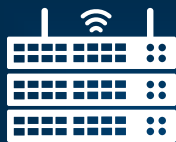




IT Event Management & Alerting with Versio.io

Practice-orientated seminar & training

Online | September 26, 2024



Versio.io Event Management & Alerting

General information

- The slides are available at www.versio.io!
- The training will be recorded and the video will be available as an online training.
- Halfway through the training we will take a 10 minute break.
- The Versio.io training environment will be available for 1 week after the training.
- If you have any questions during the presentation, please write them in the chat.
- Each participant receives a training certificate.

Versio.io Event Management & Alerting

Agenda

1. Versio.io fundamentals
2. Event management fundamentals
3. Import IT events (PE)
4. Event features (PE)
 - Inventory Integration (Digital Twin)
 - Close events
 - Archive events
 - Event deduplication (event storm)
5. Coffee & tea break - 10 min
6. Event analysis (PE)
 - Event filtering
 - Event insight dashboard
 - Event explorer
7. Alerting (PE)
 1. Event selection
 2. Actions
 3. Action „Event reference instance“
8. Subscription model
9. Questions & Answers

* PE = Practical exercise

Online training

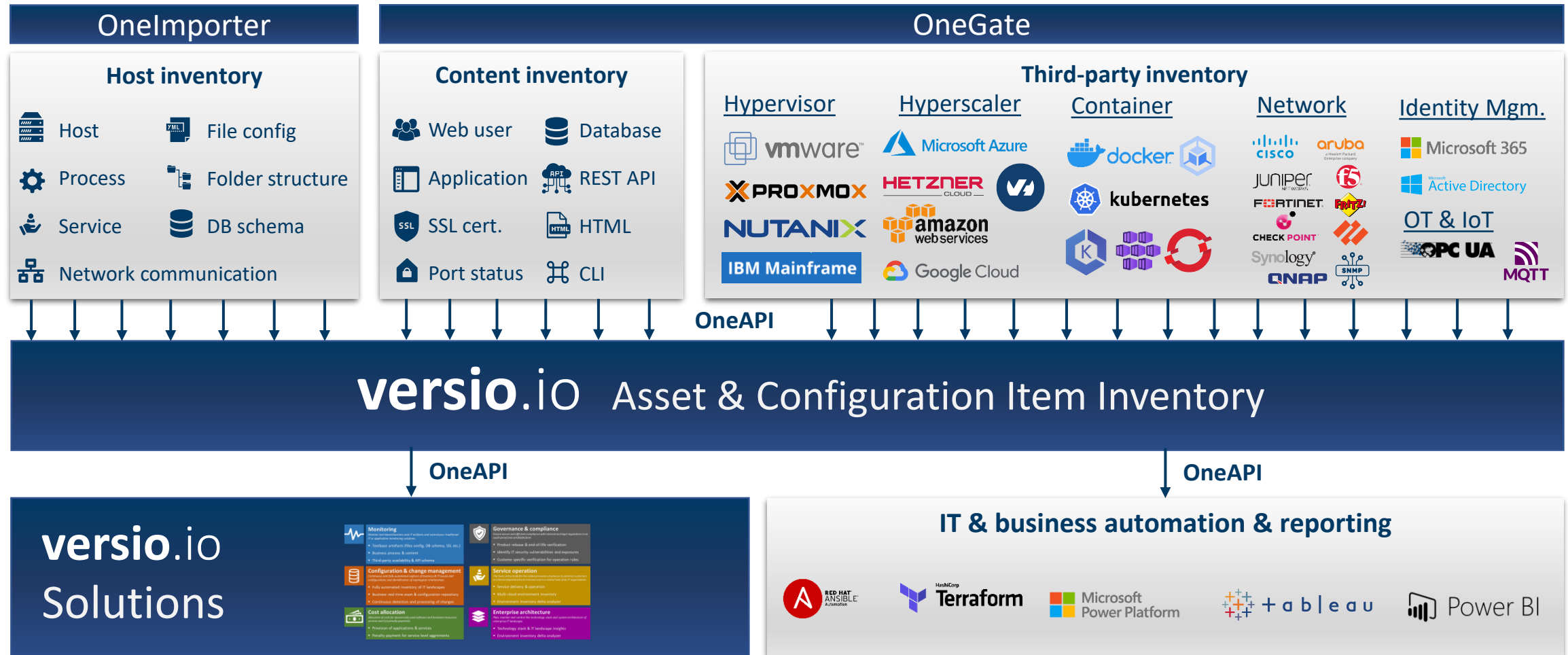
© 2024 | Versio.io | Inventory | Cybersecurity | Governance | IT Event



Versio.io is a **software solution** that offers a central **asset & configuration inventory** for business and IT, **detects their changes** and **processes them.**

Versio.io in nutshell

Data integrations, asset & configuration inventory and solutions



Versio.io Insights

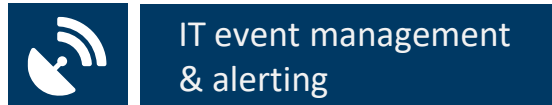
© 2024 | Versio.io | Inventory, change monitoring, cybersecurity, policies, event & logs



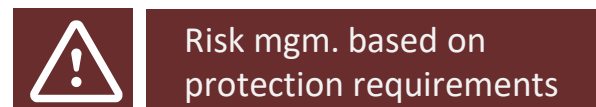
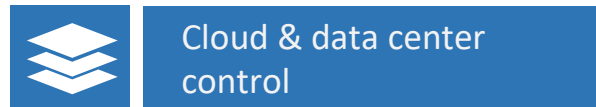
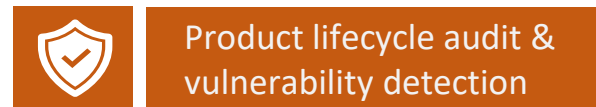
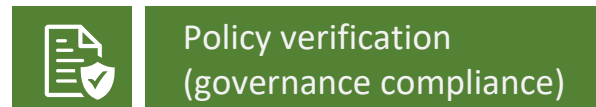
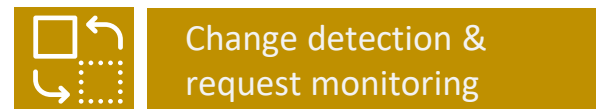
Versio.io in a nutshell

Solutions for an innovative, cost-effective and secure DevOps & IT Operating Management

Versio.io core



Versio.io solution



Customer motivation

- Ensure information availability
- Manage complexity
- Minimize employee effort
- Ensure IT governance compliance (security, operations, regulatory, business)
- Optimize business and IT processes
- Increase service availability
- Enable controllability of deployed technologies
- Increase the degree of automation

➔ **Reduce IT risks and costs**

Versio.io Event Management & Alerting

Agenda

1. Versio.io fundamentals
2. Event management fundamentals
3. Import IT events (PE)
4. Event features (PE)
 - Inventory Integration (Digital Twin)
 - Close events
 - Archive events
 - Event deduplication (event storm)
5. Coffee & tea break - 10 min
6. Event analysis (PE)
 - Event filtering
 - Event insight dashboard
 - Event explorer
7. Alerting (PE)
 1. Event selection
 2. Actions
 3. Action „Event reference instance“
8. Subscription model
9. Questions & Answers

* PE = Practical exercise

Online training

Versio.io Event Management & Alerting

Fundamentals of IT event management

- What: An IT event refers to a specific state or action of an IT infrastructure, system or component.
- Why: IT events are control-relevant information to ensure stable IT operations.
- Challenge: The frequency of events and the quality of the event message depend on the IT component.

Which IT components create events?

- Server & Desktops
- Network devices
- Printer
- Hypervisor
- Hyperscaler
- Kubernetes
- OT/IoT devices
- 3-party systems / apps
- ...

What are the reasons for creating events?

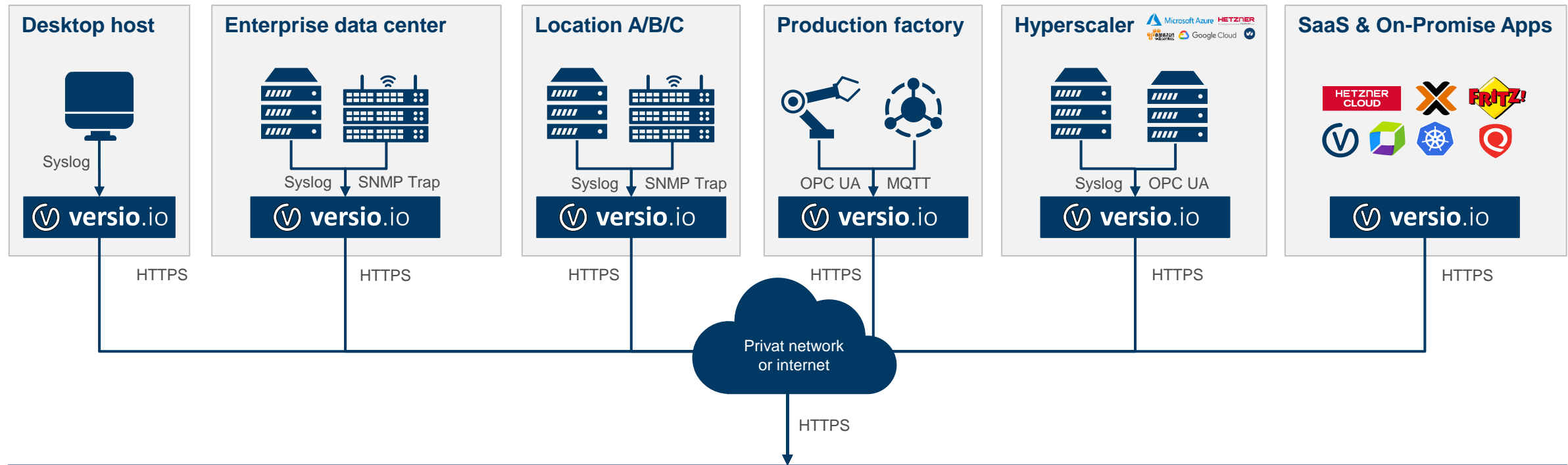
- System infos
- Security alerts
- User activities
- Network events
- Failed functions
- Capacity limits
- Health status
- ...

Why do I need the events for IT/OT/IoT operations?


- Monitoring and fault detection
- Safety management
- Performance optimization
- Compliance and auditing
- Automation and responsiveness
- Capacity planning
- Error cause analysis
- Documentation and transparency
- ...

Versio.io Event Management & Alerting

An enterprise event management for the full IT, OT, IoT, cloud, factory and app landscape



versio.io Event Management

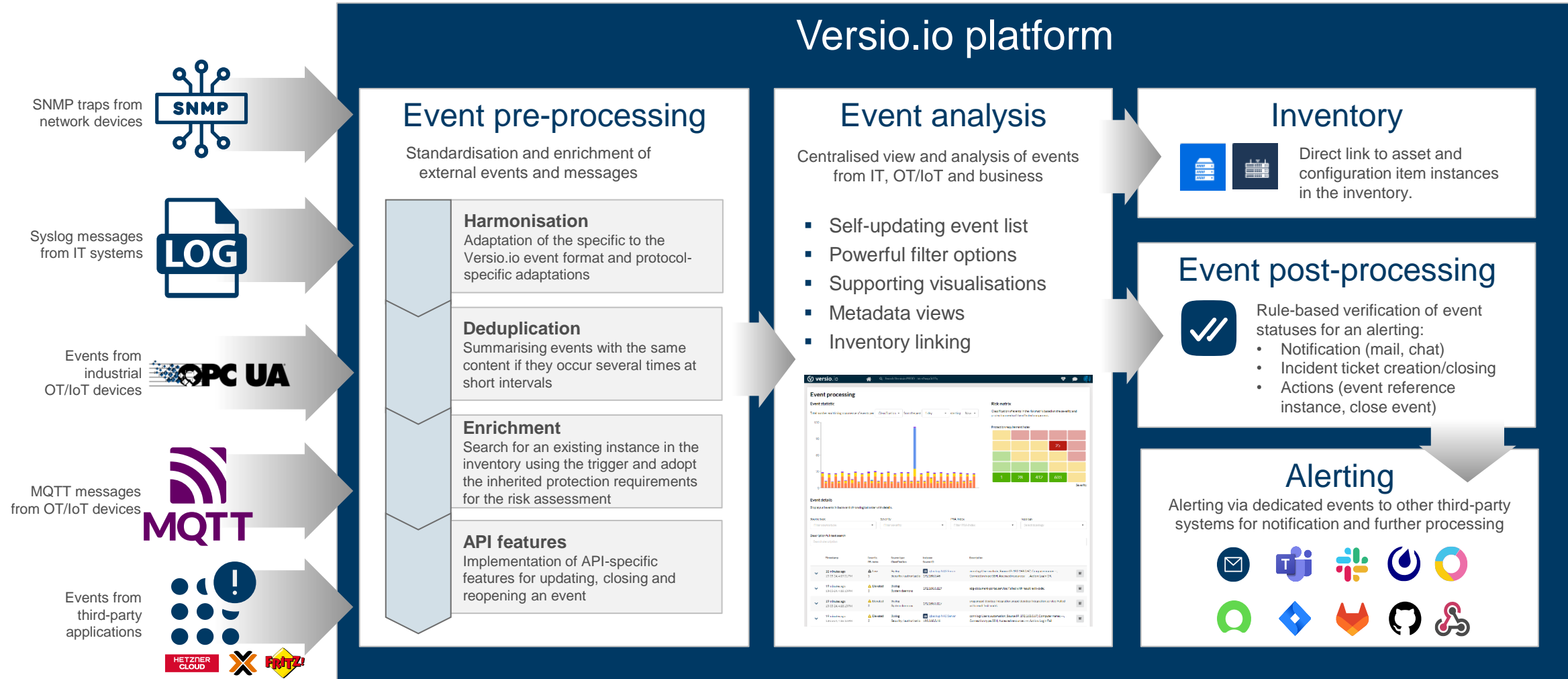
 = Versio.io OneGate

Online training



Versio.io Event Management & Alerting

Unified and centralised processing of IT, OT/IoT, third-party and business events

