



How Veeam can help with NIS2 directive

Tomasz Turek

Senior Systems Engineer
Veeam

What does it mean

What is NIS2

Which obligations does the NIS2 directive impose?

Duty of care

You must carry out a risk assessment. Based on this risk assessment you should take measures to guarantee continuation of services as much as possible and protect the information used.

Duty to report

You have to report incidents to the supervising authority within 24 hours. It concerns incidents that (can) significantly disrupt the provision of the essential services. Does it concern a cyber incident? Then this must also be reported to the Cyber Security Incident Response Team.

Supervision

Organizations covered by the NIS2 directive will be under supervision. The supervisory body will look at compliance with the obligations of the directive, such as the duty of care and the duty to report. It is currently being worked out which sectors will fall under which supervisory body.

How can Veeam help?

Veeam Data Platform





Recovery Orchestration

Monitoring & Analytics



Backup & Recovery

Native APIs

Platform
Extensions

-  AWS
-  Azure
-  Google Cloud
-  Kubernetes



-  Microsoft 365
-  Salesforce

On-Premises • In the Cloud • XaaS

NIS2 goal: maintaining data integrity; preventing and minimizing the impact of cybersecurity incidents

Veeam immutable backups can help prevent ransomware attacks and unauthorized deletions and changes by making backup data impervious to modifications.

It works **across all supported workloads** in any environment – physical, virtual, cloud

Repository

Repository
Type in path to the folder where backup files should be stored, and set repository load control options.

Location

Path to folder:
/backup Browse...

Capacity: <Unknown> Populate
Free space: <Unknown>

Use fast cloning on XFS volumes (recommended)
Reduces storage consumption and improves synthetic backup performance.

Make recent backups immutable for: 7 days
Protects backups from modification or deletion by ransomware or hackers. GFS full backups are made immutable for the entire duration of their retention policy.

Load control

Running too many concurrent tasks against the repository may reduce overall performance, and cause I/O timeouts. Control storage device saturation with the following settings:

Limit maximum concurrent tasks to: 4

Limit read and write data rate to: 1 MB/s

Click Advanced to customize repository settings. Advanced...

< Previous Next > Finish Cancel

NIS2 goal: safe recovery from incidents

Veeam offers **secure restore** features that can verify the backup integrity and scan for malware before data is restored, thus helping to avoid reintroducing threats into the environment.

The screenshot shows the Veeam Backup & Replication console. On the left, a navigation pane highlights 'Malware Detection'. The main area displays the 'Settings' dialog for 'Veeam Incident API' with the 'Notifications' tab selected. Under 'Encryption detection', the 'Enable inline entropy analysis' checkbox is checked. Below this, a sensitivity slider is set to 'Normal'. A text box explains that extreme sensitivity can generate many false positives. In the bottom left, a sidebar shows 'Upgrade', 'Credentials & Passwords', 'Users & Roles', 'Malware Detection', and 'Network Traffic Rules'. To the right, an 'Event Details' window is open, showing a 'General' tab with the following information:

- Object: HK-1944-encyl
- Activity date: 10/2/2023 11:05 AM
- Type: Built-in detection engine
- Initiated by: LAB\SYSTEM
- Status: Suspicious
- Details: Possible malware activity detected

The screenshot shows the 'New SureBackup Job' wizard in Veeam Backup & Replication. The 'Settings' step is active, with a red box highlighting the 'Content analysis' section. The 'Content analysis' section includes the following options:

- Scan backup content with an antivirus software
- Scan backup content with the following YARA rule:
 - Rule name: eicary.yara
 - YARA rules location: C:\Program Files\Veeam\Backup and Replication\Backup\YaraRules\
- Continue scanning remaining files after the first occurrence

Below this, the 'Backup integrity' section has the option Perform backup integrity check (read and verify each block against a checksum) unchecked. At the bottom, the 'Backup verification' section has the radio button for 'Backup verification and content scan only' selected. The wizard includes navigation buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

NIS2 goal: safe recovery from incidents

Veeam allows to scan backups **on demand** giving flexibility of scanning any restore point at any given time. This is applicable to backups created **with older versions of our products.**

