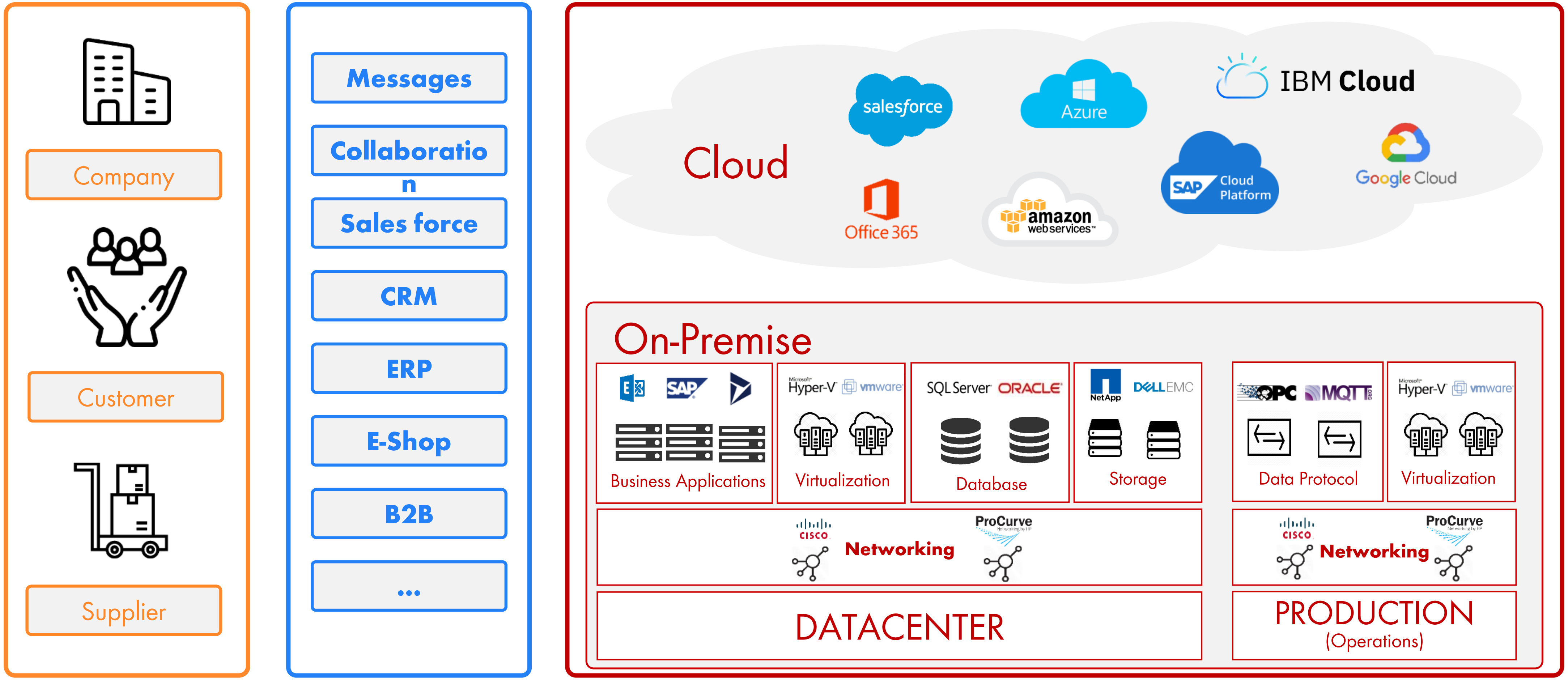
NetEye User Group

NetEye Innovation and Cyber Security

IT becomes crucial for the business



Company

Customer

Supplier

USER

Messages

Collaboratio
n

Sales force

CRM

ERP

E-Shop

B2B

...

BUSINESS

Cloud

On-Premise

Business Applications

Virtualization

Database

Storage

Data Protocol

Virtualization

Networking

Networking

DATACENTER

PRODUCTION
(Operations)

