2026
FIRST
Regional
Symposium
Central Asia

Tashkent, UZ
February 26-27

How to Scale Up Your SOC Capabilities with Open-Source Tools

ARŪNAS VENCLOVAS

ARŪNAS VENCLOVAS

Director of Product Development

About

Arūnas is an experienced leader in product development with a deep understanding of cybersecurity, IT, and telecommunication markets. Currently serving as the Director of Product Development at NRD Cyber Security, Arūnas is responsible for deploying cyber security solutions in National and sectorial CERTs with the aim to automate operations, build capacity and empower for successful work.

Arunas has played a major role in automating and modernizing CSIRTMalta, Eg-FinCIRT, etc. in assisting them to improve network detection capabilities by automating threat hunting, rulesets adjustment and solving other related challenges.

Areas of expertise

- CSIRT/SOC establishment
- Cybersecurity resilience and governance

OUR PORTFOLIO: SERVICES

Cyber SOC

24/7 managed SOC

- Round the clock network monitoring
- Experienced team of analysts
- State-of-the art technology

CSIRT/SOC services

- Establishment
- Modernisation
- Training courses

○ Cybersecurity capacity building

○ CISO advisory

○ ISO 27001 standard implementation

○ Technology solutions

○ Training courses

○ Preparation for NIS2

Current CyberSOC services

Monitoring and Detection 24/7
SIEM, EDR/XDR, NDR

Reaction to security alerts

Incident Handling

Vulnerability identification
scanning, pentests, social engineering

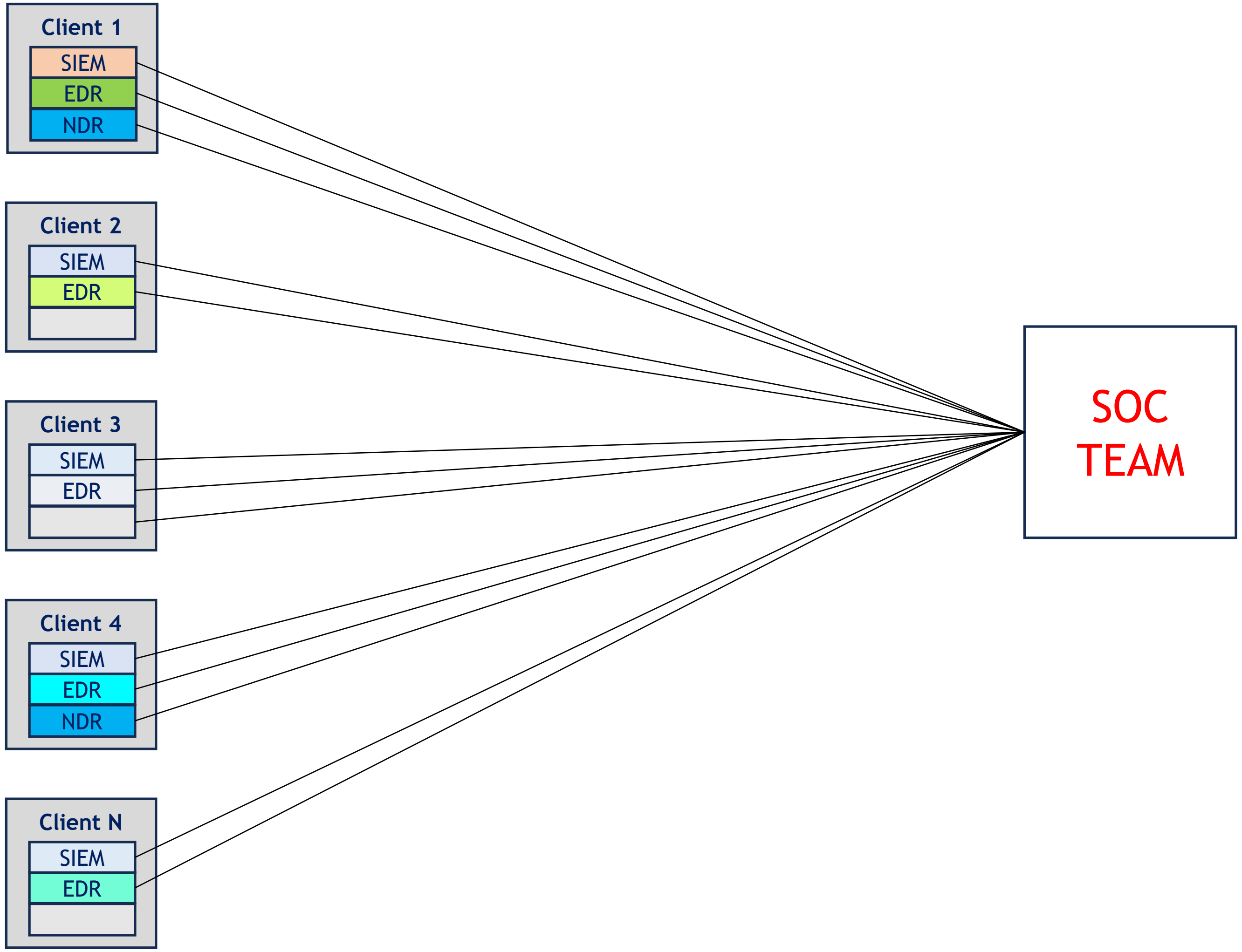
Vulnerability Management

CTI

Tools deployment and maintenance

Consultations and reporting

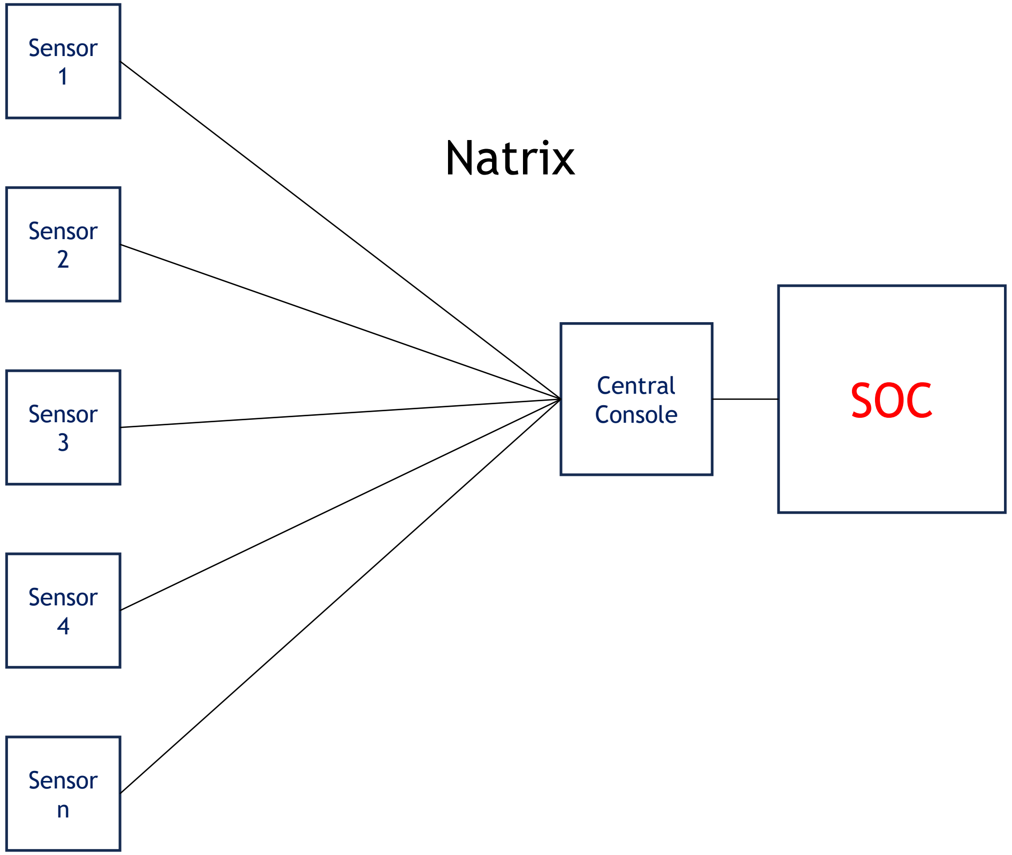
SOC challenge



New customers = new problems

- New investments
- New analysts
- New CTI managers
- New problems with monitoring tools

New Approach of Service Delivery



SOC Centralized Management Platform

Main tool for security analysts

Standardized representation of alerts from any kind of monitoring tool

Tool for alert triage and threathunting

CIT management

Open-Source tools

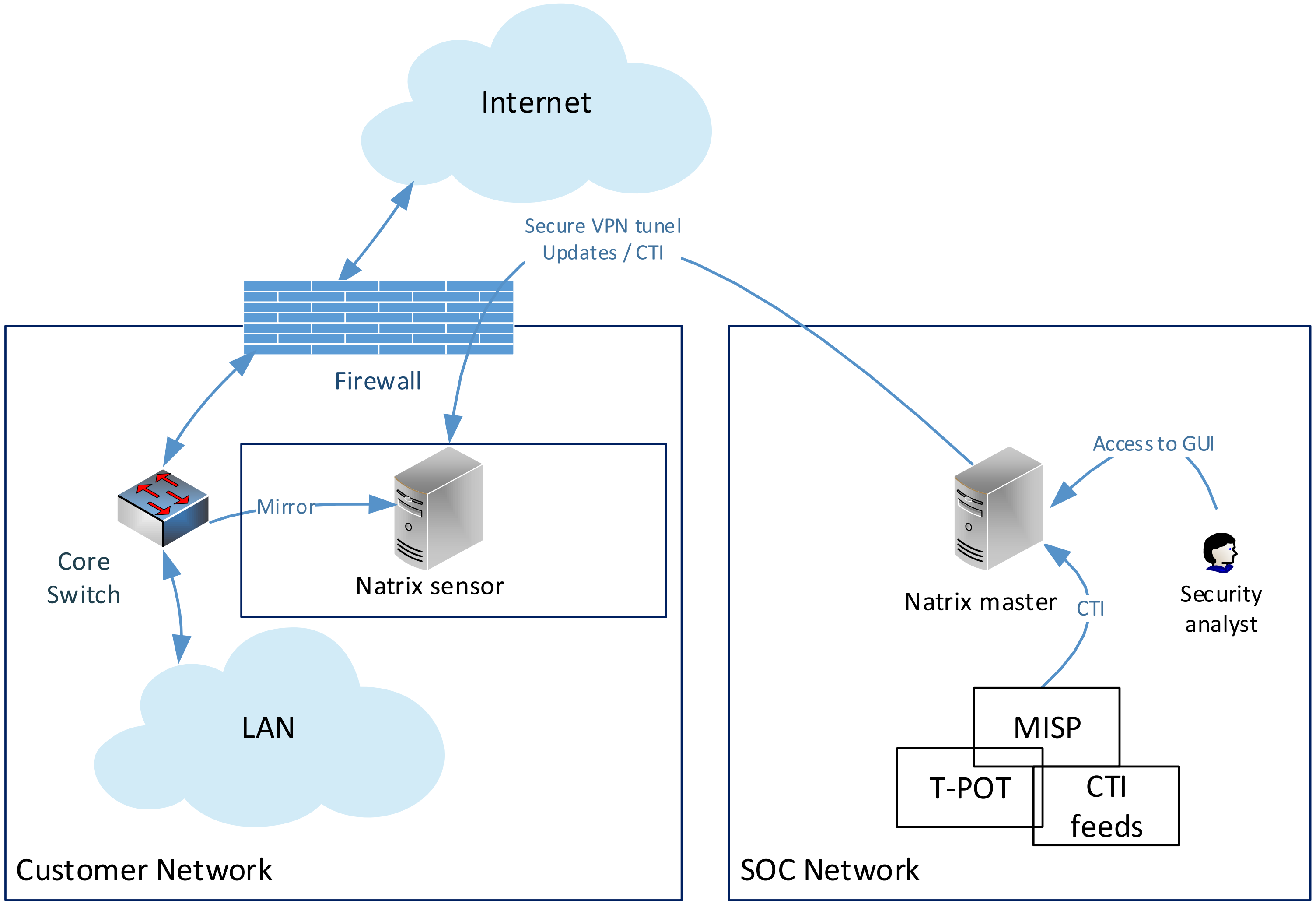
⬇

Better scalability
(human and hardware resources)

