MARINHA DO BRASIL
DIRETORIA DE ENSINO DA MARINHA
CENTRO DE INSTRUÇÃO ALMIRANTE WANDENKOLK

CURSO DE APERFEIÇOAMENTO AVANÇADO EM
SEGURANÇA DAS INFORMAÇÕES E COMUNICAÇÕES

PRIMEIRO-TENENTE DANIEL GOUVEA COSTA

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM):
Contribuição da plataforma para segurança de redes e informações digitais da Marinha

Rio de Janeiro
2020

PRIMEIRO-TENENTE DANIEL GOUVEA COSTA

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM):
Contribuição da plataforma para segurança de redes e informações digitais da Marinha

Monografia apresentada ao Centro de Instrução Almirante Wandenkolk como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado em Segurança das Informações e Comunicações

Orientadores:
Professor Dr. Anderson Oliveira da Silva
SC Eng. Victor Hugo Okabayashi

CIAW
Rio de Janeiro
2020

COSTA, Daniel Gouvea.
Security Information and Event Management (SIEM): contribuição da plataforma para segurança de redes e informações digitais da Marinha / Daniel Gouvea Costa. — Rio de Janeiro, 2020.
57f.: il.

Orientador: Prof. Dr. Anderson Oliveira da Silva;
Eng. MSc. Victor Hugo Okabayashi.

Monografia (Curso de Aperfeiçoamento Avançado de Segurança da Informação e Comunicações) — Centro de Instrução Almirante Wandenkolk, Rio de Janeiro, 2020.

1. SIEM. 2. Log. 3. Defesa em profundidade. 4. Segurança da informação e comunicações. 5. Guerra cibernética. I. Centro de Instrução Almirante Wandenkolk. II. Título.

PRIMEIRO-TENENTE DANIEL GOUVEA COSTA

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM):

Contribuição da plataforma para segurança de redes e informações digitais da Marinha

Monografia apresentada ao Centro de Instrução Almirante Wandenkolk como requisito parcial à conclusão do Curso de Aperfeiçoamento Avançado em Segurança das Informações e Comunicações.

Aprovada em 24 de abril de 2020.

Banca Examinadora:

_____

Anderson de Oliveira da Silva, D. Sc. – PUC-Rio

_____

Victor Hugo Okabayashi, MSc. – DCTIM

_____

CMG (RM1-EN) Gian Karlo Huback Macedo de Almeida – CIAW

CIAW
Rio de Janeiro
2020

Dedico esse trabalho primeiramente a Deus, por sua infinita misericórdia e por estar sempre presente em minha vida e na vida da minha família, a minha esposa e meus filhos que com todo carinho e apoio incondicional, não mediram esforços para que eu chegasse até esta etapa da minha vida.

AGRADECIMENTOS

Acima de tudo agradeço a Deus a cada vitória alcançada ao longo de todo percurso até aqui. Pelo Seu amor e misericórdia me deu a vida e a todos os momentos está comigo, segurando-me com Sua forte mão. Agradeço ainda pelos tropeços que o Senhor permitiu que ocorressem, que serviram de trampolim e aprendizagem para superar situações adversas.

Agradeço a minha esposa, pelo companheirismo, amizade e amor, que independente dos desafios caminha lado a lado comigo buscando ao máximo retirar o peso dos afazeres no lar, para que meus esforços fossem concentrados nos estudos e na confecção deste trabalho. Agradeço aos meus filhos que sempre me apoiaram e tiveram compreensão nos momentos em que estive afastado das brincadeiras por motivos de trabalho ou estudo. Muito obrigado por serem a motivação dos meus esforços.

Aos meus pais, agradeço por toda dedicação e investimento, tanto no meu caráter como homem, quanto em meus estudos. Hoje como pai, sei o quão grande é a responsabilidade de educar e ensinar. Por esse motivo agradeço por todo empenho, e dedicação.

Agradeço ao meu orientador acadêmico, Professor Doutor Anderson Oliveira da Silva, que além de ter sido fundamental para escolha do tema deste trabalho e orientações, foi professor de 4 das 22 disciplinas deste curso, dos quais destaco: Segurança de Redes de Computadores, Gestão de segurança da Informação e Comunicações e Fundamentos de Segurança da Informação e Comunicações, cujo conteúdo e experiências passadas, contribuíram para a elaboração e o enriquecimento deste trabalho.

Ao Engenheiro Victor Hugo Okabayashi, agradeço a dedicação e esforços investidos, que mesmo diante de inúmeras responsabilidades e encargos que ocupa, na Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM), aceitou prontamente ser meu orientador técnico. Apesar do tema SIEM ser um assunto de caráter sigiloso na Marinha do Brasil com relação a coleta, tratamento e apresentação de dados, o engenheiro Victor soube contribuir com orientações valiosas e de grande enriquecimento.

Ao Capitão de Mar-e-Guerra, da reserva, Gian Karlo Huback Macedo de Almeida, agradeço pela forma que conduziu o curso de Curso de Aperfeiçoamento Avançado em Segurança das Informações e Comunicações, na qualidade de coordenador, cuja empolgação, entusiasmo e fogo sagrado contribuíram sobre maneira para o sucesso em mais uma etapa da formação dos Oficiais de Marinha, sempre atento ao bom senso sem perder a eficiência de aprendizagem. Além destes, agradeço a disponibilidade de integrar minha banca examinadora e pelas orientações e experiências passadas visando o enriquecimento deste trabalho.

Ao Capitão de Fragata, da reserva, Wagner Santana de Freitas, instrutor do Centro de Eletrônica do CIAW, de diversas disciplinas relacionadas a Tecnologia da Informação, agradeço a forma como ministrou as diversas disciplinas. Aulas e matérias que influenciaram diretamente na minha escolha pelo Curso de Aperfeiçoamento Avançado em Segurança das Informações e Comunicações.

Agradeço aos demais professores da Pontifícia Universidade Católica do Rio de Janeiro (PUC-RIO) que contribuíram para o aprendizado e enriquecimento teórico no Curso de Aperfeiçoamento Avançado em Segurança das Informações e Comunicações.

Por fim, agradeço aos meus amigos de turma, em especial aos Oficiais Álvares, que me disponibilizou de sua coleção pessoal dois dos livros utilizados para a confecção deste trabalho e ao Ramalho cuja troca de informações e conhecimentos contribuíram para a formatação e organização deste trabalho.

"*When something is important enough, you do it even if the odds are not in your favor*"

(Elon Musk)

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM):
Contribuição da plataforma para segurança de redes e informações digitais da Marinha

Resumo

Com o avanço das tecnologias e a constante necessidade de comunicação e troca de dados, o mundo está cada vez mais conectado. Com isso surgem ameaças que buscam vulnerabilidades para se aproveitarem dos dados e informações que trafegam na rede. É impossível tratar da troca de dados e informações sem se preocupar com a segurança. A escolha do tema possui total relevância nesse sentido, pois por mais que sejam implementadas barreiras de proteção, como, por exemplo, firewall, proxy e antivírus, tais componentes não garantem a segurança da rede ou dos dados na sua plenitude. O objetivo deste trabalho é destacar a importância da implementação de uma plataforma SIEM, capaz de agregar logs e dados dos diversos componentes de uma rede, correlacioná-los e apresentá-los de forma a oferecer uma visão centralizada a favor da segurança. Para que o objetivo seja alcançado, este trabalho aborda conceitos sobre a guerra cibernética, segurança da informação e comunicações, conceitos básicos do protocolo TCP/IP e o conceito de defesa em profundidade abordando os principais componentes de um perímetro de segurança. Com base nesses conceitos, são definidos os processos gerais de um SIEM, bem como os benefícios e desafios de sua implementação e sua importância para a Marinha do Brasil.

Palavras- chave: SIEM. Log. Defesa em profundidade. Segurança da informação e comunicações. Guerra Cibernética.

LISTA DE FIGURAS

Figura 3.1 - Evolução da Defesa Cibernética 22
Figura 3.2 - Níveis de decisão 24
Figura 3.3 - Principais componentes da Proteção Cibernética na MB 26
Figura 3.4 - Cabeçalho IPv4 29
Figura 3.5 - Estabelecimento da conexão TCP 3-Way handshake 31
Figura 3.6 - Topologia de um roteador de borda e firewall 33
Figura 3.7 - esquema 1 – perímetro de segurança 36
Figura 3.8 - Modelo de arquitetura com NIDS e HIDS 38
Figura 3.9 - Esquema 2 – Perímetro de segurança completo 40
Figura 4.1 - Quebra-cabeça dos componentes de rede. 45
Figura 4.2 - Processos básicos do SIEM 47
Figura 4.3 - Arquitetura básica do SIEM e seus componentes 49

LISTAS DE SIGLAS E ABREVIATURAS

ACK	*Acknowledge*
CASNAV	Centro de Análises de Sistemas Navais
CASOP	Centro de Apoio a Sistemas Operativos
C²	Comando e Controle
CDCiber	Centro de defesa cibernética
CIM	Centro de Inteligência da Marinha
CLTI	Centros Locais de Tecnologia da Informação
Com1DN	Comando do primeiro Distrito Naval
ComOpNav	Comando de Operações Navais
CTI	*Cyber Threat Intelligence*
CTIM	Centro de Tecnologia e Informação da Marinha
CTIR	Centros de Tratamento de Incidentes de Redes
CTIR Gov	Centro de Tratamento e Respostas a Incidentes Cibernéticos de Governo
CTIR.mb	Centro de tratamento de Incidentes de Redes da Marinha do Brasil
DCTIM	Diretoria de Comunicações e Tecnologia da Informação da Marinha
DMZ	*Desmilitarized Zone*
DNS	*Domain Name System*
DSIC	Departamento de Segurança da Informação e Comunicações
EMCFA	Estado Maior Conjunto das Forças Armadas
END	Estratégia Nacional de Defesa
FTP	*File Transfer Protocol*
GSI/PR	Gabinete de Segurança Institucional da Presidência da República
GSIC	Gestão de Segurança da Informação e Comunicações
HIDS	*Host-based Intrusion Detection System*

HTTP	*Hypertext Transfer Protocol*
IBM	*International Business Machines*
IDS	*Identification Detection System*
IHL	*Internet Header Length*
IN	Instrução Normativa
IP	*Internet Protocol*
IPS	*Intrusion Prevention System*
IPv4	*Internet Protocol Version 4*
LAN	*Local Area Network*
MAN	*Metropolitan Area Network*
MB	Marinha do Brasil
MD	Ministério da Defesa
NIDS	*Network Intrusion Detection System*
OM	Organização Militar
PAN	*Personal Area Network*
PETIM	Plano Estratégico de Tecnologia da informação da Marinha
RECIM	Rede de Comunicações Integradas da Marinha
SAN	*Storage Area Network*
SEM	*Security Event Management*
SIC	Segurança da Informação e Comunicações
SIEM	*Security Information and Event Management*
SIM	*Security Information Management*
SMDC	Sistema Militar de Defesa Cibernética
SO	Sistemas Operacionais
STIC2	Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle

SYN	*Synchronized*
TCP	*Transmission Control Protocol*
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicações
ToS	*Type of Service*
TTL	*Time to Live*
UDP	*User Datagram Protocol*
VPN	*Virtual Private Network*
WAN	*Wide Area Network*

SUMÁRIO

1 INTRODUÇÃO 14
1.1 Apresentação do Problema 15
1.2 Justificativa e Relevância 16
1.3 Objetivos 17
1.3.1 Objetivo Geral 17
1.3.2 Objetivos Específicos 17

2 METODOLOGIA 18
2.1 Classificação da Pesquisa 18
2.1.1 Quanto aos fins 18
2.1.2 Quanto aos meios 18
2.2 Limitações do Método 19

3 REFERENCIAL TEÓRICO 20
3.1 Conceitos gerais de Guerra Cibernética 21
3.1.1 Evolução da Defesa Cibernética no Brasil e nas Forças Armadas 21
3.1.2 Espaço Cibernético 22
3.1.3 Guerra Cibernética 23
3.2 A concepção do Sistema Militar de defesa cibernética 23
3.3 Guerra Cibernética na Marinha do Brasil 25
3.4 Segurança da Informação e Comunicações (SIC) 26
3.5 Classificação das redes quanto à extensão geográfica 27
3.5.1 LAN 28
3.5.2 MAN 28
3.5.3 WAN 28
3.6 Conceitos do protocolo TCP/IP utilizados na filtragem de pacotes 29
3.6.1 Three-Way handshake do TCP 30
3.7 Defesa em profundidade 31
3.7.1 O Perímetro de segurança 32
3.7.1.1 Roteador de borda 32
3.7.1.2 Firewall com estado 33
3.7.1.3 Firewall proxy ou Gateway de aplicação 35

3.7.1.4 Zona desmilitarizada (DMZ) e Redes com triagem (screened subnets).....*36*
3.7.1.5 IDS.....*37*
3.7.1.6 IPS.....*38*
3.7.2 Rede Interna.....39
3.7.3 Fator humano.....39

4 DESCRIÇÃO E ANÁLISE DOS RESULTADOS 41
4.1 Importância da análise de logs da rede 43
4.2 Surgimento da plataforma SIEM.....43
4.3 Definição e processos gerais do SIEM 44
4.4 Desafios da implementação e benefícios do SIEM.....47
4.5 A importância do SIEM na Marinha do Brasil 50

5 CONCLUSÃO.....51
5.1 Considerações Finais.....51
5.2 Sugestões para Futuros Trabalhos.....52

REFERÊNCIAS.....53

1 INTRODUÇÃO

Existe uma rede de computadores, quando os computadores que são independentes estão interconectados através de uma única tecnologia. Essa interconexão permite que haja a troca de informações. (TANENBAUM, 2003).

Inicialmente, o sistema de redes de computares “[...]foi projetado com o objetivo de pesquisa, com a finalidade fundamental de estabelecer interatividade entre computadores, portanto, a segurança estava ausente no sistema” (COSTA, DA SILVA, DA CRUZ, 2012, p.79). Atualmente é impossível falarmos de rede de computadores e troca de informações sem ter a preocupação com a segurança. "A segurança da informação de uma empresa garante, em muitos casos, a continuidade de negócio, incrementa a estabilidade e permite que as pessoas e os bens estejam seguros de ameaças e perigos." [BLUEPHOENIX, 2008 apud ESPÍRITO SANTO, 2011, p.1].

“A nova fonte de poder não é o dinheiro nas mãos de poucos, mas informação nas mãos de muitos” (JOHN NAISBITT, apud MARQUES; ODA, 2012, p.135). Com mais essa afirmação, percebe-se que a informação traz grandes benefícios para aqueles que conseguem obtê-la e processá-la. Segundo Da Silva (2011a), obter informação é de suma importância para as Forças Armadas, pois utilizada de maneira correta, potencializa o emprego de recursos, humanos e materiais, nas atividades de inteligência, permitindo obter dados e fraquezas do adversário.

Garantir a segurança da informação de uma organização civil ou militar é uma tarefa complexa, pois de nada adianta serem estabelecidas barreiras e camadas de proteção, normas e procedimentos para serem seguidos, se o conjunto desse sistema não for eficiente. Em apropriação ao ditado popular, pode-se dizer que: a segurança da rede é tão forte quanto seu elo mais fraco.

A delimitação do tema adotada nesse trabalho apresenta o conceito de segurança em camadas bem como o funcionamento básico de alguns dos principais componentes de um perímetro de segurança (Firewall, IPS e antivírus), que são alguns dos diversos sistemas e dispositivos que podem fornecer logs para o sistema de Gerenciamento de eventos e Informações de Segurança (SIEM). Além disso, este trabalho destacará como a coleta, normalização e correlação dos dados realizadas pela solução SIEM são importantes para segurança de qualquer empresa. Por questões de segurança e sigilo, este trabalho não aborda detalhes de como o SIEM coleta, armazena, analisa e apresenta os dados.

