Glossário de Termos Preliminar

Term Termo	Definição PT	Definição EN	Fonte da Definição	Terminologia Relacionada	Relações entre Termos	Sinônimos ou Conflitos
information asset ativo de informação	Merge com base em Op3 (LLM?). Op1 - Pessoa, estrutura organizacional, instalação, informação e registros, sistemas e recursos de tecnologia da informação, material, processo, relacionamentos ou reputação que tem valor. [3] Op2 - Qualquer coisa que tenha valor para uma pessoa ou organização. [5] Op3 - Meios de armazenamento, transmissão e processamento de dados e informação, os equipamentos necessários a isso (computadores, equipamentos de comunicações e de interconexão), os sistemas utilizados para tal, os sistemas de	Op1 - A person, structure, facility, information, and records, information technology systems and resources, material, process, relationships, or reputation that has value. [3] Op2 - Anything that has value to a person or organization. [5]	[3], [5], [14] [15]	[1] UcoProduct; UcoHardware; UcoSoftware. [6] socsSecurity_asset	campaign targets information_asset **OK** attack targets information_asset **OK**	product, hardware, software, target,

	informação de um modo geral, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso [1514]. OP4 - Asset identifies a critical resource or entity within an organization's cybersecurity framework, such as hardware, software, or data, characterized by attributes like sensitivity (e.g., "high"). It is a primary focus for protection and monitoring in incident response. [7, ?]					
attack ataque	Merge com base em Op3 Op1 - Tentativa de danificar, interromper ou obter acesso não autorizado a sistemas de computador, redes ou dispositivos. [4] Op2 - Qualquer tipo de atividade maliciosa que tente coletar, interromper, negar, degradar ou destruir recursos do sistema de informação (e.g., de computador, redes ou dispositivos) ou a própria informação. [5] Op 3 - Attack is defined	Op1 - An attempt to damage, disrupt or gain unauthorised access to computer systems, networks or devices. [4] Op2 - Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself. [5]	[4, 5, 7, 15, 16, 17]	[1] ucoAttack; ucoIncident; [6] socsIncident	attack affects organization **OK** attack targets asset **OK** attack follows attack_pattern attack is-a event TTPs (MITRE ATTACK)	incident

	as an event that has the potential to compromise the confidentiality, integrity, security, or availability of information, systems, or IT networks, along with all their stakeholders. [7, ?] Op 4 - Qualquer tentativa, bem ou mal sucedida, de acesso ou uso não autorizado de um serviço, computador ou rede [16]. Isto é, uma série de passos dados por um atacante para produzir um resultado não autorizado [17]. [15]					
attack_vector vetor de ataque	Merge com base em Op1 Op1 - Métodos (e.g., Tactics, Techniques and Procedures - TTPs) que um atacante usa para obter acesso não autorizado a um sistema ou dispositivo de computador. [4] Op2 - vetor de ataque são TTP (Táticas, Técnicas e Procedimentos) que representam o comportamento ou modus operandi dos adversários cibernéticos	Op1 - The method an attacker uses to gain unauthorised access to a computer system or device. [4] Op2 - attack vector are TTP (Tactics, Techniques and Procedures) that represent the behavior or modus operandi of cyber adversaries [7].	[4, 7]	[1] ucoMeans; ucohasAccessVector	attack uses technology attack_vector **OK** attack_vector is-part-of course–action **OK**	tool, technology, malware, TTP técnicas, procedimentos

	[7].					
backdoor “porta dos fundos” ou vulnerabilidade	Op1 - Backdoor é uma ferramenta instalada após um comprometimento para dar a um invasor acesso mais fácil ao sistema comprometido em torno de quaisquer mecanismos de segurança que estejam em vigor. [2] Op2 - Maneira não documentada (e.g., usando um malware) de obter acesso a um sistema de computador. Backdoor é um risco potencial de segurança. [5]	Op1 - A backdoor is a tool installed after a compromise to give an attacker easier access to the compromised system around any security mechanisms that are in place. [2] Op2 - An undocumented way (e.g., using a malicious program) of gaining access to a computer system. A backdoor is a potential security risk. [5]	[2] ou [5]	[1] ucoBackdoor	backdoor is-a attack_vector **OK** backdoor is-a malware Incluir outros vetores attack_vector -> Técnica -> backdoor e outros	vulnerability, weakness, tool, technology, malware attack_vector
campaign campanha	O termo Campanha descreve qualquer agrupamento de atividades de intrusão conduzidas durante um período específico com alvos e objetivos comuns. [7]	The term Campaign describes any grouping of intrusion activity conducted over a specific period with common targets and objectives. [7]	[7]	[1] ucoCampaign	campaign targets organization **OK**	attack set_of_attacks
characteristics características	Informações detalhadas ou estruturadas sobre um elemento conceitual estratégico do domínio.	Detailed or structured information about a strategic conceptual element of the domain.	[?]	[1] ucoObservable	attack has characteristics **OK** vulnerability has characteristics **OK** malware has characteristics	features, behaviors, properties, aspects

					OK security has characteristics **OK**	
consequence consequência	O efeito de um evento, incidente ou ocorrência. Em segurança cibernética, o efeito de uma perda de confidencialidade, integridade ou disponibilidade de informações ou de um sistema de informações nas operações de uma organização, seus ativos, em indivíduos, outras organizações ou em interesses nacionais. [3]	The effect of an event, incident, or occurrence. In cybersecurity, the effect of a loss of confidentiality, integrity or availability of information or an information system on an organization's operations, its assets, on individuals, other organizations, or on national interests. [3]	[3]	[1] ucoConsequence	incident has consequence **OK**	Synonym of impact [3] damage
course of action “curso de ação” ou “sequência de passos” ou “passo a passo”	Op1 - Combinação de medidas de resposta a riscos em fases ou dependentes da situação. [5] Op2 - Modelo de segurança cibernética que divide um ataque cibernético típico em estágios para ajudar as equipes de segurança a identificar ataques cibernéticos em andamento e detê-los. Inclui oito fases: reconhecimento, armamento, entrega, exploração, instalação,	Op1 - A time-phased or situation-dependent combination of risk response measures. [5] Op2 - The cyber kill chain is a cybersecurity model that breaks down a typical cyberattack into stages to help security teams identify in-progress cyberattacks and stop them. It includes eight phases: reconnaissance, weaponization, delivery, exploitation, installation, command and control, actions on objectives, and monetization. [8]	[5] ou [8]	[1] ucoCourseofAction; ucoKillChain; ucoKillChainPhase; [6] socsCourse_of_action	attack has course_of_action **OK**	KilChain, KillChainPhase CyberKillChain

	comando e controle, ações sobre objetivos e monetização. [8]					
damage dano	Efeito de um evento, incidente ou ocorrência. Em segurança cibernética, o efeito de uma perda de confidencialidade, integridade ou disponibilidade de informações ou de um sistema de informações nas operações de uma organização, seus ativos, em indivíduos, outras organizações ou em interesses nacionais. [3]	The effect of an event, incident, or occurrence. In cybersecurity, the effect of a loss of confidentiality, integrity or availability of information or an information system on an organization's operations, its assets, on individuals, other organizations, or on national interests. [3]	[3]	[1] ucoConsequence	incident has damage **OK**	consequence ; impact
event evento	Op1 - Ocorrência observável em um sistema de informação ou rede. Às vezes fornece uma indicação de que um incidente está ocorrendo ou pelo menos levanta a suspeita de que um incidente pode estar ocorrendo. [3] Op2 - Ações tomadas por meio do uso de um sistema de informação ou rede que resultam em um efeito adverso (real ou potencial) em um sistema de informação, rede ou nas informações nele contidas. [5]	Op1 - An observable occurrence in an information system or network. Sometimes provides an indication that an incident is occurring or at least raises the suspicion that an incident may be occurring. [3] Op2 - Actions taken through the use of an information system or network that result in an actual or potentially adverse effect on an information system, network, and/or the information residing therein. [5]	[3] ou [5]	[1] ucoObservable [6] socsSecurity_event	organization detects incident **OK** attack causes incident **OK**	incident [3] and [5]

attacker atacante	Op1 - Indivíduo, grupo, organização ou governo que conduz ou tem a intenção de conduzir atividades prejudiciais. [3] Op2 - Uma parte, incluindo um insider, que age com intenção maliciosa de comprometer um sistema. [5]	Op1 - An individual, group, organization, or government that conducts or has the intent to conduct detrimental activities. [3] Op2 - A party, including an insider, who acts with malicious intent to compromise a system. [5]	[3] ou [5]	[1] ucoAttacker	attacker runs attack **OK**	threat agent, adversary [3]
incident incidente	Ocorrência que efetivamente ou potencialmente coloca em risco a confidencialidade, integridade ou disponibilidade de um sistema de informação ou das informações que o sistema processa, armazena ou transmite, ou que constitui uma violação ou ameaça iminente de violação de políticas de segurança, procedimentos de segurança ou políticas de uso aceitável. [5]	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. [5]	[5]	[1] ucoIncident; ucoAttack [6] socsIncident	incident has impact **OK** incident has consequence **OK**	event [3] and [5]
location localização	Um lugar ou posição específica. [9]	A particular place or position. [9]	[9]	[1] ucoAddress [6] socsLocation	organization has location **OK**	organization
malware software malicioso	Op1 - Software que compromete a operação de um sistema ao executar uma função ou	Op1 - Software that compromises the operation of a system by performing an unauthorized function or	[3], [4] ou [5]	[1] ucoMalware	malware supports course of action **OK**	malicious code malicious

