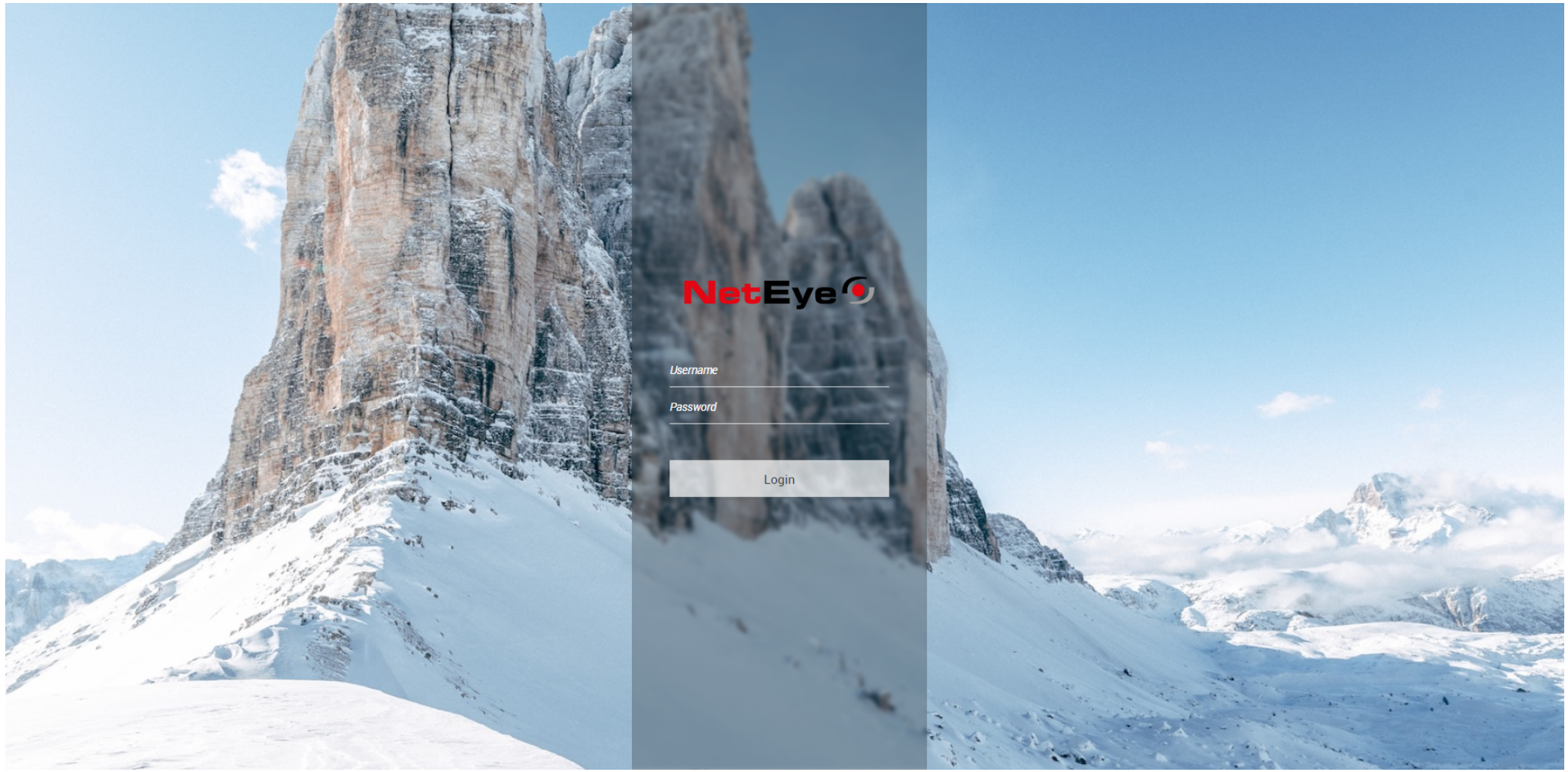

LIVE MEETING
NetEye
5. Mai 2020

NETEYE SIEM



NetEye

- UNIFIED MONITORING -

MONITORING – VISIBILITY - OBSERVABILITY

UNIFIED MONITORING
AVAILABILITY
SERVICE LEVEL MANAGEMENT

- Unified Monitoring
- Business Service Monitoring
- Distributed Monitoring
- Iot – IIoT Monitoring
- Asset Management
- Visual Synthetic Monitoring Alyvix
- Web Automation Monitoring

IT OPERATION ANALYTICS
APM
END2END

- Real User Experience
- User Experience
- IT Operation Analytics
- Application Performance Management
- Anomaly Detection
- Forecasting - Prediction
- Machine Learning

GDPR – SECURITY
LOG MGMT
SIEM

- Log Management
- Anomlay Detection
- SIEM
- Machine Learning

SERVICE & SUPPORT
SERVICE MANAGEMENT
TICKETING

- Jira Service Desk
- Confluence
- Ops Genie
- ITIL Consulting
- ServiceDesk

on premises – Hybrid – Cloud – Cloud SaaS

NetEye

MONITORING – VISIBILITY - OBSERVABILITY

UNIFIED MONITORING
AVAILABILITY
SERVICE LEVEL MANAGEMENT

IT OPERATION ANALYTICS
APM
END2END

GDPR – SECURITY
LOG MANAGEMENT
SIEM

SERVICE & SUPPORT
SERVICE MANAGEMENT
TICKETING

ICINGA
ntop
InfluxDB
Grafana
elastic
ATLASSIAN
Jira Service Desk
Confluence
Opsgenie
GLPI
OCS inventory NG
elastic
NXLog

CentOS
redhat

strong technology partnership to drive innovation

LOG ANALYTICS CHALLANGES

- Analyzing Logs for Relevant Security Intelligence
- Centralizing Log Collection
- Meeting IT Compliance Requirements
- Conducting Effective Root Cause Analysis
- Making Log Data More Meaningful
- Tracking Suspicious User Behavior

N4 siem *_sub

DATA INGESTION

INGEST FROM ANYWHERE

Applications Web apps, servers, APIs log4j, JMX Twitter, Salesforce, Github	**Platform Infrastructure** Windows, Linux/Unix, MacOS Load balancers, proxies, caches S3, HDFS
Containers & Cloud Docker, Kubernetes AWS, Azure, GCP Openshift	**Data Stores & Streams** DBs, Data Warehouses NoSQL Kafka, Spark, Storm, Hive
Networking Netflow, PCAP HTTP, TCP, UDP, DNS, TLS syslog, auditd	**Security Devices** NSM, IDS/IPS, firewalls Web proxies, endpoints ArcSight
Messaging & Alerting Slack, HipChat Pagerduty, Email Nagios, Zabbix	**Raw Documents** PDF, XLS, PPT Technical, legal, healthcare documents
IoT Sensors, robots Connected cars Smart homes	**Build Your Own**

