# Consciência de Situação Aplicada à Segurança de Ambientes Ubíquos

**Ricardo Borges Almeida**[1], **Roger da Silva Machado**[1],
**Lucas Medeiros Donato**[2], **Ana Marilza Pernas**[1],
**Adenauer Corrêa Yamin**[1]

[1]Programa de Pós-Graduação em Computação (PPGC)
Universidade Federal de Pelotas (UFPel), Pelotas, RS, Brasil

[2]De Montfort University – Cyber Security Centre
Leicester, Reino Unido

{rbalmeida,rdsmachado,marilza,adenauer}@inf.ufpel.edu.br,

lucas.donato@myemail.dmu.ac.uk

***Abstract.*** *The objective of this paper is to present a proposal of a SIEM academic solution, open-source, customizable and simple understandable, which employs the concepts of Situation Awareness. The proposed solution has been developed as a prototype software, applied to middleware for Ubiquitous Computing. Simulations were developed to test the behavior of the solution in detecting security risk situations, which showed a stable solution for creating customized new security rules, flexible, scalable and suitable for Modern Distributed Systems.*

***Resumo.*** *O objetivo deste artigo é apresentar uma proposta de solução de SIEM acadêmica, de código aberto, customizável e de simples compreensão, que emprega os conceitos de Consciência de Situação. A solução proposta foi desenvolvida na forma de um protótipo de software, aplicado a um middleware para Computação Ubíqua. Simulações foram desenvolvidas de forma a testar o comportamento da solução na detecção de situações de risco a segurança, as quais apresentaram a solução estável para criação customizada de novas regras de segurança, com caráter flexível, escalável e adequado aos Sistemas Distribuídos Modernos.*

## 1. Introdução

O desenvolvimento de novas tecnologias da informação, bem como a evolução dos meios de comunicação e troca de dados, têm sido propiciados pela Computação Ubíqua (UbiComp), idealizada por Mark Weiser (1991) [Weiser 1991]. Na UbiComp, tecnologias se tornam mais integradas ao cotidiano das pessoas, nas comunicações, no setor financeiro e até no entretenimento. Infelizmente, todas as facilidades e potencialidades oferecidas por esta evolução também acabam sendo objeto de interesse de pessoas mal intencionadas. Logo, segurança e privacidade são desafios que se tornam potencializados na UbiComp devido à natureza volátil, espontânea, heterogênea e invisível da comunicação nos sistemas ubíquos [Langheinrich 2010].

A preocupação com a Segurança da Informação nas empresas tem aumentado nos últimos anos, e isto é consequência natural do aumento dos crimes realizados via Internet e das perdas financeiras decorrentes [Ponemon 2012]. Atento a este cenário, o Instituto Ponemon, cita em dois de seus relatórios [Ponemon 2012], [Ponemon 2013] que as soluções de SIEM (*Security Information and Event Management*) vem sendo uma boa estratégia tanto no combate à fraude interna, quanto na economia de acordo com a solução de segurança adotada.

Apesar de existirem soluções eficientes de SIEM, responsáveis por colocar esta categoria de solução em primeiro lugar em ambos relatórios do Instituto Ponemon, não foi encontrada uma SIEM com código fonte aberto e desenvolvida no meio acadêmico. A concepção de uma solução de SIEM de código aberto, possui como vantagem a transparência da solução, ou seja, o conhecimento dos algoritmos utilizados e da forma de implementação, além de propiciar uma maior flexibilidade e customização por parte dos usuários, e da possibilidade de auditoria da solução e contribuição no desenvolvimento do software. Como benefício de um projeto proveniente do meio acadêmico, observa-se que estes normalmente possuem uma preocupação quanto a base conceitual, além de gerarem como resultado uma documentação detalhada.

