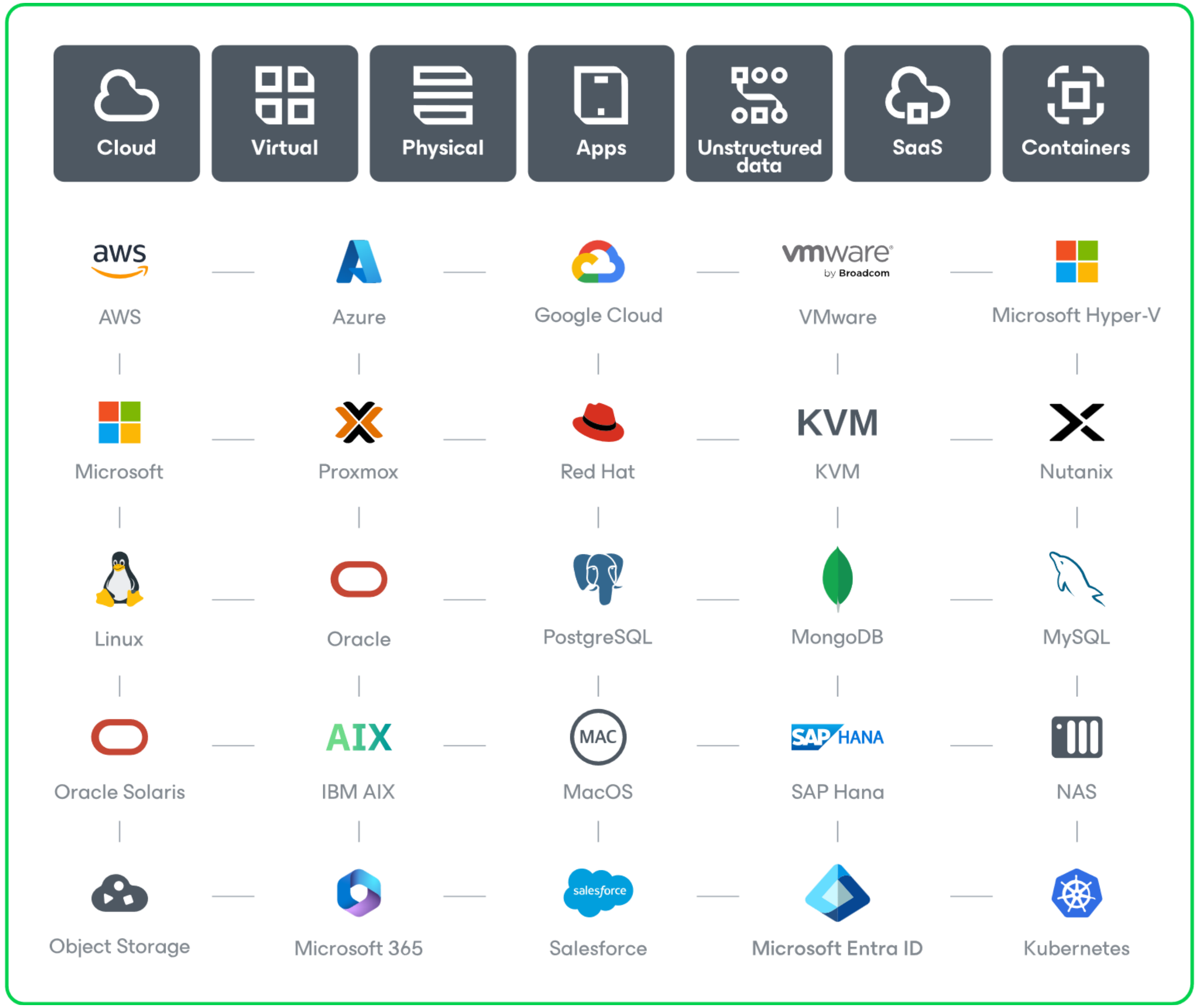
Renforcez votre Cyberdéfense

Comment intégrer Veeam dans une Stratégie de sécurité globale.

Christian Bocquet
Senior System Engineer
Christian.bocquet@veeam.com

Veeam Protection Goes Beyond VMware...



Cloud | Virtual | Physical | Apps | Unstructured data | SaaS | Containers

AWS	Azure	Google Cloud	VMware	Microsoft Hyper-V
Microsoft	Proxmox	Red Hat	KVM	Nutanix
Linux	Oracle	PostgreSQL	MongoDB	MySQL
Oracle Solaris	IBM AIX	MacOS	SAP Hana	NAS
Object Storage	Microsoft 365	Salesforce	Microsoft Entra ID	Kubernetes

Let's have a guess

What is the most important security metric ?

INITIAL COMPROMISE

INTRUSION DETECTED

INVESTIGATION AND RESPONSE

RECOVERY PHASE

LESSONS LEARNED

Mean Time To Resolve

Mean Time to **Detect**

Mean Time to **Respond**

Mean Time to **Recovery**

Veeam Data Platform v12.2 - v13

A year full of security features and enhancements

Recon Scanner

Proactive threat assessment based on collection of logs, events, and potential adversary content

AI-based in-line detection

Data stream scanning to detect **encryption anomalies** and malware artifacts.

Indicators of Compromise

Detection of potentially **malicious tool** appearances on the machines.

Suspicious File System Activity Analysis

Detection of **unusual file system behavior** patterns.

Index Analytics

Detection of potentially **malicious file** appearances on the machines.

Threat Hunter

Signature-based scans with an out-of-the-box experience.

SIEM

Consolidation and mapping of all events of your infrastructure and Veeam into RFC 5424 and SIEM integration

Role-based Security / Separation of duty

New **limited roles** with scopes defined by administrators and separation of duty.
enhanced in v13

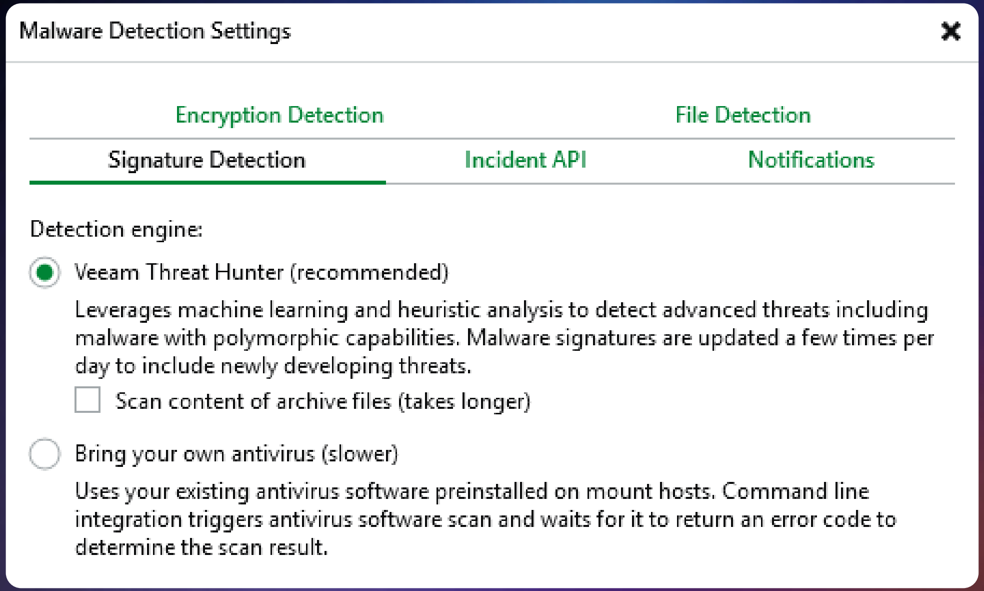
Did you knew:

Veeam help on MTTD ?

