

# SOC 1

**Status:**

**Disabled**

**Starting Prompt:** get\_recent\_alerts for the last 1 hour via SamiGPT then triage the first one using the initial alert triage runbook

**Condition Function:** get\_recent\_alerts

**Interval:** 5s (5s)

**Last Run:** 11/26/2025, 1:57:09 AM

**Next Run:** 11/26/2025, 1:57:14 AM

**Export Date:** 11/26/2025, 2:16:05 AM

## Chat History

[11/26/2025, 1:42:29 AM]

> [CONDITION CHECK] get\_recent\_alerts

✓ CONDITION PASSED: Found 5 uninvestigated alert(s) (total: 5, groups: 3).  
Proceeding with autorun execution.

[11/26/2025, 1:42:29 AM]

> get\_recent\_alerts for the last 1 hour via SamiGPT then triage the first one using the initial alert triage runbook

```
## Triage Summary

**Alert:** Guest Account Activated or Modified (ID: `323d3bfc2f8f8d4534813ebb2d6038f0dd04de18cbae1029f5dedaa4d863b45c`)

**Assessment:** Uncertain

**Key Findings:**
- Hostname "win10-stand-alone-test-3" does not match KB naming conventions (cannot verify)
- IP 10.10.0.82 is internal (Data Center Server Network subnet)
- User "Administrator" verified as known admin account in KB
- No IOC matches found
- Multiple alerts (6 total) on the same host within minutes
- Guest account was enabled and then modified (2 events)

**Action Taken:**
- Alert verdict set to "uncertain"
- Investigation findings documented in alert note
- No case created (per SOC1 guidelines: uncertain alerts do not warrant case creation)
- Alert left open for monitoring

**Recommendation:**
Alert requires additional context. SOC2 may investigate if a pattern emerges from multiple uncertain alerts. Consider verifying if this is a test/lab system or unmanaged device. If legitimate, consider adding to KB or adjusting detection rules to exclude test environments.

The triage is complete. The alert has been assessed, documented, and left open for monitoring per SOC1 triage guidelines.
```

[11/26/2025, 1:43:29 AM]

> [CONDITION CHECK] get\_recent\_alerts

✓ CONDITION PASSED: Found 5 uninvestigated alert(s) (total: 5, groups: 4). Proceeding with autorun execution.

[11/26/2025, 1:43:29 AM]

> get\_recent\_alerts for the last 1 hour via SamiGPT then triage the first one using the initial alert triage runbook

```
## Triage summary

**Alert triaged:** "Account added to Remote Desktop Users group"
**Alert ID:** `bf3fb8080c7966488dfe30536cb50fc889564b6b31bdःa327e6a801e1f984731`
```

```
### Investigation findings
```

1. KB verification:

- Host IP `10.10.0.82` is internal (Data Center Server Network subnet)
- Administrator account verified in KB with RDP tags
- Hostname "win10-stand-alone-test-3" doesn't match KB naming patterns (suggests test/lab machine)

2. IOC check: No IOC matches found

3. Related activity: 6 alerts on the same host in the last 24 hours, all involving the Administrator account

4. Assessment: True positive/suspicious

- Guest account (SID -501) was added to Remote Desktop Users group
- Unusual activity; not standard administrative practice
- Could indicate privilege escalation or unauthorized access configuration

#### ### Actions taken

- Case created: Case #326 with all alert details documented
- Observables attached: Host, IP address, and user
- Alert note added: Investigation summary and findings
- Alert verdict updated: Set to `true\_positive`
- Case status: Set to `in\_progress` for SOC2 investigation

#### ### Escalation

Case escalated to SOC2 for deep investigation. The case includes:

- Complete alert and event details
- Investigation findings
- Related alerts on the same host
- Clear investigation requirements for SOC2

Triage complete. SOC2 can proceed with the investigation using Case #326.

[11/26/2025, 1:44:29 AM]

> [CONDITION CHECK] get\_recent\_alerts

✓ CONDITION PASSED: Found 4 uninvestigated alert(s) (total: 4, groups: 3). Proceeding with autorun execution.

[11/26/2025, 1:44:29 AM]

> get\_recent\_alerts for the last 1 hour via SamiGPT then triage the first one using the initial alert triage runbook

Triage complete. Summary:

```
## Triage Summary

**Alert:** Account Added to Administrators Group
**Alert ID:** `29d3db4b71fae7d8943c3b532612627ee1b95ea7022a06e39b6a4e8941b4afa8` 

### Assessment: Confirmed True Positive

### Findings

1. Privilege escalation: Guest account (SID: `S-1-5-21-1717527356-3680816920-1387935965-501`, Account Name: "-") was added to the Administrators group.

2. Pattern correlation: The same Guest account was also added to the Remote Desktop Users group within minutes (related alert already in Case 326).

3. Host context:
- Host: `win10-stand-alone-test-3` (10.10.0.82)
- IP verified as internal (Data Center Server Network subnet)
- Hostname does not match KB naming patterns (suggests test/lab machine)
- 6 related alerts on the same host in the last 24 hours

4. User context:
- Action performed by: Administrator account (verified in KB)
- No IOC matches found
```

#### ### Actions Taken

1. Alert verdict set to `in-progress` (then `true\_positive`)
2. Alert note added with investigation summary
3. Added to existing Case 326 (related activity on the same host)
4. Case comment added with alert details
5. Observables attached:
  - Host IP: `10.10.0.82`
  - Guest account SID: `S-1-5-21-1717527356-3680816920-1387935965-501`
6. Escalated to SOC2 for deep investigation

#### ### Escalation Rationale

Guest account addition to Administrators is a clear privilege escalation indicator. The coordinated pattern (added to both Administrators and Remote Desktop Users) suggests a potential security incident requiring SOC2 investigation.