Dentre as soluções de SIEM disponíveis no mercado, é possível identificar uma tendência na utilização dos conceitos relativos a Consciência de Situação [Hewlett-Packard 2014], [McAfee 2013]. Estes conceitos estão diretamente relacionados com o tratamento de eventos, função inerente à uma solução de SIEM, e apresentam como vantagem uma visão global sobre o ambiente, o que é essencial para auxiliar um SOC (*Security Operations Center*), especialmente considerando a atual complexidade dos ambientes computacionais, os quais empregam às vezes até dezenas de tecnologias de fabricantes distintos.

O objetivo central deste trabalho é a concepção de uma solução de SIEM sem custo e de código aberto (FOSS - *Free and Open Source Software*) consciente de situação. Para isto, a solução foi concebida com base em um *middleware* para UbiComp, denominado EXEHDA (*Execution Environment for Highly Distributed Applications*), e explora a Consciência de Situação por meio da correlação de eventos identificados no monitoramento contínuo de logs e de informações sobre o estado do sistema. Os logs são decorrentes da operação dos diversos equipamentos e aplicações existentes na infraestrutura computacional.

O texto do artigo está estruturado da seguinte forma. A seção 2 apresenta os conceitos relacionados tanto a Consciência de Situação como a soluções de SIEM. Na sequência, a seção 3 descreve a solução desenvolvida, para posteriormente a seção 4 discutir o estudo de caso. A seção 5 apresenta os trabalhos relacionados. Finalmente a seção 6 discute algumas contribuições alcançadas ao final deste trabalho e os possíveis trabalhos futuros.

## 2. Base Conceitual

Esta seção apresenta os conceitos inerentes à Consciência de Situação e à soluções de SIEM no que tange a área de abrangência do trabalho desenvolvido.

### 2.1. Consciência de Situação

O termo **situação** consiste de um conjunto de elementos contextuais de interesse instanciados relacionados de forma a prover alguma informação válida em um intervalo de tempo específico. Dentre os diversos significados existentes para Consciência de Situação, devida a diversidade de áreas em que esta teoria é aplicada, neste trabalho optou-se por utilizar o seguinte conceito:

> **Consciência de situação** consiste da percepção e compreensão de uma ou mais situações e a projeção de seus efeitos em um futuro próximo [Endsley 1995].

De acordo com a definição de Endsley (1995), existem três níveis para a obtenção de Consciência de Situação: a percepção, a compreensão e a projeção:

- **Percepção**: O primeiro passo para alcançar a Consciência de Situação é a percepção clara dos elementos relevantes. Sendo assim, este nível (Nível 1) envolve os processos de monitoramento, detecção e reconhecimento, que levam a uma consciência de múltiplos elementos situacionais (objetos, eventos, pessoas, sistemas, fatores ambientais) e seus estados atuais (locais, condições, formas, ações).
- **Compreensão**: A percepção só não basta, é necessário ter um entendimento do significado de todos os elementos e eventos. Dessa forma, o próximo passo da formação de consciência situacional envolve uma síntese dos elementos desconexos identificados no primeiro nível por intermédio dos processos de reconhecimento de padrões, interpretação e avaliação. Este nível (Nível 2) requer a integração dessas informações para entender como isso vai impactar as metas e objetivos do indivíduo/sistema. Isto é normalmente realizado pela correlação de eventos, o que inclui o desenvolvimento de uma visão global do ambiente, ou da parte do ambiente que é de interesse.
- **Projeção**: O último nível é responsável pela capacidade de antecipação de ocorrências futuras, a partir da compreensão dos elementos no ambiente atual. Ele é alcançado por meio do conhecimento da situação, da dinâmica dos elementos, e da compreensão da situação (Níveis 1 e 2), para depois projetar esta informação à diante no tempo e assim determinar se elas afetarão os futuros estados do ambiente operacional.

