


**ACADEMIA MILITAR DAS AGULHAS NEGRAS
ACADEMIA REAL MILITAR (1811)
CURSO DE CIÊNCIAS MILITARES**

Nilton Rodrigues Martins Filho

**O SISTEMA MISP COMO FERRAMENTA DE COMPARTILHAMENTO DE
INTELIGÊNCIA DE AMEAÇAS EM EXERCÍCIOS NO TERRENO**

Resende
2022

	<p align="center">APÊNDICE II AO ANEXO B (NITCC) ÀS DIRETRIZES PARA A GOVERNANÇA DA PESQUISA ACADÊMICA NA AMAN</p> <p align="center">TERMO DE AUTORIZAÇÃO DE USO DE DIREITOS AUTORAIS DE NATUREZA PROFISSIONAL</p>	<p align="center">AMAN 2022</p>
---	--	--

TERMO DE AUTORIZAÇÃO DE USO DE DIREITOS AUTORAIS DE NATUREZA PROFISSIONAL

<p>TÍTULO DO TRABALHO: O SISTEMA MISP COMO FERRAMENTA DE COMPARTILHAMENTO DE INTELIGÊNCIA DE AMEAÇAS EM EXERCÍCIOS NO TERRENO</p>
<p>AUTOR: NILTON RODRIGUES MARTINS FILHO</p>

Este trabalho, nos termos da legislação que resguarda os direitos autorais, é considerado de minha propriedade.

Autorizo a Academia Militar das Agulhas Negras a utilizar meu trabalho para uso específico no aperfeiçoamento e evolução da Força Terrestre, bem como a divulgá-lo por publicação em revista técnica da Escola ou outro veículo de comunicação do Exército.

A Academia Militar das Agulhas Negras poderá fornecer cópia do trabalho mediante ressarcimento das despesas de postagem e reprodução. Caso seja de natureza sigilosa, a cópia somente será fornecida se o pedido for encaminhado por meio de uma organização militar, fazendo-se a necessária anotação do destino no Livro de Registro existente na Biblioteca.

É permitida a transcrição parcial de trechos do trabalho para comentários e citações desde que sejam transcritos os dados bibliográficos dos mesmos, de acordo com a legislação sobre direitos autorais.

A divulgação do trabalho, em outros meios não pertencentes ao Exército, somente pode ser feita com a autorização do autor ou da Direção de Ensino da Academia Militar das Agulhas Negras.

Resende, 22 de agosto de 2022.



 Cad Nilton Rodrigues Martins Filho

Dados internacionais de catalogação na fonte

M528a MARTINS FILHO, Nilton Rodrigues

O sistema MISP como ferramenta de compartilhamento de inteligência de ameaças em exercícios no terreno. / Nilton Rodrigues Martins Filho – Resende; 2022. 29 p. : il. color. ; 30 cm.

Orientador: Miquelângelo Souza Dias
TCC (Graduação em Ciências Militares) - Academia Militar das Agulhas Negras, Resende, 2022.

1.MISP 2.Proteção Cibernética 3.Cibernética I. Título.

CDD: 355

Ficha catalográfica elaborada por Jurandi de Souza CRB-5/001879

Nilton Rodrigues Martins Filho

**O SISTEMA MISP COMO FERRAMENTA DE COMPARTILHAMENTO DE
INTELIGÊNCIA DE AMEAÇAS EM EXERCÍCIOS NO TERRENO**

Monografia apresentada ao Curso de Graduação em Ciências Militares, da Academia Militar das Agulhas Negras (AMAN, RJ), como requisito parcial para obtenção do título de **Bacharel em Ciências Militares**.

Orientador: Cap Miquelângelo de Souza Dias

Resende
2022

Nilton Rodrigues Martins Filho

**O SISTEMA MISP COMO FERRAMENTA DE COMPARTILHAMENTO DE
INTELIGÊNCIA DE AMEAÇAS EM EXERCÍCIOS NO TERRENO**

Monografia apresentada ao Curso de Graduação em Ciências Militares, da Academia Militar das Agulhas Negras (AMAN, RJ), como requisito parcial para obtenção do título de **Bacharel em Ciências Militares**.

Aprovado em 01 de junho de 2022:

Banca examinadora:

NO IMPEDIMENTO

Miquelângelo de Souza Dias – Cap

(Orientador)

Allanderson R. Teixeira

Allanderson Rodrigues Teixeira - TC

(Avaliador)

Antônio Fernando Pires Paturoy Júnior

Antônio Fernando Pires Paturoy Júnior - TC

(Avaliador)

Rôber Yamashita

Rôber YAMASHITA

Idt. 013150274-2 MD/EB

Major do Exército

Dedico este trabalho a minha mãe, que sempre me apoiou e me aconselhou em todas as decisões que eu tomei, e ao meu pai (in memoriam), que fez de tudo para que hoje eu pudesse estar realizando o sonho de me tornar Oficial do Exército Brasileiro.

AGRADECIMENTOS

Agradeço primeiramente à Deus, por ter me direcionado para a carreira militar e me proporcionado conhecimento para lidar com as dificuldades.

À minha família, por sempre estarem ao meu lado, prestando apoio e incentivo em todos os momentos.

Ao meu orientador, por sempre exigir mais de mim do que eu exigia de mim mesmo.

Ao CDCiber, por me proporcionar informações importantes para a elaboração deste trabalho.

