



Ferramenta de apoio a Segurança

- ✓ PALESTRANTE
- ✓ PILARES DA STI
- ✓ VISÃO SISTêmICA DA STI
- ✓ PORQUE MONITORAR A SEGURANÇA?
- ✓ ONDE O ZABBIX PODE AJUDAR?
- ✓ ZABBIX vs. RANSOWARES

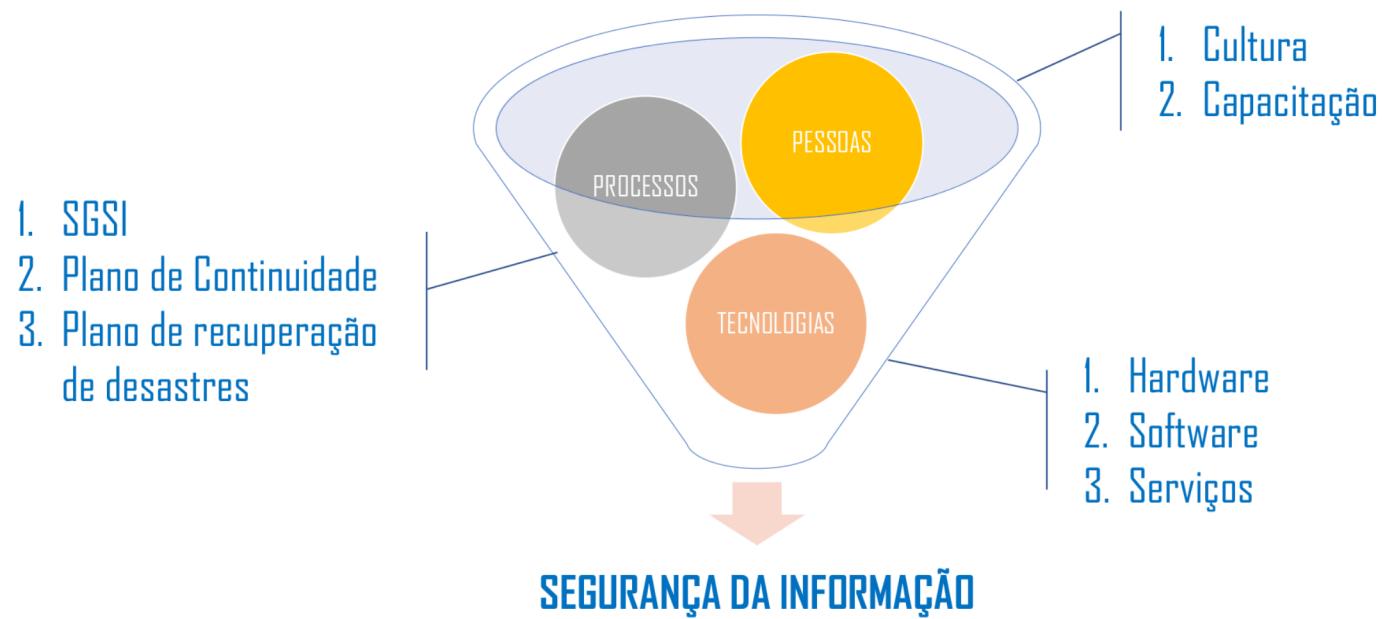
Zabbix como Ferramenta de apoio à segurança

- ✓ Graduado em Redes de Computadores – SENAI
- ✓ Especialista em Redes de Computadores e Segurança da Informação – UFG
- ✓ Agente de informática da Saneamento de Goiás – SANEAGO
- ✓ Professor Universitário no SENAI FATESG
- ✓ Analista de Sistemas – SENAC Goiás
- ✓ Sócio proprietário da NOX5 Tecnologia
- ✓ Perito Forense Computacional
- ✓ Analista de Vulnerabilidade de Sistema – Pentester