45

Logs

Metrics

Configs

Messages

Scripts

Tickets

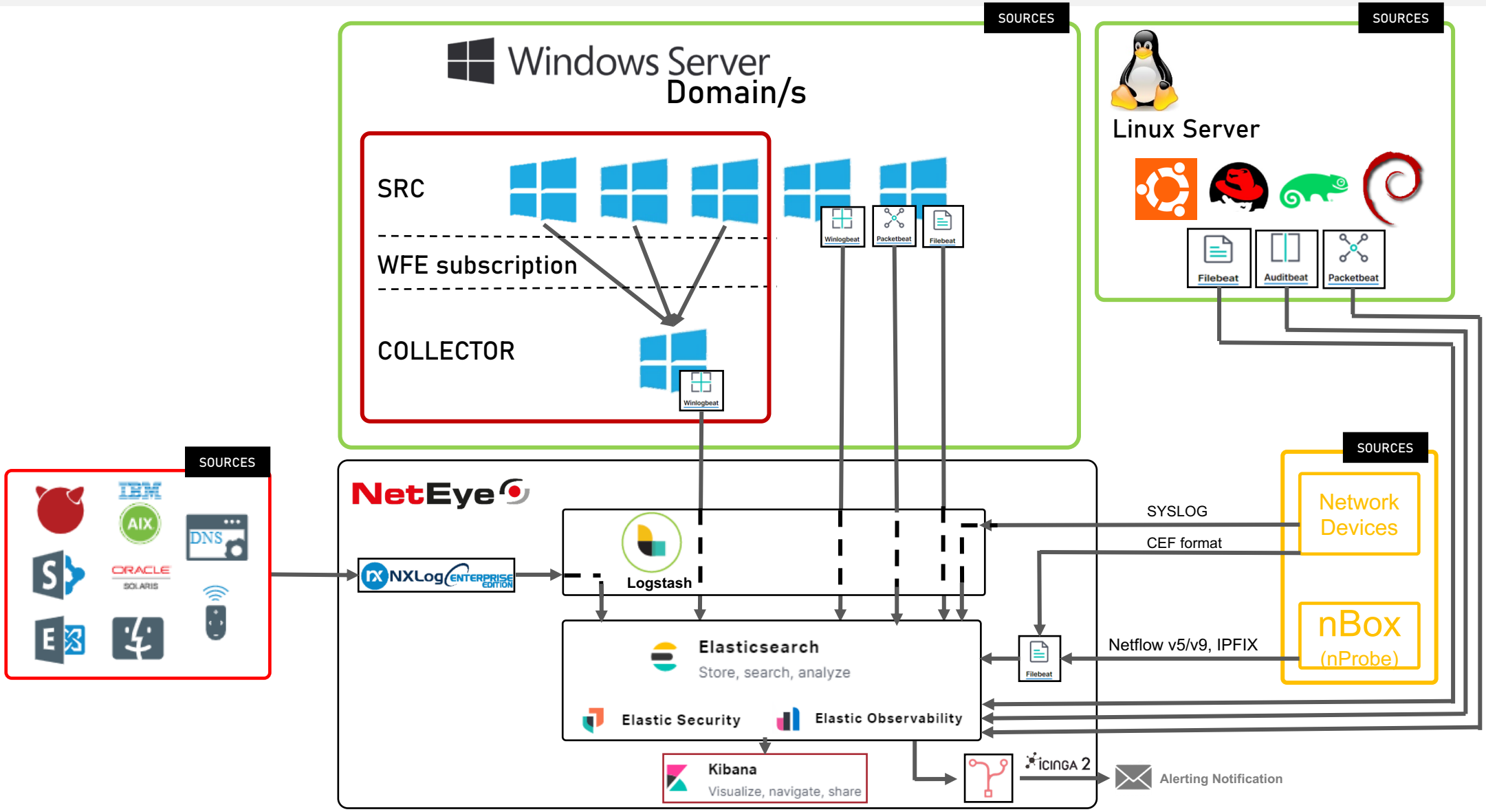
Alerts

NetEye

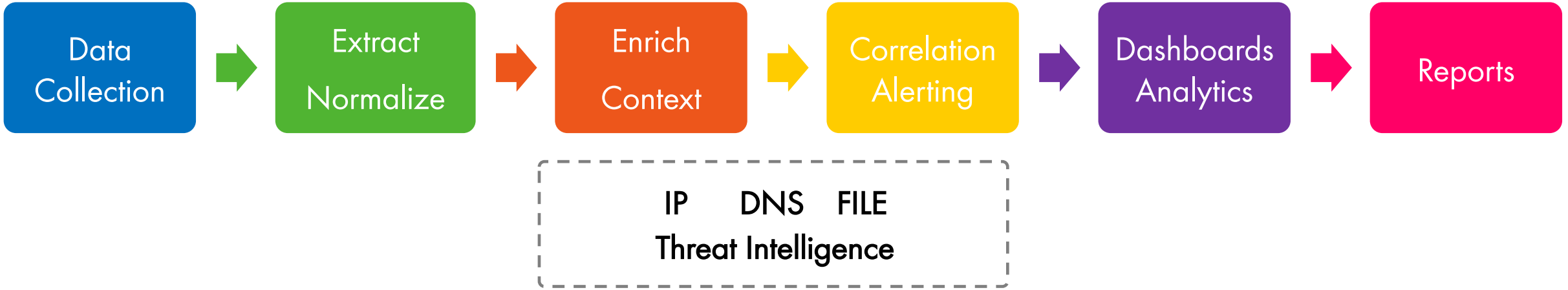
Ingest Integrations

The Elastic Stack

INGEST FROM ANYWHERE – USE CASE



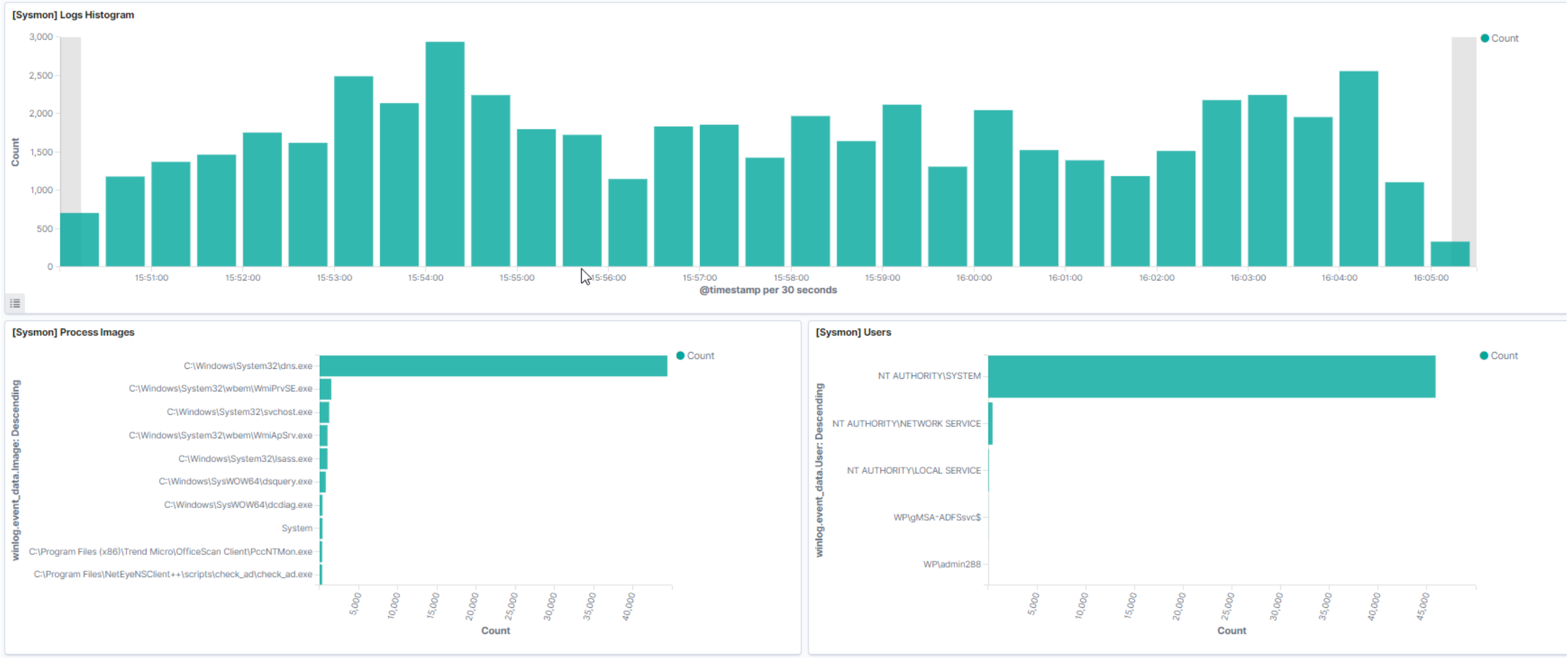
SIEM FLOW



N4 siem *_sub

DATA VISUALIZATION

SYSMON LOGS

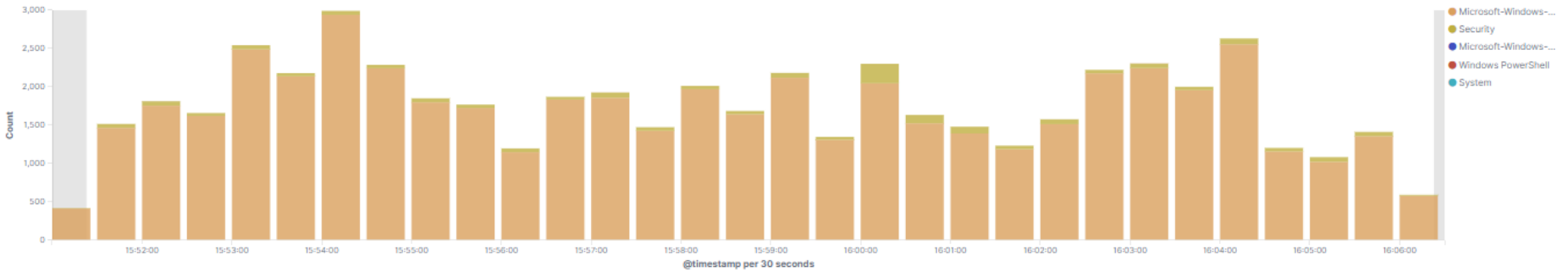

[Sysmon] Logs Histogram
Count
3,000
2,500
2,000
1,500
1,000
500
0
15:51:00
15:52:00
15:53:00
15:54:00
15:55:00
15:56:00
15:57:00
15:58:00
15:59:00
16:00:00
16:01:00
16:02:00
16:03:00
16:04:00
16:05:00
@timestamp per 30 seconds
[Sysmon] Process Images
winlog.event_data.Image: Descending
C:\Windows\System32\dns.exe
C:\Windows\System32\wbem\WmiPrvSE.exe
C:\Windows\System32\svchost.exe
C:\Windows\System32\wbem\WmiApSrv.exe
C:\Windows\System32\lsass.exe
C:\Windows\SysWOW64\dsquery.exe
C:\Windows\SysWOW64\dcdiag.exe
System
C:\Program Files (x86)\Trend Micro\OfficeScan Client\PccNTMon.exe
C:\Program Files\NetEyeNSClient++\scripts\check_ad\check_ad.exe
