



PUCRS

Pontifícia Universidade Católica
do Rio Grande do Sul



Extração e Gerenciamento de Incidentes em SIEM

Charles V. Neu, Evandro L. C. Trebien, Daniel D. Bertoglio,
Roben C. Lunardi e Avelino F. Zorzo

- Introdução
- Referencial Teórico
- Trabalhos Relacionados
- Sistema de Tratamento de Logs SIEM Seguindo ITIL
- Estudo de caso em um Ambiente Simulado (Testes)
- Conclusão e Trabalhos Futuros
- Referências

- IoT e dispositivos conectados à rede
- Ameaças/segurança
- Logs
- SIEM
- Tickets/TTS
- ITIL

- IoT e dispositivos conectados à rede
- Ameaças/segurança
- Logs
- SIEM
- Tickets/TTS
- ITIL

Objetivo principal:

Gerar tickets automaticamente, a partir de logs do SIEM, e gerenciar o atendimento destes seguindo ITIL

- Introdução
- Referencial Teórico
- Trabalhos Relacionados
- Sistema de Tratamento de Logs SIEM Seguindo ITIL
- Estudo de caso em um Ambiente Simulado (Testes)
- Conclusão e Trabalhos Futuros
- Referências

→ SIEM – *Security Information and Event Management*
(Gerenciamento e Correlação de Eventos de Segurança)

- ◆ Coleta
- ◆ Agregação
- ◆ Correlação
- ◆ Notificação

- Tickets fazem partes de sistemas *Help Desk*, são utilizados para fazer o gerenciamento dos chamados (MUNI *et al.*, 2017)
 - ◆ Resolução dos incidentes de forma eficiente
 - ◆ Base de conhecimento
 - ◆ Auditoria

1. Estratégia de serviço
2. Desenho de serviço
3. Transição de serviço
4. Operação de serviço
5. Melhoria de serviço continuada



- Introdução
- Referencial Teórico
- **Trabalhos Relacionados**
- Sistema de Tratamento de Logs SIEM Seguindo ITIL
- Estudo de caso em um Ambiente Simulado (Testes)
- Conclusão e Trabalhos Futuros
- Referências

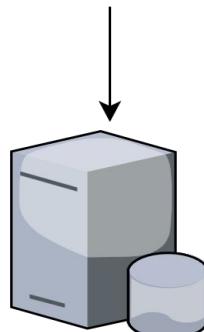
Trabalhos Relacionados

Trabalhos relacionados	Desenvolvimento	Possibilita integração com outras ferramentas de segurança	Gera incidentes a partir dos eventos	Trata ou gerencia os incidentes seguindo ITIL
Profiling SIEM tools and correlation engines for security analytics. (SEKHARAN; KANDDASAMY, 2017)	AVALIAÇÃO	SIM	SIM	NÃO
SIEM selection criteria for an efficient contextual security. (NABIL <i>et al.</i> , 2017)	AVALIAÇÃO	SIM	NÃO	NÃO
Real time monitoring of security events for forensic purposes in Cloud environments using SIEM. (BACHANE; ADSI, 2016)	AVALIAÇÃO	NÃO	NÃO	NÃO
SIEM approach for a higher level of IT security in enterprise networks. (DETEKEN <i>et al.</i> , 2015)	IMPLEMENTAÇÃO	SIM	SIM	NÃO
Este trabalho	IMPLEMENTAÇÃO	SIM	SIM	SIM

- Introdução
- Referencial Teórico
- Trabalhos Relacionados
- **Sistema de Tratamento de Logs SIEM Seguindo ITIL**
- Estudo de caso em um Ambiente Simulado (Testes)
- Conclusão e Trabalhos Futuros
- Referências