A Consciência de Situação pode ser alcançada por meio da **correlação de eventos** que fornece a capacidade de unir vários eventos semelhantes ou diferentes em uma única peça de conhecimento de que algo maior está acontecendo, ao invés de obter uma visão incompleta a partir da análise de eventos únicos [Chuvakin et al. 2012]. Devido à complexidade que a correlação de eventos pode alcançar, surgiram diferentes abordagens para este processo. Após um estudo das estratégias consideradas mais relevantes de acordo com o objetivo deste trabalho, a correlação baseada em regras foi selecionada para a prototipação, pois a incerteza, principal razão que justificaria a escolha de outra abordagem, não é algo comumente encontrado nos eventos a serem tratados [Almeida 2013].

### 2.2. Gerenciamento de Eventos e Informações de Segurança

As soluções de SIEM abrangem a agregação de dados de eventos produzidos por dispositivos de segurança (por exemplo, *secure web gateways*, *appliances de firewall*), infraestruturas de rede (por exemplo, *switches*, *access points*, *modens*), sistemas e aplicações.

Estas soluções podem processar dados, tais como tabelas de bases de dados, tráfego de rede, estado do sistema operacional, entre outros, porém, a principal fonte de dados são os logs. Dados de eventos podem ser combinados com a informação contextual sobre os usuários, ativos, ameaças e vulnerabilidades. Os dados são normalizados de modo que eventos, dados e informações contextuais de diferentes fontes possam ser correlacionados e analisados para fins específicos, tais como o monitoramento de eventos de segurança da rede, monitoramento de atividade dos usuários e relatórios de conformidade com leis e regulamentações vigentes .

De acordo com Chuvakin (2012), uma solução de SIEM pode ser avaliada a partir das seguintes funcionalidades: coleta de logs e dados de contexto; normalização e categorização; correlação; notificação e/ou alertas; priorização; visualização; geração de relatórios; e auxílio ao fluxo de trabalho para Segurança da Informação. Estas funcionalidades citadas podem ser encontradas em algumas soluções de SIEM comerciais, as quais são resumidamente apresentadas na seção 5. Neste trabalho, algumas destas funcionalidades também estão presentes, sendo o foco a Consciência de Situação por meio da correlação de eventos.

## 3. Proposta: SIEM-SA

A solução concebida, denominada SIEM-SA (*Security Information and Event Management - Situation Awareness*), é caracterizada principalmente pela capacidade de Consciência de Situação apoiada pela correlação de eventos baseada em regras. A solução teve como base o *middleware* EXEHDA por ele possuir uma arquitetura distribuída que oferece suporte à aquisição, processamento e armazenamento de informações contextuais, além dos procedimentos de atuação sobre o meio, sendo estes fatores imprescindíveis para a obtenção de consciência situacional [Lopes et al. 2012].

No que se refere ao subsistema de adaptação e reconhecimento de contexto do EXEHDA, o serviço de consciência do contexto é proposto de forma distribuída, oferecendo suporte as etapas de aquisição, armazenamento e processamento de informações contextuais, bem como os decorrentes procedimentos de atuação sobre o meio. Estas funcionalidades são propiciadas pelos dois servidores presentes na arquitetura:

- Servidor de Borda (SB): responsável pela interação com o meio utilizando sensores e atuadores;
- Servidor de Contexto (SC): realiza o processamento das informações contextuais recebidas dos diferentes SB's, e o armazenamento dessas informações no RIC (Repositório de Informações Contextuais).

A concepção da solução foi baseada nos dois servidores citados. A seguir, é discutida a arquitetura de software concebida para ambos os servidores.

### 3.1. Arquitetura de Software

O modelo de software proposto e desenvolvido para o SB pode ser visualizado na Fig. 1, que apresenta uma abstração da implementação realizada.

