versio.io

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

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

Versio.io

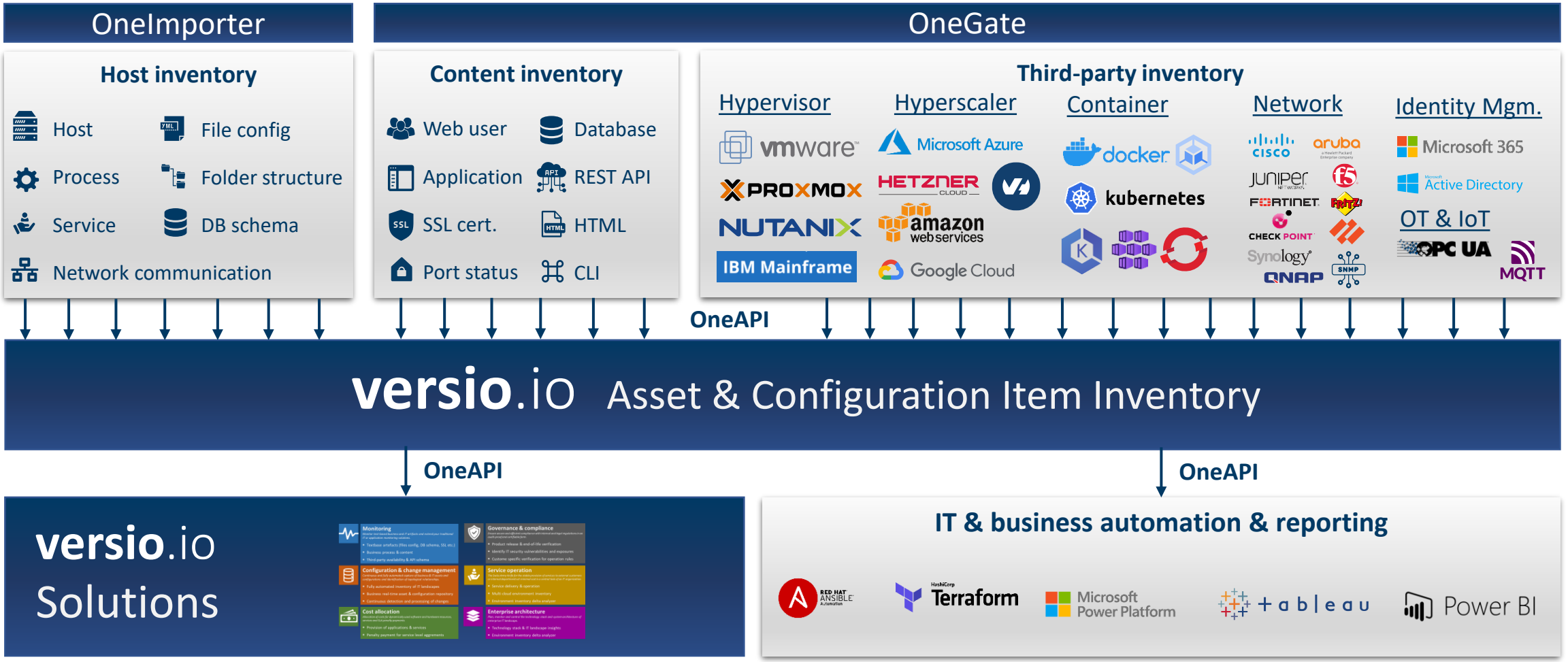
In a nutshell

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

Versio.io in nutshell

Data integrations, asset & configuration inventory and solutions



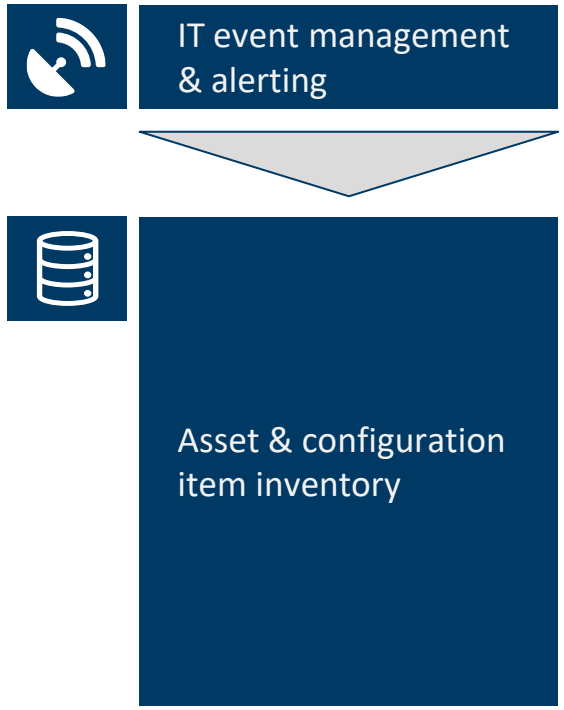
Versio.io Insights

versio.io

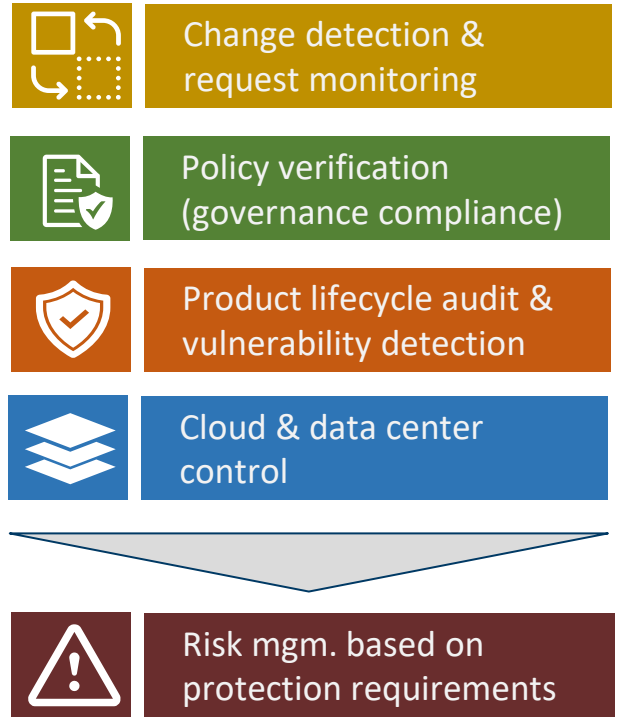
Versio.io in a nutshell

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

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?

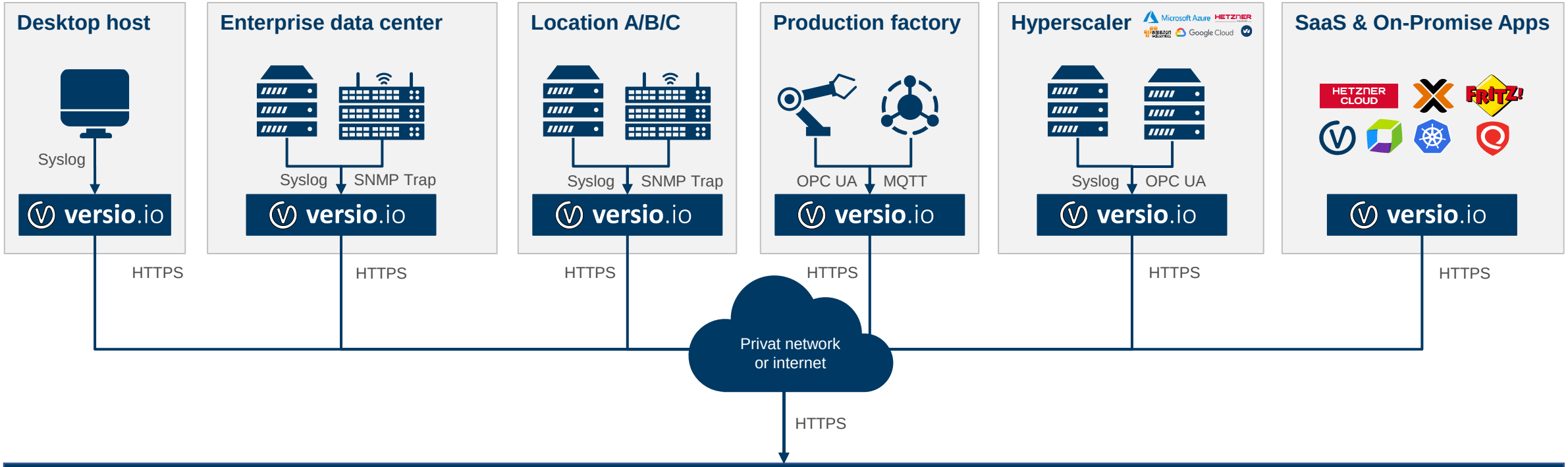
- Monitoring and fault detection
- Safety management
- Performance optimization
- Compliance and auditing
- Automation and responsiveness
- Capacity planning
- Error cause analysis
- Documentation and transparency
- …

Online training

versio.io

Versio.io Event Management & Alerting

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



versio.io = Versio.io OneGate

Online training

versio.io

Versio.io Event Management & Alerting

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

SNMP traps from network devices

Syslog messages from IT systems

Events from industrial OT/IoT devices

MQTT messages from OT/IoT devices

Events from third-party applications

Versio.io platform

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

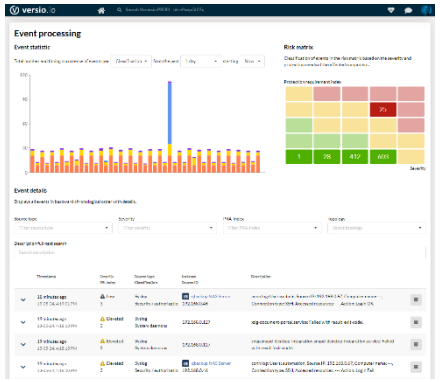
Enrichment
Search for an existing instance in the inventory using the trigger and adopt the inherited protection requirements for the risk assessment

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

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

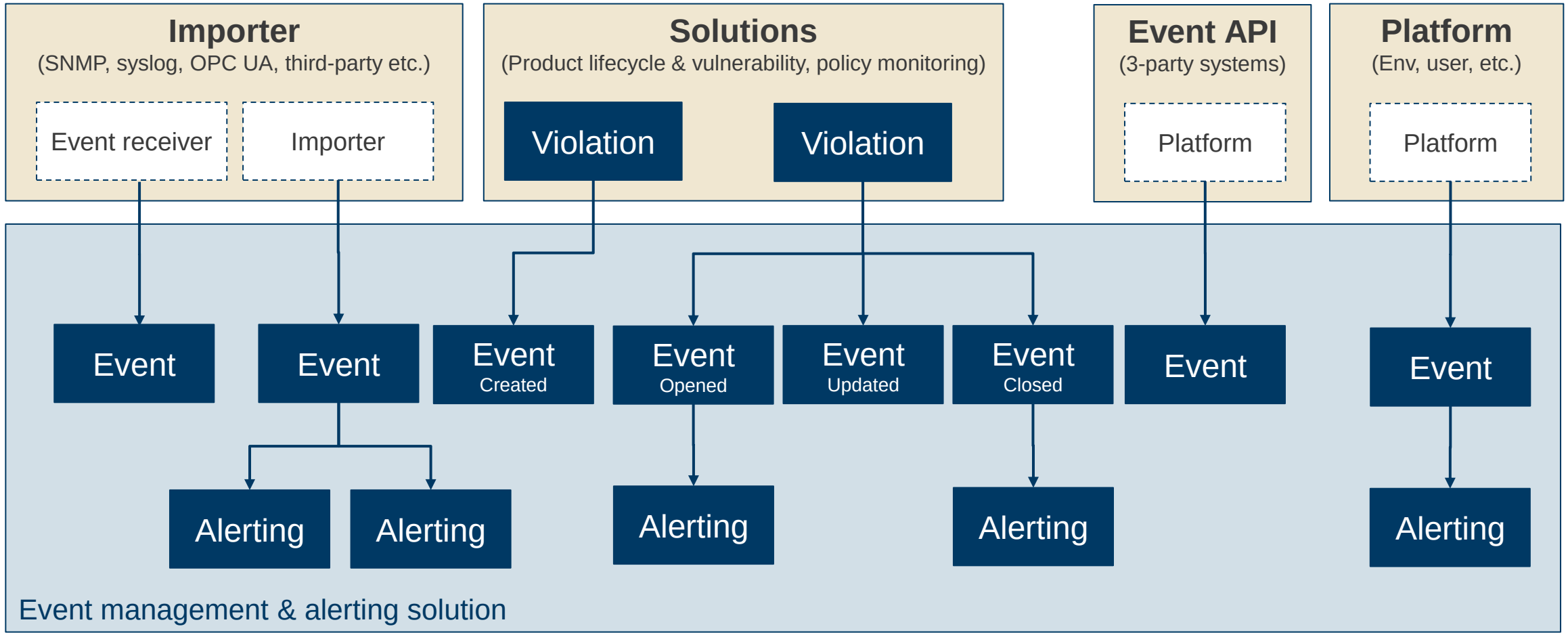
Alerting via dedicated events to other third-party systems for notification and further processing

Online training

versio.io

Versio.io Event Management & Alerting

Relationship between violations, events & alerting



Online training

versio.io

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).

