Elastic Security SIEM & Automated Incident Response Project

By: Ritvik Indupuri

Executive Summary

Developed an end-to-end security monitoring and automated incident response pipeline using Elastic SIEM and Tines SOAR. This project showcases real-time detection of administrative login events, automated incident triage, and immediate alerting workflows, simulating enterprise SOC operations.

Objective

Designed and implemented a full-stack security monitoring and automated incident response system using **Elastic Security (SIEM/EDR)** and **Tines (SOAR)**. This project focused on real-time log ingestion, threat detection, and automated alert notifications to streamline incident response workflows. The goal was to simulate enterprise-grade SOC operations, enhancing visibility into endpoint activity and reducing response latency.

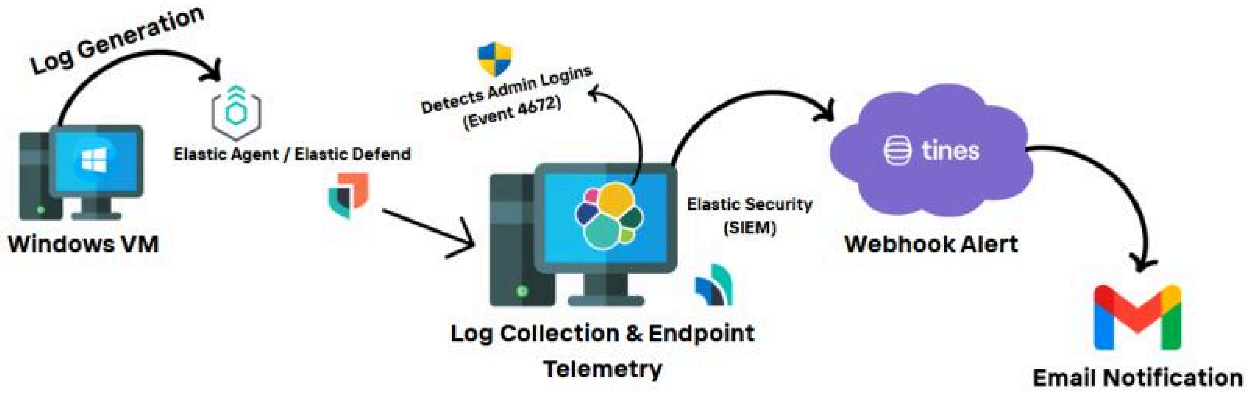
Environment Overview

- **Log Source**: Windows 10 Virtual Machine
- **Security Agent**: Elastic Agent with Elastic Defend (EDR)
- **SIEM Platform**: Elastic Security (Kibana/Elasticsearch Stack)
- **SOAR Integration**: Tines (Webhook Automation)
- **Notification Channel**: Automated Email Alerts via Tines Workflow

