Gerenciamento de incidentes em SIEM seguindo ITIL

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 Managemen" 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 faz 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 proteção, como *firewalls*, IDS (*Intrusion Detection System*), IPS (*Intrusion Prevention System*) e ferramentas de monitoramento, que funcionam de forma independente, com o objetivo de aumentar a segurança nas redes e sistemas computacionais. 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. Adicionalmente, muitas vezes os *logs* apresentam informações redundantes, o que pode atrasar a ação de prevenção e/ou reação ao ataque ou à 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 têm 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, em muitos casos, não ocorre o gerenciamento eficiente dos alertas gerados.

Com o objetivo de mitigar estes problemas, este artigo apresenta uma proposta para identificar e gerenciar os incidentes relacionados aos eventos de segurança mais críticos em um SIEM. Este gerenciamento é realizado seguindo a metodologia ITIL [Foundation 2012], que consiste em um conjunto de processos para boas práticas de gerenciamento de serviços de Tecnologia da Informação (TI). A solução proposta foi implementada e avaliada através de um estudo de caso.

O restante deste artigo está dividido da seguinte forma: a seção 2 apresenta os conceitos necessários ao entendimento dos objetivos propostos, descrevendo sobre a solução SIEM, ITIL e ferramentas de gerenciamento de informações; a seção 3 apresenta alguns trabalhos semelhantes encontrados na literatura. A seção 4 descreve a ferramenta desenvolvida para extrair e gerenciar *tickets* a partir de *logs* SIEM. Na Seção 5 é apresentado um ambiente para testes e a avaliação da solução desenvolvida através de um estudo de caso. E por fim, a Seção 6, traz considerações finais com indicações para trabalhos futuros.

2. Referencial Teórico

Nesta seção serão apresentados os principais conceitos utilizados neste trabalho. Desta forma, serão abordados os principais conceitos de segurança em redes de computadores e sistemas da informação utilizados neste trabalho. Além disso, serão apresentados os principais definições na área de Sistemas de Gerenciamento de Eventos e Informações de Segurança (SIEM), bem como o ciclo de vida da metodologia ITIL.

2.1. Princípios de Segurança em Redes e Sistemas

Ao tratar estudos que abordam a segurança da informação nos mais diversos âmbitos, é essencial delimitar os conceitos basilares que sustentam as discussões na área. Comumente, esses conceitos podem ser abordados conforme a especificação X.800 [ITU 2018], que descreve os principais princípios da segurança como:

- **Autenticidade**: garante que as entidades envolvidas na comunicação são aquelas que afirmam ser;
- **Privacidade**: O recurso deve ser disponibilizado somente se houver autorização;
- **Confidencialidade**: proteção dos dados contra divulgação não autorizada;
- **Integridade**: Garantir a que os dados recebidos são os mesmos que foram transmitidos, ou seja, não foram indevidamente alterados;
- **Disponibilidade**: o recurso deve estar sempre acessível às pessoas (ou sistemas) previamente autorizadas, sempre que for necessário acessá-lo.
- **Não-repúdio**: assegura que transmissor dos dados (mensagem) não pode negar sua autoria e que a mensagem foi recebida pelo receptor.

Estes princípios, que são base para a segurança, podem ser comprometidos por diversos tipos de ataques, sendo que os mais comuns são ataques de negação de serviço (DoS/DDoS)[Neu et al. 2016], Scan [Neu et al. 2018], Fraude e Worms, segundo

o CERT.br [CERT.br 2018]. A invasão de um sistema sempre trará consequências, que podem variar entre monitoramento sem autorização, danos à imagem da empresa e retrabalho para recuperar o que foi danificado. Além disso, podem levar a exposição e/ou alteração indevida de dados sensíveis, lentidão ou indisponibilidade de serviço e o consequente prejuízo financeiro [Tatar et al. 2016].

