4/4)
Search Open Technical Databases (2/2)	Trusted Relationship (4/4)	Valid Accounts (4/4)	Shared Modules (4/4)	Execution Guardrails (1/1)	Execution Guardrails (1/1)	Execution Guardrails (1/1)	Modify Authentication Process (4/4)	Domain Trust Discovery (1/1)	Software Deployment Tools (4/4)	Data from Configuration Repository (2/2)	Fallback Channels (4/4)	Exfiltration Over Physical Medium (1/1)	Firmware Corruption (4/4)
Search Open Websites/Domains (2/2)	Valid Accounts (4/4)	System Services (2/2)	User Execution (1/1)	Create or Modify System Process (4/4)	Create or Modify System Process (4/4)	Create or Modify System Process (4/4)	Network Sniffing (4/4)	File and Directory Permissions Modification (2/2)	Use Alternate Authentication Material (4/4)	Data from Information Repositories (3/3)	Ingress Tool Transfer (4/4)	Exfiltration Over Web Service (2/2)	Network Denial of Service (2/2)
Search Victim-Owned Websites (2/2)	System Services (2/2)	Windows Management Instrumentation (4/4)	External Remote Services (4/4)	Event Triggered Execution (10/15)	Event Triggered Execution (10/15)	Event Triggered Execution (10/15)	OS Credential Dumping (4/4)	Group Policy Discovery (1/1)	Multi-Stage Channels (4/4)	Data from Local System (4/4)	Non-Application Layer Protocol (4/4)	Scheduled Transfer (4/4)	Resource Hijacking (4/4)
			Hijack Execution Flow (11/15)	Hijack Execution Flow (11/15)	Hijack Execution Flow (11/15)	Hijack Execution Flow (11/15)	Steal Application Access Token (4/4)	Network Service Scanning (4/4)	Use Alternate Authentication Material (4/4)	Data from Network Shared Drive (4/4)	Non-Standard Port (4/4)	Transfer Data to Cloud Account (4/4)	System Shutdown/Reboot (4/4)
			Implant Internal Image (4/4)	Scheduled Task/Job (4/4)	Scheduled Task/Job (4/4)	Scheduled Task/Job (4/4)	Steal or Forge Kerberos Tickets (4/4)	Network Share Discovery (4/4)	Network Sniffing (4/4)	Data from Removable Media (4/4)	Protocol Tunneling (4/4)	Transfer Data to Cloud Account (4/4)	System Shutdown/Reboot (4/4)
			Modify Authentication Process (4/4)	Valid Accounts (4/4)	Valid Accounts (4/4)	Valid Accounts (4/4)	Steal Web Session Cookie (4/4)	Password Policy Discovery (4/4)	Peripheral Device Discovery (4/4)	Data Staged (2/2)	Proxy (4/4)	Transfer Data to Cloud Account (4/4)	System Shutdown/Reboot (4/4)
			Office Application Startup (4/4)	Office Application Startup (4/4)	Office Application Startup (4/4)	Office Application Startup (4/4)	Two-Factor Authentication Interception (4/4)	Permission Groups Discovery (4/4)	Process Discovery (4/4)	Email Collection (3/3)	Remote Access Software (4/4)	Traffic Signaling (1/1)	System Shutdown/Reboot (4/4)
			Pre-OS Boot (4/4)	Pre-OS Boot (4/4)	Pre-OS Boot (4/4)	Pre-OS Boot (4/4)	Unsecured Credentials (1/1)	Query Registry (4/4)	Remote System (4/4)	Input Capture (2/4)	Web Service (3/3)		
			Scheduled Task/Job (4/4)	Scheduled Task/Job (4/4)	Scheduled Task/Job (4/4)	Scheduled Task/Job (4/4)				Screen Capture (4/4)			
										Video Capture (4/4)			

Gambar 8 - Conti TTP not covered by 800-53

### c. Gap analysis antara detection rules dan data source.

Pada beberapa contoh diatas, penulis tidak secara eksplisit menggambarkan bahwa adanya akses atas sebuah *data source* tidak selalu berarti *alert* atas data *source* tersebut tersedia, karena ini adalah dua hal yang berbeda. Sebagai contoh, PT X mencurigai adanya *threat actor* yang menggunakan teknik T1550.002<sup>13</sup> (*Use Alternate Authentication Material: Pass the Hash*). Maka hanya dengan melihat bagian *coverage* yang kita buat pada Gambar 3, PT X dapat salah memahami bahwa teknik T1550.002 tersebut akan terdeteksi. Karena PT X mencatat event ID 4624 (login), sehingga pada bagian *coverage* yang kita buat dalam Gambar 4 (*coverage data sources default* PT X), T1550.002 ditandai dengan terdeteksi.

