

Roteiro 2 - Plataforma de Segurança

Integrantes: Antonio Amaral, Ariel Leventhal, Enricco Gemha

Perguntas

1. O que é e quais são as características de um SIEM?

O gerenciamento de informações e eventos de segurança, ou SIEM, é uma solução de segurança que ajuda as organizações a reconhecer e abordar possíveis ameaças e vulnerabilidades de segurança antes que elas tenham a chance de interromper as operações comerciais. SIEMs podem ser instalados on-premise (na própria infraestrutura da empresa) ou na nuvem.

Algumas características de um SIEM são:

- Coleta de dados: Recebe logs de dispositivos, aplicativos, sistemas e outras fontes de segurança.
- Normalização: Padroniza os dados coletados para facilitar a análise.
- Armazenamento: Armazena os dados coletados para análise histórica e forense.
- Análise: Identifica e correlaciona eventos de segurança para detectar ameaças.
- Alerta: Notifica sobre eventos de segurança que podem ser potenciais ameaças.
- Investigação: Fornece ferramentas para investigar e responder a incidentes de segurança.
- Relatórios: Gera relatórios sobre a atividade de segurança da organização.

2. Em que situações o grupo instalaria um SIEM?

Existem algumas razões pelas quais poderia-se instalar um SIEM como, por exemplo, atender a regulamentações ou questões de compliance internos, ou talvez melhorar o tempo de resposta a incidentes, para assegurar um uptime "ótimo" da aplicação. Também existe a possibilidade de ser instalado para ter uma visão unificada dos eventos ocorrendo simultaneamente nos sistemas de segurança da empresa, ajudando a detectar ameaças de forma mais eficaz.

3. Qual a diferença de um SIEM para um Gerenciador de LOG (SYSLOG)?

O Gerenciador de LOG (SYSLOG) realiza a coleta dos logs e fornece ferramentas para pesquisa e análise deles, porém não tem a capacidade de correlacionar eventos para detectar ameaças. Ou seja, ele é uma forma sofisticada de centralizar os logs de vários sistemas diferentes.

Por outro lado, o SIEM possui as mesmas funcionalidades que um gerenciador de log, mas não se limita somente a elas, já que ele obtém informações também de outros serviços, como software antivírus, sistemas de detecção de intrusão e bancos de dados. Ele também é capaz de correlacionar eventos de segurança para detectar ameaças, provendo ferramentas de resposta a incidentes de segurança.

4. O que é o OSSEC?

OSSEC (Sistema de Detecção de Intrusão baseado em Host de código aberto) é uma plataforma de código aberto completa para monitorar e controlar uma ou múltiplos sistemas. Ele combina todos os aspectos de HIDS (detecção de intrusão baseada em host), monitoramento de log e SIEM em uma solução só. Ele

performa, por exemplo, análise de logs, checagem de integridade de arquivos, monitoramento de policies, detecção de rootkit, alertas em tempo real e resposta a incidentes.

5. Qual a função do Kibana no Wazuh?

Kibana faz parte da ELK Stack (Elasticsearch, Logstash e Kibana), a qual pode ser facilmente integrada com o Wazuh para armazenamento, análise e visualização de dados de segurança. Isso permite criar dashboards personalizados e executar análises avançadas sobre os eventos de segurança coletados pelo Wazuh.