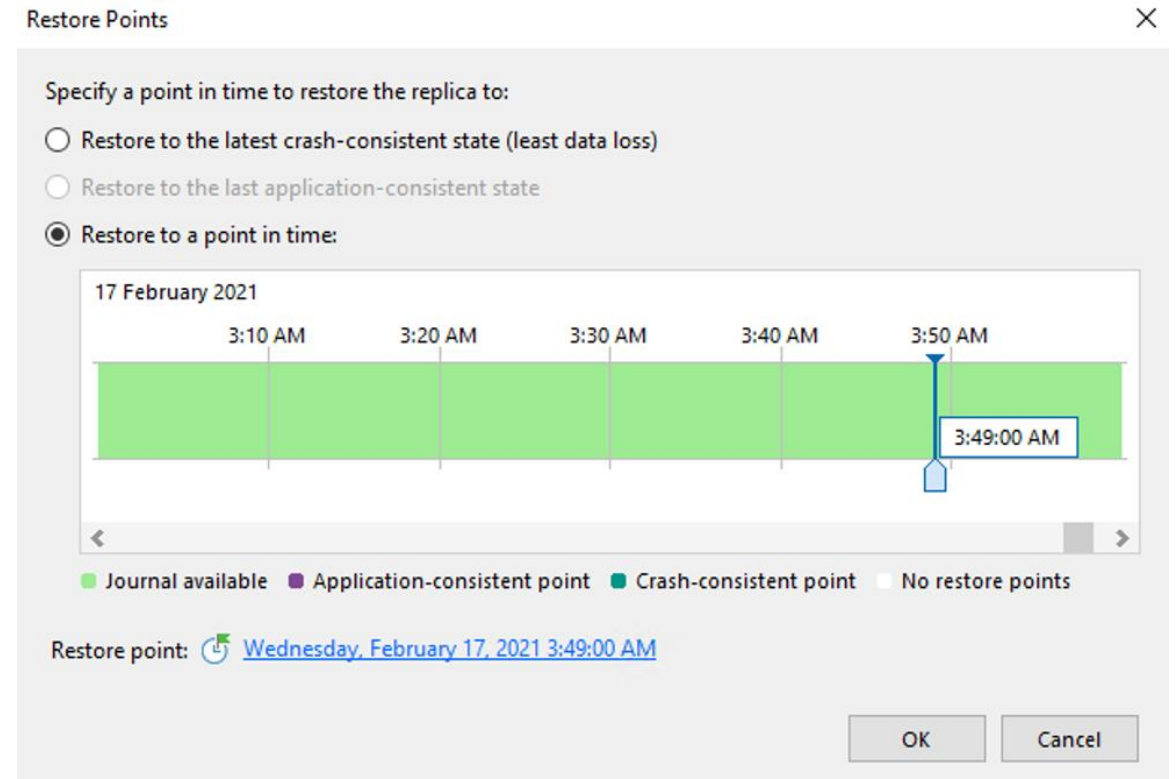
The image shows a screenshot of the Veeam Backup & Replication console. On the left, the 'Home' view is displayed with a tree structure containing 'Jobs', 'Backups', 'Disk', 'Disk (Copy)', 'Object Storage', 'Object Storage (Copy)', 'Tape', 'Replicas', and 'Last 24 Hours'. The 'Backups' folder is expanded, and a context menu is open over a backup job named 'HK-DC01'. The 'Scan backup...' option at the bottom of the menu is highlighted with a red rectangle. To the right, the 'Scan Backup' dialog box is open, showing the following configuration:

- Scan mode:**
 - Find the last clean restore point: Restore points will be scanned sequentially starting from the most recent one until the first malware-free one is found. Use this option when a cyber-attack is known to have started recently.
 - Find the last clean restore point in range: Restore points will be scanned in an optimal order to identify the last clean backup in range with least number of scans possible. Use this option if you are not sure when the attack started, or when dealing with a known sleeping malware.
 - Scan all restore points in range for content analysis: All restore points in range will be scanned sequentially. Use this option for backup content analysis with an applicable YARA rule, for example to look for personally identifiable information (PII), personal health information (PHI) or payment card industry (PCI) data.
- Scan engine:**
 - Scan restore points with an antivirus
 - Scan restore points with the following YARA rule: eicar.yar
- YARA rules location:** C:\Program Files\Veeam\Backup and Replication\Backup\YaraRules\
- Scan range:**
 - From:** Most recent restore point
 - To:** Oldest available restore point
 - Start date:
 - End date:
 - Continue scanning all remaining files after the first occurrence

Buttons: Hide scan range, OK, Cancel

NIS2 goal: resilience and quick recovery

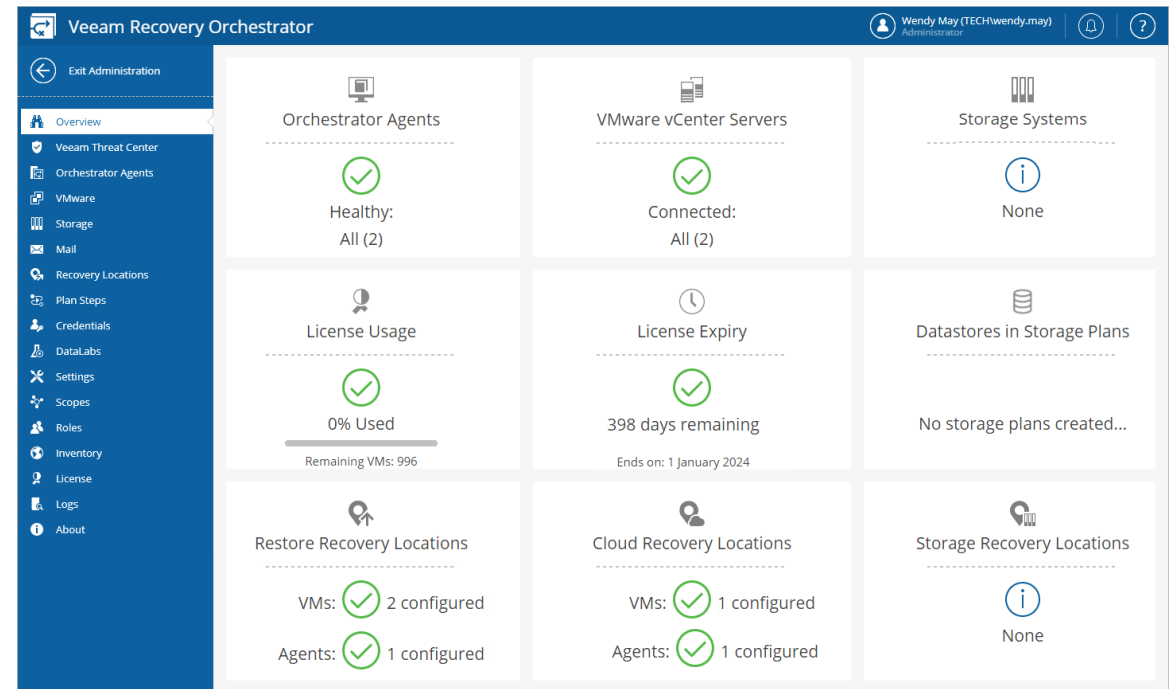
Veeam's **Continuous Data Protection** can provide near-zero recovery point objectives (RPOs) for critical workloads, ensuring that businesses can recover their data quickly in the event of cyber incidents or data corruption.



