Mandiant

CLOUD VALIDATION MODULE AND CLOUD ACTIONS OVERVIEW

Security Validation's Cloud Validation Module lets you continuously validate the configuration in your cloud environment against both traditional and cloud attacks. This module offers the following validation capabilities:

- Execution of targeted Actions against and inside supported cloud provider environments
- Verification of cloud infrastructure monitoring and reporting capabilities through multiple cloud integrations, such as AWS CloudTrail
- Execution of cloud-specific tactics and techniques using real attack behaviors
- Verification of the configuration of cloud-hosted capabilities around access control and real time monitoring of unauthorized entry into cloud storage by running authenticated and unauthenticated requests across an environment

The following are examples of configuration vulnerabilities that Cloud Validation Module can help you detect:

- Publicly accessible S3 buckets
- Publicly accessible databases
- Publicly accessible backups
- Unencrypted backups

Cloud Actions

Cloud Actions are designed to validate cloud security controls. They are created by writing Python scripts that interact with cloud APIs, using the Python SDKs for AWS (boto3), Azure, or Google Cloud. Cloud Actions correlate events from cloud security controls with those API interactions. Identifiers such as request IDs are automatically collected. The Python script defines the action result (blocked or not) and, optionally, returns additional correlation identifiers for event matching.

When running a Cloud Action, you can use a Cloud Profile to provide credentials. Cloud Actions use up to three Cloud Profiles to do the following test steps:

- Setup
- Test
- Cleanup

Because changes are temporarily made in the cloud environment, the setup and cleanup steps generally need administrative permissions to do the cleanup activities.

Cloud Validation includes a special content pack that contains Cloud Actions, and you can create your own. For more information, see the following topics:

- **Cloud Profiles** (https://docs.mandiant.com/home/msv-cloud-profiles)
- **Adding Cloud Actions** (https://docs.mandiant.com/home/adding-cloud-actions)
- **Running Cloud Actions** (https://docs.mandiant.com/home/msv-running-cloud-actions)

The following table includes the lists of integrations that are supported and their capabilities:

	Cloud Action Pack	Azure Actions	Google Cloud Actions	AWS Actions
AWS CloudTrail (https://docs.mandiant.com/home/msv-aws-cloudtrail)	✔			✔

	Cloud Action Pack	Azure Actions	Google Cloud Actions	AWS Actions
AWS GuardDuty (https://docs.mandiant.com/home/msv-aws-guardduty)	✔			✔
Azure Log Analytics (https://docs.mandiant.com/home/msv-microsoft-azure-log-analytics)	✔	✔		
Google Cloud Logging (https://docs.mandiant.com/home/msv-google-cloud-logging)	✔		✔	