



Validate Your Cloud Exposure from Unseen Threats



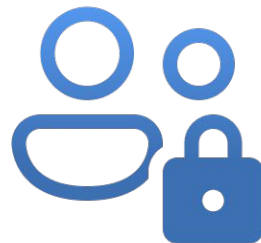
How Would You Know If Your...



Cloud Incident
Response Playbooks



Cloud Security
Mechanisms



Security Team



Security Tools

Will Work Effectively to **Protect Your Cloud & AI** From Cyber Threats?



Many Organizations Are Unprepared for Cyberattacks

93%

Organizations have low cloud security maturity level with minimum cloud security strategy

<https://www.itprotoday.com/cloud-security/companies-lack-capabilities-to-secure-cloud-infrastructure-report>

76%

GenAI initiatives are not yet protected with the necessary security strategy

IBM Cost of a Data Breach Report 2024

59%

Organizations have immature security incident response strategy

Wavestone Cyber Benchmark 2024

58%

Data breaches are unidentified by security teams and tools

IBM Cost of a Data Breach Report 2024



Verify Cloud Resilience with World's First Cloud Adversarial Exposure Validation Platform



Automatically **emulate cloud attacks** with easy-to-use interface based on MITRE ATT&CK & ATLAS frameworks



Discover security blindspots within the cloud security strategy, security team, and security tools during the “cloud attacks”



Improve the mean time to detect and react against potential cloud attacks

The screenshot displays the Mitigant Cloud Attack Emulation interface. At the top, there are logos for AWS, Azure, and Google Cloud, along with a red 'Soon' button. The interface shows a 'Report for Attack Actions - 02 Aug 2024 2:36 AM'. The left sidebar contains navigation options: Dashboard, CSPM, Attack Emulation, Overview, Attack, Scenario, MITRE ATT&CK..., KSPM, Settings, Help, and Sign Out. The main content area shows two attack actions: 'Abuse Elevation Control' and 'Privilege Enumeration', both marked as 'SUCCESS' and 'RECOVERED'. The 'Privilege Enumeration' section details the attack steps, including 'Privilege Enumeration has started', 'Target acquisition in progress', and a list of discovered IAM resources: 61 IAM users, 12 IAM User Groups, 116 IAM Customer Managed Policies, and 728 IAM Roles. The interface also includes a 'Summary' tab and an 'Attack Path Analysis' section on the right.

Onboarding in Just 15 Minutes

Cloud Attack Emulation Functionalities



Agentless & Safe

No agents needed to be installed.
Onboarding and attacks are orchestrated via cloud provider APIs



Plug-and-Play Attacks

All attack actions are plug-and-play that can be easily combined. No need to maintain the attack scripts!



Realistic Attack Emulation

Target environment is enumerated on-the-fly, vulnerable targets are selected & attacked.



Evidence Collection

Attack telemetry is automatically collected for further security analysis.



Automatic Cloud Recovery

Target environments are automatically clean up after emulated cloud attacks.



Comprehensive Reporting

Detailed reports with the related MITRE ATT&CK & MITRE ATLAS Tactics, Techniques and remediation steps.



Cyber Threat Intelligence

Corresponding threat actors are shown due to the integration of CTI.



Attack Path Analysis

The attack paths are visualized to provide clear situational awareness.

Example Cloud Attack Emulation Scenarios



Ransomware Attacks



Privilege Escalation



GenAI Data Poisoning



Data Breaches



LLMJacking

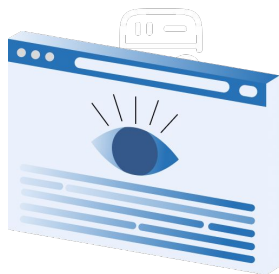


Storage Takeover

How Cloud Attack Emulation Works



Select several attack action(s)
or an attack scenario to be
emulated in the target cloud
environment



Observe how the cloud and the
security team will react under
“the cloud attacks” to discover
security blindspots



Improve incident response
playbook to be better prepared
and resilient against
cyberattacks

