

Wazuh

- Custom Rule Oluřturma
 - Wazuh için Custom Rule
 - Custom Rule İçin Alert Oluřturma

Custom Rule Oluřturma

Wazuh için Custom Rule

Amaç

Unknown user or bad password. 5 dakikada aynı kullanıcı adı ve řifre için bu hatayı alıyorsa bunu bir mail ile ilgililere bildirmek.

Adımlar

1. EventID ile ilişkili Rule'u bulmaca (rule'un yanında 0580-win-security_rules.xml 'e bak RuleID=60122)

Rules (1) [Manage rules files](#) [Add new rules file](#) [Export formatted](#) [Refresh](#)

From here you can manage your rules.

[Filter or search](#) [Custom rules](#)

ID	Description	Groups	Regulatory compliance	Level	File	Path
60122	Logon failure - Unknown user or bad password.	authentication_failed, windows, windows_security	PCI_DSS GPG13 HIPAA GDPR NIST_800_53 TSC MITRE	5	0580-win-security_rules.xml	ruleset/rules

Rows per page: 15 [1](#) [>](#)

2. Bu Rule'u notepad veya benzeri bir alana kopyala
3. /var/ossec/ruleset/rules/0580-win-security_rules.xml dosyasını aç. 60122 ID li kuralı bul.

Nano ile ^w kullanabilirsiniz.

```
<rule id="60122" level="5">
<if_sid>60105</if_sid>
<field name="win.system.eventID">^529$|^4625$</field>
<options>no_full_log</options>
<description>Logon failure - Unknown user or bad password.</description>
<mitre>
  <id>T1078</id>
  <id>T1531</id>
</mitre>

<group>authentication_failed,gdpr_IV_32.2,gdpr_IV_35.7.d,gpg13_7.1,hipaa_164.312.b,nist_800_53_AC.7,nist_8
```

```
00_53_AU.14,pci_dss_10.2.4,pci_dss_10.2.5,tsc_CC6.1,tsc_CC6.8,tsc_CC7.2,tsc_CC$
```

```
</rule>
```

4. Custom Rule'ların ID leri 100.000 ile 120.000 arası olması gerekiyor. Bu nedenle 3 ncü adımda kopyaladığımız Rule da ID yi değiştir. Örn=1000001 yap.

Aşağıdaki gibi olmalıdır

```
<group name="custom rules">
  <rule id="100001" frequency="2" timeframe="300" level="10" overwrite="yes">
    <if_sid>60105</if_sid>
    <field name="win.system.eventID">^529$|^4625$</field>
    <options>no_full_log</options>
    <description>Logon failure - Unknown user or bad password(HM).</description>
    <mitre>
      <id>T1078</id>
      <id>T1531</id>
    </mitre>

    <group>authentication_failed,gdpr_IV_32.2,gdpr_IV_35.7.d,gpg13_7.1,hipaa_164.312.b,nist_800_53_A
    C.7,nist_800_53_AU.14,pci_dss_10.2.4,pci_dss_10.2.5,tsc_CC6.1,tsc_CC6.8,tsc_CC7.2,tsc_CC$
  </rule>
</group>
```

Not: Rule Id satırındaki frequency (300 saniye de 2 kez olursa) ve level parametrelerini eklemeyi unutma!!!

5. wazuhu yeniden başlat.

```
sudo systemctl restart wazuh-manager
```

Custom Rule İin Alert Oluřturma

Ama

Yeni olřturduėumuz custom rule iin alert tipi tanımlama.

Adımlar

/var/ossec/etc nano ossec.conf ile gir. email_alert_level 10 yap.

```
<alerts>
  <log_alert_level>3</log_alert_level>
  <email_alert_level>10</email_alert_level>
</alerts>
```

Mail gnderilecek adresi yaz. rule_id'yi custom rule'a verdiėin ID yap.

```
<email_alerts>
  <email_to>it-helpdesk@solviads.com</email_to>
  <rule_id>100001</rule_id>
  <do_not_delay />
</email_alerts>
```

^x ile ık ve ıkarken kaydetmeyi unutma.

sudo systemctl restart wazuh-manager servisi yeniden bařlat.

wazuh discover a gir. Custom ID filtrele sonucu gr.

