Extração e gerenciamento de incidentes em SIEM

Charles V. Neu[1,2], Evandro Trebien[1], Daniel D. Bertoglio[2], Roben C. Lunardi[2,3], Avelino F. Zorzo[2]

[1]Universidade de Santa Cruz do Sul (UNISC)

[2]Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS)

[3]Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul (IFRS)

Abstract. *Currently, both the number and diversity of devices connected to the Internet still increasing. Thus, security management has become a major challenge. Hence, Security Information and Event Management (SIEM) can help to collect and analyze events generated by different management tools. However, SIEM often depends on specialized human task force to analyze each event and to provide decision according to the incident. Moreover, generated alerts management is typically not efficient on current solutions. In order to help to tackle these issues, this paper presents an approach to manage incidents through tickets related to critical security events in a SIEM, following the "Incident Management"process from Information Technology Infrastructure Library (ITIL).*

Resumo. *Atualmente, o número e a diversidade de dispositivos conectados à internet continua aumentando. Consequentemente, o gerenciamento de segurança se tornou um grande desafio. Desta forma, o Gerenciamento de Eventos e Informações de Segurança (SIEM) pode ajudar a coletar e analisar eventos gerados por diferentes ferramentas de gerenciamento. No entanto, muitas vezes, estas ferramentas, dependem de uma força-tarefa humana especializada para analisar cada evento e fornecer uma decisão de acordo com o incidente. Além disso, o gerenciamento de alertas gerado geralmente não é eficiente nas soluções atuais. A fim de ajudar a lidar com essas questões, este artigo apresenta uma abordagem para gerenciar incidentes através de tickets relacionados a eventos críticos de segurança, seguindo o processo de Gerenciamento de Incidentes da Information Technology Infrastructure Library (ITIL).*

1. Introdução

A utilização da Internet tornou-se parte do cotidiano das pessoas e dos mais diferentes setores da indústria. Com isso, temas referentes a privacidade e segurança tem estado cada vez mais em voga [Detken et al. 2015]. Porém, melhorar os mecanismos de confiabilidade e segurança não é uma tarefa simples. Tipicamente, são utilizados diversos mecanismos de segurança, como *firewalls*, IDS/IPS e ferramentas de monitoramento, que funcionam de forma independente, com o objetivo de aumentar a segurança, provendo maior integridade, disponibilidade, confidencialidade, não-repúdio e confiabilidade.

Os *logs* ou registros possibilitam uma análise mais detalhada sobre o incidente ou alerta gerado pelas ferramentas. Desta forma, é possível buscar informações de alterações de registros, tentativas inválidas de autenticação, endereço de origem do ataque ou incidente, destino e tipo de protocolo utilizado. Porém, o administrador ou responsável pelo monitoramento enfrenta a dificuldade de buscar os *logs* em diferentes ferramentas. Ainda, muitas vezes os *logs* apresentam informações redundantes, o que pode atrasar a ação de prevenção do ataque ou a correção de problemas [Bachane et al. 2016].

Para facilitar este processo, podem ser utilizadas ferramentas de Gerenciamento de Eventos e Informações de Segurança (SIEM). Estas ferramentas tem como objetivo compilar e apresentar informações contidas em *logs*, além de informar aos responsáveis pelo monitoramento a ação necessária. Com a implantação de um sistema SIEM, é possível monitorar e responder de forma ágil a eventos maliciosos detectados [Scholzel et al. 2015]. Entretanto, SIEMs, muitas vezes, dependem de uma equipe especializada para analisar cada evento gerado e tomar a decisão de acordo com o incidente. Ainda, por vezes não ocorre o gerenciamento eficiente dos alertas gerados.