	processo não autorizado. [3] Op2 - Derivado de 'software malicioso', malware é qualquer tipo de software que pode danificar sistemas de computador, redes ou dispositivos. Inclui vírus, ransomware e trojans. [4] Op3 - Software ou firmware destinado a executar um processo não autorizado que terá impacto adverso na confidencialidade, integridade ou disponibilidade de um sistema de informação. Um vírus, worm, cavalo de Troia ou outra entidade baseada em código que infecta um host. Spyware e algumas formas de adware também são exemplos de código malicioso. [5]	process. [3] Op2 - Derived from 'malicious software', malware is any kind of software that can damage computer systems, networks or devices. Includes viruses, ransomware and trojans. [4] Op3 - Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code. [5]			malware exploits vulnerability **OK** malware is-part-of / belongs-to malware_family **OK**	software malicious program
malware family família de software malicioso	Categoria de malware. Exemplos: Vírus, Ransomware, Worms, Spyware.	Malware category. Examples: Vírus, Ransomware, Worms, Spyware.			malware_family follows attackPattern **OK**	
Ransomware software de resgate	Op1 - Um tipo de malware que é uma forma de extorsão. Ele funciona criptografando o disco rígido da vítima,	Op1 - A type of malware that is a form of extortion. It works by encrypting a victim's hard drive denying them access to key files.	[1] ou [3]		Ransomware is-a malware_family **OK**	type of / instance of malware family

	negando a ela acesso aos arquivos-chave. A vítima deve então pagar um resgate para descriptografar os arquivos e obter acesso a eles novamente. [1] Op2 - Um malware projetado para negar a um usuário ou organização o acesso aos arquivos em seu computador.	The victim must then pay a ransom to decrypt the files and gain access to them again. [1] Op2 - A malware designed to deny a user or organization access to files on their computer.				
Attack Pattern Padrão de Ataque	Eventos ou comportamentos cibernéticos semelhantes que podem indicar que um ataque ocorreu ou está ocorrendo, resultando em uma violação de segurança ou uma potencial violação de segurança. [3]	Similar cyber events or behaviors that may indicate an attack has occurred or is occurring, resulting in a security violation or a potential security violation. [3]	[3]	[1] ucoAttackPattern	malware_family has attackPattern **OK**	malware behavior
motivation motivação	Motivo que leva um atacante a planejar ou executar um ataque (e.g., ganho financeiro ou perda de credibilidade)	Reason an attacker plans or executes an attack (e.g., financial gain or loss of credibility)	[?]	[1] ucoStatementType; ucohasMotivation	attack has motivation **OK**	reason, rationale
system sistema	Combinação de elementos interativos organizados para atingir um ou mais propósitos declarados. Nota 1: Existem muitos tipos de sistemas. Exemplos incluem: sistemas de informação de propósito	Combination of interacting elements organized to achieve one or more stated purposes. Note 1: There are many types of systems. Examples include: general and special-purpose information systems;	[5]	[1] ucoSystem	system is-a asset **OK**	operating system

	geral e especial; sistemas de comando, controle e comunicação; módulos criptográficos; unidade de processo central e placas de processador gráfico; sistemas de controle industrial e de processo; sistemas de controle de voo; sistemas de armas, mira e controle de fogo; dispositivos médicos e sistemas de tratamento; sistemas de transações financeiras, bancárias e de merchandising; e sistemas de redes sociais. Nota 2: Os elementos interativos na definição de sistema incluem hardware, software, dados, humanos, processos, instalações, materiais e entidades físicas naturais. Nota 3: Sistemas de sistemas estão incluídos na definição de sistema. Fontes: NIST SP 800-37 Rev. 2 da ISO/IEC 15288 [5]	command, control, and communication systems; crypto modules; central process unit and graphics processor boards; industrial and process control systems; flight control systems; weapons, targeting, and fire control systems; medical devices and treatment systems; financial, banking, and merchandising transaction systems; and social networking systems. Note 2: The interacting elements in the definition of system include hardware, software, data, humans, processes, facilites, materials, and naturally occurring physical entities. Note 3: Systems of systems is included in the definition of system. Sources: NIST SP 800-37 Rev. 2 from ISO/IEC 15288 [5]				
organization organização	Entidade de qualquer tamanho, complexidade ou posicionamento dentro de uma estrutura	An entity of any size, complexity, or positioning within an organizational structure (e.g., a federal	[5]	[1] ucoBaseGroup; ucoEnvironmentalGroup; ucoTemporalGroup	organization has asset **OK** campaign targets	institution enterprise entity

	organizacional (e.g., uma agência federal ou, conforme o caso, qualquer um de seus elementos operacionais). [5]	agency or, as appropriate, any of its operational elements). [5]			organization **OK**	
software logiciário ou “programa de computador”	Op1 - Programas de computador (que são armazenados e executados pelo hardware do computador) e dados associados (que também são armazenados no hardware) que podem ser dinamicamente escritos ou modificados durante a execução. [2] Op2 - Programas de computador e dados associados que podem ser dinamicamente escritos ou modificados durante a execução do dispositivo (e.g., código de aplicativo, bibliotecas). [5]	Op1 - Computer programs (which are stored in and executed by computer hardware) and associated data (which also is stored in the hardware) that may be dynamically written or modified during execution. [2] Op2 - Computer programs and associated data that may be dynamically written or modified during the device’s execution (e.g., application code, libraries). [5]	[2] ou [5]	[1] ucoSoftware	software is-Part-of system **OK**	system
threat ameaça	Op1 - Um potencial para violação de segurança, que existe quando há uma circunstância, capacidade, ação ou evento que pode violar a segurança e causar danos. [2] Op2 - Definição: Uma circunstância ou evento	Op1 - A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. [2] Op2 - Definition: A circumstance or event that has or indicates the	[2], [3] ou [5]	[1] ucoMeans	malware is-a threat **OK**	attack (risk of) cyber threat

	que tem ou indica o potencial de explorar vulnerabilidades e impactar adversamente (criar consequências adversas para) operações organizacionais, ativos organizacionais (incluindo informações e sistemas de informação), indivíduos, outras organizações ou sociedade. Definição estendida: Inclui um indivíduo ou grupo de indivíduos, entidade como uma organização ou nação), ação ou ocorrência. De: DHS Risk Lexicon, NIPP, CNSSI 4009, NIST SP 800-53 Rev 4 [3] Op3 - Qualquer circunstância ou evento com potencial de impactar adversamente operações organizacionais (incluindo missão, funções, imagem ou reputação), ativos organizacionais ou indivíduos por meio de um sistema de informação via acesso não autorizado,	potential to exploit vulnerabilities and to adversely impact (create adverse consequences for) organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society. Extended Definition: Includes an individual or group of individuals, entity such as an organization or a nation), action, or occurrence. From: DHS Risk Lexicon, NIPP, CNSSI 4009, NIST SP 800-53 Rev 4 [3] Op3 - Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system				

	destruição, divulgação, modificação de informações ou negação de serviço. Além disso, o potencial de uma fonte de ameaça explorar com sucesso uma vulnerabilidade específica do sistema de informação. Fontes: FIPS 200 sob THREAT do CNSSI 4009 - Adaptado; NIST SP 1800-15B sob Threat do FIPS 200 [5]	vulnerability. Sources: FIPS 200 under THREAT from CNSSI 4009 - Adapted; NIST SP 1800-15B under Threat from FIPS 200 [5]				
threat actor ator de ameaça	Op1 - Indivíduo, grupo, organização ou governo que conduz ou tem a intenção de conduzir atividades prejudiciais. [3] Op2 - Indivíduo ou grupo que representa uma ameaça. Fonte: NIST SP 800-150 [5]	Op1 - An individual, group, organization, or government that conducts or has the intent to conduct detrimental activities. [3] Op2 - An individual or a group posing a threat. Source: NIST SP 800-150. [5]	[3] ou [5]	[1] ucoThreatActor	threat_actor threatens organization **OK**	threat agent; attacker; adversary [3]
technology tecnologia	Justificativa: Tecnologia da Informação (HD/SW) usada para atacar ou defender. Op1 - Tecnologia da Informação: Qualquer equipamento ou sistema interconectado ou subsistema de equipamento que processa, transmite, recebe ou troca dados ou informações. Fonte:	Rationale: Information Technology (HD/SW) used to attack or defend. Op1 - Information Technology: Any equipment or interconnected system or subsystem of equipment that processes, transmits, receives, or interchanges data or information. Source: CNSSI 4009, NIST SP 800-53 Rev. 4, based	[3]	[1] ucoProbe; ucoExploit; ucoMeans	attack uses technology **OK** playbook uses technology **OK**	technology, exploit, means, tool (attack and defense)

