Kasus Kebocoran Data di Dunia Kesehatan dan Kemampuan Solusi Keamanannya

Modul 5

Muhammad Ogin Hasanuddin

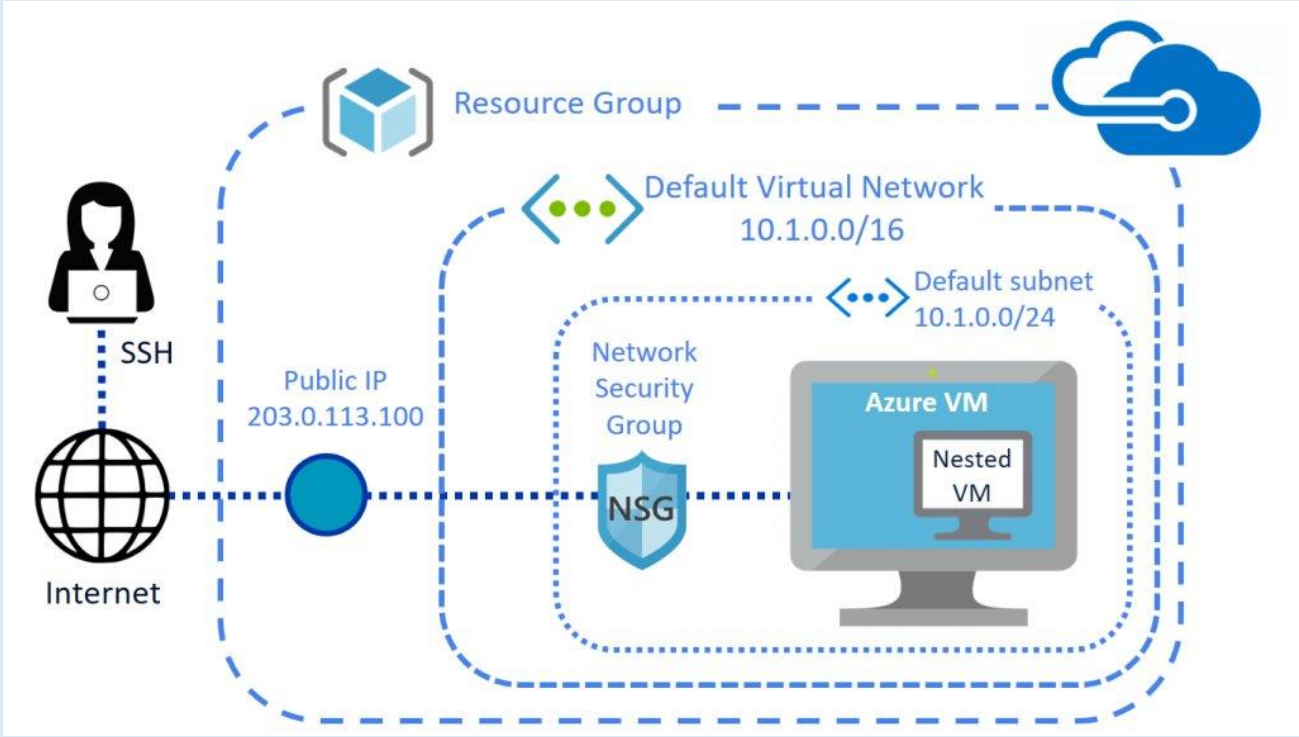
KK Teknik Komputer
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung

- Kemampuan Keamanan di Microsoft
- Cakupan Kemampuan Jaringan dan Platform Komputasi Awan Terhadap Manajemen Keuangan
- Perlindungan Ancaman di Microsoft 365 Defender
- Studi Kasus Bidang Kesehatan Menggunakan Platform Komputasi Awan