Cloud Attack Emulation Use Cases



AI Red Teaming

Ensure cloud GenAI workloads are resilient against potential cyberattacks



Empower Cloud Security Operation Center

Improve time to detect and respond to potential cloud attacks with simplified red/purple teaming capabilities via no-code interfaces



Automated Internal Cloud Penetration Testing

Automate cloud security testing using the Mitigant API, e.g., as an event-based process integrated into a CI/CD pipeline or as part of a custom security workflow



Threat Detection Validation

Ensure implemented security strategy and incident response playbook to work as intended



Cloud Attack Emulation Use Cases

GenAI Red Teaming

Run AI Red Teaming Exercises

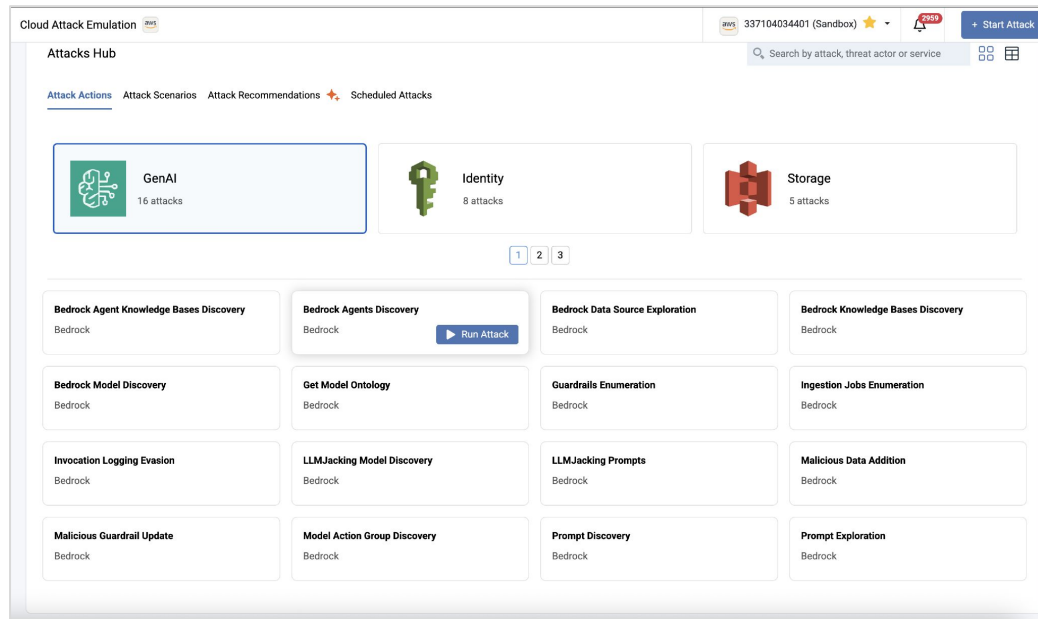
Select and execute attacks against GenAI infrastructure, aligned with the MITRE ATLAS.

Ensure Responsible AI

Implement attacks that mirror AI threats with impact on privacy, abuse the system capabilities and have security implications.

Extend AI Security Posture

Leverage the integrated GenAI configuration checks and asset inventory to make informed decision such as contextual attacks.