	CNSSI 4009, NIST SP 800-53 rev. 4, com base em 40 U.S.C. sec. 1401. [3]	on 40 U.S.C. sec. 1401. [3]				
APT - Advanced Persistent Threats	Um adversário com níveis sofisticados de especialização e recursos significativos, permitindo que ele, por meio do uso de vários vetores de ataque diferentes (e.g., cibernético, físico e fraude), gere oportunidades para atingir seus objetivos, que são tipicamente estabelecer e estender pontos de apoio dentro da infraestrutura de tecnologia da informação de organizações para fins de exfiltração contínua de informações ou para minar ou impedir aspectos críticos de uma missão, programa ou organização, ou se colocar em uma posição para fazê-lo no futuro; além disso, a ameaça persistente avançada persegue seus objetivos repetidamente por um longo período de tempo, adaptando-se aos esforços de um defensor	An adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors (e.g., cyber, physical, and deception) to generate opportunities to achieve its objectives, which are typically to establish and extend footholds within the information technology infrastructure of organizations for purposes of continually exfiltrating information and/or to undermine or impede critical aspects of a mission, program, or organization, or place itself in a position to do so in the future; moreover, the advanced persistent threat pursues its objectives repeatedly over an extended period of time, adapting to a defender's efforts to resist it, and with determination to maintain the level of interaction needed to execute its objectives.	[5]		APT is-a threat **OK**	technology

	para resistir a ela e com determinação para manter o nível de interação necessário para executar seus objetivos. Fontes: NIST SP 800-137 do NIST SP 800-39. [5]	Sources: NIST SP 800-137 from NIST SP 800-39. [5]				
vulnerability vulnerabilidade	Uma fraqueza característica ou específica que torna uma organização ou ativo (como uma informação ou um sistema de informação) aberto à exploração por uma determinada ameaça ou suscetível a um determinado perigo. [3]	A characteristic or specific weakness that renders an organization or asset (such as information or an information system) open to exploitation by a given threat or susceptible to a given hazard. [3]	[3]	[1] ucoVulnerability; ucoCWE	malware exploits vulnerability **OK**	weakness, exposure
risk risco	Risco é o produto do nível de ameaça com o nível de vulnerabilidade. Ele estabelece a probabilidade de um ataque ser bem-sucedido. [2]	Risk is the product of the level of threat with the level of vulnerability. It establishes the likelihood of a successful attack. [2]	[2]	[1] ucoIndicator (key risk indicator - KRI) ?	asset has risk **OK**	risk_indicator risk_level
impact impacto	Op1 - O efeito de um evento, incidente ou ocorrência. Em segurança cibernética, o efeito de uma perda de confidencialidade, integridade ou disponibilidade de informações ou de um	Op1 - The effect of an event, incident, or occurrence. In cybersecurity, the effect of a loss of confidentiality, integrity or availability of information or an information system on an organization's operations,	[3] ou [5]	[1] ucohasImpact	incident has impact **OK**	Synonym of consequence [3] damage [5]

	sistema de informações nas operações de uma organização, seus ativos, em indivíduos, outras organizações ou em interesses nacionais. [3] Op2 - Dano causado a algo de forma a reduzir ou destruir seu valor, utilidade ou função normal. [5]	its assets, on individuals, other organizations, or on national interests. [3] Op2 - Harm caused to something in such a way as to reduce or destroy its value, usefulness, or normal function. [5]				
Security Property Propriedade de Segurança	Propriedades de segurança são princípios ou características específicas de segurança de informações ou sistemas. Exemplos de propriedades de segurança: Disponibilidade, Integridade, Confidencialidade, Autenticidade, Rastreabilidade, Privacidade, Auditabilidade, Legalidade, Resiliência e Não retroatividade. Outras propriedades podem ser incluídas, especialmente quando campos de conhecimento específicos são abordados. [10]	Security properties are principles or specific security characteristics of information or systems. Examples of security properties: Availability, Integrity, Confidentiality, Authenticity, Traceability, Privacy, Auditability, Legality, Resilience, and Non-retroactivity. Other properties may be included, especially when specific knowledge fields are addressed. [10]	[10[	[1] ucoConfidenceType	security has security_property **OK** confidentiality is-a security_property **OK** integrity is-a security_property **OK** availability is-a security_property **OK**	features, properties, aspects of security
process	Conjunto de atividades	Set of interrelated or	[5]		playbook is-a	procedure

processo	inter-relacionadas ou interativas que usam entradas para fornecer um resultado pretendido. Fontes: NIST SP 800-160v1r1 da ISO 9000:2015. [5]	interacting activities that use inputs to deliver an intended result. Sources: NIST SP 800-160v1r1 from ISO 9000:2015. [5]			process **OK**	
playbook procedimento de defesa ou restabelecimento	Playbooks são procedimentos operacionais para o planejamento e a condução de atividades de resposta a incidentes e vulnerabilidades de segurança cibernética. [3]	Playbooks are operational procedures for planning and conducting cyber security vulnerability and incident response activities. [3]	[3]	[1] ucoCourseofAction [6] socsCourse_of_action	playbook is-a process **OK**	course of action, runbook
Attack Scenario Cenário de Ataque	Consciência situacional de um ataque. Os playbooks são acionados de acordo com o cenário. Exemplos de cenários a serem abordados: Infecção por worm; Intrusão de SO (Windows, Linux); Negação de serviço distribuída - DDOS; Comportamento de rede malicioso; Desfiguração de site; Detecção de malware do Windows; Chantagem; Malware de smartphone; Engenharia social; Vazamento de informações; Abuso interno; Phishing de	Situational awareness of an attack. Playbooks are triggered according to the scenario. Examples of scenarios to be addressed: Worm Infection; OS (Windows, Linux) Intrusion; Distributed Denial Of Service - DDOS; Malicious Network Behaviour; Website Defacement; Windows Malware Detection; Blackmail; Smartphone Malware; Social Engineering; Information Leakage; Insider Abuse; Customer Phishing; Scam; Trademark infringement; Phishing; Ransomware;	[11]	[1] ucoCampaign; ucoKillChain; ucoKillChainPhase	playbook address attack_scenario **OK**	campaign, killchain / TTP

	cliente; Golpe; Violação de marca registrada; Phishing; Ransomware; Comprometimento em larga escala. [11]	Large scale compromise. [11]				
incident handling steps passos para lidar com incidentes	A mitigação de violações de políticas de segurança e práticas recomendadas. [5] Seis etapas são definidas para lidar com incidentes de segurança: 1. Preparação: prepare-se para lidar com o incidente; 2. Identificação: detecte o incidente; 3. Contenção: limite o impacto do incidente; 4. Remediação: remova a ameaça; 5. Recuperação: recupere para um estágio normal; 6. Lições aprendidas: elabore e melhore o processo. [11]	The mitigation of violations of security policies and recommended practices. [5] Six steps are defined to handle security incidents: 1. Preparation: get ready to handle the incident; 2. Identification: detect the incident; 3. Containment: limit the impact of the incident; 4. Remediation: remove the threat; 5. Recovery: recover to a normal stage; 6. Lessons learned: draw up and improve the process. [11]	[5] and [11]	[1] ucoCourseofAction [6] socsCourse_of_action	playbook has incident_handling_steps **OK**	course of action
countermeasure	Op1 - Métodos reativos usados para evitar que uma exploração ocorra com sucesso uma vez que uma ameaça tenha sido detectada. Os Sistemas de Prevenção de Intrusão (IPS) geralmente empregam contramedidas para	Op1 - Reactive methods used to prevent an exploit from successfully occurring once a threat has been detected. Intrusion Prevention Systems (IPS) commonly employ countermeasures to prevent intruders from gaining further access to a	[2] and [5]		countermeasure meets security_property **OK**	Synonymous: security control, safeguard [5]

	evitar que intrusos obtenham mais acesso a uma rede de computadores. Outras contramedidas são patches, listas de controle de acesso e filtros de malware. [2] Op2 - Medidas de proteção prescritas para atender aos objetivos de segurança (ou seja, confidencialidade, integridade e disponibilidade) especificados para um sistema de informação. As salvaguardas podem incluir recursos de segurança, controles de gerenciamento, segurança de pessoal e segurança de estruturas físicas, áreas e dispositivos. Sinônimo de controles de segurança e contramedidas. Fontes: NIST SP 800-128 sob salvaguardas do CNSSI 4009-2015 - Adaptado [5]	computer network. Other counter measures are patches, access control lists and malware filters. [2] Op2 - Protective measures prescribed to meet the security objectives (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management controls, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures. Sources: NIST SP 800-128 under safeguards from CNSSI 4009-2015 - Adapted [5]				
Tactic	A tática representa um objetivo estratégico do adversário em um determinado momento.	The tactic represents an adversary's strategic objective at a given moment.	[1, 7]			