Yes we do and since 2019! A few examples:

Veeam Threat Hunter

- Polymorphic signature-based scan of backup data
- Millions of signatures updated live
- Fast and ready
- Scan continuously your backups and look back for malicious traces undetected in production



Malware Detection Settings

Detection engine:

● Veeam Threat Hunter (recommended)

Leverages machine learning and heuristic analysis to detect advanced threats including malware with polymorphic capabilities. Malware signatures are updated a few times per day to include newly developing threats.

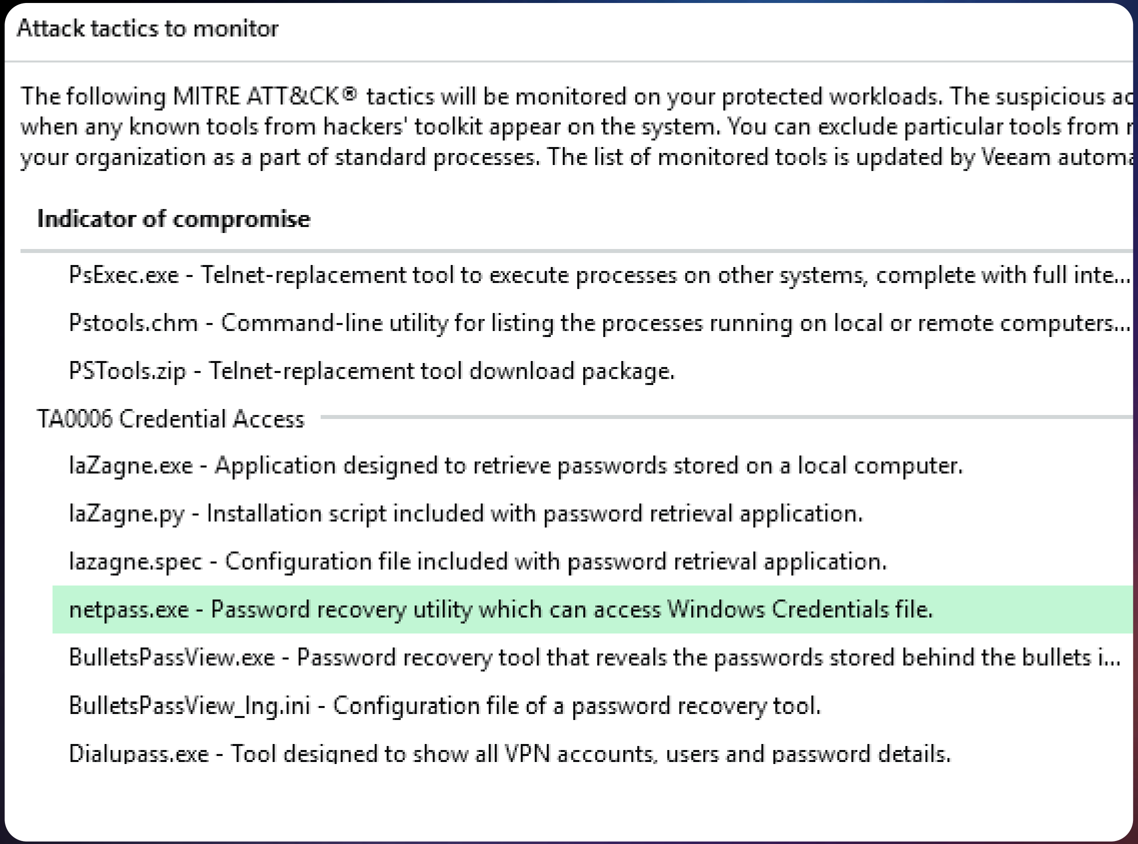
□ Scan content of archive files (takes longer)

○ Bring your own antivirus (slower)

Uses your existing antivirus software preinstalled on mount hosts. Command line integration triggers antivirus software scan and waits for it to return an error code to determine the scan result.

Indicators of Compromise

- Use of guest index and analytics
- Database of potentially unwanted tools from MITRE ATT&CK Matrix
- Fast and ready



Attack tactics to monitor

The following MITRE ATT&CK® tactics will be monitored on your protected workloads. The suspicious ac when any known tools from hackers' toolkit appear on the system. You can exclude particular tools from r your organization as a part of standard processes. The list of monitored tools is updated by Veeam automa

Indicator of compromise

PsExec.exe - Telnet-replacement tool to execute processes on other systems, complete with full inte...
Pstools.chm - Command-line utility for listing the processes running on local or remote computers...
PSTools.zip - Telnet-replacement tool download package.

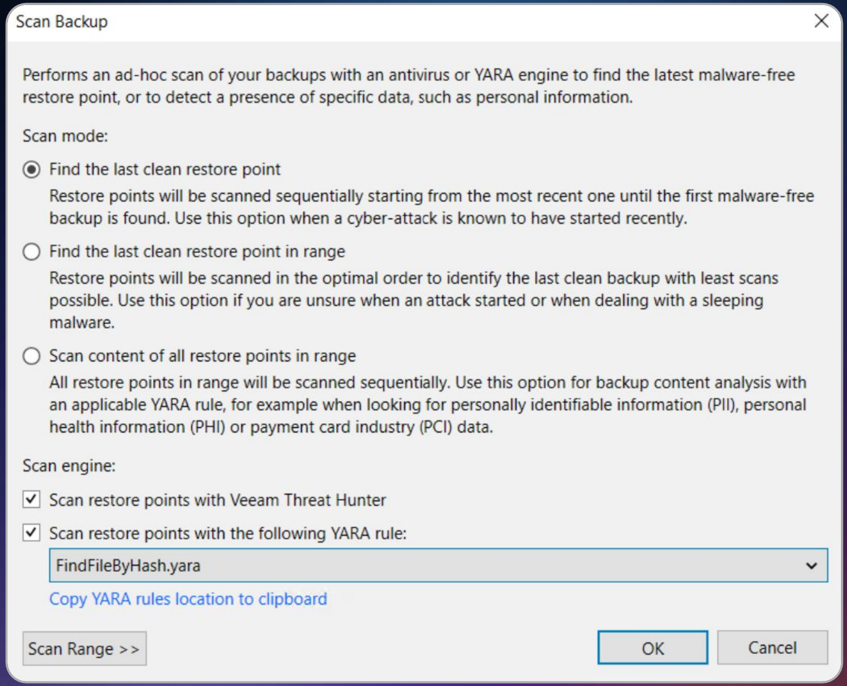
TA0006 Credential Access

laZagne.exe - Application designed to retrieve passwords stored on a local computer.
laZagne.py - Installation script included with password retrieval application.
lazagne.spec - Configuration file included with password retrieval application.
netpass.exe - Password recovery utility which can access Windows Credentials file.
BulletsPassView.exe - Password recovery tool that reveals the passwords stored behind the bullets i...
BulletsPassView_lng.ini - Configuration file of a password recovery tool.
Dialupass.exe - Tool designed to show all VPN accounts, users and password details.

https://attack.mitre.org/

Veeam Yara

- Used in digital forensics and incident response
- Integrated into SureBackup and secure restore
- Can be used with a SOC git for example
- Find your last clean backup



Scan Backup

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

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 backup 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 the optimal order to identify the last clean backup with least scans possible. Use this option if you are unsure when an attack started or when dealing with a sleeping malware.