Zabbix como Ferramenta de apoio à segurança

- ✓ Disponibilidade
- ✓ Confidencialidade
- ✓ Integridade

Zabbix como Ferramenta de apoio à segurança



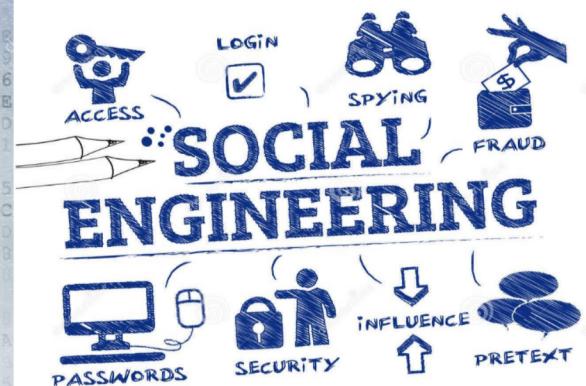
Zabbix como Ferramenta de apoio à segurança

- ✓ Há diversas soluções de segurança diferentes no mercado que fazem trabalhos complexos ou muito específicos, como controle de portas de rede, análise de conteúdo de pacotes, verificação de integridade de arquivos e dados, análise de log e outras ações de segurança.

Zabbix como Ferramenta de apoio à segurança

- ✓ Alguém abrir uma porta de comunicação por apenas 1 minuto e esquecer de fechá-la.
- ✓ Um malware chegar por e-mail e alterar os arquivos do sistema ou dar controle sobre ele a terceiros.
- ✓ O arquivo de senha for alterado quando ele deveria permanecer inalterado.
- ✓ Tentativas de logon com a senha de root for realizada por muitas vezes.
- ✓ Um gabinete de servidor foi aberto em local remoto.
- ✓ Temperatura do datacenter está subindo rapidamente.

Zabbix como Ferramenta de apoio à segurança



Zabbix como Ferramenta de apoio à segurança

- ✓ Mapear corretamente os pontos chaves a serem monitorados.
- ✓ Alinhar ações com especialista em segurança.
- ✓ Saber quando e por quanto tempo guardar esses dados, pois a cada segundo eles possuem mais informações da infra.
- ✓ Os dados coletados devem ser apresentados com visão: operacional e estratégica, pois vão conter dados sensíveis.
- ✓ O monitoramento não pode interferir no funcionamento do dispositivo monitorado
- ✓ Acesso ao frontend deve ser ainda mais controlado.

Zabbix como Ferramenta de apoio à segurança



✓ Ajuda a lidar com inúmeras questões e potenciais problemas

- Má configuração e falha humana
- Indisponibilidade de serviços e sistemas
- Acessos indevidos a informações sensíveis
- Garantir não repúdio
- Auxílio a auditoria

✓ Manutenção pró-ativa e corretiva

✓ Alerta a parte interessada sobre a sensibilidade da sua estrutura monitorada

Zabbix como Ferramenta de apoio à segurança

- ✓ Execução de comandos remotos
- ✓ Monitoramento de Logs
- ✓ Agentes ativos
- ✓ Monitoramento criptografado
- ✓ Alertar mudanças em arquivos sensíveis

Zabbix como Ferramenta de apoio à segurança



- ✓ Zabbix pode definir um comando a ser executado automaticamente sob determinada condição.
- ✓ Mecanismo eficiente para monitoração pró-ativa.
- ✓ As situações mais comuns onde se utiliza este recurso são:
 - Reiniciar automaticamente alguma aplicação (servidor web, aplicações, CRM) se ele não estiver respondendo
 - Utilizar o comando IPMI de 'reboot' para reiniciar remotamente um servidor que não responde
 - Liberar automaticamente espaço em disco (removendo arquivos antigos, limpando o /tmp)
 - Migrar uma VM para outro servidor físico dependendo do esgotamento de CPU do servidor físico atual