RESUMO

O SISTEMA MISP COMO FERRAMENTA DE COMPARTILHAMENTO DE INTELIGÊNCIA DE AMEAÇAS EM EXERCÍCIOS NO TERRENO

AUTOR: Nilton Rodrigues Martins Filho

ORIENTADOR: Miquelângelo de Souza Dias

As ameaças cibernéticas representam grande preocupação para qualquer exército, e no Brasil isso não é diferente. Novas ameaças surgem diariamente e lutar contra elas individualmente é quase impossível. A fim de enfrentar esse problema, o Exército Brasileiro utiliza a ferramenta de compartilhamento de inteligência de ameaças *Malware Information Sharing Platform* (MISP), que permite coletar e compartilhar ameaças e vulnerabilidades de dispositivos com outras organizações no âmbito nacional e internacional, como instituições financeiras e países aliados. O objetivo deste trabalho consiste em expor uma configuração básica do sistema MISP para que ele seja utilizado em exercícios táticos do Exército Brasileiro, aprimorando assim a Segurança Cibernética da Força Terrestre. Uma das contribuições da pesquisa fundamentou-se em identificar algumas das principais vulnerabilidades associadas aos serviços de rede simulados em exercícios táticos. A fim de se proteger dessas vulnerabilidades foi apresentada a configuração básica do sistema, permitindo acesso a Bases de Inteligência de Ameaças sobre vulnerabilidades e demais ameaças a que o espaço cibernético está sujeito. Com isso, foi possível identificar a eficiência do sistema MISP no sentido de aprimorar a segurança cibernética por meio do compartilhamento de Inteligência de Ameaças em exercícios táticos.

Palavras-chave: Segurança. Segurança Cibernética. Compartilhamento de Inteligência de Ameaças. MISP.

ABSTRACT

THE MISP SYSTEM AS A THREAT INTELLIGENCE SHARING TOOL IN FIELD EXERCISES

AUTHOR: Nilton Rodrigues Martins Filho

ADVISOR: Miquelânglo de Souza Dias

Cyber threats represent a major concern for any army, and in Brazil this is no different. New threats emerge daily and fighting them individually is almost impossible. In order to address this problem, the Brazilian Army uses the Malware Information Sharing Platform (MISP) threat intelligence sharing tool, which allows it to collect and share device threats and vulnerabilities with other national and international organizations, such as financial and allied countries. The objective of this work is to expose a basic configuration of the MISP system so that it can be used in tactical exercises of the Brazilian Army, thus improving the Cyber Security of the Land Force. One of the research contributions was based on identifying some of the main vulnerabilities associated with simulated network services in tactical exercises. In order to protect against these vulnerabilities, the basic configuration of the system was presented, allowing access to Threat Intelligence Bases on vulnerabilities and other threats to which cyberspace is subject. With this, it was possible to identify the efficiency of the MISP system in order to improve cyber security through the sharing of Threat Intelligence in tactical exercises.

Keywords: Security. Cyber Security. Threat Intelligence Sharing. MISP.

LISTA DE FIGURAS

Figura 1 – Como funciona o MISP	15
Figura 2 – Como as informações são compartilhadas entre os usuários	16
Figura 3 – Aba “ <i>Home</i> ” inicial	19
Figura 4 – Aba “ <i>Feeds</i> ”	19
Figura 5 – Aba “ <i>Home</i> ” final.....	20
Figura 6 – Compartilhamento de inteligência	23

LISTA DE ABREVIATURAS E SIGLAS

EB	Exército Brasileiro
MISP	<i>Malware Information Sharing Platform</i>
Com D Ciber	Comando de Defesa Cibernética
CDCiber	Centro de Defesa Cibernética
DNS	<i>Domain Name System</i>
IoT	<i>Internet of Things</i>
DoS	<i>Denial of Service</i>
END	Estratégia Nacional de Defesa
OWASP	<i>Open Web Application Security Project</i>
CIRCL	<i>Computer Incident Response Center Luxembourg</i>
CERT	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança
ORM	Mapeamento Relacional de Objeto
IoCs	<i>Indicators of Compromise</i>
SQL	<i>Structured Query Language</i>
NoSQL	<i>Not only Structured Query Language</i>
C ²	Comando e Controle
OM	Organização Militar
PyMISP	<i>Python Malware Information Sharing Platform</i>

SUMÁRIO

1	INTRODUÇÃO	10
	OBJETIVOS	11
	Objetivo geral	11
	Objetivos específicos	11
2	REFERENCIAL TEÓRICO	13
	REVISÃO DA LITERATURA E ANTECEDENTES DO PROBLEMA	13
	AMEAÇA CIBERNÉTICA, VULNERABILIDADE E RISCO DE SEGURANÇA .	13
	Ameaça Cibernética	13
	Vulnerabilidade	14
	Risco de Segurança	14
	COMPARTILHAMENTO DE INTELIGÊNCIA.....	15
	UTILIZAÇÃO DO SISTEMA	16
3	REFERENCIAL METODOLÓGICO	18
	TIPO DE PESQUISA	18
	MÉTODO DE PESQUISA.....	18
	Avaliação da operação do sistema	18
	Avaliação da eficiência do sistema	20
	ETAPAS DA PESQUISA	20
	INSTRUMENTO DE PESQUISA	21
4	RESULTADOS E DISCUSSÃO	22
	RESULTADOS	22
	Quebra de Controle de Acesso	22
	Falhas Criptográficas	22
	Injeção	22
	ANÁLISE DOS RESULTADOS	23
	DISCUSSÃO DOS RESULTADOS	23
5	CONSIDERAÇÕES FINAIS	26
	REFERÊNCIAS	27

1 INTRODUÇÃO

O Exército Brasileiro vem recebendo grandes investimentos na área de cibernética e, desde então, vem buscando adotar medidas preventivas para se manter atualizado com as novas demandas que surgem com o acelerado desenvolvimento dessa atividade. Um exemplo constitui-se na criação do Comando de Defesa Cibernética (Com D Ciber) e do Centro de Defesa Cibernética (CDCiber), que têm como missão planejar, orientar, coordenar e controlar as atividades operativas, doutrinárias, de desenvolvimento e capacitação no âmbito do Sistema Militar de Defesa Cibernética (SINGER; FRIEDMAN, 2017).

O advento do Com D Ciber brasileiro segue o rumo das recentes iniciativas das mais poderosas forças armadas do mundo. Nesse contexto de aceleradas inovações no ciberespaço, como tecnologias de Internet das Coisas, conectividade 5G, entre outras, que vem abarcando equipamentos militares, podendo ser denominadas Internet das Coisas Militares, propiciando assim um aumento da importância da Segurança Cibernética (SINGER; FRIEDMAN, 2017).

