An Adaptive Middleware Solution for Complex-Event Processing

A. L. Gonzalez, R. L. A. Rocha and J. J. Neto

***Abstract*— The occurrence of events is growing because of the increasing rate of use of services made available via internet, such as data storage. On that basis, however, there is a growing number of threats to the information, requiring approaches capable of promptly responding to unknown threats. The objective of this research is to create an approach that is able to adapt itself from an initial configuration based on historical data threats, in order to obtain the means to respond to new and unknown threats. For this, an approach involving complex-event processing (CEP) and ontologies, to coordinate the CEP, is proposed. Thus, it is expected that it is possible to treat a wide variety of threats, known or unknown, in a effective and efficient manner. Thus, one can ensure greater security to the information storage services located in clouds.**

***Keywords*— Complex-Event Processing (CEP); Adaptivity; Middleware; Ontology.**

I. INTRODUÇÃO

O TRABALHO apresentado por este artigo refere-se a um trabalho de pesquisa em andamento. Este trabalho está sendo desenvolvido no contexto do Programa de Pós-Graduação em Engenharia de Computação da POLI/USP. Por se tratar de um trabalho em andamento, alguns pontos ainda estão indefinidos e é necessária maior pesquisa para fazer as escolhas da forma mais embasada possível. Assim, este artigo apresenta o projeto de pesquisa, os pontos principais e alguns tópicos ainda a serem definidos.

A pesquisa envolve temas relacionados à segurança cibernética, processamento de eventos, técnicas adaptativas e representação de conhecimento. A área de segurança cibernética foi escolhida com o intuito de delimitar o escopo da abordagem a ser proposta, mas a aplicação da mesma poderá ser expandida, caso seja notada esta necessidade.

A utilização de técnicas adaptativas foi imaginada no decorrer da disciplina PCS5004 – Fundamentos e Aplicações da Tecnologia Adaptativa, da POLI/USP.

O crescente volume de dados gerados no monitoramento e supervisão dos recursos disponibilizados pelos sistemas de informação, armazenados em bases de dados de séries temporais dificultam a adoção bem fundamentada de ações de controle e supervisão de um operador humano no contexto de segurança cibernética.

A utilização de ontologias e técnicas adaptativas para representação computacional de conhecimento e sua utilização em uma solução automática e de tempo-real para classificação de eventos primários e lançamento de eventos complexos para aumentar a consciência situacional do estado de operação do sistema e de seu contexto de operação, torna mais fácil a adoção de ações de controle e supervisão de um operador humano no contexto de segurança cibernética.

A Figura 1 apresenta o resumo gráfico da abordagem proposta.

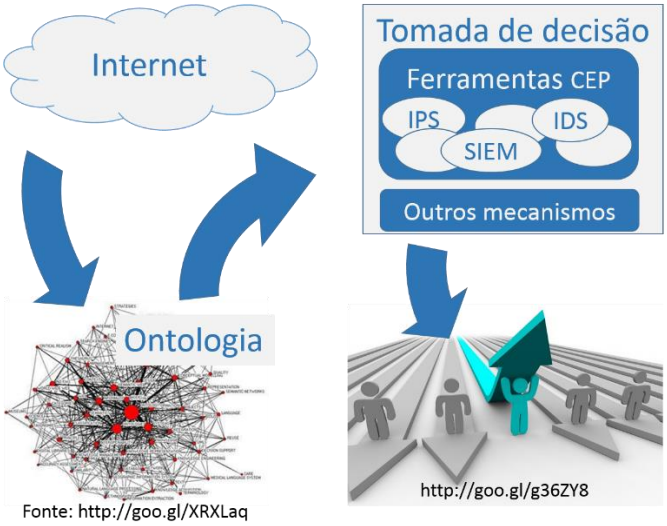

Figura 1- Resumo da abordagem proposta

A. *Problema de Pesquisa*

O problema de pesquisa a ser abordado neste trabalho visa atender ao tema de pesquisa do trabalho de pós-graduação do autor. Este tema foi levantado nas pesquisas iniciais, realizadas previamente ao início dos trabalhos, e aprimorado no contexto da disciplina PCS5012 – Metodologia de Pesquisa Científica para Engenharia de Computação, da POLI/USP. Este trabalho de pesquisa visa encontrar uma resposta para o problema de pesquisa que considera a dificuldade em adotar ações para controle e supervisão de eventos, levando-se em conta o contexto de segurança cibernética.

