©YE

Hyver Integrations Hub

Integrate security and IT data to continuously monitor your cyber exposure, correlate findings, and remediate faster.

Assets		Findings		
C 21 From the last 24H Total Accests 81	6	Operating Operating <t< th=""><th>Top 2 Integration</th><th>Know64 72 Rapi67 41 Defender for cloud 27 Software 11 Other 11</th></t<>	Top 2 Integration	Know64 72 Rapi67 41 Defender for cloud 27 Software 11 Other 11
Filters Clear •	Showi	g Latest 50 from 1234 Q. Search &		
Name 👃 Sav	recity 👃	Description	J Type J	Source 4
CVIC-2021-64832	Critical	The library 'org assets logging log4(log4) cont' version 2:14.1' was detected in 'Grefiel Ibrary manager' located at 'https://aspool- rego/12275347-3620-46006_gets/6074492044550546941iyandio.loc/80' and is vulneable to 'OVE-2023-44022' which exists in versione '> 2.1	3.0, . Vulnerabilities	a ==
Secrets not stored in a secret co	Critical	Not available	Valvenbillies	O Tenable
Scenne rmep.org	High	Hoot asset	Asset	Qualyo
VPC subnet should have Private	Hat	This rule checks whether the submet has Private Google Access enabled, which allows access to Geogle APIs and services from an internal P This rule skips submets that have a purpose of REGIONALLMANNUED.PROCET, "PRIVATE_SERVICE_CONNECT," WITERNAL_HTTPS_LOAD_BALA	NCE Vulnerabilities	🗘 Microsoft
CVIC-0023-0978	ledun	The library galang orgivited 'vension' 0.0.0202200211102010-040023be2k58F' was detected in 'Ceberg binary' located at 'vitaesdawgood der' a valenable to 'CVC-2023-979F', which exists in vensions' < 0.13.0° be valenability was found in the (Ditbab Security Advisory)/trips.vjpHab com-	nd is Vulnerabilities	Ane
81.4.108.41	lot. Avail Dre	Host asset	Asset	🕾 AWS
SCANTREAMADLOG	M. Avallie	Heat asset	Asset	D Repid?
CVE-2123-0978	Fiel	The library 'galaxy org/s/set' version '0.0-20220621195019-' was detected in 'Oplang binary' located at 'shared/argood der' and is vulnerabl 'DYE-2023-9796', which exis	e 30 Vuinerabilities	Know84

Correlate findings. Create tasks. Remediate faster.

Hyver integrates the telemetry from your existing tools to correlate data into a central page with prioritization of the findings to be addressed. Hyver's mathematical model analyzes the telemetry and eliminates duplicates, to determine the finding's contribution to the overall cyber exposure. This allows organizations to prioritize remediation actions based on their value to reduce cyber exposure.

Key Benefits

Correlate & Deduplicate Findings:

Eliminate redundant alerts by integrating telemetry from your cybersecurity stack, including VM, cloud, AppSec, IAM, EDR, and awareness tools.

Prioritize Based on Exploitation Likelihood and Impact: Use Likelihood of Breach (LoB) and Cost of Breach (CoB) to surface the most critical exposures in your attack surface.

Single, Central View in Context: Centralize findings from all sources into a single, contextualized page.

🗸 Remediate Fast:

Push remediation actions to the relevant teams across the organization via SecOps and enterprise solutions such as your SIEM, Jira, and ServiceNow.

Scale with Automated Workflows:

Connect with 1,000+ tools, including custom and non-standard platforms, using Workato to expand remediation execution across your specific enterprise tools and processes.

How the integration works

Integrate data (tools and reports)



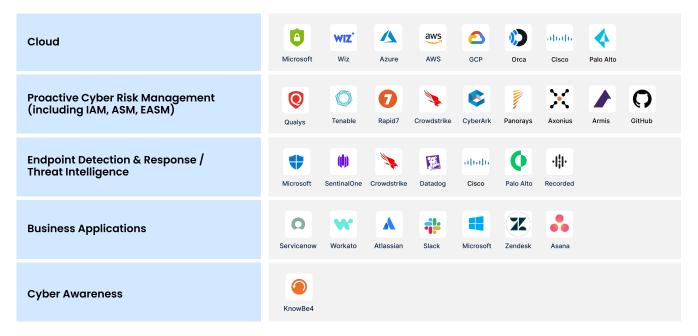
See your maturity, risk, and exposure metrics



Create and execute mitigation plans (ITSM / workflows)

Integrations Hub

Hyver connects with 100+ tools across your environment, some of which are mentioned in the table below, representing the more common tools as reference.



The Hyver Advantage

Gain clarity from the data in your cybersecurity tools by

- Automatically correlating and mapping findings on your organizational attack graph with likelihood of vulnerabilities' exploitability
- Determining your cyber exposure in financial terms to drive outcome-driven priorities
- Identifying the findings that are more critical to block to reduce your exposure
- Dispatching remediation tasks across your organization
- Monitoring and tracking your mitigation outcomes with a continuous feedback
 loop from your cybersecurity stack

Start Managing Cyber Exposure To Enable Your Business Growth Discover how Hyver enables you to continuously reduce your cyber exposure, prioritize remediation, and improve your cyber resilience over time.

Schedule a demo

About CYE

CYE's exposure management platform, Hyver, transforms the way security teams protect their organizations. With CRQ at its core, the platform reveals enterprises' exposure in financial terms, visualizes the most exploitable attack routes to critical business assets, and creates mitigation plans tailored to each business. CYE's customized reporting enables the sharing of vital board-level metrics and validating exposure reduction over time. In addition, CYE improves cybersecurity maturity by mapping weaknesses and defining targets based on industry frameworks. Founded in 2012 in Israel with operations around the world, CYE has served hundreds of organizations across industries globally. Visit us at cyesec.com.