○ Scan content of all restore points in range

All restore points in range will be scanned sequentially. Use this option for backup content analysis with an applicable YARA rule, for example when looking for personally identifiable information (PII), personal health information (PHI) or payment card industry (PCI) data.

Scan engine:

☑ Scan restore points with Veeam Threat Hunter

☑ Scan restore points with the following YARA rule:

FindFileByHash.yara

SIEM

- RFC5424 to MITRE ATT&CK

Veeam Event	MITRE Tactic	Technique	Description
Backup deletion	Impact	T1490	Prevent restoration
Repository deletion	Impact	T1490	Neutralise storage
Repeated MFA failures	Credential Access	T1110	Force authentication
MFA deactivation	Defense Evasion	T1556.006	Bypass controls
Malicious tools detection	Impact	T1486	Ransomware indicators
Activity detected (entropy)	Impact	T1486	Encryption detected
Privileged account added	Persistence	T1098	Privilege escalation
Lockdown deactivated	Defense Evasion	T1562	Protection reduction
Ransomware alarm	Impact	T1486	Behavioural detection

https://attack.mitre.org/

Did you knew:

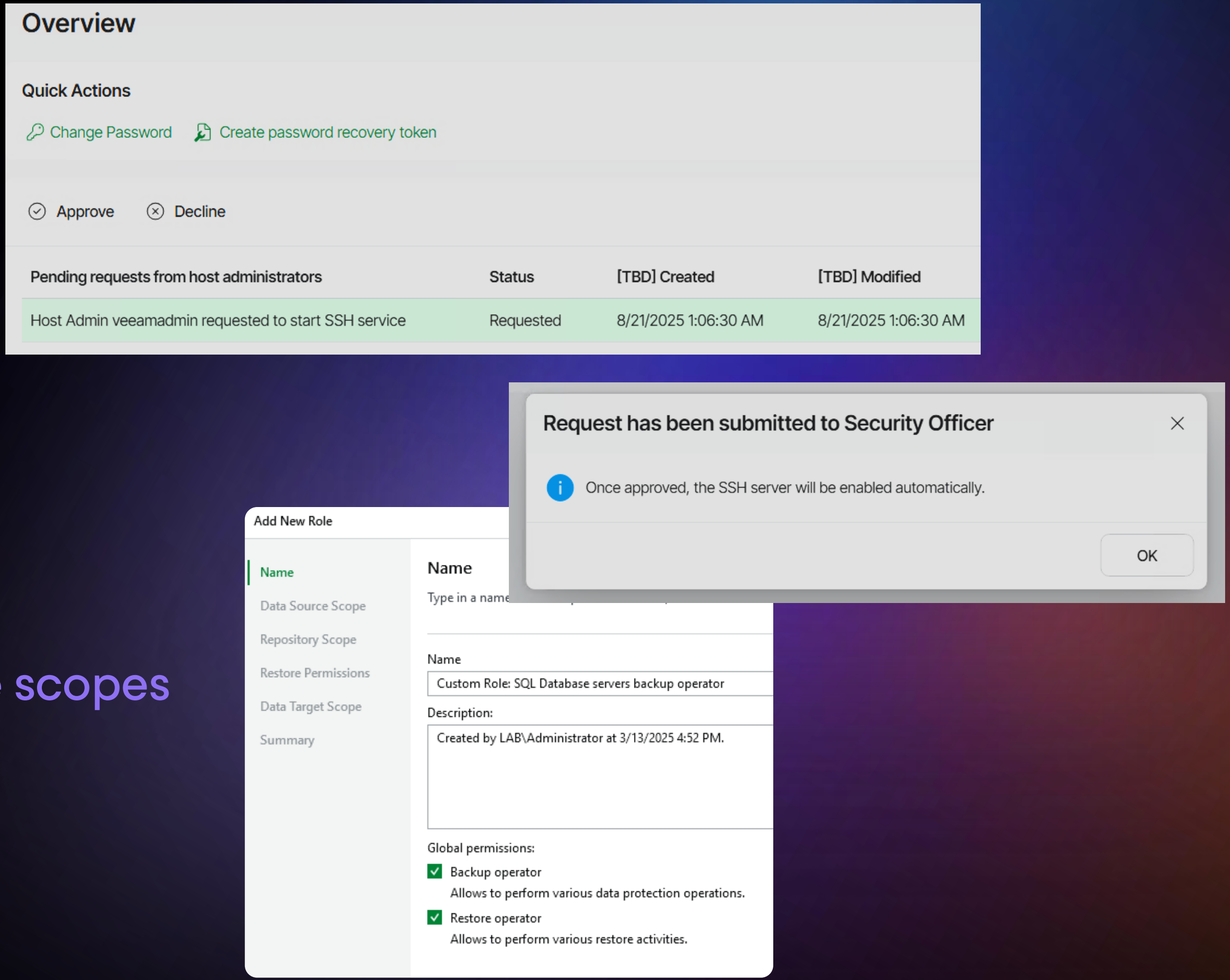
Veeam has full separation of duty?

Yes we do!

Separation of Duty

New roles available today!

- Security administrator and Incident API operator in **V13**
- Advanced filtering of available infrastructure scopes
- Limit available restore operations
- Split and independent from administrator
- Security officer for the cockpit in **V13**
    - **No risky change w/o 2nd validation**



Overview

Quick Actions

Pending requests from host administrators	Status	[TBD] Created	[TBD] Modified
Host Admin veeamadmin requested to start SSH service	Requested	8/21/2025 1:06:30 AM	8/21/2025 1:06:30 AM

Request has been submitted to Security Officer

Once approved, the SSH server will be enabled automatically.

Add New Role

Name

Type in a name

Name: Custom Role: SQL Database servers backup operator

Description: Created by LAB\Administrator at 3/13/2025 4:52 PM.

Global permissions:

☑ Backup operator
Allows to perform various data protection operations.

☑ Restore operator
Allows to perform various restore activities.

The Veeam Security Ecosystem and Marketplace Apps

1+1=3, we are better together

Cyber Resilient Ecosystem

SOAR (Security Orchestration, Automation and Response)

- PREDATAR
- paloalto NETWORKS
- valicyber
- servicenow
- Progress Flowmon
- torq
- veeam

SIEM (Security information and event management)

- paloalto NETWORKS
- CROWDSTRIKE
- SOPHOS
- splunk>
- veeam

Readiness

- DARKTRACE
- kyndryl
- PAESSLER THE NETWORK MONITORING COMPANY
- elastio
- D3 SECURITY
- checkmk
- PREDATAR

Incident Response

- COVEWARE

Tape / WORM

- DELL
- SPECTRA
- IBM
- FUJITSU
- FALCONSTOR
- FAST LTA We secure Petabytes.
- OVERLAND TANDBERG
- ORACLE
- StarWind
- Quest
- Quantum

Storage Integrations

- Microsoft
- Hewlett Packard Enterprise
- Lenovo
- vmware
- HITACHI
- PURESTORAGE
- NUTANIX
- CISCO
- NetApp
- HUAWEI
- DELL
- inspur
- FUJITSU
- NEC
- DATACORE
- INFINIDAT
- IBM
- Tintri

Encryption / KMS

- Azure
- aws
- IBM Security
- Google Cloud
- Fortanix
- ENTRUST
- THALES

SureBackup Light, Secure Restore & Ransomware Detection

- Bitdefender
- Microsoft Defender
- Symantec by Broadcom
- eset
- SOPHOS
- Trellix
- veeam