1.1 Apresentação do Problema

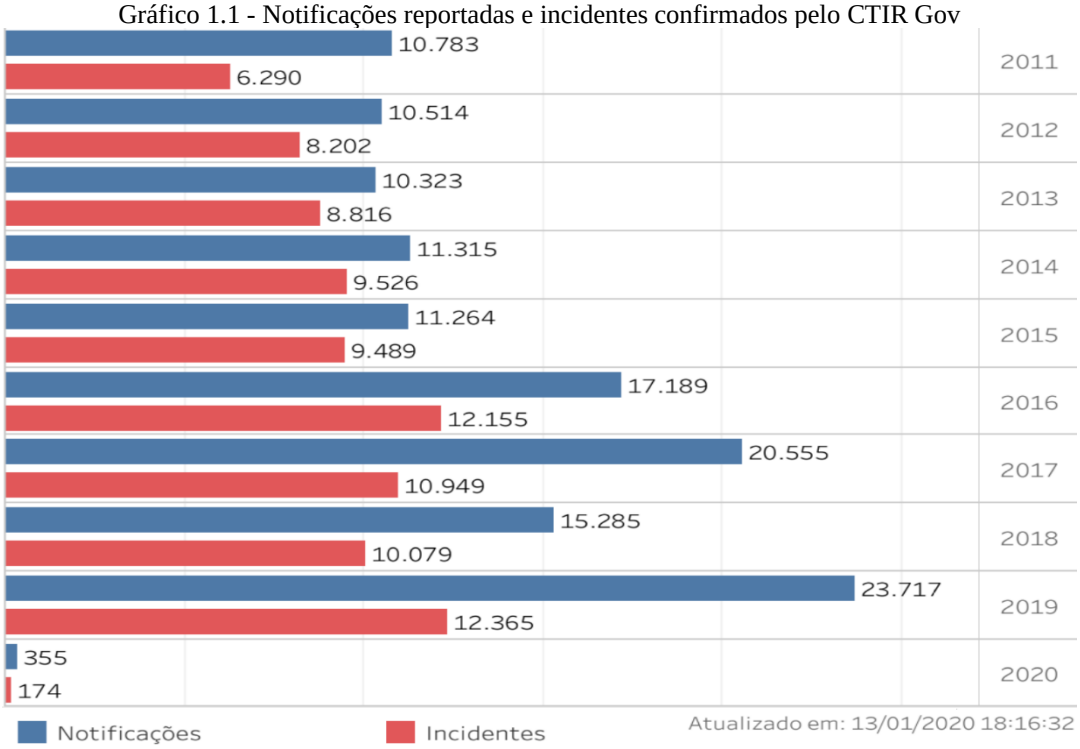
Ter a capacidade de operar sistemas conectados em rede trazem muitos benefícios, em virtude do compartilhamento de recursos e facilidade para disseminar informações. Entretanto, estar conectado em rede significa: “possibilitar condições específicas de controle com acesso externo aos recursos no contexto computacional, principalmente às informações” (COSTA, DA SILVA, DA CRUZ, 2012)

O problema em análise neste trabalho está relacionado aos incidentes de segurança da informação, que segundo Brasil (2019, p. 7-2), pode ser

> Indicado por um único ou por uma série de eventos, sequenciais ou não, de segurança da informação indesejados ou inesperados, por agentes internos ou externos, voluntários ou não, que tenham probabilidade de comprometer as operações de sistema de comunicações e ameaçar a segurança da informação.

Segundo o Centro de Tratamento e Respostas a Incidentes Cibernéticos de Governo (CTIR Gov), o número de incidentes de segurança confirmados no ano de 2019, foi de 12.365 eventos. Números que conforme demonstrado pelo gráfico 1.1, representa um recorde em relação a todos os dados registrados desde o ano de 2011.

Gráfico 1.1 - Notificações reportadas e incidentes confirmados pelo CTIR Gov



Fonte: CTIR Gov (2020)

Observa-se ainda que além dos incidentes confirmados, o ano de 2019 também superou, em relação ao registro de anos anteriores, o número de notificações de eventos reportados com 23.717 ocorrências relacionadas à atividade de tratamento de incidentes cibernéticos.

O problema em análise nesse trabalho consiste no entendimento de que nada adianta implementar várias camadas de segurança, investindo em diversos produtos de hardware e software, se as informações (registros de logs) geradas por esses sistemas não forem armazenadas, analisadas e correlacionadas possibilitando identificar atividades anômalas e incidentes de rede que não seriam evidentes se os eventos fossem analisados isoladamente. O grande desafio nesse processo é fazer o uso de tecnologia que possa filtrar, analisar e identificar incidentes de forma mais rápida e confiável.

1.2 Justificativa e Relevância

O número de ataques e incidentes de rede têm se intensificado no Brasil. É de vital importância que empresas e instituições como a Marinha do Brasil (MB), invistam e implementem barreiras e ferramentas para mitigar essas vulnerabilidades.

A justificativa pela escolha do tema foi motivada pelo fato de que o SIEM, apesar de ser utilizado por grandes empresas a algum tempo, ainda é uma ferramenta relativamente nova no âmbito das Forças Armadas, especificamente na Marinha do Brasil, onde vem ganhando espaço e mostrando ser uma forte aliada em prol da proteção dos recursos da rede.

Nos dias atuais onde tudo e todos estão conectados, a segurança de redes apresenta-se como uma necessidade para proteção e prosperidade dos negócios de uma empresa ou organização, fatos estes que evidenciam a importância e relevância do tema deste trabalho. (MENDONÇA, 2015)

A importância do estudo de plataformas de SIEM, se dá pelo fato de como elas focam em interligar a informação de diversos dispositivos da rede de maneira a tratá-los de forma centralizada, o que faz com que esse tipo de solução seja um grande aliado para garantia da segurança.

1.3 Objetivos

Nesta seção, serão descritos os objetivos gerais que representam a finalidade deste trabalho e os objetivos específicos, assunto dos quais o entendimento é de fundamental importância para que seja alcançado o objetivo geral.

1.3.1 Objetivo Geral

Como alicerce para se alcançar o objetivo deste trabalho, faz-se necessário analisar a importância da análise de logs da rede bem como os desafios e benefícios da implementação de uma plataforma SIEM na rede.

Com isso, o objetivo principal deste trabalho é destacar a importância da aplicação e contínuo desenvolvimento da aplicação de SIEM, como um agregador, capaz de fornecer uma visão centralizada e eficiente dos eventos, em prol da segurança contra ameaças internas e externas.

1.3.2 Objetivos Específicos

Para que o objetivo geral deste trabalho seja alcançado, faz-se necessário situar o leitor a respeito dos conceitos gerais de Guerra cibernética, classificação das redes e segurança da informação e comunicações.

Além desses, tem como objetivos específicos analisar os conceitos básicos do protocolo TCP/IP relacionados a filtragem de pacotes na rede e, em continuidade, elencar os conceitos e componentes presentes na técnica de defesa em profundidade e como os logs, que são os registros gerados por cada um dos componentes do perímetro de segurança, contribuem com o SIEM para potencializar a detecção de ataques e vulnerabilidades.

2 METODOLOGIA

Este capítulo apresenta a metodologia aplicada neste trabalho, por meio do qual foram definidos os instrumentos e fontes para coleta dos dados. As seções seguintes definem a classificação da pesquisa quanto aos fins e quanto aos meios, bem como as limitações das atividades e métodos aplicados.

2.1 Classificação da Pesquisa

A classificação da pesquisa quanto aos fins, nesse trabalho, é definida como descritiva. Já em relação a classificação metodológica quanto aos meios, é classificada como pesquisa bibliográfica e documental.

2.1.1 Quanto aos fins

A pesquisa é classificada como descritiva, pois, segundo Prodanov e De Freitas (2013), esse tipo de classificação visa descrever as características de determinado fenômeno ou estabelecer relações entre variáveis além de envolver o uso de técnicas padronizadas de coleta de dados. Ainda segundo os mesmos autores, esse tipo de pesquisa observa, registra, analisa e ordena os dados, buscando descobrir a frequência com que um fato ocorre, sua natureza, características e relações.

Esta pesquisa é classificada desta forma, pois expõe os principais componentes que compõem uma barreira para segurança das redes de computadores. Além disso, a coleta, análise e correlação dos registros realizados por cada um daqueles componentes são o objetivo fim do SIEM, que é o tema central deste trabalho.

2.1.2 Quanto aos meios

Com relação aos meios, para que o objetivo geral deste trabalho seja alcançado, foi utilizada a metodologia de pesquisa bibliográfica, que teve como fonte artigos de Websites, artigos científicos, livros, publicações em periódicos, dissertações e monografias, a maior parte relacionadas a assuntos sobre rede de computadores, segurança de redes e Guerra cibernética.

Para confecção deste trabalho também foi realizada uma pesquisa documental, com estudo baseado nas Normas de tecnologia da informação da Marinha, Plano estratégico de Tecnologia da Informação da Marinha, Doutrina Militar de defesa Cibernética do Ministério da Defesa e Manual de Campanha Guerra Cibernética do Exército Brasileiro. Além desses, também foram estudados relatórios de pesquisas, tabelas estatísticas e relatórios de empresas de segurança de redes e das informações digitais.

2.2 Limitações do Método

Esse trabalho tem como escopo o entendimento e a manutenção do uso do SIEM em conjuntos com outros componentes já existentes na rede da Marinha do Brasil com a finalidade de realizar um alarme antecipado e prover maior segurança em relação aos incidentes de redes.

Devido ao tema conter informações e aplicações muito específicas em relação a como e de onde o SIEM coleta, armazena, analisa, correlaciona e apresenta as informações, poucos documentos encontram-se em domínio público, pois a maioria dessas informações são sigilosas, limitando a pesquisa a tratar apenas dos aspectos gerais de como o sistema funciona e quais componentes fornecem essas informações para ele.

3 REFERENCIAL TEÓRICO

Os logs ou sistemas log, do inglês *System logs*, são uma fonte de dados universal que contém informações importantes como padrões de uso, status de execução, trilha de execução, entre outros ativos que são extremamente valiosos para que analistas de sistemas obtenham informações úteis para melhorar a integridade, estabilidade e usabilidade do sistema (DU; LI, 2016).

Em ambientes de grande volume de acesso e infraestrutura de diversos servidores, como é o caso da Marinha do Brasil, processar essa enorme quantidade de logs gerados e correlacioná-los de forma a identificar situações que podem ser um ataque ou até mesmo identificar uma vulnerabilidade de segurança, é um enorme desafio. Esse desafio é maior ainda já que a necessidade é que toda essa análise seja feita praticamente em tempo real para que possa surtir o efeito desejado. Para que surta efeito, além de coletar todos esses logs, seriam necessários centenas ou até milhares de analistas de sistemas trabalhando dia e noite, gerando uma despesa insustentável por qualquer empresa. Baseado nesse problema surgiu o SIEM.

O SIEM é a sigla para *Securty Information and Event Management*, que em tradução direta significa: Gerenciamento de Eventos e Informações de Segurança. Segundo Miller et al., (2010), o sistema de gerenciamento de eventos e informações de segurança é uma coleção complexa de tecnologias projetado para fornecer uma visão de forma clara do sistema coorporativo de Tecnologia da Informação (TI) como um todo, o que beneficia analistas de segurança e administradores de redes.

Para que um sistema SIEM seja eficiente é necessário que ele receba ou solicite as informações de logs de diversas soluções de segurança, como por exemplo firewall, proxy, sistemas de detecção de intrusão (IDS), entre outros, além de logs gerados pela própria infraestrutura como os switch, roteadores, servidores e máquinas que podem ter sistemas operacionais Windows, Linus ou Mac OS. Todos eles têm a capacidade de gerar e enviar logs.

Para melhor entendimento, antes de abordar o SIEM, serão apresentados neste capítulo um breve histórico sobre defesa cibernética e suas definições; conceitos básicos sobre defesa em profundidade, bem como os principais componentes de um perímetro de segurança e como cada um de seus componentes pode contribuir para a segurança da rede.

3.1 Conceitos gerais de Guerra Cibernética

Este capítulo tem como finalidade apresentar um breve histórico da criação e designação de responsabilidades sobre o assunto, bem como apresentar as características e definições acerca da Guerra Cibernética.

3.1.1 Evolução da Defesa Cibernética no Brasil e nas Forças Armadas

Logo na virada do século, o Brasil necessitava de capacidade para contrapor as ameaças, já que era nítido o aumento do risco de ataques por Estados, organizações ou qualquer grupo, com as mais diversas motivações e pretensões. (BRASIL, 2014)

Neste contexto, em 31 de agosto de 2001, foi criado por medida provisória, o Gabinete de Segurança Institucional da Presidência da República (GSI/PR), cuja competência é coordenar as atividades de Segurança da Informação. Em 8 de maio de 2006, dentro do GSI/PR, foi criado o Departamento de Segurança da Informação e Comunicações (DSIC), com a missão de planejar e coordenar a execução das atividades de Segurança da Informação e Comunicações (SIC) na Administração pública federal. Em novembro de 2009, por intermédio da Diretriz Ministerial n 0014, o Ministério da Defesa (MD), definiu providencias para cumprir a Estratégia Nacional de Defesa (END), que no ano anterior havia estabelecido prioridades estratégicas para defesa nacional nos setores nuclear, espacial e cibernéticos, estabelecendo responsabilidades para cada Força Armada. O setor cibernético ficou a cargo do Exército, enquanto que a Marinha e a Aeronáutica ficaram a cargo dos setores nuclear e espacial respectivamente. Em 2012, o Centro de defesa cibernética (CDCiber) foi incluído na estrutura regional do Exército, responsável pela coordenação e integração das atividades de Defesa Cibernética, no âmbito do Ministério da Defesa. No mesmo ano foi aprovado a política cibernética de Defesa, que foi atualizada em 2013 junto com a aprovação do livro branco de defesa nacional, cujos objetivos principais são desenvolver e manter atualizado a doutrina de emprego do setor cibernético. (BRASIL, 2014)

Para uma melhor visualização, a figura 3.1 apresenta em uma linha temporal a data de criação dos órgãos citados acima.

Figura 3.1 - Evolução da Defesa Cibernética

Fonte: Elaborado pelo autor, dados retirados da Doutrina Militar de Defesa Cibernética. Brasil (2014)

3.1.2 Espaço Cibernético

A chegada do século XXI trouxe novas ameaças e desafios. As missões e operações militares passaram a ser mais complexas e dinâmicas devido à expansão significativa dos computadores e principalmente da rede de dados empregadas para interligá-los, passa-se então a viver em um ambiente virtual, que foi sendo criado sem fronteiras, denominado Espaço cibernético. (GOMES, CORDEIRO, PINHEIRO, 2016)

> Cada vez mais computadores, seus equipamentos de interconexão, sistemas de comando, controle, comunicações e informação e sistemas de apoio à decisão compõem o espaço cibernético militar, em que a informação é o objetivo maior. Dessa forma, esse espaço se tornou fundamental na guerra, em decorrência da grande importância militar dos computadores e de suas redes para a circulação de ordens ou informações. (DA SILVA, 2014, p. 195)

As afirmações acima citadas, enfatizam ainda mais a importância de se manter uma mentalidade de segurança voltada ao espaço cibernético, já que a informação é o bem mais precioso nessa guerra.

3.1.3 Guerra Cibernética

Segundo Da Silva (2014), as informações que trafegam na rede, ou seja, no espaço cibernético, interligam navios, aeronaves, centros de controle estratégico, entre outros. A tentativa de invadir essas redes em busca de capturar segredos, publicá-los ou simplesmente usar em proveito próprio é o principal objetivo da guerra cibernética.