Assim, o uso de ferramentas de proteção, como IDS/IPS [Neu et al. 2018], *firewall*, antivírus, controle de acesso, entre outras, é fundamental para proteger um ambiente de TI. Como diferentes ferramentas e tecnologias podem ser utilizadas para aumentar a segurança, a gestão e a correta implantação destas pode se tornar uma tarefa complexa. Por isso, pode ser adequado a utilização/criação de Centros de Operações de Segurança (*Security Operation Center - SOC)* nos ambientes de TI, centralizando os serviços em equipes especializadas como objetivo de gerenciar e melhorar a segurança. Em um SOC são centralizados processos de prevenção, detecção, gestão e resposta à incidentes, avaliação e monitoramento dos serviços utilizados. Um SOC pode proporcionar o monitoramento em tempo real dos principais servidores, processos e de toda a infraestrutura de TI, trazendo maior agilidade na respostas à incidentes. Além disso, facilita o processo de auditoria em segurança e otimiza a gestão da segurança, reduzindo o número de incidentes através de um trabalho proativo [Miloslavskaya 2017].

Princípios gerais do gerenciamento de redes também podem ser aliados à segurança. Por exemplo, o modelo FCAPS (*Fault, Configuration, Accounting, Performance and Security*) [Abdallah et al. 2018] que tem como objetivo atender os requisitos de qualidade de serviço e operação de toda a rede e infraestrutura de TI. O modelo consiste em cinco pontos de gerenciamento: **gerenciamento de falhas (F)**, **gerenciamento de configuração (C)**, **gerenciamento de contabilização (A)**, **gerenciamento de performance (P)** e **gerenciamento de segurança (S)**. Nesse sentido, o presente trabalho aborda os itens referentes ao gerenciamento de falhas e ao gerenciamento de segurança.

2.2. SIEM

SIEM realiza o monitoramento de eventos e ameaças de segurança, permitindo a captura dos registros de ativos na rede para informar os responsáveis de forma a auxiliar a tomada de ações a partir disso. No geral, as soluções de SIEM objetivam fornecer as informações mais relevantes dos *logs* para os administradores da rede [Detken et al. 2015]. Um sistema SIEM completo consiste em diferentes módulos, que devem suportar algumas funcionalidades como a **correlação de eventos**, **detecção de situação**, **mapeamento de identidade** e ***Interface* de programação de aplicativos (API)**.

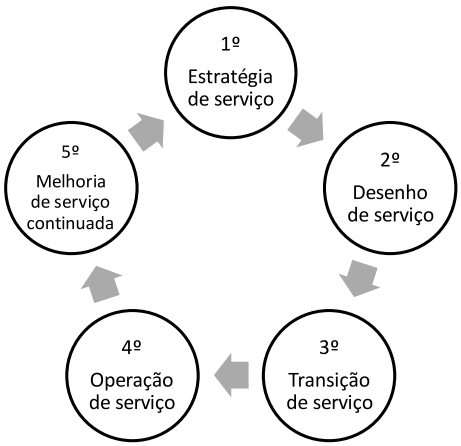
As principais funcionalidades de um sistema SIEM são: **Coleta**, responsável por receber os *logs* de outras ferramentas de segurança e dispositivos; **Agregação**: onde os *logs* coletados são agregados e normalizados (agrupamento dos eventos que tem semelhanças entre si); **Correlação**, cujo objetivo é vincular vários eventos ou alertas de segurança entre vários sistemas e ferramentas que gerenciam a rede, a fim de identificar atividades anômalas; e **Notificação**, onde são gerados alertas. Existem atualmente diversas soluções de SIEM, como por exemplo, *IBM Qradar*, *HP ArcSight*, *ossim*, *Splunk* [Splunk 2018], *LogRhythm* [LogRhythm 2018] e *ELK* [ELK 2018].

2.3. ITIL

ITIL [Foundation 2012] é um conjunto de boas práticas para o gerenciamento de serviços de TI. A adoção de metodologias como ITIL é importante nos ambientes de TI modernos para otimizar custos, agilizar e otimizar o gerenciamento de processos

[Veronica and Suryawan 2017]. A metodologia ITIL sugere que as atividades de gerenciamento de serviços sejam estruturadas com base no ciclo de vida do serviço de TI de forma a melhorar a qualidade dos serviços, auxiliando em um melhor gerenciamento [Jasek et al. 2015]. É composto por cinco livros, onde cada um deles é específico para o ciclo de vida do serviço, sendo eles **Estratégia de Serviço**, **Desenho de Serviço**, **Transição de Serviço**, **Operação de Serviço** e **Melhoria de Serviço Continuada**. A Figura 1 ilustra os ciclos de vida desta metodologia [Veronica and Suryawan 2017].