NIS2 goal: resilience and quick recovery

Through **Veeam Recovery Orchestrator**, businesses can automate and simplify disaster recovery planning, ensuring that they are prepared for a wide variety of scenarios

- With VRO organisation can **create** DR plans and **test** them to ensure they will work when they need it most
- Documentation of DR plans is **updated automatically**
- VRO can **automate** recovery, orchestrating **all recovery workflows** and help to speed up recovery regardless where DR site is (on-prem or cloud)



Orchestration - Daily Readiness Report

Veeam Recovery Orchestrator

Scopes (All)

Dashboard

Planning

Inventory

Recovery Plans

Testing

DataLabs

Lab Calendar

Documentation

Reporting

Search by Plan

Launch Manage Verify

Mode	Plan	Type	Status
In-Use	Sharepoint Replica Plan	Replication	Ready
In-Use	Replica Plan	Replication	Ready
In-Use	Test Restore Plan	Restore	Ready
In-Use	Exchange Restore Plan	Restore	Ready
Disa...	NetApp	Storage	Warning
In-Use	Test HPE Plan	Storage	Ready
In-Use	CDP Plan	CDP Replica	Ready

Run Data Halt Data Power On Run Readiness Halt Readiness

Summary

Result	Details
[!] Warning	1 Warnings

Execution Details

Item	Details
Run/Scheduled By	Olivia Dias (TECH\olivia.dias)
Duration (HH:mm:ss)	00:00:03

Plan

Result	Group	Details
✓ Ready	Pre-Plan Steps	No errors
[!] Warning	Replication Job for Testing:172.24.28.186	1 VM(s) with warnings
✓ Ready	Post-Plan Steps	No errors

RPO

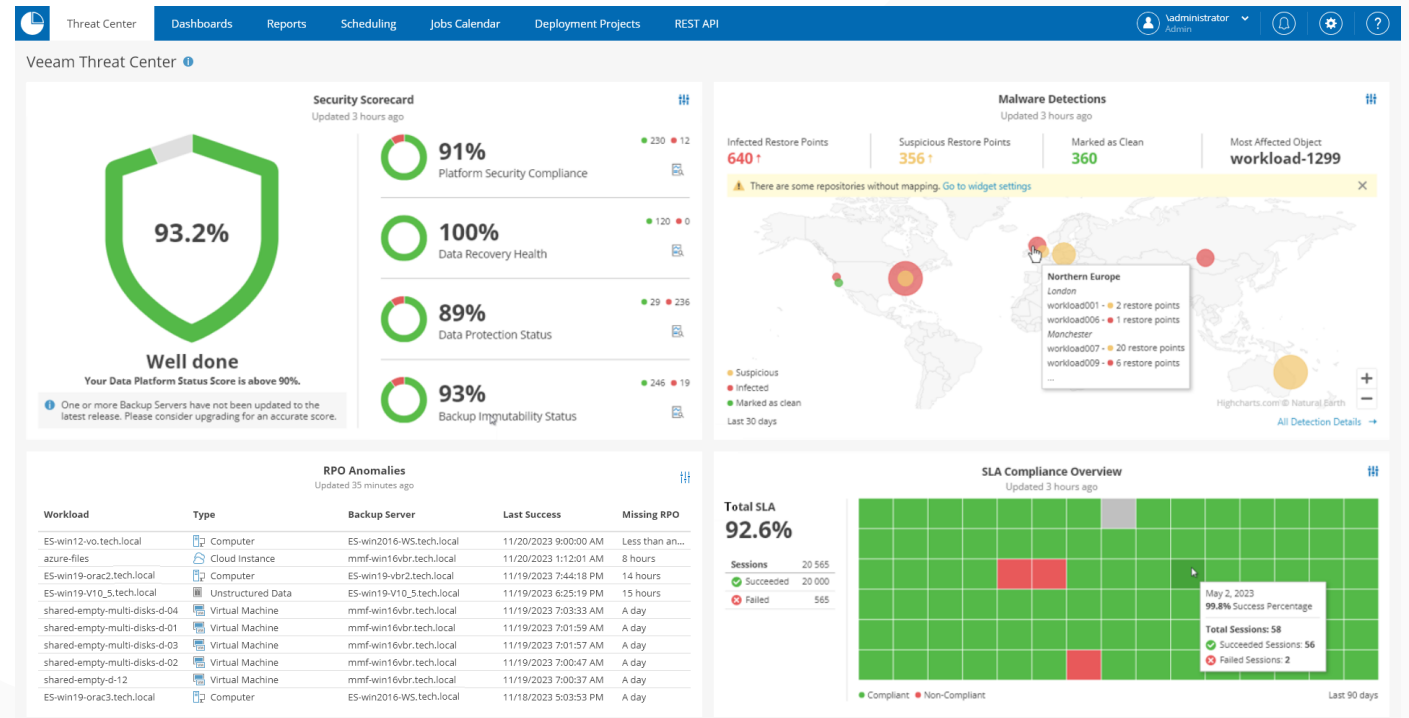
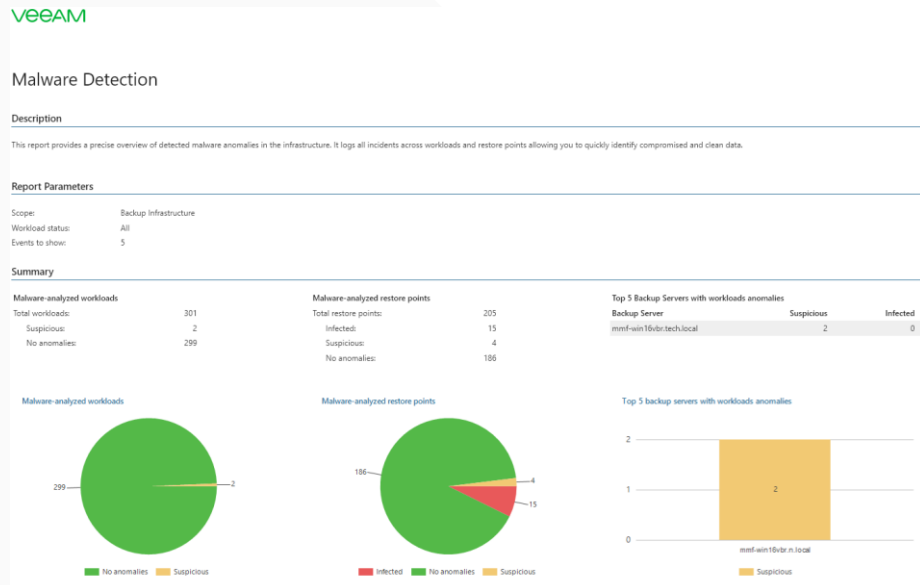
Result	Check	Details
[i] Info	RPO	Target RPO is 24:00:00 (HH:mm:ss)
✗ Not ready	Target RPO Met	No
✗ Not ready	Number of RPO failures	1
✗ Not ready	Worst RPO failure	Restore point age 317:39:03 (HH:mm:ss)