Online training

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)

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

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
  - Custome specific events (Qualys, CRM, ERP, …)

Advantages of the Versio.io approach:

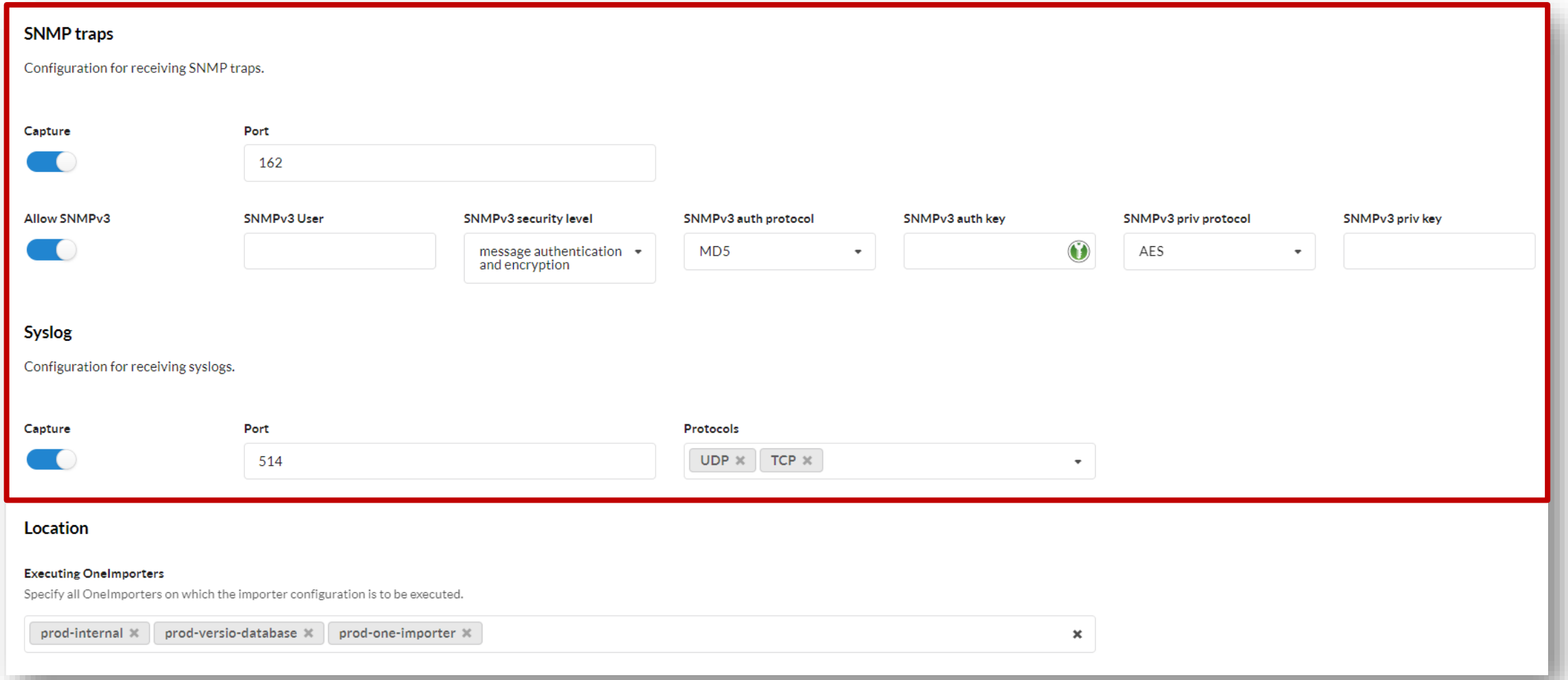
- The Event Receiver enables the capture of events based on **standard protocols** in any network zone (cloud, data centre, dedicated host, etc.).
- Versio.io **ready to use integration** with minimal configuration and no implementation effort.
- The open API can easily be used to capture **customised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

