Alert Rules Configuration

A. Elastic SIEM Alert Rule

Rule Name

`Detect 5+ Failed Logins in 5 Minutes`

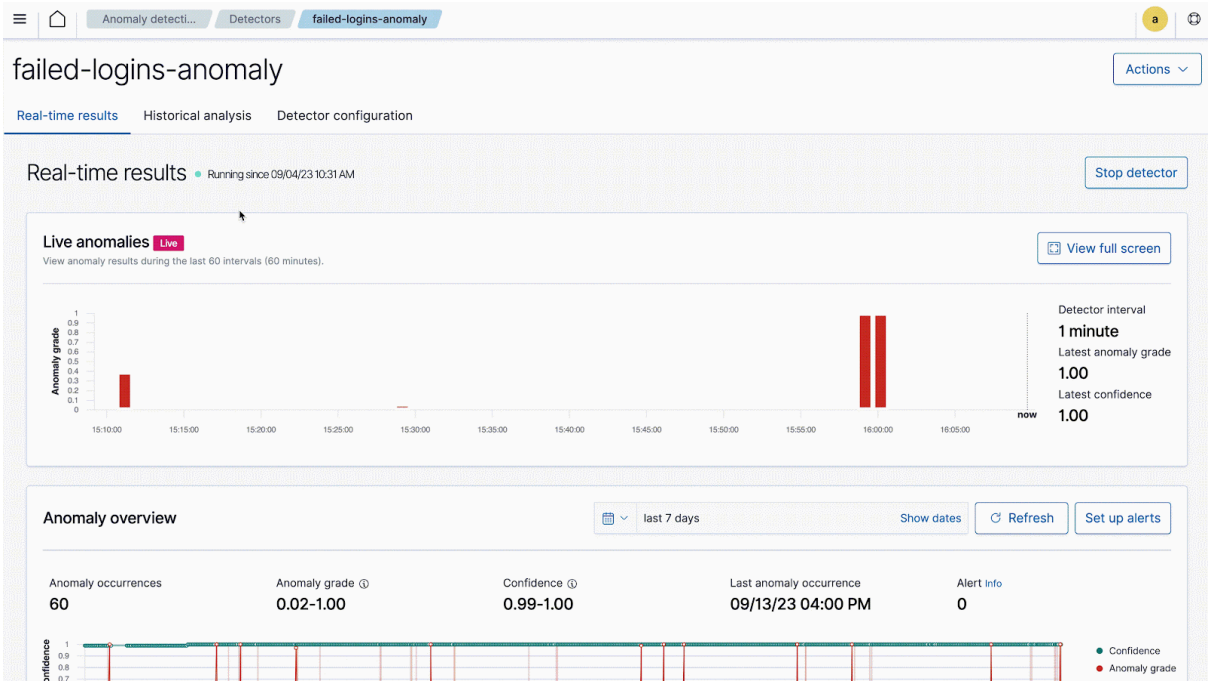
Configuration

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

Test

- Simulated failed SSH logins
- Alert triggered successfully

B. Wazuh Custom Alert Rule



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