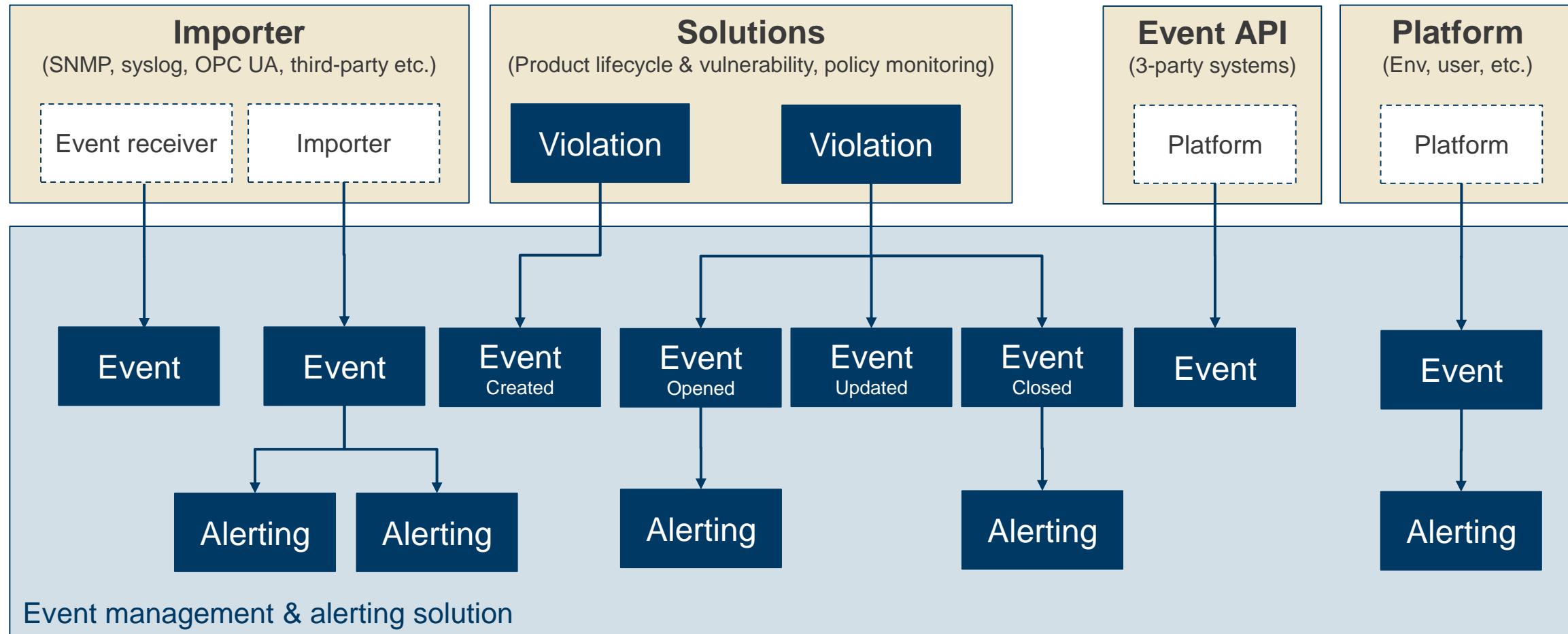


Online training



Versio.io Event Management & Alerting

Relationship between violations, events & alerting



Versio.io Event Management & Alerting

Markt positioning and unique selling points



Target customers

- Future-oriented technological focus on cloud, multi-location and API-based approaches for centralised IT event management.
- Processing of technical and business events from third-party systems, applications and standard event protocols in the order of 1,000 to 100 million events.
- Automatic linking between IT events and existing assets & configuration items in the inventory for more information availability.
- Unique Versio.io events based on changes to assets & configuration items and monitoring of compliance with internal and regulatory guidelines.



No target customers

- Terabyte orientated log file events with long-term storage (classic log file management).

Unique selling points

- + Recording and centralisation of IT events from various locations (data centre, cloud, SaaS, internet)
- + Manufacturer-independent processing of IT and business events (REST API)
- + Event Insights Dashboard enables even beginners to analyse and identify key events
- + Consolidation of the status of a trigger across the entire history of IT events (event reference instance)
- + Bi-directional integration between IT events and inventoried assets & configuration items
- + Inclusion of customer-specific protection requirements in the risk assessment of the IT event
- + Free choice of data location (Versio.io SaaS in Germany or Versio.io on-premise in the customer's preferred location)
- + Support of version 1, 2 and 3 for the Simple Network Management Protocol (SNMP)

Online training



Versio.io Event Management & Alerting

Agenda

1. Versio.io fundamentals
2. Event management fundamentals
3. Import IT events (PE)
4. Event features (PE)
 - Inventory Integration (Digital Twin)
 - Close events
 - Archive events
 - Event deduplication (event storm)
5. Coffee & tea break - 10 min
6. Event analysis (PE)
 - Event filtering
 - Event insight dashboard
 - Event explorer
7. Alerting (PE)
 1. Event selection
 2. Actions
 3. Action „Event reference instance“
8. Subscription model
9. Questions & Answers

* PE = Practical exercise

Online training

Versio.io Event Management & Alerting

Import IT event messages

How to import event messages into Versio.io:

- Event receiver at OneGate for standard protocols

- SNMP Traps
- Syslogs
- MQTT



- OneGate importer

- OPC UA
- Kubernetes
- Hetzner Cloud
- Proxmox
- Fritz!Box
- etc.



- Event API

- Custom specific events (Qualys, CRM, ERP, ...)

Advantages of the Versio.io approach:

- The Event Receiver enables the capture of events based on **standard protocols** in any network zone (cloud, data centre, dedicated host, etc.).
- Versio.io **ready to use integration** with minimal configuration and no implementation effort.
- The open API can easily be used to capture **customised and individual events**.

Online training

Versio.io Event Management & Alerting

Import event messages - Event receiver configuration for generic event protocols

SNMP traps

Configuration for receiving SNMP traps.

Capture **Port**

Allow SNMPv3 **SNMPv3 User** **SNMPv3 security level** **SNMPv3 auth protocol** **SNMPv3 auth key** **SNMPv3 priv protocol** **SNMPv3 priv key**

Syslog

Configuration for receiving syslogs.

Capture **Port** **Protocols**

Location

Executing OneImporters
Specify all OneImporters on which the importer configuration is to be executed.

Online training



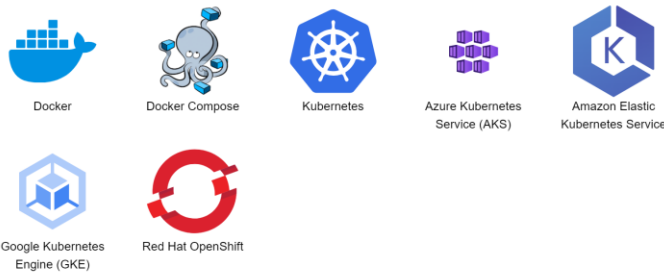
Versio.io Event Management & Alerting

Import event messages - Importer configuration for third-party integrations

Cloud & hosting platforms



Kubernetes & container platforms



Hypervisor & Mainframe



Operational technologies



Online training

Proxmox Virtual Environment access

Configuration for access to query the data instances.

Server URL

Credential (API token)

[Need help?](#)

Select Proxmox Virtual Environment entities to import

Select the desired entities to be imported from Proxmox Virtual Environment. The entity name consists of the name of the entity to be imported plus the entity suffix (e.g. 'cluster-pve').

Entities: all|clear

Instance modification

Before saving an instance, it can be modified to adjust attribute names and values (mask, hash, delete, regex, rename).

Event detection

Configure which types of events should be imported.

Severities: all|clear

Versio.io Event Management & Alerting

Import event messages - Event API

- The Event Rest API is secured by HTTPS and API tokens.
- Auto update and reopen feature.
- Creation of customer events based on the Versio.io Event REST API:

```
POST {{baseUrl}}/api-versio.eventProcessing/1.0/environments/{{environment}}/events HTTP/1.1
Authorization: apiToken {{apiToken}}
Content-Type: application/json

[
  {
    "sourceType": "Qualys",
    "trigger": "192.168.0.102",
    "externalIdLink": "http://qualys.com?id=EVENT-12345",
    "severity": 4,
    "classification": "Security vulnerability",
    "message": "Very long description text",
  }
]
```

Versio.io Event Management & Alerting

Import event messages - Practical exercise

What we want to see and understand live in the practical exercise!

■ Event Receiver

- Installation and configuration of event receiver for SNMP trap and Syslog
- Configure a Syslog event forwarding on a Linux host (host test-training)
- Configure a SNMP trap on a network device (QMETHODS NAS)
- Create your own OneGate to receive local SNMP or Syslog events

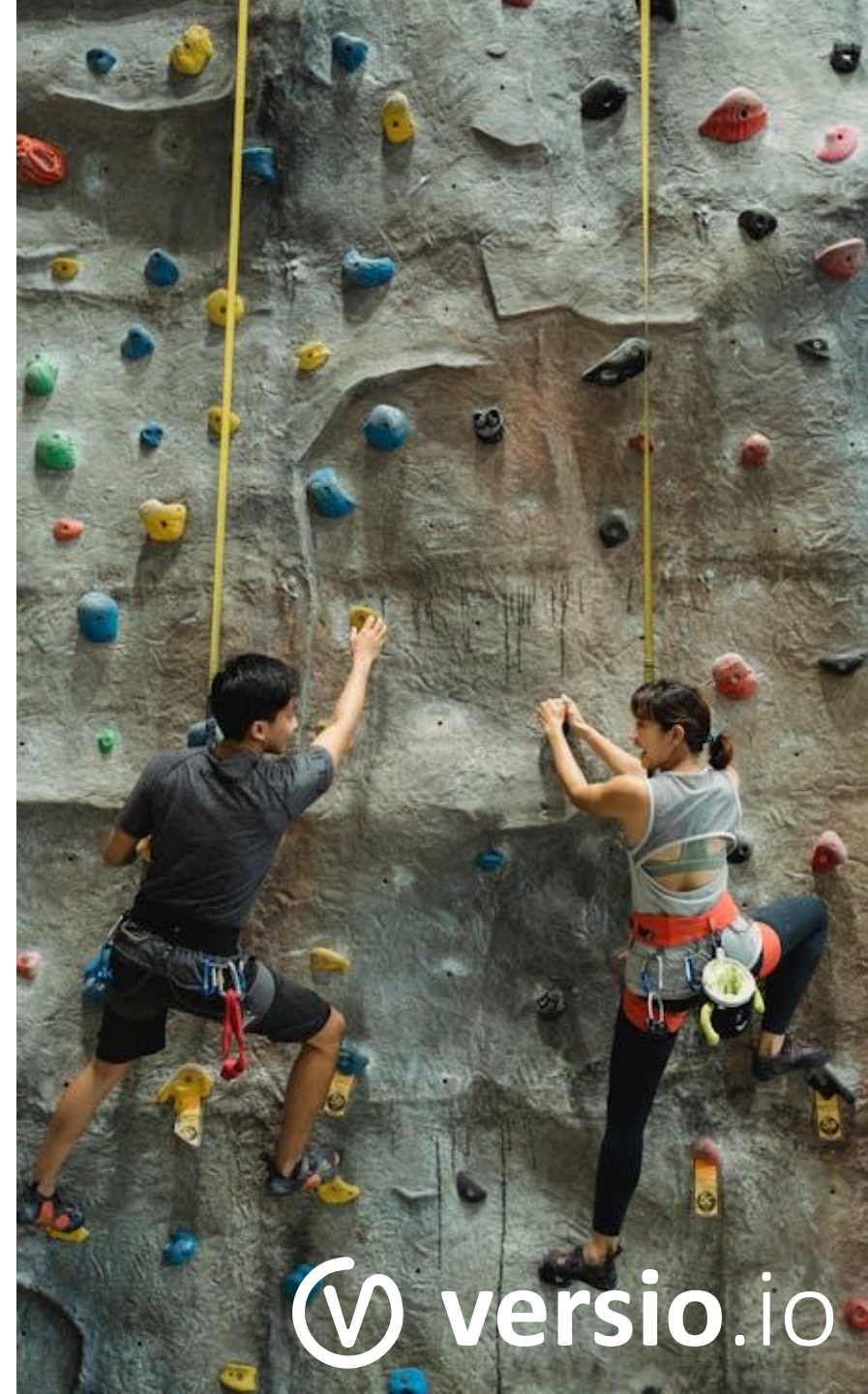
■ Importer

- Activate event detection for a hypervisor importer (Proxmox)