Security & Compliance Monitoring

- CONTINUITY
- XM Cyber
- veeam

Veeam Ready Immutability

- Red Hat
- wasabi
- IBM
- DELL
- NetApp
- NUTANIX
- BACKBLAZE
- DATACORE
- CLOUDIAN
- PURESTORAGE
- FAST LTA We secure Petabytes.
- Impossible Cloud
- OBJECT FIRST
- HITACHI
- iTernity
- MINIO
- NEXSAN
- 11:11 SYSTEMS
- ORACLE
- OSNEXUS
- Quest
- OVHcloud
- QNAP
- Quantum
- SEAGATE
- STONEFLY
- POINT software & systems
- SOFTIRON
- Ugloo
- Infortrend
- SWARM
- SUSE
- SPECTRA
- SCALITY
- RSTOR
- SwiftStack
- VAST
- Synology

Veeam Integrated Immutability

- aws
- Azure
- IBM Cloud
- wasabi

Identity Management/SAML

- CYBERARK THE IDENTITY SECURITY COMPANY

Veeam App for PaloAlto

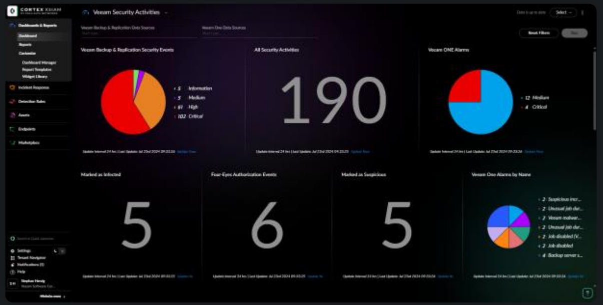
Get visibility with XSIAM and automate with XSOAR

Integrate Veeam Data Platform Advanced and Premium editions with Palo Alto Networks

> "Veeam is the **first** Palo Alto Networks partner to independently develop and publish a Cortex XSIAM collector integration."

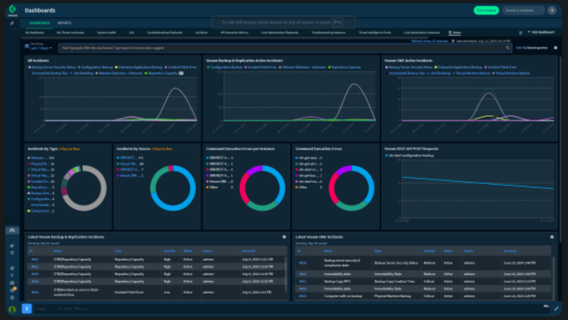
Veeam App for Palo Alto Networks XSIAM

- Event forwarding from both Veeam Backup & Replication and VeeamONE
- Veeam monitoring dashboard
- Veeam security dashboard
- Pre-created parser
- Automatic event filtering
- Documented correlation rules



Veeam App for Palo Alto Networks XSOAR

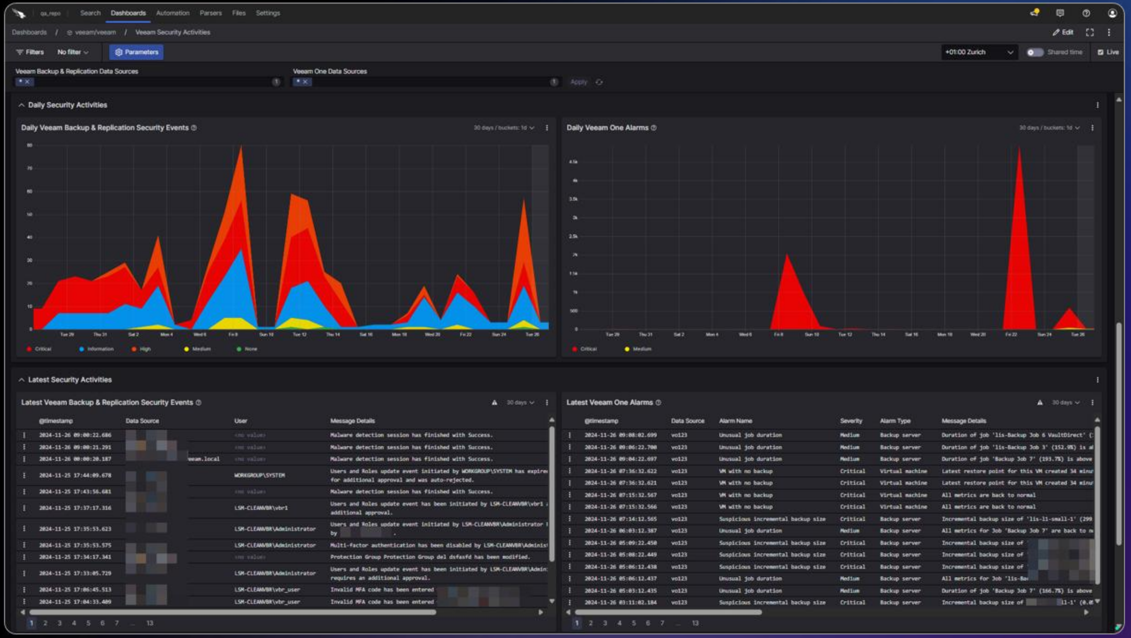
- API-level connection to both Veeam Backup & Replication and VeeamONE
- Incident dashboard for SOC teams
- Veeam security event handling
- Playbooks and functions for remediation



Veeam App for CrowdStrike Falcon LogScale

Integrate Veeam Backup & Replication and VeeamONE with CrowdStrike

- Monitor Veeam application events, including the new Entra ID backup and Indicator of Compromise events, for operational metrics and issues
- Identify internal security threats
- Improve threat response time
- Use pre-defined and scheduled searches to receive notifications

