OMICRON

StationGuard GridOps

What’s New in Version 2.00

Version 2.00

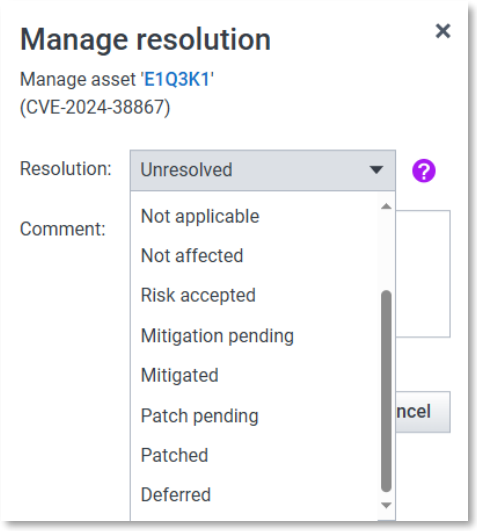
Highlights

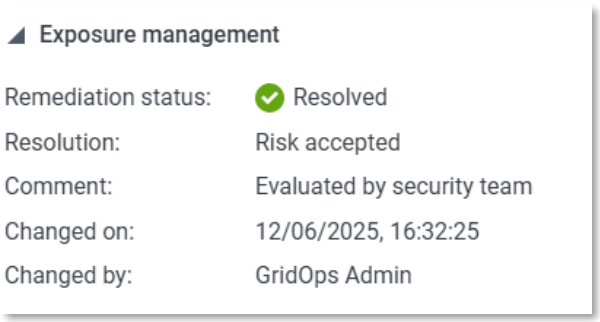
- > Status-based vulnerability resolution
- > Smarter vulnerability matching with improved precision
- > More insights into vulnerability matching
- > Continuous extension of vulnerability and asset type database
- > Real-time sensor state
- > Dashboard improvements

1. Status-based vulnerability resolution

Coordinate your response to exposures more efficiently with the following capabilities:

- > Track matched vulnerabilities and easily define a status for each matched vulnerability to indicate which action is to be taken. For example:
  - > *Unresolved*
  - > *Under investigation*
  - > *False positive*
  - > *Not applicable*
  - > *Not affected*
  - > *Risk accepted*
  - > *Mitigation pending*
  - > *Mitigated*
  - > *Patch pending*
  - > *Patched*
  - > *Deferred*
- > You can see at any time who treated potential threats and when a resolution was applied.
- > It is possible to manage multiple affected assets at once.





2. Smarter vulnerability matching with improved precision

Building on our industry-leading accuracy in vulnerability detection, GridOps now introduces several enhancements that push precision even further:

- **Support for CSAF relationships**: We have laid the groundwork to match vulnerabilities specifically to the affected hardware of individual vendors. This enables GridOps to read CSAF relationships, recognizing that certain CVEs from specific vendors often impact only particular hardware models rather than entire product series.

- **Module-specific vulnerability matching:** GridOps extracts the CP module type from SIEMENS device product codes for more accurate vulnerability matching – especially in cases where CVE applicability varies between base modules (e.g., CP100, CP200) and expansion modules.

- We have further reduced false positives by introducing smarter filters and refined matching techniques – even when asset data is incomplete.

- **GridOps recognizes product name variations**: It can identify device models even when listed with different naming conventions – such as synonyms, acronyms, and abbreviations – and accurately assign them to the correct product group. This further improves the precision of the vulnerability matching algorithm.

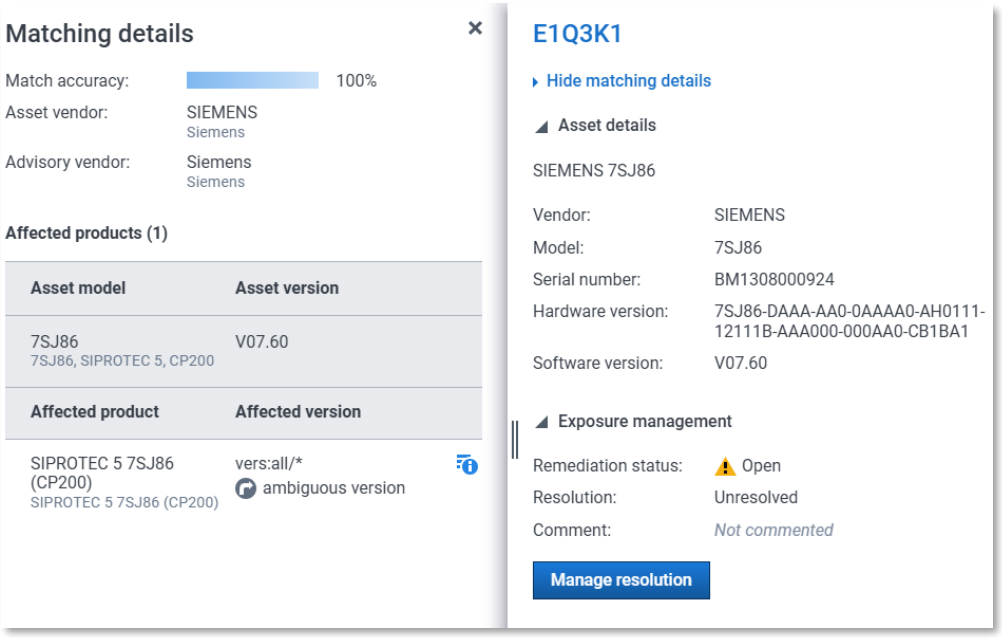
    - **Schneider**
        - Distributed Control System – DCS
        - Tricon Communication Model/Module – TCM
        - Tricon Processor Model/Module – TPM
        - APC PowerChute Network Shutdown – PCNS
    - **Siemens**
        - Totally Integrated Automation – TIA
    - **Hitachi**
        - ASPECT Enterprise - ASP-ENT
        - Harmony OPC Server – HAOPC
    - **Westermo**
        - RedFox Industrial Rack – RFIR
    - **Cisco**
        - Application Policy Infrastructure Controller – APIC
        - Aggregation Services Router – ASR
        - Analog Telephone Adapter – ATA
        - Adaptive Security Appliance – ASA
        - Cisco Secure Firewall – CSF
        - Firepower Management Center – FMC
        - Firepower Threat Defense – FTD
        - Firepower Extensible Operating System – FXOS
        - IoT Field Network Director - IoT FND
        - Integrated Services Router – ISR
        - Network Convergence System – NCS
        - Wide Area Application Services – WAAS
        - WAN Automation Engine – WAE
        - Wireless LAN Controller – WLC

- False positives for A8000 assets have been significantly reduced. Previously, CP-802x models were also matched to CP-803x, but the matching logic has now been refined to distinguish CP models more precisely.

