São Paulo, Brazil
November 4-5, 2019

The Eleventh International Conference on
FORENSIC COMPUTER SCIENCE and CYBER LAW

www.ICoFCS.org

DOI: 10.5769/C2019002 or http://dx.doi.org/10.5769/C2019002

Uso da Inteligência na Detecção de Ameaças Cibernéticas

Marjori Klinczak[1]

(1) Paraná Perícias, Mosaic Web, Email: contato@mosaicweb.com.br

Abstract: Sendo a segurança de dados um dos grandes desafios do século devido aos impactos serem cada vez mais elevados faz-se necessário a adoção de medidas proativas na detecção de ameaças cibernéticas, pois os ataques também evoluiram, fazendo com que muitos métodos tradicionais não sejam mais adequados para detecção de ameaças. Dessa forma a segurança orientada por inteligência mitiga os riscos de operar no mundo digital. Temos então como objetivo geral desse trabalho a apresentação teórica do modelo Diamond e Kill Chain como solução proativa para detecção, controle e exploração não somente das ameaças mas também dos autores da mesmas, sendo possível inclusive criar um perfil dos mesmos, suas motivações e ferramentas utilizadas nos ataques.

Key words: Segurança da informação, sistemas de inteligência, inteligência, kill chain, modelo diamond.

I. Introdução

Diariamente a internet é utilizada para as mais diversas finalidades, desde estudo com as ferramentas de ensino a distância, socialização através das redes sociais, serviços financeiros através de banco online ou corretoras, compra e venda de serviços e produtos, entre outros. Dessa forma, segundo Oliveira e Torres [2] a internet já está presente no cotidiano das pessoas.

Por outro lado, temos os criminosos, que se aproveitam do contínuo uso de serviços online por parte dos usuários para a aplicação de golpes, roubo ou sequestro de dados, execução de softwares maliciosos, entre outros.

Segundo o relatório *Economic Impact of Cybercrime – no slowing down*, publicado pela Mcaffe [1], o Brasil possui um dos ecossistemas mais exclusivos do mundo para crimes cibernéticos, onde pelo menos 54% dos ataques digitais são originados do próprio país.

Grande parte desses crimes acontecem, pois segundo [2], os criminosos usufruem de um suposto anonimato no meio digital, que diminui seus riscos e geralmente aumenta seu lucro. Sendo que dessa forma, muitos crimes do mundo fisíco migraram para o mundo digital, tal como roubo de identidade e dados ou lavagem de dinheiro. Outro ponto que favorecem esse crimes são as brechas na legislação e a falta de políticas internacionais a respeito.

Temos então que, segundo [4], a segurança de dados é um dos grandes desafios do século, e a tendência é os danos causados serem cada vez

maiores devido a tendência das informações a cada vez mais se tornarem apenas online.

Dessa forma, a maior parte das políticas de segurança visam a criação de políticas de segurança e implementações para que nenhum incidente ocorra, porém usuários mal intencionados frequentemente burlam essas ferramentas de detecção de ameaças, de acordo com [3] e o que ocorre é uma infiltração constante nos sistemas.

Com o uso de sistemas orientados por inteligência esse risco pode ser mitigado, pois tanto a rede quanto equipamentos periféricos recebem um monitoramento constante e muitas vezes em tempo real, são utilizadas técnicas para análise de grande quantidade de informações de forma alertar os analistas de segurança sobre comportamentos suspeitos, e a memória e disco rígido também é analisada para impedir malwares de se infiltrarem nos equipamentos e na rede, e por fim, é criada uma prática de detecção de incidentes para que as respostas sejam alinhadas ao risco que representam.

Pode-se dizer então que os sistemas de segurança baseados em inteligência trabalham de forma proativa no aprimoramento da detecção e resposta a ataques, de forma a evitar que os sistemas sejam de fato comprometidos.

