BAB III
METODE PENELITIAN

3.1 Objek Penelitian

Objek pada penelitian ini merupakan sebuah sistem keamanan sudah diterapkan di Institusi XYZ. Secara langsung, sistem tersebut sudah berjalan sesuai dengan keinginan Institusi, namun secara keamanan, institusi tersebut masih belum terlihat apakah sistem yang sudah biasa digunakan aman atau tidak. Untuk mengetahui apakah keamanan dari sistem yang dibuat sudah mencapai tahap seperti apa. Hal ini dapat membantu institusi tersebut mengembangkan keamanan dari sistem tersebut.

3.1.1. Metode Penelitian

Metode penelitian yang diterapkan dalam penelitian ini yaitu metode dengan menggunakan Framework NIST 1.1. Framework NIST 1.1 merupakan kerangka kerja manajemen risiko yang berkarakter suatu kerangka kerja yang bersifat sukarela, mencakup standar, pedoman, dan praktik terbaik yang digunakan dalam pengelolaan risiko yang berkaitan dengan keamanan siber. Framework ini dikembangkan oleh National Institute of Standards and Technology (NIST)., sebuah lembaga Departemen Perdagangan AS. Framework ini dirilis di tanggal 16 April 2018. Dikembangkan untuk industri yang penting bagi keamanan nasional dan ekonomi, serta energi, perbankan, komunikasi, dan basis industri pertahanan. Semenjak awal mula dikembangkan, framework NIST 1.1 sudah lebih dari cukup secara fleksibelitas untuk diadopsi secara sukarela oleh perusahaan dan organisasi besar dan kecil di semua sektor industri, juga oleh pemerintah federal, negara bagian, dan lokal.

Framework NIST 1.1 meliputi pembaruan mengenai autentikasi dan identitas, penilaian risiko keamanan siber sendiri, pengelolaan keamanan siber dalam rantai pasokan, dan pengungkapan kerentanan. Terdapat perubahan yang terjadi di framework ini yang didasarkan pada umpan balik yang dikumpulkan melalui panggilan publik untuk komentar, pertanyaan yang diterima oleh anggota tim, dan lokakarya yang diadakan pada 2016 dan 2017. Framework ini

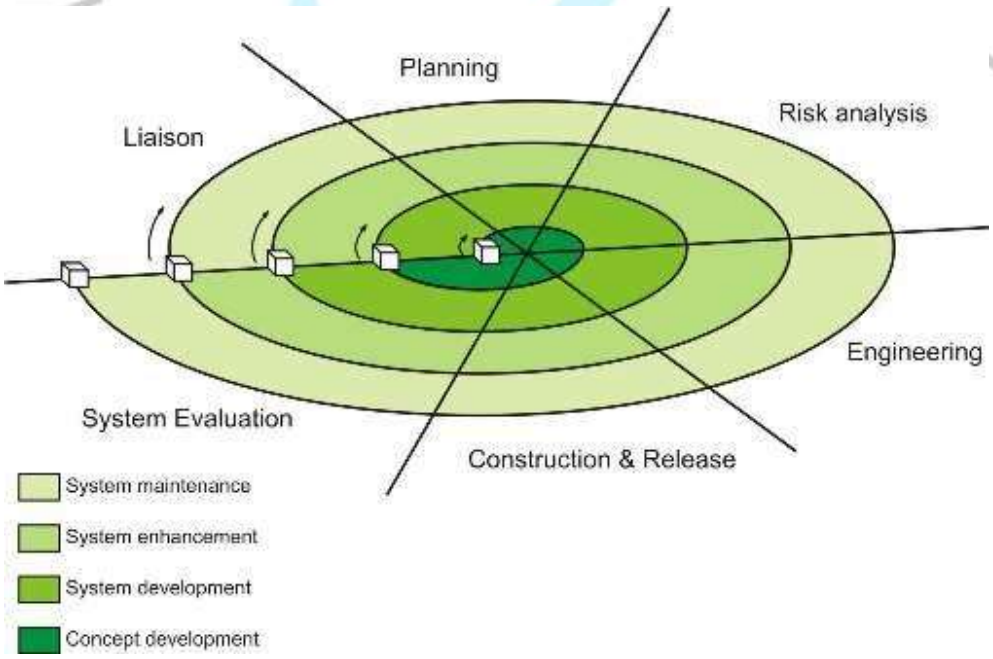
dirancang untuk memenuhi kebutuhan bisnis atau misi organisasi individu dan berlaku untuk berbagai lingkungan teknologi seperti teknologi informasi, sistem kontrol industri, dan Internet of Things. Framework NIST 1.1 terdiri dari 5 fungsi *Identify, Protect, Detect, Respond, Recover*.