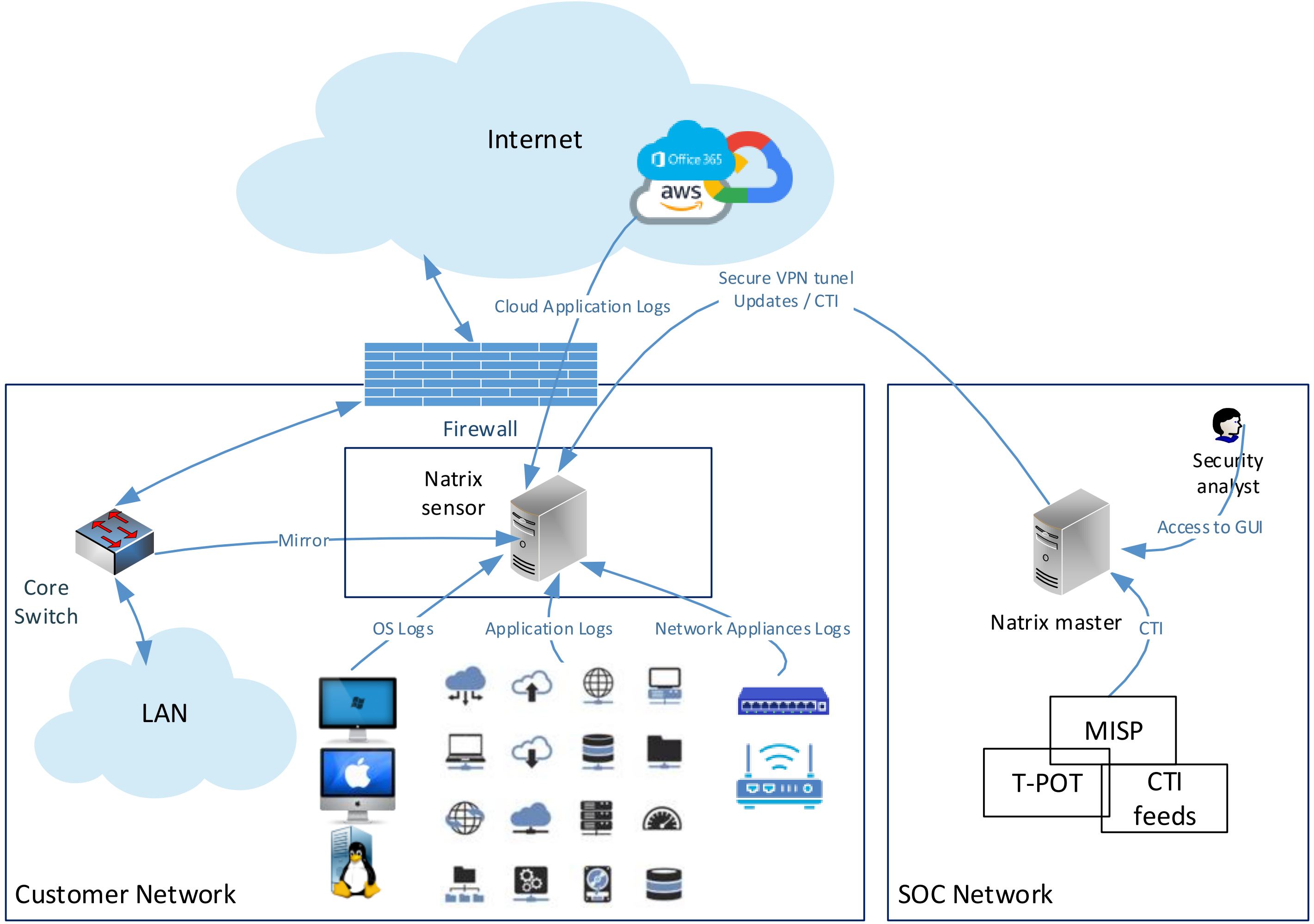
Better quality of services

More flexibility in pricing

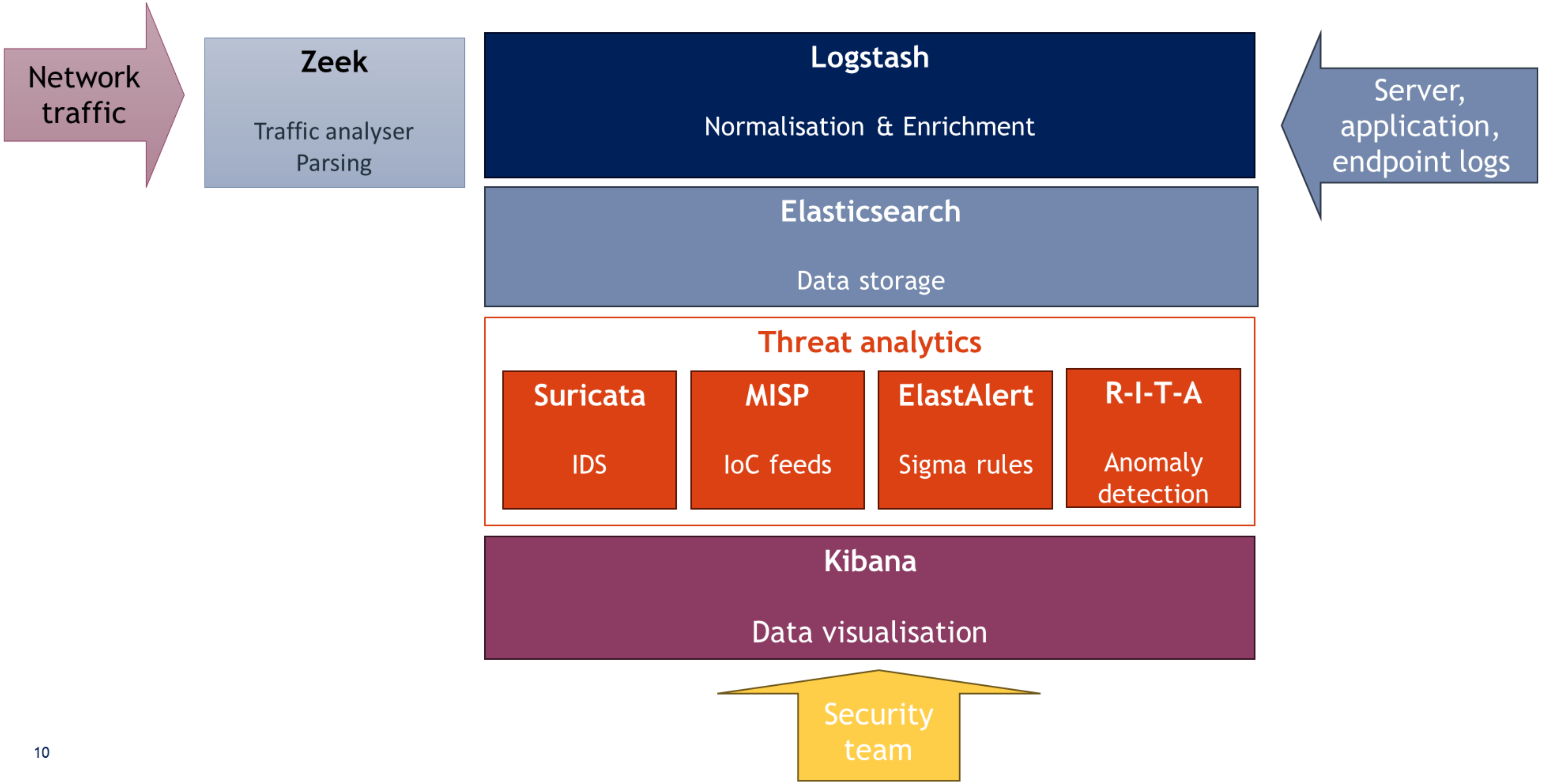
Multi-Organisation Monitoring Architecture