Online training

versio.io

Versio.io Event Management & Alerting

Import event messages - Event receiver configuration for generic event protocols

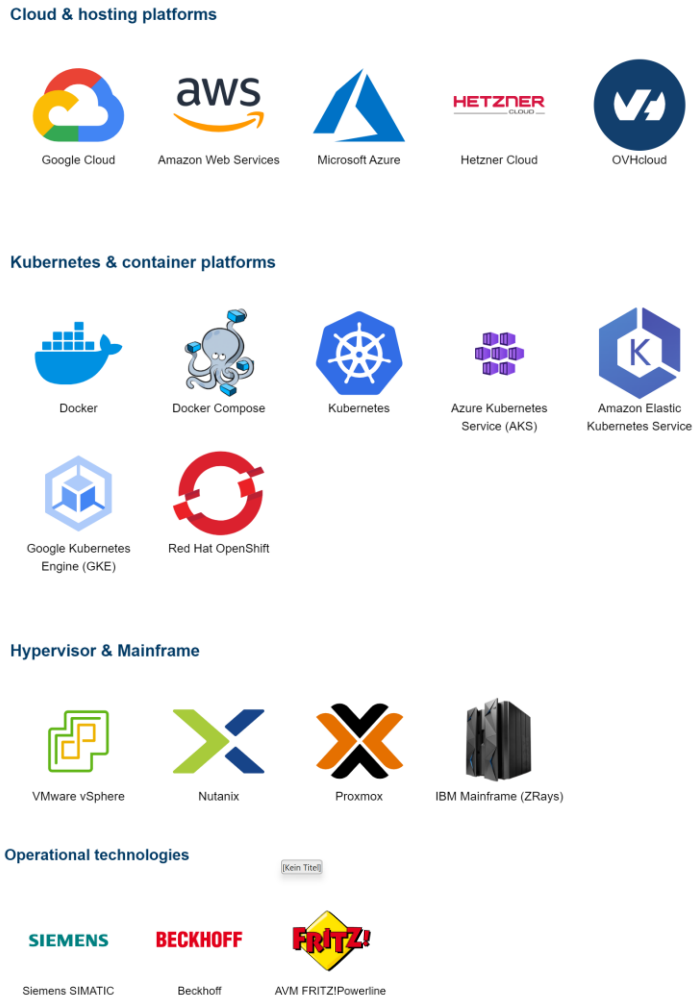


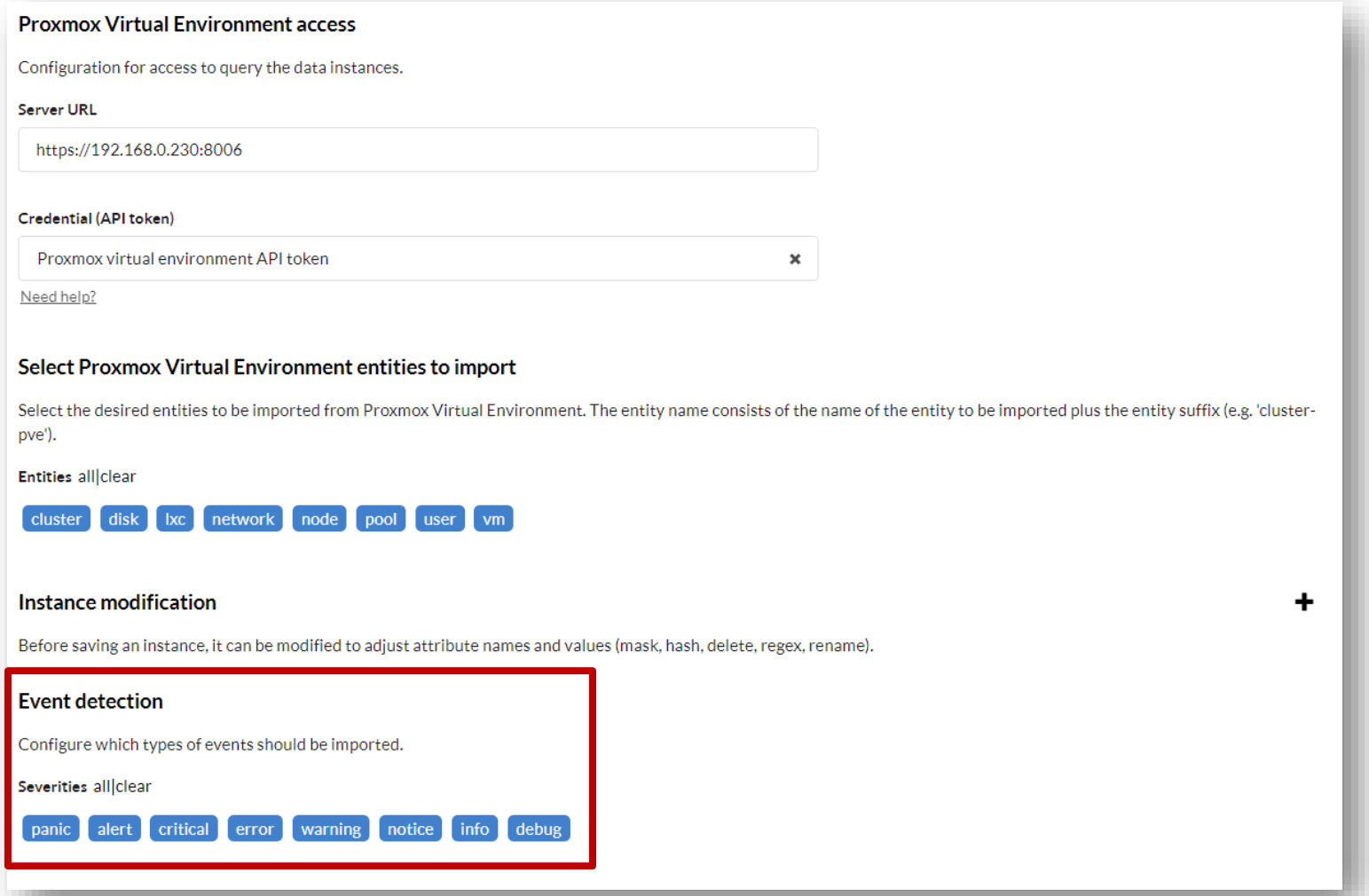
Online training

versio.io

Versio.io Event Management & Alerting

Import event messages - Importer configuration for third-party integrations





Online training

versio.io

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",
  }
]
```

Online training

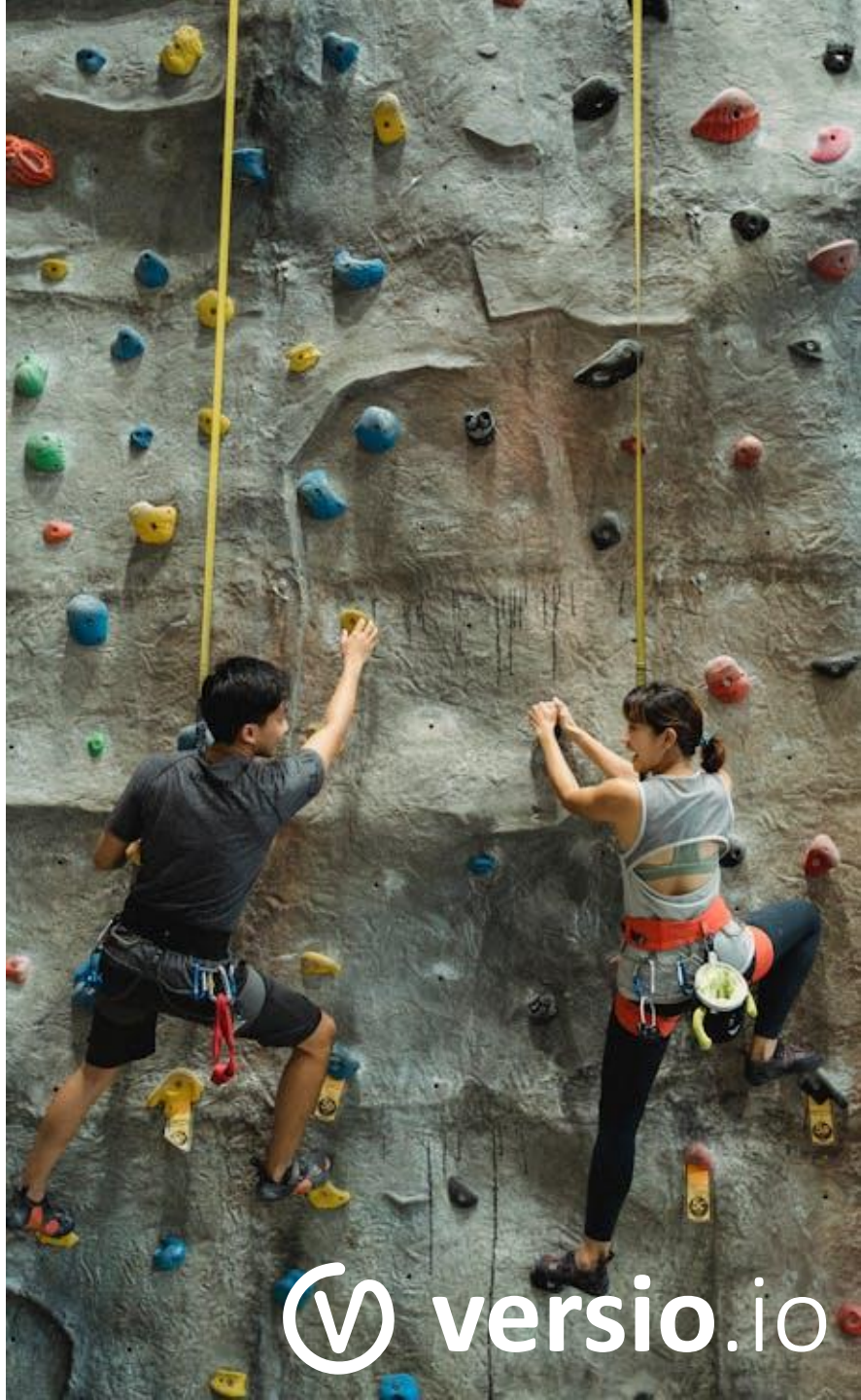
versio.io

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

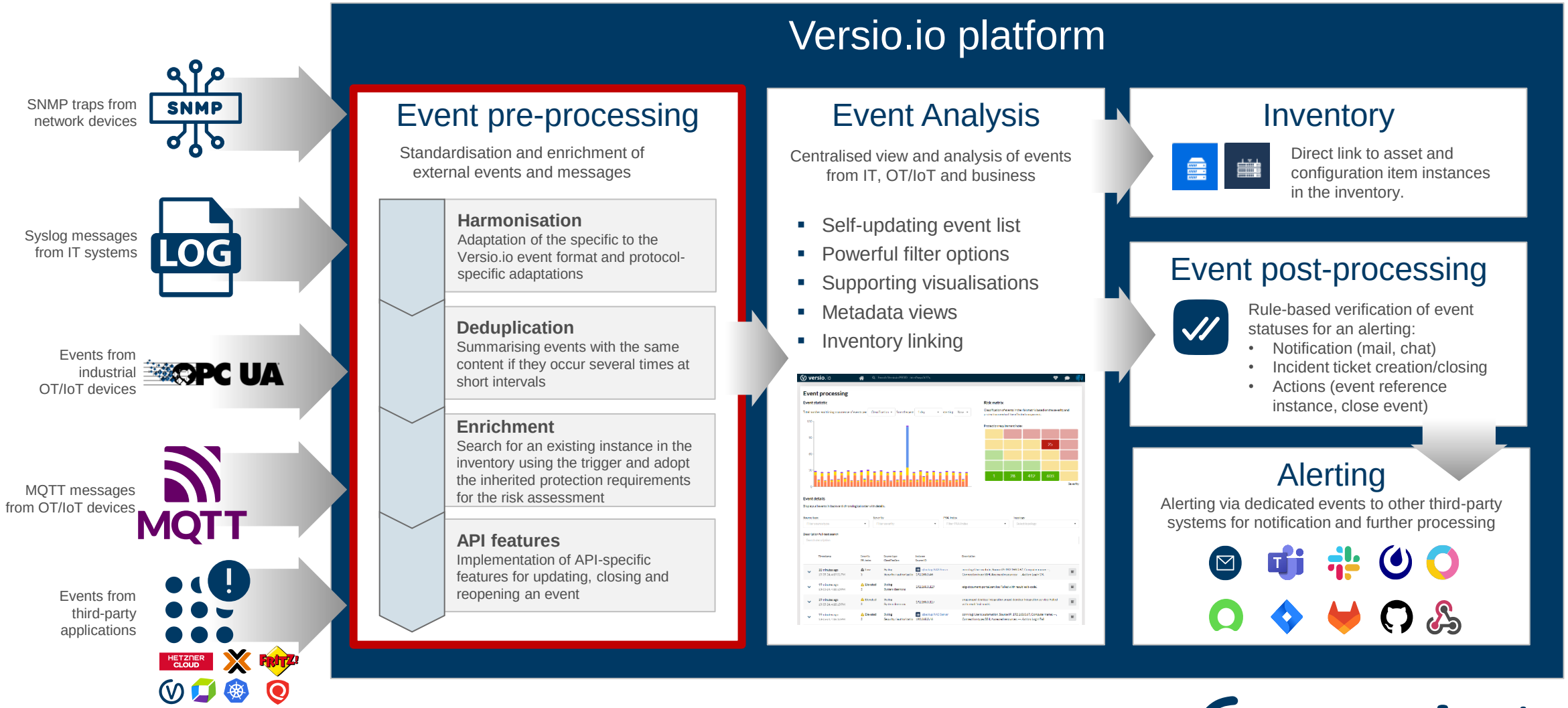
* PE = Practical exercise

Online training

versio.io

Versio.io Event Management & Alerting

Event pre-processing

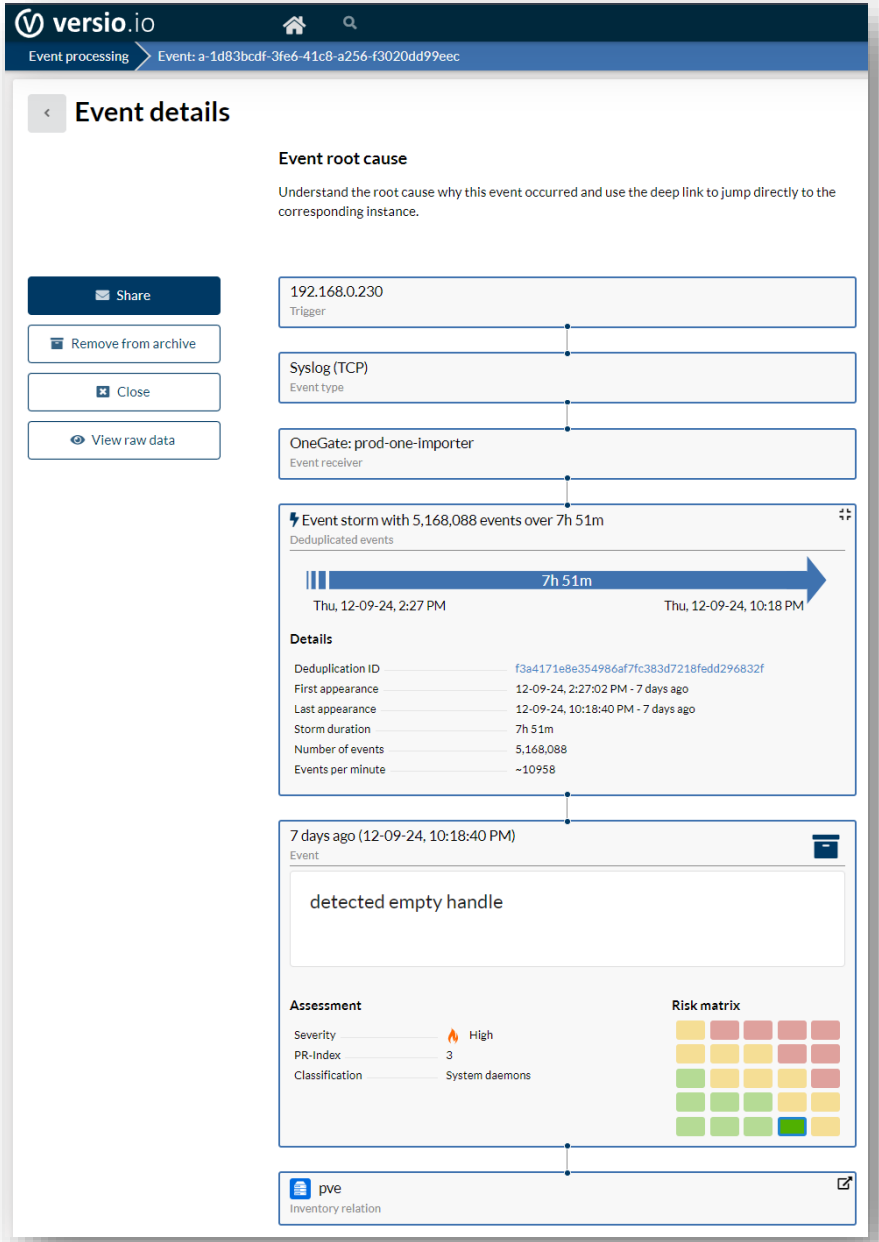


Online training