Visão Geral da Solução

Logs das ferramentas e dispositivos de segurança

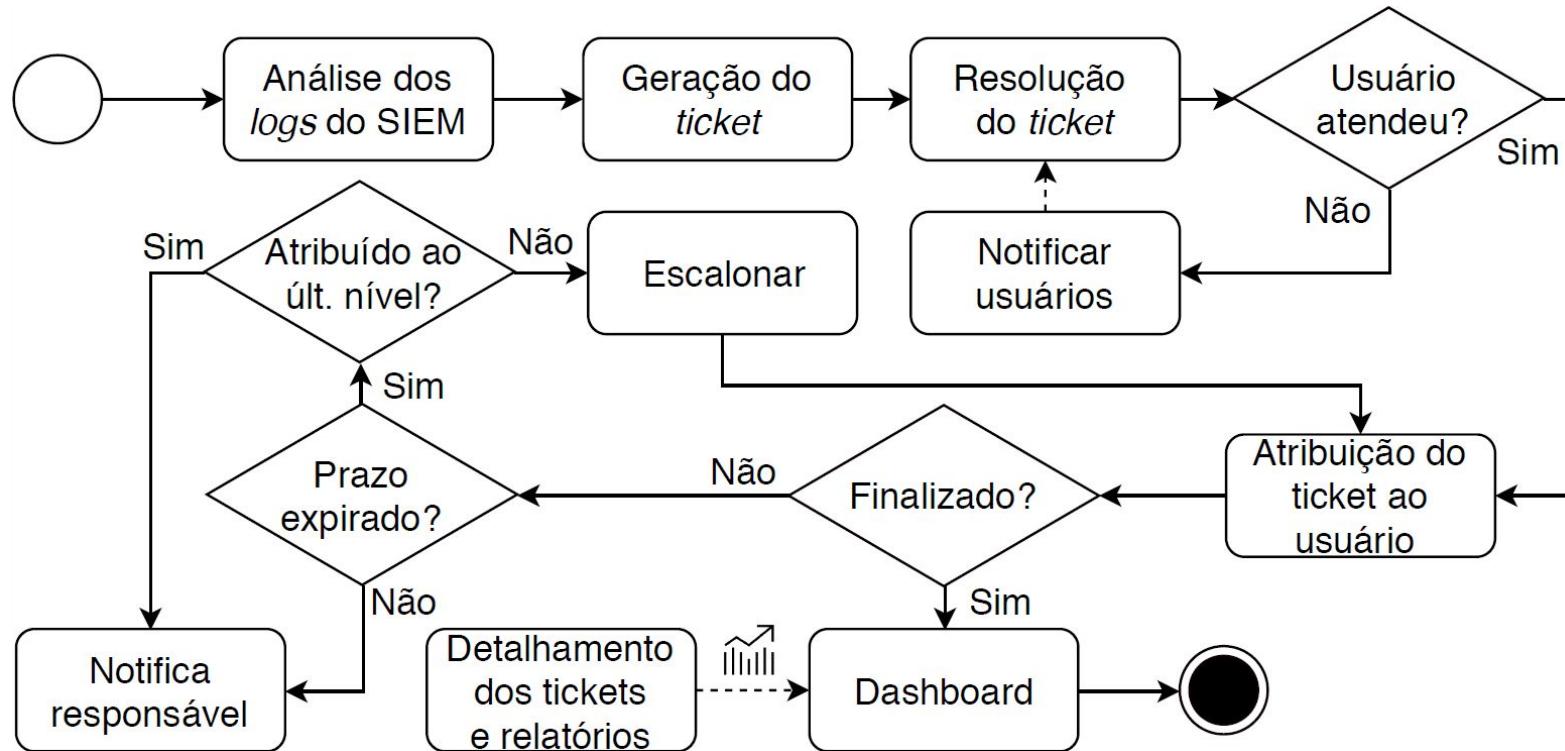


Solução desenvolvida



- Inserção de ferramentas de segurança (fontes de log)
- Cadastro de usuários/setores na solução
- Gerar tickets de forma automática
- Notificações por e-mail sobre incidentes/tickets
- Escalonar os tickets caso não cumprido às SLA's
- Tela com relatórios