5,000
10,000
15,000
20,000
25,000
30,000
35,000
40,000
Count
[Sysmon] Users
winlog.event_data.User: Descending
NT AUTHORITY\SYSTEM
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\LOCAL SERVICE
WP\gMSA-ADFSsvc$
WP\admin288
5,000
10,000
15,000
20,000
25,000
30,000
35,000
40,000
45,000
Count

WINDOWS EVENTS OVERVIEW

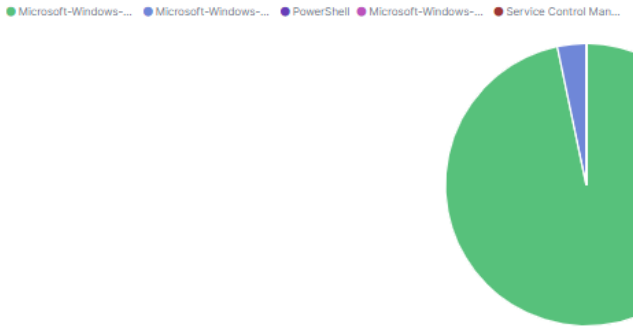
Number of Events

54,455
Count

Number of Events Over Time By Event Log



Sources



Top Event IDs

winlog.event_id: Descending	Count
3	46,448
7	4,871
4624	1,324
18	999
4634	206
5140	141
17	105
1	100
4648	89
5	52

Export: Raw Formatted

Event Levels

log.level: Descending	Count
information	54,455

Export: Raw Formatted

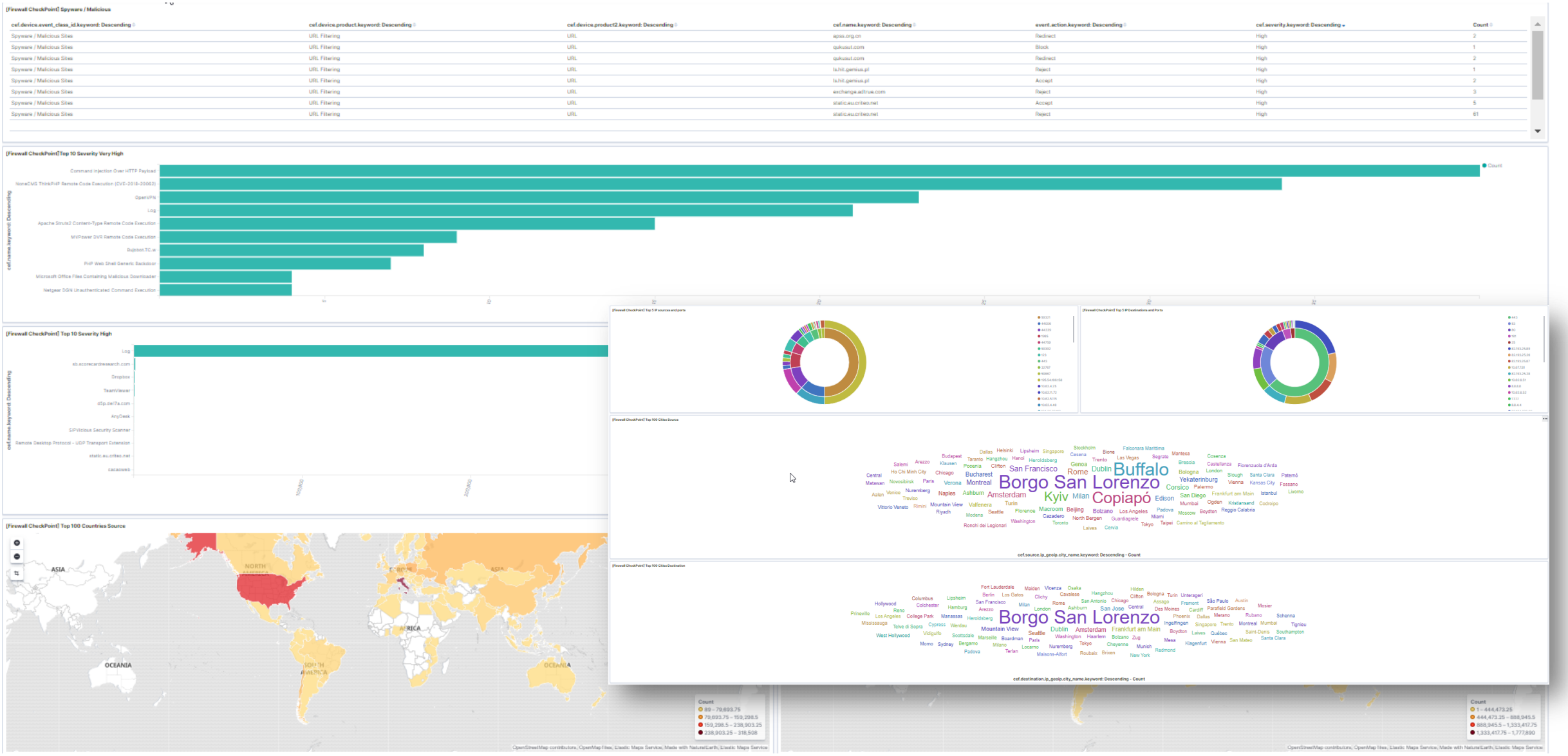
[Winlogbeat] - Table user-event

user	event_id	Count
xphxcitrixldapro	4624	703
xphxneteye3ldapro	4624	184
bz_mailbox_03	4624	56
bz_mailbox_03	4648	56
PBZFS02$	4634	44
PBZFS02$	4624	40
PBZDC01$	4624	40
PBZDC01$	4634	39
PBZADFS02$	4634	40
PBZADFS02$	4624	37
PBZADFS01$	4624	31
PBZADFS01$	4634	29

