Gestão & Tecnologia
Faculdade Delta
Ano VIII,
V. 1 Edição 28
Jan/Jun 2019

MONITORAMENTO DE REDES UTILIZANDO O FRAMEWORK OPENSOURCE OSSIM

NETWORK MONITORING USING THE FRAMEWORK OPENSOURCE OSSIM

Maykel Agostinho Silva[1];
Fábio Barbosa Rodrigues [2]

RESUMO

O gestor de redes de computadores tem um grande desafio, manter sua rede estável e segura. A busca por soluções para auxiliar no dia-a-dia é constante, e neste contexto será apresentado uma ferramenta opensource para o monitoramento de sua rede, auxiliando nas tomadas de decisões, o OSSIM possui uma interface web, gerando relatórios, mostrando alertas de possíveis ataques em tempo real, apresentando comportamento de dispositivos, servidores e serviços disponíveis. Implementado em um ambiente de laboratório, onde apresentaremos no caso de uso, utilizamos para monitorar o servidor sob o ataque de força bruta, foi a forma de simular sua eficácia, para proporcionar um ambiente seguro para seus usuário e clientes.
Palavras-chave: Redes. Segurança. Framework. Sistema.

ABSTRACT

The computer network manager has a great challenge, keeping your network stable and secure. The search for solutions to help without day-to-day is constant, and thinking of this we present this work an open solution for the monitoring of your network the aid in decision making, OSSIM has a web interface, generating information, showing alerts Real-time attacks by displaying behavioral devices, servers, and services available. Implemented in a virtual machine environment, Demonstrating some forms of background monitoring, and clients.
Key-words: Networks. Safety. Framework. System.

[1]Pós-graduando no curso Lato Sensu Gestão e Segurança em Redes de Computadores pela Universidade do Estado de Goiás (UEG). E-mail para contato: maykegyn@gmail.com
[2]Doutor em Engenharia Elétrica e de Computação pela UFG (2015). Email para contato: prof.fabiobrodrigues@gmail.com.

ISSN 2176-2449

Gestão & Tecnologia
Faculdade Delta
Ano VIII,
V. 1 Edição 28
Jan/Jun 2019

1 INTRODUÇÃO

Com os avanços da tecnologia da informação, levando as, a serem armazenadas em servidores locais ou em nuvem, exige muito conhecimento da equipe de Tecnologia da Informação (TI) no sentido de proteger seus dados, onde diariamente é atacada por hackers utilizado a internet ou até mesmo a rede interna para isso. Geralmente as informações que almeja é o bem mais precioso da empresa, diante dessa ameaça a necessidade de ter ferramentas para monitorar seus servidores é alta.

Segundo Black (2008) o ambiente de rede monitorado por um software é de fundamental importância, saber o que acontece em sua rede irá proporcionar segurança e o principal, ter condições de agir preventivamente para evitar perca de informação ou paralizações indesejadas.

Open Source Security Information Management (OSSIM) é uma solução open source para gerenciamento de eventos de segurança (SIEM-Security Information and Event Management) com inteligência para classificar riscos de eventos e ativos, verificar a conformidade com as normas ISO 27001 e PCI-DSS e gestão de incidentes de segurança, tudo integrado em uma única plataforma. Não consiste apenas em monitorar os ativos, mas alertando caso algum serviço fique fora do ar, também monitora serviços, vulnerabilidades, logs, tentativas de ataques, ações maliciosas, tráfego de rede e etc, integrando essas informações para gerar um relatório mais completo.

O OSSIM ou Alien Vault Open Source SIEM é sistema Linux com diversas ferramentas voltadas a segurança da informação, que agindo em conjunto, concedem um ambiente incrível para administradores de rede e de sistemas ou usuários comuns, que possibilita um monitoramento detalhado de uma rede (Alien Vault User Guide).

Características Gerais, Software Livre, possui Acesso Web, Atualização direta da Internet por componente, Ativação parcial dos módulos, Geração de TICKETs de segurança para os problemas identificados, Scan da Rede configurável, Adição de nós sensores/coletores em pontos diferentes da rede. Por ser um projeto de código aberto tem a possibilidade de personalizar de qualquer forma, e existe também uma ferramenta paga a Unified Security Management (USM) onde possui características adicionais a versão gratuita.

