BAB IV
HASIL DAN PEMBAHASAN

4.1 Hasil Studi Lapangan

4.1.1 Perlindungan Keamanan Siber yang Digunakan

Dari hasil studi lapangan yang telah dilakukan diketahui bahwa ada 3 sisi perlindungan keamanan siber yang telah dilakukan oleh institusi XYZ, yaitu perlindungan dari sisi firewall internet, kemudian perlindungan dari sisi endpoint, terakhir ada perlindungan dari sisi email. Untuk perlindungan dari sisi firewall internet dengan menggunakan *tool* yang bernama Sangfor NGAF, lalu untuk perlindungan dari sisi end user menggunakan *tool* Bitdefender, terakhir untuk perlindungan dari sisi email adalah dengan menggunakan *tool EOP (Exchange Online Protection).*

4.2.1. Perlindungan dari sisi Firewall Internet (Sangfor NGAF)

Sangfor NGAF adalah Sangfor Next Generation Application Firewall (Sangfor NGAF) adalah solusi keamanan aplikasi web generasi terkini yang dikembangkan oleh Sangfor Technologies. Sebagai perusahaan keamanan siber asal China, Sangfor berfokus dalam melindungi aplikasi dan data penting organisasi dari ancaman dunia maya yang kian canggih. Dalam dekade terakhir, serangan siber yang mengeksploitasi celah pada aplikasi web kian marak. Mulai dari defacement, injeksi SQL, remote code execution, hingga skenario peretasan yang lebih rumit seperti botnet dan ransomware. Sangfor NGAF hadir dengan kemampuan artificial intelligence dan machine learning terdepan untuk memberikan proteksi menyeluruh bagi aplikasi web perusahaan.

Berbekal algoritma pembelajaran mandiri, Sangfor NGAF mampu secara cerdas membedakan lalu lintas web normal dan aktivitas mencurigakan yang mengindikasikan upaya serangan atau eksploitasi. Produk ini belajar pola perilaku pengguna dan aplikasi secara dinamis untuk mendeteksi ancaman baru maupun yang sudah ada sebelumnya (known and unknown threats). Sangfor NGAF menyediakan perlindungan komprehensif mulai dari pencegahan remote code execution injection lalu cross site scripting (XSS) kemudian hingga serangan DDoS. Fitur pemindaian antivirus secara runtime dan intersepsi konten berbahaya juga turut memperkokoh lapisan pertahanan. Produk ini bahkan mampu menginspeksi lalu lintas HTTPS terenkripsi guna mencegah peretas menyusup lewat celah SSL/TLS.

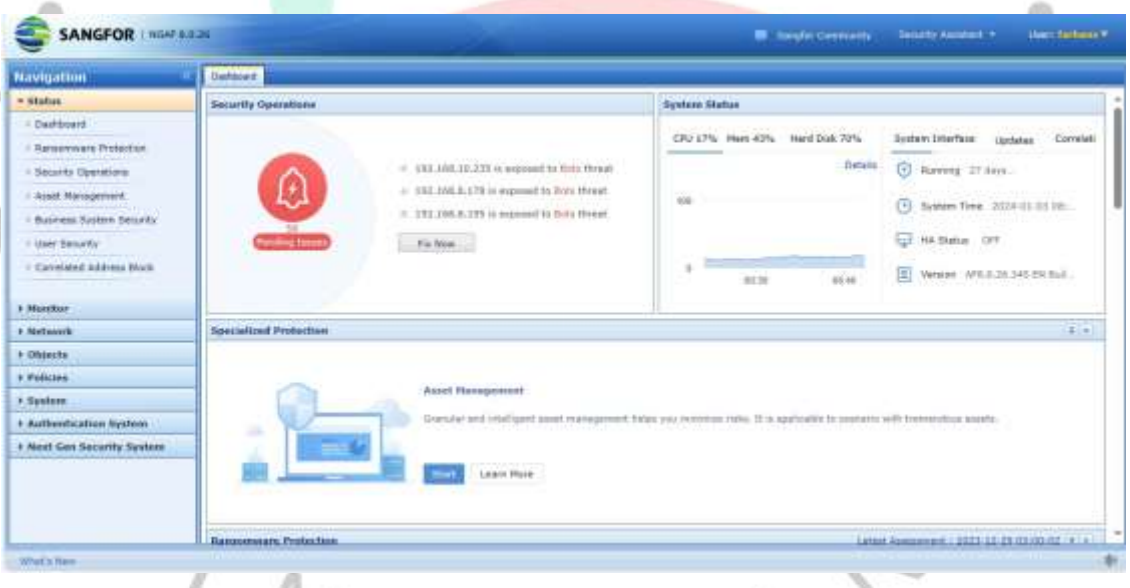
Administrator dapat dengan mudah mendefinisikan kebijakan keamanan berdasarkan perilaku pengguna, geografis, waktu request dan faktor lainnya. API terbuka juga disediakan

untuk memudahkan integrasi dan otomatisasi bersama solusi keamanan yang telah ada. Antarmuka dan dashboard sangfor NGAF dirancang intuitif agar pengelolaan proteksi web app dapat lebih sederhana. Dengan berbagai kemampuan canggih tersebut, organisasi kini dapat mengamankan aplikasi web seperti website institusi, e-commerce, portal pelanggan dan lainnya dari evolusi ancaman siber. Melalui sangfor NGAF, ketahanan sistem informasi dan reputasi brand perusahaan lebih terjaga di tengah trend serangan siber yang makin hari makin kompleks. Inovasi AI dan machine learning dari Sangfor NGAF membuat perlindungan aplikasi web lebih cerdas dan adaptif; sejalan dengan tuntutan transformasi digital saat ini.

Sangfor NGAF memiliki fitur-fitur firewall yang komprehensif meliputi:

- Status

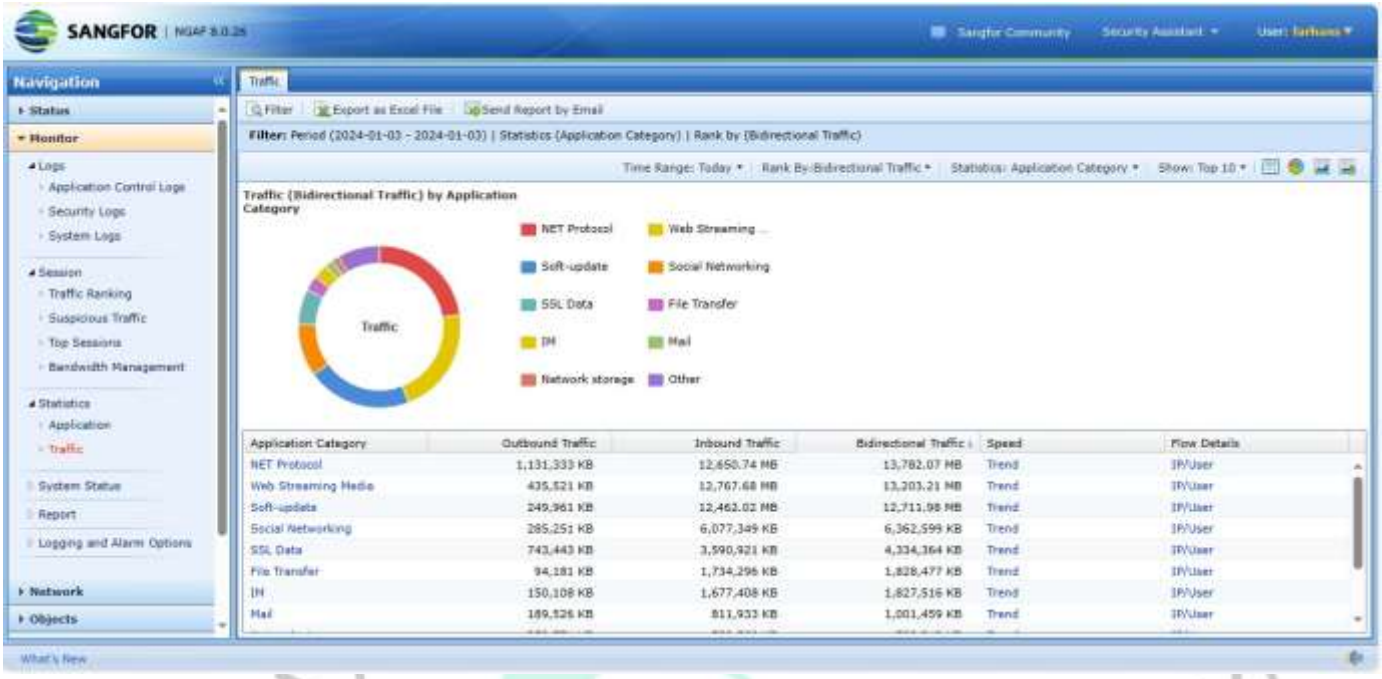
Status menyediakan gambaran keseluruhan mengenai status atau situasi terkini keamanan jaringan firewall. Status dipecah menjadi 7 bagian, bagian-bagian tersebut yaitu Dashboard, Ransomware Protection, Security Operations, Asset Mangement, Business System Security, User Security, Corralated Addres Block



4.1.1.1 Gambar Fitur Status di bagian Dashboard

- Monitor

Monitor berfungsi untuk memberikan visibilitas dan analisis mendalam terhadap lalu lintas jaringan dan aktivitas keamanan di lingkungan perusahaan. Fitur ini memungkinkan administrator untuk memantau, menganalisis, dan mengelola lalu lintas data secara real-time, memberikan pemahaman yang mendalam tentang keamanan jaringan, serta membantu dalam mendeteksi dan merespons ancaman siber dengan lebih cepat. Monitor dipecah menjadi 6 bagian, bagian-bagian tersebut yaitu Logs, Session, Statistics, System Status, Report, Logging and Alarm Options



4.1.1.1 Gambar Fitur Monitor di bagian Traffic

4.1.1.2 Perlindungan dari sisi End user (Bitdefender)

Bitdefender GravityZone Business Security adalah solusi keamanan terkemuka yang dirancang khusus untuk memenuhi kebutuhan perlindungan keamanan informasi di lingkungan bisnis. Dikembangkan oleh Bitdefender, perusahaan yang diakui secara global dalam industri keamanan cyber, GravityZone Business Security menyediakan berbagai fitur dan layanan yang terintegrasi untuk melindungi jaringan, perangkat, dan data dari ancaman siber yang beragam.