3.1.2. Metode Pengumpulan Data

Peneliti akan menggunakan metode wawancara sebagai teknik pengumpulan data pada penelitian ini. Peneliti menggunakan metode ini karena untuk mengetahui bagaimana sistem yang digunakan oleh institusi XYZ bekerja. Selain itu, Peneliti bisa mempertanyakan kebutuhan keamanan apa saja yang dibutuhkan oleh pengurus sistem tersebut.

3.1.3. Metode Pengembangan Data

Peneliti akan menerapkan metode spiral dalam rangka melakukan penelitian ini. Sebagaimana dijelaskan oleh Zidniryi (2021), metode spiral merupakan suatu model proses yang menggabungkan sifat iteratif dari prototipe dengan mengendalikan aspek model secara sekuensial linear. ini merupakan metode yang cocok dengan penggunaan NIST *cyber security framework*, karena *framework* tersebut biasanya akan menggunakan sistem keamanan yang sudah dipakai oleh Institusi kemudian digabungkan dengan sistem keamanan *framework*.



Gambar 3.1 Metode Pengembangan Data Spiral (qnp.co.id, 2022)

Metode spiral ini memiliki fase-fase yang serupa dengan fase security development life cycle, yaitu:

a. *Planning* : Fase ini merencanakan bagaimana sistem keamanan yang ingin dirancang. Hal ini membutuhkan diskusi terhadap institusi XYZ.
b. *Risk Analysis* : Di fase ini, Peneliti akan menganalisa risiko dari hasil *planning* tersebut. Hal ini menjamin bahwa sistem yang akan dikembangkan telah memenuhi kebutuhan institusi. Melihat apakah ada kekeliruan dari hasil *planning*.
c. *Engineering* : Fase ini, peneliti mulai mengerjakan sistem yang ingin dibuat. Biasanya Peneliti akan mencari orang yang mengerti cara membuat sistem keamanan, dan menjelaskan bagaimana sistem keamanan tersebut bekerja.
d. *Evaluation* : Fase ini peneliti melakukan tes uji coba sistem yang sudah dibuatnya. Tes uji coba ini dilakukan oleh pihak institusi yang bertugas di bagian keamanan aplikasi. Setelah dilakukan tes, Peneliti mulai memberikan kuesioner terhadap penguji untuk menilai apakah ada kekurangan atau apa yang ingin ditambahkan dari sistem keamanan tersebut.
e. *New Planning* : Fase ini akan digunakan secara opsional, karena fase ini sama seperti fase *planning*. Namun, fase ini akan digunakan jika sistem yang sudah dibuat tersebut masih dianggap penguji sebagai kurang memuaskan atau sistem yang sudah dibuat tersebut ingin dikembangkan kembali atau pihak institusi ingin mengganti sistem keamanan tersebut.

3.2 Analisis Sistem yang Berjalan

Kesadaran terhadap serangan siber di kalangan civitas akademika perlu ditingkatkan. Meskipun teknologi informasi dan komunikasi vital dalam operasional universitas, pemahaman tentang ancaman siber masih kurang. Mahasiswa, dosen, dan staf administrasi belum sepenuhnya menyadari risiko serangan siber. Tantangan utama melibatkan ketidakpahaman mengenai cara serangan siber terjadi dan dampaknya terhadap operasional harian universitas.