Licensing

Result	Check	Details
[i] Info	Summary	0 of 125 license instances used
✓ Ready	Usage	0 licenses are used in this plan (0 managed VMs, 1 new)
✓ Ready	Expiry	The license will expire in 397 days
✓ Ready	Exceeded	The license limit is not exceeded on the Orchestrator server

NIS2 goal: compliance with risk management and reporting obligations

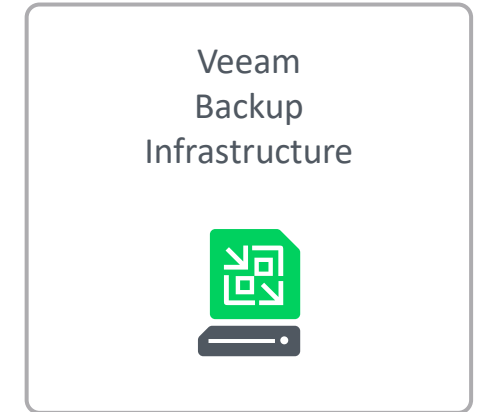
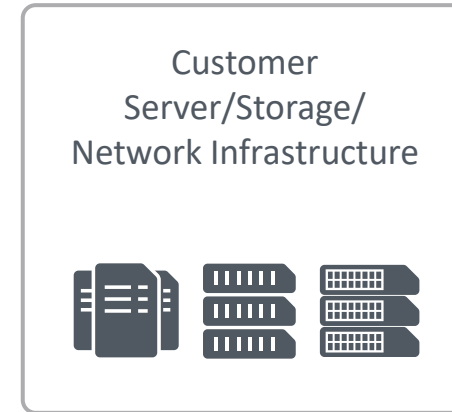
Utilizing Veeam ONE, the Veeam Data Platform Premium offers solutions for real-time **monitoring, reporting, and capacity planning** for the backup infrastructure.



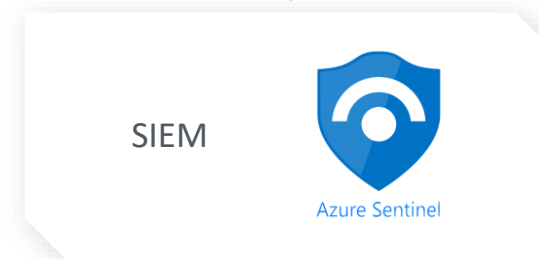
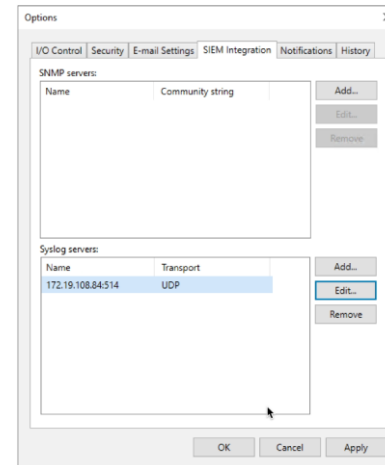
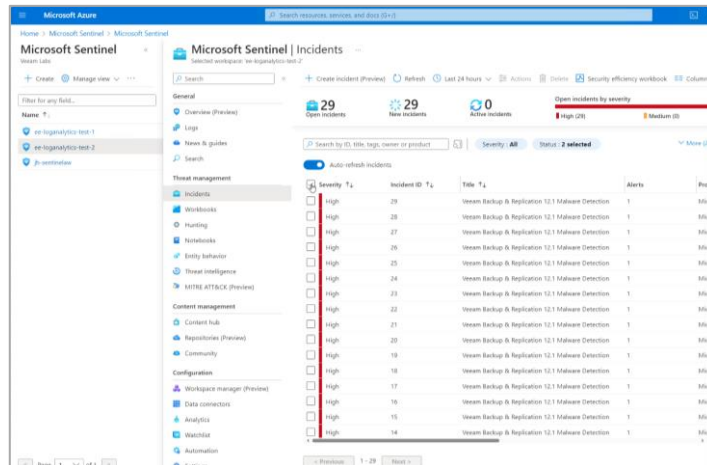
SIEM Integration – Example: Microsoft Azure Sentinel