IT OPERATIONS

CHALLENGE

ITOpSOC

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**

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

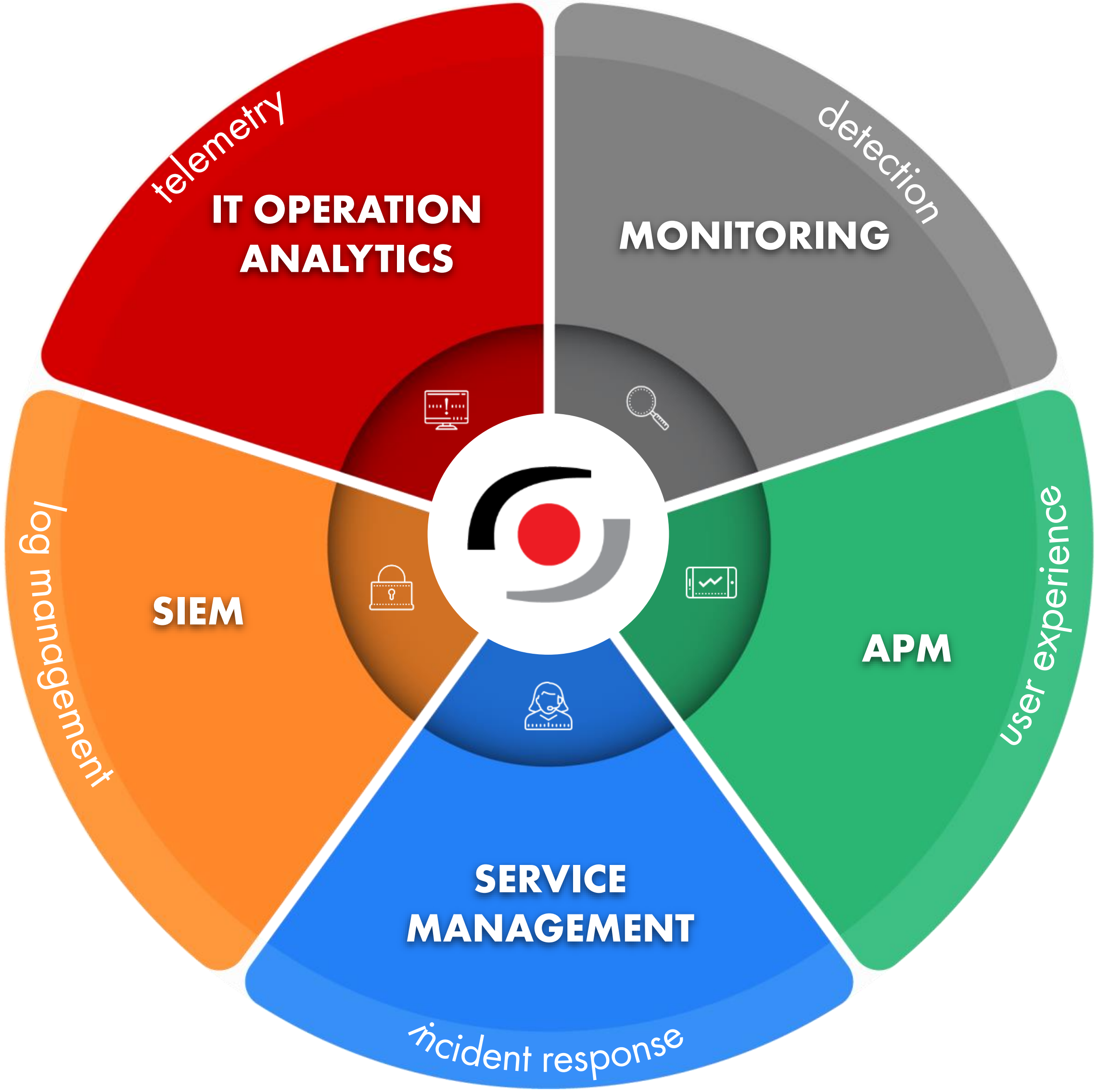
Developers gain **more influence on ITOps** (DevOps) but the accountability still rests with the core IT