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



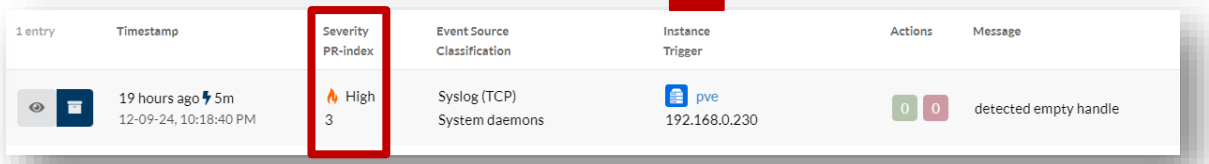
Online training

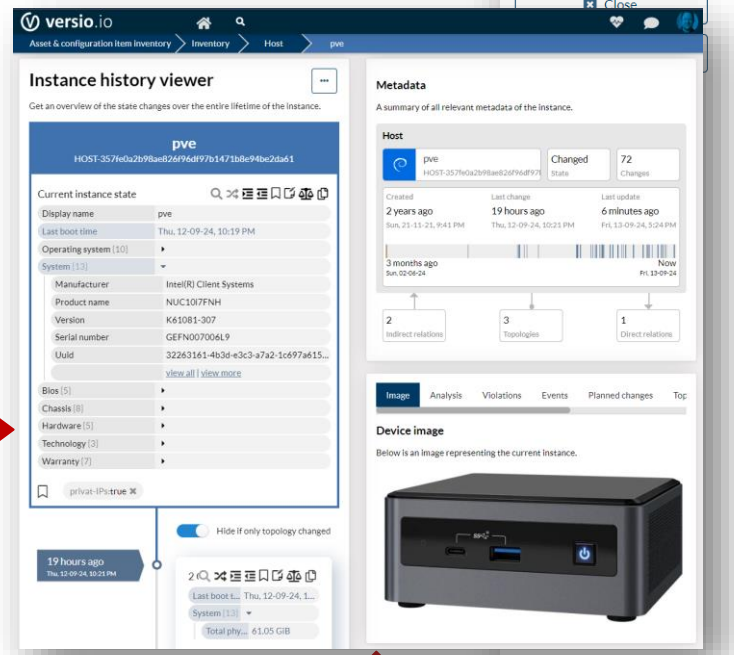
versio.io

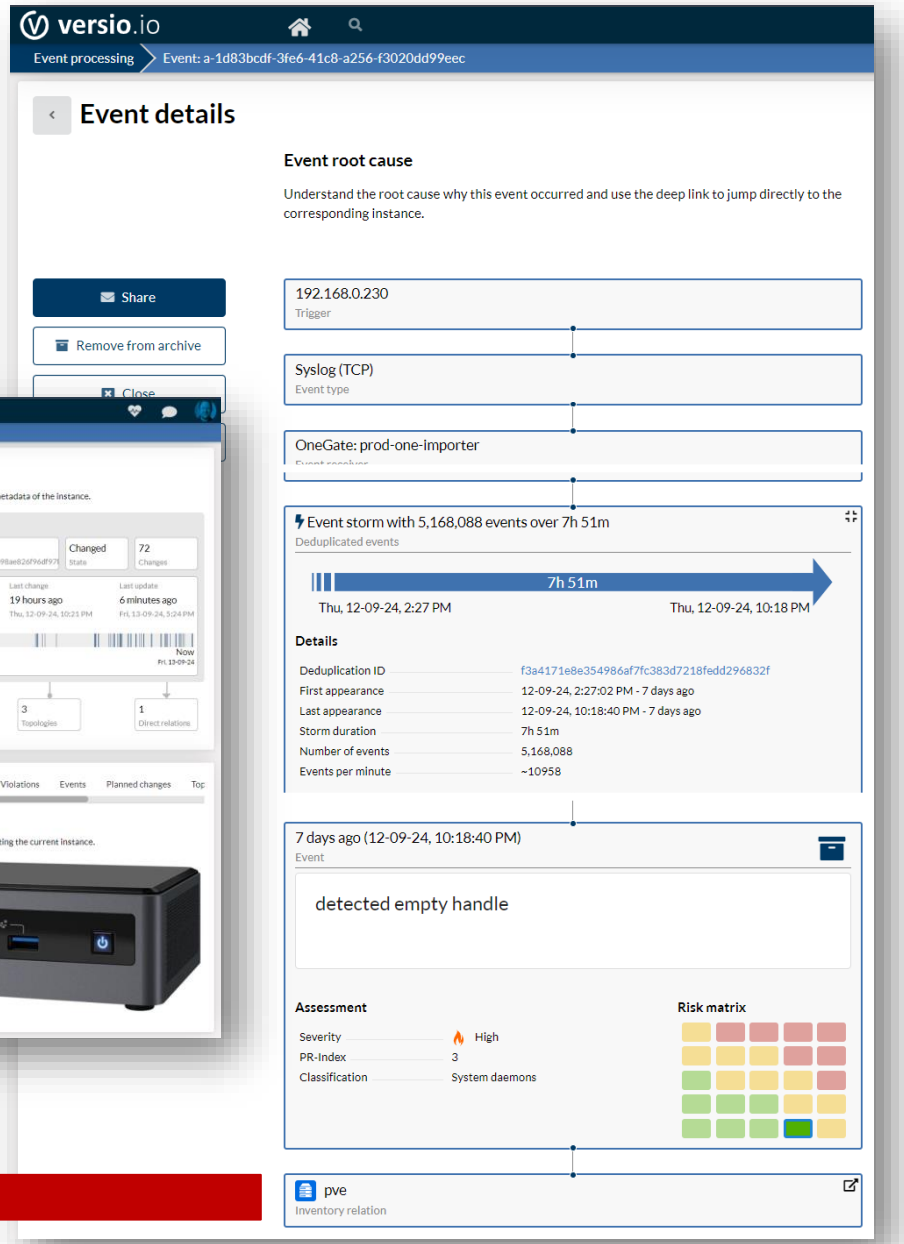
Versio.io Event Management & Alerting

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.







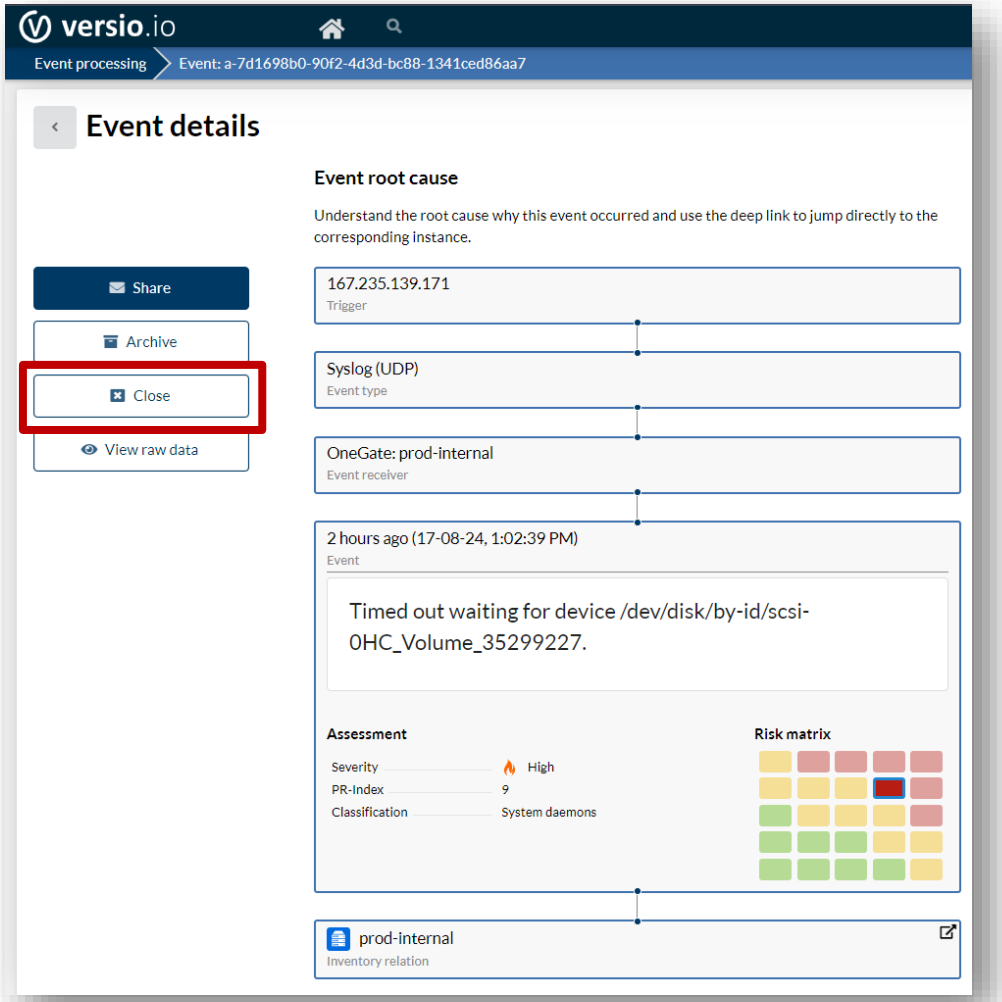
Online training

versio.io

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

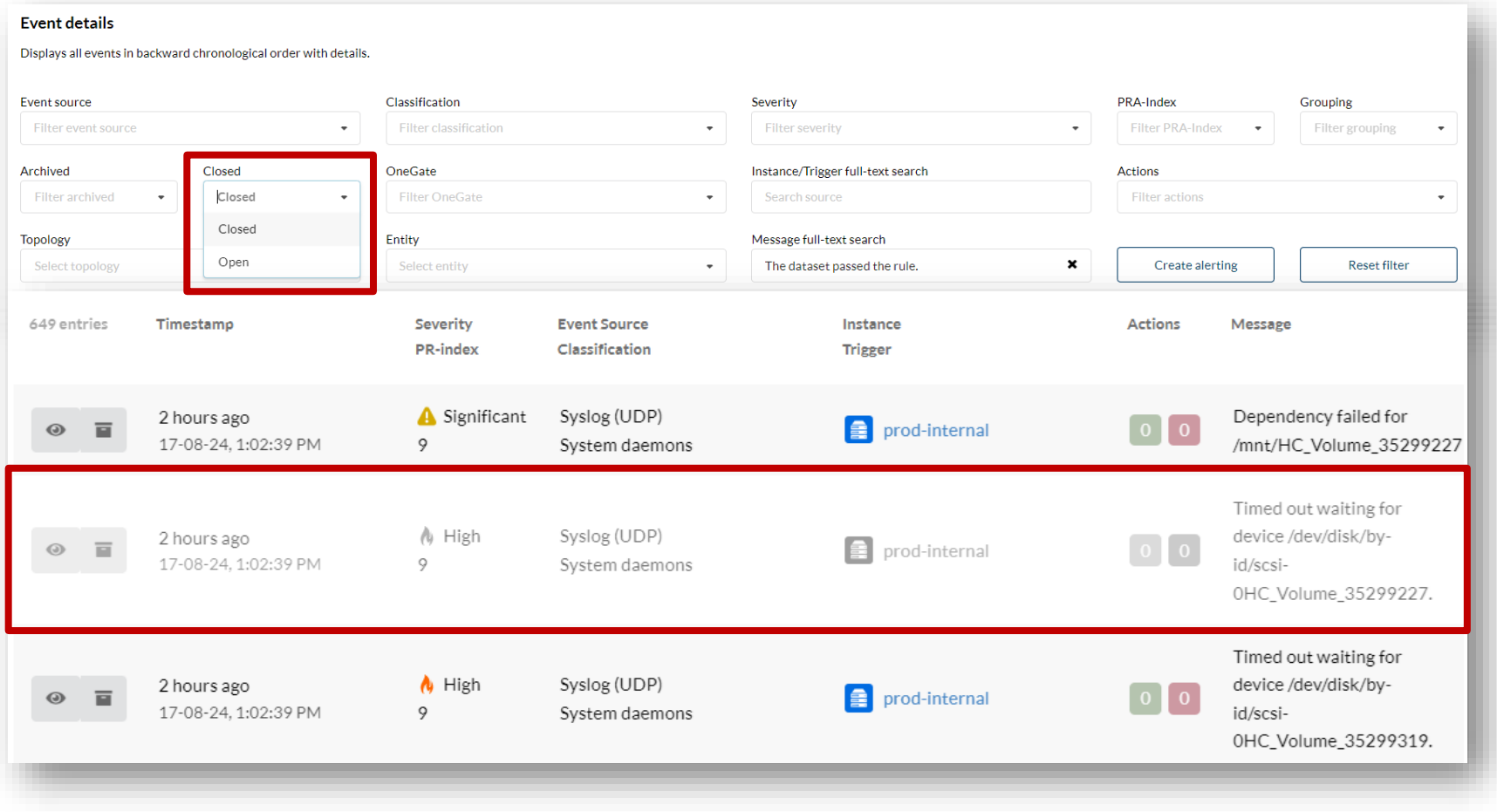


Online training

versio.io

Versio.io Event Management & Alerting

Features: Close event



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

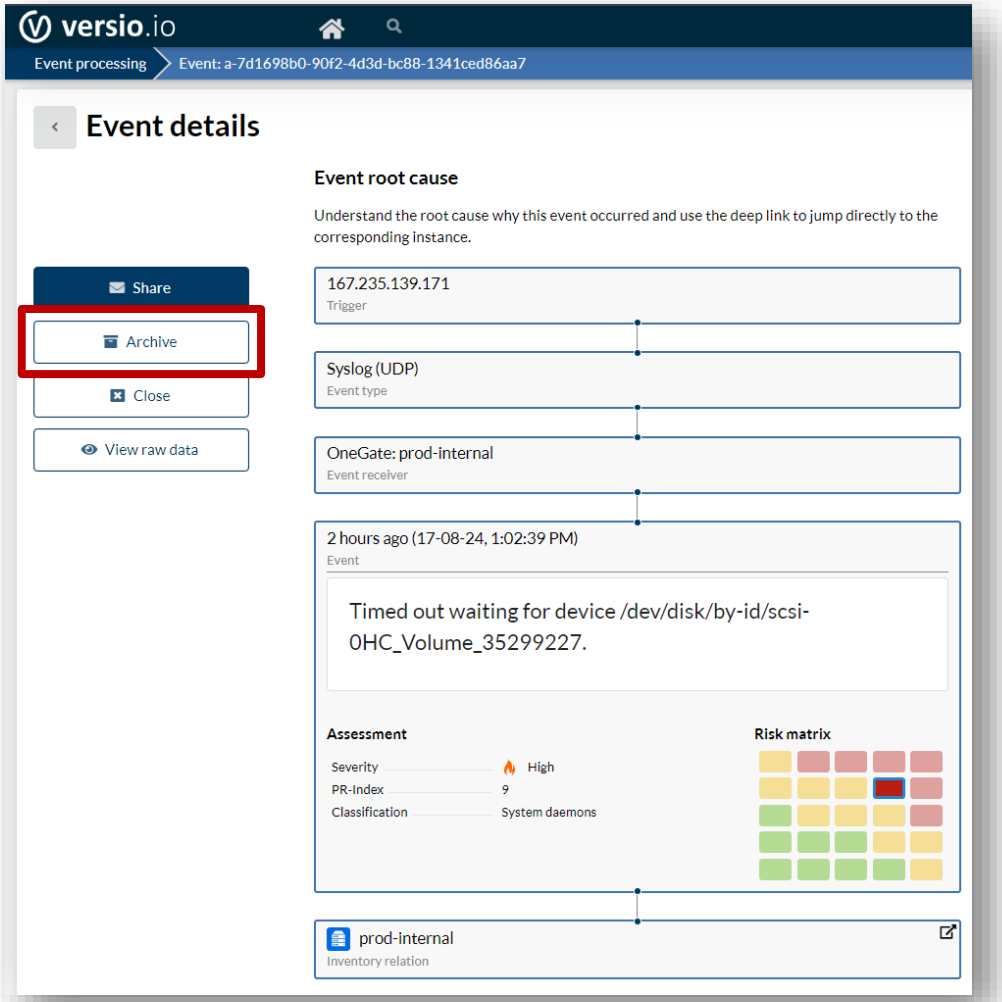
Online training

versio.io

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.

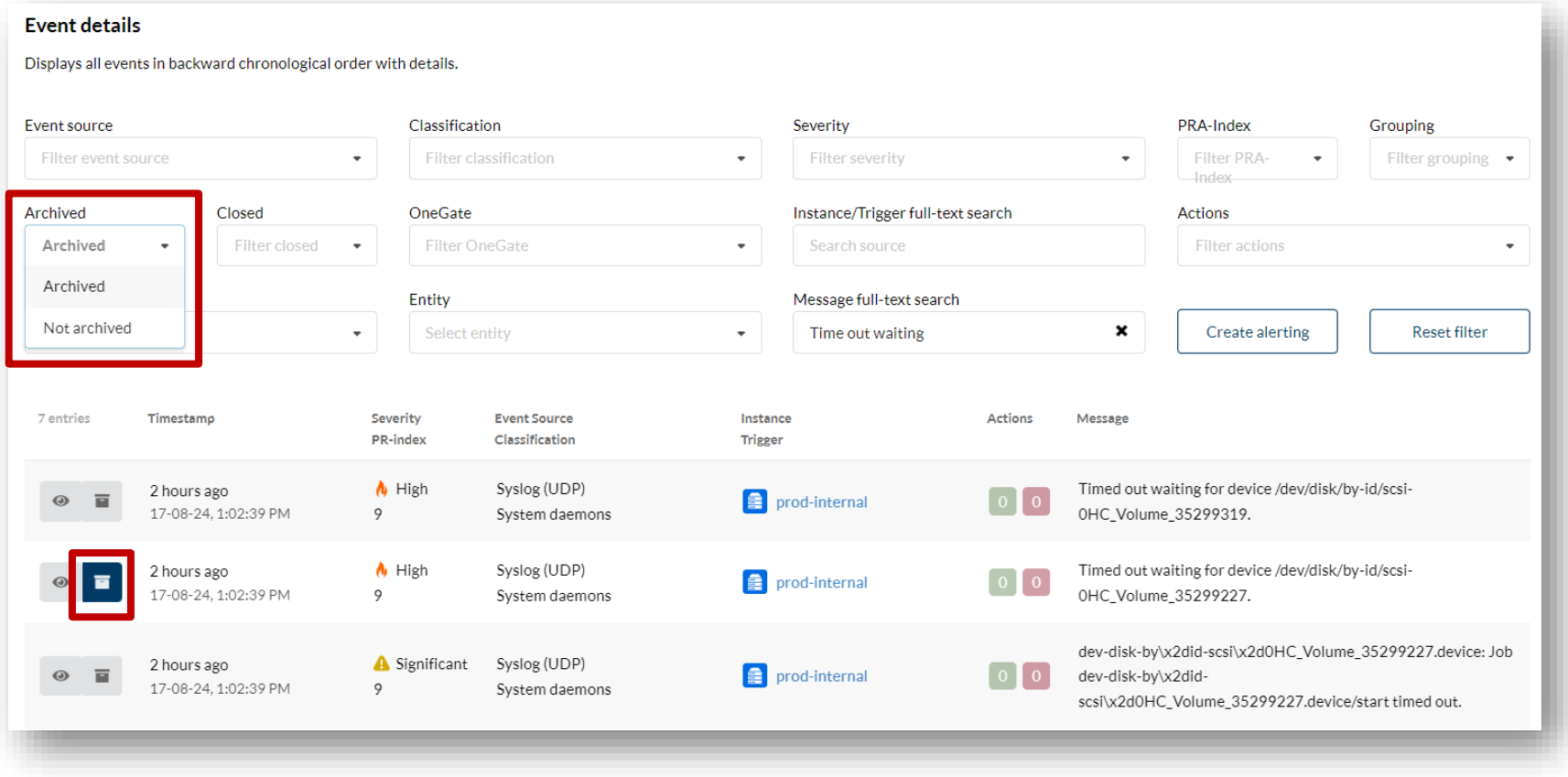


Online training

versio.io

Versio.io Event Management & Alerting

