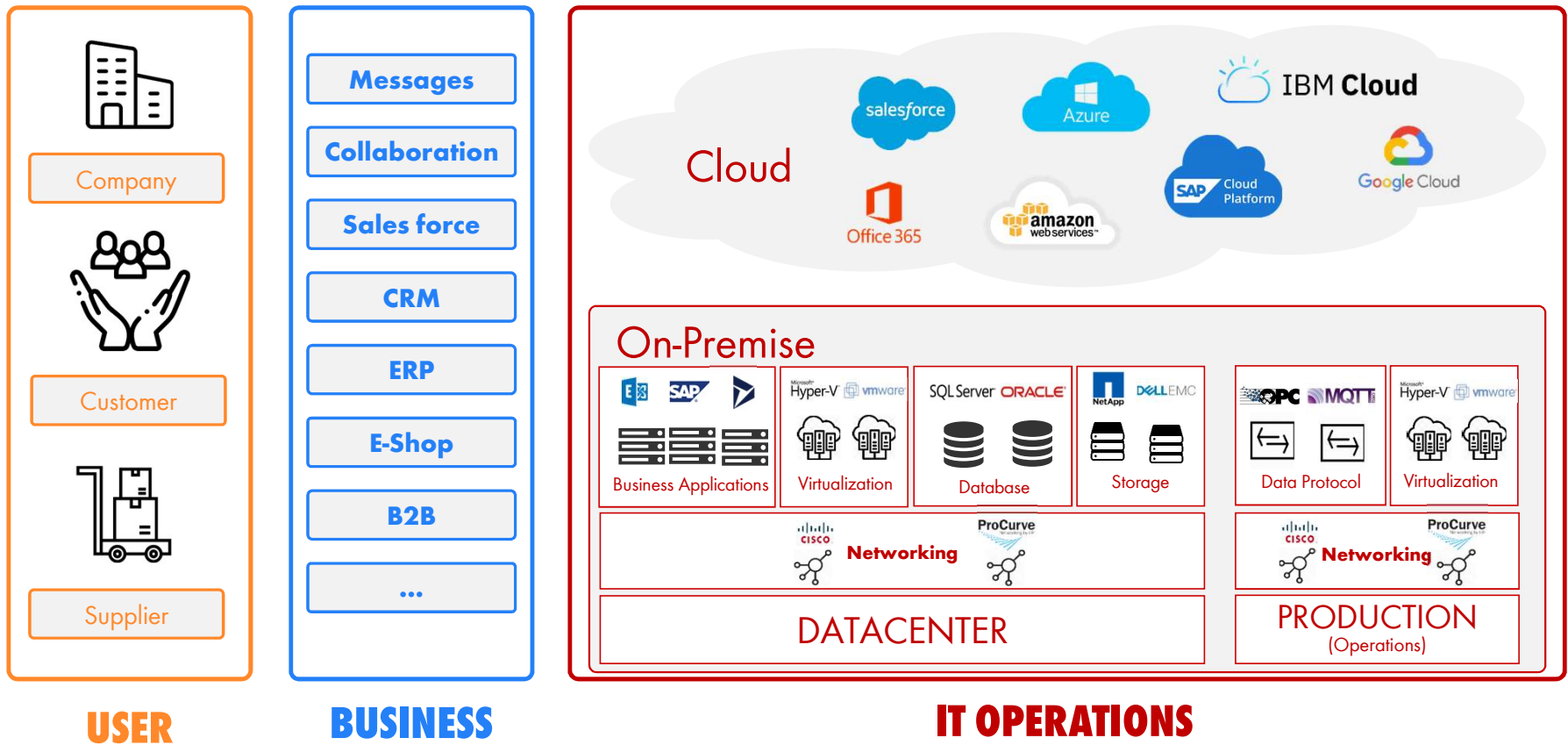




NetEye User Group

NetEye Innovation and Cyber Security

IT becomes crucial for the business





IT Infrastructure events must be addressed **at ever-increasing velocity**

IT environments **exceeding human scale**

Cyber Security challenges: **ransomware, phishing attacks, malware attacks, supply chain**

**C
H
A
L
L
E
N
G
E**

I T O p S O C

The amount of IT metrics that ITOps needs to check **is increasing exponentially**

Developers gain **more influence on ITOps** (DevOps) but the accountability still rests with the core IT