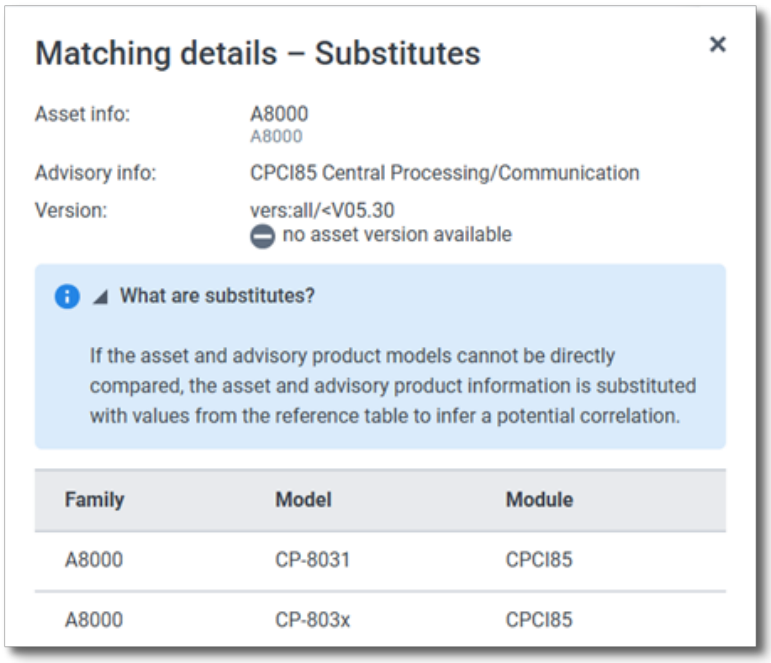
3. More insights into vulnerability matching

Vulnerability matches are presented with even clearer insights and better transparency:

> **New matching details:** You are provided with information on why a specific vulnerability matches an asset. This offers deeper insights into the matching process and helps you understand the context and rationale behind each vulnerability match.



> We have extended the *Matching details* to include the option to view substitutes when they were used to match a product.



4. Continuous extension of vulnerability database

Our vulnerability database is constantly growing – recently, we have added over 3 000 new vulnerabilities from more than 1 000 new advisories.

Vulnerabilities	Vendors	Advisories
13 000 +	**39 +**	**5 500 +**

Total: July 5, 2025

5. Continuous extension of asset type database

The asset database in GridOps has been extended to include additional device vendors and families. This allows more accurate classification of assets by type, family, and vendor, which improves precision in vulnerability matching.

These are the newly added asset families:

- **Schneider**
  - Andover Continuum
  - Sage RTU
  - TCM
  - UCM
  - TPM
  - TriStation
- **Hitachi**
  - SAM-IO
- **Siemens**
  - A8000 modules
  - A8000 / CP-801x
  - DIGSI
  - M969
  - RUGGEDCOM switches (12 series)
  - Reyrolle
  - S7-300 / S7-400 / S7-1500
  - Scalance series (24 series)
  - i800
- **FortiNet**
  - FortiAP
  - FortiGate
  - FortiProxy
  - FortiSwitch
- **Cisco**
  - ASA firmware
  - FTD firmware
  - FXOS firmware
  - NX-OS firmware
  - ASA series
  - ASR series
  - CGS series
  - CSF series
  - Catalyst series
  - Firepower series
  - IE series
  - ISR series
  - MDS series
  - NCS series
  - Nexus series
  - UCS series
- **Phoenix Contact**
  - RS4000
  - PLCnext
- **Rockwell**
  - Kinetix families
  - Stratix families

6. Real-time sensor state

We have improved the transparency of StationGuard Sensor in GridOps to help you stay informed at a glance.

- The sensor connection state is now displayed, including real-time updates. You can find it under the *Sensor management* tab.

- Additionally, the sensor connection state can also be found in the *Sensors* dashboard. There, you can also see whether the maintenance mode for each sensor is enabled or not.

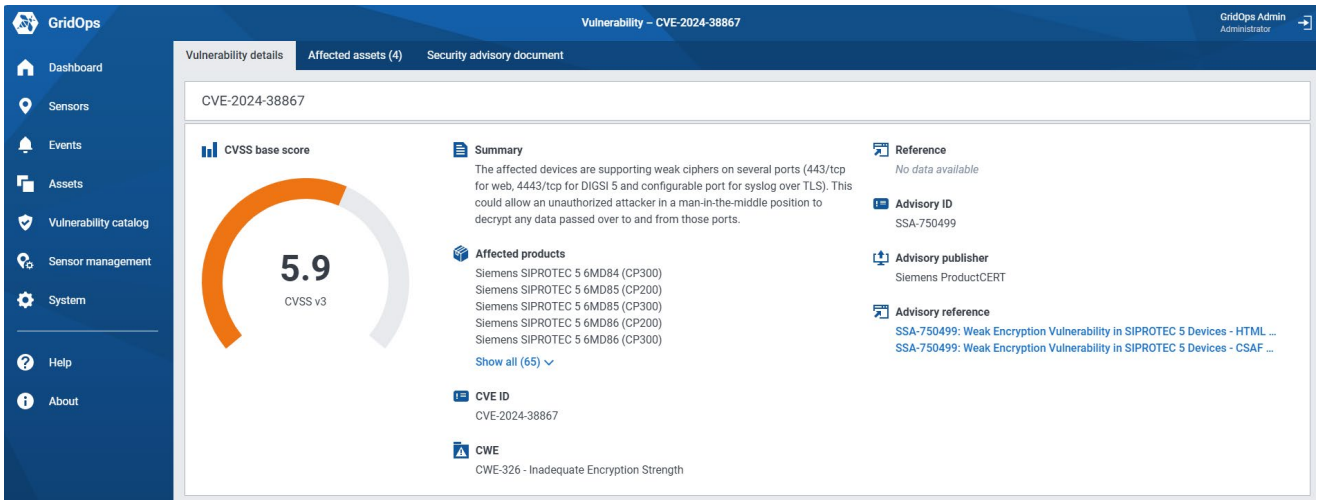
7. Dashboard improvements

We've made several improvements to the dashboards to provide clearer insights and increase performance – especially when you are working with large asset environments:

- The *Event detail* dashboard includes VLAN ID and VLAN priority for GOOSE alerts.
- New panels added into *Event detail* dashboard:
  - *Network layer*: Used by events that overlap with the selected time range.
  - *Transport layer:* Used by events that overlap with the selected time range.
  - *Application layer:* Used by events that overlap with the selected time range.
  - *Service*: Used by events that overlap with the selected time range.
- Dashboards now filter out vulnerabilities marked as *Resolved*.
- The related terminology is renamed from *Vulnerabilities* (*Assets affected by vulnerabilities*) to *Exposures* (*Exposed assets*).
- Dashboard panel performance improved for environments with many affected assets. In relation, storage usage for vulnerability matching has been optimized.
- The readability of PDF reports has been improved with optimized table generation.
- The setup of the Grafana Alerting email integration has been simplified.