Configurando a infraestrutura

Considerações extras

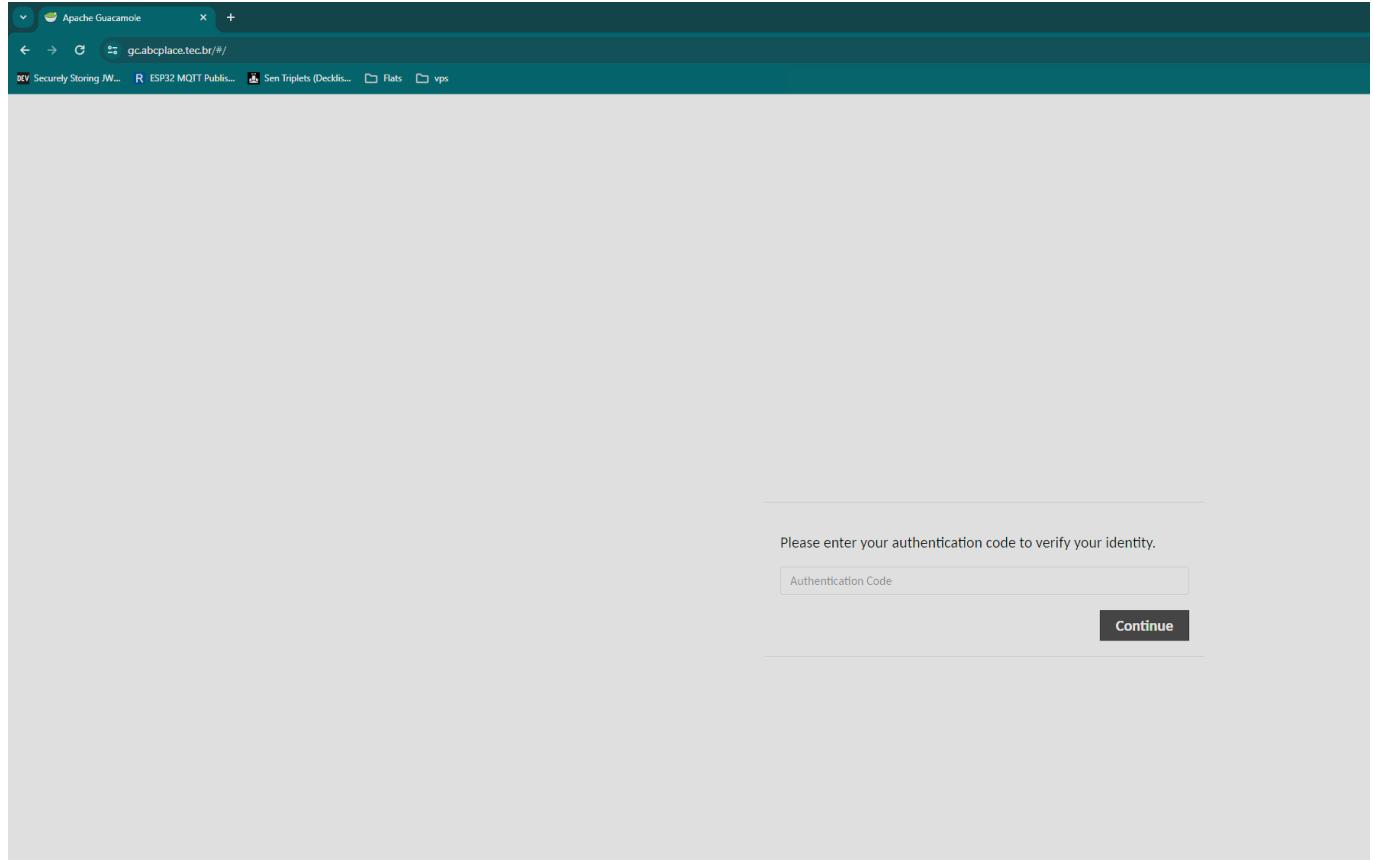
Durante uma atividade recente, foi identificado a necessidade de atualizar a máquina do Guacamole para uma instância t2.large. Essa atualização oferece recursos computacionais e memória RAM adicionais em comparação com a configuração anterior. Após discussão e aprovação do Professor Rodolfo Avelino, foram realizadas a mudança de instância. A decisão foi motivada pelo fato de que as instâncias t2.micro e t2.medium não estavam suportando o acesso SSH de todos os membros do grupo por meio do Guacamole.

Anteriormente, era enfrentado problemas nos quais a instância do Guacamole alcançava 100% de utilização de CPU, resultando em travamentos.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 IP	Elastic IP	IPv6 IPs	Monitoring	Security group
cp1-t2-large	i-0eb69e6e96f06651	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a	ec2-52-71-75-150.com...	52.71.75.150	-	-	disabled	cp1-mySQL
cp1-t2-medium	i-04612ab016a6388b	Running	t2.medium	2/2 checks passed	View alarms +	us-east-1a	ec2-52-237-2-107.com...	54.237.2.107	54.237.2.107	-	disabled	cp1-guacan...
cp1-t2-micro	i-042fc9625cc7ec1bc	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a	ec2-54-237-2-107.com...	54.237.2.107	54.237.2.107	-	disabled	cp1-wp-sg
cp1-wazuh-t2-micro	i-01feb682bbfcfa2e4	Running	t2.medium	2/2 checks passed	View alarms +	us-east-1a	ec2-54-204-25-105.co...	54.204.25.105	54.204.25.105	-	disabled	cp1-wazuh-t2-micro

Configuração Guacamole

O guacamole foi configurado com necessidade de autenticação de dois fatores através de TOTP:



As conexões com as instâncias foram separadas em dois grupos:

The screenshot shows the Apache Guacamole interface for managing connections. At the top, there's a header bar with a logo, a title 'Apache Guacamole', and a search bar containing the URL 'gc.abcplace.tec.br/#/settings/mysql/connections'. Below the header are several tabs: 'DEV Securely Storing JW...', 'R ESP32 MQTT Publis...', 'Sen Triplets (Decklis...)', 'Flats', and 'vps'. The main area is titled 'SETTINGS' and has a sub-navigation bar with tabs: 'Active Sessions', 'History', 'Users', 'Groups', 'Connections' (which is highlighted), and 'Preferences'. A message below the tabs says, 'Click or tap on a connection below to manage that connection. Depending on your access level, you may be able to edit or delete it.' There are two buttons at the top left: 'New Connection' and 'New Group'. To the right is a 'Filter' input field. The main content area displays a hierarchical tree of connections and groups. The 'admin' group is expanded, showing 'guac' and 'wazuh' connections. The 'dev' group is also expanded, showing 'mysql' and 'wordpress' connections. Both 'mysql' and 'dev' are highlighted with a light green background. There are also 'New Connection' and 'New Group' options under each group.