No cenário cibernético atual, o número de usuários de redes de computadores se estende cada vez mais e os *malwares* ficam cada vez mais curtos e simples, tendo o atacante que empreender pouco esforço para comprometer todos os esforços defensivos de uma organização. Com essas implicações para a estratégia e o modo de atuação do Exército Brasileiro, vem se tornando cada vez mais premente a necessidade de aumentar os níveis de segurança e de capacidade de tratamento de incidentes das redes conectadas à internet, especialmente em exercícios táticos (SINGER; FRIEDMAN, 2017).

Essa necessidade, que vem ocorrendo globalmente, tem fomentado iniciativas como o Malware Information Sharing Platform (MISP), que é tanto uma plataforma de software livre para compartilhamento de dados de inteligência de ameaças, quanto um conjunto de padrões abertos para compartilhamento destas informações (CERT.br, 2021).

O sistema MISP vem permitindo que organizações compartilhem informações de inteligência de ameaças, indicadores, sobre atacantes ou qualquer outro tipo de ameaça, como servidores DNS maliciosos, *phishing*, binários, comando e controle de *botnets Internet of Things* (IoT) e amplificadores usados em ataques *Denial of Service* (DoS). Os usuários do MISP vem se beneficiando do conhecimento colaborativo sobre *malwares* e outras ameaças existentes. E este é o objetivo desta plataforma: ajudar a melhorar as medidas usadas contra ataques direcionados e a definir ações preventivas e de detecção de forma confiável (CIRCL.lu, 2021).

O objetivo deste trabalho constitui-se de apresentar o funcionamento dessa ferramenta e seus reflexos para a proteção cibernética em Exercícios Táticos da Força Terrestre. Esta pesquisa justifica-se pela necessidade atual e relevante de um processo definido que contenha as fases de detecção, triagem, análise e resposta a incidentes de segurança.

Desse modo, no referencial teórico, foi feita uma revisão de literatura e uma breve explanação dos antecedentes do problema. Em seguida, foram destacados alguns conceitos especialmente importantes para o entendimento de como ocorre o compartilhamento efetivo de informações via MISP.

Em seguida, foi apresentado o referencial metodológico, abordando o tipo de pesquisa utilizado no estudo, assim como o método, as etapas e o instrumento de pesquisa. Dessa forma foi possível relatar com detalhes a forma em que a pesquisa foi feita e estruturada.

No quarto capítulo, foram listados os principais riscos de segurança para aplicações como as utilizadas pelo Exército. Após a listagem foi apresentado como o MISP contribui para a segurança em relação aos riscos descritos.

Ainda no quarto capítulo, foram apresentados os principais reflexos da utilização do MISP como ferramenta de proteção cibernética em Exercícios Táticos. Buscou-se analisar os impactos sobre as operações, influenciando diretamente na consciência situacional do tomador de decisões, assim como os impactos na rotina operacional de uma OM.

Por fim, concluiu-se com a finalidade de verificar se o objetivo geral da pesquisa foi plenamente atingido, adicionando ainda algumas considerações acerca do assunto. Após isso, foram referenciados os autores citados no trabalho, conforme as normas da ABNT.

OBJETIVOS

Objetivo geral

Apresentar o funcionamento do sistema MISP como meio de compartilhamento de inteligência de ameaças de forma automatizada em Exercícios Táticos, visando aprimorar a segurança cibernética do Exército Brasileiro.

Objetivos específicos

Identificar os principais riscos de segurança presentes nos serviços de rede comumente utilizados pelo Exército Brasileiro em Exercícios Táticos.

Apresentar as configurações do sistema MISP, permitindo a utilização de catálogos com inteligência de ameaças, compartilhados entre organizações que utilizam o sistema.

Identificar a eficiência do sistema MISP como ferramenta de proteção cibernética das redes utilizadas pelo Exército Brasileiro em Exercícios Táticos.

2 REFERENCIAL TEÓRICO

REVISÃO DA LITERATURA E ANTECEDENTES DO PROBLEMA

Em 2008, a Estratégia Nacional de Defesa (END) estabeleceu prioridade em três setores estratégicos para a Defesa Nacional: Nuclear, Cibernético e Espacial. Em 2009, ficou estabelecida para o Exército a responsabilidade pela coordenação e pela integração do setor cibernético. Em cumprimento a isso foi ativado em 2010 o Núcleo do Centro de Defesa Cibernética e aprovada em 2012 a Política Cibernética de Defesa, que contém a doutrina de emprego do Setor Cibernético (BRASIL, 2014).

A Política Cibernética de Defesa define três tipos de ações cibernéticas: ataque cibernético, proteção cibernética e exploração cibernética. A vertente mais relevante para essa pesquisa, a proteção cibernética, é definida da seguinte forma:

Abrange ações para neutralizar ataques e exploração cibernética contra os nossos dispositivos computacionais e redes de computadores e de comunicações, incrementando as ações de Segurança, Defesa e Guerra Cibernética em face de uma situação de crise ou conflito. É uma atividade de caráter permanente (BRASIL, 2014).

AMEAÇA CIBERNÉTICA, VULNERABILIDADE E RISCO DE SEGURANÇA

Aplicativos de rede simulados em Exercícios Táticos estão sujeitos a inúmeros riscos de segurança. Esses riscos são gerados por ameaças que podem ou não explorar vulnerabilidades existentes na rede da operação. A seguir, esses importantes conceitos serão abordados, a fim de formar a base teórica sobre a qual se desenvolverá a pesquisa.

Ameaça Cibernética

Ameaça Cibernética é definida como uma causa potencial de um incidente indesejado, que pode resultar em dano ao espaço cibernético de interesse (Política Cibernética de Defesa, 2014).

Esse programa malicioso pode ser instalado à distância e pode ter formas diversas: código executável, script ou outros tipos de programas que, à primeira vista, parecem inofensivos (CERT.br).

Ameaças cibernéticas podem ter diversos objetivos, como a obtenção de acesso à arquivos e dados. Em operações militares as consequências dessas ações podem ser catastróficas.