Solusi ini menawarkan keseluruhan fitur keamanan yang meliputi proteksi terhadap malware, ransomware, virus, phishing, dan ancaman siber lainnya. Dengan pendekatan yang proaktif, GravityZone Business Security menggunakan teknologi canggih seperti deteksi perilaku, kecerdasan buatan, dan analisis heuristik untuk mengidentifikasi dan menghentikan ancaman sebelum mereka dapat menyebabkan kerusakan pada sistem. Salah satu keunggulan utama dari GravityZone Business Security adalah kegunaan dan manajemen yang mudah. Platformnya dirancang untuk dapat dikelola dengan mudah bahkan oleh pengguna yang tidak memiliki pengalaman teknis yang mendalam. Antarmuka pengguna yang intuitif memungkinkan administrator untuk mengatur dan mengelola keamanan jaringan dari satu titik kontrol, menyediakan visibilitas menyeluruh terhadap status keamanan, serta kemampuan untuk

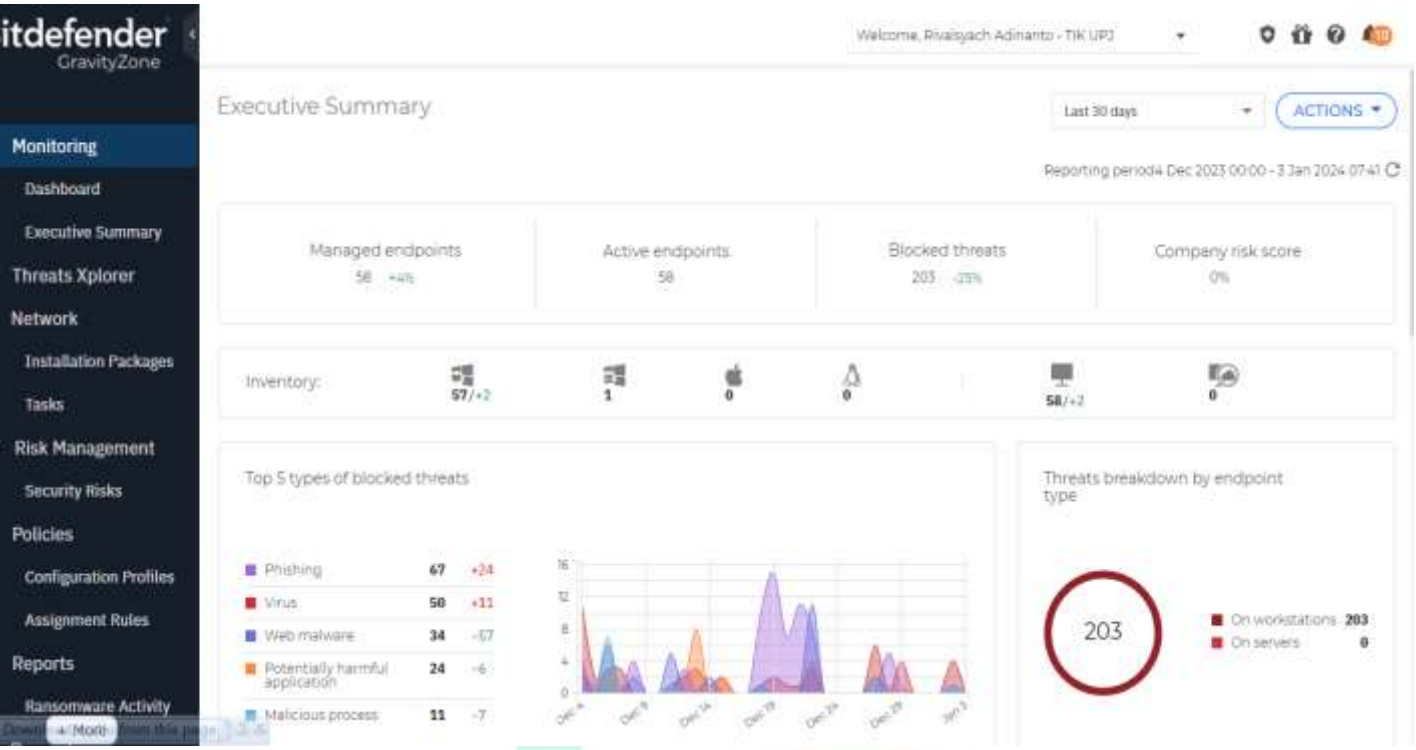
memberikan kebijakan keamanan yang disesuaikan dengan kebutuhan perusahaan.

Selain itu, solusi ini juga menawarkan kemampuan manajemen perangkat yang komprehensif. Ini termasuk pengelolaan perangkat mobile dan endpoint, memungkinkan administrator untuk melindungi semua perangkat yang terhubung ke jaringan perusahaan, termasuk PC, laptop, server, dan perangkat mobile seperti smartphone dan tablet. Dengan fitur-fitur ini, GravityZone Business Security membantu perusahaan dalam meminimalkan risiko keamanan dari berbagai jenis perangkat yang digunakan oleh karyawan. Fitur lain yang penting dari GravityZone Business Security adalah kemampuannya untuk memberikan perlindungan terhadap serangan yang terus berkembang, seperti serangan phishing yang semakin canggih dan serangan ransomware yang menargetkan data sensitif perusahaan. Solusi ini menggabungkan teknologi canggih untuk mendeteksi dan menghentikan serangan ini sebelum mereka mencapai titik yang dapat merugikan perusahaan. Dalam konteks kepatuhan peraturan dan privasi data yang semakin ketat, GravityZone Business Security juga memberikan fokus pada kepatuhan dan ketaatan regulasi. Solusi ini membantu perusahaan untuk memenuhi persyaratan keamanan data dan privasi, mengurangi risiko pelanggaran peraturan, serta melindungi informasi sensitif dan penting dari akses yang tidak sah. Bitdefender GravityZone Business Security juga menonjol dalam hal kinerja dan efisiensi. Solusi ini menggunakan pendekatan yang ringan terhadap sumber daya sistem, memastikan perlindungan yang kuat tanpa mengorbankan kinerja perangkat atau jaringan. Dengan demikian, perusahaan dapat menikmati perlindungan yang canggih tanpa mempengaruhi produktivitas dan kinerja operasional.

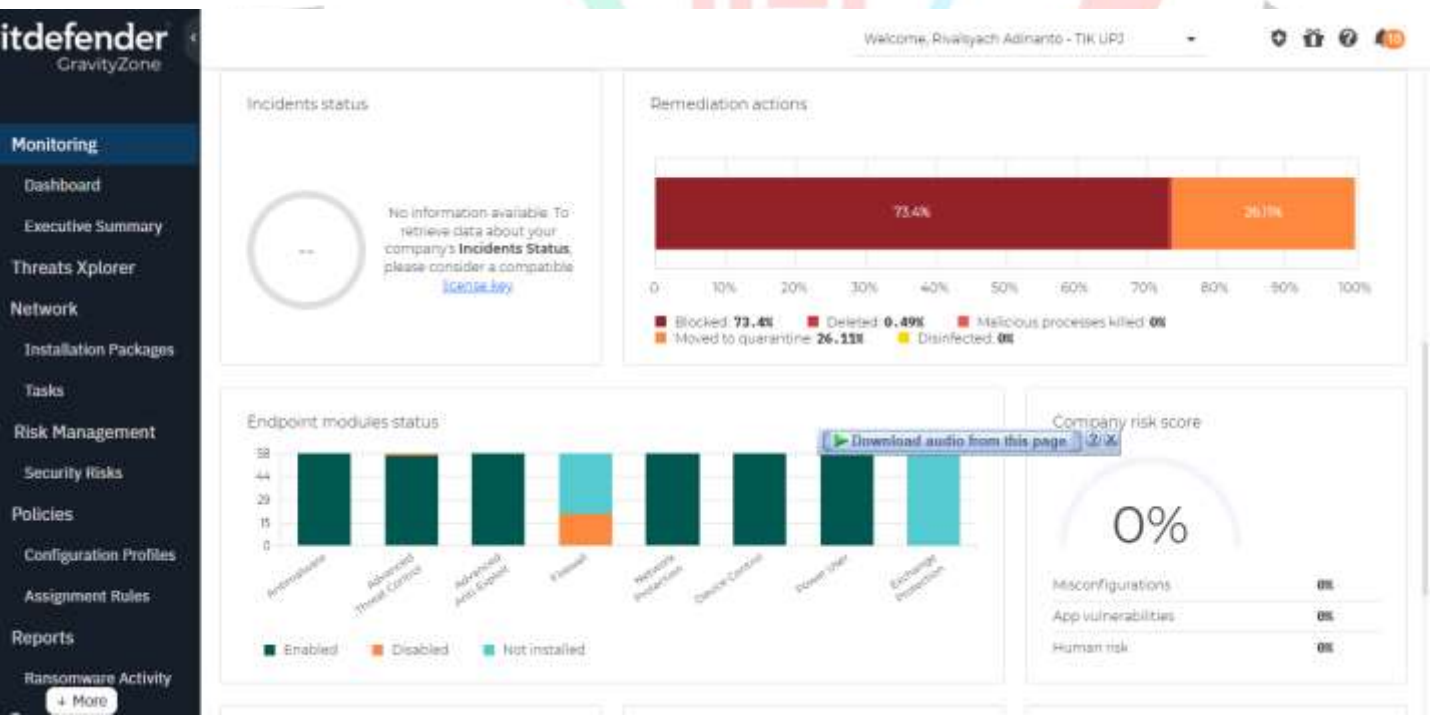
Pada Bitdefender GravityZone Business Security terdapat fitur-fitur yang lengkap meliputi:

- Monitoring

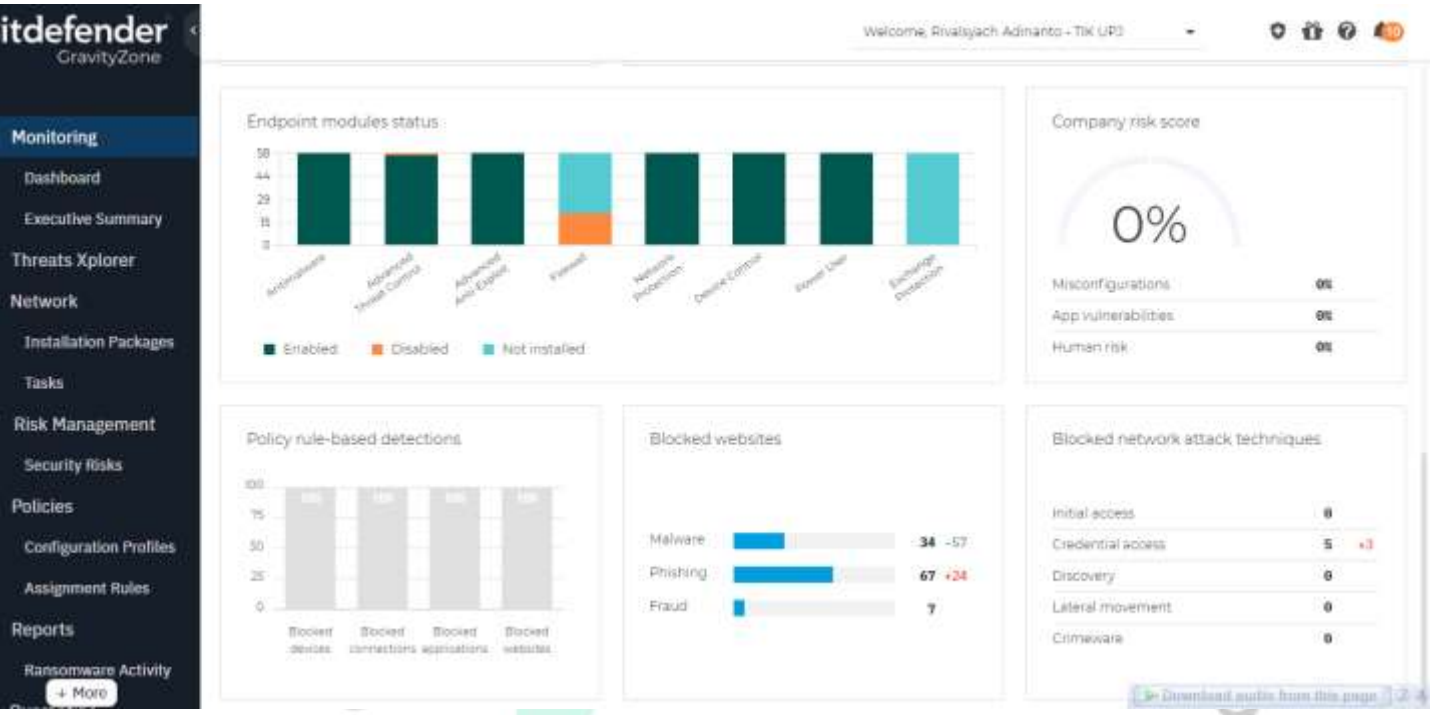
Monitoring menyediakan Executive Summary yang merangkum seluruh aspek perlindungan Bitdefender mulai dari Blocked threats lalu Manged endpoints selanjutnya Active endpoints kemudian Company risk score. Kemudian ada Top 5 types of blocked threats, Threats breakdown by endpoint type, Incidents status, Remediation actions, Endpoint modules status, Policy rule-based detections, Blocked websites, Blocked network attack techniques.



