

Maitrisez vos données avec Veeam.

Protection intégrale de toutes vos plateformes – donnez la main aux experts de la cyber resilience.

Bechtle IT Forum | 11.06.2024 | SwissTech Convention Center

Alina Maciuca, Senior Inside Systems Engineer, Veeam

Christian Bocquet, Solution Architect Datacenter, Bechtle Suisse

The Veeam logo is displayed in white lowercase letters on a green rectangular background with a slight gradient and rounded corners.



Agenda

1 Cyber Secure

2 NIST by Veeam & Bechtle

Section 1

Cyber Secure

Best-in-class Incident Recovery

How Can Veeam Help?

With a comprehensive approach to Ransomware protection

When Ransomware attacks, you need best-in-class:

- Technology
- People, and
- Processes

To protect your organization from a worst-case scenario



Full Support for Every Stage

Pre-incident

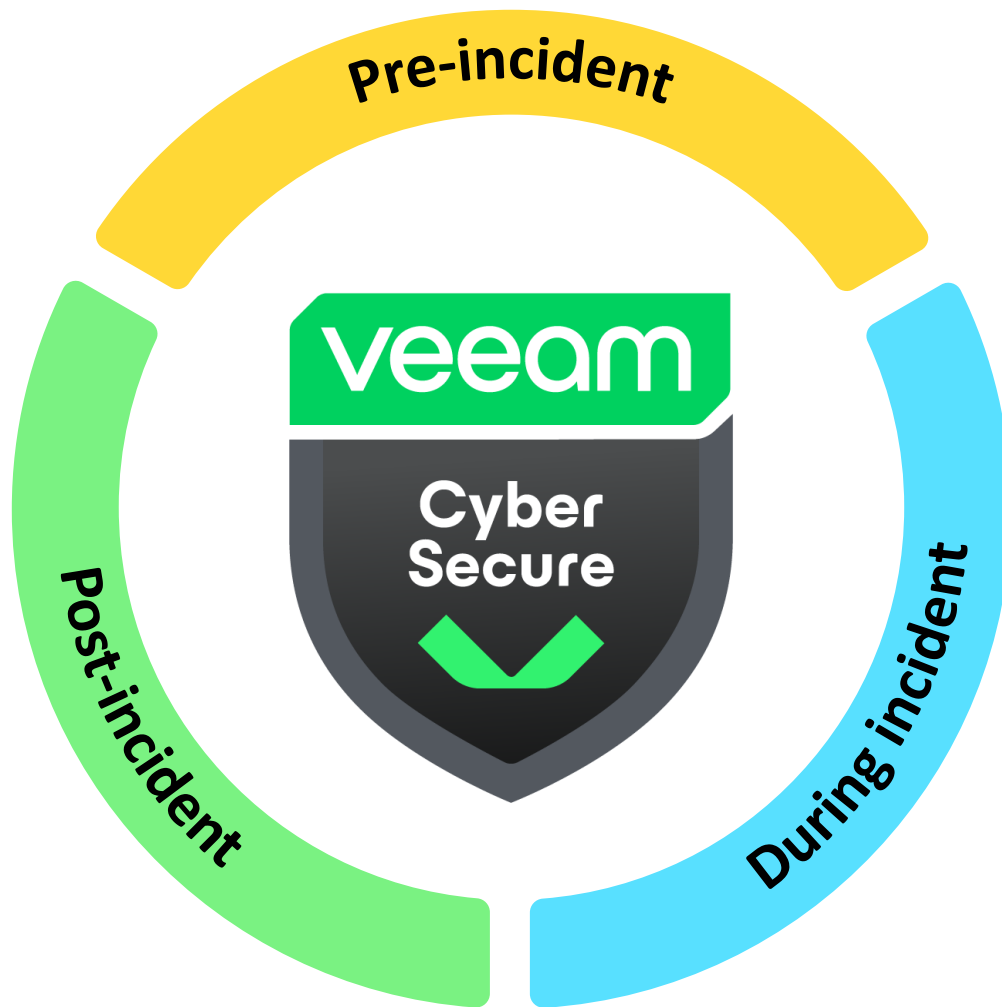
- Quarterly security assessments
- Advanced onboarding support
- Design and implementation services