B. *Hipótese*

Para responder ao problema de pesquisa levantado, imagina-se que a utilização de ontologias e técnicas adaptativas para representação computacional de conhecimento proporciona um aumento da consciência situacional do estado de operação do sistema e de seu contexto de operação e, além disso, a utilização desta forma de representação de conhecimento, em uma solução automática e de tempo-real para classificação de eventos primários e lançamento de eventos complexos, torna mais fácil a adoção de ações de controle e supervisão de um operador humano no contexto de segurança cibernética.

C. *Justificativa*

As hipóteses, são importantes pois direcionam o trabalho em desenvolvimento. Esta hipótese será o rumo que o trabalho deverá seguir e sua aceitação, ou rejeição, deverá ser discutido e apresentado como resultado do trabalho. A rejeição da hipótese não significa que o trabalho não tem valor, pois pode-se gerar conhecimento novo no processo de investigação para a rejeição da mesma.

D. *Objetivos*

Com o intuito de desenvolver este trabalho e verificar seus resultados, foi delineado um objetivo geral, que deverá ser validado ao término do trabalho. A partir deste objetivo geral, foram traçados objetivos específicos, que serão verificados durante o trabalho, de forma similar a checkpoints do processo de desenvolvimento do trabalho.

Este trabalho propõe a construção adaptativa de ontologias para representação computacional de conhecimento extraído de análises realizadas no crescente volume de dados gerados no monitoramento e supervisão dos recursos disponibilizados pelos sistemas de informação, armazenados em bases de dados de séries temporais e sua utilização em uma solução automática e de tempo-real para classificação de eventos primários e lançamento de eventos complexos para aumentar a consciência situacional do estado de operação do sistema e de seu contexto de operação, suportando a adoção bem fundamentada de ações de controle e supervisão de um operador humano no contexto de segurança cibernética.

A partir do objetivo geral apresentado acima, podem-se traçar alguns objetivos específicos, que serão abordados no decorrer do desenvolvimento do trabalho. Os objetivos específicos são:

- Estudo e escolha de ferramentas CEP;
- Integração da solução às ferramentas CEP escolhidas;
- Escrita de artigos para compartilhamento do conhecimento.

E. *Resultados Esperados*

A partir do objetivo do trabalho, podem-se definir alguns resultados esperados deste trabalho de pesquisa. Os resultados esperados são:

- Definição de uma abordagem para CEP na área de cybersecurity que se utilize dos benefícios das ontologias para aumentar a segurança da informação;
- A verificação da aplicabilidade da abordagem proposta também faz parte dos resultados esperados.

F. *Organização do Trabalho*

Este trabalho está organizado de forma que a Seção II apresenta uma revisão dos principais trabalhos relacionados, fornecendo o embasamento teórico necessário para a discussão da escolha relacionada ao dispositivo adaptativo. A Seção III descreve a solução adaptativa para processamento de eventos complexos proposta neste trabalho. A Seção IV apresenta as conclusões do trabalho. Por fim, são apresentadas as referências consultadas para a concepção deste trabalho.

II. CONCEITOS GERAIS

A área de tecnologia da informação (TI) está passando por um período de grande crescimento do fluxo de informação. Fortes pressões na forma de utilização de sistemas de informação, com usuários utilizando seus próprios dispositivos (BYOD, do inglês, *Bring-Your-Own-Device*) para acessar sistemas antes disponíveis apenas dentro do ambiente corporativo e a alta capilaridade na aquisição de dados de fontes diversas (IoT, do inglês, *Internet-of-Things*) tornam possível a disponibilização em tempo-real de informação contextualizada e distribuída para um usuário tomar decisões bem fundamentadas.