The amount of events and alerts the SOC needs to keep monitored is increasing



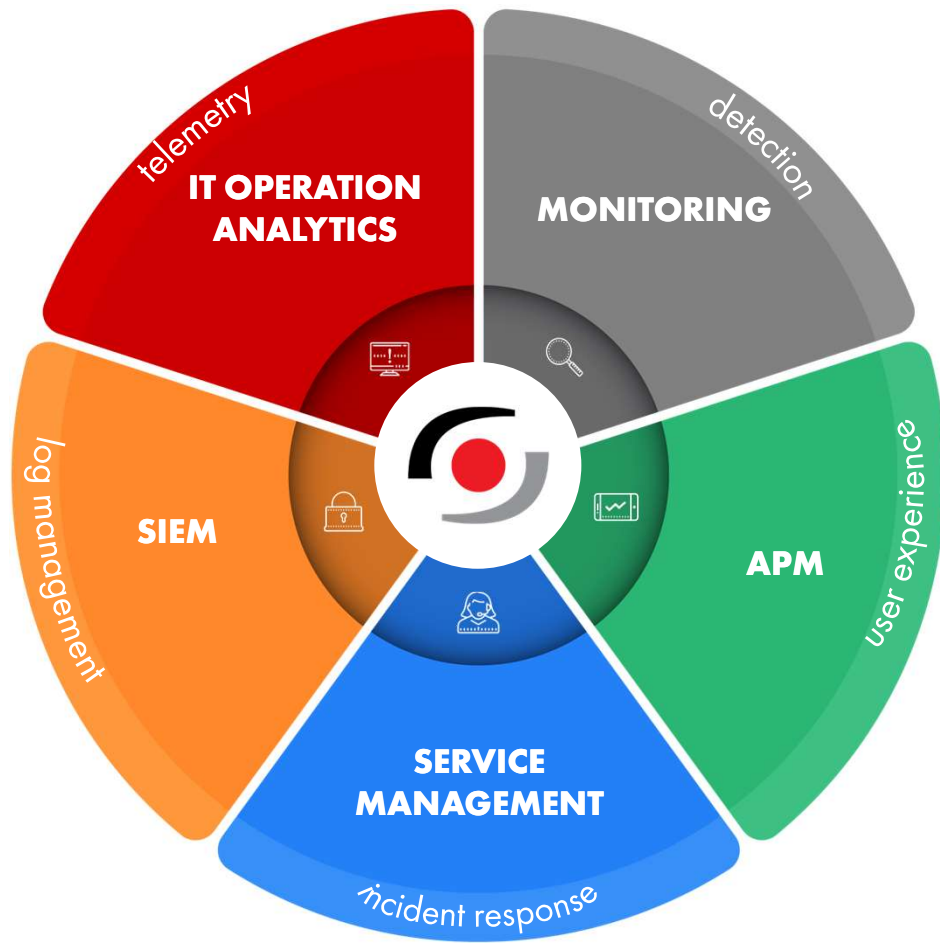


IT Operations Analytics Security Operations Analytics

Method that allows to **gather various types of data** from an IT infrastructure and analyzes them to **recognize patterns and behaviors**.



NetEye provides modules with the purpose of **gathering, processing, and analyzing** the full spectrum of IT operational data and **to guide decisions**, understand resource utilization and **predict** potential issues



#WEINNOVATE





Monitoring

Check events to achieve overall health across your IT

Detection

- Uptime
- End to End
- Correlation
- Visual Synthetic Robot
- Server; Storage
- Network

ITOA

Observe metrics to identify potential resource saturation

Telemetry

- Performance
- Scalability
- Cost Management
- Trend Analysis
- Forecast
- Anomaly Detection

APM

Use trace data to get full application insights

Insights

- Identify bottlenecks
- Response time
- Incoming requests
- Queries - Errors
- External http(s) request
- Real User Experience

SIEM LOG

Collect overall log(s) to get full visibility of your IT

Visibility

- Event correlation
- Threat Detection
- Anomalies
- Behavior driven alarms

Service Management

Be smart based on monitoring data to be pro active and automate remediation

Continuous Improvement

- SLA
- Incident management
- Monitoring data to learn
- Pro Active
- Postmortem report

NetEye Unified Integrated Approach





NetEye



Reliability

- ✓ RHEL8
- ✓ High Availability
- ✓ High Availability cross datacenter

Scalability

- ✓ Distributed
- ✓ Scale out physical node
- ✓ Scale out virtual node

Usability

- ✓ UX
- ✓ Carbon Design
- ✓ User Guide

DEVELOPMENT

Security

- ✓ OWASP Application Security - OSS
- ✓ DevSecOps - CI/CD - Burp Suite Enterprise
- ✓ Supply Chain - signing RPM