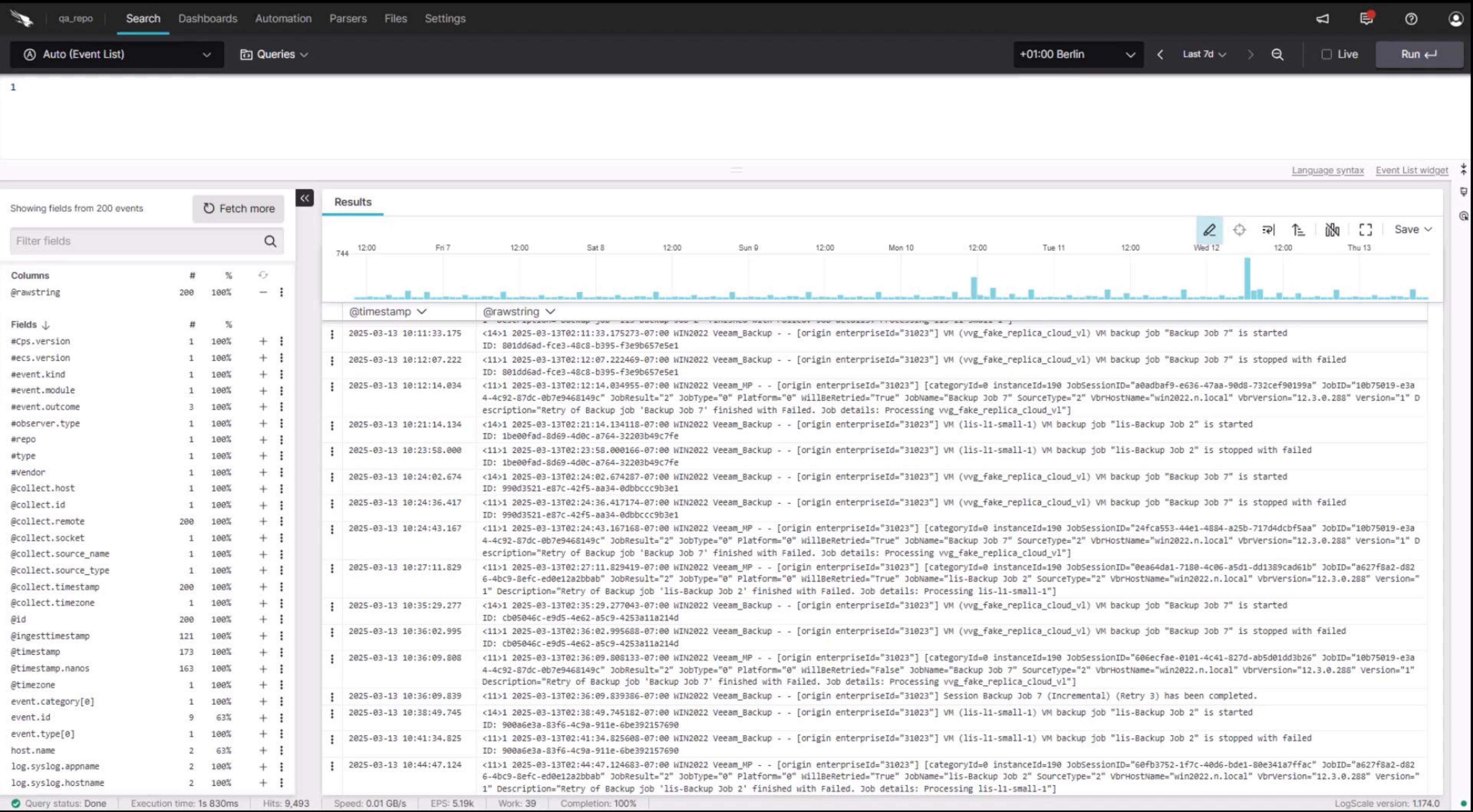


Latest Veeam Backup & Replication Security Events

@timestamp	Data Source	User	Message Details
2024-11-26 09:00:22.686	[redacted]	<no value>	Malware detection session has finished with Success.
2024-11-26 09:00:21.291	[redacted]	<no value>	Malware detection session has finished with Success.
2024-11-26 00:00:20.187	[redacted] eeam.local	<no value>	Malware detection session has finished with Success.
2024-11-25 17:44:09.678	[redacted]	WORKGROUP\SYSTEM	Users and Roles update event initiated by WORKGROUP\SYSTEM has expire for additional approval and was auto-rejected.
2024-11-25 17:43:56.681	[redacted]	<no value>	Malware detection session has finished with Success.
2024-11-25 17:37:17.316	[redacted]	LSM-CLEANVBR\vbr1	Users and Roles update event has been initiated by LSM-CLEANVBR\vbr1 additional approval.
2024-11-25 17:35:53.623	[redacted]	LSM-CLEANVBR\Administrator	Users and Roles update event initiated by LSM-CLEANVBR\Administrator by [redacted] .
2024-11-25 17:35:53.575	[redacted]	LSM-CLEANVBR\Administrator	Multi-factor authentication has been disabled by LSM-CLEANVBR\Adminis
2024-11-25 17:34:17.341	[redacted]	<no value>	Protection Group Protection Group del dsfasfd has been modified.
2024-11-25 17:33:05.729	[redacted]	LSM-CLEANVBR\Administrator	Users and Roles update event has been initiated by LSM-CLEANVBR\Admin requires an additional approval.
2024-11-25 17:06:45.513	[redacted]	LSM-CLEANVBR\vbr_user	Invalid MFA code has been entered [redacted]
2024-11-25 17:04:33.409	[redacted]	LSM-CLEANVBR\vbr_user	Invalid MFA code has been entered [redacted]

Latest Veeam One Alarms

@timestamp	Data Source	Alarm Name	Severity	Alarm Type	Message Details
2024-11-26 09:08:02.699	vo123	Unusual job duration	Medium	Backup server	Duration of job '1is-Backup Job 6 VaultDirect' (
2024-11-26 09:06:22.700	vo123	Unusual job duration	Medium	Backup server	Duration of job '1is-Backup Job 3' (152.9%) is a
2024-11-26 09:04:22.697	vo123	Unusual job duration	Medium	Backup server	Duration of job 'Backup Job 7' (193.7%) is above
2024-11-26 07:36:32.622	vo123	VM with no backup	Critical	Virtual machine	Latest restore point for this VM created 34 minu
2024-11-26 07:36:32.621	vo123	VM with no backup	Critical	Virtual machine	Latest restore point for this VM created 34 minu
2024-11-26 07:15:32.567	vo123	VM with no backup	Critical	Virtual machine	All metrics are back to normal
2024-11-26 07:15:32.566	vo123	VM with no backup	Critical	Virtual machine	All metrics are back to normal
2024-11-26 07:14:12.565	vo123	Suspicious incremental backup size	Critical	Backup server	Incremental backup size of '1is-11-small-1' (299
2024-11-26 06:03:12.387	vo123	Unusual job duration	Medium	Backup server	All metrics for Job 'Backup Job 7' are back to n
2024-11-26 05:09:22.450	vo123	Suspicious incremental backup size	Critical	Backup server	Incremental backup size of [redacted]
2024-11-26 05:08:22.449	vo123	Suspicious incremental backup size	Critical	Backup server	Incremental backup size of [redacted]
2024-11-26 05:06:12.438	vo123	Suspicious incremental backup size	Critical	Backup server	Incremental backup size of [redacted]
2024-11-26 05:06:12.437	vo123	Unusual job duration	Medium	Backup server	All metrics for Job '1is-Ba [redacted]
2024-11-26 05:03:12.435	vo123	Unusual job duration	Medium	Backup server	Duration of job 'Backup Job 7' (166.7%) is above
2024-11-26 03:11:02.184	vo123	Suspicious incremental backup size	Critical	Backup server	Incremental backup size of [redacted] 11-1' (0.0



Columns	#	%
@rawstring	200	100%

Fields	#	%
#Cps.version	1	100%
#ecs.version	1	100%
#event.kind	1	100%
#event.module	1	100%
#event.outcome	3	100%
#observer.type	1	100%
#repo	1	100%
#type	1	100%
#Vendor	1	100%
@collect.host	1	100%
@collect.id	1	100%
@collect.remote	200	100%
@collect.socket	1	100%
@collect.source_name	1	100%
@collect.source_type	1	100%
@collect.timestamp	200	100%
@collect.timezone	1	100%
@id	200	100%
@ingesttimestamp	121	100%
@timestamp	173	100%
@timestamp.nanos	163	100%
@timezone	1	100%
event.category[0]	1	100%
event.id	9	63%
event.type[0]	1	100%
host.name	2	63%
log.syslog.appname	2	100%
log.syslog.hostname	2	100%