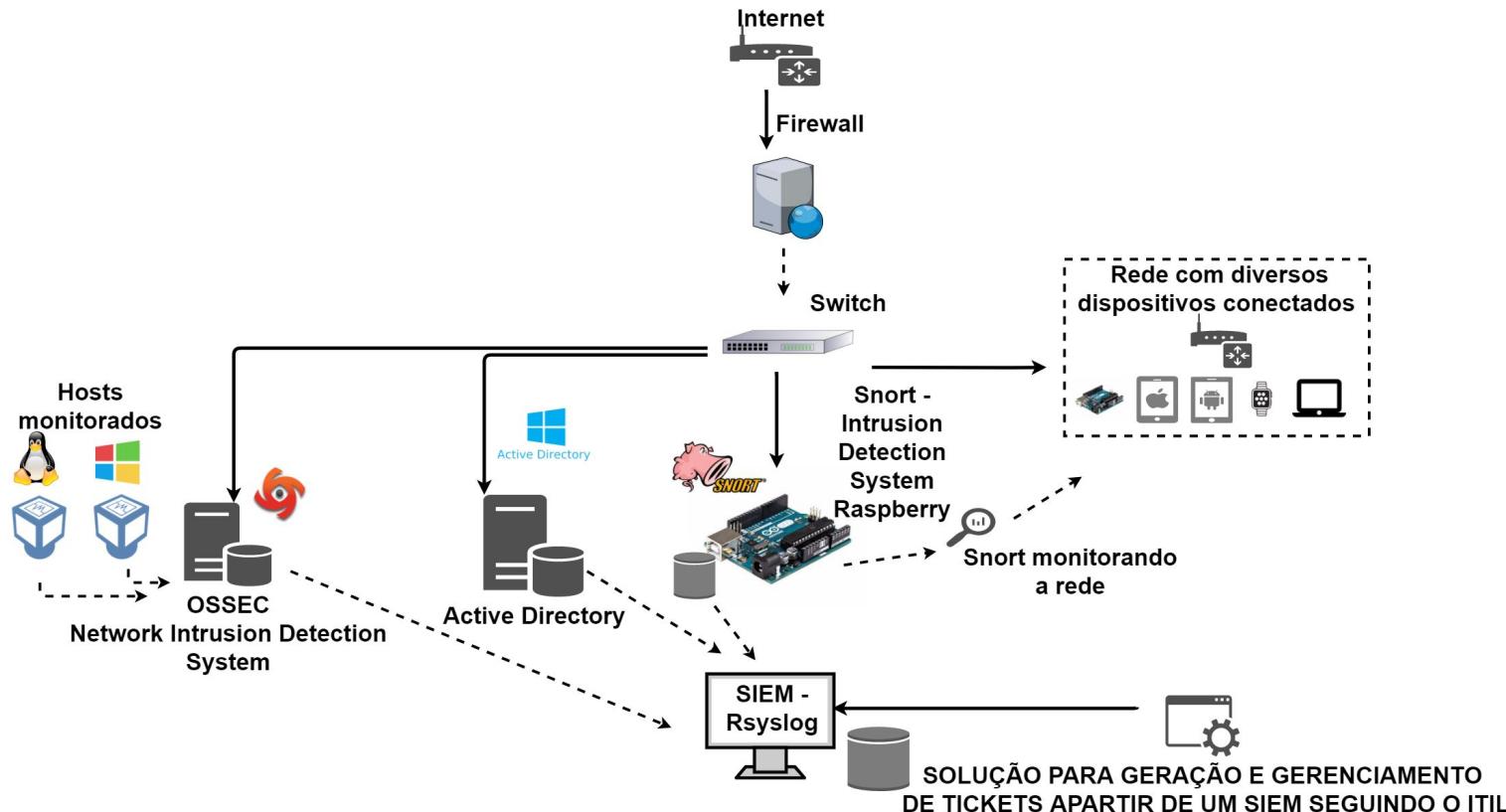
Diagrama do Fluxo de Atividades



- Introdução
- Referencial Teórico
- Trabalhos Relacionados
- Sistema de Tratamento de Logs SIEM Seguindo ITIL
- **Estudo de caso em um Ambiente Simulado (Testes)**
- Conclusão e Trabalhos Futuros
- Referências

- Configuração e implantação do cenário de testes
- Configuração inicial da ferramenta
 - ◆ Cadastro das SLA's
 - ◆ Cadastro das fontes de LOG
 - ◆ Cadastro dos usuários e níveis de suporte
- Inserção de ataques
- Detecção do incidente e criação do ticket
- Atribuição do ticket e tratamento do incidente seguindo ITIL

Estudo de Caso em um Ambiente Simulado



Estudo de Caso - Tela de Login



GerenciadorDeIncidentes.exe

Gerenciador De Incidentes - Login x

Usuário:

Senha:

LOGIN

Estudo de Caso - Tela Inicial

Central De Serviços - Usuário: Administrador (Suporte Nível 2)

Central De Serviços

Filtros
De 03/12/2018 07:52 até 10/12/2018 07:52 Prioridade 0

Mensagem Aplicar Filtro Taxa de Atualização

Legendas
Verde - Tickets abertos recentemente Amarelo - Tickets abertos já a bastante tempo Vermelho - Tickets fechando prazo SLA