Deployment

- ✓ On Prem
- ✓ Cloud IaaS
- ✓ **Cloud SaaS**
- ✓ Multi Tenancy

Automation

- ✓ NetEye Extension Pack
- ✓ Release Upgrade
- ✓ Ansible

IMPROVEMENT





RedHat Enterprise Linux 9

- ✓ Upgrade latest language runtime
- ✓ Monitor - Maintain Environment
- ✓ Identity and Security

Icinga 2.13 - IcingaDB

- ✓ Performance
- ✓ Multi-Tenancy
- ✓ New UX

Elastic 8 - ElastiFlow

- ✓ Endpoint Security
- ✓ Central Elastic Agent with Fleet
- ✓ Better EBP Proxy integration

Influx 2 - Influx IOX - Nats

- ✓ Scalability - distributed
- ✓ Tasks - Checks
- ✓ No cardinality limitations

TECHNOLOGY

Grafana 9

- ✓ New Dashboards
- ✓ Alerts
- ✓ Smother integration

GLPI 10

- ✓ New UX
- ✓ GLPI Agent
- ✓ Smother Integration

NTOPNG 5

- ✓ Network Visibility
- ✓ Network based Cyber Defense
- ✓ Clickhouse for alerts and historical flows

Alyvix 3

- ✓ Central Configuration Management
- ✓ Reports
- ✓ Dashboards





NetEye Extensions Pack

<https://siwuertthphoenix.atlassian.net/jira/dashboards/10903>

NetEye Extension Packs - Issues

Heat Map: NetEye Extension Packs

Common Monitoring Core
NEP Setup Network Base

There are 34 distinct 'Components' values in 295 issues.

Jira Road Map: Next 90 Days (Until 06/Dec/2022 13:06)

NetEye Extension Packs NE-4.26

30/Sep/2022 00:00

1 of 61 issues resolved.

NetEye Extension Packs NE-4.27

30/Nov/2022 00:00

0 of 14 issues resolved.

Two Dimensional Filter Statistics: NEP - Public Issues (Unreleased)

Status	Bug	Epics	Story	Sub-task	Task	T
DISCARDED - WON'T...	1	0	0	0	0	1
PENDING	1	0	1	0	1	3
WAITING FOR REVIEW	1	1	1	0	4	7
SELECTED FOR DEVEL...	0	1	1	6	4	12
IN PROGRESS	4	0	4	0	5	13
TODU	0	1	12	11	19	43
DONE	63	1	15	39	98	216
Total Unique Issues:	70	4	34	56	131	295

Grouped by: Issue Type
Showing 7 of 7 statistics.

Filter Results: NEP - Public Issues (Unreleased)

T	Key	Summary	P	Components	Fix versions	Affects versions	Status	Development
	NEP-336	Nagios Plugin perl deprecated		Monitoring Core	NE-4.25		IN PROGRESS	1 commit
	NEP-335	Prepare basic integration with VMD 1.4+		VmWare VMD	NE-4.26		DONE	MERGED

NetEye User Guide

Introduction to NEP

Introduction to NEP

NetEye helps you take care of several aspects of IT Service Management, from monitoring to log analysis and asset/resource management, with a free form approach. However, because of its wide range of features, building and maintaining an efficient design can become quite challenging:

- What's the best layout for arranging objects, reducing both the initial implementation effort and future management effort?
- Does the chosen strategy allow for easy management of each object's lifecycle?
- Can the chosen strategy easily and efficiently accommodate future growth, in terms of number of managed objects and of new functionalities?

Every day, we at Würth Phoenix deal with these questions, and our accumulated

Introduction to NEP

What are NetEye Extension Packs?

The idea behind NEPs

The fundamental unit: NEP Package

Package management

#WEINNOVATE

<https://neteye.guide/current/nep.html>





CUSTOMER

WÜRTHPHOENIX

Infrastructure Monitoring

Network Monitoring

IT Ops Analytics

Log Management

APM

Asset Management

SATELLITE # 1

SATELLITE # 2

...

SATELLITE # n



Internet
VPN

#WEINNOVATE





Cyber Security

OSINT

Discover the attack surface and keep it monitored over time.

