

Задание 1

Интерфейс Kibana

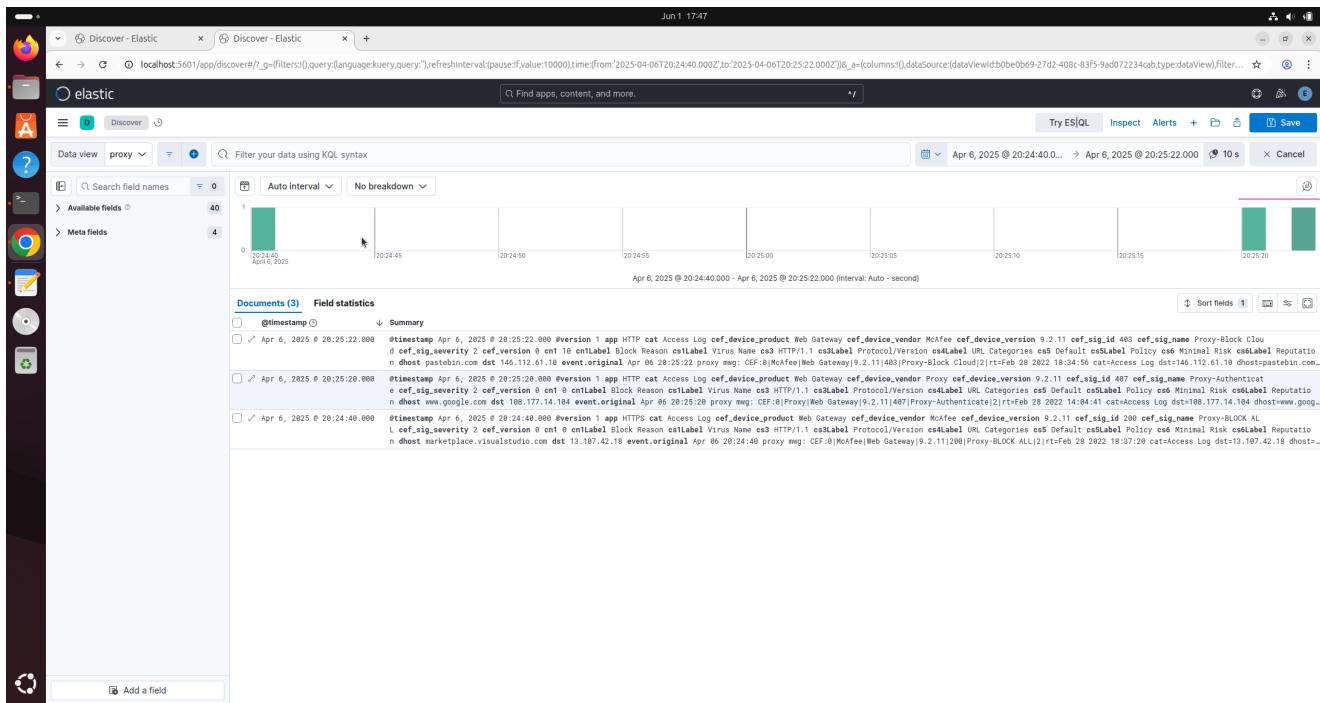
The screenshot shows the Kibana home page. At the top, there's a navigation bar with tabs for 'Discover - Elastic' and 'Home - Elastic'. Below the navigation is a search bar with placeholder text 'Find apps, content, and more.' On the left, there's a sidebar titled 'Spaces' with a 'Manage spaces' button. The main content area has a 'Welcome home' section with four cards: 'Elasticsearch' (yellow), 'Observability' (pink), 'Security' (teal), and 'Analytics' (blue). Below this is a 'Get started by adding integrations' section with a 'Add integrations' button, a 'Try sample data' link, and an 'Upload a file' link. To the right of this is a 'Try managed Elastic' section with a 'Move to Elastic Cloud' button. At the bottom, there's a 'Management' section with four cards: 'Manage permissions', 'Monitor the stack', 'Back up and restore', and 'Manage index lifecycles'. A 'Dev Tools' and 'Stack Management' link is also present.

