PUSAT OPERASI KESELAMATAN (SOC): MODEL PERANAN DAN TANGGUNGJAWAB, TAHAP PENDIDIKAN SERTA KEMAHIRAN AHLI PASUKAN

HISHAM BIN HASHIM

UNIVERSITI KEBANGSAAN MALAYSIA

PUSAT OPERASI KESELAMATAN (SOC): MODEL PERANAN DAN TANGGUNGJAWAB, TAHAP PENDIDIKAN SERTA KEMAHIRAN AHLI PASUKAN

HISHAM BIN HASHIM

PROJEK YANG DIKEMUKAKAN UNTUK MEMENUHI SEBAHAGIAN
DARIPADA SYARAT MEMPEROLEHI
IJAZAH SARJANA KESELAMATAN SIBER

FAKULTI TEKNOLOGI DAN SAINS MAKLUMAT
UNIVERSITI KEBANGSAAN MALAYSIA
BANGI

2022

PENGAKUAN

Saya akui karya ini adalah hasil kerja saya sendiri kecuali nukilan dan ringkasan yang tiap-tiap satunya telah saya jelaskan sumbernya.

30 Mac 2022

HISHAM BIN HASHIM
GP06368

PENGHARGAAN

Dengan nama Allah yang Maha Pengasih lagi Maha Penyayang.

Alhamdulillah, syukur kepada Allah SWT kerana dengan rahmatnya dapat saya menyiapkan kertas projek ini. Selawat dan salam ke atas junjungan besar Nabi Muhammad S.A.W, ahli keluarga, dan sahabat baginda.

Pertamanya, saya mengucapkan jutaan terima kasih yang tidak terhingga kepada penyelia saya iaitu Dr. Khairul Akram Bin Zainol Ariffin. Bimbingan, tunjuk ajar, teguran serta menaikkan semangat saya sepanjang menjalankan kajian ini adalah sesuatu yang terlalu bernilai dan tidak mampu saya balas. Terima kasih tidak terhingga kepada semua pensyarah dan warga Fakulti Teknologi dan Sains Maklumat, Universiti Kebangsaan Malaysia yang telah banyak memberi tunjuk ajar dan berkongsi ilmu, memberikan idea, komen, dan sokongan untuk memantapkan projek ini.

Saya juga mengucapkan terima kasih kepada penaja saya iaitu Jabatan Perkhidmatan Awam atas tajaan yang diberikan. Tidak lupa juga kepada majikan saya iaitu MAMPU yang meluluskan cuti belajar untuk saya melanjutkan pengajian peringkat Sarjana ini.

Tidak dilupakan kepada isteri dan anak-anak tercinta; Suhaily Binti Hoseni, Hadira Binti Hisham, Haziqa Binti Hisham dan Haqeem Bin Hisham di atas segala sokongan moral, doa, kesabaran menunggu dan pengorbanan yang diberikan tanpa henti.

Akhir kata, terima kasih diucapkan kepada semua yang telah membantu saya menyiapkan kertas projek ini secara langsung atau tidak langsung. Semoga Allah merahmati anda semua.

ABSTRAK

Sejak pengenalan Pusat Operasi Keselamatan (SOC) kira-kira 15 tahun yang lalu, kepentingannya telah berkembang dengan ketara, terutamanya sejak lima tahun yang lepas. Perkara ini disebabkan oleh peningkatan insiden keselamatan di organisasi yang menyaksikan kerugian jutaan ringgit kepada sesebuah organisasi itu. Serangan dan ancaman siber semakin rumit dan perkakasan pertahanan sedia ada tidak lagi dapat membendung perkara ini. Oleh itu penubuhan sesebuah SOC diperlukan bagi mengesan ancaman dengan lebih berkesan dan pantas. Sesebuah SOC yang mantap mempunyai tiga (3) elemen penting iaitu teknologi, proses dan manusia. Walau bagaimanapun dalam kajian ini, faktor manusia menjadi asas kajian kerana teknologi dan proses sedia ada mencukupi dalam sesebuah SOC tetapi banyak faktor kelemahan manusia lain harus dilihat seperti kecuaian, kompetensi yang rendah dan kemahiran yang tidak mencukupi. Oleh itu, organisasi yang ingin membangunkan SOC atau menambahbaik SOC sedia ada perlu mengetahui kriteria minimum dari segi peranan dan tanggungjawab, tahap pendidikan dan kemahiran, sebelum seseorang itu dipilih menjadi ahli pasukan SOC. Justeru, kaedah kajian ini adalah melibatkan tinjauan kesusasteraan yang komprehensif yang telah dijalankan bagi mengumpulkan pandangan yang berbeza dan pengesahan pakar ke atas model yang akan dibangunkan. Di akhir kajian ini satu model Peranan dan Tanggungjawab, Tahap pendidikan serta Kemahiran bagi SOC berjaya dihasilkan dan diharap agar model ini boleh digunakan sebagai panduan organisasi untuk melakukan pemilihan ahli SOC baru atau menambahbaik SOC sedia ada dari segi faktor manusia umumnya dan ahli pasukan SOC khususnya.

SECURITY OPERATION CENTER : MODEL OF ROLES AND RESPONSIBILITIES, LEVEL OF EDUCATION AND SKILLS OF TEAM MEMBERS

ABSTRACT

Since the introduction of the Security Operations Center (SOC) about 15 years ago, its importance has grown significantly, especially over the past five years. This is due to the increase in organized security incidents which have seen the loss of millions of ringgits to an organization. Cyber-attacks and threats are becoming more complex and advanced where existing defence hardware can no longer contain this. Therefore, the establishment of an SOC is very necessary to detect threats more effectively and quickly. A strong SOC has three (3) important elements, namely technology, process and people. However, in this study, human factors are the basis of the study because although the existing technology and processes are sufficient in an SOC but many other human weakness factors should be seen such as negligence, low competence and insufficient skills. Therefore, organizations wishing to develop an SOC or improve an existing SOC need to know the minimum criteria in terms of roles and responsibilities, level of education and skills, before a person is selected to be a member of the SOC team. Thus, the approach of this study involves a comprehensive literature review that has been conducted to gather different views and expert validation on the model to be developed. At the end of this study, a prototype model of Roles and Responsibilities, Education Level and Skill for SOC was successfully produced and it is hoped that this model can be used as an organizational guide to select new SOC members or improve existing SOC in terms of human factors in general and SOC team members in particular.

KANDUNGAN

Halaman

SENARAI JADUAL

SENARAI ILUSTRASI

SENARAI SINGKATAN

AI	*Artificial Intelligence*
APT	*Advanced Persistent Threat*
AV	*Antivirus*
CHE	*Certified Ethical Hacker*
CISSP	*Certified Information Systems Security Professional*
CSOC	*Cyber Security Operation Center*
DOS	*Denial Of Service*
ENISA	Agensi Kesatuan Eropah untuk Rangkaian dan Keselamatan Maklumat
HTTP	*Hypertext Transfer Protocol*
ICT	*Information and Communications Technology*
IDS	*Intrution Detection System*
IPS	*Intrution Prevention system*
MAHB	*Malaysia Airports Holdings Berhad*
NOC	*Network Operation Center*
RFC	*Request For Comments*
SANS	*Institute is the most trusted resource for cybersecurity training, certifications and research*
SIEM	*Security Information and Event Management*
SOC	Pusat Operasi Keselamatan
URL	*Uniform Resource Locator*
WAF	*Web Application Firewall*

BAB I

PENDAHULUAN

1.1 PENGENALAN

Dalam beberapa tahun kebelakangan ini, bilangan peranti yang disambungkan meningkat dengan pantas, melebihi 17 bilion pada tahun 2018. Penyebaran dan peningkatan peranti yang disambungkan ke infrastruktur siber adalah secara eksponensial, yang menyebabkan kadar kerosakan peranti yang lebih tinggi. Tahap kemungkinan mengalami pelanggaran keselamatan telah meningkat dengan ketara dalam beberapa tahun kebelakangan ini. Menurut Ponemon Institute (2018) serangan telah meningkat dari segi jumlah dan kerumitan. Ukuran rangkaian yang semakin meningkat bukan satu-satunya faktor yang mempengaruhi jumlah penyerang yang berpotensi, tetapi juga alat yang tersedia untuk penyerang menjadi lebih kompleks, canggih, berkebolehan, dan kuat.

Kepantasan industri keselamatan siber memaksa unit pusat operasi keselamatan (SOC) berkembang supaya unit SOC dapat mempertahankan organisasi daripada ancaman semasa dan akan datang. Pertahanan reaktif tidak lagi mencukupi dengan sendirinya, kerana landskap ancaman siber menjadi semakin pelbagai dan kompleks. Misi utama unit SOC adalah untuk membina dan mengekalkan gambaran situasi keselamatan siber bagi sesebuah organisasi. Pembangunan pusat operasi keselamatan ialah aktiviti yang melindungi aset maklumat daripada serangan siber. Ia memantau dan bertindak balas kepada peristiwa keselamatan dan log dalam masa nyata.

Keselamatan aset maklumat dijalankan oleh kumpulan khas, dan organisasi boleh memberi tumpuan kepada kecekapan teras. Ia menyediakan maklumat tentang kelemahan, faktor pelanggaran dan tindakan balas, serta melaksanakan analisis dan

makluman masa nyata untuk mengelakkan pelanggaran tidak sengaja daripada berlaku. Operasi keselamatan yang berkesan dan aktiviti tindak balas pencerobohan, adalah perlu untuk mengesan percubaan serangan siber dengan berkesan. Pengesanan yang berkesan adalah perlu untuk mengeluarkan bunyi penggera apabila peristiwa penting berlaku atau memaparkan skrin yang boleh membantu secara langsung aktiviti kerja ahli pasukan operasi keselamatan pada skrin papan pemuka untuk pemeriksaan visual dengan mudah.

Dari perspektif keselamatan siber, adalah perlu untuk menyeragamkan papan pemuka operasi keselamatan untuk menyokong operasi keselamatan yang cekap. Pusat Operasi Keselamatan (SOC) ialah unit berpusat yang terdiri daripada orang, proses dan teknologi yang memberikan kesedaran situasi keselamatan siber kepada syarikat atau organisasi. Matlamat unit SOC adalah untuk mencegah dan menganalisis insiden keselamatan maklumat. Unit SOC mencapainya dengan menganalisis data berkaitan keselamatan yang dikumpul dari persekitaran teknikal organisasi. Serangan siber dan pelanggaran data menjadi biasa berbanding sebelum ini menjejaskan semua manusia dan semua perusahaan baik kecil mahupun besar.

Hampir semua data termasuk maklumat peribadi disimpan dan dikawal oleh sistem komputer. Memandangkan serangan siber menjadi lebih canggih, adalah penting untuk bertindak balas dengan cepat terhadap insiden keselamatan, sebelum penyerang mendapat capaian kepada sistem yang lebih penting atau bertapak dalam rangkaian. Tujuan SOC adalah untuk mewujudkan dan mengekalkan gambaran situasi keselamatan organisasi sambil bertindak balas dengan pantas terhadap kemungkinan perubahan di dalamnya. Sistem terkawal komputer ada di mana-mana, dan tanpa langkah keselamatan yang mencukupi, ia menimbulkan risiko terjadinya insiden keselamatan. Selain itu, fungsi unit SOC untuk memusatkan pengurusan keselamatan di seluruh organisasi supaya organisasi boleh bertindak balas terhadap ancaman sebelum ia bertukar menjadi insiden keselamatan

Memandangkan masyarakat semakin bergantung pada fungsi sistem ini, pertaruhannya adalah tinggi. Bidang keselamatan siber sentiasa berubah, dan serangannya lebih rumit dan pelbagai berbanding sebelum ini. Secara tradisinya,

terdapat sedikit alat yang digunakan untuk melindungi rangkaian maklumat. Apabila bilangan alatan adalah lebih rendah, pengurusan dan pemantauan adalah agak mudah. Tembok api (*Firewall*), sistem pengesanan pencerobohan (IDS) dan perisian antivirus (AV) mempunyai antara muka pengguna khusus pembekal yang berasingan untuk konfigurasi, pengurusan dan pemantauan. *Firewall* rangkaian ialah peranti yang menapis trafik mengikut peraturan yang dikonfigurasikan. IDS rangkaian (NIDS) menganalisis trafik untuk mengesan pelanggaran keselamatan. Perisian AV biasanya dipasang pada sistem pengendalian hos dan menganalisis peranti untuk perisian hasad. Bagaimanapun, serangan yang semakin rumit telah mewujudkan permintaan untuk alatan seperti sistem pencegahan pencerobohan (IPS) dan tembok api yang dipertingkatkan, yang sering dipasarkan sebagai tembok api generasi akan datang. IPSec adalah serupa dengan IDS tetapi mampu cuba menyekat pencerobohan yang dikesan, tidak seperti IDS.

Pengurusan berpusat menjadi lebih kompleks apabila bilangan peranti keselamatan meningkat. Biasanya, vendor perisian dan perkakasan mempunyai alat yang bertujuan untuk menyatukan pengurusan antara peranti yang berbeza. Walau bagaimanapun, menggunakan produk semata-mata daripada vendor tunggal mungkin tidak selalu boleh atau berkesan, kerana vendor biasanya pakar dalam beberapa produk. Pasaran pelbagai vendor mewujudkan jurang dan merumitkan proses mencipta dan mengekalkan gambaran situasi.

Organisasi hari ini menyedari bahawa, teknologi merupakan bahagian penting untuk perniagaan, operasi bisnes mereka terdedah dan mempunyai risiko tinggi terhadap ancaman keselamatan siber. Mereka perlu melindungi maklumat sensitif mengenai setiap pelanggan, rakan kongsi serta operasi dari penjenayah siber dan perisian penggodaman. Organisasi sudah mula meneroka kaedah baru untuk melindungi aset ICT mereka dari serangan yang berpotensi menjadi insiden. Strategi yang telah diwujudkan antaranya adalah dengan membeli perisian untuk mengimbas rangkaian *(Security Scanning Tools)* organisasi untuk mencari kelemahan pada rangkaian dan sistem mereka. Walaubagaimanapun organisasi mestilah mempunyai sumber manusia yang mahir dan berpengalaman untuk menggunakan perisian *(tools)* tersebut. Oleh itu, dengan kekangan sumber manusia yang mahir, organisasi mula mengalih penjagaan

keselamatan ICT kepada penyedia perkhidmatan luaran *(MSSP).* Selain itu, pendekatan paling berkesan yang mula mendapat banyak perhatian di antara organisasi adalah dengan mewujudkan Pasukan Pusat Operasi Keselamatan sendiri. (Blackstratus, 2019)

Perlindungan keselamatan dianggap sebagai "proses untuk melindungi objek dari kerosakan fizikal, capaian tanpa izin, kecurian, atau kehilangan, dengan menjaga kerahsiaan tinggi dan integriti maklumat tentang objek tersebut dan membuat maklumat tentang objek itu tersedia bila diperlukan" (Abomhara & Køien 2015). Justeru, sistem yang selamat menjamin bahawa maklumat yang diterima oleh pengguna belum diubah setelah dihantar (integriti data) dan sistem yang selamat akan menjamin kerahsiaan pengguna dengan tidak membenarkan pihak yang tidak disahkan untuk mencapai atau memeriksa data yang dihantar. Oleh itu, menjaga integriti dan kerahsiaan data adalah amat penting.

