# Segurança na Internet das Coisas: uma abordagem de SIEM customizável e baseada em Consciência de Situação

**Ricardo Almeida**[1], **Roger Machado**[1],
**Diórgenes Yuri da Rosa**[1], **Patrícia Davet**[1], **Lucas Donato**[2],
**Ana Pernas**[1], **Adenauer 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,dyurirosa,ptdavet,adenauer,marilza}@inf.ufpel.edu.br

lucas.donato@myemail.dmu.ac.uk

***Abstract.*** *The objective of this paper is to present a proposal of a SIEM (Security Information and Event Management) academic solution, open-source and customizable, which employs the concepts of Situation Awareness. The proposed solution has been developed as a prototype software, based on middleware for Ubiquitous Computing. Simulations were developed to test the behavior of the solution in detecting security risk situations, which characterized the SIEM solution proposed as stable, flexible, scalable and suitable for Internet of Things.*

***Resumo.*** *O objetivo deste artigo é apresentar uma proposta de solução de SIEM (Security Information and Event Management, ou Gerenciamento de Eventos e Informações de Segurança) acadêmica, de código aberto e customizável, que emprega os conceitos de Consciência de Situação. A solução proposta foi desenvolvida na forma de um protótipo de software, com base em 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 caracterizaram a solução de SIEM proposta como estável, dotada de suporte para criação customizada de novas regras de segurança, de caráter flexível, escalável e adequada à Internet das Coisas.*

## 1. Introdução

O desenvolvimento de novas tecnologias de informação, a evolução dos meios de comunicação, e a decorrente troca automatizada de informações entre dispositivos e seus usuários, vem promovendo a evolução da IoT (*Internet of Things*, ou Internet das Coisas). A IoT é um cenário em que os objetos, animais ou pessoas são dotados de identificadores únicos e com a capacidade de transferir automaticamente dados de interesse por meio de canais de comunicação [Gonzalez and Djurica 2015]. A premissa é que o principal meio de comunicação seja a Internet.

A IoT presume que as novas tecnologias estejam cada vez mais integradas à vida cotidiana das pessoas, nas comunicações, no setor financeiro e até no entretenimento. Entretanto, todas as facilidades e oportunidades oferecidas pela IoT também acabam sendo

objeto de interesse de pessoas mal-intencionadas que usam esses recursos para cometer fraudes e ataques contra os sistemas de informação e/ou seus usuários. Logo, percebe-se um aumento no risco relacionado a segurança da informação para as pessoas ou empresas, o que potencializa a segurança e privacidade na IoT devido à natureza volátil, espontânea, heterogênea e invisível da comunicação [Langheinrich 2010].

A preocupação com a Segurança da Informação nas empresas, particularmente, 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*, ou Gerenciamento de Eventos e Informações de Segurança) 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, desenvolvida no meio acadêmico na qual seja contemplado o emprego de Consciência de Situação.

Por sua vez, 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*, ou Centro de Operações de Segurança), especialmente considerando a complexidade dos ambientes computacionais na IoT, 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 customizável, do tipo FOSS (*Free and Open Source Software*) consciente de situação. Para isto, a solução foi concebida com base em um *middleware* para Computação Ubíqua, 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 a base conceitual explorada no desenvolvimento deste trabalho. 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 a mesma é aplicada, neste trabalho optou-se por considerar 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 [Onwubiko 2012].

Desta forma, 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 atividades 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 Figura 1, que apresenta uma abstração da implementação realizada.

O módulo "Coletor de Logs (Internos)", junto ao "Coletor de Status", realiza 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