ID	Host	Mensagem	Data do Log	Prioridade
86	raspberrypi	[1:10001:1] Possible DoS detected! {TCP} 192.168.2.28:52442 -> 192.168.2.57:80	segunda-feira, 10 de...	ALTA [12 HRs]
80	raspberrypi	[1:10000001:1] ICMP PING detected !! {ICMP} 192.168.2.57 -> 192.168.2.28	segunda-feira, 10 de...	ALTA [12 HRs]
81	raspberrypi	[1:1000002:1] Alerta! FTP connection! {TCP} 192.168.2.28:61742 -> 192.168.2.57:21	segunda-feira, 10 de...	URGENTE [2 HRs]
82	ossecserver	Alert Level: 5; Rule: 5710 - Attempt to login using a non-existent user; Location: (debiancliente2) 192.168.2.31->/var/log/auth.log; classification: s...	segunda-feira, 10 de...	URGENTE [2 HRs]
84	ossecserver	Alert Level: 10; Rule: 5551 - Multiple failed logins in a small period of time.; Location: (debiancliente2) 192.168.2.31->/var/log/auth.log; classificatio...	segunda-feira, 10 de...	URGENTE [2 HRs]
85	raspberrypi	[1:1228:7] SCAN nmap XMAS [Classification: Attempted Information Leak] [Priority: 2] {TCP} 192.168.2.28:34995 -> 192.168.2.57:25	segunda-feira, 10 de...	URGENTE [2 HRs]
87	raspberrypi	[1:10000001:1] ICMP PING detected !! {ICMP} 192.168.2.57 -> 192.168.2.28	segunda-feira, 10 de...	ALTA [12 HRs]
83	ossecserver	Alert Level: 5; Rule: 18210 - Security Enabled Local Group Changed; Location: (win7cliente1) 192.168.2.30->WinEvtLog; classification: windows....	segunda-feira, 10 de...	BAIXA [48 HRs]
79	ossecserver	Alert Level: 3; Rule: 502 - Ossec server started.; Location: ossecserver->ossec-monitord; classification: ossec; ossec: Ossec started.	segunda-feira, 10 de...	BAIXA [48 HRs]

1 – Cadastra expressões

2 – Cadastra SLA's

3 – Cadastra Grupos/Setores

4 – Cadastra Usuários

5 – Tela de relatórios

6 – Tela de tickets

7 - Atualiza

Estudo de Caso - Tela de Cadastro de SLA's



Central De Serviços - Usuário: Charles V. Neu (Suporte Nível 1)

Central De Serviços

Filtros

De 03/12/2018 08:09 até 10/12/2018 08:09 Prioridade 0 Mensagem Aplicar Filtro Taxa de Atualização

Legendas
Verde - Tickets abertos recentemente

Tickets Abertos

ID	Host	Mensagem
86	raspber...	[1:10001:1] Possible DoS dete...
80	raspber...	[1:10000001:1] ICMP PING de...
81	raspber...	[1:10000002:1] Alert! FTP cor...
82	ossecse...	Alert Level: 5; Rule: 5710 - Att...
84	ossecse...	Alert Level: 10; Rule: 5551 - N...
85	raspber...	[1:1228:7] SCAN nmap XMAS de...
87	raspber...	[1:10000001:1] ICMP PING de...
83	ossecse...	Alert Level: 5; Rule: 18210 - S...
79	ossecse...	Alert Level: 3; Rule: 502 - Oss...

SLA

URGENTE [2 HRs]

Novo

Edição

ID: 1

Descrição: URGENTE

Nível: 2

Resolver em até: 2 Horas

Salvar

Vermelho - Tickets fechando prazo SLA

Prioridade

- ALTA [12 HRs]
- ALTA [12 HRs]
- URGENTE [2 HRs]
- URGENTE [2 HRs]
- URGENTE [2 HRs]
- URGENTE [2 HRs]
- ALTA [12 HRs]
- BAIXA [48 HRs]
- BAIXA [48 HRs]

- Cadastro uma parte da mensagem de log e a ferramenta faz a busca no BD.
- LOG:

Date: 2018-10-31 21:39:45

Host: **raspberrypi**

Messagetype: Syslog

Message [1:1000002:1] Alerta! **FTP connection!** {TCP} 192.168.2.28 [More Information] :53896 -> 192.168.2.29 [More Information] :21

Central De Serviços - Usuário: Charles V. Neu (Suporte Nível 1)

Central De Serviços

Filtros

De 03/12/2018 08:09 até 10/12/2018 08:09 Prioridade 0 Mensagem Aplicar Filtro Taxa de Atualização

Legendas

Verde - Tickets abertos recentemente

Tickets Abertos

ID	Host	Mensagem
86	raspberry...	[1:10001:1] Possible [1:1000001:1] ICMP
80	raspberry...	[1:10000001:1] Alert!
81	raspberry...	[1:10000002:1] Alert!
82	ossecse...	Alert Level: 5; Rule: 5
84	ossecse...	Alert Level: 10; Rule: 1
85	raspberry...	[1:1228:7] SCAN nmap
87	raspberry...	[1:10000001:1] ICMP
83	ossecse...	Alert Level: 5; Rule: 1
79	ossecse...	Alert Level: 3; Rule: 5