Na arquitetura OSSIM conforme a figura 1, sensores/coletores são os dispositivos de origem, que alimentam o sistema. O Collector é responsável pela coleta de logs, onde a normalização das informações é feita no próprio collector.

O armazenamento dos logs fica por parte do nas/san storage, que é alimentado pelo logger. Para armazenar as regras de eventos, o SIEM utiliza a sql storage, chamada MySQL. O MySQL é uma ferramenta de gerenciamento de dados relacional com código aberto.

O OSSIM está disponível em https://www.alienvault.com. Atualmente o OSSIM está na versão 5.30 e possui versão 32 bits (x86) e 64 bits (x64), sendo que os desenvolvedores do sistema, recomendam explicitamente a versão 64 bits, por possuir mais recursos e ser a versão que será continuada nos próximos lançamentos, como a versão 6.0 do OSSIM.

Por fim o OSSIM disponibiliza a web interface para monitorar sua rede.

ISSN 2176-2449

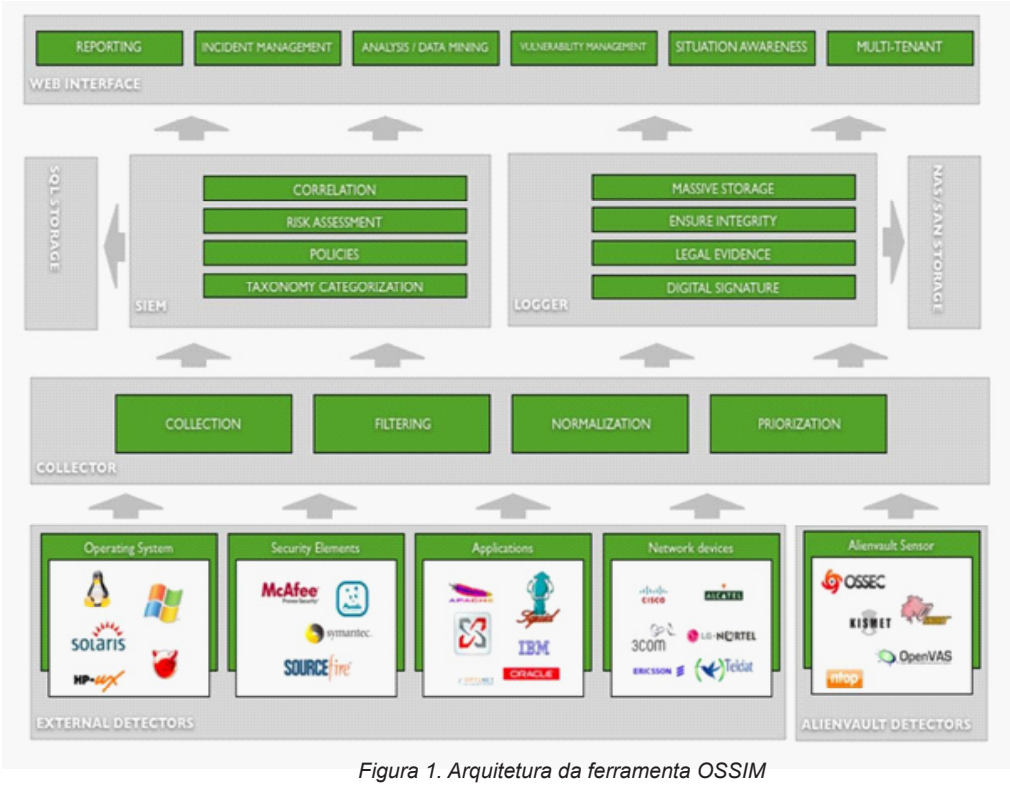

Figura 1. Arquitetura da ferramenta OSSIM
Fonte: Alien Vault User Guide.

1.1 Sensores

Sensores são responsáveis por gerar as fontes de dados, classificam e normalizam antes de encaminhar para o SIEM e o Logger (versão USM paga). Eles é que verifica a detecção de intrusos, anomalias e vulnerabilidades.

Os sensores podem ser baixados pela comunidade ou até mesmo ser desenvolvido como sistema independente.

