Phát hiện các lần đăng nhập không thành công:

Quy tắc này được sử dụng để phát hiện các lần đăng nhập không thành công và tạo cảnh báo khi vượt quá ngưỡng. Sau đây là ví dụ về quy tắc Wazuh để phát hiện các lần đăng nhập không thành công:

<rule id="100000" level="7" group="authentication,syslog" frequency="5" timeframe="30">

<description>Failed login attempts</description>

<match>

<login\_failed/>

</match>

<options>

<threshold>5</threshold>

<full\_log>yes</full\_log>

</options>

<action>

<email>

<to>security-team@example.com</to>

<subject>Failed login attempts detected on server X</subject>

<message>Failed login attempts detected on server X. Check the logs for more information.</message>

</email>

</action>

</rule>

Phát hiện truy cập trái phép:

Quy tắc này được sử dụng để phát hiện truy cập trái phép vào hệ thống và tạo cảnh báo khi điều kiện được đáp ứng. Sau đây là ví dụ về quy tắc Wazuh để phát hiện truy cập trái phép:

<rule id="100001" level="10" group="access\_control,syslog" frequency="1">

<description>Unauthorized access</description>

<match>

<access\_control>Denied</access\_control>

<username>!root</username>

<program>!sudo</program>

</match>

<action>

<syscheck>

<frequency>1</frequency>

<command>find /home -type f -exec chmod 600 {} \;</command>

</syscheck>

<email>

<to>security-team@example.com</to>

<subject>Unauthorized access detected on server X</subject>

<message>Unauthorized access detected on server X. Check the logs for more information.</message>

</email>

</action>

</rule>

Phát hiện hoạt động mạng độc hại:

Quy tắc này được sử dụng để phát hiện hoạt động mạng độc hại và tạo cảnh báo khi điều kiện được đáp ứng. Sau đây là ví dụ về quy tắc Wazuh để phát hiện hoạt động mạng độc hại:

<rule id="100002" level="12" group="network,syslog" frequency="1">

<description>Malicious network activity</description>

<match>

<srcip>192.168.0.0/16</srcip>

<dstip>!192.168.1.1</dstip>

<dstport>22</dstport>

</match>

<action>

<syscheck>

<frequency>1</frequency>

<command>find /var/log -type f -name "auth.log" -exec grep "Failed password" {} \;</command>

</syscheck>

<email>

<to>security-team@example.com</to>

<subject>Malicious network activity detected on server X</subject>

<message>Malicious network activity detected on server X. Check the logs for more information.</message>

</email>

</action>

</rule>

Phát hiện các sửa đổi tệp đáng ngờ:

Quy tắc này được sử dụng để phát hiện các sửa đổi tệp đáng ngờ và tạo cảnh báo khi điều kiện được đáp ứng. Sau đây là ví dụ về quy tắc Wazuh để phát hiện các sửa đổi tệp đáng ngờ:

<rule id="100003" level="8" group="file\_integrity,syslog" frequency="1">

<description>Suspicious file modification</description>

<match>

<filename>/etc/passwd</filename>

<checksum\_changed/>

</match>

<action>

<syscheck>

<frequency>1</frequency>

<command>find /var/log -type f -name "auth.log" -exec grep "Failed password" {} \;</command>

</syscheck>

<email>

<to>security-team@example.com</to>

<subject>Suspicious file modification detected on server X</subject>

<message>Suspicious file modification detected on server X. Check the logs for more information.</message>

</email>

</action>

</rule>

Phát hiện các cuộc tấn công vũ phu:

Quy tắc này được sử dụng để phát hiện các cuộc tấn công vũ phu và tạo cảnh báo khi điều kiện được đáp ứng. Sau đây là một ví dụ về quy tắc Wazuh để phát hiện các cuộc tấn công vũ phu:

<rule id="100004" level="9" group="intrusion\_detection,syslog" frequency="1">

<description>Brute force attack</description>

<match>

<login\_failed/>

<username>root</username>

<srcip>!192.168.1.1</srcip>

</match>

<options>

<threshold>3</threshold>

<interval>120</interval>

</options>

<action>

<syscheck>

<frequency>1</frequency>

<command>find /var/log -type f -name "auth.log" -exec grep "Failed password" {} \;</command>