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



IT OPERATION ANALYTICS
telemetry

MONITORING
detection

APM
user experience

SERVICE MANAGEMENT
incident response

SIEM
log management

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

#WEINNOVATE

Reliability

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

Scalability

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

Usability

- ✓ UX
- ✓ Carbon Design
- ✓ User Guide

Security

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

Deployment

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

Automation

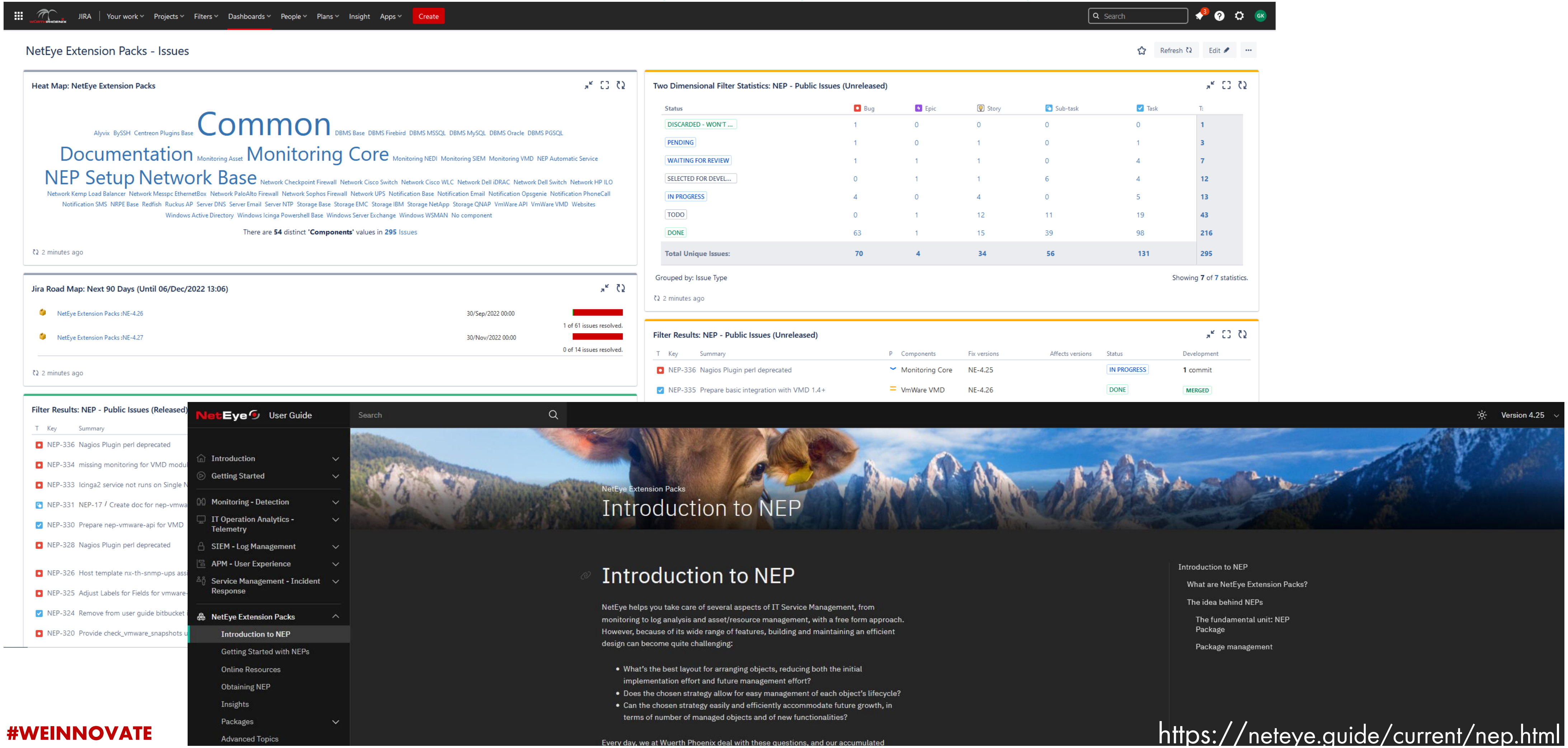
- ✓ NetEye Extension Pack
- ✓ Release Upgrade
- ✓ Ansible

DEVELOPMENT

IMPROVEMENT

NetEye Extensions Pack

https://siwuerthphoenix.atlassian.net/jira/dashboards/10903



NetEye Extension Packs - Issues

Heat Map: NetEye Extension Packs

Alyvix BySSH Centreon Plugins Base Common DBMS Base DBMS Firebird DBMS MSSQL DBMS MySQL DBMS Oracle DBMS PGSQL Documentation Monitoring Asset Monitoring Core Monitoring NEDI Monitoring SIEM Monitoring VMD NEP Automatic Service NEP Setup Network Base Network Checkpoint Firewall Network Cisco Switch Network Cisco WLC Network Dell iDRAC Network Dell Switch Network HP ILO Network Kemp Load Balancer Network Messpc EthernetBox Network PaloAlto Firewall Network Sophos Firewall Network UPS Notification Base Notification Email Notification Opsgenie Notification PhoneCall Notification SMS NRPE Base Redfish Ruckus AP Server DNS Server Email Server NTP Storage Base Storage EMC Storage IBM Storage NetApp Storage QNAP VmWare API VmWare VMD Websites Windows Active Directory Windows Icinga Powershell Base Windows Server Exchange Windows WSMAN No component

There are **54** distinct **'Components'** values in **295** Issues

2 minutes ago

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.

2 minutes ago

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

Status	Bug	Epic	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**
TODO	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.

2 minutes ago

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

Filter Results: NEP - Public Issues (Released)

T	Key	Summary
	NEP-336	Nagios Plugin perl deprecated
	NEP-334	missing monitoring for VMD modu
	NEP-333	Icinga2 service not runs on Single N
	NEP-331	NEP-17 / Create doc for nep-vmwa
☑	NEP-330	Prepare nep-vmware-api for VMD
	NEP-328	Nagios Plugin perl deprecated
	NEP-326	Host template nx-th-snmp-ups ass
	NEP-325	Adjust Labels for Fields for vmware-
☑	NEP-324	Remove from user guide bitbucket
	NEP-320	Provide check_vmware_snapshots u

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 Wuerth 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

