SIEM Alert Automation & Noise Reduction

(**Wazuh → Telegram Integration**)

Project Type

Security Monitoring & Alert Automation (Blue Team)

Scope

Endpoint & Log-Based Detection | High-Severity Alerting

Summary

Designed and implemented an automated alert delivery system to improve incident visibility and reduce alert fatigue in a SIEM environment. The solution integrates **Wazuh SIEM** with **Telegram** using **Node-RED**, delivering only high-severity and actionable security alerts to responders in near real-time.

The primary objective was to enhance response efficiency by filtering excessive low-value alerts and focusing on events that require immediate attention.

Architecture Overview (High-Level)

- **Wazuh SIEM** as centralized log collection and detection engine
- **Node-RED** as automation and filtering layer
- **Telegram Bot** as alert delivery channel

Alerts are processed through rule-based logic before being forwarded, ensuring only relevant security events are escalated.

Key Capabilities

- **High-Severity Alert Filtering**
  Only alerts above a defined severity threshold are forwarded to reduce noise.
- **Signal-to-Noise Optimization**
  Low-confidence and repetitive alerts are suppressed to prevent alert fatigue.
- **Automated Alert Delivery**
  Critical security events are pushed automatically to a secure messaging channel.
- **Readable Incident Context**
  Alerts include essential metadata such as severity level, source, and event summary to support quick triage.

Use Case Scenarios

- Detection of suspicious endpoint behavior
- High-risk authentication anomalies
- Policy violation or integrity monitoring alerts
- Security events requiring immediate human review

Risk & Value Assessment

Risk Addressed:

- Missed critical alerts due to excessive SIEM noise
- Delayed incident response
- Analyst fatigue and reduced detection effectiveness

Business Value:

- Faster awareness of critical security incidents
- Improved monitoring efficiency
- Reduced operational overhead for security teams
- Practical alignment with real-world SOC workflows

Security Considerations

- No sensitive log content is exposed externally
- Alert messages are sanitized to avoid data leakage
- Access to alert channels is restricted
- The integration follows least-privilege principles

