Elastic SIEM Zeek Log Ingestion & Validation

Project Type: Endpoint Detection Engineering / SOC Telemetry

Prepared by: Niknaz Sadehvandi

Role: Founder & Cybersecurity Consultant

Organization: NS Cybersecurity

Date: December 2024

Objective

The objective of this project was to deploy, ingest, and validate **Zeek-based network telemetry** within **Elastic SIEM** to establish SOC-grade visibility into DNS and network connection activity. The goal was to confirm reliable log ingestion, validate data quality in Kibana, and demonstrate readiness for detection engineering and continuous monitoring.

Tools & Technologies

- **Network Sensor:** Zeek
- **SIEM Platform:** Elastic SIEM (Elastic Security)
- **Log Shipper:** Filebeat (Zeek module)
- **Operating System:** Ubuntu 24.04
- **Visualization & Search:** Kibana Discover
- **Detection Engineering:** Elastic Security Detection Rules

Technical Steps Performed

1. Installed and configured **Zeek** on an Ubuntu 24.04 host to generate network telemetry, including `conn.log` and `dns.log`.
2. Enabled and configured the **Filebeat Zeek module** to forward Zeek logs to Elastic SIEM.
3. Verified successful Filebeat service operation and confirmed log forwarding to Elastic indices.
4. Validated indexed Zeek events in **Kibana Discover**, confirming:
   - DNS queries and network connection events
   - Proper field mapping and normalization
   - Accurate timestamps aligned with live traffic generation
5. Created **Elastic Security detection rules** using Zeek DNS telemetry to demonstrate operational SOC use.
6. Configured rule scheduling, severity, and risk scores to validate alerting readiness.

Findings

- Zeek-generated DNS and network connection events were successfully ingested into Elastic SIEM.
- Events were searchable, structured, and time-aligned in Kibana Discover.
- Host metadata and source IP fields were consistently populated.
- Detection rules could be created and scheduled using Zeek telemetry.
- No ingestion failures, parsing errors, or pipeline interruptions were observed.

Outcome

This project resulted in a **fully functional SOC-grade network telemetry pipeline** using Zeek and Elastic SIEM. Centralized visibility into DNS and network activity was established, enabling detection engineering, alerting, and threat-hunting workflows. The environment demonstrates real-world SIEM ingestion, validation, and operational readiness consistent with SOC analyst responsibilities.

Portfolio Status

Status: Completed
Evidence:

- Kibana Discover screenshots showing Zeek DNS and network events

- Elastic Security detection rule configuration

Artifact:
Elastic_SIEM_Zeek_Log_Ingestion_and_Validation.pdf

Figure 1, Kibana Discover: Zeek Network Telemetry

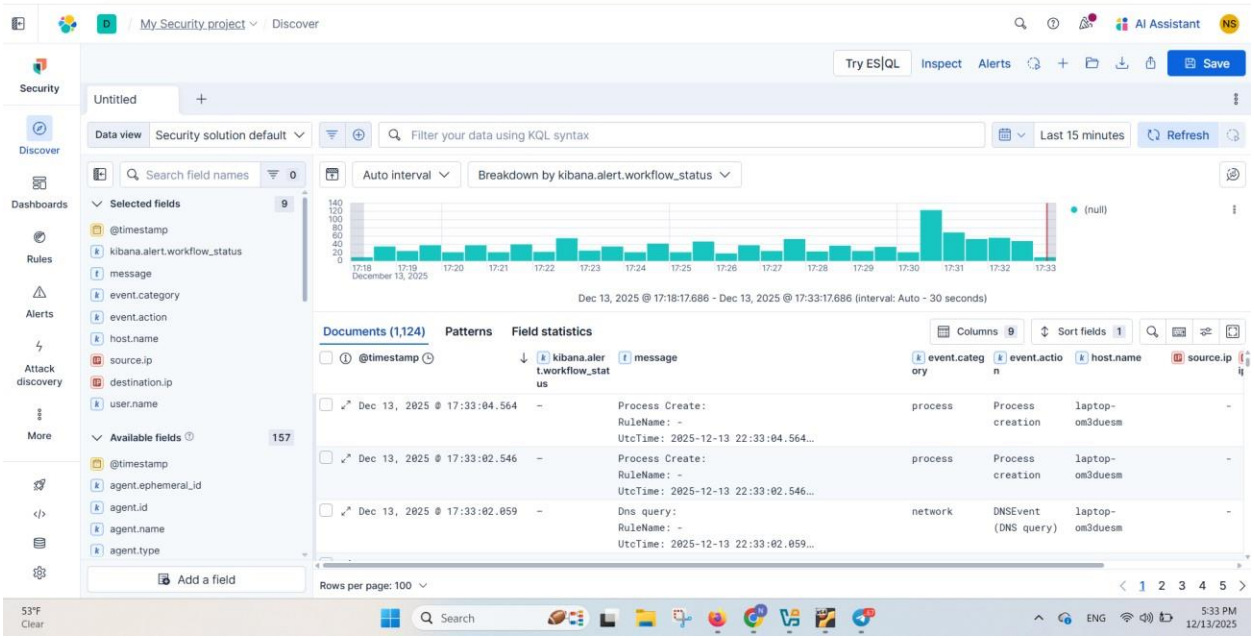
Caption:
Kibana Discover view confirming successful ingestion of Zeek network telemetry into Elastic SIEM. DNS queries, network connection events, host metadata, and source IP fields are visible with the time range set to **Last 15 minutes**, validating real-time SOC ingestion of Zeek logs forwarded via the Filebeat Zeek module.

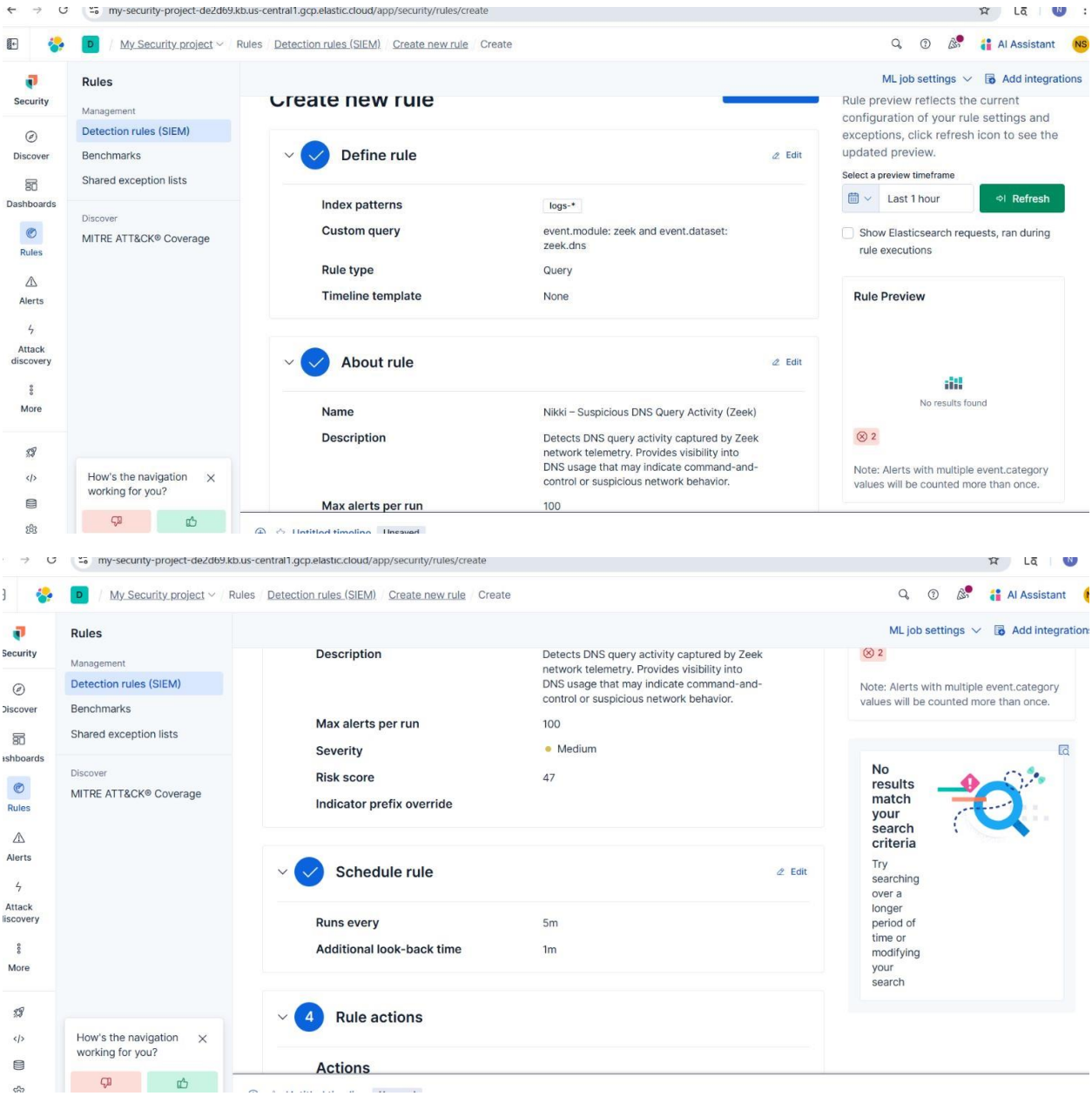
Figure 2, Detection Rule Creation (Zeek DNS Activity)