</syscheck>

<email>

<to>security-team@example.com</to>

<subject>Brute force attack detected on server X</subject>

<message>Brute force attack detected on server X. Check the logs for more information.</message>

</email>

</action>

</rule>

Phát hiện lưu lượng mạng đáng ngờ:

Quy tắc này được sử dụng để phát hiện lưu lượng mạng đáng ngờ và tạo cảnh báo khi điều kiện được đáp ứng. Sau đây là ví dụ về quy tắc Wazuh để phát hiện lưu lượng mạng đáng ngờ:

<rule id="100005" level="10" group="network\_traffic,syslog" frequency="1">

<description>Suspicious network traffic</description>

<match>

<srcip>!192.168.1.1</srcip>

<dstip>192.168.1.1</dstip>

<srcport>!80</srcport>

<dstport>80</dstport>

</match>

<options>

<threshold>5</threshold>

<interval>120</interval>

</options>

<action>

<firewall>

<command>iptables -A INPUT -s %srcip% -j DROP</command>

</firewall>

<email>

<to>security-team@example.com</to>

<subject>Suspicious network traffic detected on server X</subject>

<message>Suspicious network traffic detected on server X. Check the logs for more information.</message>

</email>

</action>

</rule>

Phát hiện truy cập trái phép:

Quy tắc này được sử dụng để phát hiện truy cập trái phép và tạo cảnh báo khi điều kiện được đáp ứng. Sau đây là ví dụ về quy tắc Wazuh để phát hiện truy cập trái phép:

<rule id="100006" level="10" group="access\_control,syslog" frequency="1">

<description>Unauthorized access</description>

<match>

<command>su</command>

<user>!root</user>

</match>

<action>

<syscheck>

<frequency>1</frequency>

<command>lastb | grep -v "root" | grep -v "nologin"</command>

</syscheck>

<email>

<to>security-team@example.com</to>

<subject>Unauthorized access detected on server X</subject>

<message>Unauthorized access detected on server X. Check the logs for more information.</message>

</email>

</action>

</rule>

Phát hiện nhiễm phần mềm độc hại:

Quy tắc này được sử dụng để phát hiện nhiễm phần mềm độc hại và tạo cảnh báo khi điều kiện được đáp ứng. Sau đây là ví dụ về quy tắc Wazuh để phát hiện nhiễm phần mềm độc hại:

<rule id="100007" level="10" group="malware\_detection,syslog" frequency="1">

<description>Malware infection</description>

<match>

<filename>\*/malware/\*</filename>

<checksum\_changed/>

</match>

<action>

<syscheck>

<frequency>1</frequency>

<command>ps aux | grep -v "grep" | grep -i "malware"</command>

</syscheck>

<email>

<to>security-team@example.com</to>

<subject>Malware infection detected on server X</subject>

<message>Malware infection detected on server X. Check the logs for more information.</message>

</email>

</action>

</rule>

Phát hiện các cuộc tấn công ứng dụng web:

Quy tắc này được sử dụng để phát hiện các cuộc tấn công ứng dụng web và tạo cảnh báo khi điều kiện được đáp ứng. Sau đây là ví dụ về quy tắc Wazuh để phát hiện các cuộc tấn công ứng dụng web:

<rule id="100008" level="10" group="web\_application,syslog" frequency="1">

<description>Web application attack</description>

<match>

<url>\*/admin\*</url>

<srcip>!192.168.1.1</srcip>

</match>

<options>

<threshold>3</threshold>

<interval>120</interval>

</options>

<action>

<firewall>

<command>iptables -A INPUT -s %srcip% -j DROP</command>

</firewall>

<email>

<to>security-team@example.com</to>

<subject>Web application attack detected on server X</subject>

<message>Web application attack detected on server X. Check the logs for more information.</message>

</email>

</action>

</rule>