4.1.1.2 Gambar Fitur Monitoring 1



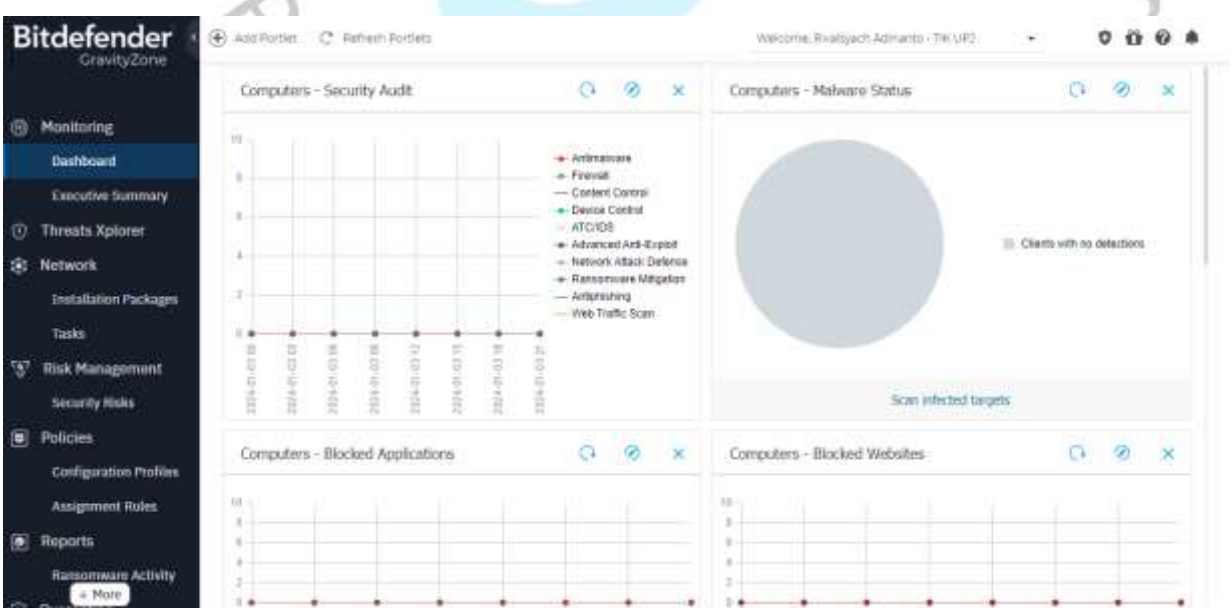
4.1.1.2 Gambar Fitur Monitoring 2



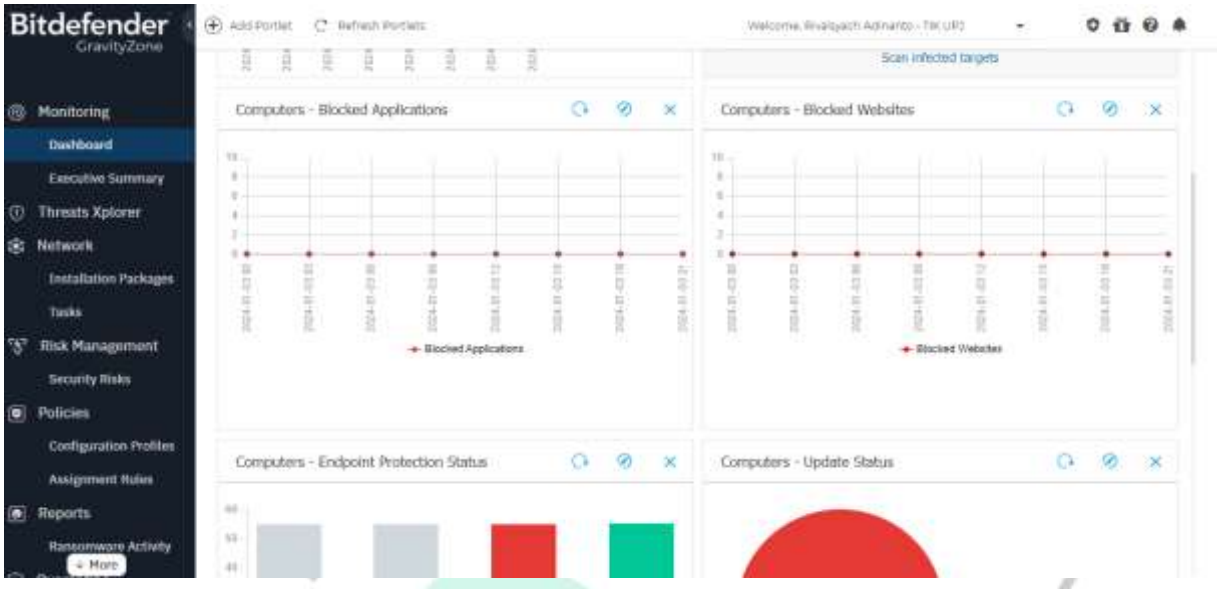
4.1.1.2 Gambar Fitur Monitoring 3

- Dashboard

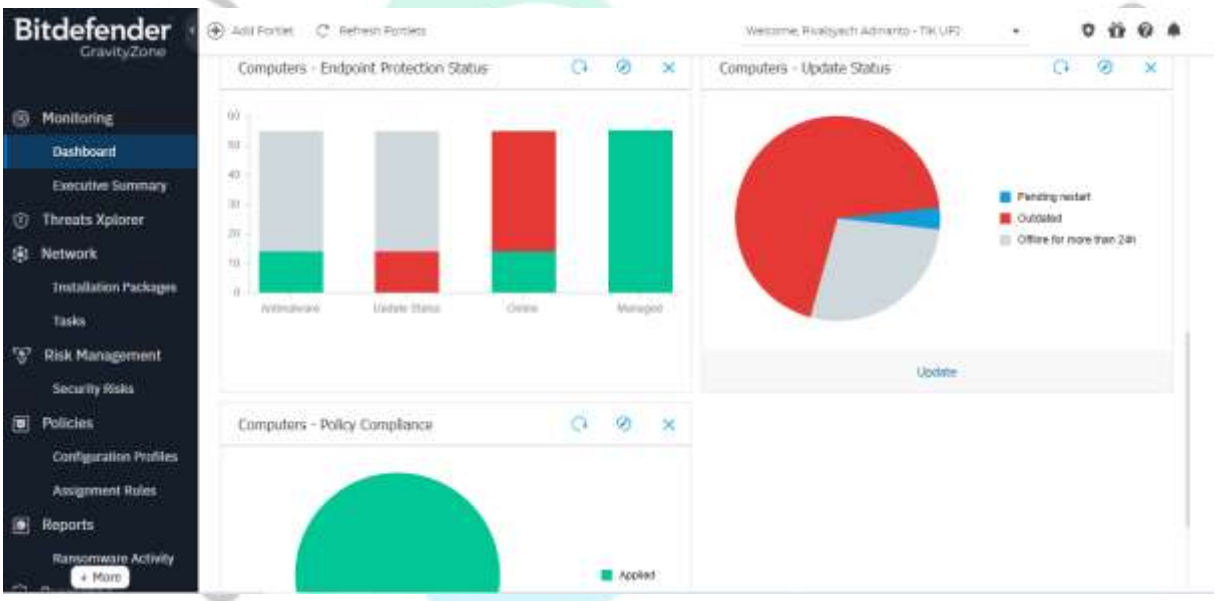
Dashboard menyediakan Grafik-grafik seluruh aspek perlindungan Bitdefender mulai dari Computers – Security Audit, Computers – Malware Status, Computers – Blocked Application, Computers – Blocked Websites, Computers – Endpoint Protection Status, Computers – Update Status, Computers – Policy Compliance



4.1.1.2 Gambar Fitur Dashboard 1



4.1.1.2 Gambar Fitur Dashboard 2



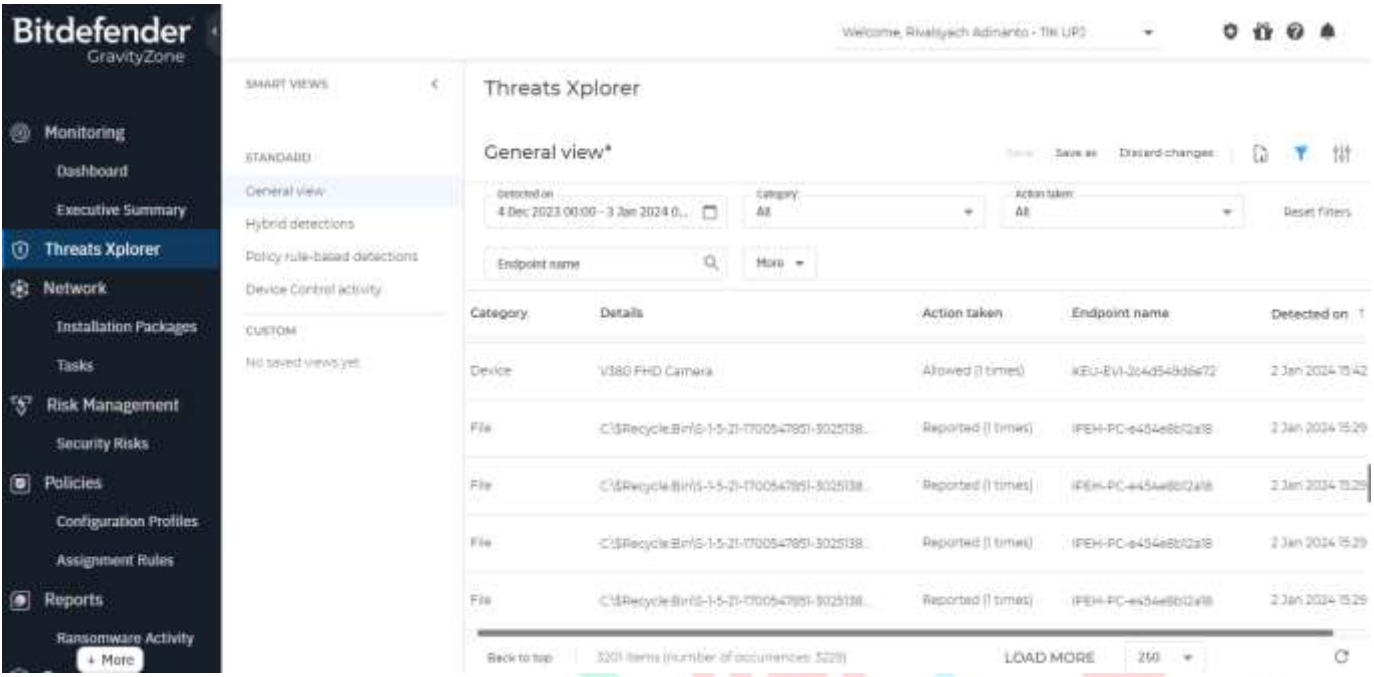
4.1.1.2 Gambar Fitur Dashboard 3

- Executive Summary

Executive Summary memiliki tampilan dan menu yang sama dengan Monitoring yang merangkum seluruh aspek perlindungan Bitdefender mulai dari Manged endpoints, Active endpoints, Blocked threats, Company risk score. Kemudian ada Top 5 types of blocked threats, Threats breakdown by endpoint type, Incidents status, Remediation actions, Endpoint modules status, Policy rule-based detections, Blocked websites, Blocked network attack techniques.

- Threats Xplorer

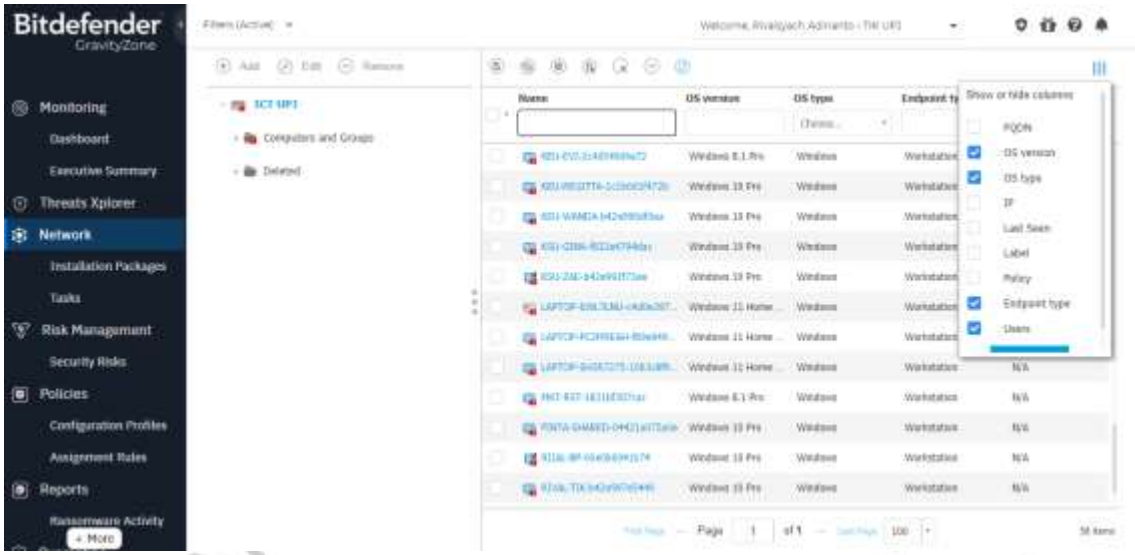
Threats Xplorer adalah fitur yang berguna untuk menampilkan hasil deteksi dan identifikasi dari setiap perlindungan yang dilakukan. Terdapat 9 kategori perlindungan yang dilakukan mulai dari perlindungan file, process, website, email, application, connection, Perangkat. Threats Xplorer juga menampilkan hasil dari tindakan yang diambil untuk melakukan perlindungan menyeluruh terhadap 9 kategori perlindungan.