During incident

- 24/7/365 30-minute first response SLA
- Dedicated Support Account Manager
- Veeam Ransomware Response Team
- Priority Issue Routing

Post-incident

- For verified attacks, get up to \$5 million USD in data recovery expense reimbursement



Pre-Incident

Advanced Onboarding Support

Expert guidance to ensure your Veeam environment is on the path to success!

- A Veeam Subject Matter Expert (SME) will be assigned to each organization
- Multi-phased approach to efficiently integrate Veeam security best practices and operational processes to rapidly reduce risk
- Quarterly assessments provided after onboarding to continually assess risk and secure your Veeam data protection solution

7 Phase On-Boarding Methodology



Pre-Incident

Veeam's Security Best Practices

Rely on a trusted partner to ensure your IT security follows best-practice

Veeam experts conduct quarterly health checks that leverage an extensive 100+ point security check list:

- **Components** within your data protection environment
- Security **permissions**, passwords, access
- Back-up **storage** practices
- Back-up **encryption** and key storage
- **Orchestrated recovery**

Leverage our extensive Veeam Accredited Service Partner (VASP) network for design and implementation services



During Incident

Ransomware SWAT Team

We'll be there to help

In the event of a ransomware attack, you get:

- Ransomware Recovery Support Account Manager
24/7/365 availability
- **30 min** response SLA
- Avg resolution time for team: **15 hours**

BECHTLE



Post-Incident

Veeam Ransomware Recovery Warranty

By following our best practices, Veeam is so confident customers can recover quickly from a ransomware attack with clean reliable backups, **They'll cover up to \$5 million (USD) in data recovery costs if the eligible solution does not permit to materially restore the Customer Data to the last clean and usable backup.**

<https://www.veeam.com/products/ransomware-recovery-warranty-terms-conditions.html>



Veeam Security Features Summary

Backup Environment Security

- **Security & Compliance Analyzer**
- **SIEM integration**
- **Threat Center & Awareness**
- **Four eyes approval**

Multi-Factor Authentication

- Veeam Backup Console
- Enterprise Manager SAML
- AWS, Azure, GCP appliances

Immutable Backups

- Veeam Hardened Repository
- Object Storage
- Multiple vendor integrations

Verified, Reliable Backups

- Storage-level corruption guard
- SureBackup automated recovery verification

Airgap

- Logical airgap Veeam Hardened Repository
- True airgap native tape support

Secure client authentication

- Microsoft gMSA support
- 100% Kerberos support
- Key-based Linux authentication

Multiple resiliency domains

- Mix immutable storage platforms
- 3-2-1-1-0 Rule

Data Freedom

- Encryption key loss protection
- Self-contained backup files
- Cloud and Hypervisor mobility

End-to-end encryption

- TLS management traffic
- TLS or AES256 data traffic
- FIPS 140-2 cryptography
- **KMIP**

Role-based security

- Local privileged accounts
- Web UI for domain accounts via SAML 2.0

Integrated Threat Detection

- **YARA backup scanner**
- **Signature-based scanner**
- **Scheduled or ad hoc**

Advanced Anomaly Detection

- **AI\ML entropy and content scanner**
- **Indexing scanner**
- **Incident API**

Section 2

NIST by Veeam

And Bechtle 😊

What is NIST ?

You are concerned !

