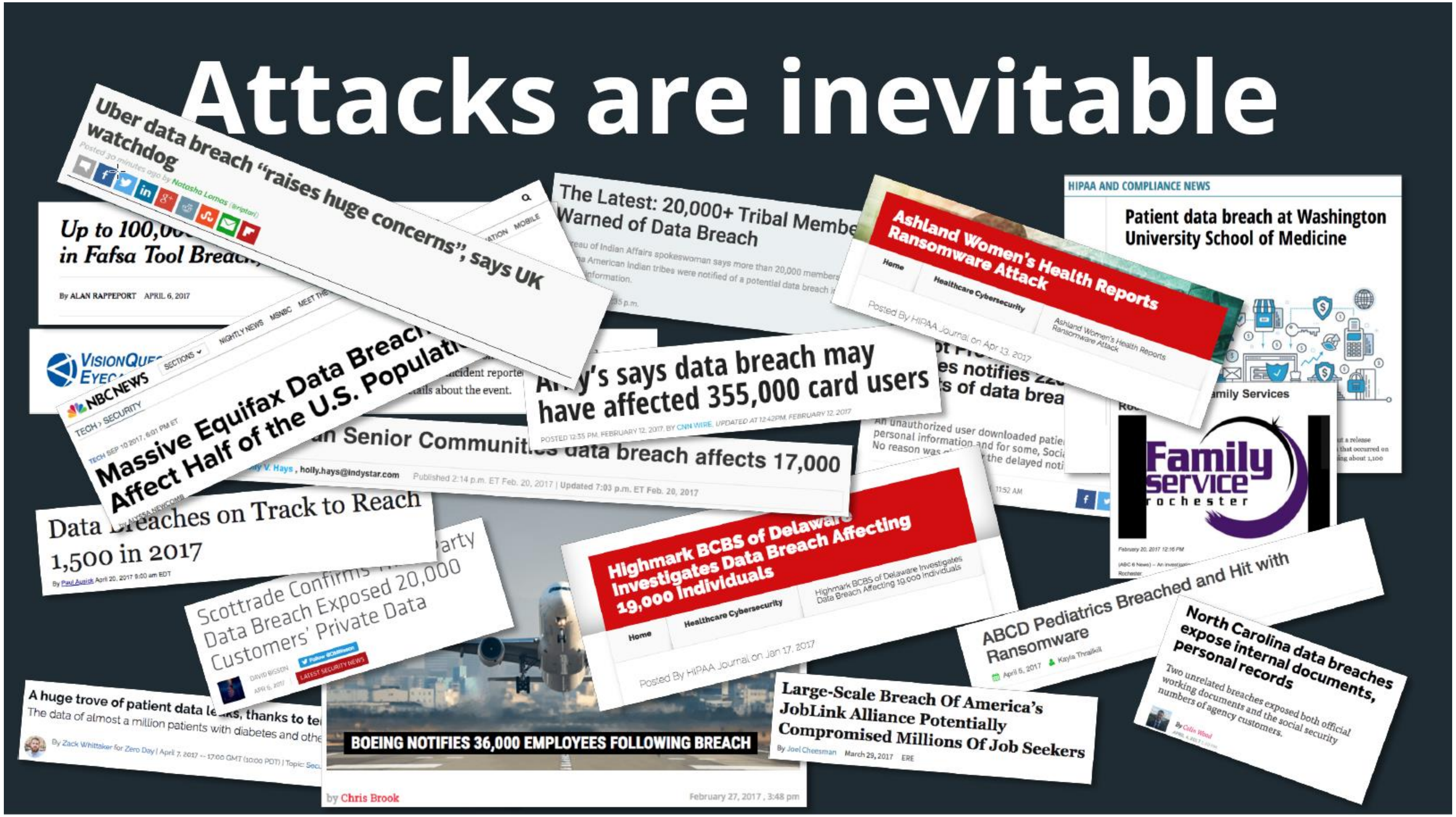
ENTERPRISE PERFORMANCE MONITORING NETEYE 4

Unified Monitoring und Security Information und Event Management

- NTOP and Würth Phoenix are long term partner (over 10 years)
  - Network monitoring and visibility
  - Integrate ntopng enterprise in NetEye 4
  - Vision NetEye 4 SIEM



Attacks are inevitable

Uber data breach "raises huge concerns", says UK watchdog

Posted 30 minutes ago by Natasha Lomas (@riptari)

