UNIVERSIDADE FEDERAL DE SANTA MARIA
CENTRO DE TECNOLOGIA
PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA

MODELO DE DADOS DE UMA BASE DE CONHECIMENTO PARA INTERNET EARLY WARNING SYSTEMS

DISSERTAÇÃO DE MESTRADO

Giani Petri

Santa Maria, RS, Brasil

2013

MODELO DE DADOS DE UMA BASE DE CONHECIMENTO PARA INTERNET EARLY WARNING SYSTEMS

por

Giani Petri

Dissertação apresentada ao Programa de Pós-Graduação em Informática da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para a obtenção do grau de

Mestre em Ciência da Computação

Orientador: Prof. Dr. Raul Ceretta Nunes (UFSM)

Santa Maria, RS, Brasil

2013

Universidade Federal de Santa Maria
Centro de Tecnologia
Programa de Pós-Graduação em Informática

A Comissão Examinadora, abaixo assinada,
aprova a Dissertação de Mestrado

MODELO DE DADOS DE UMA BASE DE CONHECIMENTO PARA INTERNET EARLY WARNING SYSTEMS

elaborada por
Giani Petri

como requisito parcial para obtenção do grau de
Mestre em Ciência da Computação

COMISSÃO EXAMINADORA:

Raul Ceretta Nunes (UFSM), Dr.
(Presidente/Orientador)

Altair Olivo Santin, Prof. Dr. (PUCPR)

Roseclea Duarte Medina, Profª. Drª. (UFSM)

Santa Maria, 4 de Março de 2013.

*Ao meu pai **Erineu Petri** e à minha mãe **Noemi Petri**, pelo carinho e compreensão.*

AGRADECIMENTOS

Em primeiro lugar a gradeço à Deus, pelo companheirismo nos momentos bons e pela força nos momentos não tão bons.

Agradeço aos meus pais Erineu Petri e Noemi Petri, pela educação, investimento e compreensão. Somente com o amor vindo de vocês foi possível realizar mais este sonho.

Também agradeço a minha irmã e melhor amiga Giovana Petri, seu carinho, sua preocupação e suas sábias palavras, sempre nos momentos exatos, contribuíram muito nesta jornada. Obrigado Gio!

Um agradecimento em especial ao amigo, professor e orientador Dr. Raul Ceretta Nunes. Um exemplo de profissional, sempre disposto a auxiliar e resolver todos os obstáculos encontrados. Suas palavras e orientações foram fundamentais para a concretização deste trabalho.

Agradeço também aos colegas e amigos dos grupos de pesquisa GTSeg e GRECA: Bruno Augusti Mozzaquatro, Tarcisio Ceolin Junior, Ricardo Tombesi Macedo, Victor Machado Alves, Victor Orozco, Renato Preigschadt de Azevedo, Taciano Balardin de Oliveira, Gleizer Voss, Felipe Becker Nunes e Andreia Mühlbeier, pelo aprendizado e conhecimento compartilhado e também pelos vários momentos de descontração, em almoços, churrascos, eventos e viagens.

Aos demais amigos de Santa Maria que se tornaram minha segunda família, em especial ao pessoal do GFG Immer Lustig.

Agradeço ao amigo e professor Gerson Antunes Soares, pessoa fundamental na minha qualificação acadêmica e profissional.

À Capes, pelo apoio financeiro essencial para a realização deste trabalho.

Muito obrigado!

“É muito melhor arriscar coisas grandiosas, alcançar triunfos e glórias, mesmo expondo-se a derrota, do que formar fila com os pobres de espírito que nem gozam muito nem sofrem muito, porque vivem nessa penumbra cinzenta que não conhece vitória nem derrota.”

— THEODORE ROOSEVELT

RESUMO

Dissertação de Mestrado
Programa de Pós-Graduação em Informática
Universidade Federal de Santa Maria

MODELO DE DADOS DE UMA BASE DE CONHECIMENTO PARA INTERNET EARLY WARNING SYSTEMS
AUTOR: GIANI PETRI
ORIENTADOR: RAUL CERETTA NUNES (UFSM)
Local da Defesa e Data: Santa Maria, 4 de Março de 2013.

A popularização da Internet tem proporcionado um aumento no número de aplicações web que trabalham com informações críticas. Em paralelo a isso, os ataques que exploram as vulnerabilidades dessas aplicações também tem crescido. Esse cenário tem estimulado as empresas a investir em ferramentas para monitorar sua infraestrutura de rede, visando a detecção de atividades mal-intencionadas. Uma das principais ferramentas utilizadas pelas empresas para o monitoramento de suas infraestruturas de redes e identificação de ataques são os Sistemas de Detecção de Intrusão. No entanto, devido a expansão do volume de dados que trafegam nas redes de computadores, estes sistemas estão tornando-se limitados. Em contrapartida, pesquisadores têm explorado a construção de *Internet Early Warning Systems* para o monitoramento de atividades maliciosas na Internet. Este trabalho propõe a modelagem de dados de uma base de conhecimento para *Internet Early Warning Systems*. O modelo representa os dados de diferentes aspectos da rede com foco em eventos relacionados a detecção de intrusão, tais como: dados de alertas gerados por sistemas de detecção de intrusão, informações sobre medidas de respostas, estatísticas do tráfego e assinaturas de ataques já conhecidos. Um estudo de caso em uma infraestrutura de rede real demonstra a aplicabilidade do modelo de dados da base de conhecimento e permite identificar as vantagens de sua utilização. Além disso, os dados armazenados na base de conhecimento potencializam a construção de uma consciência situacional do ambiente monitorado, direcionando as atividades da equipe de segurança e auxiliando no processo de decisão de respostas a ataques em potencial.

Palavras-chave: Segurança. Base de Conhecimento. Internet Early Warning Systems. Consciência Situacional.

ABSTRACT

Master's Dissertation
Graduate Program in Computer Science
Federal University of Santa Maria

DATA MODEL OF A KNOWLEDGE BASE FOR INTERNET EARLY WARNING SYSTEMS

AUTHOR: GIANI PETRI
ADVISOR: RAUL CERETTA NUNES (UFSM)
Defense Place and Date: Santa Maria, March 4th, 2013.

The popularization of the Internet has provided an increase in the number of web applications that work with critical information. Parallel to this, attacks that exploit the vulnerabilities of these applications has also grown. This scenario has stimulated companies to invest in tools to monitor their network infrastructure in order to detect malicious activity. One of the main tools used by companies to monitor their network infrastructures and identifying attacks are Intrusion Detection Systems. However, due to expansion of the volume of data in computer networks, these systems are becoming limited. In contrast, researchers have explored the construction of Internet Early Warning Systems to monitor malicious activities on the Internet. This work proposes a data model of a knowledge base for Internet Early Warning Systems. The model represents the data of different aspects of the network with a focus on events related to intrusion detection, such as data of alerts generated by intrusion detection systems, information on response measures, traffic statistics and signatures of known attacks. A case study on a real network infrastructure demonstrates the applicability of the data model of knowledge base and identifies the advantages of its use. Furthermore, the data stored in the knowledge base potentializes the construction of situational awareness of monitored environment, directing the activities of the security team and helping in the decision process responses to potential attacks.

Keywords: Security. Knowledge Base. Internet Early Warning Systems. Situational Awareness.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ATM	*Asynchronous Transfer Mode*
CGI	*Common Gateway Interface*
Coperves	Comissão Permanente do Vestibular
CPD	Centro de Processamento de Dados
DoS	*Denial of Service*
HIDS	*Host Intrusion Detection System*
HTTP	*Hypertext Transfer Protocol*
HTTPS	*Hypertext Transfer Protocol Secure*
IAS	*Internet Analysis System*
ICMP	*Internet Control Message Protocol*
IDS	*Intrusion Detection System*
IDMEF	*Intrusion Detection Message Exchange Format*
IDREF	*Intrusion Detection Response Exchange Format*
IDWG	*Instrusion Detection Work Group*
IETF	*Internet Engineering Task Force*
IP	*Internet Protocol*
KBAM	*Knowledge Base Attack Monitoring*
MAC	*Media Access Control*
NIDS	*Network Intrusion Detection System*
SA	*Situational Awareness*
SIP	*Session Initiation Protocol*
SMTP	*Simple Mail Transfer Protocol*
SMTPS	*Simple Mail Transfer Protocol Secure*
SNMP	*Simple Network Management Procotol*
TCP	*Transmission Control Protocol*
UDP	*User Datagram Protocol*
UFSM	Universidade Federal de Santa Maria
URL	*Uniform Resource Locator*
VM	*Virtual Machine*
XML	*Extensible Markup Language*

SUMÁRIO

1 INTRODUÇÃO

A popularização da Internet está em constante evolução, na medida em que provê diversos serviços que auxiliam na comunicação, na efetivação de negócios, transações comerciais, além da realização de tarefas pessoais. Esses serviços, geralmente, são realizados através de aplicações *web* que, normalmente, trabalham com informações críticas e que são estratégicas para as organizações. No entanto, o número de ataques que visam explorar as vulnerabilidades encontradas nessas aplicações *web* tem crescido gradativamente nos últimos anos (SYMANTEC, 2012).

De mesmo modo, conforme o Centro de Estudos, Resposta e Tratamento de Incidentes no Brasil (CERT.BR, 2012), o número acumulado de ataques notificados no ano de 2011 é de 399.515. E, em 2012 as notificações de ataques tendem a aumentar, até o mês de agosto tem-se um montante de 303.445, como pode ser observado na Figura 1.1.

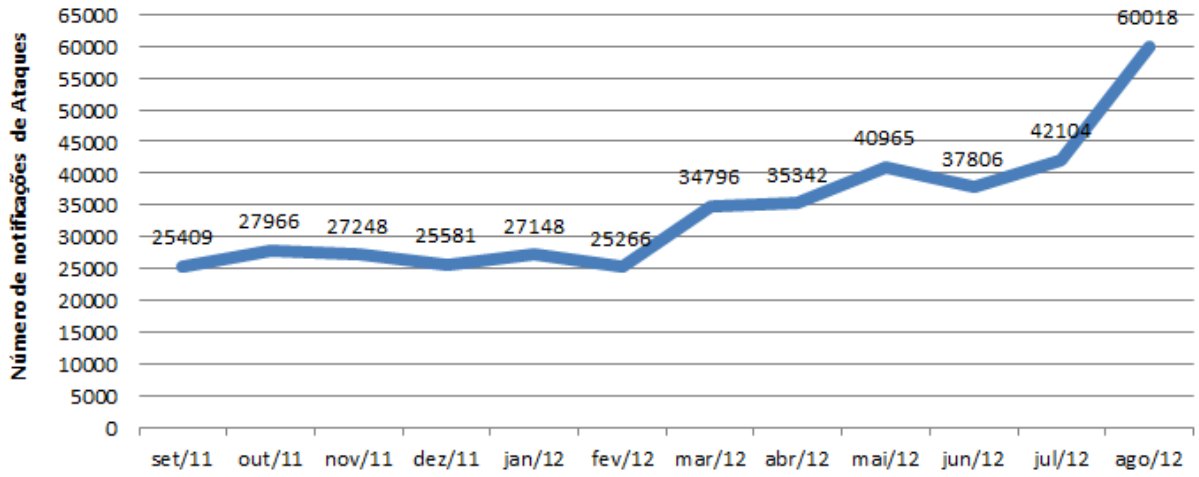


Figura 1.1: Notificações de ataques entre os meses de Setembro de 2011 e Agosto de 2012 (adaptado de (CERT.BR, 2012)).

Diante desta ascensão no número de ataques, as empresas e organizações estão se conscientizando e estimulando a investir em técnicas e ferramentas que as auxiliem a monitorar seus sistemas de informações e sua infraestrutura de redes de computadores. Estas ferramentas são utilizadas para a identificação de atividades maliciosas, objetivando manter as informações íntegras, com um alto nível de confidencialidade e disponibilidade.

Uma das principais ferramentas utilizadas pelas empresas para o monitoramento de suas infraestruturas de redes e identificação de ataques são os Sistemas de Detecção de Intrusão (IDS). Um IDS é um sistema responsável por identificar possíveis tentativas de ataques em

redes de computadores ou em um computador em específico (KIZZA, 2005).

Na medida em que a Internet tem se popularizado, há também um acréscimo significativo no número de dados que trafegam nas redes de computadores. Conforme (GOGULF, 2012), em 60 segundos o mecanismo de busca do Google[1] atende a mais de 600 mil consultas e um montante superior a 168 milhões de e-mails são enviados. Diante desse cenário, Golling e Stelte (2011) citam que os IDSs tradicionais estão tornando-se limitados. A quantidade de dispositivos conectados à rede, *petabytes* de dados, *gigabytes* de informações transferidas já não estão mais sendo suportadas pelos IDSs tradicionais (GOLLING; STELTE, 2011).

No entanto, para suprir a necessidade de monitorar a Internet perante esse novo cenário, a construção de *Internet Early Warning Systems* tem sido explorada (HESSE; POHLMANN, 2008) (BASTKE; DEML; SCHMIDT, 2010). Estes sistemas objetivam detectar ameaças precocemente, visando proteger as funcionalidades da Internet, antes que as ameaças causam qualquer perigo, ou antes que elas possam causar o máximo de perigo. Além disso, permitem obter uma consciência situacional (percepção da situação de segurança dos recursos de rede) que possibilita uma reação precoce a um evento malicioso, um maior controle e monitoramento dos recursos envolvidos, auxiliando em tomadas de decisões (GOLLING; STELTE, 2011).

Diante deste cenário, as tarefas de monitorar infraestruturas de redes e obter um conhecimento dos eventos maliciosos que estão ocorrendo tornam-se imprescindíveis para as empresas e organizações. Assim sendo, este trabalho propõe um modelo de dados de uma base de conhecimento que representa os dados de diferentes aspectos de uma rede de computadores e que potencializa as equipes de segurança na compreensão das atividades ocorridas no ambiente monitorado.

1.1 Motivação

Uma base de conhecimento é um dos principais componentes técnicos de um *Internet Early Warning System*, por manter informações que possibilitam ações mais efetivas no monitoramento de ataques. Deste modo, Bastke et al. (2010) definem os aspectos que uma base de conhecimento deve armazenar. Estes aspectos correspondem aos dados sobre o comportamento da rede, informações sobre assinaturas de ameaças, incidentes e medidas de respostas (BASTKE; DEML; SCHMIDT, 2010).

No entanto, os trabalhos existentes na literatura não englobam todos os aspectos de uma

[1] http://www.google.com

base de conhecimento para *Internet Early Warning Systems*, dificultando a construção de uma consciência situacional do ambiente monitorado. Em (LIMA; DEGASPARI; SOBRAL, 2008) é proposto uma abordagem para detecção de intrusão utilizando redes neurais artificiais como mecanismo de detecção e uma base de conhecimento contendo assinaturas de ataques conhecidos para a fase de treinamento e aprendizagem, desconsiderando informações sobre medidas de respostas.

Em (FLIOR et al., 2010) é apresentado um sistema que captura e analisa o tráfego de rede com o objetivo de criar uma base de conhecimento com regras que permita a tomada de decisões, porém esta proposta desconsidera o armazenamento de registros de incidentes. Em (MORE; MATTHEWS; A. JOSHI, 2012) é proposta uma abordagem baseada em conhecimento para a modelagem de detecção de intrusão, mas essa abordagem também não engloba medidas de respostas.

Em síntese, existem diversos trabalhos que envolvem bases de conhecimento na literatura, entretanto, os mesmos não abordam os aspectos necessários de uma base de conhecimento para *Internet Early Warning Systems*.

No entanto, a motivação deste trabalho visa explorar um modelo de dados de uma base de conhecimento para *Internet Early Warning Systems*, que armazene informações que possibilitam a construção da consciência situacional do ambiente monitorado e auxilie no processo de decisão de medidas de respostas a ataques.

1.2 Objetivos e Contribuições

O objetivo deste trabalho é apresentar um modelo de dados de uma base de conhecimento chamada KBAM (*Knowledge Base Attack Monitoring*), que engloba os diferentes aspectos de uma base de conhecimento para *Internet Early Warning Systems*.

A base de conhecimento KBAM representa os dados de eventos de detecção de intrusão explorando o padrão de formatação de dados *Intrusion Detection Message Exchange Format* (IDMEF) (DEBAR; CURRY; FEINSTEIN, 2007) para as mensagens de detecção de intrusão e o formato *Intrusion Detection Response Exchange Format* (IDREF) (SILVA; WESTPHALL, 2006) para as mensagens de respostas. A representação dos dados contidos na base de conhecimento KBAM contempla os seguintes aspectos: dados de alertas gerados por sistemas de detecção de intrusão, informações sobre as medidas aplicadas em resposta a um alerta, além dos parâmetros para captura do tráfego da rede, conforme destacados em (RICCI, 2008).

A principal contribuição deste trabalho é o modelo de dados da base de conhecimento KBAM que ao representar os dados de diferentes aspectos de uma rede, explorando padrões utilizados por sistemas de detecção de intrusão, permite a construção de uma consciência situacional do ambiente de rede monitorado. A prova de conceito foi realizada através de um estudo de caso implementado na rede da Universidade Federal de Santa Maria que demonstra que o uso da base KBAM permite a obtenção de uma consciência situacional do ambiente de rede da instituição, pois fornece informações que possibilitam um conhecimento da atual situação de segurança da rede, direcionando as atividades da equipe de segurança e auxiliando no processo de decisão de respostas a ataques em potencial.

1.3 Organização do Texto

O texto da dissertação está organizado da seguinte forma. O Capítulo 2 apresenta uma fundamentação teórica que aborda os conceitos importantes para a compreensão do trabalho. O Capítulo 3 apresenta a proposta do modelo de dados da base de conhecimento KBAM, destacando as principais entidades e atributos, além de apresentar os trabalhos relacionados encontrados na literatura. No Capítulo 4 é apresentado um estudo de caso que demonstra a inserção da base de conhecimento KBAM em uma infraestrutura de redes e a construção da consciência situacional do ambiente de rede da instituição a partir dos dados armazenados na base de conhecimento KBAM. Por fim, o Capítulo 5 apresenta as conclusões do trabalho e sugestões de trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

O acréscimo no número de notificações de ataques registrados nos últimos anos (CERT.BR, 2012) têm conscientizado as empresas a implantar ferramentas de monitoramento que permitam a identificação de atividades maliciosas em suas infraestruturas de redes.

Nesse contexto, este capítulo apresenta conceitos importantes para a compreensão deste trabalho. A Seção 2.1 apresenta uma conceituação sobre as características dos *Internet Early Warning Systems* e seus componentes técnicos. Na sequência, a Seção 2.2 apresenta uma breve descrição sobre os tradicionais Sistemas de Detecção de Intrusão. Na Seção 2.3 é descrito alguns padrões de formatação de dados para sistemas de detecção de intrusão. Na Seção 2.4 é apresentado os conceitos sobre bases de conhecimento e a Seção 2.5 destaca as considerações parciais do capítulo.

2.1 Internet Early Warning Systems

Um *Internet Early Warning System* visa a detecção precoce de eventos que ameaçam as funcionalidades da Internet (BASTKE; DEML; SCHMIDT, 2010). Devido a grande complexidade das redes de computadores atuais, esses sistemas integram sensores distribuídos em uma rede e trabalham no monitoramento e detecção de eventos que possam causar algum perigo.

Conforme Bastke et al. (2010), o objetivo desses sistemas é construir uma consciência situacional e gerar contramedidas para ameaças atuais com base nas informações adquiridas na consciência situacional do ambiente monitorado. Além disso, esses sistemas também objetivam coletar e analisar informações para suportar a criação de medidas de segurança. Em resumo, a definição de um *Internet Early Warning System* é representado pela fórmula que segue:

$$F = (N, P, O, L, G, C) \tag{2.1}$$

Onde:

- N = Rede monitorada.
- P = Organizações que fazem parte do sistema.
- O = Definição das estruturas e processos organizacionais.
- L = Enquadramento jurídico.

- G = Objetivos a serem alcançados por um *Internet Early Warning System*.
- C = Componentes Técnicos de um *Internet Early Warning System*.

O elemento (*N*) descreve a rede monitorada, no caso de um *Internet Early Warning System*, a Internet. O segundo elemento representado por (*P*) refere-se ao conjunto de organizações e pessoas ativamente ou passivamente envolvidas com o sistema. O componente (*O*) representa a organização de um *Internet Early Warning System*, que pode ser dividida em estrutura organizacional e estrutura operacional. A estrutura organizacional define as unidades organizacionais de um *Internet Early Warning System* e seus relacionamentos entre si. Já a estrutura operacional define os processos necessários para a operação de um *Internet Early Warning System*. O elemento representado por (*L*), refere-se ao enquadramento jurídico onde destacam até que ponto as leis existentes apoiam a operação de um *Internet Early Warning System*. O elemento (*G*) representa os objetivos a serem alcançados na operação de um *Internet Early Warning System*. Por fim, o elemento (*C*) identifica os componentes técnicos que compõem a arquitetura e estão descritos na Seção 2.1.1.

2.1.1 Componentes Técnicos

Um *Internet Early Warning System* é formado por diversos componentes técnicos: sensores, componente de detecção, base de conhecimento, componente de reação e gerenciamento de incidentes, componente de perpetuação de evidências e componente de distribuição das informações (BASTKE; DEML; SCHMIDT, 2010).

Os sensores são utilizados para a geração da visão da atual situação do ambiente monitorando, criando a consciência situacional. Além disso, são responsáveis pela detecção dos eventos de segurança e identificação de novas ameaças. O componente de detecção é dividido em duas camadas: a camada de sinal, onde os dados da rede ou os logs são analisados por métodos de detecção por anomalia ou assinaturas, e a camada de eventos, onde ocorre o relacionamento dos eventos da camada de sinal com eventos reportados por órgãos externos.

A base de conhecimento é um dos principais componentes de um *Internet Early Warning System*, pois armazena informações de diferentes aspectos da rede. As assinaturas de ameaças, o comportamento da rede, as informações sobre os incidentes e suas medidas de respostas estão armazenadas na base de conhecimento e dão suporte a construção da consciência situacional do ambiente monitorado.

O componente de reação e gerenciamento de incidentes é conectado a base de conhecimento

e dá suporte aos usuários ao processo de tomada de decisão, sugerindo etapas para a análise da situação do incidente e tipo da contramedida a ser aplicada. Por sua vez, o componente de perpetuação de evidências objetiva o armazenamento de informações que podem ser usadas em processos criminais. O componente de distribuição de informações é responsável por distribuir os dados de incidentes, contramedidas e alertas a todos os usuários do sistema, de forma rápida e precisa (BASTKE; DEML; SCHMIDT, 2010).

A Figura 2.1 apresenta graficamente os elementos que compõem um *Internet Early Warning System* e seus relacionamentos.