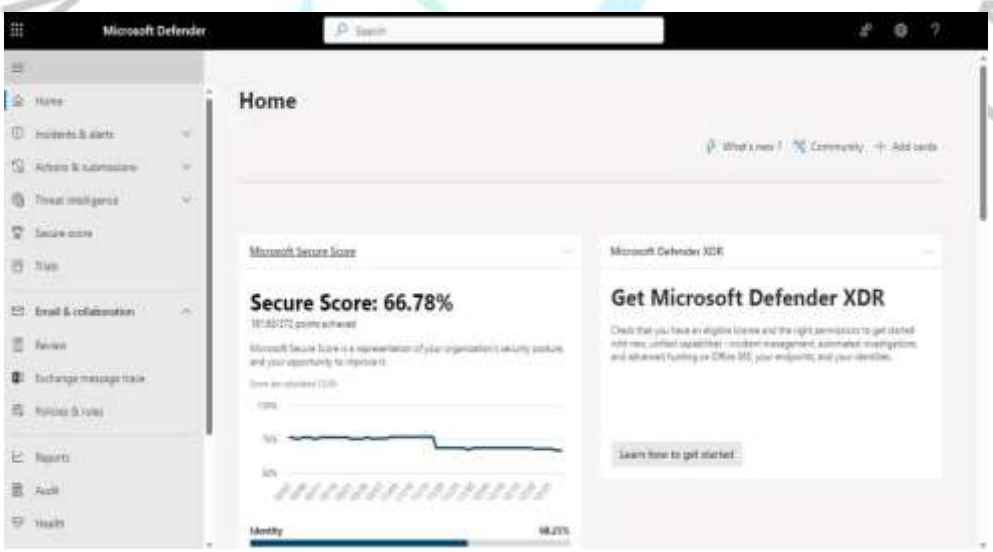
Mahasiswa, terutama yang aktif dalam perkuliahan daring, mungkin tidak menyadari potensi pencurian data pribadi atau serangan terhadap infrastruktur digital universitas. Dosen dan staf administrasi, yang memiliki akses ke data sensitif, juga bisa menjadi sasaran empuk. Kurangnya pemahaman terhadap teknik serangan siber dapat menyebabkan kelalaian dalam melindungi informasi. Ketidakpahaman ini bisa disebabkan oleh kurangnya pelatihan dan edukasi keamanan siber. Universitas perlu meningkatkan upaya memberikan pemahaman tentang serangan siber, mengenali pola umum serangan, dan cara melindungi diri secara efektif. Pusat keamanan siber di universitas dapat berperan penting dalam memberikan pelatihan rutin, seminar, dan sumber daya informatif. Dukungan aktif dari pihak universitas, termasuk perumusan dan penerapan kebijakan keamanan siber yang kuat, diperlukan untuk meningkatkan kesadaran civitas akademika. Pengembangan kebijakan dengan partisipasi semua pihak dapat menciptakan lingkungan yang aman. Integrasi teknologi keamanan mutakhir juga diperlukan untuk mendeteksi dan melawan serangan siber lebih efektif.