Langkah pertama dalam proses ini adalah mengenal pasti aset sistem rangkaian dan menyediakan inventori setiap komponen dalam sistem rangkaian. Aset merujuk kepada sebarang sumber yang merupakan sebahagian daripada rangkaian. Aset tersebut dapat dibahagikan kepada dua kategori: "lembut" yang akan merangkumi program perisian dan "keras", yang meliputi komputer hos, pelayan, komputer, dan komputer riba. Aset rangkaian adalah aset saling berkaitan dan bergantungan untuk menyediakan perkhidmatan di dalam sesebuah organisasi.

Istilah "kerentanan" meliputi semua kelemahan yang terdapat di dalam sistem atau dalam perancangan sistem yang dapat dieksploitasi dengan membiarkan penyerang untuk melaksanakan serangan, mencapai data yang tidak sah, atau melakukan serangan penolakan-layanan (DOS). Kelemahan ini dapat dijumpai dalam perkakasan, perisian, firmware, sistem operasi, rangkaian, atau polisi dan prosedur yang digunakan dalam sistem. Beberapa kelemahan keselamatan perisian yang paling biasa ditemui adalah overflow buffer, penyulitan data yang hilang, skrip lintas tapak dan pemalsuan, suntikan arahan OS, dan pengalihan URL ke laman yang tidak dipercayai.

Potensi kerentanan untuk dieksploitasi adalah disebut ancaman. Ancaman boleh dibahagikan kepada dua kategori berdasarkan sumbernya: alam semula jadi seper dan

manusia. Kategori alam merangkumi kejadian seperti bencana alam yang akan mempengaruhi perkakasan sistem komputer. Jenis bencana ini tidak mungkin dapat dihindarkan daripada berlaku dan hanya perlindungan kecil yang dapat dijalankan. Selain itu, kategori manusia merangkumi ancaman yang dikeluarkan oleh individu atau organisasi, atau oleh orang dalaman, yang memiliki capaian yang dibenarkan, seseorang yang berada di luar rangkaian dan dapat dilakukan secara berstruktur atau tidak berstruktur (Abomhara & Køien 2015). Kemungkinan ancaman terjadi terdapat dalam pengukuran risiko yang harus dipertimbangkan ketika mengutamakan kelemahan dan tahap ancaman mereka.

Di dunia sekarang, serangan siber telah meningkatkan tahap kerumitan dan serangan mereka menjadi lebih canggih dan serangan keselamatan meningkat secara drastik dalam beberapa tahun terakhir ini. Menurut Ponemon Institute (2018), di Amerika Syarikat (AS), satu daripada empat organisasi akan terlibat dengan serangan siber setiao tahun. Oleh yang demikian, dengan adanya pasaran yang menawarkan "perpustakaan alat penyerang yang tersusun dengan baik yang dibungkus pada edaran Linux percuma untuk dimuat dan digunakan seperti Backtrack dan Kali" (Muniz et al. 2015) ancaman siber tidak lagi terkecuali tetapi lebih merupakan kenyataan harian dalam era teknologi hari ini. Sebagai tindak balas, organisasi sedang menyediakan kaedah baru untuk melindungi diri mereka dari serangan siber mereka sanggup melabur dalam alat canggih bagi mengimbas rangkaian dan melakukan penyumberan luar keselamatan siber kepada organisasi pihak ketiga. Selain itu, mereka juga menimbang untuk mewujudkan pusat operasi keselamatan (SOC) didalam premis.

Penggabungan Pusat Operasi Keselamatan (SOC) dalam organisasi mula menjadi popular dalam kalangan syarikat yang berfokus pada strategi. Mempunyai pasukan SOC adalah kepentingan utama dalam pengenalan dan pertahanan terhadap jenayah siber. Tanggungjawab utama yang berkaitan dengan pasukan adalah peningkatan pengesanan insiden keselamatan melalui pemantauan dan analisis aktiviti data secara berterusan, meminimumkan kerugian dengan mencegah pelanggaran yang merugikan perniagaan, meningkatkan kawalan dan menjaga imej organisasi.

McAfee, salah satu pemain yang berpengaruh dalam industri keselamatan ICT, menyatakan bahawa tanggungjawab SOC adalah "memantau, mengesan, dan mengasingkan insiden dan pengurusan produk keselamatan organisasi, peranti rangkaian, peranti pengguna akhir, dan sistem". Fungsi ini dilakukan sepanjang waktu (24/7), bertahan dari pencerobohan setiap saat sepanjang hari tanpa mengira jenis atau sumber serangan. Teknologi yang membantu mereka dalam operasi ini adalah rangkaian firewall, IPS, APT,WAF, sistem pengurusan acara, dan penyiapan yang mengumpulkan data dan memantau jaringan (SIEM).

Kerosakan (kebocoran maklumat) melalui serangan siber dengan menghantar e-mel untuk serangan yang disasarkan atau kelemahan laman web telah meningkat sejak beberapa tahun kebelakangan ini. Serangan siber yang bertujuan memperoleh wang secara haram melalui perisian hasad dan perisian tebusan perbankan juga semakin meningkat. Khususnya, serangan yang dikaitkan dengan organisasi jenayah siber profesional adalah semakin inovatif dan canggih, menjadikan langkah untuk menanganinya adalah amat sukar untuk dicapai.

Contohnya, produk tindakan balas jenis padanan corak seperti perisian antivirus, IDS dan IPS sering gagal dalam mengesan teknik serangan baharu dan perisian hasad, jadi ianya tidak berkesan terhadap serangan sehingga vendor produk mengedarkan tandatangan terkini *(signature update)* kepada mereka hanya selepas kerosakan dikesan dalam organisasi yang diserang. Pada 23 Disember 2015, tiga syarikat kuasa Ukraine telah diserang oleh penggodam yang berjaya mengganggu pengagihan tenaga di kemudahan pusat tersebut. Serangan itu menyebabkan kira-kira 225,000 pelanggan berada tanpa bekalan elektrik selama 1 hingga 6 jam pada pertengahan musim sejuk.

1.2 PERMASALAHAN KAJIAN

Mewujudkan SOC adalah menjadi penting kepada setiap organisasi supaya semua insiden keselamatan yang akan datang dapat dipantau dan ditangani dengan pantas dan efisien. SOC yang akan dibangunkan menurut Vielberth et al. (2020) mestilah menggabungkan tiga (3) elemen penting seperti Manusia, Proses dan Teknologi untuk menjadikan sesebuah SOC itu berkesan. Menurut Heartfield & Loukas (2018), dalam kajian mereka manusia adalah penyumbang utama kepada faktor

kegagalan keselamatan ICT (manusia adalah elemen yang terlemah) kerana banyak faktor yang menyumbang seperti kekurangan kemahiran, kecuaian, keletihan dan lain-lain yang berpunca dari kelemahan manusia. Oleh itu jika proses yang terbaik dan teknologi yang canggih juga tidak dapat membendung masalah dari ancaman siber dan kesalan manusia ini. Oleh itu, elemen manusia ini perlu diberi perhatian bagi menjadikan sesebuah SOC dapat berfungsi dengan baik dan berkesan.

Peranan dan tanggungjawab ahli pasukan SOC yang kurang jelas boleh mengakibatkan pengurusan sesebuah SOC itu berada dalam keadaan yang tidak teratur dan insiden tidak dapat di kesan dengan pantas dan berkesan. Peranan dan tanggungjawab menjadi amat penting untuk penganalisis dah Ahli pasukan SOC untuk mengekalkan standard keberkesanan dan prestasi operasi pada tahap yang tinggi kerana prestasi operasi yang lemah akan menghalang kecekapan keseluruhan sebuah SOC, (Enoch Agyepong, Yulia Cherdantseva, Philipp Reinecke & Pete Burnap, 2020)

Selain itu banyak SOC tidak mempunyai ahli yang mempunyai kemahiran dan tahap pendidikan yang tinggi. Pekara ini telah menjadi antara penyebab insiden siber tidak dapat dikesan dengan lebih awal dan menyebabkan kerugian kepada organisasi. Menurut. Schinagl, K. Schoon and R. Paans,(2015), setiap ahli pasukan SOC mestilah mereka yang mempunyai tahap pendidikan dan kemahiran yang tinggi, walau bagaimanapun, komuniti keselamatan masa kini menghadapi kekurangan yang serius bagi kakitangan yang berkemahiran tinggi dan berkelayakan.

Pusat operasi keselamatan tidak mempunyai bentuk standard dan model yang lengkap yang mengkhususkan peranan dan tanggungjawab, tahap pendidikan dan kemahiran serta kriteria yang diperlukan dalam sesebuah SOC, oleh itu projek ini akan menilai bagaimana SOC boleh dipertingkatkan lagi dari segi faktor manusia dan mengurangkan kesalahan manusia di dalam SOC supaya tahap keselamatan dapat ditingkatkan lagi, kebergantungan kepada pada satu jenis produk keselamatan, teknologi yang canggih serta proses yang mampan tidak dapat menjamin keberkesanan SOC jika manusia yang bekerja dan menguruskan SOC tidak diberi perhatian yang penuh dengan kemahiran, latihan dan pendidikan yang betul dan mencukupi serta mempunyai pengalaman yang luas.

1.3 PERSOALAN KAJIAN

Berdasarkan pernyataan masalah yang dinyatakan, persoalan kajian adalah seperti berikut:

1. Apakah (peranan dan tanggungjawab) ahli pasukan SOC ?
2. Apakah tahap pendidikan, sijil professional , pengetahuan dan kemahiran dalam bidang IT security yang diperlukan bagi ahli SOC?
3. Adakah wujud model matrik pemilihan ahli pasukan SOC yang memenuhi elemen manusia.

1.4 OBJEKTIF KAJIAN

Oleh itu, dalam kertas kajian ini akan membincangkan dan menumpukan kepada elemen seperti berikut :

1. Mengenal pasti peranan dan tangunjawab kumpulan ahli SOC.
2. Mengenal pasti tahap pendidikan, sijil professional, pengetahuan dan Kemahiran dalam bidang IT security yang diperlukan bagi ahli SOC
3. Mewujudkan model peranan dan tanggungjawab, tahap pendidikan serta kemahiran - SOC.

1.5 KEPENTINGAN KAJIAN

Kepentingan kajian ini dapat memberi faedah kepada organisasi sektor awam dan swasta yang merancang untuk membangunkan SOC sendiri. Selain itu, ia dapat membantu untuk meningkatkan kualiti pemilihan kakitangan atau pasukan SOC sedia ada melalui model ahli pasukan SOC yang akan dihasilkan kelak. Ianya juga dapat membantu organisasi memantapkan lagi tahap ketersediaan keselamatan ICT dengan adanya pasukan SOC yang cekap dan efisien.

Mengesan, mengesahkan, membetulkan insiden keselamatan di dalam SOC menjadi lebih mudah dengan adanya ahli pasukan yang mempunyai ciri-ciri yang bakal dibincangkan di dalam model ahli pasukan SOC di bab yang seterusnya.

1.6 SKOP

Skop dan kajian adalah seperti berikut:

a) Kajian ini hanya akan memfokuskan kepada faktor manusia didalam sesebuah SOC baharu atau sedia ada.
b) Kajian ini hanya memfokuskan 3 ahli pasukan SOC yang akan dibincangan.
c) Kajian ini menentukan apakah tahap pendidikan, kemahiran, interpersonal / sahsiah diri dan daya tahan ahli pasukan yang diperlukan.

1.7 STRUKTUR BAB

Disertasi kajian ini terbahagi kepada lima (5) bab seperti berikut:

a) **BAB I** terdiri daripada tentang pengenalan, penyataan masalah, objektif kajian, persoalan kajian, skop kajian dan kepentingan kajian.

b) **BAB II** mengandungi kajian kesusasteraan yang dibuat terhadap kajian terdahulu bagi menentukan jurang pengetahuan dan indikator faktor kajian dalam pemahaman berkaitan SOC, faktor manusia dan serangan siber termasuklah konsep asas dan terminologi, aspek kesediaan dan kajian lampau.

c) **BAB III** menerangkan metodologi kajian yang digunakan untuk mencapai objektif kajian dan juga menjawab persoalan kajian. Dalam bab ini perincian metodologi kajian merangkumi reka bentuk kajian, proses pengumpulan dan penentusahan maklumat, penganalisaan, kaedah pengiraan dan proses pengesahan model dan model kajian.

d) **BAB IV** menerangkan secara terperinci mengenai dapatan kajian bermula dengan analisis penentusahan pakar, analisis pengesahan dan penilaian model dan oleh pakar yang bagi mengesahkan keberkesanan model kajian.

e) **BAB V** merupakan kesimpulan kepada kajian yang akan dilaksanakan mengandungi perbincangan dan ulasan sebagai rumusan hasil kajian menerusi dapatan kajian, sumbangan kajian dan cadangan penambahbaikan kajian ini pada masa hadapan.

1.8 KESIMPULAN

Secara keseluruhannya, bab ini memberikan gambaran awal tentang kajian yang akan dilaksanakan. Manakala bagi objektif kajian yang telah diperincikan mengikut penyataan masalah di dalam bab ini. Persoalan kajian diharapkan akan dijawab berdasarkan analisis yang dilakukan ke atas data yang diperolehi daripada kajian kesusasteraan dan pakar.

Melalui kajian ini diharapkan dapat menghasilkan satu model peranan dan tanggungjawab, tahap pendidikan serta kemahiran ahli pasukan SOC dalam sesebuah organisasi supaya insiden siber dapat dikekang pada peringkat awal. Dengan adanya model ini dapat membantu pemilihan dan dapat mengurangkan kesalahan dan kecuaian manusia *(human error)* yang tidak disengajakan kerana ahli pasukan yang tidak kompeten dan bertanggungjawab. Hasil kajian ini juga diharap berupaya membantu meningkatkan imej organisasi dan meningkatkan tahap kepercayaan kepada pasukan keselamatan ICT melalui SOC yang mantap dengan pengurangan insiden.