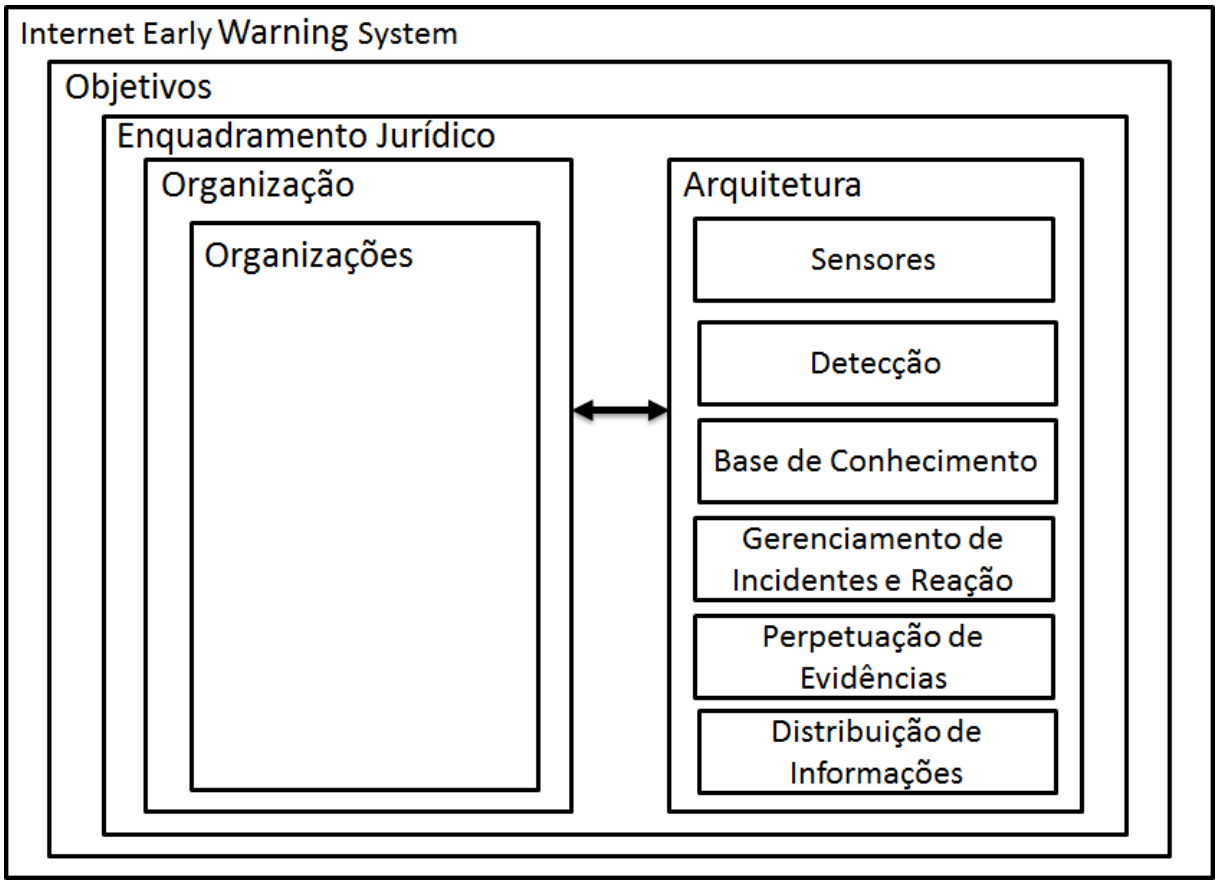


Figura 2.1: Elementos de um *Internet Early Warning System* (adaptado de (BASTKE; DEML; SCHMIDT, 2010)).

2.1.2 Consciência Situacional

A consciência situacional (*Situational Awareness* - SA) é um termo antigo, que se originou de pesquisas em fatores humanos nas áreas de espaço aéreo, aviação e operações militares (LIU et al., 2007).

Diversos autores conceituam o termo consciência situacional relacionando-o a áreas específicas. De uma perspectiva militar, a consciência situacional significa o conhecimento do nível

de ameaça e o *status* atual dos ativos de rede que suportam operações militares (GREGOIRE; BEAUDOIN, 2005).

O conceito de consciência situacional foi introduzido na área de segurança de redes por Bass (1999). Bass relaciona o termo em combinação com a integração de dados de sistemas de detecção de intrusão distribuídos (BASS, 1999).

Nos últimos anos, a aplicação de consciência situacional tem sido revolucionária, principalmente nas áreas de defesa do espaço e controle do tráfego aéreo. Em contrapartida, a aplicação do termo na área de segurança de redes ainda está em estágios iniciais (ONWUBIKO, 2009).

A definição de consciência situacional mais utilizada foi escrita por Endsley (1995), que a define informalmente, como um entendimento do que está acontecendo. E, formalmente, como a percepção dos elementos do ambiente considerando o tempo e o espaço, a compreensão de seus significados e a projeção de medidas futuras (WICKENS, 2008).

Um modelo proposto por Endsley (1995) define a consciência situacional em três níveis hierárquicos, conforme apresenta a Figura 2.2.

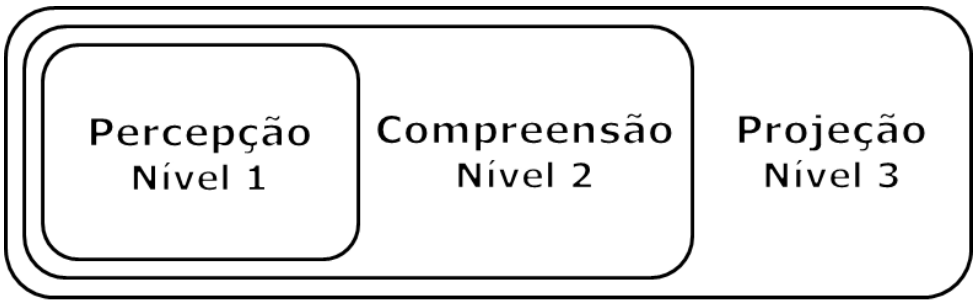


Figura 2.2: Modelo de consciência situacional em três níveis (adaptado de (LIU et al., 2007)).

O primeiro nível do modelo de Endsley refere-se a percepção. De acordo com Salerno et al. (2004), a percepção fornece informações sobre o *status* e atributos dos elementos do ambiente. A percepção é adquirida através de alertas reportados por sistemas de detecção de intrusão, logs de *firewalls* ou ainda através de evidências de segurança que reportaram alertas ou geraram logs (ONWUBIKO, 2009).

O segundo nível refere-se a compreensão dos eventos que estão ocorrendo no ambiente. Conforme Onwubiko (2009), a compreensão é adquirida através de metodologias, técnicas, processos e procedimentos que a equipe de segurança utiliza para analisar, sintetizar e agregar evidências percebidas nos elementos de rede. Além disso, a compreensão consiste na criação de uma imagem da situação de segurança do ambiente e quando novas evidências são capturadas deve-se atualizar a base de conhecimento para refletir as mudanças (SALERNO; HINMAN;

BOULWARE, 2004).

A projeção é o terceiro nível do modelo de Endsley (1995) e corresponde a capacidade de fazer futuras predições ou previsões baseada no conhecimento extraído do ambiente monitorado. Nesta etapa os analistas de segurança realizam a criação de padrões de ocorrência de eventos, além da criação de controles preventivos para conter situações em potencial.

Uma extensão ao modelo de Endsley (1995) foi proposta por McGuiness e Foy (2000), adicionando um quarto nível ao modelo original. O nível adicionado refere-se a resolução e corresponde a implementação de contramedidas necessárias para tratar os riscos identificados. A Tabela 2.1 apresenta um resumo dos níveis do modelo de Endsley (1995) com a extensão proposta por McGuiness e Foy (2000).

Tabela 2.1: Resumo dos níveis do modelo de Endsley e extensão de McGuiness e Foy.

Nível	**O quê?**	**Como?**
Percepção - Nível 1	Eventos, estados, valores	Detecção, identificação
Compreensão - Nível 2	Significados, tipos de situação	Interpretação, sínteses
Projeção - Nível 3	Projeto	Predição, dados históricos
Resolução - Nível 4	Implementação	Aplicação prática

De modo que as redes de computadores são ambientes dinâmicos, a aplicação de cada etapa do modelo de consciência situacional deve ocorrer em paralelo com os outros níveis (SALERNO et al., 2003), ou seja, enquanto a equipe de segurança está trabalhando em uma determinada etapa, os outros níveis devem estar ocorrendo em paralelo, identificando novos eventos. Esta característica potencializa a construção da consciência situacional do ambiente que se está monitorando, através da atualização contínua com os novos eventos detectados.

2.2 Sistemas de Detecção de Intrusão

A detecção de intrusão refere-se a técnicas utilizadas para a identificação de intrusões e ataques em computadores específicos ou em redes de computadores. Kizza (2005) define uma intrusão como uma tentativa ilegal e deliberada, bem sucedida ou não, de manipulação, quebra ou rompimento do funcionamento de um sistema.

Um Sistema de Detecção de Intrusão (IDS) é constituído por três componentes funcionais (NORTHCUTT; NOVAK, 2002): fonte de informação, análise e resposta. A fonte de informação é composta por um coletor de dados, responsável por capturar informações do tráfego da rede para serem utilizadas pelo analisador. A análise é o componente responsável por verificar os dados advindos da fonte de informação, objetivando encontrar sinais que indiquem a tentativa

ou ocorrência de uma intrusão, utilizando para isso mecanismos de comparação. O componente de resposta é responsável por executar medidas de reações a intrusões com base nos resultados da análise, essas medidas podem ser através de contra-ataques, bloqueio de recursos ou então, simplesmente gerando alarmes e relatórios para uma intervenção de um administrador de rede.

Um IDS é classificado em duas categorias conforme a sua fonte de informações (NORTHCUTT; NOVAK, 2002): Sistemas de Detecção de Intrusão baseados em Host (HIDS) e Sistemas de Detecção de Intrusão baseados em Rede (NIDS).

Um Sistema de Detecção de Intrusão baseado em Host é uma ferramenta de segurança utilizada para a identificação de atividades maliciosas em um computador específico (KIZZA, 2005). Um HIDS é responsável por monitorar as atividades do sistema operacional e dos programas de um único computador. O sistema compara as alterações em arquivos ou parâmetros monitorados com as assinaturas predefinidas e em caso de similaridade gera um alerta indicando uma atividade maliciosa.

Diferentemente de um HIDS, um Sistema de Detecção de Intrusão baseado em Rede trabalha no monitoramento de toda uma rede, objetivando a detecção de anomalias, ataques e atividades ilegais (KIZZA, 2005). Um NIDS trabalha com a análise de informações capturadas por um coletor em uma rede. A análise é realizada a partir do volume do tráfego, da quantidade de conexões além do número de pacotes perdidos.

Além da classificação conforme a fonte de informação, os IDSs também são classificados em duas categorias conforme seu método de detecção: Sistemas de Detecção de Intrusão baseados em Assinatura e Sistemas de Detecção de Intrusão baseados em Anomalias. Estas duas classificações são apresentadas, respectivamente, nas Seções 2.2.1 e 2.2.2.

2.2.1 Sistemas de Detecção de Intrusão baseados em Assinatura

Um Sistema de Detecção de Intrusão baseado em Assinatura trabalha com a comparação dos dados coletados em uma determinada rede com a base de dados de assinaturas conhecidas. Um alerta é gerado pelo IDS quando os dados coletados são compatíveis com alguma regra predefinida (KIZZA, 2005). Entre os IDSs baseados em assinaturas destacam-se o Snort (SNORT, 2012a), Bro (BRO, 2012) e Suricata (SURICATA, 2012).

Uma das principais desvantagens de um IDS baseado em assinatura refere-se a necessidade de constante atualização da base de dados de assinaturas, devido ao surgimento de novas variações de ataques. Além disso, estes sistemas tem dificuldade na detecção de ataques desco-

nhecidos.

A principal vantagem de um IDS baseado em assinatura refere-se a sua alta taxa de detecção. Ao utilizar uma base de dados de assinaturas atualizadas os IDSs tornam-se bastante precisos em suas detecções, apresentando um baixo número de falsos positivos (KIZZA, 2005).

2.2.2 Sistemas de Detecção de Intrusão baseados em Anomalia

A detecção de intrusão baseada em anomalias trabalha com a ideia de que um ataque cria um comportamento diferente do padrão definido para o sistema (KRUEGEL; VALEUR; VIGNA, 2004). O perfil do sistema é criado com base em informações históricas e quando o comportamento observado desvia do padrão é então detectado um ataque e disparado um alerta.

Uma das principais características na detecção baseada em anomalias corresponde a detecção de ataques desconhecidos, diferentemente da abordagem por assinaturas. Porém, o tráfego de rede apresenta alta variabilidade e, muitas vezes, pode erroneamente ser identificado como uma anomalia, gerando um alerta falso (KIZZA, 2005).

A detecção baseada em assinatura é adequada para a detecção de ataques definidos. No entanto, a abordagem por anomalias destaca-se pela detecção de ataques sem conhecimento prévio. Levando em consideração a constante variação de ataques existentes e o rápido surgindo de novos ataques, destaca-se a utilização de IDSs híbridos, que trabalham com as duas abordagens de detecção, integrando as vantagens na utilização de ambas as tecnologias.

2.3 Padrões de Formatação de Dados para Sistemas de Detecção de Intrusão

Na área de detecção de intrusão existem alguns padrões para interoperabilidade de mensagens de detecção e de respostas a intrusões. Estes padrões definem uma formatação dos dados a serem compartilhados entre os componentes de um sistema ou reportados a entidades externas.

2.3.1 O Formato IDMEF

Criado pelo grupo IDWG (*Intrusion Detection Work Group*) do IETF (*Internet Engineering Task Force*), o IDMEF (*Intrusion Detection Message Exchange Format*) (DEBAR; CURRY; FEINSTEIN, 2007) é um formato de dados padrão que sistemas de detecção de intrusão utilizam para reportar e compartilhar alertas sobre eventos considerados suspeitos. O principal objetivo do formato IDMEF é definir uma formatação de dados e procedimentos para a interoperabilidade entre sistemas de detecção de intrusão.

Umas das principais aplicações do formato IDMEF é para a comunicação de alertas entre o componente de análise e o gerenciador de um IDS. Além disso, o formato IDMEF também pode ser usado para a troca de informações e correlação de alertas, além da possibilidade de padronização de informações em um banco de dados.

O formato IDMEF possui uma classe que é base para todo o modelo (*IDMEF-Message*) e todas as outras classes derivam desta classe base. A classe *IDMEF-Message* possui duas classes especializadas que agregam uma série de classes, são elas: *Alert* e *Heartbeat*. O relacionamento entre as classes principais e as classes agregadas é sumariamente representado na Figura 2.3.

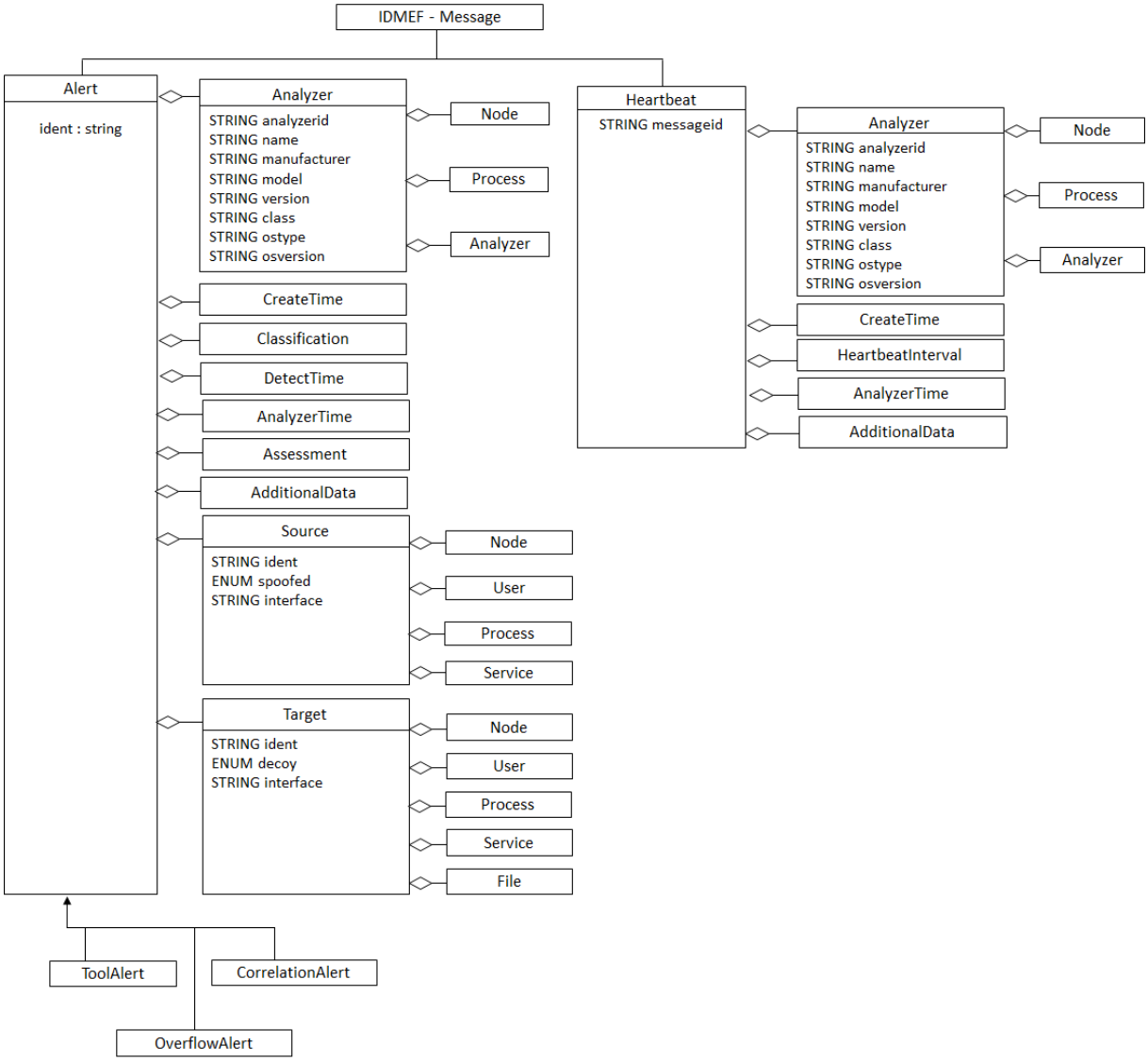


Figura 2.3: Visão geral do formato IDMEF (adaptado de (SÁ BRANDÃO, 2007)).

Conforme apresenta a Figura 2.3, as classes *Alert* e *Heartbeat* são subordinadas a classe base *IDMEF-Message*. Uma mensagem de *Heartbeat* é utilizada pelos analisadores para indicar seu estado de funcionamento atual para os gerenciadores. Uma mensagem enviada em um período

de tempo regular indica que o analisador está instalado e funcionando corretamente, por outro lado, a falta de uma ou mais mensagem(ns) de *heartbeat* indica que o analisador, ou sua conexão de rede, falhou.

A mensagem *Alert* representa um evento de segurança disparado por um IDS. A mensagem deve conter a descrição do analisador, representado pela classe *Analyzer*, o instante de criação da mensagem pelo analisador, classe *CreateTime* e uma possível classificação para o evento, determinada na classe nomeada *Classification*. Algumas informações das mensagens de detecção de intrusão não se encaixam no formato original do IDMEF, assim sendo, tais informações são representadas na classe *AdditionalData*. O momento em que o evento que gerou o alerta foi detectado, representado na classe *DetectTime*, o momento de envio da mensagem de alerta pelo analisador, classe *AnalyzerTime*, a possível origem do evento (*Source*) e a identificação do possível alvo do evento (*Target*), também fazem parte da mensagem de alerta.

O formato também representa, através da classe *Assessment*, informações que permitem uma avaliação do evento que gerou o alerta. Além disso, é possível determinar o impacto do evento, ou seja, se o mesmo teve um impacto alto, médio ou baixo sobre o sistema, além de representar as ações realizadas pelo analisador em resposta ao evento e determinar o nível de confiança na avaliação das informações fornecidas pelo analisador.

A classe *ToolAlert* representa informações referentes a ataques realizados por programas ou ferramentas. Já a classe *CorrelationAlert* adiciona informações para agrupar alertas relacionados. A Classe *OverflowAlert* representa as informações de um ataque específico do tipo *overflow*.

A classe *Alert* ainda possui outras classes agregadas, conforme apresenta a Figura 2.3. Deste modo, possibilita uma flexibilidade do formato IDMEF para a inserção de novas especificações conforme a necessidade do alerta.

2.3.2 O Formato IDREF

Outro formato de dados que objetiva dar continuidade nos trabalhos desenvolvidos pelo grupo IDWG, criando mecanismos de envio de respostas aos alertas identificados, é o formato IDREF (*Intrusion Detection Response Exchange Format*) (SILVA; WESTPHALL, 2006). O IDREF é compatível com o formato de alertas IDMEF, possibilitando assim, a integração dos dois formatos.

De forma similar ao formato IDMEF, o IDREF também é representado em classes. A Figura

2.4 apresenta as principais classes do formato IDREF.

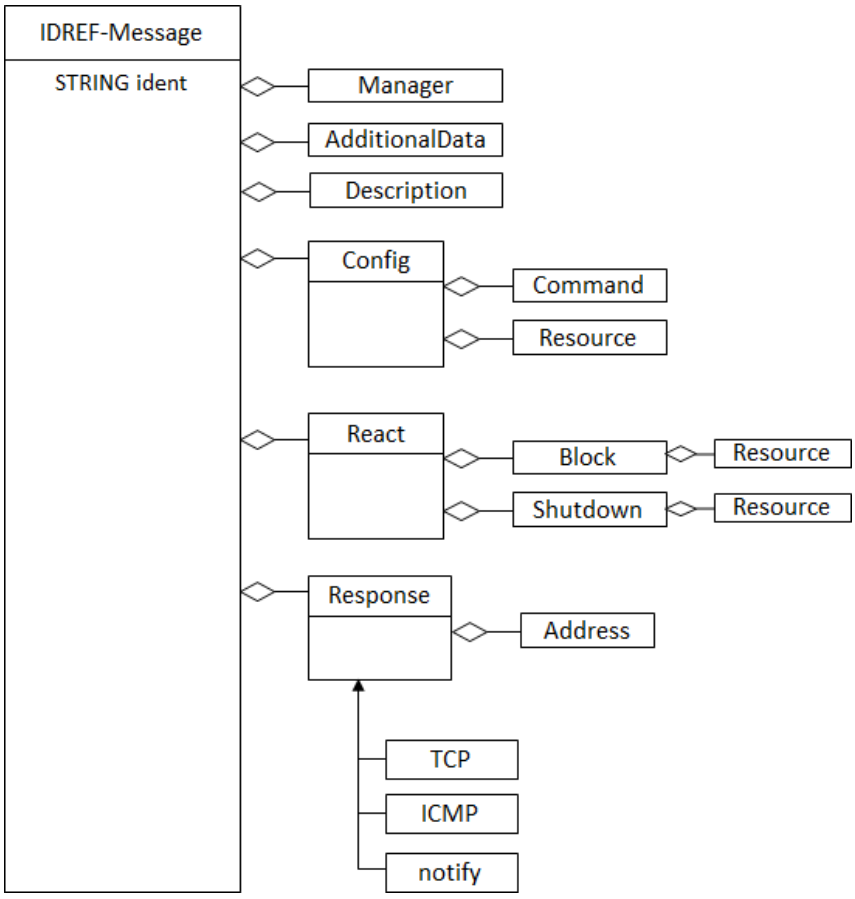


Figura 2.4: Visão geral do formato IDREF (adaptado de (SILVA, 2004)).