Up to 100,00… in Fafsa Tool Breach

By ALAN RAPPEPORT APRIL 6, 2017

The Latest: 20,000+ Tribal Membe… Warned of Data Breach

Ashland Women's Health Reports Ransomware Attack

Home | Healthcare Cybersecurity | Ashland Women's Health Reports Ransomware Attack

Posted By HIPAA Journal on Apr 13, 2017

HIPAA AND COMPLIANCE NEWS

Patient data breach at Washington University School of Medicine

NBC NEWS

TECH > SECURITY

TECH SEP 10 2017, 6:01 PM ET

Massive Equifax Data Breach… Affect Half of the U.S. Population

Arby's says data breach may have affected 355,000 card users

POSTED 12:35 PM, FEBRUARY 12, 2017, BY CNN WIRE, UPDATED AT 12:42PM, FEBRUARY 12, 2017

…n Senior Communities data breach affects 17,000

Published 2:14 p.m. ET Feb. 20, 2017 | Updated 7:03 p.m. ET Feb. 20, 2017

Data Breaches on Track to Reach 1,500 in 2017

By Paul Ausick April 20, 2017 8:00 am EDT

Scottrade Confirms Third-Party Data Breach Exposed 20,000 Customers' Private Data

Highmark BCBS of Delaware Investigates Data Breach Affecting 19,000 Individuals

Home | Healthcare Cybersecurity | Highmark BCBS of Delaware Investigates Data Breach Affecting 19,000 Individuals

Posted By HIPAA Journal on Jan 17, 2017

Family Service Rochester

February 20, 2017 12:16 PM

ABCD Pediatrics Breached and Hit with Ransomware

April 6, 2017 Kayla Thrailkill

North Carolina data breaches expose internal documents, personal records

Two unrelated breaches exposed both official working documents and the social security numbers of agency customers.

By Colin Wood

A huge trove of patient data leaks, thanks to te…

The data of almost a million patients with diabetes and othe…

By Zack Whittaker for Zero Day | April 7, 2017 -- 17:00 GMT (10:00 PDT) | Topic: Secu…

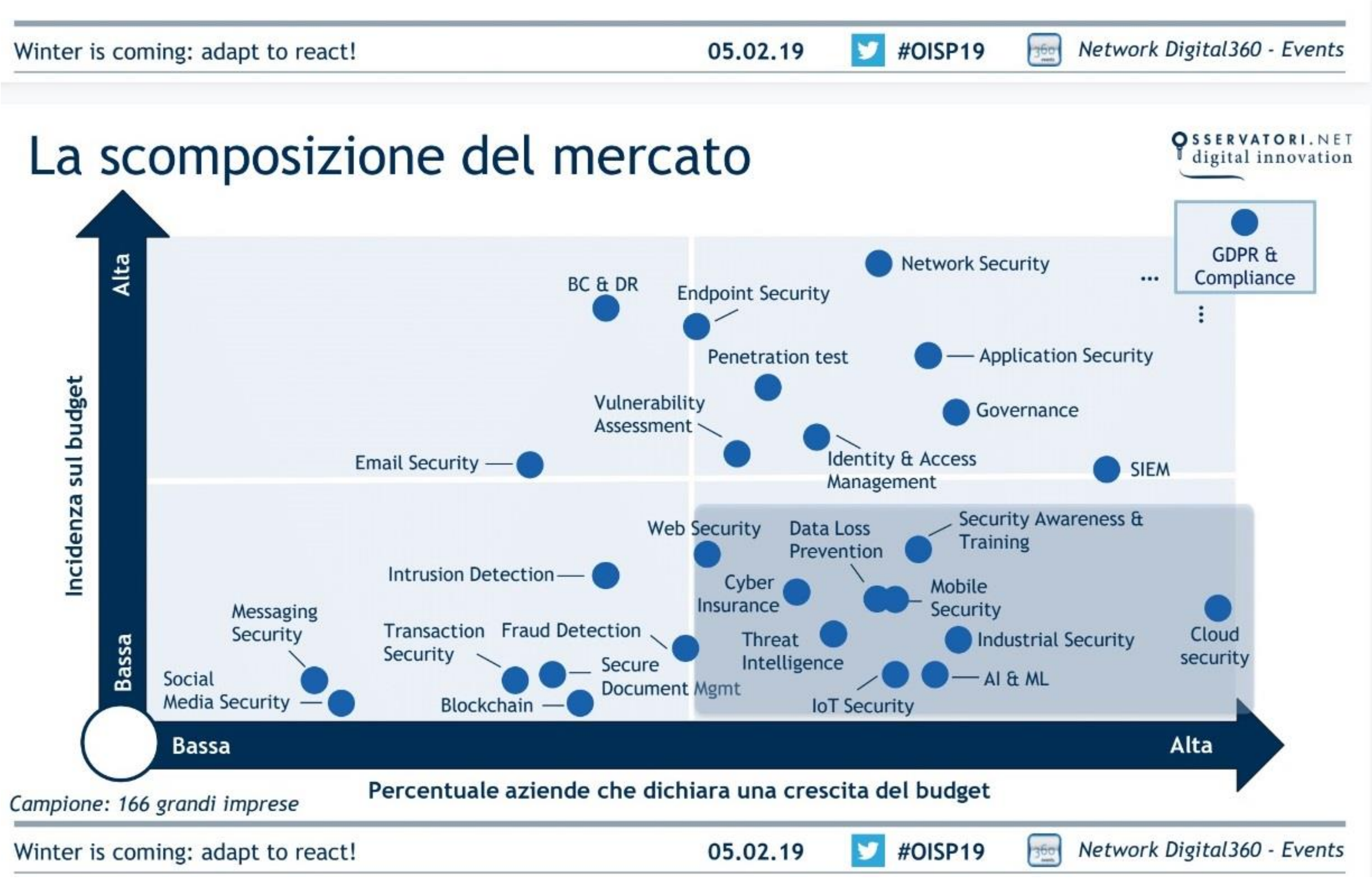
BOEING NOTIFIES 36,000 EMPLOYEES FOLLOWING BREACH