Figura 1. Ciclos de vida da metodologia ITIL



A ITIL contém um conjunto de melhores práticas para o gerenciamento de serviços de TI e é considerada como a mais reconhecida referência de práticas de gerenciamento de TI. A ITIL sugere que as atividades de gerenciamento de serviços sejam estruturadas com base no ciclo de vida do serviço de TI, com o objetivo de melhorar a qualidade e gerenciamento dos serviços [Jasek et al. 2015]. É composta por cinco livros, onde cada um deles é específico para o ciclo de vida do serviço, conforme ilustrado na Figura 1. Nesta seção é apresentada a ITIL v3 [Foundation 2012], pois a ITIL 4 [Foundation 2019] foi publicada após este trabalho ter sido iniciado.

1. **Estratégia de serviço**: define as melhores estratégias para agregar valor ao negócio e gerenciar os serviços de TI. Ainda, são definidas as demandas do negócio, as necessidades e quais os principais recursos que a infraestrutura de TI deve fornecer para alcançar os objetivos propostos;
2. **Desenho de serviço**: define como implementar a estratégia definida na etapa anterior. Devem ser planejados os serviços, a utilização dos recursos e a capacidade que a TI dispõem para entregar os requisitos definidos anteriormente. Assim, consequentemente, reduzirá os riscos de uma implementação de serviços inadequada;
3. **Transição de serviço**: define quais novos serviços devem ser colocados em operação e quais devem ser descontinuados. Nesta etapa, o serviço é instanciado conforme os requisitos modelados na etapa anterior, evitando erros e trazendo o maior retorno possível do investimento;
4. **Operação de serviço**: os serviços entregues devem cumprir os níveis definidos no desenho e implementados na transição de serviços. É feita a gestão de acesso aos serviços, dos incidentes e o acompanhamento dos serviços implementados;
5. **Melhoria de serviço continuada**: trata da melhoria contínua dos serviços através de pequenas melhorias incrementais, utilizando metas e indicadores.

3. 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 identificar e gerenciar incidentes.

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 operacionais 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 anomalias.

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 servidor 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.

Portanto, percebe-se diferentes propostas de trabalhos relacionados a SIEM. A Tabela 1 mostra um comparativo entre os trabalhos relacionados descritos nesta seção. São destacados trabalhos que apresentam novas estratégias para implementação e também trabalhos que avaliam e comparam implementações existentes (coluna ”Contribuição/Objetivo”). Algumas soluções de SIEM permitem integração com outros sistemas de segurança (coluna ”Integração”) e geram incidentes (coluna ”Gera Incidentes”). Entretanto, existe pouca discussão sobre o gerenciamento e tratamento dos incidentes identificados nos SIEMs e, em nossas pesquisas, não encontramos nenhuma proposta que utiliza a ITIL para esse gerenciamento.

4. Extração e gerenciamento de eventos de segurança de SIEM

Nesta Seção é descrita a ferramenta desenvolvida para gerenciar o tratamento dos eventos de segurança mais importantes detectados nos *logs* de um SIEM. A Figura 2 ilustra as principais etapas dos processos implementados.

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

Trabalhos	Contribuição/Objetivo	Integração	Gera Incidentes	ITIL
SEKHARAN; KANDDASAMY, 2017	Avaliação	Sim	Sim	Não
NABIL *et al.*, 2017	Avaliação	Sim	Não	Não
BACHANE; ADSI, 2016	Avaliação	Não	Não	Não
DETEKEN *et al.*, 2015	Implementação	Sim	Sim	Não
Este trabalho	Implementação	Sim	Sim	Sim