Exposure assessment

- Monitor the exposed attack surface
- Cyber Threat Intelligence - Dark Web
- Collect Indicator of compromise

satay 
SEARCH ALL THINGS ABOUT YOUR ORG

SIEM – LOG

Collect overall log(s) to get full visibility of your IT

Visibility

- Event correlation
- Threat Detection
- Anomalies
- Behavior driven alarms

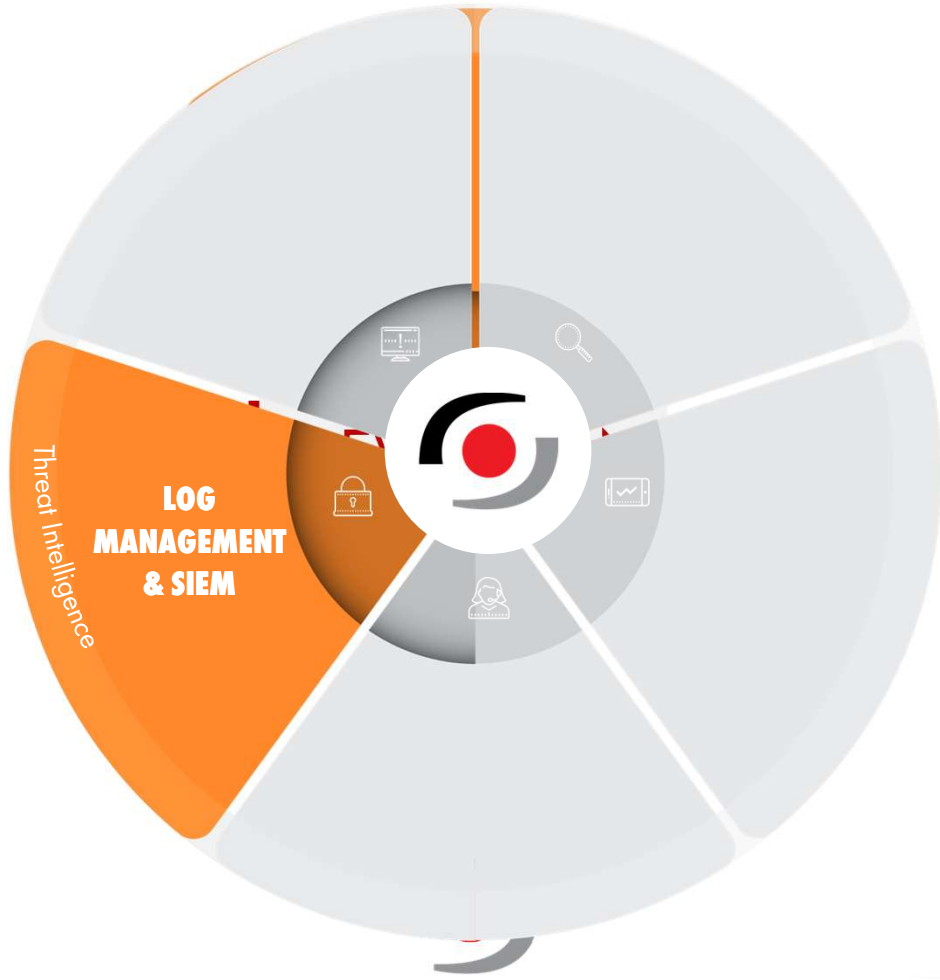
NetEye 


#WEINNOVATE





- LOGS
- FLOWS - EDR
- exposed ports
- ~~social network presence~~
- RED TEAM**
exposed buckets
- subdomains takeover
- IoC



- IoPC
- ransomware gangs sites
- vulnerabilities
-  similar domains
- BLUE TEAM**
data leak forums
- Telegram groups & channels
- data breaches

#WEINNOVATE





CUSTOMER



Red Team simulate attacks vs sources

Monitoring Perimeter: events sources (fw, webapp, AD, netflow, EDR, XDR, IoT, IIoT...)



NTOPNG

Network based Cyber Security Alerts

#WEINNOVATE

Competence Center (maintain infrastructure)



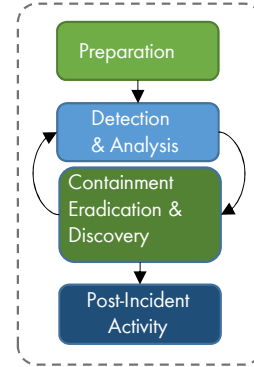
Cover Recon Phase

satellite(s) send events
Blue Team can gather additional data from target host through Icinga for a deeper analysis