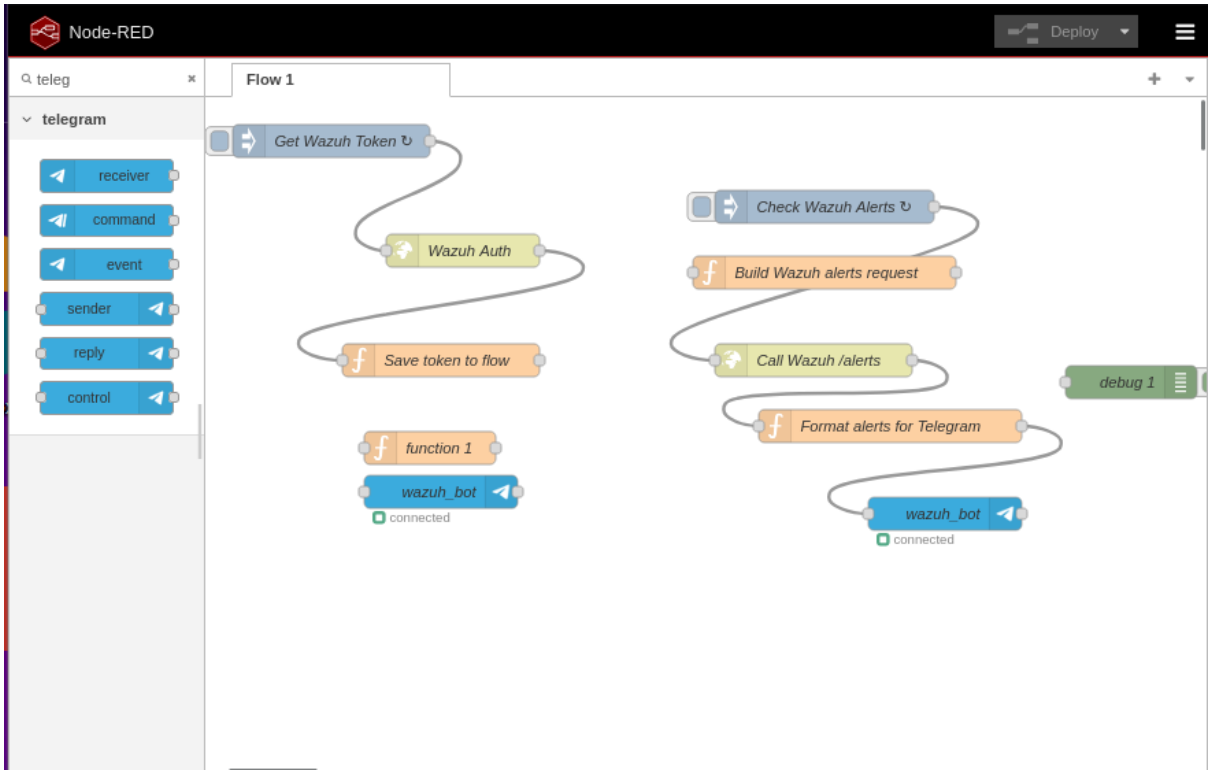
Outcome

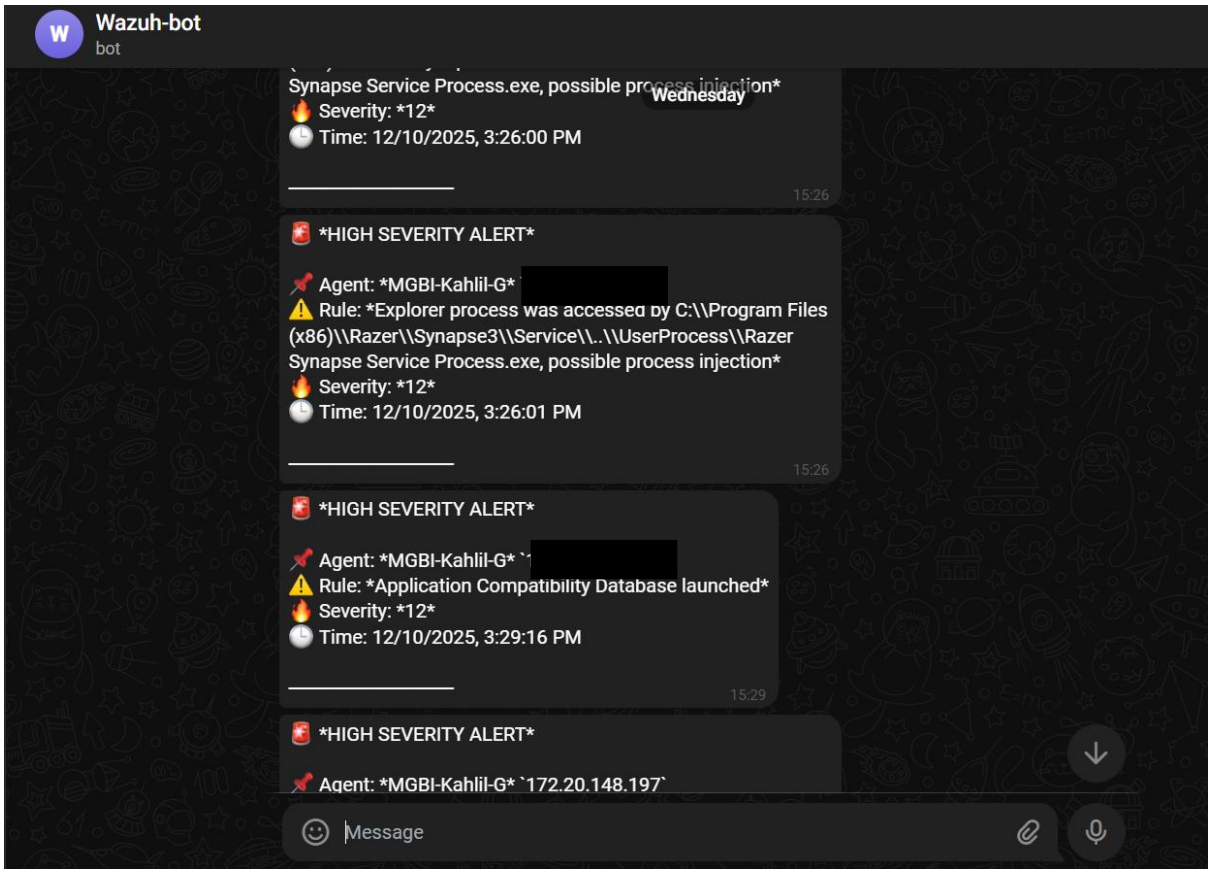
This automation improved security visibility by ensuring that only actionable, high-confidence alerts reached responders. The implementation demonstrates a practical approach to SIEM optimization, balancing detection coverage with operational efficiency.

Security Takeaway

Effective security monitoring is not about generating more alerts, but about delivering the **right alerts to the right people at the right time**. Automation and filtering play a critical role in transforming raw SIEM data into actionable intelligence.

Evidence :


Node-RED
Deploy
teleg
telegram
receiver
command
event
sender
reply
control
Flow 1
Get Wazuh Token
Wazuh Auth
Save token to flow
function 1
wazuh_bot
connected
Check Wazuh Alerts
Build Wazuh alerts request
Call Wazuh /alerts
Format alerts for Telegram
wazuh_bot
connected
debug 1


Wazuh-bot
bot
Synapse Service Process.exe, possible process injection*
Severity: *12*
Time: 12/10/2025, 3:26:00 PM
Wednesday
15:26
HIGH SEVERITY ALERT
Agent: *MGBI-Kahlil-G*
Rule: *Explorer process was accessed by C:\\Program Files (x86)\\Razer\\Synapse3\\Service\\..\\UserProcess\\Razer Synapse Service Process.exe, possible process injection*
Severity: *12*
Time: 12/10/2025, 3:26:01 PM
15:26
HIGH SEVERITY ALERT
Agent: *MGBI-Kahlil-G*
Rule: *Application Compatibility Database launched*
Severity: *12*
Time: 12/10/2025, 3:29:16 PM
15:29
HIGH SEVERITY ALERT
Agent: *MGBI-Kahlil-G* `172.20.148.197`
Message