Cadastro de tipos de Incidentes

Tipos Conexão FTP detectada - RB Editar Remover Criar Novo

Edição

ID 16

Fonte de Log raspberry

SLA URGENTE [2 HRs]

Expressão %FTP connection%

Descrição Conexão FTP detectada - RB

Salvar

Vermelho - Tickets fechando prazo SLA

Prioridade

URGENTE [12 HRs]
URGENTE [12 HRs]
URGENTE [2 HRs]
URGENTE [48 HRs]
URGENTE [48 HRs]

- Principais expressões cadastradas:
- Conexão FTP/SSH
- TCP DoS
- Falha de login
- Bloqueio de conta por tentativas inválidas de login
- Possível scan
- Usuário/Grupo - adicionado/removido do sistema

Estudo de Caso - Cadastro de Cargos | Setores



Central De Serviços - Usuário: Charles V. Neu (Suporte Nível 1)

Central De Serviços

Filtros
De 03/12/2018 08:09 até 10/12/2018

Legendas
Verde - Tickets abertos recentemente

Tickets Abertos

ID	Host	Mensagem
86	raspber...	[1:10001:1] Possible DoS
80	raspber...	[1:10000001:1] ICMP PIN
81	raspber...	[1:1000002:1] Alerta FTP
82	ossecse...	Alert Level: 5; Rule: 5710
84	ossecse...	Alert Level: 10; Rule: 5551
85	raspber...	[1:1228:7] SCAN nmap XMAS
87	raspber...	[1:10000001:1] ICMP PIN
83	ossecse...	Alert Level: 5; Rule: 18210
79	ossecse...	Alert Level: 3; Rule: 502 -

Cargo de Usuários

Cargo: Suporte Nível 1

Aplicar Filtro Taxa de Atualização

Vermelho - Tickets fechando prazo SLA

Edição

ID: 1

Título: Suporte Nível 1

Nível: 1

Fonte de Log: Adicionar todas fontes de log

Grupos de logs:

- Grupo deletado - OSS
- Usuario adicionado ao sistema - OSS
- Conta deletada ou desabilitada - OSS
- Detecção de ping - RB
- Conexão FTP detectada - RB
- Senha incorreta - RB

Responsável: [charles/admin] Charles V. Neu

Salvar

Estudo de Caso - Cadastro de Usuários

Central De Serviços - Usuário: Charles V. Neu (Suporte Nível 1)

Central De Serviços

Filtros

De 03/12/2018 08:09 até 10/12/2018 08:09 Prioridade 0 Mensagem Aplicar Filtro Taxa de Atualização

Legendas

Verde - Tickets abertos recentemente

ID	Host	Mensagem
86	raspber...	[1:10001:1] Possible Do...
80	raspber...	[1:1000001:1] ICMP PI...
81	raspber...	[1:1000002:1] Alert! FT...
82	ossecse...	Alert Level: 5; Rule: 571
84	ossecse...	Alert Level: 10; Rule: 55
85	raspber...	[1:1228:7] SCAN nmap...
87	raspber...	[1:10000001:1] ICMP PI...
83	ossecse...	Alert Level: 5; Rule: 182
79	ossecse...	Alert Level: 3; Rule: 502

Usuários - Usuário: Charles V. Neu

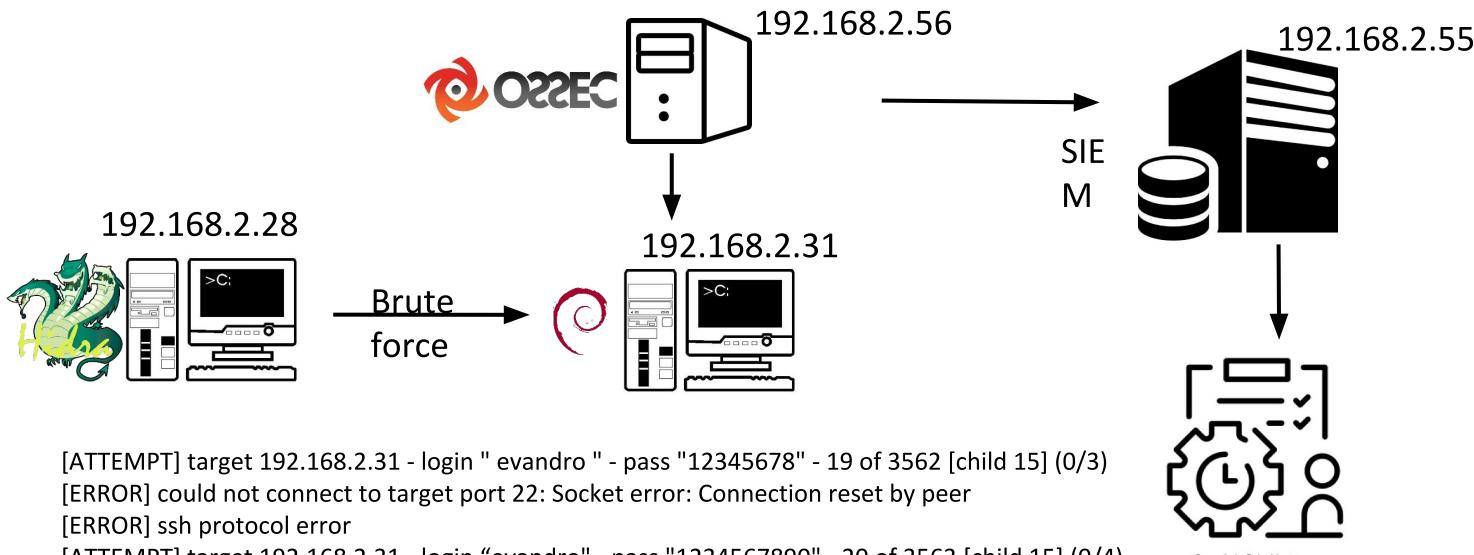
Usuários [gilson/admin] Gilson Helfer Editar Novo