Com o objetivo de mitigar estes problemas, este trabalho apresenta uma proposta para gerenciar os incidentes relacionados aos eventos de segurança mais críticos em um SIEM. Este gerenciamento é realizado seguindo a metodologia ITIL, que consiste em um conjunto de processos para boas práticas de gerenciamento de serviços de TI desenvolvidas pelas organizações públicas e privadas de todo o mundo [Gupta et al. 2008]. O seu principal objetivo é unir diversos métodos e proporcionar um serviço de TI mais eficiente [Ahmad and Shamsudin 2013]. Portanto, este trabalho apresenta um sistema para identificar e gerenciar incidentes encontrados em SIEM seguindo a metodologia ITIL, discutindo a validade da solução em um estudo de caso.

2. Trabalhos Relacionados

Diferentes trabalhos foram propostos para tratar e automatizar o Gerenciamento de Incidentes, tanto utilizando métodos de aprendizado de máquina [Gupta et al. 2008], quanto para identificar causas-raiz dos problemas [dos Santos et al. 2011] utilizando workflows. Porém, pouco tem se discutido em utilizar SIEMs para esse gerenciamento e identificação de incidentes. A seguir serão discutidos os principais trabalhos que discutem SIEMs e que servem de base para construção deste trabalho.

O trabalho proposto por Sekharan e Kandasamy [Sekharan and Kandasamy 2017] faz uma análise comparativa entre ferramentas SIEMs. Dentre os principais pontos, são elencados os recursos oferecidos e os tipos de correlação utilizados, em especial, nas ferramentas *IBM Qradar*, *HP ArcSight*, *Splunk* e *LogRhythm*. Durante a comparação, são discutidos os seguintes recursos oferecidos pelos SIEMs: Monitoramento de segurança em tempo real, inteligência para ameaça, perfil de comportamento, monitoramento de dados e usuários, monitoramento de aplicativos, gerenciamento e armazenamento. Durante a comparação, foram discretizadas notas para cada ferramenta, onde a *HP ArcSight* obteve a maior média, seguido por *IBM Qradar*, Splunk, e em último *LogRhythm*.

Bachane *et al.* [Bachane et al. 2016] propõe uma solução SIEM para investigação forense em tempo real. A solução realiza a captura de evidências contidas nos *logs* e as envia para um servidor local de *logs*, onde pode ser feita a análise detalhada. Porém, a solução apresenta limitação quanto ao sistema operacional utilizado (apenas para registros de sistemas Windows). Portanto, diversos outros sistemas operacionais não são contemplados. Com base nesta solução, o autor sugere melhorar esta abordagem utilizando um SIEM no lugar de um servidor de *logs*, enviando os eventos de serviços que estão hospedados na nuvem para o SIEM, para correlacionar e identificar alguma anomalia.

Dekten *et al.* [Detken et al. 2015] propõe uma arquitetura dividida em duas camadas: a primeira é responsável por coletar os dados que estão na rede; a segunda tem como objetivo tratar estes dados, aplicar o processamento, correlação, armazenamento e apresentar em uma *interface* ao usuário. Os dados coletados são obtidos a partir de diversas ferramentas, como: *Nagios*, *syslog collector*, Snort, android *collector*, *log-file collector*, OpenVas. Estas informações são mantidas em um banco de dados que é acessado pelo ser-

vidor responsável por analisar e detectar situações que oferecem riscos à rede. Caso seja detectada alguma situação maliciosa, existem mecanismos de segurança pré configurados que reagem ao incidente, a fim de momentaneamente conter a situação.

Considerando os trabalhos apresentados, percebe-se que as ferramentas SIEM apresentadas pelos autores Sekharan e Detken utilizam os eventos contidos nos *logs* para gerar os incidentes, porém nenhuma das ferramentas apresentadas segue uma metodologia ou técnica para tratar os incidentes gerados. Portanto, nenhum destes trata ou gerencia os incidentes seguindo ITIL. Nas próximas seções é apresentada a proposta deste trabalho e uma avaliação desta através de um estudo de caso considerando um ambiente controlado utilizando equipamentos reais para analisar a detecção e gerenciamento de incidentes em um SIEM, aplicando ainda a metodologia ITIL.