4.1.1.2 Gambar Fitur Threats Xplorer

- Network

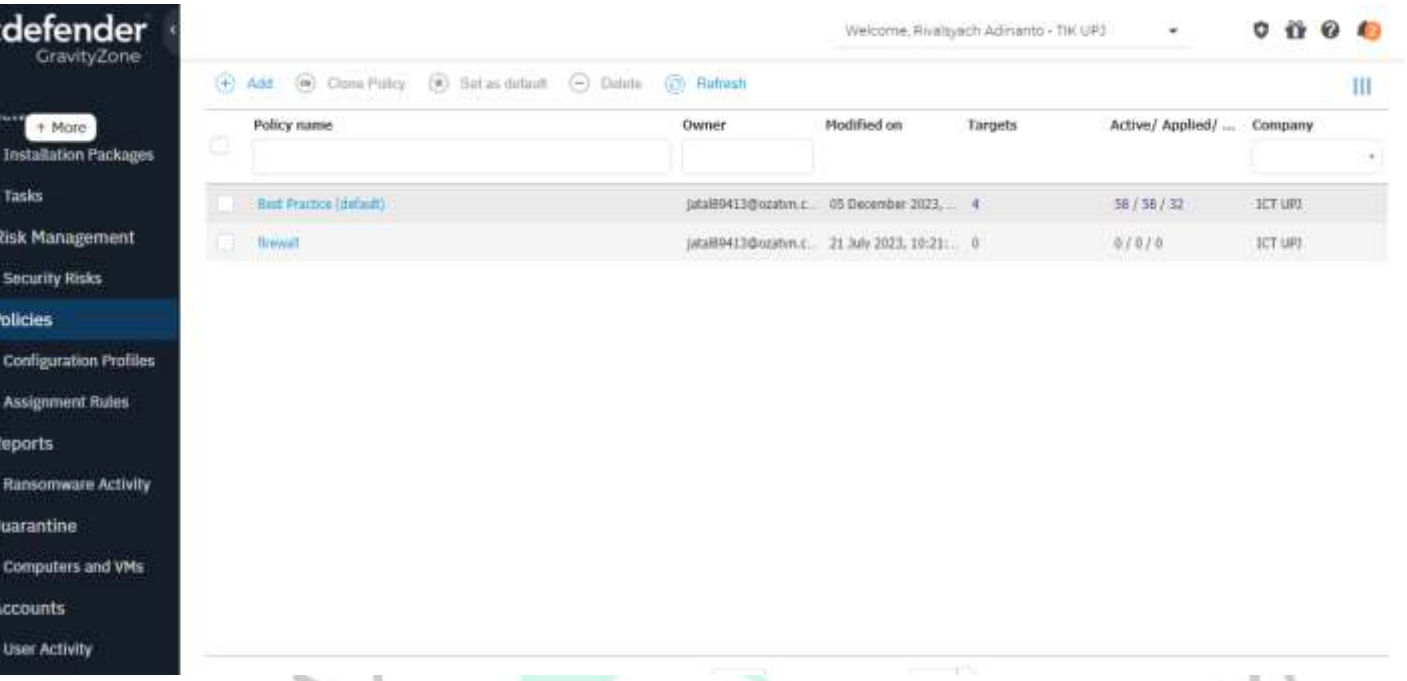
Fitur network adalah fitur yang berguna untuk menampilkan dan melakukan konfigurasi dari perangkat-perangkat komputer di Institusi XYZ yang telah di install Bitdefender. Pada fitur network dapat difilter informasi apa saja yang ingin ditampilkan mulai dari FQDN, OS Version, OS type, IP, Last Seen, Label, Policy, Endpoint type, Users



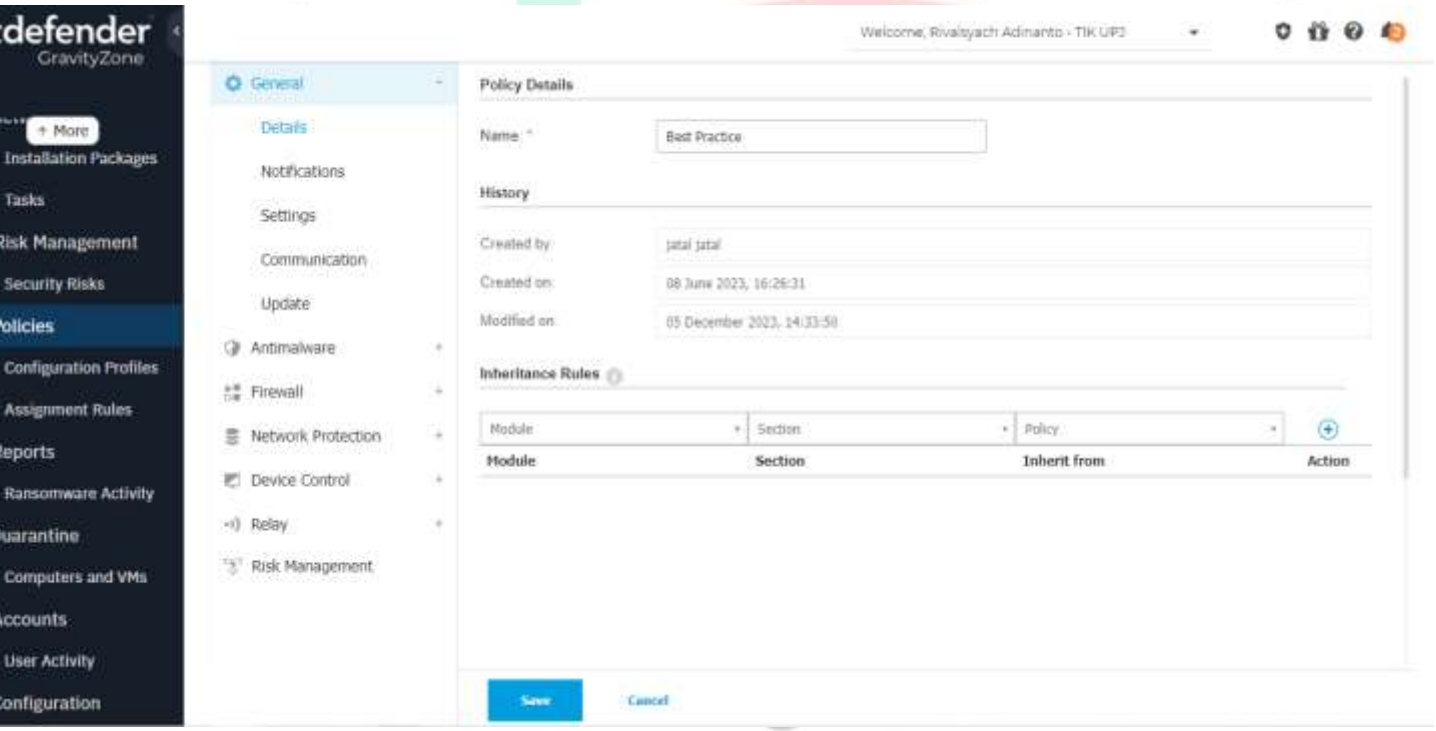
4.1.1.2 Gambar Fitur Network

- Policies

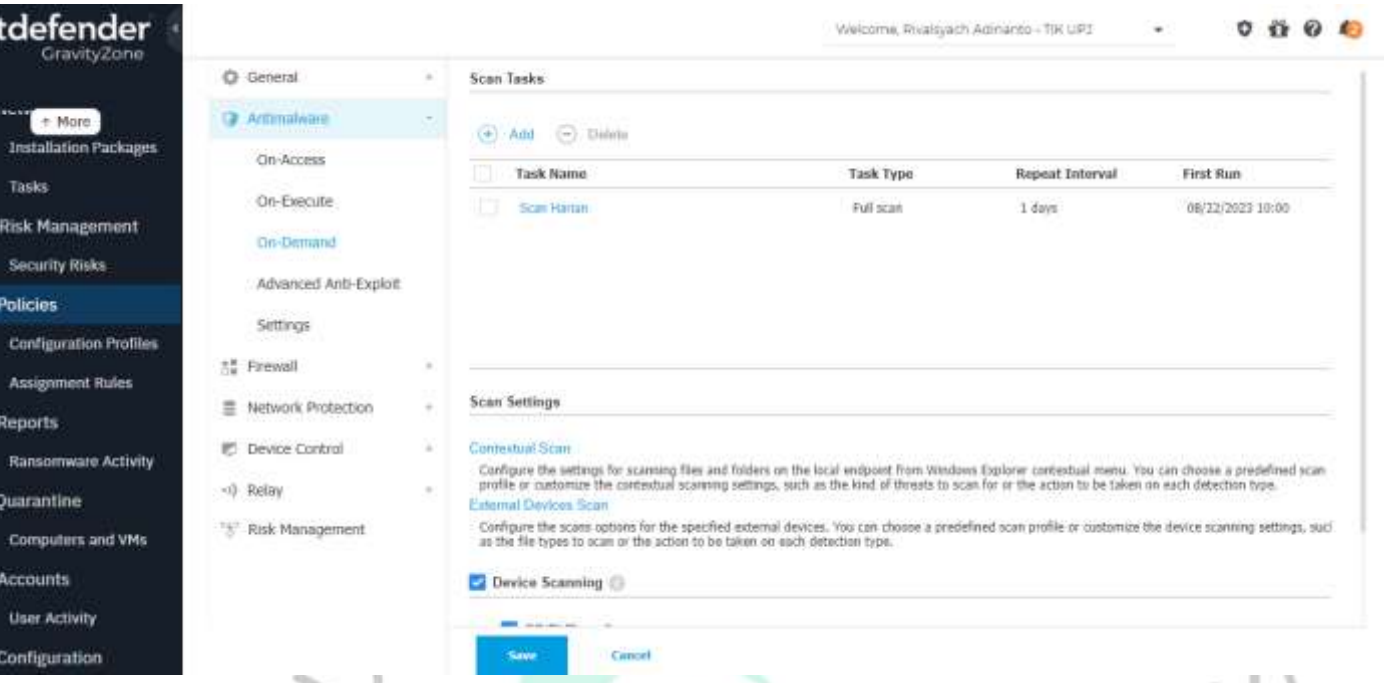
Fitur Policies adalah serangkaian pengaturan dan aturan keamanan yang dapat disesuaikan oleh administrator untuk mengelola dan mengendalikan perlindungan keamanan dalam lingkungan bisnis. Fitur ini memberikan kontrol yang detail terhadap pengaturan keamanan yang diterapkan pada jaringan, perangkat, dan pengguna di seluruh infrastruktur IT perusahaan. Policies ini memungkinkan administrator untuk mengatur berbagai aspek keamanan, mulai dari perlindungan terhadap malware dan ransomware hingga manajemen perangkat serta akses pengguna. Administrator dapat menyesuaikan kebijakan keamanan dengan kebutuhan spesifik perusahaan, termasuk menetapkan aturan untuk pemindaian malware, mengatur cara penanganan file yang mencurigakan, mengelola hak akses perangkat, dan mengatur kebijakan akses pengguna ke aplikasi dan data sensitif.