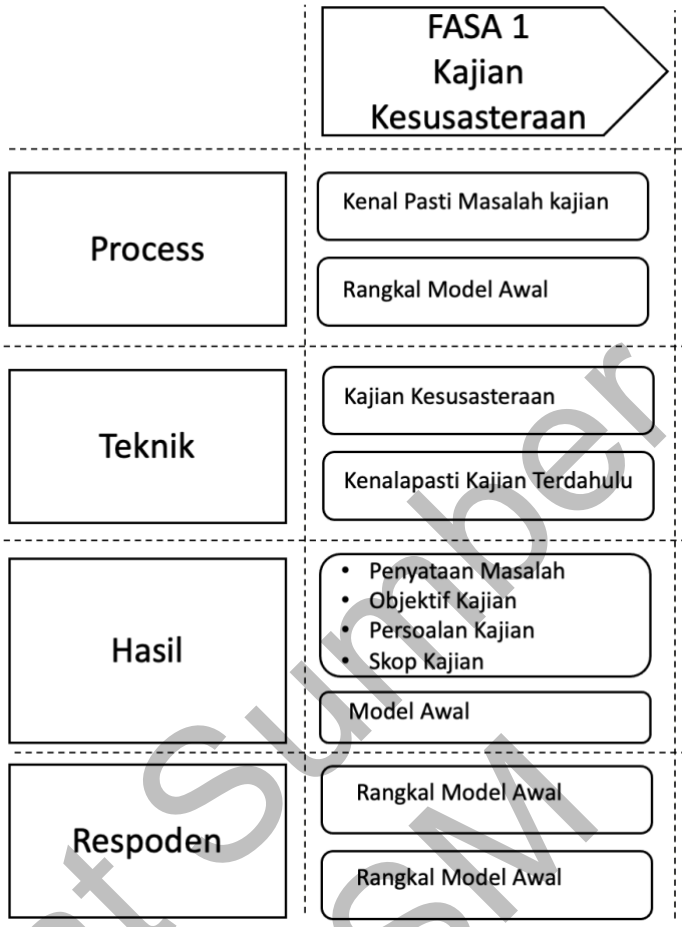
BAB II

KAJIAN LITERATUR

2.1 PENGENALAN

Bab ini membincangkan mengenai teori, model dan kajian terdahulu yang berkaitan dengan kajian ini. Teori, model dan dapatan kajian tersebut penting dan berguna untuk dijadikan asas dan panduan untuk lebih memahami permasalahan kajian. Melalui kajian kesusasteraan penyelidik dapat memahami, menilai dan mentafsir berdasarkan hasil penulisan oleh penyelidik terdahulu dan juga pengamal dalam bidang berkaitan dengan permasalahan yang dikaji melalui penelitian sistematik (Fink 2019).

Hasil kajian kesusasteraan ini akan dijadikan panduan dalam hasil kajian, perbandingan kajian dan seterusnya membangunkan model pasukan SOC. Pelaksanaan kajian kesusasteraan ini merupakan fasa pertama iaitu kajian awal. Dalam fasa ini proses yang terlibat adalah mengenal pasti masalah kajian seterusnya merangka model kajian ini. Perincian proses dalam fasa ini boleh dirujuk di Rajah 2.1.



Rajah 2.1 Proses fasa kajian kesusasteraan (kajian awal)

2.2 PUSAT KESELAMATAN OPERASI *(SOC)*

Pusat operasi keselamatan (SOC) ialah kemudahan yang menempatkan ahli pasukan keselamatan yang bertanggungjawab untuk memantau dan menganalisis aset ICT dan rangkaian keselamatan organisasi secara berterusan. Matlamat pasukan SOC adalah untuk mengesan, menganalisis dan bertindak balas terhadap insiden keselamatan siber menggunakan gabungan manusia, teknologi dan set proses yang berkesan. Pusat operasi keselamatan biasanya mempunyai kakitangan seperti pengurus SOC, penganalisis amaran, responden insiden dan *subject matter expert* (Tores 2015) yang melengkapkan pasukan ini. Ahli pasukan SOC harus bekerjasama rapat dengan pasukan yang lain dan saling melengkapi untuk memastikan isu keselamatan ditangani dengan cepat selepas sebarang penemuan amaran atau insiden. Menurut Os (2016) dalam kajiannya, SOC ialah entiti organisasi dimana elemen keselamatan operasi, seperti tindak balas insiden keselamatan, pemantauan keselamatan, analisis keselamatan, pelaporan keselamatan

dan pengurusan kelemahan, dipusatkan dan pekara ini lah yang menjadi tunjang sesebuah SOC yang beroperasi pada masa kini.

SOC juga merujuk kepada platform untuk mengesan dan bertindak balas terhadap insiden pencerobohan. Selain itu, SOC adalah tempat di mana penganalisis, pengendali, pengurus dan kakitangan lain memantau sistem maklumat, infrastruktur dan perkhidmatan (Onwubiko 2015). Seorang penyelidik lain menerangkan pusat operasi keselamatan sebagai "Pusat Perisikan Keselamatan." Ia menerangkan bahawa keupayaan pengumpulan data, pengecaman, pengesanan, dan keupayaan pemulihan adalah perlu sebagai elemen teknikal untuk mengendalikan pusat operasi keselamatan.

Kerentanan turut disemak dan dipantau oleh SOC supaya ianya berupaya untuk bertindak balas dan pulih daripada insiden dengan pantas yang juga disifatkan sebagai salah satu faktor teknikal yang penting dalam sesebuah SOC. Selain itu, istilah baharu yang dipanggil NSIC (Pusat Pintar Keselamatan Rangkaian) telah dicadangkan dengan menyepadukan SIC dengan NOC (Pusat Operasi Rangkaian) (Miloslavskaya 2018). SIEM (Maklumat Keselamatan dan Pengurusan Acara) diperkenalkan untuk menambah baik operasi keselamatan. Dengan menggunakan peralatan SIEM, acara keselamatan sebenarnya berniat jahat atau tidak, dan kemudahan perniagaan telah meningkat dengan banyak (Feng et al. 2017).

Salah satu alat yang penting yang perlu ada dalam SOC ialah SIEM (Maklumat Keselamatan dan Pengurusan Acara). SIEM adalah untuk mengesan amaran dan mencari penyelesaian keselamatan siber dan ianya berupaya untuk belajar daripada keseluruhan infrastruktur IT dan mengenal pasti anomali seperti serangan siber (Podzins et al. 2019). Selain itu, SOC juga turut membolehkan pengesanan insiden, penyiasatan dan keupayaan tindak balas yang lebih baik dengan menggunakan data daripada peranti titik akhir, log, sistem keselamatan dan aliran rangkaian (Janos & Nguyen 2018). Salah satu penyelesaian popular untuk mempertahankan diri daripada ancaman ini ialah dengan melaksanakan Pusat Operasi Keselamatan Siber (CSOC) untuk memantau, menjejak dan mengendalikan insiden siber (Abd Majid & Zainol Ariffi 2019).

Pengurusan data amaran ialah salah satu fungsi teratas yang dilakukan oleh Pusat Operasi Keselamatan Siber (CSOC) (Shah et al. 2019). Setiap amaran berisiko SOC memerlukan siasatan lanjut oleh penganalisis manusia. Makluman itu diuji menjadi makluman berkeutamaan tinggi, sederhana dan rendah, dan makluman keutamaan tinggi disiasat terlebih dahulu oleh penganalisis keselamatan siber suatu proses yang dikenali sebagai giliran keutamaan (Shah et al. 2019). SOC adalah kritikal apabila menentukan postur keselamatan siber organisasi kerana ia boleh digunakan untuk mengesan, menganalisis dan melaporkan pelbagai aktiviti berniat jahat (Mutemwa & Mouton 2018).

Salah satu cabaran utama SOC adalah untuk mengintegrasikan alat keselamatan dan aktiviti operasi dengan cepat (Chadni Islam et al. 2020). Purata organisasi bersaiz sederhana mencatatkan lebih kurang. 10 hingga 500 juta acara sehari pada sistem. Hanya kurang daripada 5% makluman ancaman sedang disiasat oleh kakitangan khusus, menjadikan lubang keselamatan terbuka untuk kemungkinan serangan (Seresht et al. 2020). Perintah dan kawalan dalam pusat operasi keselamatan dikuasai oleh pengalaman manusia, menunjukkan keperluan untuk sistem yang mengukuhkan kesedaran situasi bersama di seluruh organisasi (Mullins et al. 2020).

Pengurusan data makluman memerlukan beberapa tugas di Pusat Operasi Keselamatan Siber seperti tugas yang berkaitan dengan analisis amaran, tugas yang berkaitan dengan pengurangan ancaman jika amaran dianggap penting, kemas kini tandatangan untuk sistem pengesanan pencerobohan dan sebagainya (Ganesan & Shah 2018).

Memandangkan kajian faktor manusia dalam persekitaran siber masih sukar dilaksanakan, alatan dan amalan kolaboratif berkembang dengan perlahan dan latihan sentiasa diperlukan untuk meningkatkan kecekapan kerja berpasukan (Kabil et al. 2018). Log hos, khususnya, Log Acara Windows, adalah sumber maklumat berharga yang sering dikumpulkan oleh pusat operasi keselamatan (SOC). Walaupun banyak algoritma yang berkuasa untuk menganalisis data siri masa dan berjujukan wujud, penggunaan algoritma sedemikian untuk kebanyakan aplikasi keselamatan siber adalah tidak boleh dilaksanakan (Verma & Bridges 2018).

Malangnya, syarikat bersaiz kecil hingga sederhana, yang biasanya tidak mampu mengupah pakar keselamatan yang berdedikasi, berminat untuk mendapat manfaat daripada Perkhidmatan Keselamatan Terurus (MSS) yang disediakan oleh Pusat Operasi Keselamatan (SOC) pihak ketiga untuk menangani ancaman seluruh rangkaian (Khalili et al. 2015). Bilangan dan keterukan ancaman keselamatan siber yang semakin meningkat, digabungkan dengan kekurangan penganalisis keselamatan yang mahir, telah membawa kepada peningkatan tumpuan pada penyelidikan keselamatan siber (DeCusatis et al. 2019). Terdapat banyak pembinaan pusat operasi keselamatan (SOC) untuk melindungi daripada serangan siber. Model Kawalan Keselamatan Dipertingkat (ESC) dengan proses Pengutamaan Penyekatan (BP) untuk infrastruktur kritikal adalah untuk menambah baik aktiviti tindak balas insiden harian (Han et al. 2019).

2.3 ANCAMAN KESELAMATAN ORGANISASI

Terdapat banyak ancaman keselamatan pada masa ini yang memerlukan pemantauan, pengesanan dan pembaikan dengan segera. Justeru, jika dilengahkan boleh mendatangkan impak yang negatif kepada organisasi seperti kehilangan data dan menjejaskan imej organisasi yang baik. Pada Januari 2018, Agensi Kesatuan Eropah untuk Rangkaian dan Keselamatan Maklumat (ENISA) mengeluarkan laporan tentang arah aliran ancaman 2017. Perisian hasad ialah ancaman keselamatan kepada individu yang berbahaya yang dapat merosakkan data yang disimpan. Perisian hasad ialah perisian yang menjadi punca awal untuk pelbagai jenis perisian berbahaya. Contohnya, perisian tebusan ialah sejenis perisian hasad yang menyulitkan fail mangsa dan memerlukan bayaran untuk menyahsulit fail tersebut. Perisian intip sebaliknya mengumpul maklumat tentang mangsa dan menghantarnya kepada pihak ketiga tanpa pengetahuan mangsa. Vektor serangan utama untuk perisian hasad biasanya pancingan data dan mengeksploitasi kelemahan yang diketahui (Brewster & Fobis 2017).

Pancingan bermaksud pihak yang berniat jahat cuba mendapatkan maklumat sensitif daripada sasaran dengan menghantar e-mel atau mesej yang meniru perkhidmatan yang sah seperti tapak web (Khonji et al. 2013). Serangan berasaskan web adalah risiko kedua terbesar bagi organisasi dan melibatkan organisasi yang menghoskan aplikasi web yang boleh dicapai daripada Internet. Serangan aplikasi web

kebanyakannya digunakan oleh penyerang untuk mendapatkan maklumat sulit seperti data pelanggan atau untuk memanfaatkan akses mereka ke dalam rangkaian dalaman. Contoh serangan aplikasi web ialah musuh yang mengeksploitasi kelemahan dalam aplikasi pelayan web (Hilton 2016).

Ancaman lain termasuk serangan Penafian Perkhidmatan (DoS) dan ancaman orang dalam. Serangan DoS bertujuan menjadikan sasaran tidak tersedia untuk pengguna yang dimaksudkan. Penafian Perkhidmatan Teragih (DDoS) ialah variasi serangan, yang mana trafik datang dari pelbagai sumber seperti penyerang boleh menjejaskan peranti yang kurang selamat untuk mencipta botnet yang boleh digunakan untuk melancarkan serangan DDoS besar-besaran (European Union Agency for Network and Information Security 2018).

Ancaman melalui manusia boleh menyebabkan kebocoran data peribadi syarikat kepada umum hingga dan berlaku kerosakan seperti gangguan perkhidmatan kritikal dengan sengaja (European Union Agency for Network and Information Security 2018). Rajah 2.2 menyenaraikan 15 jenis ancaman keselamatan siber teratas pada 2016 dan 2017. SOC yang matang mampu mengesan semua ancaman dan dapat mengurangkan kerosakan, kecurian dan kehilangan data.

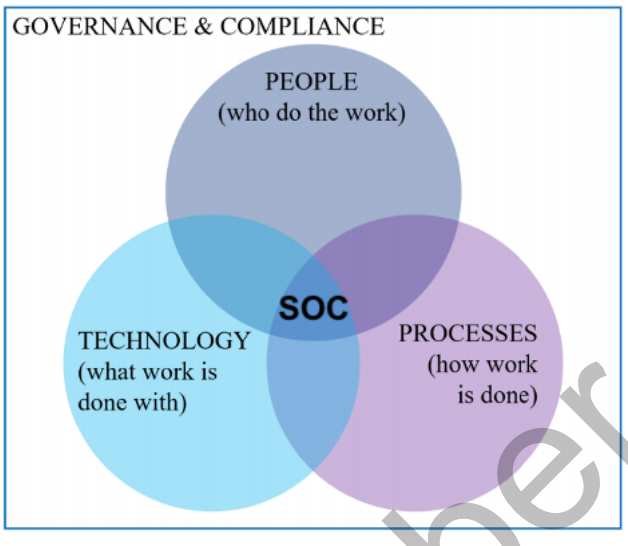
Top Threats 2016	Assessed Trends 2016	Top Threats 2017	Assessed Trends 2017	Change in ranking
1. Malware	↑	1. Malware	→	→
2. Web based attacks	↑	2. Web based attacks	↑	→
3. Web application attacks	↑	3. Web application attacks	↑	→
4. Denial of service	↑	4. Phishing	↑	↑
5. Botnets	↑	5. Spam	↑	↑
6. Phishing	→	6. Denial of service	↑	↓
7. Spam	↓	7. Ransomware	↑	↑
8. Ransomware	→	8. Botnets	↑	↓
9. Insider threat	→	9. Insider threat	→	→
10. Physical manipulation/damage/ theft/loss	↑	10. Physical manipulation/damage/ theft/loss	→	→
11. Exploit kits	↑	11. Data breaches	↑	↑
12. Data breaches	↑	12. Identity theft	↑	↑
13. Identity theft	↓	13. Information leakage	↑	↑
14. Information leakage	↑	14. Exploit kits	↓	↓
15. Cyber espionage	↓	15. Cyber espionage	↑	→

Legend: Trends: ↓ Declining, → Stable, ↑ Increasing
Ranking: ↑Going up, → Same, ↓ Going down

Rajah 2.2 Membandingkan 15 Ancaman Siber Teratas Pada Tahun 2016 Dan 2017 Side-By-Side (European Union Agency for Network and Information security 2018).