Infrastructure and backup environments in a single pane of glass for your security

- Use Veeam Backup & Replication with Microsoft Azure Sentinel to forward all Veeam events, ransomware, or virus detections.
- Events forwarded through SYSLOG
- Veeam provides customers with the flexibility to interpret Veeam events in a customer own created parser to build own alarms, dashboards, and reports.



Events forwarded through
SYSLOG



SIEM Integration – Veeam app for Splunk

The screenshot displays the Splunk Veeam App interface for monitoring security events. The top navigation bar includes 'splunk-enterprise', 'Apps', and user roles like 'Administrator'. The main section is titled 'Veeam Security Events' and features filters for Data Sources (All), Locations (All x), and Global Time Range (Last 30 days). Below the filters, a summary dashboard shows:

- Security Status (Last 24 Hours): 1 Critical event
- All Security Events: 393 total
- Marked as Infected: 13
- Marked as Suspicious: 1
- Four-Eyes Authorization Events: 11

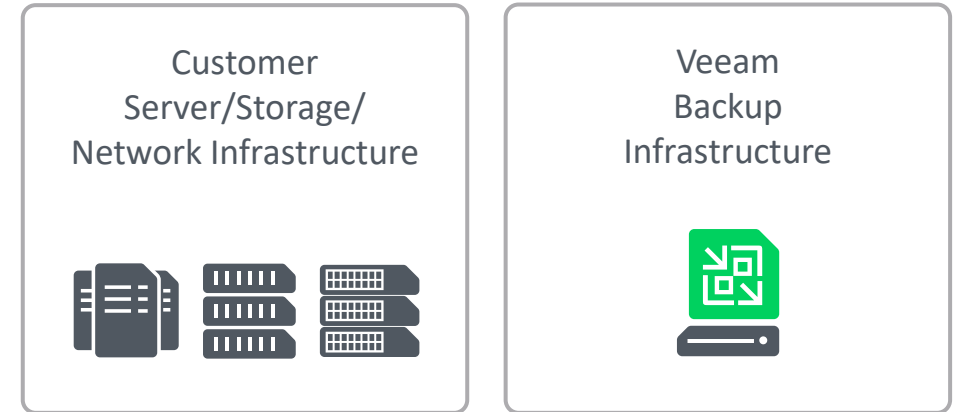
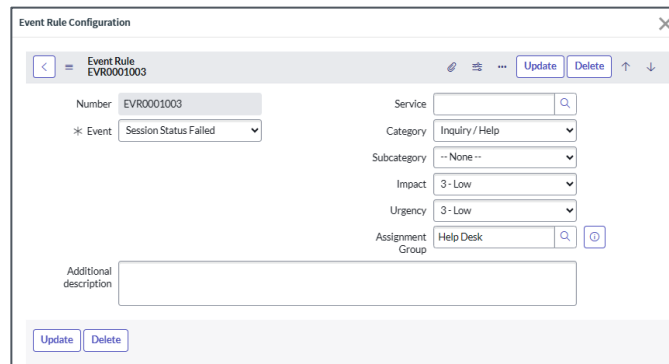
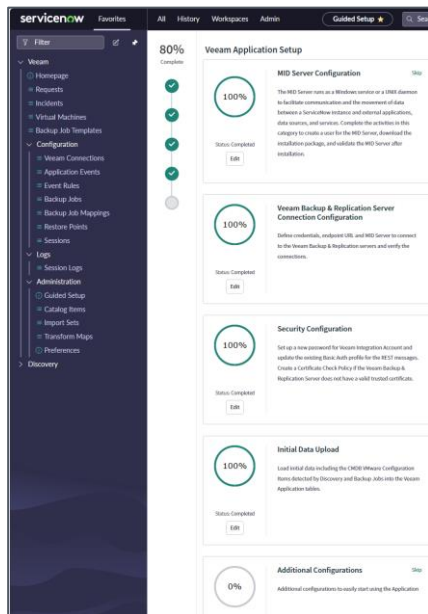
 A 'Daily Security Events' chart shows event counts from March 18 to April 8, 2024, categorized by severity: Critical (green), High (orange), Medium (yellow), and Information (red). A world map highlights event locations, with Brazil marked in purple (Warning) and a small area in Europe marked in pink (Error). The bottom section, 'Latest Security Events', contains a table of recent incidents.