4.1.1.1 Gambar Fitur Policies 1



4.1.1.1 Gambar Fitur Policies 2



4.1.1.1 Gambar Fitur Policies 3

4.1.1.3 Perlindungan dari sisi Email (Microsoft EOP)

Microsoft Exchange Online Protection atau yang biasa disingkat EOP adalah layanan keamanan email berbasis cloud yang disediakan oleh Microsoft. Layanan ini memberikan perlindungan terhadap ancaman email berbahaya bagi organisasi dan pengguna melalui fitur-fitur filtering email lanjutan. EOP dapat digunakan oleh pelanggan Office 365 untuk melindungi alamat email mereka dari spam, phishing, dan malware. Namun demikian, layanan ini juga dapat digunakan oleh pelanggan yang tidak memiliki langganan Office 365. EOP bekerja dengan cara menyaring semua email masuk ke akun email organisasi sebelum emails tersebut tiba di kotak masuk pengguna. Filtering dilakukan berdasarkan daftar putih dan hitam, serta teknologi machine learning untuk mendeteksi ancaman berbahaya seperti spam, phishing, dan malware. Email yang diidentifikasi berbahaya akan ditolak dan dikuarantina sebelum tiba ke kotak masuk pengguna. Hal ini membantu menjaga keamanan akun email serta perlindungan pengguna dari ancaman berbahaya.

Untuk mendeteksi ancaman, EOP menganalisis konten, tampilan, dan perilaku email masuk. Teknologi machine learning yang dimiliki EOP sangat cerdas untuk mengenali pola baru ancaman berdasarkan email masuk yang pernah disaring sebelumnya. Selain itu, EOP juga bekerja sama dengan jejaring global Microsoft untuk berbagi informasi tentang ancaman terbaru di seluruh dunia. Dengan demikian, EOP dapat mendeteksi ancaman terbaru yang belum pernah dilihat sebelumnya.

Fitur lain yang dimiliki EOP antara lain adalah deteksi spam berdasarkan daftar putih

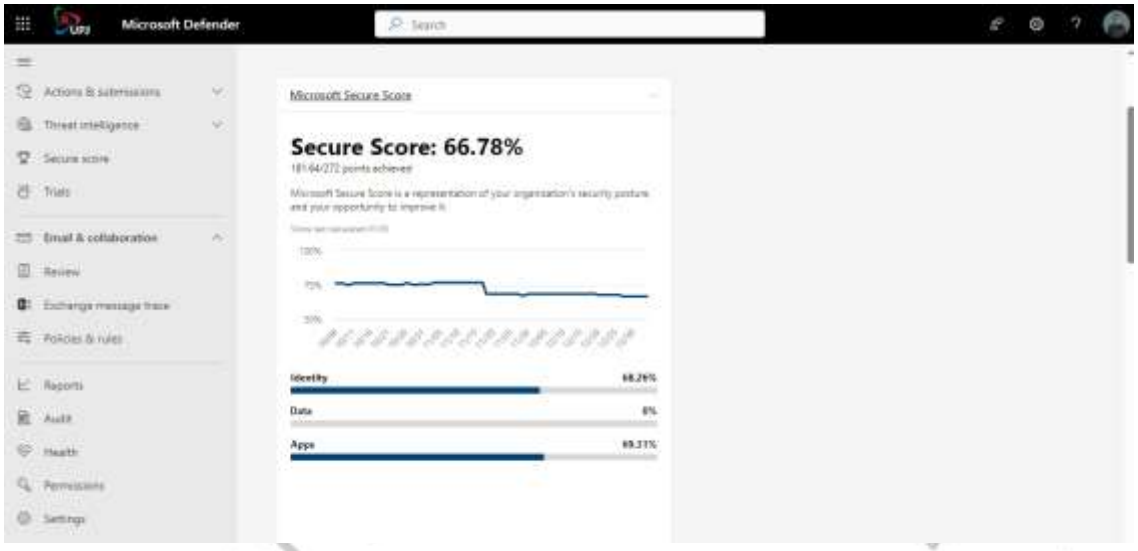
dan hitam, sandboxing untuk menganalisis perilaku email mencurigakan, deteksi phishing canggih, antivirus/antispyware, filtering berbasis lokasi dan jam, pengiriman ulang email yang ditolak, pelaporan insiden keamanan, dan integrasi dengan layanan keamanan Microsoft lainnya seperti Windows Defender ATP. EOP juga memiliki antarmuka pengguna yang mudah digunakan untuk memfasilitasi pengelolaan keamanan email secara real-time.

Dengan berbagai fitur yang dimiliki, EOP sangat membantu organisasi dalam menjaga keamanan infrastruktur email. Ancaman seperti spam, phishing, ataupun malware dapat terdeteksi dan ditolak sebelum merugikan organisasi dan pengguna. E-mail yang valid dan aman tetap dapat tiba dengan lancar di kotak masuk pengguna. Selain itu, EOP juga memberikan laporan rinci tentang ancaman yang terdeteksi untuk keperluan penanganan insiden keamanan di masa datang. Dengan demikian, EOP menjadi solusi keamanan email yang handal, aman, dan mudah dikelola untuk menjaga akun email organisasi.

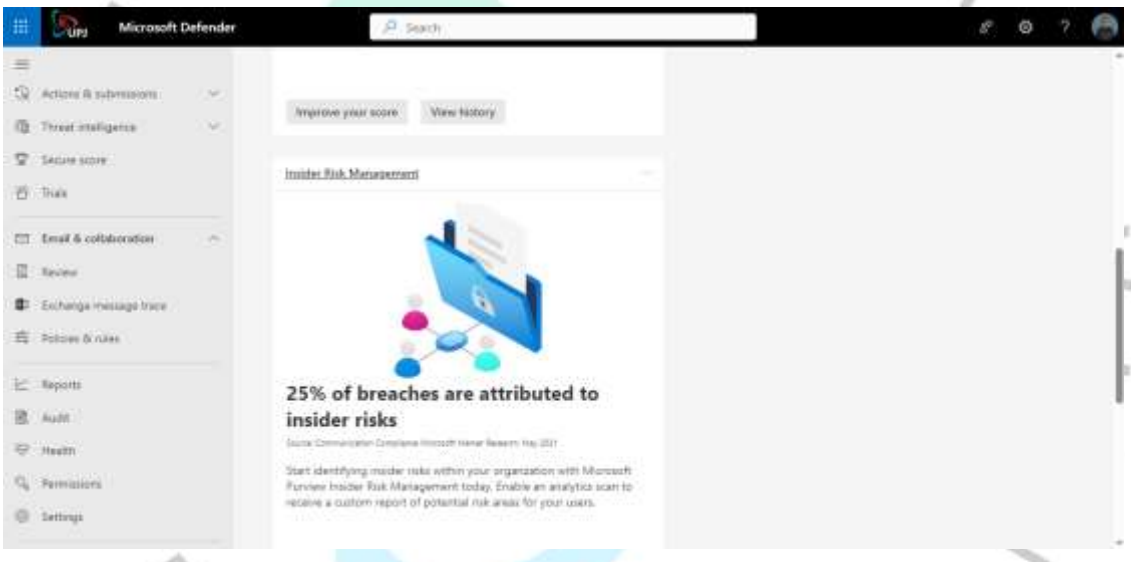
Didalam EOP terdapat fitur-fitur yang mumpuni terdiri dari:

・Home

Home berfungsi untuk menyediakan informasi terkait Microsoft Secure Score yang mana merupakan alat penilaian keamanan siber yang dikembangkan oleh Microsoft untuk membantu organisasi mengukur dan meningkatkan postur keamanan pengguna mereka. Secure Score memberikan skor numerik berdasarkan konfigurasi keamanan berbagai layanan dan produk Microsoft yang digunakan organisasi, seperti Azure, Office 365, dan Windows. Semakin tinggi skornya, semakin baik tingkat keamanan siber organisasi tersebut, dan Insider Risk Mangement yaitu solusi keamanan siber yang dirancang untuk membantu organisasi mendeteksi, menyelidiki, dan merespon ancaman internal yang berasal dari orang dalam organisasi, seperti karyawan, kontraktor, atau pihak ketiga lainnya yang memiliki akses ke informasi sensitif atau sistem kritis. Microsoft EOP IRM menggunakan berbagai teknologi keamanan, termasuk deteksi anomali, analisis perilaku pengguna, dan pembelajaran mesin, untuk mengidentifikasi aktivitas yang tidak biasa atau mencurigakan yang dapat mengindikasikan adanya ancaman serangan siber.