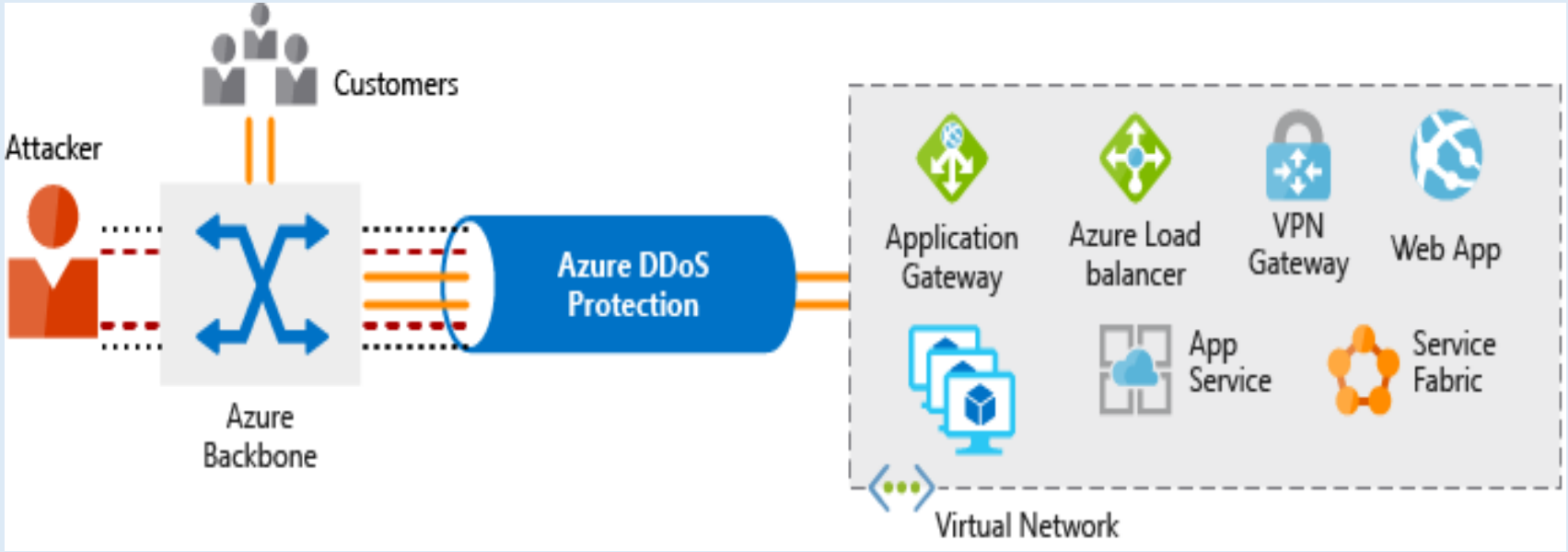
Kemampuan Keamanan di Microsoft

Grup keamanan jaringan (NSG) membantu dalam proses izin dan tolak lalu lintas jaringan dari sumber daya Azure yang ada pada jaringan VNet yang kita gunakan seperti virtual mesin. Grup keamanan jaringan terdiri dari sebuah aturan yang menentukan bagaimana lalu lintas tersebut akan disaring saat proses addressing atau pengalamatan. Untuk setiap aturannya, dapat dilakukan penentuan sumber dan tujuan, port, protokol dan tindakan yang diperlukan.

Aturan diproses berdasarkan prioritasnya dan Azure membuat serangkaian aturan yaitu tiga aturan masuk dan tiga aturan keluar agar memberikan tingkat keamanan dasar. Tidak dapat menghapus aturan default akan tetapi dapat menggantinya dengan membuat aturan baru dengan prioritas yang lebih tinggi dari sebelumnya.



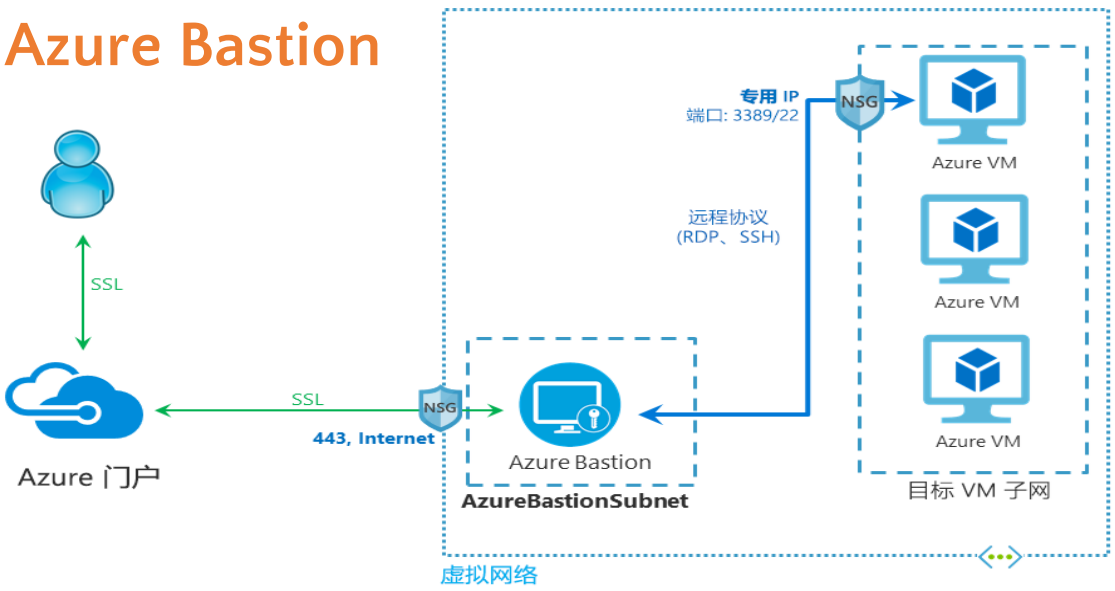
Servis Terdistribusi Penolakan Serangan (DDoS)