3. Extração e gerenciamento de eventos de segurança de SIEM

Nesta Seção é descrita, de forma resumida, a ferramenta desenvolvida para gerenciar os *logs* de um SIEM - nesse caso, a solução completa a ser desenvolvida neste trabalho baseia-se no *Splunk*. O objetivo principal da ferramenta é analisar os logs, definir quais eventos precisam ser tratados e gerenciar esse tratamento, com base na metodologia ITIL. A Figura 1 ilustra as principais etapas dos processos implementados.

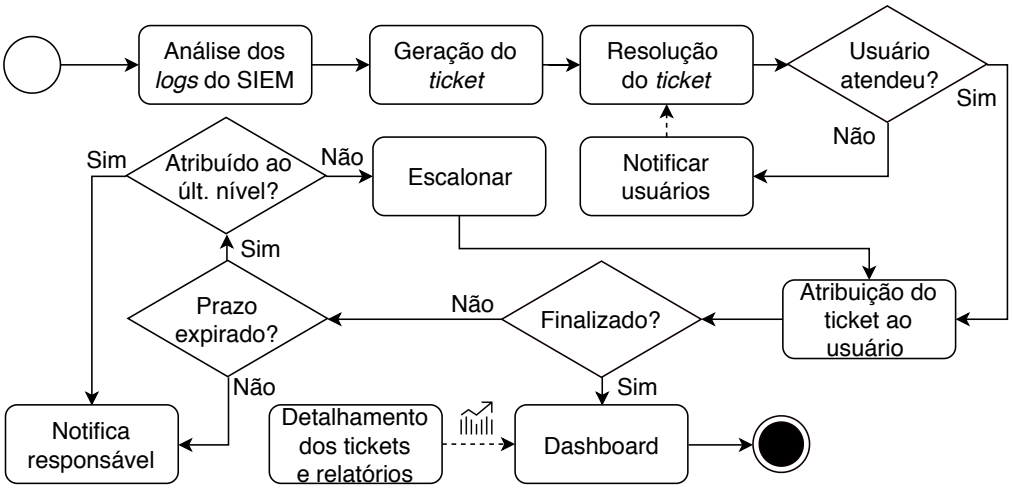

Figura 1. Diagrama do fluxo de atividades.

Análise dos logs do SIEM e geração de *ticket*: Nesta etapa são análisados os *logs* armazenados no banco de dados em intervalos pré-definidos (configuráveis na interface de acordo com as necessidades do usuário). Esta análise é feita a partir da busca por termos-chave nos *logs*. Para definir esses termos-chave, foi desenvolvida uma tela para cadastrar os mesmos, com respectivo grau de prioridade (por exemplo, alto, médio ou baixo), o tempo máximo para sua resolução (em horas) e um nível de usuário para geração do *ticket*. Os usuários do sistema são cadastrados em outra tela, com seu nível. Ao gerar um novo *ticket*, é gravado a categoria do mesmo, o nível de usuário, a data e hora da criação, o IP do *host* para o qual o log foi gerado, a mensagem completa que está contida no *log* e quantas vezes este foi encontrado na última análise.

A metodologia ITIL define que um sistema de *tickets* deve conter a opção de cadastro de cargos ou níveis, que devem ser responsáveis pelos mesmos incidentes, tendo um tempo de resolução definido e escalonado. Assim, existe a opção de ”adicionar todas

as fontes de *log*"para monitorar ou definir fonte(s) específica(s). Ainda existe a opção de "responsável", que é o usuário encarregado pelo setor, que pode acompanhar os *tickets* e receber as notificações de início, escalonamento, fechamento e detalhamento. Na tela principal, os *tickets* ainda não resolvidos são listados em diferentes cores: a)verde indica que o registro foi criado recentemente e está dentro do prazo de resolução; b)amarelo indica que passou metade do tempo definido para sua resolução; c)vermelho indica que o prazo de resolução acabou.

