Agile and Keyless Cloud Security Response

Benefits

- Orchestrate cloud security monitoring, enrichment, and response actions through playbooks.
- Avoid credential management through seamless use of IAM roles for API integrations.
- Reduce time to resolution by using one platform to collaborate, investigate, and document.

Compatibility

- Products: Demisto Enterprise, Amazon EC2, Amazon GuardDuty, AWS IAM, Amazon Route 53, Amazon S3, Amazon SQS, Amazon CloudWatch Logs, AWS Security Hub, AWS CloudTrail
- Platform: Platform independent

Cloud adoption has heralded a new age of business and technology, as organizations share compute, storage, and infrastructure resources to innovate and scale. But these developments have brought with them their own set of security hurdles to overcome.

From an incident response standpoint, cloud security data and processes are often isolated from traditional security measures, requiring multiple consoles to manage overall security posture. The disparate environments resulting from rapid cloud provisioning and multiple cloud security products also leads to a lack of visibility. Finally, from an operations standpoint, managing service credentials is a time-consuming and potentially dangerous exercise. Since each service needs keys or passwords to call different sets of APIs, the ensuing credential transfer and storage can result in exposed assets that attackers can exploit for lateral movement and compromise.

Demisto's security orchestration and automation capabilities can now be used to deploy and manage a variety of AWS services in a keyless and secure manner. Even the most complex AWS environments can be unified with traditional security measures via Demisto for repeatable and scalable cloud security incident response.