■ API

- Create event via Versio.io REST API
- Create your own events via REST API

Online training



Versio.io Event Management & Alerting

Agenda

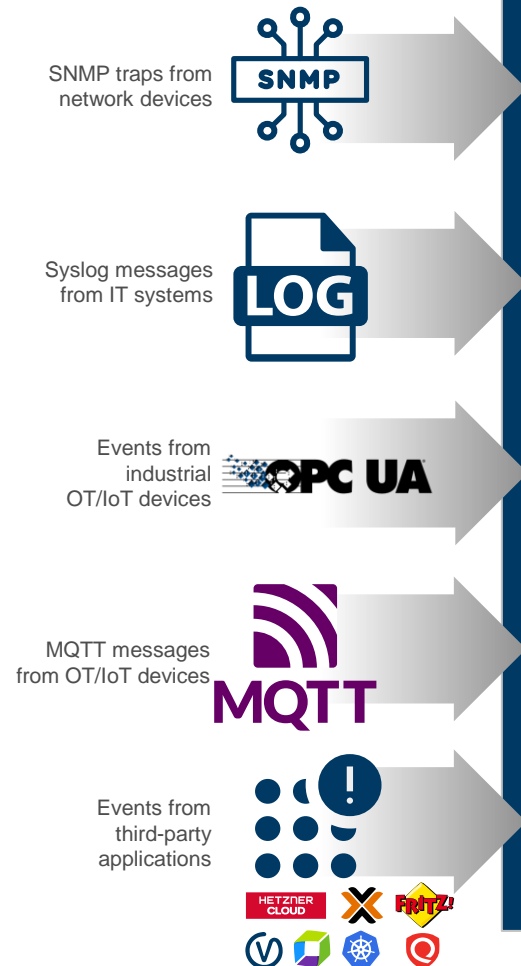
1. Versio.io fundamentals
2. Event management fundamentals
3. Import IT events (PE)
4. Event features (PE)
 - Pre-processing
 - Inventory Integration (Digital Twin)
 - Close events
 - Archive events
 - Event deduplication (event storm)
5. Coffee & tea break - 10 min
6. Event analysis (PE)
 - Event filtering
 - Event insight dashboard
 - Event explorer
7. Alerting (PE)
 1. Event selection
 2. Actions
 3. Action „Event reference instance“
8. Subscription model
9. Questions & Answers

* PE = Practical exercise

Online training

Versio.io Event Management & Alerting

Event pre-processing



Event pre-processing

Standardisation and enrichment of external events and messages

Harmonisation

Adaptation of the specific to the Versio.io event format and protocol-specific adaptations

Deduplication

Summarising events with the same content if they occur several times at short intervals

Enrichment

Search for an existing instance in the inventory using the trigger and adopt the inherited protection requirements for the risk assessment

API features

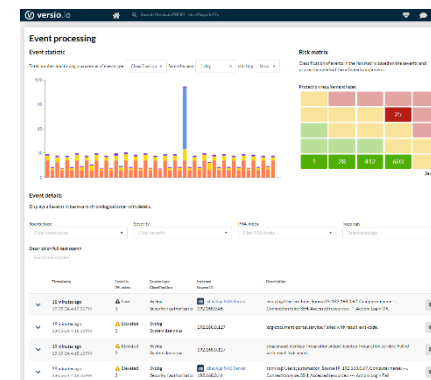
Implementation of API-specific features for updating, closing and reopening an event

Versio.io platform

Event Analysis

Centralised view and analysis of events from IT, OT/IoT and business

- Self-updating event list
- Powerful filter options
- Supporting visualisations
- Metadata views
- Inventory linking



Inventory

Direct link to asset and configuration item instances in the inventory.

Event post-processing

Rule-based verification of event statuses for an alerting:

- Notification (mail, chat)
- Incident ticket creation/closing
- Actions (event reference instance, close event)

Alerting

Alerting via dedicated events to other third-party systems for notification and further processing



Online training

Versio.io Event Management & Alerting

Event details

- Event root cause
 - **Trigger:** Who created the event (e.g. IP, Produkt-ID)?
 - **Event type:** How was the event transmitted to Versio.io (e.g. Syslog)?
 - **Recipient of the event:** Which Versio.io component was used to receive the event (Event Receiver, Importer, API)?
 - **Deduplicated event:** How often has the same event been sent in a period of time (event storm)?
 - **Event core information:** Time, message and ratings for the event
 - **Inventory relation:** Is there a reference for the trigger in the inventory?
- Features
 - **Share** an event via deep link in an email
 - **Archive** an event to protect it from being deleted
 - **Close** an event to filter it out in the event view
 - **View raw data** of the event as Versio.io received it

The screenshot displays the 'Event details' page in the Versio.io interface. At the top, it shows the event ID: 'Event: a-1d83bcd9-3fe6-41c8-a256-f3020dd99eec'. The main content is organized into several sections:

- Event root cause:** A section explaining the root cause and providing a deep link to the instance.
- Trigger:** A box containing the IP address '192.168.0.230'.
- Syslog (TCP):** A box indicating the event type.
- Event receiver:** A box identifying the receiver as 'OneGate: prod-one-importer'.
- Event storm:** A visualization showing a storm of 5,168,088 events over a 7h 51m period, with a timeline from 'Thu, 12-09-24, 2:27 PM' to 'Thu, 12-09-24, 10:18 PM'.
- Details:** A table of event statistics:

Deduplication ID	f3a4171e8e354986af7fc383d7218fedd296832f
First appearance	12-09-24, 2:27:02 PM - 7 days ago
Last appearance	12-09-24, 10:18:40 PM - 7 days ago
Storm duration	7h 51m
Number of events	5,168,088
Events per minute	~10958
- Event message:** A box showing the message 'detected empty handle'.
- Assessment:** A section with 'Severity: High', 'PR-Index: 3', and 'Classification: System daemons'.
- Risk matrix:** A 4x4 grid of colored squares (yellow, red, green) representing risk levels.
- Inventory relation:** A box at the bottom showing a reference to 'pve' in the inventory.

Versio.io Event Management & Alerting

Event details - Inventory integration

- For the event trigger, we try to find the adequate instance in the Versio.io inventory so that all information is easily available to you.
- Furthermore, we take over the protection requirements of the instance for the event in order to be able to position it in the risk matrix.

Instance history viewer
Get an overview of the state changes over the entire lifetime of the instance.

Current instance state

Display name	pve
Last boot time	Thu, 12-09-24, 10:19 PM
Operating system (10)	
System (13)	
Manufacturer	Intel(R) Client Systems
Product name	NUC107FNH
Version	K61081-307
Serial number	GEFND07004L9
Uuid	32263161-4b3d-e3c3-a7a2-1c697a615...
Bios (5)	
Chassis (8)	
Hardware (5)	
Technology (3)	
Warranty (7)	

Metadata
A summary of all relevant metadata of the instance.

Host

Created	2 years ago	Last change	19 hours ago	Last update	6 minutes ago
	Sun, 21-11-21, 9:41 PM		Thu, 12-09-24, 10:21 PM		Fri, 13-09-24, 10:24 PM

Device image
Below is an image representing the current instance.

Event details

Event root cause
Understand the root cause why this event occurred and use the deep link to jump directly to the corresponding instance.

192.168.0.230
Trigger

Syslog (TCP)
Event type

OneGate: prod-one-importer

Event storm with 5,168,088 events over 7h 51m
Deduplicated events

7h 51m
Thu, 12-09-24, 2:27 PM Thu, 12-09-24, 10:18 PM

Details

Deduplication ID	f3a4171e8e354986af7fc383d7218fdd296832f
First appearance	12-09-24, 2:27:02 PM - 7 days ago
Last appearance	12-09-24, 10:18:40 PM - 7 days ago
Storm duration	7h 51m
Number of events	5,168,088
Events per minute	~10958

7 days ago (12-09-24, 10:18:40 PM)
Event

detected empty handle

Assessment

Severity	High
PR-index	3
Classification	System daemons

Risk matrix

High	High	High	High	High	High
High	High	High	High	High	High
High	High	High	High	High	High
High	High	High	High	High	High
High	High	High	High	High	High
High	High	High	High	High	High

1 entry	Timestamp	Severity PR-index	Event Source Classification	Instance Trigger	Actions	Message
	19 hours ago ⚡ 5m 12-09-24, 10:18:40 PM	High 3	Syslog (TCP) System daemons	pve 192.168.0.230	0 0	detected empty handle

Online training

Versio.io Event Management & Alerting

Features: Close event

- Why?
 - With the “Closed” status, you can mark an event to indicate to other users that no further analysis is required.
- How?
 - Manually: “Close” and “Reopen” button in the event detail view
 - Automated: Use the action “Close event” in the alerting

The screenshot displays the Versio.io interface for an event. The top navigation bar shows the Versio.io logo, a home icon, and a search icon. Below the navigation bar, the breadcrumb trail reads "Event processing > Event: a-7d1698b0-90f2-4d3d-bc88-1341ced86aa7". The main content area is titled "Event details" and features a sidebar on the left with buttons for "Share", "Archive", "Close" (highlighted with a red box), and "View raw data". The main content area is divided into several sections: "Event root cause" with a description, "167.235.139.171" (Trigger), "Syslog (UDP)" (Event type), "OneGate: prod-internal" (Event receiver), "2 hours ago (17-08-24, 1:02:39 PM)" (Event), "Timed out waiting for device /dev/disk/by-id/scsi-OHC_Volume_35299227." (Event description), "Assessment" section with "Severity: High", "PR-Index: 9", and "Classification: System daemons", and a "Risk matrix" grid. At the bottom, there is an "Inventory relation" section for "prod-internal".

Versio.io Event Management & Alerting



















Features: Close event

Event details
Displays all events in backward chronological order with details.

Event source: Filter event source
Classification: Filter classification
Severity: Filter severity
PRA-Index: Filter PRA-Index
Grouping: Filter grouping

Archived: Filter archived
Closed: Closed
OneGate: Filter OneGate
Instance/Trigger full-text search: Search source
Actions: Filter actions

Topology: Select topology
Entity: Select entity
Message full-text search: The dataset passed the rule.