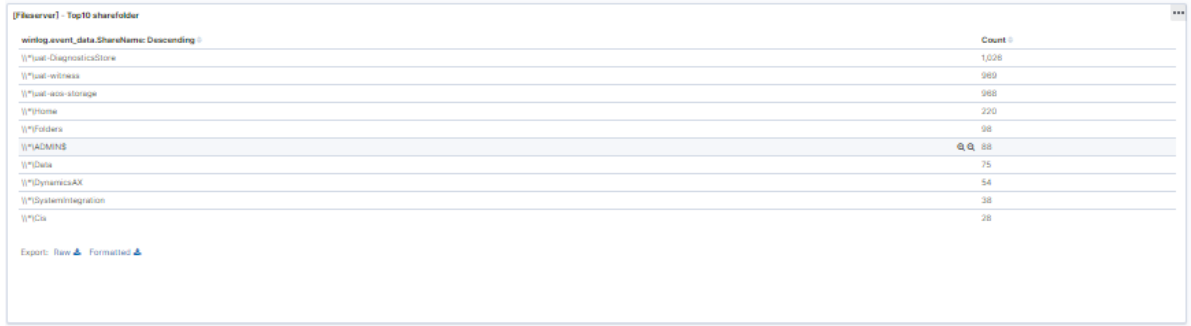
Table user-event-audit

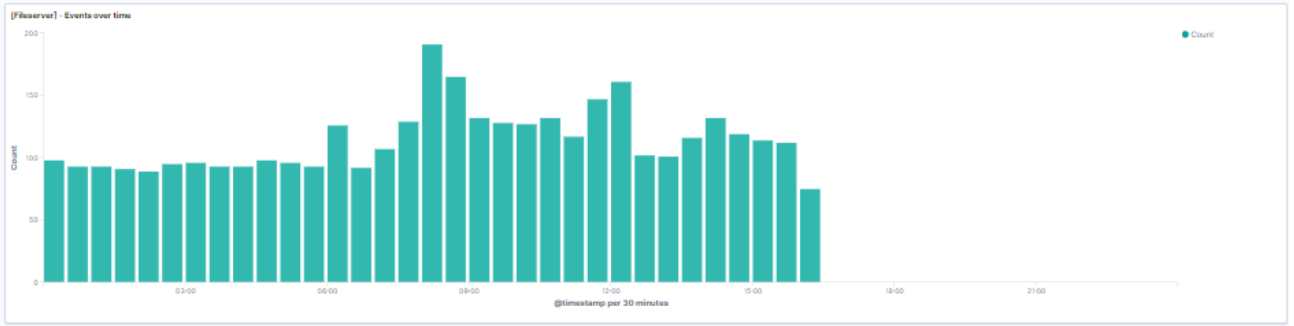
user	event_id	audit	action	Count
PBZFS02$	4634	Audit Success	Logoff	44
PBZFS02$	4624	Audit Success	Logon	40
PBZDC01$	4624	Audit Success	Logon	40
PBZDC01$	4634	Audit Success	Logoff	39
PBZADFS02$	4634	Audit Success	Logoff	40
PBZADFS02$	4624	Audit Success	Logon	37
PBZADFS01$	4624	Audit Success	Logon	31
PBZADFS01$	4634	Audit Success	Logoff	29
PRMDC03$	4634	Audit Success	Logoff	37
PRMDC03$	4624	Audit Success	Logon	23
PBZDC02$	4624	Audit Success	Logon	33
PBZDC02$	4634	Audit Success	Logoff	17