Conforme verificado em pesquisas realizadas, não existe uma definição única para guerra cibernética. No Brasil, a Marinha define como "ações ofensivas e defensivas destinadas a explorar, danificar ou destruir informações digitais, ou negar o acesso às suas informações. Tais ações utilizam-se de sistemas de informação e de redes de computadores". (BRASIL, 2007, p. 1-3)

Com uma definição mais ampla, o Ministério da Defesa define que a Guerra Cibernética

> corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de C² do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de Tecnologia da Informação e Comunicações (TIC) para desestabilizar ou tirar proveito dos Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC2) do oponente e defender os próprios STIC2. Abrange, essencialmente, as Ações Cibernéticas. A oportunidade para o emprego dessas ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação à TIC. (BRASIL, 2014, p. 19)

3.2 A concepção do Sistema Militar de defesa cibernética

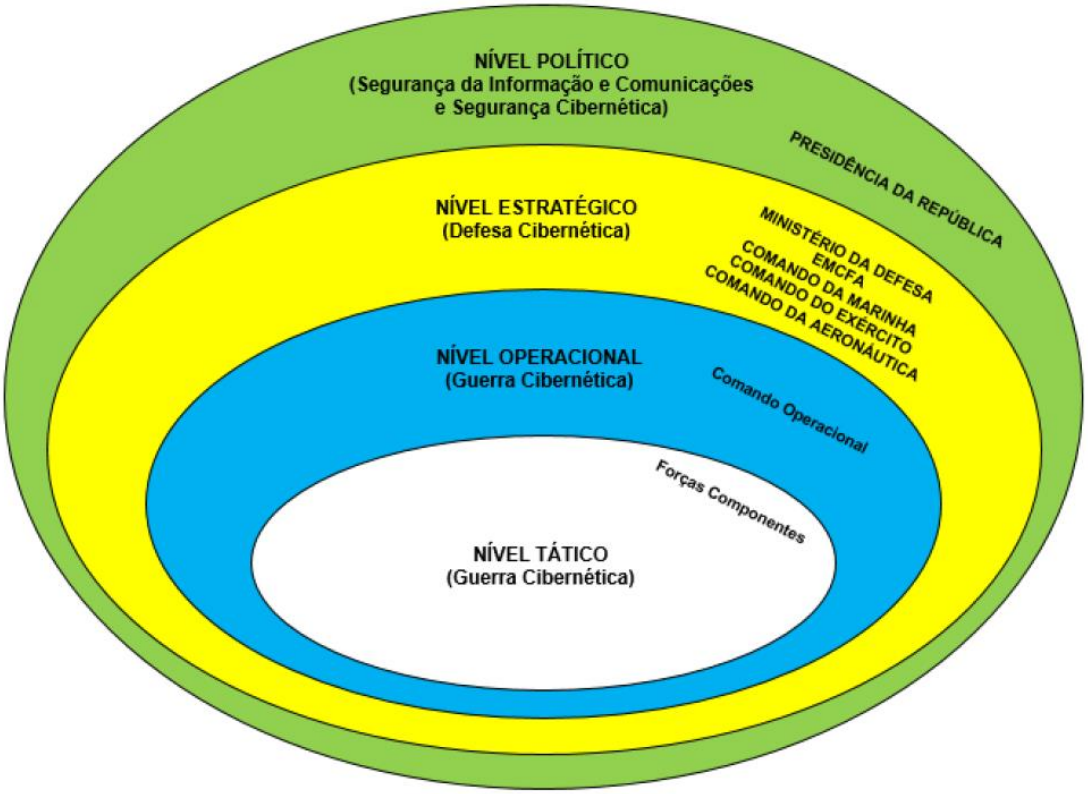
Por se tratar de um dos três setores de prioridade da Defesa Nacional, a Defesa Cibernética é missão das Forças Armadas, conforme referenciado na seção 3.1.1. Entretanto, a abrangência e peculiaridades do Espaço Cibernético tornam essa missão um verdadeiro desafio, que necessita do comprometimento de toda sociedade.

> A eficácia das ações de Defesa Cibernética depende, fundamentalmente, da atuação colaborativa da sociedade brasileira, incluindo, não apenas o MD, mas também a comunidade acadêmica, os setores público e privado e a base industrial de defesa. Nesse contexto, avulta de importância a necessidade de interação permanente entre o MD e os demais atores externos envolvidos com o Setor Cibernético, nos níveis nacional e internacional, conforme estabelece a END. (BRASIL, 2014, p. 25)

O Sistema Militar de Defesa Cibernética (SMDC) abrange um conjunto de instalações, doutrinas, tecnologias, serviços e pessoal que de forma coordenada busca realizar as atividades e ações de defesa do Espaço cibernético. (BRASIL, 2017)

A Doutrina Militar de Defesa Cibernética, Brasil (2014), classifica as ações no Espaço Cibernético de acordo com três níveis de decisão, que são o Nível Político, Nível Estratégico e o Nível Operacional e Tático. (figura 3.2)

Figura 3.2 - Níveis de decisão



Fonte: Brasil (2014)

Na esfera da administração pública, é de responsabilidade da Presidência da República, o Nível Político que compreende a Segurança da Informações e Comunicações e Segurança Cibernética. (BRASIL, 2014)

O Nível estratégico, que compreende a Defesa Cibernética, fica a cargo do Ministério da Defesa, Estado Maior Conjunto das Forças Armadas (EMCFA) e o Comando das Forças Armadas, por intermédio de seus respectivos órgãos de Defesa Cibernética e Centros de Tratamento de Incidentes de Redes (CTIR). O Centro de Tratamento de Incidentes de Redes da Marinha do Brasil (CTIR.mb) é o responsável pela implementação e controle do SIEM na MB, que é o objetivo de estudo deste trabalho. (BRASIL, 2014)

O Nível Operacional e Tático abrange as ações de Guerra Cibernética. O Operacional fica a cargo dos Comandos Operacionais e seus Estados-Maiores, caso sejam ativados. O Tático fica a cargo das Forças componentes com seus respectivos elementos de

Guerra Cibernética e o destacamento conjunto de Guerra Cibernética, caso sejam ativados. (BRASIL, 2014)

3.3 Guerra Cibernética na Marinha do Brasil

A Marinha do Brasil foi uma das instituições pioneiras na utilização de recursos informatizados na administração pública federal desde o final da década de 60. Como exemplo, foi a primeira das três Forças Armadas a empregar sistemas de armas computadorizados, com a aquisição das Fragatas Classe *Niterói*, na década dos anos 70. Além disso a MB realiza exercícios de Guerra Cibernética desde 2010. (DA SILVA, 2014; SALMON, 2018)

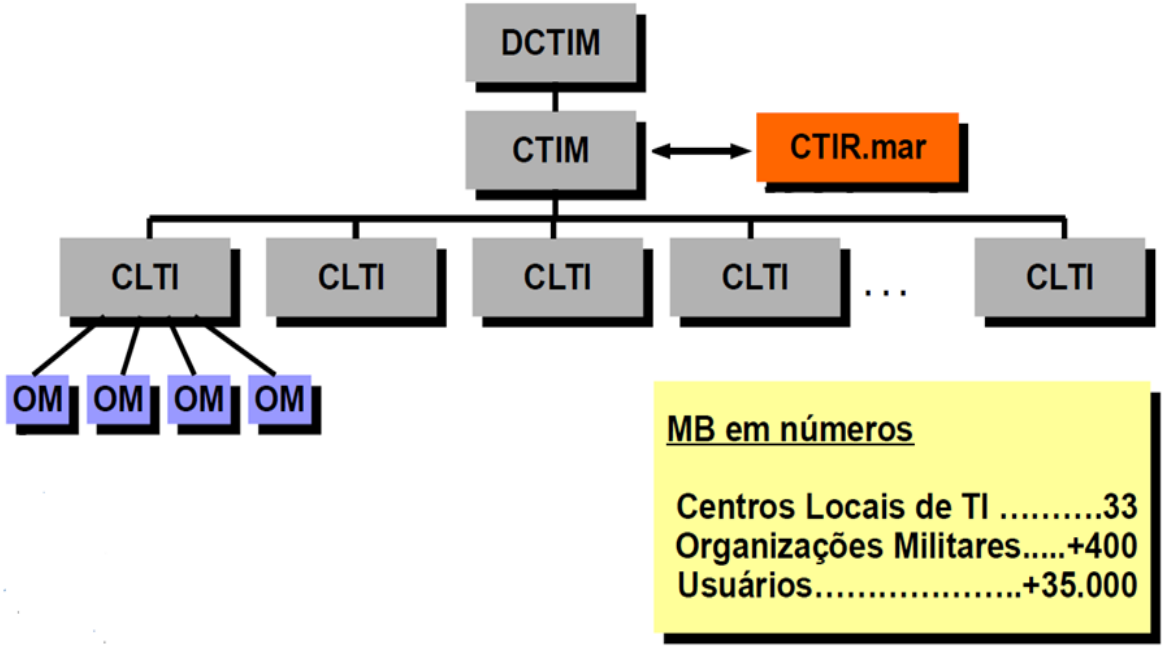
Com relação às organizações institucionais responsáveis pela proteção cibernética na MB, a Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM) é o órgão especializado que dentre outras atribuições, elabora normas, instruções técnicas e procedimentos padronizados na área da tecnologia da informação da MB, além de realizar ações de segurança, auditoria computacional, guerra cibernética, criptológica e forense computacional. (ASSIS, 2019; BRASIL, 2007).

Outro órgão fundamental na defesa cibernética é o Centro de Tecnologia e Informação da Marinha (CTIM). Subordinado diretamente à DCTIM, o CTIM tem a missão de implantar, gerenciar, operar e manter os sistemas de proteção da Rede de Comunicações Integradas da Marinha (RECIM), que por intermédio do CTIR.mar monitoram por exemplo firewalls, proxy, sistema de detecção de Intrusão (IDS) e o SIEM, que são abordados na seção 3.7.1 deste trabalho. Dentre outras tarefas, o CTIM tem a responsabilidade de salvaguardar informações digitais e guiar ações relacionadas à Guerra Cibernética. (ASSIS, 2019; BRASIL, 2007; SALMON, 2018).

Atuando como elementos organizacionais de apoio, os Centros Locais de Tecnologia da Informação (CLTI) são subordinados à CTIM. Compete aos CLTI: configurar, operar e manter, em primeiro escalão, os recursos de telecomunicações da MB e da infraestrutura da RECIM, além de apoiar o CTIM na solução de problemas que necessitem de ações de reparo para o restabelecimento da RECIM, entre outras atribuições. (BRASIL, 2007)

A figura 3.3 representa um organograma simplificado de subordinação dos componentes de proteção cibernética na MB.

Figura 3.3 - Principais componentes da Proteção Cibernética na MB



Fonte: Retirado do 1° Simpósio Regional de Segurança Cibernética Comando do 5° Distrito Naval. Salmon (2018). Modificado pelo autor.

Além desses, existem o Centro de Ações de Guerra Cibernética do Comando de Operações Navais (ComOpNav), responsável por coordenar recursos e ações em resposta à um possível ataque cibernético, o Centro de Inteligência da Marinha (CIM), o Centro de Análises de Sistemas Navais (CASNAV) e o Centro de Apoio a Sistemas Operativos (CASOP). (ASSIS, 2019)

Com relação aos documentos e normas, a Marinha do Brasil, além de seguir os principais documentos relacionados a Defesa Cibernética citadas na seção 3.1.1, também possui documentos específicos a respeito da segurança das comunicações e informações. As principais publicações são: EMA-416 que é a Doutrina de Tecnologia da Informação da Marinha, o DGMM-0540 atinente as Normas de tecnologia da informação da Marinha e o Plano Estratégico de Tecnologia da informação da Marinha (PETIM). (BRASIL, 2007; BRASIL, 2016; BRASIL, 2019).

3.4 Segurança da Informação e Comunicações (SIC)

O Comitê Gestor de Segurança da informação, sob a aprovação da Secretaria Executiva do conselho de defesa nacional, elaborou a Instrução Normativa nº 01 do Gabinete de Segurança Institucional da Presidência da República (IN nº 01 GSI/PR/2008) de 13 de junho de 2008. A IN nº 01 GSI/PR/2008 tem o objetivo de nortear as atividades de SIC, apresentando

orientações para a Gestão de Segurança da Informação e Comunicações (GSIC), que devem ser implementadas direta ou indiretamente pelos Órgãos da Administração pública Federal. (BRASIL, 2008)

Segundo a DGMM-0540, que adere ao proposto pela IN nº 01 GSI/PR/2008 com relação as práticas de SIC, cita que a informação é um bem de valor inestimável, que

> [...] pode estar impressa em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma apresentada ou o meio através do qual a informação é compartilhada ou armazenada, é fundamental que ela seja sempre protegida adequadamente. (BRASIL, 2019, p. III-2)

A fim de buscar proteção adequada face as ameaças e vulnerabilidades do tráfego e dos ambientes que armazenam e processam a informação, a SIC, é definida como um conjunto de medidas e ações, cujo objetivo é viabilizar os requisitos de confidencialidade, autenticidade, integridade e disponibilidade que podem ser definidas como (BRASIL, 2019):

a) **Confidencialidade**: propriedade que garante o sigilo da informação, ou seja, nenhuma pessoa, sistema, órgão ou entidade não autorizada, pode ter acesso à informação.
b) **Autenticidade**: garante que a informação realmente foi produzida, expedida, modificada ou destruída por uma pessoa, órgão ou sistema.
c) **Integridade**: assegura que determinada informação não foi modificada ou destruída sem autorização, mesmo que de maneira acidental.
d) **Disponibilidade**: assegura que a informação esteja acessível e utilizável quando solicitada por pessoa física, órgão ou sistema.

3.5 Classificação das redes quanto à extensão geográfica

Esta seção tratará das redes classificadas como LAN, MAN e WAN, tanto em relação as suas definições gerais, quanto como cada uma delas é representada na MB. Além dessas, existem também as redes classificadas como SAN e PAN, que correspondem, respectivamente, à rede de área de armazenamento e rede de área pessoal, e que não serão abordadas por não terem relevância para o trabalho em questão.

