VEEAMON 2023

How to SIEM with Veeam

Brett Gavin

Senior Systems Engineer
Northern California
Veeam Software

Eric Ellenberg

Solutions Architect, Enterprise Applications
Product Management Alliances
Veeam Software

Agenda

- Security + operations
- SIEM: what and why
- What can Veeam do: notify
- What can Veeam do: respond
- Examples
- Conclusion

VEEAMON 2023

Security + Operations

Veeam's® role in your environment

Security

Backup is the last line of defense

Security is an ecosystem:

- Multiple solutions working together
- Each solution suited to a purpose
- Nothing is perfect

Backup is your reserve parachute:

- It must work!
- Data must be safe
- Data must be available
- Data management must be simple
- 3-2-1-1-0 rule

© 2023 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Operations

Backup is the restoration engine

Get back online:

- You don’t want this to take a long time (usually)
- You don’t want this to be complex
- You don’t want to have zero options

Get into the cloud:

- Migrate or extend your environment to leverage the cloud
- Pay per GB storage, amiright?

Get your applications tested:

- Sandboxes and staging areas

© 2023 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

VEEAMON 2023

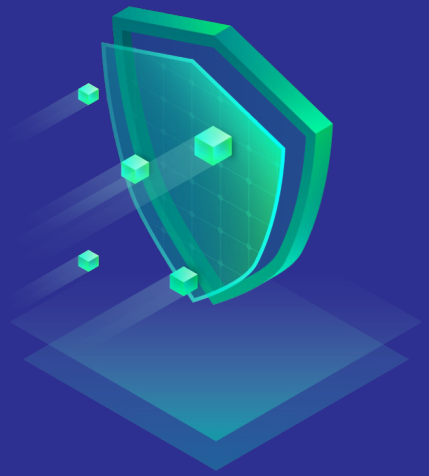
Backup = Security + Operations

VEEAMON 2023

Security information & event management

Keep track of it all

What is a SIEM?



Security information
and event management

Detection, analysis, response

Consolidate log sources
Translate data into action

© 2023 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

SIM, SEM, SIEM, SOAR, XDR, etc.

Got all that?

Digital immune system:

- Lots of solutions with different focus areas

If it can trigger scripts or REST APIs,
it can work with Veeam.

© 2023 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Building security operations

NIST cybersecurity framework

Real-time detection

Consolidate log sources
Translate data into action

© 2023 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Why?

Compliance

Cyber insurance

Reinforces best practices:

- Audit trails
- Change management
- Incident management
- Business impacts

This is the world we live in!

- When everything is connected, everything is vulnerable

© 2023 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

VEEAMON 2023

Veeam + SIEM

Send notifications and alerts

Notifications and alerts

Intelligent alerting

Veeam ONE™

Automation

PowerShell & RESTful API

Do more with less

Data re-use

© 2023 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Veeam ONE

Let Veeam ONE do even more for you

- Automatically triggered SMTP alarms
- SNMP traps
- Monitors infrastructure as well as Veeam

© 2023 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Filters and categories

NORMAL OPERATION	WARNING	CRITICAL // FAILURE	INFORMATIONAL ONLY
Healthy server	Tasks waiting in queue	Repository offline	Infrastructure audits
Plenty of storage	Unexpected data growth	Backup job failed	Capacity planning info
CPU load low	VM backup retries	SLA not met	Admin1 logged in
Backup job successful	Repository low space	High CPU + high disk write	Restore operation
WAN bandwidth low	User1 attempted login	Malware scan hit	MFA enabled
BCJ successful	High CPU	Expired app-aware creds	Set logging level 6

© 2023 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

VeeAMON 2023

Veeam + SIEM

Respond to events using APIs

Automation

PowerShell & REST API

Triggered verification using SureBackup® that last night's backup can be brought onlineNew-VBRSureBackupVM:

- $backup = Get-VBRBackup -Name "MSExchange“
- $RestPoint = Get-VBRRestorePoint -Name "Winsrv2047" -Backup $backup
- New-VBRSureBackupVM -RestorePoint $RestPoint -Role MailServer

Edit traffic rules

Scale-out Backup Repository™ Capacity Tier offload job

- Apply temporary throttling to prevent new fancy cloud-hosted phone system from going down at night
- Apply temporary throttling to prevent manufacturing subnet across WAN connection from losing connection to the C&C – lost/flappy connections in the digital can translate to broken parts in the real

© 2023 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Data re-use

Data Integration API:

- Images - cats vs. dogs: when did they arrive?

Data labs:

- Forensic analysis
- Spin up a copy of your environment to find out when malware first appeared in backups

© 2023 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

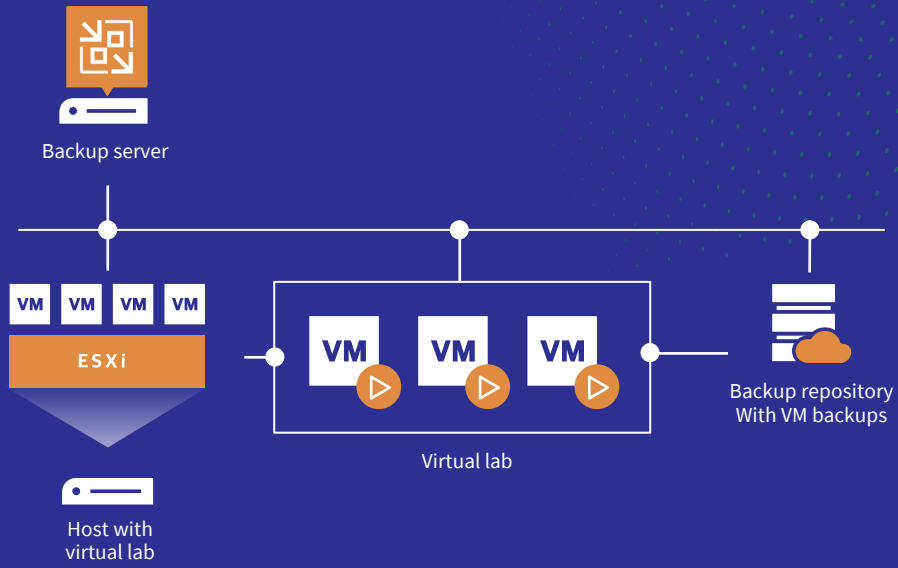
SureBackup

SureBackup:
built-in backup verification feature

Live verification:
backup is scanned for malware, booted in an isolated environment, tested, then powered off

Report is created with verification results

Can run on schedule



© 2023 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Use case example

Malware activity detected on a server

CISA Ransomware Guide:

- Isolate or power down
- Triage
- Create and execute recovery plan

Restore a VM using PowerShell:

- Start-VBRRestoreVM

Restore a VM using REST API:

- /api/v1/restore/vmRestore/vmware/

© 2023 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Wrap up

Build out your security operations:

- Refer to NIST cybersecurity framework
- Start with most critical workloads, then expand

Protect your reserve parachute:

- Backup alerts are high-priority
- Safeguard your repositories

Notifications and responses:

- Set up notifications and alerts in Veeam products
- Use Veeam APIs with SIEM response capabilities
- Automation reduces business impact

© 2023 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.


Thank you!
VEEAMON2023