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

#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

satayo

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

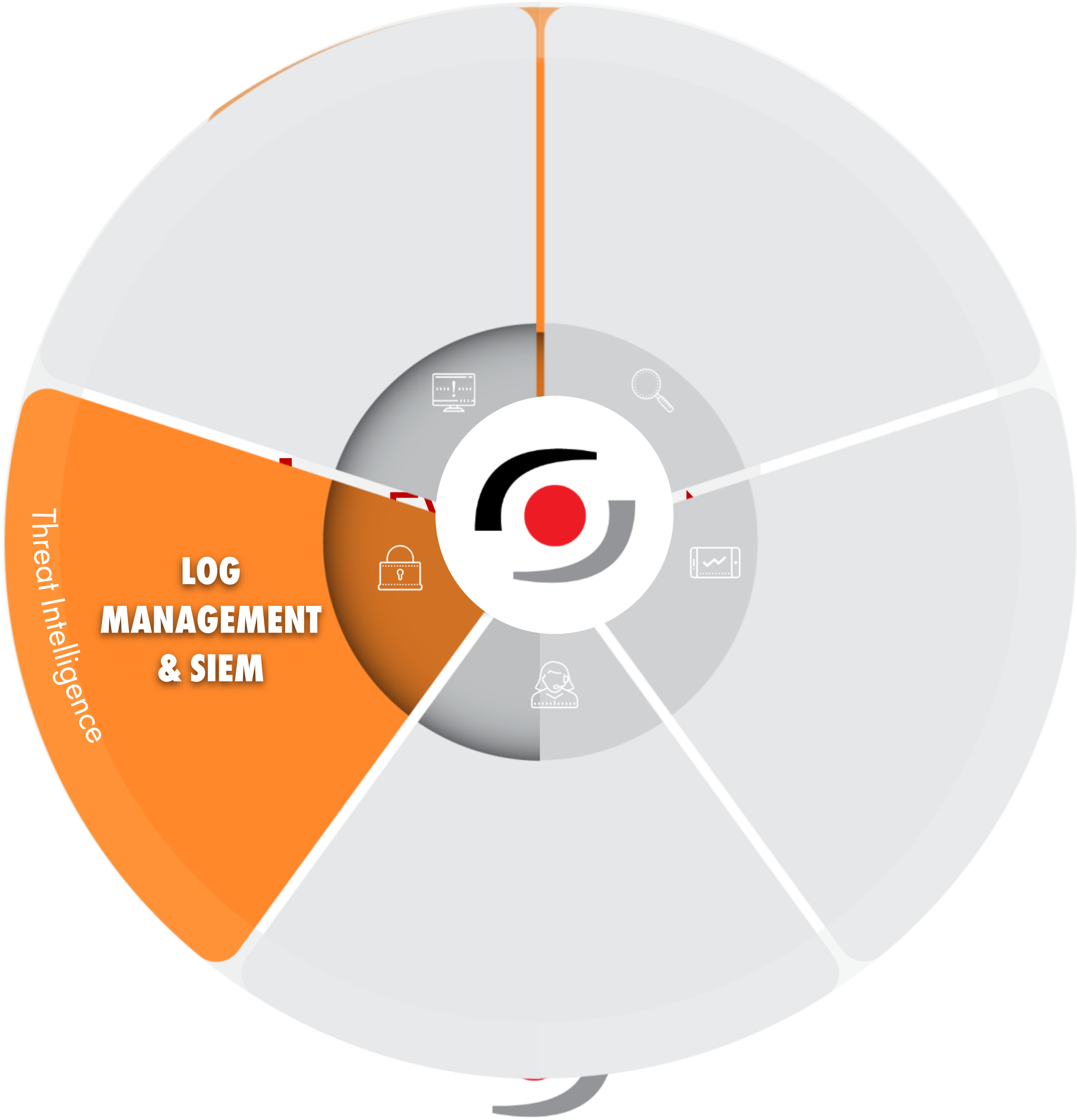
social network presence

RED TEAM

exposed buckets

subdomains takeover

IoC



IoPC

ransomware gangs sites

vulnerabilities

similar domains

BLUE TEAM

data leak forums

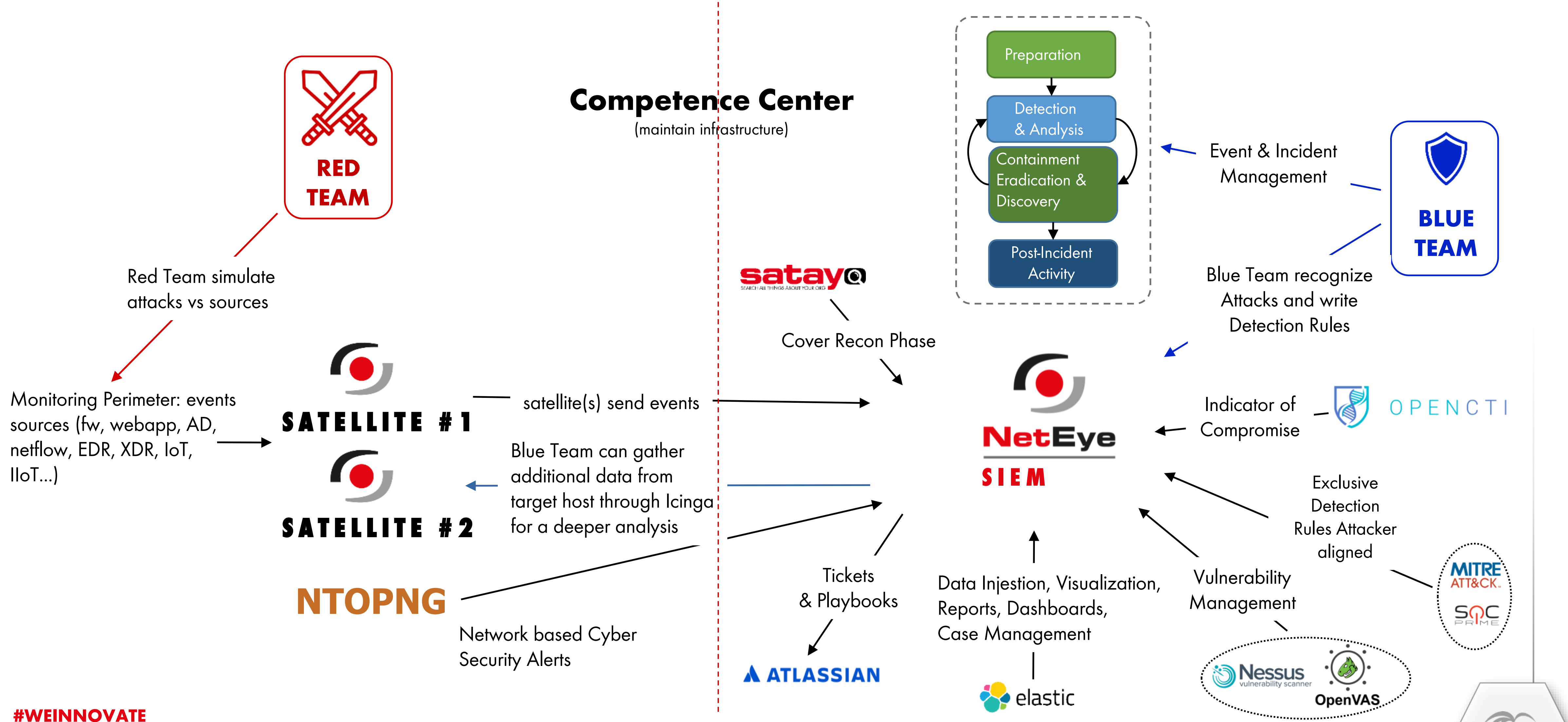
Telegram groups & channels

data breaches

#WEINNOVATE

CUSTOMER

SECURITY OPERATION CENTER



Competence Center

(maintain infrastructure)

RED TEAM

Red Team simulate attacks vs sources

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

SATELLITE #1

SATELLITE #2

satellite(s) send events

Blue Team can gather additional data from target host through Icinga for a deeper analysis