Hal ini tidak sepenuhnya benar, karena walaupun PT X sudah mencatat *event* ID 4624, namun tanpa adanya *alert*, maka apabila teknik T1550.002 digunakan, PT X baru akan mengetahuinya setelah dilakukan kegiatan analisis/ digital forensic atas event ID 4624. Untuk itu, idealnya PT X, selain memiliki *data source* (event ID 4624), harus memiliki alert atas penggunaan teknik T1550.002, sebagai contoh sederhana maka kita dapat menggunakan *sigma rule* untuk mendeteksi pass the hash<sup>14</sup> sebagai pelengkap dari data source event ID 4624 yang dimiliki PT X.

<sup>13</sup> <https://attack.mitre.org/techniques/T1550/002/>

<sup>14</sup> <https://github.com/mdcrevoisier/SIGMA-detection-rules/blob/main/windows-os/win-os-Pass-the-hash%20login%20with%20Mimikatz.yaml>

Hal sebaliknya juga berlaku, yaitu ada kemungkinan PT X memiliki *detection/alert rule* atas sebuah TTP tertentu yang dipetakan ATT&CK, namun tidak memiliki *data source* untuk men-*trigger alert*-nya. Untuk meminimalisir hal tersebut maka dapat dilakukan perbandingan layer antara *data source* dengan *detection/alert rule* yang dimiliki PT X.

#### 4. Melakukan langkah perbaikan berdasarkan langkah 3

Tahapan terakhir ini bukan merupakan fokus bahasan pada tulisan ini. Pada langkah terakhir, maka PT X sudah memiliki bagian-bagian yang perlu ditingkatkan, baik untuk *visibility (data source)* maupun untuk *prevention (security control)* yang diperoleh dari kegiatan pada langkah 3.

## Penutup

---

Proses sebelumnya tentu saja bisa diulangi tidak hanya antara TTP *Threat Actor* dengan *current detection* atau *current control*, melainkan bisa juga menyandingkan antara *alert rule* atau *security tools* (EDR, DLP, firewall) yang dimiliki, sampai berbagai skenario *detection* atau *prevention* lainnya.

Selain untuk meningkatkan postur keamanan (*detection & prevention*), *interface* ATT&CK yang berbasis grafis menjadi sarana yang tepat sebagai media komunikasi. Salah satu contohnya adalah, ATT&CK dapat digunakan untuk membantu mengkomunikasikan seberapa penting/seberapa luas cakupan dari sebuah kontrol keamanan kepada manajemen, sehingga dapat mengkomunikasikan kebutuhan penerapan kontrol tersebut.

## Referensi

---

1. <https://cloudyhappypeople.com/2021/04/17/using-detect-and-the-mitre-attck-framework-to-assess-your-security-posture/>
2. <https://www.youtube.com/watch?v=1zgpTR6D3M8>
3. <https://mitre-attack.github.io/attack-navigator/>
4. <https://attack.mitre.org/>

5. <https://github.com/rabobank-cdc/DeTTECT>
6. <https://blog.netwrix.com/2021/11/30/how-to-detect-pass-the-hash-attacks/>
7. <https://github.com/mdecrevoisier/SIGMA-detection-rules>
8. <https://www.infocyte.com/cyber-security/mitre-attck-framework/2021/03/26/best-way-to-evaluate-mitre-attack-coverage/>

## TENTANG PENULIS



### **Ewaldo Simon Hiras**

seorang penggiat tidur siang, keamanan informasi, digital forensik yang bekerja di Direktorat Jenderal Pajak (DJP).



