Indicator of Attack (IOA) Playbook - CrowdStrike CSPM

Last updated by | Ear, Kevin | Jan 9, 2026 at 11:08 AM EST

This playbook outlines the steps to investigate and respond to Indicator of Attack (IOA) findings identified by CrowdStrike's Cloud Security Posture Management (CSPM) for Azure. IOAs represent suspicious activities that, while not definitively malicious, suggest potential attacks or misconfigurations that warrant investigation.

Purpose: This playbook aims to provide a standardized process to triage, analyze, and respond to IOAs, minimizing potential damage and improving the organization's security posture.

Scope: This playbook covers IOAs related to Azure resources monitored by CrowdStrike CSPM.

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 assigned to our Cloud Security Shared Mailbox.

Prerequisites:

- Access to the CrowdStrike Falcon console.
- Access to Azure portal with appropriate permissions.
- Familiarity with Azure services and resources.
- Knowledge of incident response procedures.

Alerting:

- IOA alerts are sent to our shared mailbox
- IOA alerts (Critical, High, or Medium) will automatically create a ServiceNow incident (coming soon)

IOA Severity Levels:

- **Critical:** Indicates a high probability of an active attack or a significant security vulnerability. Requires immediate action.
- **High:** Suggests a potential attack or a serious security risk. Requires prompt investigation and response.
- **Medium:** Represents a moderate security concern that needs to be addressed.
- **Low:** Indicates a minor security issue or a misconfiguration that should be reviewed and fixed.

Playbook Steps:

1. **Triage and Initial Assessment:**

- **Review the IOA Details:** In the Falcon console or the team's shared mailbox, review the details of the IOA, including:
  - **IOA Name:** The name of the specific IOA triggered.
  - **Severity:** The severity level assigned to the IOA.
  - **Affected Resource(s):** The Azure resource(s) impacted by the IOA.
  - **Description:** A description of the suspicious activity.
  - **Recommendations:** CrowdStrike's recommended actions.
- **Initial Validation:** Perform basic checks to validate the IOA. For example, if the IOA relates to a suspicious log-in, check the sign-in logs.

2. **Initial Investigation**

- **Gather Context:** Collect additional information about the affected resource(s) and the suspicious activity.

- **Analyze the Evidence:** Analyze the collected data to understand the nature of the suspicious activity. Is it a false positive? Is it a misconfiguration? Or is it a sign of an actual attack?

3. **Response and Remediation**:

- **Escalation to TVM team:** If the investigation suggests an active attack, take immediate steps to escalate by sending an email to securityalerts@ and include details about the alert.

- If the alert doesn't suggest an active attack, please reach out to the user who triggered the alert to confirm if the behavior was legitimate. (Example Below) ;

IOA email template:

```
Hi user

    We are reaching out from the Emory's Cloud Security Team. We were alerted by our cloud posture management tool regarding activity relating to your account. Please confirm the activity.

      -Include alert details
      -Include the resource details (storage account, VM, key vault, etc) involved
      -Include a date/time stamp

  Can you kindly confirm if this activity is legitimate business activity?
```

Please copy our shared mailbox in communications to the end-users for visibility

Documentation:

- Document all medium, high, and critical alerts that you investigate in the cloud tracker using the URL

Document the following information.

- Timestamps of event (date and time)
- Actor UPN or Object ID
- Alert Source
- Source Event URL (if available)
- ServiceNow ticket (if available)

Informational and lows alerts should still be reviewed but it is not necessary to enter it into the tracker above

Common IOA Alerts:

1. **False Positives Due To J2C Testing**

- Often times, the users triggering some of the critical/high alerts are from our Accenture J2C project team, who will be actively working/testing in the Azure environment until the end of 2025 to assist with the migration to Azure.

2. **User Applied "Global Administrator" Role in Entra ID**

- This alert will trigger if a user elevates their Global Admin PIM role. Important to verify with user who trigger this alert. Often times, it is legitimate and authorized but a quick email and team's message for confirmation is required.

3. **User applied "Owner" role to themselves at the Subscription level**

- This alert will trigger if a user assigned themselves Owner role at Subscription level. Important