Além dos desafios impostos a demandas de conectividade e capacidade de armazenamento de dados, os sistemas de informação passam a ser mais valiosos, do ponto de vista de disponibilidade de informação mais detalhada de cada usuário, como hábitos e contexto de utilização de informação e mais expostos, do ponto de vista de segurança, uma vez que se tornam acessíveis de praticamente qualquer lugar através de qualquer dispositivo.

A expansão da conectividade, o armazenamento e coleta de um volume cada vez maior de dados, o aumento da capacidade de análise e a obtenção da informação a partir dos dados tornam a proteção destes sistemas uma tarefa desafiadora, de forma que abordagens tradicionais de segurança de rede continuam necessárias, mas estão longe de serem suficientes num contexto em que as consequências do roubo de informação se tornam cada vez mais abrangentes.

Soluções de segurança do tipo caixa-forte, com forte separação entre ambiente interno e externo, não são mais aplicáveis em muitos cenários, exigindo uma consciência situacional maior para identificação e monitoramento de atividades de cada usuário.

Nesta abordagem, além da capacidade de trabalhar sobre grande volume de dados em tempo-real, há a dificuldade de se lidar com a imprevisibilidade e não sincronismo das ações e intenções de um usuário. A consciência da necessidade de acompanhar as ações de usuários específicos dentro de um sistema levou à construção de soluções SIEM, que vão além do estabelecimento de uma barreira de acesso e buscam a identificação e rastreamento de ações que ocorrem dentro do sistema em tempo-real baseando-se no processamento de eventos de segurança provenientes de dispositivos de controle de acesso, IDS, IPS e sobre eventos gerados por sistemas como o SPLUNK, que monitoram logs textuais de diversos sistemas e aplicam regras pré-definidas.

Existem, hoje, inúmeros sistemas capturando, recebendo e gerando informação de e para o mundo real. Uma dificuldade crescente está em dar significado a toda esta informação existente, de forma que a qualidade da informação para uso em diversos outros fins seja aumentada e que possam ser obtidas respostas mais eficientes a partir delas [6]. No contexto de segurança da informação, tentativas de intrusão não autorizada a redes e sistemas de armazenamento deixam rastros de informações que podem ser transformados em eventos. Estes podem ser coletados, classificados, processados

e utilizados para decisão de quais medidas apropriadas serão adotadas para evitar ou minimizar as consequências de eventos indesejáveis. [4] define evento como algo notável que acontece. Desta forma, pode-se considerar este fluxo de informação como um conjunto de eventos observados em um intervalo de tempo, sob uma determinada óptica. Sistemas orientados a eventos permitem que eventos sejam, automaticamente, interpretados e correlacionados.

A. *Adaptatividade*

A adaptabilidade oferece ao usuário de um sistema a possibilidade de alterar as configurações, a partir de uma quantidade limitada de opções previstas no processo de desenvolvimento e pré-programadas. A adaptatividade, por outro lado, permite que um sistema se autoconfigure, em tempo de execução, sem a interferência de um agente externo.

Pela utilização de técnicas adaptativas, o sistema é capaz de se adaptar a situações novas ao se confrontar com situações imprevistas. Estas alterações ocorrem de maneira automática pelo sistema, e de forma transparente ao usuário [13] [14]. Pela utilização da adaptatividade, pode ser impossível reconhecer um software após algum tempo em execução.

B. *Dispositivos Adaptativos*

Dispositivos orientados a regras são quaisquer dispositivos que sejam dependentes de sequências finitas de regras pré-definidas.

A adaptatividade de um dispositivo se dá a partir da existência de funções que permitam que tal dispositivo altere as suas próprias regras de construção.

Em [15] é proposto um modelo híbrido, que permite a adoção de técnicas adaptativas sobre dispositivos orientados a regras já existentes. Neste trabalho, os dispositivos adaptativos são formados por duas camadas, sendo uma delas não adaptativa (dispositivo convencional) e a outra responsável por implementar as funções de adaptatividade. Desta forma, a camada adaptativa tem a capacidade de modificar a camada convencional, mudando seu conjunto de regras.

C. *Statecharts Adaptativos*

Nos artigos [13] e [14], os autores apresentam os conceitos e a formulação geral acerca das técnicas adaptativas.