Zabbix como Ferramenta de apoio à segurança

EXECUÇÃO DE COMANDOS REMOTOS



ZABBIX

```
#sudo /etc/init.d/apache2 restart
```

Actions

Action Conditions Operations

Type of calculation: And/Or A and B and C and D

Conditions	LABEL	NAME
A	Maintenance status not in <i>maintenance</i>	
B	Trigger value = <i>PROBLEM</i>	
C	Application like <i>Apache</i>	
D	Trigger severity >= <i>Disaster</i>	

Zabbix como Ferramenta de apoio à segurança

✓ Métodos de notificação

- E-mail, SMS e Chat Jabber
- Telegram
- Execução de comandos
 - Comando de reinicialização de um serviço parado.



Zabbix como Ferramenta de apoio à segurança

- ✓ Os logs de diversos dispositivos e serviços podem estar centralizados em um único lugar, como por exemplo um servidor Linux com o Syslog-NG.
- ✓ O Zabbix pode ser utilizado para monitoração e análise destes arquivos de logs centralizados.
- ✓ O Zabbix avisa os usuários quando um arquivo de log contém determinados textos ou padrões de texto.
- ✓ O Zabbix identifica anomalias ou atividades estranhas em vários tipos de serviços e dispara alertas.
- ✓ Através do Zabbix é possível monitorar o EventLog do Windows

Windows Logs (1 item)		60	90	Agente Zabbix ... 17-04-2017 18:40:39	Falha no logon de uma conta...
<input type="checkbox"/>	Security Log (Audit Failure) eventlog[Security...,4625]				

Zabbix como Ferramenta de apoio à segurança

MONITORAMENTO DE LOGS



Name

Type

Key

Type of information

Update interval (in sec)

History storage period (in days)

Log time format

Zabbix como Ferramenta de apoio à segurança

- ✓ Zabbix suporta comunicação criptografada entre os seus componentes
- ✓ É opcional e configurada para cada componente (server, proxy, agent)
- ✓ É flexível. Permite por exemplo, o Proxy utilizar diferentes configurações de criptografia para se comunicar com os hosts
- ✓ Altamente recomendada para servidores com dados sensíveis
- ✓ Adicionar a criptografia não exigirá a abertura de novas portas nos firewalls
- ✓ O Zabbix pode utilizar certificados no formato PEM, assinados por uma CA.

Zabbix como Ferramenta de apoio à segurança

Servidor



Requisição: Carga do CPU

Resposta: 0.5

Agent
Passivo



Servidor



Requisição: O que quer coletar?