NTOPNG

Network based Cyber Security Alerts

satayo

Cover Recon Phase

Tickets & Playbooks

ATLASSIAN

Preparation

Detection & Analysis

Containment Eradication & Discovery

Post-Incident Activity

Event & Incident Management

BLUE TEAM

Blue Team recognize Attacks and write Detection Rules

NetEye SIEM

Indicator of Compromise

OPENCTI

Exclusive Detection Rules Attacker aligned

MITRE ATT&CK

SOC PRIME

Data Injestion, Visualization, Reports, Dashboards, Case Management

elastic

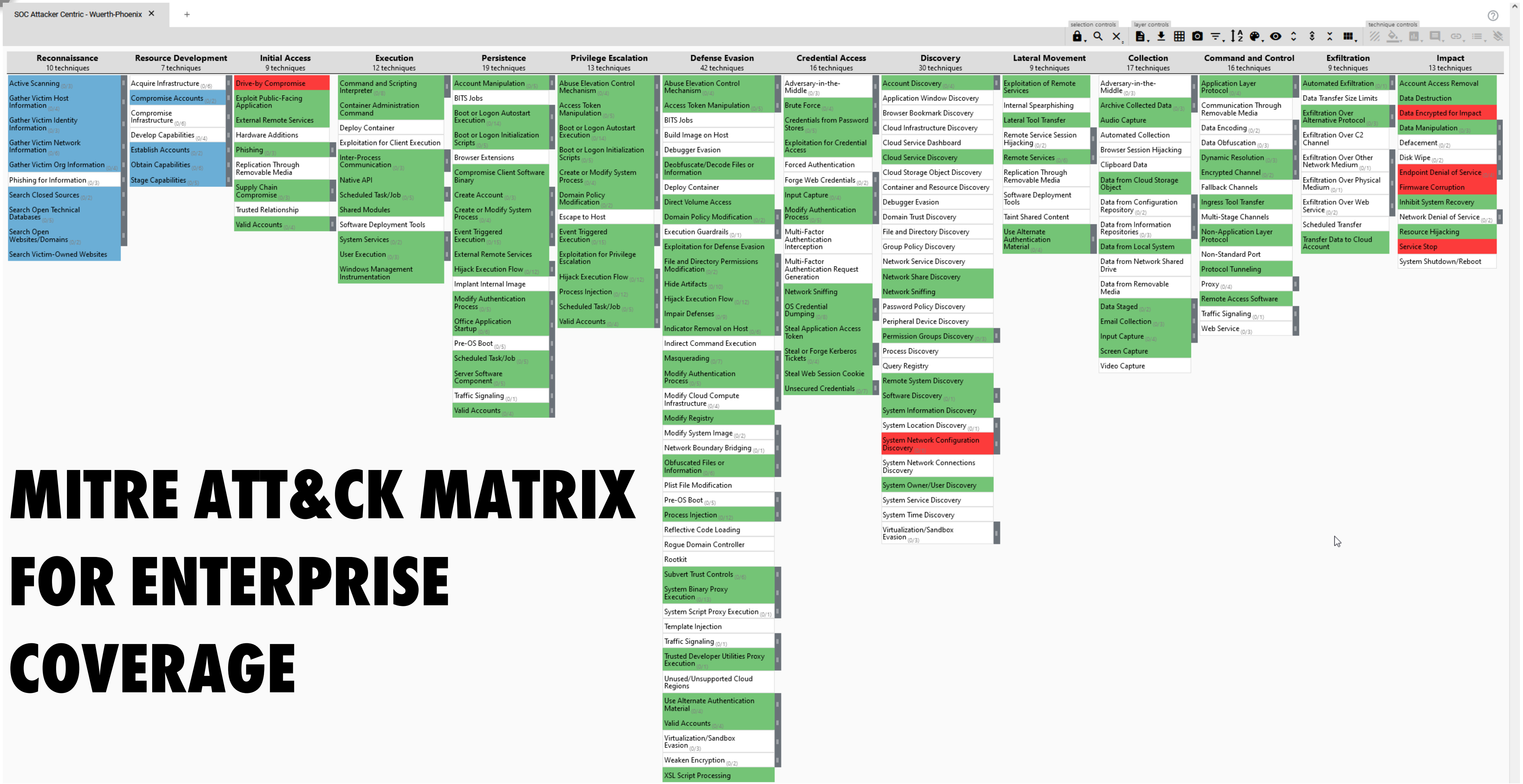
Vulnerability Management

Nessus vulnerability scanner

OpenVAS

#WEINNOVATE

MITRE ATT&CK MATRIX FOR ENTERPRISE COVERAGE



Reconnaissance 10 techniques

- 🟦 Active Scanning (0/3)
- 🟦 Gather Victim Host Information (0/4)
- 🟦 Gather Victim Identity Information (0/3)
- 🟦 Gather Victim Network Information (0/6)
- 🟦 Gather Victim Org Information (0/4)
- Phishing for Information (0/3)
- 🟦 Search Closed Sources (0/2)
- 🟦 Search Open Technical Databases (0/5)
- 🟦 Search Open Websites/Domains (0/2)
- 🟦 Search Victim-Owned Websites

Resource Development 7 techniques

- Acquire Infrastructure (0/6)
- 🟦 Compromise Accounts (0/2)
- Compromise Infrastructure (0/6)
- Develop Capabilities (0/4)
- 🟦 Establish Accounts (0/2)
- 🟦 Obtain Capabilities (0/6)
- 🟦 Stage Capabilities (0/5)

Initial Access 9 techniques

- 🟥 Drive-by Compromise
- 🟩 Exploit Public-Facing Application
- 🟩 External Remote Services
- Hardware Additions
- 🟩 Phishing (0/3)
- Replication Through Removable Media
- 🟩 Supply Chain Compromise (0/3)
- Trusted Relationship
- 🟩 Valid Accounts (0/4)

Execution 12 techniques

- 🟩 Command and Scripting Interpreter (0/8)
- 🟩 Container Administration Command
- Deploy Container
- Exploitation for Client Execution
- 🟩 Inter-Process Communication (0/3)
- 🟩 Native API
- 🟩 Scheduled Task/Job (0/5)
- 🟩 Shared Modules
- Software Deployment Tools
- 🟩 System Services (0/2)
- 🟩 User Execution (0/3)
- 🟩 Windows Management Instrumentation

Persistence 19 techniques

- 🟩 Account Manipulation (0/5)
- BITS Jobs
- 🟩 Boot or Logon Autostart Execution (0/14)
- 🟩 Boot or Logon Initialization Scripts (0/5)
- Browser Extensions
- 🟩 Compromise Client Software Binary
- 🟩 Create Account (0/3)
- 🟩 Create or Modify System Process (0/4)
- 🟩 Event Triggered Execution (0/15)
- 🟩 External Remote Services
- 🟩 Hijack Execution Flow (0/12)
- Implant Internal Image
- 🟩 Modify Authentication Process (0/5)
- 🟩 Office Application Startup (0/6)
- Pre-OS Boot (0/5)
- 🟩 Scheduled Task/Job (0/5)
- 🟩 Server Software Component (0/5)
- Traffic Signaling (0/1)
- 🟩 Valid Accounts (0/4)