# WINDOWS CORE PROCESS

oleh Ewaldo Simon Hiras



## PENGANTAR

---

Dalam sebuah kegiatan *incident response*, adakalanya kita perlu mengetahui karakteristik proses yang sedang berjalan, sehingga dapat memutuskan apakah proses tersebut *malicious* atau tidak. Berikut beberapa proses inti windows (*Windows core processes*), dengan sedikit deskripsi dan karakteristik masing-masing, sebagai acuan baseline, sehingga ketika melakukan *incident response* kita memiliki kemudahan untuk melakukan *filtering* proses yang *malicious* atau tidak. Sebelum melihat lebih jauh proses yang berjalan, baiknya perlu dipahami kembali beberapa topik pengantar berikut.

## 1. User Mode vs Kernel Mode

Sebuah proses bisa dijalankan dalam dua buah mode yang berbeda, yaitu *kernel mode* dan *user mode*. aplikasi biasa berjalan di *user mode*, sedangkan *core operating system component* berjalan di *kernel mode*.

## 2. Session 0 Vs Session 1

Sejak sistem operasi Windows Vista, Microsoft memperkenalkan "**session 0 isolation**". **Session 0** diperuntukan untuk layanan dan aplikasi non-interaktif. User yang login akan berada di session 1 atau selanjutnya. Proses yang berjalan di **session 0** tidak memiliki GUI. sedangkan **session 1** (dan seterusnya) untuk proses yang terkait/ dijalankan user.

## 3. Tools

Beberapa *tools* yang bisa digunakan untuk memahami lebih jauh proses ini, kita akan menggunakan *processes explorer*<sup>15</sup> dan *processes hacker*<sup>16</sup>. Selain itu terdapat pula beberapa perangkat berbasis *command line* yaitu *tasklist*, *wmic*, *Get-Process* atau *ps* (PowerShell).