by Chris Brook February 27, 2017 , 3:48 pm

Large-Scale Breach Of America's JobLink Alliance Potentially Compromised Millions Of Job Seekers

By Joel Cheesman March 29, 2017 ERE

SECURITY MARKET



Winter is coming: adapt to react! 05.02.19 #OISP19 Network Digital360 - Events

La scomposizione del mercato

Campione: 166 grandi imprese

Winter is coming: adapt to react! 05.02.19 #OISP19 Network Digital360 - Events

SIEM DEFINTION

- The term **Security Information Event Management (SIEM)**, coined by Mark Nicolett and Amrit Williams of Gartner in 2005.

- Describes the product capabilities of
  - **gathering**, **analyzing** and **presenting** information from network and security devices
  - identity and access management applications
  - vulnerability management and policy compliance tools
  - operating system, database and application logs

  ...and external threat data.

- SIEM is a term for software and products services combining security information management (SIM) and security event manager (SEM).
  - The acronyms SEM, SIM and SIEM have been sometimes used interchangeably.
  - The segment of security management that deals with real-time monitoring, correlation of events, notifications and console views is commonly known as Security Event Management (SEM).
  - The second area provides long-term storage, analysis and reporting of log data and is known as Security Information Management (SIM).

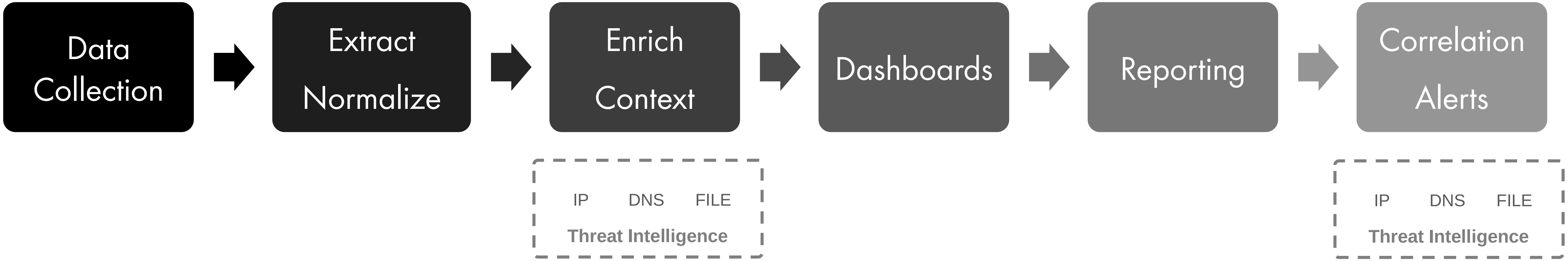
DATASOURCES