4. **Successful high-risk sign-in**

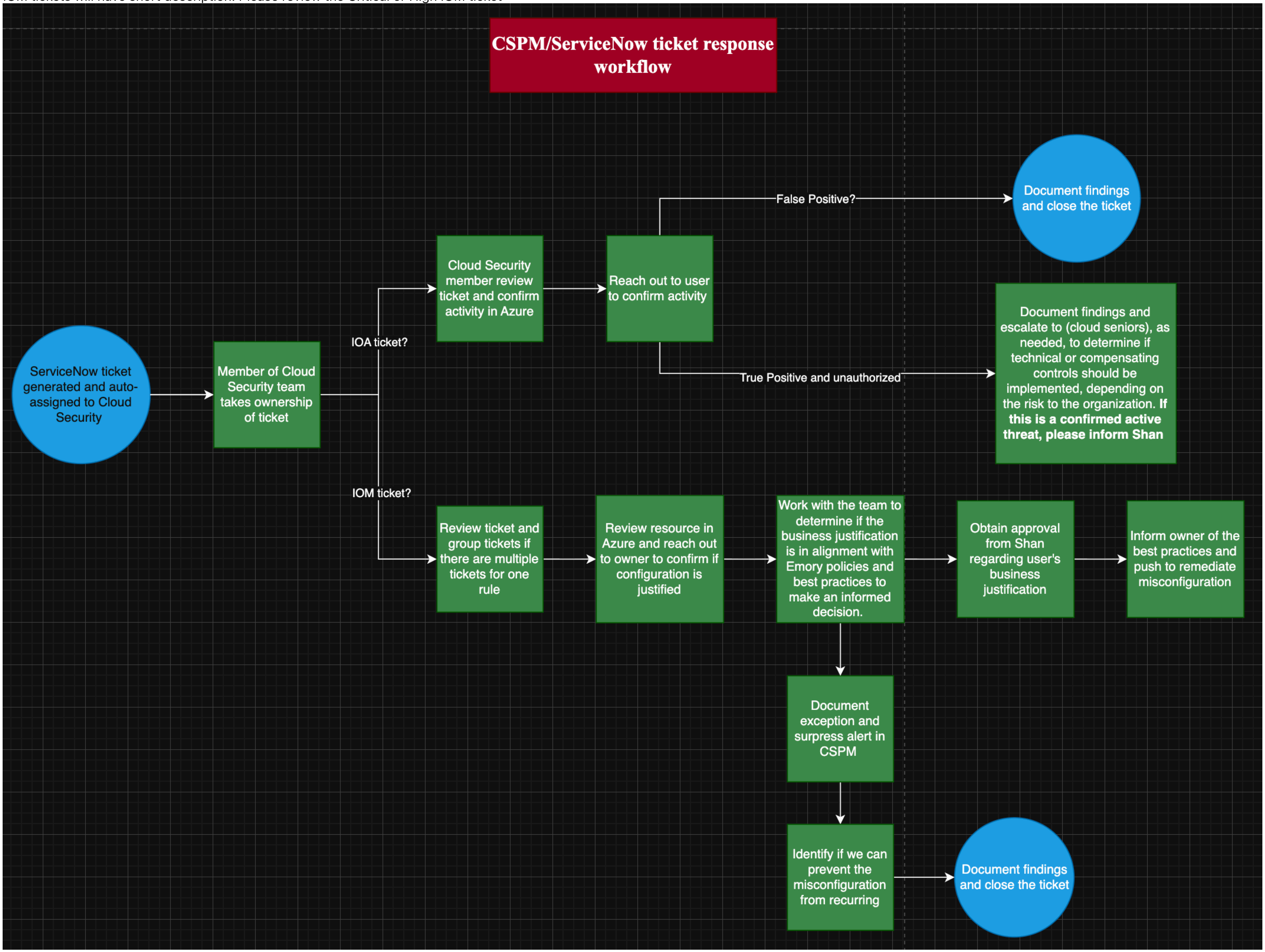
- There will be many high-risk sign in alerts related to users sign in from different countries within a matter of minutes. (These are common use-cases of users connected to the VPN). However, these alerts are now going to Elliot's team.

You can confirm who's on the Accenture team by going to this J2C SharePoint site > Who's Who In the Zoo > Slide 3 "Accenture Detailed Structure Team"

Future State ServiceNow ticket response workflow:

- IOA tickets will have the short description: Please review the Real-Time Visibility alert

- IOM tickets will have short description: Please review the Critical or High IOM ticket



CSPM/ServiceNow ticket response workflow

ServiceNow ticket generated and auto-assigned to Cloud Security

Member of Cloud Security team takes ownership of ticket

IOA ticket?

Cloud Security member review ticket and confirm activity in Azure

Reach out to user to confirm activity

False Positive?

Document findings and close the ticket

True Positive and unauthorized

Document findings and escalate to (cloud seniors), as needed, to determine if technical or compensating controls should be implemented, depending on the risk to the organization. **If this is a confirmed active threat, please inform Shan**

IOM ticket?

Review ticket and group tickets if there are multiple tickets for one rule

Review resource in Azure and reach out to owner to confirm if configuration is justified

Work with the team to determine if the business justification is in alignment with Emory policies and best practices to make an informed decision.

Obtain approval from Shan regarding user's business justification

Inform owner of the best practices and push to remediate misconfiguration

Document exception and surpress alert in CSPM

Identify if we can prevent the misconfiguration from recurring

Document findings and close the ticket