Date	Data Source	User	Message	Severity
15.04.2024 07:53	VBRI2SHED		Backup server has lost connection to backup repository Backup Copy Repository (Windows).	Critical
15.04.2024 07:53	VBRI2SHED		Backup server has lost connection to backup repository Backup Repository (Windows).	Critical
13.04.2024 00:00	TIEM		Malware detection session has finished with Success.	Information
12.04.2024 23:51	VBRI2SHED		Backup server has lost connection to backup repository Backup Copy Repository (Windows).	Critical
12.04.2024 23:51	VBRI2SHED		Backup server has lost connection to backup repository Backup Copy Repository (Windows).	Critical
12.04.2024 19:52	VBRI2SHED		Backup server has lost connection to backup repository Backup Repository (Windows).	Critical
12.04.2024 19:52	VBRI2SHED		Backup server has lost connection to backup repository Backup Copy Repository (Windows).	Critical
12.04.2024 17:00	GER2019VBR	NT-AUTORITÄT\SYSTEM	Four-eyes authorization is no longer available (license change). Event has been initiated by NT-AUTORITÄT\SYSTEM.	Critical
12.04.2024 15:52	VBRI2SHED		Backup server has lost connection to backup repository Backup Copy Repository (Windows).	Critical
12.04.2024 15:52	VBRI2SHED		Backup server has lost connection to backup repository Backup Repository (Windows).	Critical

ITSM Integration – ServiceNow

Infrastructure and backup environments in a single pane of glass for your security

- Veeam offers a ServiceNow plug-in to automate and manage Veeam from ServiceNow including tickets for Veeam alarms and status changes.
- SIEM solutions with integrations in ServiceNow can be leveraged to integrate through ServiceNow with Veeam.

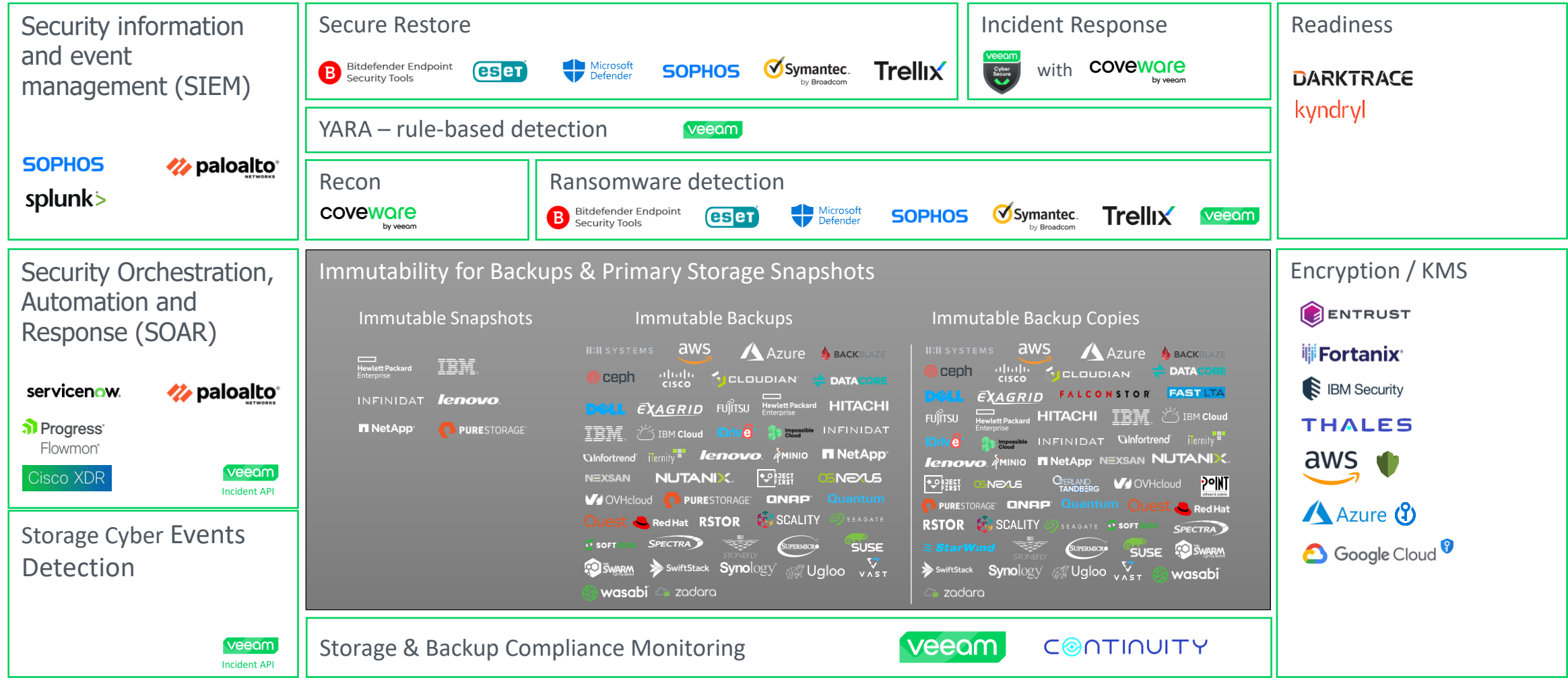


2-way through APIs

servicenow

Other SIEM Solutions

Veeam Cyber Resiliency - Ecosystem



NIS2 goal: Risk Analysis and information system security

VBR Improved Security & Compliance Analyzer

Backup Infrastructure & Product Security

- Password requirements
- Configuration backup encryption
- Outdated TLS versions
- Reverse Incremental deprecated
- And many more...

Runs by schedule or manually

The screenshot displays the 'Security & Compliance Analyzer' window. It features a table of best practices categorized into 'Backup infrastructure security' and 'Product configuration'. Each entry includes a description, a status indicator (green checkmark for 'Passed', red X for 'Not implemented', or yellow warning triangle for 'Unable to detect'), and a status label. On the right side, there are buttons for 'Analyze', 'Schedule...', 'Suppress', 'Reset', and 'Reset All'. At the bottom right, there is a 'Last run...' button and a 'Close' button.