Privilege Escalation 13 techniques

- 🟩 Abuse Elevation Control Mechanism (0/4)
- 🟩 Access Token Manipulation (0/5)
- 🟩 Boot or Logon Autostart Execution (0/14)
- 🟩 Boot or Logon Initialization Scripts (0/5)
- 🟩 Create or Modify System Process (0/4)
- 🟩 Domain Policy Modification (0/2)
- Escape to Host
- 🟩 Event Triggered Execution (0/15)
- 🟩 Exploitation for Privilege Escalation
- 🟩 Hijack Execution Flow (0/12)
- 🟩 Process Injection (0/12)
- 🟩 Scheduled Task/Job (0/5)
- 🟩 Valid Accounts (0/4)

Defense Evasion 42 techniques

- 🟩 Abuse Elevation Control Mechanism (0/4)
- 🟩 Access Token Manipulation (0/5)
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- 🟩 Deobfuscate/Decode Files or Information
- Deploy Container
- 🟩 Direct Volume Access
- 🟩 Domain Policy Modification (0/2)
- Execution Guardrails (0/1)
- 🟩 Exploitation for Defense Evasion
- 🟩 File and Directory Permissions Modification (0/2)
- 🟩 Hide Artifacts (0/10)
- 🟩 Hijack Execution Flow (0/12)
- 🟩 Impair Defenses (0/9)
- 🟩 Indicator Removal on Host (0/6)
- Indirect Command Execution
- 🟩 Masquerading (0/7)
- 🟩 Modify Authentication Process (0/5)
- Modify Cloud Compute Infrastructure (0/4)
- 🟩 Modify Registry
- Modify System Image (0/2)
- Network Boundary Bridging (0/1)
- 🟩 Obfuscated Files or Information (0/6)
- Plist File Modification
- Pre-OS Boot (0/5)
- 🟩 Process Injection (0/12)
- Reflective Code Loading
- Rogue Domain Controller
- Rootkit
- 🟩 Subvert Trust Controls (0/6)
- 🟩 System Binary Proxy Execution (0/13)
- System Script Proxy Execution (0/1)
- Template Injection
- Traffic Signaling (0/1)
- 🟩 Trusted Developer Utilities Proxy Execution (0/1)
- Unused/Unsupported Cloud Regions
- 🟩 Use Alternate Authentication Material (0/4)
- 🟩 Valid Accounts (0/4)
- Virtualization/Sandbox Evasion (0/3)
- Weaken Encryption (0/2)
- 🟩 XSL Script Processing

Credential Access 16 techniques

- Adversary-in-the-Middle (0/3)
- 🟩 Brute Force (0/4)
- 🟩 Credentials from Password Stores (0/5)
- 🟩 Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials (0/2)
- 🟩 Input Capture (0/4)
- 🟩 Modify Authentication Process (0/5)
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- 🟩 Network Sniffing
- 🟩 OS Credential Dumping (0/8)
- 🟩 Steal Application Access Token
- 🟩 Steal or Forge Kerberos Tickets (0/4)
- 🟩 Steal Web Session Cookie
- 🟩 Unsecured Credentials (0/7)

Discovery 30 techniques

- 🟩 Account Discovery (0/4)
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- 🟩 Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Network Service Discovery
- 🟩 Network Share Discovery
- 🟩 Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- 🟩 Permission Groups Discovery (0/3)
- Process Discovery
- Query Registry
- 🟩 Remote System Discovery
- 🟩 Software Discovery (0/1)
- 🟩 System Information Discovery
- System Location Discovery (0/1)
- 🟥 System Network Configuration Discovery (0/1)
- System Network Connections Discovery
- 🟩 System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion (0/3)

Lateral Movement 9 techniques

- 🟩 Exploitation of Remote Services
- Internal Spearphishing
- 🟩 Lateral Tool Transfer
- Remote Service Session Hijacking (0/2)
- 🟩 Remote Services (0/6)
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- 🟩 Use Alternate Authentication Material (0/4)

Collection 17 techniques

- Adversary-in-the-Middle (0/3)
- 🟩 Archive Collected Data (0/3)
- 🟩 Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- 🟩 Data from Cloud Storage Object
- Data from Configuration Repository (0/2)
- Data from Information Repositories (0/3)
- 🟩 Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- 🟩 Data Staged (0/2)
- 🟩 Email Collection (0/3)
- 🟩 Input Capture (0/4)
- 🟩 Screen Capture
- Video Capture

Command and Control 16 techniques

- 🟩 Application Layer Protocol (0/4)
- Communication Through Removable Media
- Data Encoding (0/2)
- Data Obfuscation (0/3)
- 🟩 Dynamic Resolution (0/3)
- 🟩 Encrypted Channel (0/2)
- Fallback Channels
- 🟩 Ingress Tool Transfer
- Multi-Stage Channels
- 🟩 Non-Application Layer Protocol
- Non-Standard Port
- 🟩 Protocol Tunneling
- Proxy (0/4)
- 🟩 Remote Access Software
- Traffic Signaling (0/1)
- Web Service (0/3)