Multi-Organisation Monitoring Architecture



Key components diagram



Network traffic

Zeek

Traffic analyser Parsing

Logstash

Normalisation & Enrichment

Server, application, endpoint logs

Elasticsearch

Data storage

Threat analytics

Suricata

IDS

MISP

IoC feeds

ElastAlert

Sigma rules

R-I-T-A

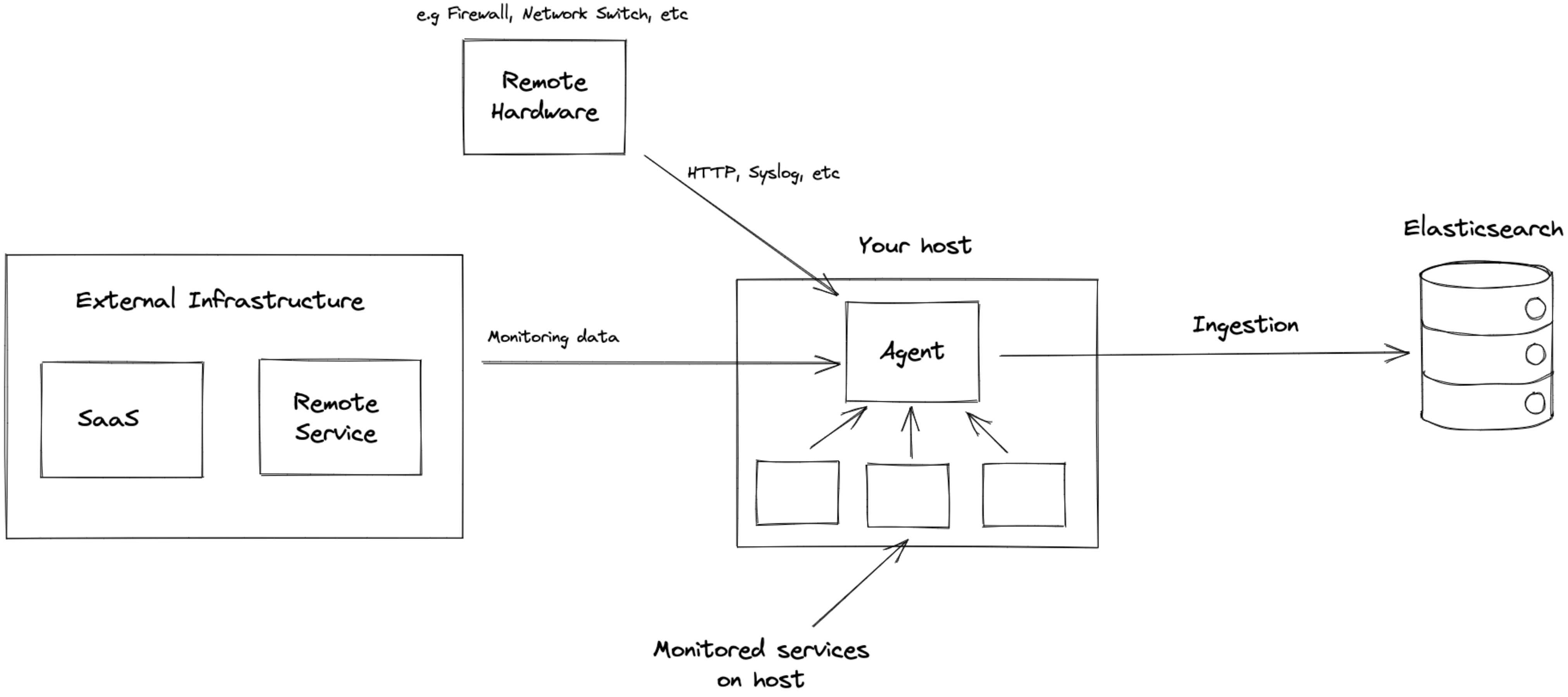
Anomaly detection

Kibana

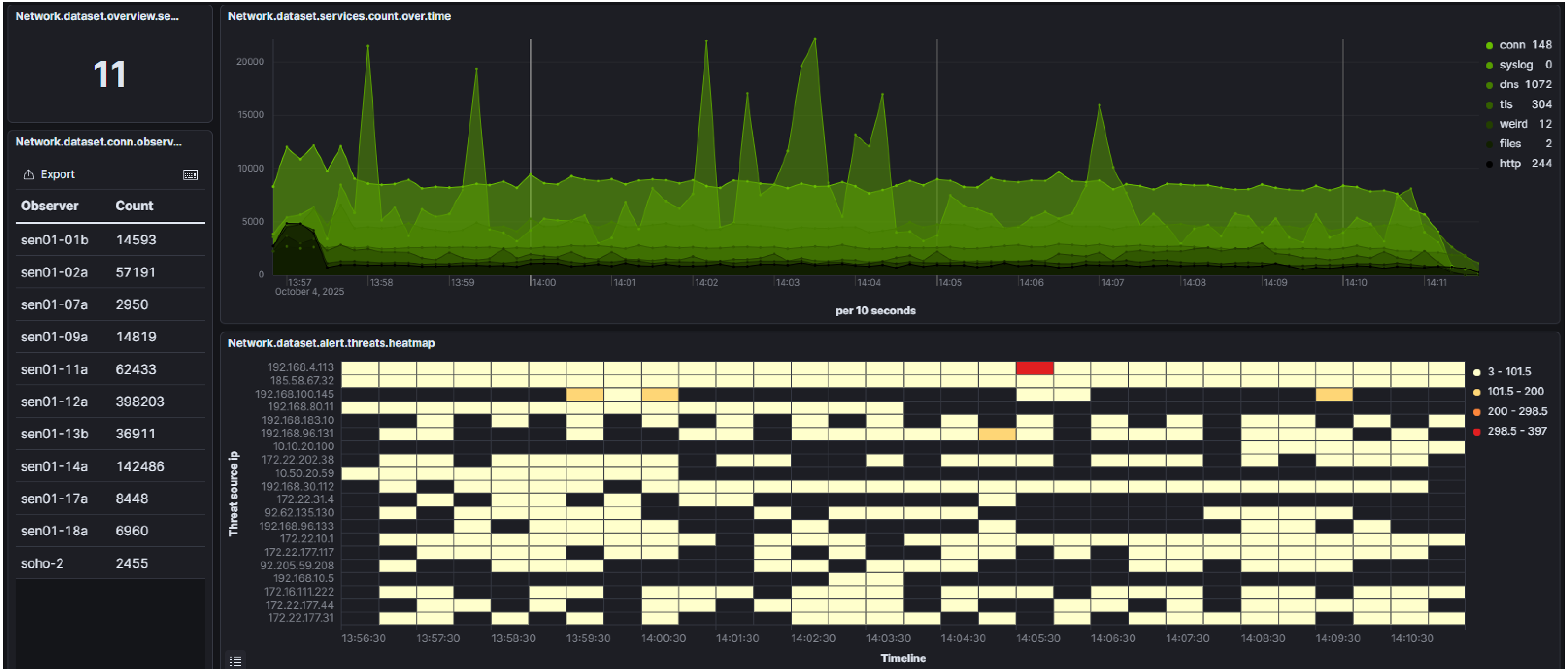
Data visualisation

Security team

Elastic Agent



Centralized Monitoring



Network.dataset.overview.se...

11

Network.dataset.conn.observ...

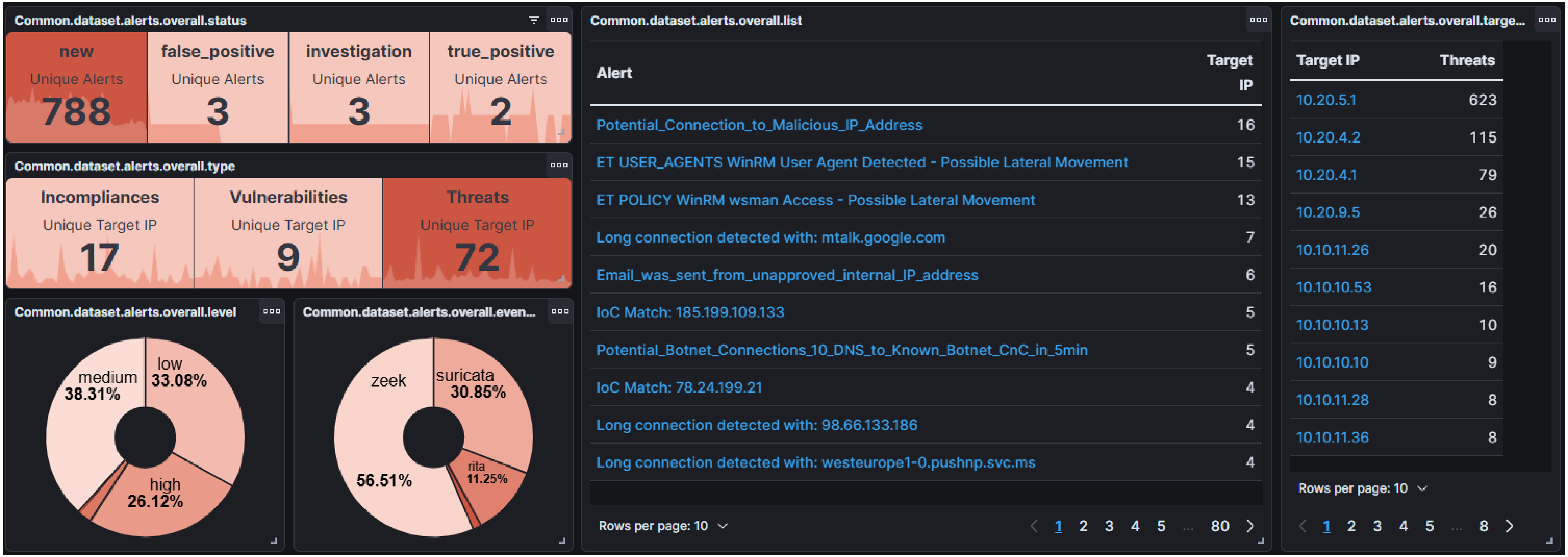
Export

Observer	Count
sen01-01b	14593
sen01-02a	57191
sen01-07a	2950
sen01-09a	14819
sen01-11a	62433
sen01-12a	398203
sen01-13b	36911
sen01-14a	142486
sen01-17a	8448
sen01-18a	6960
soho-2	2455

Network.dataset.services.count.over.time

Network.dataset.alert.threats.heatmap

Centralized Alerts Handling



Common.dataset.alerts.overall.status

new	false_positive	investigation	true_positive
Unique Alerts	Unique Alerts	Unique Alerts	Unique Alerts
788	3	3	2

Common.dataset.alerts.overall.type

Incompliances	Vulnerabilities	Threats
Unique Target IP	Unique Target IP	Unique Target IP
17	9	72

Common.dataset.alerts.overall.level

Common.dataset.alerts.overall.even...

Common.dataset.alerts.overall.list

Alert	Target IP
Potential_Connection_to_Malicious_IP_Address	16
ET USER_AGENTS WinRM User Agent Detected - Possible Lateral Movement	15
ET POLICY WinRM wsman Access - Possible Lateral Movement	13
Long connection detected with: mtalk.google.com	7
Email_was_sent_from_unapproved_internal_IP_address	6
IoC Match: 185.199.109.133	5
Potential_Botnet_Connections_10_DNS_to_Known_Botnet_CnC_in_5min	5
IoC Match: 78.24.199.21	4
Long connection detected with: 98.66.133.186	4
Long connection detected with: westeurope1-0.pushnp.svc.ms	4