Vulnerabilidade

Vulnerabilidade é uma causa potencial de um incidente indesejado ou um conjunto de fatores internos, que podem resultar em risco para um sistema, e podem ser evitados por uma ação interna de segurança da informação (GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES, 2013).

A fundação *Open Web Application Security Project* (OWASP), reconhecida internacionalmente por atuar na segurança de aplicações considera que um aplicativo de rede fica vulnerável quando:

- * Os dados fornecidos pelo usuário não são validados, filtrados ou higienizados pelo aplicativo.
- * Consultas dinâmicas ou chamadas não parametrizadas sem escape ciente do contexto são usadas diretamente no interpretador.
- * Dados hostis são usados nos parâmetros de pesquisa de mapeamento relacional de objeto (ORM) para extrair registros confidenciais adicionais.
- * Dados hostis são usados diretamente ou concatenados. O SQL ou comando contém a estrutura e os dados maliciosos em consultas dinâmicas, comandos ou procedimentos armazenados (OWASP.org, 2021).

Aplicações são utilizadas pelo Exército Brasileiro em sistemas de Comando e Controle a fim de gerar consciência situacional para os comandantes em diversos escalões. Essas aplicações estão sujeitas a apresentar vulnerabilidades.

Risco de Segurança

Risco de segurança pode ser definido como a potencial exploração de uma ou mais vulnerabilidades de um sistema, por parte de uma ou mais ameaças, gerando impacto negativo nesse sistema (GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES, 2013).

Conforme mostra o diagrama da figura 1, o sistema MISP armazena informações sobre *malwares* e ataques detectados em um banco de dados (*database*) local, de forma a alimentar o seu sistema de detecção. Isso cria uma plataforma confiável de armazenamento de informações.

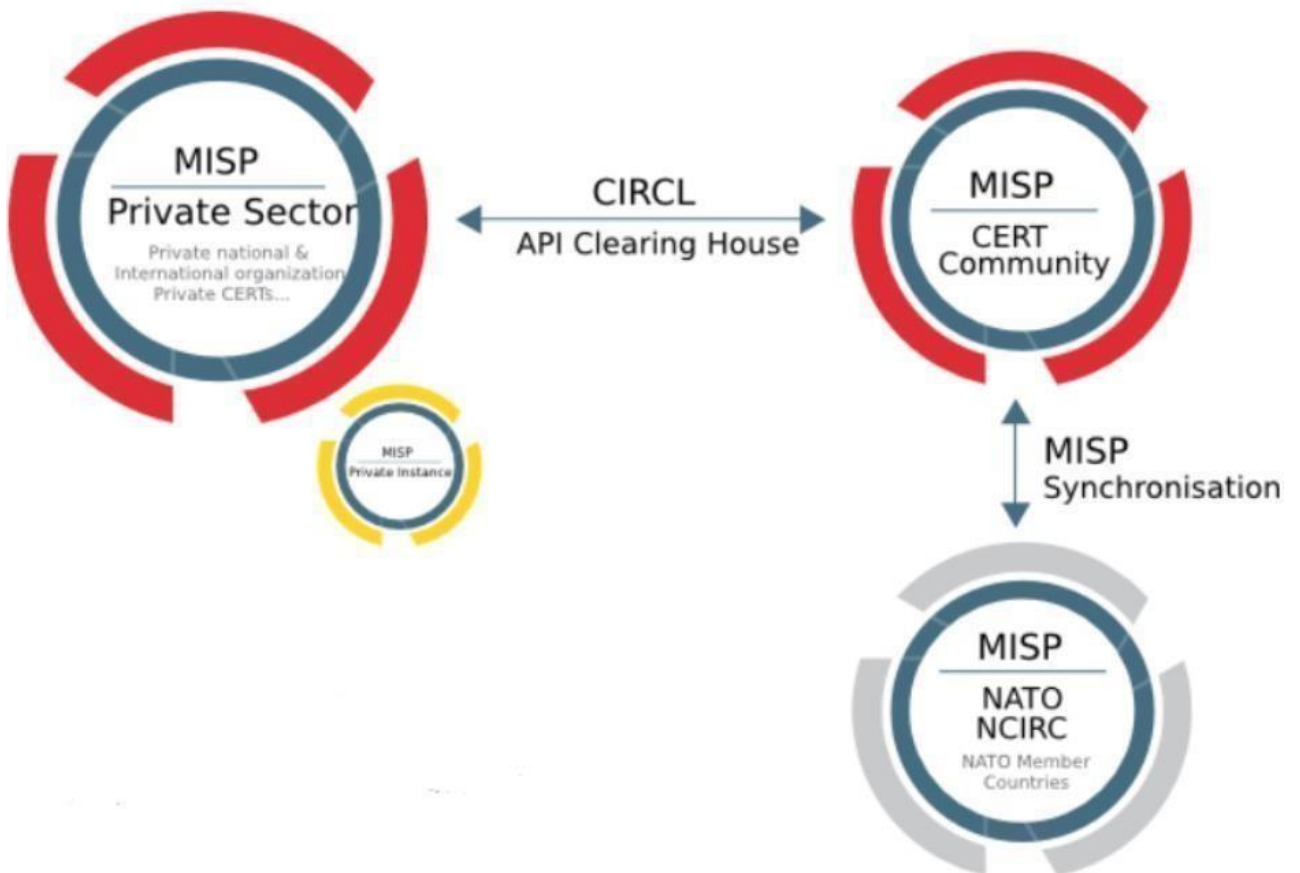
Figura 1: Como funciona o MISP



Fonte: CIRCL.lu (2021)

No diagrama da figura 2 é possível ter uma visão geral de como acontece o compartilhamento de informações entre os bancos de dados das diferentes organizações. A distribuição de eventos acontece por meio da conectividade entre as organizações que utilizam o MISP, de forma que os participantes selecionem a categoria de distribuição apropriada para cada operação.

Figura 2: Como as informações são compartilhadas entre os usuários.