Edição	ID	Nome	Senha	Permissão	Cargo	Apelido	E-mail
	21	gilson	*****	Admin	Suporte Nível 2	Gilson Helfer	g.h@mx2.unisc.br

Vermelho - Tickets fechando prazo SLA

Prioridade
a. 10 de... ALTA [12 HRs]
a. 10 de... ALTA [12 HRs]
a. 10 de... URGENTE [2 HRs]
a. 10 de... URGENTE [2 HRs]
a. 10 de... URGENTE [2 HRs]
a. 10 de... URGENTE [2 HRs]
a. 10 de... ALTA [12 HRs]
a. 10 de... BAIXA [48 HRs]
a. 10 de... BAIXA [48 HRs]

- Após finalizado os cadastros e configurações iniciais da ferramenta, já será possível detectar os incidentes e gerar os tickets.



```
[ATTEMPT] target 192.168.2.31 - login "evandro" - pass "12345678" - 19 of 3563 [child 15] (0/3)
[ERROR] could not connect to target port 22: Socket error: Connection reset by peer
[ERROR] ssh protocol error
[ATTEMPT] target 192.168.2.31 - login "evandro" - pass "1234567890" - 20 of 3563 [child 15] (0/4)
[ATTEMPT] target 192.168.2.31 - login "evandro" - pass "abc123" - 21 of 3563 [child 9] (0/4)
[ATTEMPT] target 192.168.2.31 - login "evandro" - pass "computer" - 22 of 3563 [child 0] (0/4)
[ATTEMPT] target 192.168.2.31 - login "evandro" - pass "tigger" - 23 of 3563 [child 1] (0/4)
[ATTEMPT] target 192.168.2.31 - login "evandro" - pass "1234" - 24 of 3563 [child 2] (0/4)
[ATTEMPT] target 192.168.2.31 - login "evandro" - pass "qwerty" - 25 of 3563 [child 5] (0/4)
[ATTEMPT] target 192.168.2.31 - login "evandro" - pass "money" - 26 of 3563 [child 6] (0/4)
[ATTEMPT] target 192.168.2.31 - login "evandro" - pass "carmen" - 27 of 3563 [child 10] (0/4)
[ATTEMPT] target 192.168.2.31 - login "evandro" - pass "mickey" - 28 of 3563 [child 11] (0/4)
```

Estudo de Caso - Detecção de Incidentes



CONSEG

Date: 2018-12-12 15:43:41

Host: ossecserver

Message type: Syslog

Message: **Multiple failed logins in a small period of time;** Location(**debiancliente2**) **192.168.2.31** -> /var/log/auth.log; classification: pam,syslog,authentication_failures, **srcip: 192.168.2.28**; DEC 12 15:43:41 **debianX64Cliente** sshd: pam_unix(sshd:auth): **authentication failure**; logname= uid=0 euid=0 tty=ssh ruser= rhost=**192.168.2.28**.