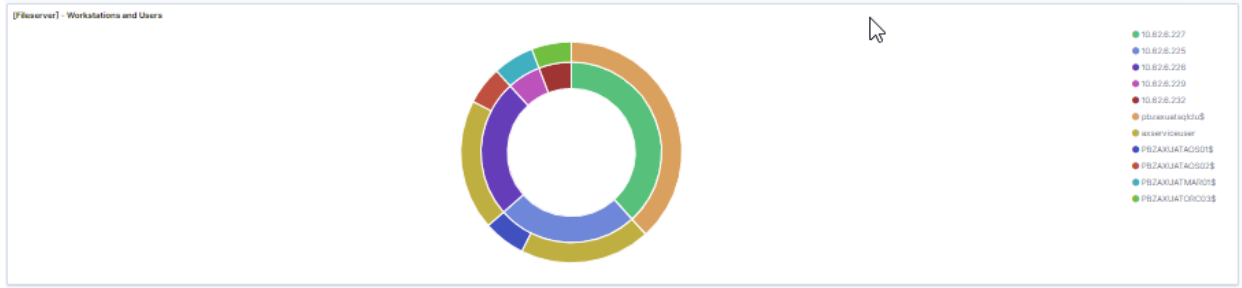
FIREWALL OVERVIEW

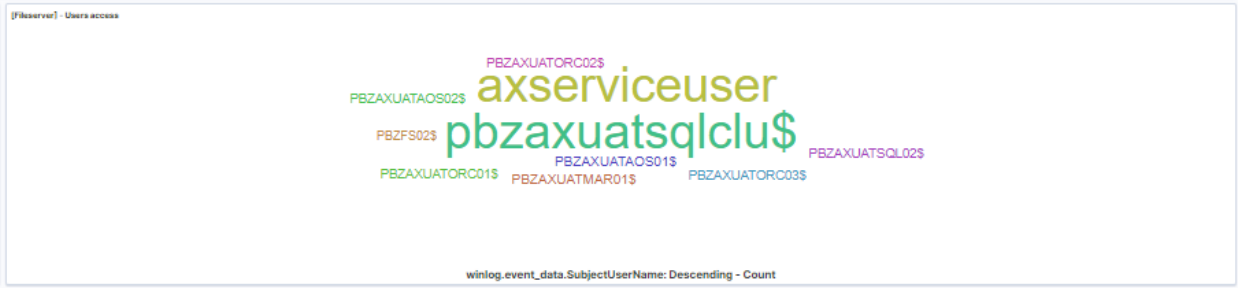


FILESERVER OVERVIEW







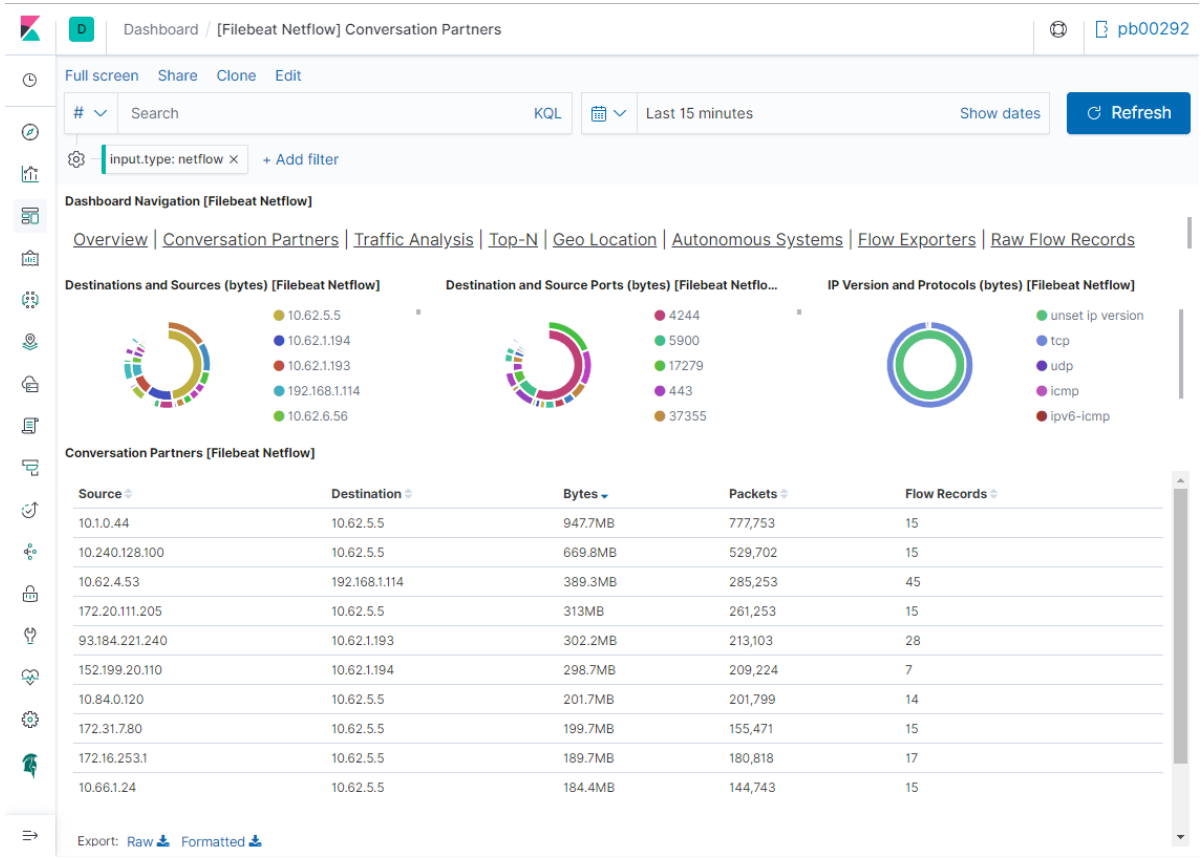


NetFlow Network Visibility

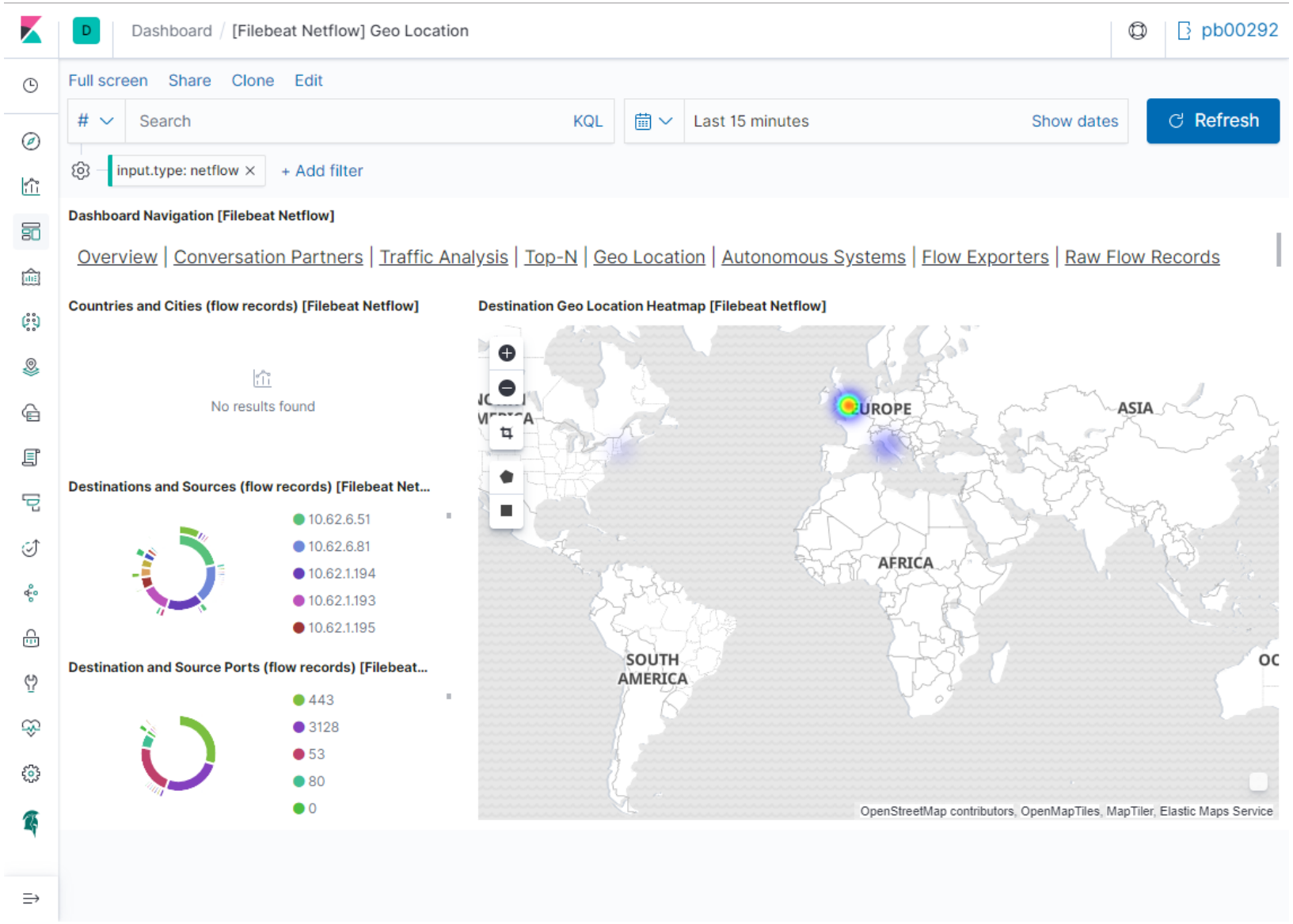
N4 core *_sub

NETWORK VISIBILITY

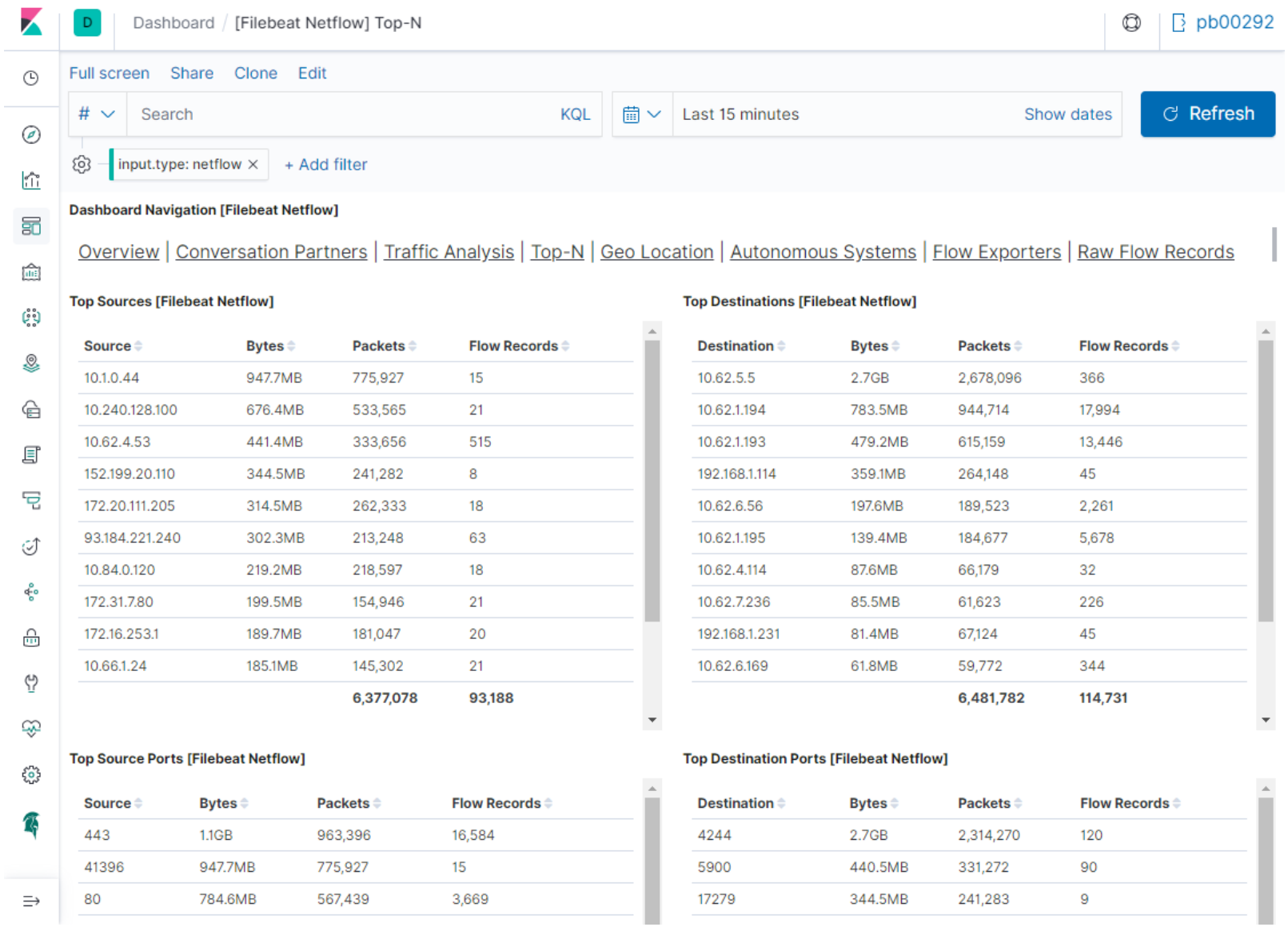
- Support to receive NetFlow v5, v9, IPFIX through Elastic 7.4
  - Collects NetFlow input from compliant network devices
  - Provides details about the traffic traversing a network
  - Built-in dashboards for Kibana
  - ECS-compliant data



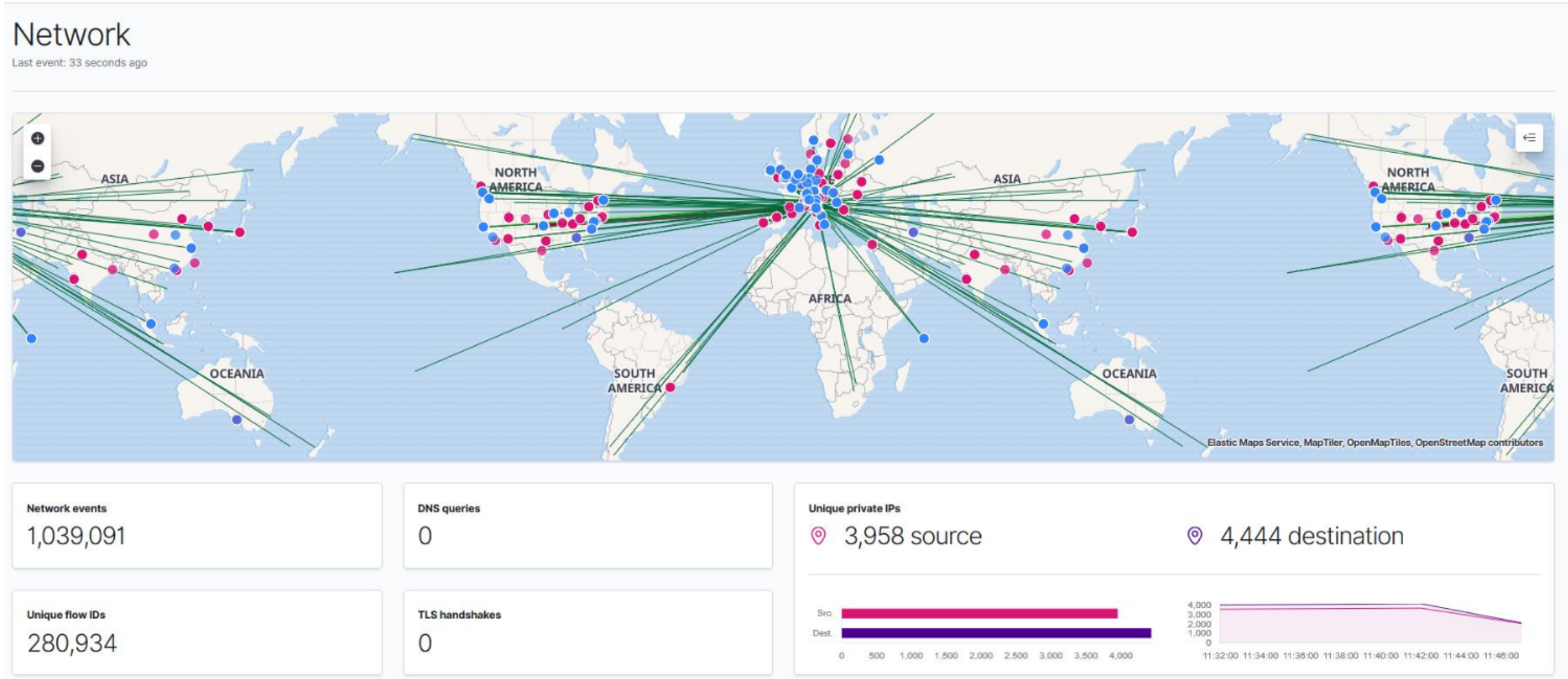
NETFLOW DASHBOARDS



NETFLOW DASHBOARDS



NETFLOW DASHBOARD (SIEM)



NETFLOW DASHBOARD (SIEM)

Source IPs

Showing: 7,640 IPs

IP	Domain	Autonomous system	Bytes in	Bytes out ↓	Flows	Destination I...
0.0.0.0	—	—	0B	0B	6	6
1.0.0.1 AU AU	—	Cloudflare, Inc. 13335	0B	0B	33	28
1.4.179.246 TH TH	—	TOT Public Company Limited 23969	0B	0B	1	1
1.34.57.14 TW TW	—	Data Communication Business Group 3462	0B	0B	1	1
1.34.158.234 TW TW	—	Data Communication Business Group 3462	0B	0B	1	1
1.34.227.58 TW TW	—	Data Communication Business Group 3462	0B	0B	1	1
1.53.67.32 VN VN	—	The Corporation for Financing & Promoting Technology 18403	0B	0B	3	1
1.53.86.115 VN VN	—	The Corporation for Financing & Promoting Technology 18403	0B	0B	1	1
1.53.129.132 VN VN	—	The Corporation for Financing & Promoting Technology 18403	0B	0B	3	1
1.64.189.213 HK HK	—	PCCW Limited 4760	0B	0B	1	1