NIS2, Network and Information Security version 2

Provides guidance to industry, government agencies, and other organizations to manage cybersecurity risks

Who is affected? Essential or Critical Infrastructure Industries, Important Entities, partners and providers

<https://nis2directive.eu>



Identify

Security and Compliance Analyzer

Infrastructure and Backup Reporting / Labeling

YARA

Backup Infrastructure Inventory

Updated a minute ago

Object	Status
Enterprise Manager Servers (1)	Healthy
Backup Servers (1)	1
Backup Proxies (5)	Healthy
Backup Repositories (18)	1 7
WAN Accelerators (1)	Healthy
Backup Jobs (20)	8
Replication Jobs (1)	Healthy
Backup Copy Jobs (5)	Healthy
File Backup Jobs (1)	1
CDP Policies (1)	1

Protected VMs Overview

Updated a minute ago

Item	Value
Protected VMs	14
Backed Up VMs	14
Replicated VMs	0
Unprotected VMs	4
Restore Points	199
Full Backups Size	9.45 TB
Increments Size	59.02 GB
Source VMs Size	725.00 GB
Successful VMs Backup Ratio	100%

Restore
Failover Plan
Import Backup
Export Backup
Security & Compliance

Security & Compliance Analyzer

The following best practices are guidelines from data protection and cyber-security experts. Not following them exposes your backup infrastructure to significant risks and reduces chances of successful recovery following a cyber attack, a natural disaster or a hardware malfunction.

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	Not implemented
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	Unable to detect
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