Resolução do *ticket*: Ao criar um *ticket* é gravada a data e hora da ocorrência, o prazo para resolução e é disparado um email para todos os usuários que podem resolver o mesmo. Para sua resolução, é disponibilizada uma tela que lista todos os *tickets* novos que um usuário pode assumir e que ainda não foram atendidos. Os usuários podem visualizar a mensagem completa do log, escrever alguma observação adicional, visualizar o status (abertos e fechados), escalonar e finalizar *tickets*. Caso a resolução não ocorra no prazo, é feito o escalonamento para os usuários de nível superior.

Escalonamento, fechamento e relatórios: o escalonamento de um *ticket* deve ocorrer em duas maneiras, segundo a ITIL [dos Santos et al. 2011]: a) Funcional: quando os usuários que estão tratando o *ticket* não conseguiram ou não possuem conhecimento suficiente; b) Hierárquico: acontece quando o tempo máximo de resolução excedeu e o *ticket* ainda não foi resolvido. O processo de fechamento consiste em gravar as informações sobre a resolução e notificar (por email) todos os usuários envolvidos. Assim, são gravados os dados sobre *tickets* resolvidos e as respectivas soluções adotadas, afim de oferecer uma base de informações para auxiliar em resoluções futuras, e também para permitir a implementação de uma ferramenta de automatização de resolução de *tickets* com base em resoluções anteriores. Para visualizar informações de gerenciamento dos *tickets*, vários relatórios foram implementados. Estes relatórios permitem, por exemplo, listar o percentual dos *tickets* resolvidos antes ou depois do prazo, comparar se esses percentuais e/ou número de *tickets* em diferentes períodos. Além disso, podem ser exibidos os principais incidentes e o número de vezes que estes ocorreram, inclusive por fonte de *log* e *host*.

4. Estudo de caso

O estudo de caso teve como objetivo executar os testes das funcionalidades do sistema desenvolvido utlizando um ambiente controlado que é apresentado na Figura 2. Em suma, o ambiente possui um *SIEM*, que é a base para a detecção dos incidentes e geração dos *tickets*. O cenário utilizado possui um servidor *AD*, um *firewall pfSense*; dois *hosts* (Windows e Linux Debian) com o *OSSEC* em modo *HIDS*; um dispositivo *Raspberry Pi 3* com o *IDS Snort*; e alguns dispositivos IoT monitorados pelo *Snort* no *Raspberry Pi 3*.

Configurações iniciais e metodologia de testes: O sistema desenvolvido requer algumas configurações iniciais. O intervalo de análise foi definido em 60s (empiricamente). No cadastro de tipos de usuários foram definidos três níveis de suporte e um nível de responsável. Foram cadastrados dois usuários por nível e um usuário responsável. Os níveis de prioridade dos *tickets* foram definidos como **baixa**, **alta** e **urgente**. A seguir foram cadastradas as expressões, com um tempo máximo de resolução e o nível de usuário. Além disso, foram configuradas as fontes de *log* definidas no ambiente de testes. No total foram cadastradas 40 expressões para as quatro fontes de *logs*, como por exemplo, "DoS/DDoS", "Flood attack", "Scan attempt", "Brute force"e "autentication failure". Os *logs* do *Snort*, AD, *firewall* e do OSSEC foram enviados para o *Rsyslog*. Notou-se que a base de *logs* recebeu as informações das diferentes ferramentas presentes na topologia por meio do protocolo UDP na porta 514. Assim, os *logs* gerados pelo servidor AD, por exemplo, foram enviados utilizando-se o *Windows SyslogAgent*, que transforma todos os