2.4 FUNGSI DAN PERANAN PUSAT KESELAMATAN OPERASI *(SOC)*

Pusat Operasi Keselamatan (SOC) boleh menyediakan penyelesaian menyeluruh bagi mengesan dan mengurangkan serangan jika dilaksana dengan betul. SOC menggabungkan manusia, proses, teknologi, dan tadbir urus dan pematuhan, untuk mengenal pasti, mengesan dan mengurangkan ancaman secara berkesan, secara ideal sebelum sebarang kerosakan berlaku. Vielberth et al. (2020), seperti rajah 2.3.



Rajah 2.3 Manusia, Proses dan Teknologi, Tadbir Urus & rangka kerja pematuhan
Sumber : Vielberth et al. 2020

SOC juga berfungsi sebagai sebuah pasukan mahir yang beroperasi dengan proses serta disokong oleh teknologi pemantauan keselamatan bersepadu seperti SIEM. SOC secara khusus memfokuskan kepada pemantauan ancaman siber, penyiasatan forensik, dan pengelolaan serta pelaporan insiden di bawah persekitaran operasi keselamatan keseluruhan dengan sokongan eksekutif yang jelas (Schinagl et al. 2015). Tanpa sokongan seperti itu, SOC tidak berkesan, dan nilainya tidak dapat direalisasikan.

Sebahagian besar fungsi SOC difokuskan pada infrastruktur teknikal, dengan jaringan, sambungan luaran, automasi pejabat, penyelesaian mudah alih dan pelayan yang menjalankan aplikasi dan memproses data. SOC melakukan pemantauan berterusan, imbasan kerentanan, imbasan pematuhan, pengumpulan data log dan lain-lain.

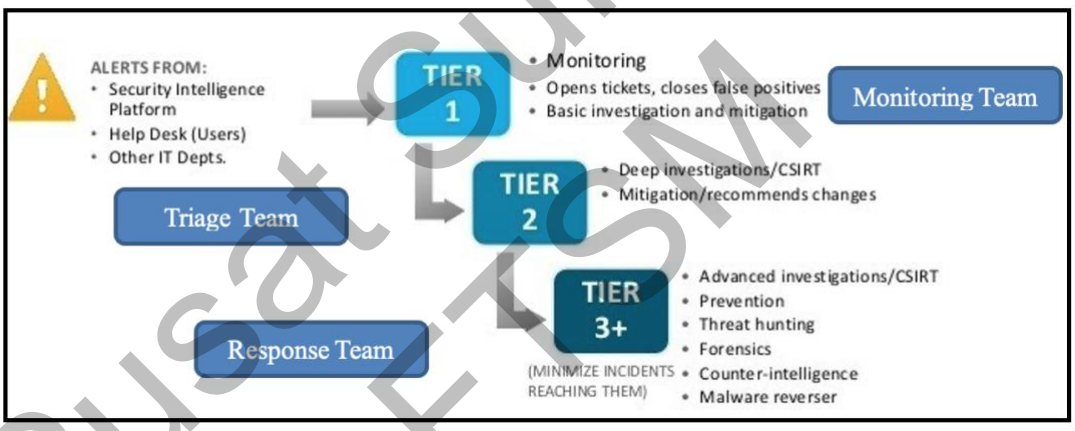
Selain itu, SOC juga turut menganalisis data dilakukan secara automatik atau sebahagiannya secara automatik, menggunakan alat analitik berbantukan komputer. Manusia cenderung menjadi keliru apabila mengendalikan sejumlah besar maklumat bertulis, jadi adalah penting untuk membayangkan data dalam bentuk gambar, carta atau corak. Seorang penganalisis SOC boleh menggunakan maklumat yang dibayangkan untuk membina gambaran keseluruhan keselamatan dengan cepat (Zimmerman 2014). Di samping itu, visualisasi membantu dalam analisis trend.

Kesedaran situasi adalah penting untuk unit SOC kerana ia membolehkan tindak balas dengan cepat, apabila unit SOC menemui ancaman baharu.

Pembuatan keputusan berlaku berdasarkan pengetahuan yang diperoleh melalui pemerhatian dan orientasi serta analisis data yang diperoleh dari sistem dan juga manusia seperti penganalisis amaran dan responder insiden. Selepas penganalisis membuat keputusan, mereka bertindak sewajarnya bagi menyekat insiden menjadi lebih serius. Oleh itu pasukan SOC harus sentiasa berada dalam keadaan sedar dengan situasi semasa dan boleh dibahagikan kepada tiga bahagian yang sama penting: rangkaian, misi dan ancaman. Ketiga-tiga bahagian mesti dipertimbangkan oleh SOC bagi membuat keputusan yang tepat. SOC harus mengetahui kuantiti, jenis dan lokasi semua aset ICT yang disambungkan ke rangkaian organisasi. Di samping itu, SOC harus mengetahui topologi rangkaian, termasuk fizikal dan logik, dan kemungkinan kelemahan dalam peranti serta dihubungkaitkan oleh responden insiden bagi mencari ancaman dan serangan yang telah atau akan berlaku kepada organisasi ini. SOC juga turut melihat dari segi misi dan misi ini ditakrifkan bagaimana cara organisasi berinteraksi dengan pihak lain. Bahagian ancaman pula termasuk motif utama musuh, keupayaan dan kemahiran mereka. Ia juga perlu untuk menekankan kepentingan menyedari motif dan niat penyerang, kerana ia membuat perbezaan yang ketara, sama ada organisasi mempertahankan diri terhadap apa yang dipanggil skrip kiddies atau penyerang tajaan kerajaan (Cole 2017). Skrip kiddie ialah penyerang dengan tahap kemahiran yang agak rendah, tetapi yang boleh memuat turun perisian mengeksploitasi yang dibangunkan oleh penggodam lain, untuk menyerang organisasi (Carlo 2003). Oleh itu, keputusan dari segi kemanusiaan dalam bentuk keinginan kekayaan, kepopularan atau ancaman dengan niat haruslah dipastikan oleh pasukan SOC.

SOC kebiasaannya dikendalikan berdasarkan Maklumat Keselamatan dan Sistem pengurusan atur cara (SIEM) (Ab Rahman & Choo 2015). Menurut Janos & Nguyen (2018), dalam persekitaran sesebuah organisasi yang mempunyai SOC, terdapat tiga peringkat peranan yang berbeza dalam pengurusan pasukan operasi SOC iaitu yang saling berkaitan antara satu sama lain seperti dalam rajah 2.4. Pasukan pemantau*(monitoring Team)* kumpulan pertama (penganalisis amaran) bertanggungjawab untuk mendapatkan data dan maklumat yang tepat yang bertujuan

untuk mengenal pasti amaran dan amaran positif palsu untuk ditangani oleh pasukan yang lebih berpengalaman. Pasukan Triage *(Triage Team)* adalah tahap kedua (responden insiden) dimana penganalisisan proses dalam menyiasat dan insiden yang dikenal pasti samada kejadian tersebut berbahaya atau tidak dan perlu diselesaikan dengan apa saja kaedah yang sesuai mengikut kemahiran dan pengalaman mereka. Seterusnya proses mengendalikan insiden ini kepada pasukan yang seterusnya dengan setiap maklumat yang diperlukan dengan lengkap. Peranan utama pasukan respons *(Respons Team)* ini adalah menyiasat dan menyelesaikan masalah atau mengurangkan kesannya dengan memutuskan pengasingan peranti yang mencurigakan atau perisian hasad yang dikeluarkan atau bertindak memulihkan stesen kerja yang dijangkiti. Selain itu, mereka akan menyampaikan perkara ini kepada pihak pengurusan yang selalunya akan dibuat oleh pengurus SOC.



Rajah 2.4 Peranan tiga (3) peringkat Pengurusan SOC dan Tanggungjawab berkaitan

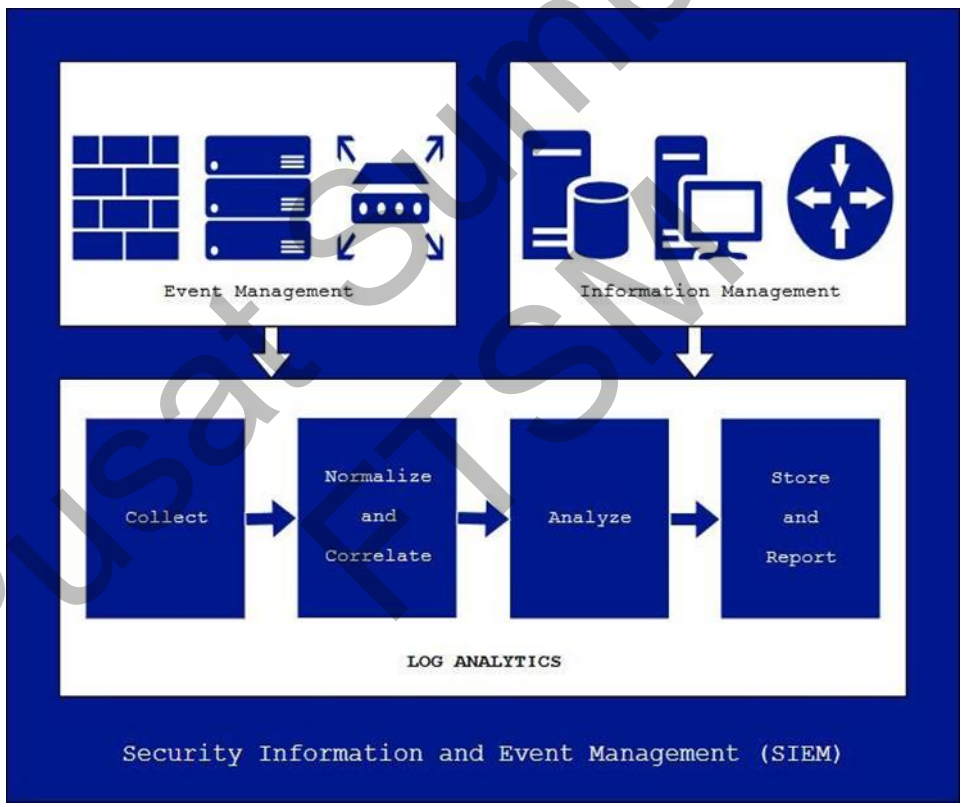
Sumber : Janos & Nguyen 2018

2.5 PERALATAN UTAMA SOC – SIEM

Insiden Keselamatan dan Sistem Pengurusan Acara (SIEM) ialah salah satu alat yang paling berharga, utama dan penting untuk SOC. Sistem SIEM berbeza daripada sistem pengurusan log tradisional dengan menambahkan beberapa ciri berkaitan keselamatan, seperti korelasi peristiwa dan keupayaan analisis. SIEM menggabungkan dua konsep, Pengurusan Acara Keselamatan (SEM) dan Pengurusan Maklumat Keselamatan (SIM). Sistem SIM mengumpul data berkaitan keselamatan daripada sumber yang berbeza

pada rangkaian dan menyimpan data di satu lokasi pusat. Selain mengumpul data, sistem MIS mampu menjana laporan dan melakukan analisis sejarah.

Sistem SEM sebaliknya, menyediakan keupayaan pemantauan masa nyata yang digunakan untuk memantau data yang di kumpul daripada pelbagai sumber oleh komponen MIS. Sistem SEM adalah cekap dalam analisis masa nyata dan korelasi peristiwa. Di samping itu, sistem SEM bertanggungjawab untuk memaklumkan penganalisis apabila peraturan dicetuskan (Sornalakshimi 2017). Seni bina peringkat tinggi sistem SIEM yang menggabungkan keupayaan sistem SIM dan SEM ditunjukkan dalam Rajah 2.5.



Rajah 2.5 Menyatukan SEM dan SIM ke dalam SIEM untuk pengurusan berpusat (Sornalakshimi 2017)

2.5.1 Mengumpul data log

Sistem SIEM boleh mengumpul data log daripada pelbagai sumber yang termasuk, tetapi tidak terhad kepada stesen kerja, pelayan, peranti rangkaian seperti penghala dan suis, tembok api, WAF, APT, IDS dan IPS. Secara amnya, mana-mana peranti yang

menghasilkan atau memproses data berkaitan keselamatan boleh ditarik lognya ke dalam SIEM. Sistem SIEM menggunakan pengumpul log untuk penarikan data keselamatan ke dalam unit berpusat utama. Pengumpul log boleh sama ada perisian atau perkakas perkakasan, bergantung pada produk dan vendor (Sekharan & Kamalanathan 2017).

Biasanya pengumpul log boleh dipasang secara berpusat, supaya menerima data menggunakan contohnya protokol syslog. Syslog ialah protokol piawai untuk mendapatkan log peristiwa. Syslog menyediakan format piawai dalam bentuk mesej log yang menggunakan protokol ditakrifkan dalam dokumen RFC 5424 (Gerhards 2009). Sebuah organisasi mungkin mempunyai berbilang pengumpul log yang bertindak sebagai pelayan syslog secara serentak. Oleh itu, organisasi tidak perlu memasang ratusan atau bahkan ribuan pengumpul log perisian pada peranti titik akhir dengan adanya SIEM ini.

2.5.2 Normalisasi

Normalisasi data adalah penting apabila bekerja dengan data log dari pelbagai sumber kerana ia haruslah menukar semua data kepada format yang konsisten. Vendor dan produk yang berbeza menggunakan pelbagai format log dalam mesej log mereka. Normalisasi data adalah penting untuk sistem SIEM, kerana SIEM akan dapat melakukan analisis korelasi dalam persekitaran pelbagai produk disamping rangkaian organisasi mungkin mengandungi ratusan atau bahkan ribuan sumber log yang berbeza. Kebanyakan produk SIEM boleh memproses format log umum dan boleh menormalkan data daripada lebih 500 peranti berbeza (Micro Focus 2018).

Di samping itu, pengguna boleh menulis penghuraian tersuai yang menormalkan mesej log kepada bentuk tertentu. (Bonilla 2017). Format penormalan data berbeza antara vendor. Matlamat utama penormalan mesej adalah untuk menukar data daripada vendor dan peranti yang berbeza kepada bentuk yang homogen. Sebagai contoh, ArcSight menggunakan Format Acara Biasa (CEF) dalam SIEM mereka. Beberapa format seperti CEF boleh disesuaikan untuk memasukkan maklumat tertentu yang biasanya tidak akan disertakan dalam mesej. CEF termasuk awalan syslog yang terdiri daripada cap masa dan nama hos peranti yang menjana log.