No ano seguinte à publicação do segundo trabalho, foi publicado [1]. Este trabalho surge como uma continuação dos primeiros, no qual é apresentada uma proposta de utilização das técnicas adaptativas de maneira gráfica.

A abordagem desenvolvida faz uso de elementos conhecidos como statecharts. Statecharts são dispositivos hierárquicos que visam descrever o comportamento reativo de sistemas de maneira gráfica.

Os statecharts aparecem como uma evolução das máquinas de estados finitos e dos diagramas de estado. Este tipo de diagrama permite que a dinamicidade dos sistemas que estão descrevendo.

Statecharts são formados por retângulos com bordas arredondadas, representando os estados. Além disso, existem também linhas que conectam os retângulos. Estas linhas representam as transições entre os estados [1].

O "funcionamento" dos statecharts se dá de maneira semelhante ao das máquinas de estados finitos. As transições dependem do estado atual em que a máquina se encontra e de um evento (entrada). Na ocorrência de eventos previstos, a transição é disparada e a máquina passa para o próximo estado.

Porém, statecharts ampliam as máquinas de estados finitos por permitirem a existência de transições ortogonais, ou seja, simultâneas.

A utilização de statecharts para a modelagem do comportamento reativo permitiu um aprofundamento e consequente evolução das abordagens adaptativas utilizadas até este momento. Os statecharts adaptativos são construídos a partir de statecharts convencionais existentes. Seu funcionamento se dará da mesma maneira, a não ser quando da existência de funções adaptativas associadas às transições.

Estas funções adaptativas, quando encontradas em uma transição entre estados, permite que o statechart execute uma transformação sobre seus estados e transições, ou seja, uma auto-reconfiguração.

As funções adaptativas permitem que novos estados ou transições sejam incluídos no statechart, ou que elementos existentes sejam eliminados.

A partir de sua utilização e após algum tempo de execução, pode tornar-se impossível reconhecer o statechart adaptativo inicial.

Statecharts são capazes de representar o comportamento dinâmico dos sistemas que descrevem. Os estados podem ser encadeados e ligados, de forma a representar os sistemas em seus comportamentos sequencial ou concorrente [1].

As ligações entre os estados são chamadas de transições, e a cada transição podem ser associadas ações que serão executadas quando a transição ocorrer. Para que uma transição ocorra, é necessário que uma condição seja satisfeita.

As ações associadas às transições dos statecharts podem ser ações adaptativas. Estas ações, quando ocorrem, podem modificar o conjunto de estados e/ou as ligações entre os estados do statechart. Estados e transições podem ser criados e eliminados dos statecharts pelas ações adaptativas.

A Figura 2 apresenta um exemplo de um statechart, com uma ação adaptativa em destaque. A ação adaptativa está representada em vermelho, com a identificação $\mathcal{A}()$.

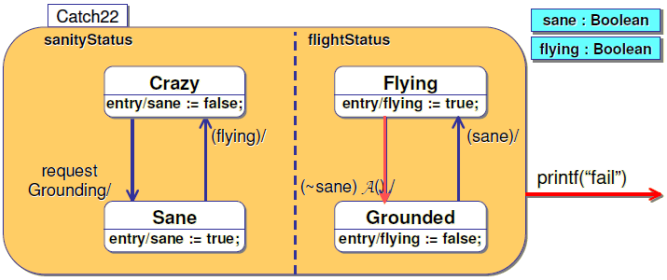

Figura 2 - Exemplo de Statechart Adaptativo (Fonte: Material de aula PCS5004)

D. Gramáticas Adaptativas

Gramáticas são formalismos baseados em regras de substituição [9]. Sua operação se baseia na aplicação sucessiva de regras, até que restem apenas terminais. Estas gramáticas permitem a auto-modificação de suas regras durante sua utilização.

E. Redes de Markov

Redes de Markov garantem que a probabilidade de um dado estado ser atingido depende exclusivamente do estado corrente da rede. Em [2], prova-se que a Máquina de Markov é equivalente ao Autômato Finito.