Destination IPs

Showing: 7,871 IPs

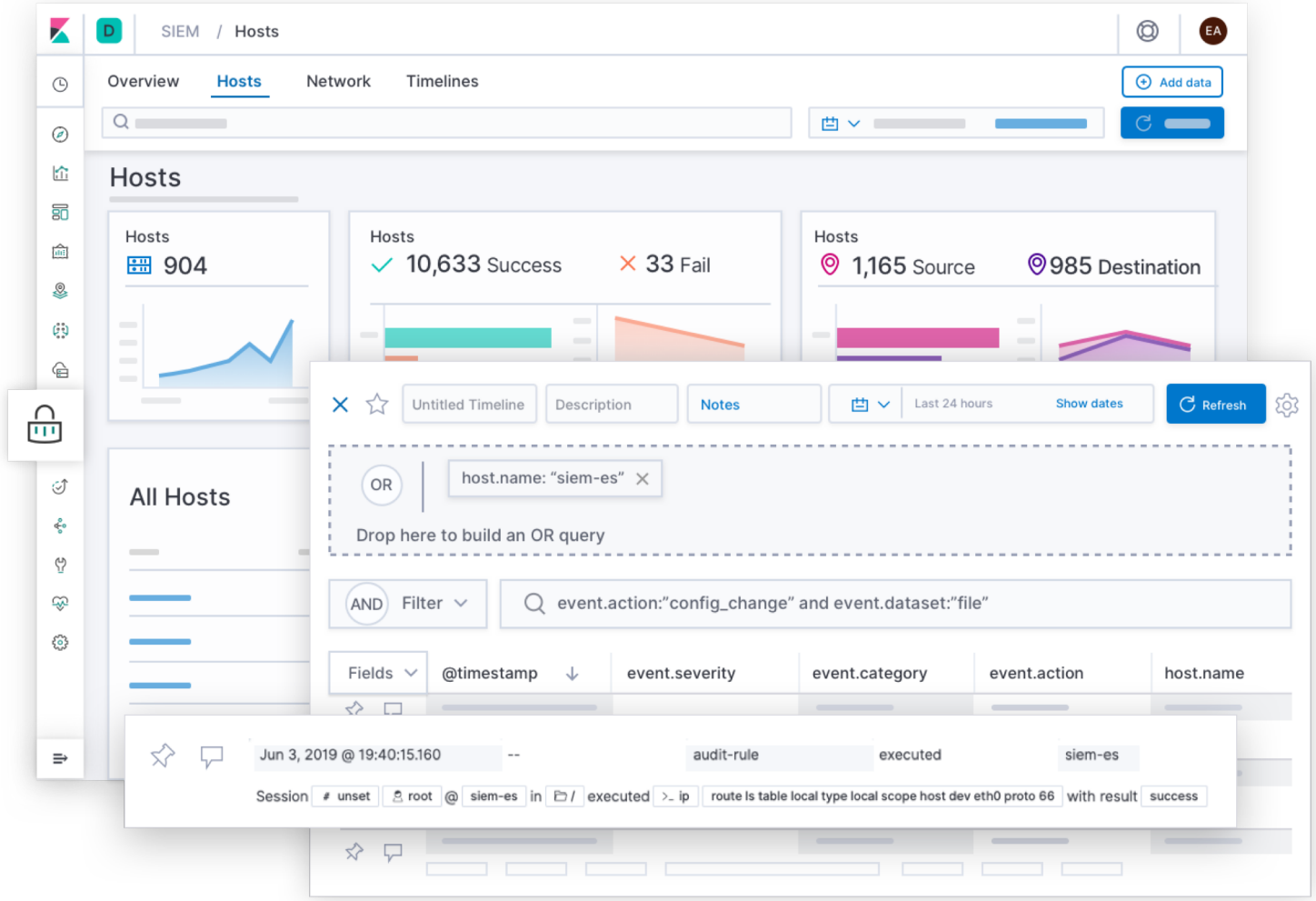
IP	Domain	Autonomous system	Bytes in	Bytes out ↓	Flows	Source IPs
1.0.0.1 AU AU	—	Cloudflare, Inc. 13335	0B	0B	32	28
1.53.129.132 VN VN	—	The Corporation for Financing & Promoting Technology 18403	0B	0B	1	1
2.16.200.34	—	Akamai Technologies, Inc. 16625	0B	0B	3	1
2.18.213.58	—	Akamai International B.V. 20940	0B	0B	3	1
2.20.226.209	—	Telecom Italia 3269	0B	0B	4	1
2.20.231.105	—	Telecom Italia 3269	0B	0B	2	2
2.20.233.122	—	Telecom Italia 3269	0B	0B	15	4
2.20.234.225	—	Telecom Italia 3269	0B	0B	120	16
2.20.235.226	—	Telecom Italia 3269	0B	0B	2	2
2.20.239.86	—	Telecom Italia 3269	0B	0B	1	1