O módulo "Coletor de Logs (Internos)", junto ao "Coletor de Status", realizam a coleta de eventos internos ao sistema, enquanto que o "Coletor de Logs (Externos)" é responsável por receber eventos de diferentes dispositivos, funcionando como um servidor

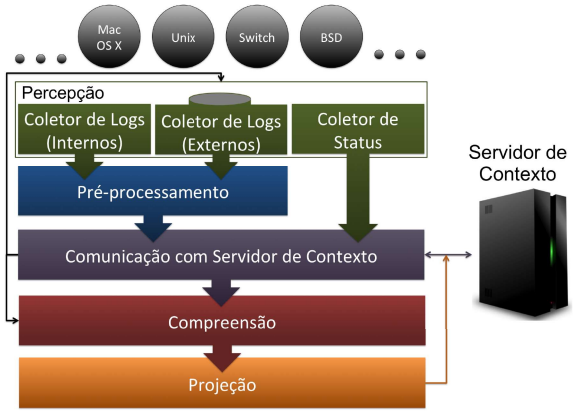


**Figura 1. Servidor de Borda**

Syslog[1], possibilitando o tratamento de eventos onde a instalação do software presente nos SB's não é possível. No topo da Fig. 1 é possível visualizar diferentes dispositivos que podem ter seus eventos enviados pelo protocolo Syslog. Estes três módulos representam a "Percepção", primeiro nível da Consciência de Situação.

Todos os eventos provenientes de logs são repassados para o módulo "Pré-processamento" que realiza a normalização e a contextualização. Já os eventos que verificam o estado do sistema (módulo "Coletor de Status"), por serem considerados eventos simples constituídos de um par chave e valor, são direcionados diretamente ao módulo "Comunicação com Servidor de Contexto" em conjunto com os eventos resultantes do pré-processamento. Este módulo, por sua vez, realiza a publicação dos eventos no SC, e os envia para o módulo "Compreensão".

O módulo "Compreensão" utiliza a correlação de eventos, verificando a existência de alguma regra que corresponda ao fluxo de eventos recebidos. Caso isto ocorra, a situação identificada é repassada ao módulo "Projeção" que possui como finalidade evitar ocorrências futuras, envolvendo desde o envio de alertas, até a efetiva atuação sobre o sistema. Estes módulos representam respectivamente o segundo e terceiro nível da Consciência de Situação. Após a projeção, a situação identificada, junto aos possíveis retornos referentes a atuação, são enviados ao SC para serem armazenados no RIC, disponibilizando assim sua visualização na interface Web.

O módulo "Comunicação com Servidor de Contexto", além de enviar os eventos e situações ao SC para serem armazenados no RIC, também solicita informações como as configurações dos sensores ("Coletor de Logs" e "Coletor de Status") e das situações a serem identificadas junto às suas respectivas projeções.

Continuando a descrição da arquitetura de software proposta, a Fig. 2 apresenta uma abstração do modelo de software proposto e desenvolvido para o SC.

O módulo "Comunicação com Servidor de Borda" é responsável por realizar o processo de comunicação utilizando o protocolo XML-RPC (*eXtensible Markup Language - Remote Procedure Call*) com os SB's. Os SB's ao coletarem as informações

[1]Syslog é um mecanismo padronizado para atividade de logging em sistemas de computador [Syslog 2013].

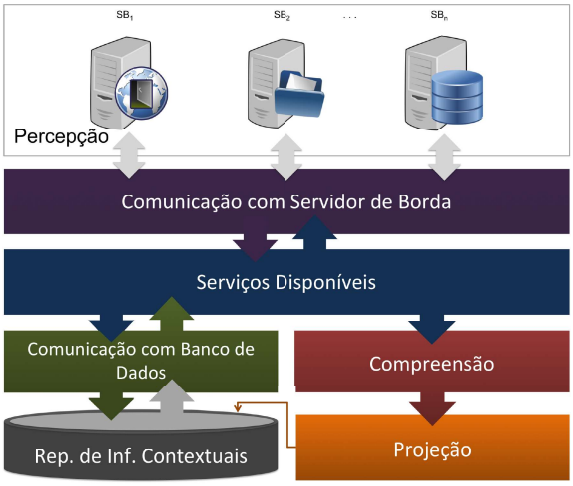


**Figura 2. Servidor de Contexto**

contextuais e disponibilizá-las ao SC proporcionam a Percepção para Consciência de Situação do SC. Os diferentes dados coletados são repassados às funções registradas no módulo "Serviços Disponíveis". Este, realiza o processo de criptografia (ao enviar dados) e descriptografia (ao receber), além da comunicação com o módulo "Comunicação com Banco de Dados" para solicitar as informações desejadas pelos SB's ou inserir os novos dados no RIC. Ele também é responsável por repassar os eventos recebidos ao módulo "Compreensão", que irá informar ao módulo "Projeção" as situações identificadas para que as ações pertinentes sejam executadas.