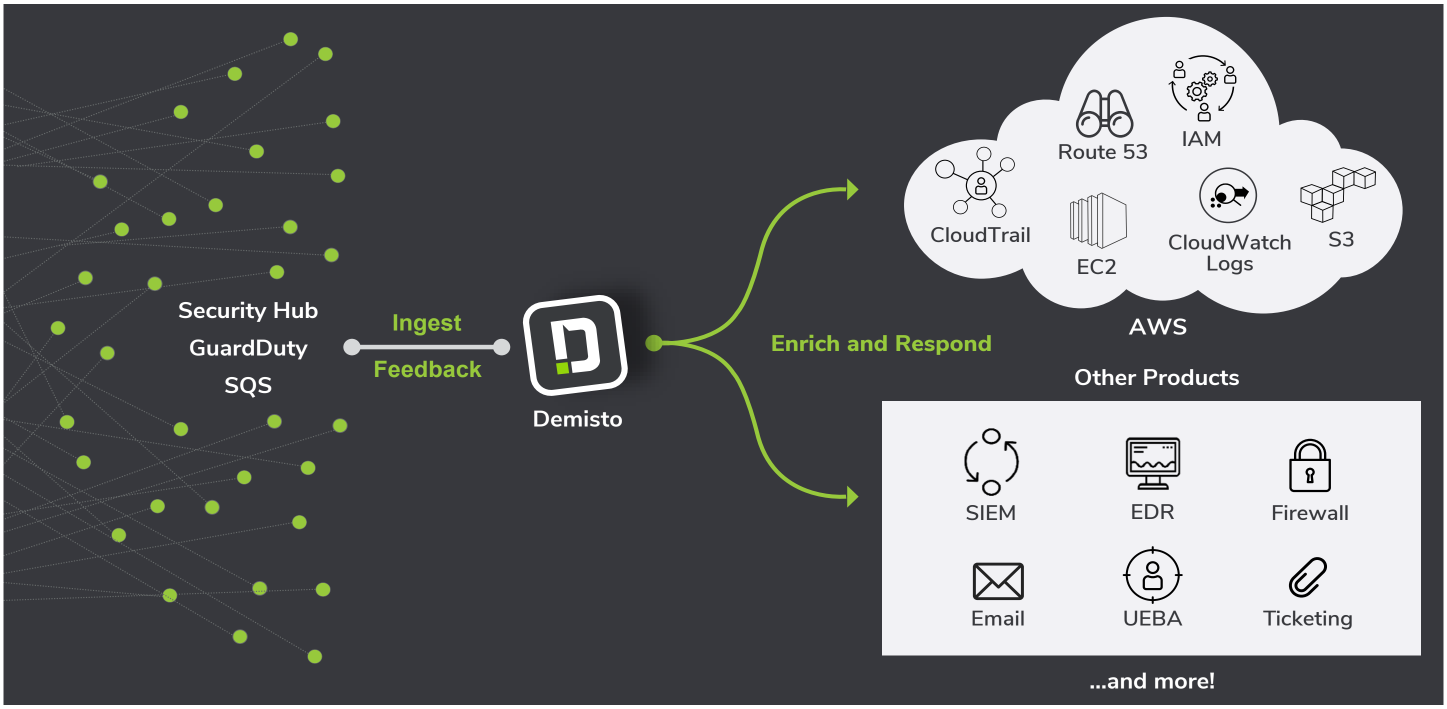
Orchestrate cloud security

Execute keyless automation

Unify security functions

Integration features

- Ingest aggregated alert data from AWS Security Hub, Amazon GuardDuty, and Amazon Simple Queue Service (SQS) to create incidents in Demisto and trigger automated playbooks tied to those incidents.
- Leverage AWS IAM roles for securely automating tasks without credentials or API keys.
- Access and edit log groups and policies from Amazon CloudWatch Logs within Demisto, either as automated playbook tasks or in real-time.
- Obtain event history of AWS account activity from AWS CloudTrail within Demisto.
- Execute tasks tied to management of S3, EC2, and SQS from Demisto.
- Capture DNS information from Route 53 through automated tasks run on Demisto.
- Leverage hundreds of Demisto product integrations to further enrich AWS alerts and coordinate response across security functions.
- Run thousands of commands (including for AWS) interactively via a ChatOps interface while collaborating with other analysts and Demisto's chatbot.

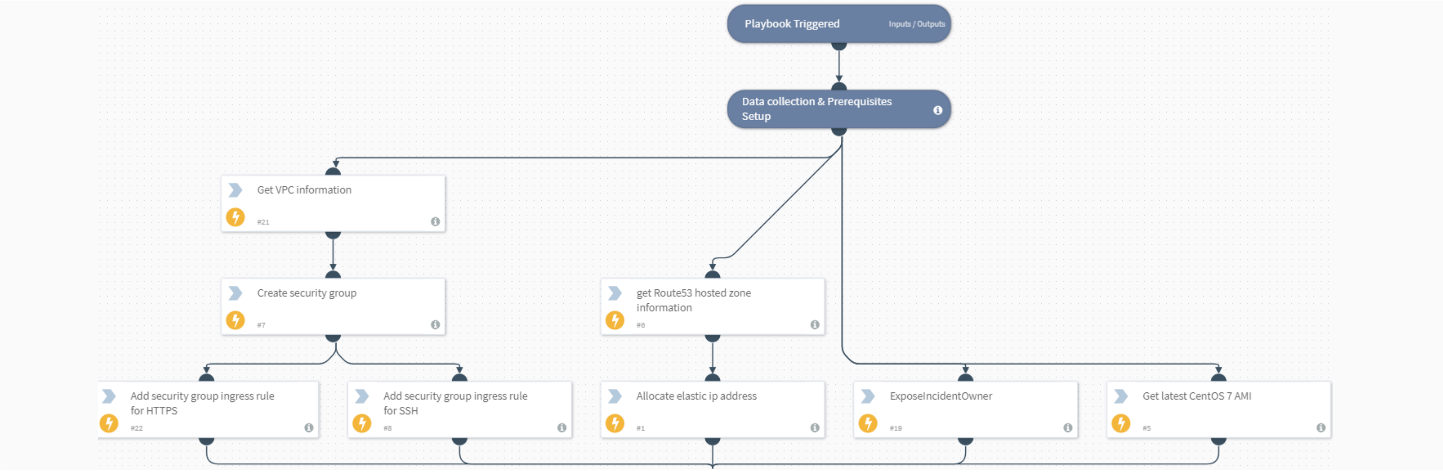


USE CASE #1 AUTOMATED ENRICHMENT AND RESPONSE FOR CLOUD SECURITY INCIDENTS

Challenge: If cloud security consoles are isolated from other functions such as EDR, malware analysis, and threat intelligence, it becomes time-consuming and repetitive for security analysts to cross-reference alerts from cloud security tools, get further context, and coordinate containment and response. Processes diverge depending on the analyst that handles the incident, and this leads to differing response quality.

Solution: Analysts can use the AWS Security Hub, Amazon GuardDuty, or Amazon SQS integrations to ingest alert data, create incidents in Demisto, and trigger standardized, automated playbooks for responding to those incidents. These playbooks can enrich the alert with more event details from GuardDuty, DNS information from Route 53, log information from Amazon CloudWatch Logs, and many other actions from AWS services. Playbooks can also coordinate across hundreds of other products to extract wider context without the need for screen switching and manual repetition.

For example, a playbook could query GuardDuty for IP sets, use Route 53 for domain information, and retrieve message queues from SQS before updating bucket policies from S3 and deleting instances from EC2 as response actions.