← LOG NO SIEM

EXPRESSÃO
CADASTRADA



Tipos	Falhas de login em um curto período	Editar	Remover
Edição			
ID	46	Cadastrar Novo	
Fonte de Log	ossecserver	Salvar	
SLA	URGENTE [2 HRs]	Salvar	
Expressão	%Multiple failed logins in a small period of time%	Salvar	
Descrição	Falhas de login em um curto período de tempo - OS	Salvar	

Estudo de Caso - Detecção de Incidentes



Central De Serviços

Filtros
De 05/12/2018 04:23 até 12/12/2018 04:23 Prioridade 0 Mensagem Aplicar Filtro Taxa de Atualização

Legendas
Verde - Tickets abertos recentemente Amarelo - Tickets abertos já a bastante tempo Vermelho - Tickets fechando prazo SLA

Tickets Abertos

ID	Host	Mensagem	Data do Log	Prioridade
109	ossecserver	Alert Level: 5; Rule: 5710 - Attempt to login using a non-existent user; Location: (d...)	quarta-feira, 12 de dezembro de 2018 15:43	URGENTE [2 HRs]
110	ossecserver	Alert Level: 10; Rule: 5551 - Multiple failed logins in a small period of time.; Locatio...	quarta-feira, 12 de dezembro de 2018 15:43	URGENTE [2 HRs]
105	ActiveDirectory	4740 A user account was locked out. Subject: Security ID:S-1-5-18 Account Name:...	quarta-feira, 12 de dezembro de 2018 13:59	URGENTE [2 HRs]
102	ossecserver	Alert Level: 8; Rule: 18112 - User account disabled or deleted.; Location: (win7clie...	terça-feira, 11 de dezembro de 2018 00:07	URGENTE [2 HRs]
97	ossecserver	Alert Level: 5; Rule: 18140 - System time changed.; Location: (win7cliente1) 192.1...	segunda-feira, 10 de dezembro de 2018 23:58	URGENTE [2 HRs]
88	raspberrypi	[1:1228:7] SCAN nmap XMAS [Classification: Attempted Information Leak] [Priority:...	segunda-feira, 10 de dezembro de 2018 23:24	URGENTE [2 HRs]
90	raspberrypi	[1:10000001:1] ICMP PING detected !! {ICMP} 192.168.2.57 -> 192.168.2.28	segunda-feira, 10 de dezembro de 2018 23:24	ALTA [12 HRs]
91	raspberrypi	[1:10000001:1] ICMP PING detected !! {ICMP} 192.168.2.57 -> 192.168.2.28	segunda-feira, 10 de dezembro de 2018 23:24	ALTA [12 HRs]
81	raspberrypi	[1:1000002:1] Alert! FTP connection! {TCP} 192.168.2.28:61742 -> 192.168.2.5...	segunda-feira, 10 de dezembro de 2018 19:50	URGENTE [2 HRs]
82	ossecserver	Alert Level: 5; Rule: 5710 - Attempt to login using a non-existent user; Location: (d...	segunda-feira, 10 de dezembro de 2018 19:50	URGENTE [2 HRs]
84	ossecserver	Alert Level: 10; Rule: 5551 - Multiple failed logins in a small period of time.; Locatio...	segunda-feira, 10 de dezembro de 2018 19:50	URGENTE [2 HRs]
85	raspberrypi	[1:1228:7] SCAN nmap XMAS [Classification: Attempted Information Leak] [Priority:...	segunda-feira, 10 de dezembro de 2018 19:50	URGENTE [2 HRs]

TICKET GERADO



Estudo de Caso - Atribuição do Ticket

Central De Serviços - Usuário: Evandro Trebien (Suporte Nível 1)

Central De Serviços

Filtros
De 03/12/2018 09:29 até 11/12/2018 09:29 Prioridade 0 Mensagem Aplicar Filtro Taxa de Atualização

Legendas
Verde - Tickets abertos recentemente Amarelo - Tickets abertos já a bastante tempo Vermelho - Tickets fechando prazo SLA

Tickets Abertos

ID	Host	Mensagem	Data do Log	Observação	Prioridade
81	raspber...	[1:1000002:1] Alert! FTP connection [TCP] 102.169.2.22:21742 - 102.169.2.5...	segunda-feira, 10 de...	FTP!	URGENTE [2 HRs]
82	ossecser...	Alert Level: 5; Rule: 5710 - Attempt to...	segunda-feira, 10 de...	(d...)	URGENTE [2 HRs]
84	ossecse...	Alert Level: 10; Rule: 5551 - Multiple...	segunda-feira, 10 de...	Locatio...	URGENTE [2 HRs]
85	raspber...	[1:1228:7] SCAN nmap XMAS [Classi...	segunda-feira, 10 de...	[Priority...]	URGENTE [2 HRs]

Alterar Observação
Capturar Ticket
Ignorar
Mostrar Mensagem

Estudo de Caso - Opções de Tratamento do Ticket



CONSEG

Meus Tickets

ID	Incidente	Mensagem	Ação	Observação Geral	Observação Recuperação	Observação Ticket
314	84	Alert Level: 10; Rule: 5551	Ver Mensagem			foi alterado a senha para
315	81	[1:1000002:1] Alerta! FTP	Escrever Observação Geral			

Opções de Ação:

- Ver Mensagem
- Escrever Observação Geral
- Encaminhar Ticket
- Escrever Observação Ticket
- Visualizar Abertos
- Visualizar Finalizados
- Finalizar Ticket
- Detalhes do Ticket

Qual o motivo?