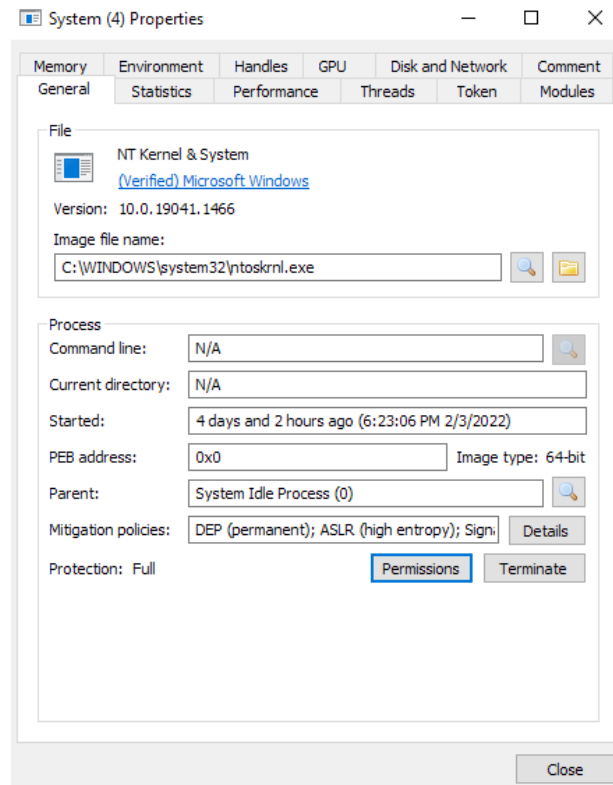
---

<sup>15</sup> <https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer>

<sup>16</sup> <https://processhacker.sourceforge.io/>



# SYSTEM



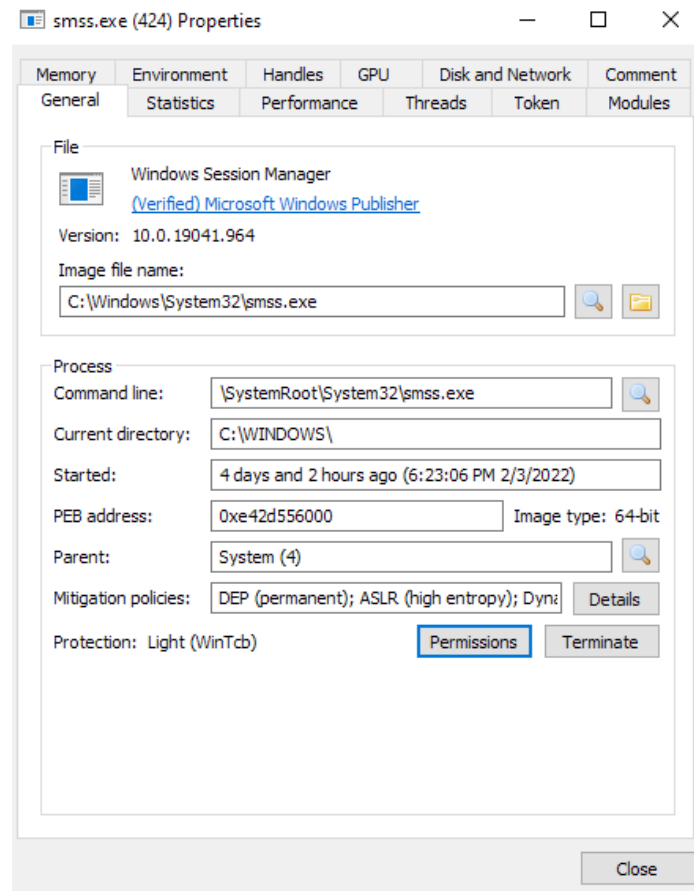
Gambar 1 - System Properties

System merupakan proses yang berjalan dalam *kernel mode*, serta menjadi rumah bagi proses-proses lain yang berjalan di *kernel mode*. System dijalankan (*parent*) oleh PID 0 (system idle process), atau pada *process explorer* tidak memiliki *parent*.

## Karakteristik System Process

- System selalu dijalankan dengan PID 4
- Hanya memiliki 1 (satu) *instance*
- Berjalan di session 0
- User account yang menjalankan SYSTEM
- Tidak memiliki *parent process* (*process explorer* atau *system idle process* PID 0 pada *process hacker*)
- Image filename berada di C:\Windows\system32\ntoskrnl.exe
- Start time: pada saat booting

## SYSTEM > SMSS.EXE



Gambar 2 - smss.exe

smss.exe (*Session Manager Subsystem*) atau *windows session manager*. smss.exe menjalankan csrss.exe dan wininit.exe di session 0, serta menjalankan csrss.exe dan winlogin.exe di session 1. Seperti yang ditulis sebelumnya, session 0 berisi proses-proses terkait layanan sedangkan session 1 untuk proses terkait user. smss.exe menjalankan proses dengan cara menjalankan child smss process setelah itu melakukan terminasi diri sendiri (*exit*), sehingga pada suatu waktu seharusnya hanya terdapat sebuah smss.exe.

### Beberapa Karakteristik smss.exe

- hanya terdapat satu *instances*
- parent process system

#### Beberapa Karakteristik smss.exe

- berjalan di session 0 (karena yang session 1 dan seterusnya menterminasi diri sendiri)
- user account yang menjalankan SYSTEM
- image path c:\Windows\System32\smss.exe
- start time: dalam beberapa detik dari *boot time* (untuk master *instance*)

## SYSTEM > CSRSS.EXE

---

proses ini bertanggung jawab menyediakan Windows API, mapping drive letters, and menangani proses shutdown Windows. csrss.exe dijalankan (parent process) oleh smss.exe yang akan mematikan dirinya sendiri setelahnya. oleh karena itu csrss.exe tidak memiliki parent process (parent process terminated/ non-existent process pada field parent).

#### Beberapa Karakteristik csrss.exe

- Tidak mempunyai parent process/ parent process sudah tidak jalan (smss.exe).
- Image path c:\Windows\System32\csrss.exe
- Bisa terdapat lebih dari satu instances (ingat smss.exe dimana tiap login akan menjalankan csrss.exe dan winlogin.exe pada session baru)
- User account yang menjalankan SYSTEM
- start time dalam beberapa detik dari boot time (untuk 2 instances pertama, dan setelah itu setiap ada login baru)

## SMSS.EXE > WININIT.EXE

---

Proses ini dijalankan oleh smss.exe, dan sama seperti csrss.exe, smss.exe akan mematikan dirinya sendiri setelah menjalankan proses ini, sehingga winit.exe tidak memiliki *parent process*. *Windows initialization process* atau wininit.exe bertanggung jawab menjalankan services.exe (*Service Control Manager*), lsass.exe (*Local Security Authority*), dan lsaiso.exe (hanya bila credential guard dinyalakan) dalam Session 0.