Hingga saat ini Institusi XYZ belum memiliki kebijakan yang memadai terkait keamanan siber dan perlindungan terhadap serangan siber. Padahal, ancaman serangan siber di era digital saat ini sangat tinggi dan berpotensi merugikan institusi pendidikan. Serangan siber dapat mengganggu kegiatan pembelajaran dan mengancam privasi data institusi XYZ. Jenis serangan siber antara lain phising, malware, ransomware, Distributed Denial of Service (DDoS), dan hacking. Serangan ini dapat mengganggu sistem TI, mencuri data sensitif institusi dan mahasiswa, bahkan meminta tebusan uang untuk mengembalikan akses ke sistem yang diserang. Akses ke sistem akademik, keuangan, dan administrasi institusi dapat terganggu jika diserang hacker. Kurangnya kebijakan keamanan siber dapat menurunkan kepercayaan mahasiswa dan masyarakat terhadap Institusi XYZ. Data pribadi dan akademik mahasiswa yang disimpan institusi dapat bocor jika sistem keamanan siber lemah. Padahal institusi pendidikan seharusnya menjadi contoh dalam penerapan keamanan siber guna melindungi komunitas kampus. Institusi XYZ perlu segera menyusun kebijakan dan panduan terkait keamanan siber. Kebijakan ini dapat berisi prosedur dan standar keamanan data dan sistem TI yang harus dipatuhi semua sivitas akademika. Misalnya, aturan

penggunaan password yang aman, prosedur backup data secara berkala, hingga pemasangan antivirus dan firewall pada semua perangkat institusi. Kebijakan dan upaya perlindungan siber yang memadai dapat menjaga operasional institusi XYZ agar tetap berjalan optimal. Mahasiswa dan orang tua juga merasa yakin data pribadi tersimpan aman. Dengan demikian, Institusi XYZ dapat fokus menjalankan tridharmanya dengan baik tanpa gangguan serangan siber yang merugikan.

Ada 3 sisi perlindungan dari perlindungan terhadap serangan siber saat ini, yaitu dari sisi Email kemudian dari sisi Firewall dan terakhir dari sisi Endpoint. Sistem keamanan yang dipakai oleh unit keamanan siber di institusi XYZ adalah menggunakan *Exchange Online Protection, Bitdefender Endpoint Security* (*Bitdefender GravityZone Business Security*), *firewall, SSH attack,* dan *IP Public Check*. *Exchange Online Protection* berguna untuk email, *Bitdefender Endpoint Security* berguna untuk melindungi perangkat *endpoint,* dan *firewall, SSH attack ,* dan *IP Public Check* melindungi jaringan dan server institusi.

Exchange Online Protection adalah sebuah aplikasi yang berguna sebagai penyaring dan pengelolaan email sehingga menghindari perangkat dari serangan email yang berisi virus, spam, dan *phising*. Dengan *Exchange Online Protection*, perangkat keras milik institusi XYZ terhindar dari serangan siber yang berpotensi membuat kebocoran data dan informasi rahasia milik institusi.

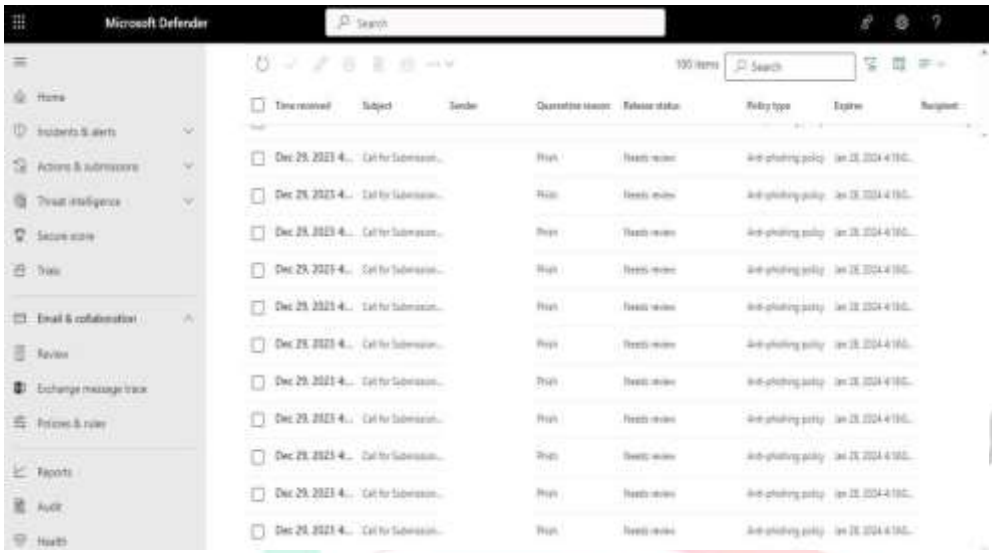


Gambar 3.1. Exchange Online Protection

Exchange online protection juga akan membantu pengguna untuk memperkuat keamanan yang dimiliki pengguna, dimulai dari memberikan *password* tambahan atau menambah email untuk memberitahukan bahwa ada