Features: Archive event



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

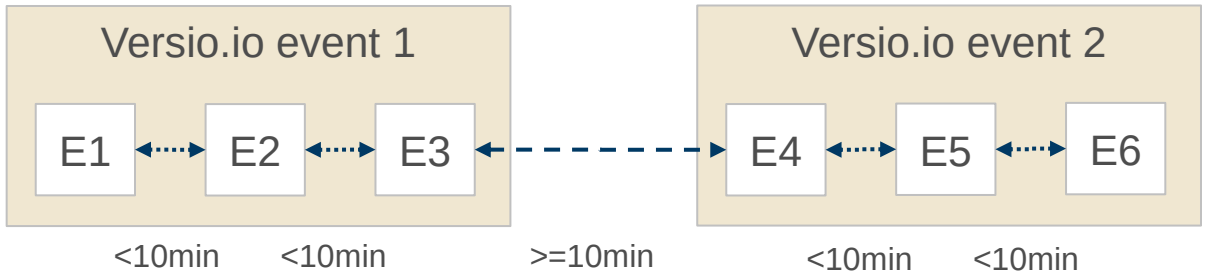
Online training

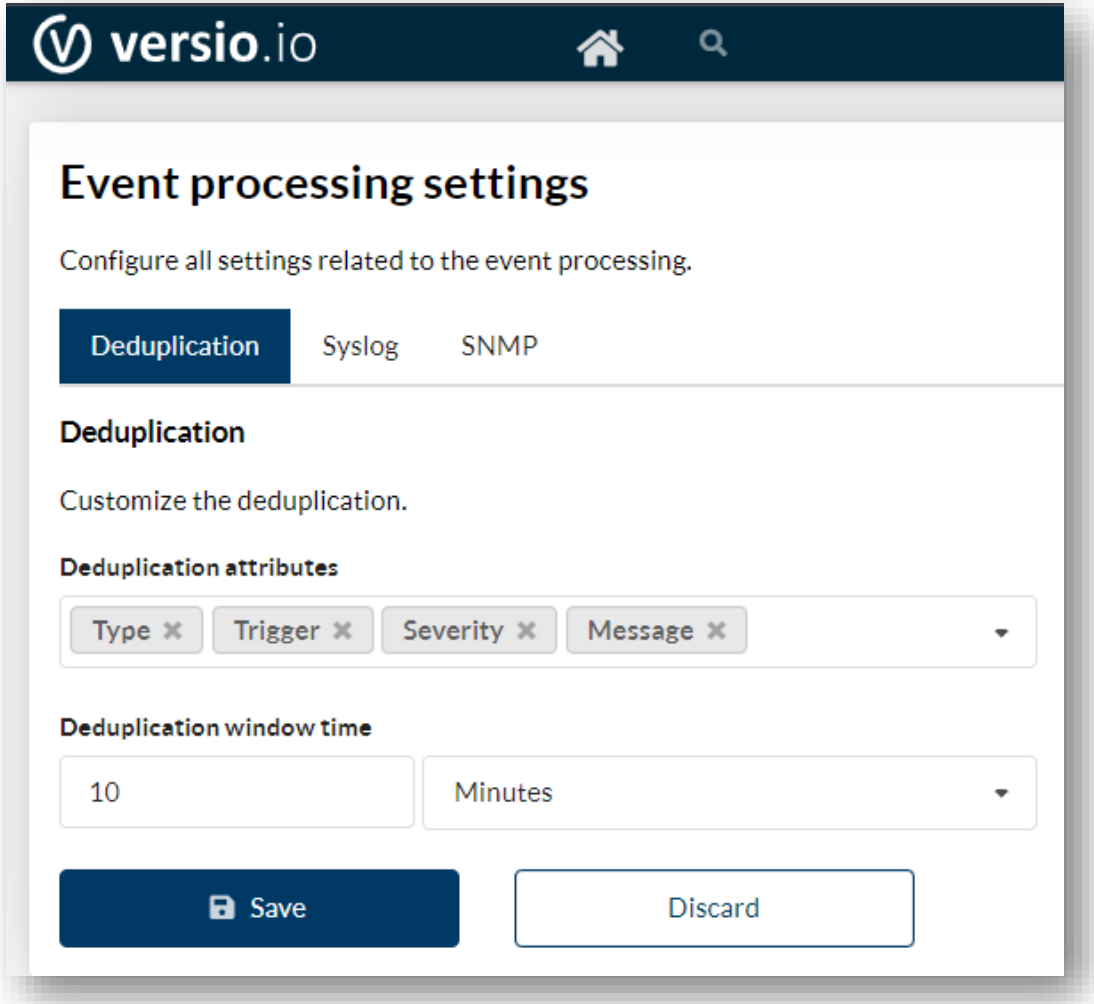
versio.io

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

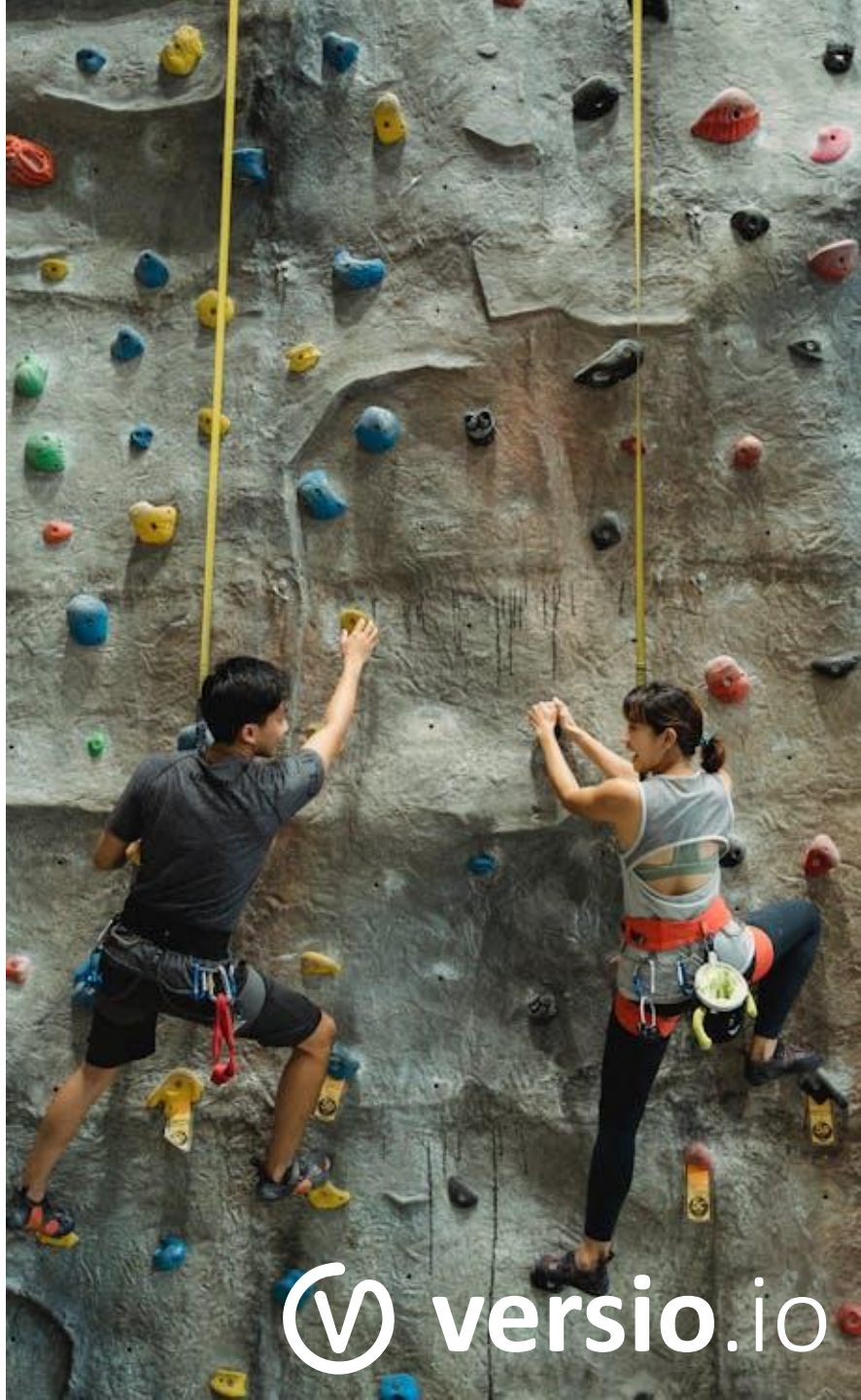
versio.io

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

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

versio.io

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

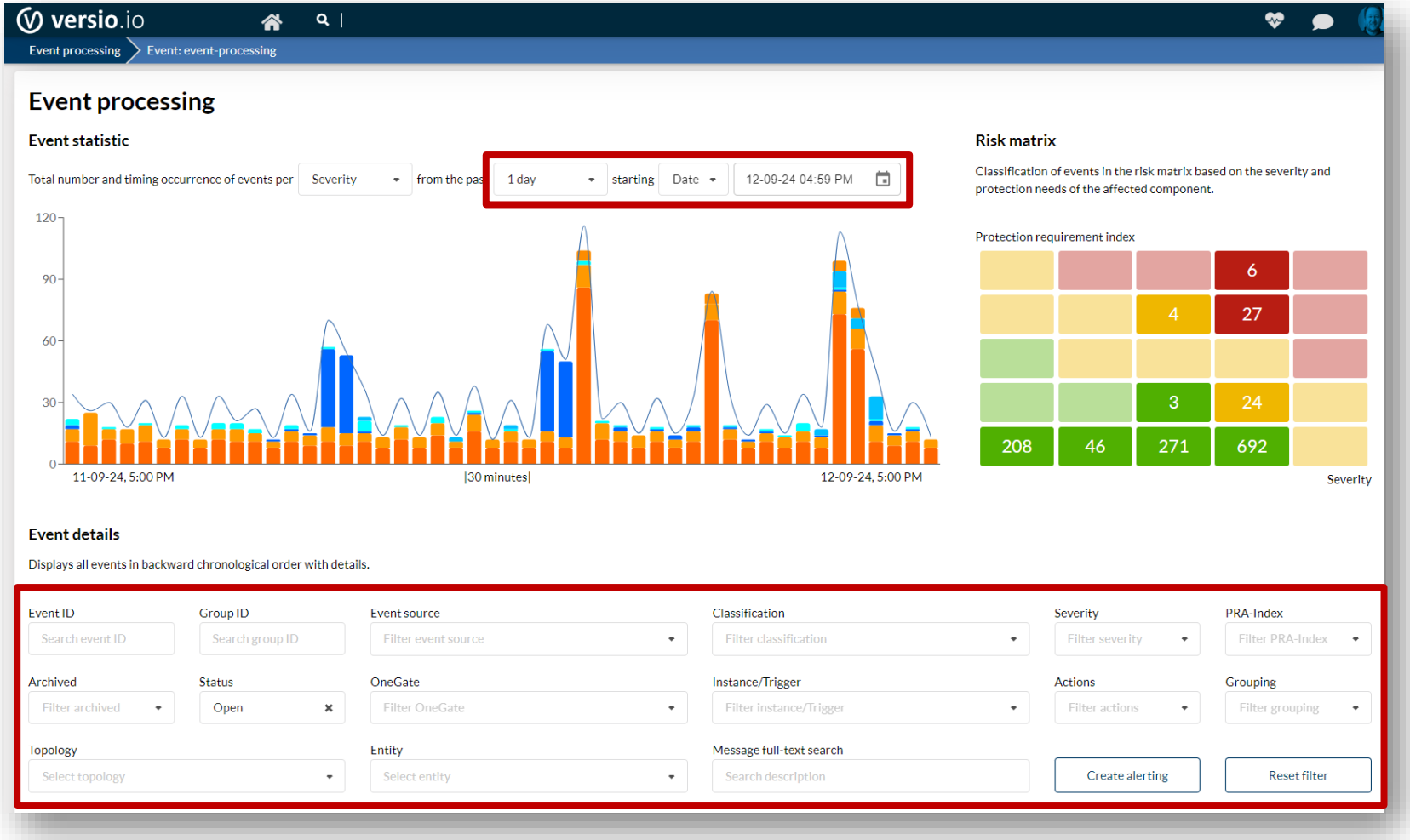
Online training

versio.io

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.



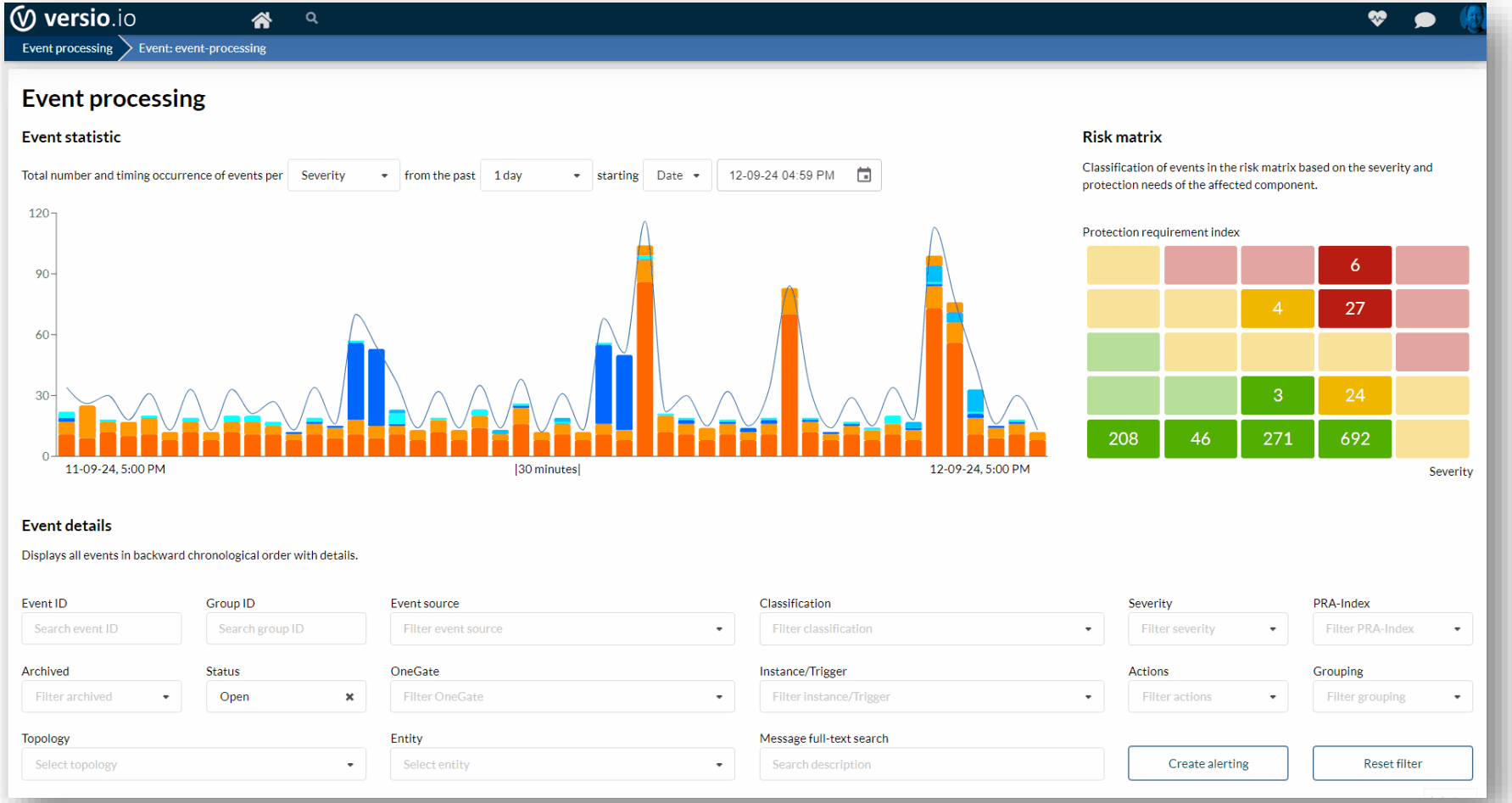
Online training

versio.io

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 ☺ ?



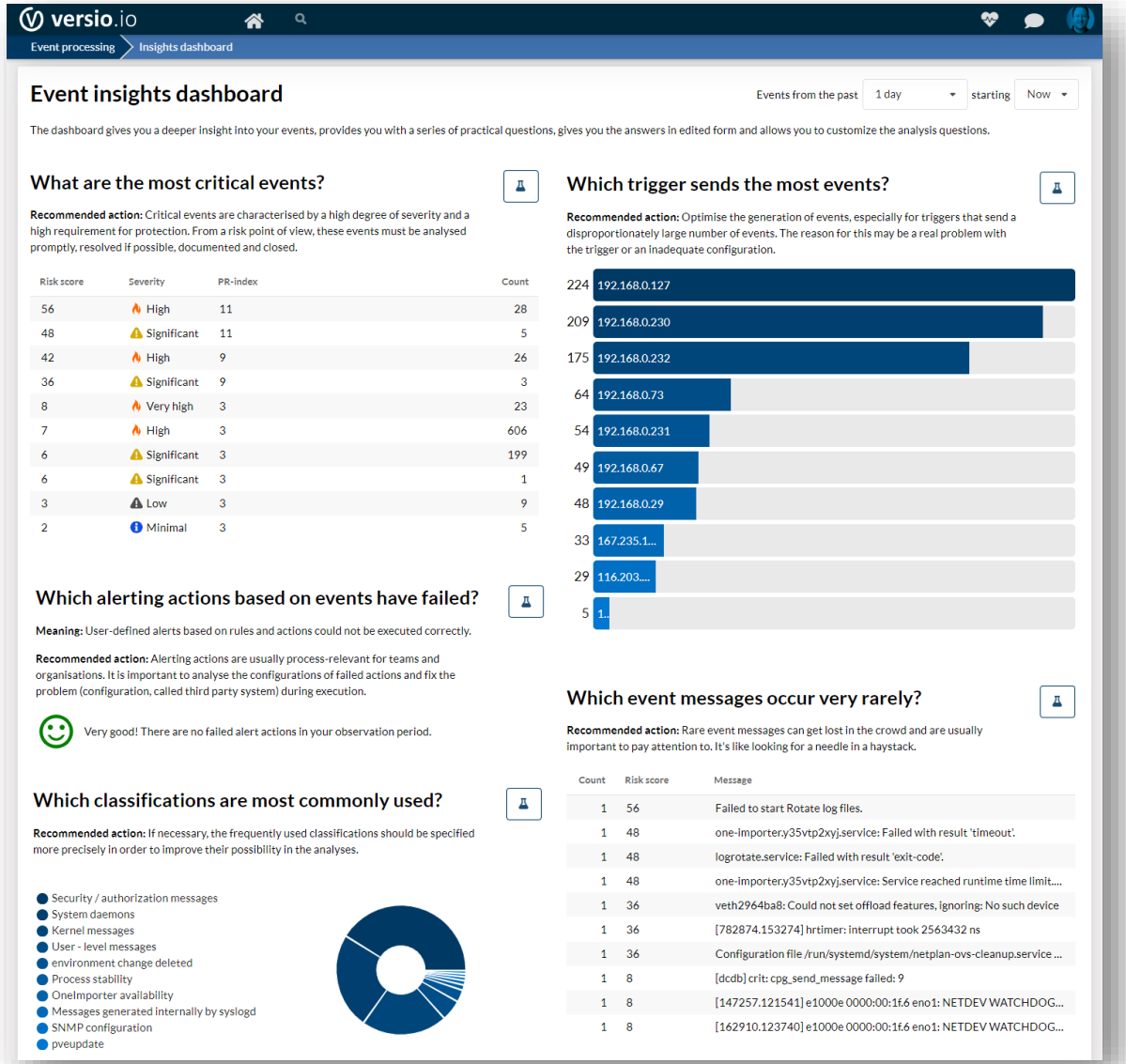
Online training

versio.io

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.