Rows per page: 10

1 2 3 4 5 ... 80

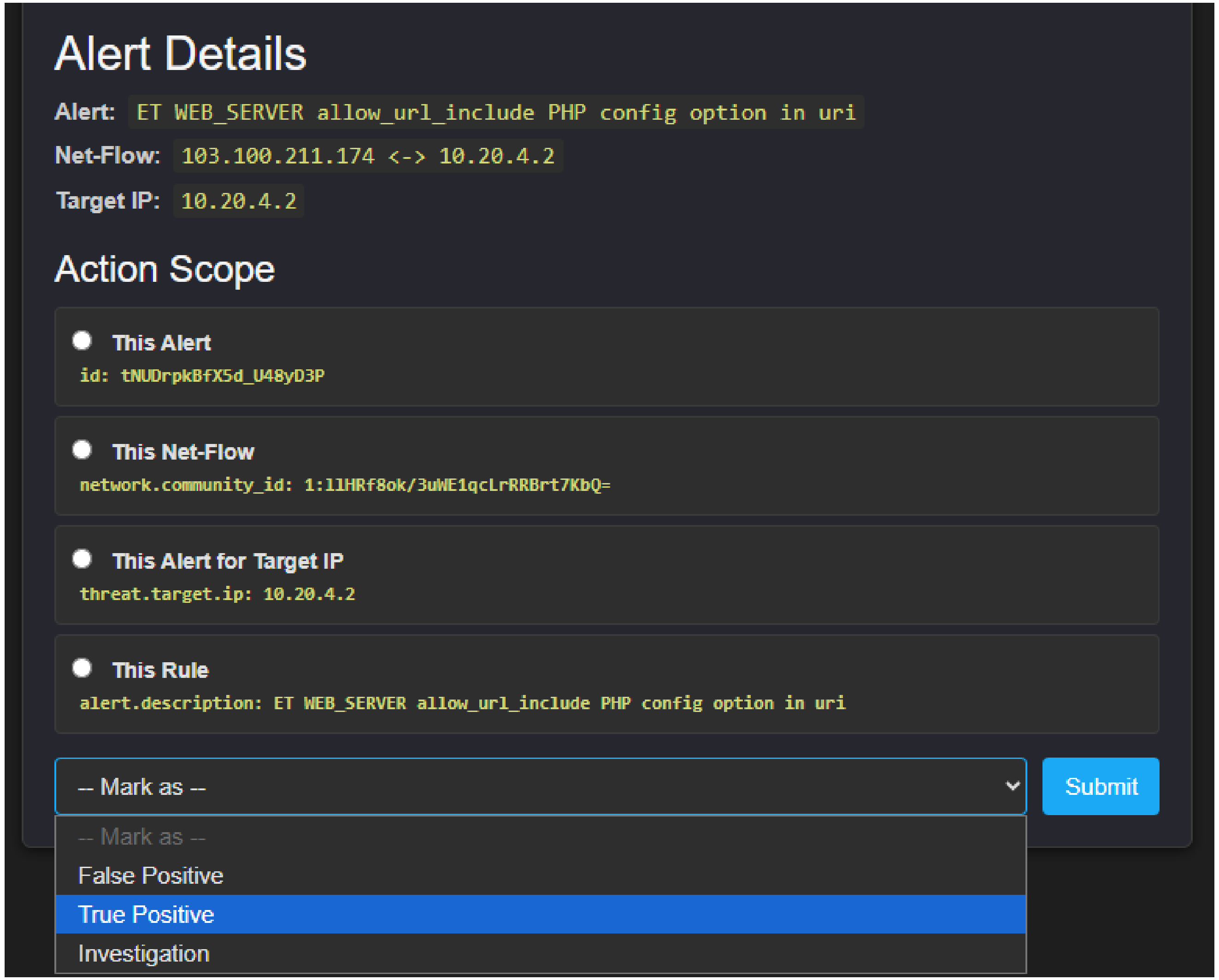
Common.dataset.alerts.overall.targe...

Target IP	Threats
10.20.5.1	623
10.20.4.2	115
10.20.4.1	79
10.20.9.5	26
10.10.11.26	20
10.10.10.53	16
10.10.10.13	10
10.10.10.10	9
10.10.11.28	8
10.10.11.36	8

Rows per page: 10

1 2 3 4 5 ... 8

Alert Classification



Alert Details

Alert: `ET WEB_SERVER allow_url_include PHP config option in uri`

Net-Flow: `103.100.211.174 <-> 10.20.4.2`

Target IP: `10.20.4.2`

Action Scope

○ **This Alert**

`id: tNUDrpkBfX5d_U48yD3P`

○ **This Net-Flow**

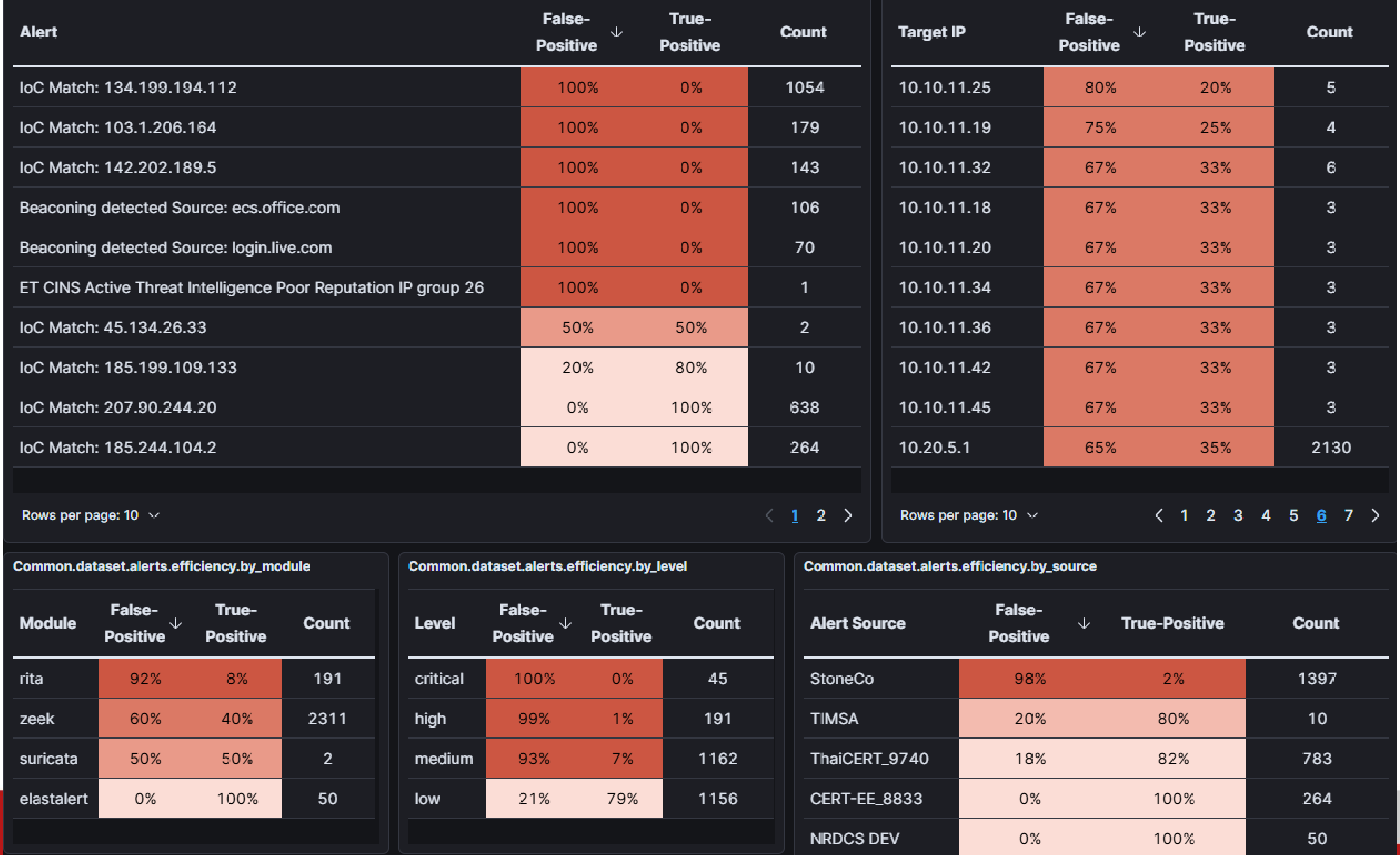
`network.community_id: 1:1lHRf8ok/3uWE1qcLrRRBrt7KbQ=`