8. New vulnerability page

Vulnerability-related information has been moved from the Grafana dashboard to a dedicated section – making it easier to access details, manage exposures, and act directly where it matters:



- **New *Vulnerability details* tab**: Vulnerability details are now available on the *Vulnerability* page, replacing their previous position on the *Vulnerability* dashboard in Grafana.
- **New *Affected assets* tab**: The affected assets of a vulnerability are now available on the *Vulnerability* page, replacing their previous position on the *Vulnerability* dashboard in Grafana. It provides detailed information about asset impacted by a vulnerability, including sensor and network interface data. It also introduces *Exposure management* for assessing and handling vulnerabilities and assigning resolutions with clear reasoning (see *Status-based vulnerability resolution* above).
- **New *Security advisory document* tab**: Security advisory documents are now available on the *Vulnerability* page, replacing their previous position on the *Vulnerability* dashboard in Grafana.

9. Accelerated vulnerability matching performance

The speed of matching vulnerabilities with existing assets has been further increased - in some cases significantly. This accelerates the processes for analyzing and handling the vulnerabilities relevant to the asset.

10. Component updates

> Keycloak is updated from 23.0.7 to 26.0.5
> Grafana is updated from 11.0.0 to 11.2.4

11. Bug fixes and minor improvements

There have been many minor fixes and improvements.

12. Product lifecycle and support notice

The update from StationGuard GridOps 1.20 to version 2.00 is free of charge. Please note that StationGuard GridOps version 2.00 replaces version 1.20 as service baseline. We strongly recommend updating all your devices to version 2.00.

At OMICRON, we take any type of vulnerability affecting our products very seriously, and we appreciate and welcome any report that helps us improve their security. Consequently, we have established a systematic approach for receiving, handling, and disclosing such vulnerabilities.

Please visit https://www.omicronenergy.com/en/support/product-security for further information.

Previous Releases

	Focus	Released in
Version 1.20	Vulnerability Database Improvement	May 2024
Version 1.10	Improved Usability	December 2023
Version 1.00	Original Software Release	December 2022

Version 1.20

1. New advisories in the vulnerability catalog

The vulnerability catalog has been expanded to include the following vendors, with new additions highlighted in **bold**:

Vendors		
ABB	**HMS Networks**	**PSI GridConnect**
Advantech	**Honeywell**	**Rockwell**
A. Eberle	**IPCOMM**	**SAE IT-systems**
Beckhoff	**Landis+Gyr**	Schneider Electric
Cisco	**Meinberg**	**Schweitzer Engineering Laboratories**
Delta Electronics	Moxa	Siemens
EFACEC	**mySCADA**	Sprecher Automation
Fortinet	**Nari**	Vivavis
General Electric (Gas Power)	**Nokia**	**WAGO**
General Electric (Grid Solution)	OMICRON	Westermo
Hirschmann/Belden/ProSoft	**Panasonic**	**Wibu-Systems**
Hitachi Energy	**Phoenix Contact**	

> Total number of advisories: **4,050+**
> Total number of vulnerabilities: **9,620+**

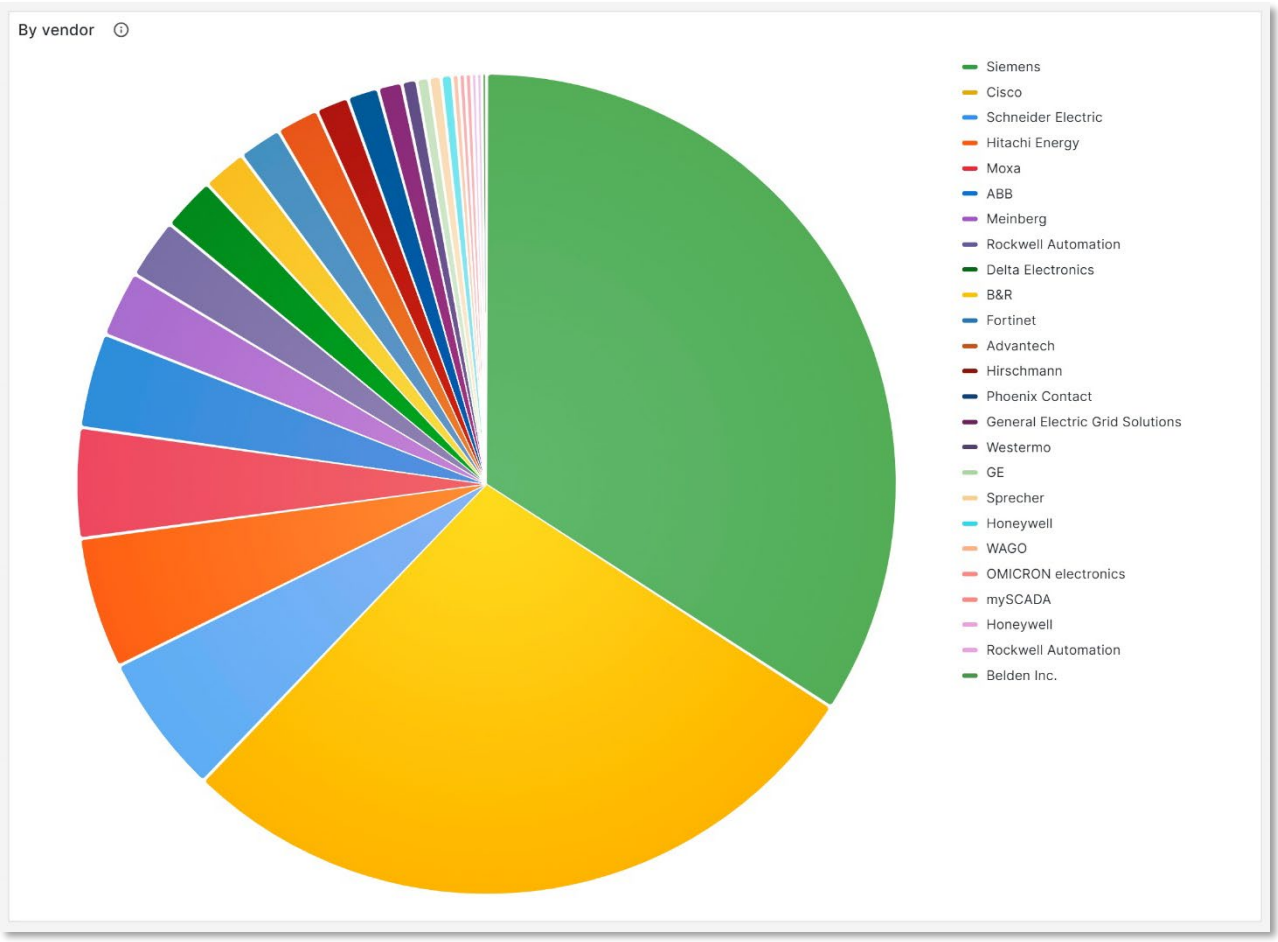


Figure 1: Vulnerabilities by vendor

2. Accelerated vulnerability matching performance

We have optimized our matching speeds across various vendors:

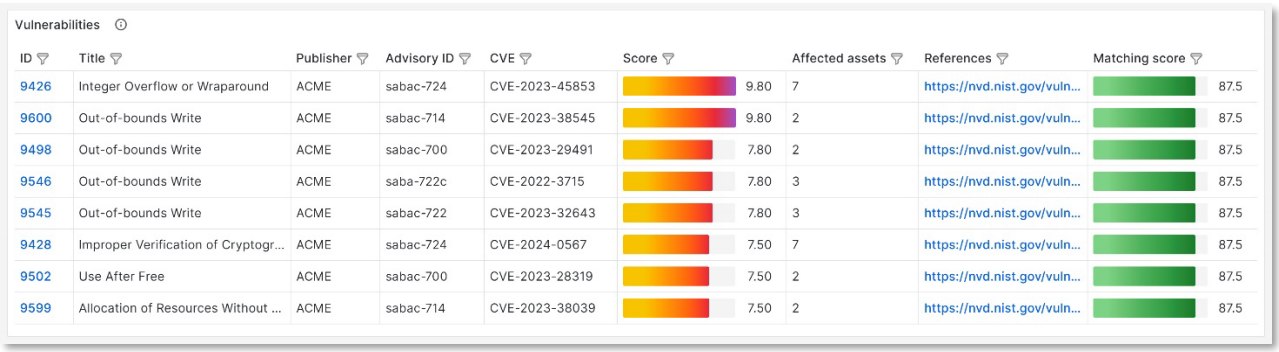
- **Cisco** ~20x faster
- **Siemens** ~10x faster
- **ABB** ~5x faster
- **Hitachi** ~5x faster
- **Schneider** ~5x faster
- **Moxa** ~3x faster
- **Hirschmann** ~2x faster

As a result, depending on the asset inventory, matching duration has been significantly reduced from a range of 1 to 900 seconds to 1 to 50 seconds per asset. For instance, with 100 assets, the process now averages about 15 minutes. Remember, the completeness, accuracy, and precision of your asset inventory directly impact the speed of the process.

3. Profound vulnerability matching accuracy

We have implemented features to enhance our data accuracy, specifically targeting the precision of vulnerability matching. In line with our commitment to thoroughness, we have differentiated between specific device families and versions, which allows for comprehensive coverage of our data. Here are a few examples:

Vendor	Enhancements
General Electric (Grid Solution)	> Added Multilin, UR, URplus, and SR device families
Meinberg	> Added LANTIME, IMS, SyncFire device families and LTOS
Siemens	> Differentiation between A8000 CP-800x/802x and CP-803x/805x > RUGGEDCOM RS900 now matches RS9xx advisories
Westermo	> Differentiation between WeOS version 4.X and 5.X > Added Wolverine device families


Vulnerabilities

ID	Title	Publisher	Advisory ID	CVE	Score	Affected assets	References	Matching score
9426	Integer Overflow or Wraparound	ACME	sabac-724	CVE-2023-45853	9.80	7	https://nvd.nist.gov/vuln...	87.5
9600	Out-of-bounds Write	ACME	sabac-714	CVE-2023-38545	9.80	2	https://nvd.nist.gov/vuln...	87.5
9498	Out-of-bounds Write	ACME	sabac-700	CVE-2023-29491	7.80	2	https://nvd.nist.gov/vuln...	87.5
9546	Out-of-bounds Write	ACME	saba-722c	CVE-2022-3715	7.80	3	https://nvd.nist.gov/vuln...	87.5
9545	Out-of-bounds Write	ACME	sabac-722	CVE-2023-32643	7.80	3	https://nvd.nist.gov/vuln...	87.5
9428	Improper Verification of Cryptogr...	ACME	sabac-724	CVE-2024-0567	7.50	7	https://nvd.nist.gov/vuln...	87.5
9502	Use After Free	ACME	sabac-700	CVE-2023-28319	7.50	2	https://nvd.nist.gov/vuln...	87.5
9599	Allocation of Resources Without ...	ACME	sabac-714	CVE-2023-38039	7.50	2	https://nvd.nist.gov/vuln...	87.5

Figure 2: Example of vulnerabilities with criticality and matching score

4. Best practices for asset inventory data

The documentation now contains suggestions on how to improve the asset data to improve the accuracy of the vulnerability matching. See "*Help* > *GridOps assets* > *Vulnerability matching* > *Best practices*" for further details.

5. Reduced loading time of Event Dashboard

The loading time of the *Event Dashboard* has been reduced by optimizing the queries for larger data sets.

6. Show search results for imperfect vulnerabilities and advisories

Previously, some vulnerabilities and advisories were missing when using the free text search in the *Vulnerability Catalog Dashboard*. Now, the results include all matching vulnerabilities and advisories.

7. Default auto-refresh intervals for dashboards

Auto-refresh intervals are now set to 1 minute across all dashboards to ensure predictable behavior. The intervals may still be customized for each dashboard.

8. Expanded storage space

When extending the virtual disk size, GridOps now automatically uses the newly available storage. See "*Help > GridOps platform > Expanding the storage space*" for more details.

9. Bug fixes and minor improvements

> The host system recovers properly when an early reboot is triggered during startup.
> The reliability of the initial sensor connection has been improved.
> And many other minor fixes and improvements.

10. Component updates

> Keycloak has been updated from 21.1.1 to 23.0.7.

Version 1.10

1. New advisories in the vulnerability catalog

The vulnerability catalog has been expanded to include the following vendors:

Vendors		
ABB	Hirschmann/Belden/ProSoft	Siemens
A. Eberle	Hitachi Energy	Sprecher Automation
Cisco	Moxa	Vivavis
Fortinet	OMICRON	Westermo
General Electric (Gas Power)	Schneider Electric	

> Total number of advisories: **3,527**
> Total number of vulnerabilities: **7,796**

2. Improved vulnerability matching

We have implemented features to enhance our data accuracy, specifically targeting the accuracy of vulnerability matching and performance. Here are a few examples:

Vendor	Enhancements
Hitachi / ABB	> Added Relion device families
Schneider	> Added P30 and P40 device families
Siemens	> Added RUGGEDCOM device families > Added SIPROTEC 4/5/Compact device families > Map CP050, CP100, CP200, CP300, and EN100 modules to the corresponding devices
Westermo	> Added Lynx, RedFox, and RFIR device families

3. Reduced loading time for dashboards

The performance of the dashboard query and the mapping of data points have been improved, resulting in a faster loading time for all dashboards.

4. Advisory reference in the *Vulnerability Dashboard*

The *Vulnerability Dashboard* now includes a reference to the corresponding advisory.