#### Beberapa Karakteristik wininit.exe

- Tidak mempunyai *parent process* atau *parent process* sudah tidak jalan (smss.exe).
- Image path c:\Windows\System32\
- Hanya satu instances
- User account yang menjalankan SYSTEM
- hati-hati terhadap image dengan nama yang mirip
- Start time: dalam beberapa detik dari boot time

## WININIT.EXE > SERVICES.EXE

services.exe/ Service Control Manager (SCM) berfungsi mengontrol services yang dijalankan serta men-set Last Known Good control set (HKLM\System\Select\LastKnownGood) setelah berhasil login. Informasi services yang dijalankan bisa dilihat di "HKLM\System\CurrentControlSet\Services" atau dengan "sc.exe query". Services.exe dijalankan oleh (parent process) winit.exe.

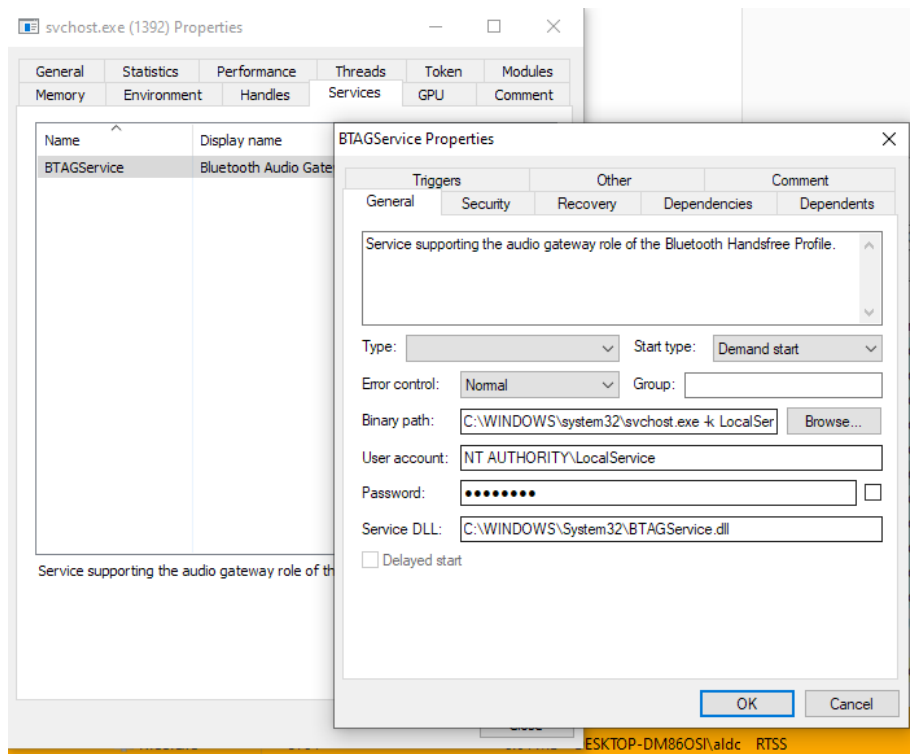
#### Beberapa Karakteristik services.exe

- parent process winit.exe
- Image path c:\Windows\System32\services.exe
- Hanya satu terdapat *instances*
- User account yang menjalankan SYSTEM
- Hati-hati terhadap image dengan nama yang mirip
- Start time dalam beberapa detik dari *boot time*

## WININIT.EXE > SERVICES.EXE > SVCHOST.EXE

svchost.exe (*service host/ host process for windows services*) bertugas mengontrol *windows services*. servis yang dijalankan proses ini berbentuk dll, dan dapat dilihat di registri (HKLM\SYSTEM\CurrentControlSet\Services\SERVICE\_NAME\Parameters). Sebagai contoh, svchost menjalankan *service* terkait *bluetooth*, maka kita bisa melihat dll yang dijalankan dengan cara:

Melalui aplikasi process hacker, **processhacker** > **right click on svchost.exe** > **properties** > **services** > **double click on name**. maka akan menampilkan gambar berikut, dimana pada *binary path* terlihat dll yang dijalankan.