1.1.1 SIEM

O SIEM é responsável por gerir de forma inteligente os dados coletados onde disponibilizará em base de dados sql onde é possível ocorrer a mineração dos dados. Funções como (Alien Vault User Guide);

- Avaliação de risco;
- Correlação;
- Métricas de risco;
- Varredura de vulnerabilidades;
- Mineração de dados para eventos;
- Monitoramento em tempo real;
- Estão disponíveis em ambas versões Free e Paga.

1.1.2 Logger (Apenas na versão USM)

Segundo MARTINS (2016) o Logger é um componente especifico para armazenar eventos. Os eventos são tratados com maior segurança, possuindo uma assinatura digital e sistema de armazenamentos de rede NAS/SAN. Esse componente é utilizado por grandes corporações que possuem informações confidenciais ou de grande valor.

1.1.3 Aplicativos

O OSSIM disponibiliza alguns aplicativos com a funcionalidade de medidas preventivas de segurança da informação. Sendo eles (Alien Vault User Guide):

• Nessus: programa de verificação de falhas e vulnerabilidades de segurança;

• Nagios: monitoramento de equipamentos e serviços;

• Dashboard: o dashboard são vários tipos de tabelas que podem ser customizadas de acordo com o usuário;

• OCS-NG (Open Computer and Software Inventory Next generation): ferramenta que relaciona os dispositivos presentes na rede;

• Snort: ferramenta de detecção e prevenção de possíveis ataques a rede;

• Tcptrack: ferramenta para informar as possíveis conexões TCP na rede;

• OSSEC: detecta ataques a rede local.

1.1.4 Normas de Seguranças

Em âmbito internacional temos a Lei Sarbanes-Oxley de 2002 (Sox) ou Public Law 107. (MARCIANO, 2015).

Elaborada por dois congressistas - o senador Paul Sarbanes e o deputado republicano Michael Oxley. Esta lei foi sancionada em 30 de julho de 2002 pelo presidente dos Estados Unidos, George W. Bush.

A lei Sarbanes-Oxley, apelidada de Sarbox ou ainda de SOX, visa garantir a criação de mecanismos de auditoria e segurança confiáveis nas empresas, incluindo ainda regras para a criação de comitês encarregados de supervisionar suas atividades e operações, de modo a mitigar riscos aos negócios, evitar a ocorrência de fraudes ou assegurar que haja meios de identificá-las quando ocorrem, garantindo a transparência na gestão das empresas.

O PCI DSS se aplica a toda e qualquer empresa que coleta, processa, armazena ou transmite informação de cartão de crédito, estando, portanto, obrigada a se adaptar ao padrão. Em linhas gerais, esta adaptação inclui comerciantes, intermediários que processam dados de cartão de crédito e estão ligados à rede da associação de cartões, assim como provedores de serviço que hospedam sites, processam transações em ATM ou coletam e processam dados de cartão de crédito em nome de membros das redes Visa e Mastercard – gateways de pagamento.

A norma ISO 27001 é o padrão e a referência Internacional para a gestão da Segurança da informação, assim como a ISO 9001 é a referência Internacional para a certificação de gestão em Qualidade. A norma ISO 27001 tem vindo, de forma continuada, a ser melhorada ao longo dos anos e deriva de um conjunto anterior de normas, tem como princípio geral a adopção pela organização de um conjunto de requisitos, processos e controlos com o objetivo de mitigarem e gerirem adequadamente o risco da organização de TI como explica Kosutic (2016).

> ISO 27001 it provides a comprehensive framework that will help you with this crucial process. It gives you the necessary guidance and building blocks for protecting your company. ISO 27001 tells you where to start from, how to run your project, how to adapt the security to the specifics of your company, how to control what the IT and security experts are doing, and much more.

A ISO 27002 (conhecida antes como ISO 17799) é uma norma internacional contendo controles para a segurança da Informação. A norma ISO 27002 deve ser usada como um conjunto completo de controles para a segurança da informação que funcionam como um guia para a organização que deseja obter a certificação empresarial ISO 27001.