Analyze
Schedule...
Suppress
Reset
Reset All
Last run...
Close

Protect

Backups

Identity management: RBAC & Data Cloud Roles

SureBackup

Security Analyzer & Threat Center

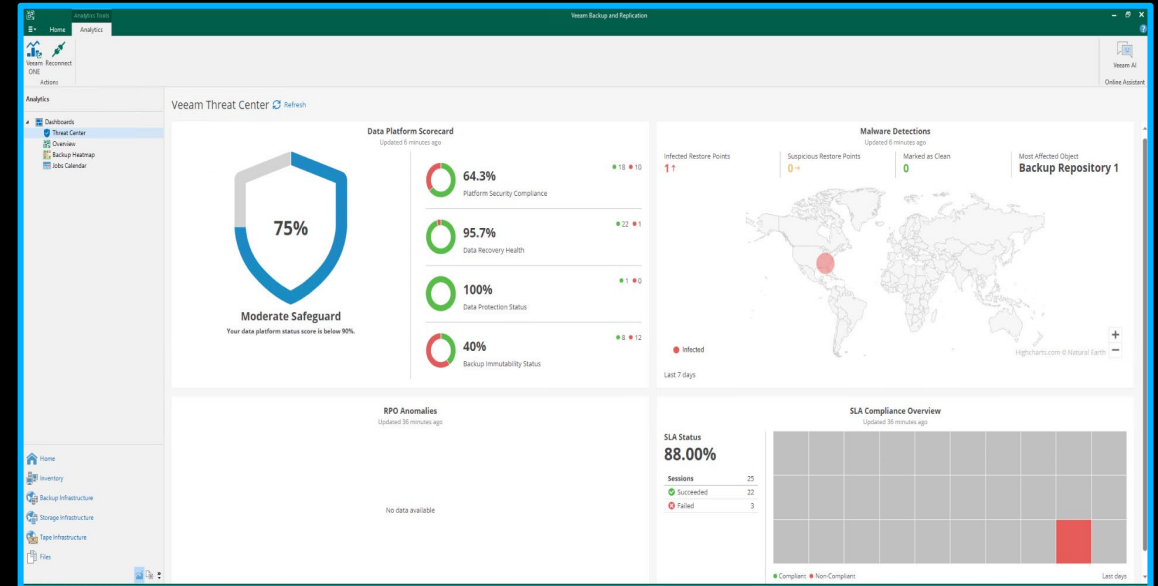
KMS / Encryption / FIPS

Immutabilities

Four Eyes approval

Veeam ONE - Monitoring and alert: Configuration tracking, SLA

Consulting



Immutable or offline (air gapped) media should be used	Passed
Password loss protection should be enabled	Not implemented
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)	Passed
Reverse incremental backup mode is deprecated and should be avoided	Passed
Unknown Linux servers should not be trusted automatically	Not implemented
The configuration backup must not be stored on the backup server	Passed
Host to proxy traffic encryption should be enabled for the Network transport mode	Passed
Hardened repositories should not be hosted in virtual machines	Passed
Network traffic encryption should be enabled in the backup network	Passed
Linux servers should have password-based authentication disabled	Passed
Backup services should be running under the LocalSystem account	Passed
Configuration backup should be enabled and use encryption	Passed
Credentials and encryption passwords should be rotated at least annually	Passed
Hardened repositories should have the SSH server disabled	Passed
S3 Object Lock in the Governance mode does not provide true immutability	Passed