Cloud Attack Emulation Use Cases

Automated Internal Cloud Penetration Testing

Automated Cloud Security Testing

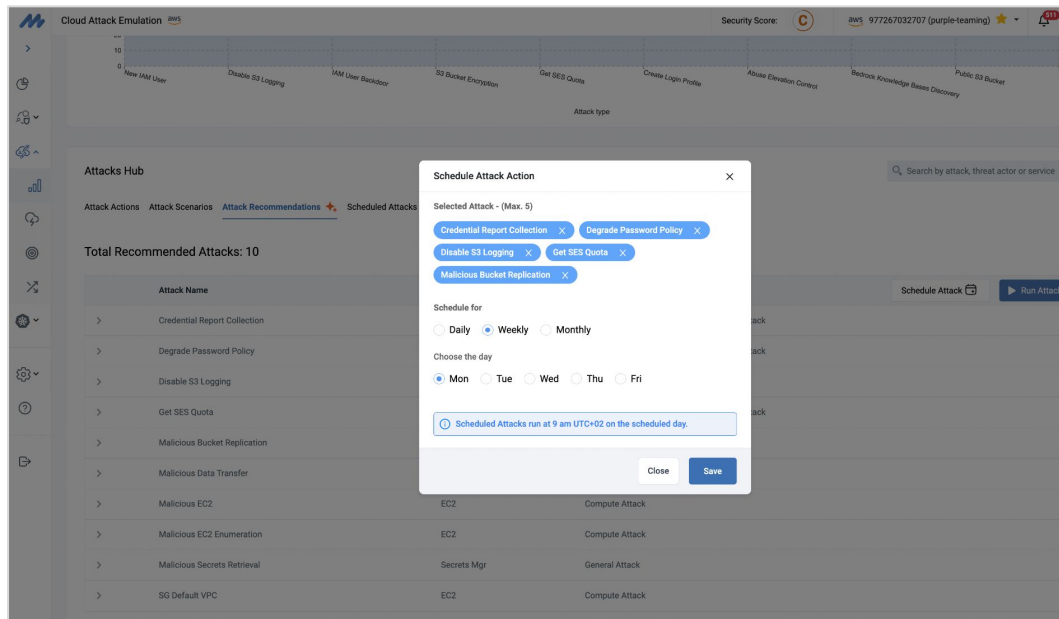
Run cloud penetration testing with customized attack actions and scenarios.

Attack Emulation Anytime Anywhere

Flexibly schedule attacks based on your threat model and continuously validate your cloud security assumptions.

Multi-Cloud Attack Emulation

Simultaneously attack multiple cloud accounts to verify multi-cloud's cyber resilience posture.





Cloud Attack Emulation Use Cases

Empower Cloud Security Operation Center

Easily Emulate Cloud Threats

Simplify red/purple teaming cloud exercises via drag-and-drop interface with low learning curve.

Automated Cloud Attack Telemetry Collection

Collect cloud log entries as attack evidences to discover cloud security blind spots.

Easily Integrate Mitigant API

Integrate with other security operations tools using the provided API to gain further insights and perspectives of cloud resilience posture.

Report for Guardrail Disruption - 16 Aug 2024 3:28 PM

Guardrail Disruption has started. Guardrail Disruption has 2 attack actions.

Attack Action	Service	Status	Progress	Action
Guardrails Enumeration	AWS Service Bedrock	SUCCESS	0.7s	RECOVER
Malicious Guardrail Update	AWS Service Bedrock	SUCCESS	1.2s	RECOVER

ATT&CK Tactic: ML Attack Staging

ATT&CK Technique: Craft Adversarial Data

Attack Steps: Attack Remediation, Attack Evidence, Attack Detection

- Starting attack 2: Malicious Guardrail Update.
- Target acquisition in progress.
- Validating attack preconditions.
- Selected guardrail r2h61dyej2ah
- Content policy before update

```
{
  "Filters": {
    "0": {
      "Type": "WHITE",
      "InputStrength": "MEDIUM",
      "OutputStrength": "MEDIUM"
    }
  },
  "2": {
    "Type": "WHITE",
    "InputStrength": "MEDIUM",
    "OutputStrength": "MEDIUM"
  },
  "3": {
    "Type": "WHITE",
    "InputStrength": "MEDIUM",
    "OutputStrength": "MEDIUM"
  },
  "4": {
    "Type": "WHITE",
    "InputStrength": "MEDIUM",
    "OutputStrength": "MEDIUM"
  },
  "5": {
    "Type": "WHITE",
    "InputStrength": "MEDIUM",
    "OutputStrength": "MEDIUM"
  }
}
```

Summary: Attack Path

Start Time	End Time	Duration	Status
16 Aug 2024 3:28 PM	16 Aug 2024 3:28 PM	2.0s	COMPLETED

Executed by: res rrs

Executed via: Web-App

Attack Objective: Validate the effect of a maliciously altered guardrail

Observations: The agent responded using hate speech, but the AWS GuardDuty did not detect the malicious changes.