Technique	A técnica descreve como um adversário atinge um objetivo tático.	It describes how an adversary achieves a tactical objective.	[1, 7]			
Mitigation	É um curso de ação. Refere-se a uma medida ou estratégia de segurança projetada para prevenir ou reduzir o sucesso de técnicas ou subtécnicas adversas. Mitigações representam conceitos, configurações ou tecnologias que as organizações podem implementar para proteger seus sistemas e dados de ameaças específicas.	It is a course of action. It refers to a security measure or strategy designed to prevent or reduce the success of adversarial techniques or sub-techniques. Mitigations represent concepts, configurations, or technologies that organizations can implement to protect their systems and data from specific threats.	[1, 7]			
A seguir são apresentadas sugestões de instâncias para táticas e técnicas						
Initial Access Tactic	Obter entrada inicial em um sistema ou rede alvo.		[1, 7]	Exploit Public-Facing Application (T1190), Valid Accounts (T1078), Phishing (T1566), Drive-by Compromise (T1189), Exploit SS7 (T1458), External Remote Services (T1133), Hardware Additions (T1200),		

				Replication Through Removable Media (T1091), Supply Chain Compromise (T1195), Taint Shared Content (T1556), Trusted Relationship (T1199), Cloud Account (T1078.004)		
Execution Tactic	Executar código ou comandos maliciosos em um sistema comprometido.		[1, 7]	Process Injection (T1055), Exploitation for Client Execution (T1203), User Execution (T1204), Command and Scripting Interpreter (T1059), Build Image on Host (T1610), Container Administration Command (T1609), Deploy Container (T1611), Execution through API (T1106), Inter-Process Communication (T1559), Shared Modules (T1129), Windows Management		

				Instrumentation (T1047), XSL Script Processing (T1220)		
Persistence Tactic	Manter acesso contínuo ao sistema após a entrada inicial.		[1, 7]	Rootkit (T1014), Scheduled Task/Job (T1053), Boot or Logon Autostart Execution (T1547), Account Manipulation (T1098), BITS Jobs (T1197), Browser Extensions (T1176), Compromise Client Software Binary (T1554), Create Account (T1136), Create or Modify System Process (T1543), Event Triggered Execution (T1546), File and Directory Permissions Modification (T1222), Hijack Execution Flow (T1574), Modify Cloud Compute Infrastructure (T1578), Modify Registry (T1112),		

				Modify System Image (T1601), Office Application Startup (T1137), Path Interception (T1574.001), Pre-OS Boot (T1542), Redundant Access (T1212), Server Software Component (T1505), Systemd Timers (T1053.006), Time Providers (T1546.015), Windows Service (T1543.003)		
Privilege Escalation Tactic	Ganhar níveis mais altos de permissão em um sistema ou rede.		[1, 7]	Exploitation for Privilege Escalation (T1068), Abuse Elevation Control Mechanism (T1548), Access Token Manipulation (T1134), Device Administrator Abuse (T1626), Escape to Host (T1612), Group Policy Modification (T1484)		
Defense Evasion	Evitar detecção ou		[1, 7]	Rootkit (T1014),		

Tactic	bloqueio por mecanismos de segurança.			Process Injection (T1055), Obfuscated Files or Information (T1027), Component Object Model Hijacking (T1546.015), Deobfuscate/Decode Files or Information (T1140), Domain Policy Modification (T1484), Execution Guardrails (T1480), Exploitation for Defense Evasion (T1211), Exploitation for Evasion (T1211), Hide Artifacts (T1564), Impair Defenses (T1562), Indirect Command Execution (T1202), Install Root Certificate (T1553), Masquerading (T1036), Modify Authentication Process (T1556), Process Doppelgänging (T1055.012), Process Hollowing		

				(T1055.013), Reflective Code Loading (T1620), Subvert Trust Controls (T1553), System Binary Proxy Execution (T1218), Unused/Unsupported Cloud Regions (T1535), Virtualization/Sandbox Evasion (T1497)		
Credential Access Tactic	Obter credenciais (ex.: senhas, tokens) para acessar sistemas ou recursos.		[1, 7]	Brute Force (T1110), Credential Dumping (T1003), Credentials from Password Stores (T1555), Browser Session Hijacking (T1185), Forced Authentication (T1187), GUI Input Capture (T1056), Input Capture (T1056), Kerberoasting (T1558), Keychain (T1555.001), LSASS Memory (T1003.001), Man-in-the-Middle (T1557),		

				Multi-Factor Authentication Interception (T1111), Network Sniffing (T1040), NTDS (T1003.003), OS Credential Dumping (T1003), Steal Application Access Token (T1528), Steal or Forge Kerberos Tickets (T1558), Steal Web Session Cookie (T1539), Unsecured Credentials (T1552), Web Session Cookie (T1539)		
Discovery Tactic	Explorar informações sobre o sistema ou rede alvo para planejar próximos passos.		[1, 7]	Remote System Discovery (T1018), Network Service Scanning (T1046), Account Discovery (T1087), Application Window Discovery (T1010), Browser Bookmark Discovery (T1217), Cloud Infrastructure Discovery (T1526), Cloud Service		

				Discovery (T1526), Container and Resource Discovery (T1613), Domain Trust Discovery (T1482), File and Directory Discovery (T1083), Network Service Discovery (T1046), Password Policy Discovery (T1201), Peripheral Device Discovery (T1120), Permission Groups Discovery (T1069), Process Discovery (T1057), Software Discovery (T1518), System Information Discovery (T1082), System Location Discovery (T1614), System Network Configuration Discovery (T1016), System Network Connections Discovery (T1049), System Owner/User Discovery (T1033), System Service		

				Discovery (T1007), System Time Discovery (T1124), User Activity Based on Authentication Logs (T1530)		
Lateral Movement Tactic	Mover-se entre sistemas dentro de uma rede comprometida.		[1, 7]	Remote Services (T1021), Use Alternate Authentication Material (T1550), Internal Spearphishing (T1534), Network Boundary Bridging (T1599), Network Device Authentication (T1556), Rogue Domain Controller (T1207), Software Deployment Tools (T1072), Valid Accounts (T1078)		
Collection Tactic	Reunir dados de interesse (ex.: arquivos, credenciais) no sistema alvo.		[1, 7]	Data from Local System (T1005), Data Staged (T1074), Automated Collection (T1119), Adversary-in-the-		

				Middle (T1557), Audio Capture (T1123), Clipboard Data (T1115), Cloud Service Dashboard (T1538), Data from Cloud Storage (T1530), Data from Configuration Repository (T1602), Data from Information Repositories (T1213), Data from Network Shared Drive (T1039), Data from Removable Media (T1025), Direct Volume Access (T1006), Email Collection (T1114), Screen Capture (T1113)		
Exfiltration Tactic	Transferir dados roubados para fora da rede comprometida.		[1, 7]	Exfiltration Over C2 Channel (T1041), Exfiltration Over Web Service (T1567), Automated Exfiltration (T1020), Data Obfuscation (T1001), Exfiltration		

				Over Alternative Protocol (T1048), Exfiltration Over Other Network Medium (T1011), Exfiltration Over Physical Medium (T1052), Exfiltration Over Symmetric Encrypted Channel (T1048), Transfer Data to Cloud Account (T1537)		
Command and Control Tactic	Estabelecer e manter comunicação com sistemas comprometidos para controle remoto.		[1, 7]	Application Layer Protocol (T1071), Non-Application Layer Protocol (T1095), Protocol Tunneling (T1572), Communication Through Removable Media (T1092), Data Encoding (T1132), Domain Generation Algorithms (T1568), Dynamic Resolution (T1568), Fallback Channels (T1008), Ingress Tool Transfer (T1105), Proxy (T1090), Remote		

				Access Software (T1219), Traffic Signaling (T1205), Web Service (T1102)		
Impact Tactic	Causar danos, interrupções ou alterações no sistema ou dados para atingir objetivos finais.		[1, 7]	Network Denial of Service (T1498), Data Encrypted for Impact (T1486), Data Destruction (T1485), Account Access Removal (T1531), Data Manipulation (T1565), Defacement (T1491), Disk Content Wipe (T1561), Disk Wipe (T1561), Endpoint Denial of Service (T1499), Inhibit System Recovery (T1490), Resource Hijacking (T1496), Service Stop (T1489), System Shutdown/Reboot (T1529)		
Resource Development Tactic	Criar, adquirir ou configurar recursos (ex.: ferramentas, infraestrutura) para o		[1, 7]	Acquire Infrastructure (T1583), Compromise		

	ataque.			Infrastructure (T1584), Compromise Accounts (T1586), Impersonation (T1656), Obtain Capabilities (T1588), Stage Capabilities (T1608)		
Reconnaissance Tactic	Coletar informações sobre o alvo antes do ataque (ex.: redes, sistemas, pessoas).		[1, 7]	Active Scanning (T1595), Gather Victim Host Information (T1592), Gather Victim Identity Information (T1589), Gather Victim Network Information (T1590), Gather Victim Org Information (T1591), Phishing for Information (T1598), Search Closed Sources (T1597), Search Open Technical Databases (T1596), Search Victim-Owned Websites (T1594), Weakness Identification (T1600)		