A distribuição dos módulos de Consciência de Situação em ambos servidores se torna útil, por exemplo, em casos em que o hardware do SB é limitado, passando a correlação de seus eventos ao SC, e também para situações que envolvam eventos incidentes sobre diferentes SB's, por exemplo, em um ataque distribuído.

A seguir, serão descritas as funcionalidades perseguidas ao longo do trabalho, e disponibilizadas pela arquitetura de software apresentada.

- Configuração simplificada: visto que algumas soluções de SIEM possuem um processo de implantação complexo, a configuração da solução é realizada primeiramente, através de um arquivo de configuração onde os parâmetros essenciais para inicialização são especificados, e posteriormente, outros parâmetros são especificados por meio de uma interface Web.
- Dinamicidade de sensores: possibilita a ativação/desativação e inserção/remoção de sensores sem a necessidade de reinicialização da solução, evitando a perda de eventos pertencentes a sensores instanciados antes da modificação.
- Desenvolvimento de novos *drivers*: a solução foi projetada de forma modular, através de uma linguagem de alto nível denominada Python, colaborando com a ideia de uma solução de código fonte aberto, facilitando o desenvolvimento de *drivers* para sensores ainda não suportados, o que potencializa sua flexibilidade.
- Descoberta automática de recursos: visando suportar a dinamicidade de hardware e das configurações dos dispositivos, através da utilização de variáveis nas configurações dos sensores e das situações, a solução descobre automaticamente os recursos que devem ser monitorados e as situações a serem avaliadas.

## 4. Estudo de Caso

Para a validação das funcionalidades da SIEM-SA, assim como das contribuições ao *middleware* EXEHDA e da compatibilidade com as versões anteriores, foram desenvolvidas duas situações de interesse que foram aplicadas no Projeto AMPLUS[2] (*Automatic Monitoring and Programmable Logging Ubiquitous System*).

Observa-se que a principal funcionalidade desenvolvida no trabalho, refere-se a identificação de situações de interesse, especificadas através de regras com sintaxe similar à SQL (*Structured Query Language*). Esta funcionalidade é realizada com o apoio de um sistema de processamento de eventos denominado Esper[3], e foi desenvolvida de forma distribuída fornecendo um melhor entendimento da situação do ambiente.

Além disso, o sistema fornece um sistema de priorização, onde é possível especificar diferentes valores de severidade para cada situação, e definir a criticidade de cada sistema monitorado. Estas duas informações, formam a prioridade da regra a ser confrontada com os eventos, e das situações identificadas pela aplicação a serem exibidas aos usuários. Por fim, destaca-se a capacidade de projeção das situações, o que estabelece a capacidade de evitar ocorrências futuras de situações indesejadas.

### 4.1. Situação 1 - Ataque ao servidor SSH (*Secure Shell*)

Esta situação foi motivada pelo fato dos SB's e dos SC's eventualmente utilizarem um servidor SSH (*Secure Shell*) para facilitar sua manutenção quando necessária. A descrição da situação a ser identificada é:

- Objetivo: advertência antecipada para ataques de força bruta, esquecimento de senhas ou aplicações mal configuradas.
- Causa: três ou mais alertas de falha de autenticação em um minuto a partir de um único endereço IP.
- Origem dos eventos: neste caso, a origem dos eventos é o log gerado pela aplicação de servidor SSH configurada no SB. No entanto, pode ser aplicado a diversos dispositivos ou aplicações.