---

System Architecture

Figure 1: End-to-End Workflow Architecture

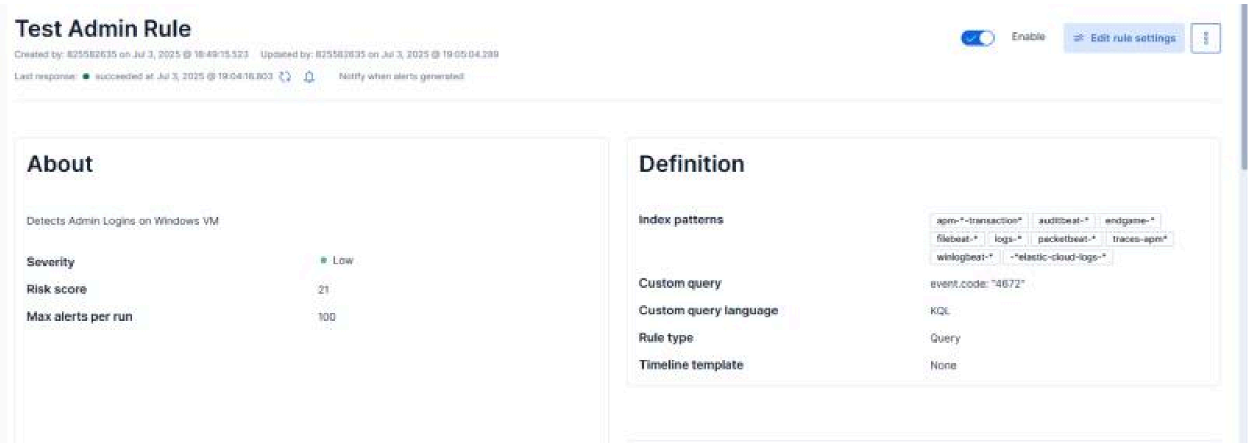

Log Generation
Elastic Agent / Elastic Defend
Windows VM
Detects Admin Logins (Event 4672)
Elastic Security (SIEM)
Log Collection & Endpoint Telemetry
tines
Webhook Alert
Email Notification

Description:
The architecture diagram illustrates the flow of telemetry from log generation to incident notification:

1. Windows VM generates security events.
2. Elastic Agent (Defend) collects logs and endpoint telemetry.
3. Events are ingested into Elastic Security (SIEM) for correlation and detection.
4. Upon detection of admin login events, alerts trigger a Tines webhook.
5. Tines summarizes incident details using AI and dispatches automated email notifications.

Detection Rule Implementation

Figure 2: Custom SIEM Rule — Test Admin Rule



Test Admin Rule

Created by: 825582635 on Jul 3, 2025 @ 18:49:15.523 Updated by: 825582635 on Jul 3, 2025 @ 19:05:04.289

Last response: ● succeeded at Jul 3, 2025 @ 19:04:16.803 Notify when alerts generated

About

Detects Admin Logins on Windows VM

Severity	● Low
Risk score	21
Max alerts per run	100

Definition

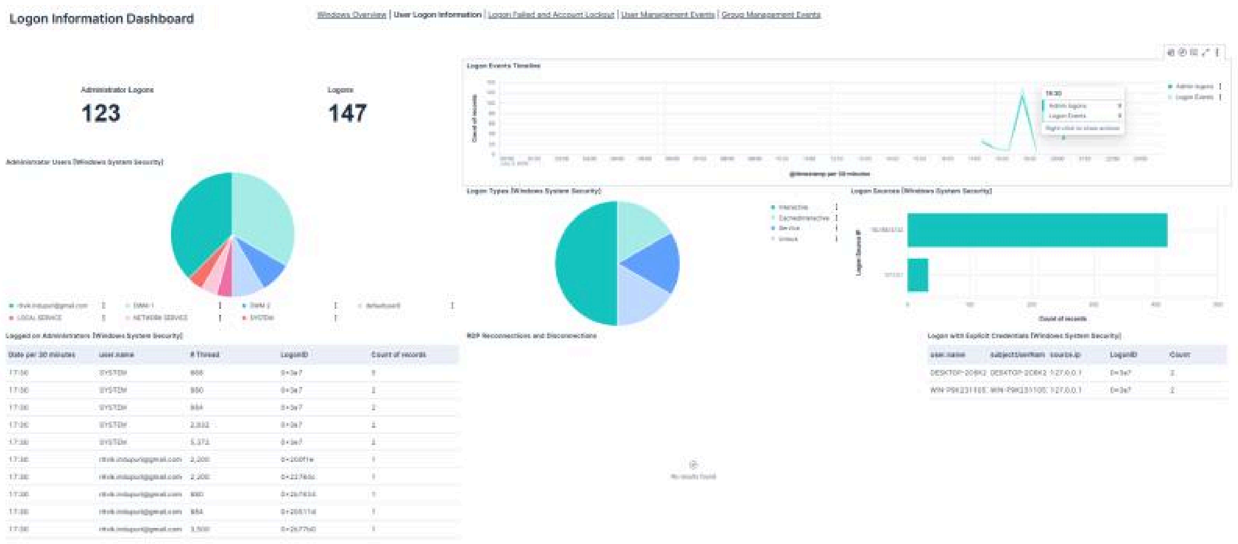
Index patterns	apm-*-transaction* auditbeat-* endgame-* filebeat-* logs-* packetbeat-* traces-apm* winlogbeat-* -*elastic-cloud-logs-*
Custom query	event.code: "4672"
Custom query language	KQL
Rule type	Query
Timeline template	None

Description:
A custom SIEM rule was created to detect administrative login events on the Windows VM by querying for **event.code: "4672"**. The rule was configured with a severity level of Low, a risk score of 21, and a maximum alert threshold of 100 per run.

