HiveWatch

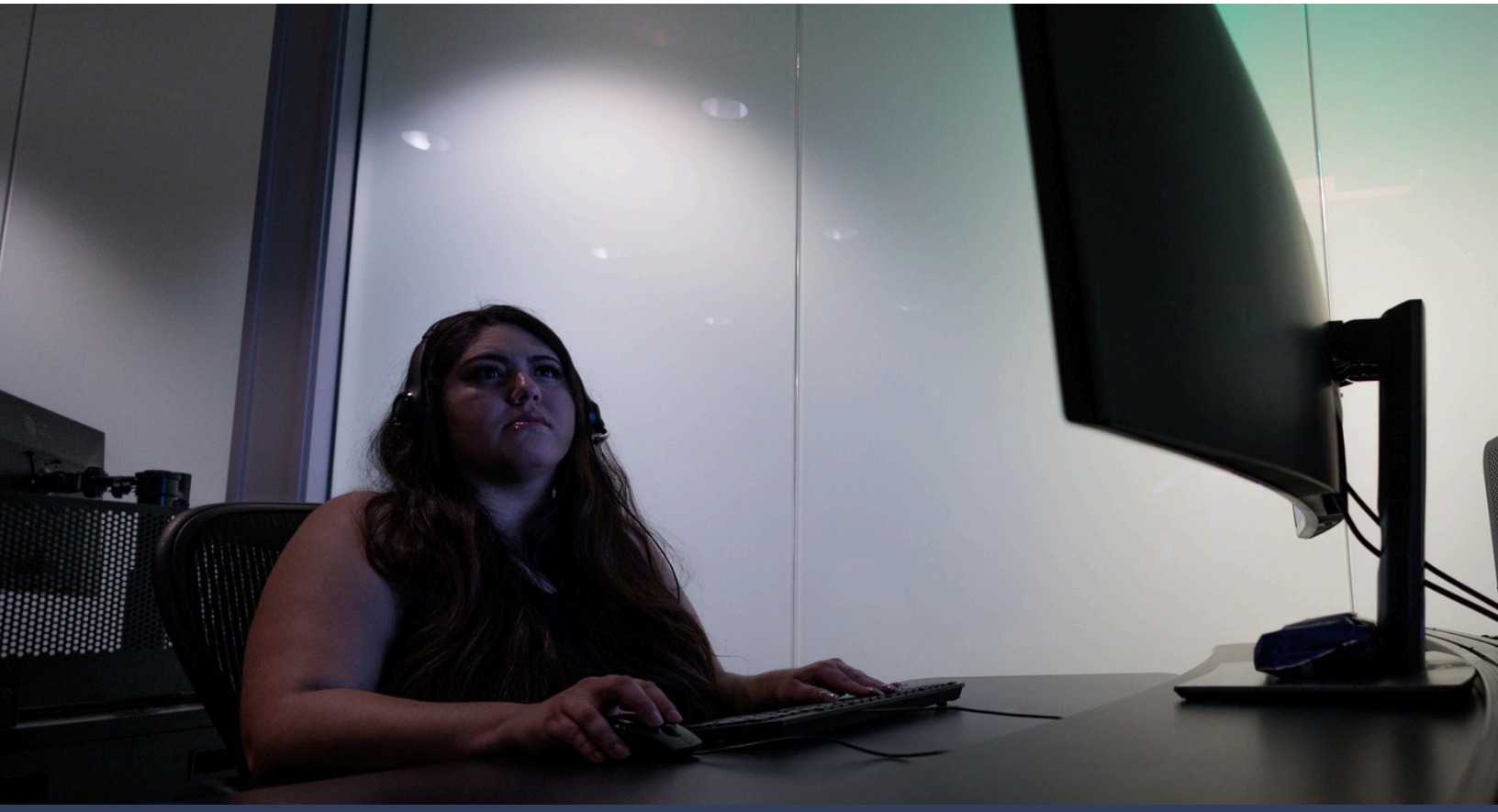
STARTER PACK

Standard Operating Procedure Templates

Kick-start your security operations with these easy-to-follow SOP templates

HiveWatch

Table of Contents



GETTING STARTED

This starter packet includes templates for Standard Operating Procedures (SOPs) that can be customized and used for your global security operations center (GSOC) operators to follow during incident triage.

The Importance of SOPs
SOPs are an essential and vital component of any security plan. They provide a clear and concise set of guidelines to help your security team understand their roles and responsibilities no matter how long they have been on the job.