A ocorrência de uma transição entre estados faz com que seja executado um conjunto de ações adaptativas. Em Sistemas de Markov Adaptativos, as ações adaptativas de uma máquina podem atuar, também, nos conjuntos de regras de outras máquinas pertencentes ao sistema.

F. Tabelas de Decisão Adaptativas

Tabelas de decisão adaptativas são definidas a partir das tabelas de decisão tradicionais (não-adaptativas). Estas tabelas consistem de um conjunto de regras representadas por condições e ações correspondentes, que serão executadas caso a condição seja satisfeita. As regras são apresentadas nas colunas, enquanto as condições são apresentadas nas linhas. As ações, assim como as condições, são apresentadas nas linhas [16].

As tabelas adaptativas apresentam estrutura similar às tradicionais, porém, com linhas adicionais após as ações, que consistem das ações adaptativas. Estas linhas de ações adaptativas são divididas em ações anteriores e ações posteriores.

Quando uma ação adaptativa é executada, seu conjunto de regras poderá ser alterado. Desta forma, as colunas da tabela poderão ser modificadas, de maneira que novas colunas podem ser adicionadas, ou colunas existentes podem ser eliminadas.

A Figura 3 apresenta um exemplo de uma tabela de decisões adaptativa. Nesta tabela de decisões, as áreas 2, 3 e 4 apresentam as as funções adaptativas, suas chamadas e as ações correspondentes.

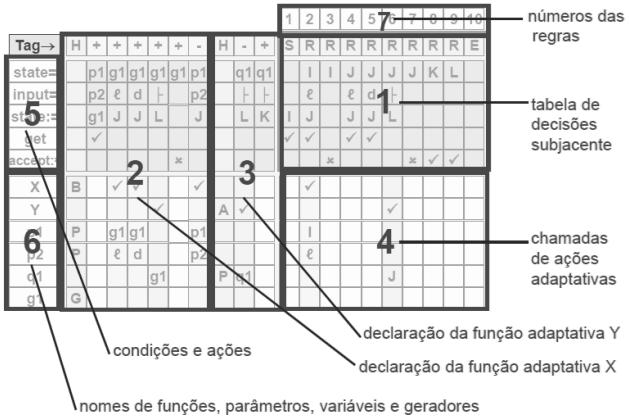

Figura 3- Exemplo de Tabela de Decisões Adaptativas (Fonte: Material de aula PCS5004)

G. Árvores de Decisão Não-Determinísticas Adaptativas

Árvores de Decisão Não-Determinísticas (*NDD-tree*) representam as decisões como folhas da árvore e os testes discretos em seus nós intermediários. Os resultados dos testes discretos indicam o caminho percorrido, desde o nó-raiz, para decidir um dado problema.

Quando buscando uma solução para determinado problema, a NDD-tree executa de maneira não-determinística, testando todos os caminhos possíveis. É possível ter mais de uma resposta para um problema tratado por NDD-tree.

[17] define a Árvore de Decisão Não-Determinística Adaptativa (ANDD-tree). Esta árvore utiliza NDD-tree como o mecanismo subjacente. A camada adaptativa permite que a NDD-tree altere sua estrutura. Operações de inspeção, adição e remoção de regras (nós de decisão) são possíveis neste tipo de dispositivo.

H. Autômatos de Estados Finitos Adaptativos

Os autômatos de estados finitos adaptativos são uma evolução, e simplificação, dos autômatos de pilha adaptativos [3]. Este dispositivo utiliza o autômato de estados finitos como mecanismo subjacente.

Neste tipo de dispositivo, o passo de operação muda juntamente com as modificações no conjunto de regras do autômato subjacente. O novo conjunto de regras associa a cada regra não-adaptativa um par de ações adaptativas (anterior e posterior).

Estes autômatos apresentam o mesmo poder computacional da Máquina de Turing, além de aceitar linguagens dependentes de contexto.