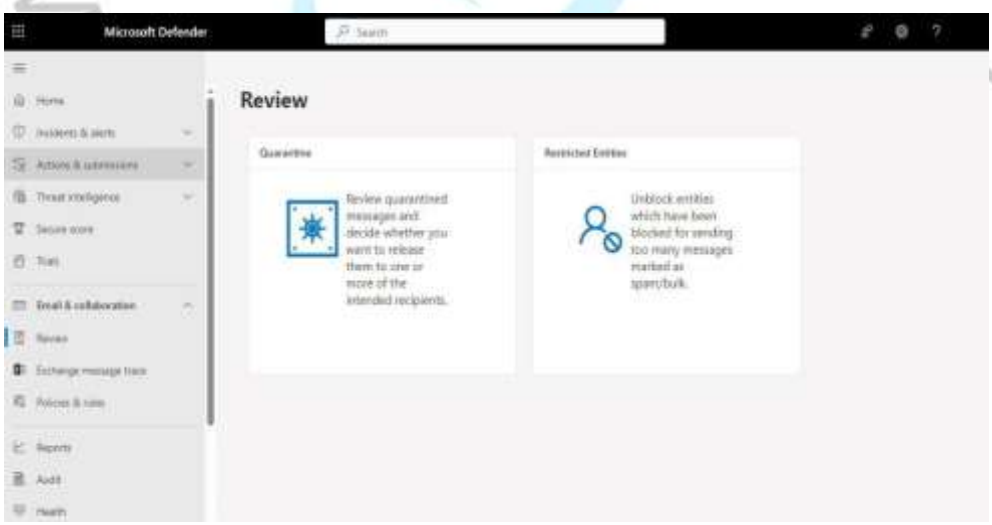
seseorang yang menggunakan email pengguna di perangkat lain.

Selain itu, *exchange online protection* akan menunjukkan email-email yang menurut aplikasi tersebut sebagai email yang berbahaya. Email-email tersebut akan diberi label oleh aplikasi tersebut, dari spam, phising, dan lain-lain.



Gambar 3.2. Email yang dianggap Exchange Online Protection sebagai email phising

Walaupun begitu, Aplikasi ini juga memiliki kekurangan, yaitu jika ada email resmi yang keseringan mengirimkan pesan yang sama secara berulang, email tersebut akan dianggap sebagai email spam. Untuk menghindari hal tersebut, aplikasi ini memiliki fitur dimana pengguna bisa memberitahukan ke aplikasi bahwa email tersebut adalah email resmi yang pengguna kenal.