Bertujuan untuk meramaikan aplikasi dan server serta membuat tidak responsif atau lambat bagi pengguna. Serangan ini akan menargetkan titik akhir yang sedang menghadapi publik melalui internet. Ada tiga jenis serangan DDoS yang sering ditemui yaitu:

- Serangan volumetrik
- Serangan protokol
- Serangan lapisan aplikasi

Azure Bastion



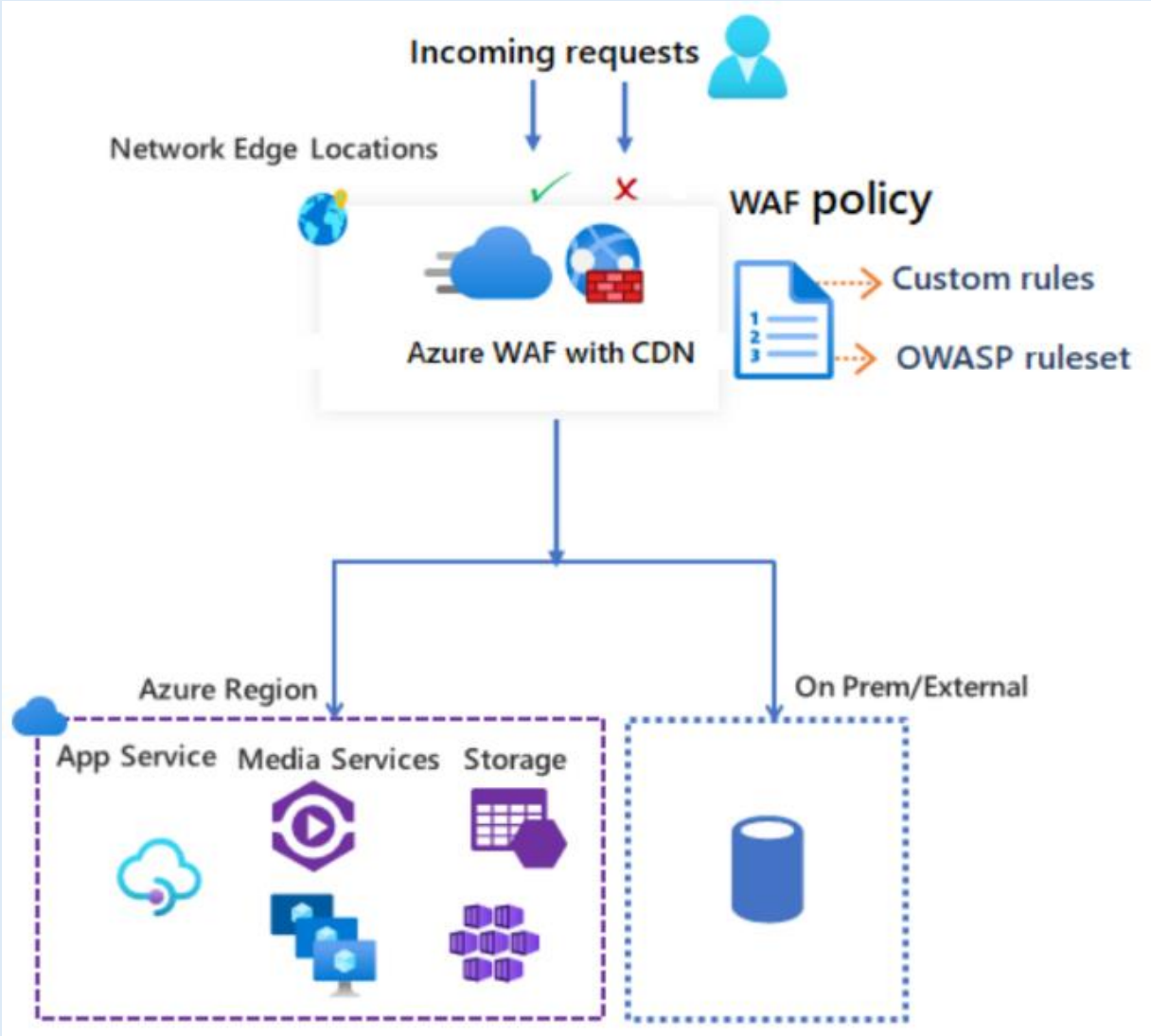
Fitur utama pada Azure Bastion yaitu:

- RDP di portal Azure, mendapatkan secara langsung di portal Azure dan menggunakan pengalaman sekali klik.
- Sesi jarak jauh melalui TLS dan traversal firewall untuk RDP, menggunakan web berbasis HTML yang secara otomatis mengalir ke perangkat lokal. Nantinya akan mendapatkan RDP dalam melintasi firewall perusahaan dengan aman.

- Tidak memerlukan IP publik di Azure VM, mendapat akses ke mesin virtual Azure menggunakan IP pribadi di VM masing – masing user.
- Tidak perlu mengelola NSG, terkelola sepenuhnya dari Azure yang diperkuat secara internal untuk menyediakan konektivitas yang aman.
- Perlindungan terhadap pemindaian port, VM melindungi dari pemindaian port oleh pengguna dan penyerang yang berada di luar jaringan virtual.
- Perlindungan terhadap eksploitasi zero – day, menjaga Azure Bastion tetap kokoh dan selalu terbarui.

Firewall Aplikasi Web

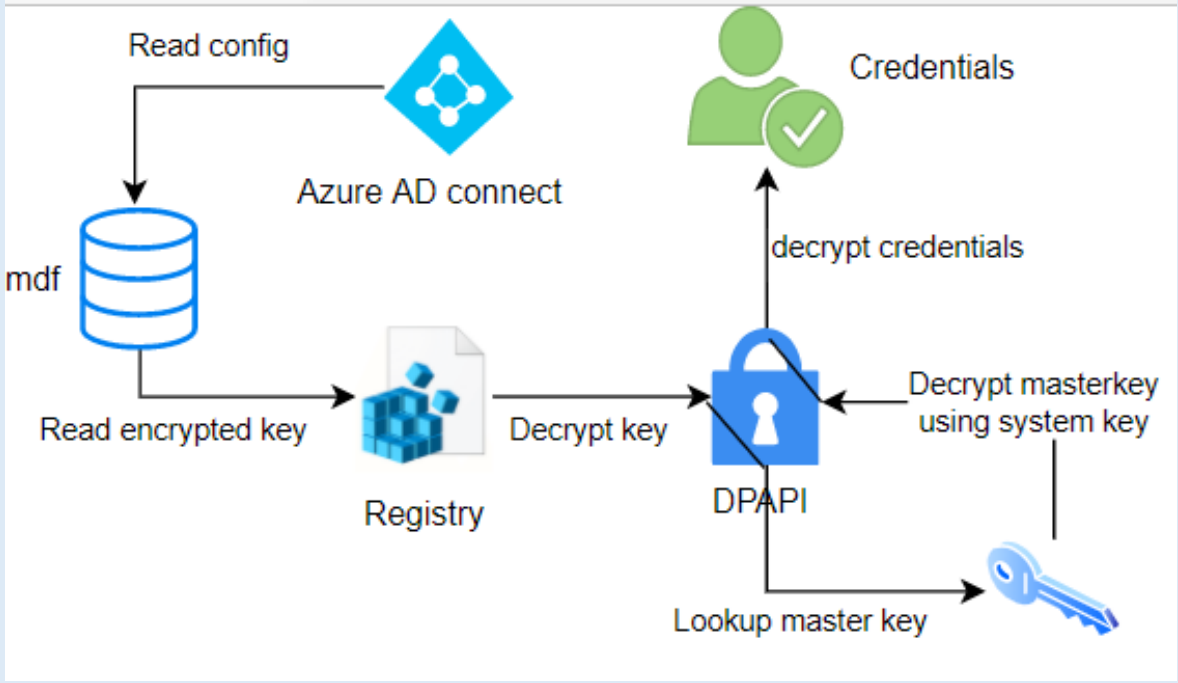
WAF memberikan jaminan perlindungan yang lebih baik kepada administrator aplikasi terhadap ancaman dan gangguan. WAF dapat digunakan dengan layanan Azure Application Gateway, Azure Front Door, dan Azure Content Delivery Network (CDN) dari Microsoft. WAF memiliki fitur yang disesuaikan untuk setiap layanan tertentu