Exploit Public-Facing Application Technique	Exploração de vulnerabilidades em aplicações voltadas ao público (ex.: sites, APIs) para acesso inicial.		[7]	Initial Access (TA0001)		
Valid Accounts Technique	Uso de contas legítimas obtidas por credenciais roubadas ou erros de configuração para entrar em sistemas.		[7]	Initial Access (TA0001)		
Spearphishing Attachment Technique	Envio de e-mails direcionados com anexos maliciosos para enganar vítimas e obter acesso inicial.		[7]	Initial Access (TA0001)		
Process Injection Technique	Injeção de código malicioso em processos legítimos para executar ações sem criar novos arquivos detectáveis.		[7]	Execution (TA0002) / Defense Evasion (TA0005)		
Exploitation for Client Execution Technique	Exploração de software cliente (ex.: via código malicioso) para executar ações no sistema do usuário.		[7]	Execution (TA0002)		
User Execution Technique	Dependência da interação do usuário para executar código		[7]	Execution (TA0002)		Backdoor

	malicioso, como abrir anexos de trojans.					
Rootkit Technique	Uso de software malicioso que se esconde no sistema operacional para ocultar atividades e manter acesso.		[7]	Persistence (TA0003) / Defense Evasion (TA0005)		
Scheduled Task/Job Technique	Criação ou manipulação de tarefas agendadas para executar código malicioso em intervalos específicos.		[7]	Persistence (TA0003)		
Boot or Logon Autostart Execution Technique	Configuração de código malicioso para iniciar automaticamente ao ligar o sistema ou fazer login.		[7]	Persistence (TA0003)		
Exploitation for Privilege Escalation Technique	Exploração de vulnerabilidades (ex.: buffer overflow) para ganhar privilégios mais altos no sistema.		[7]	Privilege Escalation (TA0004)		
Abuse Elevation Control Mechanism Technique	Abuso de mecanismos de controle de elevação (ex.: UAC bypass) para obter privilégios elevados.		[7]	Privilege Escalation (TA0004)		
Obfuscated Files	Ocultação de arquivos ou		[7]	Defense Evasion		

or Information Technique	dados maliciosos (ex.: ofuscação de código) para evitar detecção por antivírus.			(TA0005)		
Brute Force Technique	Tentativas repetidas de adivinhar credenciais para acessar sistemas ou contas.		[7]	Credential Access (TA0006)		
Credential Dumping Technique	Extração de credenciais armazenadas em sistemas (ex.: memória ou arquivos) para uso em ataques futuros.		[7]	Credential Access (TA0006)		
Credentials from Password Stores Technique	Obtenção de credenciais de locais de armazenamento (ex.: navegadores, gerenciadores de senhas).		[7]	Credential Access (TA0006)		
Remote System Discovery Technique	Identificação de sistemas ativos em uma rede, usando ferramentas como pings para mapeamento.		[7]	Discovery (TA0007)		
Network Service Scanning Technique	Varredura de portas e serviços em uma rede (ex.: SYN scan) para encontrar pontos de		[7]	Discovery (TA0007)		

	entrada.					
Account Discovery Technique	Tentativa de identificar contas válidas em um sistema (ex.: enumeração de usuários) para ataques futuros.		[7]	Discovery (TA0007)		
Remote Services Technique	Uso de serviços remotos (ex.: RDP, SSH) para se mover entre sistemas em uma rede comprometida.		[7]	Lateral Movement (TA0008)		
Use Alternate Authentication Material Technique	Uso de materiais alternativos de autenticação (ex.: certificados, tokens) para acessar outros sistemas.		[7]	Lateral Movement (TA0008)		
Data from Local System Technique	Coleta de dados sensíveis diretamente de sistemas locais comprometidos (ex.: arquivos, logs).		[7]	Collection (TA0009)		
Data Staged Technique	Organização de dados coletados em locais temporários antes da exfiltração.		[7]	Collection (TA0009)		
Automated Collection Technique	Uso de scripts ou ferramentas automatizadas para coletar dados em massa		[7]	Collection (TA0009)		

	de sistemas comprometidos.					
Exfiltration Over C2 Channel Technique	Transferência de dados roubados por meio de canais de comando e controle já estabelecidos.		[7]	Exfiltration (TA0010)		
Exfiltration Over Web Service Technique	Uso de serviços web (ex.: Dropbox, Google Drive) para transferir dados roubados para fora da rede.		[7]	Exfiltration (TA0010)		
Application Layer Protocol Technique	Uso de protocolos de camada de aplicação (ex.: HTTP) para comunicação de comando e controle (C2).		[7]	Command and Control (TA0011)		
Non-Application Layer Protocol Technique	Uso de protocolos como ICMP para comunicação furtiva entre sistemas comprometidos.		[7]	Command and Control (TA0011)		
Protocol Tunneling Technique	Encapsulamento de dados maliciosos em protocolos (ex.: flags IP) para comunicação oculta.		[7]	Command and Control (TA0011)		
Network Denial of Service Technique	Ataques como Syn Flood para interromper serviços de rede e afetar disponibilidade.		[7]	Impact (TA0040)		

Data Encrypted for Impact Technique	Criptografia de dados por ransomware para extorquir vítimas, tornando informações inacessíveis.		[7]	Impact (TA0040)		
Data Destruction Technique	Destruição intencional de dados para causar interrupção ou prejuízo ao alvo.		[7]	Impact (TA0040)		
Acquire Infrastructure Technique	Aquisição de infraestrutura (ex.: servidores, domínios) para preparar um ataque.		[7]	Resource Development (TA0042)		
Stage Capabilities Technique	Configuração de capacidades maliciosas (ex.: payloads, exploits) antes do ataque.		[7]	Resource Development (TA0042)		
Compromise Accounts Technique	Comprometimento de contas (ex.: e-mails, redes sociais) para uso em ataques futuros.		[7]	Resource Development (TA0042)		
Gather Victim Host Information Technique	Coleta de informações sobre sistemas do alvo (ex.: hardware, software) antes do ataque.		[7]	Reconnaissance (TA0043)		
Phishing for Information Technique	Uso de phishing para coletar informações sensíveis (ex.:		[7]	Reconnaissance (TA0043)		

	credenciais) antes do ataque principal.					
Gather Victim Org Information Technique	Coleta de dados sobre a organização alvo (ex.: estrutura, funcionários) para planejar ataques.		[7]	Reconnaissance (TA0043)		
Boot or Logon Autostart Execution Technique	Configuração de código malicioso para iniciar automaticamente ao ligar o sistema ou fazer login.		[7]	Persistence (TA0003)		
Access Token Manipulation Technique	Manipulação de tokens de acesso para escalar privilégios ou se passar por outros usuários.		[7]	Privilege Escalation (TA0004)		
Account Access Removal Technique	Remoção ou desativação de contas para interromper acesso legítimo ao sistema.		[7]	Impact (TA0040)		
Account Manipulation Technique	Alteração de contas (ex.: permissões, senhas) para manter acesso ou facilitar ataques.		[7]	Persistence (TA0003)		
Active Scanning Technique	Varredura ativa de redes ou sistemas para coletar informações antes do ataque.		[7]	Reconnaissance (TA0043)		
Adversary-in-the-	Interceptação de		[7]	Collection (TA0009)		

Middle Technique	comunicações entre sistemas ou usuários para roubar dados ou credenciais.					
Audio Capture Technique	Captura de áudio de dispositivos (ex.: microfones) para coletar informações sensíveis.		[7]	Collection (TA0009)		
Automated Exfiltration Technique	Uso de ferramentas automatizadas para transferir dados roubados para fora da rede.		[7]	Exfiltration (TA0010)		
BITS Jobs Technique	Uso do Background Intelligent Transfer Service (BITS) para executar ou baixar código malicioso.		[7]	Persistence (TA0003)		
Bootkit Technique	Instalação de malware no processo de inicialização do sistema para persistência em nível baixo.		[7]	Persistence (TA0003)		
Browser Bookmark Discovery Technique	Identificação de favoritos do navegador para coletar informações sobre o alvo.		[7]	Discovery (TA0007)		
Browser Extensions	Instalação ou manipulação de		[7]	Persistence (TA0003)		