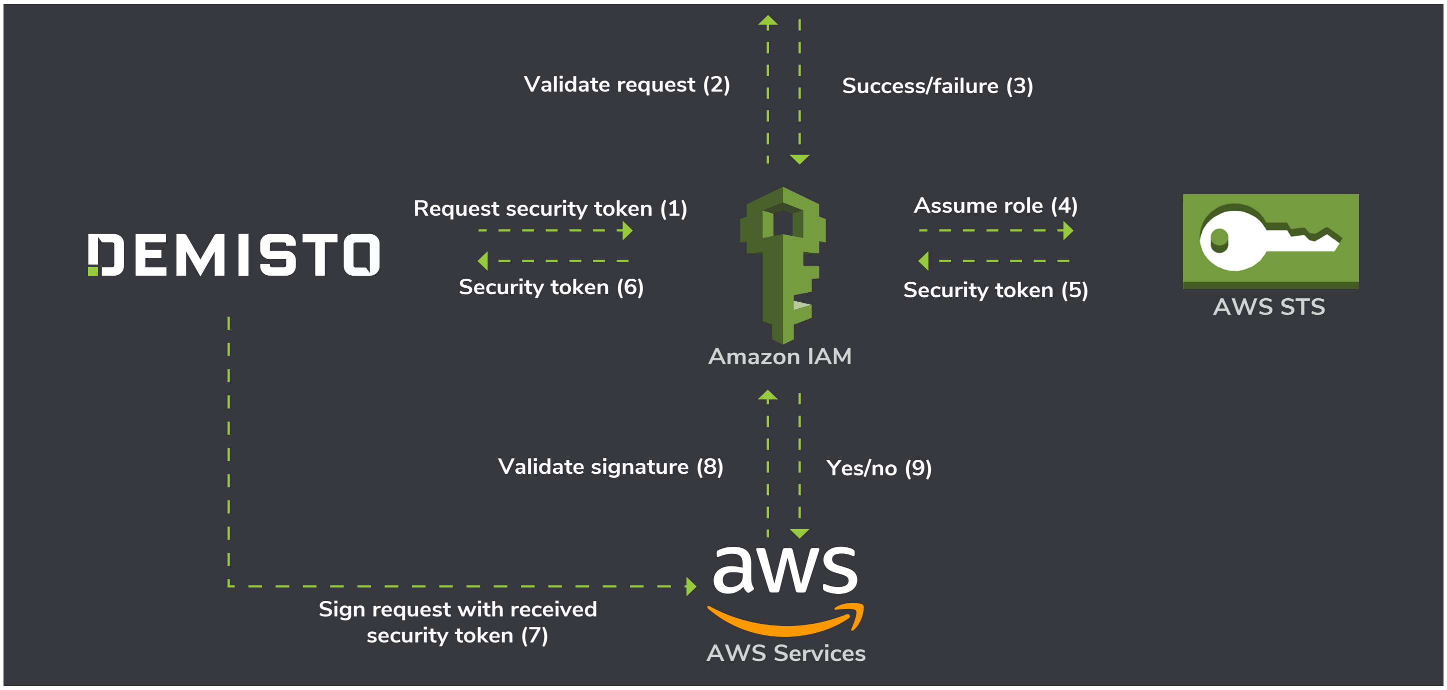

Playbook Triggered
Inputs / Outputs
Data collection & Prerequisites Setup
Get VPC information
#21
Create security group
#7
get Route53 hosted zone information
#6
Add security group ingress rule for HTTPS
#22
Add security group ingress rule for SSH
#8
Allocate elastic ip address
#1
ExposeIncidentOwner
#19
Get latest CentOS 7 AMI
#5

Benefit: Aggregating AWS data across products and executing actions from a central console can save screen switching time. Orchestrating other product actions in the same window can also help analysts coordinate across security functions for richer and more comprehensive incident context.

USE CASE #2 KEYLESS AUTOMATION OF TASKS FOR ZERO-TRUST SECURITY

Challenge: Using static credentials tied to AWS services is an exercise that poses potential business and security risk. Securely passing the credentials among teams during hand-offs, managing the keys for each app at a central location, and ensuring that external forces don't get access to these credentials are all exercises that involve additional work and don't represent the most secure option.

Solution: Demisto's integration with AWS Identity and Access Management (IAM) enables users and automated playbooks to access AWS services in a secure and keyless manner. Users can leverage IAM roles from within Demisto, attach privileges and users to those roles, execute automated actions through playbooks tied to those roles without the need for credential storage and transfer.