Enkripsi Data di Azure

Enkripsi di Azure terbagi menjadi tiga seperti berikut:

- Enkripsi layanan penyimpanan Azure membantu melindungi data saat istirahat dengan mengenkripsi otomatis sebelum menyimpannya ke disk yang dikelola Azure serta mendekripsi data sebelum pengambilannya.
- Enkripsi disk Azure membantu mengenkripsi disk mesin virtual Windows dan Linux IaaS. Menggunakan fitur BitLocker standar industri untuk menyediakan enkripsi volume untuk OS dan disk data.
- Enkripsi data transparan (TDE) membantu melindungi Azure SQL Database dan Azure Data Warehouse dari ancaman aktivitas jahat dengan melakukan enkripsi dan dekripsi real – time dari database, terkait backup juga file log transaksi tanpa memerlukan perubahan di aplikasi



Cakupan Kemampuan Jaringan dan Platform Komputasi Awan Terhadap Manajemen Keamanan (CSPM)

CSPM menggunakan alat dan layanan di lingkungan komputasi awan untuk memantau dan memprioritaskan peningkatan dan fitur keamanan. Alat dan layanan yang dimaksud yaitu:

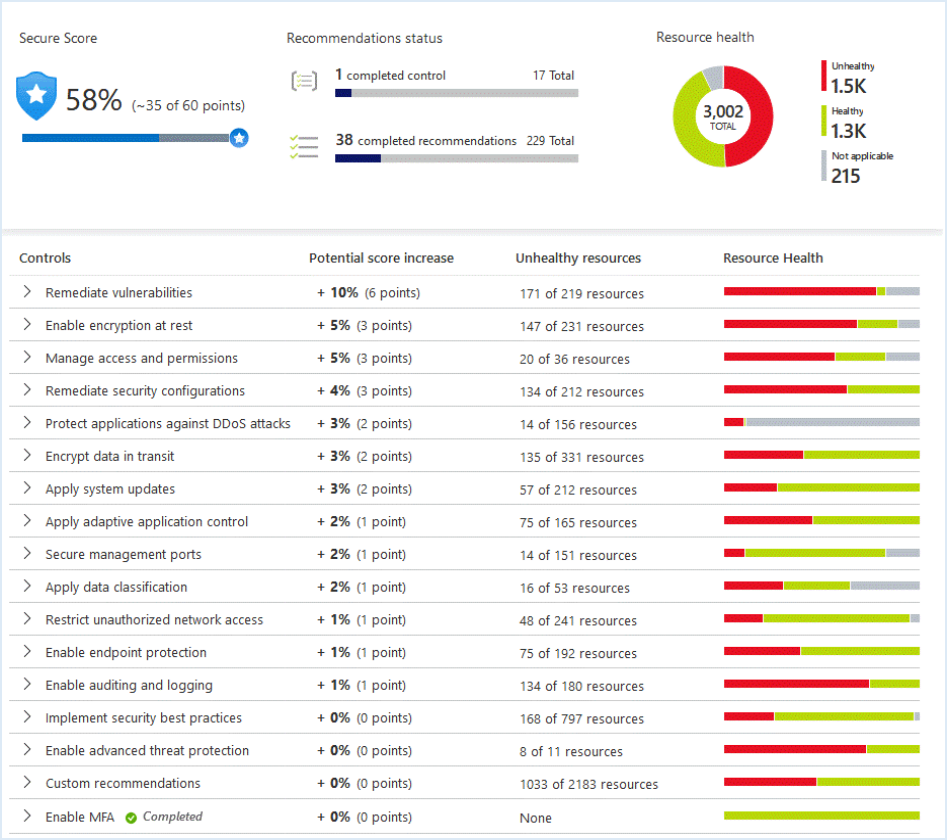
- Kontrol akses berbasis zero trust
- Penilaian risiko real time
- Manajemen ancaman dan kerentanan (TVM)
- Kebijakan teknis
- Sistem dan arsitektur pemodelan ancaman

Tujuan utama tim keamanan komputasi awan yang bekerja pada CSPM adalah untuk melaporkan dan meningkatkan postur keamanan organisasi setiap saat dengan berfokus dalam mengganggu laba atas investasi penyerang potensi.