Exfiltration 9 techniques

- 🟩 Automated Exfiltration (0/1)
- Data Transfer Size Limits
- 🟩 Exfiltration Over Alternative Protocol (0/3)
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium (0/1)
- Exfiltration Over Physical Medium (0/1)
- Exfiltration Over Web Service (0/2)
- Scheduled Transfer
- 🟩 Transfer Data to Cloud Account

Impact 13 techniques

- 🟩 Account Access Removal
- 🟩 Data Destruction
- 🟥 Data Encrypted for Impact
- 🟩 Data Manipulation (0/3)
- Defacement (0/2)
- Disk Wipe (0/2)
- 🟥 Endpoint Denial of Service (0/4)
- 🟥 Firmware Corruption
- 🟩 Inhibit System Recovery
- Network Denial of Service (0/2)
- 🟩 Resource Hijacking
- 🟥 Service Stop
- System Shutdown/Reboot

#WEINNOVATE

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

Data is gold

Human experience still matters to look at the right metrics

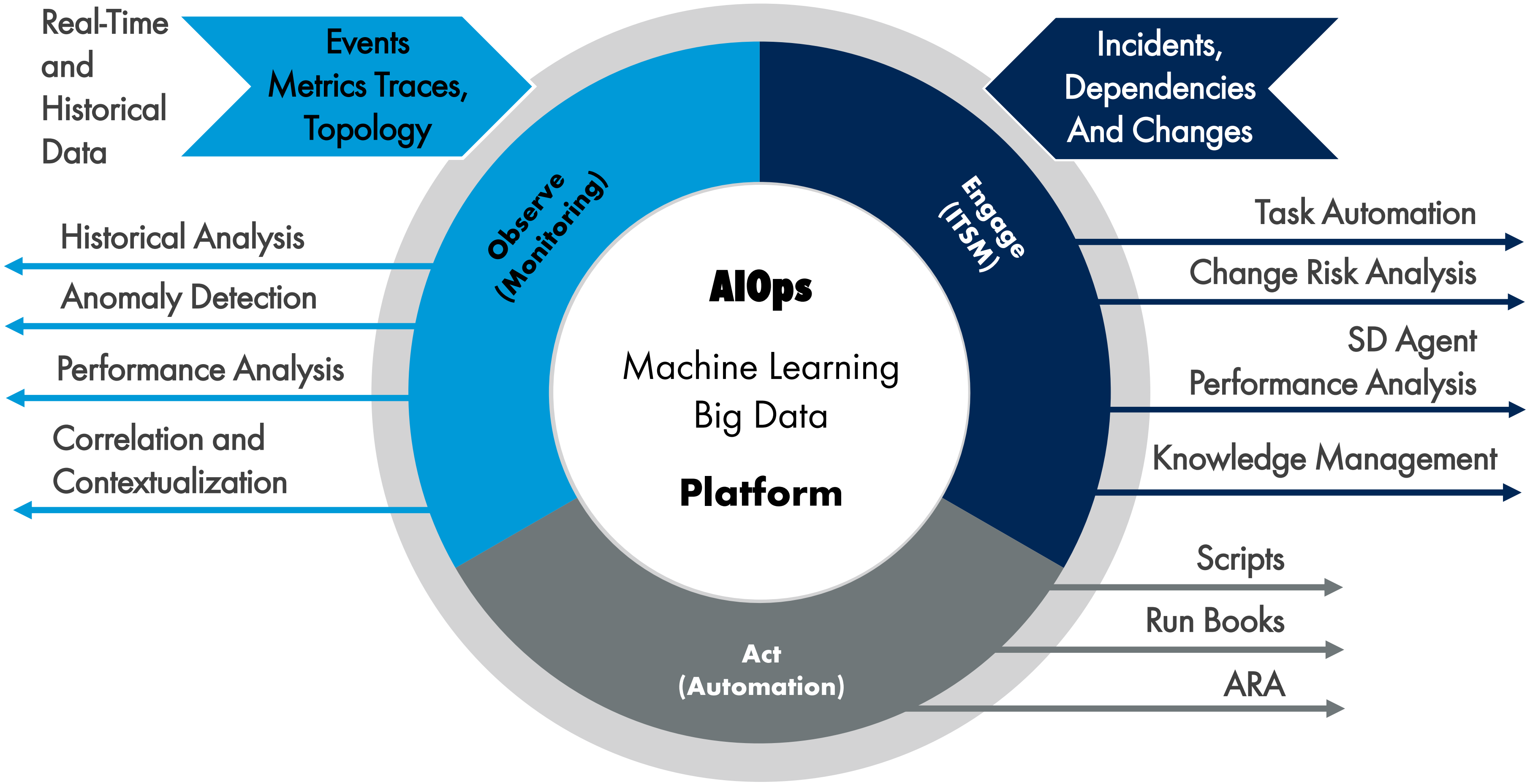
Feature engineering is as important as model training

Differentiate real-time and non-real-time analytics

Human experience needs to be codified

Data quality

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



Recommended by Gartner

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

NetEye | WÜRTHPHOENIX

Thank you
Grazie Danke

#WEINNOVATE