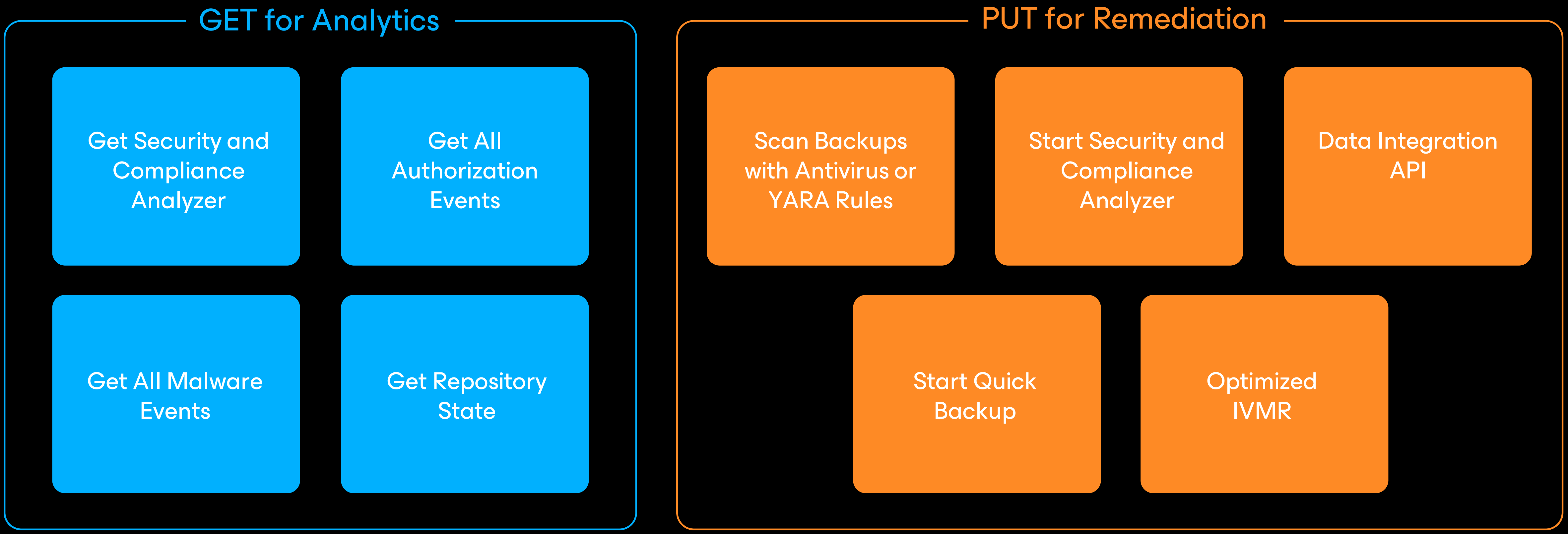
```
@timestamp               @rawstring
2025-03-13 10:11:33.175  <14>1 2025-03-13T02:11:33.175273-07:00 WIN2022 Veeam_Backup - - [origin enterpriseId="31023"] VM (vvg_fake_replica_cloud_vl) VM backup job "Backup Job 7" is started
                         ID: 801dd6ad-fce3-48c8-b395-f3e9b657e5e1
2025-03-13 10:12:07.222  <11>1 2025-03-13T02:12:07.222469-07:00 WIN2022 Veeam_Backup - - [origin enterpriseId="31023"] VM (vvg_fake_replica_cloud_vl) VM backup job "Backup Job 7" is stopped with failed
                         ID: 801dd6ad-fce3-48c8-b395-f3e9b657e5e1
2025-03-13 10:12:14.034  <11>1 2025-03-13T02:12:14.034955-07:00 WIN2022 Veeam_MP - - [origin enterpriseId="31023"] [categoryId=0 instanceId=190 JobSessionID="a0adbaf9-e636-47aa-90d8-732cef90199a" JobID="10b75019-e3a
                         4-4c92-87dc-0b7e9468149c" JobResult="2" JobType="0" Platform="0" WillBeRetried="True" JobName="Backup Job 7" SourceType="2" VbrHostName="win2022.n.local" VbrVersion="12.3.0.288" Version="1" D
                         escription="Retry of Backup job 'Backup Job 7' finished with Failed. Job details: Processing vvg_fake_replica_cloud_vl"]
2025-03-13 10:21:14.134  <14>1 2025-03-13T02:21:14.134118-07:00 WIN2022 Veeam_Backup - - [origin enterpriseId="31023"] VM (lis-l1-small-1) VM backup job "lis-Backup Job 2" is started
                         ID: 1be00fad-8d69-4d0c-a764-32203b49c7fe
2025-03-13 10:23:58.000  <11>1 2025-03-13T02:23:58.000166-07:00 WIN2022 Veeam_Backup - - [origin enterpriseId="31023"] VM (lis-l1-small-1) VM backup job "lis-Backup Job 2" is stopped with failed
                         ID: 1be00fad-8d69-4d0c-a764-32203b49c7fe
2025-03-13 10:24:02.674  <14>1 2025-03-13T02:24:02.674287-07:00 WIN2022 Veeam_Backup - - [origin enterpriseId="31023"] VM (vvg_fake_replica_cloud_vl) VM backup job "Backup Job 7" is started
                         ID: 990d3521-e87c-42f5-aa34-0dbbccc9b3e1
2025-03-13 10:24:36.417  <11>1 2025-03-13T02:24:36.417174-07:00 WIN2022 Veeam_Backup - - [origin enterpriseId="31023"] VM (vvg_fake_replica_cloud_vl) VM backup job "Backup Job 7" is stopped with failed
                         ID: 990d3521-e87c-42f5-aa34-0dbbccc9b3e1
2025-03-13 10:24:43.167  <11>1 2025-03-13T02:24:43.167168-07:00 WIN2022 Veeam_MP - - [origin enterpriseId="31023"] [categoryId=0 instanceId=190 JobSessionID="24fca553-44e1-4884-a25b-717d4dcbf5aa" JobID="10b75019-e3a
                         4-4c92-87dc-0b7e9468149c" JobResult="2" JobType="0" Platform="0" WillBeRetried="True" JobName="Backup Job 7" SourceType="2" VbrHostName="win2022.n.local" VbrVersion="12.3.0.288" Version="1" D
                         escription="Retry of Backup job 'Backup Job 7' finished with Failed. Job details: Processing vvg_fake_replica_cloud_vl"]
2025-03-13 10:27:11.829  <11>1 2025-03-13T02:27:11.829419-07:00 WIN2022 Veeam_MP - - [origin enterpriseId="31023"] [categoryId=0 instanceId=190 JobSessionID="0ea64da1-7180-4c06-a5d1-dd1389cad61b" JobID="a627f8a2-d82
                         6-4bc9-8efc-ed0e12a2bbab" JobResult="2" JobType="0" Platform="0" WillBeRetried="True" JobName="lis-Backup Job 2" SourceType="2" VbrHostName="win2022.n.local" VbrVersion="12.3.0.288" Version="
                         1" Description="Retry of Backup job 'lis-Backup Job 2' finished with Failed. Job details: Processing lis-l1-small-1"]
2025-03-13 10:35:29.277  <14>1 2025-03-13T02:35:29.277043-07:00 WIN2022 Veeam_Backup - - [origin enterpriseId="31023"] VM (vvg_fake_replica_cloud_vl) VM backup job "Backup Job 7" is started
                         ID: cb05046c-e9d5-4e62-a5c9-4253a11a214d
2025-03-13 10:36:02.995  <11>1 2025-03-13T02:36:02.995688-07:00 WIN2022 Veeam_Backup - - [origin enterpriseId="31023"] VM (vvg_fake_replica_cloud_vl) VM backup job "Backup Job 7" is stopped with failed
                         ID: cb05046c-e9d5-4e62-a5c9-4253a11a214d
2025-03-13 10:36:09.808  <11>1 2025-03-13T02:36:09.808133-07:00 WIN2022 Veeam_MP - - [origin enterpriseId="31023"] [categoryId=0 instanceId=190 JobSessionID="606ecfae-0101-4c41-827d-ab5d01dd3b26" JobID="10b75019-e3a
                         4-4c92-87dc-0b7e9468149c" JobResult="2" JobType="0" Platform="0" WillBeRetried="False" JobName="Backup Job 7" SourceType="2" VbrHostName="win2022.n.local" VbrVersion="12.3.0.288" Version="1"
                         Description="Retry of Backup job 'Backup Job 7' finished with Failed. Job details: Processing vvg_fake_replica_cloud_vl"]
2025-03-13 10:36:09.839  <11>1 2025-03-13T02:36:09.839386-07:00 WIN2022 Veeam_Backup - - [origin enterpriseId="31023"] Session Backup Job 7 (Incremental) (Retry 3) has been completed.
2025-03-13 10:38:49.745  <14>1 2025-03-13T02:38:49.745182-07:00 WIN2022 Veeam_Backup - - [origin enterpriseId="31023"] VM (lis-l1-small-1) VM backup job "lis-Backup Job 2" is started
                         ID: 900a6e3a-83f6-4c9a-911e-6be392157690
2025-03-13 10:41:34.825  <11>1 2025-03-13T02:41:34.825608-07:00 WIN2022 Veeam_Backup - - [origin enterpriseId="31023"] VM (lis-l1-small-1) VM backup job "lis-Backup Job 2" is stopped with failed
                         ID: 900a6e3a-83f6-4c9a-911e-6be392157690
2025-03-13 10:44:47.124  <11>1 2025-03-13T02:44:47.124683-07:00 WIN2022 Veeam_MP - - [origin enterpriseId="31023"] [categoryId=0 instanceId=190 JobSessionID="60fb3752-1f7c-40d6-bde1-80e341a7ffac" JobID="a627f8a2-d82
                         6-4bc9-8efc-ed0e12a2bbab" JobResult="2" JobType="0" Platform="0" WillBeRetried="True" JobName="lis-Backup Job 2" SourceType="2" VbrHostName="win2022.n.local" VbrVersion="12.3.0.288" Version="
                         1" Description="Retry of Backup job 'lis-Backup Job 2' finished with Failed. Job details: Processing lis-l1-small-1"]
```