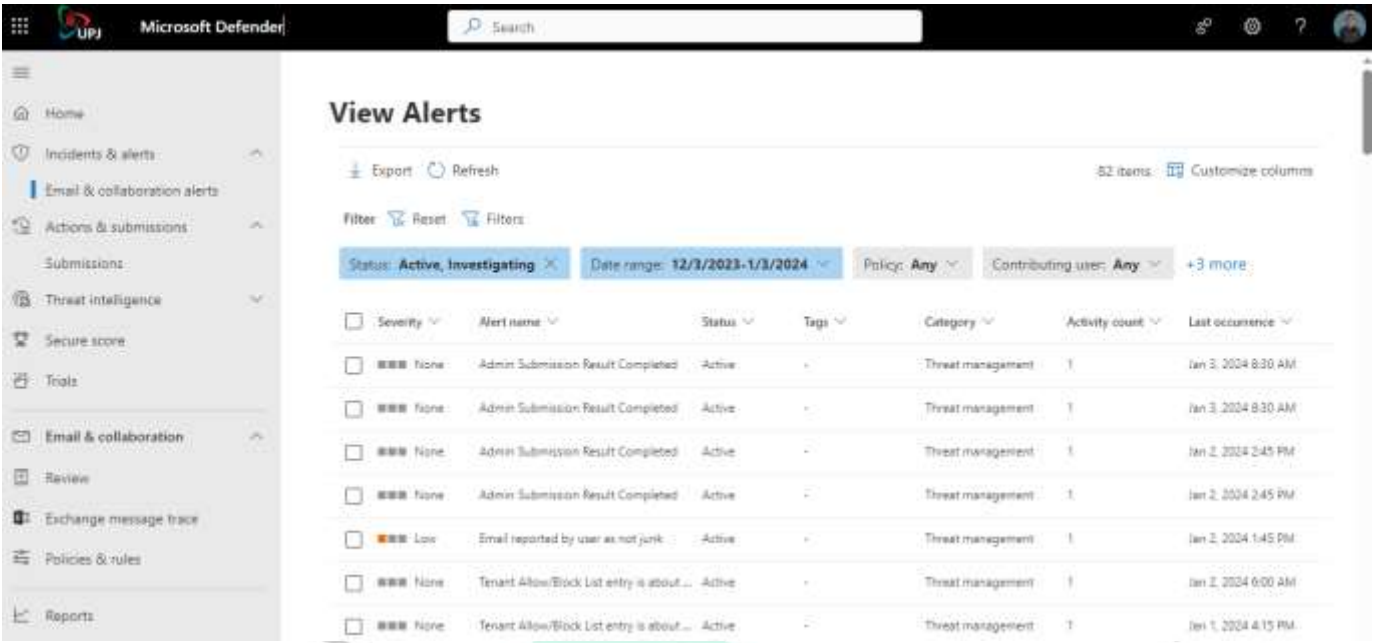
4.1.1.3 Gambar Fitur Home 1



4.1.1.3 Gambar Fitur Home 2

- Incidents & alerts

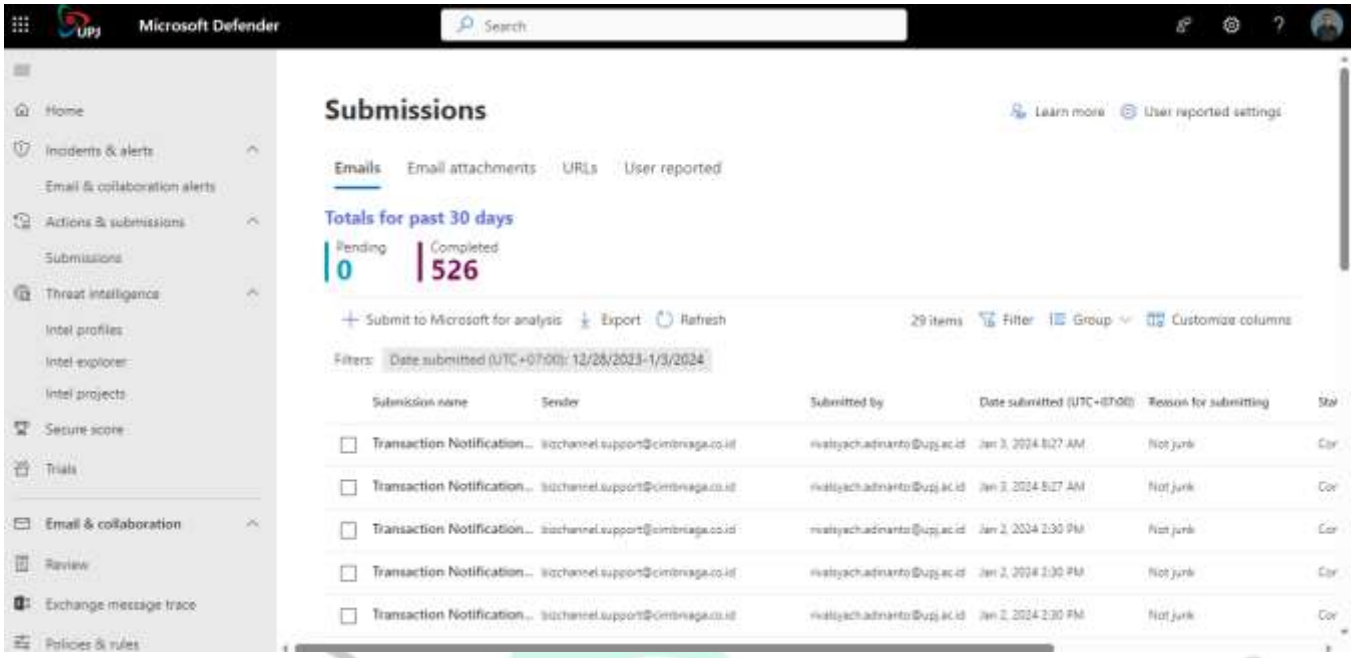
Incidents & alerts berfungsi untuk fitur yang melihat dan mengelola insiden keamanan dan peringatan di lingkungan Microsoft 365 pengguna. Insiden adalah peristiwa yang dapat mengindikasikan adanya pelanggaran keamanan, seperti serangan siber atau akses tidak sah ke data. Peringatan adalah pemberitahuan tentang aktivitas yang mencurigakan atau berpotensi berbahaya.



4.1.1.3 Gambar Fitur Incident & alerts

- Actions & submissions

Incidents & alerts memungkinkan pengguna untuk mengambil tindakan terhadap email yang dianggap mencurigakan atau berpotensi berbahaya. Pengguna dapat mengirim email ke Microsoft untuk ditinjau lebih lanjut atau melaporkan email yang mencurigakan sebagai serangan phishing atau spam. Fitur ini juga memungkinkan pengguna untuk mengirim email yang salah terdeteksi sebagai spam atau false positive untuk ditinjau ulang. Dengan adanya Actions & submissions, pengguna dapat berpartisipasi dalam memperbaiki keamanan email dan meningkatkan daya tanggap sistem keamanan Microsoft Exchange Online Protection.



4.1.1.3 Gambar Fitur Action & submissions

· Secure Score

Microsoft Secure Score adalah pengukuran postur keamanan organisasi, dengan angka yang lebih tinggi menunjukkan lebih banyak tindakan yang direkomendasikan untuk diambil. Itu dapat ditemukan di Microsoft Secure Score di portal Microsoft Defender. Mengikuti rekomendasi Secure Score dapat melindungi organisasi Anda dari ancaman. Dari dasbor terpusat di portal Microsoft Defender, organisasi dapat memantau dan menangani keamanan identitas, aplikasi, dan perangkat Microsoft 365 mereka.

Secure Score membantu organisasi:

- Laporkan keadaan postur keamanan organisasi saat ini.
- Meningkatkan postur keamanan mereka dengan memberikan kemampuan untuk ditemukan, visibilitas, panduan, dan kontrol.
- Bandingkan dengan tolok ukur dan tetapkan indikator kinerja utama (KPI).

4.1.1.3 Gambar Fitur Secure Score

4.1.2 Hasil Temuan

4.1.2.1 Hasil temuan dari sisi Firewall Internet (Sangfor NGAF)

Meningkatkan dan mempertahankan kualitas layanan dan Pendidikan di kampus, maka infrastruktur IT memerlukan teknologi security yang dapat memproteksi layanan agar dapat terus beroperasi dengan baik. Tetapi topologi existing membuat solusi keamanan membengkak karena banyaknya area server dan user yang harus diproteksi.

Selain itu, meningkatnya jumlah mahasiswa juga menimbulkan tantangan baru berupa meningkatnya akses illegal menggunakan fasilitas jaringan kampus, sehingga dibutuhkan juga perangkat teknologi yang memungkinkan untuk menyaring trafik berbahaya (malicious) agar IP publik kamus menjadi aman dari indikasi penyalahgunaan sehingga tidak sampai masuk ke dalam blacklist internet. Dari beberapa latar belakang tersebut, Sangfor Next Generation Application Firewall (Sangfor NGAF) bisa menjadi Solusi untuk melindungi seluruh aplikasi dan service institusi secara keseluruhan.

- SANGFOR Network Security (sebelumnya dikenal dengan NGAF) adalah NGFW + WAF di dalam 1 box. (masuk ke dalam Gartner MQ untuk enterprise firewall. WAF sudah dinilai oleh NSS Labs untuk rating

tertinggi ” Recommended”).

- SANGFOR NGAF memberikan modul exclusive untuk “risk-assessment”.
- SANGFOR NGAF memberikan “best-of-breed” service-level report security.

4.1.2.2 Hasil temuan dari dari sisi End user (Bitdefender)

Seluruh Perangkat milik end user yang sudah terinstall Bitdefender telah disetting Policies nya untuk melakukan Full Scan setiap hari nya di jam 10 pagi. Dari hasil Full Scan yang dilakukan setiap hari nya akan teridentifikasi apakah Perangkat tersebut aman atau ada malware nya. Jika Perangkat terjangkit malware maka oleh Bitdefender akan dimasukkan ke dalam Quarantine sehinnga malware tersebut tidak bisa melakukan serangan siber.

4.1.2.3 Hasil temuan dari dari sisi Email (Microsoft EOP)

Setiap mailflow email yang terjadi baik dari internal maupun eksternal akan di filter oleh EOP, jika sebuah email terdapat indikasi mencurigakan EOP akan melakukan identifikasi jenis email tersebut apakah email tersebut adalah spam atau phising atau malware. Kemudian jika memang email tersebut benar sebuah email yang mencurigakan maka oleh EOP akan

dimasukkan kedalam Quarantine sehingga email tersebut tidak terkirim ke email tujuan. Didalam Quarantine jenis-jenis email serangan yang dapat teridentifikasi ada transport rule, bulk, spam, data loss prevention, malware, admin action – File type block, phising, high confidence phising.

4.2 Identifikasi Dengan Metode NIST

Terdapat 5 buah fungsi dalam NIST dengan masing-masing fungsi tersebut memiliki kategori-kategori pada tiap fungsi NIST. Fungsi pada NIST merupakan Kegiatan keamanan siber pada tingkat tertinggi melibatkan fungsi-fungsi kunci, yaitu Identifikasi, Perlindungan, Deteksi, Respons, dan Pemulihan. Fungsi-fungsi ini membantu organisasi mengelola risiko keamanan siber dengan menyusun informasi, memfasilitasi pengambilan keputusan manajemen risiko, menghadapi ancaman, dan melakukan perbaikan melalui pembelajaran dari pengalaman sebelumnya. Sementara dalam kategori NIST, terdapat subdivisi fungsi keamanan siber menjadi kelompok-kelompok hasil yang erat kaitannya dengan kebutuhan program dan aktivitas tertentu.

