Indicator of Misconfiguration Playbook (CrowdStrike CSPM)

Last updated by | Ear, Kevin | Jan 9, 2026 at 10:51 AM EST

This playbook outlines the procedures for responding to Indicators of Misconfiguration (IOMs) identified by CrowdStrike's Cloud Security Posture Management (CSPM) for Azure. IOMs represent deviations from security best practices and compliance benchmarks, increasing your cloud environment's risk exposure.

Purpose:
This playbook aims to standardize the incident response process for investigating and remediating IOMs, minimizing risk, and improving overall security posture.

Scope:
This playbook applies to all IOMs generated by CrowdStrike Falcon Cloud Security for Azure.

Current State: All alerts going to our Cloud Security Shared Mailbox are only ***Critical*** or ***High*** alerts from CSPM.

Future State: ***Critical*** and ***High*** alerts will generate a ServiceNow ticket and be auto-assigned to our Cloud Security Shared Mailbox.

Definitions:

- **IOM (Indicator of Misconfiguration):** A finding reported by CrowdStrike CSPM indicating a deviation from a defined security benchmark or best practice.
- **Severity:** IOMs are categorized by severity (Critical, High, Medium, Low) based on their potential impact.
- **Remediation:** The process of correcting the misconfiguration identified by the IOM.
- **False Positive:** An IOM that is incorrectly flagged as a misconfiguration.

Process Flow:

1. **IOM Detection:** CrowdStrike Falcon Cloud Security detects and reports IOMs.
2. **Notification:** The cloud security team are notified of new IOMs via (Email)

3.Triage and Validation:

- Review the IOM details in the Falcon console, including the affected resource, the specific misconfiguration, and the recommended remediation steps.
- Determine the severity of the IOM.
- Investigate the IOM to validate its accuracy. Check if the resource is indeed misconfigured and if the reported issue is genuine.

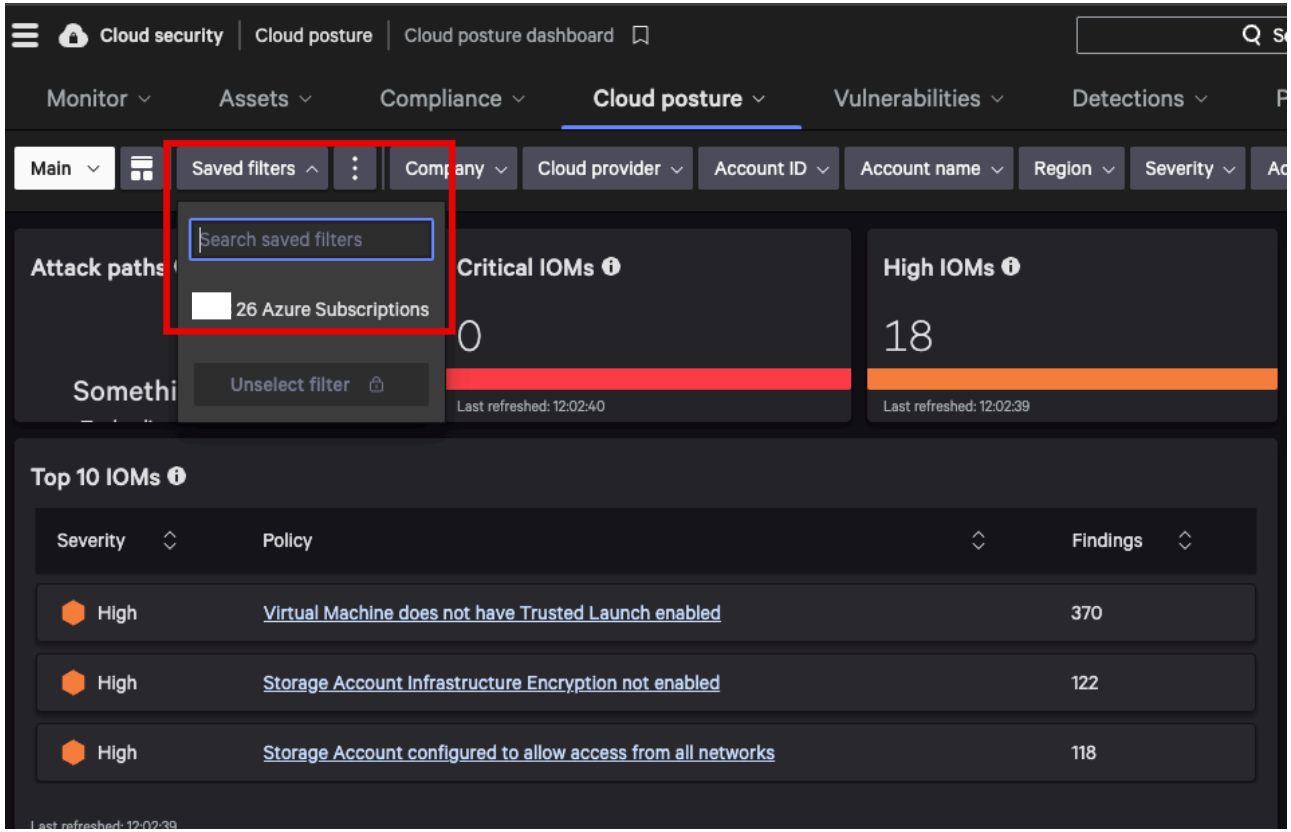
4. Remediation:

- **Manual Remediation:** follow the recommended remediation steps provided by CrowdStrike. Document the manual remediation steps taken.

2. Leverage CrowdStrike to download an export of the misconfigured resources that violates a specific policy

- Ex: Policy: Virtual Machines does not have Trusted Launch Enabled

Note: CrowdStrike Dashboard currently gets data from ALL Azure subscriptions
If we want only azure subscriptions, you may need to create a filter and select all the EHC subscriptions and then save the filter. You can find the list of subscriptions here



- To get an export of the resources, click on the specific policy

- Click on export
- Download and take the "Resource ID" column and clean it up by sorting the individual data points into their own column. You can use excel or whichever method you prefer.

- We will need to pass this data along to the team that needs to be involved. After obtaining all of the data in the "Resource ID" column and cleaning it up, data sheet should look like this

Subscription	Resource Group	Provideres	Virtual Machine
37f6e145-e909-4aff-87a6-f76ddc23ad76	zhe2-hub-addc-rg-sbx	microsoft.compute	zhe2wscsdcsm001
37f6e145-e909-4aff-87a6-f76ddc23ad76	zhe2-hub-addc-rg-sbx	microsoft.compute	zhe2wscsdcsm002
37f6e145-e909-4aff-87a6-f76ddc23ad76	zhe2-hub-testvm-rg-sbx	microsoft.compute	zhe2lteptest001
37f6e145-e909-4aff-87a6-f76ddc23ad76	zhe2-hub-testvm-rg-sbx	microsoft.compute	zhe2wteptest001
458417d6-bddc-4326-a2bb-36f4d1b62e01	gic-testing	microsoft.compute	zhe2lnnegicg001

Email template for IOMs:

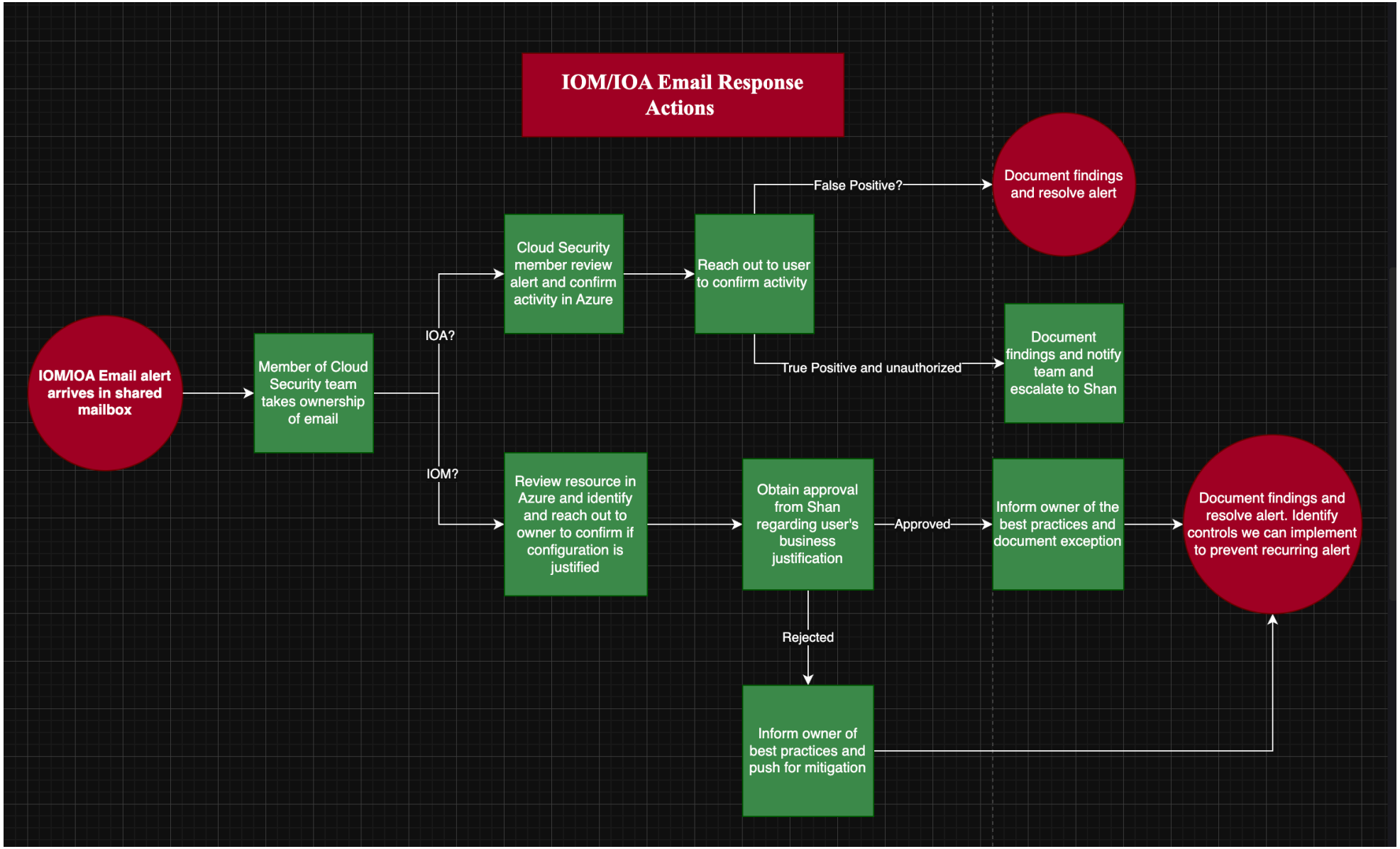
Identifying owners and reaching out to confirm ownership

```
Hi user(

    I am from the                Cloud Security Team. I'm reaching out to identify owners of these misconfigured resources and provide remediation steps. Please evaluate the recommendation and determi


      -Recommendation steps:
      -Step 1:


  Please let us know if you have further questions and we will be happy to answer.
```


IOM/IOA Email Response Actions
IOM/IOA Email alert arrives in shared mailbox
Member of Cloud Security team takes ownership of email
IOA?
IOM?
Cloud Security member review alert and confirm activity in Azure
Reach out to user to confirm activity
False Positive?
Document findings and resolve alert
True Positive and unauthorized
Document findings and notify team and escalate to Shan
Review resource in Azure and identify and reach out to owner to confirm if configuration is justified
Obtain approval from Shan regarding user's business justification
Approved
Inform owner of the best practices and document exception
Document findings and resolve alert. Identify controls we can implement to prevent recurring alert
Rejected
Inform owner of best practices and push for mitigation