2 DASHBORDS

O OSSIM tem sua interface gráfica (GUI) bem simples e objetiva que pode ser acessada através do navegador web de um dos PCs que esteja na rede, o que permite com que o usuário visualize o que quer na hora que quiser, com clique no menu DASHBORDS situado na parte superior da página conforme a figura 2.

Figura 2. Módulo de dashboards do OSSIM.
Fonte: http://alienvault.cdn.rackfoundry.net

O OSSIM disponibiliza as informações através de tabelas chamadas dashboards, permitindo que o administrador tenha uma visão geral do monitoramento da rede. Como mostra a figura 2 em overview:

• Executive: gráfico geral do monitoramento dos logs que permitem uma visão geral da ferramenta;
• Network: status da rede, informações colhidas por meio de agentes;
• Tickets: incidentes de segurança gerados;
• Security: estatísticas, eventos de segurança que permite gráficos para uma análise posterior;
• Vulnerabilities: vulnerabilidades disponíveis pelo Nessus;
• Inventory: estatísticas dos dispositivos da rede.

2.1 Modulo Analysis

No Analysis é onde se encontra os eventos gerados, é possível editar e visualizar os alertas dos incidentes gerados. O componente especifico dos logs o Logger fica no módulo Analysis, disponível na versão paga.

Os alertas são compostos pelo nome do sensor que gerou, o IP de origem, IP

de destino, a data e o tipo do alerta, que são cinco tipos: system compromisse, exploitation & installation, delivery & attack, reconnaissance & probing e evironmental awareness. (Figura 3).

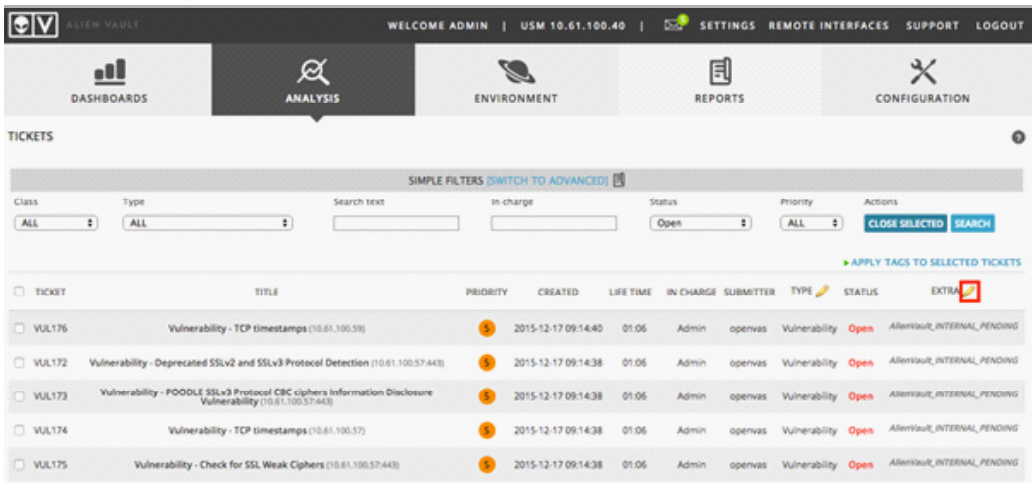

Figura 3. Analysis OSSIM.
Fonte: http://alienvault.cdn.rackfoundry.net

2.2 Modulo Enviroment

Em Enviroment o administrador de rede visualizar onde o OSSIM está monitorando, os tipos de protocolo (UDP, TCP, ICMP e outros), onde varre no intuito de encontrar qualquer tipo de vulnerabilidade.

2.3 Modulo Reports

O OSSIM disponibiliza para facilitar a visualização um arquivo pdf ou envia esse arquivo para o e-mail do administrador basta inserir a faixa de data que permite exportar.

2.4 Modulo Configuration

Neste módulo é possível criar novos usuários para ter acesso a ferramenta, permite ainda fazer backup de todo o sistema, também permite a criação e alteração de políticas de segurança para ter o melhor rendimento diante de cada cenário.

3 ESTUDO DE CASO

3.1 Descrição do ambiente

Nosso cenário foi configurado para um ambiente laboratorial, onde teremos um servidor de aplicação instalado e configurado Linux Debian com o serviço ISPConfig, um servidor de arquivos instalado no Windows Server 2012, o OSSIM 5.2 com o hardware I5vpro, memoria 8gb de ram, hd 240gb ssd, modem roteador, todos monitorado pelo OSSIM.

3.1.1 Monitoramento

Agentes Instalados e configurados começamos a monitorar os nossos servidores conforme a figura 4.

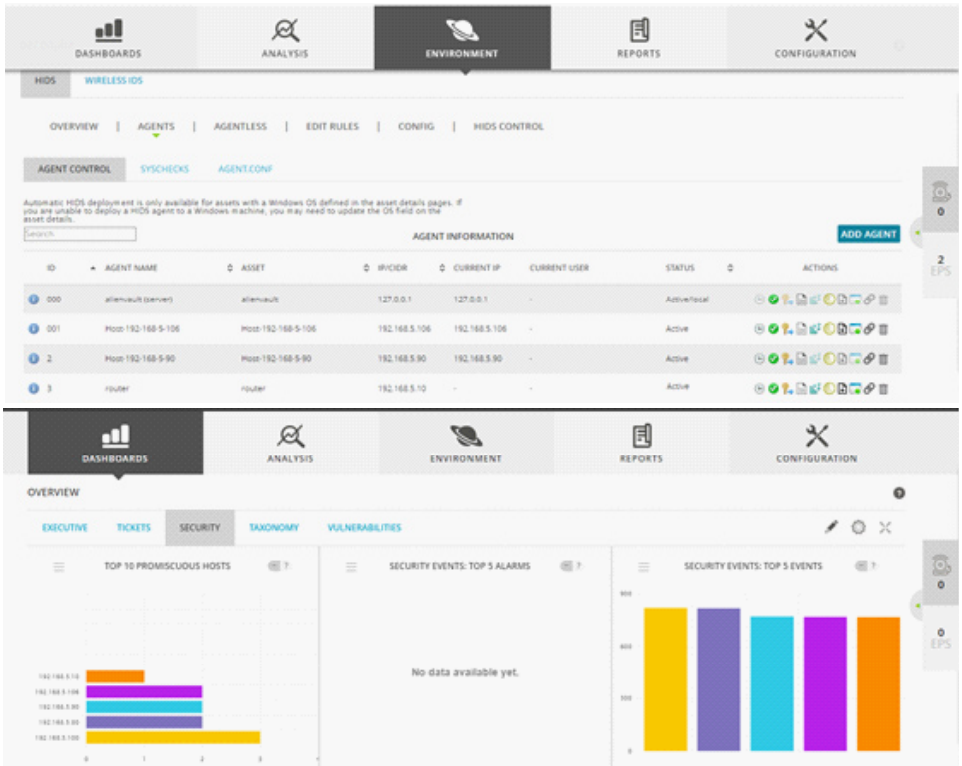

Figura 4. Demonstração do monitoramento dos Agentes Instalados.
Fonte: OSSIM Versão 5.30

3.1.3 Teste de Penetração

Para testar o OSSIM criamos o seguinte cenário. Utilizar força bruta para acessar o servidor de arquivo remotamente e ser notificado via email para analizar as ações. Para isso criaremos a seguinte Ação notificar via email a tentativa de invasão que fica em CONFIGURAÇÕES > THREAT INTELLIGENCE > ACTIONS e criar uma nova ação (Figura 5).

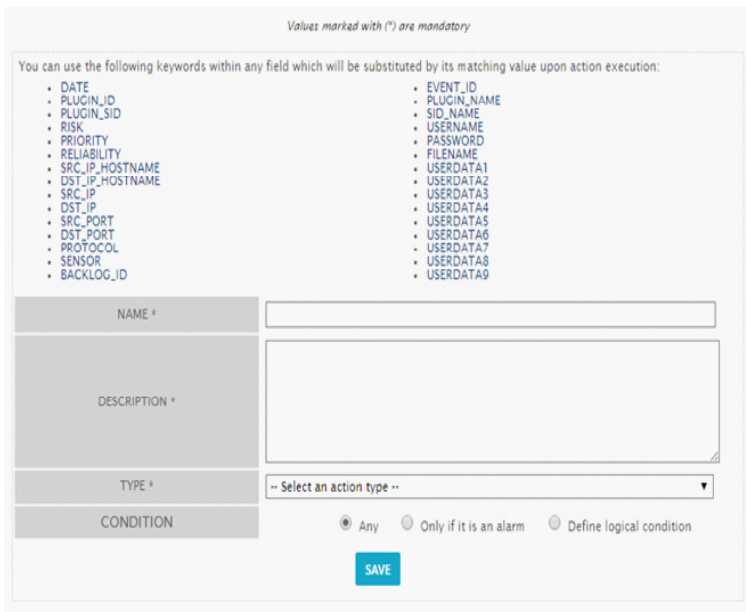

Figura 5. Demonstração Configuração de Agente.
Fonte: OSSIM Versão 5.30

Após preencher e salvar, ficara conforme a figura 6.

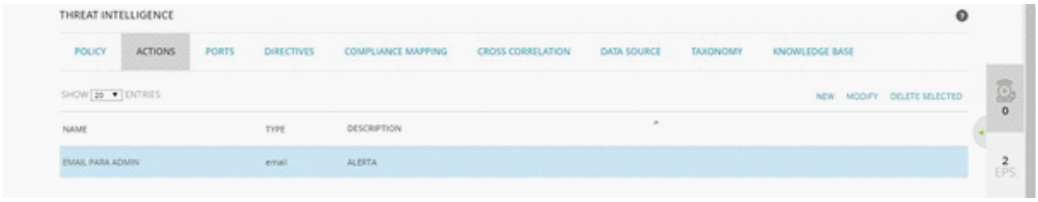

Figura 6. Demonstração Configuração de Agente.
Fonte: OSSIM Versão 5.30

Em PORTS cadastramos a porta 3389 onde iremos monitorar (Figura 7).

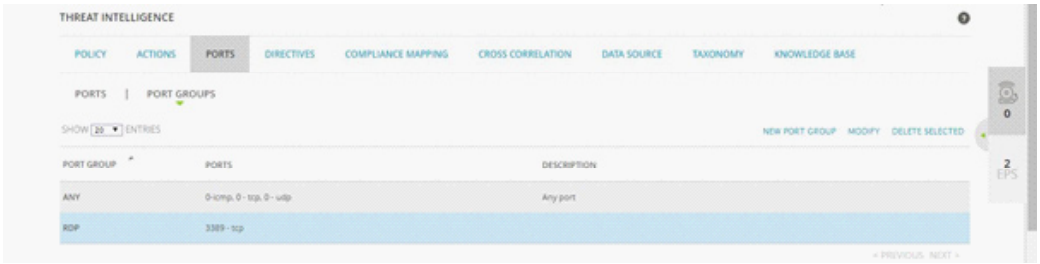

Figura 7. Demonstração Configuração de Agente.
Fonte: OSSIM Versão 5.30

Em POLICY criamos uma política onde é disparado para o email informando qualquer anormalidade. (Figura 8).

Figura 8. Demonstração Configuração de Agente.
Fonte: OSSIM Versão 5.30

Utilizando um ataque de força bruta moderado no Windows Server e também acessos com usuário e senhas corretas, para gerar tráfego de rede e, consequentemente, produzir dados para o OSSIM analisar. (Figura 9)

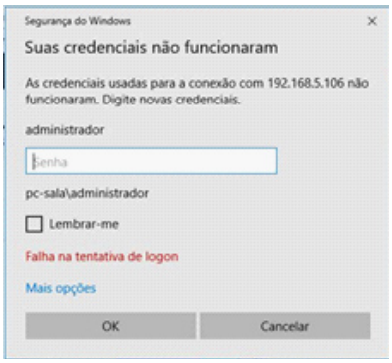

Figura 9. Acesso Windows Server.
Fonte: Windows Server 2012

Em seguida dos ataques já recebemos várias alertas no email, e no painel ANALYSIS – SECURITY EVENTS (SIEM), as atividades envolvendo o IP 192.168.5.106. Pode-se observar na figura abaixo que houve requisições de login de administrador com origem no IP 187.52.126.194 e destino na máquina com IP 192.168.5.196 que estava escutando na porta 3389/tcp. Os eventos foram

todos classificados com risco zero, pois não houve invasão. (Figura 10).

