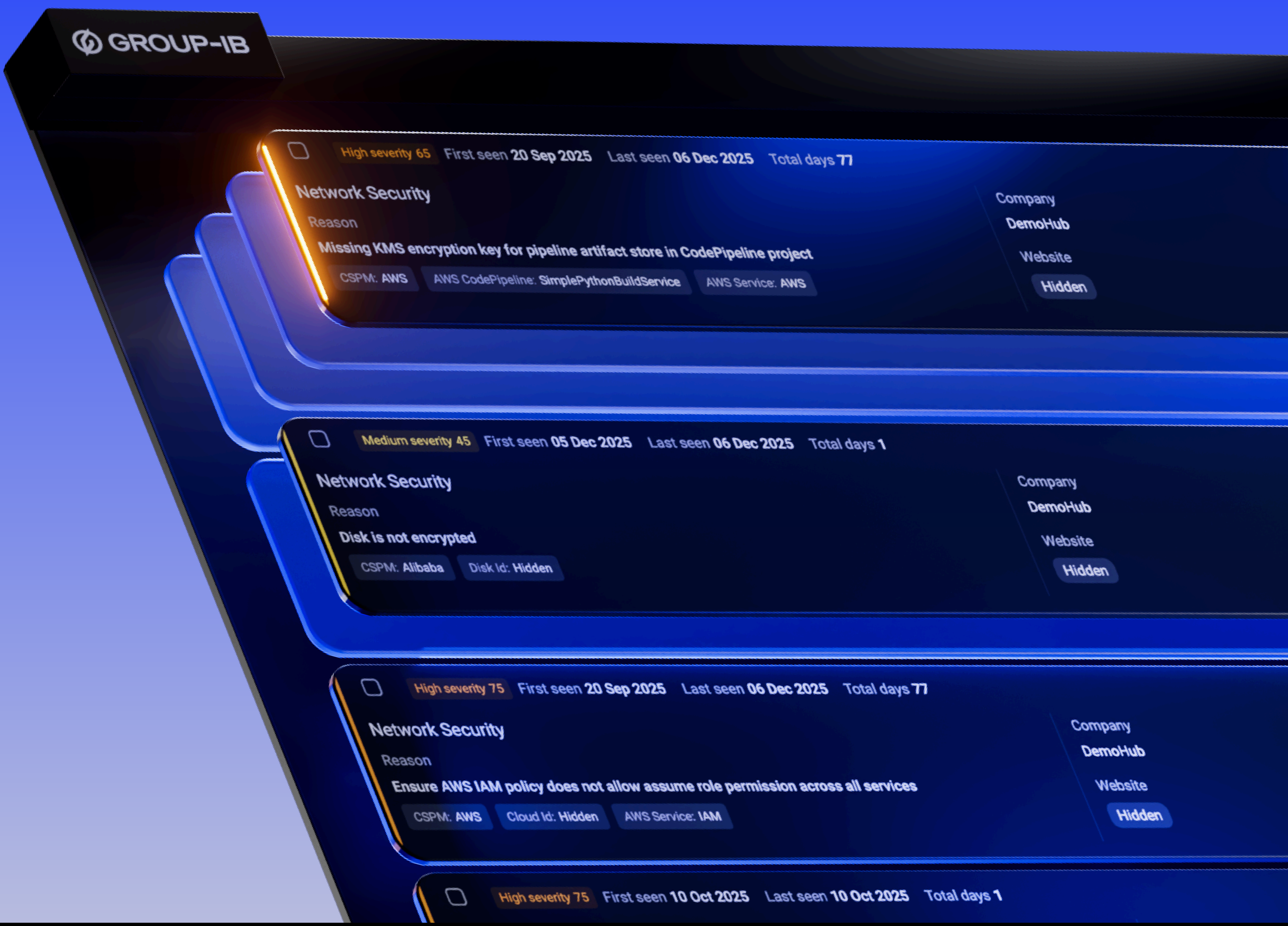

High severity 65 First seen 20 Sep 2025 Last seen 06 Dec 2025 Total days 77

Network Security

Reason

Missing KMS encryption key for pipeline artifact store in CodePipeline project

CSPM: AWS | AWS CodePipeline: SimplePythonBuildService | AWS Service: AWS

Company: DemoHub

Website: Hidden

Medium severity 45 First seen 05 Dec 2025 Last seen 06 Dec 2025 Total days 1

Network Security

Reason

Disk is not encrypted

CSPM: Alibaba | Disk Id: Hidden

Company: DemoHub

Website: Hidden

High severity 75 First seen 20 Sep 2025 Last seen 06 Dec 2025 Total days 77

Network Security

Reason

Ensure AWS IAM policy does not allow assume role permission across all services

CSPM: AWS | Cloud Id: Hidden | AWS Service: IAM

Company: DemoHub

Website: Hidden

High severity 75 First seen 10 Oct 2025 Last seen 10 Oct 2025 Total days 1

Product overview

See the misconfigurations that matter

Cloud Security Posture Management

Make sure your cloud supports speed and scale, not risks. By combining cloud threat visibility, real-world exposure intelligence, and threat context, Group-IB Cloud Security Posture Management (CSPM) reveals and closes critical misconfigurations before attackers exploit them.

