SILVERSKY™

*Change the Rules of Engagement*

outSOC

# outSOC Contact Playbooks

## SOC Guidance, Use Cases, & Recommended Configurations

Version 3.4

4FEB23

# Document History

| Revised On | Version | Description | Author |
|---|---|---|---|
| 11JAN23 | 3 | Migration to customer facing | Ben Harrison |
| 21JAN23 | 3.2 | Additional notes for severity config | Ben Harrison |
| 25JAN23 | 3.3 | Additional review and updates | Ben Harrison |
| 4FEB23 | 3.4 | Release Version | Ben Harrison |

# Table of Contents

# Introduction

OutSOCs' Notification Playbook feature is designed to allow users and customers using the OutSOC platform to choose what security incidents they are notified about, as part of the security monitoring function in their security programme.

It is critical that this is configured and updated in line with your security program needs, or notifications of security incidents which are important to you will not be sent.

The SilverSky SOC supply this document to expand the OutSOC user guide's UI description, with guidance, use cases, and recommended configurations for all OutSOC customers on all services.

It should be used in conjunction with the User Guide, and not as an isolated document.

## Responsibilities

During managed service onboarding with OutSOC, the deployment coordinator will share this documentation and provide support with notification playbook configuration. They will also attempt to configure a default notification playbook, using their primary contact's email address, and notification preferences for "Medium Severity" & "Reviewed" Incidents. This default Playbook is for training purposes only and is not customized to meet individual security program needs.

During the outSOC onboarding process, the deployment project coordinator will also help configure a Playbook for designed by the customer. Customers should work with their deployment coordinator (during onboarding) or their account manager (after onboarding) to customise the Playbook for their specific needs, available technical resources, and incident response plans.

After the onboarding process, customers are responsible for configuring and maintaining their Contact Playbook configurations, Guidance and recommendations from the SilverSky SOC are provided in this document and questions can be asked via the Support Ticket function in outSOC.

## Related Documentation

Please refer to the associated outSOC Single User Portal Guide for a full description of theoutSOC platform and the Contact Playbook feature.

# Determining Notification Strategy

Before configuring a Contact Playbook, it is important to consider and understand how the needs of your security program will impact your configuration.

1. Who are the key people in your organisation to be notified?
   (E.g. Use the RACI method: R = Responsible, A = Accountable, C = Consulted, I = Informed)
   - Who is Responsible for taking action on different severity incidents?
   - Do you have a CISO who is Accountable for all Critical & High incidents?
   - Do you have an MSP or IT provider who needs to be Consulted on incidents?
   - Do you have an internal ticketing system of record or an IIT department which must be kept Informed?

2. What is the tolerance for potential false positives and noise in your notification strategy?
   - Do you want notification of every incident, regardless of risk?
   - Do you only want to be notified of the High and Critical threats?
     (*Note the Incident Severity definitions for guidance...)
   - Do you want a mix of the above with low risk notifications to one user or group and High or Critical to another?

3. When are your business hours and what is the 24/7/365 working strategy of your organisation?
   (Breaches can occur at any time so someone in your organization must be contactable outside normal business hours.)
   - What are your business operating hours and business staffing hours?
   - How do you ensure you have contact availability at all times?
   - How do you ensure coverage is present when key staff members are on leave?
   - Do you have staff working 24/7/365, and if not, what is your on-call policy?

4. How does your organization balance reactive response to notification and proactive review?
   - Does your security program include weekly reviews of all incidents, including those assessed as non-threat?
   - Does your organisation only actively review any security platform when a notification is raised?

Note: These are examples of policy decisions which must be considered to effectively configure notifications. These questions are not exhaustive nor customized to your organisation.

# Guidance on Implementation

This section provides specific guidance on implementation of Contact Playbooks.

1. Preparation Phase
    - Review your environment's security program documentation to help build a notification strategy, paying special attention to the IR plan and those areas which list security team responsibilities / contacts.
    - Understand the environment's security monitoring notification requirements.
    - Consider notification recipients in a RACI matrix before adding them as Contacts into outSOC to understand individual responsibilities and use cases for each Contact.
    - Consider holding a tabletop exercise for various use cases with all parties involved to ensure alignment of expectations and assumptions.

2. Contacts - Individual VS Group
    - Contacts can be set up in outSOC as an individual or as a group distribution list. For a Contact set up as an individual, notifications will be sent to an email address or phone number which only go to a single individual.
    - For "RACI – Responsible" 24/7/365 use case notifications:
        - avoid using individual Contacts to prevent staff PTO / illness / churn impacting notifications.
        - Instead, try to use a Contact set up as a group email distribution list or ticketing systems (E.g. Jira, ZenDesk), and party phone lines (E.g. MS Teams, Zoom, etc.).
    - Use personal contacts only for "RACI – Inform" use cases, where individual staffing changes won't risk operational impacts.