Temos então que o objetivo principal desse trabalho é apresentar, de forma teórica, o que é a inteligência de ameças com base na inteligência, como ela pode ser utilizada e seus respectivos modelos.

Esse trabalho está organizado da seguinte forma: na sessão 2 serão apresentados os conceitos que norteiam esse trabalho, tal como o conceito de inteligência e crimes digitais. Na sessão 3 será apresentado o uso da inteligência na detecção de ameaças digitais e seus modelos, e por fim, na sessão 4 serão apresentadas as conclusões e trabalhos futuros.

2. Referencial Teórico

Nessa seção apresentaremos alguns conceitos de crimes digitais bem como o conceito de inteligência.

A. Crimes Digitais

De acordo com a Secretaria de Nacional Segurança Pública [5], as ações no meio digital podem ser classificadas de 2 formas: próprias e impróprias. As impróprias ocorrem quando a tecnologia é utilizada como uma ferramenta, sendo que o crime já está previsto na legislação, tal como crimes de extorção. E as próprias quando o crime necessita da existência do espaço digital.

Muitos criminosos também fazem com que as vitímas acabem se infectando, segundo [6], através da execução de alguma ação ou código malicioso que irá infectar o dispositivo e dar acesso do mesmo aos atacantes. Dessa forma, segundo [2], torna-se fácil obter informações de usuários desprotegidos ou descuidados.

Como exemplos de crimes digitais podemos citar: roubo de identidade, fraude em compras online, phishing, sequestro de dados, extorção, entre outros.

B. Inteligência

O conceito de inteligência vem de 1832, do livro da Guerra [7], onde o autor aponta a necessidade de termos “todo o tipo de informações sobre o inimigo e o seu país - a base, em resumo, dos nossos planos e operações.”.

Temos então o conceito de não somente nós precavermos de ataques, sendo eles de qualquer natureza, mas de nós anteciparmos a eles, conhecendo o inimigo e seus métodos utilizados.

De acordo com [8], podemos dizer que as ações no ambiente virtual se classificam em ofensivas, exploratórias ou de proteção, conforme pode ser visualizado na Figura 1, sendo que a inteligência está logo abaixo das ações ofensivas, sendo então seu objetivo o de coletar dados, explorá-los de forma a convertê-los em informação e dessa forma transformá-los em inteligência.

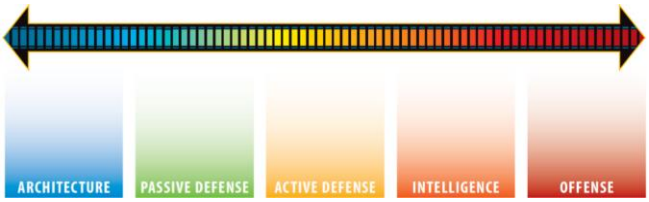


Figura 1. Escala de segurança digital [8].

Dessa forma, segundo [7], as nações vêm se preparando para evitar ou tentar minizar ataques cibernéticos às redes e sistemas de informação do governo e dos demais segmentos da sociedade.

Uma boa inteligência deve ser, antes de tudo acionável, e então possuir as seguintes características, de acordo com [8], ser completa, acurada, relevante e oportuna. Completa significa que a mesma deve ser suficiente para tomada de decisão, acurada significa que deve ser precisa para tomada de decisão, relevante aborda que a mesma deve estar relacionada com sua missão e objetivos, e por fim, oportuna significa que deve ser entregue no tempo correto.

Outras perguntas que a inteligência vai procurar responder é qual ou quais são suas ameaças, quais são os agentes que irão realizar ações maliciosas contra o alvo, e por fim, qual será a técnica utilizada.

Temos então que o conceito de inteligência relacionado as ameças vai muito além de simplesmente conhecer o adversário, englobando também uma grande quantidade de dados capturado e posteriormente analisados, para depois relacionar com as entidades que tem intenção, oportunidade e capacidade de realizar as ações.