A classe base do padrão IDREF é nomeada *IDREF-Message*, ela possui três classes derivadas (*Response*, *React* e *Config*), representando os tipos de respostas que o modelo IDREF suporta. Além disso, possui algumas classes agregadas, *AdditionalData*, *Description* e *Manager*. A classe *AdditionalData* possui a mesma função do formato IDMEF, ou seja, armazenar informações adicionais que não estão representadas no modelo. A classe *Description* armazena uma simples descrição da resposta que está sendo aplicada. E a classe *Manager* contém informações sobre o gerenciador que enviou a resposta.

O primeiro tipo de resposta está representado pela classe *Response*, que representa o envio de informações cujo objetivo é avisar ou controlar um ataque. Esta classe possui três classes especializadas, são elas (*TCP*, *ICMP* e *notify*) e uma classe agregada (*Address*). As classes *TCP* e *ICMP* representam, respectivamente, o envio de pacotes TCP e mensagem ICMP em resposta a um alerta ocorrido. Por sua vez, a classe *notify* armazena uma *string* que contém informações referentes ao ataque, podendo conter o próprio alerta no formato IDMEF que gerou a resposta, além disso, é responsável por comunicar interfaces externas sobre a existência de um ataque.

A classe agregada *Address* representa as informações referentes ao endereço de destino que a resposta será aplicada, o tipo do endereço é representado no atributo *type*.

Outro tipo de resposta suportado pelo formato IDREF é representado pela classe *Config*. A classe *Config* possibilita a alteração de configurações de um recurso do ambiente para conter um ataque. A classe possui duas classes agregadas: *Command* e *Resource*. A classe *Command* representa o(s) comando(s) a ser(em) executado(s) pelo recurso a ser configurado e a classe *Resource* determina o recurso a ser configurado.

Além de permitir o envio de informações e a alteração de configurações, o formato IDREF também permite a reação do ambiente contra um ataque. Este tipo de resposta é representado pela classe *React* que possui duas classes agregadas, são elas: *Block* e *Shutdown*. A classe *Block* representa o bloqueio de algum recurso. Já a classe *Shutdown* determina o fechamento de algum recurso. Um recurso bloqueado não pode ser utilizado por um determinado período de tempo, já um recurso fechado só poderá ser utilizado após ser aberto novamente.

A classe *Resource* está agregada as classes *Block* e *Shutdown* e representa um recurso ao qual a resposta será aplicada. Um recurso pode ser um nó ou um serviço da rede, uma lista de usuário, uma lista de arquivos ou um processo do sistema operacional. Estes recursos são representados, respectivamente, pelas classes: *Node*, *Service*, *UserList*, *FileList* e *Process*.

2.4 Base de Conhecimento

Uma base de conhecimento é um repositório centralizado de informações relacionadas a um assunto em específico de um sistema de informação ou de uma organização (RUSSEL; NORVING, 2003). Sendo parte integrante de um sistema de gestão do conhecimento, uma base de conhecimento é utilizada para o agrupamento de informações relativas a uma determinada área e que auxilia pessoas e organizações no acesso facilitado a essas informações.

Uma base de conhecimento fornece um meio das informações serem coletadas, organizadas, compartilhadas e utilizadas, podendo ser legível por máquina (Seção 2.4.1) ou destinada ao uso humano (Seção 2.4.2) (RUSSEL; NORVING, 2003).

2.4.1 Base de Conhecimento Legível por Máquina

Uma base de conhecimento legível por máquina é formada por um conjunto de regras definidas que descrevem o conhecimento de uma forma lógica e consistente possuindo um raciocínio dedutivo automatizado. Este tipo de base de conhecimento normalmente é utilizado na área de

inteligência artificial, integradas a um sistema especialista concentrado em um domínio específico (RUSSEL; NORVING, 2003).

Geralmente na construção de uma base de conhecimento legível por máquina é aplicada uma ontologia que é utilizada para definir a estrutura dos dados que serão armazenados na base de conhecimento. A ontologia deve conter as definições dos tipos de entidades que serão armazenadas, além de seus atributos e relacionamentos (GRUBER, 1995).

2.4.2 Base de Conhecimento Destinada ao uso Humano

Uma base de conhecimento destinada ao uso humano é projetada para auxiliar na recuperação e no uso do conhecimento nela armazenado. Normalmente é utilizada em sistemas de *help desk*, ou no compartilhamento de informações empresariais, armazenando informações sobre resolução de problemas, artigos, manuais, dados históricos e até mesmo respostas a perguntas frequentes (RUSSEL; NORVING, 2003).

Este tipo de base de conhecimento é interativa, onde os usuários buscam as soluções para os problemas existentes, mas dependem da inserção de informações através da interação humana, que posteriormente é utilizada na resoluções de novos problemas.

2.5 Considerações Parciais

Esse capítulo apresentou os conceitos importantes para a compreensão do trabalho, onde foram descritas as características e os elementos que compõem um *Internet Early Warning System*. Como observado, um *Internet Early Warning System* é formado por diversos elementos e componentes técnicos que juntos trabalham no monitoramento de atividades maliciosas e na construção da consciência situacional do ambiente monitorado. Como foi destacado, a base de conhecimento é um dos principais componentes técnicos de um *Internet Early Warning System*, pois guarda informações essenciais para criar a consciência situacional, que corresponde a percepção e compreensão dos eventos ocorridos no ambiente monitorado.

Além disso, foram detalhados os sistemas de detecção de intrusão, apresentando as características e classificação dos IDSs quanto a fonte de informação e conforme o método de detecção. Do mesmo modo, foram descritos os padrões de formatação de dados de mensagens de detecção de intrusão e de respostas, destacando as principais classes que integram os formatos. Os padrões de formatação de dados são utilizados para a interoperabilidade entre os componentes e também para serem reportados a entidades externas. Por fim, foi apresentada uma classificação

de uma base de conhecimento, podendo ser legíveis por máquina, onde possui uma ontologia que define a estruturação dos dados, ou destinada ao uso humano, armazenando dados úteis de áreas específicas.

3 MODELO DE DADOS DE UMA BASE DE CONHECIMENTO PARA INTERNET EARLY WARNING SYSTEMS

Neste capítulo é apresentado o modelo de dados da base de conhecimento KBAM, que engloba os diferentes aspectos de uma base de conhecimento para *Internet Early Warning Systems*.

A Seção 3.1 apresenta a proposição do modelo de dados da base de conhecimento KBAM e destaca sumariamente os aspectos que a compõem. Na Seção 3.2 é descrita a forma em que os aspectos estão representados na base de conhecimento. A Seção 3.3 apresenta detalhadamente a modelagem dos dados que compõem a base de conhecimento KBAM, destacando as entidades, atributos e os relacionamentos. Por fim, a Seção 3.4 apresenta os trabalhos relacionados encontrados na literatura.

3.1 Proposta

O cenário atual da Internet tem demandado um esforço dos cientistas para a criação de novas ferramentas que permitam monitorar as atividades maliciosas que ocorrem nas redes de computadores, buscando um aumento no nível de segurança. Neste contexto, a construção de *Internet Early Warning Systems* tem sido investigada. De modo a manter as funcionalidades da Internet operando corretamente, através da geração de alertas precocemente utilizando sensores distribuídos, estes sistemas trabalham com diversos componentes técnicos que juntos realizam um efetivo monitoramento e permitem a construção da consciência situacional do ambiente.

Um dos principais componentes técnicos de um *Internet Early Warning System* é a base de conhecimento, por manter informações que possibilitam ações mais efetivas, pois o objetivo é detectar ameaças precocemente, antes que elas possam causar qualquer dano. Logo, criar uma consciência situacional, que corresponde a uma imagem da situação de segurança, depende das informações contidas na base de conhecimento.

Diante disso, este trabalho propõe a modelagem de dados de uma base de conhecimento para *Internet Early Warning Systems*. Os dados modelados na base de conhecimento chamada KBAM, representam os aspectos necessários para a construção de uma base de conhecimento para *Internet Early Warning Systems* e estão inicialmente apresentados em (PETRI et al., 2012) e (PETRI et al., 2013a). Com foco em eventos relacionados a detecção de intrusão, a base de conhecimento KBAM representa os seguintes aspectos: dados dos alertas gerados por sistemas de detecção de intrusão, informações sobre as medidas aplicadas em resposta a um alerta e os

parâmetros necessários para a quantificação dos pacotes que trafegam na rede.

A modelagem dos dados dos alertas gerados pelos IDSs e das medidas de respostas exploram os padrões de formatação de dados IDMEF e IDREF. Desta forma, possibilita a inserção da base de conhecimento KBAM em arquiteturas de redes que trabalham com IDSs que suportam estes formatos padrões. Além disso, a base de conhecimento KBAM também representa os parâmetros que armazenam a quantificação dos pacotes que trafegam na rede. A definição dos parâmetros utilizados está em acordo com o trabalho de (RICCI, 2008), que destaca os parâmetros necessários para a construção de uma consciência situacional.

A inserção de dados na base de conhecimento KBAM é realizada a partir de sua implantação em uma arquitetura de redes de computadores. Esta arquitetura deve conter IDSs baseados em assinaturas e que suportam o formato IDMEF para a geração dos alertas, além de conter um *sniffer* que seja responsável pela captura e armazenamento dos contadores do tráfego da rede. Para a criação das medidas de respostas é necessário integrar a arquitetura o Componente IDREF, este componente é responsável por modelar a resposta em acordo com o padrão de formatação de dados IDREF. O processo de criação da medida de resposta realizado através do Componente IDREF exige a interação humana, geralmente da equipe de segurança. Nesta etapa é onde concentra-se o registro do conhecimento na base KBAM, pois o processo de geração de medidas de respostas é cíclico, onde a equipe de segurança seleciona um alerta e cria a medida de resposta ao alerta inserindo-a na base de conhecimento KBAM. Desta forma, a medida de resposta é refinada continuamente a cada ciclo em que a mesma é utilizada para ser aplicada em resposta a um novo alerta.

Assim sendo, a KBAM classifica-se como uma base de conhecimento destinada ao uso humano, pois todos os dados armazenados nela estão disponíveis para dar suporte e direcionar as equipes de segurança.

3.2 Aspectos Representados na Base de Conhecimento KBAM

Conforme Bastke et al. (2010), as informações que devem ser armazenadas em uma base de conhecimento de *Internet Early Warning Systems* correspondem aos seguintes aspectos: dados sobre o comportamento da rede, informações sobre assinaturas de ameaças, incidentes e medidas de respostas. Fundamentado nesses parâmetros e com foco em eventos relacionados a detecção de intrusão, a base de conhecimento KBAM representa os seguintes aspectos: dados dos alertas gerados por sistemas de detecção de intrusão, informações sobre as medidas de

respostas e os parâmetros necessários para a quantificação dos pacotes que trafegam na rede.

As subseções que seguem apresentam como os aspectos de uma base de conhecimento para *Internet Early Warning Systems* estão representados na base de conhecimento KBAM.

3.2.1 Alertas de Detecção de Intrusão

Com foco em eventos específicos da área de detecção de intrusão, os dados dos alertas gerados pelos IDSs correspondem ao aspecto de incidentes de segurança conforme destacado por Bastke et al. (2010). Deste modo, os dados dos alertas dos sistemas de detecção de intrusão estão representados na base de conhecimento KBAM em conformidade com as classes e atributos do formato IDMEF.

Por ser um formato padronizado e de possível expansão, o IDMEF permite uma flexibilidade na extensão de informações dos alertas de ataques. Desta forma, as classes e atributos originais do formato IDMEF estão representados no modelo de dados da base de conhecimento KBAM para armazenar as informações dos alertas gerados pelos IDSs.

3.2.2 Medidas de Respostas

A representação das respostas aplicadas aos eventos detectados está em acordo com as classes e atributos contidos no formato de dados para troca de respostas de detecção de intrusão IDREF. O IDREF é um formato padrão similar ao IDMEF, os modelos possuem um forte relacionamento. Além disso, da mesma forma que o IDMEF, o formato IDREF também permite uma flexibilização na extensão de informações das medidas de respostas.

O formato representa as informações de três tipos de respostas aos eventos, as que correspondem ao envio de informações cujo objetivo é avisar ou controlar um ataque; as de alteração de configurações de um recurso do ambiente para conter um ataque; e as que possibilitam a reação do ambiente contra um ataque.

O processo de armazenamento das medidas de respostas na base de conhecimento KBAM não é automatizado, deste modo, é preciso a interação humana da equipe de segurança para inserir as informações que serão aplicadas em resposta a um evento específico. Desta forma, a cada criação de uma nova resposta, as medidas de respostas históricas e contidas na base de conhecimento KBAM podem ser refinadas, agregando conhecimento continuamente as medidas de respostas armazenadas na base de conhecimento KBAM.

3.2.3 Tráfego da Rede

O tráfego da rede é determinado através da quantificação dos pacotes que trafegam na rede. A quantificação é realizada através de um coletor, também conhecido como *sniffer*, que é responsável pela escuta e captura do que está acontecendo na rede e também pelo armazenamento desses dados.

A base de conhecimento KBAM representa os parâmetros quantificados a partir do tráfego da rede fundamentado nos descritores usados pela sonda do sistema IAS (*Internet Analysis System*) apresentado em (HESSE; POHLMANN, 2008) e detalhados em (RICCI, 2008). A sonda de um IAS trabalha de forma similar a um *sniffer*, realizando a captura de dados do tráfego de uma rede. Os parâmetros considerados neste trabalho e que estão representados na base de conhecimento KBAM estão apresentados na Tabela 3.1.

Tabela 3.1: Parâmetros de rede representados na Base de Conhecimento KBAM.

Parâmetros
IP
UDP
TCP
TCP Flag SYN
TCP Flag SYN-ACK
TCP Flag ACK
TCP Flag PSH-URG-ACK
TCP Flag RST-ACK
TCP Flag SYN-FIN SCAN
TCP Flag URG-PSH-FIN
HTTP
TCP (Porta Origem 80)
TCP (Porta Destino 80)
HTTPS
TCP (Porta Origem 443)
TCP (Porta Destino 443)
HTTP Post
HTTP Get
HTTP Head
HTTP Response Code 400
HTTP Response Code 500
SMTP
TCP (Porta Origem 25)
TCP (Porta Destino 25)
Envio SMTP (TCP Porta Destino 587)
Envio SMTP (TCP Porta Destino 587)
SMTP Response Code 400

continua na próxima página

Tabela 3.1: Parâmetros de rede representados na Base de Conhecimento KBAM (continuação).

Parâmetros
SMTP Response Code 500
SMTPS
TCP (Porta Origem 465)
TCP (Porta Destino 465)
IMAP / POP
TCP (Porta Origem 110)
TCP (Porta Destino 110)
TCP (Porta Origem 143
TCP (Porta Destino 143)
TCP (Porta Origem 993)
TCP (Porta Destino 993)
TCP (Porta Origem 995)
TCP (Porta Destino 995)
SIP
TCP (Porta Origem 5060
TCP (Porta Destino 5060)
UDP (Porta Origem 5060)
UDP (Porta Destino 5060)
ICMP
ICMP (Type 0)
ICMP (Type 3)
ICMP (Type 4)
ICMP (Type 5)
ICMP (Type 6)
ICMP (Type 8)
ICMP (Type 11)

A seleção dos parâmetros apresentados na Tabela 3.1 tem como base o trabalho de Ricci (2008) onde é destacado os parâmetros considerados essenciais para a criação de uma visão global, que permita a construção de uma consciência situacional para detectar possíveis eventos maliciosos. Além de considerar o tráfego dos já conhecidos protocolos TCP, IP, UDP, SMTP, ICMP, HTTP e suas ramificações, é também coletado o tráfego do protocolo SIP, que é amplamente utilizado no controle de sessões de comunicação, tais como voz e vídeo.

3.2.4 Assinaturas de Ameaças

As assinaturas de eventos maliciosos já conhecidos e aceitos pela comunidade científica e pela indústria estão representadas em arquivos de regras padronizadas, conforme utiliza o IDS Snort (SNORT, 2012a). A utilização de regras definidas possibilita um aumento na precisão da confirmação de atividades maliciosas já consolidadas.

No escopo deste trabalho, assume-se que não há uma representação formal das assinaturas das ameaças na base de conhecimento KBAM. Por se tratar de regras já consolidadas e amplamente utilizadas pelos IDSs na indústria, não há necessidade de uma nova representação dessas assinaturas. No entanto, no ambiente em que se está monitorando deve estar instalado um IDS baseado em assinatura para a geração de alertas quando um evento é compatível com alguma assinatura de ameaça. Desta forma, a base de conhecimento KBAM é alimentada com os dados dos alertas gerados pelos IDSs quando algum evento da rede é compatível com as assinaturas dos ataques existentes.

3.3 Modelagem de Dados da Base de Conhecimento KBAM

Esta seção apresenta o modelo de dados da base de conhecimento KBAM, destacando as entidades, atributos, e relacionamentos, em acordo com os aspectos descritos na Seção 3.2.

O modelo de dados da base KBAM representa os aspectos necessários para uma base de conhecimento de *Internet Early Warning Systems*, tais aspectos correspondem aos dados de alertas de detecção de intrusão gerados quando da compatibilidade das assinaturas de ameaças dos IDSs, medidas de respostas e o fluxo do tráfego da rede através da quantificação dos pacotes. A Figura 3.1 apresenta graficamente os aspectos que estão representados na base de conhecimento KBAM.

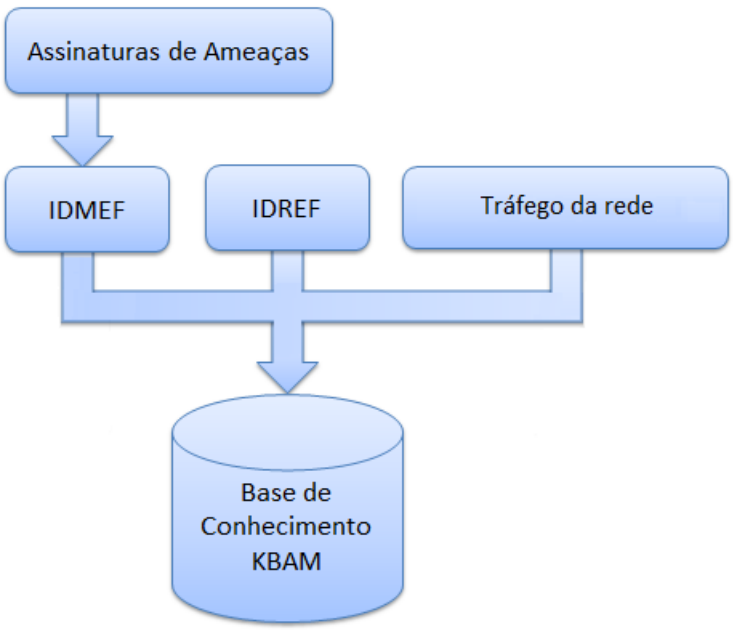


Figura 3.1: Aspectos representados na base de conhecimento KBAM.

O modelo de dados da base de conhecimento KBAM é composto por 50 entidades que

representam as classes e atributos dos formatos IDMEF, IDREF e os parâmetros para quantificar o tráfego da rede. As subseções que seguem apresentam detalhadamente as principais entidades e atributos do modelo de dados.

3.3.1 Entidades que Representam os Alertas de Detecção de Intrusão

Conforme destacado na Seção 3.2, os alertas de detecção de intrusão são representados através do modelo IDMEF. A Figura 3.2 apresenta as principais entidades que representam os dados dos alertas gerados pelos sistemas de detecção de intrusão.

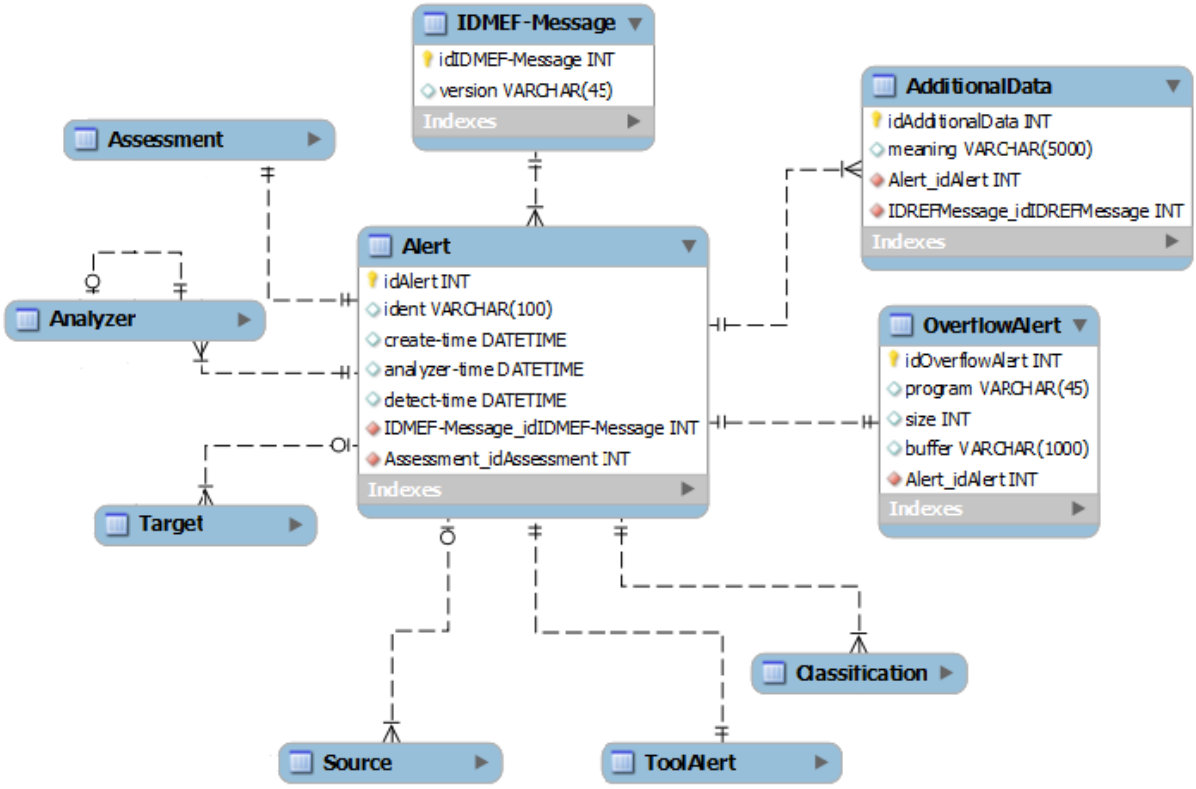


Figura 3.2: Principais entidades que representam os alertas de detecção.