Benefits of SOPs
Quickly train and onboard employees: SOPs can be used as training materials for operators and guards to understand what to do in case of specific events. Employees can get up to speed quickly and speed up their time to value.

- Expansion and scalability: Quickly enable your team at new locations, or onboard more employees.
- Increased productivity: When everything is documented, there is no question as to what needs to be done.
- Records against potential litigation: When there is a specific process to follow, which includes documentation, a company can use their SOPs as evidence of training and procedure.

How HiveWatch Can Help
The best way to utilize SOPs is to get them out of paper binders sitting in your SOC - and embedded into your security operations platform.

- Improve efficiency and response times while accessing the SOPs within the same platform you use to manage security incidents
- Limit context switching between multiple systems during an incident
- Increase training effectiveness by streamlining next steps within the HiveWatch® GSOC Operating System (OS) for operators to follow

More on Embedded SOPs.

You'll notice additional tips throughout these SOPs so you can further understand the benefits of HiveWatch and how it would fit into your everyday security operations.

Learn more and request a demo at hivewatch.com.

TAILGATING

Purpose

To provide guidance on managing a tailgating incident at any [COMPANY NAME] secure space.

Definitions

- Tailgating - The passage of an unauthorized person, forced or accidental, behind that of an authorized user

Procedure

If Tailgating is observed, the operator should create and acknowledge the incident and follow the below protocol:

1. Visually verify if the tailgating incident is real
2. If the alarm was triggered inadvertently by a [COMPANY NAME] employee:
   - Document the name (if known) or description of the employee
3. If the operator suspects that the tailgating incident was malicious, take the following actions:
   - Provide a clear description of the situation
   - Dispatch guards to investigate the incident
   - Continue to visually monitor the individual(s) via video surveillance
   - If the individual is presenting a clear and imminent security threat, contact law enforcement and activate the appropriate Incident Response SOP
   - Escalate to the GSOC Shift Supervisor
   - Cooperate with [COMPANY NAME] security and/or law enforcement
   - Add any and all additional notes for documentation until the incident management is complete using the template below

HiveWatch can automatically detect tailgating when one person uses their badge to scan in, but more than one person enters through a door. This instantly creates an alert for the GSOC where they can confirm tailgating, and follow the appropriate SOP.

TAILGATING

Template

Situational Awareness Report

Tailgating at [LOCATION].

- Description of Individual(s):
- Incident Description:
- Current location of Individual(s):

VIRTUAL PATROL

Purpose

The purpose of a Virtual Patrol is to conduct randomized checks of the secure [COMPANY NAME] space to monitor for unintentional security vulnerabilities and/or for potential or ongoing security threats or incidents.

Definitions

- Virtual Patrol - Conducting randomized checks of the secure [COMPANY NAME] space
- Unintentional Security Vulnerabilities - lapse in security controls that may be exploited by a threat actor (i.e., door propped open)
- BAU - acronym for "Business As Usual." Indicative of a stable security environment. This means that the [COMPANY NAME] secure space has no visible, unintentional security vulnerabilities and/or ongoing security threats

Scope

Operators will conduct a Virtual Patrol every [SET FREQUENCY] and will, at minimum, visually surveil all of the below secure areas:

1. [Placeholder for Camera Name or campus location]
2. [Placeholder for Camera Name or campus location]
3. [Placeholder for Camera Name or campus location]
4. [Placeholder for Camera Name or campus location]

Procedure

1. Click on each camera in the list of devices (list above)
2. Visually monitor each video feed for no less than 15 seconds to ensure BAU

VIRTUAL PATROL

Following actions will differ based on visual observations:

If a security incident or vulnerability is observed:

1. Activate the appropriate Incident Response SOP

If BAU:

1. Document the successful patrol according to pass-down procedures

If device(s) are offline:

Note: *Take these steps only if one or some cameras are offline. See System Outage SOP for guidance on how to report full system outages.*

1. Contact [SUPPORT CONTACT] with the below template to send device information

System Outage Email Template:

Hi Customer Support,

Please be advised that [Camera Name(s)] was observed offline during the routine Virtual Patrol conducted at [TIME]. Please inform me when the device is brought back online.

Thank you,
[Name]

HiveWatch enables operators to embed device health into their workflow. When an unhealthy device is identified, an email is automatically sent to a technician for repair. Device is noted as “unhealthy” until remidiated.