○ **This Alert for Target IP**

`threat.target.ip: 10.20.4.2`

○ **This Rule**

`alert.description: ET WEB_SERVER allow_url_include PHP config option in uri`



Alert	False-Positive ↓	True-Positive	Count
IoC Match: 134.199.194.112	100%	0%	1054
IoC Match: 103.1.206.164	100%	0%	179
IoC Match: 142.202.189.5	100%	0%	143
Beaconing detected Source: ecs.office.com	100%	0%	106
Beaconing detected Source: login.live.com	100%	0%	70
ET CINS Active Threat Intelligence Poor Reputation IP group 26	100%	0%	1
IoC Match: 45.134.26.33	50%	50%	2
IoC Match: 185.199.109.133	20%	80%	10
IoC Match: 207.90.244.20	0%	100%	638
IoC Match: 185.244.104.2	0%	100%	264

Rows per page: 10

‹ 1 2 ›

Target IP	False-Positive ↓	True-Positive	Count
10.10.11.25	80%	20%	5
10.10.11.19	75%	25%	4
10.10.11.32	67%	33%	6
10.10.11.18	67%	33%	3
10.10.11.20	67%	33%	3
10.10.11.34	67%	33%	3
10.10.11.36	67%	33%	3
10.10.11.42	67%	33%	3
10.10.11.45	67%	33%	3
10.20.5.1	65%	35%	2130

Rows per page: 10

‹ 1 2 3 4 5 6 7 ›

Common.dataset.alerts.efficiency.by_module

Module	False-Positive ↓	True-Positive	Count
rita	92%	8%	191
zeek	60%	40%	2311
suricata	50%	50%	2
elastalert	0%	100%	50

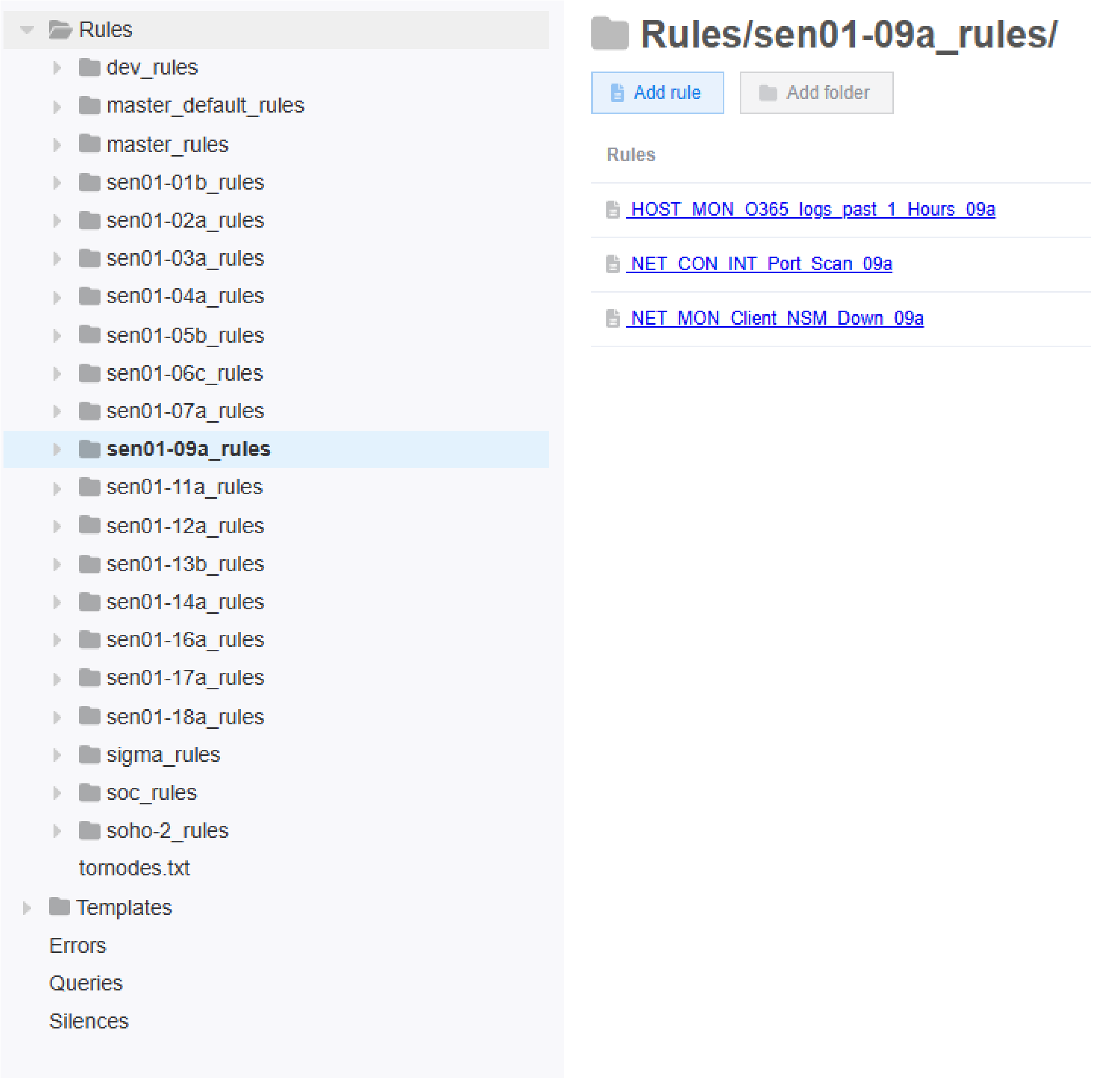
Common.dataset.alerts.efficiency.by_level