III. PROCESSAMENTO DE EVENTOS COMPLEXOS ADAPTATIVO PARA SEGURANÇA DA INFORMAÇÃO

O processamento de eventos (EP) consiste de um conjunto de técnicas e ferramentas que auxiliam na compreensão e controle de sistemas orientados a eventos [11]. A ideia principal é explorar relacionamentos causais, temporais e semânticos entre eventos, de forma a dar sentido a eles em tempo hábil de resposta [6]. Este comportamento permite identificar oportunidades e riscos tão logo um evento ocorra. Também possibilita que os eventos sejam diagnosticados e decisões sejam tomadas em um curto intervalo de tempo.

A partir do correlacionamento entre dois ou mais eventos, é possível identificar novos eventos. Eventos gerados a partir destas relações, e que podem ocorrer somente pela existência dos eventos relacionados, são conhecidos como eventos complexos, de forma que eventos complexos são abstrações de mais alto nível que representam uma situação, um evento composto, inferido pela ocorrência de outros eventos mais elementares e diretamente observados ou identificados [5]. Porém, é necessário que exista um contexto para que eventos complexos sejam identificados, não sendo suficiente a simples correlação entre os eventos. Ou seja, a combinação entre dois ou mais eventos necessita de significado semântico e

conhecimento situacional para gerar novos eventos complexos.

Os eventos, por si só, não carregam valor semântico que permita que conhecimento seja obtido a partir de sua análise ou da análise de seu comportamento. Uma forma de agregar significado aos eventos é pela utilização de ontologias. Estas ontologias permitem que as informações referentes aos eventos sejam estruturadas adequadamente e analisadas automaticamente em ambiente computacional, possibilitando a realização de previsões e a tomada das ações devidas. O processamento de eventos complexos (CEP) baseia-se na observação de que, em muitos casos, ações são disparadas não pela ocorrência de um evento isolado, mas pela composição de diversos eventos, que podem ocorrer em momentos distintos (temporalidade) e sob contextos diferentes (causalidade e semântica).

A. Middleware Adaptativo

A segurança da informação é uma área na qual utilizam-se técnicas de processamento de eventos. Esta área trata da proteção da informação quanto ao acesso, alteração e destruição não autorizados. Segundo [12], falhas de segurança em sistemas são exploradas por atacantes por 229 dias até serem detectadas. Após a detecção, há ainda um período de aproximadamente 30 dias até que os agressores sejam banidos da rede da vítima [10]. Segundo boletim [7], obteve-se um índice indicando que mais de 97% dos sistemas contém falhas de segurança, independentemente das camadas de segurança adotadas.

Devido à natureza das ameaças, a imprevisibilidade e a criticidade do tempo de resposta são características importantes. Desta forma, é necessário um monitoramento constante das ações para que, no momento em que um evento de ameaça à segurança seja identificado, contramedidas sejam disparadas, proporcionando o menor atraso possível para que sejam reduzidos os riscos e danos causados pelos eventos. Identificar eventos, ou séries de eventos, e reagir a eles de maneira apropriada e com a menor latência são os principais objetivos de sistemas nesta área. Em outras palavras, quanto antes uma ameaça for identificada, mais cedo uma ação poderá ser disparada em resposta, mitigando seus efeitos.

As abordagens tradicionais de processamento de eventos de segurança levam em conta apenas eventos considerados de segurança, de forma que os sistemas identificam como ameaças eventos previamente indicados como sendo relacionado à área de segurança. Ou seja, caso ocorra um evento que não conste da lista de eventos de segurança dos sistemas de detecção, este evento é desconsiderado no momento da verificação, não sendo submetido a qualquer tipo de análise. Outro problema das abordagens tradicionais é a falta de integração entre os eventos provenientes de fontes heterogêneas e distribuídas. Existem diversas ferramentas voltadas para a captura de eventos em diferentes áreas de cybersecurity, como SIEM, IDS/IPS, DLP, APT, entre outras. Porém, não existem ferramentas que correlacionem estes eventos, de forma a identificar padrões de diferentes ameaças que possam ter alguma relação entre si.