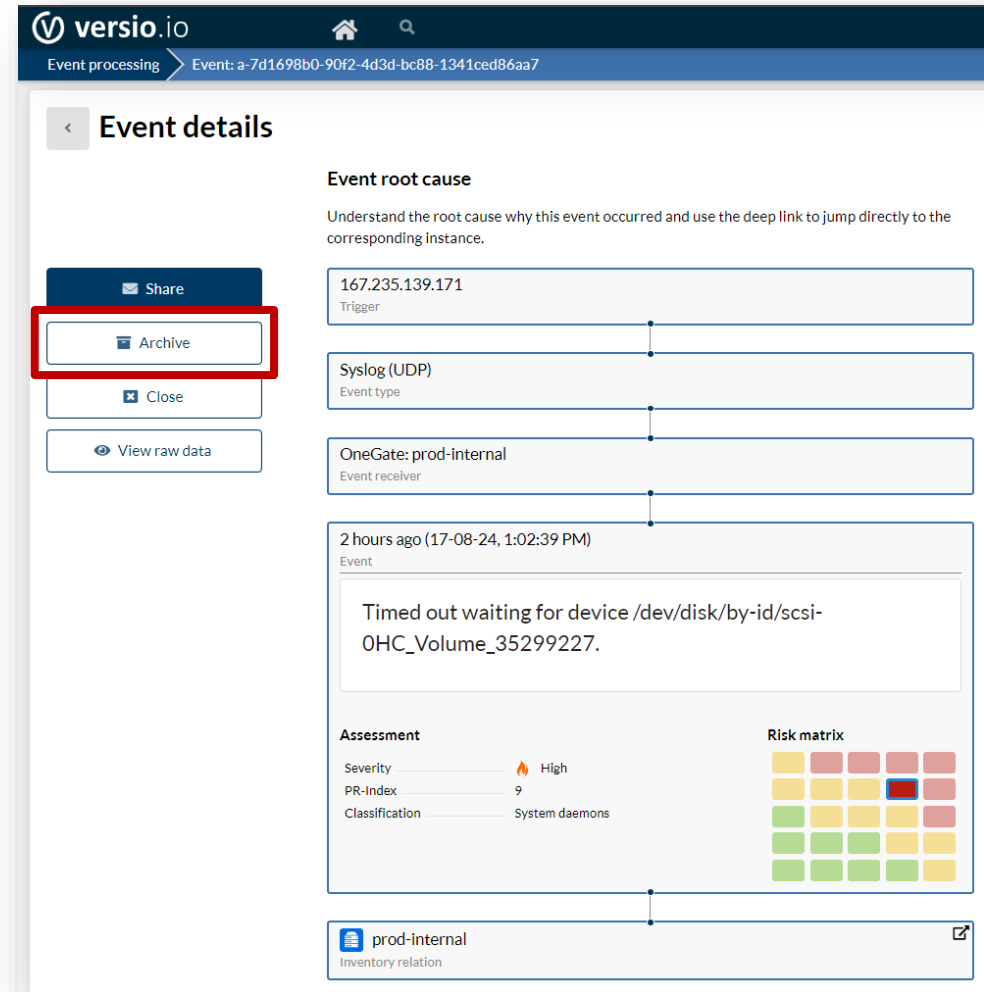
649 entries	Timestamp	Severity PR-index	Event Source Classification	Instance Trigger	Actions	Message
 	2 hours ago 17-08-24, 1:02:39 PM	 Significant 9	Syslog (UDP) System daemons	 prod-internal	 	Dependency failed for /mnt/HC_Volume_35299227
 	2 hours ago 17-08-24, 1:02:39 PM	 High 9	Syslog (UDP) System daemons	 prod-internal	 	Timed out waiting for device /dev/disk/by-id/scsi-OHC_Volume_35299227.
 	2 hours ago 17-08-24, 1:02:39 PM	 High 9	Syslog (UDP) System daemons	 prod-internal	 	Timed out waiting for device /dev/disk/by-id/scsi-OHC_Volume_35299319.

- Closed events are greyed out in the event list and can be filtered out (default).

Versio.io Event Management & Alerting

Features: Archive event

- Why?
 - With the ‘Archived’ status, you can mark an event to prevent it from being deleted after historisation and to make it easier to find at a later time.
- How?
 - Manually: “Archive” and “Remove from archive” button in the event detail view.



The screenshot displays the 'Event details' page in the Versio.io interface. The page title is 'Event details' and the event ID is 'a-7d1698b0-90f2-4d3d-bc88-1341ced86aa7'. On the left sidebar, there are four buttons: 'Share', 'Archive', 'Close', and 'View raw data'. The 'Archive' button is highlighted with a red rectangular border. The main content area shows the event details, including the event root cause, event type, event receiver, event time, and assessment. The event root cause is '167.235.139.171 Trigger'. The event type is 'Syslog (UDP)'. The event receiver is 'OneGate: prod-internal'. The event time is '2 hours ago (17-08-24, 1:02:39 PM)'. The event description is 'Timed out waiting for device /dev/disk/by-id/scsi-OHC_Volume_35299227.'. The assessment shows a severity of 'High', a PR-index of '9', and a classification of 'System daemons'. A risk matrix is also displayed, showing a grid of colored squares (yellow, green, red) representing different risk levels. The inventory relation is 'prod-internal'.

Versio.io Event Management & Alerting

Features: Archive event

- Archived events are displayed specifically in the event list and can be filtered.

Event details
Displays all events in backward chronological order with details.

Event source: Filter event source
Classification: Filter classification
Severity: Filter severity
PRA-Index: Filter PRA-Index
Grouping: Filter grouping

Archived: Archived (selected), Archived, Not archived
Closed: Filter closed
OneGate: Filter OneGate
Instance/Trigger full-text search: Search source
Actions: Filter actions

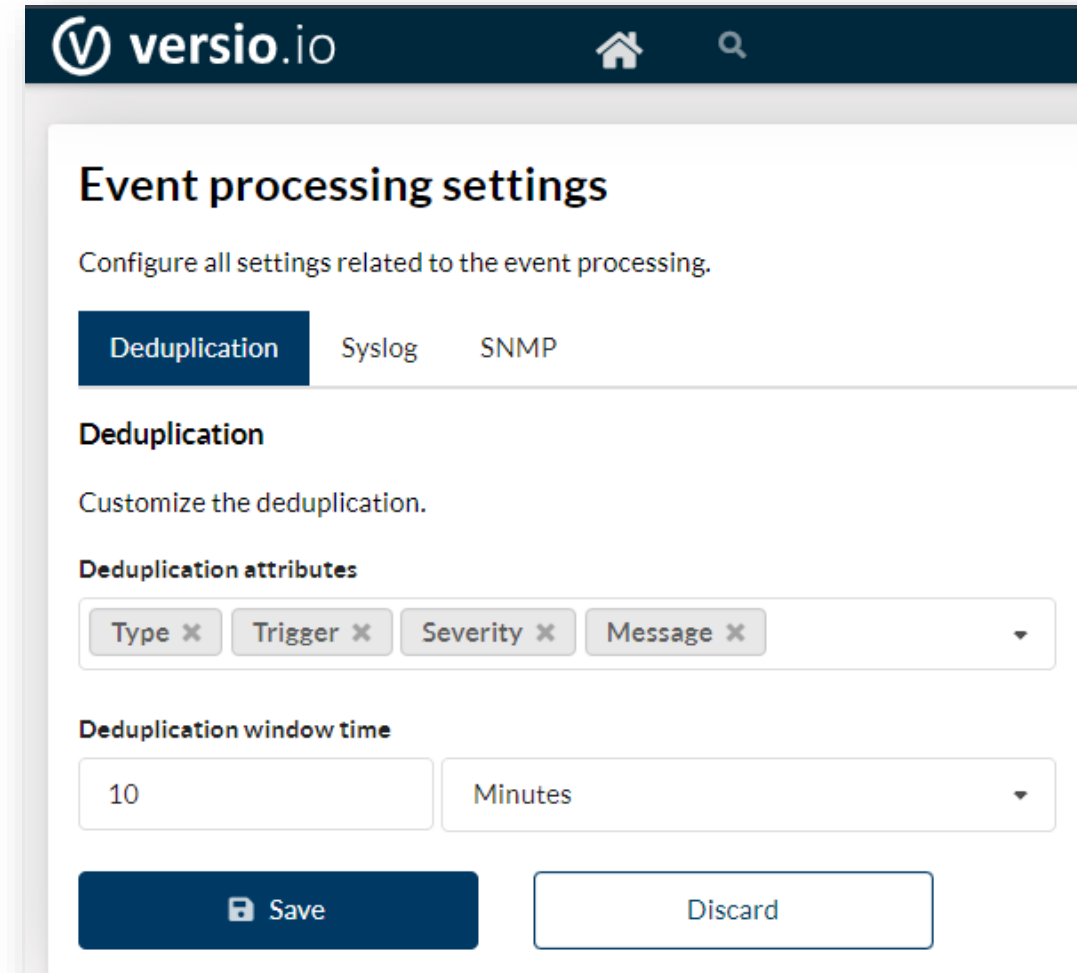
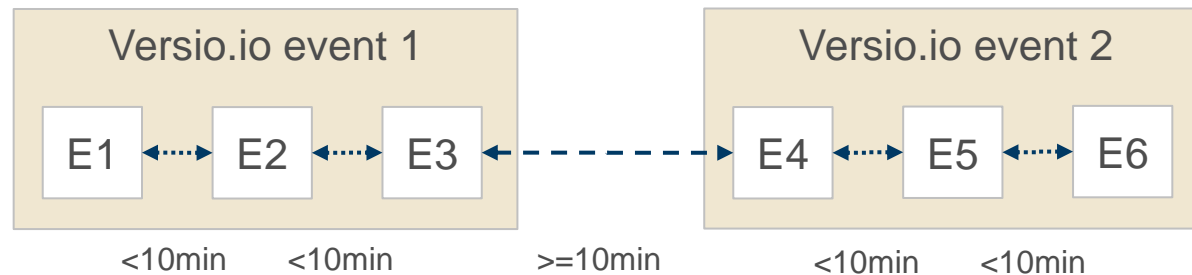
Entity: Select entity
Message full-text search: Time out waiting
Create alerting
Reset filter

7 entries	Timestamp	Severity PR-index	Event Source Classification	Instance Trigger	Actions	Message
	2 hours ago 17-08-24, 1:02:39 PM	High 9	Syslog (UDP) System daemons	prod-internal	0 0	Timed out waiting for device /dev/disk/by-id/scsi-0HC_Volume_35299319.
	2 hours ago 17-08-24, 1:02:39 PM	High 9	Syslog (UDP) System daemons	prod-internal	0 0	Timed out waiting for device /dev/disk/by-id/scsi-0HC_Volume_35299227.
	2 hours ago 17-08-24, 1:02:39 PM	Significant 9	Syslog (UDP) System daemons	prod-internal	0 0	dev-disk-by\x2did-scsi\x2d0HC_Volume_35299227.device: Job dev-disk-by\x2did-scsi\x2d0HC_Volume_35299227.device/start timed out.

Versio.io Event Management & Alerting

Features: Event deduplication

- Event deduplication refers to the process of identifying and summarising multiple events with the same content in a short period of time.
- Advantage of deduplication:
 - Recognising event storms.
 - Reduction of the individual events to be analysed in the event analysis.
 - The number of alerts is reduced.



Online training

Versio.io Event Management & Alerting

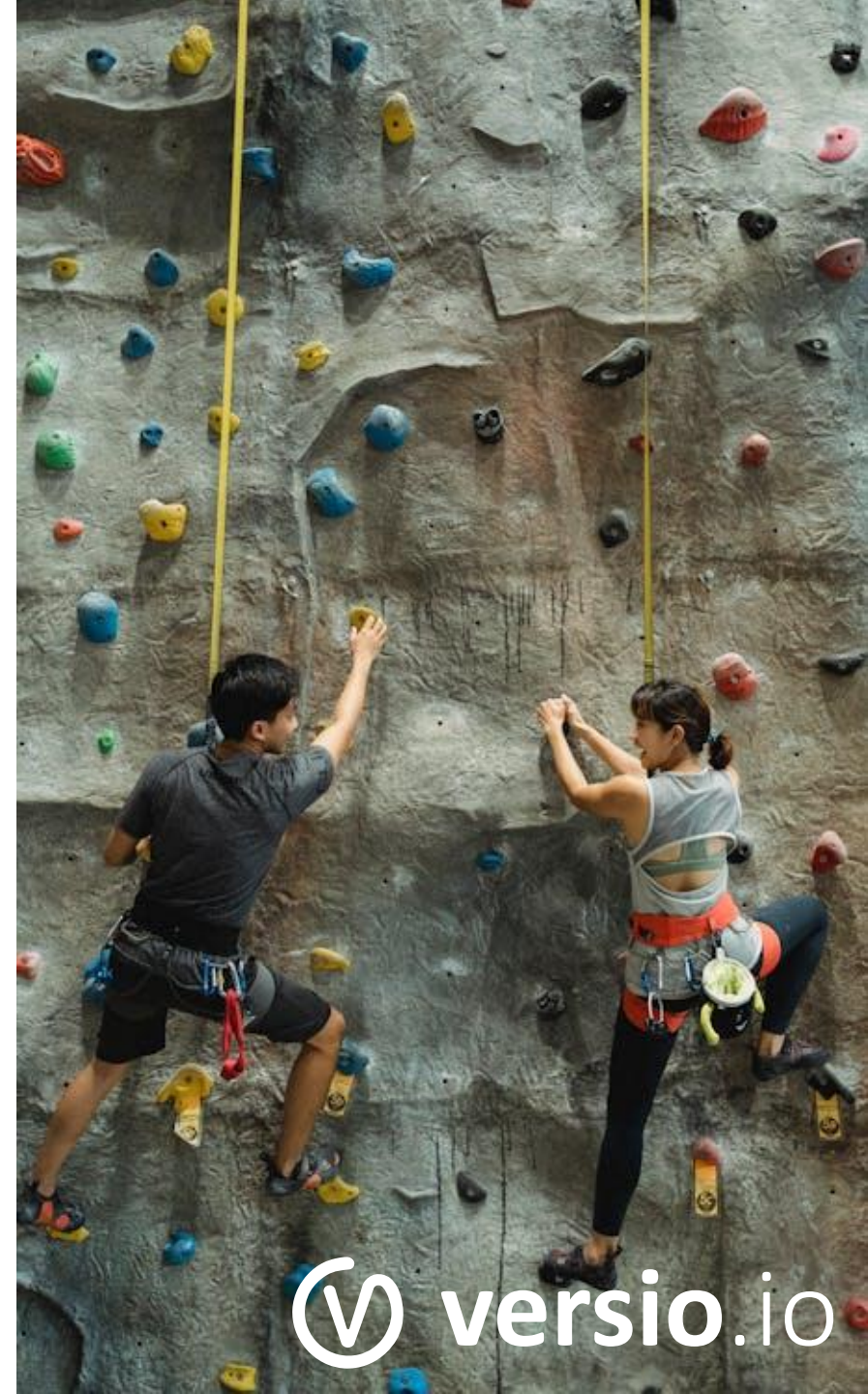
Event details & features - Practical exercise

What we want to see and understand live in the practical exercise!