Technique	extensões de navegador para executar código ou roubar dados.					
Browser Session Hijacking Technique	Sequestro de sessões de navegador para acessar sistemas ou dados autenticados.		[7]	Credential Access (TA0006)		
Build Image on Host Technique	Criação de imagens de sistema ou contêineres maliciosos diretamente no host comprometido.		[7]	Execution (TA0002)		
Cloud Account Technique	Comprometimento ou uso de contas de serviços em nuvem para acessar recursos.		[7]	Initial Access (TA0001)		
Cloud Infrastructure Discovery Technique	Exploração de informações sobre infraestrutura de nuvem do alvo (ex.: serviços, regiões).		[7]	Discovery (TA0007)		
Cloud Service Dashboard Technique	Acesso a painéis de serviços em nuvem para coletar dados ou controlar recursos.		[7]	Collection (TA0009)		
Cloud Service Discovery Technique	Identificação de serviços em nuvem usados pelo alvo para planejar ataques.		[7]	Discovery (TA0007)		

Command and Scripting Interpreter Technique	Uso de interpretadores (ex.: PowerShell, Bash) para executar comandos maliciosos.		[7]	Execution (TA0002)		
Component Firmware Technique	Modificação de firmware de hardware para persistência ou controle de baixo nível.		[7]	Persistence (TA0003)		
Component Object Model Hijacking Technique	Sequestro de objetos COM no Windows para executar código ou evitar detecção.		[7]	Defense Evasion (TA0005)		
Compromise Client Software Binary Technique	Alteração de binários de software cliente legítimo para incluir código malicioso.		[7]	Persistence (TA0003)		
Compromise Infrastructure Technique	Controle de infraestrutura legítima (ex.: servidores) para usá-la em ataques.		[7]	Resource Development (TA0042)		
Container Administration Command Technique	Execução de comandos administrativos em contêineres para comprometer sistemas em nuvem.		[7]	Execution (TA0002)		
Container and Resource Discovery Technique	Identificação de contêineres e recursos (ex.: Docker, Kubernetes) em um ambiente		[7]	Discovery (TA0007)		

	comprometido.					
Create Account Technique	Criação de novas contas no sistema alvo para acesso persistente ou lateral.		[7]	Persistence (TA0003)		
Create or Modify System Process Technique	Criação ou alteração de processos do sistema para executar código ou manter acesso.		[7]	Persistence (TA0003)		
Data Encoding Technique	Codificação de dados para ocultar comunicações ou payloads maliciosos.		[7]	Command and Control (TA0011)		
Data from Cloud Storage Technique	Coleta de dados armazenados em serviços de nuvem comprometidos (ex.: S3, Google Drive).		[7]	Collection (TA0009)		
Data from Configuration Repository Technique	Roubo de dados de repositórios de configuração (ex.: Git, LDAP) para obter informações sensíveis.		[7]	Collection (TA0009)		
Data from Information Repositories Technique	Coleta de dados de repositórios internos (ex.: SharePoint, Confluence) para разведка ou exfiltração.		[7]	Collection (TA0009)		

Data from Network Shared Drive Technique	Acesso a dados em unidades de rede compartilhadas para coleta ou exfiltração.		[7]	Collection (TA0009)		
Data from Removable Media Technique	Roubo de dados de mídias removíveis (ex.: USB) conectadas ao sistema comprometido.		[7]	Collection (TA0009)		
Data Manipulation Technique	Alteração de dados para enganar usuários ou sistemas, afetando integridade ou confiabilidade.		[7]	Impact (TA0040)		
Data Obfuscation Technique	Ofuscação de dados para dificultar análise ou detecção durante exfiltração ou comunicação.		[7]	Exfiltration (TA0010)		
Data Staged Technique	Organização de dados coletados em locais temporários antes da exfiltração.		[7]	Collection (TA0009)		
Deobfuscate/Decode Files or Information Technique	Desofuscação ou decodificação de arquivos ou dados para evitar análise ou detecção.		[7]	Defense Evasion (TA0005)		
Deploy Container	Implantação de		[7]	Execution (TA0002)		

Technique	contêineres maliciosos em um ambiente para executar código ou persistir.					
Device Administrator Abuse Technique	Abuso de permissões de administrador em dispositivos (ex.: mobile) para controle ou persistência.		[7]	Privilege Escalation (TA0004)		
Direct Volume Access Technique	Acesso direto a volumes de armazenamento para coletar dados ou injetar código.		[7]	Collection (TA0009)		
Disk Wipe Technique	Apagamento de discos ou partições para destruir dados e causar interrupção.		[7]	Impact (TA0040)		
Domain Policy Modification Technique	Alteração de políticas de domínio (ex.: GPOs) para facilitar acesso ou persistência.		[7]	Defense Evasion (TA0005)		
Domain Trust Discovery Technique	Identificação de relações de confiança entre domínios para planejar movimento lateral.		[7]	Discovery (TA0007)		
Drive-by Compromise Technique	Comprometimento de sistemas via sites maliciosos acessados		[7]	Initial Access (TA0001)		

	sem interação direta do usuário.					
Dynamic Resolution Technique	Uso de resolução dinâmica (ex.: DNS dinâmico) para comunicação de comando e controle.		[7]	Command and Control (TA0011)		
Email Collection Technique	Coleta de e-mails de caixas de entrada ou servidores comprometidos para obter informações.		[7]	Collection (TA0009)		
Endpoint Denial of Service Technique	Ataques de negação de serviço direcionados a endpoints específicos para interromper operações.		[7]	Impact (TA0040)		
Escape to Host Technique	Escape de um ambiente virtualizado ou contêiner para comprometer o host subjacente.		[7]	Privilege Escalation (TA0004)		
Event Triggered Execution Technique	Execução de código malicioso disparada por eventos específicos do sistema (ex.: login, inicialização).		[7]	Persistence (TA0003)		
Execution Guardrails	Restrição da execução de código malicioso a		[7]	Defense Evasion (TA0005)		

Technique	condições específicas para evitar detecção.					
Exfiltration Over Alternative Protocol Technique	Transferência de dados roubados usando protocolos alternativos (ex.: FTP, SMTP).		[7]	Exfiltration (TA0010)		
Exfiltration Over Other Network Medium Technique	Uso de redes não padrão (ex.: Bluetooth) para exfiltrar dados.		[7]	Exfiltration (TA0010)		
Exfiltration Over Physical Medium Technique	Transferência de dados roubados via mídia física (ex.: USB, disco externo).		[7]	Exfiltration (TA0010)		
Exploit SS7 Technique	Exploração do protocolo SS7 em redes de telecomunicações para interceptar comunicações ou dados.		[7]	Initial Access (TA0001)		
External Remote Services Technique	Uso de serviços remotos externos (ex.: VPN) para acessar redes internas comprometidas.		[7]	Initial Access (TA0001)		
Fallback Channels Technique	Uso de canais de backup para comando e controle caso o principal seja bloqueado.		[7]	Command and Control (TA0011)		
File and Directory	Exploração de arquivos e		[7]	Discovery (TA0007)		

Discovery Technique	diretórios no sistema alvo para identificar dados de interesse.					
File and Directory Permissions Modification Technique	Alteração de permissões de arquivos ou diretórios para facilitar acesso ou execução.		[7]	Persistence (TA0003)		
Forced Authentication Technique	Forçar autenticação em sistemas para capturar credenciais ou hashes (ex.: SMB relay).		[7]	Credential Access (TA0006)		
Gather Victim Identity Information Technique	Coleta de informações sobre identidades do alvo (ex.: nomes, e-mails) antes do ataque.		[7]	Reconnaissance (TA0043)		
Gather Victim Network Information Technique	Obtenção de dados sobre a rede do alvo (ex.: topologia, IPs) para planejamento.		[7]	Reconnaissance (TA0043)		
Group Policy Modification Technique	Modificação de políticas de grupo para alterar configurações ou executar código no domínio.		[7]	Privilege Escalation (TA0004)		
Hardware Additions Technique	Adição de hardware malicioso (ex.: dispositivos USB) para comprometer sistemas.		[7]	Initial Access (TA0001)		

Hide Artifacts Technique	Ocultação de artefatos (ex.: logs, arquivos) para evitar detecção por ferramentas de segurança.		[7]	Defense Evasion (TA0005)		
Hijack Execution Flow Technique	Sequestro do fluxo de execução de programas legítimos para rodar código malicioso.		[7]	Persistence (TA0003)		
Impair Defenses Technique	Desativação ou comprometimento de mecanismos de defesa (ex.: antivírus, firewalls).		[7]	Defense Evasion (TA0005)		
Impersonation Technique	Imitação de usuários ou entidades legítimas para enganar alvos ou sistemas.		[7]	Resource Development (TA0042)		
Indicator Removal Technique	Remoção de indicadores de comprometimento (ex.: logs, arquivos temporários) para evitar rastreamento.		[7]	Defense Evasion (TA0005)		
Inhibit System Recovery Technique	Prevenção da recuperação do sistema (ex.: desativação de backups) para maximizar impacto.		[7]	Impact (TA0040)		
Input Capture	Captura de entradas do		[7]	Credential Access		