Tabela 1. Comparativo com trabalhos relacionados

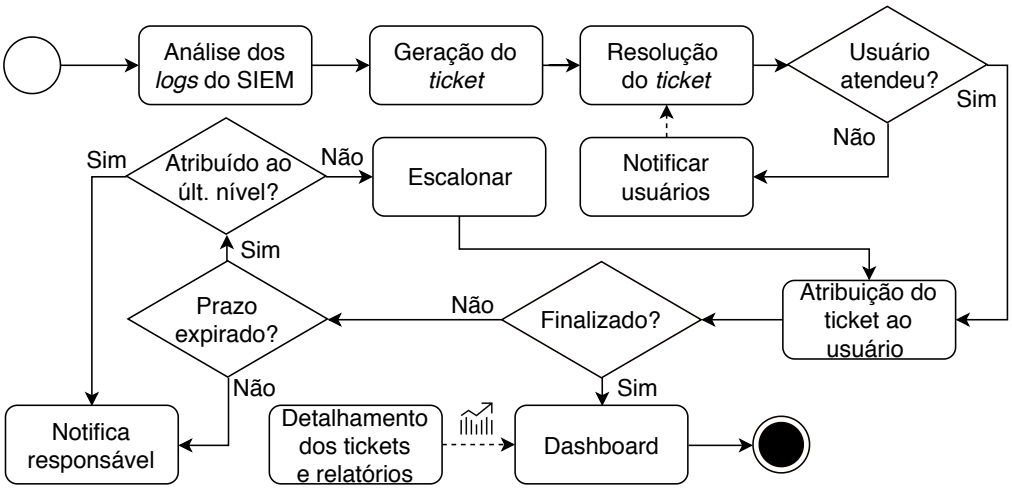


Figura 2. Diagrama do fluxo de atividades.

acordo com as necessidades do usuário). Esta análise é feita a partir da busca por termos-chave nos *logs*, aos quais é atribuído um nível de importância e um tempo máximo de resolução. 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 Figura 3 mostra um exemplo de informações que são extraídas nos logs (*"Possible DoS detected"*) e comparadas com os termos-chave pré-cadastrados (*"DoS detected"*) para gerar os tickets.

Figura 3. Eventos do SIEM que serão detectados como incidentes

Date: 2018-11-02 09:04:45
Host: **raspberrypi**
Messagetype: Syslog
Message: [1:10001:1] Possible DoS detected! {TCP} 192.168.2.28 [More Information] :2522 -> 192.168.2.57 [More Information] :80

Cadastro no banco de dados da solução:
Id:57 host: raspberry expression: %DoS detected% description: possível ataque DoS

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”, 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*.

Assim, as principais funcionalidades implementadas em nosso protótipo e que são disponibilizadas na tela de gerenciamneto dos tickets são:

- Ver Mensagem: exibe o *log* completo coletado do SIEM;
- Escrever observação geral: permite adicionar uma descrição genérica ao *ticket*.
- Escalonar *ticket*: usado para escalonar o atendimento a outro usuário.
- Escrever observação *ticket*: usado para descrever como o incidente foi resolvido;
- Visualizar abertos: lista os *tickets* ainda não resolvidos atribuídos ao usuário;
- Visualizar finalizados: lista os *tickets* já resolvidos pelo usuário.
- Finalizar *ticket*: conclui o *ticket*;
- Detalhes do *ticket*: lista detalhes sobre o *ticket* e qual usuário responsável.
- *Relatórios*: disponibiliza alguns relatórios com informações estatísticas sobre tickets abertos e fechados, tempo de resolução, base com soluções adotadas e principais tipos de incidentes encontrados/resolvidos.

5. 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 4. Em suma, o ambiente possui um *SIEM*, que é a base para a detecção dos incidentes e geração dos