Domain	Data sources	Timing	Collector
Network	Pcap, netflow, ipfix, DPI	Real time packet processing	nProbe, n2disk, Packetbeats, Logstash
Host	Syslog, system state	Real time, Asynchronous	Safed, Auditbeats, Logstash, Winlogbeats
Database	JDBC, File export	Real time, Asynchronous	Safed, Logstash
Application	Logs	Real time, Event based	Beats, Logstash
Cloud	Logs, API	Real-time, Event based	Beats, Logstash
Container	Logs, eBPF	Real time packet processing	nProbe, Logstash

CLOUD

On Premise (Internal Service)	Infrastructure (as a Service)	Container (as a Service)	Platform (as a Service)	Function (as a Service)	Software (as a Service)
Functions	Functions	Functions	Functions	Functions	Functions
Applications	Applications	Applications	Applications	Applications	Applications
Data	Data	Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware	Middleware	Middleware
Container	Container	Container	Container	Container	Container
Orchestrator	Orchestrator	Orchestrator	Orchestrator	Orchestrator	Orchestrator
O/S	O/S	O/S	O/S	O/S	O/S
Virtualization	Virtualization	Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking	Networking	Networking

SIEM FLOW



Data Collection

Extract Normalize

Enrich Context

Dashboards

Reporting

Correlation Alerts

IP DNS FILE

Threat Intelligence

IP DNS FILE

Threat Intelligence

SIEM ADD CONTEXT

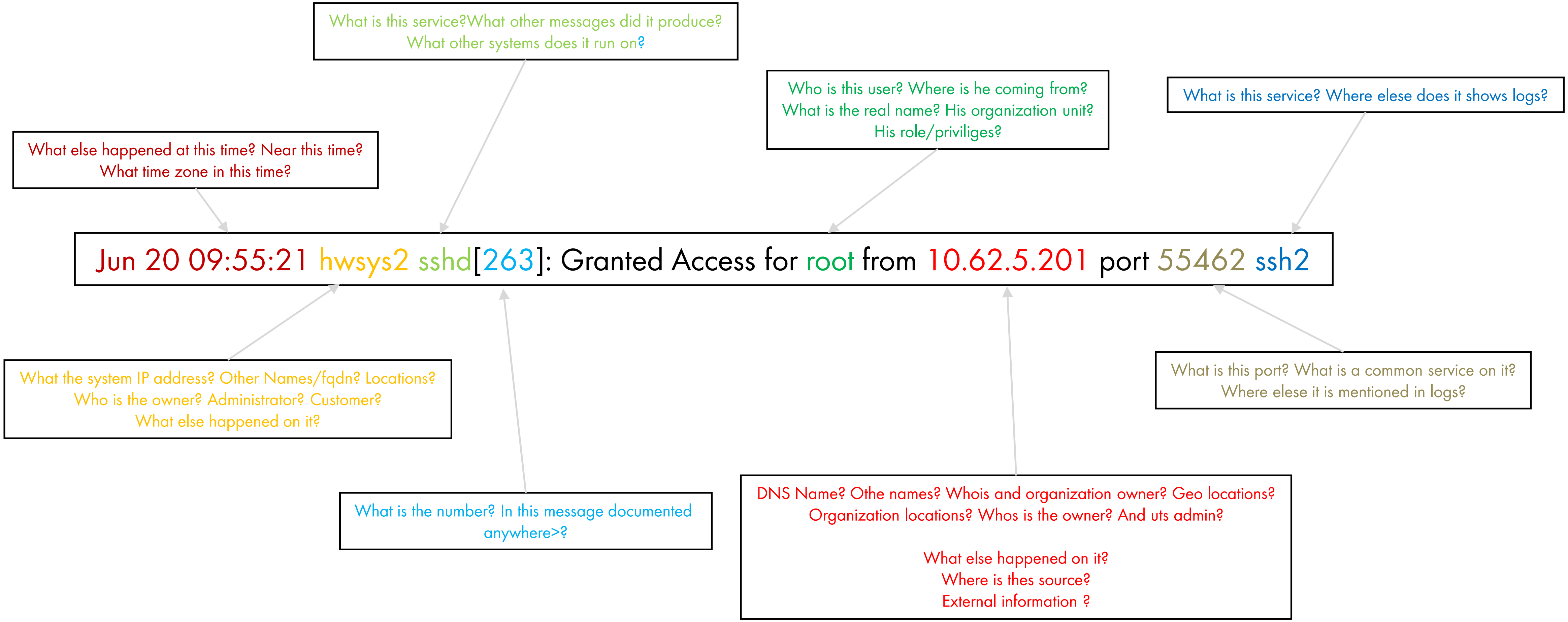
Examples of context

- Add geo-location information
- Get information from DNS, Thread Intelligence
- Get User details (Department, Policy)