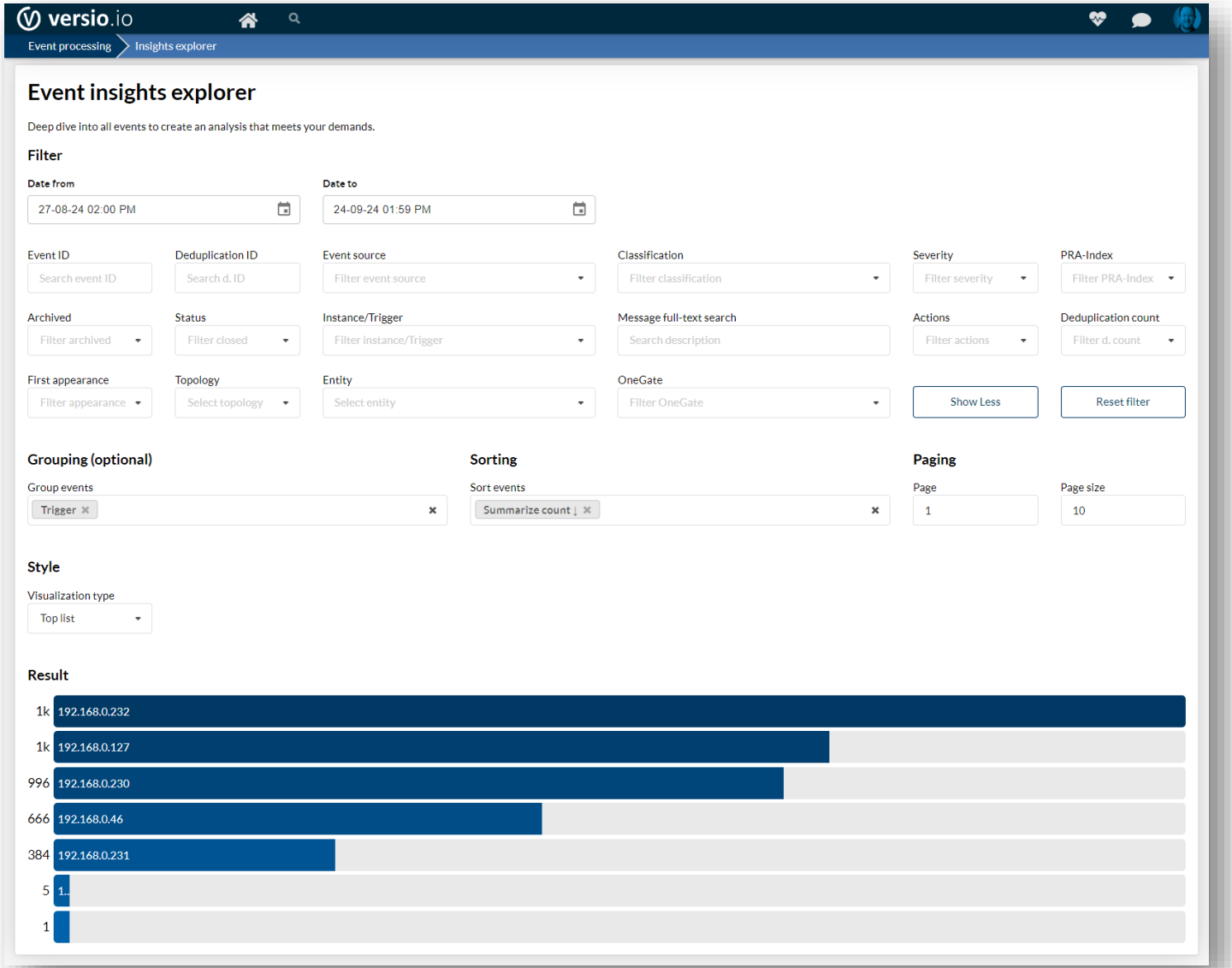


Online training

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.



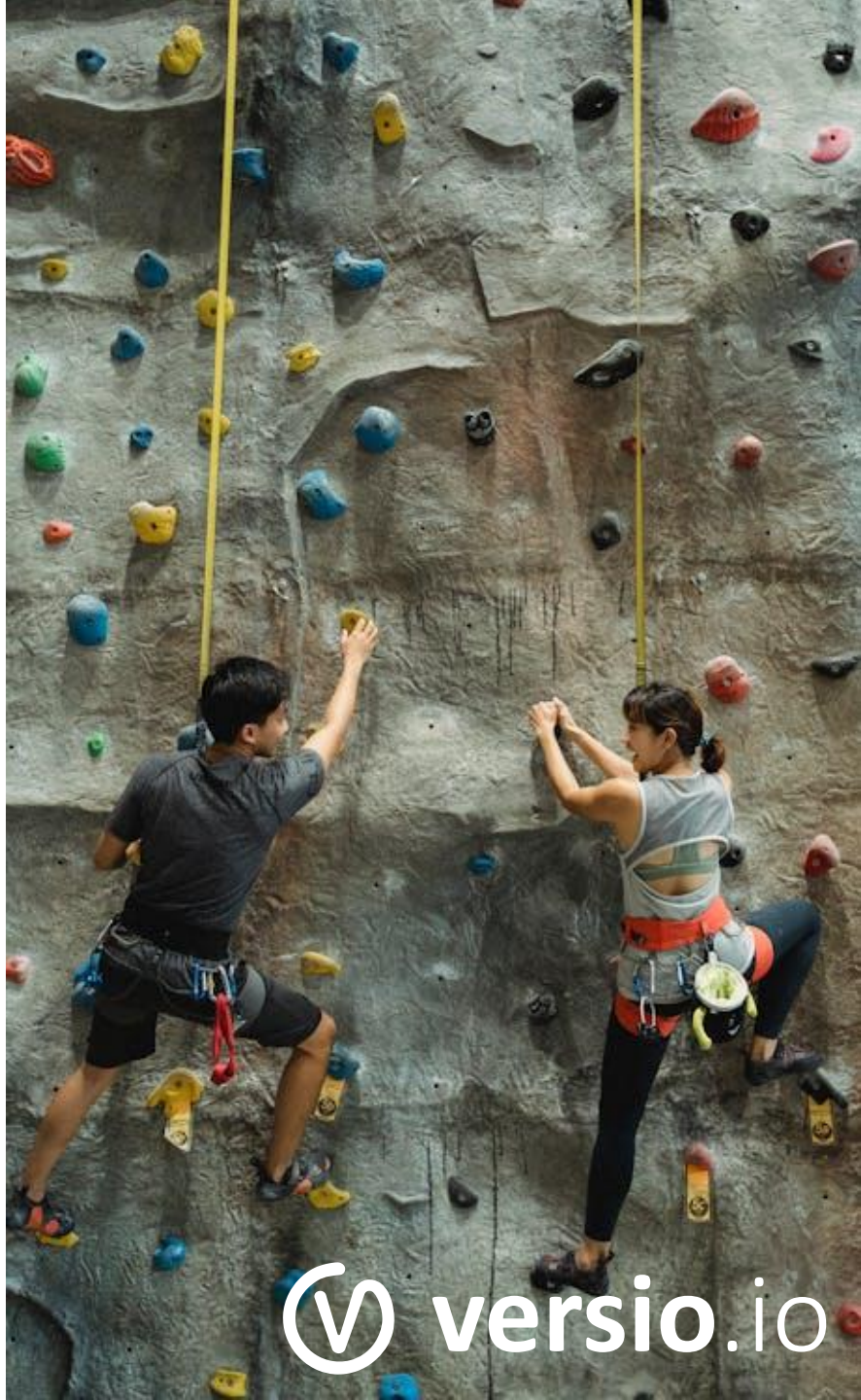
Online training

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

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

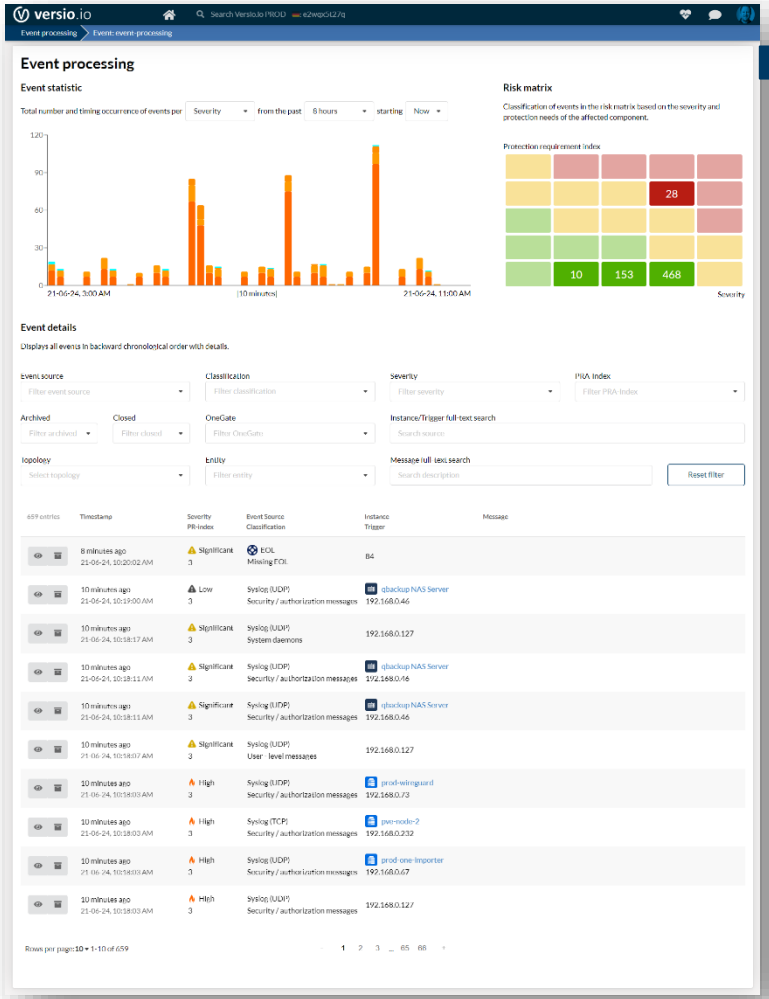
* PE = Practical exercise

Online training

versio.io

Versio.io Event Management & Alerting

Event post-processing: Alerting & actions



Online training

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

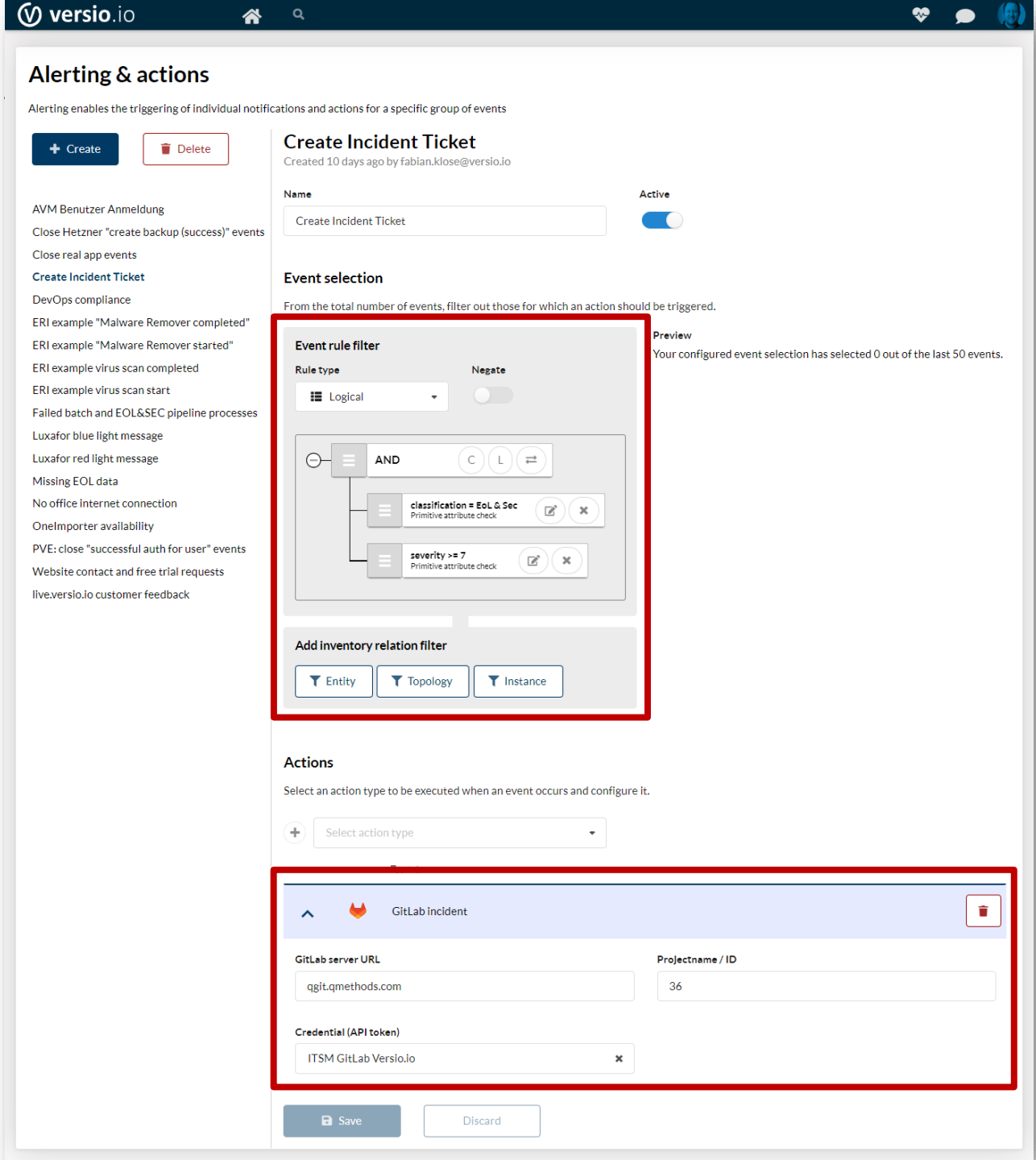
- Close event
- Event reference instance

versio.io

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.

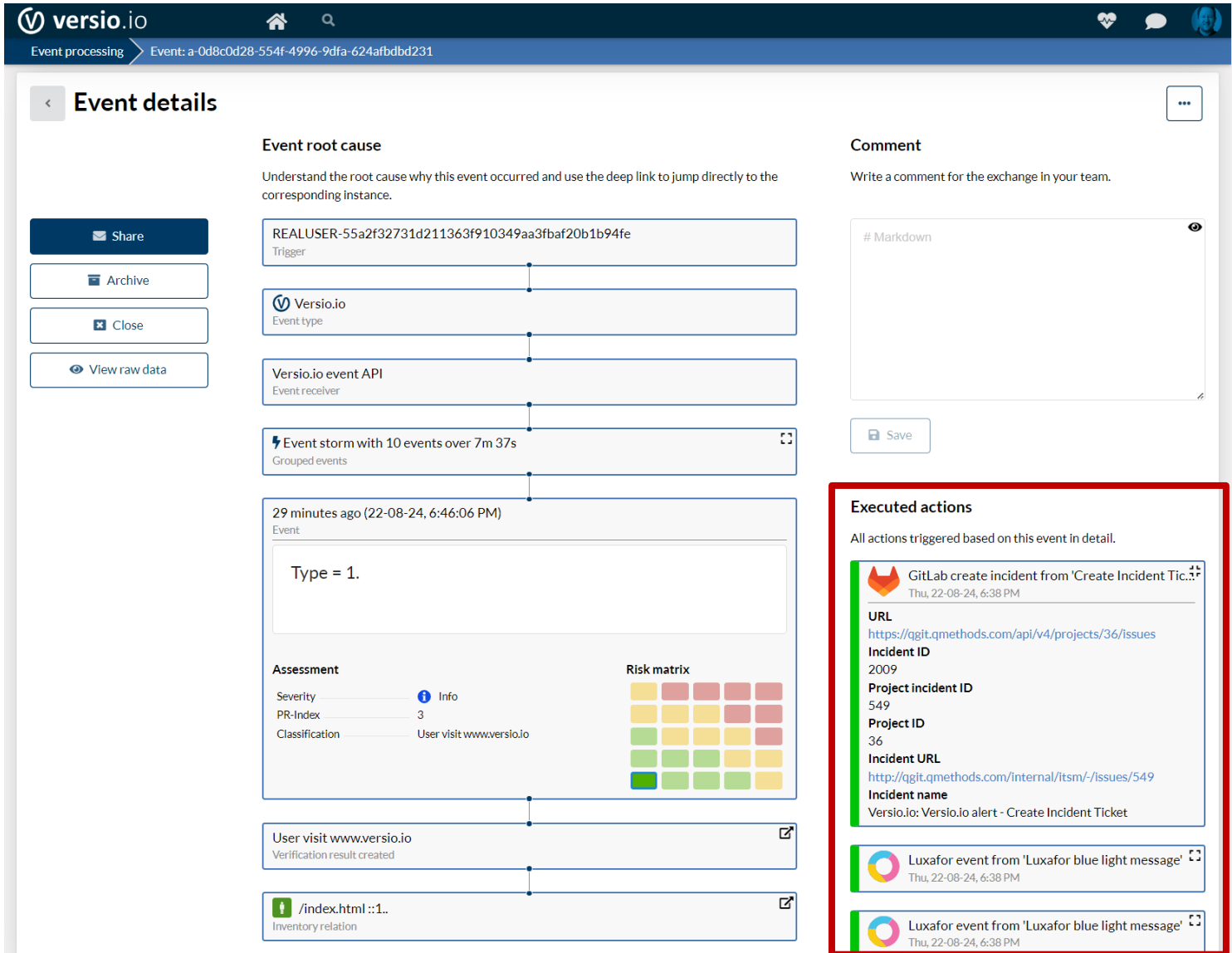


Online training

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

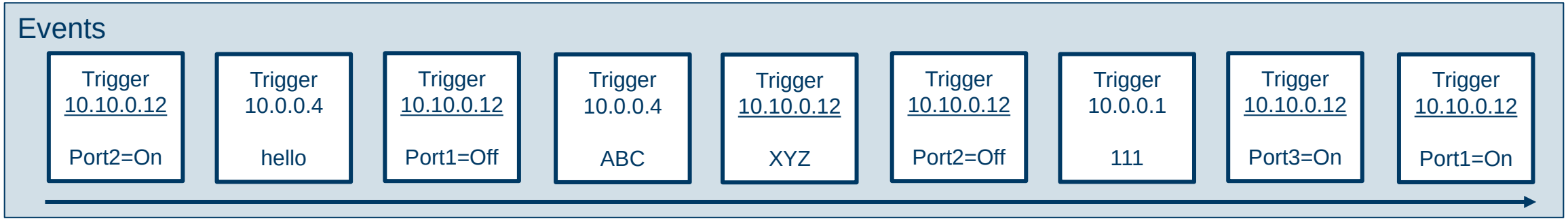