Resposta: Carga do CPU

Carga do CPU: 0.43
Memória disponível: 4096 MB
Disco disponível: 25GB

Agent
Ativo



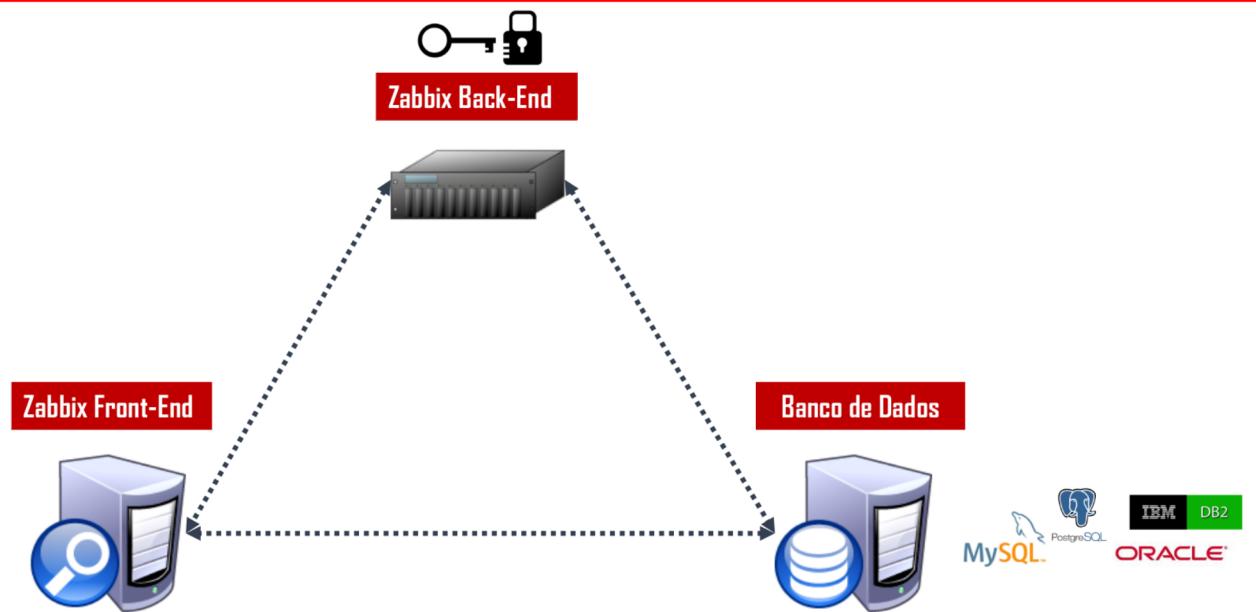
Zabbix como Ferramenta de apoio à segurança

✓ Verificar CheckSUM de arquivos

- Por exemplo, mudanças em arquivos como:
 - /etc/passwd
 - /etc/apache2/apache2.conf
 - /etc/ssh/sshd_config.
- Itens
 - LINUX - vfs.file.cksum[file]
 - WINDOWS - vfs.file.md5sum[file]



Zabbix como Ferramenta de apoio à segurança



Zabbix como Ferramenta de apoio à segurança



Zabbix como Ferramenta de apoio à segurança

Ransomware e os Números

 **U\$30M**

Final de 2014

 **U\$203M**

Final de 2015

 **U\$1B**

Final de 2016

Zabbix como Ferramenta de apoio à segurança

- ✓ Monitorar se servidores Windows estão com o Windows Update ativo e se as atualizações estão em dia.
 - <https://github.com/DavidWGilmore/zabbix/tree/master/templates/Windows-Updates>
- ✓ Monitorar se há tentativas de acesso a IP's e url's relacionadas ao Wanna Cry
 - 213.61.66.116 - 171.25.193.9 - 163.172.35.247 - 128.31.0.39 - 185.97.32.18, 178.62.173.203, 136.243.176.148
- ✓ Disparar alertas ao encontrar hosts com o serviço de Firewall parado
- ✓ Monitorar se há tentativas de conexão na porta 445 provenientes de redes externas.

Zabbix como Ferramenta de apoio à segurança

- ✓ Monitorar log de firewall em busca do padrão
`http://iuqerfsodp9ifap0sdfjhgosurijfaewrwegwea.com`
- ✓ Alertar caso haja conexões estabelecidas nas portas 9003, 9101 e 9001 no firewall.
 - `net.tcp.service[service,<ip>,<port>]`
- ✓ Disparar alertas casos os processos tasksche.exe, taskhsvc.exe, wannacry.exe, tor.exe e taskdl.exe
 - `{HOSTNAME:proc_info[processo.exe,wkset,min].last(#!)}<1`
- ✓ Monitorar hosts que tem o serviço mssecsvc2.0 com status ativado

Zabbix como Ferramenta de apoio à segurança

✓ O ZABBIX fornece um bom apoio às atividades de segurança da informação das instituições, contudo, precisa ser configurado em parceria com a equipe de segurança, e de forma alguma deve substituir ferramentas específicas para esta atividade.

Zabbix como Ferramenta de apoio à segurança

PERGUNTAS??



[f](#) [t](#) [e](#) [i](#) [y](#) /vitorluigi
vitorluigi@gmail.com

Zabbix como Ferramenta de apoio à segurança