Conforme mostra a Figura 3.2, a entidade que registra as informações referentes aos alertas disparados pelos detectores é a entidade *Alert*. O atributo *ident* armazena um identificador para o alerta, o instante da criação do alerta é armazenado no atributo *create-time*, o atributo *analyzer-time* armazena o momento em que o alerta foi disparado, já o instante em que o evento foi detectado está no atributo *detect-time*. A entidade *Alert* relaciona-se com as entidades *Assessment*, *Analyzer*, *Target*, *Source*, *ToolAlert*, *Classification*, *OverflowAlert* e *AdditionalData*, além da entidade *IDMEF-Message* que armazena a versão do formato IDMEF que o alerta foi gerado.

A entidade *AdditionalData* com o atributo *meaning* armazena as informações que não se

encaixam no formato IDMEF. Informações que não estão previstas no formato de alertas podem ser armazenadas neste atributo tornando-se uma extensão para o modelo IDMEF.

A entidade *OverflowAlert* representa informações específicas de alertas do tipo *overflow*. O atributo *program* armazena o nome do possível programa que é utilizado para gerar o ataque. O atributo *size* registra a quantidade de *bytes* que o atacante enviou para causar o *overflow*. Já o atributo *buffer* armazena o conjunto de dados contidos no ataque *overflow*.

A entidade *Assesment*, apresentada na Figura 3.3, armazena as informações que permitem uma avaliação do evento causador do alerta. A entidade relaciona-se a três outras, *Impact*, *Action* e *Confidence*, conforme mostrado na Figura 3.3.

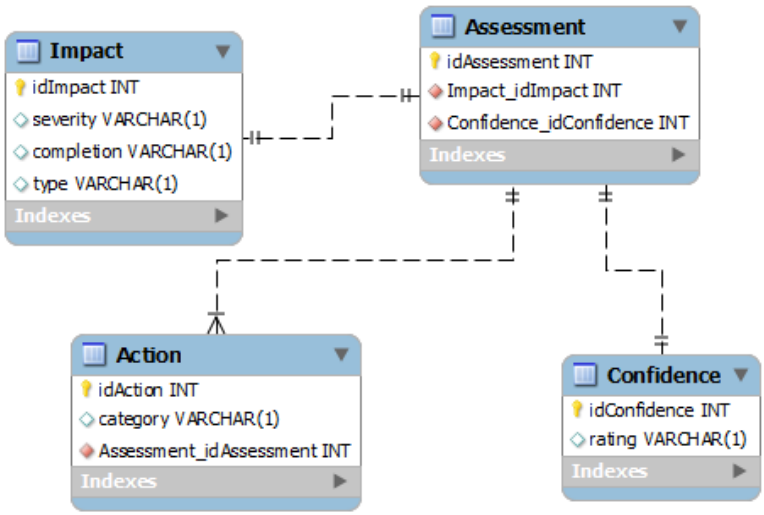


Figura 3.3: Relacionamentos da entidade *Assessment*.

Para uma avaliação do evento é necessário determinar o nível de seu impacto. A entidade *Impact*, provê informações referentes ao nível do impacto do evento sobre o sistema. O atributo *severity* armazena uma *string* com o identificador do nível do impacto (0-Alerta representa uma atividade informativa; 1-Impacto Baixo; 2-Médio; 3-Alto). O atributo *completion* armazena a informação se o evento foi completado com sucesso ou não, os valores aceitos neste campo são: *failed* (0) e *succeeded* (1).

O último campo da entidade *Impact* é o *type*, esse atributo refere-se ao tipo de tentativa do evento. Este atributo aceita os seguintes valores: 0-*admin*, tentativa ou obtenção de privilégios administrativos; 1-*dos*, tentativa ou realização de ataque de negação de serviço; 2-*file*, tentativa ou realização de ações em um arquivo; 3-*recon*, tentativa ou realização de ações de reconhecimento do sistema; 4-*user*, tentativa ou obtenção de privilégios de usuários; e 5-*other*, o evento

não se enquadra em nenhuma das categorias anteriores.

Ainda relacionada a entidade *Assessment*, a entidade *Action* define as ações tomadas pelos administradores em resposta ao evento. A entidade possui somente um atributo (*category*) e nele podem estar armazenadas as seguintes categorias: 0-*block-installed*, algum tipo de bloqueio (endereço, porta, desabilitar conta de usuário, etc) foi realizado para prevenir que um ataque atinja seu destino; 1-*notification-send*, uma mensagem de notificação foi enviada através de e-mail, pager, etc; 2-*taken-offline*, um sistema, computador ou usuário envolvido com o ataque foi tirado de funcionamento; 3-*other*, ação que não se enquadra nas categorias acima.

Outra entidade relacionada com *Assessment* é a *Confidence*. Esta entidade determina o nível de confiança das informações prestadas pelo componente de análise. O atributo *rating* armazena o nível de confiança, podendo ter os seguintes valores: 0-*low*, baixo nível de confiança; 1-*medium*, média; 2-*high*, alta; e 3-*numeric*, valor numérico que especifica o percentual de confiança.

A entidade *Analyzer*, apresentada na Figura 3.4, armazena informações referentes a identificação do analisador que originou o alerta. Apenas um analisador pode ser identificado para cada alerta originado. Os dados sobre o nome, a versão, a classificação, o modelo e o fabricante do analisador ficam registrados nesta entidade, além de informações do tipo e a versão do sistema operacional que o analisador atua. A entidade *Analyzer* possui um auto relacionamento, pois quando o alerta é enviado para outro analisador, é necessário atualizar a informação do analisador original.

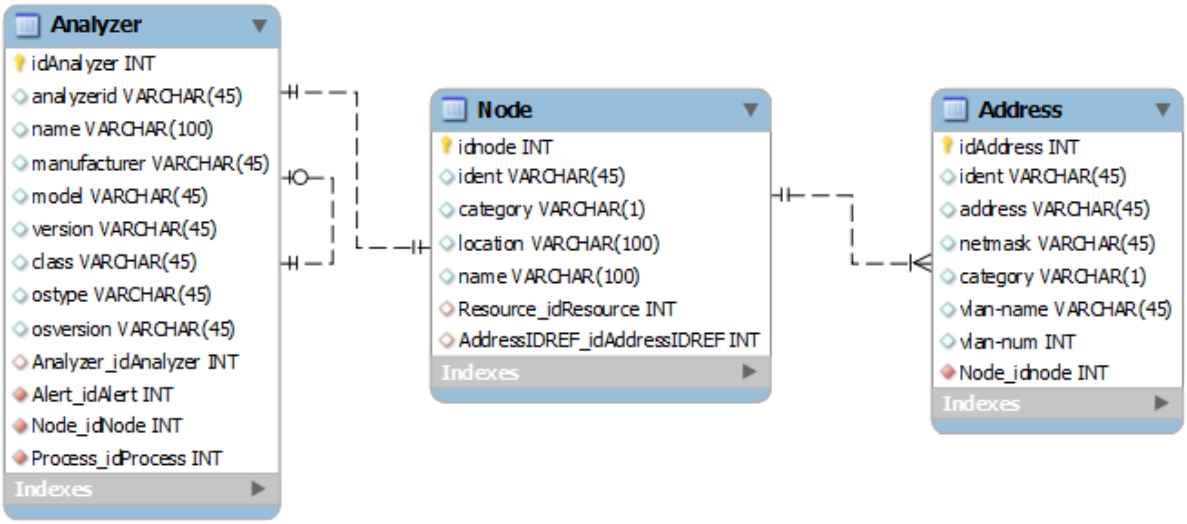


Figura 3.4: Relacionamentos da entidade *Analyzer*.

Um analisador reside em um *host* ou em um dispositivo de rede (roteadores, switches, etc),

esta informação é armazenada na entidade *Node*. Os atributos desta entidade armazenam informações referentes a localização do dispositivo (*location*), o ambiente onde o dispositivo atua (*category*) e o nome do equipamento (*name*), além de seu identificador (*ident*).

A representação da rede em que o dispositivo está alocado é realizada na entidade *Address*. A entidade possui um identificador único representado pelo campo *ident*, o atributo *category* armazena informações referentes ao tipo de endereço de rede que está sendo utilizado, o atributo pode conter valores que identificam endereços de rede dos tipos IPv4, IPv6, ATM, MAC, etc. Os atributos *vlan-name* e *vlan-num* representam respectivamente, o nome e o número que identifica a rede que o endereço pertence. O campo *address* especifica o endereço e por fim, o atributo *netmask* armazena a máscara de rede, quando apropriada para o endereço utilizado.

De acordo com a Figura 3.5 a entidade *Process* também se relaciona com a entidade *Analyzer*. Esta entidade contém informações referentes a um processo que está sendo executado. Os atributos *ident*, *name*, *pid* e *path* representam, respectivamente, o identificador único do processo, o nome do programa que está em execução, o identificador do processo e a localização do programa.

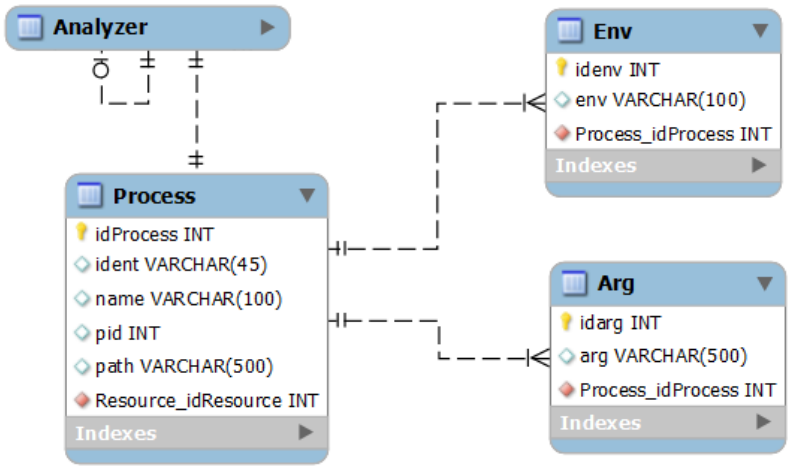


Figura 3.5: Relacionamentos da entidade *Process*.

A entidade *Process* relaciona-se com *env* e *arg* que representam, respectivamente, as linhas de comando envolvidas na execução do processo e as variáveis de ambiente relacionadas ao programa que está sendo executado.

A entidade *Source* armazena informações sobre a possível origem do evento. Conforme apresenta a Figura 3.6, a entidade *Source* possui dois atributos além do identificador (*ident*). O atributo *spoofed* contém um indicador se o componente de análise conseguiu identificar se

as informações de origem do ataque são verdadeiras. Os valores aceitos neste campo são: 0-*unknow*, 1-*yes* e 2-*no*. O valor *yes* (1) determina que as informações de origem são falsas e o valor *no* (2) determina que as informações prestadas pelo analisador são verdadeiras. No atributo *interface*, é determinada a interface de rede que gerou o alerta.

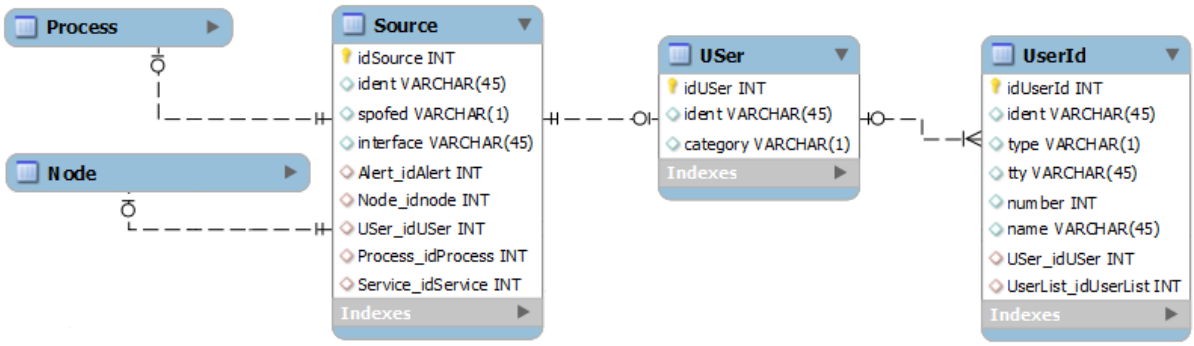


Figura 3.6: Relacionamentos da entidade *Source*.

A entidade *Source* relaciona-se com outras entidades para mapear a origem do evento. O relacionamento com a entidade *Node* representa o dispositivo de rede que possivelmente pode ser o causador do evento, e o relacionamento com a entidade *Process* determina o processo que pode ter iniciado o evento. Além disso, um usuário também pode ser o causador do evento. Estas informações estão representadas na entidade *User* e *UserId*.

De acordo com a Figura 3.7, a entidade *Service* determina o serviço de rede envolvido no evento. Os atributos *name*, *port*, *portlist* e *protocol* representam respectivamente o nome, o número da porta, uma listagem com os números de portas utilizadas e o protocolo referente ao serviço de rede envolvido. Um serviço pode ainda ser um serviço web ou SNMP. A entidade *WebService* contém informações específicas para serviços *web* tais como, comandos HTTP, descrição de requisições URL e CGI e argumentos de script CGI. Já a entidade *SNMPService* carrega informações adicionais relacionadas ao tráfego SNMP, como o nome de segurança do objeto, contexto do nome e identificador do contexto do objeto.

De forma similar a entidade *Source*, a entidade *Target*, apresentada na Figura 3.8, representa informações sobre os possíveis alvos dos eventos que geraram um alerta. A entidade *Target* relaciona-se com *Node*, *User*, *Process* e *Service* que representam as informações do endereço, do usuário, do processo ou do serviço que pode ser o possível alvo do evento.

Além destas entidades, a entidade *Target* também se relaciona com a entidade *File*, conforme apresenta a Figura 3.8. Esta entidade armazena informações referentes aos arquivos relacionados ao destino do evento. A entidade *File* possui vários atributos que representam o nome,

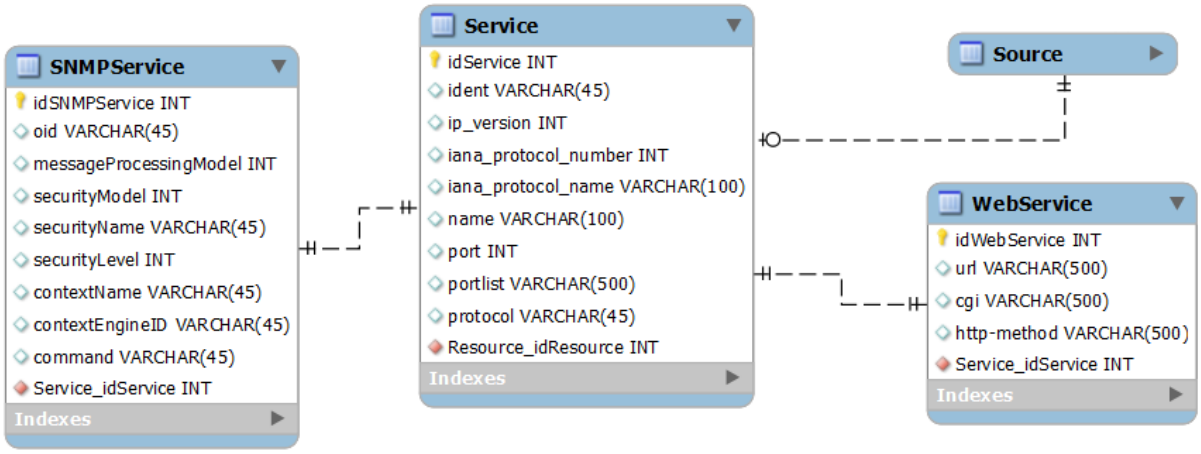


Figura 3.7: Relacionamentos da entidade *Service*.

a localização, a data de criação, a data de alteração e o último acesso, além do seu tamanho em disco.

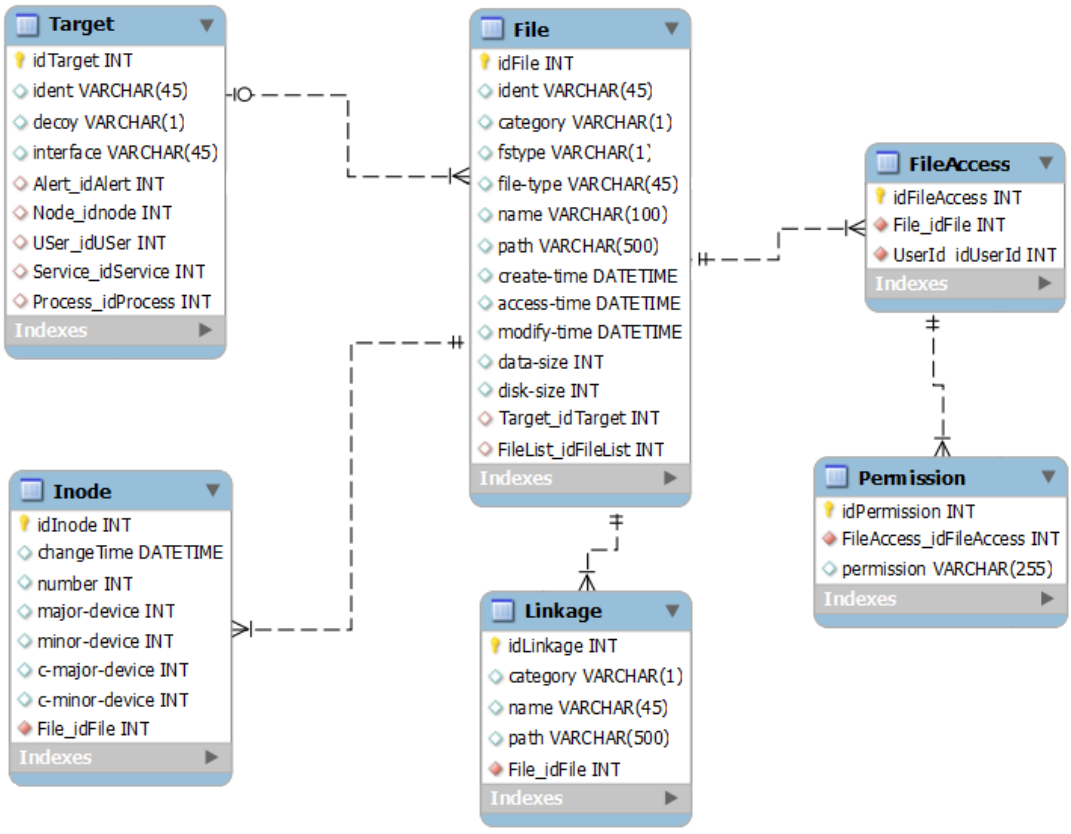


Figura 3.8: Relacionamentos da entidade *Target*.

Conforme mostra a Figura 3.8, as permissões de acesso a um arquivo estão armazenadas nas entidades *FileAccess* e *Permission*. A entidade *Linkage* representa os arquivos do sistema que estão interligados com o arquivo registrado na entidade *File*, armazenando em seus atri-

butos o nome e caminho dos arquivos. Por sua vez, a entidade *Inode* é usada para representar informações adicionais contidas em um sistema de arquivos *Unix i-node*.

A entidade *ToolAlert*, representada na Figura 3.9, contém informações referentes a alertas de ataques gerados por programas ou ferramentas. Um alerta com estas informações é gerado quando o analisador consegue identificar qual a ferramenta ou programa foi o causador do evento. O atributo *name* armazena uma *string* com o nome da ferramenta utilizada no ataque e o atributo *command* contém o comando executado pela ferramenta.

Os ataques gerados por programas ou ferramentas podem causar inúmeros alertas, desta forma, a entidade *ToolAlert* relaciona-se a *alertident*. A entidade *alertident* contém um único atributo que armazena o identificador único de outro alerta, também gerado pela ferramenta e que está relacionado com o alerta atual.

Há também a necessidade de correlacionar alertas, ou seja, quando um analisador necessita criar várias mensagens de alertas que representam um único ataque. Essa correlação é representada na entidade *CorrelationAlert*. Esta entidade também relaciona-se com *alertident* onde irá armazenar os identificadores dos alertas correlacionados.

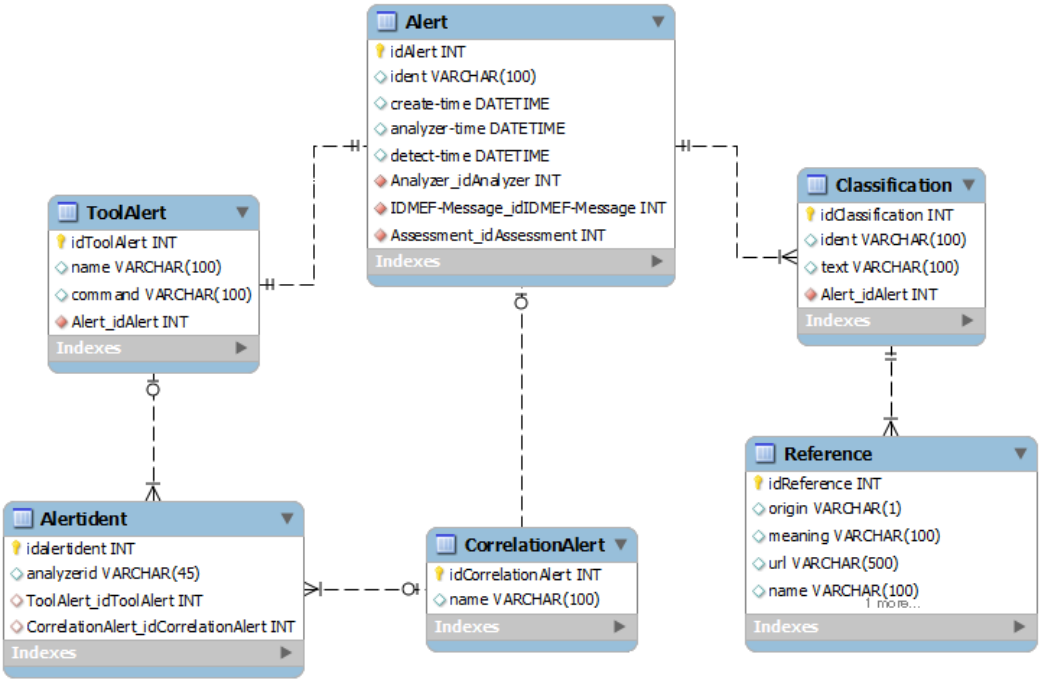


Figura 3.9: Relacionamentos das entidades *ToolAlert* e *Classification*.