Technique	usuário (ex.: keystrokes, senhas) para roubar credenciais ou dados.			(TA0006)		
Install Root Certificate Technique	Instalação de certificados raiz falsos para facilitar ataques de interceptação ou validação falsa.		[7]	Defense Evasion (TA0005)		
Inter-Process Communication Technique	Uso de mecanismos de comunicação entre processos (ex.: pipes) para executar código ou coletar dados.		[7]	Execution (TA0002)		
Internal Spearphishing Technique	Phishing direcionado dentro da organização usando contas comprometidas para atingir outros usuários.		[7]	Lateral Movement (TA0008)		
Kerberoasting Technique	Exploração de tíquetes Kerberos para extrair hashes de senhas de contas de serviço.		[7]	Credential Access (TA0006)		
Keychain Technique	Roubo de credenciais armazenadas em keychains (ex.: macOS) para acesso a sistemas ou serviços.		[7]	Credential Access (TA0006)		
LSASS Memory Technique	Acesso à memória do LSASS no Windows para		[7]	Credential Access (TA0006)		

	extrair credenciais ou hashes.					
Man-in-the-Middle Technique	Interceptação de comunicações para roubar dados ou injetar conteúdo malicioso.		[7]	Credential Access (TA0006)		
Masquerading Technique	Disfarce de arquivos ou processos maliciosos como legítimos para evitar detecção.		[7]	Defense Evasion (TA0005)		
Modify Authentication Process Technique	Alteração de processos de autenticação (ex.: MFA) para facilitar acesso ou persistência.		[7]	Defense Evasion (TA0005)		
Modify Cloud Compute Infrastructure Technique	Modificação de infraestrutura de computação em nuvem (ex.: VMs) para executar código ou persistir.		[7]	Persistence (TA0003)		
Modify Registry Technique	Alteração do registro do sistema (ex.: Windows Registry) para persistência ou evasão.		[7]	Persistence (TA0003)		
Modify System Image Technique	Alteração de imagens de sistema (ex.: firmware, OS) para incluir código malicioso.		[7]	Persistence (TA0003)		

Network Boundary Bridging Technique	Conexão de redes separadas (ex.: bypass de firewalls) para facilitar acesso ou movimento lateral.		[7]	Lateral Movement (TA0008)		
Network Device Authentication Technique	Uso de credenciais roubadas para autenticar em dispositivos de rede (ex.: roteadores).		[7]	Lateral Movement (TA0008)		
Network Sniffing Technique	Captura de tráfego de rede para coletar credenciais ou informações sensíveis.		[7]	Credential Access (TA0006)		
OS Credential Dumping Technique	Extração de credenciais diretamente do sistema operacional (ex.: SAM no Windows).		[7]	Credential Access (TA0006)		
Obtain Capabilities Technique	Obtenção de capacidades ou exploits para uso em ataques futuros.		[7]	Resource Development (TA0042)		
Office Application Startup Technique	Uso de inicialização de aplicativos Office (ex.: macros) para persistência ou execução.		[7]	Persistence (TA0003)		
Password Policy Discovery Technique	Identificação de políticas de senha (ex.: complexidade, expiração)		[7]	Discovery (TA0007)		

	para planejar ataques.					
Path Interception Technique	Modificação de caminhos de execução (ex.: PATH no Linux) para executar código malicioso.		[7]	Persistence (TA0003)		
Peripheral Device Discovery Technique	Identificação de dispositivos periféricos conectados (ex.: USB) para coleta ou exploração.		[7]	Discovery (TA0007)		
Permission Groups Discovery Technique	Exploração de grupos de permissões (ex.: Active Directory) para identificar alvos ou escalar acesso.		[7]	Discovery (TA0007)		
Phishing Technique	Uso de mensagens falsas (ex.: e-mail, SMS) para enganar usuários e obter acesso ou informações.		[7]	Initial Access (TA0001)		
Phishing for Information Technique	Phishing direcionado para coletar informações sensíveis antes do ataque principal.		[7]	Reconnaissance (TA0043)		
Pre-OS Boot Technique	Comprometimento do processo de inicialização antes do sistema operacional carregar (ex.: BIOS).		[7]	Persistence (TA0003)		

Process Discovery Technique	Identificação de processos em execução no sistema para planejar ataques ou evasão.		[7]	Discovery (TA0007)		
Process Hollowing Technique	Substituição do conteúdo de um processo legítimo por código malicioso para execução furtiva.		[7]	Defense Evasion (TA0005)		
Proxy Technique	Uso de proxies para ocultar comunicações de comando e controle ou exfiltração.		[7]	Command and Control (TA0011)		
Redundant Access Technique	Criação de métodos de acesso reserva (ex.: backdoors) para garantir persistência.		[7]	Persistence (TA0003)		
Reflective Code Loading Technique	Carregamento de código malicioso diretamente na memória para evitar escrita em disco.		[7]	Defense Evasion (TA0005)		
Remote Access Software Technique	Uso de software de acesso remoto legítimo (ex.: TeamViewer) para controlar sistemas comprometidos.		[7]	Command and Control (TA0011)		
Remote System Discovery Technique	Identificação de sistemas remotos em uma rede para planejar movimento		[7]	Discovery (TA0007)		

	lateral ou ataques.					
Replication Through Removable Media Technique	Propagação de malware por meio de mídias removíveis (ex.: USB) para infectar outros sistemas.		[7]	Initial Access (TA0001)		
Resource Hijacking Technique	Uso de recursos do sistema (ex.: CPU para mineração de criptomoedas) para benefício do atacante.		[7]	Impact (TA0040)		
Rogue Domain Controller Technique	Configuração de um controlador de domínio falso para interceptar autenticações ou dados.		[7]	Lateral Movement (TA0008)		
Search Closed Sources Technique	Pesquisa em fontes fechadas (ex.: dark web) para obter informações sobre o alvo.		[7]	Reconnaissance (TA0043)		
Search Open Technical Databases Technique	Uso de bases técnicas públicas (ex.: Shodan) para coletar informações sobre alvos.		[7]	Reconnaissance (TA0043)		
Search Victim-Owned Websites Technique	Exploração de sites pertencentes ao alvo para coletar dados ou identificar vulnerabilidades.		[7]	Reconnaissance (TA0043)		

Server Software Component Technique	Exploração ou modificação de componentes de software de servidor (ex.: SQL Server) para acesso.		[7]	Persistence (TA0003)		
Service Stop Technique	Parada de serviços críticos no sistema para facilitar ataques ou causar interrupção.		[7]	Impact (TA0040)		
Shared Modules Technique	Uso de módulos compartilhados (ex.: DLLs) para executar código malicioso.		[7]	Execution (TA0002)		
Software Deployment Tools Technique	Abuso de ferramentas de implantação (ex.: SCCM) para distribuir malware ou executar comandos.		[7]	Lateral Movement (TA0008)		
Software Discovery Technique	Identificação de softwares instalados no sistema alvo para planejar explorações específicas.		[7]	Discovery (TA0007)		
Steal Application Access Token Technique	Roubo de tokens de acesso de aplicações para autenticação em serviços comprometidos.		[7]	Credential Access (TA0006)		
Steal or Forge Kerberos Tickets	Roubo ou falsificação de tíquetes Kerberos para		[7]	Credential Access (TA0006)		

Technique	acessar sistemas ou recursos em um domínio.					
Steal Web Session Cookie Technique	Roubo de cookies de sessão web para acessar sistemas ou serviços autenticados.		[7]	Credential Access (TA0006)		
Subvert Trust Controls Technique	Subversão de controles de confiança (ex.: assinatura de código) para executar código malicioso.		[7]	Defense Evasion (TA0005)		
Supply Chain Compromise Technique	Comprometimento da cadeia de suprimentos (ex.: software de terceiros) para atingir alvos.		[7]	Initial Access (TA0001)		
System Binary Proxy Execution Technique	Uso de binários do sistema (ex.: rundll32) para executar código malicioso de forma indireta.		[7]	Defense Evasion (TA0005)		
System Information Discovery Technique	Coleta de informações sobre o sistema (ex.: OS, versão) para planejar ataques.		[7]	Discovery (TA0007)		
System Location Discovery Technique	Identificação da localização geográfica do sistema para ajustar		[7]	Discovery (TA0007)		

	ataques ou evitar detecção.					
System Network Configuration Discovery Technique	Exploração da configuração de rede do sistema (ex.: IPs, proxies) para planejamento.		[7]	Discovery (TA0007)		
System Network Connections Discovery Technique	Identificação de conexões de rede ativas no sistema para mapeamento ou exploração.		[7]	Discovery (TA0007)		
System Owner/User Discovery Technique	Descoberta de proprietários ou usuários do sistema para direcionar ataques ou phishing.		[7]	Discovery (TA0007)		
System Service Discovery Technique	Identificação de serviços em execução no sistema para exploração ou interrupção.		[7]	Discovery (TA0007)		
System Shutdown/Reboot Technique	Desligamento ou reinicialização forçada do sistema para causar interrupção ou evitar detecção.		[7]	Impact (TA0040)		
System Time Discovery Technique	Obtenção da hora do sistema para sincronizar ataques ou explorar		[7]	Discovery (TA0007)		