3. Inteligência na Detecção de Ameaças

De forma a fazer um bom uso da inteligência, uma organização deve ter amplo conhecimento de si mesma, métodos, processos e tecnologias que utiliza, bem como dos ataques e atacantes a que pode estar sujeita.

Primeiramente a organização deve saber quais atores são uma ameaça para ela, considerando a capacidade, oportunidade e intenção dos mesmos. Como segundo passo deve-se avaliar como as ameaças operam e qual seria o objetivo de cada tipo de ameaça. Por exemplo, visa-se tirar os sistemas da organização por um determinado tempo do ar ou então roubar seus dados.

Após a identificação das ameaças, deve-se considerar qual o risco da organização ser alvo de cada uma delas através da probabilidade x impacto.

E por fim, avaliar quais seriam as melhores formas de prevenção, detecção e resposta das ameaças de maneira oportuna e proativa.

Como forma de auxiliar a organização na identificação das ameaças utiliza-se a “Piramid of Pain”, apresentada na Figura 2. Ela identifica as ameças da mais baixa para a mais alta, sendo que para as mais simples as organizações devem estar preparadas, e o grande risco de grandes danos estão nas ameaças próximas ao topo.

Do primeiro ao quarto degrau tem-se os ataques mais simples e fáceis de resolver e identificar. No primeiro degrau estão problemas que podem ser identificados geralmente por antivírus e firewalls e consistem usualmente em portas abertas ou arquivos infectados. No segundo degrau já temos ameças que podem ser barrados por uma defesa ativa, tal como avisos por email ao acessar alguma conta em local desconhecido. No terceiro degrau podem ser executados ataques, por exemplo, de mudança de registros DNS na máquina de usuário para acesso de páginas falsas como se fossem as reais. O quarto degrau causa mais irritação que real dano, sendo reservado a alguns problemas externos de infra-estrutura.

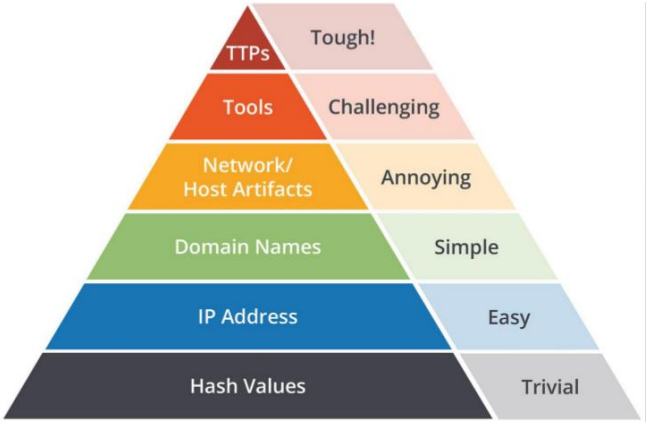


Figura 2. Piramid of Pain [8].

A partir do quinto degrau, as ameaças tornam-se mais desafiadores, tanto para o atacante em já ter se infiltrado e passado pelos outros degraus sem ter sido detectado, quanto para a organização que pode ter grandes danos. No quinto degrau tem-se a infraestrutura interna, enquanto que no sexto e último degrau tem-se todos os sistemas e controles da organização.

Pode-se visualizar então, que tanto a organização quanto o atacante tem longas etapas a percorrer de forma a obter acessos expressivos. Apresentamos então, na Figura 3, a forma como o autor de uma ameça opera, desde seu reconhecimento até seu objetivo final através da Cyber Kill Chain, que é definida como uma cadeia de 7 etapas para se realizar um ataque.

A primeira etapa consiste no reconhecimento e coleta de informações sobre o alvo, sendo que nessa etapa é utilizado de varredura de servidores abertos, engenharia social, coleta de endereços de email e pesquisa dos respectivos perfis em redes sociais.

A segunda etapa tem por objetivo encontrar a ameaça certa para atingir o alvo, um malware que possa comprometer a rede, por exemplo.