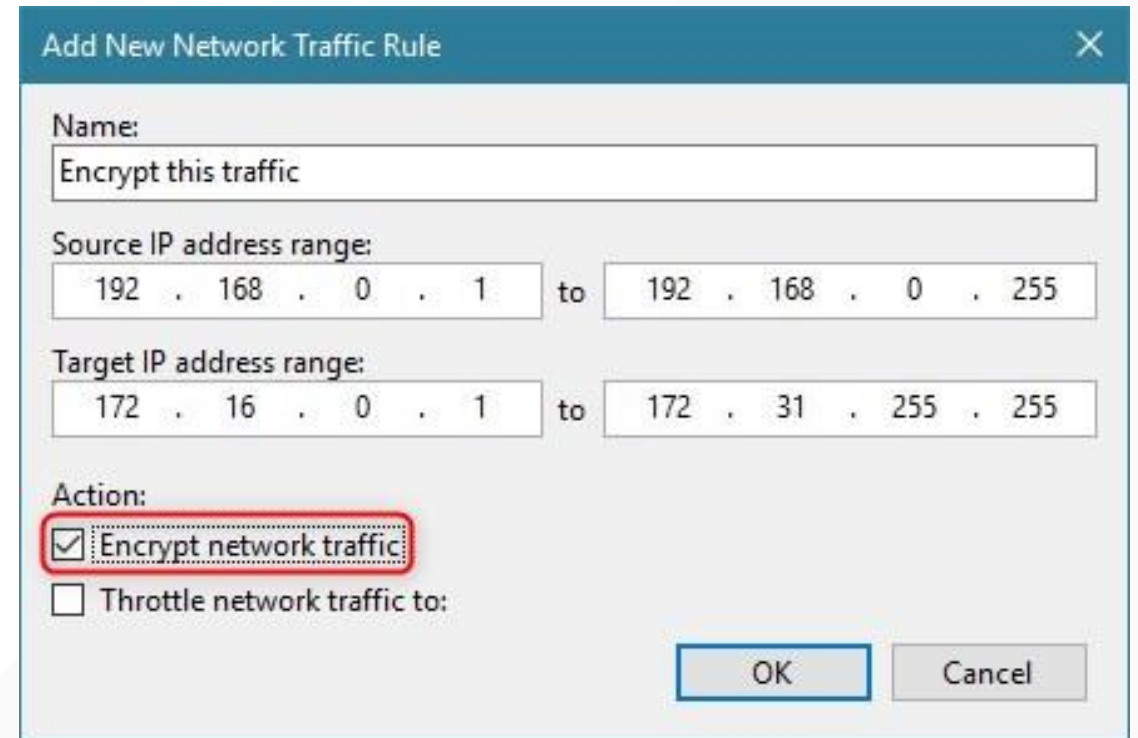
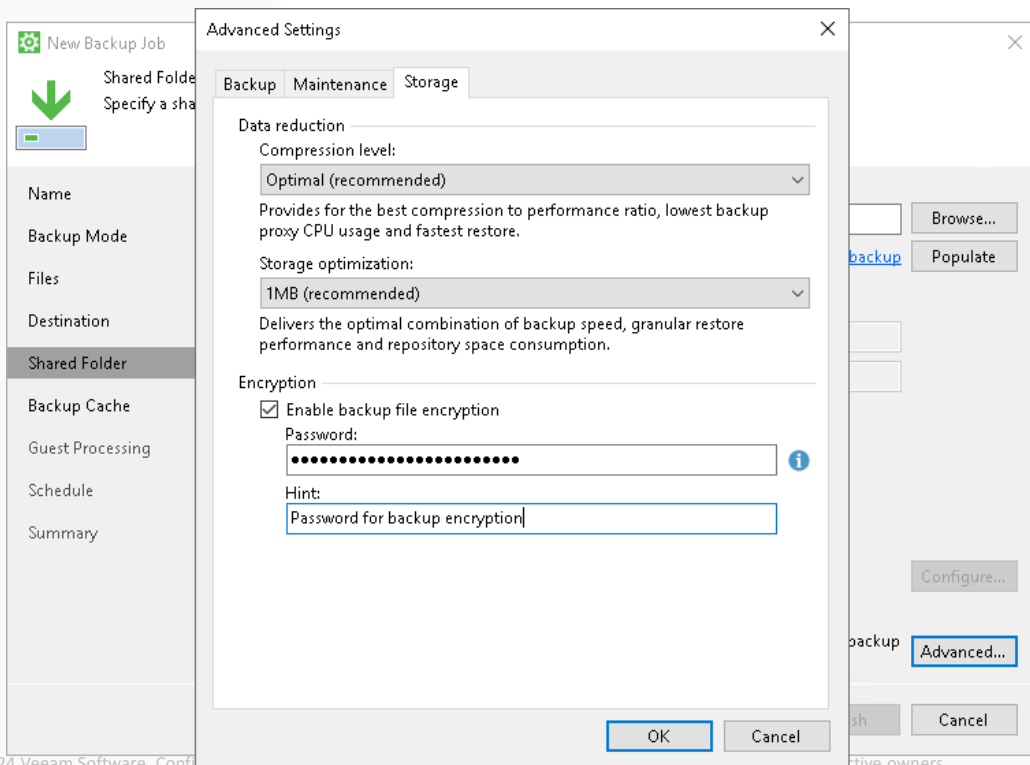
Best Practice	Status
Backup infrastructure security	
Remote Desktop Service (TermService) should be disabled	Not implemented
Remote Registry service (RemoteRegistry) should be disabled	Not implemented
Windows Remote Management (WinRM) service should be disabled	Not implemented
Windows Firewall should be enabled	Passed
WDigest credentials caching should be disabled	Passed
Web Proxy Auto-Discovery service (WinHttpAutoProxySvc) should be disabled	Not implemented
Deprecated versions of SSL and TLS should be disabled	Not implemented
Windows Script Host should be disabled	Not implemented
SMBv1 protocol should be disabled	Passed
Link-Local Multicast Name Resolution (LLMNR) should be disabled	Not implemented
SMBv3 signing and encryption should be enabled	Not implemented
Product configuration	
MFA for the backup console should be enabled	Not implemented
Immutable or offline (air gapped) media should be used	Not implemented
Password loss protection should be enabled	Passed
Backup server should not be a part of the production domain	Unable to detect
Email notifications should be enabled	Not implemented
All backups should have at least one copy (the 3-2-1 backup rule)	Not implemented
Deprecated and should be avoided	Passed
trusted automatically	Not implemented
stored on the backup server	Not implemented
be enabled for the Network transport mode	Passed
hosted in virtual machines	Passed
enabled in the backup network	Passed
based authentication disabled	Passed
der the LocalSystem account	Passed
led and use encryption	Not implemented
should be rotated at least annually	Passed
SSH Server disabled	Passed
de doesn't provide true immutability	Passed
uld use encryption	Passed