Gambar 3 - svchost dan dll yang diload

Perlu juga diperhatikan flag/parameter "-k" pada command line di *binary path*, hal ini merupakan perintah pengelompokan services sejenis (sejak Windows 10 Version 1703 services sejenis dilakukan pengelompokan pada mesin dengan memory di atas 3.5 GB); atau pada registry key

"\HKLM\SYSTEM\CurrentControlSet\Services\BTAGService\Parameters"

#### Beberapa Karakteristik svchost.exe

- parent process services.exe
- Image file path C:\Windows\System32
- Hati-hati terhadap image dengan nama yang mirip
- Adanya "-k" flag/parameter

#### Beberapa Karakteristik svchost.exe

- *User account* yang menjalankan beragam (SYSTEM, Network Service, Local Service) tergantung jenis *services* (pada Windows 10 ada yang dijalankan *logged-in* user)
- start time: dalam beberapa detik dari *boot time*, namun mungkin ada yang berjarak dari *boot time*.

## WININIT.EXE > LSASS.EXE

*Local Security Authority Subsystem Service* (LSASS) adalah *process Windows OS* yang berfungsi meng-*enforce security policy*. Beberapa hal yang dilakukan antara lain verifikasi **user login**, perubahan *password* membuat *access tokens*, dan menulis *Windows Security Log*.

#### Beberapa Karakteristik lsass.exe

- Parent *process* wininit.exe
- Hanya satu instances
- Hati-hati terhadap image dengan nama yang mirip
- start time: dalam beberapa detik dari boot time
- Image file path C:\Windows\System32\lsass.exe
- user account yang menjalankan adalah SYSTEM

## WINLOGON.EXE

windows logon (winlogon.exe) berperan dalam menangani *secure attention sequence* (key combination **CTRL+ALT+DEL** yang menampilkan user login/password), memuat *user profile* (**NTUSER.DAT** ke registry HKCU), menjalankan userinit.exe (yang kemudian memuat

HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell dan kemudian exit), mengunci layar, dan juga screen saver.

#### Beberapa Karakteristik winlogon.exe

- Tidak memiliki *parent process* (karena parent smss.exe exit)
- Bisa terdapat lebih dari satu instances

#### Beberapa Karakteristik winlogon.exe

- Image file path C:\Windows\System32\winlogon.exe
- Start time dalam beberapa detik dari *boot time*

## EXPLORER.EXE

---

windows explorer (explorer.exe) bertanggung jawab untuk menampilkan *interface* untuk mengakses folder dan files, start menu, taskbar, dan lainnya. explorer.exe dijalankan oleh userinit.exe (memuat "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell"), yang kemudian exit sendiri sehingga tidak memiliki *parent process*.

#### Beberapa Karakteristik explorer.exe

- Tidak memiliki *parent process*
- Lokasi image di C:\WINDOWS\explorer.exe
- Dijalankan oleh *user* yang winlogin
- Seharusnya tidak memiliki koneksi *outbound* TCP/IP
- Start time beberapa saat setelah login (*interactive logon*)

## PENUTUP

---

Dengan menggunakan processhacker, procexp, atau perangkat lain, maka sebagai Tim Tanggap Insiden kita bisa membandingkan antara karakteristik asli (*baseline*) dari beberapa proses utama windows. Hal ini dapat dijadikan acuan untuk memutuskan apakah sebuah proses malicious atau tidak. Selain yang disebutkan di atas, proses malicious juga seringkali menggunakan nama yang serupa (mengganti huruf tertentu) untuk menyembunyikan dan menyamarkan diri menjadi proses yang *legitimate*, sehingga dapat menjadi perhatian selain hal-hal yang disebutkan sebelumnya.

## REFERENSI

---

1. <https://docs.microsoft.com/en-us/windows-hardware/drivers/gettingstarted/user-mode-and-kernel-mode>
2. <http://securityinternals.blogspot.com/2014/02/windows-session-0-isolation.html>
3. <https://yungchou.wordpress.com/2016/03/14/an-introduction-of-windows-10-credential-guard/>
4. [https://en.wikipedia.org/wiki/Service\\_Control\\_Manager](https://en.wikipedia.org/wiki/Service_Control_Manager)
5. <https://nasbench.medium.com/windows-system-processes-an-overview-for-blue-teams-42fa7a617920>
6. <https://andreafortuna.org/2017/06/15/standard-windows-processes-a-brief-reference/>
7. <https://tryhackme.com/room/btwindowsinternals>

### TENTANG PENULIS



#### **Ewaldo Simon Hiras**

seorang penggiat tidur siang, keamanan informasi, digital forensik yang bekerja di Direktorat Jenderal Pajak (DJP).