Recover Attack



Cloud Attack Emulation Use Cases

Threat Detection Validation

Easily Emulate Cloud Threats

Continuously run cloud attacks aligned with the MITRE ATT&CK and MITRE ATLAS frameworks without writing a single line of code.

Improve Threat Detection Strategy

Quickly identify detection gaps and blind spots to improve cloud threat's responsiveness

Adopt Threat-Informed Defense Strategy

Implement validated security measures based on Cyber Threat Intelligence

● S3 Ransomware (Policy) has started. ● S3 Ransomware (Policy) has 3 attack actions.

✔

New IAM User ↗

AWS Service:IAM

SUCCESS 0.9s

RECOVERED

ATT&CK Tactic

Persistence

ATT&CK Technique

Create Account

Attack Steps

Attack Remediation

Attack Evidence

Attack Detection

title: AWS IAM Backdoor Users Keys

id: 0a5177f4-6ca9-44c2-aacf-d3f3d8b6e4d2

status: test

description: |

Detects AWS API key creation for a user by another user.

Backdoored users can be used to obtain persistence in the AWS environment.

Also with this alert, you can detect a flow of AWS keys in your org.

references:

- https://github.com/RhinoSecurityLabs/pacu/blob/866376cd711666c775bbfcd8524c817f2c5b181/pacu/modu

author: faloker

date: 2020/02/12

modified: 2022/10/09

tags:

- attack.persistence

- attack.t1098

logsource:

product: aws

service: cloudtrail

detection:

selection_source:

eventSource: iam.amazonaws.com

eventName: CreateAccessKey

filter:

userIdentity.arn[contains: responseElements.accessKey.userName

condition: selection_source and not filter

fields:

- userIdentity.arn

- responseElements.accessKey.userName

- errorCode

- errorMessage

falsePositives:

- Adding user keys to their own accounts (the filter cannot cover all possible variants

of user naming)

- AWS API keys legitimate exchange workflows

level: medium

Summary

Attack Path

Start Time

End Time

Duration

Status

23 May 2025 11:42 AM

23 May 2025 11:42 AM

16.8s

COMPLETED

Executed by

Executed via

MIT Mitigant Tester

Web-App

Attack Objective

Edit

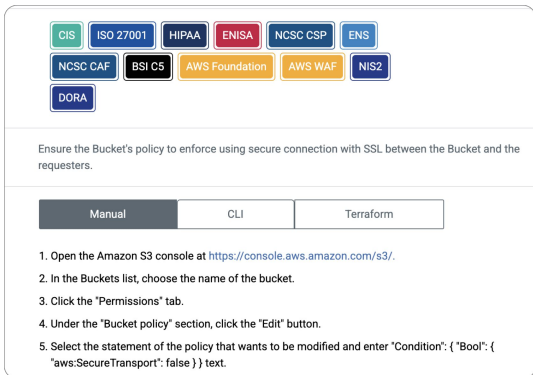
Enter your attack objective

Observations

Edit

Enter the observations

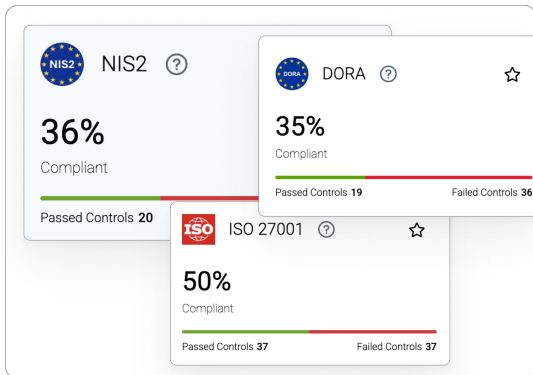
Additional Features to Secure Your Clouds & AI