	dependências temporais.					
Taint Shared Content Technique	Contaminação de conteúdo compartilhado (ex.: repositórios) para distribuir malware ou enganar usuários.		[7]	Initial Access (TA0001)		
Traffic Signaling Technique	Uso de sinais de tráfego (ex.: pacotes específicos) para ativar ou controlar malware.		[7]	Command and Control (TA0011)		
Transfer Data to Cloud Account Technique	Transferência de dados roubados para contas de nuvem controladas pelo atacante.		[7]	Exfiltration (TA0010)		
Trusted Relationship Technique	Exploração de relações de confiança (ex.: parceiros, fornecedores) para acessar redes internas.		[7]	Initial Access (TA0001)		
Unsecured Credentials Technique	Uso de credenciais expostas ou mal protegidas para acessar sistemas ou serviços.		[7]	Credential Access (TA0006)		
Unused/Unsupported Cloud Regions Technique	Uso de regiões de nuvem não utilizadas ou sem suporte para ocultar atividades ou infraestrutura.		[7]	Defense Evasion (TA0005)		

User Activity Based on Authentication Logs Technique	Análise de logs de autenticação para identificar padrões de uso ou alvos para ataques.		[7]	Discovery (TA0007)		
Valid Accounts Technique	Uso de contas válidas obtidas para acessar sistemas ou redes de forma legítima.		[7]	Lateral Movement (TA0008)		
Virtualization/Sandbox Evasion Technique	Técnicas para evitar detecção em ambientes virtualizados ou sandboxes (ex.: anti-VM checks).		[7]	Defense Evasion (TA0005)		
Weakness Identification Technique	Identificação de fraquezas (ex.: CVEs, configurações) no alvo para planejar explorações.		[7]	Reconnaissance (TA0043)		
Web Service Technique	Uso de serviços web legítimos para comando e controle ou exfiltração de dados.		[7]	Command and Control (TA0011)		
Windows Management Instrumentation Technique	Uso do WMI para executar comandos ou coletar informações no Windows.		[7]	Execution (TA0002)		
XSL Script Processing	Uso de scripts XSL em documentos XML para		[7]	Execution (TA0002)		

Technique	executar código malicioso.					
Abuse Elevation Control Mechanism Technique	Abuso de mecanismos de controle de elevação (ex.: UAC bypass) para obter privilégios elevados.		[7]	Privilege Escalation (TA0004)		
Application Window Discovery Technique	Identificação de janelas de aplicativos abertas para planejar ataques ou coletar informações.		[7]	Discovery (TA0007)		
Clipboard Data Technique	Roubo de dados armazenados na área de transferência (ex.: textos copiados) para coleta de informações.		[7]	Collection (TA0009)		
Communication Through Removable Media Technique	Uso de mídias removíveis (ex.: USB) para comunicação entre sistemas infectados.		[7]	Command and Control (TA0011)		
Defacement Technique	Alteração visual de sistemas ou sites (ex.: webpages) para propaganda ou interrupção.		[7]	Impact (TA0040)		
Disk Content Wipe Technique	Apagamento de conteúdos específicos de discos para destruir		[7]	Impact (TA0040)		

	dados seletivamente.					
Domain Generation Algorithms Technique	Uso de algoritmos para gerar domínios dinâmicos para comando e controle ou evasão.		[7]	Command and Control (TA0011)		
Execution through API Technique	Execução de código malicioso por meio de chamadas de API do sistema operacional.		[7]	Execution (TA0002)		
Exfiltration Over Symmetric Encrypted Channel Technique	Transferência de dados roubados por canais simetricamente criptografados (ex.: VPN).		[7]	Exfiltration (TA0010)		
Exploitation for Defense Evasion Technique	Exploração de vulnerabilidades para evitar detecção por sistemas de segurança.		[7]	Defense Evasion (TA0005)		
Exploitation for Evasion Technique	Uso de exploits para burlar defesas específicas (ex.: sandbox, antivírus).		[7]	Defense Evasion (TA0005)		
GUI Input Capture Technique	Captura de entradas gráficas do usuário (ex.: cliques, senhas) para roubo de dados.		[7]	Credential Access (TA0006)		
Indirect	Execução indireta de		[7]	Defense Evasion		

Command Execution Technique	comandos por meio de intermediários (ex.: scripts chamados por binários).			(TA0005)		
Ingress Tool Transfer Technique	Transferência de ferramentas maliciosas para o sistema alvo após o acesso inicial.		[7]	Command and Control (TA0011)		
Multi-Factor Authentication Interception Technique	Interceptação de códigos ou tokens de autenticação multifator para acesso não autorizado.		[7]	Credential Access (TA0006)		
Network Service Discovery Technique	Identificação de serviços de rede ativos (ex.: protocolos, portas) para exploração ou mapeamento.		[7]	Discovery (TA0007)		
NTDS Technique	Roubo do arquivo NTDS.dit no Active Directory para extrair credenciais de domínio.		[7]	Credential Access (TA0006)		
Process Doppelgänging Technique	Uso de técnicas de duplicação de processos para injetar código malicioso sem detecção.		[7]	Defense Evasion (TA0005)		
Screen Capture Technique	Captura de screenshots do sistema alvo para		[7]	Collection (TA0009)		

	coletar informações visíveis na tela.					
Systemd Timers Technique	Uso de temporizadores do systemd (Linux) para agendar execução de código malicioso.		[7]	Persistence (TA0003)		
Time Providers Technique	Manipulação de provedores de tempo do sistema para persistência ou sincronização de ataques.		[7]	Persistence (TA0003)		
Web Session Cookie Technique	Uso de cookies de sessão web roubados para acessar sistemas ou serviços autenticados.		[7]	Credential Access (TA0006)		
Windows Service Technique	Criação ou modificação de serviços do Windows para executar código ou manter acesso.		[7]	Persistence (TA0003)		

Referências:

1) Unified-Cybersecurity-Ontology (UCO) - https://github.com/Ebiquity/Unified-Cybersecurity-Ontology/tree/master
2) SANS - Glossary of Cyber Security Terms - https://www.sans.org/security-resources/glossary-of-terms/

3) CISA-USA Gov (Cybersecurity and Infrastructure Security Agency) - NICCS (National Initiative for Cybersecurity Careers and Studies) - Glossary of Common Cybersecurity Words and Phrases - https://niccs.cisa.gov/cybersecurity-career-resources/vocabulary
4) NCSC-UK (The National Cyber Security Centre) - Glossary of definitions for common cyber security terms used on the NCSC website - https://www.ncsc.gov.uk/section/advice-guidance/glossary
5) NIST Computer Security Resource Center - USA - Glossary of terms. This Glossary is an aggregation of terms and definitions specified in NIST's cybersecurity and privacy standards, guidelines, and other technical publications. - https://csrc.nist.gov/glossary
6) SOCS [ref] - Interna
7) MITRE ATTACK - https://attack.mitre.org/
8) The Cyber Kill Chain in Cybersecurity - Microsoft Security - https://www.microsoft.com/en-us/security/business/security-101/what-is-cyber-kill-chain
9) Cambridge Dictionary - https://dictionary.cambridge.org/dictionary/
10) Rosa, F. de F., Jino, M., & Bonacin, R. (2018). Towards an Ontology of Security Assessment: A Core Model Proposal. In S. Latifi (Ed.), Information Technology - New Generations (pp. 75–80). Cham: Springer International Publishing.
11) Cyber Security Playbooks (CERT Australian Government): https://soc.cyber.wa.gov.au/guidelines/playbooks/
12) 11 Strategies of a World-Class Cybersecurity Operations Center - https://soc.cyber.wa.gov.au/pdfs/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf
13) MD. Ministério da Defesa - Doutrina Militar de Defesa Cibernética. 1. ed. [S.l.: s.n.], 2014. 73, 75, 76.
14) Norma australiana
15) Faria, Marta Rigaud. DEFESA: uma Metodologia para Análise de Incidentes de Segurança da Informação. Dissertação (mestrado) – Instituto Militar de Engenharia, Sistemas e Computação, 2020.
16) DissertaçãoTese Marta
17) CERT.BR. Estatísticas do CERT.br. 2017. Dezembro de 2019. Disponível em: <https://www.cert.br/stats/incidentes/>.
18) HOWARD, J. D.; LONGSTAFF, T. A. A common language for computer security incidents. Sandia National Laboratories, v. 1, p. 1–19, 1998.
19) Para lista de ataques mais comuns https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros / https://stats.cert.br/