Список отрываемых портов

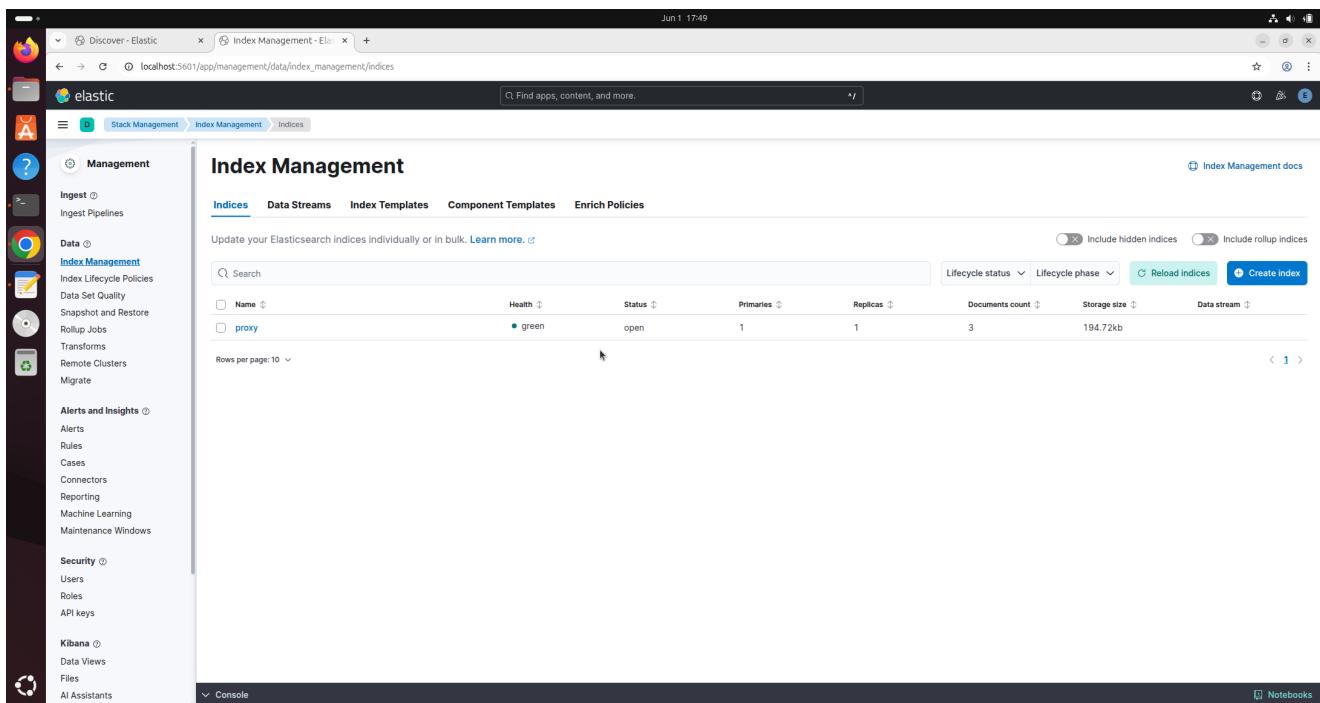
- 9200 - Elasticsearch
- 5601 - Kibana
- 5000-5001, 5044 - Logstash

Задание 2

Содержимое лога proxy.log



Название индекса во вкладке Index Management.



Задание 3

Правила фильтрации в auth.conf

Скриншоты DataView auth-лога

Screenshot of the Kibana interface showing a search results page for Elasticsearch logs. The search bar at the top contains the query: `_g(filters:[],refreshInterval:'5000ms',time:(from:now-15m,to:now))_a:@columns:[],dataSource:(dataViewId:'ba398a77-45ec-4b50-9f54-7d057b48e6e2')type:dataView,filters:[],interval:auto,query:(language:kuery,query:""),sort:[{id:@_score}],size:10`. The results show 52 documents from June 2, 2025, between 19:44 and 19:59. The left sidebar includes sections for Available fields, Empty fields, and Meta fields. The right sidebar features tabs for Try ES/SQL, Inspect, Alerts, and Save, along with filters for Last 15 minutes and Refresh.

Правило определения brute force

Create new rule - Kibana | Discover - Elastic | Detection rules (SIEM) | Alerts - Kibana | Create index API | Cases - Management - El | Elastic

localhost:5601/app/security/rules/id/5677fc9d-376f-4f69-9b04-085396b03613/alerts?sourceer=(default:(idsecurity-solution-default,selectedPatterns:[])),&timerange=(global:(linkTo:(timeline)),timerange:(from:%272025-06-02T00:00:00.000Z%27,to:%272025-06-02T23:59:59.999Z%27,fromStr:now%2Fd,kind:relative,toStr:now%2Fd,kind:relative))

Brute force rule

Created by: elastic on Jun 2, 2025 @ 20:12:58.458 Updated by: elastic on Jun 2, 2025 @ 20:12:58.458
Last response: succeeded at Jun 2, 2025 @ 20:18:00.397 Notify when alerts generated

About

Brute force rule

Severity: Medium

Risk score: 47

Max alerts per run: 100

Definition

Data view ID: 8a398a77-45ec-4b50-9f54-7d057b48e6e2
Data view index pattern: auth*
Custom query: program: "login" and auth_message: **authentication failure**
Custom query language: KQL
Rule type: Threshold
Timeline template: None
Threshold: Results aggregated by hostname.keyword >= 5

Schedule

Runs every: 5m
Additional look-back time: 99999h

Get started | Manage | Alerts | Rule exceptions | Execution results

Untitled timeline | Unsaved

Сработка правила

Create new rule - Kibana | Discover - Elastic | Detection rules (SIEM) | Alerts - Kibana | Create index API | Cases - Management - El | Elastic

localhost:5601/app/security/rules/management?sourceer=(default:(idsecurity-solution-default,selectedPatterns:[])),&timerange=(global:(linkTo:(timeline)),timerange:(from:%272025-06-02T00:00:00.000Z%27,to:%272025-06-02T23:59:59.999Z%27,fromStr:now%2Fd,kind:relative,toStr:now%2Fd,kind:relative))

Rules

Installed Rules: 1 | **Rule Monitoring**: 1

Showing 1-1 of 1 rule Selected 0 rules Select all 1 rule Bulk actions Refresh

Rule	Risk score	Severity	Last run	Last response	Last updated	Notify	Enabled
Brute force rule	47	Medium	3 minutes ago	Succeeded	3 minutes ago	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Rows per page: 20