Add context aids in identifying

- Access from foreign locations
- Suspect data transfer (location, volume,...)
- Suspect network activities

SIEM ADD CONTEXT



What is this service?What other messages did it produce?
What other systems does it run on?

Who is this user? Where is he coming from?
What is the real name? His organization unit?
His role/priviliges?

What is this service? Where elese does it shows logs?

What else happened at this time? Near this time?
What time zone in this time?

```
Jun 20 09:55:21 hwsys2 sshd[263]: Granted Access for root from 10.62.5.201 port 55462 ssh2
```

What the system IP address? Other Names/fqdn? Locations?
Who is the owner? Administrator? Customer?
What else happened on it?

What is this port? What is a common service on it?
Where elese it is mentioned in logs?

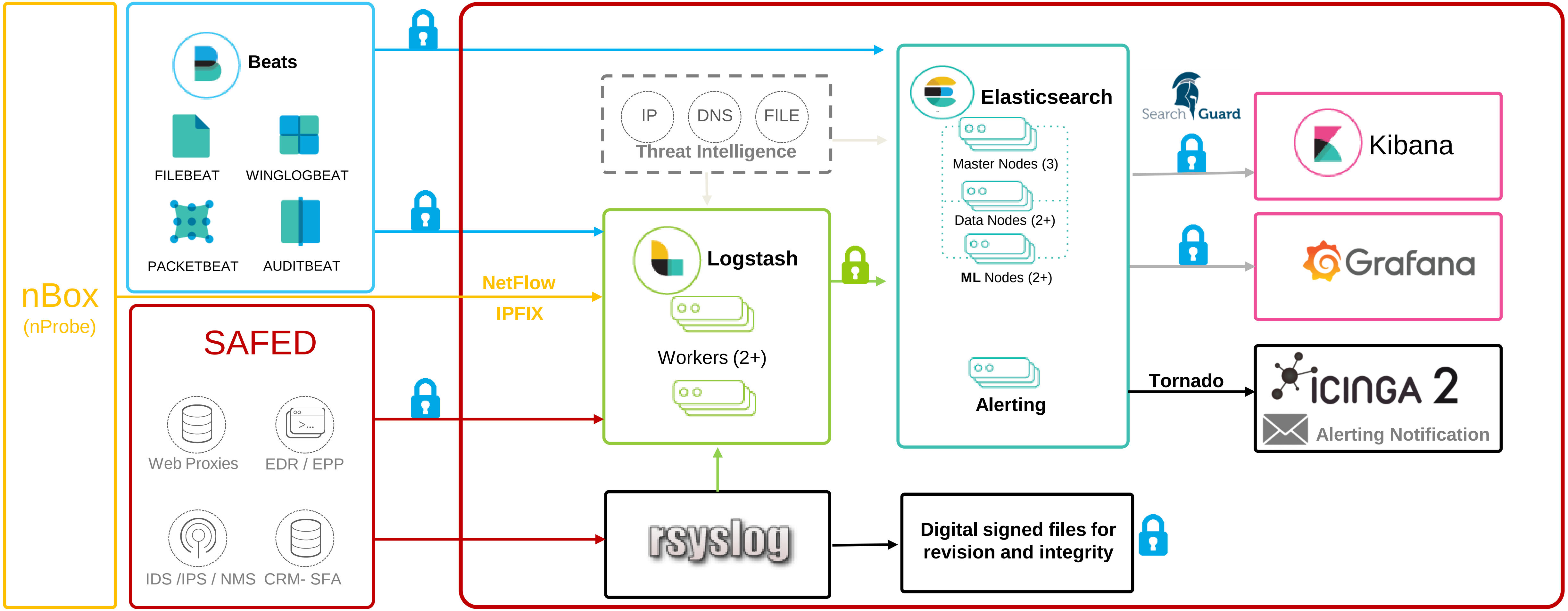
What is the number? In this message documented anywhere>?