Figura 3. Cyber Kill Chain [16].

A terceira etapa consiste em entregar a ameaça para a vítima, sendo que pode ser feito de diversas formas: por email, pen drive, web, entre outros. Posteriormente, a quarta etapa consiste na exploração, ou seja, utilizar alguma vulnerabilidade no sistema de destino de forma a executar ou instalar o software malicioso, sendo essa a quinta etapa.

Por fim, na sexta etapa o alvo é totalmente comprometido, de forma que o atacante possa atingir o objetivo planejado na sétima e última etapa.

Um exemplo é apresentado nas Tabelas 1 e 2, onde na Tabela 1 é apresentado as etapas de uma intrusão e na Tabela 2, a timeline da mesma.

Phase	Action
Reconnaissance	Phishing e-mail
Weaponization	Attachment
Delivery	Malware
Exploitation	Execute
Installation	Install
C2	Control
Actions on Objectives	Carry out goals

Tabela 1: Exemplo das etapas de intrusão [9].

Phase	Jan.	Feb.	Mar.	Apr.
Reconnaissance	Phishing e-mail			
Weaponization		Attachment		
Delivery		E-mail with malware		
Exploitation			Execute	
Installation			Install	
C2				Control
Actions on Objectives				Carry out goals

Tabela 2. Exemplo da linha do tempo de intrusão [9].

A detecção de intrusão pode ocorrer em qualquer uma das etapas, na Figura 4 apresentamos uma detecção logo no inicial, e na Figura 5, a detecção durante a etapa de entrega. Dessa forma, segundo [10] o Kill Chain Model é o único a combinar a inteligência de diferentes etapas para identificar a natureza e o grau de invasão.

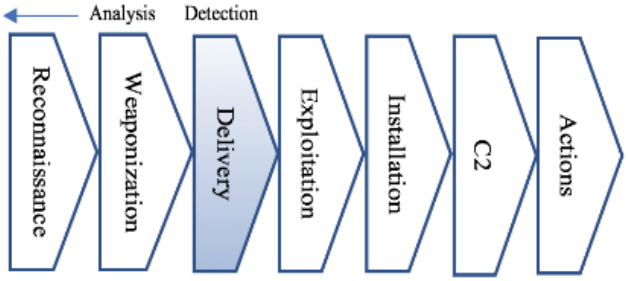


Figura 4: Detecção no ínicio do processo [9].

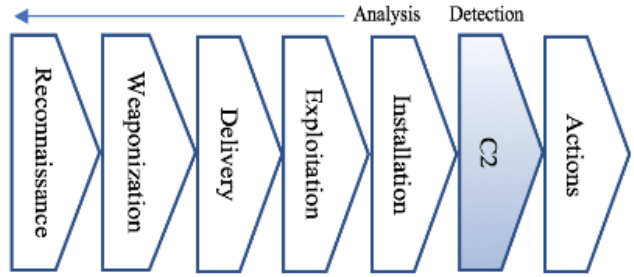


Figura 5: Detecção nas etapas finais do processo [9].

Geralmente junto com o modelo Kill Chain é utilizado o modelo Diamond, segundo [11]. Seu modelo base é apresentado na Figura 6, e cada processo implementado é chamado de evento. De acordo com [9] esses dois modelos são extremamente complementares, onde o modelo Diamond reune as informações para posterior aplicação no Kill Chain, que auxilia no entendimento das fases da invasão, de acordo com [15].

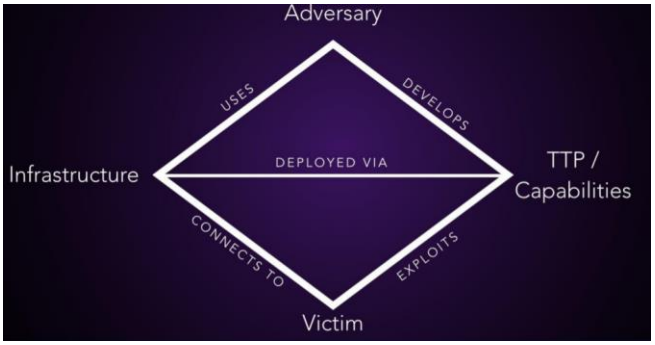


Figura 6: Modelo Diamond [8].