- **Rule Type**: KQL Query
- **Trigger Condition**: Admin logon detection (event code 4672)
- **Response Action**: Send webhook to Tines upon alert generation

Alert Visualization & Dashboarding

Figure 3: Logon Information Dashboard



Logon Information Dashboard

Windows Overview | User Logon Information | Logon Failed and Account Lockout | User Management Events | Group Management Events

Administrator Logons
123

Logons
147

Logged on Administrators [Windows System Security]

Date per 30 minutes	user.name	# Thread	LogonID	Count of records
17:30	SYSTEM	808	0x3e7	5
17:30	SYSTEM	850	0x3e7	2
17:30	SYSTEM	884	0x3e7	2
17:30	SYSTEM	2,032	0x3e7	2
17:30	SYSTEM	5,372	0x3e7	2
17:30	ritvik.indupuri@gmail.com	2,200	0x200f1e	1
17:30	ritvik.indupuri@gmail.com	2,200	0x22760c	1
17:30	ritvik.indupuri@gmail.com	800	0x2b7634	1
17:30	ritvik.indupuri@gmail.com	884	0x20511d	1
17:30	ritvik.indupuri@gmail.com	3,500	0x2b77b0	1

Logon with Explicit Credentials [Windows System Security]

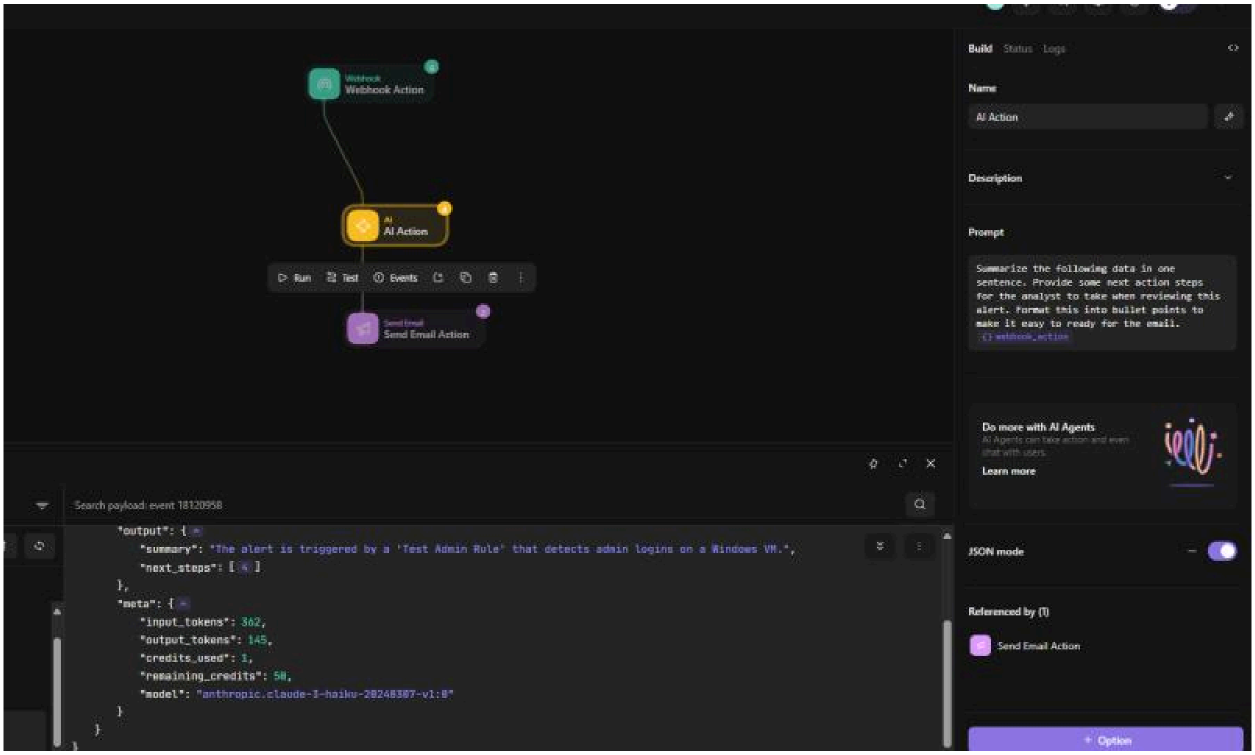
user.name	subjectUserName	source.ip	LogonID	Count
DESKTOP-2O8K2	DESKTOP-2O8K2	127.0.0.1	0x3e7	2
WIN-P9K231105	WIN-P9K231105	127.0.0.1	0x3e7	2