- Event details
 - Event root cause
 - Inventory integration
 - Event comment
 - Executed actions
- Event features
 - Share
 - Close
 - Archive
 - Deduplicated events

Online training

© 2024 | Versio.io | Inventory | Cybersecurity | Governance | IT Event



Versio.io Event Management & Alerting

Agenda

1. Versio.io fundamentals
2. Event management fundamentals
3. Import IT events (PE)
4. Event features (PE)
 - Pre-processing
 - Inventory Integration (Digital Twin)
 - Close events
 - Archive events
 - Event deduplication (event storm)
5. Coffee & tea break - 10 min
6. Event analysis (PE)
 - Event filtering
 - Event insight dashboard
 - Event explorer
7. Alerting (PE)
8. Event reference instance (PE)
9. Subscription model
10. Questions & Answers

* PE = Practical exercise

Online training

© 2024 | Versio.io | Inventory | Cybersecurity | Governance | IT Event



Versio.io Event Management & Alerting

Agenda

1. Versio.io fundamentals
2. Event management fundamentals
3. Import IT events (PE)
4. Event features (PE)
 - Pre-processing
 - Inventory Integration (Digital Twin)
 - Close events
 - Archive events
 - Event deduplication (event storm)
5. Coffee & tea break - 10 min
6. Event analysis (PE)
 - Event filtering
 - Event insight dashboard
 - Event explorer
7. Alerting (PE)
 1. Event selection
 2. Actions
 3. Action „Event reference instance“
8. Subscription model
9. Questions & Answers

* PE = Practical exercise

Online training

Versio.io Event Management & Alerting

Event filter

- Strong filter options are available for the event analysis and list:
 - Period of occurrence
 - Event characteristics
- The filter configuration is deep-link capable.
- By default, only open events are displayed.

The screenshot displays the Versio.io Event Management & Alerting interface. The main section is titled "Event processing" and includes an "Event statistic" chart showing the total number and timing occurrence of events per [30 minutes] from 11-09-24, 5:00 PM to 12-09-24, 5:00 PM. The chart is a stacked bar chart with a line graph overlay, showing peaks in event occurrence. A red box highlights the filter configuration for the chart, including "Severity", "from the past 1 day", "starting Date", and "12-09-24 04:59 PM".

To the right of the chart is a "Risk matrix" section, which includes a "Protection requirement index" table. The table shows a grid of colored cells representing risk levels, with numerical values in some cells. The values are: 6, 4, 27, 3, 24, 208, 46, 271, 692. The table is labeled "Severity" at the bottom right.

Below the chart is an "Event details" section, which includes a description: "Displays all events in backward chronological order with details." Below this is a filter configuration panel with a red border, containing various filter options:

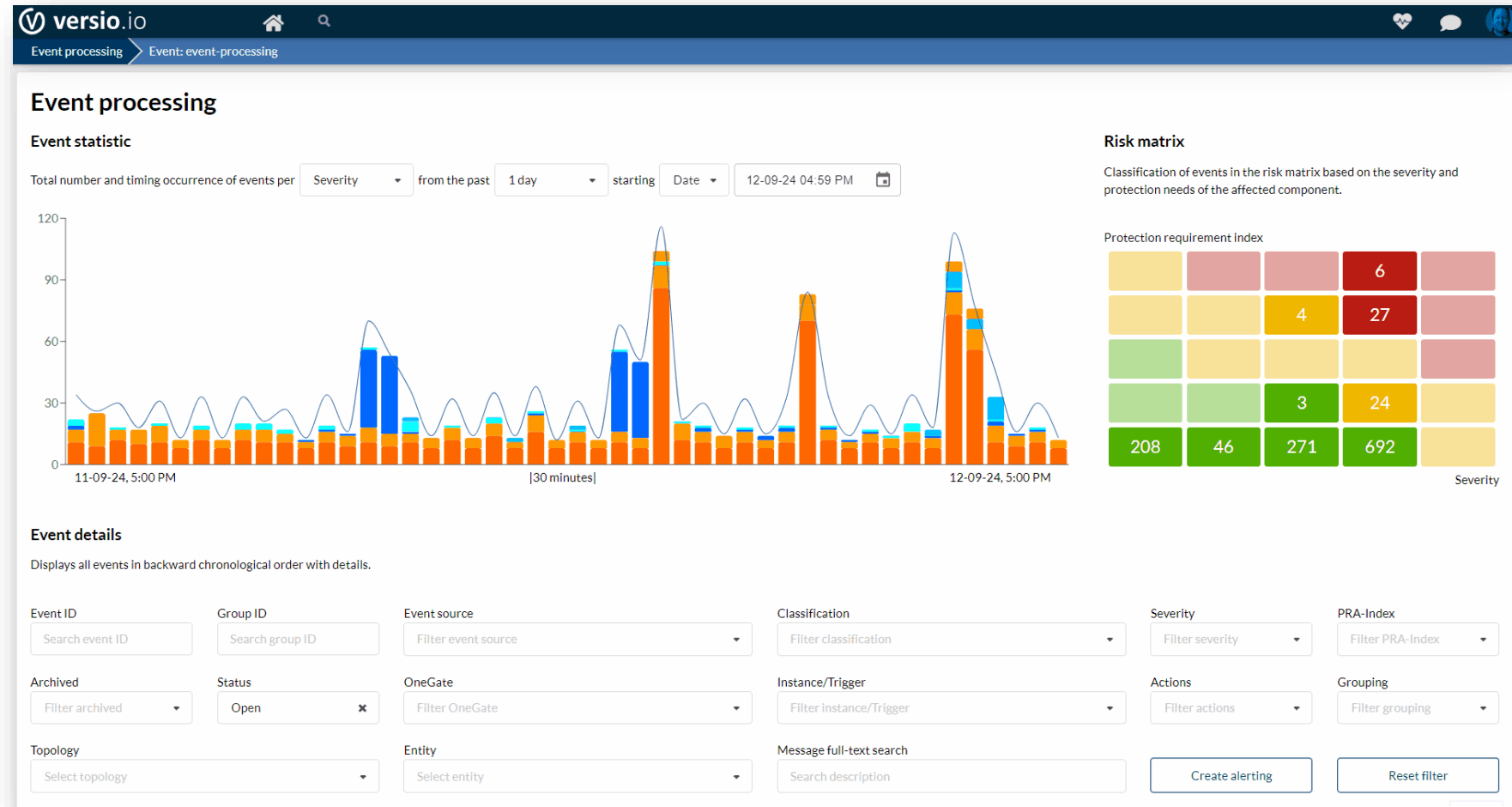
- Event ID: Search event ID
- Group ID: Search group ID
- Event source: Filter event source
- Classification: Filter classification
- Severity: Filter severity
- PRA-Index: Filter PRA-Index
- Archived: Filter archived
- Status: Open
- OneGate: Filter OneGate
- Instance/Trigger: Filter instance/Trigger
- Actions: Filter actions
- Grouping: Filter grouping
- Topology: Select topology
- Entity: Select entity
- Message full-text search: Search description

At the bottom right of the filter panel are buttons for "Create alerting" and "Reset filter".

Versio.io Event Management & Alerting

Event analysing

- Change the visualisation using grouping and filters to easily identify anomalies and outliers.
- Have you recognised the event storm 😊 ?

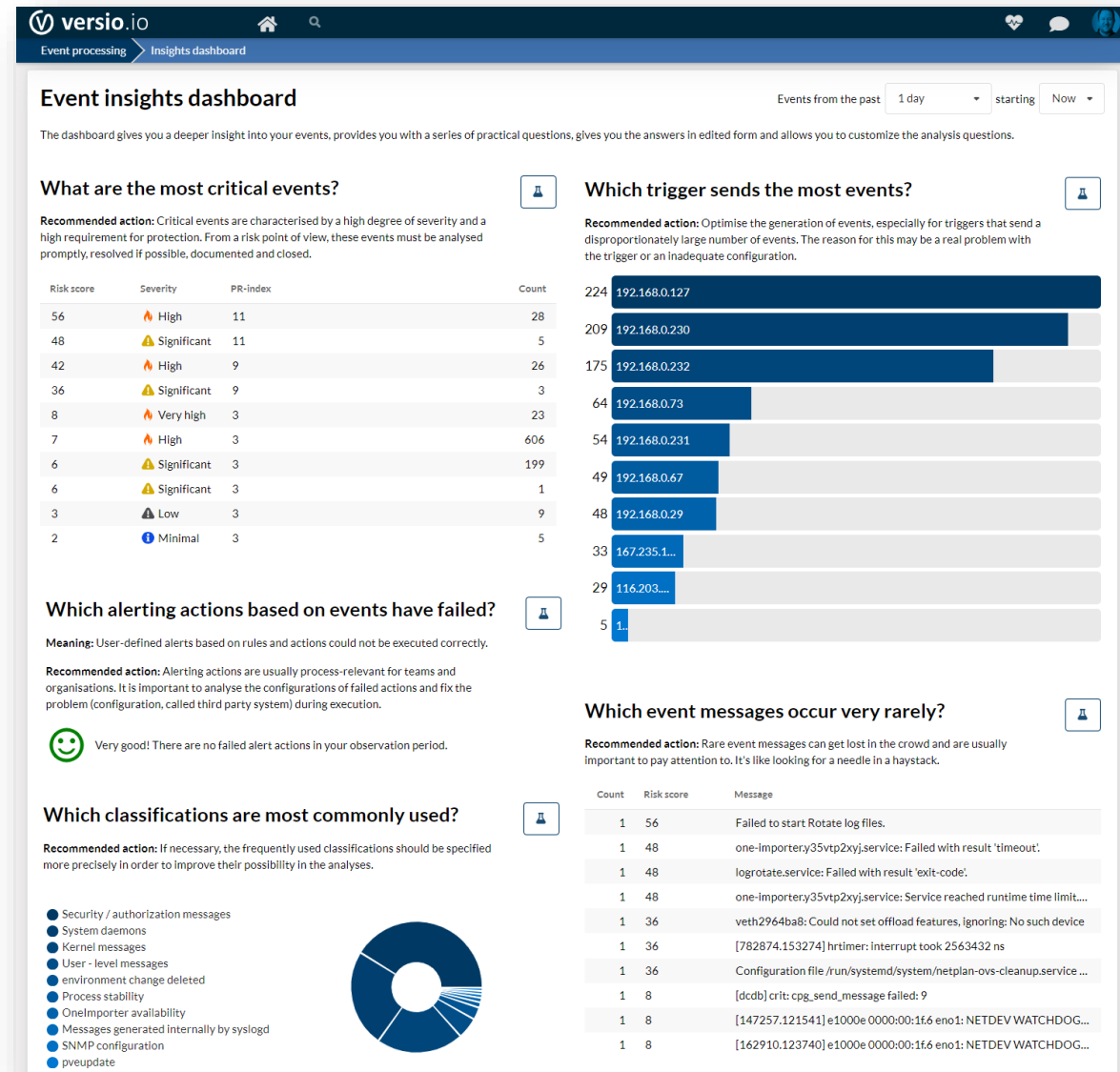


Versio.io Event Management & Alerting

Event insight dashboard

- The Event Insight Dashboard provides you with answers and recommendations for typical questions in IT event management.
- This allows you to identify ...
 - relevant events for problem detection more easily.
 - optimisation potential in the configuration of the individual IT components in your IT landscape.
 - problems in the execution of alerting actions to avoid errors in ITSM/ITOM process integration.

Online training



Versio.io Event Management & Alerting

Event insight explorer

- The Event Insight Explorer offers you analysis and evaluation options for all events, which provide answers to complex questions and can visualise them in different ways.
- The possibility of grouping according to various attributes plays a central role here.

Event insights explorer
Deep dive into all events to create an analysis that meets your demands.