3.5.1 LAN

Uma *Local Area Network* (LAN), que também é conhecida como rede local, compreende uma rede com cobertura limitada. Conecta dispositivos eletrônicos através de meios físicos como fios metálicos, cabos e fibras ópticas, possibilitando o compartilhamento de recursos e trocas de informação. (FRANCISCATTO, DE CRISTO, PERLIN, 2014)

Segundo as normas técnicas de tecnologia da informação da Marinha, 2019, seu limite geográfico é normalmente limitado por um prédio, uma Organização Militar (OM) ou complexos compostos por OM vizinhas. Possuem altas taxas de transmissão e baixo custo. Estão associadas as redes internas das OM e aos complexos de OM como por exemplo Complexo Naval de Mocanguê, complexo Naval de Abastecimento da Av. Brasil. (BRASIL, 2019; FRANCISCATTO, DE CRISTO, PERLIN, 2014)

3.5.2 MAN

A *Metropolitan Area Network* (MAN) é a rede metropolitana e compreende um espaço de média dimensão. Uma MAN está associada a interligação de várias LAN`s e pode ser considerada uma parte menor da WAN. A rede metropolitana representa as Redes dos Distritos Navais, que são compostas por redes locais interligadas localizadas na mesma área geográfica, como por exemplo a rede do Comando do Primeiro Distrito Naval (Com1DN). (BRASIL, 2019; FRANCISCATTO, DE CRISTO, PERLIN, 2014)

3.5.3 WAN

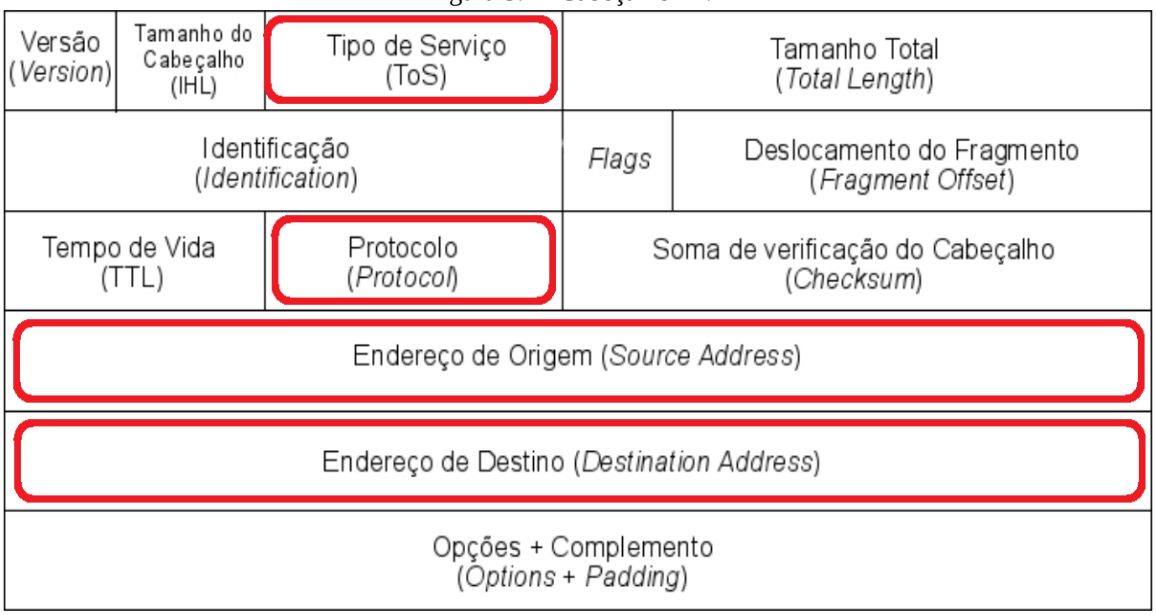
Chamada de rede de área grande, a *Wide Area Network* (WAN), corresponde a uma rede que abrange grande área geográfica, caracterizada pela comunicação a longas distâncias. Para cobrir essa área, normalmente são utilizados enlaces de fibra óptica e de satélites. A WAN pode ser composta por diversas MAN ou LAN interligadas. Para aplicação e utilização da Marinha do Brasil, devido a cobertura dessas distancias, os enlaces são contratados junto aos provedores de serviço de comunicações. (BRASIL, 2019; FRANCISCATTO, DE CRISTO, PERLIN, 2014)

3.6 Conceitos do protocolo TCP/IP utilizados na filtragem de pacotes

Para que os sistemas de uma rede se comuniquem adequadamente, é necessário que estejam falando a mesma língua, ou seja, que estejam se comunicando através de um mesmo protocolo. O TCP/IP é um conjunto de protocolos de comunicação utilizados na internet, em que as informações ou dados que se deseja encaminhar são divididos em partes manipuláveis, conhecidas como *pacotes*. Para que sejam identificados, cada pacote possui fixado em seu início, pequenos segmentos de informações que o identificam, denominado *cabeçalho*. (NORTHCUTT et al., 2002)

Os pacotes são direcionados, ou seja, roteados com base nos dados de seus cabeçalhos. O cabeçalho é composto por diversas informações, entretanto com base no escopo desse trabalho, apenas quatro delas serão abordadas. São elas: endereço IP de origem, endereço IP de destino, a identificação do protocolo presente na área de carga e o tipo de serviço ao qual o pacote oferece suporte. A figura 3.4 ilustra um cabeçalho IPv4 completo, com destaque nos itens dos campos anteriormente citados.

Figura 3.4 - Cabeçalho IPv4



Fonte: Tanenbaum (2003). Modificado pelo autor

Segundo Northcutt et al., (2002), o *Transmission control protocol* (TCP) é uma maneira segura de ser transportar informações, já o *User Datagram Protocol* (UDP) é um protocolo que não oferece nenhum tipo de segurança. Ambos utilizam portas para fazer o

transporte de dados. Algumas portas, inferiores a porta 1023, são reservadas para se comunicar com um servidor executando determinado serviço, por exemplo a porta 80 é reservada para o serviço de HTTP, e a porta 53 para o DNS, entre muitos outros casos. Já um cliente sempre utilizará uma porta superior a 1023. Para melhor entendimento, segue um exemplo

> Quando um cliente contata um servidor, ele específica aleatoriamente uma porta com número superior a 1023 para utilizar. Depois, o cliente contata o servidor em uma porta definida, como a porta 23 para Telnet. Quando o servidor responde, as informações saem na porta 23 e retornam para o cliente na porta >1023 aleatória, onde são deixados. Essa é a única maneira pela qual um filtro de pacotes pode determinar o serviço que está sendo filtrado. (NORTHCUTT et al., 2002, p. 24)

Na citação acima, caso fosse necessário bloquear todo tráfego do tipo Telnet destinado a sua porta padrão, deveria ser criado uma regra na lista de controle de acesso no dispositivo de segurança no qual se está usando o filtro (por exemplo um roteador de borda), afim de bloquear todo tráfego que esteja direcionado para a porta 23.

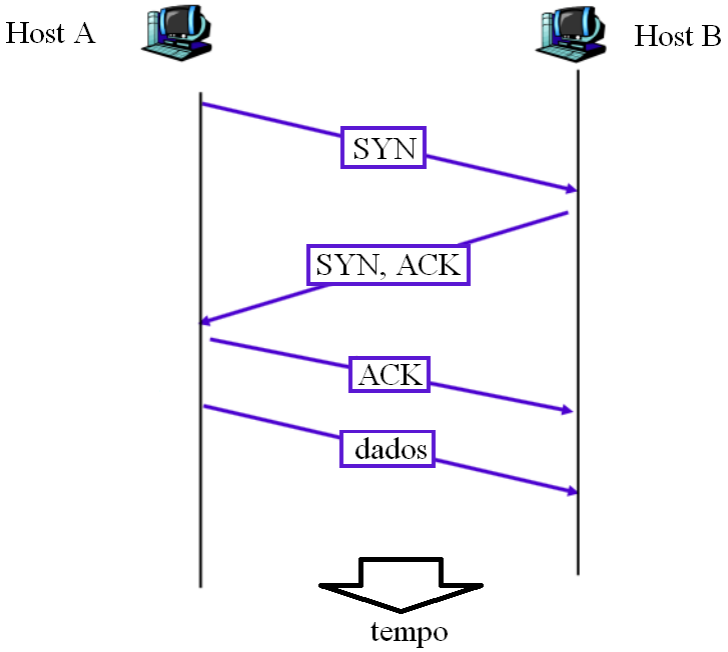
3.6.1 Three-Way handshake do TCP

No protocolo TCP, para se iniciar uma comunicação é necessário usar o *three-way handshake*, que é um protocolo que executa 3 etapas para estabelecer uma conexão virtual entre a origem e o destino. O livro desvendando segurança em redes, cita o seguinte exemplo para se estabelecer conexão entre o host A e o host B.

> Quando o host A deseja se conectar com o host B para transferir dados, ele precisa informar ao host B que ele deseja se conectar. O host A faz isso enviando um pacote para o host B com o flag SYN (sincronização) ativado, significando “Quero iniciar uma nova conversação.” Se o host B puder e quiser conversar com o host A, ele retorna um pacote com os flags SYN e ACK (confirmação) ativados, significando “Está bem, vamos conversar”. Finalmente, o host A retorna a terceira parte do handshake, um pacote com o flag ACK ativado, significando “Fico feliz que você queira conversar, então vamos falar!” Com isso, os dados começam a ser transferidos. (NORTHCUTT et al., 2002, p. 24)

A figura 3.5 demonstra de maneira simplificada o estabelecimento da conexão TCP com o *three-way handshake*:

Figura 3.5 - Estabelecimento da conexão TCP 3-way handshake



Fonte: Elaborado pelo autor

Baseado nas flags SYN e ACK é possível verificar em qual fase da tentativa de conexão o processo se encontra, ou seja, se é uma tentativa de iniciar uma conexão, ou uma resposta à solicitação de início de conexão, ou uma resposta final do estabelecimento da conexão. Um sistema de filtro de pacotes baseia-se nessas flags para verificar em que fase se encontra o processo do *three-way handshake*. (NORTHCUTT et al., 2002)

3.7 Defesa em profundidade

Para o melhor entendimento do que representa o conceito de defesa em profundidade, os autores do livro *Desvendando segurança em redes: o guia definitivo para fortificação de perímetro de Rede usando Firewalls, VPNs, Roteadores e Sistemas de detecção de intrusão*, fazem uma analogia de que a segurança da rede deve ser como uma cebola. “Quando você descasca a camada da mais externa, muitas camadas permanecem por baixo dela. Nenhum conceito transmite mais importância ao discutirmos segurança de rede do que a defesa em profundidade” (NORTHCUTT et al., 2002, p. 7)

Segundo Franceschett, Onça e Fernandes (2017), a funcionalidade da defesa em profundidade ou defesa em camadas foi pensada baseada em uma estratégia militar, que tem o objetivo, de pelo menos, atrasar o ataque. Com mais tempo para chegar ao alvo, o sistema de defesa tem um intervalo maior para detectar o ataque e reagir.

Baseado nessas definições e analogias, percebe-se que o uso dessa técnica melhora a proteção dos recursos de rede, pois mesmo que uma das camadas seja comprometida, haverá outras, cada uma delas com suas próprias características para prover a defesa.

A defesa em profundidade envolve o *perímetro*, a *rede interna* e um *fator humano*, em que "cada um desses fatores inclui muitos componentes, que isoladamente, não são suficientes para proteger uma rede. O segredo está no fato de que cada componente complementa os outros para formar um quadro de segurança completo" (NORTHCUTT et al., 2002, p. 8)

3.7.1 O Perímetro de segurança

O perímetro é uma *borda fortificada*, uma *linha imaginária*, que separa a rede e dispositivos ao qual se quer proteger de outras redes e da própria internet. Fazer a segurança de perímetro consiste em controlar tudo que tenta ultrapassar essa barreira. Um perímetro de segurança pode ser composto por diversos componentes. (NORTHCUTT et al., 2002)

Nessa seção serão abordados seus principais componentes, que além de proverem segurança, são capazes de gerar e disponibilizar logs para o SIEM, que é o principal objeto de estudo desse trabalho.

3.7.1.1 Roteador de borda

O objetivo primário de um roteador é interligar duas ou mais redes, realizando o encaminhamento de pacotes de um segmento de rede para outro. Entretanto, dependendo de seu posicionamento dentro da estrutura da rede, o roteador pode ser projetado com medidas de segurança internamente embutidas, como por exemplo, suporte para filtro de pacote, recursos de Firewall com estado, entre outros. (NORTHCUTT et al., 2002)

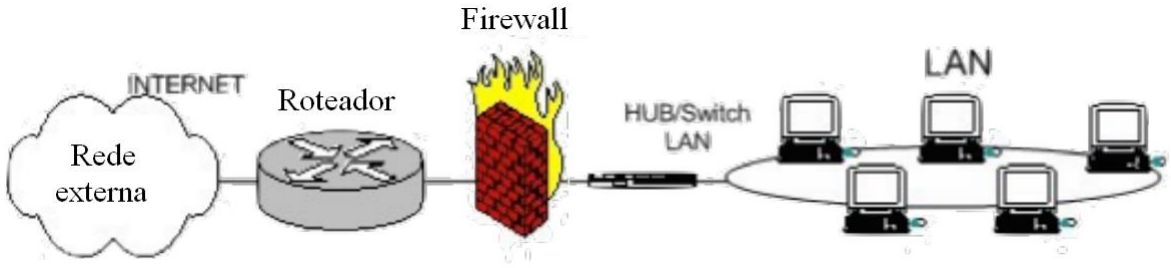
O roteador de borda está posicionado de maneira que seja o último do qual se tem controle antes da uma rede externa, logo ele não é apenas um roteador de tráfego entre redes, ele precisa oferecer segurança e por esse motivo é utilizado o *roteador de borda com filtro de pacotes*. A funcionalidade do filtro de pacotes, se baseia em regras que formam as listas de controle de acesso e baseada nela os pacotes são autorizados a trafegar ou não entre as redes. Vale ressaltar que um filtro de pacotes não possui a capacidade de distinguir os tipos de tráfego de rede, ou seja, não se aprofundam na análise do fluxo do tráfego. O filtro de pacotes bloqueia ou permite o tráfego, simplesmente baseado no endereço IP de origem. Em outras palavras ele

não tem a capacidade de filtrar com base no endereço de destino ou número de porta, entretanto, como primeira linha de defesa isso já traz uma grande vantagem, pois seu processamento é mais rápido do que um firewall por exemplo, e já consegue bloquear certos tipos de ameaças, como os endereços não autorizados em função do conjunto de regras de ingresso e egresso. (NORTHCUTT et al., 2002)

3.7.1.2 Firewall com estado

Um firewall é um dispositivo que combina hardware e software com a mesma função do roteador de borda. Entretanto, possui regras mais detalhadas, pois faz o monitoramento das conexões em uma *tabela de estado*, permitindo ou bloqueando o tráfego de pacotes, baseado em uma política de controle de acesso. Esses registros do tráfego na tabela de estado é um exemplo de log, registro, gerado pelo firewall. A figura 3.6 apresenta um exemplo de topologia de rede com o firewall posicionamento logo após um roteador com filtro de pacotes. (NORTHCUTT et al., 2002; VIDAL, 2006)

Figura 3.6 - Topologia de um roteador de borda e firewall



Fonte: Retirado da apresentação Segurança de redes: Firewall, do professor Raulino. Raulino (201-?). Modificado pelo autor.

Nas palavras de Northcutt et al., (2002), o termo *estado* representa a condição de pertencer a determinada seção de comunicação, ou seja, em qual fase da tentativa de conexão o processo se encontra, se é uma tentativa de iniciar uma conexão, ou uma resposta à solicitação de início de conexão, ou uma resposta final do estabelecimento da conexão, como citado na seção 3.6.1 deste trabalho. Esse controle é realizado em uma tabela de estado onde cada entrada mantém informações que identifica a seção de comunicação que ela representa. Diferentemente de um roteador de filtro de pacotes que apenas analisa o endereço de IP de origem, o firewall com estado baseia-se em outras informações. As principais delas incluem: (NORTHCUTT et al., 2002; VIDAL, 2006)

a) Endereço IP de origem (de onde supostamente vem o pacote)
b) endereço de destino
c) flags SYN e ACK citadas na seção 3.6.2 deste trabalho
d) protocolo de aplicação que está sendo utilizado
e) porta de destino e origem
f) número de sequencias do pacote

Baseando-se nessas informações o funcionamento ocorre da seguinte maneira:

> Uma entrada na tabela de estado é criada quando uma conexão é iniciada através de um dispositivo com estado. Depois, quando o tráfego retorna, o dispositivo compara a informação do pacote com a informação da tabela de estado, determinando se ela faz parte de uma seção de comunicação atual. Se o pacote estiver relacionado a uma entrada atual na tabela, ele tem permissão para passar. (NORTHCUTT et al., 2002, p.56)

Com relação à segurança, com o estabelecimento desse tipo de controle de conexão, registrando o fluxo da rede em um log, é possível bloquear o tráfego que não esteja estabelecido na tabela de estado.

O estado da conexão TCP é verificado observando-se os flags (SYN e ACK), que estão sendo transportados no cabeçalho dos pacotes. Fazer o acompanhamento das informações de flags em combinação com o endereço de IP e endereço da porta para cada uma das partes da comunicação, mais os números de sequência e confirmação dos pacotes enriquecem a tabela de estado e consequentemente a segurança do firewall, bloqueando ataques de réplicas. (NORTHCUTT et al., 2002)

O preço pago para todo esse controle, como geração de logs, é um custo geral de processamento e desempenho. De acordo com Northcutt et al., (2002), esse tipo de inspeção com estado monitora as informações da camada 4 (camada de transporte) além de acrescentar exame em nível de aplicação (camada 7 do modelo OSI) para fornecer os detalhes sobre a seção de comunicação, o que aumenta a segurança contra fluxos de tráfego TCP/IP fora do padrão. Logo, o firewall com estado oferece muito mais segurança do que um simples filtro de pacote e apesar de exigir mais performance, ainda possui uma necessidade de desempenho inferior a um firewall proxy. Contudo, apesar da inspeção com estado ter vantagens de desempenho em relação ao firewall proxy, também o torna menos seguro para os casos onde se faz necessário considerar todos os aspectos da comunicação em nível de aplicação.