A associação de ontologias com o processamento de eventos complexos na área de segurança permite que questões como o apoio a processos de análise da causa raiz de conjuntos de eventos de segurança sejam passíveis de ações preventivas e/ou reativas de forma automática, a partir da definição do contexto de cada evento e a regra a ser aplicada em cada caso. Segundo [8], ontologias são capazes de inferir novo conhecimento a partir de informações existentes, de forma a possibilitar uma maior automatização dos sistemas, que podem reagir de forma automática a determinadas ações.

Com o intuito de obter melhores resultados, quanto aos tempos de detecção eventos ou identificação de eventos complexos e tempo de reação do sistema de segurança, é proposta uma abordagem adaptativa baseada em ontologias para a classificação de eventos de segurança. Esta abordagem visa correlacionar eventos provenientes de diversas fontes e adicionar semântica a estes eventos, possibilitando a identificação de eventos complexos a partir do monitoramento contínuo de eventos.

Pela utilização desta abordagem, espera-se obter uma maior consciência situacional, possibilitando tomadas de decisão baseadas no significado dos eventos. Adicionalmente, torna-se possível a adaptação automática e online da ontologia utilizada através da realimentação de eventos previamente identificados de forma a evolui-la dinamicamente. Esta realimentação se daria a partir da análise de dados históricos, por exemplo, que possibilitariam a atualização da ontologia. A capacidade de adaptação possibilitaria antecipar as conclusões a respeito do espaço cibernético de contexto e, consequentemente, diminuir o tempo de reação a uma ameaça.

B. CEP com Middleware Adaptativo

A solução proposta é composta por duas partes. A primeira parte corresponde à um conjunto de ferramentas de processamento de eventos complexos já existentes no mercado. Estas ferramentas são responsáveis por tratar os eventos capturados e, se possível, disparar as ações necessárias para tratá-los.

Caso os eventos sejam desconhecidos pelo conjunto de ferramentas, os eventos são passados, na forma de estímulos, para a segunda parte da abordagem proposta. Esta segunda parte corresponde à parte adaptativa da proposta. A parte adaptativa é composta por uma máscara, responsável por verificar um conjunto condições, a partir dos estímulos. Estas condições servirão de entrada para a Tabela de Decisão.

Na Tabela de Decisão estão configuradas ações adaptativas que permitem alterar a ontologia, de forma que próximos conjuntos de estímulos (eventos complexos) possam ser tratados prontamente pela solução.

Além disso, existem ações adaptativas que alteram a própria Tabela de Decisão, de forma a refletir as alterações realizadas na ontologia.

Por fim, a Tabela de Decisão contém conjuntos definidos de ações, que permitem disparar as respostas adequadas aos conjuntos de estímulos, por meio das ferramentas CEP.

A abordagem proposta, descrita acima, é apresentada, graficamente, abaixo, por meio da Figura 4.

Esta abordagem foi proposta, inicialmente, para tratar eventos relacionados à área de cybersecurity. Por isso, a ontologia utilizada descreve o universo relacionado à esta área.

Porém, durante o desenvolvimento da mesma, foi observado que, ao se alterar a ontologia, pode-se tratar eventos de quaisquer áreas.

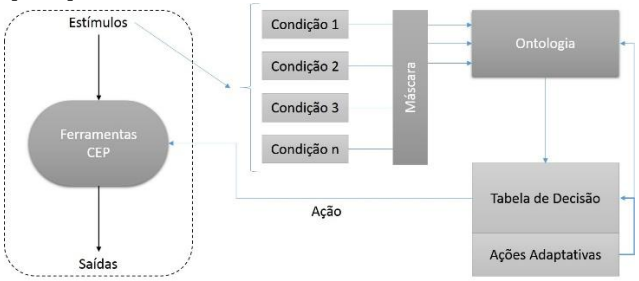

Figura 4 - Abordagem Proposta

IV. CONCLUSÕES

O trabalho apresentado possui uma vertente na análise e processamento automatizado de eventos no contexto de segurança cibernética. O desenvolvimento de uma abordagem para CEP visa auxiliar na tomada de decisão e reação de sistemas frente a identificação de ameaças à sistemas de informação.