Esse modelo é utilizado para se descobrir e detectar eventos através de seus vértices, que são conectados por arestas que demonstram as relações naturais entre os recursos, podendo descobrir as operações do adversário, infra-estruturas, recursos e a vitíma.

De acordo com [12] o recurso de capacidade explica as ferramentas e técnicas usadas pelo adversário no evento. O recurso de infraestrutura explica o sistema de comunicação lógica e física utilizado pelo adversário para transportar um recurso e manter o controle dos recursos. A vitima é sempre o alvo, podendo ser uma pessoa ou organização, e os ativos da vítima estão relacionados a parte tecnologica, como por exemplo falhas em softwares que utiliza.

A conexão desses 4 rercursos principais (adversário, capacidade, vítima, infraestrutura) é chamada de análise analítica, e a rotação análitica permite o entendimento do relacionamento entre os principais recursos, segundo [13].

Como um evento é somente um entre as várias etapas da cadeia que precisam ser executados antes do adversário atingir seu objetivo, eles são orientados por fases e conectados segmentos de atividade pelo relacionamento adversário-vítima.

Dessa forma, o modelo descreve uma atividade programada, limitada a uma frase específica na

qual o adversário exige recursos externos e utiliza uma capacidade metodológica sobre uma infraestrutura contra uma vitíma, segundo [10]. Um detalhe do modelo é que não há uma necessidade de que todos os recursos sejam conhecidos.

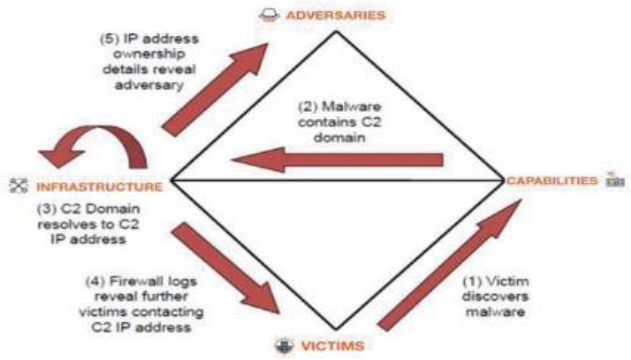


Figura 7: Análise de pivo utilizando o modelo diamond [9].

Na Figura 7 é apresentado um exemplo do modelo através de 5 etapas, onde na primeira delas a vítima descobre o malware, na segunda observa-se que o malware contém o domínio C2, que na etapa 3 o domínio C2 resolve para um endereço IP C2. Na etapa 4 é revelado informações sobre vítimas adicionais que entram em contato com o IP C2 através dos logs do firewall, e por fim, na etapa 5, os detalhes de propriedade do endereço IP revelam informações sobre o adversário ou adversários, segundo [14].

Após essa análise ser relizada, pode-se responder algumas das questões que foram levantadas sobre o perfil dos atacantes que são uma ameça e suas motivações. Um exemplo desses passos é apresentado na Figura 8, que contém uma lista de exemplos de classes de adversários, possíveis motivações, ativos desejados, impactos que podem ser causados e vetores utilizados. Já na Figura 9 foram selecionados alguns elementos de forma a exemplificar o perfil do ator.