Framework Core Structure

		Categories	Subcategories	Informative Reference
	Identify	firewall internet	Ransomware Protection	Perlindungan dari Sangfor untuk melindungi Firewall dari ancaman Ransomware. Terdapat fitur yang memberitahukan port-port yang rentan terhadap ransomware dan saran mengatasi nya
			Attack Events	Adalah fitur dari Sangfor untuk mengidentifikasi ip yang menyerang firewall juga deskripsi celah keamanan yang coba diserang. Juga terdapat opsi untuk dilakukan block ip penyerang tersebut sehingga ip tersebut tidak dapat menyerang lagi.

		end user protection	Installation Packages	Bertujuan untuk Perangkat end user terinstall Bitdefender agar aman terlindungi dari serangan malware
		email protection	Incident and alerts	Berfungsi untuk memperingati saat terjadi sebuah insiden
	Protect	**Categories**	**Subcategories**	**Informative Reference**
		firewall internet	Sangfor Policies	Konfigurasi perlindungan untuk memproteksi firewall
		end user protection	Bitdefender Policies	Konfigurasi perlindungan untuk memproteksi Perangkat
		email protection	EOP Policies & rules	Konfigurasi perlindungan untuk memproteksi email

	Detect	**Categories**	**Subcategories**	**Informative Reference**
		firewall internet	Security Operations	Untuk melakukan deteksi terhadap isu-isu yang berlangsung
		end user protection	Quarantine	Hasil deteksi akan dimasukkan ke kuarantina
		email protection	Quarantine	Hasil deteksi akan dimasukkan ke kuarantina
	Respond	**Categories**	**Subcategories**	**Informative Reference**
		firewall internet	Security Policy Template	Untuk penangan terhadap intrusion prevention, web app protection, apt detection, content security
		end user protection	Empty Quarantine	Mengosongkan malware-malware yang ada di karantina
		email protection	Deleted messages	Menghapus email-email yang ada di karantina

			Submit for review	Untuk dianalisa oleh EOP agar perlindungan semakin meningkat
	Recover	**Categories**	**Subcategories**	**Informative Reference**
		firewall internet	Next gen security system	Untuk peningkatan terhadap perlindungan yang telah ada
		end user protection	Risk Management	Mengukur tingkat resiko terhadap serangan siber
		email protection	Secure Score	Melakukan rekomendasi aksi yang disarankan oleh EOP

4.2.1. Fungsi *Identity* (Identifikasi) dan Kategorinya

Fungsi *identity* merupakan salah satu fungsi NIST yang bertugas mengembangkan pemahaman organisasi dalam mengelola resiko keamanan siber. Dalam penerapannya di sisi *Firewall* internet, pihak institusi XYZ sudah menggunakan *SangFor NGAF* untuk melindungi perangkat dari serangan *ransomware* dan serangan IP yang lolos dari pelindung *ransomware*. Di sisi *End user Protection*, pihak institusi menggunakan *Bitdefender* sebagai pelindung dari serangan *malware*. Kemudian di sisi *Email protection*, mereka menggunakan fitur *incident and alerts* milik *exchange online protector* sebagai memberi kabar bahwa ada email *phising* atau spam.

4.2.2. Fungsi *Protect* (Proteksi) dan Kategorinya

Fungsi *Protect* merupakan salah satu fungsi dalam mengupayakan perlindungan yang tepat untuk memastikan penyediaan layanan infrastruktur penting. Dari tiga komponen penting milik institusi, masing-masing memiliki satu komponen

pelindung. Di sisi *firewall* internet, mereka menggunakan *Sangfor policies*, di sisi *end user protection*, mereka menggunakan *bitdefender policies*, dan di sisi email *protection*, mereka menggunakan EOP *policies and rules*.

4.2.3. Fungsi *Detect* (Deteksi) dan Kategorinya

Fungsi *detect* membantu penemuan sebuah peristiwa keamanan siber secara tepat waktu. Dari sisi *firewall* internet, sistem *Sangfor NGAF* melakukan operasi keamanan untuk mengetahui isu-isu yang yang berlangsung. Sedangkan dari sisi *end user protection* dan *email protection*, *Bitdefender* dan EOP menggunakan sistem *quarantine*, dimana jika ada aplikasi atau email yang dianggap sistem mencurigakan, mereka akan dipindahkan ke menu *quarantine*.

4.2.4. Fungsi *Respond* (Menanggapi) dan Kategorinya

Fungsi *respond* mencakup tindakan yang harus dilakukan setelah sistem mendeteksi kejadian keamanan siber tersebut. Di sisi *firewall* internet, memiliki security policy template dalam penanganan *intrusion prevention, web app protection, apt detection, content security*/. Di sisi *end user* protection, mereka menggunakan *empty quarantine*, dimana aplikasi yang dikarantina tersebut akan dihapus, atau diberitahukan bahwa aplikasi tersebut tidak berbahaya. Di sisi *email protection*, EOP memiliki *deleted message*, untuk menghapus email yang dianggap pengguna berbahaya atau *phising* dan *submit for review*, dimana EOP akan menganalisa email tersebut dan dapat dijadikan bahan untuk meningkatkan keamanannya.

4.2.5. Fungsi *Recovery* (Pemulihan) dan Kategorinya

Fungsi *Recovery* merupakan tindakan selanjutnya setelah kegiatan keamanan siber ini sudah selesai. Biasanya fungsi ini berguna untuk meningkatkan kembali sistem yang sudah berjalan tersebut. Dari sisi *firewall* internet, mereka melakukan *next-gen security system* dimana mereka mulai meningkatkan perlindungan yang mereka sudah miliki. Di sisi end user protection, mereka menggunakan *risk management* dimana mereka mulai mengukur tingkat resiko terhadap serangan tersebut. Hal tersebut diarahkan agar pengguna dapat mengembangkan kembali keamanan tersebut. Dan di sisi email protection, mereka menggunakan secure score, dimana mereka akan merekomendasikan kepada pengguna aksi yang harus dilakukan agar meningkatkan keamanan tersebut.

4.3. Strategi Keamanan Siber yang Diusulkan

Dari hasil analisa pada Hasil Studi Lapangan dan Identifikasi Dengan Metode NIST didapatkanlah strategi usulan yang bisa dilakukan guna lebih menguatkan lagi perlindungan keamanan siber di Institusi XYZ.

1. Untuk meningkatkan kesadaran terhadap serangan siber di universitas, diperlukan strategi keamanan siber terintegrasi. Langkah pertama adalah menyertakan pendidikan keamanan siber dalam kurikulum, melibatkan mahasiswa, dosen, dan staf dalam pelatihan rutin. Pusat keamanan siber universitas dapat menyelenggarakan workshop, seminar, dan pelatihan online. Integrasi materi keamanan siber ke dalam mata kuliah umum juga perlu dipertimbangkan. Kampanye informasi proaktif melalui media sosial, email, dan papan pengumuman digital dapat meningkatkan kesadaran. Kerjasama dengan industri keamanan siber dan pemerintah perlu diperkuat melalui forum diskusi atau seminar dengan ahli eksternal untuk mendapatkan wawasan dan dukungan dalam menghadapi serangan siber yang semakin kompleks.
2. Institusi XYZ perlu memiliki komitmen untuk menyusun kebijakan keamanan siber guna melindungi seluruh aset data dan sistem teknologi informasi. Strategi pertama, pembentukan tim khusus yang bertanggung jawab dalam pengembangan dan penegakan kebijakan. Kedua, kebijakan harus berisi acuan hukum, standar minimal pengamanan data, prosedur penanganan insiden keamanan siber, dan sanksi pelanggaran. Ketiga, sosialisasi kebijakan kepada seluruh pemangku kepentingan agar memahami standar keamanan data baru. Keempat, audit dan penegakan secara berkala untuk memantau kepatuhan dan mendorong terbentuknya budaya keamanan data. Dengan strategi tersebut, diharapkan institusi memiliki kebijakan keamanan siber yang matang, sejalan dengan ancaman dunia maya, untuk meminimalkan risiko insiden keamanan data.
3. Terakhir adalah melakuka upaya peningkatan 3 sisi perlindungan yang sudah ada. Sehingga perlindungan terkait keamanan siber akan semakin kuat dan ampuh.

- Meningkatkan lagi pemanfaatan fitur-fitur Sangfor NGAF

  Meningkatkan pemanfaatan fitur-fitur Sangfor NGAF menjadi sangat penting dalam mengoptimalkan keamanan jaringan dan perlindungan data perusahaan.

Agar serangan-serangan terhadap jaringan dapat di proteksi dengan sangat kuat oleh Firewall Sangfor.

- Meningkatkan jumlah Perangkat yang di install Bitdefender GravityZone Business Security

  Perangkat yang sudah di install Bitdefender sudah terlindungi dengan sangat baik dari ancaman-ancaman siber, hal ini dikarenakan update rutin yang dilakukan oleh Bitdefender selain itu juga oleh tim IT Instsitusi XYZ telah dilakukan setting agar setiap hari nya dilakukan full scan. Sehingga untuk kedepannya perlu di perluas cakupan perangkat-perangkat yang di install nya karena saat ini baru hanya ada 58 perangkat yang di install Bitdefender.

- Memaksimalkan Secure Score EOP

  Secure Score pada EOP adalah pengukuran postur keamanan organisasi, melalui angka tinggi menggambarkan lebih banyak tindakan yang direkomendasikan untuk diambil. Itu dapat ditemukan di Microsoft Secure Score di portal Microsoft Defender. Mengikuti rekomendasi Secure Score dapat melindungi organisasi Anda dari ancaman. Oleh karena itu Secure Score yang saat ini berada di kisaran 66% perlu untuk maksimalkan dengan melakukan rekomendasi aksi yang disarankan sehingga identifikasi, proteksi, deteksi, respon, pemulihan di EOP akan lebih kuat dan ampuh untuk melindungi dari ancaman serangan siber.