Fonte: CIRCL.lu (2021)

Legenda:

- Sua organização apenas
- Comunidades conectadas
- Todas as comunidades

UTILIZAÇÃO DO SISTEMA

Este trabalho propõe a utilização do sistema MISP nas redes utilizadas pelo Exército Brasileiro em Exercícios Táticos. Conforme a seção 2.3 demonstra, ele reúne informações sobre ameaças de diversas fontes em um banco de dados, a fim de salvaguardar os sistemas da instituição. Ao acessar o menu da plataforma é possível utilizar-se de catálogos já existentes feitos por diversas instituições.

Ameaças atuais invadem sistemas eletrônicos e prejudicam suas atividades. Isso evidencia que a preocupação com a segurança cibernética é atual e crescente, tanto na área de defesa quanto na área de inteligência. Essa latente preocupação já está normatizada nas Estratégias Nacional de Defesa e Nacional de Inteligência (GOIS, 2018).

A utilização desse “*software*” de código aberto objetiva assegurar ao máximo a disponibilidade, confidencialidade, integridade e autenticidade dos dados e informações que trafegam nos sistemas de comunicações, haja vista sua importância para o processo decisório da Força (CANONGIA E MANDARINO, 2009).

O corpo técnico do Exército Brasileiro deve salvaguardar esses dados e informações, evitando os altos prejuízos decorrentes de ataques cibernéticos. Com a utilização da plataforma MISP ações podem ser tomadas de forma automatizada em resposta às ameaças cibernéticas na rede (GOIS, 2018).

3 REFERENCIAL METODOLÓGICO

TIPO DE PESQUISA

O tipo de pesquisa utilizado no presente estudo é de cunho qualitativo, pois a pesquisa examina evidências relacionadas ao objeto. Foram analisados e interpretados os dados referentes ao MISP, buscando produzir informações sobre o seu funcionamento e esclarecendo características, possibilidades e limitações do sistema que protege o espaço cibernético do Exército Brasileiro.

MÉTODO DE PESQUISA

O método de pesquisa utilizado foi o experimental, pois o MISP foi abordado sob a influência de variáveis controladas a fim de analisar o impacto dessas interações. Ou seja, foram realizados procedimentos a partir dos quais foi possível identificar a eficiência do objeto de estudo como ferramenta de proteção cibernética.

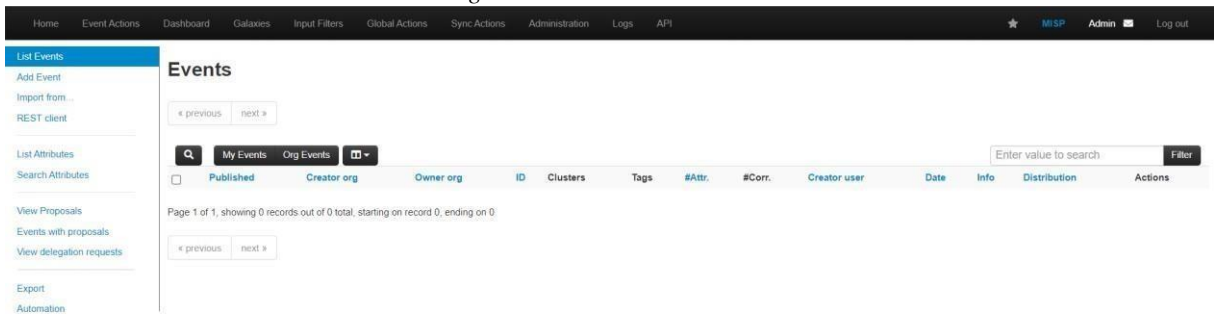
Como visto na seção 2.4, o MISP propicia segurança cibernética à rede. Desta forma, a pesquisa se baseou na utilização do sistema para coletar inteligência de ameaças.

Avaliação da operação do sistema

A operação do sistema teve como base a documentação fornecida pelo site oficial do projeto (misp-project.org).

Ao acessar o sistema, inicialmente o usuário se depara com a aba “*Home*”, conforme mostra a figura 3. Essa aba é onde os eventos são disponibilizados para acesso. No entanto, se encontra vazio, pois ainda não foi feito o *download* de nenhum repositório.

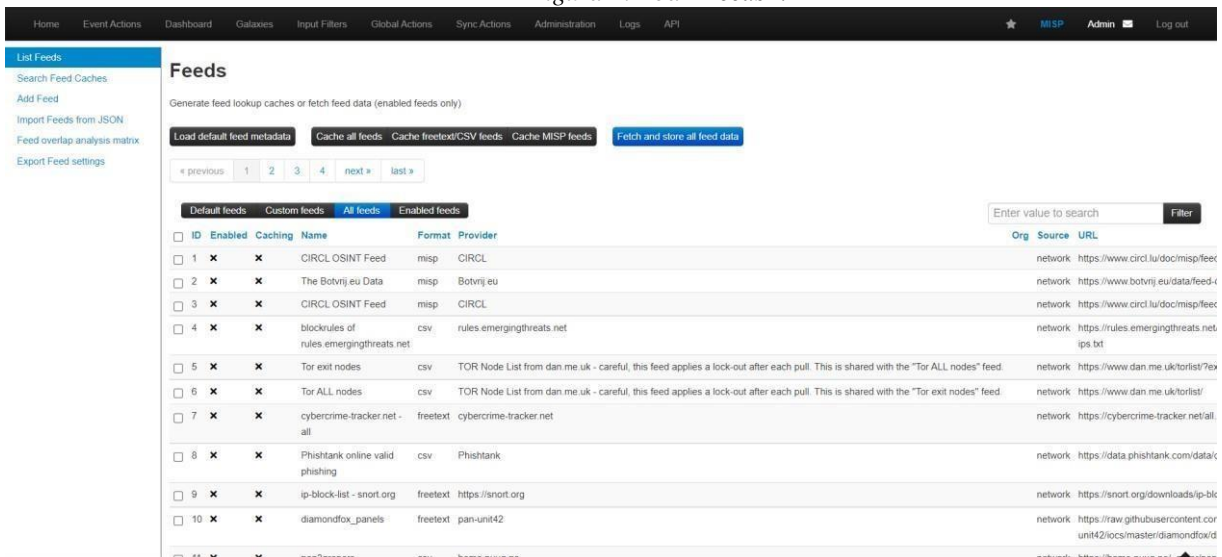
Figura 3: Aba “Home” inicial.