Schedule Settings

- Scan the backup infrastructure daily at: 10:00 PM
- Send scan results to the following recipients:
 - admin@lab.intern
- Use global notification settings
- Use custom notification settings specified below:
 - Subject: Daily Security & Compliance Report
 - Notify on success
 - Notify on warning
 - Notify on error

NIS2 goal: data confidentiality and integrity

Veeam provides options to **encrypt backup data at rest and in transit**, helping to protect sensitive data from unauthorized access or interception.



Veeam Go-To NIS2 site

veeam

ARE YOU READY? OVERVIEW WHO'S AFFECTED? SOLUTIONS **WHITEPAPER**

NIS2 is Coming: Everything You Need to Know and More!


Understand what the cybersecurity directive means to your business, and how Veeam can help with NIS2 compliance... time is ticking

OVERVIEW WHO IS AFFECTED?

Are You Ready for NIS2?

Veeam Go-To NIS2 resources

NIS2 Compliance Checklist



Discovered that you need to comply with the NIS2 directive? Knowing what steps to take to be compliant is not an overnight fix. We've created this handy checklist, so you can work out a plan of action. The penalties for non-compliance can be severe, make sure you know what is at stake that you, as an individual and your organization could face. Here, we focus on articles 21 and 23 which outline the requirements needed to comply. Visit our website to understand more about NIS2 and how your business could be affected.

NIS2 Article	Ask yourself... and tick when you can confidently answer	How the Veeam Data Platform can help
21-2(a): policies on risk analysis and information system security;	<ul style="list-style-type: none"><input type="checkbox"/> Do I know what risks I have in my current environment?<input type="checkbox"/> Do I have insights in internal and external factors?<input type="checkbox"/> Can I recover within agreed Recovery Time Objective when disaster strikes?	<p>Foundation: Built-in security and compliance check</p> <p>Advanced: Anomaly and trend reports</p> <p>Premium: Daily readiness reports</p>
21-2(c): business continuity, such as backup management and disaster recovery, and crisis management;	<ul style="list-style-type: none"><input type="checkbox"/> Do I have backups of all important systems?<input type="checkbox"/> I moved workloads to the cloud, are they safe?<input type="checkbox"/> Can I recover quickly from outages without spare resources?<input type="checkbox"/> Do we have a cybersecurity hygiene policy?	<p>Foundation: Tags ensure that new workloads are backed-up</p> <p>Advanced: Full overview of your workloads, anytime, anywhere</p> <p>Premium: Recover to Azure as your spare DC</p>
21-2(i): human resources security, access control policies and asset management;	<ul style="list-style-type: none"><input type="checkbox"/> Can I keep out non-authorized users?<input type="checkbox"/> Am I still relying on insecure passwords?<input type="checkbox"/> Can a rogue administrator impact my recovery options?<input type="checkbox"/> Have I educated all staff about safely handling data?	<p>Multi-Factor Authentication and role-based access control</p> <p>Support for external Key Management systems</p> <p>Immutable on-prem and cloud repositories</p>
23-4(a) and (b): Report to CSIRT (...) without undue delay and in any event within 24(a)/72(b) hours of becoming aware of the significant incident,	<ul style="list-style-type: none"><input type="checkbox"/> How do I know which systems are impacted?<input type="checkbox"/> How do we handle vulnerabilities and disclosure?<input type="checkbox"/> How do I report to my Computer Security Incident Response Team (CSIRT)?<input type="checkbox"/> Can I meet the report deadlines when my systems are down?	<p>Built-in Malware and YARA rule scanning to identify impacted systems</p> <p>Preconfigured reports ready to submit to CSIRT</p> <p>Best practices to ensure Veeam report availability</p>

Fill the gaps in your cybersecurity with Veeam

Not in the EU and think you're exempt? Sad news, you're not... NIS2 impacts supply chains and is far reaching. Talk to us today and see how we can help start your journey to compliance now.

LET'S TALK



Follow us!



Join the community hub:

