SIEM Project Report: Elastic Security (ELK Stack)

# 1. SIEM Architecture Components

This project is based on Elastic Security, a SIEM solution built on the Elastic Stack (ELK). The architecture includes the following components:  
  
- Elasticsearch: This is the core engine responsible for storing, indexing, and searching the logs.  
- Logstash and Beats: These are data shippers that collect logs from various sources and send them into Elasticsearch.  
- Kibana: The user interface for data visualization and security operations. It provides dashboards, rule management, and alert tracking.  
- Elastic Security Plugin: A security-focused application within Kibana that supports detection rules, case management, threat intelligence, and investigations.  
  
The architecture ensures that logs collected from diverse sources are parsed, stored, and analyzed efficiently, with a focus on real-time threat detection and incident response.

# 2. Sample Correlation Rule

A custom correlation rule has been created to detect brute force attacks based on failed login attempts. The rule is defined as follows:  
  
- Rule Name: Excessive Failed Logins  
- Description: Detects when a user fails to log in more than five times within a 10-minute window.  
- Logic:   
 IF event.category:authentication AND event.outcome:failure AND user.name has > 5 failures in 10 minutes  
- Action: Trigger alert and send notification to SOC team  
- Purpose: To identify brute-force or credential-stuffing attempts  
  
This rule was created and activated through the "Manage rules" section of the Elastic Security app in Kibana.

# 3. Log Sources

Three different log sources are integrated into this SIEM environment for comprehensive monitoring:  
  
1. Windows Security Logs:  
 - Captures login attempts, user privilege changes, and account management events.  
 - Significance: Helps detect unauthorized access or privilege escalation.  
  
2. Firewall Logs (Cisco ASA):  
 - Tracks allowed/blocked traffic, connection attempts, and port scans.  
 - Significance: Monitors network boundaries and detects suspicious network activity.  
  
3. Web Server Logs (Apache):  
 - Logs HTTP requests, user-agents, response codes, and request paths.  
 - Significance: Useful for identifying abnormal browsing patterns or exploitation attempts.  
  
These logs are ingested through Filebeat and parsed using Logstash.

# 4. Notification Settings Configuration

Notification settings have been configured within Elastic Security to ensure timely alerting of critical events. The configuration includes:  
  
- Alert Action: Email Notification  
- Recipients: soc\_team@company.com  
- Trigger: When rule "Excessive Failed Logins" is matched  
- Frequency: Every time the rule condition is met  
  
This setup ensures that the SOC team receives immediate updates when potential brute-force attempts are detected, allowing for faster response.

# 5. Alerts Dashboard Overview (Screenshot Explanation)

The included screenshot displays the Elastic Security Alerts dashboard. The filters show the system is currently displaying 'open' alerts. Although no severity levels are currently listed in the Summary tab, this dashboard provides powerful filtering based on status, user, severity, and host.  
  
Other tabs such as Trend, Counts, and Treemap offer alternative views for identifying alert patterns and understanding threat trends over time. This central interface allows security analysts to manage incidents effectively and track security rules in real-time.

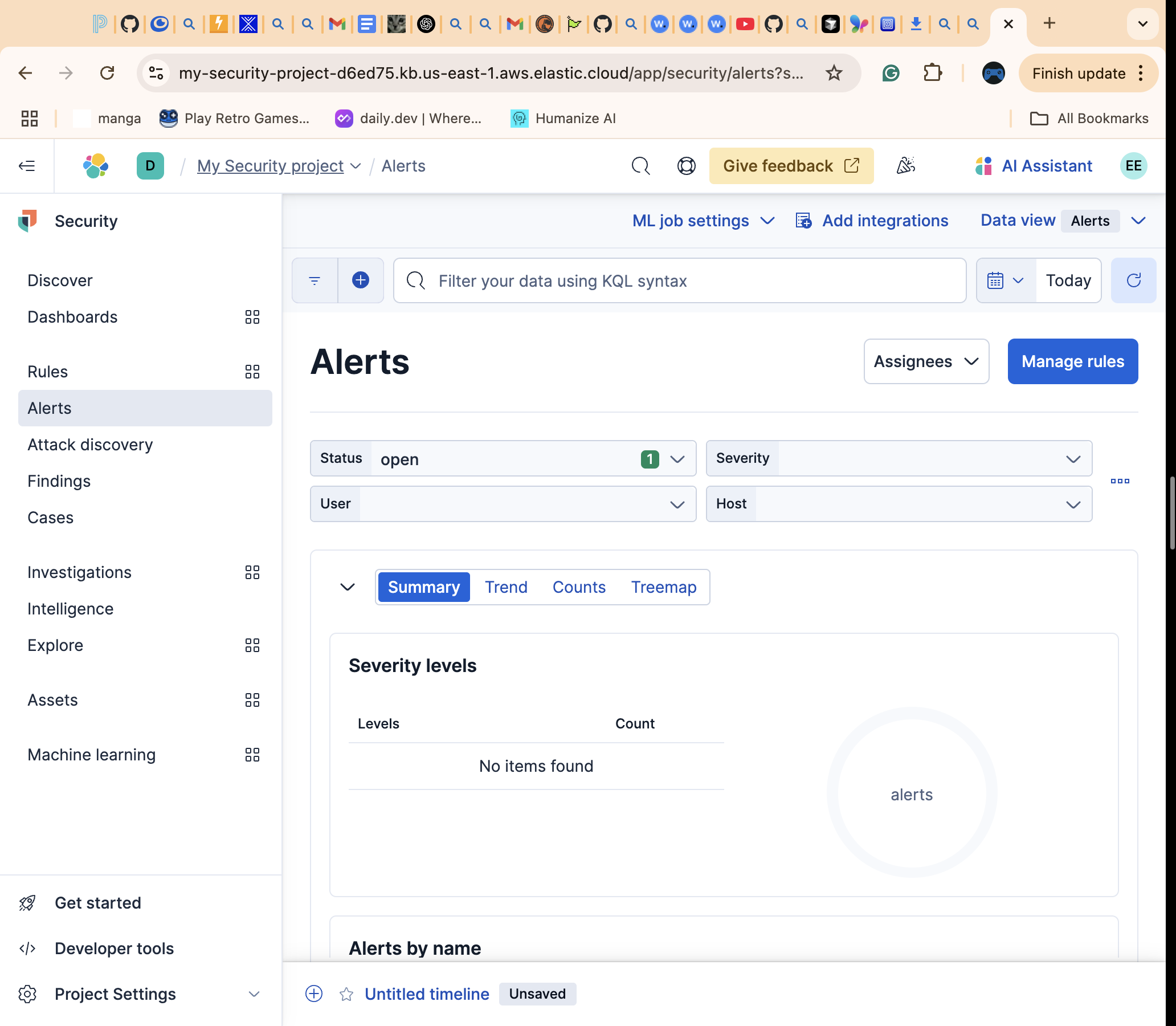


Figure 1: Elastic Security Alerts Dashboard (Source: Kibana Interface)