

Alert Rules Configuration

A. Elastic SIEM Alert Rule

Rule Name

Detect 5+ Failed Logins in 5 Minutes

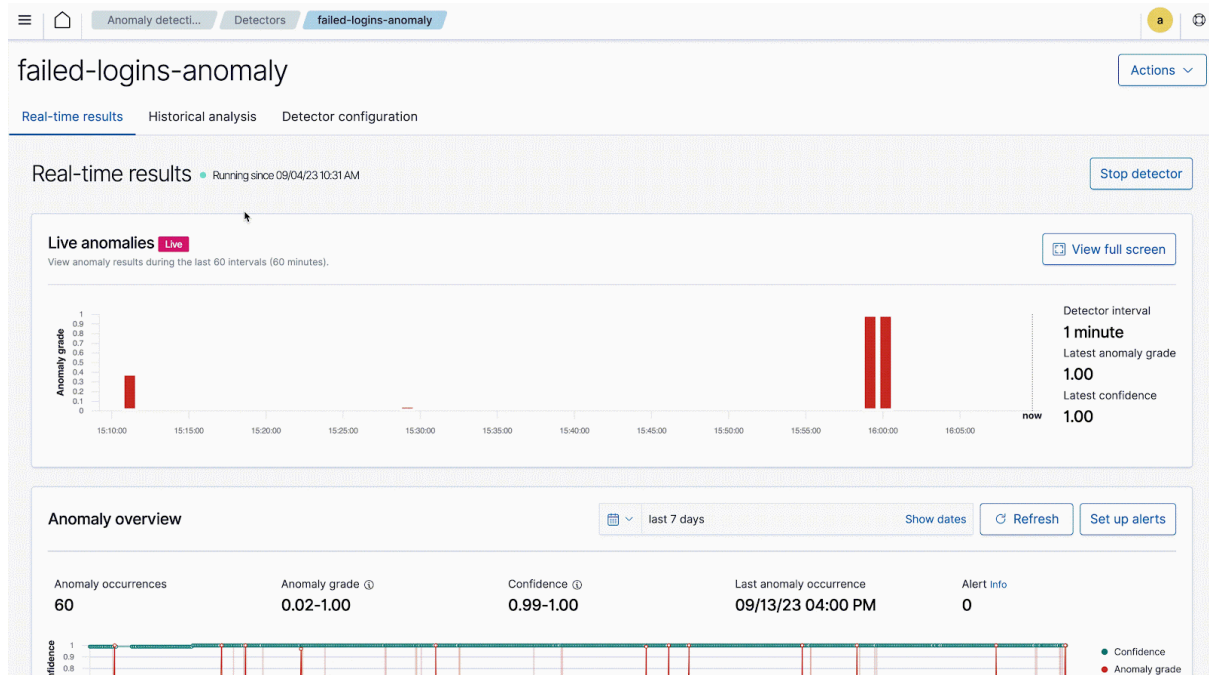
Configuration

- Index: `security-login-*`
- Condition: `count > 5`
- Time window: `5 minutes`

Test

- Simulated failed SSH logins
- Alert triggered successfully

B. Wazuh Custom Alert Rule



```

* <group name="ossec,syslog,sshd,sysmon,">
|
| <!--
| Dec 10 01:02:02 host sshd[1234]: Failed none for root from 1.1.1.1 port 1066 ssh2
| -->
|
| <rule id="100001" level="3" overwrite="yes">
|   <if_sid>5716,5750,5760,5762,5802</if_sid>
|   <match>*Failed*error: PAM: Authentication*error: maximum authentication attempts exceeded*Failed password*Failed keyboard*authentication error*Connection reset*more authentication failures*|REPEATED login failures</match>
|   <description>SSH brute force attack detected/Too many attempts were missed</description>
|   <group>authentication_failed,gdpr_IV_35.7.d,gdpr_IV_32.2,gpg13_7.1,hipaa_164.312.b,nist_800_53_AU.14,nist_800_53_AC.7,pci_dss_10.2.4,pci_dss_10.2.5,tsc_CC6.1,tsc_CC6.8,tsc_CC7.2,tsc_CC7.3,</group>
| </rule>
|
| <rule id="100002" level="6" overwrite="yes">
|   <if_sid>92657,92052</if_sid>
|   <description>Authentication using NTLM/Possible Pass the Hash Attack Detected</description>
|   <group>authentication_success,pci_dss_10.2.5,gpg13_7.1,gpg13_7.2,gdpr_IV_32.2,hipaa_164.312.b,nist_800_53_AU.14,nist_800_53_AC.7,tsc_CC6.8,tsc_CC7.2,tsc_CC7.3,</group>
| </rule>
|
| </group>

```

Tool Used: Wazuh

Custom Rule Created

```

<rule id="100200" level="10">
  <if_matched_sid>5710</if_matched_sid>
  <frequency>3</frequency>
  <timeframe>120</timeframe>
  <description>Multiple failed login attempts detected</description>
</rule>

```

Test Executed

```

ssh user@192.168.1.x
# enter wrong password 3 times

```

Result

- Alert appeared in Wazuh dashboard
- Severity: High