## FOLLINA

# MSDT VULNERABILITY

**CVE-2022-30190**

## APA ITU FOLLINA?

---

Follina adalah kerentanan Remote Code Execution (RCE) terbaru yang menyoroti aplikasi Microsoft Office. Nama Follina sendiri diambil dari nama penemu kerentanan ini yakni Kevin Beaumont setelah ia melihat sebuah dokumen di VirusTotal yang mengandung exploit untuk kerentanan ini bernama 05-2022-0438.doc.

05-2022 merujuk pada bulan Mei tahun 2022, sementara 0438 merujuk pada kode nomor telepon sebuah daerah bernama Follina, sebuah daerah yang berlokasi tidak jauh dari Venesia, Italia.

## CARA KERJA

---

- Penyerang mengirimkan phishing email ke korbannya yang berisi dokumen Microsoft Word yang sudah dimodifikasi.
- Korban membuka dokumen tersebut, seketika dokumen tersebut akan memanggil fungsi ms-msdt untuk menjalankan berbagai perintah sesuai yang dikehendaki oleh penyerang.
- Kerentanan ini tidak memerlukan fungsi macro sehingga membuat kerentanan ini menjadi sangat berbahaya.

Kerentanan ini saat ini sangat banyak sekali dimanfaatkan oleh penyerang, karena tidak memerlukan Macro pada Microsoft Word untuk menjalankannya.

## CARA MITIGASI SEMENTARA

---

Untuk menjalankan langkah mitigasi ini diperlukan hak akses setingkat Administrator pada sistem operasi windows

- Jalankan Command Prompt sebagai Administrator
- Lakukan pencadangan terhadap data registry dengan menjalankan perintah berikut

```
“reg export HKEY_CLASSES_ROOT\ms-msdt filename”
```

- Lakukan eksekusi perintah berikut untuk menghapus registri tersebut

```
“reg delete HKEY_CLASSES_ROOT\ms-msdt /f”
```

Langkah ini kerap kali menimbulkan sejumlah permasalahan, maka untuk mengembalikan konfigurasi tersebut, lakukan langkah berikut

- Jalankan Command Prompt sebagai Administrator
- Untuk melakukan restore jalankan perintah berikut  
“reg import filename”

## TIPS

---

Pastikan untuk memantau update dari Microsoft dan lakukan patching terhadap Microsoft Word dan Sistem Operasi Windows yang anda gunakan.

Selalu waspada terhadap email yang diterima dari sumber yang tidak dikenal, serta pastikan lakukan pemindaian dengan anti virus sebelum membuka file yang diterima.

# JOIN US! CYBER DEFENSE COMMUNITY INDONESIA



**WWW.CDEF.ID**

| Kunjungi situs/website resmi komunitas CDEF



**HTTPS://S.ID/CDEF-DISCORD**

| Ikuti diskusi streaming kami di Spotify



**HTTPS://TWITTER.COM/CDEF\_ID**

| Follow twitter akun resmi komunitas CDEF



**HTTPS://GITHUB.COM/CDEFID**

| Bergabung dan berkontribusi bersama kami melalui Github resmi komunitas CDEF



**REDAKSI@CDEF.ID**

| Info lebih lanjut silahkan kirim e-mail melalui alamat resmi e-mail kami



**HTTPS://CDEF.ID/GABUNG-DISKUSI-CDEF**

| bergabunglah dalam forum diskusi kami di Discord CDEF



**HTTPS://S.ID/CDEF-LINKEDIN**

| Follow akun LinkedIn komunitas CDEF



**HTTPS://S.ID/CDEF-YOUTUBE**

| Subscribe channel Youtube resmi komunitas CDEF

# THE FIRST LINE OF DEFENSE FROM INSIDER THREATS IS THE EMPLOYEES THEMSELVES

| CMU CYLAB