Tickets & Playbooks

SECURITY OPERATION CENTER



Event & Incident Management



Blue Team recognize Attacks and write Detection Rules

Indicator of Compromise



OPENCTI

Exclusive Detection Rules Attacker aligned



Vulnerability Management

Data Ingestion, Visualization, Reports, Dashboards, Case Management





Conclusions



Don't build a black box,
make the tool interactive

Start with less factors and
gradually increase the complexity

Data-driven mindset is as
important as data

Prediction is important, so is the explanation

Feature engineering is
as important as model
training

**Data is
gold**

Human experience still
matters to look at the
right metrics

Data quality

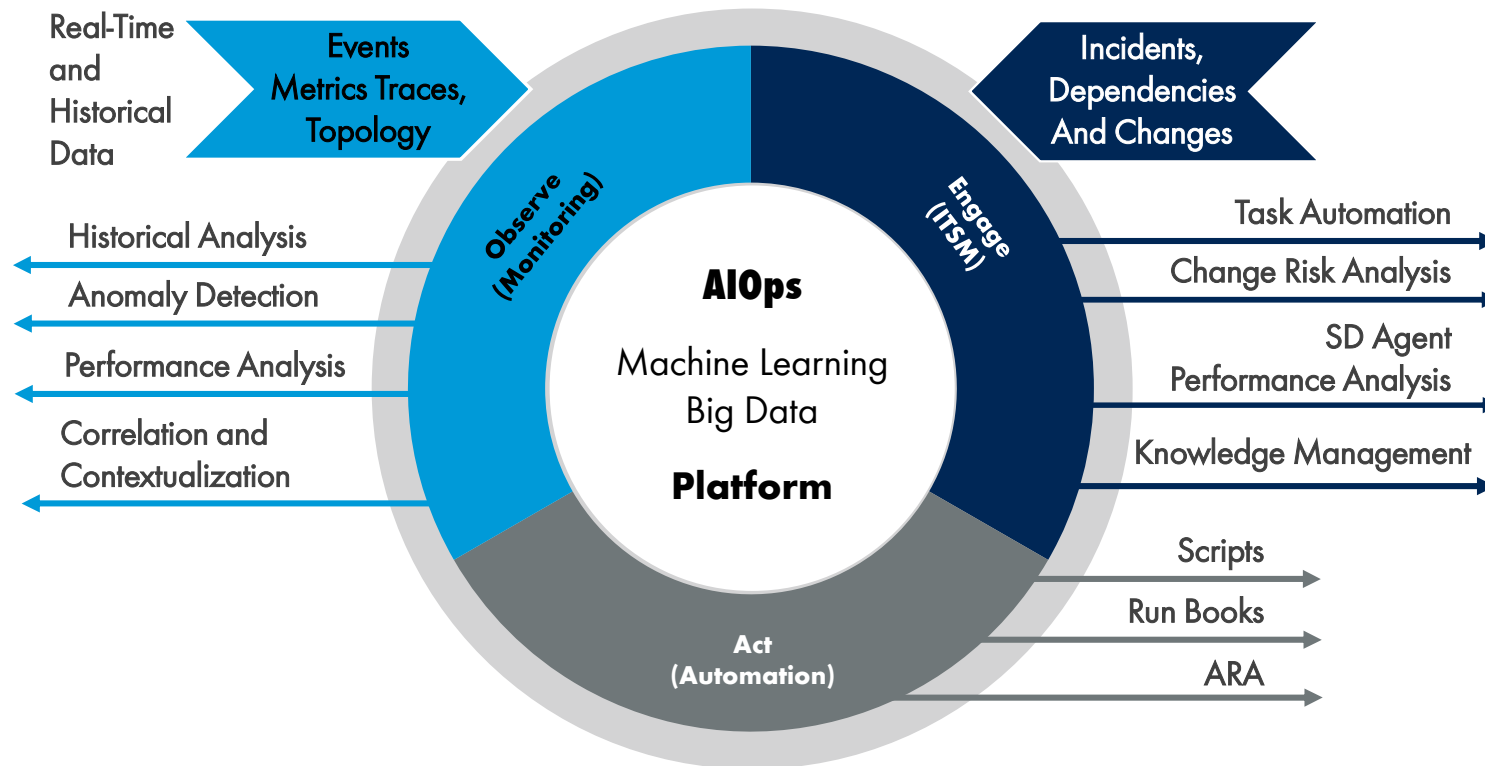
Differentiate
real-time and
non-real-time
analytics

Human experience
needs to be codified





AIOps Platform Enabling Continuous Insights Across IT Operations Monitoring (ITOM)



Recommended by Gartner





info@wuerth-phoenix.com
www.wuerth-phoenix.com



Thank you
Grazie Danke

#WEINNOVATE