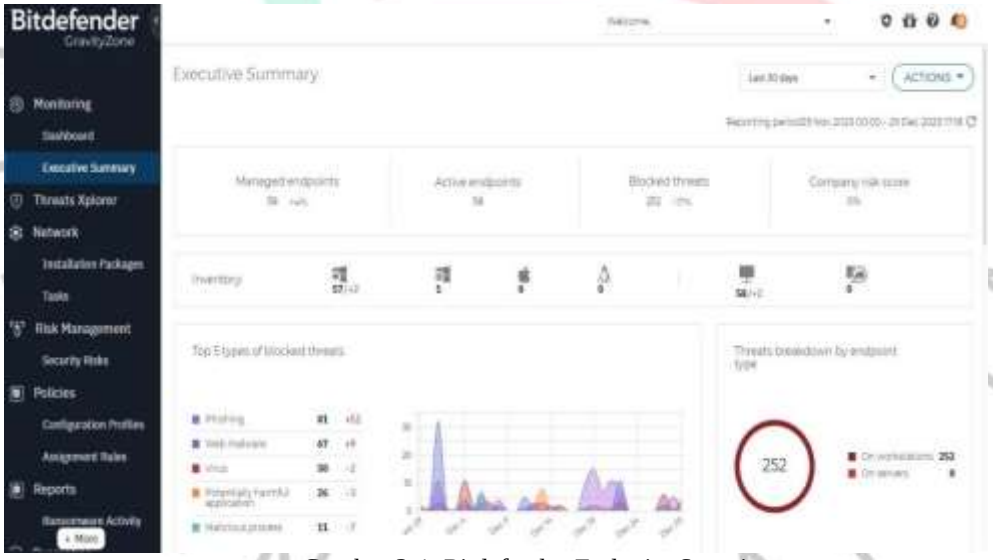
Gambar 3.3. menu review Exchange Online Protection

Berdasarkan Gambar 3.3., Ada dua pilihan untuk fitur pemberitahuan email, yaitu *Quarantine* dan *restricted entities*. *Quarantine* berfungsi sebagai menunjukkan email-email yang dikarantina. Email yang dikarantina tersebut adalah

email yang dianggap aplikasi tersebut sebagai email spam, *phising*, dan email yang membawa virus.

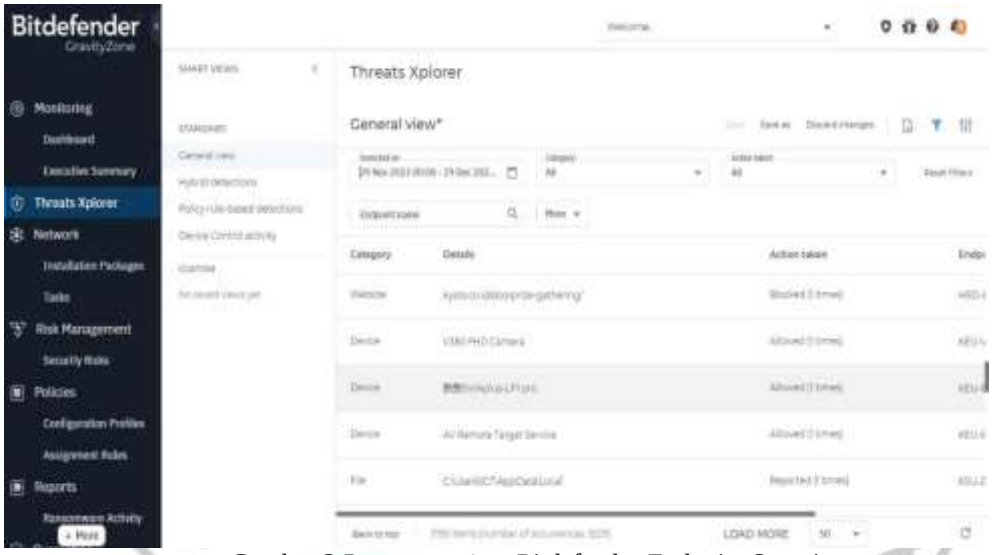
Sedangkan *restricted entities* berfungsi sebagai meng-*unblock* email yang dianggap sebagai spam. Fitur ini dapat digunakan oleh pengguna untuk memberitahukan kepada sistem bahwa email yang mereka anggap spam adalah email yang sah dan merupakan milik institusi, sehingga suatu saat email tersebut memberikan email kedepannya, sistem tidak akan menganggap email tersebut sebagai email spam.