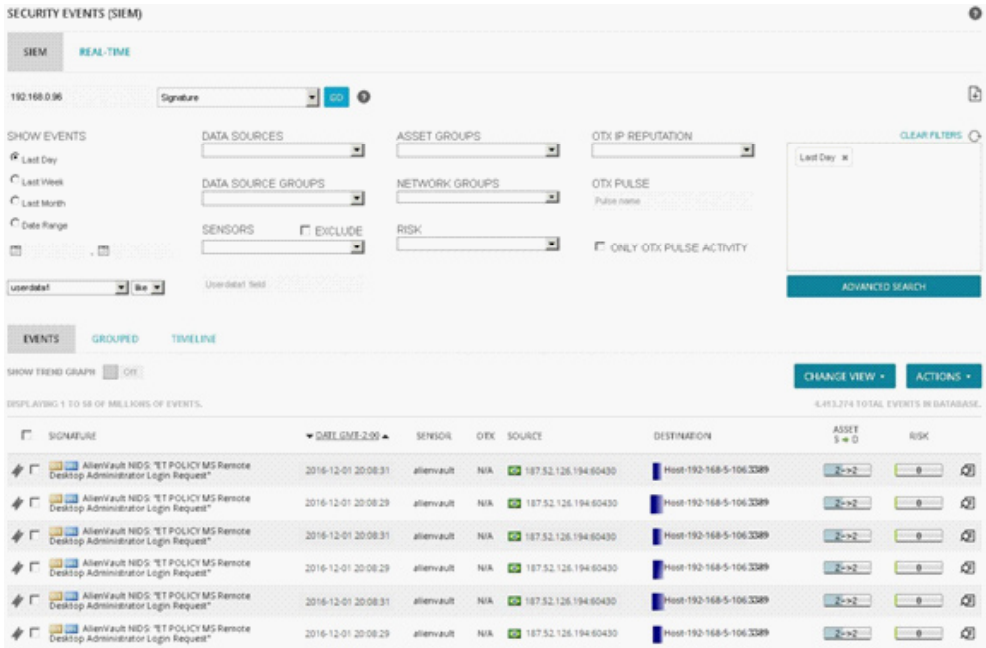

Figura 10. Tela de Eventos.
Fonte: OSSIM Versão 5.30

4 CONCLUSÃO

Apesar de poucos testes efetuados, o framework atende as expectativas de software para o monitoramento, é de fácil operação, e possui uma gama grande de relatórios. Apesar de opensource possui robustez de software pago. No quesito hardware ele exige muito da máquina hospedeira, principalmente no aspecto memória ram. Vale ressaltar a sua eficiência na detecção de ataques e na fácil instalação dos agentes, e não poderia esquecer que também possui uma grande equipe de desenvolvedores e por isso está sempre sendo atualizado, que é disponibilizado para todos.

REFERÊNCIAS

BLACK, T.L. Comparação de Ferramentas de Gerenciamento de Redes. 64f. Especialização (Tecnologias, Gerencia e Segurança em Redes de Computadores) - Universidade Federal do Rio Grande do Sul, Instituto de Informática, Rio Grande do Sul.

ALIEN VAULT USER GUIDE. OSSIM Web Site. Disponível em: <https://scadahacker.com/library/Documents/Manuals/AlienVault_Users_Manual_1.0.pdf>. Acesso em: 20 out. 2016.

ALIEN VAULT. OSSIM Web Site. Disponível em: <https://www.alienvault.com/products/ossim >. Acesso em out.2016.

MARCIANO, L.M.S. A LEI SARBANES – OXLEY E SEUS EFEITOS EM EMPRESAS BRASILEIRAS, São Paulo, 2015.

ISO. International Organization for Standardization Web Site. Disponível em: <http://www.iso.org/>. Acesso em: 02 out. 2016.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 10520: informação e documentação: apresentação de citações em documentos. Rio de Janeiro, 2002.

KOSUTIC, D. SECURE & SIMPLE A SMALL-BUSINESS GUIDE TO IMPLEMENTING ISO 27001 ON YOUR OWN. EPPS Services Ltd. Croatia 2016.