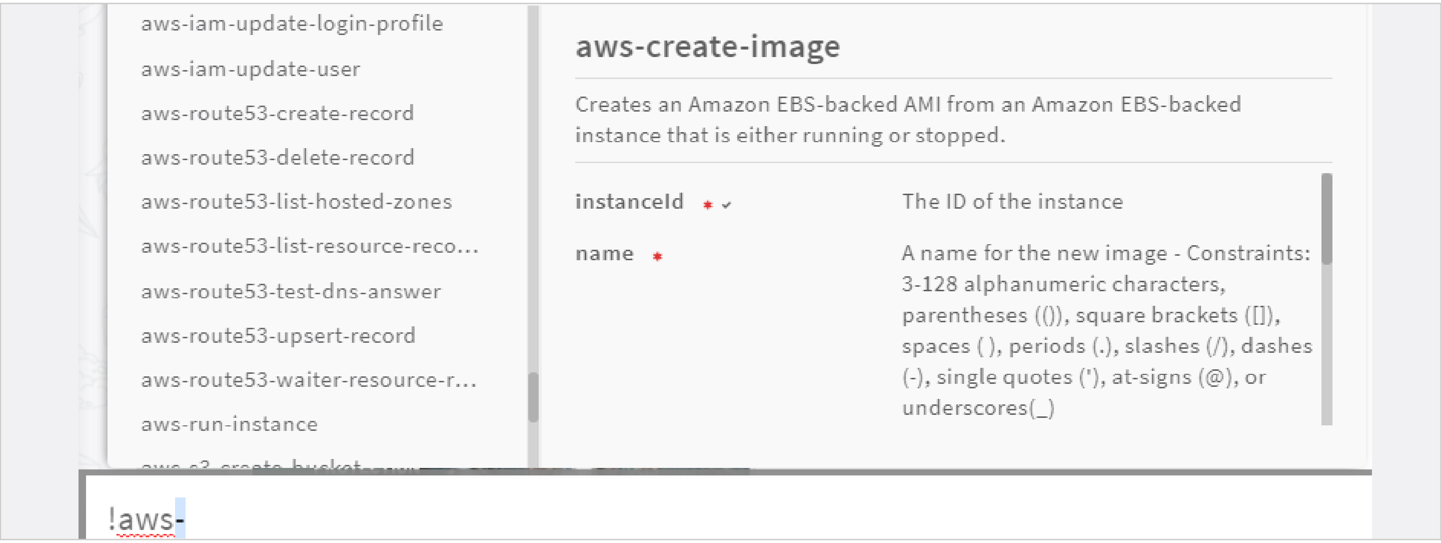
Benefit: A keyless approach ensures that no credentials slip through the cracks onto external domains, thus minimizing the possibilities of attacks perpetrated through weak credential management. Enterprises can continue to leverage the benefits of actioning complex AWS environment use cases through automation without sacrificing the granular role-based security of AWS services.

USE CASE #3 INTERACTIVE, REAL-TIME INVESTIGATION FOR COMPLEX THREATS

Challenge: While standardized, repeatable playbooks can automate commonly performed tasks to ease analyst load, an attack investigation usually requires additional tasks such as pivoting from one suspicious indicator to another to gather critical evidence, drawing relations between incidents, and finalizing resolution. Running these commands traps analysts in a screen-switching cycle during investigation and a documentation-chasing cycle after investigations end.

Solution: After running enrichment playbooks, analysts can then gain greater visibility and new actionable information about the attack by running AWS commands in the Demisto War Room. For example, if playbook results throw up alert details, analysts can get the GuardDuty detector tied to the alert or the list of IAM users affected by the alert in real-time. Analysts can also run commands from other security tools in real-time using the War Room, ensuring a single-console view for end-to-end investigation.

The War Room will document all analyst actions and suggest the most effective analysts and command-sets with time.



aws-iam-update-login-profile
aws-iam-update-user
aws-route53-create-record
aws-route53-delete-record
aws-route53-list-hosted-zones
aws-route53-list-resource-reco...
aws-route53-test-dns-answer
aws-route53-upsert-record
aws-route53-waiter-resource-r...
aws-run-instance
aws-s3-create-bucket

aws-create-image

Creates an Amazon EBS-backed AMI from an Amazon EBS-backed instance that is either running or stopped.

instanceId *	The ID of the instance
name *	A name for the new image - Constraints: 3-128 alphanumeric characters, parentheses (()), square brackets ([]), spaces ( ), periods (.), slashes (/), dashes (-), single quotes ('), at-signs (@), or underscores(_)

```
!aws-
```

Benefit: The War Room allows analysts to quickly pivot and run unique commands relevant to incidents in their network from a common window. All participating analysts will have full task-level visibility of the process and be able to run and document commands from the same window. They will also prevent the need for collating information from multiple sources for documentation.

About Demisto

Demisto is the only Security Orchestration, Automation, and Response (SOAR) platform that combines security orchestration, incident management, and interactive investigation to serve security teams across the incident lifecycle. Our orchestration engine coordinates and automates tasks across 100s of partner products, resulting in an increased return on existing security investments. Demisto enables security teams to reduce Mean Time to Response (MTTR), create consistent incident management processes, and increase analyst productivity. For more information, visit www.demisto.com or follow @demistoinc on Twitter.