Filter

Date from: 27-08-24 02:00 PM | Date to: 24-09-24 01:59 PM

Event ID: Search event ID | Deduplication ID: Search d. ID | Event source: Filter event source | Classification: Filter classification | Severity: Filter severity | PRA-Index: Filter PRA-Index

Archived: Filter archived | Status: Filter closed | Instance/Trigger: Filter instance/Trigger | Message full-text search: Search description | Actions: Filter actions | Deduplication count: Filter d. count

First appearance: Filter appearance | Topology: Select topology | Entity: Select entity | OneGate: Filter OneGate | Show Less | Reset filter

Grouping (optional) | **Sorting** | **Paging**

Group events: Trigger | Sort events: Summarize count | Page: 1 | Page size: 10

Style

Visualization type: Top list

Result

Count	IP Address
1k	192.168.0.232
1k	192.168.0.127
996	192.168.0.230
666	192.168.0.46
384	192.168.0.231
5	1.
1	1

Online training

Versio.io Event Management & Alerting

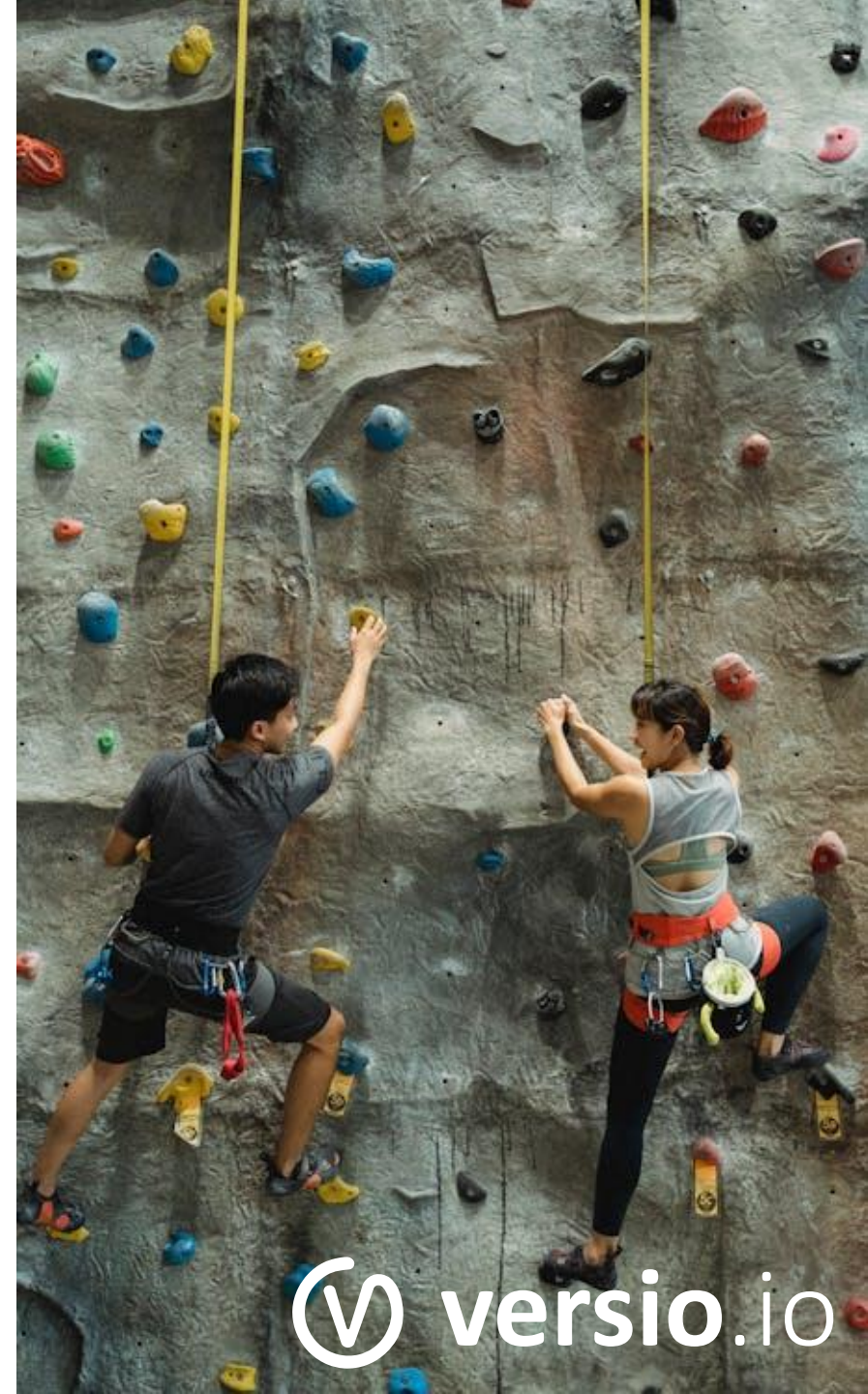
Event analysis - Practical exercise

What we want to see and understand live in the practical exercise!

- Define the observation period
- Analyse events by
 - Attribute grouping (visualisation)
 - attribute filtering (table)
- Use the Event Insights Dashboard to get answers instead of data.
- Create your own complex analysis with the Event Insights Explorer.

Online training

© 2024 | Versio.io | Inventory | Cybersecurity | Governance | IT Event



Versio.io Event Management & Alerting

Agenda

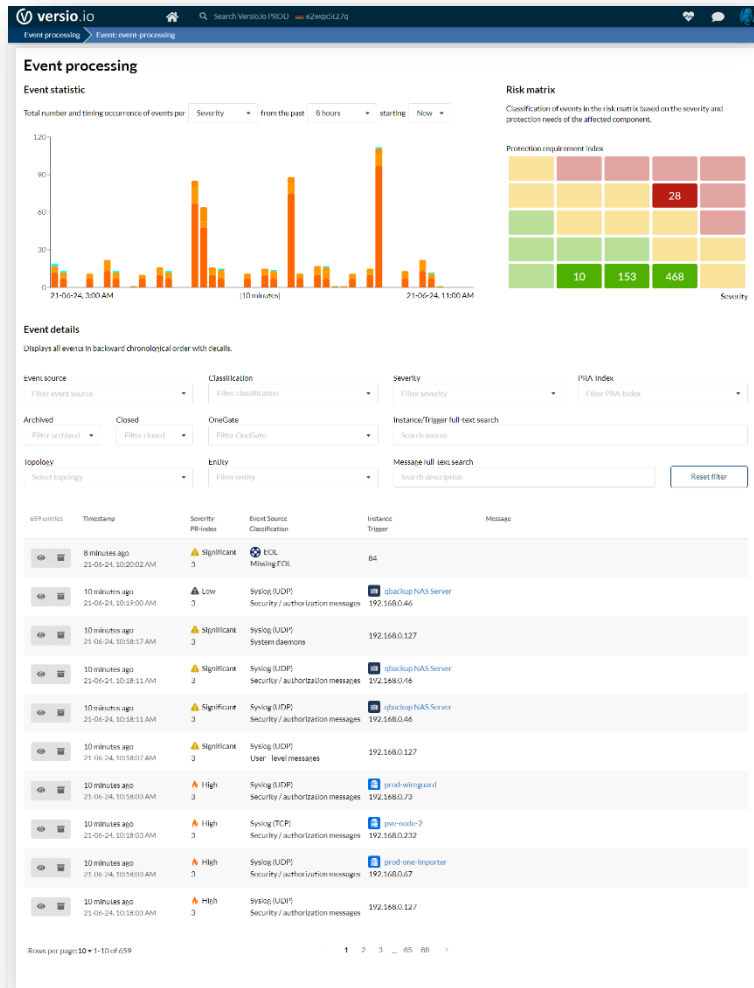
1. Versio.io fundamentals
2. Event management fundamentals
3. Import IT events (PE)
4. Event features (PE)
 - Pre-processing
 - Inventory Integration (Digital Twin)
 - Close events
 - Archive events
 - Event deduplication (event storm)
5. Coffee & tea break - 10 min
6. Event analysis (PE)
 - Event filtering
 - Event insight dashboard
 - Event explorer
7. Alerting (PE)
 1. Event selection
 2. Actions
 3. Action „Event reference instance“
8. Subscription model
9. Questions & Answers

* PE = Practical exercise

Online training

Versio.io Event Management & Alerting

Event post-processing: Alerting & actions



Event Post-Processing

Event selection (filter)

The dataset can be used to define whether each new event should be post-processed.

Alerting

An action can now be executed based on the selected event.

Notification

- E-mail
- Chat
- Luxafor lamp

ITSM

- Incident tickets
- Tasks

Webhook

- Third-party integration

Versio.io internal

- Close event
- Event reference instance

Versio.io Event Management & Alerting

- Why?
 - Versio.io Alerting enables notifications to be sent to users and third-party systems on the basis of events.
 - Alerting therefore supports integration into the existing tool landscape.
- How?
 1. Define the events relevant for alerting on the basis of a filter using a rule or a JavaScript.
 2. Create one or more actions that are to be executed when an alert occurs.

Online training

Alerting & actions

Alerting enables the triggering of individual notifications and actions for a specific group of events

[+ Create](#) [Delete](#)

AVM Benutzer Anmeldung
Close Hetzner "create backup (success)" events
Close real app events
Create Incident Ticket
DevOps compliance
ERI example "Malware Remover completed"
ERI example "Malware Remover started"
ERI example virus scan completed
ERI example virus scan start
Failed batch and EOL&SEC pipeline processes
Luxafor blue light message
Luxafor red light message
Missing EOL data
No office internet connection
Onemporter availability
PVE: close "successful auth for user" events
Website contact and free trial requests
live.versio.io customer feedback

Create Incident Ticket
Created 10 days ago by fabian.klose@versio.io

Name Active

Event selection
From the total number of events, filter out those for which an action should be triggered.

Event rule filter
Rule type: Logical Negate

AND

- classification = EOL & Sec
Primitive attribute check
- severity >= 7
Primitive attribute check

Add inventory relation filter

Actions
Select an action type to be executed when an event occurs and configure it.

GitLab incident

GitLab server URL: Projectname / ID:

Credential (API token):

Versio.io Event Management & Alerting

Alerting - Actions

- Executed actions are displayed in the event details.
- Supported alerting actions:
 - E-Mail
 - Chat
 - Microsoft Teams
 - Mattermost
 - Slack
 - Telegram
 - IT Service Management - create/close incident ticket
 - ServiceNow
 - TopDesk
 - Jira
 - GitHub
 - GitLab
 - Versio.io
 - Close event
 - Event reference instance
 - Sonstige
 - Custom WebHook
 - Luxafor Light

Online training

The screenshot displays the 'Event details' page in the Versio.io interface. The page shows a timeline of events and actions. On the left, there are buttons for 'Share', 'Archive', 'Close', and 'View raw data'. The main content area shows the 'Event root cause' section with a description and a deep link. Below this, there is a list of events and actions, including 'REALUSER-55a2f32731d211363f910349aa3fbaf20b1b94fe' (Trigger), 'Versio.io' (Event type), 'Versio.io event API' (Event receiver), 'Event storm with 10 events over 7m 37s' (Grouped events), and '29 minutes ago (22-08-24, 6:46:06 PM) Event' (Type = 1). The 'Assessment' section shows 'Severity' (Info), 'PR-Index' (3), and 'Classification' (User visit www.versio.io). The 'Risk matrix' is a 4x4 grid of colored squares. Below the event details, there are more actions listed, such as 'User visit www.versio.io' (Verification result created) and '/index.html ::1..' (Inventory relation). On the right, there is a 'Comment' section with a text input and a 'Save' button. At the bottom right, there is a red-bordered box titled 'Executed actions' which lists all actions triggered based on this event in detail, including 'GitLab create incident from 'Create Incident Tic...' and 'Luxafor event from 'Luxafor blue light message''.

Event details

Event root cause
Understand the root cause why this event occurred and use the deep link to jump directly to the corresponding instance.

REALUSER-55a2f32731d211363f910349aa3fbaf20b1b94fe
Trigger

Versio.io
Event type

Versio.io event API
Event receiver

Event storm with 10 events over 7m 37s
Grouped events

29 minutes ago (22-08-24, 6:46:06 PM)
Event

Type = 1.

Assessment

Severity Info
PR-Index 3
Classification User visit www.versio.io

Risk matrix

User visit www.versio.io
Verification result created

/index.html ::1..
Inventory relation

Comment
Write a comment for the exchange in your team.

Markdown

Save

Executed actions
All actions triggered based on this event in detail.