Bitdefender Endpoint Security adalah sebuah anti-virus yang bertugas sebagai pelindung perangkat lunak. Jika ada serangan *hacker* dan membuka perangkat lunak, atau ketika pengguna mengunduh suatu aplikasi, namun aplikasi tersebut menyimpan virus, anti-virus akan mendeteksi serangan tersebut dan mengeliminasi ancaman-ancaman tersebut



Gambar 3.4. *Bitdefender Endpoint Security*

Selain itu, *Bitdefender endpoint security* akan melakukan pengecekan terhadap ancaman-ancaman yang sudah masuk ke dalam perangkat tersebut. Pengguna dapat mengecek apakah hal yang masuk ke perangkat tersebut berbahaya atau tidak.



Gambar 3.5. menu review *Bitdefender Endpoint Security*

Untuk melindungi jaringan internet dan server milik institusi XYZ, mereka menggunakan *firewall*, *SSH attack,* dan *IP Public Check*. Menurut Ardyanto, *firewall* berfungsi sebagai mengontrol dan mengawasi arus paket data, Menjadi pos pengamanan jaringan, mencatat aktivitas pengguna, dan mencegah kebocoran informasi. Selain firewall, *IP Public Check* berfungsi sebagai pengecek *IP address* yang masuk kedalam perangkat apakah *IP address* tersebut merupakan *IP address* milik institusi, atau tidak.

3.2 Analisis dan Pengumpulan Data

3.2.1. Analisis Penelitian

1.4.1.1.1 *Identify* (Identifikasi)

Fungsi Identifikasi terdiri dari enam kategori. Pertama adalah Asset Management (ID.AM) melibatkan identifikasi dan manajemen data, personel, perangkat, sistem, dan fasilitas yang menjadi elemen-elemen kunci dalam mencapai tujuan bisnis organisasi. Pengelolaan ini dilakukan secara konsisten dengan memperhatikan kepentingan relatifnya terhadap tujuan dan strategi risiko organisasi. Kategori kedua adalah Business Environment (ID.BE), yang mencakup pemahaman dan prioritas terhadap misi, tujuan, pemangku kepentingan, dan kegiatan organisasi. Data ini dipergunakan untuk memberikan arahan terhadap peran, tanggung jawab, serta keputusan dalam manajemen risiko keamanan siber.

Selanjutnya, Governance (ID.GV) merupakan kategori ketiga,

yang mencakup Kebijakan, prosedur, dan proses ini dirancang untuk mengelola dan memantau peraturan organisasi, hukum, risiko, lingkungan, serta persyaratan operasional. Informasi ini memberikan landasan bagi manajemen risiko keamanan siber. Kategori keempat adalah Risk Assessment (ID.RA), di mana organisasi memahami risiko keamanan siber terhadap operasi, aset, dan individu-individu.

Kemudian, Risk Management Strategy (ID.RM) menjadi kategori kelima, yang melibatkan penetapan prioritas, kendala, toleransi risiko dan asumsi organisasi ditetapkan sebagai landasan untuk mendukung pengambilan keputusan terkait risiko. operasional. Terakhir, kategori keenam adalah Supply Chain Risk Management (ID.SC), di mana organisasi menetapkan prioritas, batasan, toleransi risiko, dan asumsi Dalam konteks mendukung keputusan risiko yang terkait dengan manajemen risiko rantai pasokan, organisasi telah menetapkan dan melaksanakan proses untuk mengidentifikasi, menilai, dan mengelola risiko-risiko yang terdapat dalam rantai pasokan.

1.4.1.1.2 *Protect* (Melindungi)

Perlindungan terbagi dalam enam kategori, dimulai dengan Identity Management, Authentication, and Access Control (PR.AC). Pada kategori ini, akses ke aset fisik dan logis serta fasilitas terkait dibatasi hanya pada pengguna, proses, dan perangkat yang memiliki otorisasi. Manajemen ini dilakukan secara konsisten dengan penilaian risiko terhadap potensi akses tidak sah ke aktivitas dan transaksi resmi.