3. Contact Information – Personal VS Business
    - Use business contact information whenever practical.
    - Personal email addresses and phone numbers are not preferred, because screening services and filters may block important notifications. There is also a risk because personal devices are often not secured in the same way as a business device.
    - However, alternative contact information may become essential to use in the case of a breach.

4. Ensuring 24/7/365 Coverage
    - All operationally important Contact Playbook should cover 24/7/365 for each RACI role as needed, with after-hours coverage or other on-call support in place to ensure full coverage.
    - Security "Systems of Record" for communications should be notified for all activity, with those notifications archived.
    - Adding notifications to the CISO role for all High & Critical is also useful for IR scenarios.

# Recommendations by Role

These recommendations are given as general cases to guide what the configurations might look like for different individuals/teams within an organization based on the RACI model. It is critical that all organisations determine their own Contact Playbook settings to match their environment and security program requirements.

## Responsible / Accountable Notification Config

The Playbooks settings below cover all the basic notification requirements when an incident or potential incident occurs requiring review or action. These settings will generally be for your IT team who will investigate, block activity, roll back endpoints, escalate internally, etc. This Playbook should include 24/7/365 coverage to ensure there is always a responder available in your organisation.

It's recommended that:

1. **All incidents reviewed by SOC of High and Critical severity should be:**
    - **Email notified to your security / IT team for review and action.**
    - **Phone notified to your security / IT team for escalation.**

2. **All incidents reviewed by SOC of Medium severity should be email notified to your security / IT team for review and awareness.**

3. **All incidents reviewed by SOC of Low and Info severity:**
    - **Should not be email or phone notified, as they can be relatively high volume and low security value.**
    - **Should be reviewed regularly by your Security / IT Team, using the OutSOC reporting and dashboard functions to identify policy violations or other non-threat IT value.**

## Consult / Inform Notification Configs

The Playbooks settings below cover all the notification requirements when incidents or potential incidents occur which may need review, notification, or further escalation. This could include your CISO, IT Manager, IR lead, or Compliance Manager, who will review the incidents or individuals and may want specific notification directly to them.

These settings generally only include working hours unless there are cases where an individual wants 24/7/365 escalation (e.g. CISO wants a phone call out of hours for any High or Critical incident).

1. **All incidents reviewed by SOC of High and Critical severity should be:**
    - **Email notified to your CISO / IT Managers for awareness.**

2. **All incidents created should be reviewed regularly by your security team to ensure that root causes of low threat or informational alerts can be diagnosed and resolved and whitelisting opportunities communicated with the SOC.**

# Example Configurations by Org Size and Role

The examples below display what the configuration might look like for different sized organisation. It is critical that all organisations determine their own Contact Playbook settings, to match their environment and security program requirements.

## Small Start-up

A small-scale operation with lots of shared responsibilities and no dedicated IT team:

3. Responsible – Medium, High and Critical email notifications are sent to the Software Engineer's email address jdoe@acme.com, for review and incident response.

4. Responsible – High & Critical phone notifications are sent to the CEO's phone number, for incident response.

5. Inform - Medium or higher notifications are sent to the CEO's personal email box for awareness.

## Small/Medium Enterprise

A maturing enterprise with dedicated IT team embracing new communication systems:

6. Responsible – Medium, High and Critical email notifications are sent to the IT team's email address it@acme.com for review and incident response.

7. Responsible – High and Critical phone notifications are sent to the IT team's phone number which triggers an afterhours outsourced service for incident response.

8. Accountable - High and Critical phone notifications are also sent to the IT manager after hours.

9. Informed - Medium or higher notifications aer also sent to the IT manager's personal email box for awareness.

## Enterprise

A large organisation with dedicated security, IT, and corporate security teams with mature communication systems:

10. Responsible - High and Critical email notifications are sent to the 24/7/365 Security Team's email address sec_incident@acme.com for incident response.

11. Accountable - High and Critical phone notifications are sent to the CISO after hours.

12. Consulted - Medium and Low notifications are sent to the 8/5 IT team's email address it_team@acme.com, to review for any potential policy violations or IT improvements.

13. Informed - Medium or higher notifications are also sent to the IT manager's personal email box for awareness.

14. Informed - Informational notifications are sent to the CRM platform for record, it_notifications@acme.com.