A partir do objetivo do trabalho, podem-se definir alguns resultados esperados deste trabalho, como a definição de uma abordagem para CEP na área de cybersecurity que se utilize dos benefícios das ontologias para aumentar o significado dos eventos. Desta forma, espera-se um aumento nos níveis de segurança da informação.

A definição de formas para a verificação da aplicabilidade da abordagem proposta também faz parte dos resultados esperados.

Os resultados obtidos durante o trabalho serão analisados e comparados com resultados obtidos a partir dos mesmos conjuntos de entrada em sistemas de código aberto já existentes e utilizados pela comunidade. Desta forma, poderão ser avaliados a eficiência, eficácia e grau de melhoria obtidos pela proposta.

Como forma de avaliação, definida de maneira preliminar, será desenvolvido um software que utilizará uma abordagem iterativo-incremental, com foco nas disciplinas de Requisitos, Análise e Projeto, Casos de Uso, Implementação, Testes, Implantação e Gerenciamento de Configuração. Este software terá seu desempenho analisado e os resultados obtidos a partir de sua execução comparados aos resultados de softwares de código aberto com melhores resultados existentes atualmente.

REFERÊNCIAS

[1] JR Almeida. STAD-Uma Ferramenta para Representação e Simulação de Sistemas. Através de Statecharts Adaptativos. PhD thesis, Tese de Doutorado, Escola Politécnica, Universidade de São Paulo, São Paulo, 1995.

[2] Bruno Arantes BASSETO. Um sistema de composição musical automatizada, baseado em gramáticas sensíveis ao contexto, implementado com formalismos adaptativos. PhD thesis, Dissertação (mestrado), EPUSP, São Paulo, 2000.

[3] Amaury Antônio de CASTRO JUNIOR. Aspectos de projeto e implementação de linguagens para codificação de programas adaptativos. PhD thesis, Universidade de São Paulo, 2009.

[4] K Mani Chandy and W Roy Schulte. Event Processing: Designing IT Systems for Agile Companies. McGraw Hill New York, 2010.

[5] Gianpaolo Cugola and Alessandro Margara. Processing flows of information: From data stream to complex event processing. ACM Computing Surveys (CSUR), 44(3):15, 2012.

[6] Opher Etzion et al. The event processing manifesto. In Dagstuhl Seminar Proceedings (10201), pages 1–60, 2011.

[7] Inc. FireEye. Cybersecurity's Maginot Line: A Real-world Assessment of the Defense-in-Depth Model. https://www2.fireeye.com/real-world-assessment.html, 2013 (Acessado em 07/05/2015).

[8] A. L. Gonzalez, R.Willrich, D. Izidoro, and C. A. S. Santos. Representação aberta e semântica de anotações de incidentes em mapas web. Simpósio Brasileiro de Sistemas da Informação, 2013.

[9] Margarete Keiko IWAI. Um formalismo gramatical adaptativo para linguagens dependents de contexto. Departamento de Computação e Sistemas Digitais (PCS)-Escola Politécnica, Tese de Doutorado, Escola Politécnica, Universidade de São Paulo (USP), São Paulo, SP (in portuguese), 2000.

[10] S Jayson. Cost of cyber crime study: Global report. Technical report, Technical Report October, Ponemon Institute, 2013.

[11] David Luckham. The power of events, volume 204. Addison-Wesley Reading, 2002.

[12] Mandiant. M-trends: Beyond the breach (2014 threat report). Technical report, 2014.

[13] João José Neto. Contribuições à metodologia de construção de compiladores. São Paulo: Tese de Livre Docência, USP, 1993.

[14] João José Neto. Adaptive automata for context-dependent languages. ACM Sigplan Notices, 29(9):115–124, 1994.

[15] João José Neto. Adaptive rule-driven devices-general formulation and case study. In Implementation and Application of Automata, pages 234–250. Springer, 2001.

[16] João José NETO. Adaptive rule-driven devices-general formulation and case study. In Implementation and Application of Automata, pages 234–250. Springer, 2002.

[17] Hemerson PISTORI, João José NETO, and Mauro Conti PEREIRA. Adaptive nondeterministic decision trees: general formulation and case study. INFOCOMP Journal of Computer Science, 5(1):35–40, 2006.