Online training

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? :

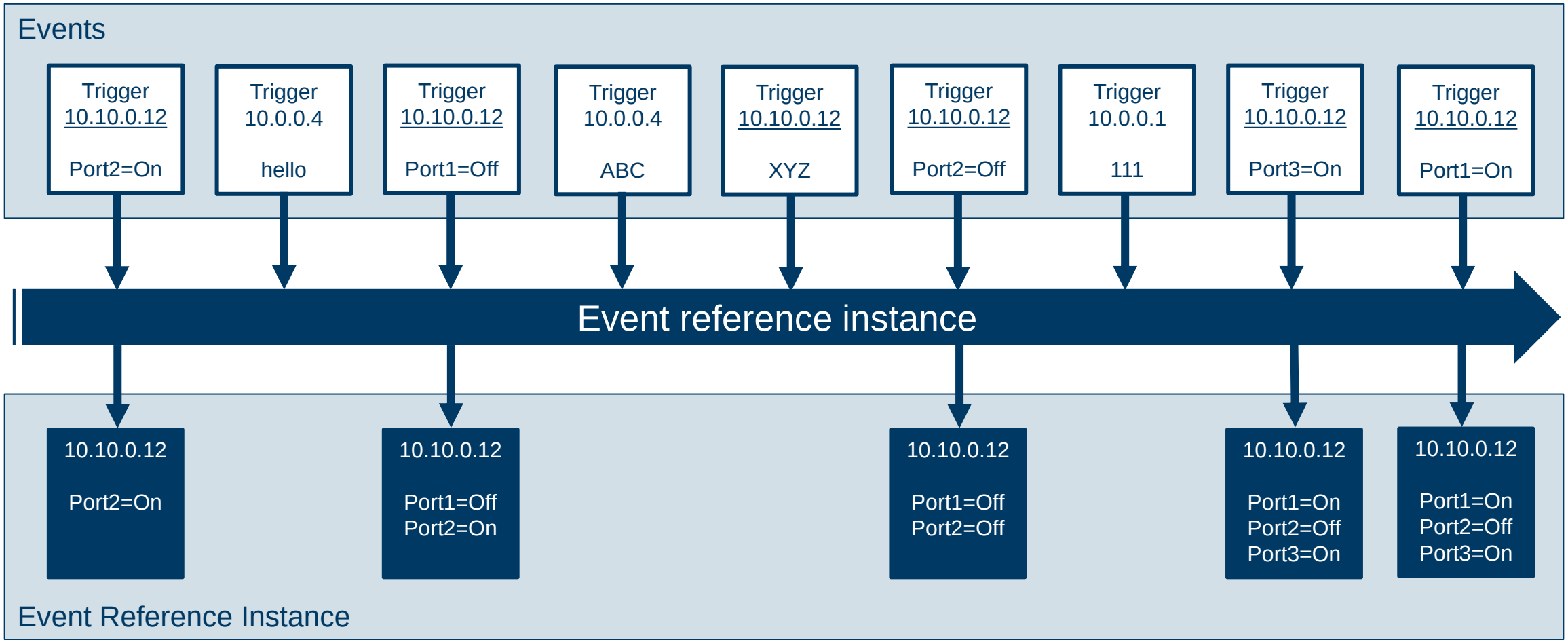


Online training

versio.io

Versio.io Event Management & Alerting

Event reference instance - Example

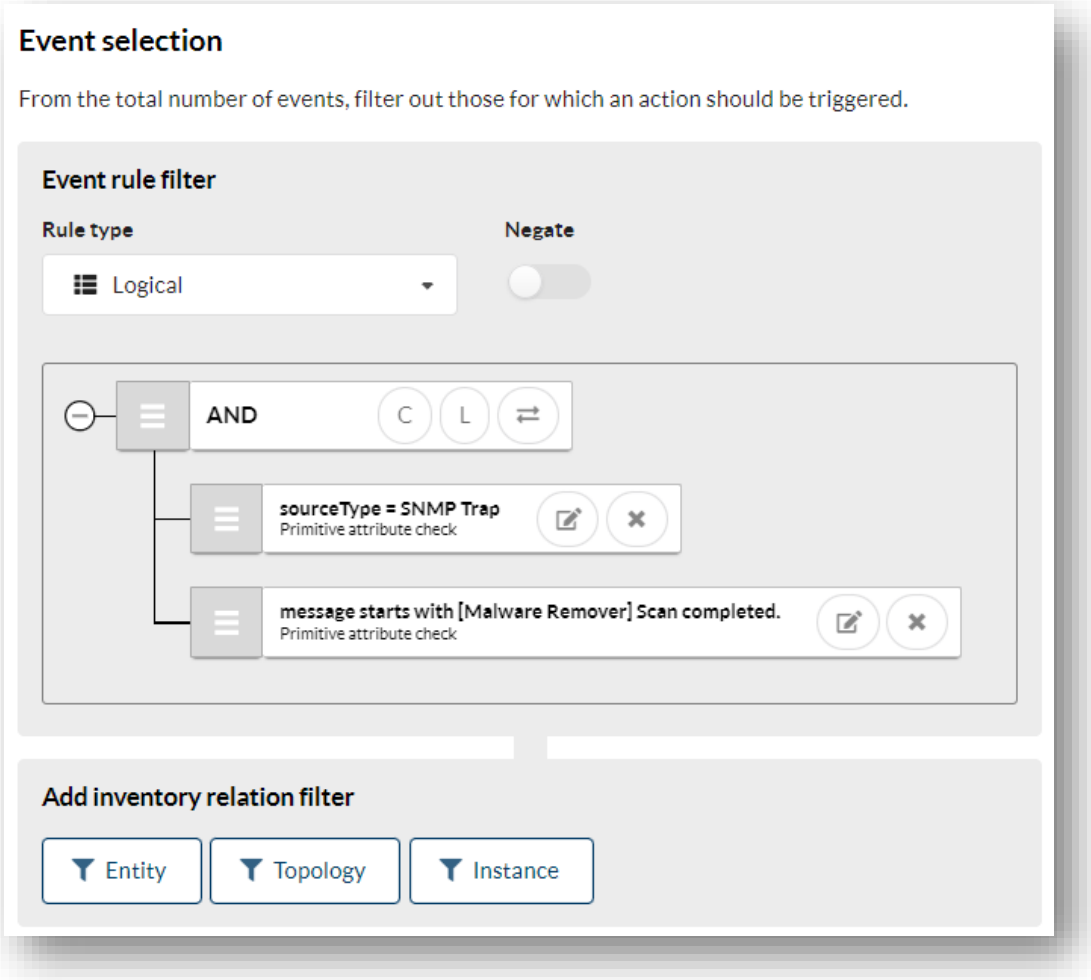


versio.io

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



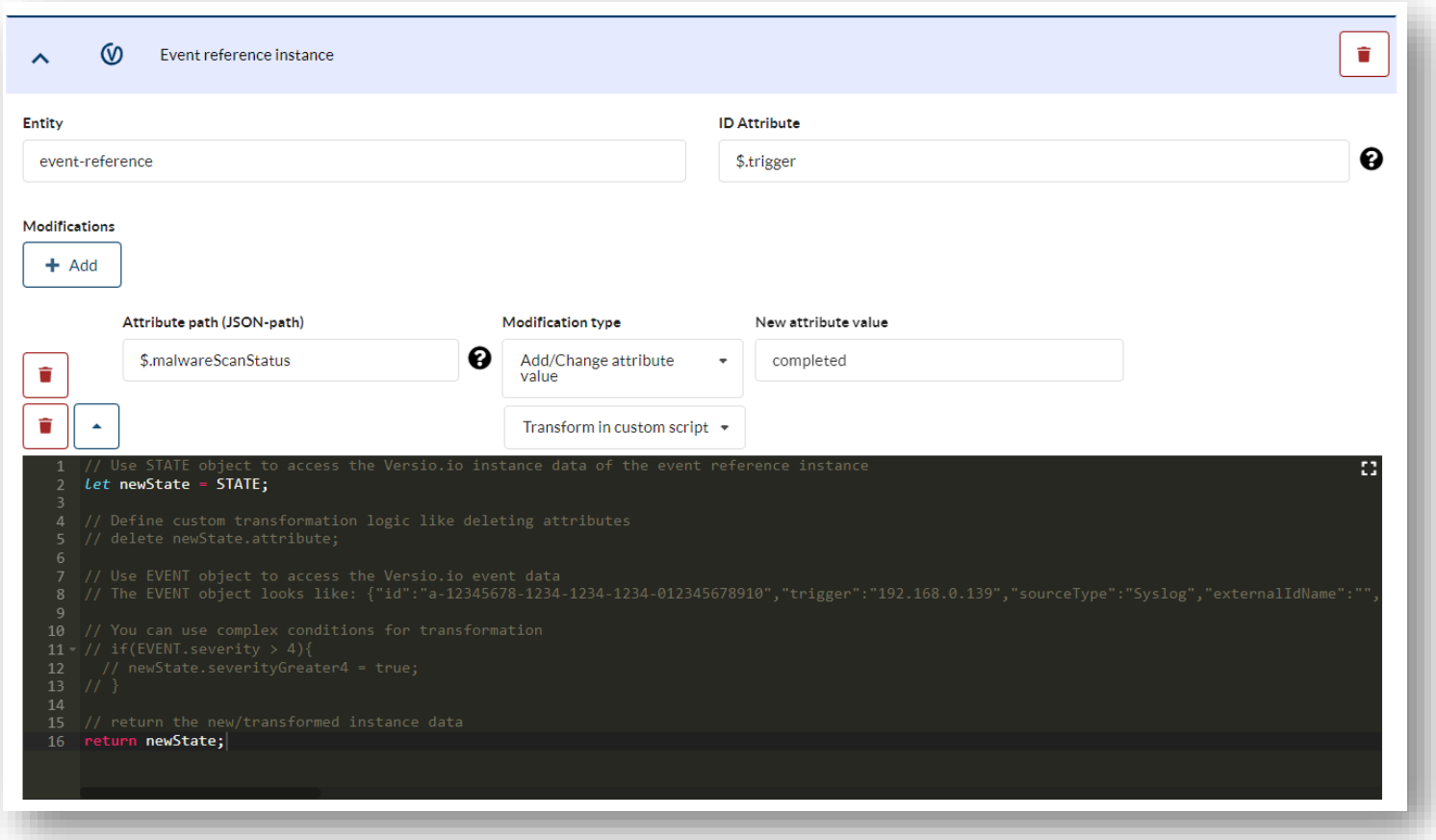
Online training

versio.io

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.



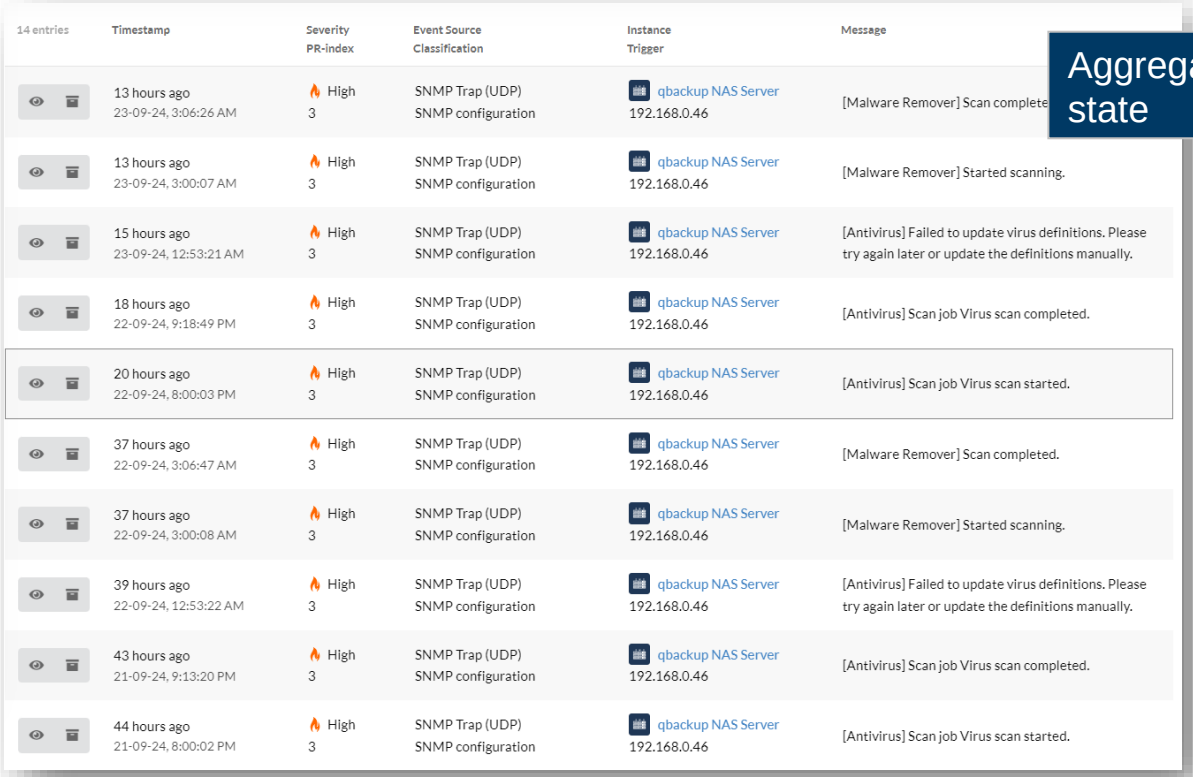
Online training

versio.io

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.

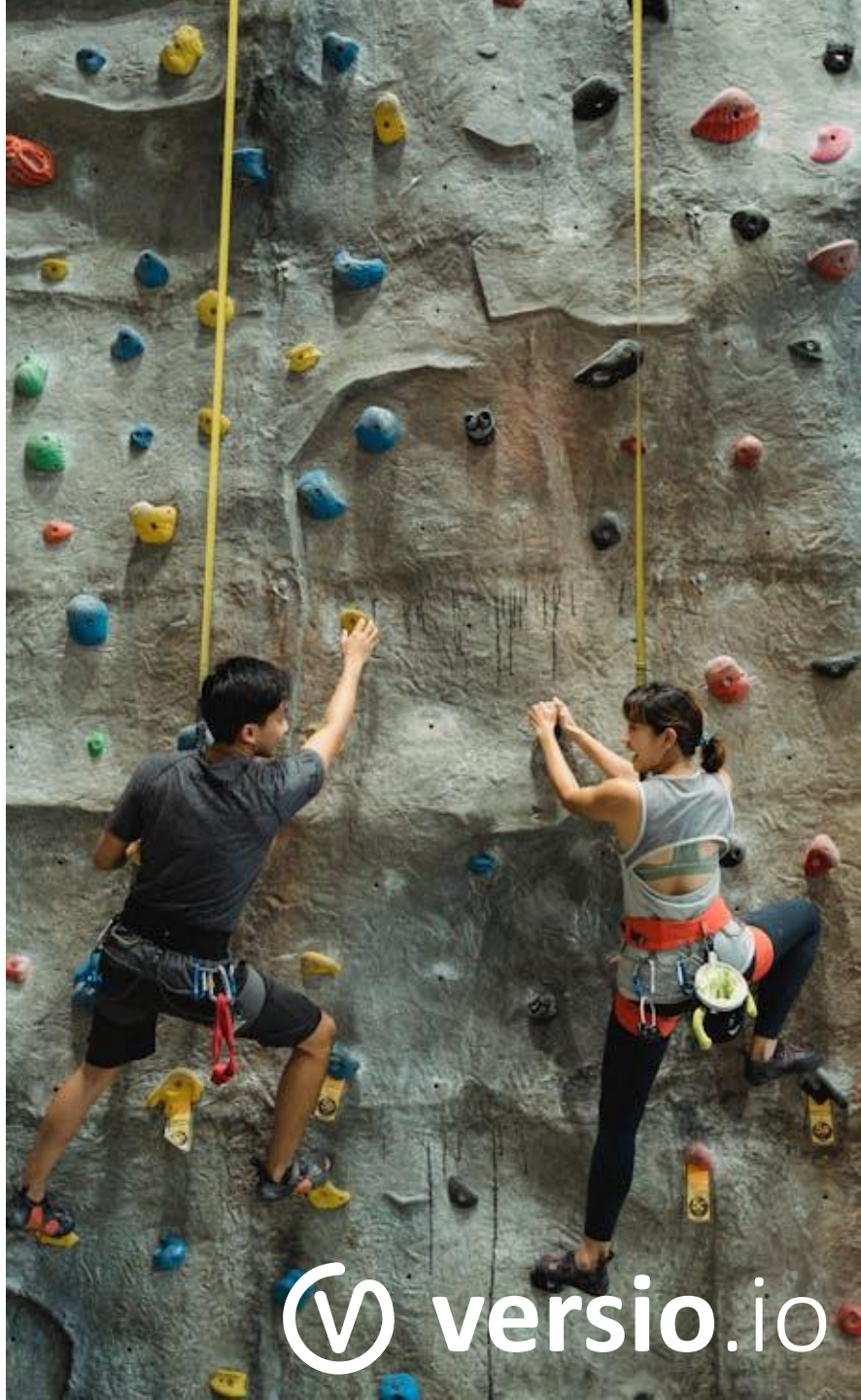
Aggregated state

Versio.io 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



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

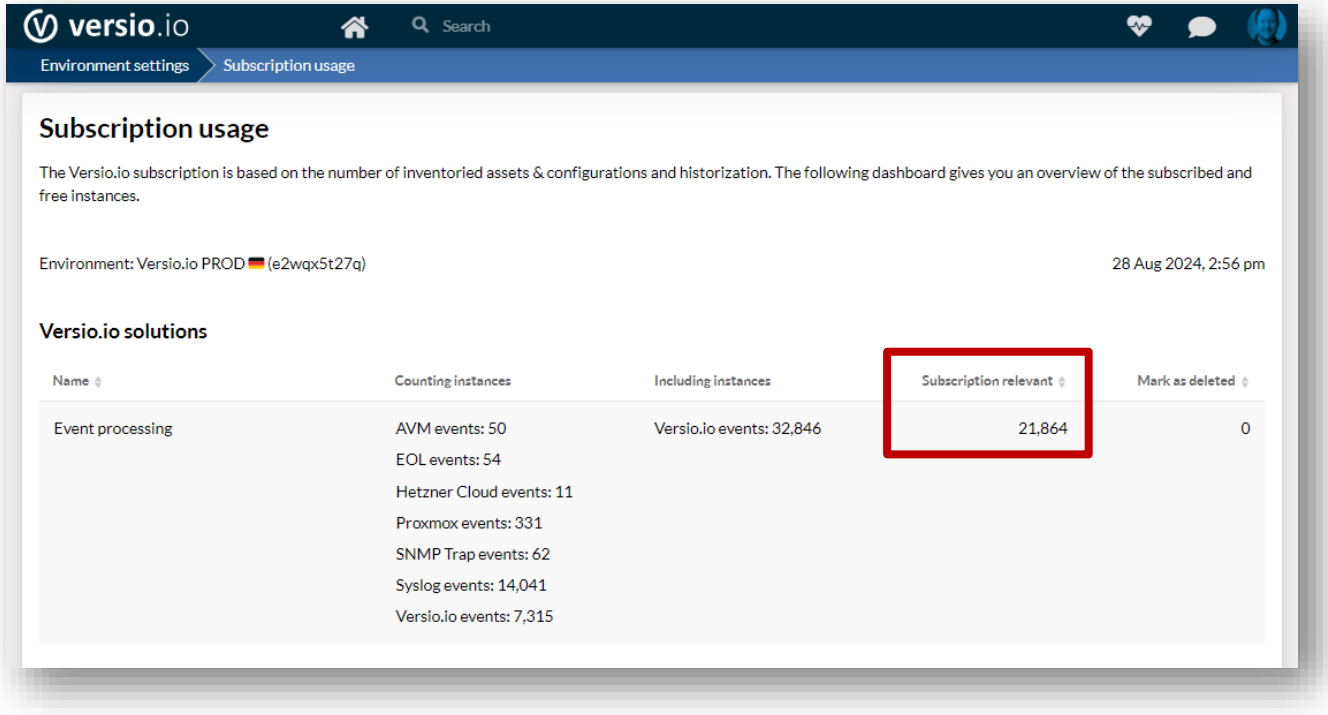