3.7.1.3 Firewall proxy ou Gateway de aplicação

Um proxy de nível de aplicação é um programa de software do tipo cliente/servidor, que oferece comunicação via protocolos da internet, normalmente com base no TCP/IP. Sua implementação é focada em oferecer comunicação entre a rede interna e a internet. Segundo Northcutt et al., (2002), um servidor proxy pode atuar em prol do cliente para acessar um determinado serviço da rede, disponível na internet, e proteger cada um dos lados contra uma conexão direta. Em outras palavras, o firewall proxy funciona como um intermediário entre os hosts envolvidos na comunicação, realizando inspeção de conteúdo dos pacotes para garantir concordância com o protocolo indicado pelo número da porta de destino.

Um proxy, consegue evitar que *hosts* na rede interna sejam acessíveis diretamente pela rede externa. Para isso o proxy mantém duas conexões distintas, uma entre o cliente (nesse caso a máquina da rede interna) com o firewall (servidor *proxy*) e outra conexão entre o servidor *proxy* e o servidor real (servidor da internet ao qual se quer estabelecer conexão). Os proxies são mais utilizados para os serviços de acesso à web (HTTP), correio eletrônico e transferência de arquivos (FTP – File Transfer Protocol), serviços que necessitam de troca de informações com a internet. (LIMA, DE GEUS, 1999; NORTHCUTT et al., 2002)

O Gateway de aplicação possui diversas vantagens em relação a outros tipos de firewall, algumas delas são:

a) Pelo fato de os servidores proxy não permitirem comunicação direta entre os servidores externos e os computadores da rede interna, os endereços IP internos não são enxergados externamente, logo são protegidos contra o mundo exterior; (NORTHCUTT et al., 2002)
b) O firewall proxy possibilita a segurança baseada no usuário, sendo eficaz para impedir o uso não autorizado com base em cada usuário; e (NORTHCUTT et al., 2002)
c) Como o firewall da camada de aplicação tem a capacidade de codificar a informação de cabeçalho da camada de aplicação, podem oferecer relatório de log de auditoria mais detalhado. (LIMA, DE GEUS, 1999)

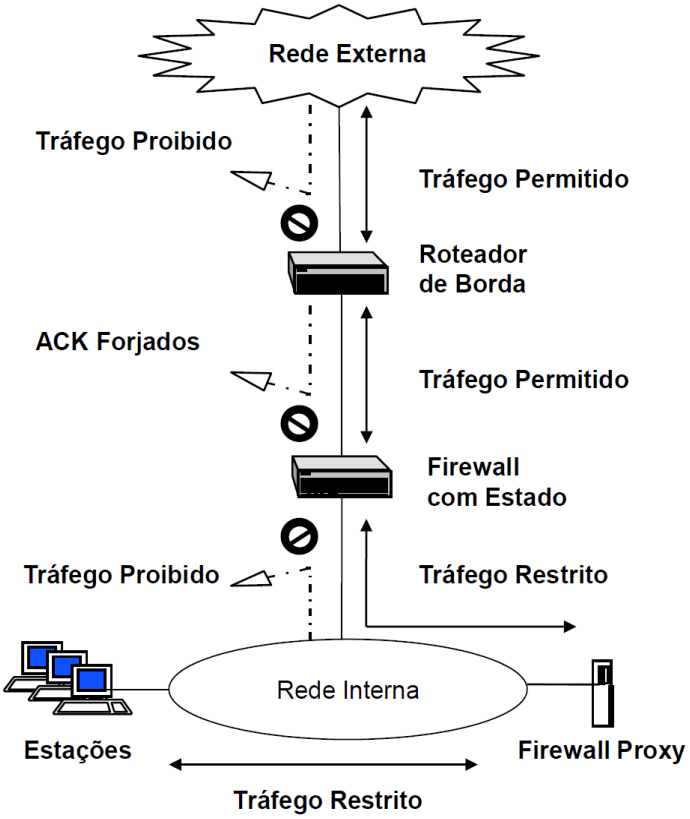
Embora os firewalls proxy ofereçam diversas vantagens de segurança em relação aos firewalls com estado, algumas desvantagens devem ser levadas em consideração:

a) Devido a todo processamento adicional exigido para a inspeção do pacote a nível de aplicação, há redução de desempenho, consequentemente os proxies de aplicação são mais lentos do que os com estado; e (LIMA, DE GEUS, 1999)

d) Para cada nova aplicação ou protocolo é necessário desenvolver um novo proxy adaptado para esse fim. (NORTHCUTT et al., 2002)

Baseado nas vantagens e desvantagens de cada um dos componentes do perímetro citados até o momento, começa a ficar claro a importância de se estabelecer um perímetro que seja composto por todas essas ferramentas. A figura 3.7, exemplifica um dos possíveis esquemas de um perímetro de segurança composto por roteador de borda, firewall de estado e firewall proxy.

Figura 3.7 - esquema 1 – perímetro de segurança



Fonte: Retirado da aula de Segurança em redes de computadores, Volume 4, slide 11, do Professor Ph. D. ciências em informática, Engenheiro de Computação, Anderson Oliveira da Silva. Da Silva (2019)

3.7.1.4 Zona desmilitarizada (DMZ) e Redes com triagem (screened subnets)

Os termos DMZ e *screened subnets* são utilizados em redes que contém servidores públicos conectados diretamente ao firewall e protegido pelo mesmo. DMZ é a sigla para o *desmilitarized zone*.

> O termo DMZ originou-se durante a Guerra da Coréia, quando uma faixa de terra no paralelo 38 estava fora de limites militares. Uma DMZ é uma área desprotegida entre áreas seguras. Exatamente como a DMZ na Coréia estava na frente de quaisquer defesas, a DMZ, quando aplicada às redes, está localizada fora do firewall. (NORTHCUTT et al., 2002, p. 6).

Uma *screened subnet* ou rede com triagem é uma rede isolada protegida por um firewall que realiza a triagem, ou seja, a seleção do tráfego que tem autorização para passar e para qual destino específico. É utilizada para separar servidores que necessitam estar disponíveis pela internet por meio de sistemas usados unicamente pelos usuários internos. A rede com triagem hospeda serviços públicos, como por exemplo: serviços de e-mail e Web. (NORTHCUTT et al., 2002)

Com relação ao posicionamento em um perímetro de segurança, uma DMZ está localizada na frente (antes) do firewall, enquanto que a rede de triagem está atrás dele.

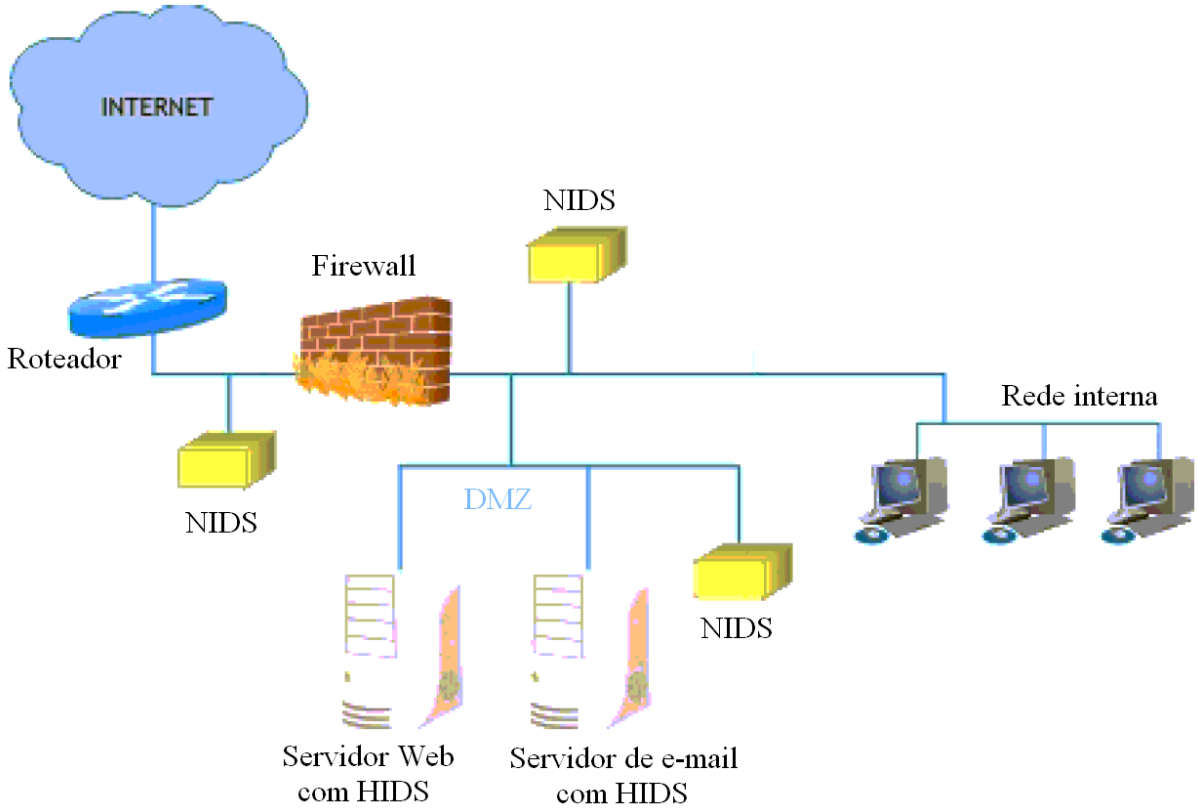
3.7.1.5 IDS

O *Intrusion Detection System* (IDS), que em português é o Sistema de Detecção de Intrusão, é um monitorador de processos que estão rodando em uma rede ou em um host, cujo objetivo é monitorar e analisar o tráfego a fim de detectar ataques e possíveis incidentes de segurança. É um sistema que além de ter a capacidade de reconhecer potenciais ataques, pode identificá-lo e emitir alertas ao administrador da rede. Os IDS são:

> [...] ferramentas de software ou *appliance* utilizadas em conjunto com outros mecanismos de segurança tais como *firewalls*, antivírus e mecanismos de criptografia para reforçar a segurança de um ambiente de rede, relatando eventos suspeitos ou impedindo que ações maliciosas tenham êxito e se propaguem pela rede. (SILVA, 2008, P. 57)

Existem alguns tipos de IDS, entretanto esse trabalho abordará os dois mais comumente utilizados que são o *Host-based Intrusion Detection System* (HIDS) e o *Network Intrusion Detection System* (NIDS). Os IDS baseados em host (HIDS), são instalados diretamente em cada máquina ao qual se deseja monitorar, analisando os registros de aplicações nos arquivos de log, eventos de acesso, modificações de sistemas de arquivos, entre outros. É a última linha de defesa, caso o ataque consiga atravessar o firewall e o NIDS. Já os IDS baseados em rede (NIDS), são instalados em segmentos de rede que estão conectados ao firewall, ou em pontos críticos da rede. Detectam intrusos com base na análise do tráfego da rede como um todo, monitorado múltiplos hosts. A figura 3.8, esquematiza um exemplo de uso do NIDS e HIDS. (CLARO, 2015; EVANGELISTA, 2008; NORTHCUTT et al., 2002)

Figura 3.8 - Modelo de arquitetura com NIDS e HIDS



Fonte: Evangelista (2008). Modificada pelo autor

Segundo Evangelista (2008), é comum inserir um NIDS antes do firewall, a fim de impedir que um usuário externo venha conhecer a topologia de rede; um depois do firewall, na DMZ, para detectar alguma ameaça que o firewall não tenha conseguido detectar; e um para detectar ataques que possam vir da rede interna. Já os HIDS são instalados em servidores de alto risco, tais como servidor web e servidor de e-mail, que possuem conexão com a rede externa. (CLARO, 2015; EVANGELISTA, 2008)

3.7.1.6 IPS

O Sistema de Prevenção de Intrusão (*Intrusion Prevention System* – IPS) surgiu a partir dos IDS e o complementa, pois, além de detectar um possível ataque, fornece a possibilidade de prevenção. Em outras palavras, enquanto o IDS detecta tentativas de ataque, faz o registro e os envia ao administrador da rede, o IPS além de detectar e registrar, executa contramedidas adicionais para bloquear as intrusões em tempo real. (CLARO, 2015; EVANGELISTA, 2008)

3.7.2 Rede Interna

Compondo o conceito de defesa em profundidade, a rede interna é a rede ao qual se quer proteger contra ameaças. Segundo Northcutt et al. (2002, p. 13), “é a rede que está protegida pelo perímetro que contém todos os servidores, estações de trabalho e infraestrutura com a qual uma empresa conduz seus negócios.”

As ameaças a uma rede interna não se limitam apenas a ataques externos, que tentam invadir e burlar o perímetro de fora para dentro. A ameaça pode partir de dentro da própria rede, mesmo que usuários sejam de confiança e não tenham intenção de prejudicar a empresa, basta um desconhecimento ou descuido para que isso permita a proliferação de um vírus. Por esse motivo é necessário restringir acesso e controlar tráfego de entrada e saída, baseado em uma rígida política de segurança. (NORTHCUTT et al., 2002)

Uma das melhores ferramentas para verificar o fiel cumprimento da política de segurança, ou seja, das normas de SIC estabelecidas pela organização, é a realização periódica de auditorias. Por intermédio das auditorias é possível estabelecer ações corretivas e divulgar a mentalidade de SIC. (BRASIL, 2019; NORTHCUTT et al., 2002)

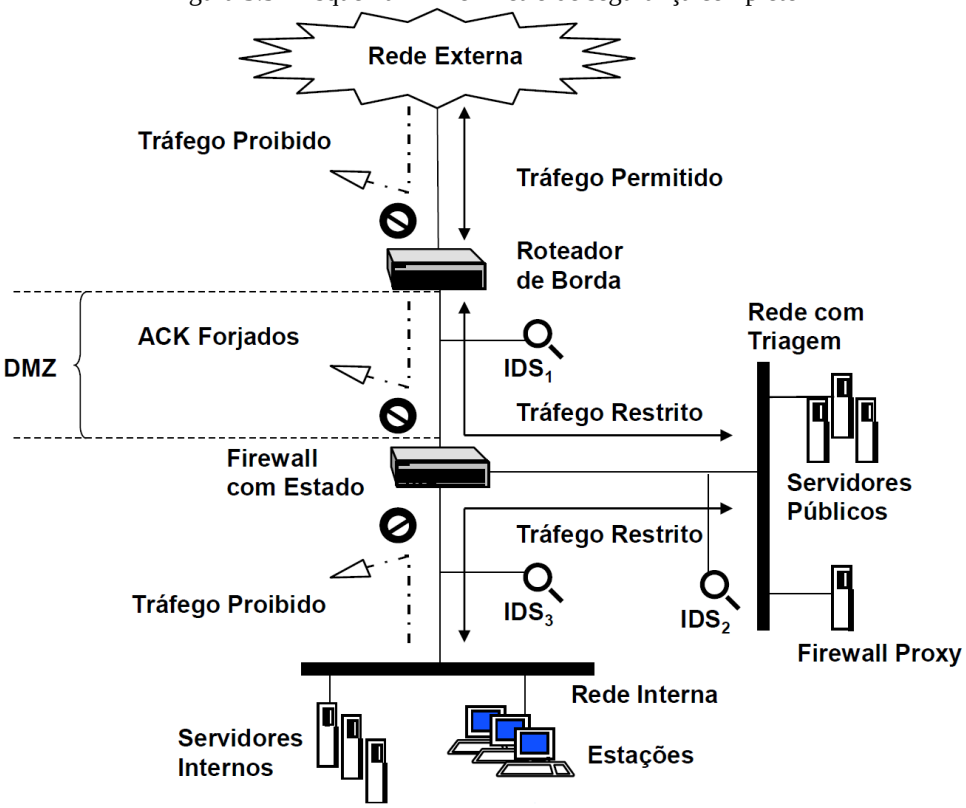
3.7.3 Fator humano

A infraestrutura da defesa em profundidade busca criar barreiras para proteger os recursos da rede, entretanto, de nada adianta investir em todos os recursos de defesa existentes se os usuários do sistema não estiverem treinados e cientes de suas reponsabilidades na SIC. Segundo a normas de tecnologia da informação da Marinha, “O fator mais importante para a SIC é a existência de uma mentalidade de segurança incutida em todo o pessoal. Pouco adiantará o estabelecimento de rigorosas medidas de segurança se o pessoal responsável pela sua aplicação não tiver delas perfeita consciência.” (BRASIL, 2019, p. 9-19)

Para que essa mentalidade de segurança seja incutida nos usuários do sistema, faz-se necessário realizar adestramentos, palestras e exercícios internos. Adestramentos para evitar ataques de engenharia social, que corresponde “ao conjunto de técnicas para se obter ou comprometer informações sobre uma organização ou seus sistemas computacionais, utilizando-se como ferramenta de ataque a interação humana ou as habilidades e fragilidades sociais do ser humano.” (BRASIL, 2019, p. 9-20)

Para melhor visualização e entendimento, a figura 3.9 demonstra um dos possíveis esquemas para se estabelecer um perímetro de segurança, baseado nos componentes citados nesse trabalho.