X

Encaminhar demanda

OK

Cancelar

Nao encontrei a requisicao da conexao FTP, favor verificar

Digite o ID do usuário desejado

X

ID: 8 / Administrador do SISTEMA

(Administradores)

OK

ID: 20 / Charles V. Neu (Suporte Nivel 1)

ID: 14 / Jean Carlo (Suporte Nivel 1)

ID: 13 / Administrador ROOT (Administradores)

Cancelar

14

Estudo de Caso - Relatório

Relatório x

Este relatório é referente aos últimos 3 dias

Dia: 3/11/2018 Dia: 4/11/2018 Dia: 5/11/2018
Tempo médio: 000:00% Tempo médio: 000:85% Tempo médio: 000:96%

Status do período atual: Aumentando tempo

Principais incidentes

Tipo	Tickets	Ocorrências
Conexão FTP detectada - RB	5	169
Detecção de ping - RB	5	2294
Servidor Ossec Iniciado - OSS	4	18

Principais incidentes por fonte de log

Selecione a fonte de log:

Tipo	Tickets	Ocorrências
Conexão FTP detectada - RB	5	169
Detecção de ping - RB	5	2294
Possível ataque brute force - RB	3	255

DEMONSTRAÇÃO!

<https://www.youtube.com/watch?v=nKUX2wiNLAc&t=53s>

- Introdução
- Referencial Teórico
- Trabalhos Relacionados
- Sistema de Tratamento de Logs SIEM Seguindo ITIL
- Estudo de caso em um Ambiente Simulado (Testes)
- **Conclusão e Trabalhos Futuros**
- Referências

- Possível comprovar a eficácia na detecção de possíveis ataques
- Encontrada uma maneira de centralizar e tratar as informações contidas nos LOGS de diversas ferramentas em um único lugar

DESAFIOS	Solução proposta	Objetivo alcançado?
Como apresentar e tratar os logs gerados por diversas ferramentas de segurança e monitoramento? Como fazer com que estes logs sejam vistos pelos responsáveis?	Utilizar um SIEM para reunir essas diversas informações. Gerar TICKETS a partir destas e disponibilizar uma solução para que os usuários accessem e possam tratá-las seguindo boas práticas da ITIL.	SIM

- Estudar uma maneira de conectar as ferramentas de segurança (fontes de log) de forma automática (descoberta na rede)
- Disponibilizar a solução para outras plataformas
- Aprimorar a tela de relatórios
- Agregar esta solução a outras ferramentas como Zabbix, Nagios

- Introdução
- Referencial Teórico
- Trabalhos Relacionados
- Sistema de Tratamento de Logs SIEM Seguindo ITIL
- Estudo de caso em um Ambiente Simulado (Testes)
- Conclusão e Trabalhos Futuros
- Referências**

- CERT.BR. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. out. 2018. 2018. Disponível em: <<http://www.cert.br/>>. Acesso em: 02 abr. 2018.
- GARTNER. Top 10 Technology Trends. mai. 2018. 2018. Disponível em: <<https://www.gartner.com/en>> Acesso em: 16 mai. 2018.
- MUNI, D. P. et al. Recommending resolutions of itil services tickets using deep neuralnetwork. In: CODS. [S.l.: s.n.], 2017.
- RSYSLOG. The rocket-fast system for log processing. out. 2018. 2018. Disponível em:<<https://www.rsyslog.com/>>. Acesso em: 25 out. 2018.
- OSSEC. Open source IDS security. mai. 2018. 2018. Disponível em: <<https://www.ossec.net/>>. Acesso em: 28 mai. 2018.
- PFSENSE. pfSense - World's Most Trusted Open Source Firewall. mai. 2018. 2018. Disponível em: <<https://www.pfsense.org/>> Acesso em: 28 mai. 2018.

Agradecimentos

- CAPES/Brasil
- Instituto Nacional de Ciência e Tecnologia em Ciências Forenses - INCT Forense (grant 465450/2014-8)
- Bolsa de produtividade CNPq (grant 315192/2018-6)