Selanjutnya, Awareness and Training (PR.AT) menjadi kategori kedua, di mana personel dan mitra organisasi diberikan edukasi tentang kesadaran keamanan siber dan diberi pelatihan untuk melaksanakan tugas dan tanggung jawab terkait keamanan siber sesuai dengan kebijakan, prosedur, dan perjanjian terkait. Kategori ketiga adalah Data Security, di mana informasi dan catatan (data) dikelola sesuai dengan strategi risiko organisasi untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi.

Berikutnya, Information Protection Processes and Procedures (PR.IP) menjadi kategori keempat, yang melibatkan pemeliharaan kebijakan keamanan, proses, dan prosedur untuk mengelola perlindungan sistem dan aset informasi. Kemudian, Maintenance (PR.MA) menjadi kategori kelima, di mana pemeliharaan dan perbaikan komponen pengendalian industri dan sistem informasi dilakukan sesuai dengan kebijakan dan prosedur yang telah ditetapkan.

Terakhir, kategori keenam adalah Protective Technology (PR.PT), di mana solusi keamanan teknis dikelola untuk memastikan keamanan dan ketahanan sistem dan aset, sesuai dengan kebijakan, prosedur, dan perjanjian yang relevan.

1.4.1.1.3 Detect (Mendeteksi)

Fungsi Mendeteksi tediri dari 3 katagori yaitu pertama adalah *Anomalies and Event (DE.AE)* yaitu Aktivitas anomali terdeteksi dan potensi dampak peristiwa dipahami. Kemudian yang kedua yaitu Security Continuous Monitoring (DE.CM) melibatkan pemantauan terus-menerus terhadap sistem informasi dan aset guna mengidentifikasi peristiwa keamanan siber serta memverifikasinya. Selanjutnya, Detection Processes (DE.DP) juga merupakan kategori terakhir, di mana sistem informasi dan aset dipantau untuk mengenali peristiwa keamanan siber dan melakukan verifikasi terhadapnya.

1.4.1.1.4 Respond (Menanggapi)

Fungsi Menanggapi terdiri dari 5 kategori. Yaitu pertama adalah Response Planning (RS.RP) melibatkan pelaksanaan dan pemeliharaan proses dan prosedur respons, dengan tujuan memastikan respons yang efektif terhadap insiden keamanan siber yang terdeteksi. Kemudian, Communications (RS.CO) adalah kegiatan di mana tanggapan darurat dikoordinasikan dengan pemangku kepentingan internal dan eksternal, seperti dukungan eksternal dari lembaga penegak hukum. Selanjutnya,

Analysis (RS.AN) melibatkan koordinasi tanggapan darurat dengan pemangku kepentingan internal dan eksternal, termasuk dukungan eksternal dari lembaga penegak hukum.

Kemudian, Mitigation (RS.MI) adalah kegiatan yang dilakukan untuk mencegah perluasan suatu peristiwa, mengurangi dampaknya, dan menyelesaikan insiden tersebut. Terakhir, Improvements (RS.IM) melibatkan peningkatan aktivitas respons organisasi dengan mengintegrasikan pembelajaran dari aktivitas deteksi/respons saat ini dan sebelumnya.

1.4.1.1.5 Recovery (Pemulihan)

Fungsi Pemulihan terdiri dari 3 kategori. Yaitu pertama adalah *Recovery* Planning (RC.RP) melibatkan pelaksanaan dan pemeliharaan proses serta prosedur pemulihan, bertujuan untuk memastikan pemulihan sistem atau aset yang terdampak oleh insiden keamanan siber. Kemudian, Improvements (RC.IM) adalah kegiatan di mana perencanaan dan proses pemulihan ditingkatkan dengan memasukkan pembelajaran ke dalam kegiatan di masa depan. Terakhir, Communications (RC.CO) melibatkan koordinasi kegiatan restorasi dengan pihak internal dan eksternal, seperti pusat koordinasi, Penyedia Layanan Internet, pemilik sistem penyerang, korban, CSIRT lain, dan vendor.