Fonte: AUTOR (2021)

Na aba “Feeds” (figura 4) são disponibilizados diversos repositórios de inteligência, basta selecionar os desejados e ativá-los. Após essa seleção inicia-se a busca e o compartilhamento de dados com a opção “Fetch and store all feed data”, que fará o *download* dos repositórios selecionados.

Figura 4: Aba “Feeds”.



Fonte: AUTOR (2021)

Ao retornar para a aba “Home” o usuário terá acesso aos eventos relacionados aos repositórios ativos no momento, como mostra a figura 5.

Figura 5: Aba “Home” final.

Published	Creator org	Owner org	ID	Clusters	Tags	#Attr	#Corr	Creator user	Date	Info	Distribution	Actions
<input type="checkbox"/>	Threat Actor	ORGNAME	9	Axiom	tip:green tip:white osint:source-type="blog-post" type:OSINT	4120	1	admin@admin.test	2014-10-28	OSINT - Operation SMN (Novetta)	All	
<input checked="" type="checkbox"/>	CthulhuSPRL.be	ORGNAME	1		type:OSINT tip:green tip:white	1067	1	admin@admin.test	2014-10-02	OSINT ShellShock scanning IPs from OpenDNS	All	
<input checked="" type="checkbox"/>	CthulhuSPRL.be	ORGNAME	7		type:OSINT tip:green	98		admin@admin.test	2014-10-20	OSINT OrcaRAT - A whale of a tale blog post by PWC	All	
<input checked="" type="checkbox"/>	CthulhuSPRL.be	ORGNAME	5		type:OSINT tip:green	1817	1	admin@admin.test	2014-09-01	OSINT Watching Attackers Through VirusTotal blog post by Brandon Dixon (Stplus)	All	
<input checked="" type="checkbox"/>	CthulhuSPRL.be	ORGNAME	8		type:OSINT tip:green	414		admin@admin.test	2014-10-23	Expansion on OSINT Operation Pawn Storm: The Red in SEDNIT from Trend Micro	All	
<input checked="" type="checkbox"/>	CthulhuSPRL.be	ORGNAME	8		type:OSINT tip:green	31		admin@admin.test	2014-10-11	OSINT Shellshock exploitation from Red Sky Weekly blog post	All	
<input checked="" type="checkbox"/>	CthulhuSPRL.be	ORGNAME	4		type:OSINT tip:green	65	1	admin@admin.test	2014-10-09	OSINT Democracy in Hong Kong Under Attack: blog post from Volexity (Steven Adair)	All	
<input checked="" type="checkbox"/>	CthulhuSPRL.be	ORGNAME	3		type:OSINT tip:green	225		admin@admin.test	2014-10-09	OSINT Evolution of the Nuclear Exploit Kit by Cisco Talos group	All	
<input checked="" type="checkbox"/>	CthulhuSPRL.be	ORGNAME	2		type:OSINT tip:green	29		admin@admin.test	2014-10-03	OSINT New Indicators of Compromise for APT Group Nitro Uncovered blog post by Palo Alto	All	

Fonte: AUTOR (2021)

Avaliação da eficiência do sistema

A eficiência do sistema como plataforma de defesa cibernética consiste na enorme quantidade de informação disponibilizada e na sua constante atualização. Isso garante ao usuário acesso a informação sobre IoCs, ataques direcionados e demais ameaças, permitindo tomar ações preventivas e contra-medidas como bloqueá-las por meio de *firewall*, filtros, ou ainda, apenas saber se elas estão afetando ou não a sua rede.

ETAPAS DA PESQUISA

A pesquisa foi constituída das seguintes etapas:

Inicialmente, o tema foi escolhido e delimitado em razão de sua importância e atualidade. Foram lidos livros e artigos científicos como Segurança e Guerra Cibernéticas, de Singer e Friedman (2017) e *Cyber situational awareness - A systematic review of the literature*, de Franke e Brynielsson (2014), a fim de aumentar o conhecimento sobre a temática.

Posteriormente, o objetivo geral foi escolhido e, baseado nele, foram estabelecidos três objetivos específicos. O problema surgiu prontamente, visto que as recentes providências tomadas em relação à segurança cibernética demonstram que o Exército deseja evoluir em relação à sua capacidade de atuação no espaço cibernético.

Em seguida, procurou-se conceituar elementos importantes para o entendimento da pesquisa, ao mesmo tempo em que o funcionamento do MISP era estudado. A redação iniciou-se pelo Projeto de Pesquisa, o qual após ser entregue conduziu os estudos para a operação do sistema, a fim de atingir os objetivos estipulados para o trabalho.

Assim, o desenvolvimento foi pautado nas demandas atuais de segurança cibernética, abordando como o MISP, com suas características, possibilidades e limitações, seria uma ferramenta eficiente.

INSTRUMENTO DE PESQUISA

A presente monografia foi realizada a partir de uma pesquisa exploratória, na qual o instrumento de pesquisa utilizado para coleta de dados foi a análise documental, com a finalidade de dar o embasamento teórico necessário e atingir os objetivos do trabalho. As principais fontes utilizadas foram: o Manual de Campanha EB70-MC-10.232 – Guerra Cibernética, a Doutrina Militar de Defesa Cibernética, o guia de usuário MISP – *User Guide*, além de diversos artigos relacionados ao assunto, retirados dos sítios eletrônicos CERT.br, CIRCL.lu e OWASP.org.

4 RESULTADOS E DISCUSSÃO

A problematização exposta pelo objetivo geral do trabalho relaciona cibernética com as operações militares, áreas de concentração que, integradas, cooperam com a expansão das capacidades operativas do Exército Brasileiro.

RESULTADOS

A fim de identificar os principais riscos de segurança presentes nos serviços de rede comumente utilizados pelo Exército Brasileiro em Exercícios Táticos, serão apresentadas as três maiores vulnerabilidades de aplicativos de internet de 2021. Elas são assim classificadas assim pelo OWASP Top 10, um documento elaborado anualmente pela fundação OWASP e reconhecido internacionalmente por desenvolvedores e profissionais de segurança na internet.