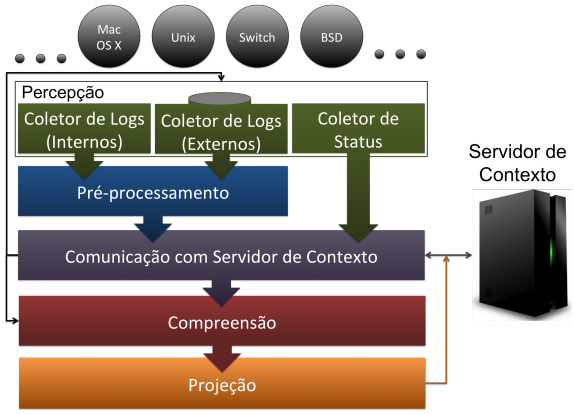


**Figura 1. Abstração do software proposto para o Servidor de Borda**

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

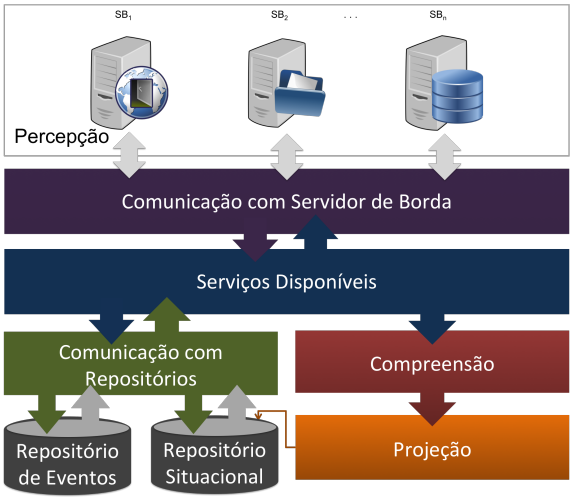


**Figura 2. Abstração do software proposto para o Servidor de Contexto**

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 tanto no SB quanto no SC possibilita a consciência distribuída para detecção de situações de interesse nos diferentes componentes da arquitetura, fornecendo assim uma visão aprimorada do ambiente monitorado. Isto é explorado, por exemplo, para situações que envolvam eventos incidentes sobre diferentes SB's, ou seja, em um ataque distribuído.

Os módulos de compreensão presentes no SB e no SC que realizam a identificação de situações de interesse, utilizam regras especificadas por meio de uma sintaxe similar à SQL (*Structured Query Language*). Isto é realizado com o apoio de um sistema de processamento de eventos denominado Esper[2].

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 SIEM-SA 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.

[2]`http://esper.codehaus.org`

- Persistência local: implementado no SB, realiza persistência local das configurações dos sensores monitorados, dos eventos coletados e situações identificadas, para que seja possível o funcionamento do sistema em casos de perda de comunicação com o SC, destacando que os dados serão armazenados criptografados em primeiro lugar na memória e mais tarde no disco (se o software for finalizado).
- 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 e explora a percepção para alcançar a Consciência de Situação.
- 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.
- NoSQL: duas das principais características do NoSQL são a sua abordagem não-relacional e ausência de esquemas. Esses recursos fornecem dinamicidade para o sistema, o qual se tornou capaz de armazenar diferentes tipos de registros, sem precisar de uma modelagem prévia da tabela personalizada. Para a implementação do modelo NoSQL foi escolhido modelo de documentos, que possui uma otimização em relação ao modelo relacional o qual permite ignorar campos vazios, comum em eventos de log. Além disso, exigido pelas normas de segurança como [Kent and Souppaya 2006], as funcionalidades de tempo do modelo escolhido propiciou uma gestão sobre os dados de retenção. Com a implantação de NoSQL espera-se alcançar uma melhoria no tempo de resposta à incidentes, proporcionando um menor atraso na visualização dos eventos, entre outros benefícios.
- Sistema de prioridades: é possível especificar diferentes valores de severidade para cada situação, e definir a criticidade de cada sistema monitorado. Estas duas informações, formam a ordem de processamento das regras a serem confrontadas com os eventos, e das situações identificadas pela SIEM-SA a serem exibidas aos usuários, conforme demonstrado na Tabela 1. Os valores resultantes da multiplicação serão mapeados para níveis de prioridade como Baixa (valores de 1 à 5), Média (de 6 à 9) e Alta (de 10 à 15).