5. More selective *dashboard* filtering

Dashboard filters have been simplified and expanded to provide more control over the narrowing down of results.

6. Updating *GridOps*

As of 1.10, GridOps can be updated using the web interface. See "*Help* > *GridOps platform* > *Updating GridOps*" for further details. In addition, the installation image has been reduced from ~8GB to ~3GB to speed up the deployment process.

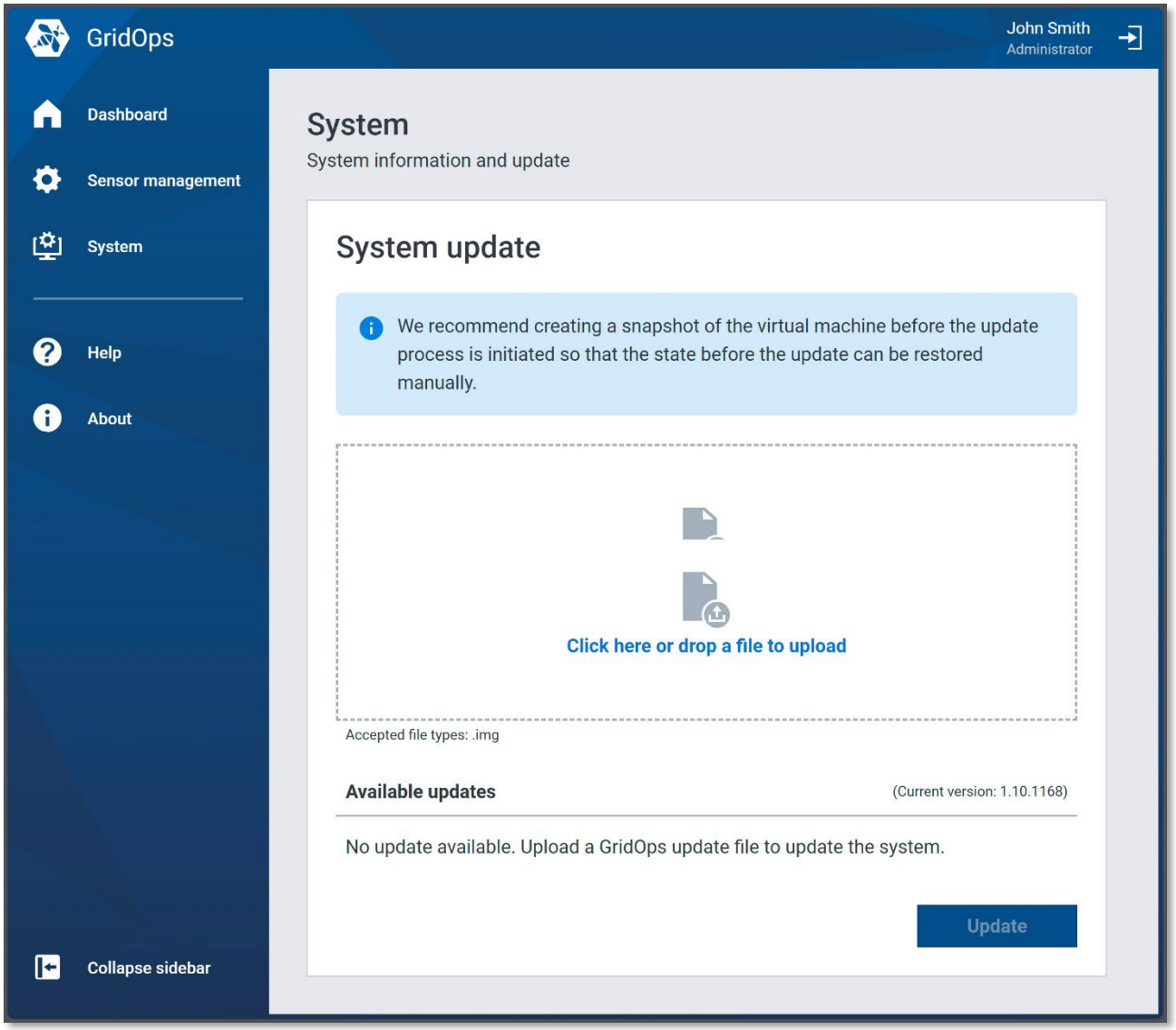


Figure 3: GridOps update user interface

7. Full *support* for StationGuard 2.30 messages

StationGuard 2.30 messages are fully supported with built-in message timestamps and sensor configuration history support. However, StationGuard 2.20 messages are only partially supported because sensor configurations are no longer updated.

8. Simplified tracking of *unacknowledged* and active events

Events now include a timestamp to improve tracking of unacknowledged and active events. This allows for more accurate analysis of events.

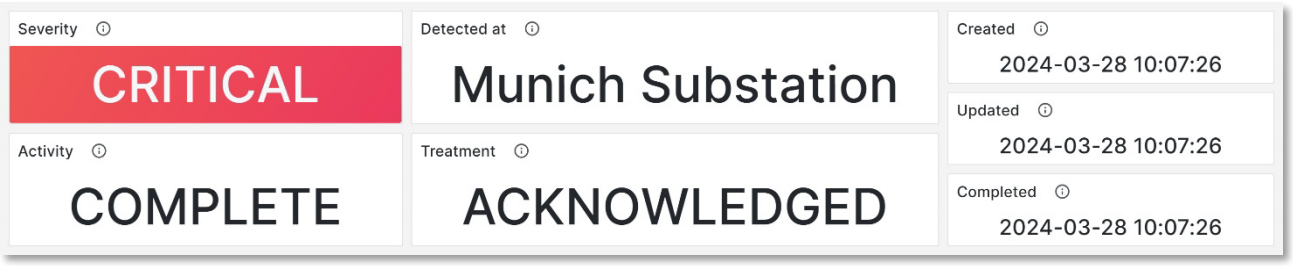


Figure 4: Events with time stamp

9. Advanced access to identity and *access* management

GridOps administrators now have advanced access to the Keycloak settings, allowing deeper control and customization of identity and access management (e.g., managing OpenID Connect clients). See "*Help* > *GridOps platform* > *Keycloak identity and access management"* for more details.

10. Data retention

To ensure sufficient available space, GridOps automatically optimizes data retention by deleting the oldest data until sufficient space is regained. See "*Help* > *GridOps platform* > *Data retention*" for more details.

11. Bug fixes and minor improvements

> GridOps services now fully recover from unexpected user actions, such as system boot interrupts.
> TLSv1 TLSv1.1 TLSv1.2 have been disabled. Only TLSv1.3 is used, which ensures perfect forward secrecy.
> And many other minor fixes and improvements.

12. Component updates

> Keycloak has been updated from 20.0.2 to 21.1.1.
> Grafana has been updated from 9.3.6 to 10.2.2.