Figura 3.9 - Esquema 2 – Perímetro de segurança completo



Fonte: Da Silva (2019)

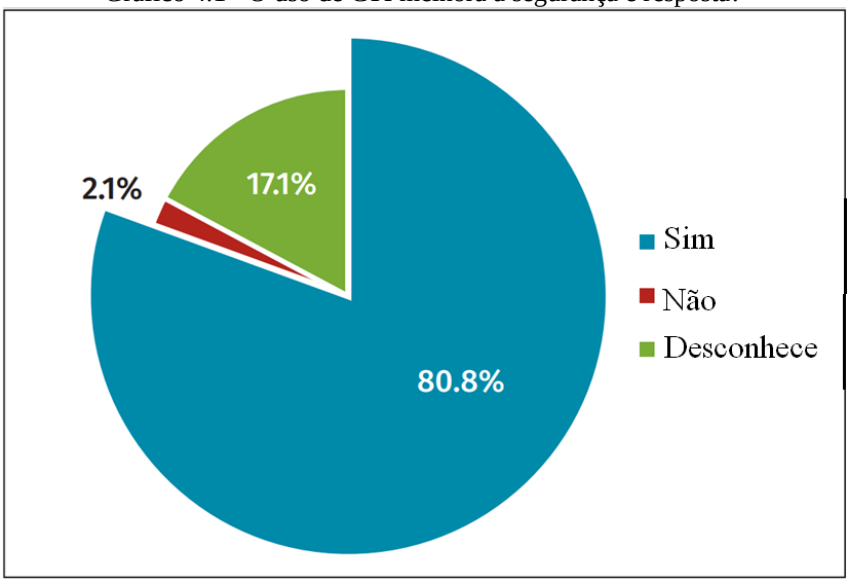
4 DESCRIÇÃO E ANÁLISE DOS RESULTADOS

Anualmente o SANS, um dos maiores institutos de treinamento em segurança digital e certificação de segurança, realiza pesquisas consultando profissionais da área de segurança de redes de diversas empresas com perguntas relacionadas a evolução da Cyber Threat Intelligence (CTI), um conceito que pode ser entendido como:

> informações precisas e contextualizadas sobre ameaças cibernéticas emergentes ou existentes que vem sendo refinadas e analisadas para fornecer recomendações adicionais que permitem que as organizações tomem decisões para se defender ou mitigar quaisquer ameaças cibernéticas (HACKERS TERMINAL, 2019, tradução do autor).

Em 2019, a pesquisa recebeu 585 respostas de empresas pequenas com menos de 100 funcionários e empresas grandes com mais de 100.000. Segundo Brown e Lee, (2019), 81% dos profissionais de segurança acreditam que investir em CTI, em que o SIEM funciona como uma plataforma de gerenciamento, contribui para melhorar a postura de segurança da empresa e apenas 2,1% do total informaram que CTI não ajuda, como vemos no gráfico 1. (BROWN; LEE, 2019).

Gráfico 4.1 - O uso de CTI melhora a segurança e resposta?



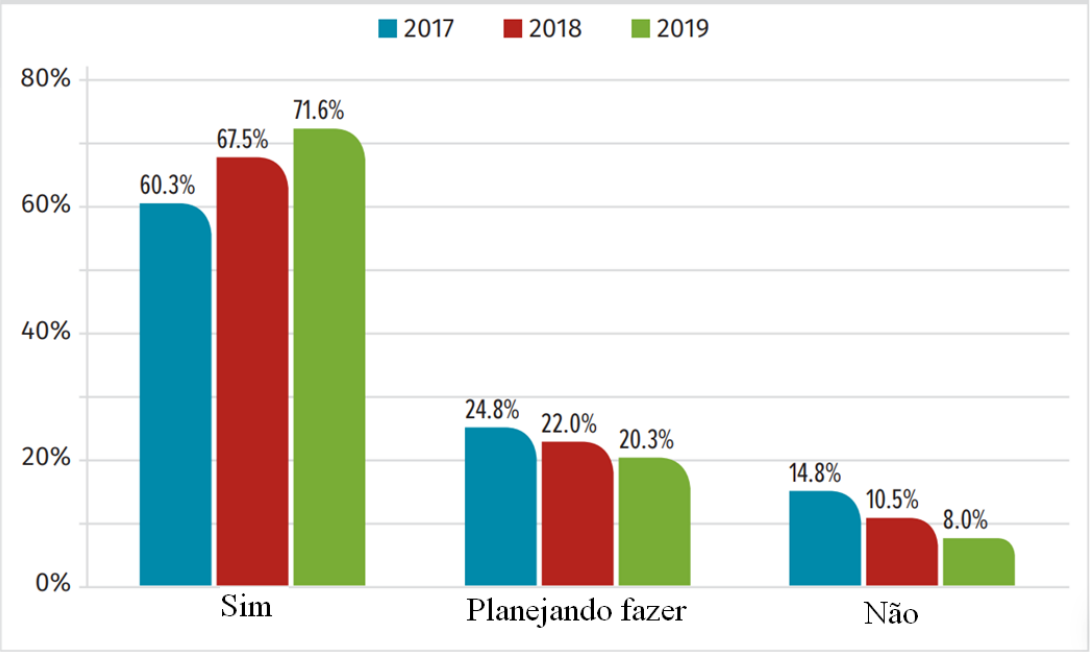
Fonte: Brown e Lee, (2019). Modificado pelo autor

Ainda analisando o gráfico 1, percebe-se que 17,1% dos profissionais informaram não possuir conhecimento suficiente a respeito do assunto para opinar sobre os benefícios que o CTI pode oferecer. Analisando melhor o gráfico, considerando como espaço amostral apenas

os profissionais que conhecem a ferramenta, pode-se concluir que dos 82,9% totais, 80,8% acreditam que CTI oferecem grandes vantagens, o que na verdade representa 97,5% de aprovação.

Em outra pergunta que foi realizada durante a pesquisa, percebe-se que a adesão ao SIEM e CTI em geral vem crescendo nas empresas, como exposto no gráfico 4.2

Gráfico 4.2 - A organização produz ou consome CTI?



Fonte: Brown e Lee, (2019). Modificado pelo autor

De acordo com o gráfico 4.2, em 2019, a pesquisa apontou que 72% das organizações disseram que produzem ou consomem CTI, números que vêm em uma crescente positiva se comparados aos 67,5% do ano de 2018 e 60,3% no ano de 2019.

Quando se trata de gerenciamento de CTI, o SIEM é a plataforma dominante, com 82% dos entrevistados, afirmando que utilizam a plataforma SIEM para o gerenciamento inteligente. Até a publicação deste trabalho, a solução SIEM é a escolha mais popular para aqueles que buscam contribuir uma capacidade de tratamento inteligente contra ameaças e vulnerabilidades. (BROWN; LEE, 2019).

Com base nessa pesquisa, percebe-se que a popularidade do SIEM é grande e vem aumentando com o passar dos anos. Nesse capítulo do trabalho, serão apresentados os principais conceitos envolvidos no sistema, caraterísticas e benefícios que a ferramenta pode disponibilizar aos utilizadores.

4.1 Importância da análise de logs da rede

Uma das características básicas dos sistemas computacionais ligados em rede é a geração de logs, que são registros/eventos gerados pelos próprios dispositivos e pela interação de seus componentes. Existem diversos tipos diferentes de arquivos de log, desde arquivos gerados por Sistemas Operacionais (SO), aplicativos e equipamentos de rede como switches e roteadores, até os componentes do perímetro de segurança (firewalls, IPS, entre outros como explanado na seção 3.7.1). (GRÉGIO, SANTOS, 2010; NORTHCUTT et al., 2002)

Nas palavras de Grégio e Santos, (2010, p. 2), os registros de logs

> [...] têm o intuito de prover informações sobre o funcionamento das partes do sistema, permitir a monitoração do tráfego da rede em busca de eventos suspeitos ou falhas, tentar identificar a atuação de *software* malicioso (*malware*) em computadores ou redes, identificar a proveniência e/ou conteúdo de mensagens de e-mail não solicitados, bem como auxiliar na auditoria em caso de incidentes envolvendo a segurança de sistemas de informação.

Pelo fato da enorme quantidade de dispositivos e software capazes de gerar *logs*, somado as inúmeras informações que cada arquivo de log pode conter, torna o armazenamento de tantas informações um verdadeiro desafio, incluindo decidir quais armazenar, onde armazenar e por quanto tempo. Se o armazenamento é uma missão árdua e custosa, então analisar cada um desses dados buscando estabelecer uma correlação entre eles, a fim de prover alguma informação que possa ajudar na identificação de uma falha de segurança ou ameaça, em tempo hábil, é uma tarefa impraticável. O SIEM surge para tentar mitigar esses desafios e prover ao usuário uma visão do todo. (GRÉGIO, SANTOS, 2010)

4.2 Surgimento da plataforma SIEM

Segundo ISACA, (2010) e Mendonça (2015), o acrônimo SIEM e seu conceito foi idealizado pelos analistas de segurança, da empresa de consultoria Gartner, Amrit Williams e Mark Nicolett em 2005, e desde então, diversas empresas têm adotado plataformas desse tipo como uma importante ferramenta para segurança de seus dados e sistemas.

O SIEM foi idealizado a partir da integração de dois conceitos, o *security event management* (SEM) e o *security information management* (SIM), que são definidos como:

a) SEM: solução focada em monitoramento em tempo real, correlação e processamento de eventos de segurança. Possui capacidade de agregar grandes volumes de dados

fazendo uso de técnicas para estabelecer relações entre os eventos. (DA SILVA, 2011b; ISACA, 2010)

b) SIM, em contra partida, tem o objetivo de manter o histórico dos eventos, arquivos de logs, de toda infraestrutura computacional pelo máximo tempo possível para, se caso necessário, serem utilizados em apoio a futuras investigações forense e auditorias. O SIM observa os mesmos eventos do SEM, mas não em tempo real. (DA SILVA, 2011b; ISACA, 2010)

O SIEM combina as características de cada uma das tecnologias apresentadas em uma única solução, permitindo o monitoramento e análise em tempo real, combinado com a análise histórica de eventos anteriormente armazenados. (MENDONÇA, 2015)

4.3 Definição e processos gerais do SIEM

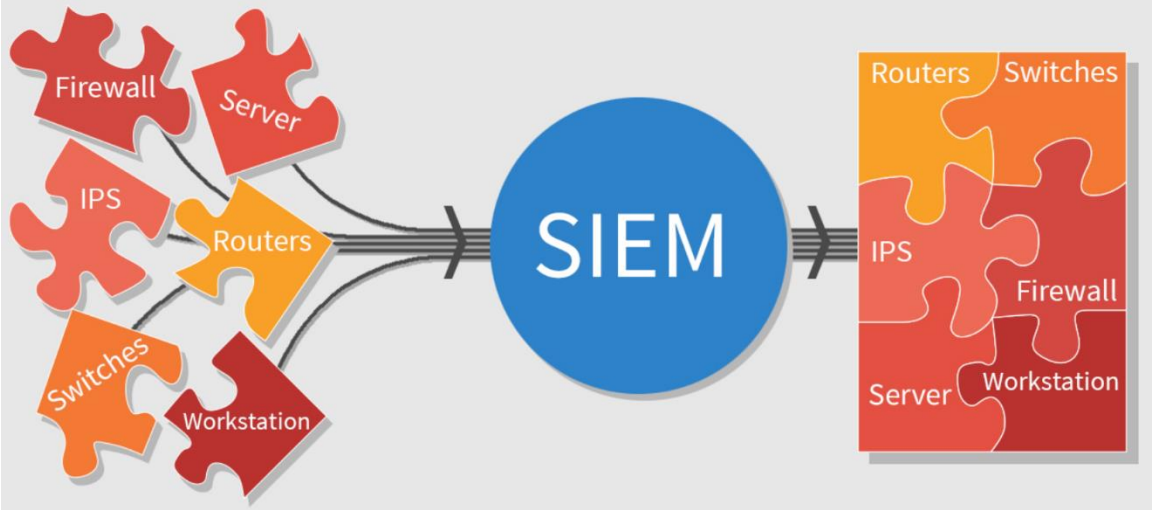
Devido as inúmeras funcionalidades e diferentes modos de apresentação e tratamento da informação atribuído por cada tipo de empresa que presta esse tipo de assessoria e serviço, torna-se difícil determinar uma única definição. Entretanto, de acordo com o glossário da página da Gartner, o SIEM pode ser definido como:

> [...] uma tecnologia que oferece suporte à detecção de ameaças, conformidade e gerenciamento de incidentes de segurança por meio da coleta e análise (ambas em tempo real e baseada em histórico) de eventos de segurança, além de uma grande variedade de outras fontes de dados contextuais e de eventos. Os principais recursos são uma grande capacidade de coletar logs e gerenciamento de eventos, a capacidade de analisar eventos de logs e outros dados das mais diversas fontes e recursos operacionais. (GARTNER, c2020, tradução do autor)

Tipicamente, o SIEM pode ser entendido como um grande gerenciador de segurança de um conjunto de camadas de sistemas de controles já existentes, como por exemplo os componentes de um bom perímetro de segurança, apresentados na seção 3.7.1 deste trabalho. O sistema busca ter a capacidade de unir dados de segurança desde dispositivos mais simples até dispositivos mais complexos e fornecer uma apresentação simplificada e organizada da integração destes em um único sistema. A figura 4.1 retrata essa finalidade, demonstrando que sem o SIEM, cada um dos componentes que compõem a rede, são como peças de um grande quebra-cabeça que não possuem relação entre si. O objetivo é montar esse quebra-cabeça de forma a fornecer informações correlacionadas em um único sistema, processo que é conhecido

como correlação de logs ou eventos, a fim de obter uma visão do todo e não apenas das partes. (KHAN, 2014; APPLEBEE, 2015)

Figura 4.1 - Quebra-cabeça dos componentes de rede.