Oleh itu, mesej CEF termasuk maklumat tentang versi CEF yang digunakan, vendor, produk peranti, versi peranti, ID tandatangan, nama, keterukan dan medan sambungan. Contoh mesej CEF daripada dokumen standard CEF dibentangkan dalam Rajah 2.6. Peranti keselamatan yang dipanggil threatmanager berjaya menghentikan perisian hasad worm dan keterukan kejadian 10. Mesej itu juga termasuk tiga sambungan: alamat IP sumber (src), alamat IP destinasi (dst) dan port sumber (spt). (Bonilla 2017).

```
Sep 19 08:26:10 host CEF:0|security|threatmanager|1.0|100|worm
successfully stopped|10|src=10.0.0.1 dst=2.1.2.2 spt=1232
```

Rajah 2.6 Contoh Mesej CEF (Bonilla 2017).

Ketepatan data masa dan tarikh dalam mesej log adalah penting. Sistem SIEM tidak dapat melaksanakan korelasi dan analitik dengan betul jika log mempunyai cap masa yang salah. Organisasi biasanya menggunakan pelayan *Network Time Protocol (NTP)* terpusat, untuk menyeragamkan jam antara semua peranti. Penggunaan pelayan NTP adalah wajib apabila mengumpul dan menganalisis data log supaya SIEM dapat berfungsi dengan tepat mengikut tarikh dan masa insiden berlaku.

2.5.3 Set peraturan dan korelasi peristiwa

Mengesan pencerobohan menggunakan hanya satu sumber log boleh menjadi sukar tetapi apabila maklumat itu digabungkan dengan log dari sumber lain, serangan yang lebih tersembunyi dapat dikesan. Korelasi bermakna data keselamatan disambungkan dan dibandingkan antara peranti yang berbeza dan juga jenis peranti. Sistem SIEM biasanya mempunyai peraturan korelasi yang telah dibuat secara lalai *(default)* , tetapi ia biasanya tidak mencukupi. Menurut Crawley, contoh peraturan korelasi boleh menjadikan sistem SIEM menaikkan amaran jika lima percubaan log masuk menggunakan nama pengguna berbeza dilakukan dari alamat IP yang sama dalam masa lima belas minit, diikuti dengan log masuk yang berjaya berlaku dari alamat IP sumber yang sama ke mana-mana mesin dalam rangkaian (Crawley 2018).

Peraturan contoh ini akan digunakan untuk mengesan serangan yang berbahaya terhadap perkhidmatan log masuk ke mana-mana sistem organisasi. Enjin korelasi

sistem SIEM boleh dibahagikan kepada tiga kategori. Enjin berasaskan persamaan berfungsi dengan membandingkan peristiwa sambil cuba mencari persamaan di dalamnya. Algoritma cuba menghimpunkan peristiwa ke dalam kumpulan mengikut persamaan. Enjin korelasi berasaskan persamaan tidak memerlukan maklumat tepat tentang jenis serangan yang berbeza, kerana ia semata-mata mencari persamaan. Kolerasi berasaskan pengetahuan membandingkan peristiwa dengan set peraturan.

Enjin berasaskan pengetahuan bergantung pada set peraturan yang sangat tepat yang mesti sentiasa dikemas kini untuk kekal relevan. Biasanya set peraturan mesti dibuat setiap serangan. Enjin korelasi statistik cuba mencari persamaan dengan peristiwa lama dan baharu (Sekharan & Kamalanathan 2017). Algoritma korelasi statistik biasanya menggunakan beberapa bentuk pembelajaran mesin untuk membina pemahaman tentang aktiviti biasa pada rangkaian.

Membangunkan peraturan untuk SIEM memerlukan ketepatan dan kepakaran yang tinggi kerana peraturan yang terlalu terperinci mungkin terlalu sempit untuk menimbulkan sebarang makluman, manakala peraturan yang terlalu umum menyebabkan banyak positif palsu yang mengurangkan kecekapan SOC. Mencipta peraturan SIEM adalah tugas yang memakan masa kerana peraturan mesti diuji dengan teliti, supaya dapat dipastikan bahawa peraturan tidak menyebabkan terlalu banyak positif palsu atau negatif palsu. Tambahan pula, peraturan mesti sentiasa dikemas kini agar sepadan dengan aliran ancaman semasa. Peraturan sistem SIEM mesti disesuaikan untuk setiap persekitaran yang bermaksud bahawa peraturan yang sama yang berfungsi dalam persekitaran mungkin tidak berfungsi dalam persekitaran yang lain (Crawley 2018).

2.5.4 Pemantauan dan pelaporan

Sistem SIEM diuruskan daripada antara muka pengguna berasaskan web atau program konsol yang dipasang secara tempatan yang bersambung kepada SIEM. Antara muka pengguna ini digunakan untuk mengkonfigurasi dan memantau SIEM serta menganalisis peristiwa keselamatan. Sistem SIEM biasanya termasuk ciri visualisasi yang boleh digunakan untuk membentuk gambaran situasi persekitaran dengan cepat. Selain itu, penganalisis SOC boleh menggunakan pertanyaan carian untuk mencari data

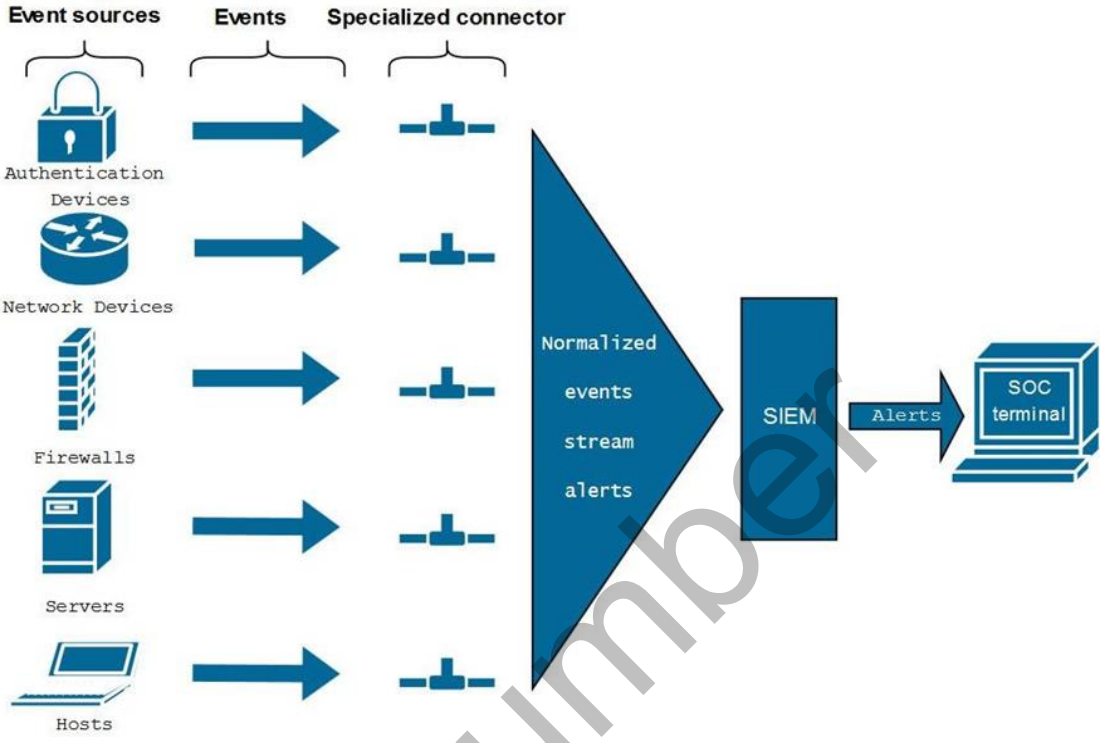
tambahan kerana penormalan dan fungsi carian yang sama boleh merentasi peranti dan perkhidmatan dari sumber yang berbeza. Semua sistem SIEM utama, termasuk pelaporan sokongan IBM QRadar, Micro Focus' ArcSight, Splunk dan Log Rhythm boleh dilakukan (Sekharan & Kamalanathan 2017).

Pelaporan ini amat berguna kerana SOC mesti dapat membuktikan nilainya kepada organisasi. Sistem SIEM boleh dikonfigurasikan untuk menjana dan menghantar laporan secara automatik pada selang masa yang tetap. Sebagai contoh, pengurus pasukan SOC mungkin ingin menerima laporan harian yang mengandungi maklumat 24 jam terakhir. Pengurus mungkin berminat dengan bilangan makluman yang dijana oleh SIEM dan masa yang diambil oleh penganalisis untuk bertindak balas kepada makluman (Jon et al. 2017). Laporan arah aliran, sebaliknya boleh digunakan untuk mengenal pasti arah aliran yang muncul dalam makluman dan ancaman keselamatan.

2.5.5 Makluman (*alert*)

Masa adalah penting dalam keselamatan siber dan unit SOC mesti dapat bertindak balas dengan cepat apabila mereka menyedari ancaman. Sistem SIEM dikonfigurasikan untuk meningkatkan amaran apabila syarat tertentu dipenuhi. Makluman biasanya boleh dikonfigurasikan dalam pelbagai cara. Sebagai contoh, makluman boleh dinaikkan ke dalam konsol sistem SIEM atau makluman boleh dihantar melalui e-mel atau mesej teks. Sesetengah sistem SIEM juga mampu untuk menolak makluman terus ke dalam sistem *ticketing* atau aplikasi tersuai menggunakan antara muka pengaturcaraan aplikasi (API). API memudahkan proses penyepaduan sistem SIEM dengan infrastruktur sedia ada.

Sebagai contoh, banyak syarikat IT menggunakan sistem tiket untuk mengatur tugas kerja. Mengintegrasikan sistem tiket dengan SIEM secara automatik adalah amat berguna jika tidak penganalisis SOC perlu mengeluarkan tiket secara manual. Fungsi utama sistem SIEM ditunjukkan dalam Rajah 2.7.



Rajah 2.7 Fungsi Utama Sistem SIEM (Bhatt et al. 2015).

Secara kesimpulannya, SIEM adala peralatan utama dalam sesebuah SOC, walaubagaimanapun mengoperasikannya adalah kompleks dan memerlukan kemahiran, pengetahuan dan motivasi yang tinggi untuk digunakan oleh ahli pasukan SOC. Oleh itu, latihan yang khusus dan secara berkala dapat meningkatkan tahap pengoperasian sistem SIEM ini oleh ahli pasukan SOC.

2.6 STRUKTUR SOC

Unit SOC perusahaan disusun di sekeliling sistem SIEM. Penganalisis SOC memantau sistem SIEM untuk aktiviti dan peristiwa yang mencurigakan. Seperti kebanyakan unit IT yang lain, unit SOC selalunya terdiri daripada pelbagai peringkat penganalisis yang mempunyai tanggungjawab yang berbeza. Biasanya penganalisis peringkat tinggi lebih berpengalaman dan pakar dalam menyiasat peristiwa kompleks. Penganalisis tahap terendah, biasanya dirujuk sebagai peringkat 1, memantau sistem SIEM untuk makluman.

Apabila amaran dinaikkan, penganalisis peringkat 1 memutuskan sama ada amaran itu positif benar atau positif palsu. Positif sebenar yang disyaki kemudiannya

ditingkatkan kepada penganalisis peringkat lebih tinggi, yang melakukan penyiasatan lebih mendalam untuk memahami punca amaran itu. Penganalisis peringkat tinggi mungkin mempunyai capaian yang lebih luas kepada sistem keselamatan dan alatan untuk penyiasatan lanjut (Krebs 2016). Berbilang positif palsu daripada peraturan yang sama mungkin membayangkan bahawa peraturan itu memerlukan konfigurasi selanjutnya. Penganalisis kanan, atau jurutera SOC yang berasingan, bertanggungjawab mengubah suai peraturan supaya ia tidak menyebabkan banyak positif palsu. Di samping itu, jurutera SOC membangun dan menyelenggara infrastruktur unit SOC supaya penganalisis boleh memberi tumpuan untuk mencari ancaman (Bhatt et al. 2015).

Unit SOC yang mempunyai kurang sumber biasanya mempunyai satu atau dua lapisan penganalisis. Ini bermakna seorang penganalisis tunggal mungkin bertanggungjawab untuk keseluruhan kitaran hayat ancaman daripada pengesanan awal hingga pembasmian akhir. Dalam unit SOC yang kecil, adalah penting bahawa penganalisis berpengalaman dan cekap. Bilangan peringkat penganalisis yang lebih rendah meningkatkan tanggungjawab untuk penganalisis tunggal. Selain membina dan mengekalkan gambaran situasi, beberapa unit SOC melaksanakan forensik digital dan tindak balas insiden (DFIR). DFIR diperlukan apabila insiden telah berlaku. Tindak balas insiden tertumpu pada menormalkan keadaan selepas insiden supaya organisasi dapat meneruskan perniagaan harian mereka.

Jika penyerang telah berjaya menceroboh rangkaian, tugas utama seorang responder insiden adalah untuk membersihkan sistem dan memastikan bahawa semua kemungkinan pintu belakang yang dicipta oleh penyerang dialih keluar. Pintu belakang biasanya perisian yang mencipta sambungan berterusan kembali kepada penyerang supaya mereka boleh mengakses sistem yang dilanggar selepas itu dan memindahkan data ke sana ke mari. Forensik digital digunakan untuk mengumpul sebanyak mungkin maklumat tentang kejadian itu. Maklumat yang di kumpul biasanya digunakan sebagai bukti undang-undang terhadap penyerang.

Sekiranya berlaku pelanggaran data, forensik digital digunakan untuk membentuk pemahaman tentang data yang boleh diperolehi oleh penyerang. Selain itu,

forensik digital boleh digunakan jika terdapat sebab untuk mengesyaki ancaman orang dalam. Sebagai contoh, pasukan forensik digital boleh menyiasat jika bekas pekerja telah mencuri sebarang data sensitif.

2.7 JUMLAH DATA YANG BERTAMBAH

Jumlah data berkaitan keselamatan yang dijana setiap hari oleh peranti pengkomputeran hanya meningkat. Hampir semua tindakan yang dilakukan pada peranti pengkomputeran menjana data log. Contohnya, memuatkan halaman web pada peranti titik akhir seperti komputer riba menghasilkan berbilang log merentas banyak peranti. *Firewall*, sebagai contoh, memutuskan sama ada paket harus dimajukan atau digugurkan bergantung pada peraturan aktif. Di samping itu, komputer riba dan AV yang berjalan padanya menghasilkan berbilang log. Mesej log ini dihantar ke dalam SIEM yang mengaitkan dan menganalisisnya.

Bilangan peristiwa yang dihantar ke sistem SIEM biasanya diukur dalam EPS (peristiwa sesaat). Sistem SIEM boleh memproses sejumlah besar acara dalam tempoh masa yang singkat. Sebagai contoh, SIEM *Micro Focus*, Pengurus Keselamatan Perusahaan ArcSight (ESM) mampu memproses sehingga 100,000 EPS dalam masa nyata (Bonilla 2017). Menganalisis sejumlah besar data memakan masa. Menurut Zimmerman (2014), SOC yang besar boleh mengumpul, menganalisis dan menyimpan puluhan atau ratusan juta acara berkaitan keselamatan setiap hari (Bonilla 2017).

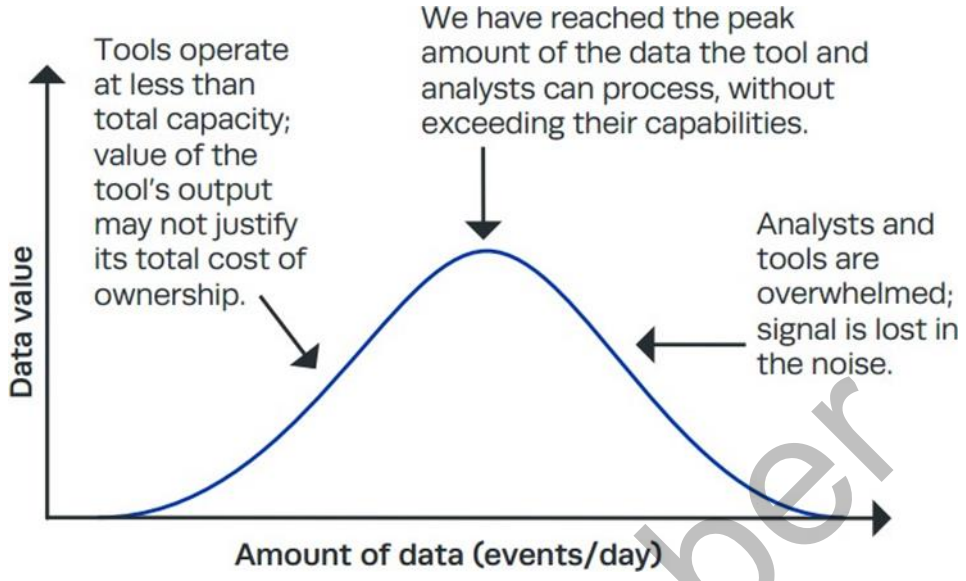
Kebanyakan peristiwa dalam rangkaian sentiasa tidak berbahaya, jadi SOC mesti mengasingkan dan mengutamakan peristiwa yang menunjukkan ancaman keselamatan. Mencari ancaman sebenar boleh menjadi hampir seperti mencari jarum dalam timbunan jerami. Unit SOC mesti cuba mengekalkan kelantangan bunyi sekecil mungkin untuk mengekalkan tumpuan kepada ancaman sebenar. Menggunakan alat yang sensitif dan tepat adalah perlu, kerana tanpanya penganalisis akan terharu dengan bilangan peristiwa. Tidak semua data semestinya sama penting. Dalam keselamatan siber, maklumat mempunyai pelbagai parameter yang mesti dinilai.

Ketepatan data adalah penting kerana alat automatik dan penganalisis manusia mungkin melakukan tindakan yang salah jika data yang tersedia tidak betul. Walaupun

sesetengah peristiwa dalam rangkaian memerlukan tindakan segera, penganalisis tidak dapat mengesan dengan lebih pantas kerana data yang dipaparkan adalah tidak tepat. Contohnya, perisian hasad yang merebak dengan cepat memerlukan penganalisis bertindak pantas untuk meminimumkan kerosakan dengan menganalisis data dan peristiwa yang tepat. Mengesan imbasan port pada perkhidmatan yang menghadap ke Internet organisasi, seperti pelayan web mungkin tidak memerlukan tindakan segera kerana pengimbasan port berlaku sering berlaku di Internet yang menyebabkan data yang diperolehi harus ditapis terlebih dahulu.

Sudah tentu, dalam kedua-dua kes penganalisis mesti menyiasat makluman untuk menilai risiko. Dalam persekitaran pusat operasi keselamatan, ketepatan amaran boleh diterangkan dengan negatif atau positif. Salah tafsir maklumat boleh mendatangkan akibat yang besar. Sebagai contoh, jika penganalisis SOC memutuskan bahawa amaran adalah positif palsu kerana maklumat yang tidak mencukupi atau salah, manakala amaran itu benar-benar positif benar, tafsiran yang salah boleh membawa kepada pelanggaran keselamatan. Negatif palsu adalah masalah untuk unit SOC, tetapi positif palsu menimbulkan ancaman yang lebih besar.

Apabila menganalisis data berkaitan keselamatan, jumlah data yang didapati mesti dipertimbangkan, kerana terlalu sedikit data akan menjejaskan ketepatan analisis, manakala terlalu banyak data akan mengakibatkan bebanan yang lebih kepada penganalisis dan alat yang digunakan. Oleh itu, alat yang berasaskan anomali yang bercirikan garis asas untuk aktiviti normal diperlukan. Membina garis dasar adalah sukar jika tidak ada data yang mencukupi untuk dianalisis (Mansfield-Devine 2016). Rajah 2.8 menjelaskan lagi sebab-sebab mengapa jumlah data yang dikumpulkan mesti dinilai, supaya jumlah dan nilai data adalah seimbang.



Rajah 2.8 Mengimbangi Jumlah Data Dengan Nilainya (Holik et al. 2015).

Unit SOC tidak semestinya mendapat manfaat daripada memeriksa tangkapan paket penuh setiap hari. Tangkapan paket penuh ialah rakaman semua trafik. Jumlah data dalam tangkapan paket penuh merentasi rangkaian boleh menjadi luar biasa untuk analisis masa nyata. Walau bagaimanapun, tangkapan paket penuh mungkin menjadi sangat berguna dalam analisis selepas kejadian. Dengan mengumpul tangkapan paket, penganalisis SOC boleh memperoleh pemahaman yang lebih kukuh tentang bagaimana peristiwa itu berlaku. Tangkapan paket boleh digunakan untuk memainkan semula peristiwa yang berlaku sebelum dan semasa serangan.

Walau bagaimanapun, tangkapan paket penuh memerlukan banyak storan dan keupayaan analisis, kerana saiz fail tangkapan paket meningkat dengan cepat (Sulkamo 2018). Sebagai contoh, jika organisasi mempunyai sambungan rangkaian 1 gigabit sesaat (Gb/s) dan secara purata separuh daripada lebar jalur digunakan, jumlah data yang di kumpul dalam tempoh 24 jam ialah 5.4TB. Pengiraan digambarkan di bawah:

$$1000\frac{megabit}{seconds} * 60\ seconds * 60\ minuntes * 24\ hours * \frac{0.5\ utilization}{8\ bits\ per\ bytes} = 5.4TB \qquad (1)$$

Organisasi itu mungkin mampu menyimpan dan memproses 5.4TB data, tetapi untuk analisis selepas kejadian 24 jam tidak mencukupi. Untuk melaksanakan analisis

sejarah, SOC memerlukan data sekurang-kurangnya sebulan, yang meningkatkan keperluan saiz storan dengan ketara.

$$5.4TB * 30\ days = 162TB \quad (2)$$

Walaupun mengumpul tangkapan paket penuh boleh menjadi sangat berguna untuk analisis selepas kejadian, semua organisasi mungkin tidak dapat mengumpul dan menganalisis jumlah besar data yang dijananya. Contoh yang digunakan di atas meliputi hanya satu sambungan 1 Gbps. Organisasi yang lazimnya besar mempunyai berbilang rangkaian dan mungkin berbilang pejabat dengan sambungan berlebihan. Dalam kes ini, saiz tangkapan paket meningkat dengan ketara. Organisasi mesti menilai kebaikan dan keburukan tangkapan paket penuh, kerana ia memerlukan sejumlah besar sumber untuk menganalisis dan menyimpan data.

NetFlow ialah teknologi yang dibangunkan oleh *Cisco Systems* yang bertentangan dengan tangkapan paket penuh hanya merekodkan ringkasan sambungan rangkaian. Rekod *NetFlow* tidak termasuk kandungan paket rangkaian, tetapi lebih kepada maklumat bahawa sambungan itu berlaku di tempat pertama. Biasanya rekod *NetFlow* mengandungi masa mula dan tamat, destinasi dan alamat IP sumber dan port yang digunakan, bait yang dihantar dan diterima dan protokol lapisan 4 OSI yang digunakan contohnya, sama ada TCP, UDP atau ICMP (Crawley 2018).

NetFlow berkembang pesat dalam meringkaskan aktiviti rangkaian dan kesederhanaannya dalam beberapa kes boleh menjadi ciri dan bukannya kecacatan. Maklumat sub-OSI lapisan 4 boleh digunakan untuk mengesan anomali. Sebagai contoh, adalah mencurigakan jika pelayan sentiasa menyambung ke hos menggunakan protokol yang tidak normal. Walau bagaimanapun, *NetFlow* tidak mencukupi dengan sendirinya, kerana ia tidak menangkap kandungan paket. Pot TCP 80 biasanya digunakan dalam sambungan *Hypertext Transfer Protocol (HTTP)*. Walau bagaimanapun, *NetFlow* tidak menangkap sebarang maklumat di atas lapisan 4 jadi ia tidak dapat memastikan bahawa sambungan adalah trafik HTTP yang sah. HTTP paling biasa digunakan dalam menyajikan kandungan web.

2.8 PUSAT OPERASI KESELAMATAN DALAMAN DAN LUARAN

Apabila organisasi mempertimbangkan SOC mereka mesti menilai sama ada mereka membina SOC dalaman atau membelinya sebagai perkhidmatan daripada pembekal perkhidmatan keselamatan terurus (MSSP) (Palo Alto Networks 2017). Lazimnya hanya organisasi besar yang mempunyai SOC dalaman, kerana membina dan menyelenggara SOC adalah mahal. Ia juga penting untuk diingat bahawa ia boleh mengambil masa yang lama sebelum SOC berjalan pada kecekapan yang diingini, kerana ia adalah unit yang sedang berkembang yang memerlukan masa untuk matang. SOC dalaman mendapat manfaat daripada mempunyai akses terus kepada persekitaran yang dipantau dan pasukan yang menguruskan infrastruktur.

Sistem SIEM sahaja selalunya mahal, dan mengendalikan SOC adalah lebih daripada sekadar SIEM. Seluruh proses membina dan mengendalikan SOC memerlukan banyak pelaburan. MSSP berbeza dalam perkhidmatan mereka, kerana sesetengahnya menyediakan SOC hanya untuk pemantauan keselamatan. Ini bermakna unit SOC MSSP memberitahu pelanggan jika mereka menemui ancaman dalam rangkaian pelanggan. Selepas pelanggan dimaklumkan tentang ancaman tersebut, pelanggan bertanggungjawab terhadap sebarang tindakan untuk mengelakkan insiden daripada berlaku.

Sesetengah MSSP menawarkan perkhidmatan untuk keseluruhan kitaran hayat serangan, yang bermaksud bahawa MSSP mengendalikan serangan daripada pengesanan sehinggalah ke pembendungan, pembasmian dan pemulihan. MSSP dan pelanggan mereka membuat kontrak yang mentakrifkan perjanjian tahap perkhidmatan (SLA). SLA mewajibkan MSSP untuk bertindak dalam masa yang ditetapkan dalam kontrak. Kewajipan ini memberi manfaat kepada pelanggan kerana kontrak memaksa SOC MSSP untuk bertindak balas dalam jangka masa yang ditakrifkan dalam kontrak. Selain itu, SLA mentakrifkan kuasa unit SOC MSSP ke atas rangkaian pelanggan (Zimmerman 2014). Menurut Duna et al. (2021) SOC boleh disediakan menggunakan 2 kaedah berbeza untuk menyediakan perkhidmatan SOC iaitu:

1) SOC Secara dalaman (In-house)

- SOC yang memenuhi keperluan keselamatan dalaman organisasi.

2) MSSP (Pembekal Perkhidmatan Keselamatan Terurus)

- Peranti dan sistem keselamatan, seperti IPS dan firewall, dipantau dan diuruskan secara jarak jauh (remote)

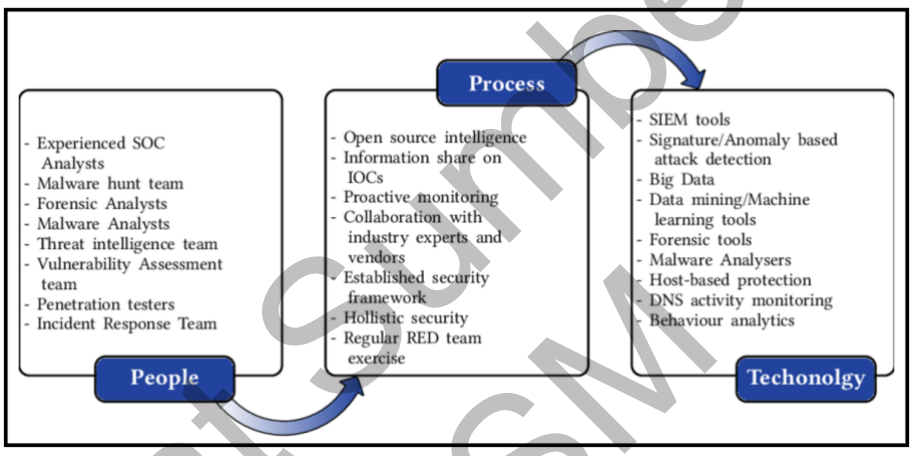
2.9 MODEL KONSEP SOC

SOC boleh dianggap sebagai salah satu penyelesaian untuk melindungi organisasi daripada serangan siber (Schinagl et al. 2015) menyatakan bahawa rangka kerja SOC adalah bergantung kepada hala tuju yang ditetapkan oleh organisasi. Ia boleh dilaksanakan oleh misi, objektif, kewangan, dan faktor lain yang mempengaruhi operasi organisasi. Walaupun SOC boleh dibangunkan berdasarkan keperluan organisasi, keperluan asas dan skopnya mesti dikenal pasti. Keperluan ini meliputi tiga bidang kritikal dalam keselamatan siber: pemantauan, analisis dan tindak balas. Seperti yang diserlahkan dalam bahagian sebelumnya, manusia, proses dan teknologi adalah elemen penting untuk kejayaan penubuhan SOC.

Faktor Proses Pembinaan SOC yang cekap digambarkan dalam Rajah 2.9. Rajah 2.9 meringkaskan hubungan dan kepentingan manusia, proses dan teknologi dalam melaksanakan SOC. Berdasarkan bukti daripada kajian lepas, faktor-faktor ini bergantung kepada peranan dan ke fungsian SOC. Dengan aplikasi teknologi dan proses yang ditetapkan dengan betul, motivasi pekerja dalam SOC boleh dipertingkatkan kerana ia membenarkan automasi prosedur berulang. Akibatnya, pekerja mempunyai lebih banyak masa untuk meneroka pengetahuan yang memerlukan sentuhan manusia, seperti kecerdasan ancaman.

Oleh itu, ia boleh membolehkan pekerja dilatih membawa kepada tenaga kerja mahir yang maju dalam keselamatan siber. Selain itu, model ini disokong oleh penambahbaikan berterusan untuk memastikan ketiga-tiga elemen ini sentiasa relevan dan terkini. Selanjutnya, ia juga merangkumi aspek kewangan, kerana ia memainkan peranan penting dalam menambah baik organisasi. Adalah menjadi persefahaman bersama bahawa pelaksanaan teknologi memerlukan peruntukan kewangan yang tinggi. Jika organisasi disokong dengan teknologi yang canggih tetapi dengan pekerja yang tidak mahir, ia akan meninggalkan SOC yang tidak cekap untuk beroperasi.

Begitu juga, jika teknologi yang diterapkan tidak memanfaatkan pengetahuan dan kemahiran yang ada kepada pekerja, ia juga akan menjejaskan pelaksanaan SOC. Tambahan pula, tanpa proses yang mantap dalam SOC, hubungan antara faktor manusia dan teknologi akan menjadi tidak berkesan. Oleh itu, pemilihan pekerja berteknologi yang sesuai, berpengetahuan dan berkemahiran, dan proses yang ditetapkan dengan secukupnya adalah penting untuk melaksanakan SOC yang berkesan dan cekap. Oleh itu, faktor-faktor ini digunakan sebagai petunjuk dalam instrumen tinjauan bagi penubuhan SOC khususnya dalam persekitaran Malaysia.



Rajah 2.9 Faktor Proses Pembinaan SOC yang Cekap

Sumber: Akinrolabu et al. (2018)

Oleh yang demikian, dalam pembinaan SOC yang cekap, ia memerlukan beberapa kunci faktor seperti manusia, prosedur, dan teknologi (Torres, 2015) dengan peranan di bawah:

- **Manusia** : memerlukan kakitangan IT untuk menangani pengurusan, penganalisis, tindak balas, dan penyelenggaraan perkakasan
- **Proses:** memerlukan standard dan proses berulang untuk melindungi dan bertindak balas kejadian pada sistem.
- **Teknologi:** teknologi pemantauan perisian dan perkakasan di dalam rangkaian yang dapat melakukan ujian penembusan, keselamatan audit, dan scan port untuk memantau, triage, paparan dan bertindak balas terhadap peristiwa tersebut.

Teknologi, manusia, dan proses telah digunakan dalam literatur sains maklumat untuk berbagai topik termasuk dalam pelbagai kajian pengetahuan (Pee & Kankanhalli 2009) dan pengurusan hubungan pelanggan (Chen & Popovich 2003) hingga kepada proses peningkatan sistem (Prodan et al. 2015). Justeru dalam kajian ini, ketiga-tiga aspek utama ini telah diadaptasi untuk menggambarkan secara efektif aspek yang bekerjasama dan berkesan merangkumi pembinaan SOC yang cekap (Hewlett-Packard 2011) yang tentunya merupakan manusia, proses, dan teknologi. Oleh itu, bagi memastikan operasi SOC yang tidak terganggu kesemua aspek tersebut haruslah digabungkan dan diguna sebaik mungkin.

2.9.1 Faktor Teknologi

SOC menggunakan banyak penyelesaian teknikal yang boleh berbeza-beza bergantung pada skop dan misi SOC. Walau bagaimanapun, teknologi yang ditunjukkan di bawah ini digunakan dalam semua SOC moden dan dianggap sebagai tulang belakang dari aspek teknologi. Berikut adalah beberapa teknologi yang digunakan :

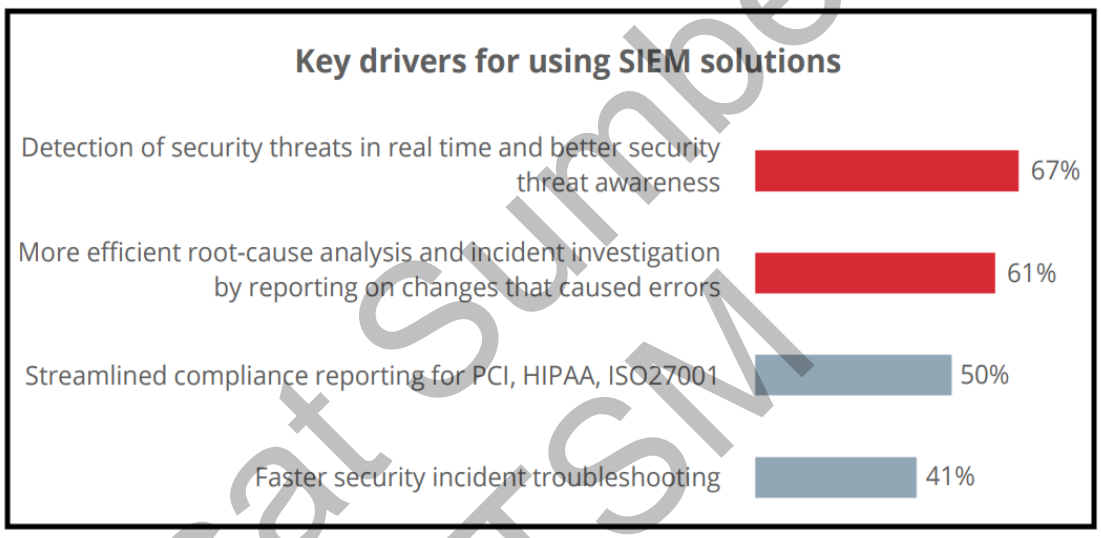
a. Sistem Maklumat Keselamatan dan Pengurusan Peristiwa (SIEM)

Sistem SIEM adalah teknologi yang menyokong setiap tindakan yang berlaku di SOC dan keupayaan sistem SIEM merangkumi:

- Gabungan data dan korelasi pengekalan
- Makluman
- Papan Pemuka
- Pematuhan
- Analisis Forensik

Kelebihan dengan adanya SOC adalah masa tindak balas menjadi lebih pantas dan singkat sekiranya terdapat sebarang insiden keselamatan. Pasukan SOC juga dapat meningkatkan kecekapan dengan pemantauan dan melaporkan pencerobohan, serangan dalam rangkaian. Keupayaan pemulihan dari serangan siber dapat dijalankan dengan lebih berkesan kerana semua maklumat ada pada SOC. Selain itu, dengan memiliki penyelesaian pasukan SOC dan perisian SIEM ianya bertindak memberi banyak

kelebihan untuk menjaga keselamatan dan pematuhan yang ditetapkan di dalam organisasi. Menurut *Netwix* di dalam kajian yang dijalankan, mengapa banyak organisasi membangunkan SOC dengan adalah seperti di rajah 2.8. Di dalam rajah tersebut 67% responden mewujudkan SOC dengan SIEM kerana SOC dapat mengesan ancaman keselamatan secara terus dalam waktu semasa dan 61% menyatakan dapat mengurangkan kesalahan dalam pelaporan. 51 % disebabkan memenuhi standard pematuhan seperti PCI, HIPAA dan ISO 27001. Di samping itu juga sebanyak 41% bersetuju proses penyelesaian masalah bertambah pantas.



Rajah 2.10 Pemacu utama penggunaan penyelesaian SIEM

Sumber : Netwrix 2016

b. Pemantauan Aktiviti Pangkalan Data *(DAM – Database activity Monitoring*)

DAM mengawasi penggunaan pangkalan data di dalam server. Ianya mengesan aktiviti luar biasa pengguna atau pentadbir sistem bagi memastikan objektif pematuhan dipenuhi dan tidak ada tindakan yang dapat mengubah integriti data atau ketersediaannya. Sekiranya tingkah laku seperti itu dikesan, pangkalan data secara automatik akan memberikan respons yang sesuai kepada DAM (Kamra et al. 2008).

c. Sistem Pengesanan Pencerobohan *(IDS – Intrusion Detection System)*

IDS adalah peranti atau aplikasi yang bermaksud untuk mengesan perilaku jahat yang disasarkan terhadap rangkaian dan sumbernya. Mereka melakukannya dalam masa dua

pendekatan, yang pertama adalah mencari corak tingkah laku jahat yang telah ditentukan yang disebut tandatangan. Pendekatan ini dilabel berdasarkan penyalahgunaan dan yang kedua adalah untuk mengesan penyimpangan dari tingkah laku yang diharapkan (berdasarkan anomali). Kedua-dua pendekatan mempunyai kekuatan dan kelemahan mereka yang telah banyak dikaji oleh pelbagai penyelidik (García-Teodoro et al. 2009; Patel et al. 2010; Shameli-Sendi et al. 2014). Manakala langkah terakhir, pengkategorian IDS lain berasal dari sumber peristiwa yang mereka analisis iaitu IDS berasaskan hos, berasaskan aplikasi dan rangkaian wujud.

d. Sistem Pencegahan Pencerobohan *(IPS – Intrusion Prevention System)*

IPS dan IDS adalah hampir sama dan kedua-duanya memantau sumber peristiwa tertentu. Perbezaan utama adalah IPS menyekat ancaman yang dikesan secara aktif manakala IDS hanya merekodkan dan memberi notifikasi yang dikesan (Scarfone & Mell 2007).

e. *Firewall*

Firewall sebuah peranti atau sekumpulan peranti yang ditetapkan untuk membenarkan, menghalang, menyulitkan, menyahsulitkan, atau memproksikan segala trafik komputer di antara domain-domain keselamatan yang berbeza berdasarkan beberapa peraturan serta kriteria mengikut satu set peraturan yang berlaku. *Firewall Aplikasi Web (WAF)* dianggap sangat penting kerana selain memastikan komunikasi internet yang selamat, ia juga menghasilkan log yang boleh digunakan untuk forensik dan pelaporan (Luthra et al. 2013)

2.9.2 Faktor Manusia

Faktor manusia adalah salah satu faktor yang amat penting dalam sesebuah pembangunan SOC. Peranan manusia juga di dalam SOC adalah menangani pengurusan, penganalisis, tindak balas, dan penyelenggaraan perkakasan. Oleh itu pelbagai perkara dilakukan dalam SOC yang melibat kat manusia seperti pemantauan, pengesanan, pentafsiran dan pembaikan yang memerlukan kemahiran dan tahap pendidikan serta pengalaman yang spesifik bagi memastikan keselamatan organisasi adalah terjamin. Salah satu tujuan SOC adalah untuk mengukuhkan pasukan

keselamatan dengan maklumat yang tepat dan kontekstual sehingga dapat menggunakannya bagi tujuan respons yang efektif. Tanggapan bahawa teknologi yang menyokong SOC tidak dapat dilaksanakan dengan sendirinya.

Bergantung pada ukuran, misi dan pelaksanaan SOC, terdapat beberapa tahap penganalisis. Setiap peringkat mesti mempunyai satu set tanggungjawab yang tegas sementara jalan peningkatan di antara peringkat mesti mematuhi prosedur yang telah ditentukan. Mengendalikan SOC bukanlah proses yang mudah kerana banyak kemahiran teknikal dan insaniah yang semestinya dimiliki oleh setiap anggota pasukan. Menurut kajian yang dilakukan oleh *International Information System Security Certification Consortium ((ISC)* mendedahkan kekurangan profesional keselamatan yang berkemampuan di pasaran antarabangsa (Suby 2013).

Berdasarkan kekurangan yang disebutkan di atas, masalah penting mengenai aspek anggota pasukan SOC adalah kenyataan bahawa penganalisis keselamatan mempunyai 'jangka hayat' yang terhad. Ini disebabkan oleh kenyataan bahawa (terutamanya dalam SOC yang beroperasi dalam jangka masa 24x7) penganalisis bekerja dengan panjang yang memenatkan. Akibatnya jangka hayat tugas penganalisis SOC hanya sekitar satu hingga tiga tahun sahaja. Justeru, pengekalan anggota pasukan SOC dibuat lebih penting lagi oleh kenyataan bahawa penganalisis menggunakan pengetahuan diam *(tacit knowledge)* untuk melaksanakan tugas mereka, yang berkaitan dengan infrastruktur IT spesifik di dalam organisasi (Goodall et al. 2009).

Disamping itu juga, terdapat cabaran besar dalam merekrut dan mengekalkan kakitangan yang ada kerana kekurangan sumber manusia dalam bidang keselamatan ICT (DeCusatis et al. 2019). Latihan dan pengalaman memainkan peranan penting dalam menangani cabaran kekurangan sumber manusia yang kompeten dalam bidang ini, oleh itu peningkatan tahap kompetensi ahli pasukan SOC melalui latihan formal seperti persijilan profesional dan latihan tidak formal adalah diperlukan. latihan dapat meningkatkan tahap kompetensi dalam bidang keselamatan ICT Baldassarre et al. (2019)

Faktor manusia juga melibatkan peranan dan tanggungjawab, tahap pendidikan, persijilan, latihan, serta kemahiran adalah penting dalam rangka pembangunan SOC secara khusus seperti berikut :

a. Peranan dan tanggungjawab ahli pasukan SOC

Dalam pembangunan SOC terdapat berapa peranan yang penting bagi melengkapkan pasukan SOC. Menurut Torres (2015) peranan dan tanggungjawab yang terdapat dalam SOC adalah seperti berikut:

- Pengurus SOC
- Pengalasis Amaran
- Responden Insiden
- *Subject Matter Expert*

Selain itu, peranan dan tanggungjawab disusun secara hierarki mengikut persekitaran SIEM, menurut Duna et al. (2021). Secara umumnya, SOC terdiri daripada beberapa tahap penganalisis keselamatan (SA). SA dibahagikan kepada tiga (3) tahap peranan dan tanggungjawab yang paling baik untuk diamalkan seperti berikut :

- Tahap 1

  i) Pemantauan pada skrin amaran sistem SIEM
  ii) Menentukan tahap keterukan peristiwa
  iii) Peningkatan peraturan kepada jurutera SOC/SA peringkat lebih tinggi sekiranya bilangan positif palsu adalah tinggi
  iv) Tingkatkan amaran untuk siasatan lanjut apabila mereka tidak boleh mengelaskan amaran sebagai sama ada serangan atau positif palsu

- Tahap 2

  i) Mengekalkan kewaspadaan terhadap skrin amaran peranti SIEM
  ii) Peristiwa diprioritikan

iii) Peningkatan peraturan kepada jurutera SOC/SA peringkat lebih tinggi sekiranya bilangan positif palsu adalah tinggi

iv) Jika mereka tidak dapat mengklasifikasikan amaran sebagai positif palsu atau serangan, mereka meningkatkan amaran tersebut untuk siasatan lanjut.

v) Menyemak makluman yang diberikan oleh SA tahap 1 yang berkemungkinan adalah serangan dan menyediakan kajian kes.

vi) Membuat kes dan menghantar ke pada pasukan forensik (jika pelanggaran dikenal pasti)

- Tahap 3

i) Mengumpulkan pasukan forensik dan jurutera keselamatan

ii) Menentukan skop dan kesan serangan.

iii) L2 boleh digunakan untuk memperhalusi peraturan untuk meminimumkan penggera palsu

b. Tahap pendidikan, persijilan dan latihan

Menurut Duna et al. (2021) juga apabila pekerja baru dilantik ke dalam pasukan SOC, mereka akan menerima latihan awal yang merangkumi latihan ke fungsian, kesedaran keselamatan dan program pembudayaan keselamatan.

i. Latihan ke fungsian

Latihan asas untuk mempelajari proses, sumber, strategi, undang-undang dan peraturan organisasi.

ii. Kesedaran keselamatan

Meminimumkan ancaman kejuruteraan sosial adalah salah satu matlamat pembelajaran. Rantaian keselamatan maklumat dikenali sebagai pautan yang paling lemah. Oleh itu, ujian secara rutin, pengetahuan keselamatan dan kejuruteraan sosial adalah amat kritikal.

iii. Program pembudayaan keselamatan

Kempen secara berterusan dan berpanjangan dalam menjadikan keselamatan sebagai budaya, ianya melebihi daripada keselamatan manusia. Semua pasukan perlu bekerjasama dan berkomunikasi secara efisien. Jika terdapat sebarang insiden yang meragukan, pekerja haruslah diarahkan supaya mendapatkan maklumat, laporan dan bertindak dengan sepatutnya. Untuk membolehkan mereka untuk mengikut undang-undang dan protokol, mereka mestilah diberitahu berkenaan sekatan dan implikasi kebocoran data atau sebarang pelanggaran keselamatan.

Oleh yang demikian, ahli pasukan SOC haruslah dilengkapkan dengan semua latihan awalan ini bagi membolehkan mereka lebih bersedia menghadapi ancaman, insiden dan serangan. Perkara ini amat penting dimulakan dengan ahli pasukkan SOC itu sendiri kerana mereka adalah tonggak keselamatan yang di hadapan. Bahagian kritikal untuk menjadikan operasi yang efisien adalah latihan untuk semua ahli pasukan. Pendidikan yang betul dan latihan yang berterusan akan memastikan kemahiran dan pengetahuan semua ahli pasukan dikemaskini dan berkembang dalam landskap ancaman yang berubah ini (Andra 2019). Persijilan adalah penting bagi memastikan ahli pasukan SOC adalah profesional dan dilengkapi dengan pengetahuan dan Teknik yang terkini. Antara persijilan yang dicadangkan oleh Torres (2015) adalah SANS SEC 401, SANS SEC 501, SANS SEC 503, SANS SEC 504, SANS SEC561, SANS FOR610, CISSP, CISA, CISM dan CGEIT.

c. Kemahiran

Kemahiran adalah satu elemen yang penting untuk melengkapkan lagi ahli pasukan SOC untuk membendung ancaman keselamatan yang makin berleluasa. Walaubagaimanapun, halangan yang paling kerap disebut untuk menjadi cemerlang adalah kekurangan kakitangan mahir (58%) dan ketiadaan orkestrasi dan automasi yang berkesan (50%) (Crowley C, 2019). Andra (2019) telah menggariskan kemahiran yang perlu ada oleh ahli pasukan SOC adalah seperti berikut :

i. Tahap 1 – Analis keselamatan

Set kemahiran yang perlu ada adalah pengurus sistem, pengaturcaraan dan keselamatan

ii. Tahap 2 – Analis keselamatan

Pada tahap dua (2) semua kemahiran pada tahap satu (1) harus dimiliki dan ditambah dengan kebolehan mengawal peristiwa yang merunsingkan dan mempunyai rasa ingin tahu untuk mencari punca berlakunya insiden.

iii. Pakar keselamatan

Selain daripada set kemahiran yang ada, pakar keselamatan telah biasa dengan alat ujian penembusan dan alat visual yang digunakan dalam proses.

iv. Pengurus SOC

Mempunyai tahap kepimpinan yang tinggi dan mempunyai kemahiran berkomunikasi yang baik.

Selain daripada pengetahuan dan kemahiran berkaitan teknikal, kemahiran insaniah juga adalah amat penting (Crowley 2019). Kemahiran komunikasi dan boleh bekerja dalam pasukan adalah amat penting bagi sesebuah SOC untuk berfungsi secara optima dan dapat meningkatkan lagi tahap keselamatan sesebuah organisasi. Oleh itu, kemahiran teknikal dan juga insaniah adalah perlu diterapkan didalam pasukan SOC.

2.9.3 Faktor Proses

Proses boleh dianggap sebagai antara muka yang digunakan bahagian fungsional lain dari SOC untuk bekerjasama. Selain itu, ianya memastikan operasi SOC yang lancar dan berkesan. Terutama yang penting adalah proses yang bertindak sebagai pengisi jurang antara manusia dan aspek teknologi (Haight et al. 2014). Proses SOC boleh dibahagikan kepada empat kategori (Hewlett-Packard 2011):

- Proses perniagaan
- Proses teknologi
- Proses operasi

- Proses analisis

Proses perniagaan menentukan dan mendokumentasikan komponen pentadbiran yang diperlukan untuk mengendalikan SOC dengan cekap sambil menjamin bahawa operasi tersebut selaras dengan tujuan organisasi. Contoh proses tersebut adalah penyediaan laporan, penyimpanan log, definisi dasar keselamatan dan jaminan pematuhan terhadapnya.

Manakala Proses teknologi memastikan bahawa infrastruktur IT berfungsi pada tahap optimum pada waktu tertentu. Ianya juga menyimpan maklumat dan mendokumentasikan tindakan-tindakan yang berkaitan dengan pengurusan konfigurasi sistem, pentadbiran sistem, integrasi teknologi dan lain-lain. Contoh proses tersebut adalah pengimbasan dan pemulihan kerentanan, pembaharuan *firmware* dan perisian serta penambahbaikan perisian.

Proses operasi menentukan tindakan yang dilakukan di dalam SOC setiap hari. Contoh proses tersebut adalah penjadualan syif dan perolehan serta latihan pekerja. Manakala proses terakhir sekali ialah proses analisis menentukan bagaimana masalah keselamatan dikesan dan diperbaiki. ianya juga termasuk tindakan yang diambil untuk mempelajari dan memahami ancaman. Contoh prosedur tersebut adalah klasifikasi kejadian, pengesanan dan forensik.

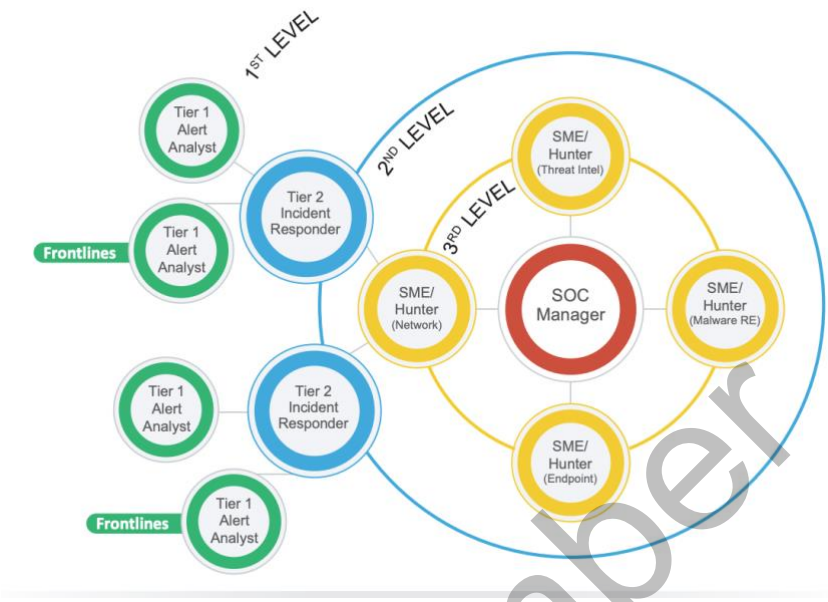
2.10 PERBANDINGAN MODEL PERANAN DAN TANGGUNGJAWAB, TAHAP PENDIDIKAN SERTA KEMAHIRAN AHLI PASUKAN

Dalam melaksanakan kajian ini, proses menganalisis model dan kajian SOC sedia ada perlu dilakukan bagi mengenal pasti jurang yang terdapat di dalam model sedia ada. Selain itu, dalam kajian kesusasteraan ini juga perlu dilihat secara lebih mendalam yang merangkumi peranan dan tanggungjawab, tahap pendididkan serta kemahiran ahli pasukan yaang akan mengagotahi SOC. Jika perkara ini tidak dapat diperincikan dan diperhalusi, pasukan SOC tidak dapat berfungi dengan efektif kerana setiap ahli tidak dapat membezakan tugas dan tanggungjawab serta saling menuding jari antara satu sama lain jika sesuatu tugas itu kurang jelas dan mereka merasakan ianya bukan tanggungjawab mereka. Selain itu , tahap pendidikan dan kemahiran juga adalah

penting dalam aspek manusia ini kerana ini membolehkan setiap ahli mampu menjalankan tugas dengan baik dan dapat meminumumkan kesilapan dan menigkatkan tahap SOC yang kepada lebih tinggi. Justeru, hasil proses penganalisaan setiap model adalah penting dalam membangunkan model awal kajian. Jadual 2.1 merujuk kepada hasil penganalisaan bagi model kesediaan sedia ada.

Jadual 2.1 Penemuan peranan dan tanggungjawab, tahap pendidikan serta kemahiran ahli pasukan dalam model pada kajian lepas

Bil	Penulis dan Tajuk	Model	Huraian
1	Torres, A. 2015. *Building a World-Class Security Operations Center*: *A Roadmap*. Rockville: SANS Institute.	Peranan Dan Tanggungjawab Mengikut Tahap Rujuk Rajah 2.11	Peranan dan tanggungjawab di terangkan mengikut tahap yang mudah dipahami yang merangkumi beberapa tahap seperti Tahap 1, Tahap 2 dan Tahap 3. Selain itu hubungan setiap peranan dan tanggungjawab ditunjukkan antara peranan-peranan seperti pengurus, SME dan penganalisis.
2	Duna, Y.T., Mohd Faizal Ab Razak, Mohamad Fadli Zolkiplib, Bee, T.F. & Ahmad Firdaus. 2021. Grasp on next generation security operation centre (NGSOC): comparative study. *International Journal of Nonlinear Analysis and Applications* 12(2): 869-895.	Peranan dan tanggungjawab ahli pasukan SOC Rujuk Rajah 2.12	Peranan dan tanggungjawab dihuraikan mengikut tahap. Setiap tanggungjawab dipecahkan mengikut tahap kemahiran dan pengalaman.
3	Vielberth, Manfred & Böhm, Fabian & Fichtinger, Ines & Pernul, Günther. (2020). Security Operations Center: A Systematic Study and Open Challenges. IEEE Access. PP. 10.1109/ACCESS.2020.3045514.	Tahap pendidikan dan kemahiran Pasukkan SOC Rujuk Rajah 2.13	Tahap pendidikan dan kemahiran dihuraikan berdasarkan 3 peringkat iaitu peringkat 1 hingga 3. Selain itu kriteria juga di terangkan dalam model ini.



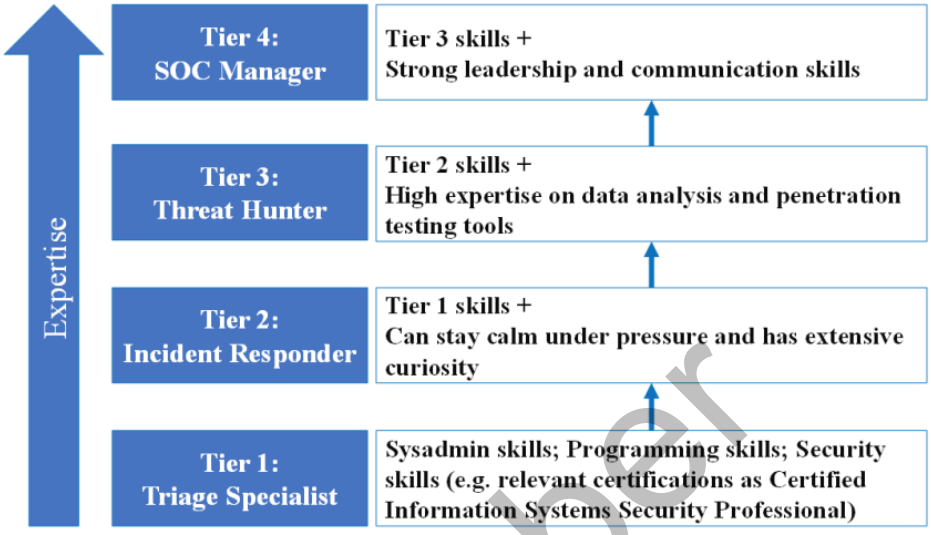
Rajah 2.11 Peranan dan tanggungjawab mengikut tahap

Sumber : Torres, A. 2015.

Security Analysts	Duties & Responsibilities
Level 1	• Monitor the SIEM system alert screen • Triage events (decide event's severity level) • Escalate rules to SOC engineer/higher level SA in case of high number of false positives • Escalate alert for further investigation for when they can't classify an alert as either an attack or false positives
Level 2	• Maintain vigilance over the SIEM device alert screen. • Events are prioritized (the intensity level of the incident is determined). • If a large number of false positives occur, escalate the rules to the SOC engineer/higher level SA. • If they are unable to classify a warning as a false positive or an attack, they escalate the alert for further investigation. • Examine the alerts that L1 SAs have mentioned as potential attacks. Prepare a case study • Make a case and send it to the forensic team (if breach is identified)
Level 3	• Assemble a forensic team and security engineers • Determine the scope and effect of the attack. • L2 can be used to fine-tune rules to minimize false alarms.

Rajah 2.12 Peranan dan tanggungjawab ahli pasukan SOC

Sumber: Duna, Y.T., Mohd Faizal Ab Razak, Mohamad Fadli Zolkiplib, Bee, T.F. & Ahmad Firdaus. 2021



Rajah 2.13 Tahap pendidikan dan kemahiran Pasukkan SOC

Sumber: Vielberth, Manfred & Böhm, Fabian & Fichtinger, Ines & Pernul, Günther. (2020).

2.11 CADANGAN MODEL AWAL

Cadangan model awal bagi kajian ini adalah berdasarkan kepada kerangka kajian Peranan dan tanggungjawab mengikut tahap (Torres, A. 2015); Peranan dan tanggungjawab ahli pasukan SOC (Duna, Y.T., Mohd Faizal Ab Razak, Mohamad Fadli Zolkiplib, Bee, T.F. & Ahmad Firdaus. 2021) ; dan Tahap pendidikan dan kemahiran Pasukkan SOC (Vielberth, Manfred & Böhm, Fabian & Fichtinger, Ines & Pernul, Günther. (2020). Ketiga-tiga kerangka kajian ini dipilih berdasarkan kajian yang telah menggariskan peranan dan tanggungjawab, tahap pendidikan dan kemahiran pasukan SOC yang menjawab persoalan awal permasalahan kajian ini.

Terdapat beberapa jurang di dalam kajian mereka seperti setiap satunya tidak menunjukkan hubungan yang lebih mudah untuk empat (4) elemen iaitu Ahli pasukan SOC, peranan dan tanggungjawab, tahap pendidikan dan kemahiran di dalam satu kerangka model yang lebih mudah dipahami. Selain itu juga, dalam tahap pendidikan elemen pendidikan formal seperti Diploma , Ijazah Sarjana Muda, dan Ijazah Sarjana tidak wujud di dalam mana-mana kajian mereka. Oleh yang demikian, model awal yang dicadangkan bagi kajian ini adalah dengan menggabungkan keempat-empat elemen dan