Discover

100001

DQL

Last 5 minutes

Show dates

Refresh

+ Add filter

wazuh-alerts-*

Search field names

Filter by type

0

Selected fields

_source

Available fields

Popular

agent.ip

data.win.eventdata.ipAddress

data.win.eventdata.targetUserName

rule.id

_index

agent.id

agent.name

data.win.eventdata.authenticationPackageName

data.win.eventdata.failureReason

data.win.eventdata.ipPort

data.win.eventdata.keyLength

data.win.eventdata.logonProcessName

data.win.eventdata.logonType

data.win.eventdata.processId

data.win.eventdata.status

data.win.eventdata.subjectLogonId

19 hits

Feb 11, 2023 @ 18:05:39.033 - Feb 11, 2023 @ 18:10:39.033

Auto

Count

timestamp per 5 seconds

Time

_source

rule.id: 100001

Input.type: log

agent.ip: 10.10.0.2

agent.name: CLD-SLV02

agent.id: 003

manager.name: wazuh-server

data.win.eventdata.subjectLogonId: 0x0

data.win.eventdata.ipAddress: 192.168.1.222

data.win.eventdata.authenticationPackageName: NTLM

data.win.eventdata.workstationName: CLD-SLV01

data.win.eventdata.subStatus: 0xc000006a

data.win.eventdata.logonProcessName: NtLmSsp

data.win.eventdata.targetUserName: fw-admin

data.win.eventdata.keyLength: 0

data.win.eventdata.subjectUserSid: S-1-0-0

data.win.eventdata.processId: 0x0

data.win.eventdata.ipPort: 61856

data.win.eventdata.failureReason: \2313

data.win.eventdata.targetDomainName: SOLVIADS.local

data.win.eventdata.targetUserSid: S-1-0-0

data.win.eventdata.logonType: 3

data.win.eventdata.status: 0xc000006d

rule.id: 100001

Input.type: log

agent.ip: 10.10.0.2

agent.name: CLD-SLV02

agent.id: 003

manager.name: wazuh-server

data.win.eventdata.subjectLogonId: 0x0

data.win.eventdata.ipAddress: 192.168.1.222

data.win.eventdata.authenticationPackageName: NTLM

data.win.eventdata.workstationName: CLD-SLV01

data.win.eventdata.subStatus: 0xc000006a

data.win.eventdata.logonProcessName: NtLmSsp

data.win.eventdata.targetUserName: fw-admin

data.win.eventdata.keyLength: 0

data.win.eventdata.subjectUserSid: S-1-0-0

data.win.eventdata.processId: 0x0

data.win.eventdata.ipPort: 61843

data.win.eventdata.failureReason: \2313

data.win.eventdata.targetDomainName: SOLVIADS.local

data.win.eventdata.targetUserSid: S-1-0-0

data.win.eventdata.logonType: 3

data.win.eventdata.status: 0xc000006d

rule.id: 100001

Input.type: log

agent.ip: 10.10.0.2

agent.name: CLD-SLV02

agent.id: 003

manager.name: wazuh-server

data.win.eventdata.subjectLogonId: 0x0

data.win.eventdata.ipAddress: 192.168.1.222

data.win.eventdata.authenticationPackageName: NTLM

data.win.eventdata.workstationName: CLD-SLV01

data.win.eventdata.subStatus: 0xc000006a

data.win.eventdata.logonProcessName: NtLmSsp

data.win.eventdata.targetUserName: fw-admin

data.win.eventdata.keyLength: 0

data.win.eventdata.subjectUserSid: S-1-0-0

data.win.eventdata.processId: 0x0

data.win.eventdata.ipPort: 61843

data.win.eventdata.failureReason: \2313

data.win.eventdata.targetDomainName: SOLVIADS.local

data.win.eventdata.targetUserSid: S-1-0-0

data.win.eventdata.logonType: 3

data.win.eventdata.status: 0xc000006d

rule.id: 100001

Input.type: log

agent.ip: 10.10.0.2

agent.name: CLD-SLV02

agent.id: 003

manager.name: wazuh-server

data.win.eventdata.subjectLogonId: 0x0

Fire

Tümünü görün

Rünlük-künlük harfe duvarlı

Fonekik icaretleri hül

Tam cözükler