Caption:
Elastic Security detection rule configuration leveraging Zeek DNS telemetry ingested through Filebeat, demonstrating the ability to operationalize network data for SOC detection and alerting workflows.

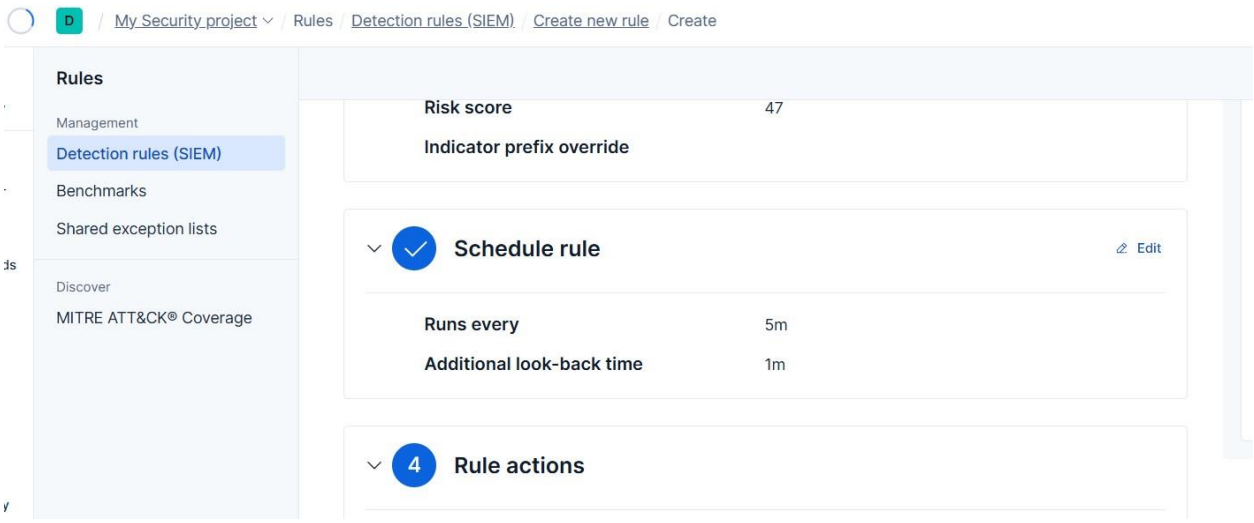
Figure 3, Detection Rule Scheduling & Risk Configuration

Caption:
Detection rule scheduling, severity, and risk score configuration within Elastic SIEM, confirming readiness for continuous monitoring and alert generation based on Zeek network events.