Versio.io Event Management & Alerting

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

versio.io

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

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?

versio.io

Inventory | Change Monitoring | Cybersecurity | Governance | Data Center & Cloud

versio.io

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

YouTube

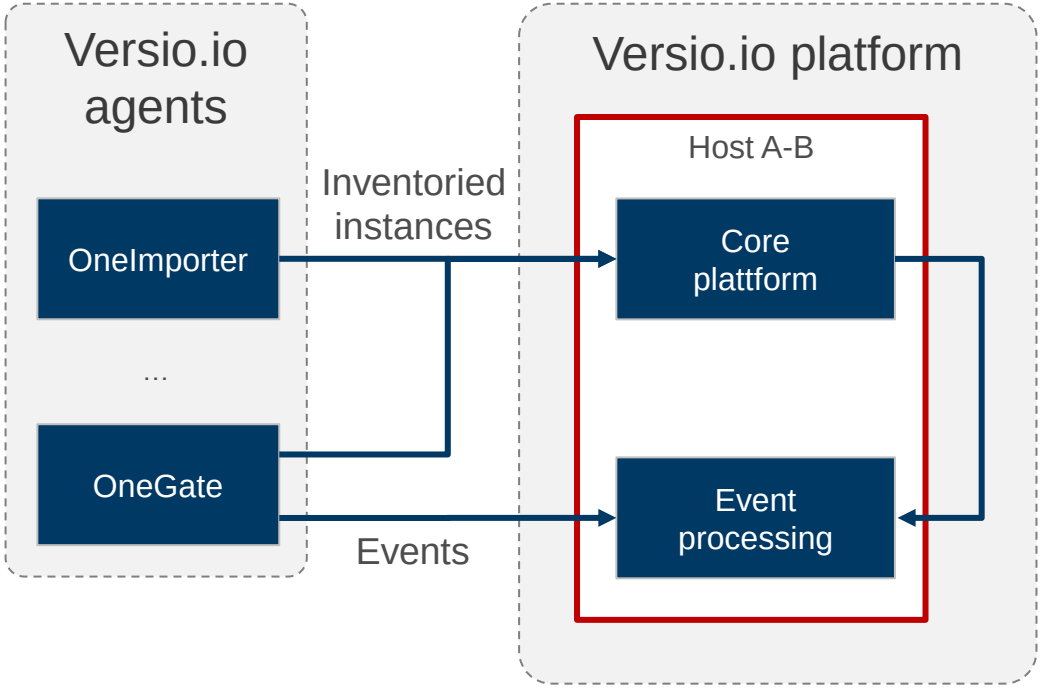
Versio in a nutshell

Versio.io Event Management & Alerting

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

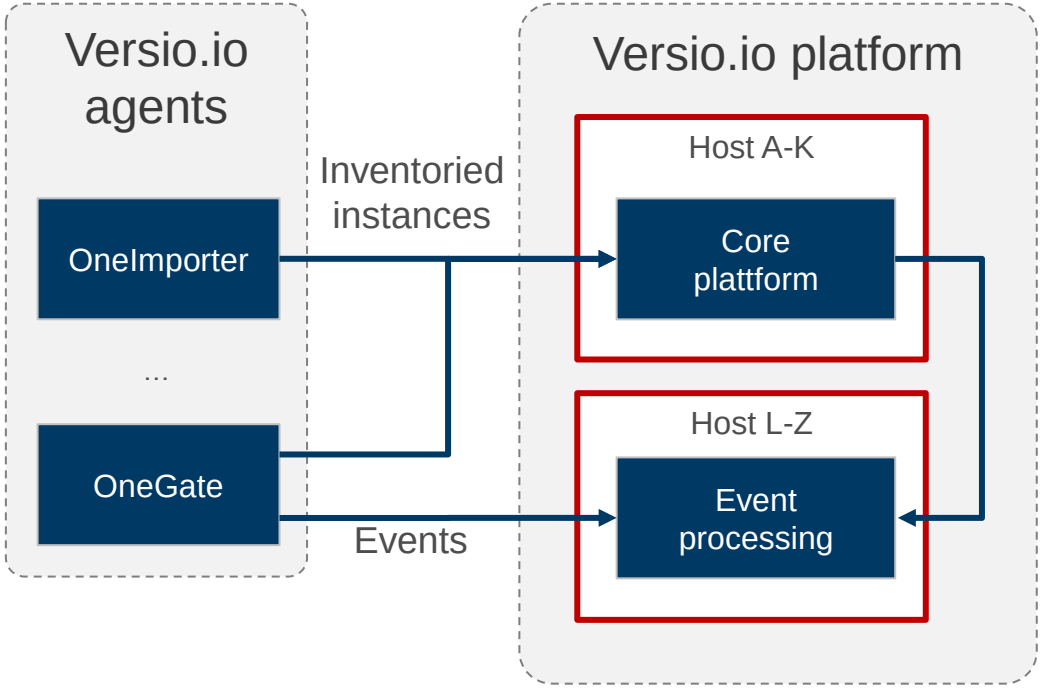
Small number of events

- 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

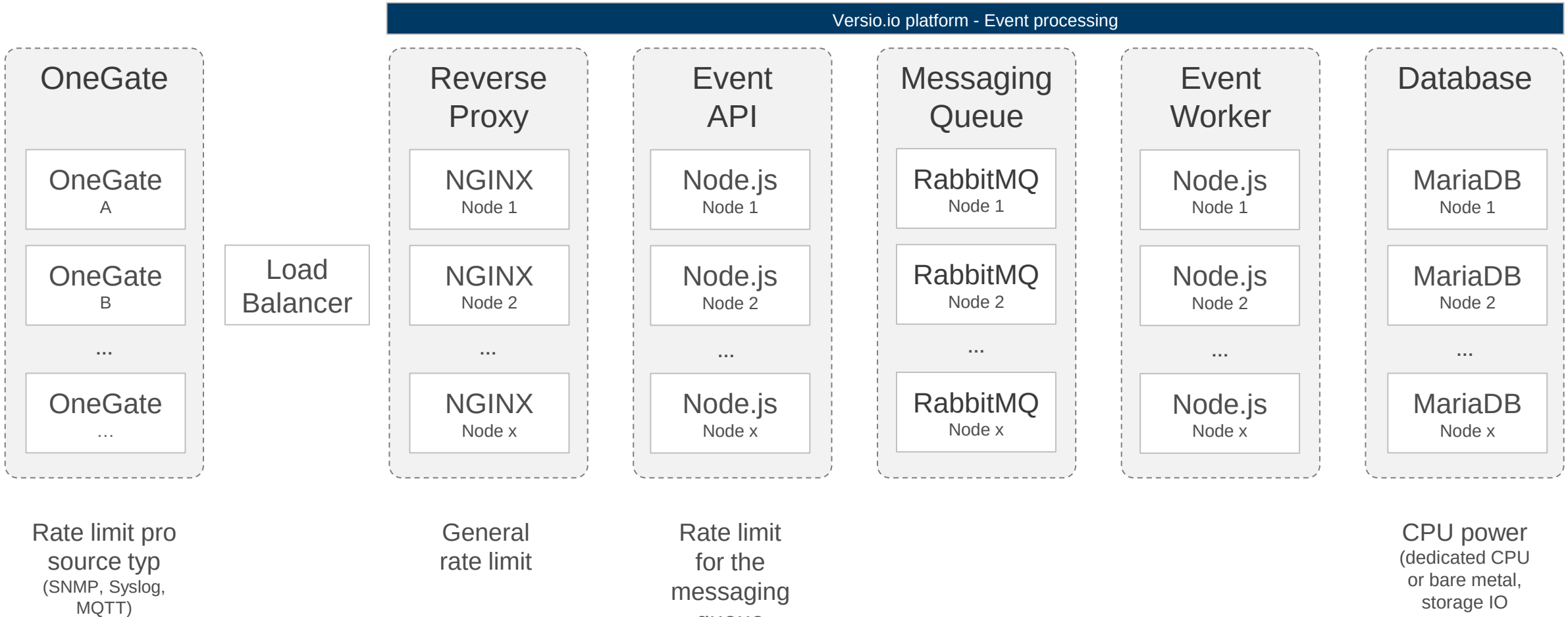


Online training

versio.io

Versio.io Event Management & Alerting

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



Online training

versio.io