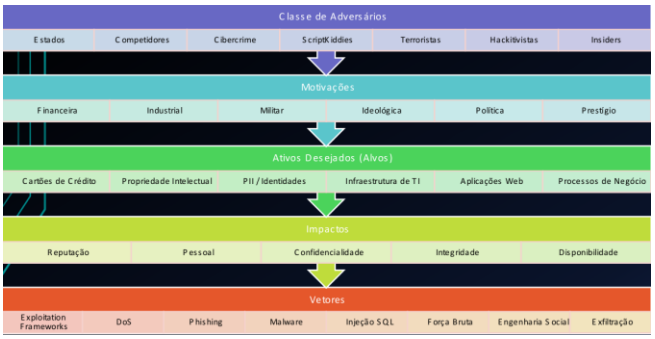
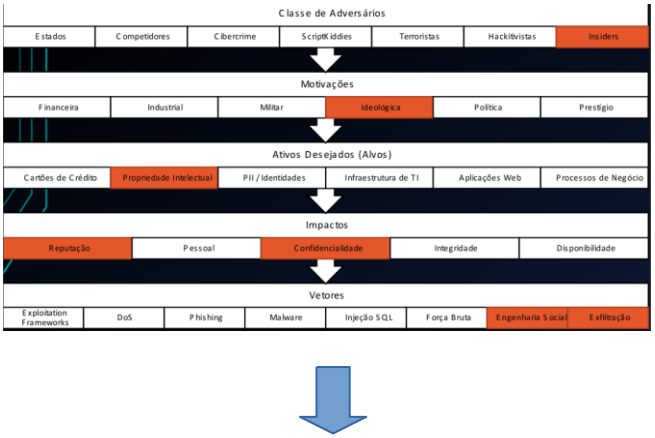


Figura 8: Seleção inicial de perfil do atacante [8].



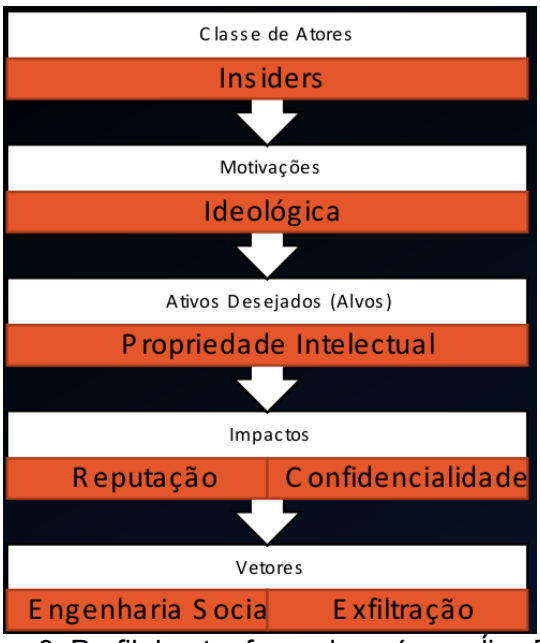


Figura 9: Perfil do ator formado após análise [8].

4. Conclusões

Conforme a internet e o meio digital se torna mais presente em nossas vidas e atividades cotidianas, maior a motivação de criminosos para conseguir acesso a nossas contas e dispositivos. De forma que não podemos mais acreditar que possuir um antivírus ou um firewall habilitado vai manter esses criminosos longe.

Assim como os recursos tecnológicos evoluíram, o mesmo aconteceu com ações criminosas no meio digital, com o adicional dos mesmo se sentirem mais confiantes devido a legislação falha e a uma falsa sensação de anonimato.

Dessa forma torna-se necessário uma postura proativa com relação as ameaças digitais, não devemos apenas impedir que tenham acesso as redes, contas e dispositivos, mas também entender suas motivações, forma de atuação e quem são os atacantes.

Temos então a segurança orientada a inteligência, que consegue processar grandes quantidade de dados quase em tempo real, procurar padrões e verificar comportamentos suspeitos.

De posse dessas informações podemos, através de modelos como o Kill Chain e o Diamond temos compreender a natureza de cada intrusão e classificá-la em fases, montando um perfil dos atacantes.