Também foram criados dois grupos de usuários:

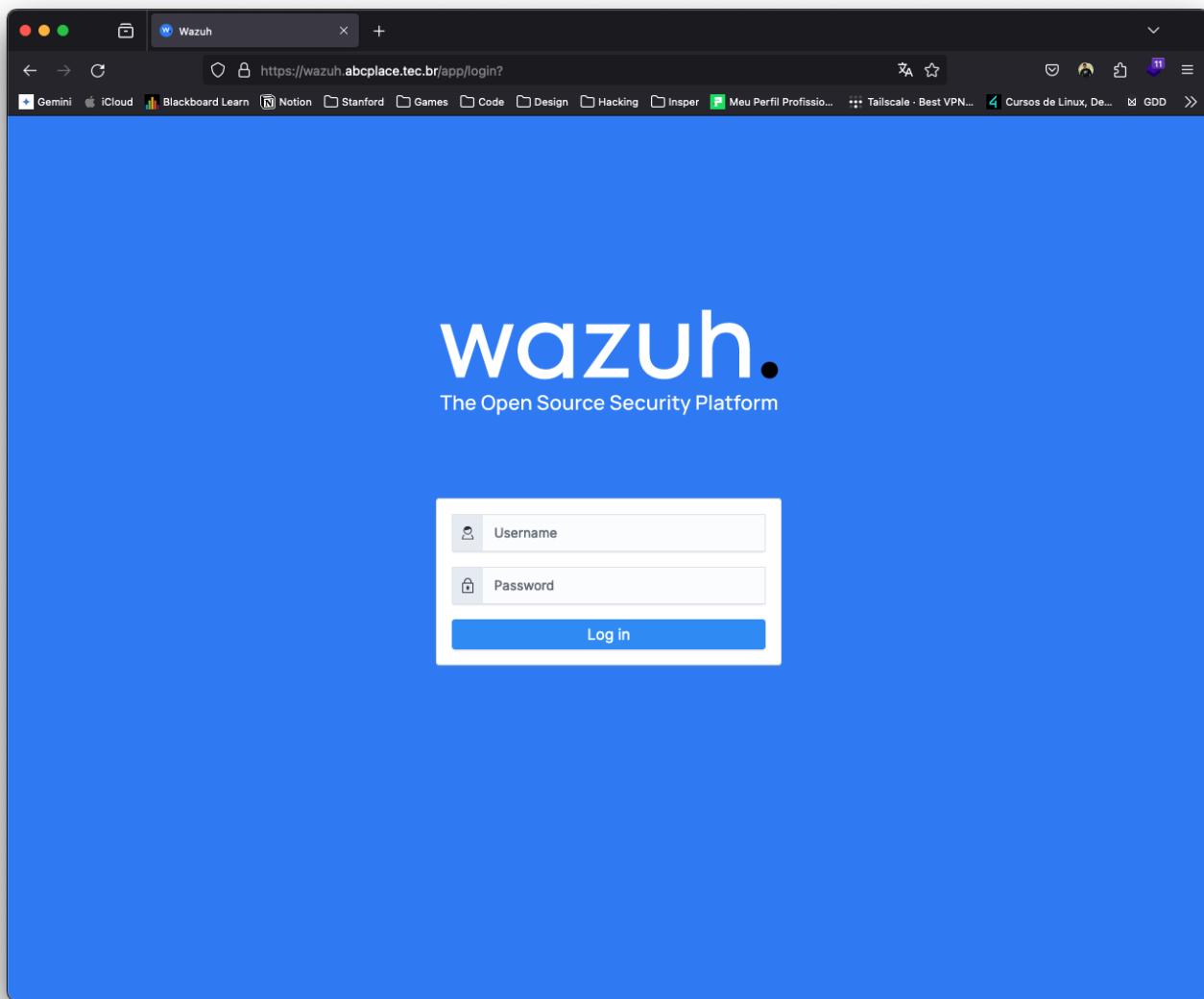
The screenshot shows the Apache Guacamole interface for managing user groups. At the top, there's a header bar with a logo, a title 'Apache Guacamole', and a search bar containing the URL 'gc.abcplace.tec.br/#/settings/userGroups'. Below the header are several tabs: 'DEV Securely Storing JW...', 'R ESP32 MQTT Publis...', 'Sen Triplets (Decklis...)', 'Flats', and 'vps'. The main area is titled 'SETTINGS' and has a sub-navigation bar with tabs: 'Active Sessions', 'History', 'Users', 'Groups' (which is highlighted), 'Connections', and 'Preferences'. A message below the tabs says, 'Click or tap on a group below to manage that group. Depending on your access level, groups can be added and deleted, and their member users and groups can be changed.' There are two buttons at the top left: 'New Group' and 'Filter'. To the right is a 'Group Name' dropdown menu. The main content area displays a list of user groups. The 'admin' group is listed first, followed by the 'dev' group.

Entao os usuários e grupos de conexões foram adicionados aos grupos de usuários:

The screenshot shows the Apache Guacamole 'Edit Group' interface for the 'dev' group. The page has a header with tabs like 'Securely Storing JW...', 'ESP32 MQTT Public...', 'Sen Triplets (Deckis...)', 'Flats', and 'vps'. The main content area is titled 'EDIT GROUP' and shows the 'Group name:' field set to 'dev'. It includes sections for 'GROUP RESTRICTIONS' (with 'Disabled:' checkbox), 'PERMISSIONS' (checkboxes for various system operations), 'PARENT GROUPS' (empty), 'MEMBER GROUPS' (empty), 'MEMBER USERS' (list of users: antonioaem, ariel, enriccog, guacadmin), and 'CONNECTIONS' (list of connections: dev, mysql, wordpress). At the bottom are 'Save', 'Clone', 'Cancel', and 'Delete' buttons.