GitLab create incident from 'Create Incident Tic...'
Thu, 22-08-24, 6:38 PM

URL
<https://qgit.qmethods.com/api/v4/projects/36/issues>

Incident ID
2009

Project incident ID
549

Project ID
36

Incident URL
<http://qgit.qmethods.com/internal/itsm/-/issues/549>

Incident name
Versio.io: Versio.io alert - Create Incident Ticket

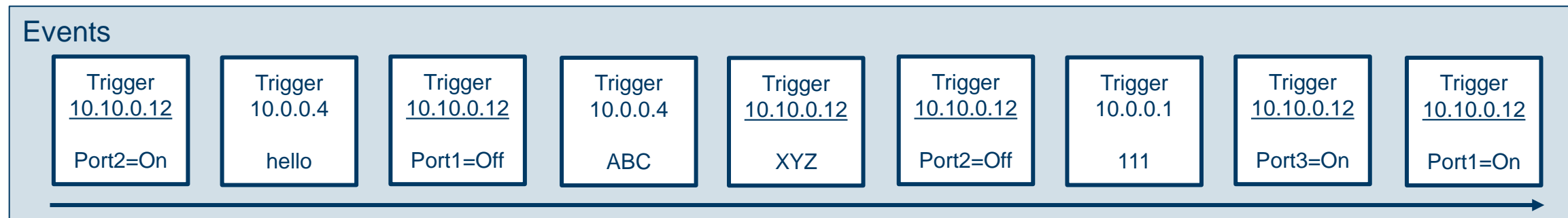
Luxafor event from 'Luxafor blue light message'
Thu, 22-08-24, 6:38 PM

Luxafor event from 'Luxafor blue light message'
Thu, 22-08-24, 6:38 PM

Versio.io Event Management & Alerting

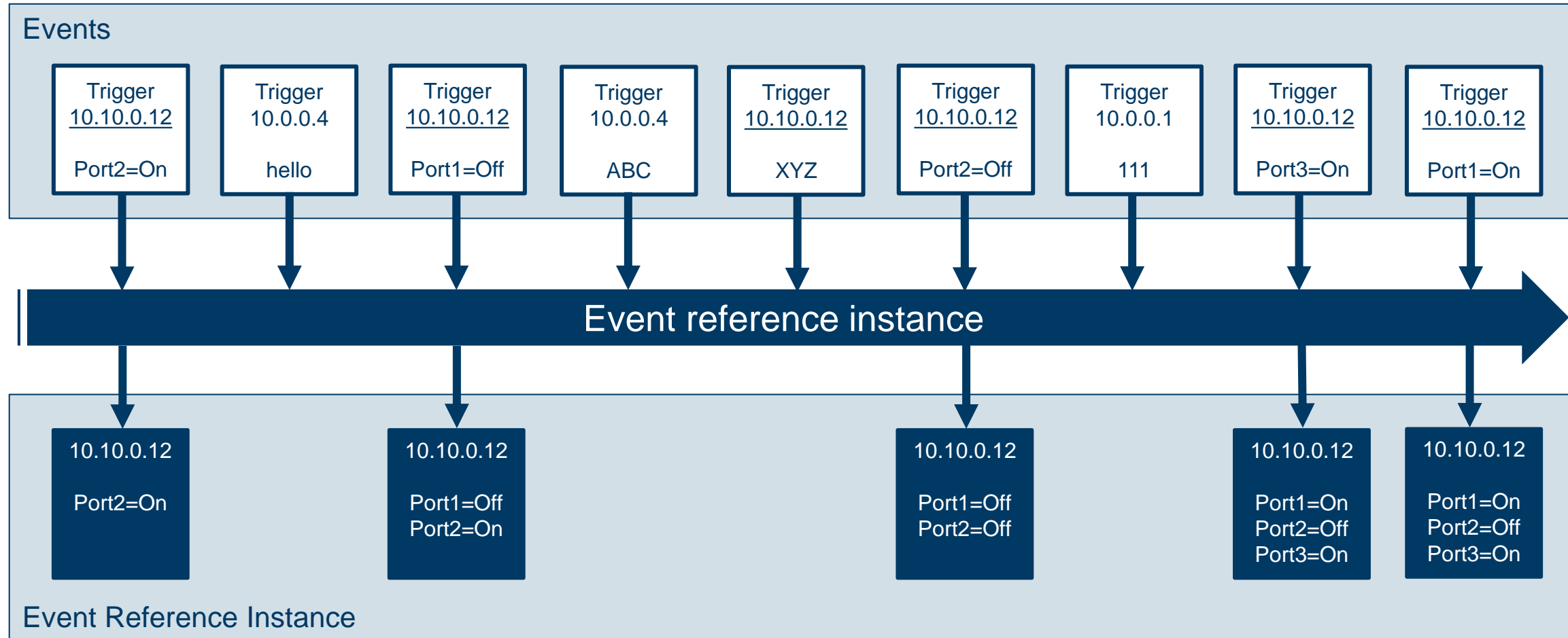
Event reference instance

- The event reference instance is a Versio.io instance per trigger whose status is created from the history of all events and is continuously updated.
- This means that a consolidated current status for a trigger is created from the chronological and content-related summary of all events.
- Application scenarios
 - Network link up/down status of a network device
 - Counter for the throughput of an access restriction (counter per time unit)
 - Recording training registrations (list of names)
- What is the status of the trigger 10.10.0.12, which results from the timed events? :



Versio.io Event Management & Alerting

Event reference instance - Example



Versio.io Event Management & Alerting

Event reference instance - Alert filtering of events for actions & ERI creation/update

- The system checks whether post-processing should take place for each event.
- The following are available:
 - Raw event & Versio.io event
 - Event reference instance
- The rule can be configured visually.
- Rule cancels as soon as a logic is not true.
- Filter criteria
 - Logic & JavaScript
 - Negation
 - Inventory relation instance
 - Entity
 - Topologie
 - Instance

The screenshot shows the 'Event selection' configuration interface. It includes a title 'Event selection' and a subtitle 'From the total number of events, filter out those for which an action should be triggered.' Below this is the 'Event rule filter' section, which has a 'Rule type' dropdown set to 'Logical' and a 'Negate' toggle switch. The main configuration area is a visual logic tree starting with a negation symbol (⊖) and a menu icon (☰). The root node is 'AND', with sub-nodes for 'sourceType = SNMP Trap' and 'message starts with [Malware Remover] Scan completed.'. Each sub-node is labeled 'Primitive attribute check' and has edit and delete icons. At the bottom, there is an 'Add inventory relation filter' section with three buttons: 'Entity', 'Topology', and 'Instance'.

Online training



Versio.io Event Management & Alerting

Event reference instance - ERI creation and update

- The instance modification is used to manipulate the reference object.
- The following data is available here:
 - Versio.io event
 - Raw data of the event from the event source
 - Current event reference instance
- The event reference instance can be manipulated using simple configurations or in the form of JavaScript.

The screenshot shows the 'Event reference instance' configuration page in the Versio.io interface. The page has a light blue header with the Versio.io logo and a trash icon. Below the header, there are two input fields: 'Entity' with the value 'event-reference' and 'ID Attribute' with the value '\$.trigger'. A 'Modifications' section contains a '+ Add' button. Below this, there are three columns: 'Attribute path (JSON-path)' with '\$.malwareScanStatus', 'Modification type' with a dropdown menu set to 'Add/Change attribute value', and 'New attribute value' with 'completed'. There are also buttons for deleting and adding more modifications. At the bottom, there is a code editor with the following JavaScript code:

```
1 // Use STATE object to access the Versio.io instance data of the event reference instance
2 let newState = STATE;
3
4 // Define custom transformation logic like deleting attributes
5 // delete newState.attribute;
6
7 // Use EVENT object to access the Versio.io event data
8 // The EVENT object looks like: {"id":"a-12345678-1234-1234-1234-012345678910","trigger":"192.168.0.139","sourceType":"Syslog","externalIdName":""}
9
10 // You can use complex conditions for transformation
11 if(EVENT.severity > 4){
12   // newState.severityGreater4 = true;
13 }
14
15 // return the new/transformed instance data
16 return newState;
```

Versio.io Event Management & Alerting

Event reference instance - Example

- The current status and the history of changes are always documented in the event reference instance.

14 entries	Timestamp	Severity PR-Index	Event Source Classification	Instance Trigger	Message
	13 hours ago 23-09-24, 3:06:26 AM	High 3	SNMP Trap (UDP) SNMP configuration	qbackup NAS Server 192.168.0.46	[Malware Remover] Scan complete
	13 hours ago 23-09-24, 3:00:07 AM	High 3	SNMP Trap (UDP) SNMP configuration	qbackup NAS Server 192.168.0.46	[Malware Remover] Started scanning.
	15 hours ago 23-09-24, 12:53:21 AM	High 3	SNMP Trap (UDP) SNMP configuration	qbackup NAS Server 192.168.0.46	[Antivirus] Failed to update virus definitions. Please try again later or update the definitions manually.
	18 hours ago 22-09-24, 9:18:49 PM	High 3	SNMP Trap (UDP) SNMP configuration	qbackup NAS Server 192.168.0.46	[Antivirus] Scan job Virus scan completed.
	20 hours ago 22-09-24, 8:00:03 PM	High 3	SNMP Trap (UDP) SNMP configuration	qbackup NAS Server 192.168.0.46	[Antivirus] Scan job Virus scan started.
	37 hours ago 22-09-24, 3:06:47 AM	High 3	SNMP Trap (UDP) SNMP configuration	qbackup NAS Server 192.168.0.46	[Malware Remover] Scan completed.
	37 hours ago 22-09-24, 3:00:08 AM	High 3	SNMP Trap (UDP) SNMP configuration	qbackup NAS Server 192.168.0.46	[Malware Remover] Started scanning.
	39 hours ago 22-09-24, 12:53:22 AM	High 3	SNMP Trap (UDP) SNMP configuration	qbackup NAS Server 192.168.0.46	[Antivirus] Failed to update virus definitions. Please try again later or update the definitions manually.
	43 hours ago 21-09-24, 9:13:20 PM	High 3	SNMP Trap (UDP) SNMP configuration	qbackup NAS Server 192.168.0.46	[Antivirus] Scan job Virus scan completed.
	44 hours ago 21-09-24, 8:00:02 PM	High 3	SNMP Trap (UDP) SNMP configuration	qbackup NAS Server 192.168.0.46	[Antivirus] Scan job Virus scan started.

Aggregated state

versio.io

Asset & configuration item inventory > Inventory > Event reference > 192.168.0.46

Instance history viewer

Get an overview of the state changes over the entire lifetime of the instance.

192.168.0.46
EVENT-REFERENCE-86f5dcdefb9ffd6d183a0ea938f3cd52cf432e04

Current instance state

Display name	192.168.0.46
Virus scan status	completed
Malware scan status	completed

Hide if only topology changed

10 hours ago
Fri, 20-09-24, 3:14 AM

1 Change

Malware scan s...	completed
-------------------	-----------

10 hours ago
Fri, 20-09-24, 3:00 AM

1 Change

Malware scan s...	start
-------------------	-------

16 hours ago
Thu, 19-09-24, 9:16 PM

1 Change

Virus scan status	completed
-------------------	-----------

Online training

Versio.io Event Management & Alerting

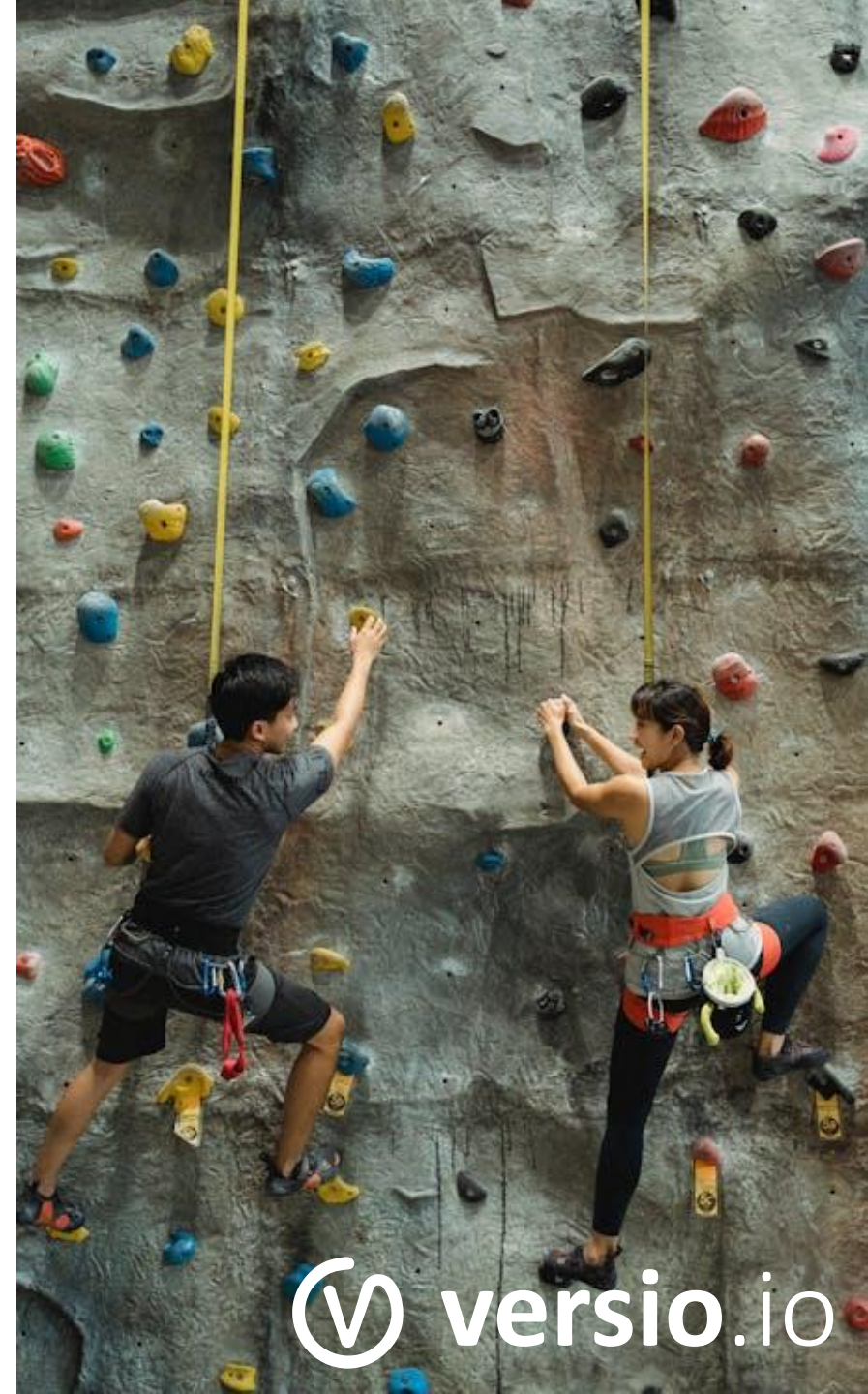
Alerting - Practical exercise

What we want to see and understand live in the practical exercise!