Detect

Inline Malware Detection

Suspicious file system activity detection

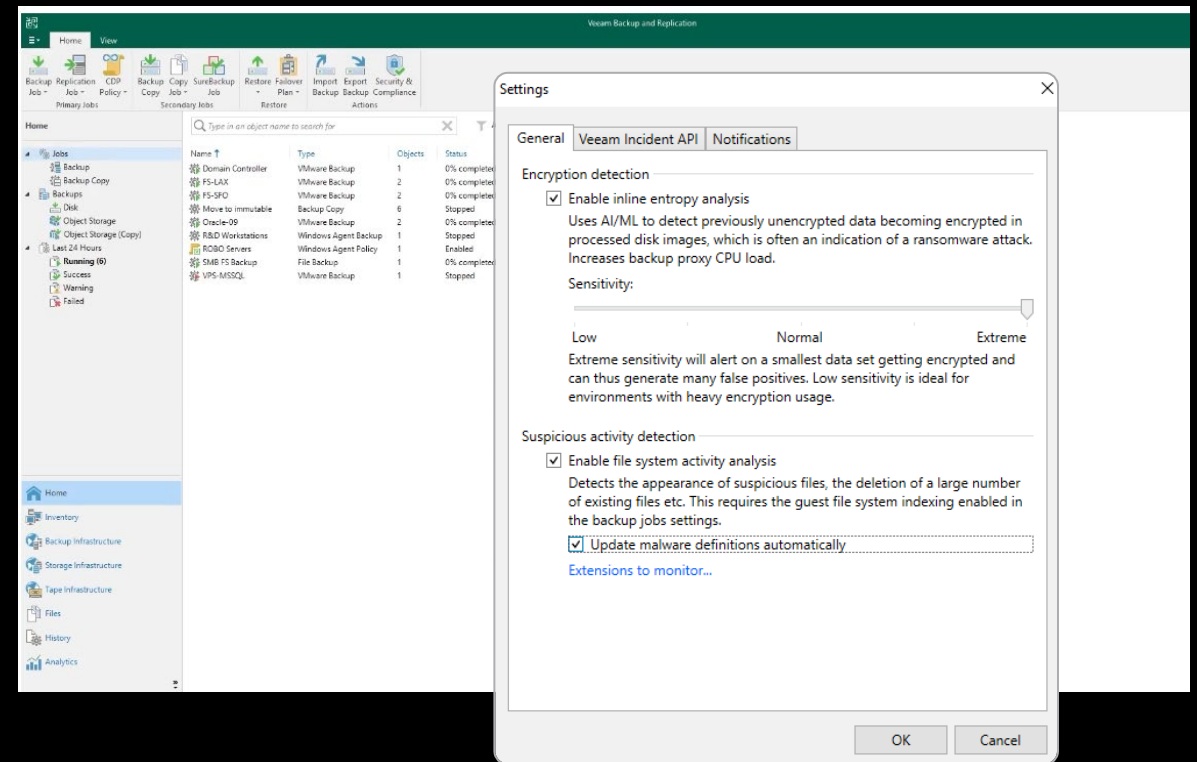
Scan Backup

Early threat detection / Incident API

Real Time Monitoring

Dedicated Ransomware Activity Alerts

Integration with Microsoft inbuilt virus scanner



Respond

Automated Alarm Remediation

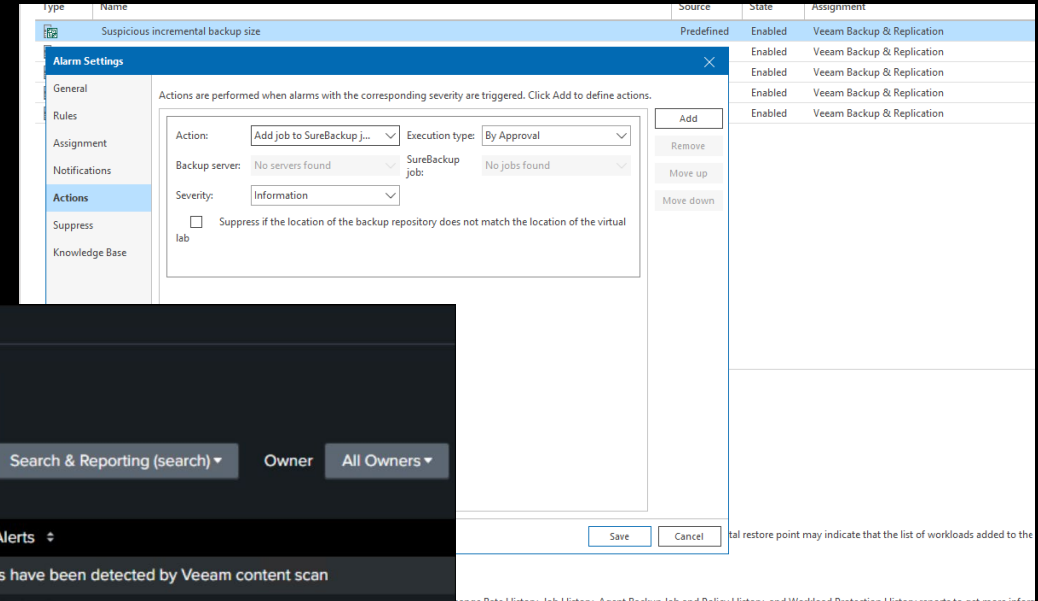
Event Forwarding via SIEM

Dynamic Documentation

E-Discovery – Veeam Data Cloud

CyberSecure

Bechtle



The screenshot shows the 'Alarm Settings' dialog for the alarm 'Suspicious incremental backup size'. The 'Actions' tab is active, showing a configuration for an action: 'Add job to SureBackup j...' with an execution type of 'By Approval'. The 'Backup server' is set to 'No servers found' and 'SureBackup job' with 'No jobs found'. The severity is set to 'Information'. There is a checkbox for 'Suppress if the location of the backup repository does not match the location of the virtual lab' which is currently unchecked. The dialog also shows 'Add', 'Remove', 'Move up', and 'Move down' buttons.

splunk > enterprise Apps

Triggered Alerts

Filter [Search] Apps Search & Reporting (search) Owner All Owners

<input type="checkbox"/>	Time	Fired Alerts
<input type="checkbox"/>	2023-11-03 11:18:01 EDT	Threats have been detected by Veeam content scan
<input type="checkbox"/>	2023-11-03 11:17:53 EDT	Threats have been detected by Veeam content scan
<input type="checkbox"/>	2023-11-03 10:57:32 EDT	Console has been launched
<input type="checkbox"/>	2023-11-03 10:56:54 EDT	User has initiated an attempt to delete multiple backups
<input type="checkbox"/>	2023-11-01 15:49:39 EDT	MFA Login Failed to Backup Console
<input type="checkbox"/>	2023-10-31 19:35:55 EDT	Backups were deleted by user
<input type="checkbox"/>	2023-10-31 14:05:03 EDT	Threats have been detected by Veeam content scan
<input type="checkbox"/>	2023-10-31 13:50:25 EDT	Console has been launched
<input type="checkbox"/>	2023-10-31 13:49:38 EDT	User has initiated an attempt to delete multiple backups

Recover

Secure restore – MDR, Yara, Third party (automate), Quarantine Net

Last known clean point

Stage restore / Data Labs with a SIRT (deep inspection)

Recovery Orchestration – VRO

Whatever Instant Recovery – DB, NAS, VMs, disks

Restore anywhere – Clouds, Nutanix, VMware, Hyper-V, Physical, KVM,...