Subindo o serviço Wazuh

Conforme solicitado no roteiro, configurou-se o serviço Wazuh em um instância EC2 da AWS, com um Elastic IP associado. Por sua vez, com posse deste IP, criou-se o subdomínio para o Wazuh, wazuh.abcplace.tec.br, que possui certificado SSL para garantir seu acesso via HTTPS. Para a instalação do Wazuh seguiu-se a documentação disponível no [site oficial](#).



Configurando os agents Wazuh

Para se obter os dados que alimentam o Wazuh, instalou-se agentes em todas as instâncias desejadas, utilizando o seguinte comando:

```
 wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-
agent_4.7.3-1_amd64.deb && sudo WAZUH_MANAGER='192.0.0.1' dpkg -i ./wazuh-
agent_4.7.3-1_amd64.deb
```

Realizando as modificações necessárias para ajustar o IP do Wazuh Manager, substituindo o IP por **172.31.0.142**. Após a instalação dos pacotes necessários, foi necessário reiniciar o serviço do agente Wazuh.

```
 sudo systemctl daemon-reload
 sudo systemctl enable wazuh-agent
 sudo systemctl start wazuh-agent
```

Este processo foi realizado em todas as instâncias. Para garantir o funcionamento, foram utilizados os seguintes comandos para acesso do ossec e visualização de logs:

```
sudo nano /var/ossec/etc/ossec.conf
```````bash
sudo tail -f /var/ossec/logs/ossec.log
```

Utilizando o dashboard do Wazuh é pode-se visualizar todos os agentes, ou seja, WordPress-BF-Agent, MySQL-BF-Agent e JMP-BF-Agent, sendo BF uma abreviação para Brute Forcing.

The screenshot shows the Wazuh dashboard with the following details:

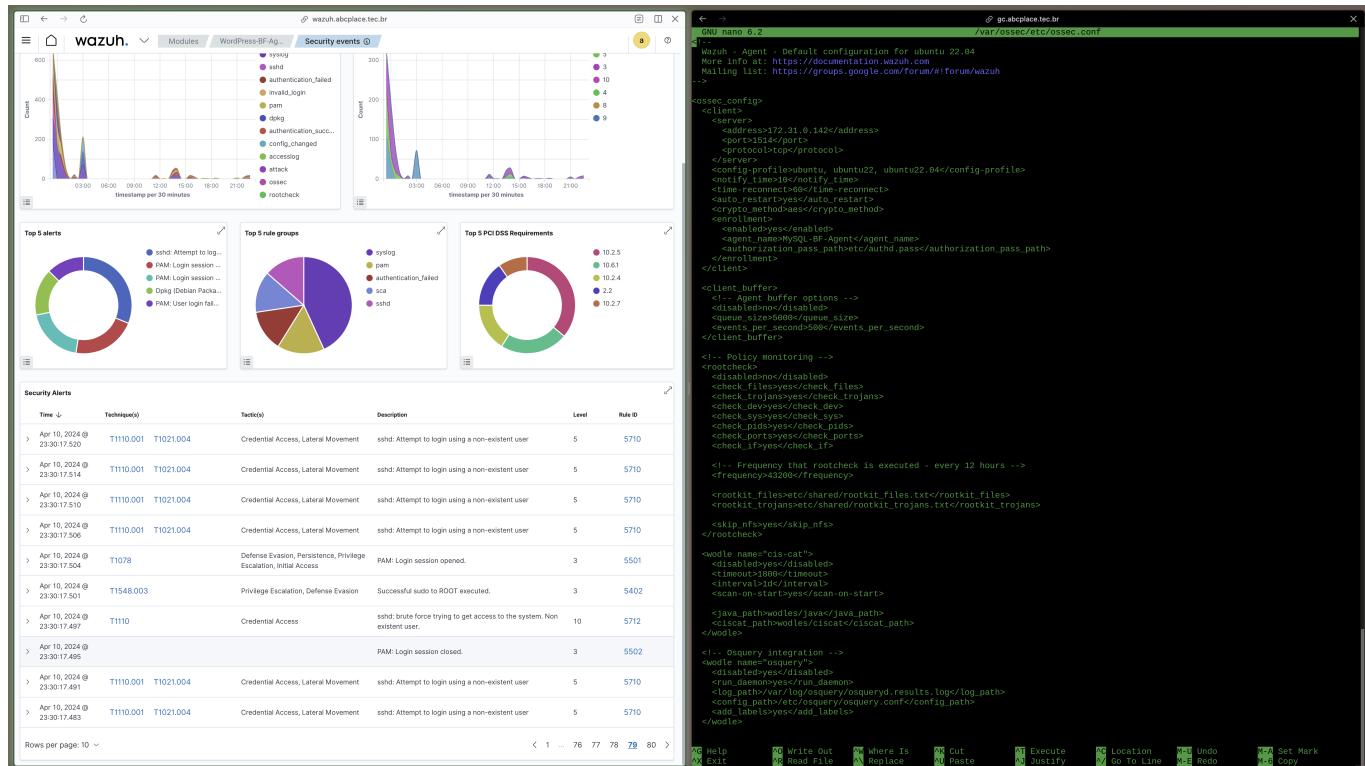
- Agents Status:** Active (3), Disconnected (0), Pending (0), Never connected (0).
- Details:** Last registered agent: JMP-BF-Agent, Most active agent: WordPress-BF-Agent.
- Evolution Graph:** A bar chart showing the count of events over the last 24 hours, with a peak at 21:00.
- Agents Table:**

ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	WordPress-BF-Agent	172.31.0.188	default	Ubuntu 22.04.4 LTS	node01	v4.7.3	● active	⋮ ⚙️
002	MySQL-BF-Agent	172.31.0.41	default	Ubuntu 22.04.4 LTS	node01	v4.7.3	● active	⋮ ⚙️
003	JMP-BF-Agent	172.31.0.147	default	Ubuntu 22.04.3 LTS	node01	v4.7.3	● active	⋮ ⚙️
- Code View:** A terminal window showing the configuration file for the MySQL-BF-Agent on an Ubuntu 22.04 host. The configuration includes sections for ossec, client, server, config-profile, and rootcheck.

## Capturando ocorrências de Brute Forcing SSH

O próximo passo tomado foi configurar o Wazuh para detectar tentativas de brute forcing ssh nos servidores da aplicação ABC Place.

Após completar a configuração, o Wazuh capturou uma ocorrência no dia 10 de abril de 2024 às 23:30:17.497, do tipo brute forcing através de SSH, sem uso de um usuário existente.



## Gerenciando o acesso às instâncias (SGs)

Todas as instâncias EC2 estão configuradas com um Security Group exclusivo e associado a elas. Nele, foi bloqueado qualquer acesso de rede externa a da VPC que não seja nas portas 80, 443, para os serviços que a necessitam, como WordPress, Guacamole e Wazuh.

The screenshot shows the AWS CloudWatch Metrics interface. A modal window is open, titled "Inbound security group rules successfully modified on security group (sg-064d9f920f0f25b | csp1-wazuh-sg) Details". It displays a table of security group rules:

Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbound rules count
csp1-guacamole-sg	sg-004fb8adefc1cad	csp1-guacamole-sg	voc-0369597b553af8bcf	Controls in-flow inside Guacamole EC2	888157825131	4 Permission entries
csp1-wp-sg	sg-0f43d5025a7f463c1	csp1-wp-sg	voc-0369597b553af8bcf	Controls in-flow in WP instance	888157825131	3 Permission entries
csp1-ec2-sg	sg-024a929a0f0e830f	csp1-ec2-sg	voc-0369597b553af8bcf	Security group for EC2	888157825131	8 Permission entries
csp1-vpc-default	sg-0d39f2ac291a9513	default	voc-0369597b553af8bcf	default VPC security group	888157825131	1 Permission entry
csp1-mysql-sg	sg-0620086475bafe672	csp1-mysql-sg	voc-0369597b553af8bcf	Controls in-flow to MySQL instance	888157825131	2 Permission entries
csp1-wazuh-sg	sg-064d9f920f0f25b	csp1-wazuh-sg	voc-0369597b553af8bcf	Controls in-flow in Wazuh instance	888157825131	6 Permission entries

- Instância MySQL: não possui acesso externo à VPC, e pode somente ser acessado internamente pela porta 3306.

**Instances (1/4) info**

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Elastic IP	IPv6 IPs	Monitoring	Security group
csp1-ec2-mysql	i-0eb69e6e96f06651	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a	-	-	-	disabled	csp1-mysql-t
csp1-ec2-guac...	i-04617ab16a16a388b	Running	t2.large	2/2 checks passed	View alarms +	us-east-1a	ec2-52-71-75-150.com...	\$2.71.75.150	\$2.71.75.150	disabled	csp1-guacam
csp1-ec2-wp	i-042fc9625cc7ec1bc	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a	ec2-54-257-2-107.com...	54.237.2.107	54.237.2.107	disabled	csp1-wp-sg
csp1-ec2-wazuh	i-01fe6828bfcc5a2ed	Running	t2.medium	2/2 checks passed	View alarms +	us-east-1a	ec2-54-204-25-105.co...	54.204.25.105	54.204.25.105	disabled	csp1-wazuh

**Instance: i-0eb69e6e96f06651 (csp1-ec2-mysql)**

**Details** **Status and alarms** **New** **Monitoring** **Security** **Networking** **Storage** **Tags**

**Security details**

IAM Role	Owner ID	Launch time
csp1-ec2-role	888137825131	Thu Apr 11 2024 14:11:33 GMT-0300 (Brasília Standard Time)

**Inbound rules**

Name	Security group rule ID	Port range	Protocol	Source	Security groups	Description
-	sgr-0ccb8c5e06a2fa49	3306	TCP	0.0.0.0/0	csp1-mysql-sg	-
-	sgr-05f48160e715f0090	22	TCP	172.31.0.0/16	csp1-mysql-sg	-

**Outbound rules**

Name	Security group rule ID	Port range	Protocol	Destination	Security groups	Description
-	sgr-0414ac1e8a2fd732c	All	All	0.0.0.0/0	csp1-mysql-sg	-

- Instância WordPress: O acesso às portas 80 e 443 estão liberados ao público, e a porta 22 está liberada somente para acesso de SSH privado, bloco CIDR da rede interna (172.31.0.0/16), utilizado pelo serviço Guacamole.

**Instances (1/4) info**

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Elastic IP	IPv6 IPs	Monitoring	Security group
csp1-ec2-mysql	i-0eb69e6e96f06651	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a	-	-	-	disabled	csp1-mysql-t
csp1-ec2-guac...	i-04617ab16a16a388b	Running	t2.large	2/2 checks passed	View alarms +	us-east-1a	ec2-52-71-75-150.com...	\$2.71.75.150	\$2.71.75.150	disabled	csp1-guacam
csp1-ec2-wp	i-042fc9625cc7ec1bc	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1a	ec2-54-237-2-107.com...	54.237.2.107	54.237.2.107	disabled	csp1-wp-sg
csp1-ec2-wazuh	i-01fe6828bfcc5a2ed	Running	t2.medium	2/2 checks passed	View alarms +	us-east-1a	ec2-54-204-25-105.co...	54.204.25.105	54.204.25.105	disabled	csp1-wazuh

**Instance: i-042fc9625cc7ec1bc (csp1-ec2-wp)**

**Details** **Status and alarms** **New** **Monitoring** **Security** **Networking** **Storage** **Tags**

**Security details**

IAM Role	Owner ID	Launch time
csp1-ec2-role	888137825131	Thu Apr 11 2024 14:11:33 GMT-0300 (Brasília Standard Time)

**Inbound rules**

Name	Security group rule ID	Port range	Protocol	Source	Security groups	Description
-	sgr-0270deb53f2359704	445	TCP	0.0.0.0/0	csp1-wp-sg	-
-	sgr-0247a0ccc4d13724b	80	TCP	0.0.0.0/0	csp1-wp-sg	-
-	sgr-0627808350cc2d3c0	22	TCP	172.31.0.0/16	csp1-wp-sg	-

**Outbound rules**

Name	Security group rule ID	Port range	Protocol	Destination	Security groups	Description
-	sgr-0779e16425f5fd5a8	All	All	0.0.0.0/0	csp1-wp-sg	-

- Instância Guacamole: Possui acesso liberado nas portas 80, 443, respectivamente, HTTP e HTTPS, e conexão SSH via porta 22, porém este somente para o bloco CIDR da rede interna (172.31.0.0/16).

The screenshot shows the AWS CloudWatch Metrics Insights interface. A search bar at the top contains the query: `CloudWatch Metrics Insights`. The results table below has one row, which is highlighted in blue. The row details the usage of CloudWatch Metrics Insights, showing a count of 1, a duration of 0 days, and a timestamp of `2024-04-11T16:46:47Z`.