DNS Name? Othe names? Whois and organization owner? Geo locations?
Organization locations? Whos is the owner? And uts admin?

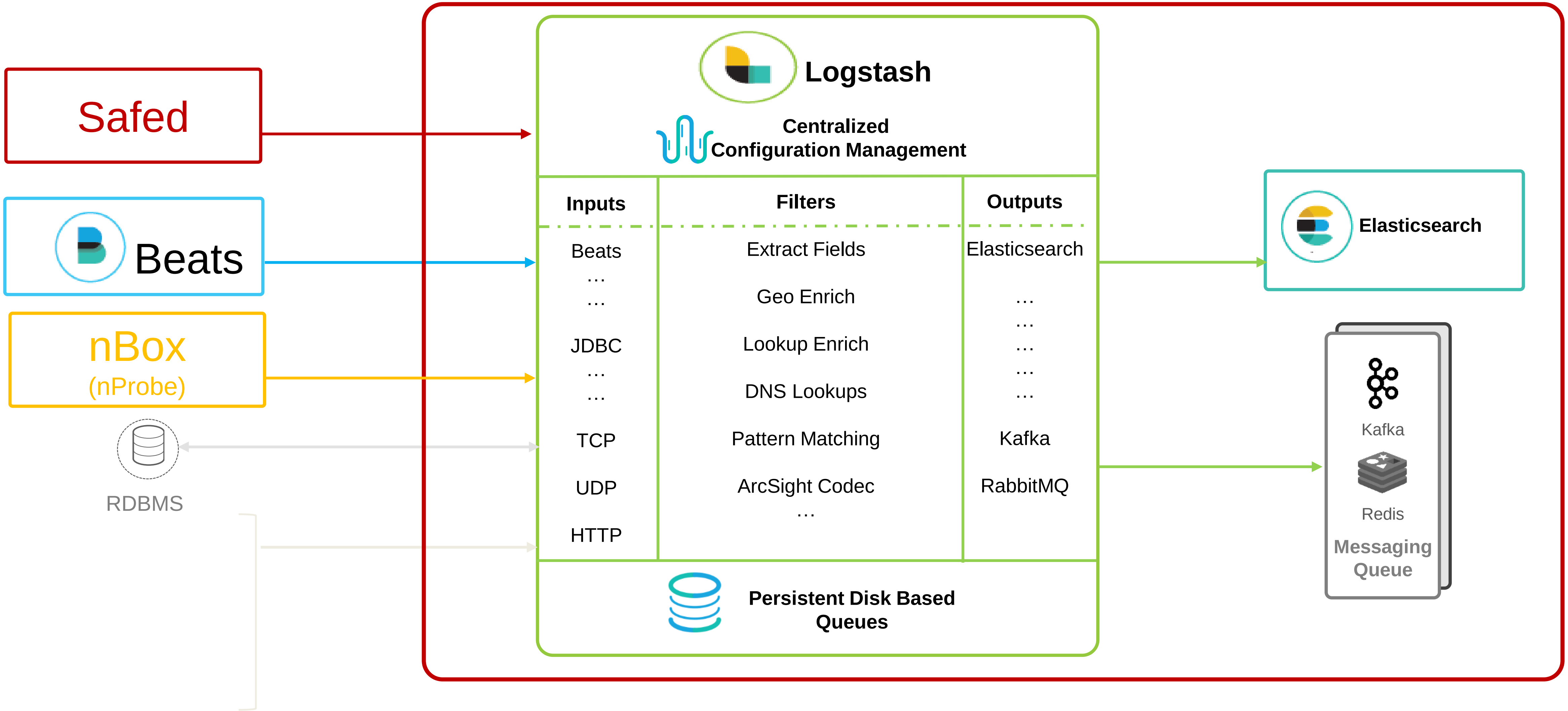
What else happened on it?
Where is thes source?
External information ?