My Security project
Discover
AI Assistant
Try ES|QL
Inspect
Alerts
Save
Security
Untitled
Discover
Dashboards
Rules
Alerts
Attack discovery
More
Data view
Security solution default
Filter your data using KQL syntax
Last 15 minutes
Refresh
Search field names
Auto interval
Breakdown by kibana.alert.workflow_status
Selected fields
@timestamp
kibana.alert.workflow_status
message
event.category
event.action
host.name
source.ip
destination.ip
user.name
Available fields
agent.ephemeral_id
agent.id
agent.name
agent.type
Add a field
(null)
Dec 13, 2025 @ 17:18:17.686 - Dec 13, 2025 @ 17:33:17.686 (interval: Auto - 30 seconds)
Documents (1,124)
Patterns
Field statistics
Columns
Sort fields
@timestamp
kibana.alert.workflow_status
message
event.category
event.action
host.name
source.ip
Dec 13, 2025 @ 17:33:04.564
Process Create:
RuleName: -
UtcTime: 2025-12-13 22:33:04.564...
process
Process creation
laptop-om3duesm
Dec 13, 2025 @ 17:33:02.546
Process Create:
RuleName: -
UtcTime: 2025-12-13 22:33:02.546...
process
Process creation
laptop-om3duesm
Dec 13, 2025 @ 17:33:02.059
Dns query:
RuleName: -
UtcTime: 2025-12-13 22:33:02.059...
network
DNSEvent (DNS query)
laptop-om3duesm
Rows per page: 100
1 2 3 4 5
53°F
Clear
Search
ENG
5:33 PM
12/13/2025


my-security-project-de2d69.kb.us-central1.gcp.elastic.cloud/app/security/rules/create
My Security project / Rules / Detection rules (SIEM) / Create new rule / Create
AI Assistant
Rules
Management
Detection rules (SIEM)
Benchmarks
Shared exception lists
Discover
MITRE ATT&CK® Coverage
Create new rule
ML job settings
Add integrations
Define rule
Edit
Index patterns
logs-*
Custom query
event.module: zeek and event.dataset: zeek.dns
Rule type
Query
Timeline template
None
About rule
Edit
Name
Nikki – Suspicious DNS Query Activity (Zeek)
Description
Detects DNS query activity captured by Zeek network telemetry. Provides visibility into DNS usage that may indicate command-and-control or suspicious network behavior.
Max alerts per run
100
Rule preview reflects the current configuration of your rule settings and exceptions, click refresh icon to see the updated preview.
Select a preview timeframe
Last 1 hour
Refresh
Show Elasticsearch requests, ran during rule executions
Rule Preview
No results found
2
Note: Alerts with multiple event.category values will be counted more than once.
How's the navigation working for you?

my-security-project-de2d69.kb.us-central1.gcp.elastic.cloud/app/security/rules/create
My Security project / Rules / Detection rules (SIEM) / Create new rule / Create
AI Assistant
Rules
Management
Detection rules (SIEM)
Benchmarks
Shared exception lists
Discover
MITRE ATT&CK® Coverage
ML job settings
Add integrations
Description
Detects DNS query activity captured by Zeek network telemetry. Provides visibility into DNS usage that may indicate command-and-control or suspicious network behavior.
Max alerts per run
100
Severity
Medium
Risk score
47
Indicator prefix override
Schedule rule
Edit
Runs every
5m
Additional look-back time
1m
4
Rule actions
Actions
2
Note: Alerts with multiple event.category values will be counted more than once.
No results match your search criteria
Try searching over a longer period of time or modifying your search
How's the navigation working for you?


D
My Security project
Rules
Detection rules (SIEM)
Create new rule
Create
Rules
Management
Detection rules (SIEM)
Benchmarks
Shared exception lists
Discover
MITRE ATT&CK® Coverage
Risk score
47
Indicator prefix override
Schedule rule
Edit
Runs every
5m
Additional look-back time
1m
4
Rule actions