The alert has been triaged and escalated to SOC2 for deep investigation. All details are documented in Case 326.

[11/26/2025, 1:45:24 AM]

> [CONDITION CHECK] get\_recent\_alerts

✓ CONDITION PASSED: Found 3 uninvestigated alert(s) (total: 3, groups: 2). Proceeding with autorun execution.

[11/26/2025, 1:45:24 AM]

```
> get_recent_alerts for the last 1 hour via SamiGPT then triage the first  
one using the initial alert triage runbook
```

```
## Triage Summary

**Alert triaged:** "Guest Account Activated or Modified" (Alert ID:  
'c72845e57624b969a027386219d602cdc27f058f75e9928c2a09ba6a454f05cb`)

**Assessment:** Suspicious/True Positive

**Findings:**  
- Guest account was enabled by Administrator account on host `win10-stand-alone-test-3` (IP: 10.10.0.82)  
- Guest account activation is not expected; Guest accounts should remain disabled  
- Multiple account modification alerts on the same host within minutes indicate a pattern  
- IP verified as internal (matches IT-WS01 workstation in KB)  
- No IOC matches found

**Actions taken:**  
1. Alert verdict set to "in-progress" then updated to "true_positive"  
2. Added to existing case #326 (same host/timeframe)  
3. Communication about details documented in case comment
```

3. Comprehensive alert details documented in case comment
4. Investigation summary added to alert note
5. Observables attached to case (IP: 10.10.0.82, Guest account)

\*\*Escalation:\*\* Ready for SOC2 deep investigation to determine if this is legitimate admin activity or unauthorized account manipulation.

The alert has been triaged and documented. SOC2 can proceed with deep investigation using case #326.

[11/26/2025, 1:46:29 AM]

> [CONDITION CHECK] `get_recent_alerts`

- ✓ CONDITION PASSED: Found 2 uninvestigated alert(s) (total: 2, groups: 1). Proceeding with autorun execution.

[11/26/2025, 1:46:29 AM]

> `get_recent_alerts` for the last 1 hour via SamiGPT then triage the first one using the initial alert triage runbook

```
## Triage complete

Completed triage of the first alert following the `initial_alert_triage` runbook.

### Alert summary
- Alert ID: `b4cd873b17387ed9d5d462632f9902d18454fefelc570cede76fda65c33eb54a`
- Title: "Windows Account or Group Discovery"
- Verdict: False Positive

### Investigation findings
1. KB verification:
   - Host `win10-stand-alone-test-3` (10.10.0.82) verified as internal IT Workstation
   - User `Administrator` verified as known privileged admin account

2. Threat intelligence:
   - `net.exe` hash lookup: Not malicious (UNKNOWN assessment)
   - No IOC matches in last 24 hours

3. Pattern analysis:
   - 6 related alerts on same host within 24h
   - 14 security events matching same pattern
   - Recurring legitimate admin activity

4. Root cause:
   - Command: `net.exe user guest Password-123*`
   - This is account modification (password change), not account discovery
   - Rule incorrectly flags modification operations as discovery

### Actions taken
```

1. Created fine-tuning recommendation (ClickUp Task ID: `86evn90a7`)
  - Suggests refining rule to distinguish discovery vs. modification
  - Includes specific logic recommendations
2. Added assessment note to alert
  - Documents investigation findings and assessment rationale
3. Updated verdict to `false\_positive`
  - With explanatory comment
4. Closed alert
  - Marked as false positive with documentation

### Outcome

Alert triaged as False Positive. No case created (per runbook: cases only for confirmed True Positives). Fine-tuning recommendation created to improve detection rule accuracy and reduce future false positives.

[11/26/2025, 1:48:49 AM]

> [CONDITION CHECK] `get_recent_alerts`

✓ CONDITION PASSED: Found 1 uninvestigated alert(s) (total: 1, groups: 1).  
Proceeding with autorun execution.

[11/26/2025, 1:48:49 AM]

```
> get_recent_alerts for the last 1 hour via SamiGPT then triage the first  
one using the initial alert triage runbook
```

Triage complete. Summary:

```
## Triage Summary
```

```
**Alert ID:**  
`4791a29d1c3d4424f4c2696354f03973a57c5fad49d956a4f9f3a09be5bb4592`  
**Alert Type:** Windows Account or Group Discovery  
**Assessment:** Confirmed True Positive
```

```
### Findings
```

This alert is the first step in a privilege escalation chain:

1. Step 1 (this alert): Guest account activated (`net.exe user guest /active:yes`)
2. Step 2: Guest account added to Administrators group (Alert `29d3db4b...`)
3. Step 3: Guest account added to Remote Desktop Users group (Alert `bf3fb808...`)

```
### Investigation Results
```

- KB verification: Host IP (10.10.0.82) is internal; hostname doesn't match KB naming patterns; Administrator account verified in KB
- IOC check: No matches found
- SIEM context: 14 net.exe events found; 6 related alerts on same host within 24 hours
- Pattern analysis: Coordinated sequence indicates an attack chain, not legitimate admin activity
- Related case: Case 326 already exists for related privilege escalation activity on the same host

```
### Actions Taken
```

1. Added investigation note to alert with findings
2. Added alert details to Case 326 (existing case for related activity)
3. Attached file hash observable to case

4. Updated alert verdict to `true\_positive`
5. Case 326 remains open and in\_progress for SOC2 investigation

The alert has been triaged and added to Case 326, which is already escalated to SOC2 for deep investigation of the privilege escalation pattern.

[11/26/2025, 1:49:54 AM]

> [CONDITION CHECK] `get_recent_alerts`

✗ CONDITION FAILED: No uninvestigated alerts found (total: 0, groups: 0).  
Skipping autorun execution.

[11/26/2025, 1:50:04 AM]

> [CONDITION CHECK] `get_recent_alerts`

✗ CONDITION FAILED: No uninvestigated alerts found (total: 0, groups: 0).  
Skipping autorun execution.

[11/26/2025, 1:54:19 AM]

> [CONDITION CHECK] `get_recent_alerts`

✓ CONDITION PASSED: Found 3 uninvestigated alert(s) (total: 3, groups: 2).  
Proceeding with autorun execution.

[11/26/2025, 1:54:19 AM]

> `get_recent_alerts for the last 1 hour via SamiGPT then triage the first one using the initial alert triage runbook`

```
## Triage Summary

**Alert ID:** `6Jo2vZoB194ksd57g5gL`
**Alert Type:** Malware Detection Alert
**Status:** Triaged and escalated to SOC2

### Investigation Findings

1. **KB Verification:**
   - User "Administrator" verified as known admin account in KB
   - Hostname "win10-stand-alone-test-3" does not match KB naming schemas
     (verification failed)

2. **IOC & Threat Intelligence:**
   - No IOC matches found for the file hash
   - Hash found in TI database but threat level is "unknown" with no indicators
```

```
3. **SIEM Analysis:**  
    - Found 2 events with this hash on host "win10-stand-alone-test-3"  
    - Processes: `powershell.exe` and `npp.8.8.8.Installer.x64.exe` (unusual  
      naming pattern)  
    - Found 9 total alerts for this host in the last 24 hours (malware, IAM,  
      process alerts)
```

```
4. **Case Correlation:**  
    - Related to existing Case #326 for the same host
```

```
### Assessment
```

**\*\*Verdict:\*\*** True Positive/Suspicious

**\*\*Confirmation indicators:\*\***

- Hostname verification failed (doesn't match KB naming conventions)
- Pattern of multiple alerts on the same host (9 alerts in 24 hours)
- Unusual process naming convention
- Unknown threat level for file hash

```
### Actions Taken
```

1. Set alert verdict to "in-progress" (then updated to "true\_positive")
2. Added investigation note to the alert
3. Added alert details to Case #326 (related case)
4. Attached file hash observable to Case #326
5. Updated case status to "in\_progress"
6. Escalated to SOC2 for deep investigation

The alert has been triaged and documented. Case #326 contains all alert details for SOC2 investigation. Task creation encountered an error, but the case comment documents the required investigation work.

[11/26/2025, 1:55:14 AM]

> [CONDITION CHECK] `get_recent_alerts`

✓ CONDITION PASSED: Found 2 uninvestigated alert(s) (total: 2, groups: 2).  
Proceeding with autorun execution.

[11/26/2025, 1:55:14 AM]

> `get_recent_alerts for the last 1 hour via SamiGPT then triage the first`

## one using the initial alert triage runbook

```
## Triage Summary

**Alert ID:** `7Zo2vZoB194ksd57g5gL`
**Title:** Potential Browser Information Discovery
**Severity:** Medium
**Assessment:** Uncertain

### Investigation Performed:
1. KB verification: Administrator account verified as known admin account in acme_corp_client KB
2. IOC check: No IOC matches found
3. SIEM search: No related security events found for browser access
4. Case search: No existing cases for this alert
5. Related alerts: Found 9 total alerts for Administrator user in last 24 hours

### Key Findings:
- User is a known administrator account in KB
- No IOC matches indicating known malicious activity
- Browser information discovery activity is not explicitly documented as expected activity for admin accounts
- Missing context: No actual event data available in alert response (events array is empty)
- Cannot determine if this is legitimate admin troubleshooting or suspicious reconnaissance

### Actions Taken:
```