Quebra de Controle de Acesso

O controle de acesso impõe que os usuários não possam agir fora de suas permissões pretendidas. As falhas nesse controle normalmente levam à divulgação, modificação ou destruição de informações não autorizadas (OWASP.org, 2022).

Falhas Criptográficas

Essas falhas estão relacionadas à criptografia (ou à falta dela). O que muitas vezes leva à exposição de dados confidenciais (OWASP.org, 2022).

Injeção

Ataques de injeção, quando bem sucedidos, abrem portas para outros tipos de ataques. Nesse tipo de ataque o invasor pode acessar informações ou executar comandos. Um invasor pode utilizar diversos vetores desse ataque, os mais comuns são o SQL, e o NoSQL. Ao encontrar uma falha de segurança, o atacante garante acesso ao banco de dados do sistema (OWASP.org, 2022).

A exploração dessas vulnerabilidades pode ter os mais variados objetivos, podendo impactar de forma negativa as operações militares. Vazamento de informação e acesso não autorizado são exemplos de possíveis ações realizadas por atacantes no espaço cibernético (OWASP.org, 2022).

ANÁLISE DOS RESULTADOS

Os riscos de segurança, definidos na subseção 2.2.3 e apresentados na seção anterior podem ser geridos por meio do compartilhamento de inteligência de ameaças entre Organizações Militares em tempo real.

O sistema MISP permite também o compartilhamento de atualizações, fazendo com que essas organizações tenham suas vulnerabilidades mitigadas antes que elas sejam exploradas.

A figura 6 a seguir mostra como o MISP pode ser utilizado para compartilhar esse tipo de inteligência por meio da interface do próprio sistema.

Figura 6: Compartilhamento de inteligência.

Galaxy Cluster Relationships Index
List all relationships between Galaxy Clusters

Navigation: - previous | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | next -

Buttons: All | Default Galaxy Cluster Relations | Custom Galaxy Cluster Relations | Search: Enter value to search | Filter

Id	Default	Galaxy Cluster Source	Galaxy Cluster Target	Relationship Type	Relationship Tag	Owner Org	Creator Org	Distribution	Actions
1	✓	tool :: Tinba	exploit-kit :: Hunter	similar	estimative-language-likelihood-probability="likely"			All communities	🗑️
2	✓	tool :: Tinba	banker :: Tinba	similar	estimative-language-likelihood-probability="likely"			All communities	🗑️
3	✓	tool :: Tinba	malpedia :: Tinba	similar	estimative-language-likelihood-probability="likely"			All communities	🗑️
4	✓	tool :: PlugX	rat :: PlugX	similar	estimative-language-likelihood-probability="likely"			All communities	🗑️
5	✓	tool :: PlugX	mitre-enterprise-attack-malware :: PlugX - S0013	similar	estimative-language-likelihood-probability="likely"			All communities	🗑️
6	✓	tool :: PlugX	malpedia :: PlugX	similar	estimative-language-likelihood-probability="likely"			All communities	🗑️
7	✓	tool :: Poison Ivy	threat-actor :: Anchor Panda	used by	estimative-language-likelihood-probability="likely"			All communities	🗑️
8	✓	tool :: Poison Ivy	rat :: PoisonIvy	similar	estimative-language-likelihood-probability="likely"			All communities	🗑️
9	✓	tool :: Poison Ivy	mitre-enterprise-attack-malware :: PoisonIvy - S0012	similar	estimative-language-likelihood-probability="likely"			All communities	🗑️
10	✓	tool :: Poison Ivy	malpedia :: Poison Ivy	similar	estimative-language-likelihood-probability="likely"			All communities	🗑️
11	✓	tool :: Poison Ivy	tool :: poisonivy	similar	estimative-language-likelihood-probability="likely"			All communities	🗑️
12	✓	tool :: Torn RAT	threat-actor :: Anchor Panda	used-by	estimative-language-likelihood-probability="likely"			All communities	🗑️
13	✓	tool :: Elise Backdoor	mitre-enterprise-attack-malware :: Elise - S0081	similar	estimative-language-likelihood-probability="likely"			All communities	🗑️
14	✓	tool :: Elise Backdoor	malpedia :: Elise	similar	estimative-language-likelihood-probability="likely"			All communities	🗑️
15	✓	tool :: Trojan.Lazik	malpedia :: Lazik	similar	estimative-language-likelihood-probability="likely"			All communities	🗑️
16	✓	tool :: Flame	threat-actor :: GMI-Rot	similar	estimative-language-likelihood-probability="likely"			All communities	🗑️

Fonte: MISP-project.org (2022)

O MISP, por ser uma plataforma de inteligência de ameaças de código aberto e padrões abertos para compartilhamento de informações, recebe atualizações constantes, aumentando a sua proteção a cada versão.

DISCUSSÃO DOS RESULTADOS

A consciência situacional proporcionada por aplicações de comando e controle (C²) é resultado de uma combinação de informações a fim de refinar estimativas e previsões. No âmbito do planejamento militar essas estimativas e previsões são interpretadas diretamente pelo tomador de decisões (FRANKE; BRYNIELSSON, 2014).

Com isso, pode-se inferir que a confiabilidade dessas informações é um fator primordial no cenário militar, em consequência dos diversos riscos de segurança existentes, como os destacados na seção anterior.

Para identificar e lidar com ataques cibernéticos, a Estônia aposta no monitoramento do tráfego de dados na internet e na habilidade de executar uma análise tática e estratégica desses dados (FRANKE; BRYNIELSSON, 2014).

Essa é basicamente a proposta do sistema MISP, que permite a utilização de catálogos com inteligência compartilhada de ameaças. Isso pode ser atingido a partir de sua configuração mais básica, conforme mostrado na subseção 3.2.1.

Desenvolver as capacidades de monitorar e controlar o espaço cibernético é uma estratégia que visa fortalecer a capacidade de dissuasão do Exército Brasileiro, que é o órgão incumbido da responsabilidade pelo setor cibernético no Brasil (ESTRATÉGIA NACIONAL DE DEFESA, 2020).