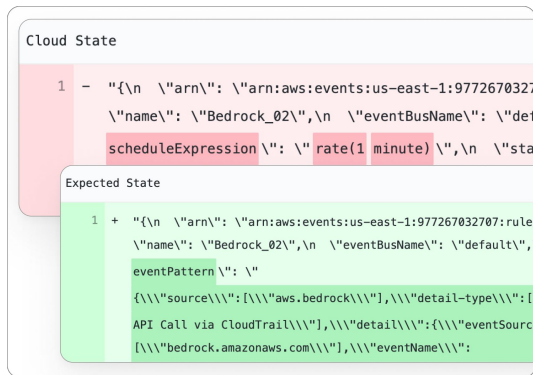
The screenshot displays a dashboard with various compliance frameworks: CIS, ISO 27001, HIPAA, ENISA, NIS2, NCSC CSP, ENS, NCSC CAF, BSI CS, AWS Foundation, AWS WAF, and DORA. Below the frameworks, a text instruction reads: "Ensure the Bucket's policy to enforce using secure connection with SSL between the Bucket and the requesters." There are three tabs: Manual, CLI, and Terraform. The Manual tab is selected, showing a 5-step guide for configuring Amazon S3 bucket policy.

1. Open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the Buckets list, choose the name of the bucket.
3. Click the "Permissions" tab.
4. Under the "Bucket policy" section, click the "Edit" button.
5. Select the statement of the policy that wants to be modified and enter "Condition": {"Bool": {"aws:SecureTransport": false}} text.

Detect and remediate cloud security vulnerabilities due to misconfigurations and compliance violations



Achieve compliance with cloud and AI security regulations and best practices



The screenshot displays two panels: "Cloud State" and "Expected State". The "Cloud State" panel shows a configuration for an AWS CloudTrail rule with a schedule expression of "rate(1 minute)". The "Expected State" panel shows the same configuration with additional details like "source" and "detail-type".

```
1 - "{\n  \"arn\": \"arn:aws:events:us-east-1:977267032707:rule,\n  \"name\": \"Bedrock_02\",\n  \"eventBusName\": \"default\",\n  \"scheduleExpression\": \"rate(1 minute)\",\n  \"state\": \"ENABLED\"}"
```

```
1 + "{\n  \"arn\": \"arn:aws:events:us-east-1:977267032707:rule,\n  \"name\": \"Bedrock_02\",\n  \"eventBusName\": \"default\",\n  \"eventPattern\": {\n    \"source\": [\"aws.bedrock\"],\n    \"detail-type\": [\"API Call via CloudTrail\"],\n    \"eventSource\": [\"bedrock.amazonaws.com\"],\n    \"eventName\": [\"\"]\n  }\n}"
```

Complete cloud security visibility for unwanted changes in cloud resources



Who Must Use Cloud Attack Emulation

✓ CISO

Plan cloud security exercises and observe how cloud and security team will behave during cloud security testing

✓ SOC Team

Automatically and safely run cloud security exercises by emulating cloud attack scenarios






✓ Detection Engineer

Ensure suspicious activities from the cloud attack emulation run can be detected with security monitoring systems

✓ Cloud Security Engineer

Improve cloud security strategy and measures based on the cloud attack emulation reports

The Only Proactive Cloud-Native Adversarial Exposure Validation Platform

	Agentless	Cloud Attack Emulation	CSPM & KSPM	Attack Path Analysis	Detection Validation	CI/CD Integration
	✓	✓	✓	✓	✓	✓
 XM Cyber	✓	✗	✓	✓	✗	✗
ATTACKIQ [®]	✗	✗	✗	✗	✗	✗
 cymulate	✓	✗	✓	✓	✗	✗
 PICUS	✓	✓	✗	✓	✗	✗
 SafeBreach	✗	✓	✗	✗	✗	✗

Some of Trusted Customers



adesso

GRENKE

 VERTAMA

VALUEWORKS
INSIGHTS TO RESULTS

mitto

 TechMiners

!KM.ON
by KARL MAYER

 **MontBlancAI**



Our Mission: Building Trust in Digital Transformation with Mitigant



Nils Karn

Chief Executive Officer

nils@mitigant.io

(+49) 331 971 83 007