CloudWatch Metrics Insights
1

Below the table, there is a section titled "Metrics Insights usage" with a table showing the number of metrics and events processed by CloudWatch Metrics Insights.

CloudWatch Metrics Insights	1
Metrics processed	0
Events processed	0

At the bottom of the page, there is a "Feedback" button.

- Instância Wazuh: Libera-se o acesso público via HTTP (80) e HTTPS (443), bem como libera-se o acesso interno para as conexões com os agentes instalados nas outras instâncias, porém este somente para o bloco CIDR da rede interna (172.31.0.0/16), através das portas 1514 e 1515, utilizadas pelo Wazuh. Por fim, liberou-se o acesso SSH (22) para instâncias dentro da VPC, utilizado pelo serviço Guacamole.

## Envio de alertas por e-mail

De acordo com o roteiro o próximo passo é a configuração de alertas via email. Para isso há a necessidade de se configurar um servidor SMTP Host para envio de e-mails. Para simplificar foi utilizado o serviço de SMTP da A2C Solutions, Software House dos integrantes Antônio Martins e Ariel Leventhal.

The screenshot shows the cPanel interface for managing email accounts. The left sidebar contains various tools and services. The main area is titled 'List Email Accounts' and displays a table of four email accounts. The columns include 'conta @ Domínio', 'Restrictions', and 'Storage: Usado / Allocated / %'. The accounts listed are:

conta @ Domínio	Restrictions	Storage: Usado / Allocated / %
acsoluti [Sistema]	Irrestrito	0 de bytes / ∞
contato@a2csolutions.com.br	Irrestrito	57,12 KB / ∞
cybersec@a2csolutions.com....	Irrestrito	102,48 KB / 250 MB / 0,04%
devtest@a2csolutions.com.br	Irrestrito	69,74 KB / 250 MB / 0,03%

Each account row includes 'Check Email', 'Gerenciar' (Manage), and 'Connect Devices' buttons. A 'Buy More' button is visible at the top right. The bottom of the page shows the cPanel logo and version (118.0.4) along with links to 'Início', 'Marcas comerciais', 'Privacy Policy', 'Documentação', and 'Give Feedback'.

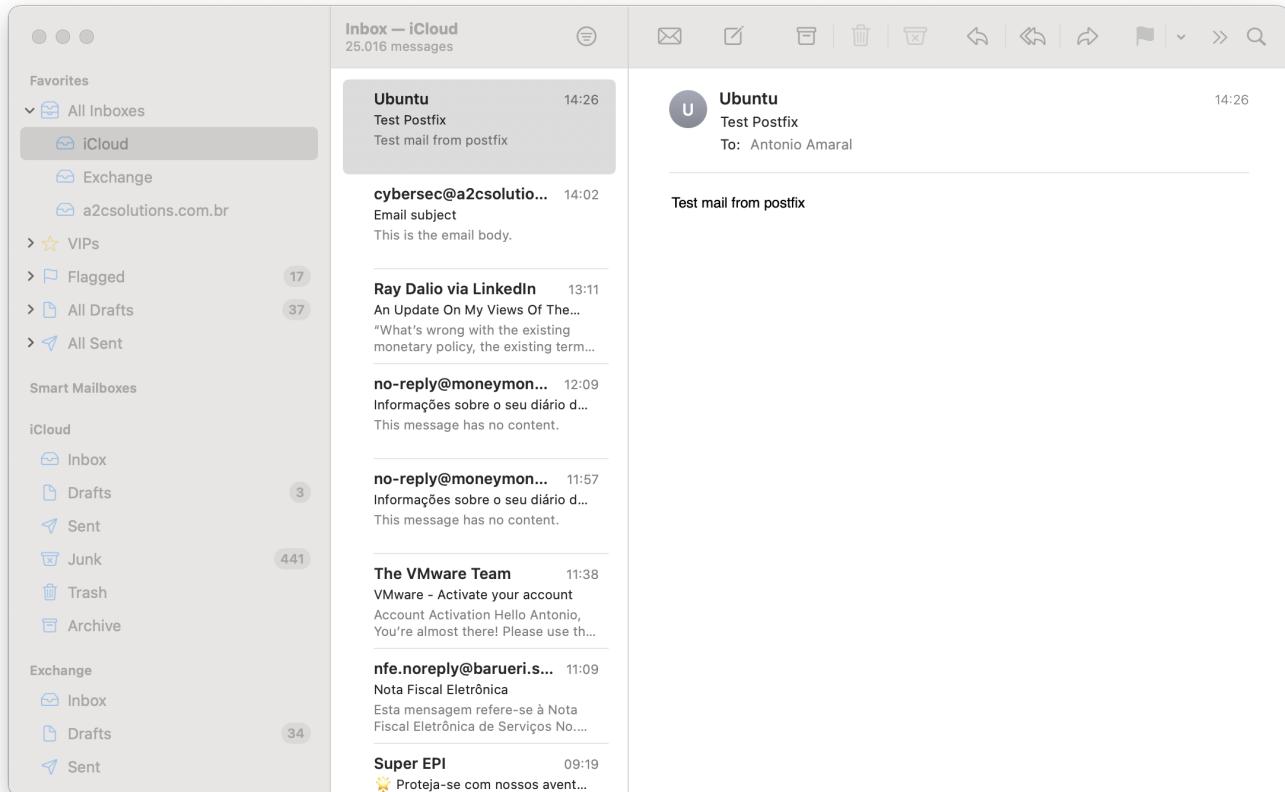
Sendo assim o email utilizado para este roteiro é o [cybersec@a2csolutions.com.br](mailto:cybersec@a2csolutions.com.br).

No restante foi utilizada a documentação do Wazuh para realizar a instalação do postfix, que possibilitou o uso do servidor SMTP [mail.a2csolutions.com.br](mailto:mail.a2csolutions.com.br) uma vez que o serviço necessita de autenticação.

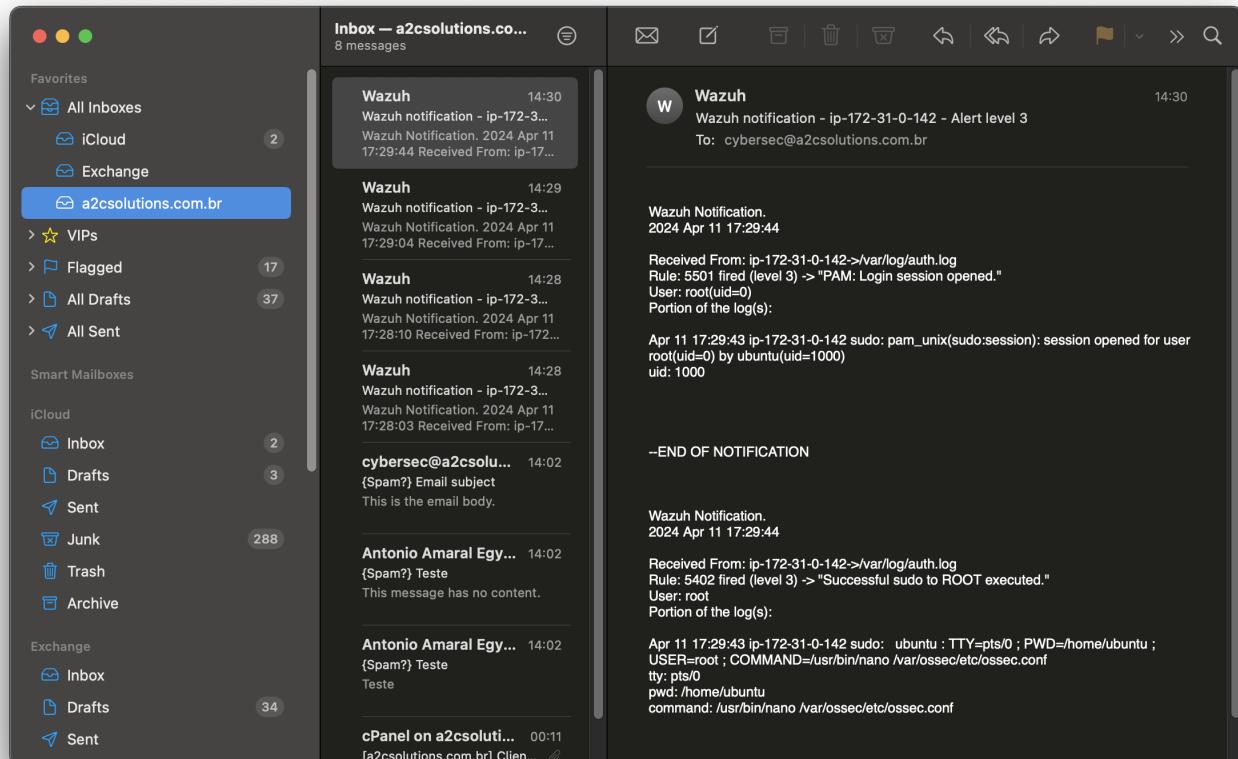
Configurou-se também o envio de alertas por e-mail, via SMTP, utilizando o comando a seguir:

```
echo "This is the email body." | mail -s "Email subject" -a "From: cybersec@a2csolutions.com.br" antonioaem@icloud.com
```

Obtendo-se o seguinte e-mail:



Com isso, o Wazuh foi configurado para enviar e-mails com alertas de nível 2, como uma forma prática de testar se o funcionamento. Sendo assim, seriam enviados alertas básicos de login e autenticação para ser possível testar o envio via Wazuh.



Vale ressaltar que atualmente, ele se encontra configurado para alertas de nível 12.

## Configurando os logs de CloudWatch

Quanto aos logs de CloudWatch, teoricamente consegui-se configurá-los, e conseguiu-se estabelecer a autenticação com o bucket S3 e, por conseguinte, as boas práticas de IAM, que consistem na criação de um usuário de serviço exclusivo para o Wazuh. Isso é evidenciado na imagem abaixo:



```

root@gc.abcpplace.tec.br: /var/ossec/etc/ossec.conf
GNU nano 6.2
</rootcheck>

<wodle name="cis-cat">
 <disabled>yes</disabled>
 <timeout>1800</timeout>
 <interval>1d</interval>
 <scan-on-start>yes</scan-on-start>
</wodle>

<!-- Osquery integration -->
<wodle name="osquery">
 <disabled>yes</disabled>
 <run_daemon>yes</run_daemon>
 <log_path>/var/log/osquery/osqueryd.results.log</log_path>
 <config_path>/etc/osquery/osquery.conf</config_path>
 <add_labels>yes</add_labels>
</wodle>

<!-- System inventory -->
<wodle name="syscollector">
 <disabled>no</disabled>
 <interval>1h</interval>
 <scan_on_start>yes</scan_on_start>
 <hardware>yes</hardware>
 <os>yes</os>
 <network>yes</network>
 <packages>yes</packages>
 <ports all="no">yes</ports>
 <processes>yes</processes>

<!-- Database synchronization settings -->
<synchronization>
 <max_eps>10</max_eps>
</synchronization>
</wodle>

<wodle name="aws-s3">
 <disabled>no</disabled>
 <interval>5m</interval>
 <run_on_start>yes</run_on_start>
 <bucket type="cloudtrail">
 <name>cybersec-wazuh-cloudwatch-p2</name>
 <access_key>AKIA4SSJDXNV3IDANPNA4</access_key>
 <secret_key>j84gMDEJTHM8RNJ+hak5ZQe03PMoufNc/29Ff0Gs</secret_key>
 </bucket>
 <service type="cloudwatchlogs">
 <aws_profile>Wazuh-Service</aws_profile>
 <aws_log_groups>cybersec-p2</aws_log_groups>
 <regions>us-east-1</regions>
 </service>
</wodle>

<sca>
 <enabled>yes</enabled>
 <scan_on_start>yes</scan_on_start>
 <interval>12h</interval>
 <skip_nfs>yes</skip_nfs>
</sca>

```

The terminal window shows the configuration file for OSSEC-HIDS. The file is named 'ossec.conf' and is located at '/var/ossec/etc/ossec.conf'. The configuration includes sections for 'cis-cat', 'osquery', 'syscollector', 'aws-s3', and 'scache'. It specifies various parameters like intervals, paths, and AWS credentials. The terminal interface includes standard nano keybindings and a menu bar.

Contudo não conseguiu-se descobrir uma forma eficaz de testar o gerenciamento e posterior tratamento dos logs capturados. Pretendemos realizar tal tarefa no próximo roteiro.

## Fontes

- [IBM](#)
- [NewRelic](#)
- [SolarWinds](#)
- [OSSEC-Hids](#)
- [Wazuh](#)

- [Wazuh Documentação](#)