Version 1.00

1. The central management system for StationGuard

As the central management system for StationGuard, GridOps can visualize OT networks in the grid on multiple dashboards with different views. For example, one dashboard can show the global asset inventory, while another dashboard can show all alerts for a specific network.

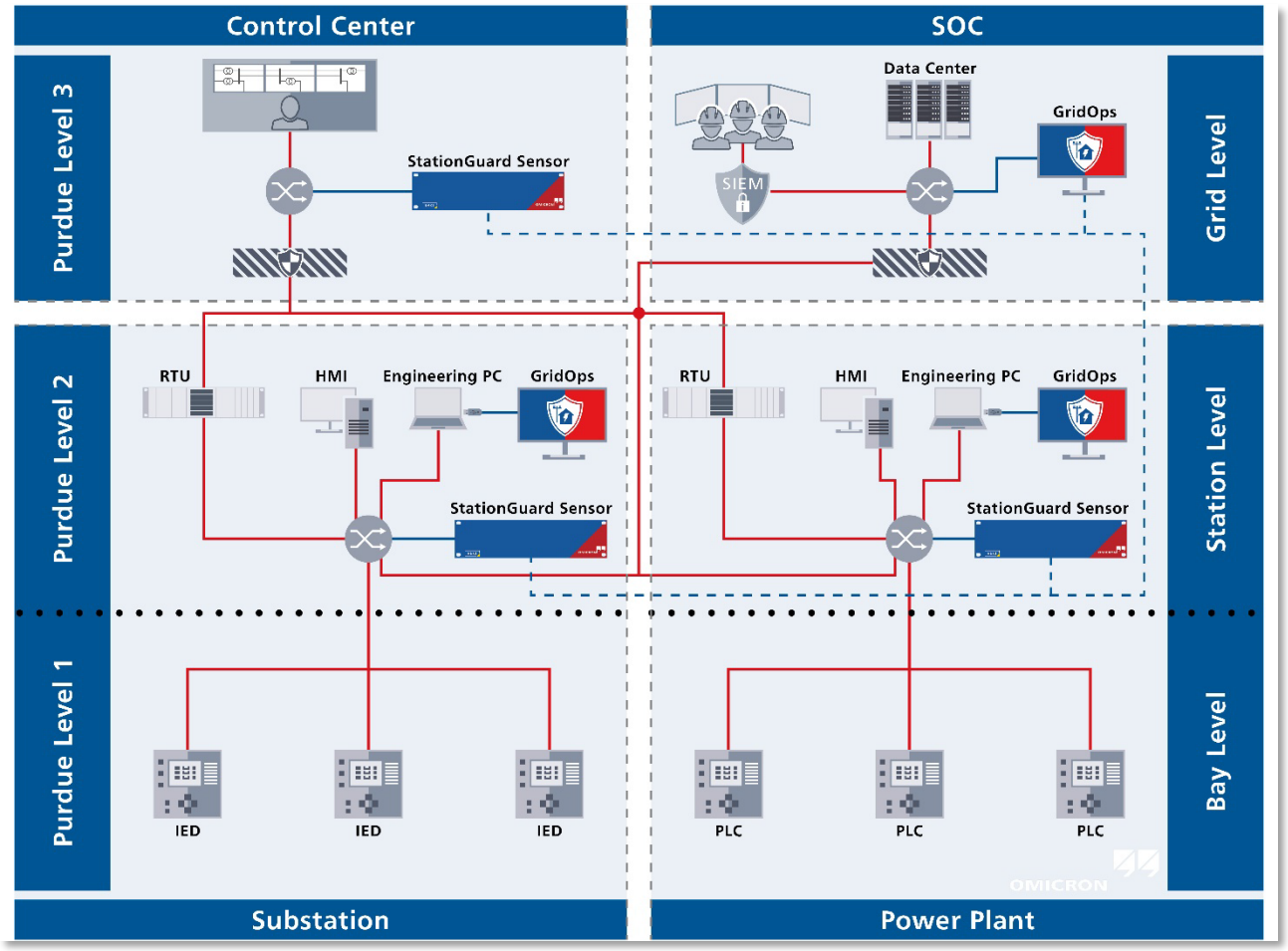


Figure 5: Typical deployment of GridOps with StationGuard

2. Grid-wide visibility

GridOps dashboards provide easy access to alert status across the grid. Users can instantly see if there are critical alerts at any given location or time. The platform provides a variety of visualization and analysis options for analyzing current and historical events. GridOps also maintains a database of all events and activities that have occurred across all sensors.

This allows users to view and search previously recorded events from all locations where sensors are installed. The Alert Overview dashboard uses time series graphs and pie charts to visualize how different types of alerts are distributed across different geographic areas within the OT network based on the type of alert.

Users can also see how these alerts relate to different asset types and how they relate to each other. The frequency of alerts can also be examined as part of the incident analysis process.

By examining event data, an analyst can identify trends that can be analyzed based on the data collected to date. It is also possible to identify patterns and anomalous activity that can help identify suspicious activity. In

addition, all operational events logged by StationGuard (called “functional events”), including successful and failed switching operations, downloaded fault records, etc., can be analyzed by the user.