Level	False-Positive ↓	True-Positive	Count
critical	100%	0%	45
high	99%	1%	191
medium	93%	7%	1162
low	21%	79%	1156

Common.dataset.alerts.efficiency.by_source

Alert Source	False-Positive ↓	True-Positive	Count
StoneCo	98%	2%	1397
TIMSA	20%	80%	10
ThaiCERT_9740	18%	82%	783
CERT-EE_8833	0%	100%	264
NRDCS DEV	0%	100%	50

Centralized CTI Management

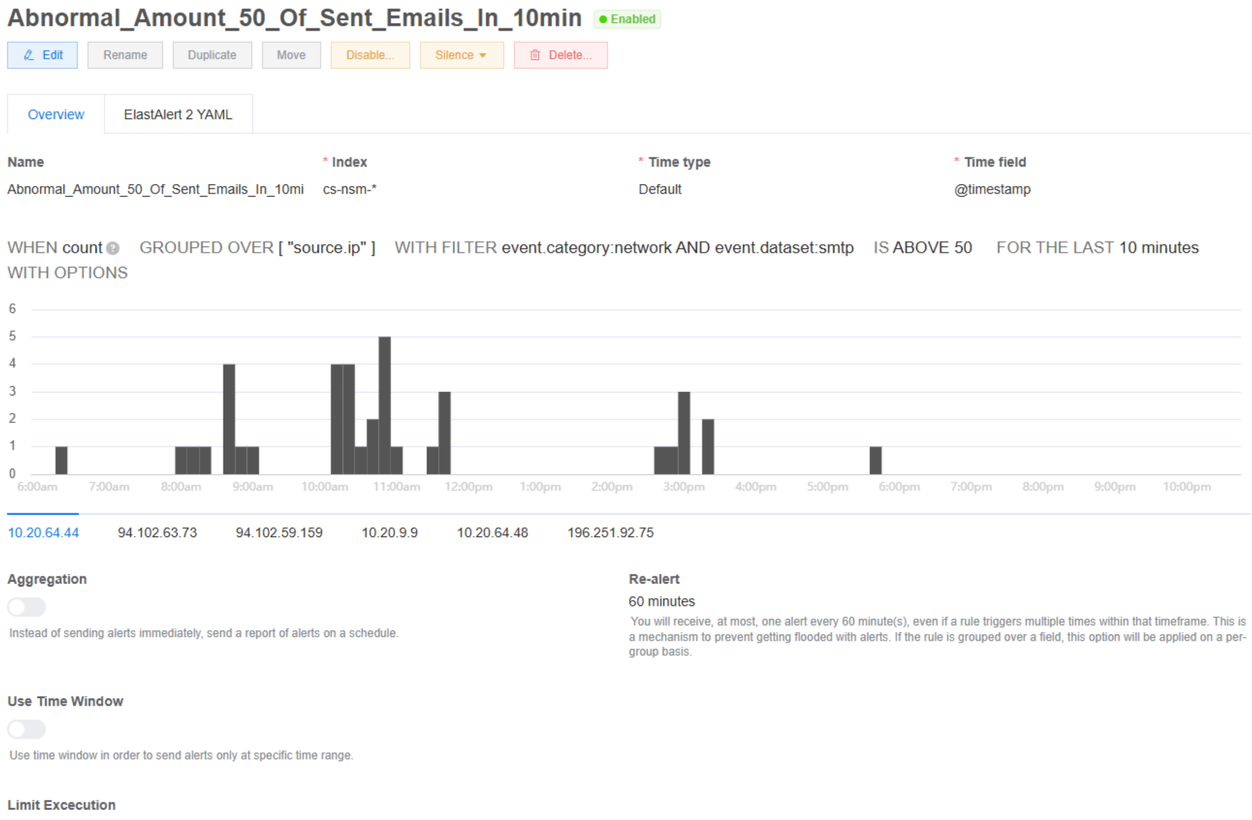


- Rules
  - dev_rules
  - master_default_rules
  - master_rules
  - sen01-01b_rules
  - sen01-02a_rules
  - sen01-03a_rules
  - sen01-04a_rules
  - sen01-05b_rules
  - sen01-06c_rules
  - sen01-07a_rules
  - **sen01-09a_rules**
  - sen01-11a_rules
  - sen01-12a_rules
  - sen01-13b_rules
  - sen01-14a_rules
  - sen01-16a_rules
  - sen01-17a_rules
  - sen01-18a_rules
  - sigma_rules
  - soc_rules
  - soho-2_rules
  - tornodes.txt
- Templates
- Errors
- Queries
- Silences

Rules/sen01-09a_rules/

Rules

- HOST_MON_O365_logs_past_1_Hours_09a
- NET_CON_INT_Port_Scan_09a
- NET_MON_Client_NSM_Down_09a



Name	* Index	* Time type	* Time field
Abnormal_Amount_50_Of_Sent_Emails_In_10mi	cs-nsm-*	Default	@timestamp

WHEN count GROUPED OVER ["source.ip"] WITH FILTER event.category:network AND event.dataset:smtp IS ABOVE 50 FOR THE LAST 10 minutes
WITH OPTIONS

Aggregation

Instead of sending alerts immediately, send a report of alerts on a schedule.

Re-alert

60 minutes

You will receive, at most, one alert every 60 minute(s), even if a rule triggers multiple times within that timeframe. This is a mechanism to prevent getting flooded with alerts. If the rule is grouped over a field, this option will be applied on a per-group basis.

Use Time Window

Use time window in order to send alerts only at specific time range.

Limit Excecution

Key to Success

- Centralized monitoring – all customers in 1 console
- Centralized Rule deployment
- Centralyzed Threat Hunting
- Centralized patching and updates

Questions & Answers

Arūnas Venclovas

ARV@NRDCS.LT

Whatsapp: +370 618 83 102

Linkedin:

https://www.linkedin.com/in/arunasvenclovas/

2026
FIRST Regional Symposium Central Asia

Tashkent, UZ
February 26-27

Thank You!

Rahmat!

Ačiū!

FIRST™
Improving Security Together