Conforme destacado na Figura 3.9, a entidade *Alert* relaciona-se com *Classification*. Este relacionamento determina uma possível classificação do tipo de alerta. A partir da classificação, o alerta pode ter alguma documentação externa que possuam maiores informações referentes ao

alerta gerado, essas informações ou *links* para os documentos ficam armazenadas na entidade *Reference*.

3.3.2 Entidades que Representam as Mensagens de Respostas

As entidades que representam os dados referentes as respostas aos alertas gerados estão modelados conforme o padrão de formatação de dados IDREF.

De acordo com o modelo da Figura 3.10, a principal entidade que representa uma resposta a um alerta é a *IDREF-Message*. Esta entidade contém os atributos *ident* e *version* que representam, respectivamente, uma identificação única para as respostas geradas e a versão do modelo de dados utilizado.

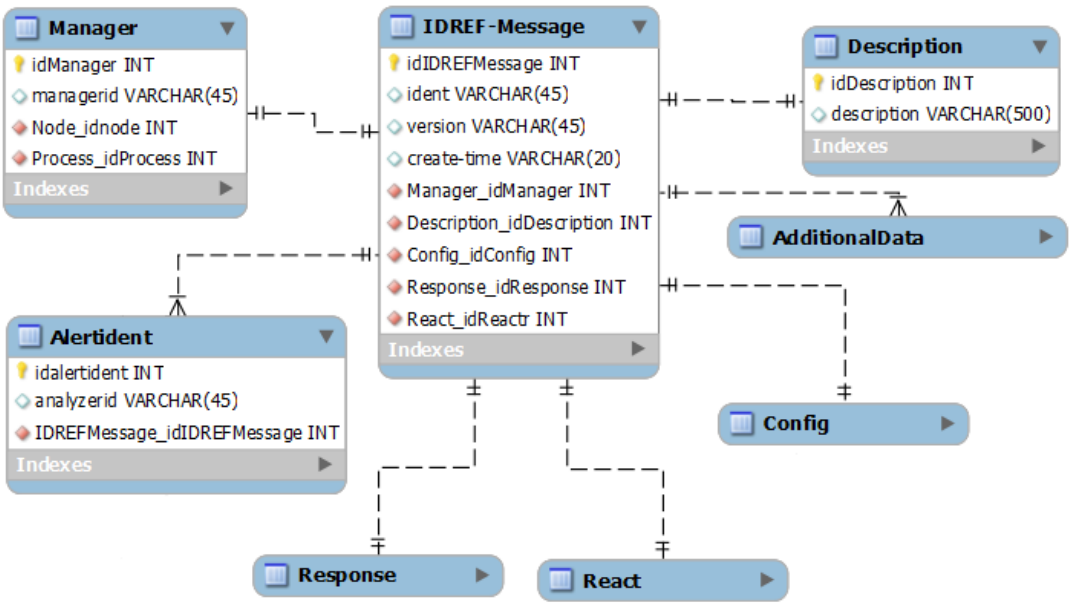


Figura 3.10: Principais entidades que representam as medidas de respostas.

A entidade *AdditionalData* que se relaciona com *IDREF-Message* possui a mesma finalidade do formato IDMEF, ou seja, armazenar informações que não são suportadas pelo formato, nesta entidade pode-se inserir informações adicionais referentes a resposta a um evento.

Já a entidade *alertident* contém a informação do identificador do alerta do modelo IDMEF que gerou a resposta. Estas informações são importantes para permitir outros relacionamentos entre alertas e respostas. Outra entidade que se relaciona a *IDREF-Message* é a entidade *Description*. Esta entidade armazena uma descrição da resposta que está sendo executada. Nesta descrição podem ser inseridas informações específicas sobre a resposta ou informações extras que sejam úteis para análises posteriores. Por sua vez, a entidade *Manager* contém informações referentes ao gerenciador que enviou a resposta ao alerta.

Além das entidades já mencionadas, a entidade *IDREF-Message* relaciona-se com *Response*, *React* e *Config*, que representam os tipos de respostas suportados pelo formato IDREF, como apresenta a Figura 3.11.

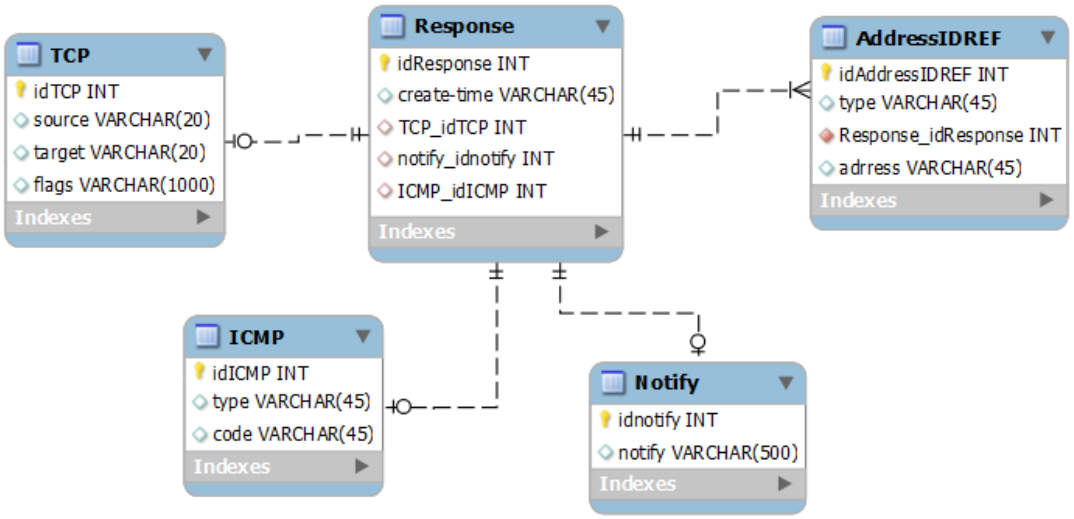


Figura 3.11: Relacionamentos da entidade *Response*.

A entidade *Response* armazena o envio de informações sobre o aviso de um ataque, a entidade possui um atributo que armazena a hora da criação da resposta. Além disso, a entidade *Response* relaciona-se com as entidades *TCP*, *ICMP*, *notify* e *AddressIDREF*.

A entidade *TCP* contém informações referentes ao envio de pacotes TCP pela rede para responder a um alerta. Seus atributos *source*, *target* e *flags* armazenam os dados que devem ser colocados no pacote TCP para ser enviado.

Já a entidade *ICMP* armazena informações sobre as mensagens ICMP enviadas em resposta a uma mensagem de alerta. Os atributos *type* e *code* contêm informações que devem ser inseridas na mensagem ICMP a ser enviada.

Logo, a entidade *notify* armazena informações sobre o ataque, podendo representar até mesmo o alerta no formato IDMEF. Por sua vez, a entidade *AddressIDREF* registra o endereço de destino da resposta, conforme o tipo identificado no atributo *type*.

Outro tipo de resposta a um alerta é representado através da entidade *React*. Esta entidade representa as reações do ambiente para conter um ataque e possui um único atributo que registra o momento que a reação foi tomada. Uma reação pode ser realizada através do bloqueio (*Block*) ou fechamento (*Shutdown*) de algum recurso. A Figura 3.12 apresenta o relacionamento destas entidades.

A entidade *Block* representa o bloqueio de um recurso. Esta entidade contém um identifi-

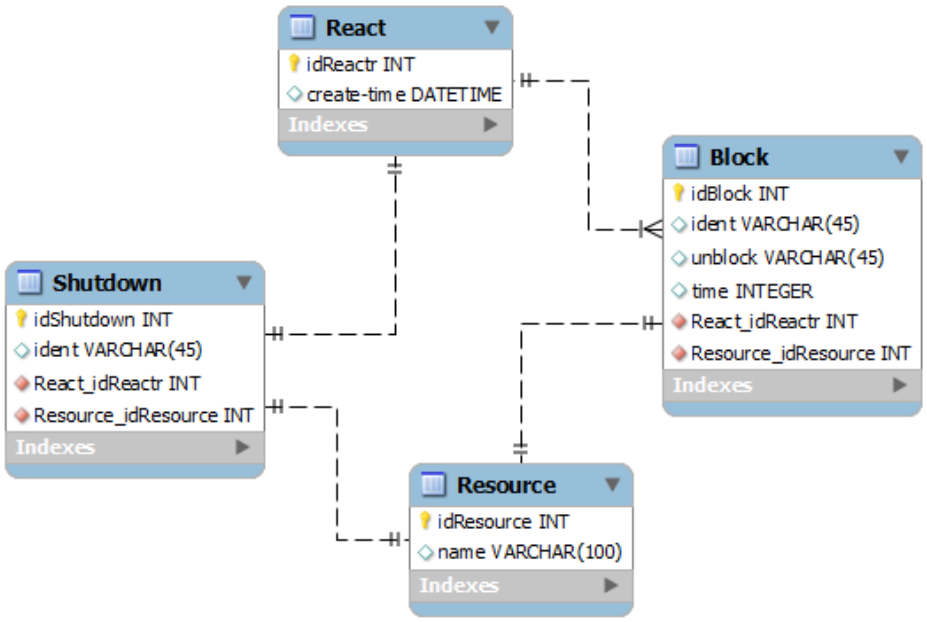


Figura 3.12: Relacionamentos da entidade *React*.

cador único do bloqueio representado pelo campo *ident*, o atributo *unblock* indica o momento que o recurso deve ser desbloqueado. Este atributo pode conter dois valores: *reset*, quando o recurso deve ser reinicializado para ser desbloqueado ou *time*, que indica que o recurso deve permanecer bloqueado por um tempo determinado no atributo *time*, que contém em minutos o tempo que o recurso deve permanecer bloqueado.

A entidade *Shutdown* representa o fechamento de algum recurso e possui um atributo que representa o identificador da reação executada. Um bloqueio ou fechamento é realizado sobre um único recurso. O recurso envolvido na reação é representado na entidade *Resource*.

Além do envio de mensagem pela rede e do bloqueio de algum recurso, outro tipo de resposta pode ser realizado através da reconfiguração dos dispositivos de rede. A alteração nas configurações de algum recurso é representada pela entidade *Config*, conforme apresenta a Figura 3.13.

Os comandos executados na reconfiguração dos recursos ficam armazenados na entidade *Command*, podendo ter vários comandos para uma única resposta a ser executada em um recurso específico.

Os dados sobre os recursos configurados estão armazenados na entidade *Resource*. Um recurso pode ser um nó ou um serviço da rede, uma lista de usuário, uma lista de arquivos ou um processo do sistema operacional. Estes recursos são representados pelas entidades: *Node*, *Service*, *UserList*, *FileList* e *Process*.

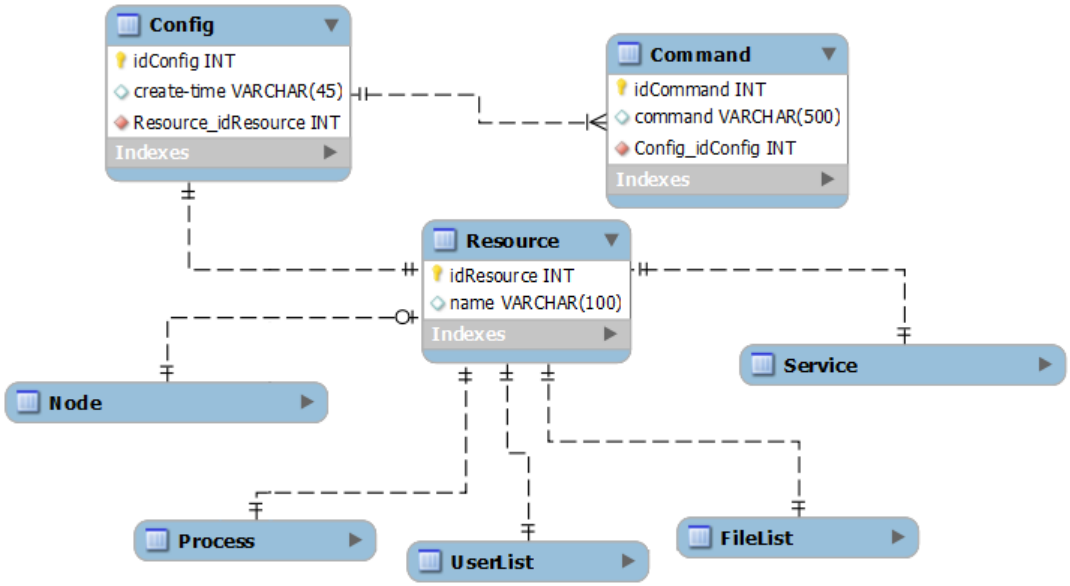


Figura 3.13: Relacionamentos da entidade *Config*.

3.3.3 Entidades que Representam a Quantificação do Tráfego da Rede

A quantificação dos dados capturados pelo *sniffer*, a partir dos parâmetros destacados na Seção 3.2.3, para o monitoramento do tráfego de uma rede são armazenadas nas entidades apresentadas na Figura 3.14.

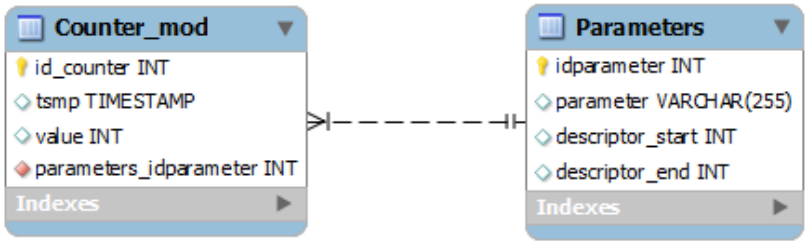


Figura 3.14: Entidades que representam a quantificação do tráfego da rede.

Conforme mostra a Figura 3.14, a entidade *parameters* contém todos os parâmetros que são capturados do tráfego da rede monitorada, a relação destes parâmetros é detalhada na Seção 3.2.3. O atributo *parameter* armazena a descrição do parâmetro utilizado e os atributos *descriptor_start* e *descriptor_end* contêm o intervalo dos descritores de cada parâmetro, caso o mesmo tenha um descritor.

Por sua vez, a entidade *counter_mod* é responsável por armazenar todos os contadores dos pacotes capturados na rede. O momento da captura dos dados é armazenado no atributo *tsmp*, a quantificação dos pacotes está no campo *value* e a identificação do parâmetro é realizada através

do relacionamento com a entidade *parameter*.

3.4 Trabalhos Relacionados

Conforme destacado na Seção 3.2, os aspectos que devem compor uma base de conhecimento para *Internet Early Warning Systems* são: dados sobre o comportamento da rede, informações sobre assinaturas de ameaças, incidentes e medidas de respostas. Porém, os trabalhos existentes na literatura não atendem a estes aspectos para a construção de uma base de conhecimento.

Em (UNDERCOFFER et al., 2004) é proposta uma ontologia que objetiva modelar os ataques categorizados em acordo com o alvo do sistema, os significados do ataque, suas consequências e a localização do atacante. No entanto, a ontologia proposta por (UNDERCOFFER et al., 2004) não representa os dados do tráfego da rede e também não aborda informações sobre as medidas de respostas para conter os ataques.

Lima et al. (2008) propõem uma abordagem para detecção de intrusão através do uso de redes neurais artificiais. A proposta apresenta o protótipo I-IDS (*Intelligent Intrusion Detection System*) que trabalha com um método de detecção híbrido e utiliza nas fases de treinamento e aprendizagem uma base de conhecimento com regras de detecção previamente definidas e utiliza as redes neurais como mecanismo para detectar variantes de intrusões.

Flior et al. (2010) propõem um sistema especialista que utiliza a classificação como técnica de mineração de dados aplicada em um conjunto de informações capturadas do tráfego da rede, objetivando criar uma base de conhecimento com regras a partir da fusão dos dados do comportamento normal e malicioso, coletados por múltiplos sensores, e que permita fazer decisões em tempo real e responder apropriadamente aos eventos. Entretanto, a proposta apresentada em (FLIOR et al., 2010) não engloba todos os aspectos de uma base de conhecimento, desconsiderando o armazenamento de informações sobre incidentes e suas medidas de respostas.

Em More et al. (2012) é apresentado um *framework* que trabalha com a integração de dados de sensores heterogêneos utilizados para a captura de dados de detecção de intrusão e logs. Os dados capturados são armazenados em uma base de conhecimento que é estruturada por uma abordagem ontológica para modelar os dados das ameaças identificadas. Porém, esta abordagem não representa informações referentes as respostas aos alertas de detecção.

Observa-se assim, que os trabalhos que utilizam bases de conhecimento, não costumam abordar todos os aspectos necessários para a criação de uma base de conhecimento voltada ao

monitoramento de ataques. Além disso, também não exploram os padrões de interoperabilidade voltados a detecção de intrusão, o que pode ser um limitador na integração a sistemas de monitoramento. O modelo de dados apresentado neste trabalho possibilita tanto o alinhamento aos padrões de interoperabilidade como a representação dos aspectos de rede essenciais para a realização de um monitoramento de ataques.

3.5 Considerações Parciais

Este capítulo apresentou o detalhamento da proposta do modelo de dados da base de conhecimento KBAM para *Internet Early Warning Systems*. Ao representar os dados de alertas gerados por sistemas de detecção de intrusão, medidas de respostas e do tráfego da rede, o modelo de dados engloba os aspectos necessários para a criação de uma base de conhecimento de *Internet Early Warning Systems*, conforme citado em (BASTKE; DEML; SCHMIDT, 2010).

A representação dos dados da base de conhecimento KBAM, ao explorar padrões de formatação de dados de mensagens de detecção de intrusão (IDMEF) e de respostas (IDREF), potencializa a integração da base de conhecimento KBAM em diferentes ambientes de rede que utilizam IDSs que suportam esses padrões de formatação de dados.

Em comparação aos trabalhos relacionados, o modelo de dados da base de conhecimento KBAM destaca-se ao englobar os aspectos necessários para a criação de uma base de conhecimento, ao contrário dos trabalhos existentes na literatura, que não costumam abordar todos os aspectos. De mesmo modo, os trabalhos relacionados não exploram os padrões de formatação de dados de detecção e respostas a intrusão, o que dificulta a sua integração a sistemas de monitoramento.

4 CONSTRUINDO UMA CONSCIÊNCIA SITUACIONAL COM A BASE DE CONHECIMENTO KBAM

Neste capítulo são apresentadas as atividades realizadas para validar o modelo de dados da base de conhecimento KBAM, proposta no Capítulo 3. A prova de conceito é realizada através da implementação do modelo de dados e inserção da base de conhecimento KBAM em um ambiente de rede de uma instituição de ensino superior e pela construção de uma consciência situacional do ambiente em que a base de conhecimento KBAM está inserida.

A Seção 4.1 apresenta um estudo de caso que integra diferentes ferramentas para a coleta e inserção de dados na base de conhecimento KBAM, demonstrando a aplicabilidade da modelagem para armazenar dados de um ambiente de rede real. Na Seção 4.2 é demonstrada a construção da consciência situacional do ambiente monitorado através da aplicação de um modelo teórico nos dados armazenados na base de conhecimento KBAM, que está inicialmente apresentado em (PETRI et al., 2013b).

4.1 Inserindo a Base de Conhecimento KBAM em uma Arquitetura de Redes

O modelo de dados da base de conhecimento KBAM permite armazenar dados coletados por diversos sistemas de detecção de intrusão integrados, além de armazenar a quantificação dos pacotes que trafegam na rede monitorada. A base de conhecimento KBAM ao representar os dados do padrão de formatação de dados de alertas de detecção de intrusão (IDMEF) e de mensagens de respostas (IDREF), potencializa a coleta de dados a partir da integração de ferramentas de detecção que utilizam estes padrões. O uso da base KBAM em um ambiente de rede com ferramentas de detecção de intrusão integradas é apresentado em um estudo de caso.

O estudo de caso realizado na rede da Universidade Federal de Santa Maria (UFSM) demonstra a aplicabilidade do modelo de dados da base de conhecimento KBAM em um ambiente de rede real e que utilize diferentes sistemas de detecção de intrusão integrados. O estudo de caso envolveu dois pontos de monitoramento para a coleta de dados na UFSM: a rede do setor responsável pelo Vestibular (Coperves) e a rede do Centro de Processamento de Dados (CPD). Estes setores são pontos estratégicos na infraestrutura de redes da instituição e estão frequentemente sob ataques.

Nos ambientes monitorados foram instalados os sistemas de detecção de intrusão basea-

dos em assinaturas Snort (SNORT, 2012a), em sua versão 2.8.5.2-2 e o Suricata (SURICATA, 2012), na versão 1.2.1.

O Snort é um sistema de detecção de intrusão para rede (NIDS) e é um dos mais populares IDSs existentes. Sua popularização dá-se através da flexibilidade nas configurações de regras e constante atualização frente às novas ferramentas de invasão (SNORT, 2012b). O Snort é um IDS baseado em assinaturas e possui um amplo cadastro de assinaturas para a detecção de intrusos. Outro ponto forte do Snort refere-se ao permanente desenvolvimento e atualização das regras de detecção.

O Suricata é um IDS *open-source*, definido como uma ferramenta da nova geração para a detecção de intrusão e prevenção. Como é um sistema *multi-thread*, oferece maior velocidade e eficiência na análise do tráfego de rede (SURICATA, 2012).

A integração dos IDSs é realizada através do uso do *framework* Prelude (PRELUDE, 2012). O Prelude é sistema gerenciador de eventos de segurança da informação e permite a unificação de vários tipos de aplicações e sensores, com código-fonte proprietário ou livre, em um sistema centralizado. O Prelude utiliza o padrão IDMEF que permite que diferentes tipos de sensores criem eventos utilizando o mesmo padrão de comunicação. Além disso, o Prelude destaca-se como uma ferramenta que integra vários sensores distribuídos e possui como principal componente em sua arquitetura o *Prelude-Manager*, que trabalha como um servidor que aceita conexões de sensores distribuídos e armazena os eventos recebidos em um banco de dados formatado com o padrão IDMEF (PRELUDE, 2012). A versão do *Prelude-Manager* utilizada foi a 0.9.15-4.

Os sensores utilizados no estudo de caso (Snort e Suricata) foram configurados para se comunicarem diretamente com o *framework* Prelude. A configuração realizada faz com que os IDSs gerem os alertas e automaticamente encaminhem para o *Prelude-Manager* armazenar os eventos conforme os dados padronizados pelo formato IDMEF.

Ao identificar algum evento malicioso, compatível com as regras de detecção dos IDSs, os sensores criam um alerta e enviam os dados formatados com o padrão IDMEF para o componente *Prelude-Manager*, que por sua vez, realiza o processo de armazenar os alertas no banco de dados, como demonstrado na Figura 4.1.

Os eventos são armazenados em um banco de dados próprio da ferramenta Prelude, também modelado de acordo com os dados do formato IDMEF. O banco de dados utilizado no estudo de caso é o PostgreSQL na versão 8.4 (POSTGRESQL, 2012).