SYSTEM OUTAGE

Purpose

To outline the process for identifying, escalating, and reporting a system outage to the appropriate internal and external stakeholders.

Definitions

- System Outage - When GSOC operator(s) cannot monitor devices
- Service disruption - When GSOC operator(s) are experiencing limited functionality

Scope

All system outages identified in the GSOC should be immediately reported to the appropriate internal stakeholders that will triage the incident in accordance with existing escalation protocol.

Procedure

If an operator believes that the monitoring capabilities of the GSOC are degraded, the operator should document the scope of the outage and escalate in accordance with the below scenario:

1. **System being used is observed to be functioning in a deteriorated state (i.e., incidents not generating, “glitching”, etc.)**
    - Document the impacted functionality
    - Contact system support staff
    - Escalate notice of outage to GSOC Supervisor
    - Document outage via existing pass-down procedures to ensure other GSOC Operators are aware of the outage

SYSTEM OUTAGE

2. **All systems failure due to power outage**
    - Activate business continuity plan for GSOC redundancy
    - Escalate notice of power outage to [COMPANY NAME] POC via GSOC Supervisor
        - [Name]<Email address of POC> or (XXX)-XXX-XXXX

GUARD DISPATCH

Purpose

To define when to dispatch guards.

Definitions

- Dispatch Guard - Sending a notification to guards to respond to an ongoing security incident or vulnerability

When to dispatch

When a guard is required to visually inspect, witness, document, or respond to the scene of an incident.

Procedure

[Document step by step how to dispatch your guards]

HiveWatch allows operators to dispatch guards via a user-friendly mobile app (bye bye, radios). Field resources can receive full context of the event they are responding to, with corresponding video, voice message, and other relevant information.

DOOR HELD OPEN

Purpose

To provide guidance on how to manage a Door Held Open incident.

Definitions

- Door Held Open - An alarm that occurs if the door is left open for a period which exceeds the programmed alarm shunt time

Scope

The [COMPANY NAME] secure space.

Procedure

If a door held alarm triggers:

1. **Visually verify if the Door Held Open incident is real**
2. **If the Door Held Open incident is real, but there was no malicious intent:**
   - Document the name (if known) or description of the employee
   - Monitor the live video feed until you can confirm that the door has returned to a secure state
3. **If the alarm was triggered maliciously:**
   - Provide a clear description of the situation by adding notes to the incident using the template (below)
   - Dispatch guard(s) to investigate the incident
   - Continue to visually monitor the individual via camera surveillance
   - If the individual is presenting a clear and imminent security threat, contact law enforcement and activate the appropriate Incident Response SOP
   - Cooperate with [COMPANY NAME] security and/or law enforcement
   - Escalate to the GSOC Shift Supervisor
   - Add any and all additional notes for documentation

HiveWatch

DOOR HELD OPEN

Incident Notes Template

Door Held Open at [LOCATION NAME]

- Description of Individual(s):
- Incident Description:
- Current location of Individual(s):

DOOR FORCED

Purpose

To provide guidance on how to manage a Door Forced incident.

Definitions

- Door Forced - A door was opened without access being granted

Scope

The [COMPANY NAME] secure space.

Procedure

If a Door Forced alarm triggers, follow the below protocol:

1. **Visually verify if the Door Forced incident is real**
   - If the door was not forced, resolve the incident
2. **If the Door Forced incident is real and the alarm was triggered accidentally:**
   - Document the name (if known) or description of the employee
3. **If the alarm was triggered maliciously:**
   - Provide a clear description of the person
   - Dispatch guard(s) following the Guard Dispatch SOP
   - Continue to monitor the individual via video surveillance
   - If the individual is presenting a clear and imminent security threat, contact law enforcement and activate the appropriate Incident Response SOP
   - Escalate to the GSOC Shift Supervisor
   - Cooperate with [COMPANY NAME] security and/or law enforcement
   - Add any and all additional notes for documentation (template below) until incident management is complete

Sometimes sensitive sensors create false alarms. HiveWatch reports on your baseline noise, determines where it's coming from, and the best way to solve for it.

HiveWatch

DOOR FORCED OPEN

Incident Notes Template

Door Forced Open at [LOCATION NAME]

- Description of Individual(s):
- Incident Description:
- Current location of Individual(s):

READY TO GET STARTED?

Let's talk.

www.hivewatch.com
info@hivewatch.com