**Tabela 1. Prioridades das regras e das situações detectadas**

| Sever. / Critic. | Baixa | Média-Baixa | Média | Média-Alta | Alta |
|---|---|---|---|---|---|
| Baixa | 1 | 2 | 3 | 4 | 5 |
| Média | 2 | 4 | 6 | 8 | 10 |
| Alta | 3 | 6 | 9 | 12 | 15 |

## 4. Estudo de Caso

Para a validação das funcionalidades da SIEM-SA, assim como das contribuições ao *middleware* EXEHDA, foram desenvolvidas algumas situações de interesse com base no artigo [Swift 2010], sendo selecionadas três destas. As duas primeiras apresentadas a seguir foram aplicadas no Projeto AMPLUS[3] (*Automatic Monitoring and Programmable Log-*

[3]http://amplus.ufpel.edu.br

*ging Ubiquitous System*) e a terceira foi implementada na infraestrutura computacional da UFPel (Universidade Federal de Pelotas).

### 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: bloqueio de 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 (*Internet Protocol*).
- Origem dos eventos: log gerado pela aplicação de servidor SSH configurada nos servidores do projeto AMPLUS. No entanto, pode ser aplicado a diversos dispositivos ou aplicações.

Para atingir o objetivo citado, a regra "SELECT * FROM SSHLog(ip!='null' and message in 'Failed password').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 -I INPUT -i eth1 -s $IP -j DROP".

Antes de colocar em produção, ataques foram realizados com o auxílio da ferramenta THC (*The Hacker's Choice*) Hydra[4] e o resultado da identificação da situação pode ser observado na Figura 3.


**Figura 3. Situação 1 - Identificação da situação de ataque ao servidor SSH**

### 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.

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.

[4] https://www.thc.org/thc-hydra/


**Figura 4. Situação 2 - Eventos referentes a detecção de ataque ao *firewall***

Para realização dos testes, inicialmente o *firewall* foi configurado, e posteriormente foi realizada uma varredura de portas no sistema, onde foram obtidos os resultados esperados. Posteriormente o sistema foi colocado em regime de produção, conforme pode-se observar na Figura 4, onde são apresentados os eventos associados a identificação de uma situação de ataque ao firewall. Além dos eventos, observa-se dados contextuais que foram adicionados referentes a geolocalização do endereço IP do atacante, e ainda a possibilidade de geração de relatórios.

Os dados contextuais, assim como a identificação da situação na Figura 3 auxiliam no entendimento por parte do administrador de algumas das perguntas utilizadas na Consciência de Situação: quem (endereço do atacante e sua geolocalização), quando (data inicial e data final, junto a data de cada evento), onde (nome do ativo sendo atacado), por que (apesar de complexa, toda a informação exibida na interface irá auxiliar o administrador neste ponto), o que (detalhes e comentários da situação ajudam por exemplo a identificar um possível serviço), como (a exibição detalhada dos eventos auxilia o administrador a inferir esta questão).

### 4.3. Situação 3 - Ataque a partir da mesma origem à diferentes serviços

Situação motivada pelo fato dos servidores de aplicações Web hospedadas em diferentes servidores na infraestrutura da UFPel utilizarem serviços de SSH (*Secure Shell*) e FTP (*File Transfer Protocol*). Esta situação validou os módulos de Consciência de Situação distribuídos entre SB e SC, neste caso, utilizando-se da visão amplificada do ambiente que o SC oferece.

O objetivo é identificar ataques de uma mesma origem à diferentes serviços presente em diferentes servidores, situação que não seria identificada ao analisar os eventos de um único servidor. Para atingir este objetivo a regra “SELECT * FROM SSHLog(ip!=‘null’).win:time(1 min) as ssh, FTPLog(ip!=‘null’).win:time(1 min) as ftp WHERE ssh.ip = ftp.ip GROUP BY ip HAVING count(*) >= 3” foi configurada.

Esta regra utiliza o módulo de compreensão do SC, sendo aplicada aos dois servidores de hospedagem presentes na UFPel que possuem os serviços mencionados em execução. A ação configurada foi bloqueio temporário do IP no firewall de ambos servidores. A regra ficou ativa durante um dia, e resultou em 20 bloqueios de tentativas de

ataques aos serviços de SSH e FTP.