A plataforma MISP garante os seguintes benefícios aos usuários:

- * Armazenar informações sobre malware e ataques detectados.
- * Aprender com os outros as questões de segurança que eles são enfrentando ou detectando.
- * Iniciar uma pesquisa específica sobre eventos presentes e passados.
- * Refletir sobre as atividades e ameaças atuais.
- * Melhorar seus próprios processos e ferramentas internas ao avaliar as ameaças atualmente compartilhadas.
- * Usar os indicadores do sistema para proteger a sua infraestrutura.
- * Coletar as informações para apoiar sua equipe de inteligência.
- * Aprender a linguagem comum e as taxonomias usadas entre as equipes de resposta a incidentes (CIRCL.lu, 2021, tradução nossa).

A infraestrutura de informação proporcionada pela plataforma MISP pode se relacionar a dois diferentes contextos no Exército Brasileiro, sendo eles a rotina operacional de uma OM (melhorando a segurança da informação) ou os trabalhos de comando e controle de uma operação específica (contribuindo para a consciência situacional do tomador de decisões) (FRANKE; BRYNIELSSON, 2014).

Apresentados os benefícios de se utilizar a plataforma é possível afirmar que o sistema MISIP é importante tanto na perspectiva do monitoramento quanto no controle do espaço cibernético. No âmbito dos exercícios no terreno realizados pelo Exército Brasileiro o sistema se mostra eficiente mesmo em sua configuração mais basilar, conforme mostrado na subseção 3.2.2.

5 CONSIDERAÇÕES FINAIS

Concluindo o trabalho, é possível identificar uma correlação entre o setor cibernético e as operações militares. Essa correlação é caracterizada pelo Sistema de Defesa Cibernética, que exerce papel fundamental para aumentar o grau de dissuasão da Força Terrestre, assim como colabora para o seu emprego efetivo nas missões que lhe são atribuídas (BRASIL, 2020).

Nesse sentido, o presente trabalho buscou estudar as ameaças cibernéticas pela perspectiva do compartilhamento de informação a partir de uma fonte confiável. Assim, o problema da segurança cibernética no âmbito dos Exercícios Táticos pode ser amenizado por meio da utilização do sistema MISP como ferramenta de compartilhamento de inteligência de ameaças de forma automatizada nessas atividades.

Somado a isso, recomenda-se como continuação natural dessa linha de pesquisa, estudos sobre o PyMISP, que consiste na utilização de bibliotecas python para acessar a plataforma MISP, a fim de automatizar ainda mais o processo de compartilhamento de ameaças.

Ainda, sugere-se como oportunidade para novos estudos a capacitação em segurança cibernética, tendo em vista a necessidade de resposta às ameaças cibernéticas atuais.

Por fim, ressalta-se a importância de se fortalecer a colaboração entre a comunidade acadêmica e o setor de defesa, especialmente em áreas que contribuam com a segurança no âmbito nacional, como é o caso do setor cibernético.

REFERÊNCIAS

BRASIL. Exército. **GUERRA CIBERNÉTICA** - Manual de Campanha. 1º Edição, 2017

CANONGIA, C.; JÚNIOR, A. G.; JUNIOR, R. M. **GUIA DE REFERÊNCIA PARA A SEGURANÇA DAS INFRAESTRUTURAS CRÍTICAS DA INFORMAÇÃO**. Brasília: Versão 01, 2010.

CANONGIA, C.; JUNIOR, R. M. **SEGURANÇA CIBERNÉTICA: O DESAFIO DA NOVA SOCIEDADE DA INFORMAÇÃO**. Parcerias Estratégicas, v. 14, p. 21–46, 2009.

CÓDIGOS MALICIOSOS (MALWARE). Disponível em: <https://cartilha.cert.br/malware/>. Acesso em: 30 maio 2021.

DOCTRINA MILITAR DE DEFESA CIBERNÉTICA - MD31- M-07. 1ª Edição, 2014

ESTRATÉGIA NACIONAL DE DEFESA. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/estrategia-nacional-de-defesa. Acesso em: 24 dez. 2021.

FRANKE, U.; BRYNIELSSON, J. *Cyber situational awareness - A systematic review of the literature*. *Computers and Security*, v. 46, p. 18–31, 2014.

GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES. Revisão 01, 2013.

GOIS, A. B. **SEGURANÇA CIBERNÉTICA: O OLHAR DA DEFESA NACIONAL E DA INTELIGÊNCIA DE ESTADO FRENTE ÀS VULNERABILIDADES DIGITAIS**. Revista Científica da Escola de Comunicações, v. 8, 2018.

MISP - PLATAFORMA DE INTELIGÊNCIA DE AMEAÇAS DE CÓDIGO ABERTO. Disponível em: <https://www.circl.lu/services/misp-malware-information-sharing-platform/>. Acesso em: 30 maio 2021.

MISP USER GUIDE. Disponível em: <https://www.circl.lu/doc/misp/>. Acesso em: 24 dez. 2021.

OWASP Top 10 Web Application Security Risks. Disponível em: <https://owasp.org/www-project-top-ten/>. Acesso em: 22 jul. 2021.

RECOMENDAÇÕES PARA MELHORAR O CENÁRIO DE ATAQUES DISTRIBUÍDOS DE NEGAÇÃO DE SERVIÇO (DDoS). Disponível em: <https://www.cert.br/docs/whitepapers/ddos/>. Acesso em: 30 maio 2021.

RECURSOS DO MISP, A PLATAFORMA DE COMPARTILHAMENTO DE AMEAÇAS DE CÓDIGO ABERTO. Disponível em: <https://www.misp-project.org/features.html>. Acesso em: 30 maio 2021.

SHARING, I. et al. *Information Sharing and Cyber Security - The Benefits of the Malware Information Sharing Platform (MISP)*. Computer Incident Response Center Luxembourg, 2016.

SINGER, P. W.; FRIEDMAN, A. *Segurança e Guerra Cibernéticas*. Biblioteca do Exército, 2017.