LOG MANAGER SOLUTION DESIGN

NetEye



LOG MANAGER INSIGHT INPUT – FILTERS - OUTPUT



Safed

Beats

nBox
(nProbe)

RDBMS

Logstash

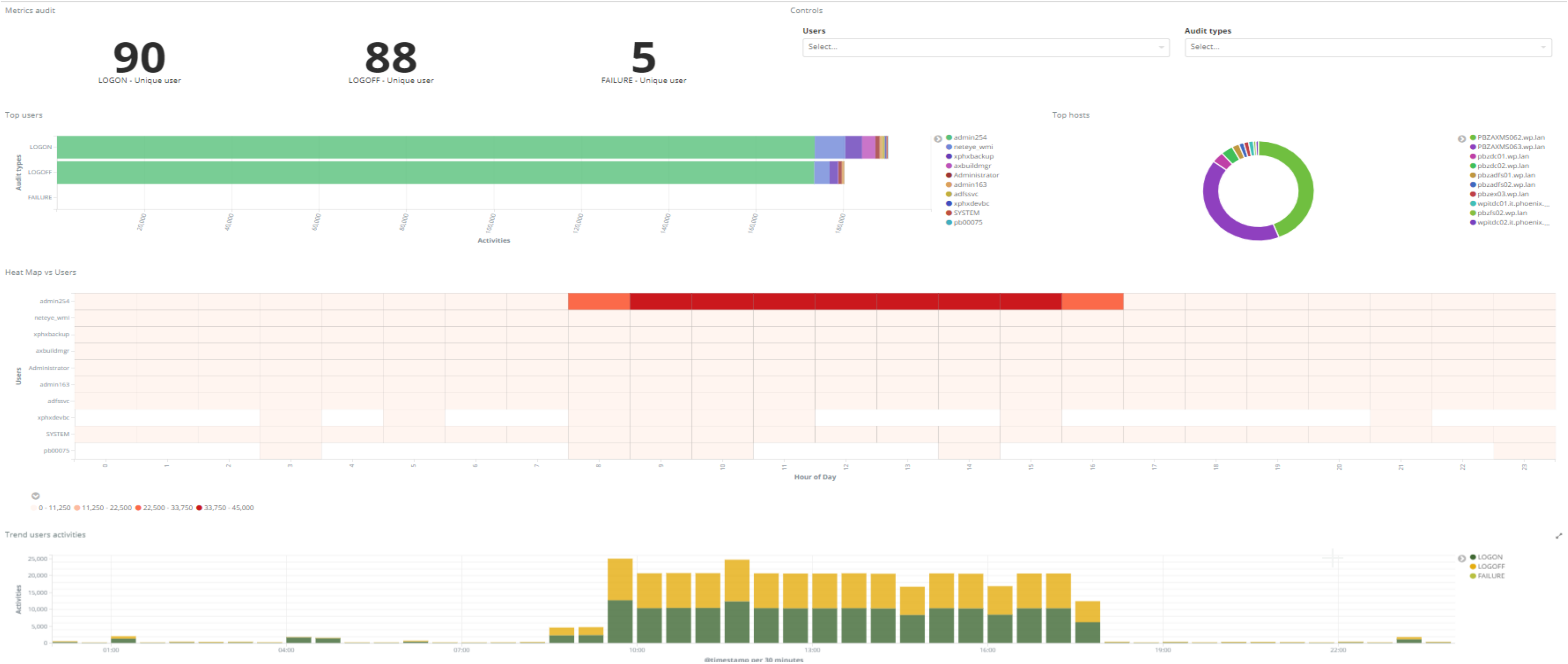
Centralized Configuration Management

Inputs	Filters	Outputs
Beats … … JDBC … … TCP UDP HTTP	Extract Fields Geo Enrich Lookup Enrich DNS Lookups Pattern Matching ArcSight Codec …	Elasticsearch … … … … … Kafka RabbitMQ

Persistent Disk Based Queues

Elasticsearch

LOG MANAGEMENT: LOG-IN/LOG-OUT ACCESS AUDITING



Metrics audit

90
LOGON - Unique user

88
LOGOFF - Unique user

5
FAILURE - Unique user

Controls

Users: Select...

Audit types: Select...

WHY SIEM PROJECTS OFTEN FAILS ?