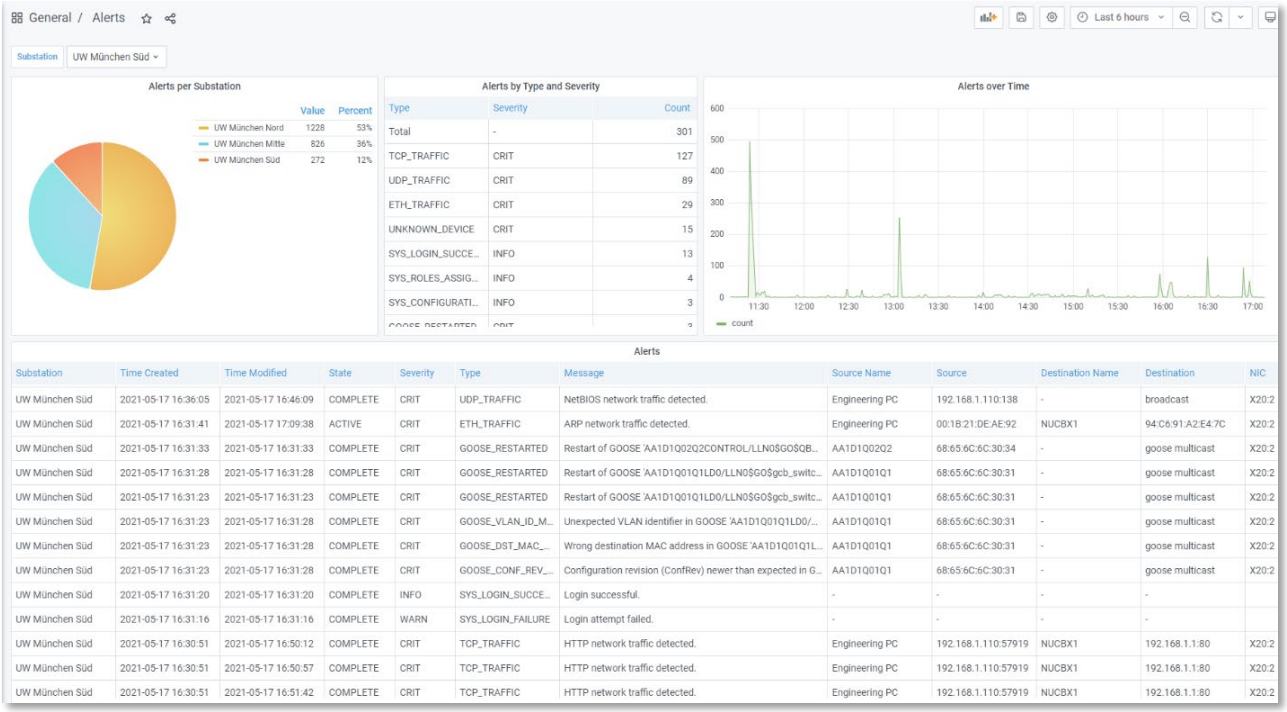


Figure 6: Alerts view

3. Global asset inventory

The GridOps platform creates a global asset inventory by combining data from all StationGuard sensors deployed across the grid. This data is made available for search and display by users of the platform. The asset inventory is updated in real time with information from all IDS sensors connected to the system. An overview of all asset properties is provided as a table, with filtering options available to locate specific asset types.

Combining all of these features with StationGuard's unmatched ability to import data from SCL files or plant documents that contain asset inventory information, OT and cybersecurity engineers can always have a detailed picture of their assets, allowing them to address any security or functional concerns.

The most important factor in effectively managing risk and vulnerability is having comprehensive data about each asset. The more information we have about a given asset, the more accurately we can prioritize and analyze vulnerabilities, and the more insightful the vulnerability assessment will be.

By using the mobile version of StationGuard for the MBX1 platform, networks that do not have a fixed (IDS) sensor installed can be scanned and added to the automated inventory.

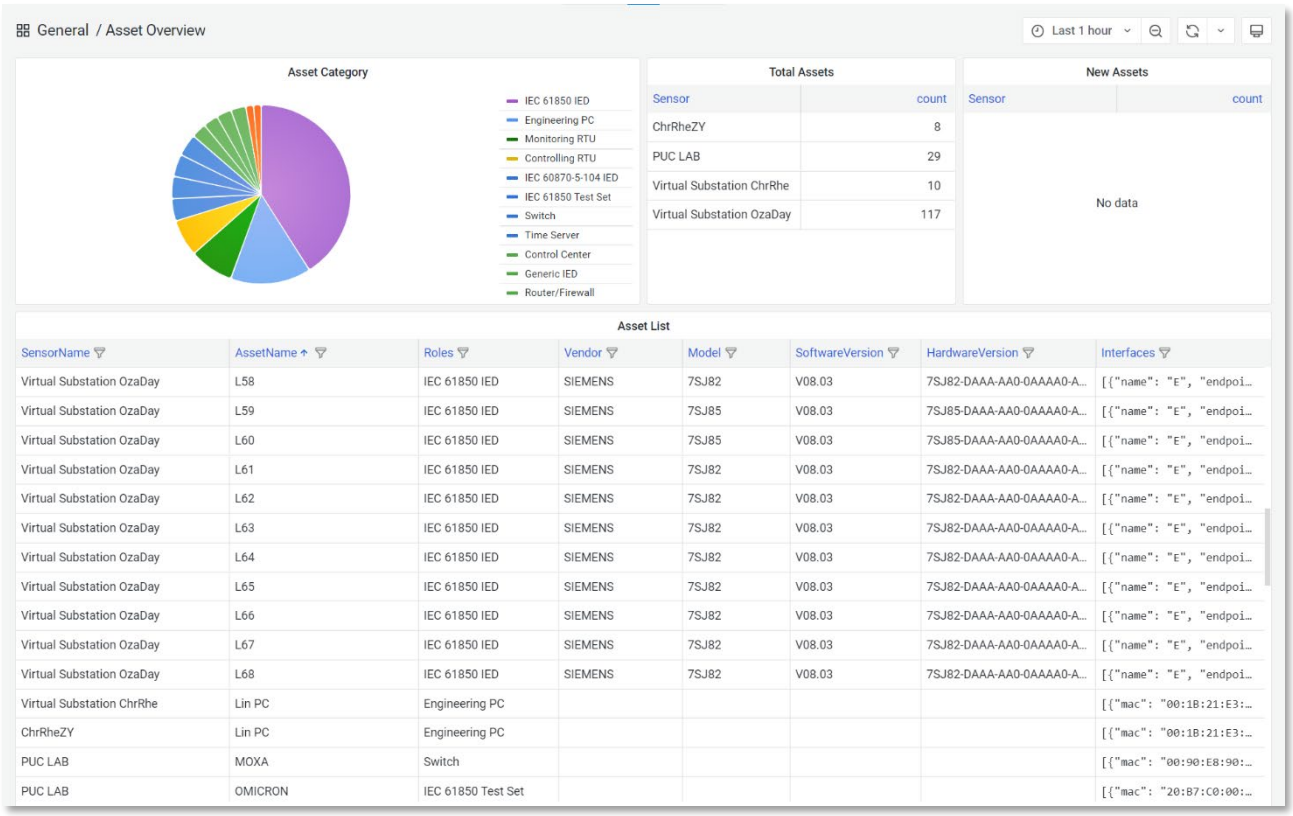


Figure 7: Asset overview

4. Vulnerability management

A critical aspect of vulnerability management is to identify, assess, report, manage, and remediate vulnerabilities that occur across a range of devices and assets within a network as part of a continuous process. The task of matching vulnerabilities disclosed for protection and automation devices with the actual devices installed in the field is surprisingly challenging.

There are several factors to consider when evaluating a vulnerability. Identifying the type of device you actually have and the version of firmware installed on it is the first step you must take to accomplish this task. In addition, you need to know whether certain network and CPU modules are installed on the device, and whether those modules are enabled.

To make matters worse, security advisories are not always as accurate as they should be. GridOps vulnerability management addresses all of the above concerns. By considering the impact of multiple *Common Vulnerability Exposures* (CVEs) and determining which IEDs are affected by a particular CVE or security advisory, we can more accurately determine whether an IED is vulnerable and, if so, to what extent. In addition, the *Asset Vulnerability Dashboard* provides insight into overall vulnerability exposure, criticality, and patchability, as well as the severity of those vulnerabilities.