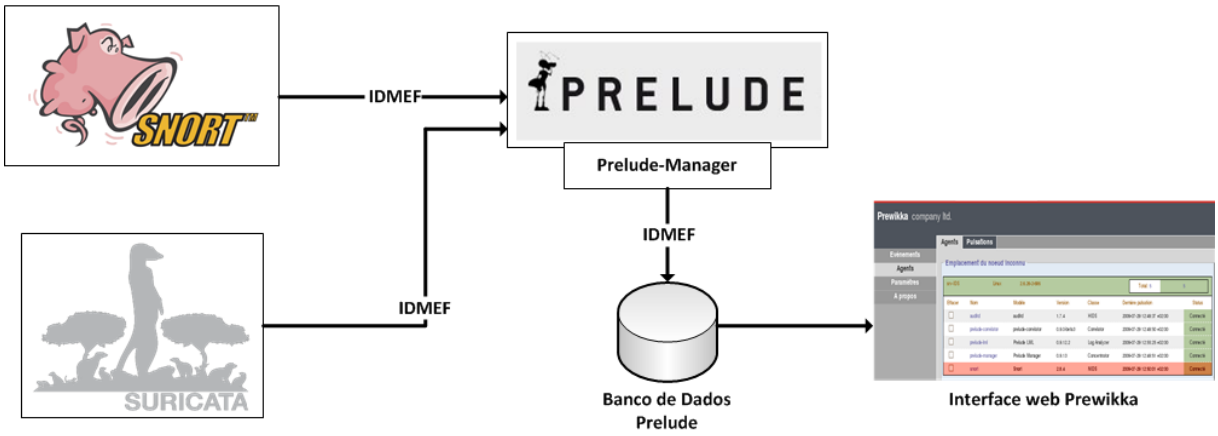


Figura 4.1: Arquitetura implementada para a integração dos IDSs.

O Prelude ainda possui uma interface *web*, chamada *Prewikka*, que fornece várias opções para a interpretação dos dados coletados e administração do ambiente. A versão do *Prewikka* utilizada no estudo de caso foi a 0.9.17.1.

Através da interface *Prewikka* é possível identificar o montante de alertas gerados por cada sensor, os detalhes de cada alerta, destacando a hora da detecção, a origem e o alvo do evento e também uma classificação inicial da gravidade do alerta. Além disso, a ferramenta ainda possibilita a visualização dos estados de cada sensor integrado, permitindo uma ampla visão sobre o funcionamento da infraestrutura implementada. A interface que apresenta os estados de cada sensor utilizado pode ser observada na Figura 4.2.

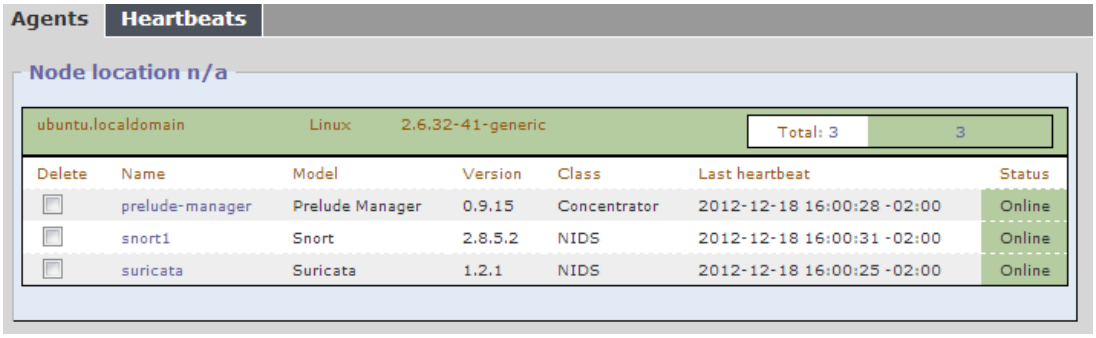


Figura 4.2: Estados dos sensores utilizados no estudo de caso.

No estudo de caso foram utilizadas três máquinas virtuais (VMs) com o sistema operacional Ubuntu Server 10.04.4 LTS x86-32 e o *VMware Workstation 8* como monitor das máquinas virtuais. Na arquitetura do estudo de caso, apresentada na Figura 4.3, uma das VMs faz o papel do gerenciador, ou seja, nela estão instalados o *framework* Prelude com o componente *Prelude-Manager*, o banco de dados e a interface *Prewikka*. As outras duas VMs realizam o processo de coleta de dados, utilizando para isso, os sensores Snort e Suricata, além de conter o

sniffer responsável pela captura e quantificação do tráfego da rede. As duas VMs estão alocadas em dois pontos na arquitetura de redes, uma para coletar dados da rede do CPD e a outra da Coperves. A Figura 4.3 apresenta toda a arquitetura implementada no estudo de caso realizado na rede de computadores da UFSM, além do fluxo dos dados até serem inseridos na base de conhecimento KBAM.

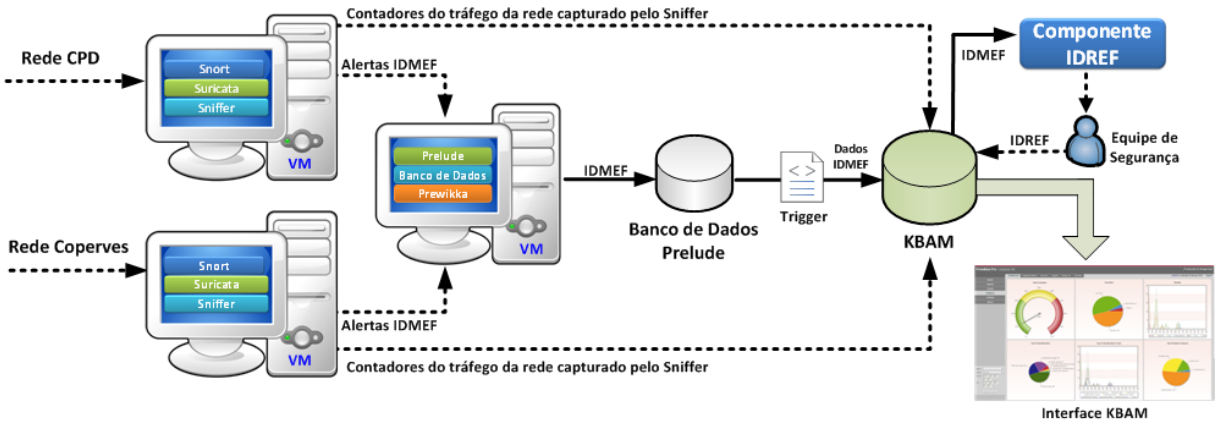


Figura 4.3: Arquitetura do estudo de caso realizado na rede de computadores da UFSM.

Como observado na Figura 4.3, no banco de dados da ferramenta Prelude está inserida uma *trigger* que realiza o processo de inserção dos dados dos alertas de detecção de intrusão na base de conhecimento KBAM. A *trigger* está anexada a entidade *Alert*, que representa a principal entidade do formato IDMEF aonde são armazenados os alertas disparados pelos sensores. A cada novo alerta gerado pelos sensores e armazenado no banco de dados pelo componente *Prelude-Manager* a *trigger* é acionada e então executa o processo de inserção dos dados do alerta nas entidades da base KBAM.

O analisador de pacotes (*sniffer*) utilizado no estudo de caso para capturar os pacotes que trafegam na rede da instituição é o Wireshark (WIRESHARK, 2012). O Wireshark (antigo Ethereal) é um *software* livre e de código aberto que trabalha na análise de pacotes de redes de computadores, possui uma interface gráfica para uma análise dos dados e possui o TShark que trabalha com linhas de comando e permite formatar a saída dos dados coletados (WIRESHARK, 2012). O Wireshark está instalado nas duas VMs e realiza o processo de coleta e quantificação do tráfego da rede da instituição. Após a captura dos dados através do Wireshark, os contadores de cada um dos parâmetros são armazenados na base de conhecimento KBAM.

O Componente IDREF utilizado para a geração de respostas aos alertas disparados pelos

sensores, foi desenvolvido utilizando a linguagem Java 1.7[1] utilizando o ambiente de desenvolvimento integrado NetBeans 7.0.1[2].

O componente está conectado diretamente a base KBAM e atende aos requisitos descritos em (SILVA; WESTPHALL, 2006). Os alertas no formato IDMEF, gerados pelos sensores e inseridos na base KBAM através da *trigger*, são listados na tela inicial do Componente IDREF para que a equipe de segurança possa selecionar o alerta no qual será aplicada uma resposta e então inserir os dados da mensagem de resposta. A Figura 4.4 apresenta a interface inicial do Componente IDREF listando alguns alertas gerados pelos sensores e que estão armazenados na base KBAM.

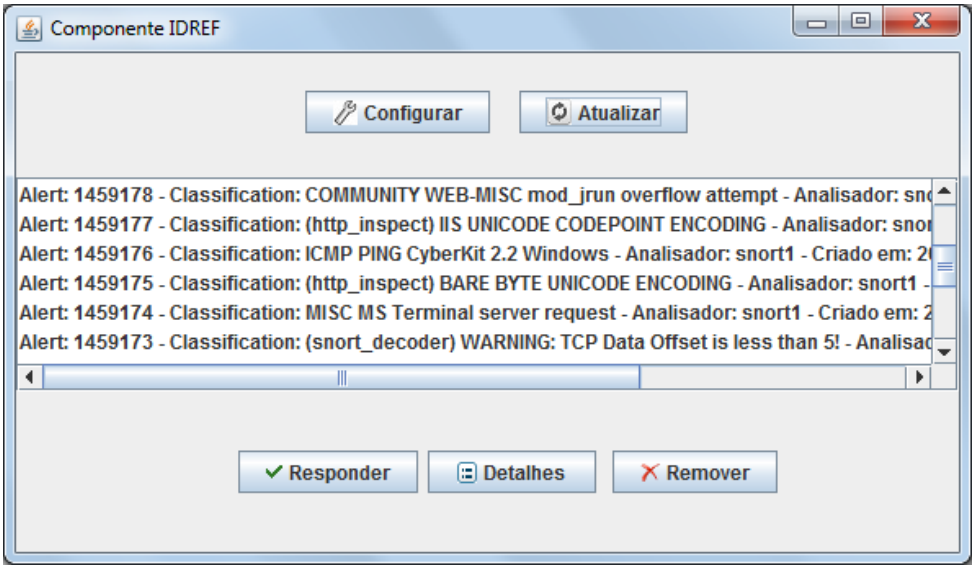


Figura 4.4: Lista de alertas na tela principal do Componente IDREF.

A listagem dos alertas apresenta os últimos eventos gerados pelos IDSs e é atualizada através do "Botão Atualizar", além disso os alertas podem ser removidos da listagem através do "Botão Remover". Este botão somente remove o alerta da listagem do componente, não o removendo da base KBAM. Outra funcionalidade do Componente IDREF é a visualização dos detalhes do alerta selecionado, esta funcionalidade é executada através do "Botão Detalhes" da tela principal.

O "Botão Responder" carrega a interface que é responsável por iniciar o processo de configuração da resposta ao alerta selecionado. As mensagens de respostas podem ser: o envio de informações, cujo objetivo é avisar ou controlar um ataque; solicitação de alteração de configuração, que permite reconfigurar um recurso do ambiente; e reação, que possibilita comandar

[1] http://www.java.com
[2] http://www.netbeans.org/

uma reação do ambiente contra um ataque. Os atributos de uma mensagem de resposta estão descritos na Seção 3.3.2. O alerta selecionado é vinculado a mensagem de resposta que então é inserida na base KBAM.

Como apresentado na Figura 4.3, o processo de criação de uma medida de resposta a um alerta através do Componente IDREF é cíclico e com interação humana da equipe de segurança. Deste modo, a medida de resposta é refinada a cada ciclo em que é utilizada para responder a um alerta. Assim sendo, a base KBAM além de armazenar os dados das mensagens de alertas gerados pelos IDSs e dos contadores dos pacotes do tráfego da rede, armazena também um conhecimento sobre as medidas de respostas que são refinadas continuamente pela equipe de segurança a cada iteração do processo de criação de uma medida de resposta.

Conforme a Figura 4.3 a visualização dos dados que estão armazenados na base de conhecimento KBAM é realizada através da interface *web* KBAM. No entanto, por estar fora do escopo deste trabalho, a interface *web* KBAM não foi implementada e está destacada como atividades para os trabalhos futuros.

A inserção da base de conhecimento KBAM no estudo de caso demonstrou a aplicabilidade do modelo de dados em um ambiente de rede real e permite destacar as vantagens de sua utilização: a possibilidade de armazenar os dados coletados a partir de ferramentas de detecção de intrusão integradas; a representação do tráfego da rede; a característica de representar informações de eventos de detecção de intrusão através de padrões e o refinamento do conhecimento utilizado no processo de criação de medidas de respostas a eventos maliciosos, também explorando padrões de formatação de dados. Tais vantagens potencializam a utilização da base de conhecimento KBAM para auxiliar as equipes de segurança no monitoramento de ataques em diversos ambientes de redes de computadores.

4.2 Aplicando um Modelo de Consciência Situacional na Base de Conhecimento KBAM

A inserção da base de conhecimento KBAM na arquitetura de redes da UFSM permite a coleta de diversos dados de eventos maliciosos ocorridos e também a quantificação do tráfego da rede. Além disso, a utilização de sensores distribuídos na rede de setores estratégicos da instituição (Coperves e CPD) potencializa a construção da consciência situacional do ambiente de rede da UFSM, atendendo a um dos principais objetivos dos *Internet Early Warning Systems*. A partir dos dados capturados na rede e armazenados na base de conhecimento KBAM é possível

construir, de forma simplificada, uma consciência situacional do ambiente monitorado.

O termo consciência situacional é bastante utilizado na área militar e no controle do tráfego aéreo e nos últimos anos vem sendo aplicado na área de segurança de redes de computadores e é um dos principais objetivos dos *Internet Early Warning Systems* (ONWUBIKO, 2009). Assim sendo, a construção da consciência situacional é importante quando a compreensão dos eventos ocorridos no ambiente monitorado é crítica para o processo de tomada de decisão (HESSE; POHLMANN, 2008).

O modelo apresentado por Endsley (1995) é referência na área de consciência situacional e vem sendo aplicado em diversos trabalhos da área de segurança de redes (HESSE; POHLMANN, 2008) (ONWUBIKO, 2009). No modelo de Endsley há três níveis para a construção de uma consciência situacional: (*i*) percepção de eventos mal-intencionados, (*ii*) compreensão das informações e (*iii*) habilidade de fazer projeções com base nas informações capturadas no ambiente monitorado (ENDSLEY, 1995). Um quarto nível foi adicionado posteriormente por McGuinness e Foy (2000), o nível adicionado refere-se a resolução, onde são aplicadas contramedidas necessárias para tratar os riscos identificados (MCGUINNESS; FOY, 2000).

A construção da consciência situacional com os dados armazenados na base de conhecimento KBAM é realizada com a aplicação do modelo de Endsley (1995) e na extensão proposta por McGuinness e Foy (2000). As subseções que seguem detalham como os dados que foram coletados no estudo de caso e que estão armazenados na base de conhecimento KBAM são utilizados em cada nível do modelo aplicado.

É importante ressaltar, que o modelo teórico de Endsley possui etapas subjetivas, que envolvem processos psicológicos. Desta forma, os procedimentos apresentados nas subseções que seguem não representam a forma exaustiva de construir a consciência situacional do ambiente monitorado a partir dos dados armazenados na base de conhecimento KBAM, ou seja, os procedimentos e consultas apresentadas podem ser melhoradas, ou ainda, outros procedimentos, atividades e ferramentas, não descritas neste trabalho, podem ser utilizadas pelas equipes de segurança para construir a percepção, a compreensão, a projeção e a resolução de eventos identificados no ambiente de rede monitorado.

4.2.1 Percepção

O primeiro nível do modelo de Endsley (1995) refere-se a percepção e identificação de atividades mal-intencionadas que ocorrem na rede monitorada. A percepção é adquirida através

de logs de *firewalls*, relatórios de *scan* e também através de mensagens de alertas de sistemas de detecção de intrusão (ONWUBIKO, 2009). Este nível é atendido pela base de conhecimento KBAM ao armazenar os alertas dos sistemas de detecção de intrusão e os contadores dos pacotes que representam o tráfego da rede.

O monitoramento da infraestrutura de redes normalmente é realizado pelas equipes de segurança, que trabalham em uma sala de monitoramento com diversas ferramentas e metodologias objetivando identificar, tratar e mitigar os incidentes identificados. Assim sendo, os sensores (IDSs) instalados na rede da UFSM reportam à equipe de segurança os alertas dos eventos maliciosos que estão ocorrendo no ambiente monitorado. A distribuição dos sensores permite a base de conhecimento KBAM armazenar dados de alertas de detecção de sensores integrados e que estão localizados em pontos estratégicos da rede da instituição (CPD e Coperves), criando uma visão abrangente do ambiente monitorado.

Os alertas disparados pelos IDSs são armazenados no banco de dados da ferramenta Prelude e direcionados automaticamente para a base de conhecimento KBAM. Os alertas assim que identificados ficam disponíveis na interface *Prewikka*, o que potencializa a percepção das atividades maliciosas pela equipe de segurança. A Figura 4.5 apresenta através da interface *Prewikka* uma lista com alguns alertas disparados pelos IDSs e que estão armazenados na base de conhecimento KBAM.

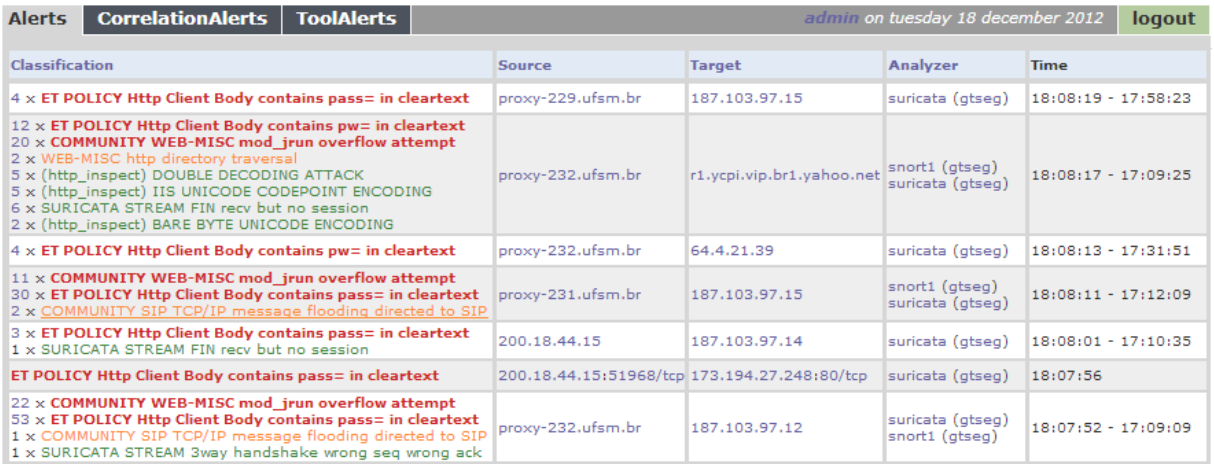


Figura 4.5: Lista de alertas detectados na rede da UFSM.

Os alertas destacados na Figura 4.5 são classificados de acordo com seu nível de gravidade, definido pelos IDSs. Os alertas em cor vermelha representam os eventos com uma gravidade alta, os eventos em cor laranja destacam os alertas com gravidade média e os eventos em cor verde são os alertas com gravidade baixa. Além do nível de gravidade destacado pelas cores, é

possível identificar a origem e o destino do ataque, representados respectivamente nas colunas *Source* e *Target*, e também da data e hora de geração do evento e o sensor (*Analyzer*) que disparou o alerta.

Os contadores dos diversos parâmetros coletados, que também estão armazenados na base de conhecimento KBAM, possibilitam o acompanhamento das equipes de segurança do tráfego da rede, permitindo a identificação de mudanças anormais. A Tabela 4.1 apresenta o número de pacotes de alguns parâmetros capturados nos dois pontos de coleta de dados na rede da instituição (Coperves e CPD) no período de um dia.

Tabela 4.1: Resultados da quantificação do tráfego da rede.

Parâmetro	**Coperves**	**CPD**
TCP	12664888	2288481016
TCP Flag SYN	131032	47316208
TCP Flag SYN-ACK	162512	21332392
TCP Flag ACK	10663832	1846000960
HTTP Porta Origem 80	7325648	1067397576
HTTP Porta Destino 80	4505528	479580104
HTTP GET	410144	36643480
UDP	205208	43732952
IMAP / POP	0	6111360
SIP	0	1593296

O tráfego de redes é irregular, variando no decorrer do tempo. As Figuras 4.6, 4.7, 4.8, 4.9 e 4.10 apresentam o tráfego dos protocolos TCP, UDP e das Flags TCP SYN e TCP SYN-ACK coletadas na rede da Coperves e do CPD e que está armazenado na base de conhecimento KBAM.

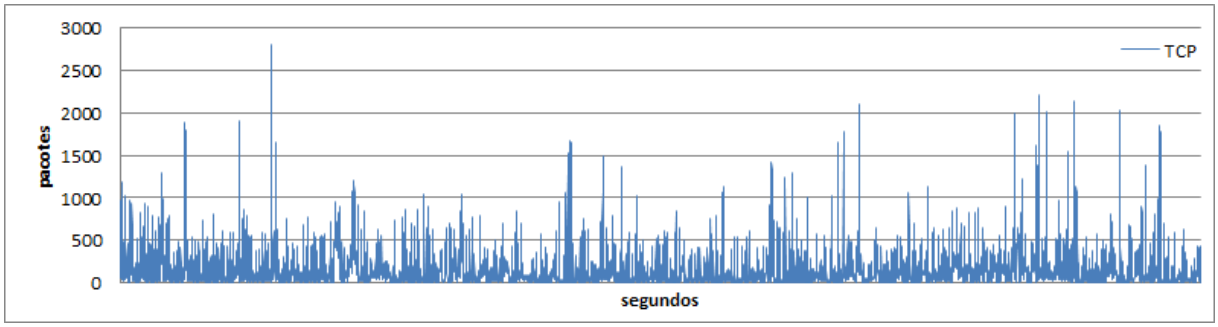


Figura 4.6: Tráfego do protocolo TCP na rede da Coperves.

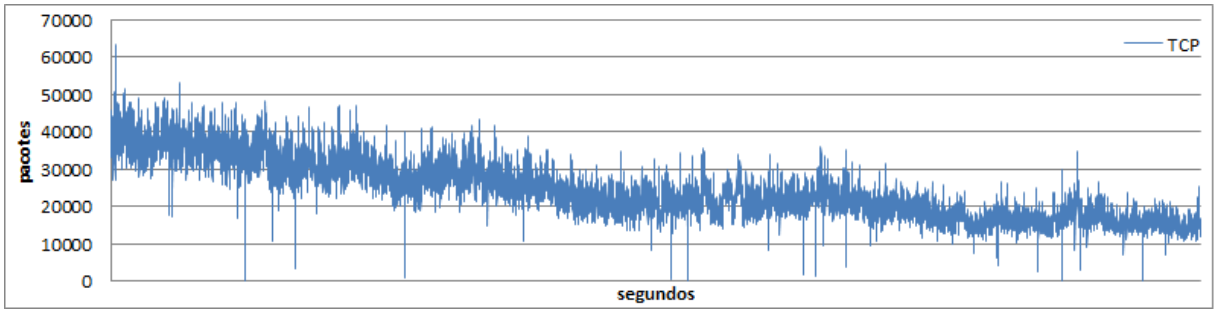


Figura 4.7: Tráfego do protocolo TCP na rede do CPD.

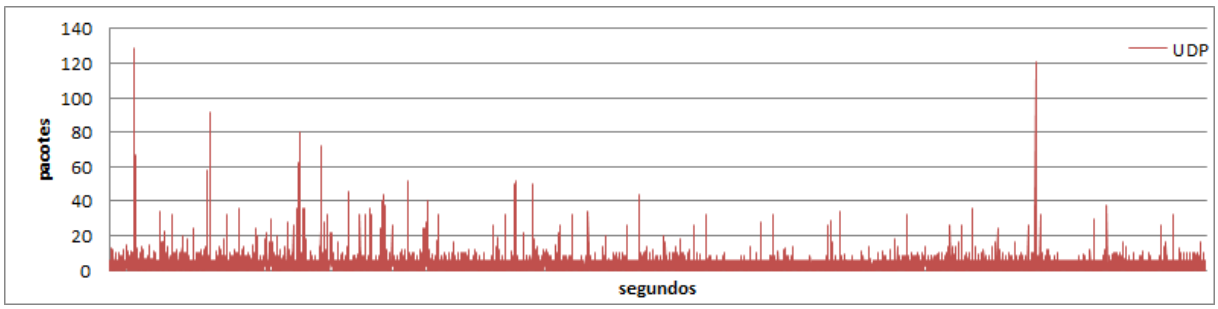


Figura 4.8: Tráfego do protocolo UDP na rede da Coperves.

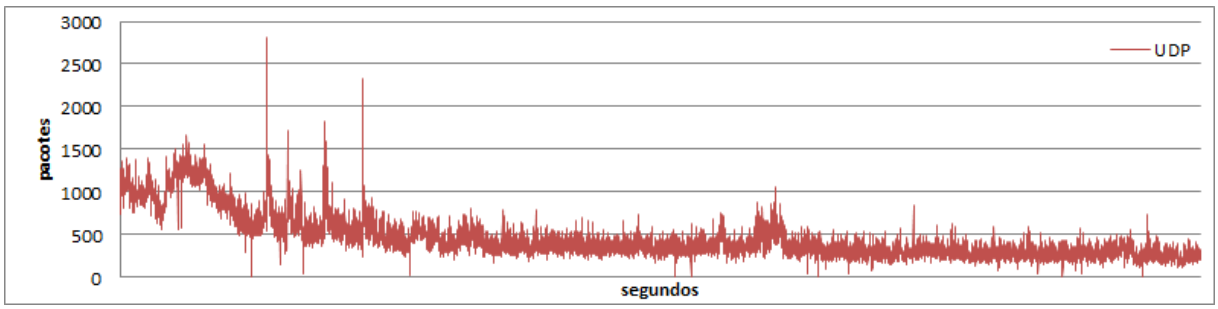


Figura 4.9: Tráfego do protocolo UDP na rede do CPD.

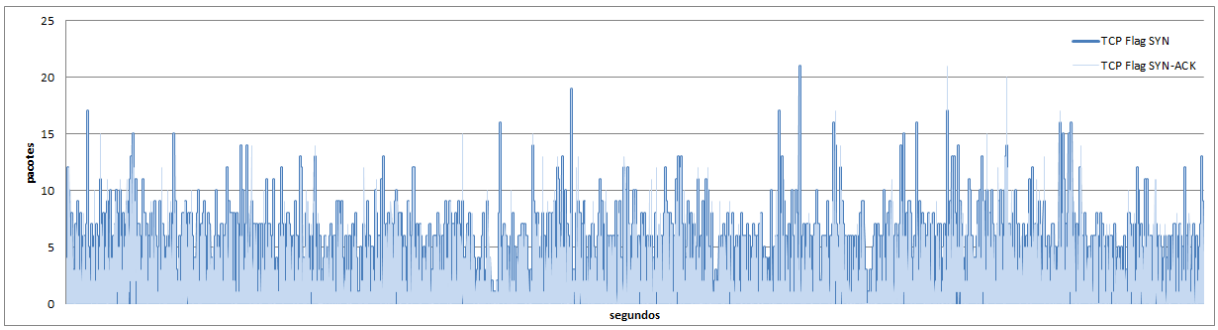


Figura 4.10: Tráfego das Flags TCP SYN e TCP SYN-ACK coletados na rede da Coperves.

Os gráficos das Figuras 4.6, 4.7, 4.8, 4.9 e 4.10 apresentam o tráfego dos protocolos TCP, UDP e das Flags TCP SYN e TCP SYN-ACK e auxiliam, de uma forma visual, a equipe de segurança na representação de mudanças anormais. A utilização de gráficos para representar o tráfego dos protocolos é importante, pois potencializa a visualização de um padrão do trá-

fego e também a identificação de mudanças abruptas, direcionando as atividades da equipe de segurança na confirmação de atividades anormais.

Nos contadores do tráfego da rede também é possível aplicar algoritmos de detecção de intrusão baseados em anomalias de fluxo. A utilização de técnicas baseadas em anomalias potencializa a detecção de ataques desconhecidos, que provocam comportamentos diferentes dos padrões do tráfego e auxiliam as equipes de segurança na detecção de novos ataques. Existem diversas técnicas de detecção de anomalias na literatura, dentre elas, destacam-se os trabalhos (AZEVEDO et al., 2012), (MOZZAQUATRO et al., 2011a) e (MOZZAQUATRO et al., 2011b).

Estas características representadas no modelo de dados e armazenadas na base de conhecimento KBAM contemplam o primeiro nível do modelo de Endsley, fazendo com que a equipe de segurança consiga obter informações necessárias para obter ciência das atividades que ocorrem no ambiente de rede da instituição.

4.2.2 Compreensão

O segundo nível do modelo de Endsley (1995) corresponde a compreensão dos eventos que estão ocorrendo no ambiente monitorado. A compreensão é adquirida através de técnicas, ferramentas e procedimentos que os analistas de segurança utilizam para analisar, sintetizar e agregar as evidências identificadas na rede (SALERNO; HINMAN; BOULWARE, 2004).

Os procedimentos adotados para a compreensão dos eventos detectados na rede da UFSM, correspondem a execução de uma série de consultas aos dados da base de conhecimento KBAM, além da visualização detalhada das atividades que estão ocorrendo no ambiente monitorado.

As principais consultas realizadas referem-se a identificação dos eventos que ocorrem em maior frequência, destacando seu nível de gravidade, além da possível origem e do alvo do evento. A partir da execução desta atividade a equipe de segurança adquire uma compreensão dos eventos que podem representar um maior risco, direcionando as atividades para conter ou minimizar as consequências de um evento.

A identificação dos eventos que ocorreram com maior frequência na rede da UFSM e seu nível de gravidade é obtida através da execução da Figura 4.11.

```
SELECT text,severity, COUNT(alert_idalert)

  FROM kbam.classification

    LEFT JOIN kbam.alert
      ON (alert_idalert = idalert)

    LEFT JOIN kbam.assessment
      ON (assessment_idassessment=idassessment)

    INNER JOIN kbam.impact
      ON (idimpact=impact_idimpact)

    GROUP BY text,severity

    ORDER BY severity, COUNT(alert_idalert) DESC;
```

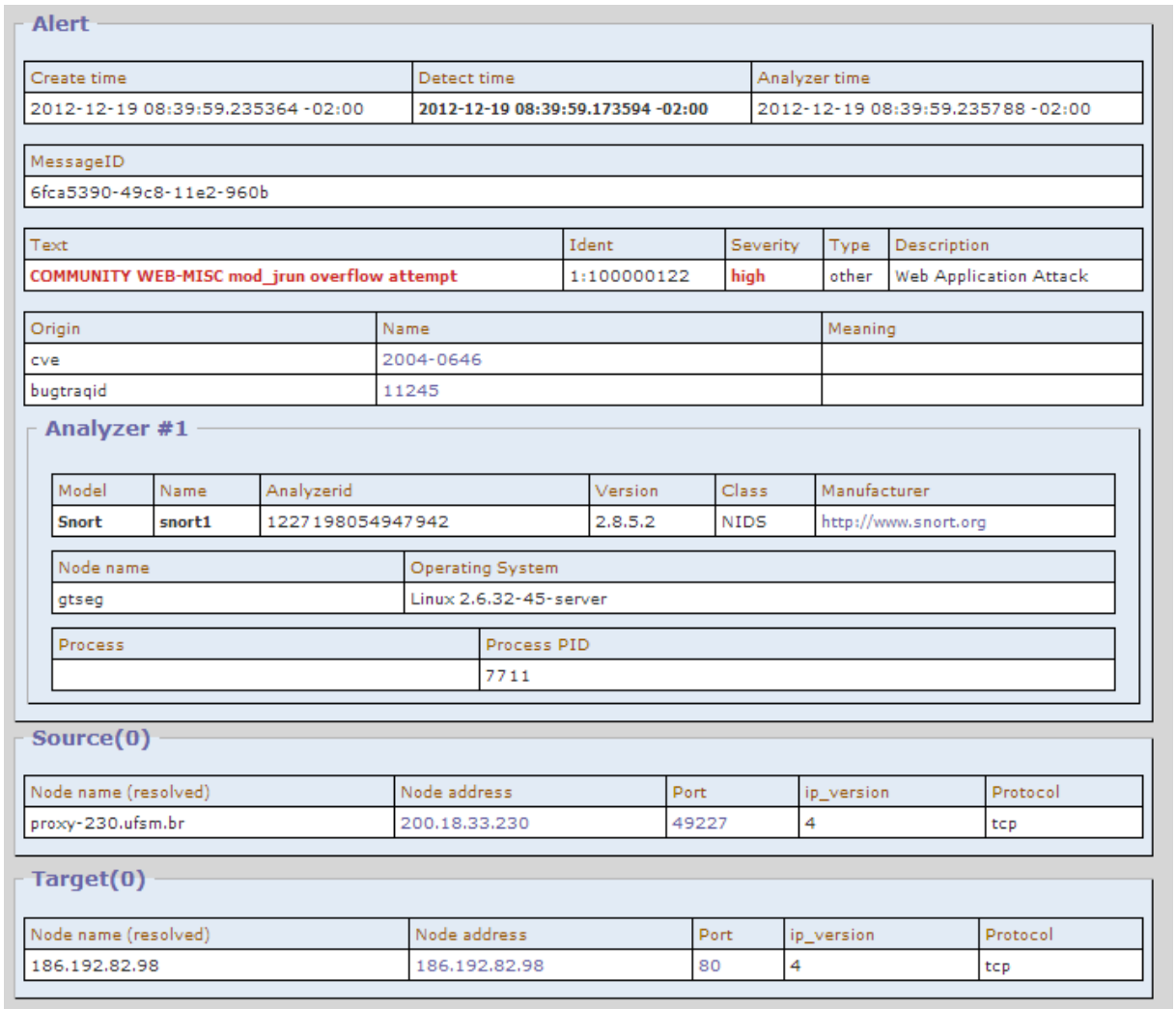
Figura 4.11: Rotina para identificar os principais alertas detectados.

A rotina apresentada na Figura 4.11 é executada e tem seu resultado demonstrado na Tabela 4.2. A Tabela 4.2 destaca os alertas detectados com maior frequência na rede da instituição. Alguns dos alertas gerados pelos sensores, podem ser considerados como falsos positivos, ou seja, o sensor detectou como um ataque, mas na verdade o evento não é um ataque. Deste modo, uma das tarefas da equipe de segurança é analisar as atividades para determinar se o mesmo é realmente classificado como um ataque. Assim sendo, a equipe de segurança pode realizar uma análise detalhada do evento através da interface *Prewikka* que apresenta os dados dos eventos detectados e que estão armazenados na base de conhecimento KBAM.

Tabela 4.2: Alertas mais frequentes no estudo de caso.

Alerta	**Gravidade**	**Quantidade**
COMMUNITY WEB-MISC mod_jrun overflow attempt	high	69686
WEB-MISC weblogic/tomcat .jsp view source attempt	high	8745
ET POLICY Http Client Body contains pass= in cleartext	high	4134
WEB-ATTACKS mail command attempt	high	3890
WEB-PHP viewtopic.php access	high	2784
NETBIOS SMB-DS Session Setup AndX request unicode username overflow attempt	high	1650
ET POLICY Dropbox Client Broadcasting	high	48
ICMP redirect host	medium	154815
COMMUNITY SIP TCP/IP message flooding directed to SIP proxy	medium	58391
SNMP request udp	medium	18852
WEB-MISC Invalid HTTP Version String	medium	8694
SNMP public access udp	medium	7050
SURICATA STREAM ESTABLISHED packet out of window	low	135667
SURICATA STREAM FIN recv but no session	low	38295
SURICATA STREAM ESTABLISHED invalid ack	low	37062
SURICATA STREAM 3way handshake with ack in wrong dir	low	26738

O detalhamento refere-se a identificação dos usuários, processos, serviços e arquivos relacionados aos eventos e auxiliam a equipe de segurança no entendimento e confirmação dos eventos detectados na rede monitorada. A Figura 4.12 apresenta através da interface *Prewikka*, o detalhamento do alerta detectado com mais frequência na rede da instituição e conforme apresentado na Tabela 4.2 é o alerta classificado como *COMMUNITY WEB-MISC mod_jrun overflow attempt*.



Alert

Create time	Detect time	Analyzer time
2012-12-19 08:39:59.235364 -02:00	**2012-12-19 08:39:59.173594 -02:00**	2012-12-19 08:39:59.235788 -02:00

MessageID
6fca5390-49c8-11e2-960b

Text	Ident	Severity	Type	Description
COMMUNITY WEB-MISC mod_jrun overflow attempt	1:100000122	high	other	Web Application Attack

Origin	Name	Meaning
cve	2004-0646	
bugtraqid	11245	

Analyzer #1

Model	Name	Analyzerid	Version	Class	Manufacturer
Snort	**snort1**	1227198054947942	2.8.5.2	NIDS	http://www.snort.org

Node name	Operating System
gtseg	Linux 2.6.32-45-server

Process	Process PID
	7711

Source(0)

Node name (resolved)	Node address	Port	ip_version	Protocol
proxy-230.ufsm.br	200.18.33.230	49227	4	tcp

Target(0)

Node name (resolved)	Node address	Port	ip_version	Protocol
186.192.82.98	186.192.82.98	80	4	tcp

Figura 4.12: Detalhamento de um alerta na interface *Prewikka*.

O detalhamento do alerta *COMMUNITY WEB-MISC mod_jrun overflow attempt* apresentado na Figura 4.12 destaca a hora de criação, detecção e envio do alerta pelo analisador. O detalhamento também apresenta a classificação do alerta, apresentando a descrição e seu nível de gravidade, além da regra do IDS que gerou o alerta (atributo *Ident*). Conforme observado na Figura 4.12 o alerta possui um nível de gravidade alta e é classificado como um ataque de aplicação *web*. Além disso, o detalhamento do alerta também apresenta as informações do sensor

(IDS) responsável pela criação do alerta, destacando a versão e endereço em que o sensor está hospedado, além de informações como o identificador do processo relacionado ao evento.

Outra informação importante visualizada no detalhamento do alerta é a identificação dos endereços de origem (*Source*) e alvo do evento (*Target*), tais informações permitem um entendimento de forma mais abrangente dos eventos que ocorrem na rede da instituição.

Considerando os ataques que ocorrem com mais frequência na rede da instituição, é realizada uma rotina de consulta para identificar quais os principais endereços que originaram os alertas dos ataques.

A origem dos alertas está armazenada na entidade *Source* e indica o endereço de IP que gerou a atividade maliciosa identificada pelo sensor (IDS). A Figura 4.13 apresenta a rotina para a identificação das origens e descreve o resultado na Tabela 4.3.

```
SELECT severity,
       address,
       COUNT(kbam.classification.alert_idalert)

  FROM kbam.classification

    INNER JOIN kbam.alert
      ON (alert_idalert
            = idalert)

    INNER JOIN kbam.assessment
      ON (assessment_idassessment
            = idassessment)

    INNER JOIN kbam.impact
      ON (idimpact
            = impact_idimpact)

    INNER JOIN kbam.source
      ON (kbam.source.alert_idalert
            = idalert)

    INNER JOIN kbam.address
      ON (kbam.source.node_idnode
            = kbam.address.node_idnode)

    GROUP BY severity,
         address

    ORDER BY severity,
         COUNT(kbam.classification.alert_idalert) DESC;
```

Figura 4.13: Rotina para identificar as principais origens dos alertas.

A Tabela 4.3 apresenta os principais endereços de rede que originaram os alertas na rede da instituição.

Tabela 4.3: Principais origens dos alertas.

Gravidade	Endereço	Número de Alertas
high	200.18.33.232	203204
high	200.18.33.229	58368
high	200.132.24.254	49192
high	200.18.44.15	26100
high	200.18.33.228	16348
medium	192.168.136.207	625748
medium	200.18.33.232	58580
medium	200.18.33.229	109920
low	200.18.33.232	142216
low	200.18.33.229	109920
low	187.103.97.13	94896

Conforme os dados apresentados na Tabela 4.3, há endereços de rede que originaram um montante de alertas com diferentes níveis de gravidade. A identificação desses endereços é importante para equipe de segurança, pois direciona as atividades no que refere-se a criação de medidas de segurança nas principais máquinas que originam os alertas.

De mesmo modo, considerando os ataques mais frequentes é realizado uma rotina para identificar os principais alvos dos eventos. Os alvos dos ataques estão armazenados na entidade *Target*, indicando o endereço de rede que possivelmente é o alvo da atividade maliciosa.

A Figura 4.14 apresenta a rotina para a identificação dos alvos e descreve o resultado na Tabela 4.4.

```
SELECT severity,
     address,
     COUNT(kbam.classification.alert_idalert)

  FROM kbam.classification

    INNER JOIN kbam.alert
      ON (alert_idalert = idalert)

    INNER JOIN kbam.assessment
      ON (assessment_idassessment=idassessment)

    INNER JOIN kbam.impact
      ON (idimpact=impact_idimpact)

    INNER JOIN kbam.target
      ON (kbam.target.alert_idalert = idalert)

    INNER JOIN kbam.address
      ON (kbam.target.node_idnode = kbam.address.node_idnode)

    GROUP BY severity ,
           address

    ORDER BY severity,
           COUNT(kbam.classification.alert_idalert) DESC;
```

Figura 4.14: Rotina para identificar os principais alvos dos alertas.

A Tabela 4.4 apresenta os endereços de rede que são os principais alvos dos alertas detectados na rede da instituição.

Tabela 4.4: Principais alvos dos alertas.

Gravidade	Endereço	Número de Alertas
high	74.125.137.116	33152
high	131.253.14.85	13272
high	74.125.234.163	12152
high	74.125.234.168	11932
high	74.125.234.169	11820
medium	122.228.177.234	446012
medium	203.250.118.23	102748
medium	65.111.174.19	77208
medium	141.212.121.10	27768
low	201.11.195.120	43432
low	200.132.35.25	9796
low	200.18.33.18	4276
low	200.18.45.220	1304

Os dados destacados na Tabela 4.4 apresentam os endereços de rede das máquinas que são alvos das mensagens dos alertas detectados da rede da UFSM. A identificação dessas informações também é importante para a equipe de segurança identificar as máquinas que estão sendo mais visadas, sendo alvo de um grande número de alertas.

Os resultados apresentados nas Tabelas 4.2, 4.3 e 4.4 destacam diversos dados que auxiliam a equipe de segurança a compreender os eventos que ocorrem na rede da instituição, identificando as principais ameaças, além da procedência dos ataques e seus principais alvos. Além disso, a análise das mensagens de alertas através da interface *web Prewikka* permite uma visualização detalhada dos alertas detectados, potencializando as atividades da equipe de segurança.

4.2.3 Projeção

Após a análise e compreensão dos dados que estão armazenados na base de conhecimento KBAM é possível fazer predições de medidas de respostas para aumentar o nível de segurança no ambiente monitorado. Esta tarefa corresponde ao terceiro nível do modelo de consciência situacional de Endsley (1995).

A projeção de medidas de resposta a um evento é realizado com base na análise das informações históricas que estão armazenadas na base de conhecimento KBAM. Nesta etapa, os analistas de segurança utilizam o conhecimento armazenado na base KBAM realizando um levantamento das medidas de respostas aplicadas aos eventos similares ocorridos anteriormente.

Uma das formas de projetar as respostas a serem aplicadas a um evento é através de um levantamento de medidas de respostas históricas com base no número da assinatura (regra) que originou o alerta. Esta rotina recupera as medidas de respostas aplicadas a alertas gerados a partir da mesma assinatura de ataque. A Figura 4.15 apresenta a rotina para a recuperação de medidas de respostas com base na assinatura de um ataque.

```
SELECT analyzerid,
       ididrefmessage,
       description.description,
       response_idresponse,
       config_idconfig,
       react_idreact

 FROM kbam.idrefmessage

   INNER JOIN kbam.description
     ON (description_iddescription
                = description.iddescription)

   LEFT JOIN kbam.alertident
     ON (ididrefmessage
         = idrefmessage_ididrefmessage)

   WHERE analyzerid IN
   (
     SELECT kbam.alert.ident

       FROM kbam.alert

         LEFT JOIN kbam.classification
           ON (kbam.classification.alert_idalert
                                    =  kbam.alert.idalert)

         WHERE kbam.classification.ident =
         (
           SELECT kbam.classification.ident

             FROM kbam.classification

               LEFT JOIN  kbam.alert
                 ON  (idalert
                     = alert_idalert)

               WHERE kbam.alert.ident
                     = identificadorAlert
         )
   )
```

Figura 4.15: Rotina de recuperação de históricos de medidas de respostas.

Conforme apresentado na Figura 4.15, a equipe de segurança deve inserir na rotina o identificador do alerta que se deseja responder (parâmetro *identificadorAlert*). Baseado no alerta a ser respondido, a rotina busca a identificação da assinatura que foi gerado o alerta e consulta as medidas de respostas que estão armazenadas na base de conhecimento KBAM e que foram aplicadas a eventos gerados a partir da mesma assinatura de ameaça. Assim sendo, as respostas recuperadas da base de conhecimento KBAM estão relacionadas ao evento em que se deseja aplicar uma resposta, através da equivalência da assinatura do ataque. A rotina da Figura 4.15

recupera as medidas de respostas armazenadas e tem seu resultado destacado na Tabela 4.5.

Tabela 4.5: Levantamento de medidas de respostas a alertas com mesma assinatura.

ID Alerta	ID Resposta	Decrição	Tipo de Resposta
1372620	100	Bloqueio	React
1373048	341	Bloqueio endereço IP	React
1373044	102	Notificação	Response
1372620	765	Bloqueio de IP	React

Os dados da Tabela 4.5 destacam as medidas de respostas aplicadas a eventos que foram gerados a partir da mesma regra de detecção do evento em que se deseja responder. Conforme observado, o principal tipo de resposta aplicado a eventos desta classificação refere-se a uma reação (React), aplicando bloqueios em endereços de rede específicos. Assim sendo, a equipe de segurança tem um embasamento de informações históricas armazenadas na base de conhecimento KBAM para apoiar na decisão da resposta ao ataque em potencial.

A partir da identificação do histórico das medidas de respostas aplicadas a eventos similares, gerados pela mesma assinatura de ataque, a equipe de segurança inicia o processo de criação da medida de resposta ao evento selecionado através do Componente IDREF.

A principal atividade da etapa de projeção é o levantamento de medidas de respostas que possam ser utilizadas para embasar a resposta a ser aplicada a atividade maliciosa. A aplicação da medida de resposta ao evento é realizada no último nível do modelo, apresentado na Seção 4.2.4.

4.2.4 Resolução

O último nível do modelo de consciência situacional foi proposto por McGuiness e Foy (2000), adicionando um quarto nível ao modelo original de Endsley (1995). Este nível refere-se a aplicação de contramedidas para tratar os riscos identificados no ambiente monitorado.

Neste nível ocorre a criação da medida de resposta a ser aplicada ao evento. Tendo como base o alerta classificado como *WEB-ATTACKS mail command attempt*, destacado na Tabela 4.2, e o levantamento do histórico das contramedidas aplicadas a eventos gerados pela mesma assinatura de ataque (Tabela 4.5), é apresentado, nas Figuras 4.16 e 4.17, o processo de criação da mensagem de resposta a ser aplicado ao evento.

O processo de criação da medida de resposta é iniciado com a seleção de um alerta na tela inicial do Componente IDREF (Figura 4.4). Após a seleção do alerta, é necessário escolher o tipo de resposta a ser aplicado ao evento (*Response*, *React* ou *Config*), com base no levanta-

mento das medidas de respostas (Tabela 4.5), a resposta a ser aplicada ao evento selecionado é do tipo *React*. A Figura 4.16 apresenta a interface do Componente IDREF aonde são inseridas as informações necessárias para criar a medida de resposta ao evento selecionado.

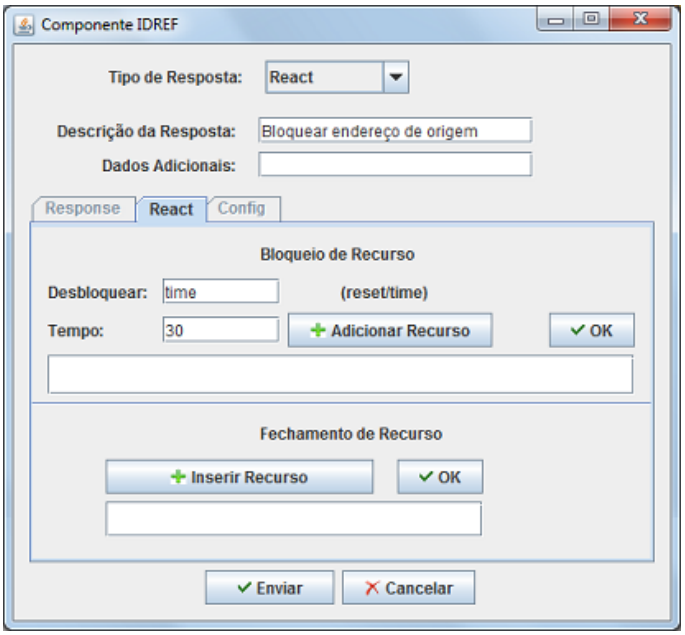


Figura 4.16: Criação de uma mensagem de resposta do tipo *React* no Componente IDREF.

Conforme apresenta a Figura 4.16, uma resposta do tipo *React* está sendo criada, onde estão sendo inseridas as informações de tempo para o bloqueio de um recurso. Um recurso pode ser um processo, um nodo, um serviço, uma lista de usuários ou uma lista de arquivos. Na medida de resposta aplicada ao evento *WEB-ATTACKS mail command attempt* configura-se um bloqueio a um nodo da rede, ou seja, o nodo específico que originou a mensagem alerta. A adição do recurso a ser inserido na medida de resposta é apresentado na Figura 4.17.

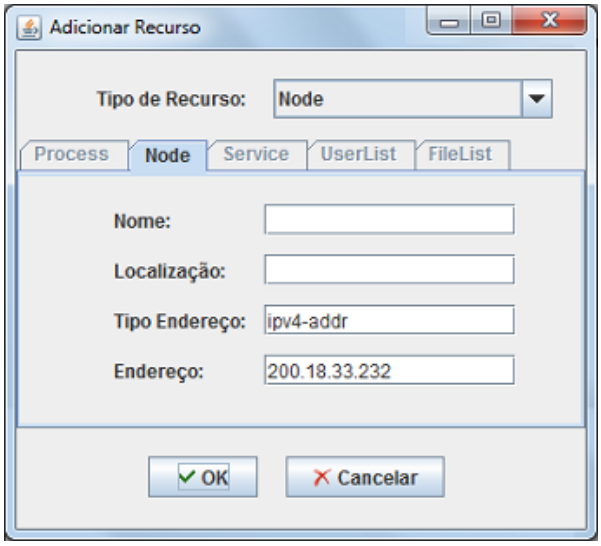


Figura 4.17: Adicionando um *Node* na medida de resposta.

A Figura 4.17 apresenta o processo de inserção de um recurso na medida de resposta. Após a criação da resposta, a mesma é vinculada ao alerta que a originou e também é inserida na base de conhecimento KBAM, estando disponível para auxiliar a equipe de segurança na decisão de novas medidas de respostas a ataques futuros. Além disso, as medidas de respostas armazenadas na base de conhecimento KBAM podem ser refinadas a cada ciclo do processo de criação de uma resposta a eventos semelhantes, pois as medidas de respostas históricas potencializam a decisão da equipe de segurança em resposta a eventos futuros.

4.3 Considerações Parciais

Este capítulo apresentou um estudo de caso aplicado na rede de computadores da UFSM para realizar a prova de conceito da proposta apresentada. No estudo de caso foi implementado o modelo de dados e inserido a base de conhecimento KBAM em uma arquitetura de rede real. A arquitetura é formada por sistemas de detecção de intrusão baseados em assinatura para a geração dos alertas de detecção de intrusão, um *sniffer* para a captura do tráfego da rede e um componente para a geração das medidas de respostas.

Os IDSs da arquitetura foram configurados para trabalhar como sensores integrados com a ferramenta Prelude e gerar os alertas no padrão de formatação de dados IDMEF. Os alertas gerados são armazenados no banco de dados próprio da ferramenta Prelude e encaminhados para a base de conhecimento KBAM através de uma *trigger*. Os dados dos pacotes que trafegam na rede são direcionados diretamente para a base de conhecimento KBAM. As medidas de respostas são criadas em um processo cíclico com interação humana da equipe de segurança,

que cria novas medidas de respostas, refinando as medidas já existentes.

O estudo de caso coletou diversos dados que foram armazenados na base de conhecimento KBAM. Desta forma, com base nos dados armazenados foi possível construir uma consciência situacional do ambiente de rede da instituição, contemplando um dos principais objetivos dos *Internet Early Warning Systems*. O modelo de consciência situacional criado por Endsley e expandido por McGuiness e Foy foi aplicado aos dados da base de conhecimento KBAM e através de cada nível do modelo, foi demostrado como os dados coletados na rede da UFSM permitem ter a consciência situacional do ambiente de rede da instituição.

5 CONCLUSÕES E CONSIDERAÇÕES FINAIS

O acréscimo no número de ataques ocorridos nos últimos anos tem demandado a implantação de técnicas e ferramentas para auxiliar as empresas no monitoramento de suas infraestruturas de redes de computadores e também na identificação de atividades maliciosas. Além disso, o aumento no volume de dados que trafegam nas redes de computadores tem tornado os sistemas tradicionais de monitoramento e detecção de atividades maliciosas limitados. Neste contexto, diversos pesquisadores tem explorado a construção de *Internet Early Warning Systems*.

Diante desta necessidade, este trabalho apresentou um modelo de dados de uma base de conhecimento para um *Internet Early Warning System*. Armazenando dados de mensagens de alertas gerados por sistemas de detecção de intrusão, do comportamento do tráfego da rede e um conhecimento das medidas aplicadas em resposta a um alerta, a base de conhecimento KBAM atende os diferentes aspectos necessários para a construção de uma base de conhecimento de um *Internet Early Warning System* voltada ao monitoramento de ataques.

Ao modelar os dados explorando os padrões de formatação de dados IDREF e IDMEF, a base de conhecimento KBAM pode ser inserida em qualquer infraestrutura de rede que possui IDSs que utilizam esses padrões, podendo ser utilizada como um componente que armazena dados de diferentes aspectos da rede, que são essenciais para o monitoramento de ataques e a construção de uma consciência situacional do ambiente em que se está monitorando.

A realização de um estudo de caso na infraestrutura de redes de computadores da Universidade Federal de Santa Maria permitiu destacar a aplicabilidade do modelo de dados da base de conhecimento KBAM em um ambiente de rede em produção e realçar as vantagens de sua utilização: o armazenamento de dados coletados através de sistemas de detecção integrados; a representação de dados através de padrões de formatação de dados existentes na literatura; a quantificação dos contadores dos pacotes que trafegam na rede e o armazenamento do conhecimento agregado no processo cíclico de criação de medidas de respostas aplicadas aos eventos maliciosos.

Adicionalmente, os dados armazenados na base de conhecimento KBAM permitiram a construção de uma consciência situacional do ambiente de rede da instituição. Através da aplicação do modelo de consciência situacional foi possível auxiliar as equipes de segurança a perceber e compreender as atividades ocorridas no ambiente monitorado, além de projetar e implementar as medidas de respostas a ataques em potencial.

5.1 Trabalhos Futuros

Como trabalho futuro sugere-se a implementação da interface *web* KBAM para a visualização dos dados armazenados na base de conhecimento KBAM, permitindo as equipes de segurança maior agilidade na compreensão de eventos e no monitoramento da infraestrutura de redes de computadores em que a base de conhecimento KBAM está inserida.

REFERÊNCIAS

AZEVEDO, R.; MOZZAQUATRO, B.; CAPPO, C.; SCHAERER, C.; KOZAKEVICIUS, A.; NUNES, R. Detecção de ataques DoS utilizando a transformada Wavelet 2D. **XXXVIII Conferência Latinoamericana en Informática**, Medelin, Colômbia, 2012. Medelin, Colômbia.

BASS, T. Multi-sensor data fusion for next generation distributed intrusion detection systems. In: IRIS NATIONAL SYMPOSIUM ON SENSOR AND DATA FUSION, 1999, COAST Laboratory, Purdue University. **Anais...** [S.l.: s.n.], 1999.

BASTKE, S.; DEML, M.; SCHMIDT, S. Internet Early Warning Systems - overview and architecture. In: EUROPEAN WORKSHOP ON INTERNET EARLY WARNING AND NETWORK INTELLIGENCE, 2010, Hamburg, Germany. **Anais...** [S.l.: s.n.], 2010.

BRO. **The Bro Network Security Monitor**. Disponível em: <http://www.bro-ids.org/>. Acesso em: 10 out. 2012.

CERT.BR. **Centro de Estudos, Resposta e Tratamento de Incidentes no Brasil**. Disponível em: <http://www.cert.br/>. Acesso em: 25 out. 2012.

DEBAR, H.; CURRY, D.; FEINSTEIN, B. **The Intrusion Detection Message Exchange Format (IDMEF)**. RFC 4765. March 2007.

ENDSLEY, M. R. Toward a theory of situation awareness in dynamic systems. **Human Factors**, [S.l.], v.37, n.1, p.32–64, 1995.

FLIOR, E.; ANAYA, T.; MOODY, C.; BEHESHTI, M.; HAN, J.; KOWALSKI, K. A knowledge-based system implementation of intrusion detection rules. **Information Technology: New Generations (ITNG)**, Las Vegas, NV, p.738–742, April 2010.

GOGULF. **60 SECONDS - THINGS THAT HAPPEN ON INTERNET EVERY SIXTY SECONDS [INFOGRAPHIC]**. Disponível em: <http://www.go-gulf.com/blog/60-seconds>. Acesso em: 28 nov. 2012.

GOLLING, M.; STELTE, B. Requirements for a future EWS - Cyber Defence in the Internet of the future. In: INTERNATIONAL CONFERENCE ON CYBER CONFLICT (ICCC), 3., 2011, Tallinn, Estonia. **Anais...** [S.l.: s.n.], 2011. p.1–16.

GREGOIRE, M.; BEAUDOIN, L. Visualisation for Network Situational Awareness in Computer Network Defence. In: VISUALISATION AND THE COMMON OPERATIONAL PICTURE, 2005, Neuilly-sur-Seine, France. **Anais...** RTO, 2005.

GRUBER, T. R. Toward principles for the design of ontologies used for knowledge sharing. **Int. J. Hum.-Comput. Stud.**, Duluth, MN, USA, v.43, n.5-6, p.907–928, dec 1995.

HESSE, M.; POHLMANN, N. Internet Situation Awareness. In: CRIME RESEARCHERS SUMMIT, 2008, Atlanta, GA. **Anais...** [S.l.: s.n.], 2008. p.1–9.

KIZZA, J. M. **A Guide to Computer Network Securit**. New York, NY: Springer, 2005. 538p.

KRUEGEL, C.; VALEUR, F.; VIGNA, G. **Intrusion Detection and Correlation Challenges and Solutions**. Santa Clara, USA: Springer-Verlag TELOS, 2004. 118p.

LIMA, I.; DEGASPARI, J.; SOBRAL, J. Intrusion detection through artificial neural networks. **Network Operations and Management Symposium (NOMS)**, Salvador, Bahia, p.867–870, April 2008.

LIU, X.; WANG, H.; LAI, J.; LIANG, Y. Network security situation awareness model based on heterogeneous multi-sensor data fusion. In: COMPUTER AND INFORMATION SCIENCES, 2007. ISCIS 2007. 22ND INTERNATIONAL SYMPOSIUM ON, 2007, Ankara. **Anais...** [S.l.: s.n.], 2007. p.1 –6.

MCGUINNESS, B.; FOY, L. A Subjective Measure of SA: the crew awareness rating scale (cars). **First Human Performance, Situation Awareness, and Automation Conference**, Savannah, Georgia, 2000.

MORE, S.; MATTHEWS, M.; A. JOSHI, T. F. A Knowledge-Based Approach to Intrusion Detection Modeling. **Security and Privacy Workshops (SPW)**, [S.l.], p.75–81, May 2012.

MOZZAQUATRO, B.; AZEVEDO, R.; CAPPO, C.; SCHAERER, C.; KOZAKEVICIUS, A.; NUNES, R. Anomaly-based Techniques for Web Attacks Detection. In: JOURNAL OF APPLIED COMPUTING RESEARCH, 2011. **Anais...** [S.l.: s.n.], 2011. v.2, p.111–120.

MOZZAQUATRO, B.; AZEVEDO, R.; CAPPO, C.; SCHAERER, C.; KOZAKEVICIUS, A.; NUNES, R. Detecção de Ataques Web usando Técnicas de Detecção de Anomalias. In: ESCOLA REGIONAL DE REDES DE COMPUTADORES, 2011, São Leopoldo, Rio Grande do Sul, Brasil. **Anais...** [S.l.: s.n.], 2011. v.9, p.101–104.

NORTHCUTT, S.; NOVAK, J. **Network Intrusion Detection**. 3.ed. New Riders Publishing, 2002. 512p.

ONWUBIKO, C. Functional Requirements of Situational Awareness in Computer Network Security. In: INTELLIGENCE AND SECURITY INFORMATICS, 2009. ISI '09. IEEE INTERNATIONAL CONFERENCE ON, 2009, Dallas, TX. **Anais...** [S.l.: s.n.], 2009. p.209–213.

PETRI, G.; NUNES, R. C.; JUNIOR, T. C.; SANTOS, O. M. Modelagem de uma Base de Conhecimento para o Monitoramento de Ataques. In: ESCOLA REGIONAL DE REDES DE COMPUTADORES, 2012, Pelotas, RS, Brasil. **Anais...** ERRC 2012, 2012. p.75–78.

PETRI, G.; NUNES, R. C.; OROZCO, V.; JUNIOR, T. C.; SANTOS, O. M. dos. KBAM: data model of a knowledge base for monitoring attacks. In: LADC 2013 - FAST ABSTRACT, 2013, Rio de Janeiro, Brazil. **Anais...** [S.l.: s.n.], 2013.

PETRI, G.; NUNES, R. C.; OROZCO, V.; JUNIOR, T. C.; SANTOS, O. M. dos. Building Situation Awareness to Monitor Critical Infrastructures. In: LADC 2013 - FAST ABSTRACT, 2013, Rio de Janeiro, Brazil. **Anais...** [S.l.: s.n.], 2013.

POSTGRESQL. **PostgreSQL, Inc.** Disponível em: http://www.pgsql.com/. Acesso em: 05 set. 2012.

PRELUDE. **PRELUDE SIEM web site**. Disponível em: <http://www.prelude-technologies.com/en/welcome/index.html>. Acesso em: 29 jun. 2012.

RICCI, G. **Betrachtung der vom ias gesammelten kommunikationsparameter auf relevanz zur anomalie und angriffserkennung (evaluation of the relevance for the detection of abnormalities and attacks of the communication parameters collected by the internet analysis system)**. 2008. Dissertação (Mestrado) — University of Applied Sciences, Gelsenkirchen, Germany.

RUSSEL, S.; NORVING, P. **Artificial Inteligence**: a modern approach. 2.ed. New York: Prentice Hall, 2003. 1080p.

SÁ BRANDÃO, J. E. M. de. **Composições de IDSs**: viabilizando o monitoramento de segurança em ambientes de larga escala. 2007. Dissertação (Mestrado) — Curso de Pós-Graduação em Engenharia Elétrica, Universidade Federal de Santa Catarina, Florianópolis, SC, Brasil.

SALERNO, J.; HINMAN, M.; BOULWARE, D. Building a framework for situation awareness. In: SEVENTH INTERNATIONAL CONFERENCE ON INFORMATION FUSION, 2004, Mountain View, CA. **Proceedings...** International Society of Information Fusion, 2004. v.I, p.219–226.

SALERNO, J.; HINMAN, M.; BOULWARE, D.; BELLO, P. Information fusion for situational awareness. In: INFORMATION FUSION, 2003. PROCEEDINGS OF THE SIXTH INTERNATIONAL CONFERENCE OF, 2003. **Anais...** [S.l.: s.n.], 2003. v.1, p.507 –513.

SILVA, P. F. da. **Extensão do Modelo IDWG para Detecção de Intrusão em Ambientes Computacionais**. 2004. Dissertação (Mestrado) — Programa de Pós-Graduação em Ciência da Computação, Universidade Federal de Santa Catarina, Florianópolis, SC, Brasil.

SILVA, P. F.; WESTPHALL, C. B. An Intrusion Answer Model Compatible with the Alerts IDWG Model. **Network Operations and Management Symposium (NOMS)**, Vancouver, BC, p.1–4, April 2006.

SNORT. **Snort Home Page**. Disponível em: <http://www.snort.org/>. Acesso em: 11 jul. 2012.

SNORT. **About Snort**. Disponível em: <http://www.snort.org/snort>. Acesso em: 12 jul. 2012.

SURICATA. **Open Information Security Fundation**. Disponível em: <http://96.43.130.5/index.php/downloads>. Acesso em: 29 jun. 2012.

SYMANTEC. **Symantec Internet Security Threat Report Trends for 2011**. Disponível em: <http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf>. Acesso em: 15 jun. 2012.

UNDERCOFFER, J.; JOSHI, A.; FININ, T.; PINKSTON, J. Using DAML+OIL to classify intrusive behaviours. **The Knowledge Engineering Review**, [S.l.], v.18, p.221–241, 2004.

WICKENS, C. D. Situation Awareness: review of mica endsley's 1995 articles on situation awareness theory and measurement. **Human Factors**, [S.l.], v.50, n.3, p.397–403, 2008.

WIRESHARK. **Wireshark**. Disponível em: < http://www.wireshark.org/>. Acesso em: 30 dez. 2012.

APÊNDICE A PUBLICAÇÕES

- As publicações realizadas até o momento relativas ao trabalho são:

  PETRI, G. ; CEOLIN JUNIOR, T. ; NUNES, R. C. ; SANTOS, O. M. **Modelagem de uma Base de Conhecimento para o Monitoramento de Ataques**. In: Escola Regional de Redes de Computadores, Pelotas - RS. Anais da ERRC, 2012. v. 10. p. 75-78.

  PETRI, G. ; CEOLIN JUNIOR, T. ; NUNES, R. C. ; SANTOS, O. M. **O uso da ferramenta Prelude no monitoramento da Internet**. In: Jornada Acadêmica Integrada, Santa Maria - RS. Anais da JAI, 2012. v. 27.

  PETRI, G. ; CEOLIN JUNIOR, T. ; NUNES, R. C. ; SANTOS, O. M. **Monitorando Ataques com a Ferramenta Prelude**. In: Encontro Anual de Tecnologia da Informação, Frederico Westphalen - RS. Anais EATI, 2012. v. 3.

  PETRI, G. ; NUNES, R. C. ; LOPEZ, V. L. O. ; CEOLIN JUNIOR, T. ; SANTOS, O. M. **KBAM: Data Model of a Knowledge Base for Monitoring Attacks**. In: 6th Latin-American Symposium on Dependable Computing, Rio de Janeiro - RJ. Brasil, 2013.

  PETRI, G. ; NUNES, R. C. ; LOPEZ, V. L. O. ; CEOLIN JUNIOR, T. ; SANTOS, O. M. **Building Situation Awareness to Monitor Critical Infrastructures**. In: 6th Latin-American Symposium on Dependable Computing, Rio de Janeiro - RJ. Brasil, 2013.

- Artigos submetidos e em processo de avaliação:

  SBRC 2013 - Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos – Artigo Completo — Modelagem de Dados para o Monitoramento de Ataques em Redes de Computadores

  RESI - Revista Eletrônica de Sistemas de Informação — Uma Base de Conhecimento para a Construção de uma Consciência Situacional Voltada ao Monitoramento de Ataques