Lack of Planning

- No defined scope

Faulty Deployment Strategies

- Incoherent log management data collection
- High volume of irrelevant data can overload the system

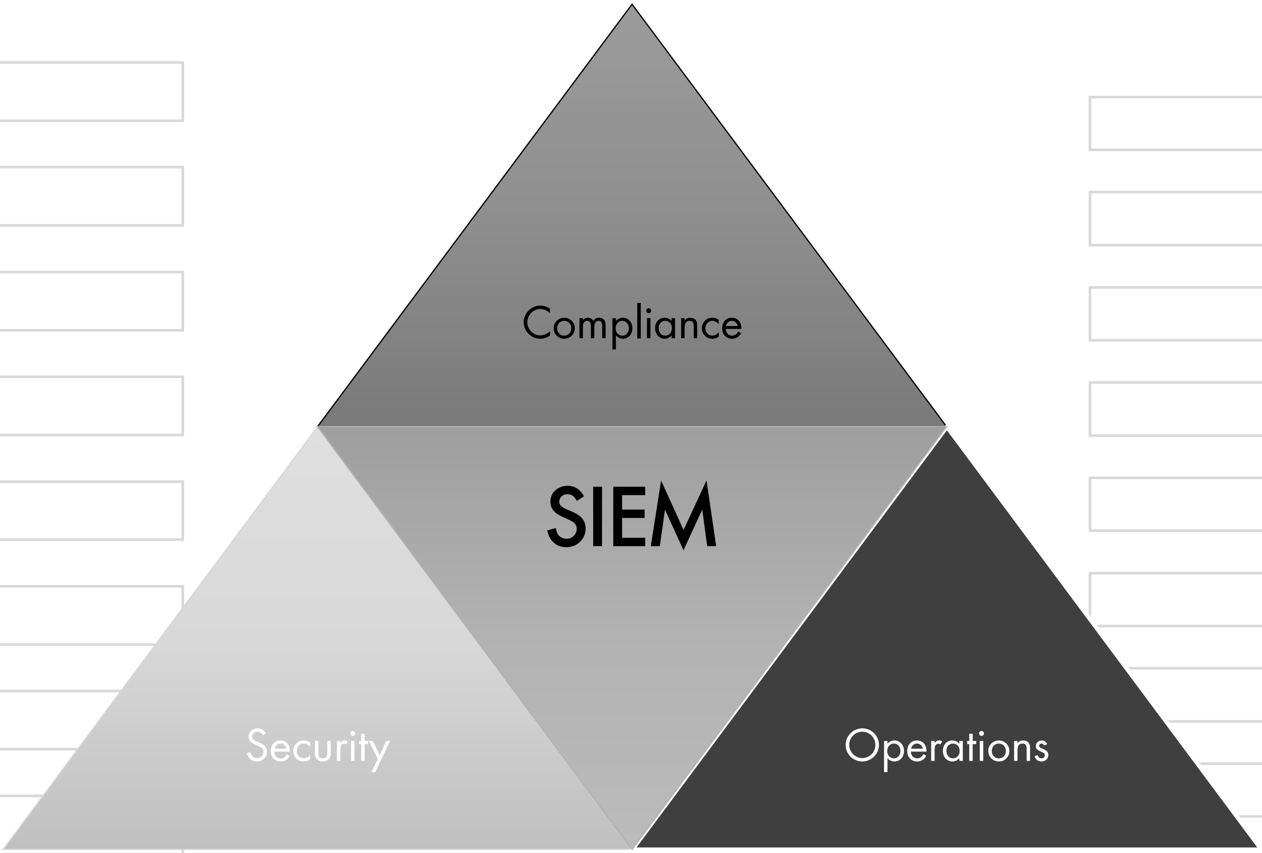
Operational

- Lack of management oversight
- Assume plug and play

"Security is a process, not a product"

VISION NETEYE 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

NetEye

on premises –Hybrid – Multi Cloud - SaaS

MONITORING – VISIBILITY - OBSERVABILITY

UNIFIED MONITORING
AVAILABILITY
SERVICE LEVEL MANAGEMENT

- Unified Monitoring
- Business Service Monitoring
- Distributed Monitoring
- Iot – IIoT Monitoring
- Asset Management
- Web Service Monitoring

IT OPERATION ANALYTICS
APM
END2END

- Visual Synthetic Monitoring Alyvix
- User Experience
- IT Operation Analytics
- Application Performance Management
- Anomaly Detection
- Forecasting - Prediction
- Machine Learning

GDPR – SECURITY
LOG MANAGEMENT
SIEM

- Log Management
- Log Analytics
- SIEM
- Machine Learning

SERVICE & SUPPORT
SERVICE MANAGEMENT
TICKETING

- EriZone - Service Management
- EriZone - CMDB
- EriZone - ITIL
- NetEye HelpDesk

NetEye

WWW.WUERTH-PHOENIX.COM