Por fim, como trabalho futuro desejamos realizar a implementação dos modelos propostos em uma rede de forma a verificar os modelos gerados e também a os resultados obtidos.

References

[1] Mcaffe. The Economic Impact of Cybercrime - No Slowing Down. Disponível <https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf>. Acessado em 10 de setembro de 2019.

[2] Oliveira, Marco & Torres, Claudines. Crimes Cibernéticos - Estudo de Caso: Técnica Maliciosa. Fatec Bauru, 2015.

[3] White Paper da RSA. Detecção e Resposta a Ameaças Orientada por Inteligência. Disponível em <https://brazil.emc.com/collateral/white-paper/h1304-intelligence-driven-threat-detection-response-wp.pdf>. Acessado em 1 de setembro de 2019. 2014.

[4] Batista, Lucas Oliveira & de Silva, Gabriel Adriano & Araújo, Vanessa Souza & Araújo, Vinícius Jonathan Silva & Rezende, Thiago Silva & Guimarães, Augusto Junio & Souza, Paulo Vitor de Campos. Utilização de Redes Neurais Nebulosas para criação de um Sistema Especialista em Invasões Cibernéticas. Icofcs, 2018.

[5] Secretaria Nacional de Segurança Pública."Crimes Cibernéticos" Procedimentos Básicos. https://ead.senasp.gov.br>. Acessado em 1 de setembro de 2019. 2014.

[6] Wendt, E. Jorge, H. "Crimes Cibernéticos" Ameaças e Procedimentos de Investigação. Rio de Janeiro, Brasport, 2ª edição. 2013.

[7] Caltagirone, Sergio. Industrial Control Threat Intelligence. Disponível em <https://dragos.com/wp-content/uploads/Industrial-Control-Threat-Intelligence-Whitepaper.pdf>. Acessado em 20 de setembro de 2019. 2018.

[8] Carvalho, P. S. M. D. A defesa cibernética e as infraestruturas críticas nacionais. Coleção Meira Mattos-Revistadas Ciências Militares. 2011.[9] Event Tracker. SIEMphonic and the Cyber Kill Chain. Disponível em <https://www.eventtracker.com/blog/2017/january/siemphonic-cyber-kill-chain/>. Acessado em 15 de setembro de 2019. 2017.

[9] Ertaul Levent & Mousa, Mina. Applying the Kill Chain and Diamond Models to Microsoft Advanced Threat Analytics. Int'l Conf. Security and Management. 2018.

[10] David Sweigert, Defensive cyber security expert Follow. "Understanding Cyber Kill Chain and OODA loop." Disponível em < www.slideshare.net/dgsweigert/under-cyber-kill-chain-and-ooda-loop>. Acessado em 11 de setembro de 2019. 2017.

[11] Faulkner, Sophia A. Looking to Deception Technology to Combat Advanced Persistent Threats. Dis Utica College, 2017.

[12] Rittenberg, Josh . The Rise of Threat Hunting in Preventing Cyber Attacks. Disponível em < breachmemo.com/the-rise-of-threat-hunting-in-

preventing-cyber-attacks/>. Acessado em 17 de setembro de 2019. 2017.

[13] Spring, J. M. Toward realistic modeling criteria of games in internet security. Journal of Cyber Security & Information Systems, 2(2), 2-11. 2014.

[14] Kotheimer, John & Kyle OMeara. Using Honeynets and the Diamond Model for ICS Threat Analysis. No. CMU/SEI-2016-TR-006. Carnegie-mellon university of Pittsburgh,USA, 2016.

[15] Posts about diamond model on Count Upon Security. (Diamond Model). Disponível em < https://countuponsecurity.com/tag/diamond-model/>. Acessado em 18 de setembro de 2019. 2018.

[16] Event Tracker. SIEMphonic and the Cyber Kill Chain. Disponível em: <https://www.eventtracker.com/blog/2017/january/siemphonic-cyber-kill-chain/>. Acessado em 15 de setembro de 2019. 2017.