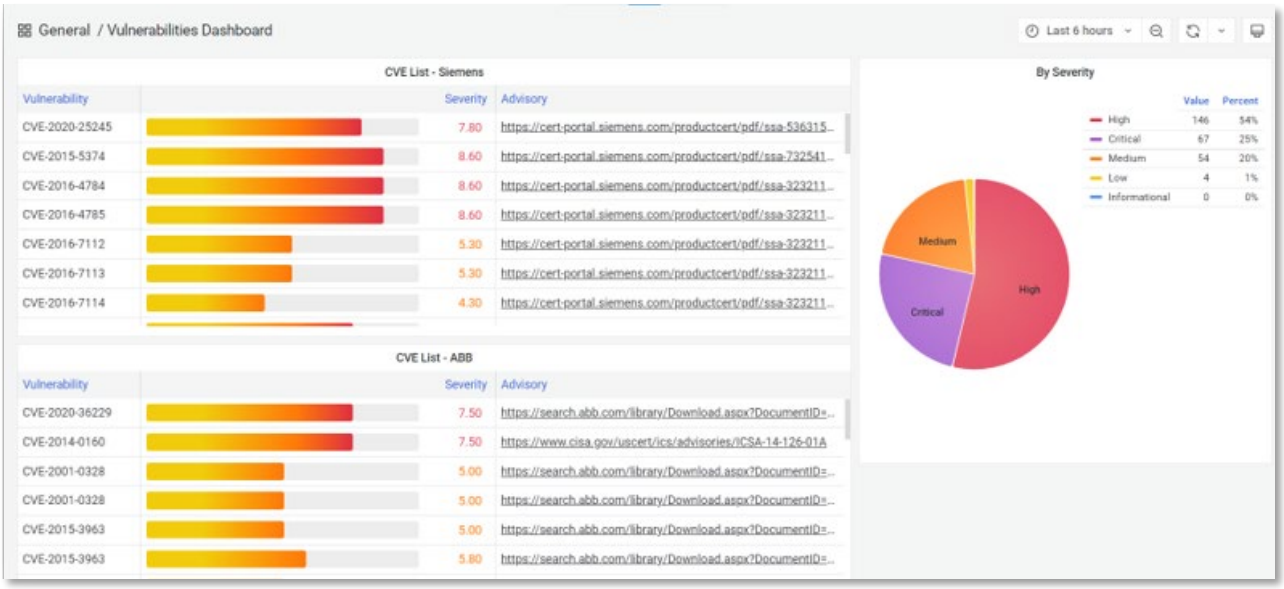


Figure 8: Vulnerability dashboard

5. Reporting

GridOps creates reports that provide you with early insights into cybersecurity trends, functional issues, statistics, your asset inventory, and the vulnerabilities associated with them. This information will allow you to document the state of your risk posture at the time of analyzing these reports. It also ensures that comprehensive and meaningful risk assessments can be prepared and presented to management, vendors, and regulators so that risk prioritization and mitigation can be guided.

6. Grid-to-station level in-depth analysis

Both power grid OT experts and IT officers will find StationGuard's unique visualization of power grid OT networks familiar. The network is visualized in a graphical form, with a complete list of all devices in the network and their position in the grid. Using GridOps, you can analyze alerts and events in the OT networks on a global scale at the grid level, as well as visualize the locations of IDS sensors in each OT network at the sensor level using a visualization of the sensor network.

For those users who would like to visualize the plant network in a way that is close to the single-line diagram and engineering documentation of the system, there is a visualization option available: the ZeroLine diagram. ZeroLine diagrams can either be automatically generated from engineering files of the plant, or they can be manually structured to closely resemble either the network structure according to the Purdue Model or the electrical layout of the plant.

GridOps provides a comprehensive approach to analysis and investigation to address emerging threats promptly. It is now possible to view all the alerts by navigating from a grid-level overview to a specific control center, power plant, or substation network view using the familiar StationGuard ZeroLine diagram visualization.

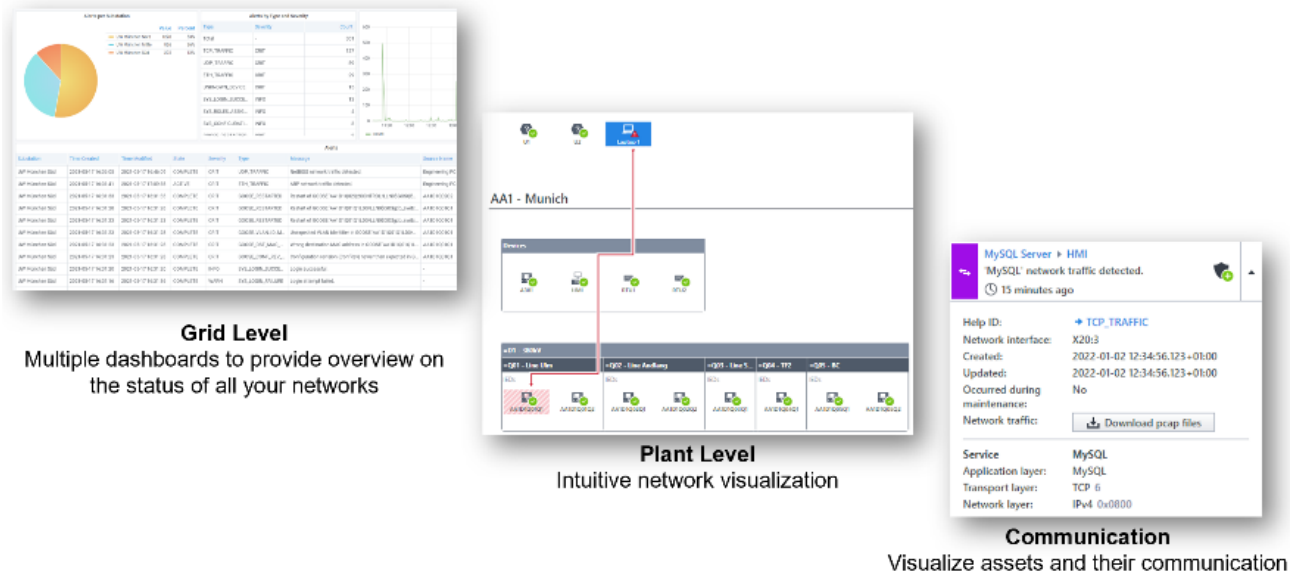


Figure 9: Views for grid level, plant level and communication

7. Active Directory integration and role-based access control

LDAP is a protocol that can be used to integrate GridOps into an Active Directory environment. StationGuard assigns specific roles to different users to regulate users' access to various functions that are available for viewing and configuring StationGuard instances. The different users have varying levels of access to various functions.

By doing this, we are limiting which sets of functions are available to which users, as well as limiting their use. Furthermore, StationGuard IDS sensors can also be accessed using the local StationGuard client user interface if for some reason the connection to the central GridOps instance is not available. By doing this, you are still able to access the sensors separately as a backup option, if you wish to.

OMICRON

For more information, additional literature, and detailed contact information of our worldwide offices, please visit our website.

www.omicronenergy.com