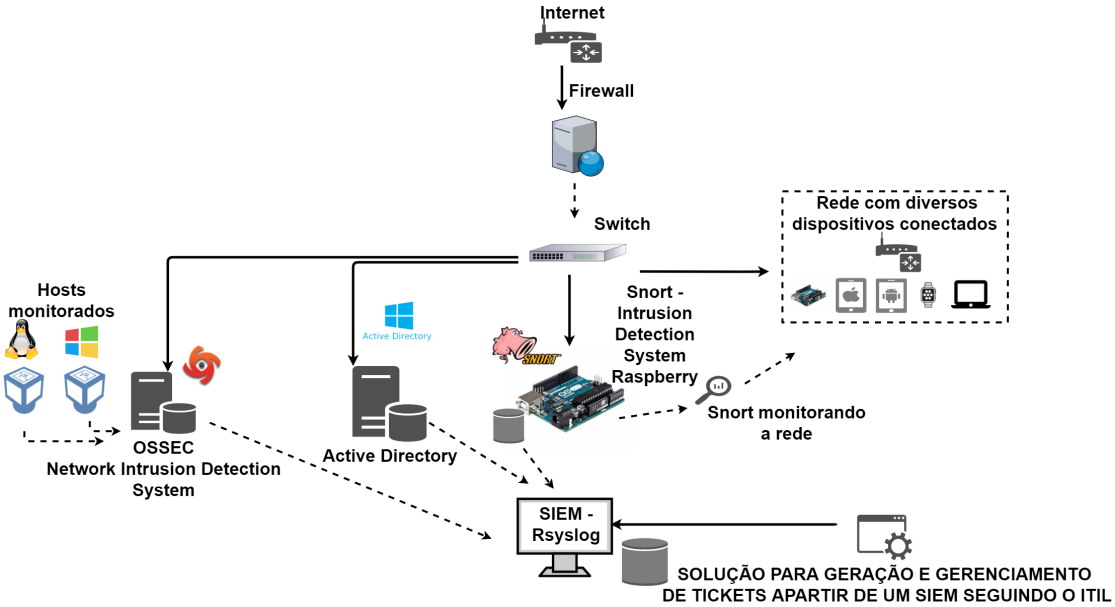

Figura 2. Ambiente de rede para testes

eventos gerados do *Windows Server* para o formato *Syslog*. Já o *Pfsense* foi configurado para enviar todos os tipos de eventos detectados pelo sistema. Este firewall já utiliza o formato *Syslog*. Da mesma forma, o *IDS Snort* foi configurado com suas regras de DoS/DDoS e port scan. O *OSSEC* foi configurado para monitorar os dois *hosts* a fim de encontrar acessos indevidos, não autorizados e detectar possíveis intrusões. Assim como no *Snort*, o *OSSEC* teve a configuração do envio dos eventos no formato *Syslog*. Durante os experimentos, foram gerados: ataques de negação de serviços, usando o Loic; port scan, usando o NMAP; tentativas de autenticação inválidas e navegação a conteúdos bloqueados por regras do firewall. Assim diversos eventos de segurança foram registrados no SIEM, sendo que alguns possuem maior relevância no âmbito de segurança de infraestrutura, como **Possível *Scan* na rede**, **Possível ataque DDoS**, **Invasão através do *Brute Force***, **Conta ou grupo deletado**, **Conexão FTP com o servidor** e **Tráfego malicioso na rede**. Assim, foram gerados 56 *tickets* a partir dos logs coletados neste estudo de caso.