Description:

The logon information dashboard visualizes administrator login activities, RDP sessions, logon types, and event timelines. Pie charts and graphs provide a quick overview of logon patterns, enabling analysts to identify abnormal spikes or unauthorized access attempts in real-time.

Automated Response Workflow

Figure 4: Tines SOAR Workflow Design



Name: AI Action

Prompt:

```
Summarize the following data in one
sentence. Provide some next action steps
for the analyst to take when reviewing this
alert. Format this into bullet points to
make it easy to ready for the email.
{} webhook_action
```

Search payload: event 18120958

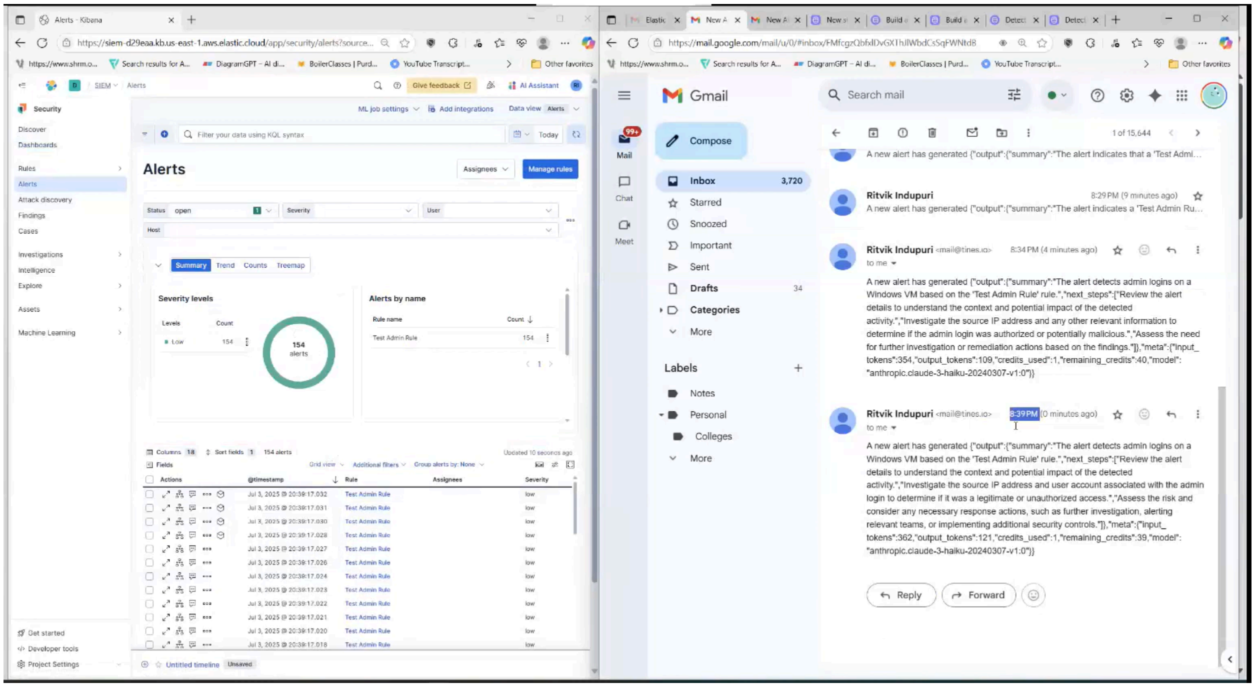
```
    "output": {
      "summary": "The alert is triggered by a 'Test Admin Rule' that detects admin logins on a Windows VM.",
      "next_steps": [ ]
    },
    "meta": {
      "input_tokens": 362,
      "output_tokens": 145,
      "credits_used": 1,
      "remaining_credits": 58,
      "model": "anthropic.claude-3-haiku-20240307-v1:0"
    }
  }
}
```