## 5. Trabalhos Relacionados

A Tabela 2 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 [Almeida 2013]. Sabe-se que as soluções do mercado oferecem funcionalidades a mais que as concebidas na SIEM-SA, como análise de vulnerabilidades, integração com demais soluções do mercado considerando parcerias comerciais formadas, possuem equipe de suporte, além de equipes especializadas para criação de regras que reflitam os novos ataques, porém o propósito desta seção é focar nos aspectos considerados relevantes neste trabalho.

**Tabela 2. 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 | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ |

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 de forma distribuída.

Quando comparado com as soluções comerciais, 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. Em [Korolov 2012] é defendida a ideia de que a adoção ampla de soluções de código aberto pode ajudar a IoT à crescer e se desenvolver, tornando mais fácil para os produtos de diferentes fornecedores se comunicarem uns com os outros, bem como proporcionar a redução das barreiras à entrada de novas empresas e a consequente redução de custos.

Observa-se ainda que a solução foi desenvolvida em Python, uma linguagem de alto nível, o que facilita a sua manutenção e a contribuição da comunidade de software livre. Além de não possuir custo, a solução desenvolvida destaca-se perante as soluções do mercado pela simplicidade na implantação.

Como benefício de um projeto proveniente do meio acadêmico, observa-se a geração de uma documentação detalhada que em geral fica disponível ao público, diferentemente das soluções disponíveis no mercado que por estratégias de negócio, além de não disponibilizarem o código fonte, resguardam suas pesquisas.

## 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 da IoT por intermédio do recebimento de eventos por protocolos padrões, como o Syslog, e pela possibilidade de desenvolvimento de novos *drivers*, proporcionando flexibilidade para o fornecimento da percepção.

A compreensão foi explorada com o uso da estratégia baseada em regras que podem ser criadas por meio da interface Web utilizando uma sintaxe similar a SQL. Cada situação poderá estar associada à ações que visam a projeção para Consciência da Situação, onde novamente para as duas característica destaca-se a sua flexibilidade.

Como contribuições à diferentes subáreas da Segurança da Informação como resposta a incidentes, análise forense, e auditoria, é possível citar que a solução concebida pode: minimizar do tempo de possíveis respostas a incidentes como consequência da Consciência de Situação distribuída; diminuir os impactos adversos destes incidentes pela tomada de ações; garantir as evidências em investigações digitais; oferecer o monitoramento contínuo, que é descrito em guias de boas práticas, e essencial para conformidade com regulamentações e/ou padrões.

Quanto às contribuições para o *middleware* EXEHDA e, consequentemente, para o Projeto AMPLUS, destaca-se: o fornecimento de Consciência de Situação por meio da correlação de eventos e criação de regras com sintaxe similar à SQL, e; a descoberta de recursos.

Além do aprimoramento dos testes para validação da solução buscando quantificar melhor os benefícios ganhos, novos esforços de pesquisa podem ser realizados com base na solução desenvolvida, para que futuramente se obtenha uma solução SIEM FOSS completa e com recursos avançados. Como exemplos de possíveis pesquisas a serem desenvolvidas é possível citar:

- Avaliar a integração com algoritmos de inteligência artificial para detecção de situações ainda não mapeadas em regras;
- Integrar análise de vulnerabilidades;
- Explorar os conceitos de Big Data, indo além do uso de um banco não-relacional;

## 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.

Gonzalez, M. H. and Djurica, J. (2015). ISACA Journal v2 - Internet of Things Offers Great Opportunities and Much Risk.

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>.

Kent, K. and Souppaya, M. (2006). National Institute of Standards and Tecnology - Special Publication 800-92. Recommendations of the National Institute of Standards and Technology - Guide to Computer Security Log Management.

Korolov, M. (2012). Acesso em: 04 abr 2015. NetworkWorld - Will open source save the Internet of Things?. Disponível em: <http://www.networkworld.com/article/2902231/internet-of-things/will-open-source-save-the-internet-of-things.html?nsdr=true>.

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.

Onwubiko, C. (2012). *Situational Awareness in Computer Network Defense: Principles, Methods and Applications: Principles, Methods and Applications*. Premier reference source. Information Science Reference.

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.

Swift, D. (2010). Successful siem and log management strategies for audit and compliance. Technical report, SANS Institute - InfoSec Reading Room.

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