Fonte: Applebee (2015)

Essa integração requer grande capacidade técnica. Atualmente existem diversas empresas que fornecem implementações da solução SIEM, cada uma delas coleta, armazena, correlaciona e apresenta os dados de modos distintos. Apesar das diversas soluções, um SIEM, deve possuir pelo menos as seguintes características e dificuldades relacionadas: (ISACA, 2010; KHAN, 2014; MILLER, 2011)

a) *Coleta de dados*: tipicamente o SIEM deve ter a capacidade de coletar dados de todos os tipos diferentes de sistemas: firewall, proxy, IPS, IDS, roteadores, switches entre outros. Alguns desses compartilham logs e funções de alertas similares, entretanto, esses dados variam em formato, protocolo e informações que podem prover. A coleta de dados ocorre de diferentes formas dependendo do sistema. Alguns sistemas podem se conectar facilmente a central do SIEM através de protocolos padronizados, enquanto que outros utilizam protocolos e softwares proprietários, fazendo com que o SIEM tenha que entender e traduzir esse tipo diferente de protocolo para conseguir coletar esse dado e extrair a informação necessária.

b) *Agregação de dados*: Uma vez coletada as informações de diversas fontes, esses dados são compostos em uma única base de dados de armazenamento, a fim de facilitar a correlação junto a outras funções do SEM, de forense relatório do SIM. Apesar de parecer simples, a agregação de dados apresenta diversos desafios e considerações, pois a arquitetura também deve ser considerada. Dependendo do

tamanho da empresa, da quantidade de dados que estão sendo coletados e da infraestrutura, a agregação pode ser feita de maneira centralizada ou distribuída.

c) *Normalização do dado*: A normalização é o processo que tem como objetivo resolver diferentes tipos de representações do mesmo tipo de arquivo, em um formato similar e então armazená-los em uma central de dados. Esse processo busca extrair informações em comum entre os dispositivos e expressá-las em um único formato consistente, o que permite a comparação direta de diferentes eventos. Esse procedimento equaliza os dados de forma a remover informações ruidosas, ou seja, que não tem valor para o tipo de coleta que se deseja fazer. Existem conectores específicos, configurados para cada tipo de dispositivo que recebem os eventos, analisam os converte para um formato comum.
d) *Correlação de eventos*: Processo que ocorre após a normalização dos dados e tem como objetivo fazer a ligação de múltiplos eventos de segurança ou alertas, em vários sistemas, possibilitando identificar atividades anômalas que não seriam evidentes se os eventos fossem analisados isoladamente. Para fazer essa função o SIEM deve possuir regras que instruam esse tipo de correlação para cada tipo de evento a fim de justificar um alerta de segurança. A grande dificuldade desse procedimento é justamente estabelecer regras eficazes, que possibilitem alarmar quando necessário, mas sem gerar alarmes falsos.
e) *Alerta*: ligado a correlação de eventos, o alerta é a função que permite ao SIEM estabelecer alertas baseados tanto em alertas já preestabelecidos ou novos.

Os processos citados anteriormente, são apenas características balizadoras mínimas que uma solução SIEM deve possuir para ser eficiente, não necessariamente possuem os nomes citados e inclusive podem possuir outros processos relacionados.

A figura 4.2 ilustra os processos básicos do SIEM sequencialmente, e apesar de estarem divididos em 4 passos, representam e compõem todas os processos citados anteriormente:

Figura 4.2 - Processos básicos do SIEM

Fonte: 42Gears (2019). Modificado pelo autor

Sobre o *console central de gerenciamento* ou *painel de controle*, embora não seja uma capacidade ou processo específico como aos apresentados anteriormente, é o componente mais customizado e variado disponibilizado pelas diferentes soluções SIEM. Ele é a interface principal de apresentação em tempo real, um dashboard, que serve para monitorar eventos, realizar análises, gerar relatórios, manipular os dados de logs armazenados, gerar alertas entre outras funções. Normalmente são compostos por gráficos que facilitam a visualização e interpretação dos dados. (CLAVIS, c2020; ISACA, 2010)

4.4 Desafios da implementação e benefícios do SIEM

Em geral, o SIEM é uma plataforma poderosa graças a correlação inteligente dos dados e eventos. Entretanto a eficiência do sistema está diretamente relacionada as regras e políticas que são inseridas e aplicadas corretamente ao tipo de ambiente. Alcançar essa eficiência requer profissionais muito bem qualificados que além de conhecer todos os sistemas

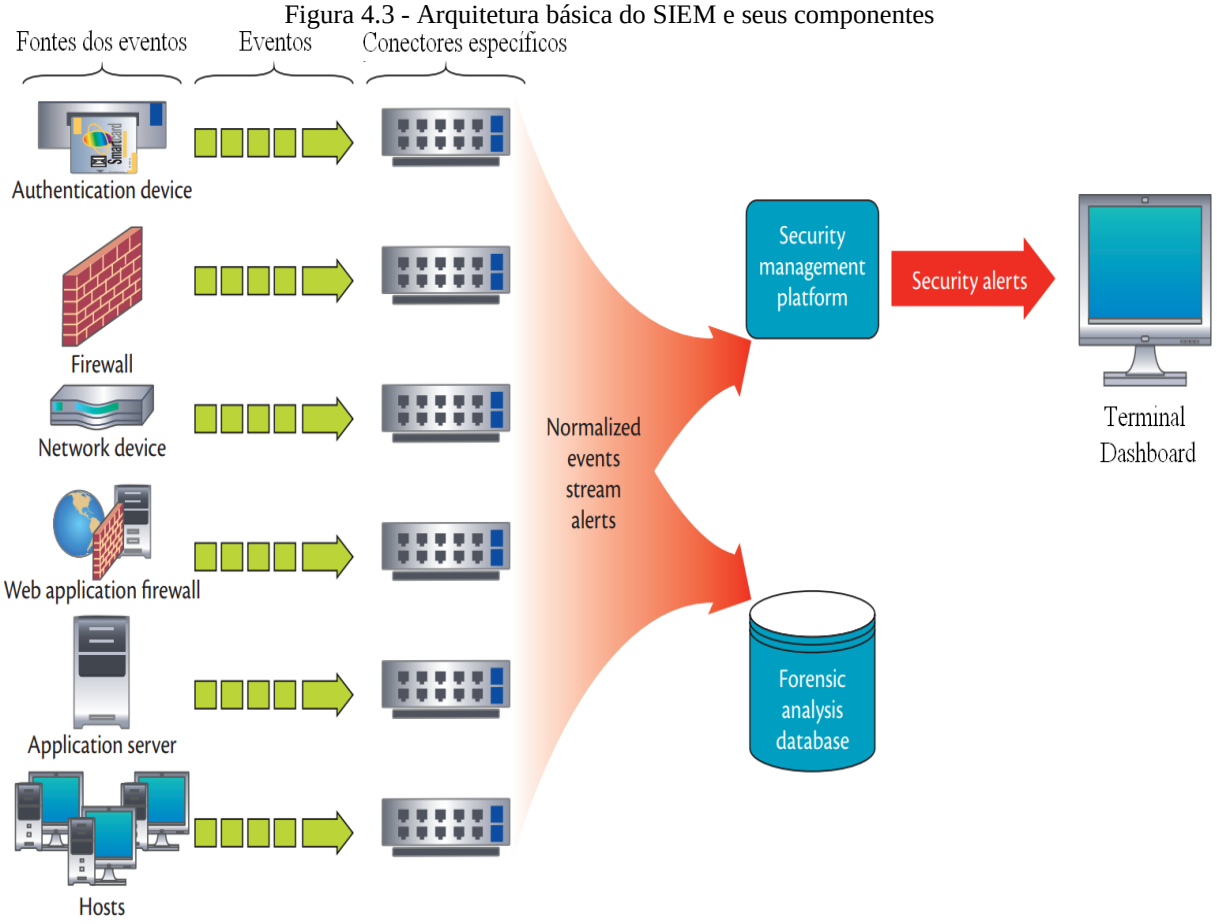
e componentes envolvidos, precisa prever como funcionaria o comportamento da rede em caso de possíveis incidentes de segurança. (MILLER, 2011; KHAN, 2014).

De acordo com empresas de segurança de redes e trabalhos acadêmicos relacionados, uma solução SIEM implementada de forma eficiente, pode gerar inúmeras vantagens. Baseado nas empresas de segurança digitais: Clavis, IBM, Pratum, Solarwinds e McAfee; e trabalhos acadêmicos relacionados ao tema, foram relacionados a seguir 3 vantagens que são comumente citadas por essas empresas e trabalhos:

a) *Visibilidade abrangente em um único sistema*: é a centralização de informações, característica que oferece a vantagem de obter acesso e a análise de logs de todos os dispositivos de rede da empresa ou organização em uma única plataforma. Além de fornece recursos de geração de relatórios que são essenciais para o gerenciamento de eventos e informações de segurança. (CLAVIS, c2020; SOLARWINDSMSP, c2020)
b) *Ganho de tempo e eficiência*: Facilitar o processo de coleta, correlação e geração de relatórios por meio de ferramentas automatizadas, uma solução SIEM pode reduzir tarefas que antes levariam dias para serem consolidadas, em apenas minutos, tendo como grande vantagem liberar analistas de segurança para se concentrar na investigação e resposta aos incidentes. (IBM, c2020; ISACA, 2010, MCAFEE, c2020)
c) *Detecção de ameaças em tempo real*: O monitoramento em tempo real permite respostas em tempo reduzido, inclusive com a possibilidade de automatizar a reação, a fim de combater os invasores e ameaças descobertas. (BRACHMAN, 2016; CLAVIS, C2020; SOLARWINDSMSP, c2020)

A figura 4.3 ilustra os componentes da arquitetura básica de um SIEM, desde a coleta de dados, ou seja, coleta dos eventos, até a sua apresentação em dashboard.

Figura 4.3 - Arquitetura básica do SIEM e seus componentes



Fonte: Bhatt, Manadhata, Zomlot (2014). Modificado pelo autor

Como ilustrado na figura 4.3, o sistema aceita e recebe entradas de vários dispositivos e sensores de segurança, incluindo componentes que compõem o perímetro de segurança, além de, sensores de host, aplicativos (sistemas de autenticação e sistemas de autenticação de aplicativos da Web) e sensores de rede. Os dispositivos geram eventos, representados no esquema, que são específicos de acordo com cada tipo de dispositivo, fornecedor e versão. Esses eventos são coletados por conectores específicos. A próxima tarefa do sistema SIEM é normalizar as diferentes representações em um formato comum para facilitar o processamento e análise, processo que simplifica a criação e manutenção de regras. Uma vez normalizados, os eventos são encaminhados para a plataforma de gerenciamento de segurança e para o arquivo do banco de dados de análise forense para consultas futuras. A plataforma de gerenciamento aplica as regras aos eventos e quando é o caso, emite um alerta que é enviado ao terminal ou dashboard do SIEM para ser analisado por um analista. (BHATT, MANADHATA, ZOMLOT, 2014)

4.5 A importância do SIEM na Marinha do Brasil

Como explanado nesse capítulo, a plataforma SIEM vem ganhando destaque nas empresas do mundo todo pelos benefícios, facilidades e ganho de tempo que atualmente tem sido cada vez mais precioso, se considerarmos que empresas conectadas a rede sofrem milhares de ataques todos os dias. Nas Forças Armadas, essa realidade não é diferente e, se fosse levado em consideração um vazamento de informações, como por exemplo as informações de uma missão sigilosa, não apenas a Forças Armadas, mas, sim, o país, poderia ser colocado em uma situação perigosa.

Baseado nesses desafios, a Marinha, Exército e Aeronáutica, por determinação do Ministério da Defesa, já possuem seus próprios SIEM. No caso da Marinha do Brasil, a plataforma foi desenvolvida pela CTIR.mb, que implementa e monitora o sistema.

Segundo dados retirados da página interna do CTIM, a CTIR.mb possui a missão de prover uma estrutura capaz de responder a ataques ou incidentes de segurança que possam ocorrer na RECIM. Além disso, baseado no conhecimento da estrutura interna, tecnologias utilizadas e recursos de segurança existentes, deve ter a capacidade de diagnosticar falhas de segurança na rede e identificar tráfego malicioso.

Para o CTIR.mb, um incidente de segurança é definido como qualquer evento adverso, relacionado a segurança de sistemas e redes de computadores, como por exemplo: uso ou tentativas de acesso não autorizado a dados ou sistemas, modificação de sistemas sem autorização, desrespeito a política de segurança ou política de uso de sistemas, entre outros.

Em geral, uma plataforma SIEM deve ser um ponto central para recebimento e notificação de incidentes de segurança, e o sistema implementado pelo CTIR.mar também tem esse objetivo, além de manter estatísticas sobre os incidentes reportados e desenvolver documentação de apoio para usuários e administradores de redes da MB.

Existem diversas empresas de segurança da informação que fornecem e implementam plataformas SIEM. Uma delas é a Clavis, reconhecida como empresa estratégica de defesa desde o ano de 2016. Além disso, em 16 de janeiro de 2018, o Ministério da defesa reconheceu o produto Octopus, nome dado a solução SIEM da empresa, como produto estratégico de defesa. Entretanto, apesar de ser uma empresa oficialmente reconhecida pelo MD, ela não foi contratada para desenvolver a plataforma para a Marinha. O desenvolvimento e controle ficou a cargo do CTIR.mb pelo fato de que as informações disponibilizadas e correlacionas são das mais diversas fontes do backbone da RECIM. (SEGINFO, 2018)

5 CONCLUSÃO

O mundo está conectado pelas redes de computadores, onde o objetivo principal de toda essa interconexão é o compartilhamento de informações. A necessidade de troca de dados e informações cria uma dependência cada vez maior das redes, que apesar dos inúmeros benefícios prestados, trazem consigo várias vulnerabilidades.

Tratando de Forças Armadas, percebe-se que atualmente uma guerra não é necessariamente definida a favor da nação que possui maior poder bélico, mas sim favorável a quem possui, antecipadamente, informações relevantes a respeito do inimigo. Por esse motivo, é necessário que a MB mantenha uma mentalidade de segurança e utilize ferramentas para proteção do espaço cibernético.

Com base nessa premissa, fica evidente a necessidade de manter barreiras, nos sistemas de informação, que dificultem a ação de elementos mal intencionados. Essas barreiras devem ser complementares e, em conformidade com os objetivos específicos, este trabalho exemplificou e defendeu a importância de se manter um perímetro de segurança fortificado composto, ao menos, pelo roteador de borda, firewall com estado, firewall proxy, IDS/IPS e redes com triagem.

A preocupação com a segurança não deve estar limitada ao pessoal de TI, deve ser uma preocupação de todos, pois de nada adianta instalar vários portões em uma casa, se quem estiver dentro deixá-los abertos, mesmo que não intencionalmente. Logo, além do estabelecimento das barreiras, é preciso estabelecer rotinas de adestramento a respeito das responsabilidades de SIC para todo pessoal da organização.

Ainda assim, não há garantia de segurança, afinal não existe nenhum sistema que seja capaz de prover 100% de segurança. Para que o objetivo geral deste trabalho fosse alcançado, destacou-se a importância da coleta dos logs gerados por cada um dos dispositivos, tanto do perímetro de segurança quanto de qualquer outro conectado à rede. Atualmente, a implementação de um sistema SIEM como um agregador centralizado para análise de eventos é indispensável para aumentar a segurança contra ameaças e prover um alarme antecipado.

5.1 Considerações Finais

Este trabalho teve como foco defender a importância da implementação do SIEM, como uma solução para prever e evitar incidentes de redes. Entretanto, ter um sistema SIEM,

não significa que, automaticamente, a organização estará completamente segura contra ameaças internas e externas. Apesar dos diversos benefícios oferecidos, ele possui várias limitações e vulnerabilidades que não devem ser ignoradas.