Description:
Tines orchestrates the incident response process by:

1. Receiving webhook alerts from Elastic SIEM.
2. Processing the alert payload through an AI summarization action.
3. Sending structured email notifications with incident details to SOC teams for immediate awareness.

Real-time Alerting & Email Notifications

Figure 5: Alerts and Email Notification Snapshot



Columns 18 · Sort fields 1 · 154 alerts · Updated 10 seconds ago

Actions	@timestamp	Rule	Assignees	Severity
	Jul 3, 2025 @ 20:39:17.032	Test Admin Rule		low
	Jul 3, 2025 @ 20:39:17.031	Test Admin Rule		low
	Jul 3, 2025 @ 20:39:17.030	Test Admin Rule		low
	Jul 3, 2025 @ 20:39:17.028	Test Admin Rule		low
	Jul 3, 2025 @ 20:39:17.027	Test Admin Rule		low
	Jul 3, 2025 @ 20:39:17.026	Test Admin Rule		low
	Jul 3, 2025 @ 20:39:17.024	Test Admin Rule		low
	Jul 3, 2025 @ 20:39:17.023	Test Admin Rule		low
	Jul 3, 2025 @ 20:39:17.022	Test Admin Rule		low
	Jul 3, 2025 @ 20:39:17.021	Test Admin Rule		low
	Jul 3, 2025 @ 20:39:17.020	Test Admin Rule		low
	Jul 3, 2025 @ 20:39:17.018	Test Admin Rule		low

A new alert has generated {"output":{"summary":"The alert indicates that a 'Test Admi…

Ritvik Indupuri 8:29 PM (9 minutes ago)
A new alert has generated {"output":{"summary":"The alert indicates a 'Test Admin Ru…

Ritvik Indupuri <mail@tines.io> 8:34 PM (4 minutes ago)
to me

A new alert has generated {"output":{"summary":"The alert detects admin logins on a Windows VM based on the 'Test Admin Rule' rule.","next_steps":["Review the alert details to understand the context and potential impact of the detected activity.","Investigate the source IP address and any other relevant information to determine if the admin login was authorized or potentially malicious.","Assess the need for further investigation or remediation actions based on the findings."]},"meta":{"input_tokens":354,"output_tokens":109,"credits_used":1,"remaining_credits":40,"model":"anthropic.claude-3-haiku-20240307-v1:0"}}

Ritvik Indupuri <mail@tines.io> 8:39 PM (0 minutes ago)
to me

A new alert has generated {"output":{"summary":"The alert detects admin logins on a Windows VM based on the 'Test Admin Rule' rule.","next_steps":["Review the alert details to understand the context and potential impact of the detected activity.","Investigate the source IP address and user account associated with the admin login to determine if it was a legitimate or unauthorized access.","Assess the risk and consider any necessary response actions, such as further investigation, alerting relevant teams, or implementing additional security controls."]},"meta":{"input_tokens":362,"output_tokens":121,"credits_used":1,"remaining_credits":39,"model":"anthropic.claude-3-haiku-20240307-v1:0"}}

Description:
The Elastic SIEM dashboard displays active alerts generated by the custom detection rule, while the Gmail interface shows corresponding automated alert emails. This real-time notification pipeline ensures rapid incident awareness and response.

Impact and Conclusion

This project demonstrates a fully integrated SIEM and SOAR pipeline designed for real-time threat detection and automated incident response. By automating the initial triage of 154 administrative login alerts, the system reduces manual analyst workload and accelerates incident awareness, simulating an enterprise SOC workflow. By configuring custom detection rules in Elastic Security and orchestrating automated alert triage using Tines, the system mirrors modern enterprise SOC workflows. The result is a scalable, efficient model for reducing alert fatigue and accelerating incident handling in security operations.