E-Discovery – Veeam VBO/Data Cloud

CyberSecure / Bechtle Advanced Support

Scan Backup

Performs an ad-hoc scan of your backups with an antivirus or the YARA engine to find the latest malware-free restore point or to detect the presence of specific entries, such as personal information.

Scan mode:
 Find the last clean restore point

Search Your Backup

Search within: Outlook as of: 22/04/2024 8:56:03 AM

Primary Search Criteria (select at least one):
 Category: All Fields Field: Bcc Address Condition: is exactly Value: + Add to List

Secondary Search Criteria (optional):
 Category: All Fields Field: Assistant Name Condition: is exactly Value: + Add to List

Find items that match these criteria:

Search Criteria	Field	Condition	Value	Actions
No data				

Reset Start Search

Point in time	Criteria	Page	Status	Message
21/04/2024 8:07:15 AM	Field: System.Subject; Condition: contains; Value: digest;	1		View result

Govern

Policy Enforcement

Risk Assessment

Access Control

Strategy Support

Supply Chain Management

Oversight and Reporting

Contextual Understanding

ERM Integration



Veeam features & editions aligned with NIST 2

Govern	Identify	Protect	Detect	Respond	Recovery
<ul style="list-style-type: none"> G Policy Enforcement G Risk Assessment G Access Control G Strategy Support G Supply Chain Management A Oversight and Reporting G Contextual Understanding G ERM Integration <input type="checkbox"/> Bechtle Consulting 	<ul style="list-style-type: none"> F Security and Compliance Analyzer F YARA A Infrastructure and Backup Reporting / Labeling <input type="checkbox"/> Bechtle Consulting 	<ul style="list-style-type: none"> F Backups F Identity management: RBAC & Data Cloud Roles F SureBackup F Security Analyzer & Threat Center F KMS (advanced) / Encryption / FIPS F Immutabilities F Four Eyes approval F Consulting A Monitoring and alert: Configuration tracking, SLA <input type="checkbox"/> Bechtle Consulting 	<ul style="list-style-type: none"> F Inline Malware Detection F Suspicious file system activity detection F Scan Backup F Early threat detection A Real Time Monitoring A Dedicated Ransomware Activity Alerts P Integration with Microsoft inbuilt virus scanner <input type="checkbox"/> Bechtle Advanced Support 	<ul style="list-style-type: none"> F Event Forwarding via SIEM A Automated Alarm Remediation P Dynamic Documentation P CyberSecure <input type="checkbox"/> Bechtle Advanced Support 	<ul style="list-style-type: none"> F Secure restore – MDR, Yara, Third party (automate), Quarantine Net A Last known clean point F Stage restore / Data Labs with a SIRT (deep inspection) P Recovery Orchestration – VRO F Whatever Instant Recovery – DB, NAS, VMs, disks F Restore anywhere – Clouds, Nutanix, VMware, Hyper-V, Physical, KVM,... C E-Discovery – Veeam Data Cloud <input type="checkbox"/> Bechtle Advanced Support

P Veeam Data Platform Premium
 A Veeam Data Platform Advanced
 F Veeam Data Platform Foundation
 C Veeam Data Cloud
 G Global



Better be ready than sorry !

Citation de: *Nous espérons vous tous*

Merci!

Des questions? Contactez-nous: it-forum.ch@bechtle.com