Esse sistema requer monitoramento constante dos logs e alertas, manutenções regulares e configurações tão boas e eficientes quanto a equipe de segurança possa prover. Um outro ponto que chama atenção é que apesar de sua implantação ser complexa, a maior parte do trabalho realmente começa após o SIEM já estar instalado, ou seja, durante sua operação. Durante sua execução e monitoramento, profissionais necessitam de recursos, ferramentas e tempo para desfrutar das funcionalidades do SIEM para melhorar a proteção contra possíveis ameaças.

5.2 Sugestões para Futuros Trabalhos

Como exposto neste trabalho, a implementação e monitoramento de um sistema SIEM não é uma tarefa fácil, entretanto, é notório os benefícios que podem ser alcançados. Atualmente a MB tem o SIEM implantado apenas no backbone da RECIM.

Como sugestão para trabalhos futuros, seria interessante a realização de estudos de viabilidades para implementação do SIEM em redes MAN na MB, que são as redes dos complexos Navais, como por exemplo o complexo do Primeiro Distrito Naval, a Base Naval da MB em Mocanguê e nos Distritos Navais nos demais estados do Brasil.

REFERÊNCIAS

42GEARS. **SIEM**: a shift in focus to threat monitoring. 43gears, 9 ago. 2019. Disponível em: < https://www.42gears.com/blog/siem-a-shift-in-focus-to-threat-monitoring/> Acesso em: 7 jan. 2020.

APPLEBEE, G. **Benefits of log consolidation in a SIEM environment**. Pratum, 18 jun. 2015. Disponível em: <https://www.pratum.com/blog/122-benefits-of-log-consolidation-in-a-siem-environment> Acesso em: 7 fev. 2020.

ASSIS. A. **A questão da proteção Cibernética na Marinha**: Organização Institucional e Normas, 2019. Disponível em: <http://redectidc.com.br/assets/files/a-questao-da-protecao-cibernetica-na-marinha.pdf> Acesso em: 17 jan. 2020.

BACHMAN, C. **How does SIEM work?**. Pratum, Pratum blog, 24 jun. 2016. Disponível em: <https://www.pratum.com/blog/313-how-does-siem-work> Acesso em: 7 fev. 2020.

BHATT, S.; MANADHATA, P. K.; ZOMLOT, L. The operational role of security information and event management systems. **IEEE** security and privacy, v. 12, n. 5, p. 35-41, set.-out. 2014. Disponível em: <https://www.researchgate.net/publication/273394505_The_Operational_Role_of_Security_Information_and_Event_Management_Systems> Acesso em: 29 jan. 2020.

BRASIL, Ministério da Defesa. Exército Brasileiro. Comando de Operações Terrestres. **Manual de Campanha Guerra Cibernética**. Brasília, EB70-MC-10.232, 1ªed., Brasília, 2017, 45p.

BRASIL. Marinha. Conselho de Tecnologia da Informação da Marinha. **PETIM 2016-2019 Plano estratégico de Tecnologia da Informação da Marinha**, 2016. Disponível em: <https://www.marinha.mil.br/sites/default/files/petim_mb.pdf>. Acesso em: 18 jan. 2020.

BRASIL. Marinha. Diretoria-Geral do Material da marinha. **DGMM-0540: Normas de Tecnologia da Informação da Marinha**. Rio de Janeiro-RJ, 2019.

BRASIL. Marinha. Estado Maior da Armada. **EMA-416: Doutrina de tecnologia da informação da Marinha.** Brasília-DF, 2007.

BRASIL. Ministério da defesa. Gabinete do Ministro. Portaria Normativa nº 3.010 – MD, de 18 de novembro de 2014. Aprova a **Doutrina Militar de Defesa Cibernética**. Disponível em: <https://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_defesa_cibernetica_1_2014.pdf.> Acesso em: 14 jan. 2020.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **Instrução Normativa nº 01** GSI/PR/2008. Brasília, DF: Gabinete de Segurança Institucional, 13 jun. 2008. Disponível em: <http://dsic.planalto.gov.br/legislacao/in_01_gsidsic.pdf > Acesso em: 7 jan. 2020.

BROWN, R.; LEE, R. M. **The Evolution of Cyber Threat Intelligence (CTI):** 2019 SANS CTI Survey. IntSight, 2019. Disponível em: <http://wow.intsights.com/rs/071-ZWD-900/images/The%20Evolution%20of%20Cyber%20Threat%20Intelligence%20%28CTI%29%202019%20SANS%20CTI%20Survey.pdf.> Acesso em: 07 jan. 2020.

CHOWDHURY. **Definitive guide to cyber threat intelligence (cti): to protect your organizations against cyber attack**. Hackers Terminal, 2019. Disponível em: <https://hackersterminal.com/cyber-threat-intelligence-cti/> Acesso em: 07 jan. 2020.

CLARO, J. R. **Sistemas IDS e IPS** – estudo e aplicação de ferramenta open source em ambiente Linux, Instituto federal de educação, ciência e tecnologia Sul-rio-grandense, Passo fundo, 2015. Disponível em: <https://painel.passofundo.ifsul.edu.br/uploads/arq/20160331191141344853464.pdf> Acesso em: 29 jan. 2020.

CLAVIS. **Sistema de gerenciamento de eventos e informações de segurança**, c2020. Disponível em: <https://clavis.com.br/solucoes/octopus-siem-analise-de-seguranca-orientada-por-dados/?gclid=CjwKCAiA1fnxBRBBEiwAVUouUiBP7PJ5CGXT7t8BE0Gv0f3HJ5mI_FtOVtHEe-FzNM18oHYe00UWYxoCroEQAvD_BwE> Acesso em: 7 jan. 2020.

COSTA, J. S.; DA SILVA, J.; DA CRUZ, M. A. P. **Segurança de redes de computadores na internet**. Revista Inova Ação, Teresina, v. 1, n. 2, art. 6, p. 77-88, 2012. Disponível em: < http://189.43.21.151/revista/index.php/inovaacao/article/download/480/pdf> Acesso em: 22 jan. 2020.

CTIR GOV. CTIR Gov em números. Estatísticas resultantes do trabalho de detecção, triagem, análise e resposta a incidentes cibernéticos, 2020. Disponível em: <https://emnumeros.ctir.gov.br/> Acesso em: 10 fev. 2020.

DA SILVA, A. O. **Segurança em redes de computadores**, Rio de janeiro, 2019. 98 slides.

DA SILVA, E. P. **A Marinha do Brasil e a era da Informação**: a aplicabilidade de Guerra Centrada em Redes. Monografia. Curso de Estado-Maior para Oficiais Superiores. Escola de Guerra Naval, 2011a.

DA SILVA, J. C. B. L. **Guerra cibernética**: A guerra no quinto domínio, conceituação e princípios. Revista da Escola de Guerra Naval, Rio de janeiro, v. 20, n. 1, p. 193-211. 2014. Disponível em: <https://revista.egn.mar.mil.br/index.php/revistadaegn/article/download/797/pdf.> Acesso em: 15 jan. 2020.

DA SILVA, N. R. L. **Método de implementação de SIEMs**: Resultados de experiências práticas. 2011b. Tese de Mestrado em Engenharia e Gestão de Sistemas de informação. Universidade do Minho em Portugal, Braga, 2011. Disponível em: <https://core.ac.uk/download/pdf/55620273.pdf> Acesso em: 1 fev. 2020.

DU, Min.; LI, Feifei. Spell: **Streaming Parsing of System Event Logs**, IEEE 16th International Conference on Data Mining (ICDM 2016), Barcelona, Spain, 2016.

ESPÍRITO SANTO. **Segurança da Informação**. Instituto Cuiabano de Educação, Cuiabá. 2011.

EVANGELISTA, S. V. B. **Sistemas de detecção de intrusos e sistemas de prevenção de intrusos**: princípios e aplicação de entropia, Instituto superior de tecnologia em ciência da computação, Petrópolis, 2008. Disponível em: <https://www.lncc.br/~borges/doc/IDS%20IPS%20e%20Entropia.TCC.pdf> Acesso em: 29 jan. 2020.

FRANCESCHETT, A. L.; ONÇA, P. R. A. S. J.; FERNANDES, A. **Conceito de defesa em profundidade aplicada na segurança cibernética de sistemas de automação de energia.** XXIV Seminário Nacional de Produção e transmissão de energia elétrica, Grupo – XV, Curitiba, 2017. Disponível em: <https://www.protcom.net/Literatura/Telecom/ARTIGOS/2017_DEFESA%20PROFUNDIDADE%20SEGURAN%C3%87A%20CIBERN%C3%89TICA%20AUTOMA%C3%87%C3%83O%20ENERGIA.pdf> Acesso em: 23 jan. 2020.

FRANCISCATTO, R.; DE CRISTO, F.; PERLIN, T. **Redes de computadores**. Universidade Federal de Santa Maria, Colégio Agrícola de Frederico Westphalen, 2014. Disponível em: < https://www.ufsm.br/unidades-universitarias/ctism/cte/wp-content/uploads/sites/413/2018/12/redes_computadores.pdf> Acesso em: 24 jan. 2020.

GARTNER. **Gartner glossary**, c2020. Disponível em: <https://www.gartner.com/en/information-technology/glossary/security-information-and-event-management-siem> Acesso em: 6 fev. 2020.

GOMES, M. G. F. M.; CORDEIRO, S. S.; PINHEIRO, W. A. **A guerra cibernética**: exploração, ataque e proteção cibernética no contexto dos sistemas de Comando e Controle. Revista Militar de Ciência e Tecnologia, v. 33, n. 2, p. 11-18. 2016. Disponível em: <http://rmct.ime.eb.br/arquivos/RMCT_3_tri_2016_web/RMCT_275.pdf.> Acesso em: 14 jan. 2020.

GRÉGIO, A. R. A.; SANTOS. R. **Análise e visualização de logs de segurança**, São Paulo, 2010. Disponível em: <http://plutao.sid.inpe.br/col/dpi.inpe.br/plutao@80/2010/06.25.15.38/doc/Gregio_Analise.pdf?languagebutton=pt-BR> Acesso em: 31 jan. 2020.

IBM. **IBM QRadar SIEM**, c2020. Disponivel em: <https://www.ibm.com/br-pt/marketplace/ibm-qradar-siem> Acesso em: 7 jan. 2020.

ISACA. **Security and Event Managemente**: Business benefits and Security, Gorvernance and Assurance perspective. 2010. Disponível em: <https://www.academia.edu/818604/Security_Information_and_Event_Management_Business_Benefits_and_Security_Governance_and_Assurance_Perspectives_ISACA> Acesso em: 1 fev. 2020.

KHAN, H. A. **Advancing security information and event management frameworks in managed enterprises using GeoLocation**. Dissertação de mestrado em ciência da computação. Universidade de Capetown, cidade do cabo, 2014. Disponível em: <https://open.uct.ac.za/bitstream/handle/11427/15561/thesis_sci_2015_khan_herah_anwar.pdf?sequence=1&isAllowed=y> Acesso em: 9 jan. 2020.

LIMA, M. B.; DE GEUS, P. L. **Comparação entre filtros de pacotes com estado e tecnologias tradicionais de firewall**. Instituto Estadual de Campinas, São Paulo, 1999. Disponível em: <https://www.lasca.ic.unicamp.br/paulo/papers/1999-SSI-marcelo.lima-spf.pdf> Acesso em: 28 jan. 2020.

MARQUES, C, F.; ODA, E. **Atividades técnicas na Operação Logística**. Curitiba. IESDE Brasil S.A., 2012. Disponível em: <https://books.google.com.br/books?id=TzdJ4CkGoTEC&pg=PA135&dq=John+Naisbitt++%22A+nova+fonte+de+poder+n%C3%A3o+%C3%A9+o+dinheiro+nas+m%C3%A3os+de+poucos,+mas+informa%C3%A7%C3%A3o+nas+m%C3%A3os+de+muitos%22&hl=pt-BR&sa=X&ved=0ahUKEwisuPzziYPnAhUXF7kGHdEFA_EQ6AEIMTAB#v=onepage&q=John%20Naisbitt%20%20%22A%20nova%20fonte%20de%20poder%20n%C3%A3o%20%C3%A9%20o%20dinheiro%20nas%20m%C3%A3os%20de%20poucos%2C%20mas%20informa%C3%A7%C3%A3o%20nas%20m%C3%A3os%20de%20muitos%22&f=false.> Acesso em: 14 jan. 2020.

MCAFEE. **McAfee enterprise security manager**: uma solução SIEM para identificar, investigar e resolver ameaças. c2020. Disponivel em: <https://www.mcafee.com/enterprise/pt-br/products/enterprise-security-manager.html> Acesso em: 7 jan. 2020.

MENDONÇA, N. M. L. **Gerador de eventos para testes de configuração de um SIEM**. 2015. Dissertação de mestrado em segurança informática – faculdade de Ciências e Departamento de Informática, Universidade de Lisboa, Lisboa, 2015. Disponível em: <https://repositorio.ul.pt/bitstream/10451/20559/1/ulfc115850_tm_Nuno_Mendon%C3%A7a.pdf> Acesso em: 1 fev. 2020.

MILLER, D. R. Et al.. **Security Information and Event Management (SIEM) Implementation**. Network Pro Library. 2011.

NORTHCUTT, S. Et al.. **Desvendando Segurança em redes**: o guia definitivo para fortificação de perímetro de rede usando Firewall, VPNs, roteadores e sistemas de detecção de intrusão. Editora Campus. Rio de janeiro, 2002.

PRODANOV, C. C.; DE FREITAS, E. C. **Metodologia do trabalho científico**: métodos e técnicas da pesquisa e do trabalho acadêmico. 2 ed., editora Freevale. Novo Hamburgo, 2013. Disponível em: <http://www.feevale.br/Comum/midias/8807f05a-14d0-4d5b-b1ad-1538f3aef538/E-book%20Metodologia%20do%20Trabalho%20Cientifico.pdf> Acesso em: 27 nov. 2019.

RAULINO, F. C. P. **Segurança de Redes** firewall. Instituto federal de educação, ciência e tecnologia, Rio Grande do Norte, 201-?. 25 slides. Disponível em: < https://docente.ifrn.edu.br/filiperaulino/disciplinas/gerencia-e-seguranca-de-redes/aulas/Firewall%20-%20Introducao.pdf/view> Acesso em: 25 jan. 2020.

SALMON, H. M. **Segurança da Informação e Guerra Cibernética na MB**. Diretoria de Comunicações e Tecnologia da Informação da Marinha. 1° Simpósio Regional de Segurança Cibernética Comando do 5° Distrito Naval, Rio Grande, 2018. Disponível em: <https://www.marinha.mil.br/com5dn/sites/www.marinha.mil.br.com5dn/files/01_Com5DN-Simposio%20v12.pdf> Acesso em: 17 jan. 2020.

SEGINFO. **Octopus e BART são reconhecidos como produtos de defesa pelo Ministério da Defesa**, 2018. Disponível em: <https://seginfo.com.br/2018/01/31/octopus-e-bart-sao-reconhecidos-como-produto-de-defesa-pelo-ministerio-da-defesa/> Acesso em: 25 jan. 2020.

SILVA, L. S. **Uma metodologia para detecção de ataques no tráfego de redes baseada em redes neurais**, Instituto Nacional de pesquisas espaciais, são José dos Campos, 2008.

SOLARWINDSMSP. **Monitoramento de SIEM**: gerenciamento de eventos e informações de segurança, c2020. Disponível em: < https://www.solarwindsmsp.com/pt-br/produtos/threat-monitor/gerenciamento-de-eventos-e-informacoes-de-seguranca> Acesso em: 7 jan. 2020.

TANENBAUM, Andrew S. **Redes de Computadores**. Tradução da 4rd. Ed. em inglês. Editora Campus. 2003.

VIDAL, M. T. V. L. **Segurança em redes 2**. Universidade Federal Fluminense, curso de criptografia e segurança em redes, Rio de janeiro, 2006. Disponível em: <https://www.telecom.uff.br/sites/www.telecom.uff.br/files/Seguranca_em_Redes_2.pdf> Acesso em: 25 jan. 2020.