Para atingir o objetivo citado, a regra "SELECT * FROM SSHLog(ip!='null').win:time(1 min) GROUP BY ip HAVING count(*) >= 3" foi configurada. Caso a situação seja identificada, o endereço IP será bloqueado no firewall pela execução do comando "iptables -A INPUT -i eth1 -s $IP -j DROP".

Ataques foram realizados com o auxílio da ferramenta THC (*The Hacker's Choice*) Hydra[4] e o sistema se comportou conforme o esperado

### 4.2. Situação 2 - Ataque ao *firewall*

O objetivo desta situação é alertar antecipadamente varreduras de serviços, propagação de *worms*, entre outros. A variável de contexto monitorada são quinze ou mais alertas no *firewall* de eventos do tipo *Drop/Reject* a partir de uma única origem em um minuto. A origem dos eventos são os logs do *firewall* configurado no SB.

[2] http://amplus.ufpel.edu.br
[3] http://esper.codehaus.org
[4] https://www.thc.org/thc-hydra/

Para esta situação, a regra “SELECT * FROM FirewallLog(source_ip!=‘null’ and policy in (‘reject’, ‘drop’)).win:time(1 min) GROUP BY source_ip HAVING count(*) >= 15” foi configurada. Como método de ação, a fim de alcançar o objetivo citado, o envio de e-mail foi configurado conforme apresentado na Fig. 3.


**Figura 3. Situação 2 - Configuração da situação “Ataque repetido ao *firewall*”**

Para realização dos testes, inicialmente o *firewall* foi configurado, e posteriormente foi realizada uma varredura de portas no sistema. Os resultados obtidos foram os esperados.

Para maiores detalhes sobre as duas situações descritas [Almeida 2013].

## 5. Trabalhos Correlatos

A Tab. 1 apresenta uma comparação do trabalho desenvolvido com algumas das principais soluções de SIEM do mercado (HP/ArcSight, IMB/Q1Labs, RSA/EM, Splunk e AlienVault) [Nicolett and Kavanagh 2013] acrescentando três soluções FOSS que realizam o tratamento de eventos, de acordo com os aspectos considerados relevantes neste trabalho [Almeida 2013].

Constata-se que o trabalho desenvolvido apresentou uma nova solução de SIEM FOSS com capacidade de Consciência de Situação - seguindo a tendência explorada pelas principais soluções do mercado - por meio da correlação baseada em regras que podem ser editadas via interface Web. Além disso, a solução destaca-se pela sintaxe similar à SQL - características que entre as soluções FOSS selecionadas não foi encontrada - e pela capacidade de correlação e consequentemente identificação de situações tanto no agente, quanto no servidor e de forma distribuída, ou seja, explorando o processamento de diferentes nodos com o apoio do software EsperHa (*Esper High Availability*).

**Tabela 1. Comparação dos trabalhos relacionados com a SIEM-SA**

| Solução / Funcion. | HP/ ArcSight | IBM/ Q1Labs | RSA/ EMC | Splunk | OSSEC | SEC | AlienVault/ OSSIM | SIEM-SA |
|---|---|---|---|---|---|---|---|---|
| FOSS | ✗ | ✗ | ✗ | ✗ | ✓ | ✓ | ✓ | ✓ |
| Consciência de Situação | ✓ | ✗ | ✓ | ✓ | ✗ | ✗ | ✗ | ✓ |
| Sintaxe ~SQL | ✗ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✓ |
| Interface | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✓ |
| Correlação Distribuída | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ |
| Coleta com e sem agente | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ |

Adicionalmente, observa-se o fato da solução ser desenvolvida em Python, uma linguagem de alto nível, o que facilita a sua manutenção e a contribuição da comunidade de software livre. Quando comparado com as soluções comerciais, além de não possuir custo, a solução desenvolvida destaca-se pela simplicidade na implantação.

## 6. Conclusões

O objetivo principal deste trabalho foi alcançado com a concepção e prototipação de uma solução de SIEM acadêmica baseada no *middleware* EXEHDA, focando na aplicação dos conceitos da Consciência de Situação. Os eventos de segurança são identificados por meio do monitoramento contínuo de logs e de informações sobre o estado do sistema, contemplando a diversidade de equipamentos que compõem a infraestrutura computacional ubíqua.

Quanto às contribuições para o *middleware* EXEHDA e, consequentemente, para o Projeto AMPLUS, destaca-se:

- Fornecimento de Consciência de Situação por meio da correlação de eventos e criação de regras com sintaxe similar à SQL;
- Descoberta de recursos.

Já no que se refere a solução de SIEM acadêmica, destacam-se como contribuições à diferentes subáreas da Segurança da Informação como resposta a incidentes, análise forense, e auditoria:

- Minimização do tempo de possíveis respostas a incidentes como consequência da Consciência de Situação;
- Diminuição de impactos adversos destes incidentes pela tomada de ações;
- Garantia das evidências em investigações digitais;
- Monitoramento contínuo, que é descrito em guias de boas práticas, e essencial para conformidade com regulamentações e/ou padrões.

Novos esforços de pesquisa podem ser realizados com base na solução desenvolvida, para que futuramente se obtenha uma solução SIEM FOSS completa, com recursos avançados e principalmente bem documentados. Como exemplos de funcionalidades a serem desenvolvidas ou aprimoradas é possível citar:

- Possibilitar mais de uma ação por situação detectada;
- Realizar testes de desempenho;
- Utilizar os conceitos de Big Data, devido a velocidade, variedade e volume dos eventos coletados principalmente provenientes de logs.

## Agradecimentos

Este trabalho foi parcialmente financiado pela Fundação de Amparo à Pesquisa do Rio Grande do Sul - FAPERGS, Brasil, com apoio do Conselho Nacional de Desenvolvimento Científico e Tecnológico – CNPq, Brasil.

## Referências

Almeida, R. B. (2013). Segurança da informação e gerenciamento de eventos: Uma abordagem explorando consciência de situação. Monografia de graduação em ciência da computação, Universidade Federal de Pelotas.

Chuvakin, A., Schmidt, K., and Phillips, C. (2012). *Logging and Log Management: The Authoritative Guide to Dealing with Syslog, Audit Logs, Events, Alerts and other IT 'Noise'*. Elsevier Science.

Endsley, M. R. (1995). Measurement of situation awareness in dynamic systems. *Human Factors*, 37:65?84.

Hewlett-Packard (2014). Acesso em: 26 abr 2014. Hewlett-Packard - SIEM Solution for Enterprise Security Management. Disponível em: <http://www8.hp.com/us/en/software-solutions/software.html?compURI=1340477#.UWZDpr_C6a5>.

Langheinrich, M. (2010). *Privacy in Ubiquitous Computing*. J. Krumm, ed., CRC Press.

Lopes, J. a. L., Souza, R. S., Geyer, C. R., Costa, C. A., Barbosa, J. V., Gusmão, M. Z., and Yamin, A. C. (2012). A model for context awareness in ubicomp. In *Proceedings of the 18th Brazilian Symposium on Multimedia and the Web*, WebMedia '12, pages 161–168, New York, NY, USA. ACM.

McAfee (2013). Acesso em: 26 abr 2014. SIEM Requirements - Focus On Five. Disponível em: <http://www.mcafee.com/sg/resources/brochures/br-focus-on-five-siem-requirements.pdf>.

Nicolett, M. and Kavanagh, K. M. (2013). Magic quadrant for security information and event management. Technical report, Gartner Group.

Ponemon (2012). 2012 cost of cyber crime study: United states. Technical report, Ponemon Institute LLC.

Ponemon (2013). The risk of insider fraud: Second annual study. Technical report, Ponemon Institute LLC.

Syslog (2013). Acesso em: 26 abr 2014. Logged | Event and Log Management. Disponível em: <http://www.syslog.org>.

Weiser, M. (1991). The computer for the 21st century. *Scientific American*, 265(3):66–75.