Query status: Done | Execution time: 1s 830ms | Hits: 9,493 | Speed: 0.01 GB/s | EPS: 5.19k | Work: 39 | Completion: 100% | LogScale version: 1.174.0

Veeam Security API enhancements

Get more out of your automation

Especially with Veeam Backup & Replication v12.3, we significantly enhanced the amount of available APIs for security purposes.



GET for Analytics

- Get Security and Compliance Analyzer
- Get All Authorization Events
- Get All Malware Events
- Get Repository State

PUT for Remediation

- Scan Backups with Antivirus or YARA Rules
- Start Security and Compliance Analyzer
- Data Integration API
- Start Quick Backup
- Optimized IVMR

What can we do with:

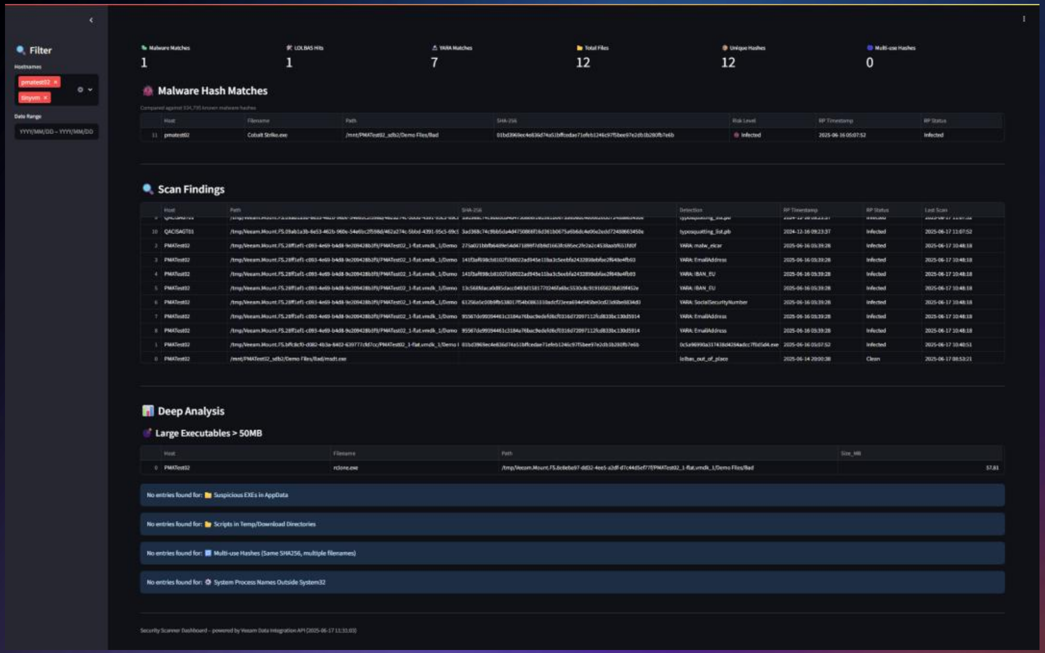
Veeam Data API?

Limitless ☺ let's see an example from one of my colleague, "Steve" Herzig

Veeam Retro Hunter

- Mount your backups
- Expose them through the Data API / MCP
- Analyse and Scale
- Streamlit dashboard
- Profit ?

- Malware Hash Matches
- Scan Findings (YARA/LOLBAS)
- Large Executables
- Suspicious EXEs in AppData
- Scripts in Temp/Download Directories
- Multi-use Hashes
- System Process Names Outside System32
- High Entropy Files in Suspicious Paths
- Windows Event Log Entries
- High-Entropy Executables with Recent PE Timestamps



Malware Matches	LOLBAS Hits	YARA Matches	Total Files	Unique Hashes	Multi-use Hashes
1	1	7	12	12	0

Malware Hash Matches

Compared against 334,735 known malware hashes

	Host	Filename	Path	SHA-256	Risk Level	RP Timestamp	RP Status
11	pmatest02	Cobalt Strike.exe	/mnt/PMATest02_sdb2/Demo Files/Bad	01bd3969ec4e836d74a51bffcedae71efeb1246c97f5bee97e2db1b280fb7e6b	Infected	2025-06-16 05:07:52	Infected