Gerenciamento de *Tickets*: consiste basicamente na atribuição do usuário, escalonamento e notificações do mesmo. Foram simulados vários incidentes, que foram detectados pela ferramenta através das expressões pré-cadastradas encontradas nos logs. Inicialmente, com o *ticket* aberto e disponível para os usuários do sistema foi possível gerenciá-lo até que o mesmo foi resolvido, ou até ser escalonado para outro usuário. Foram simuladas várias situações, como *tickets* não atendidos no prazo, escalonamento, resolvidos no prazo e não resolvidos. Através dos relatórios desenvolvidos, é possível listar: 169 ocorrências de conexão FTP pelo *Raspberry* e destes foram gerados e resolvidos 5 *tickets*; 2294 ocorrências de detecção de *ping* pelo *raspberry*, dos quais foram gerados e resolvidos 5 *tickets*; 18 ocorrências de inicialização do servidor *ossec* e destes gerados e resolvidos 4 *tickets*. Com o uso da ferramenta desenvolvida, foi possível verificar que todos os incidentes detectados foram devidamente resolvidos, a partir da gerência dos mesmos seguindo a metodologia adotada. Além disso, várias informações estatísticas e de segurança puderam ser observadas, como por exemplo o aumento do tempo de resolução dos *tickets* comparando os três últimos dias observados.

5. Considerações finais

Este trabalho apresentou uma solução para gerenciar *logs* de SIEM, extraindo eventos definidos como importantes e criando *tickets* que são gerenciados de forma a serem resolvidos. Esta solução pode ser aplicada em diversos cenários, independente do hardware ou sistemas utilizados. Além disso, diversas ferramentas de SIEM podem ser integradas, adaptando a forma de conexão com o banco de dados e sua estrutura. No estudo de caso é demonstrada a aplicabilidade desta solução em um cenário de forma que *logs* de eventos de segurança importantes sejam tratados seguindo a metodologia ITIL, sem a necessidade dos usuários observarem os logs de forma manual e constante.

O gerenciamento de *tickets* auxilia na identificação e resolução dos principais eventos de segurança, evitando que passem despercebidos pelos responsáveis. Além disso, várias informações gerenciais podem ser obtidas, como por exemplo, tempo de resolução, usuários mais ativos, tipos de problemas mais comuns e *hosts* mais problemáticos. Foi possível verificar a eficácia na resolução e a reação à possíveis ataques, alterações de registro, conexões indevidas, por exemplo, pois a solução proposta identificou tais eventos, gerou os respectivos *tickets* e automatizou o gerenciamento destes.

Para a sequencia deste trabalho, estão sendo desenvolvidos métodos de descoberta das ferramentas de segurança através da conexão com o SIEM de maneira automática, permitindo fazer a inserção dos *logs* a uma lista de possíveis incidentes, sem a necessidade do cadastro inicial. Além disso, pretende-se usar métodos de inteligência artificial para automatizar a geração e a resolução de *tickets* com base em resoluções anteriores.

Referências

Ahmad, N. and Shamsudin, Z. M. (2013). Systematic approach to successful implementation of itil. *Procedia Computer Science*, 17:237 – 244. First International Conference on Information Technology and Quantitative Management.

Bachane, I., Adsi, Y. I. K., and Adsi, H. C. (2016). Real time monitoring of security events for forensic purposes in cloud environments using siem. In *2016 Third International Conference on Systems of Collaboration (SysCo)*, pages 1–3.

Detken, K. O., Rix, T., Kleiner, C., Hellmann, B., and Renners, L. (2015). Siem approach for a higher level of it security in enterprise networks. In *2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*.

dos Santos, R. L., Wickboldt, J. A., Lunardi, R. C., Dalmazo, B. L., Granville, L. Z., Gaspary, L. P., Bartolini, C., and Hickey, M. (2011). A solution for identifying the root cause of problems in it change management. In *12th IFIP/IEEE International Symposium on Integrated Network Management (IM 2011)*, pages 586–593.

Gupta, R., Prasad, K. H., and Mohania, M. (2008). Automating itsm incident management process. In *2008 International Conference on Autonomic Computing*, pages 141–150.

Scholzel, M., Eren, E., and Detken, K. O. (2015). A viable siem approach for android. In *2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*.

Sekharan, S. S. and Kandasamy, K. (2017). Profiling siem tools and correlation engines for security analytics. In *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, pages 717–721.