- Define an alerting
 - Event selection
 - Action (Gitlab ticket and Telegam notification)
- Use API events to test your alerting
- Find events with successful and failed events
- Try to reproduce or create the example of the event reference instance and recognise its power

Online training

© 2024 | Versio.io | Inventory | Cybersecurity | Governance | IT Event



Versio.io Event Management & Alerting

Agenda

1. Versio.io fundamentals
2. Event management fundamentals
3. Import IT events (PE)
4. Event features (PE)
 - Pre-processing
 - Inventory Integration (Digital Twin)
 - Close events
 - Archive events
 - Event deduplication (event storm)
5. Coffee & tea break - 10 min
6. Event analysis (PE)
 - Event filtering
 - Event insight dashboard
 - Event explorer
7. Alerting (PE)
 1. Event selection
 2. Actions
 3. Action „Event reference instance“
8. Subscription model
9. Questions & Answers

* PE = Practical exercise

Online training

Versio.io Event Management & Alerting

Subscriptionmodel for event management

- Versio.io subscriptions Dashboards provide an overview of currently managed events.
- Versio.io internal events are free charge with a charge for 90 days.
- Deletion of old events is carried out according to the FIFO principle.

Pricing

- 100 Euro/Month per 10.000 Events Package
- 1.000 Euro/Month per 1 Million Events Package
- 7.500 Euro/Month per 10 Million Events Package
- 50.000 Euro/Month per 100 Million Events Package

Online training

Subscription usage

The Versio.io subscription is based on the number of inventoried assets & configurations and historization. The following dashboard gives you an overview of the subscribed and free instances.

Environment: Versio.io PROD (e2wqx5t27q) 28 Aug 2024, 2:56 pm

Versio.io solutions

Name	Counting instances	Including instances	Subscription relevant	Mark as deleted
Event processing	AVM events: 50 EOL events: 54 Hetzner Cloud events: 11 Proxmox events: 331 SNMP Trap events: 62 Syslog events: 14,041 Versio.io events: 7,315	Versio.io events: 32,846	21,864	0

Versio.io Event Management & Alerting

Agenda

1. Versio.io fundamentals
2. Event management fundamentals
3. Import IT events (PE)
4. Event features (PE)
 - Pre-processing
 - Inventory Integration (Digital Twin)
 - Close events
 - Archive events
 - Event deduplication (event storm)
5. Coffee & tea break - 10 min
6. Event analysis (PE)
 - Event filtering
 - Event insight dashboard
 - Event explorer
7. Alerting (PE)
 1. Event selection
 2. Actions
 3. Action „Event reference instance“
8. Subscription model
9. Questions & Answers

* PE = Practical exercise

Online training

Versio.io Event Management & Alerting

Questions & answers

- What unanswered questions do you have?
- What should we present better to make it easier for customers to understand?
- Do you have any new ideas or suggestions for improvement?
- What can we do better?





Matthias Scholze
+49 (30) 22 19 86 51
matthias.scholze@versio.io

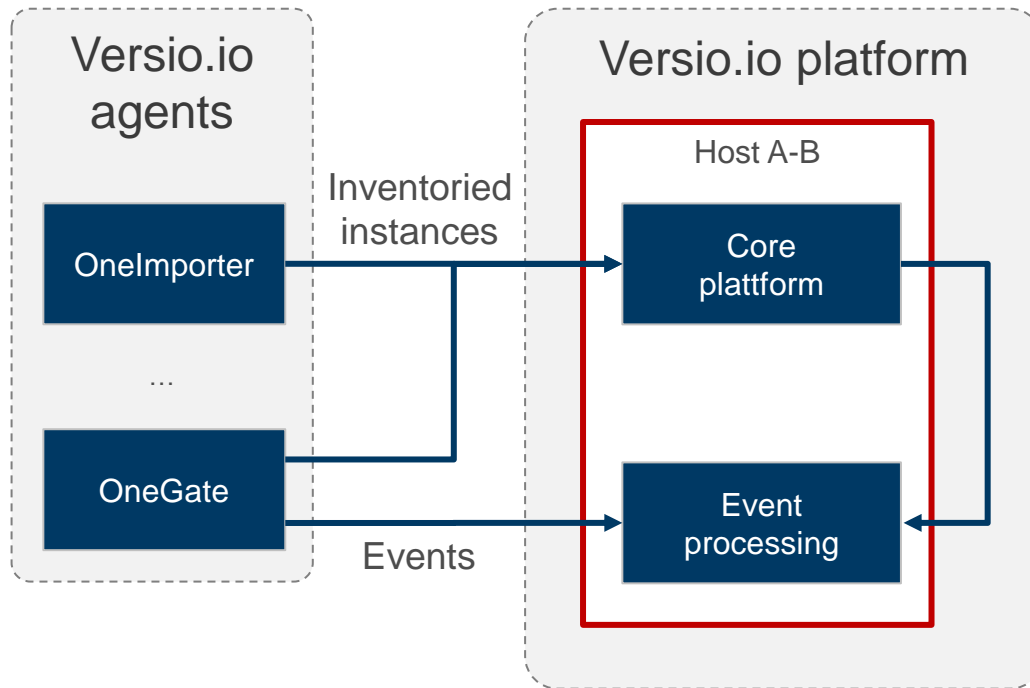


Versio.io Event Management & Alerting

Scalability & reliability - Separation of the Versio.io platform and event processing

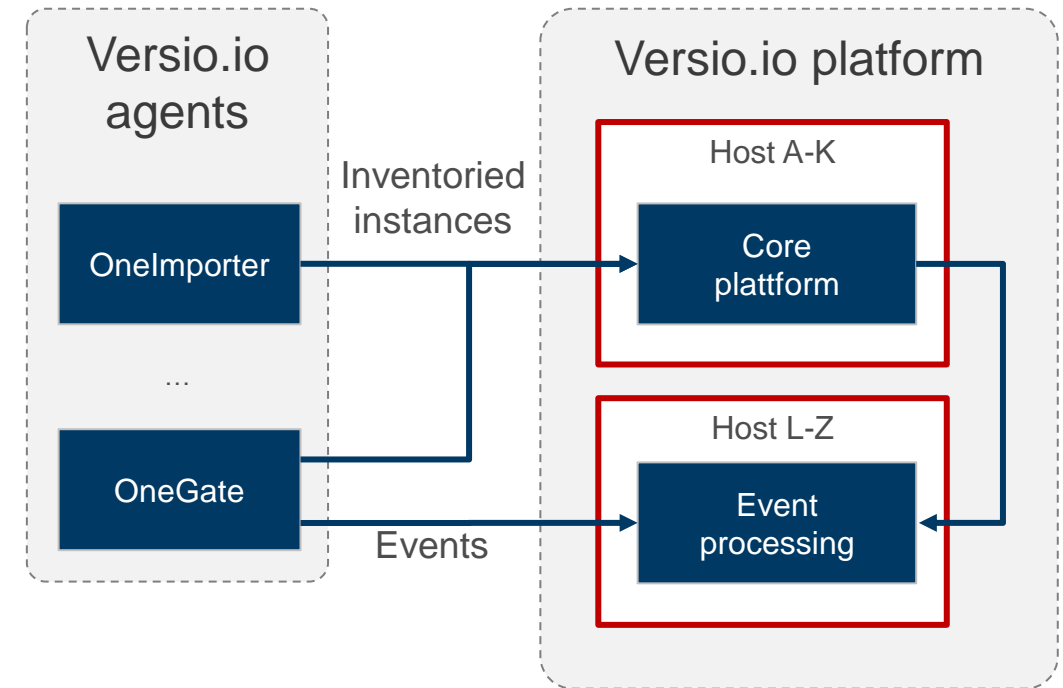
Small number of events

- Cost-effective operation of the Versio.io overall platform on one host



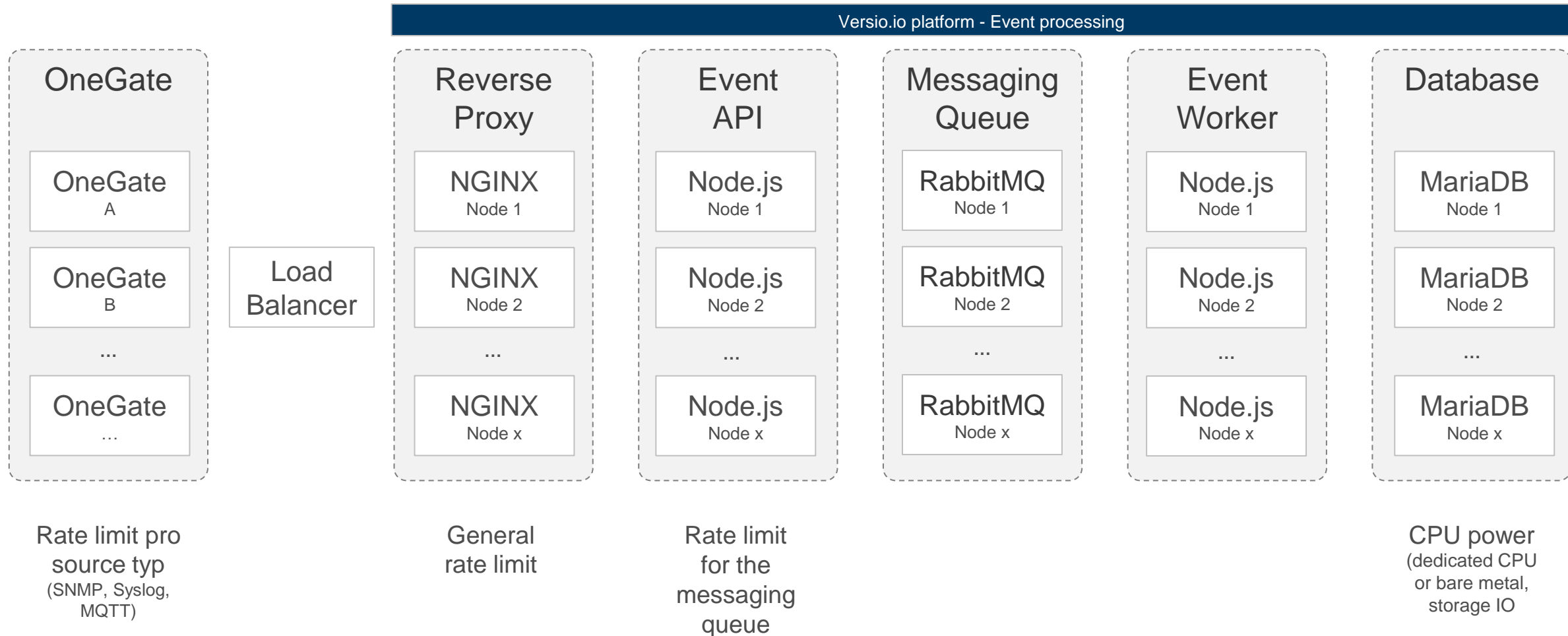
High number of events

- No interference due to physical host separation of the subcomponents



Versio.io Event Management & Alerting

Scalability & reliability - Scalability for all components of the event processing



Online training