Microsoft Defender for Cloud Computing

Azure Defender (Microsoft Defender for Cloud) adalah manajemen postur keamanan dan perlindungan ancaman. Microsoft Defender memenuhi tiga kebutuhan ketika mengelola keamanan sumber daya dan beban kerja di awan dan lokal:

- Mengkaji terus – menerus, mengetahui postur keamanan, identifikasi dan melacak kerentanan.
- Aman – memperkuat semua sumber daya dan layanan yang terhubung.
- Defend – mendeteksi dan mengatasi ancaman terhadap sumber daya, beban kerja dan layanan.



Paket Microsoft Devender	Fungsi
Microsoft Defender untuk server	Menambahkan deteksi ancaman dan pertahanan tingkat lanjut untuk Windows dan Linux
Microsoft Defender untuk app service	Mengidentifikasi serangan yang menargetkan aplikasi yang berjalan di atas App Service
Microsoft Defender untuk storage	Mendeteksi aktivitas yang berpotensi berbahaya di akun Azure storage
Microsoft Defender untuk SQL	Mengamankan database dan datanya di mana pun berada
Microsoft Defender untuk kubernetes	Menyediakan pengerasan lingkungan keamanan Kubernetes cloud – native, perlindungan beban kerja dan perlindungan run – time
Microsoft Defender untuk menampung pendaftar	Melindungi semua pendaftar berbasis Azure Resource Manager
Microsoft Defender untuk key vault	Melindungi ancaman tingkat lanjut
Microsoft Defender untuk manajer sumber daya	Memantau operasi manajemen sumber daya di organisasi
Microsoft Defender untuk DNS	Menyediakan lapisan perlindungan tambahan untuk sumber data yang menggunakan kemampuan resolusi yang disediakan
Microsoft Defender untuk perlindungan relasional terbuka	Menghadirkan perlindungan ancaman untuk basis data relasional sumber terbuka

Perlindungan Ancaman Microsoft 365 Defender

Manajemen informasi keamanan (SIEM), respons otomatis orkestrasi keamanan (SOAR), dan deteksi respons yang diperluas (XDR) memberikan wawasan keamanan yang sangat baik dan otomatisasi keamanan yang dapat meningkatkan perimeter keamanan jaringan organisasi. SIEM adalah alat yang digunakan dalam mengumpulkan data dari seluruh area termasuk infrastruktur, perangkat lunak dan sumber daya. Di mana akan dilakukan analisis dengan mencari korelasi atau anomali dan menghasilkan peringatan. Sedangkan SOAR berperan dalam pengambilan peringatan dari banyak sumber yang akan memicu alur kerja dan proses secara otomatis yang dapat digerakkan oleh tindakan untuk menjalankan tugas keamanan yang mengurangi masalah. XDR hadir untuk keamanan yang cerdas, otomatis dan terintegrasi di seluruh domain organisasi. Ini membantu dalam mencegah, mendeteksi dan merespons ancaman di seluruh identitas, titik akhir, aplikasi, email, IoT, infrastruktur dan platform cloud.

1. Microsoft Sentinel Melindungi Ancaman Terintegrasi
2. Microsoft 365 Defender
3. Microsoft Defender Endpoint
4. Microsoft Defender Aplikasi Awan

Studi Kasus

Sebagian besar penerapan komputasi awan untuk bidang kesehatan di Indonesia masih tergolong baru, namun teknologi tersebut sudah digunakan di negara – negara maju. Indonesia perlu adanya edukasi serta pelatihan – pelatihan ke pengguna lokal untuk mengantisipasi adanya kekhawatiran tentang masalah keamanan dan privasi. Contohnya seperti CT – Scan mendapat dukungan dari perkembangan teknologi informasi, karena dapat menggambarkan struktur bagian dalam tubuh manusia yang hasilnya dapat disimpan sebagai data elektronik dan dilihat di layar komputer.

Studi kasus secara detail silahkan baca di modul 5 ☺


Thank You ☺