Scan Findings

	Host	Path	SHA-256	Detection	RP Timestamp	RP Status	Last Scan
10	QACISAGT01	/tmp/Veeam.Mount.FS.09ab1a3b-6e53-462b-960e-54e6bc2f598d/462a274c-5bbd-4391-95c5-69c5	3ad368c74c9bb5da4d4750888f16d361b0675a6b6dc4e06e2edd72488663450e	typosquatting_list.pb	2024-12-16 09:23:37	Infected	2025-06-17 11:07:52
2	PMATest02	/tmp/Veeam.Mount.FS.28ff1ef1-c093-4e69-b4d8-9e209428b3f9/PMATest02_1-flat.vmdk_1/Demo	275a021bbfb6489e54d471898f7db9d1663fc695ec2fe2a2c4538aabf651f80f	YARA: malw_eicar	2025-06-16 03:39:28	Infected	2025-06-17 10:48:18
3	PMATest02	/tmp/Veeam.Mount.FS.28ff1ef1-c093-4e69-b4d8-9e209428b3f9/PMATest02_1-flat.vmdk_1/Demo	141f3af698cb8102f1b0022ad945e11ba3c5eebfa2432898ebfae2f648e4fb93	YARA: EmailAddress	2025-06-16 03:39:28	Infected	2025-06-17 10:48:18
4	PMATest02	/tmp/Veeam.Mount.FS.28ff1ef1-c093-4e69-b4d8-9e209428b3f9/PMATest02_1-flat.vmdk_1/Demo	141f3af698cb8102f1b0022ad945e11ba3c5eebfa2432898ebfae2f648e4fb93	YARA: IBAN_EU	2025-06-16 03:39:28	Infected	2025-06-17 10:48:18
5	PMATest02	/tmp/Veeam.Mount.FS.28ff1ef1-c093-4e69-b4d8-9e209428b3f9/PMATest02_1-flat.vmdk_1/Demo	13c568fdaca0d85dacc0493d1581770246fa6bc5530c8c9191656823b839f452e	YARA: IBAN_EU	2025-06-16 03:39:28	Infected	2025-06-17 10:48:18
6	PMATest02	/tmp/Veeam.Mount.FS.28ff1ef1-c093-4e69-b4d8-9e209428b3f9/PMATest02_1-flat.vmdk_1/Demo	61256a5c00b9fb538017f54b0861010adcf23eea694e945be0cd23d6be8834d0	YARA: SocialSecurityNumber	2025-06-16 03:39:28	Infected	2025-06-17 10:48:18
7	PMATest02	/tmp/Veeam.Mount.FS.28ff1ef1-c093-4e69-b4d8-9e209428b3f9/PMATest02_1-flat.vmdk_1/Demo	95567de99394461c3184a76bac9edefd6cf0316d72097112fcd833bc130d5914	YARA: EmailAddress	2025-06-16 03:39:28	Infected	2025-06-17 10:48:18
8	PMATest02	/tmp/Veeam.Mount.FS.28ff1ef1-c093-4e69-b4d8-9e209428b3f9/PMATest02_1-flat.vmdk_1/Demo	95567de99394461c3184a76bac9edefd6cf0316d72097112fcd833bc130d5914	YARA: EmailAddress	2025-06-16 03:39:28	Infected	2025-06-17 10:48:18
1	PMATest02	/tmp/Veeam.Mount.FS.bffc8cf0-d082-4b3a-8402-639777cfd7cc/PMATest02_1-flat.vmdk_1/Demo I	01bd3969ec4e836d74a51bffcedae71efeb1246c97f5bee97e2db1b280fb7e6b	0c5a96990a317438d4284adcc7f0d5d4.exe	2025-06-16 05:07:52	Infected	2025-06-17 10:40:51
0	PMATest02	/mnt/PMATest02_sdb2/Demo Files/Bad/msdt.exe		lolbas_out_of_place	2025-06-14 20:00:38	Clean	2025-06-17 08:53:21

Deep Analysis

Large Executables > 50MB

	Host	Filename	Path	Size_MB
0	PMATest02	rclone.exe	/tmp/Veeam.Mount.FS.8e8eba97-dd32-4ee5-a2df-d7c44d5ef77f/PMATest02_1-flat.vmdk_1/Demo Files/Bad	57.81

No entries found for: Suspicious EXEs in AppData

No entries found for: Scripts in Temp/Download Directories

No entries found for: Multi-use Hashes (Same SHA256, multiple filenames)

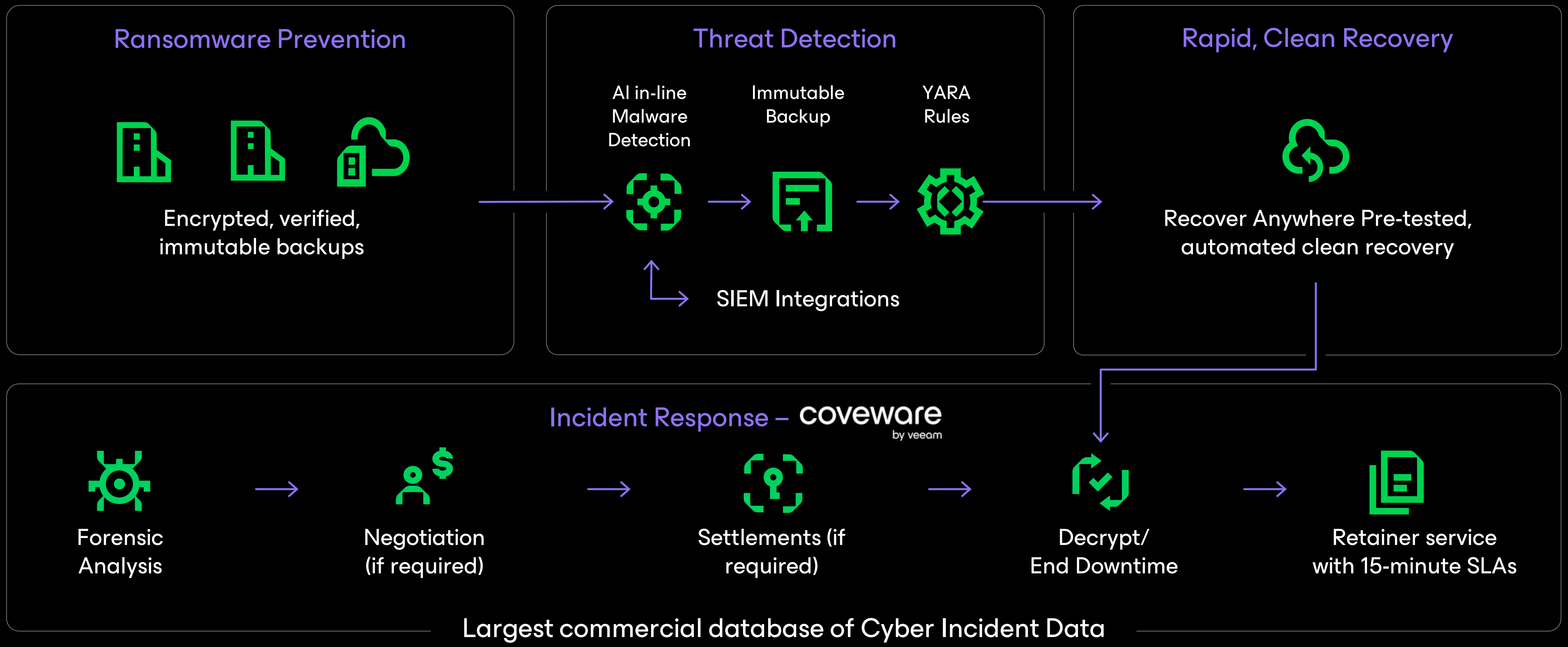
No entries found for: System Process Names Outside System32

Security Scanner Dashboard – powered by Veeam Data Integration API (2025-06-17 11:31:03)

Veeam provides the most complete end-to-end ransomware protection and recovery

Veeam Cyber Secure Program

24/7/365 SWAT Team | Health Checks | Ransomware Warranty | Incident Response Retainer



Ransomware Prevention

Encrypted, verified, immutable backups

Threat Detection

AI in-line Malware Detection → Immutable Backup → YARA Rules

SIEM Integrations

Rapid, Clean Recovery

Recover Anywhere Pre-tested, automated clean recovery

Incident Response – coveware by veeam

Forensic Analysis → Negotiation (if required) → Settlements (if required) → Decrypt/ End Downtime → Retainer service with 15-minute SLAs

Largest commercial database of Cyber Incident Data

Summary

What to remember
and try at home

veeam
Help Center - API

RETRO HUNTER

paloalto NETWORKS

Security

Lower your mean time of detection

Implement separation of duty

Veeam Threat Hunter

Leverage your third-party security app with Veeam

Exploit the Veeam Data API

Christian Bocquet
Senior system engineer
Christian.bocquet@veeam.com

MERCI DE VOTRE ATTENTION !

Sondage de satisfaction

Merci de votre feedback

Scannez-moi

Cyberdefense