Rows per page: 10 ⌄

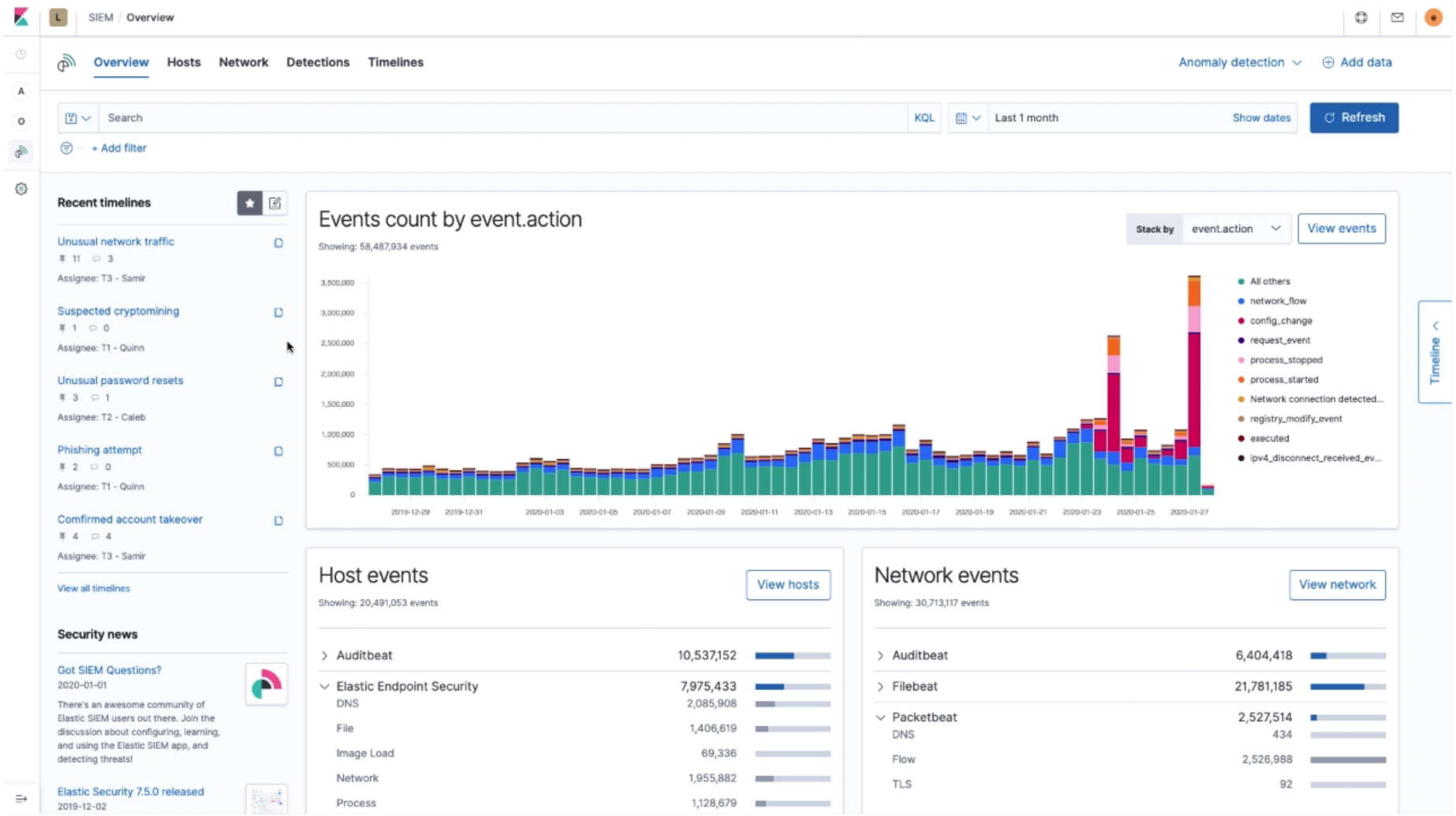
‹ 1 2 3 4 5 ... ›

DATA CORRELATION

SIEM APP

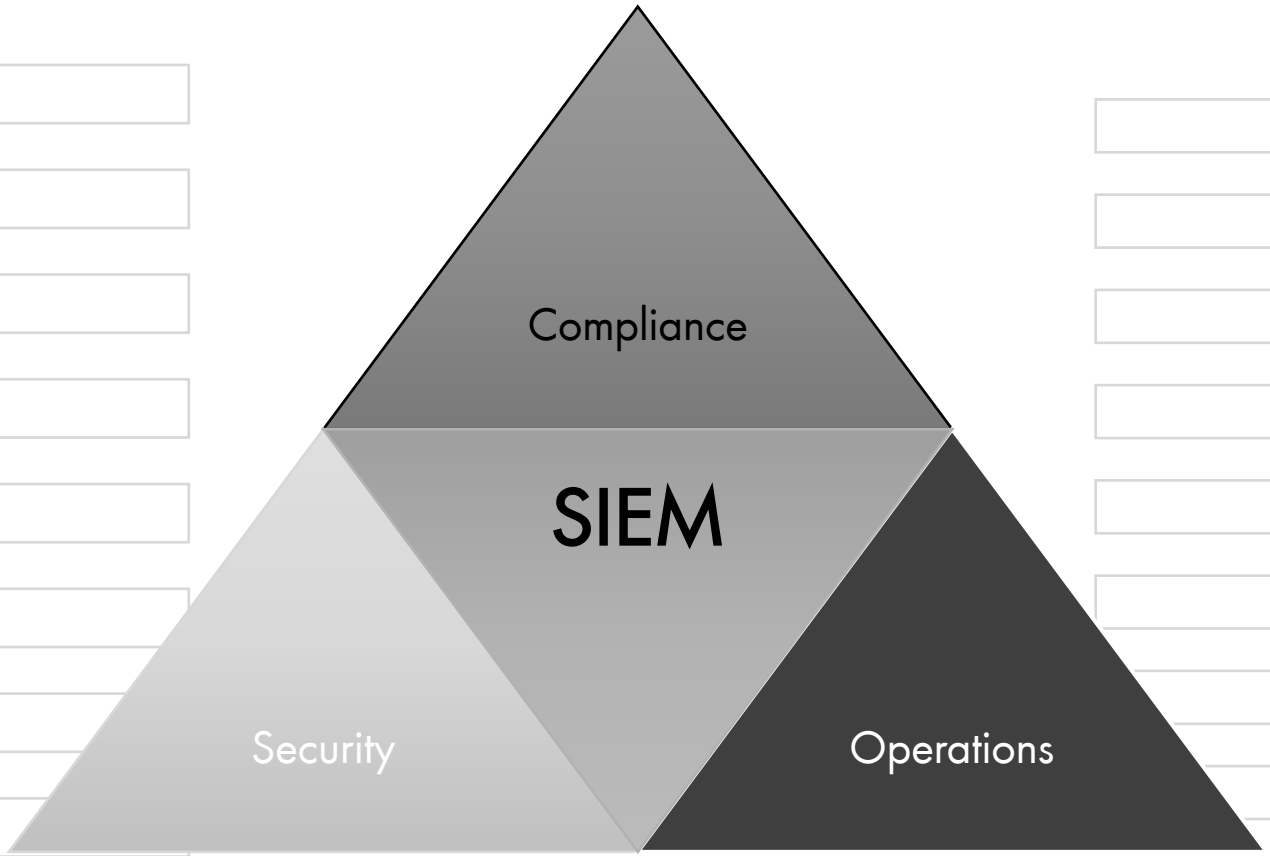

SIEM / Hosts
Overview
Hosts
Network
Timelines
Add data
Hosts
Hosts
904
Hosts
10,633 Success
33 Fail
Hosts
1,165 Source
985 Destination
All Hosts
Untitled Timeline
Description
Notes
Last 24 hours
Show dates
Refresh
OR
host.name: "siem-es"
Drop here to build an OR query
AND
Filter
event.action:"config_change" and event.dataset:"file"
Fields
@timestamp
event.severity
event.category
event.action
host.name
Jun 3, 2019 @ 19:40:15.160
--
audit-rule
executed
siem-es
Session
unset
root
@
siem-es
in
/
executed
ip
route ls table local type local scope host dev eth0 proto 66
with result
success

SIEM APP


SIEM / Overview
Overview
Hosts
Network
Detections
Timelines
Anomaly detection
Add data
Search
KQL
Last 1 month
Show dates
Refresh
+ Add filter
Recent timelines
Unusual network traffic
Assignee: T3 - Samir
Suspected cryptomining
Assignee: T1 - Quinn
Unusual password resets
Assignee: T2 - Caleb
Phishing attempt
Assignee: T1 - Quinn
Comfirmed account takeover
Assignee: T3 - Samir
View all timelines
Security news
Got SIEM Questions?
2020-01-01
There's an awesome community of Elastic SIEM users out there. Join the discussion about configuring, learning, and using the Elastic SIEM app, and detecting threats!
Elastic Security 7.5.0 released
2019-12-02
Events count by event.action
Showing: 58,487,934 events
Stack by
event.action
View events
All others
network_flow
config_change
request_event
process_stopped
process_started
Network connection detected...
registry_modify_event
executed
ipv4_disconnect_received_ev...
Timeline
Host events
Showing: 20,491,053 events
View hosts
Auditbeat 10,537,152
Elastic Endpoint Security 7,975,433
DNS 2,085,908
File 1,406,619
Image Load 69,336
Network 1,955,882
Process 1,128,679
Network events
Showing: 30,713,117 events
View network
Auditbeat 6,404,418
Filebeat 21,781,185
Packetbeat 2,527,514
DNS 434
Flow 2,526,988
TLS 92

VISION SIEM

- Log collection
- Log Analysis
- Event Correlation
- Log Forensic
- IT Compliance
- Application Log Monitoring
- Object Access Auditing
- Container Log Monitoring



- Real-time Alerting
- User Activity Monitoring
- Dashboard
- Reporting
- File Integrity Monitoring
- System & Device Log monitoring
- Object Access Auditing
- Cloud awareness


WWW.WUERTH-PHOENIX.COM
WWW.NETEYE-BLOG.COM