Is your cloud as secure as you think it is?

Cloud misconfigurations like open buckets, undefined IAM roles, and exposed secrets are attackers’ easiest way in. Multi-cloud adoption and fast-moving DevOps add to the risk.

- Continuously scan for misconfigurations
- Detect compliance violations (CIS, NIST)
- Prioritize exploitable risks to cut alert fatigue
- Support audits and secure DevOps adoption

Why trust Group-IB for your cloud security?

Typical Cloud Security Posture Management	Group-IB Cloud Security Posture Management
⊗ Lists misconfigurations	✓ Shows which misconfigurations attackers can actually exploit
⊗ Endless alerts — Prioritization becomes a task	✓ Adds exploitability context that gives your team time and clarity to stay ahead of attackers
⊗ No enrichment	✓ Enriched with: • External exposure visibility from Group-IB Attack Surface Management (ASM) • Live attacker infrastructure data from Group-IB Threat Intelligence (TI)
⊗ No additional pipeline-level misconfiguration checks	✓ Checks for CI/CD misconfigurations to secure the software delivery lifecycle
⊗ Requires additional integrations and licenses	✓ All-in-one solution, no hidden costs for ASM and TI usage

How it works

See and act like adversaries in your cloud — and outsmart them with Group-IB Cloud Security Posture Management. Frictionless architecture. Powerful integrations. Real-time clarity on risks that matter.

How Does Group-IB Cloud Security Posture Management Work?

All-in-one solution to fix critical cloud misconfigurations

Connect

01

Fast, agentless setup for a complete multi-cloud view

- API integrations with AWS, Azure, GCP, Alibaba
- Centralized visibility through one portal for all cloud environments.

Google Cloud · aws · Alibaba Cloud · Microsoft Azure

Get complete cloud visibility without disruption

Discover

02

Catch cloud and pipeline risks early

- Automated discovery of IPs, domains, assets, software inventory, and vulnerabilities.
- Additional detection of CI/CD environments like CodeBuild, CodeDeploy, CodePipeline.

Detect DevOps pipeline risks and misconfigurations early on

Map

03

Align risks with compliance frameworks.

- CIS 8.1 and NIST 800-53 mapping
- Risk scoring by severity and asset type
- Export findings for audits with remediation guidance and status.

Stay compliant and audit-ready

Enrich

04

Enrich every finding with exposure and threat intelligence. No additional licenses needed.

- Correlates assets with external visibility from ASM
- Highlights attacker infrastructure using live threat intelligence
- Visual graphs of risk propagation and lateral movement

Prioritize risks that are exploitable

Act

05

Prioritize, fix critical risks, and prove compliance

- Push alerts to SIEM, SOAR, ticketing systems
- Pull posture data (GRC or compliance systems) into audit dashboards
- Automate remediation and track progress

Integrate with your workflows

How do you become compliant?

- ✓ Maps misconfigurations to CIS and NIST out of the box
- ✓ Help you prepare for audits against frameworks like ISO 27001, PCI DSS, or NIS2
- ✓ Gain clear guidance on resolving compliance issues
- ✓ Export structured lists of issues, including their resolution status, for audit purposes.

CIS Controls

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Why choose Group-IB?

Most Cloud Security Posture Management tools stop at discovering misconfigurations. Group-IB CSPM goes further

Capability	Group-IB CSPM	Typical CSPM Vendors
Multicloud posture visibility for AWS, Azure, GCP, Alibaba	✓	✓
Compliance benchmarking against CIS 8.1, NIST 800-53	✓	✓
CI/CD misconfiguration checks in CodeBuild, CodeDeploy, and CodePipeline	✓	✗
Real-world exposure validation of assets from Group-IB Attack Surface Management	✓	✗
Threat infrastructure correlation using Group-IB Threat Intelligence	✓	✗
Risk-based prioritization using exposure and threat context	✓	✗
Software inventory & vulnerabilities	✓	✓

GROUP-IB

Group-IB is a creator of cybersecurity technologies to investigate, prevent and fight digital crime.

1,550+
Successful investigations of high-tech crime cases

500+
Employees

60
Countries

$1 bln+
Saved by our client companies through our technologies

#1*
Incident Response Retainer vendor

*According to Cybersecurity Excellence Awards

11
Unique Digital Crime Resistance Centers

Global partnerships

- INTERPOL
- EUROPOL
- AFRIPOL

Recognized by top industry experts

- FORRESTER
- Aite Novarica
- KuppingerCole ANALYSTS
- Gartner
- IDC
- FROST & SULLIVAN

Fight against cybercrime

GROUP-IB.COM
INFO@GROUP-IB.COM

APAC
+65 3159 4398

EU & NA
+31 20 226 90 90

MEA
+971 4568 1785