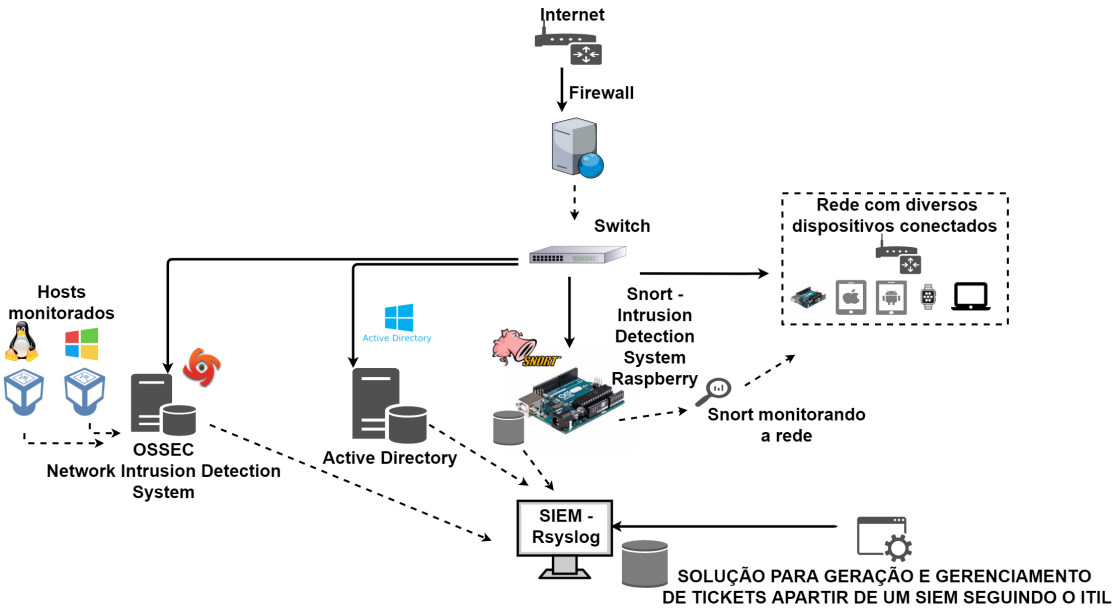


Figura 4. Ambiente de rede para testes

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 detected”, ”Flood attack”, ”Scan attempt”, ”Brute force”e ”authentication 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 através do *Windows SyslogAgent*, que transforma todos os eventos gerados do *Windows Server* para o formato *Syslog*. O *Pfsense* foi configurado para enviar todos os tipos de eventos detectados pelo sistema. Este firewall utiliza o formato *Syslog*. Da mesma forma, o *IDS Snort* foi configurado com suas regras padrão 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 serviço com o Loic; port scan com o NMAP; tentativas de autenticação inválidas e navegação a conteúdos bloqueados por regras de firewall. Assim, diversos eventos de segurança foram registrados no SIEM. Podem ser citados com maior relevância para a segurança da infraestrutura: **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.

6. 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. A solução proposta foi eficaz na resolução e reação à possíveis ataques, alterações de registro e conexões não autorizadas(indevidas). Além disso, a partir da identificação de tais eventos, foram gerados automaticamente os respectivos *tickets* e o gerenciamento destes até a sua resolução.

Para a sequência 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. Por fim, pretende-se avaliar e adotar as recomendações do ITIL 4 [Foundation 2019], publicado recentemente, no gerenciamento de incidentes de segurança.

Referências

Abdallah, S., Elhajj, I. H., Chehab, A., and Kayssi, A. (2018). A network management framework for sdn. In *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pages 1–4.

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.

CERT.br (2018). Centro de estudos, resposta e tratamento de incidentes de segurança no brasil.

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.

ELK (2018). Elasticsearch, logstash, kibana — elastic.

Foundation, I. (2012). *ITIL® Foundation Handbook 3rd*, volume 1. AXELOS, 3rd edition.

Foundation, I. (2019). *ITIL® Foundation, ITIL 4 edition*, volume 1. AXELOS, 4 edition.

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

ITU (2018). Telecommunication standardization sector.

Jasek, R., Kralik, L., Zak, R., and Kolcavová, A. (2015). Differences between itil® v2 and itil® v3 with respect to service transition and service operation. *AIP Conference Proceedings*, 1648(1):550017.

LogRhythm (2018). Logrhythm, the security intelligence company — logrhythm.

Miloslavskaya, N. (2017). Soc- and sic-based information security monitoring. In Rocha, Á., Correia, A. M., Adeli, H., Reis, L. P., and Costanzo, S., editors, *Recent Advances in Information Systems and Technologies*, pages 364–374, Cham. Springer.

Neu, C. V., Tatsch, C. G., Lunardi, R. C., Michelin, R. A., Orozco, A. M. S., and Zorzo, A. F. (2018). Lightweight ips for port scan in openflow sdn networks. In *NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium*, pages 1–6.

Neu, C. V., Zorzo, A. F., Orozco, A. M. S., and Michelin, R. A. (2016). An approach for detecting encrypted insider attacks on openflow sdn networks. In *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*.

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.

Splunk (2018). Splunk: Inteligência operacional, gerenciamento de logs.

Tatar, U., Bahsi, H., and Gheorghe, A. (2016). Impact assessment of cyber attacks: A quantification study on power generation systems. In *2016 11th System of Systems Engineering Conference (SoSE)*, pages 1–6.

Veronica and Suryawan, A. D. (2017). Information technology service performance management using cobit and an itil framework: A systematic literature review. In *2017 International Conference on Information Management and Technology (ICIMTech)*.