

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: 11/28/2025, 2:09:01 PM

Next Run: 11/28/2025, 2:09:06 PM

Export Date: 11/29/2025, 3:15:40 PM

Chat History

[11/28/2025, 1:59:10 PM]

> [CONDITION CHECK] get_recent_alerts

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

[11/28/2025, 1:59:10 PM]

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

```
## Triage complete

**Alert triaged:** Malicious RDP Connection (ID: `252c103df01908c4824c19c3664731396be39341bd59fdda5a982fc1f0ef42c8`)

**Assessment:** False Positive

**Summary:**
- Source IP 10.10.10.7 is internal (HQ Corporate LAN subnet)
- User "Administrator" is a known admin account with RDP-expected tags
- Host `win10-stand-alone-test-3` is a known admin workstation
- No IOC matches or suspicious indicators
- Single isolated event, no pattern of malicious activity

**Actions taken:**
1. Set alert verdict to `in-progress` to lock it
2. Performed KB verification (internal IP, known entities)
3. Checked IOC matches (none found)
4. Searched for related cases (none found)
5. Investigated SIEM context (legitimate internal RDP)
6. Added detailed alert note with investigation summary
7. Updated verdict to `false_positive` with reasoning
8. Created fine-tuning recommendation for detection rule improvement
```

Fine-tuning recommendation created: Task ID `86evpbtdx` - recommends excluding or reducing severity for internal-to-internal RDP connections involving known admin accounts and workstations.

The alert has been closed as a false positive without creating a case, following the SOC1 initial alert triage runbook workflow.

[11/28/2025, 2:00:00 PM]

> [CONDITION CHECK] get_recent_alerts

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

[11/28/2025, 2:00:00 PM]

> 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:** `0ea0d232b54ab0303f454942915cca36649b2cce4a6b4389b075fe5ede56d1cc`
- **Assessment:** TRUE POSITIVE
- **Case created:** #408
```

```
### Findings
```

1. **Event details:**

- Guest account enabled on `win10-stand-alone-test-3` by Administrator account
 - Windows Security Event 4738 at 10:52:27 UTC
 - UAC changed from 0x215 (disabled) to 0x214 (enabled)

2. **KB verification:**

- Host `win10-stand-alone-test-3`: Known workstation (IP 10.10.0.82, internal network)
 - User `Administrator`: Known admin account with RDP-expected tags
 - IP addresses: All internal, no external indicators

3. **IOC checks:**

- No IOC matches found

4. **Related activity:**

- RDP connection alert occurred ~3 minutes before Guest activation
- Same host and Administrator account involved

5. **Case correlation:**

- No existing cases for this hostname within 24 hours
- New case created (#408)

```
### Actions taken
```

- Alert verdict set to `in-progress` (locked for triage)
- Case #408 created with details
- Observables attached: hostname, Administrator user, Guest user
- Case comment added with triage summary
- Alert note added with investigation details
- Alert verdict updated to `true_positive`
- Escalated to SOC2 for investigation

```
### SOC2 next steps
```

1. Verify if Guest account activation was authorized
2. Check for other suspicious account modifications
3. Review Administrator account activity timeline
4. Investigate if Guest account has been used for logons
5. Correlate with the related RDP connection alert

Triage complete. The alert has been escalated to SOC2 for investigation.

[11/28/2025, 2:01:21 PM]

> [CONDITION CHECK] `get_recent_alerts`

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

[11/28/2025, 2:01:31 PM]

> [CONDITION CHECK] get_recent_alerts

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

[11/28/2025, 2:01:41 PM]

> [CONDITION CHECK] get_recent_alerts

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

[11/28/2025, 2:01:41 PM]

> 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:
`ce1a51d65a2ed3c59e2a63c6cf52c811631965a50a3cf45378f35c2fa852f10a`
- **Title:** Account Added to Administrators Group
- **Severity:** Medium
- **Assessment:** TRUE POSITIVE

Findings

1. **Attack chain identified:**
 - 10:49:11 – RDP connection (FP – legitimate internal admin access)
 - 10:52:27 – Guest account activation (TP – Case #408)
 - 10:54:10 – Account added to Administrators group (TP – current alert)

```
2. **Case correlation:**  
    - Linked to existing Case #408 (same host `win10-stand-alone-test-3` within  
24 hours)  
    - All alerts share the same host, user (Administrator), and Logon ID  
(0xC3CC680)  
  
3. **Investigation results:**  
    - KB verification: Host and user verified as known/legitimate  
    - IOC checks: No IOC matches  
    - Suspicious indicator: Account with no name (Account Name: -) added to  
Administrators group  
  
### Actions taken  
  
- Alert verdict set to `true_positive`  
- Alert linked to Case #408 with detailed notes  
- Case comment added documenting the privilege escalation  
- Observables attached: hostname, user, IP addresses  
- Escalated to SOC2 for deep investigation
```

The alert has been triaged and linked to Case #408 for SOC2 investigation. The runbook workflow is complete.

[11/28/2025, 2:02:36 PM]

```
> [CONDITION CHECK] get_recent_alerts
```

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

[11/28/2025, 2:02:46 PM]

```
> [CONDITION CHECK] get_recent_alerts
```

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

[11/28/2025, 2:02:56 PM]

```
> [CONDITION CHECK] get_recent_alerts
```

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

[11/28/2025, 2:03:06 PM]

> [CONDITION CHECK] `get_recent_alerts`

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

[11/28/2025, 2:03:16 PM]

> [CONDITION CHECK] `get_recent_alerts`

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

[11/28/2025, 2:03:26 PM]

> [CONDITION CHECK] `get_recent_alerts`

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

[11/28/2025, 2:03:26 PM]

> `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:**  
'bda2fd47ad0b1d63002bcfffb8b41627f205e3a8fa8a00637f54181824070544`
```

```
### Investigation findings
```

```
**Assessment:** TRUE POSITIVE – Part of a privilege escalation attack chain
```

```
**Attack chain timeline (all events share Logon ID 0xC3CC680):**  
1. 10:49:11 – RDP connection from 10.10.10.7 (triaged as FP – legitimate internal admin access)  
2. 10:52:27 – Guest account activation (Case #408 created)  
3. 10:54:10 – Guest account added to Administrators group (linked to Case #408)  
4. 10:55:46 – Guest account added to Remote Desktop Users group (current alert)
```

```
**Key finding:** The member SID (S-1-5-21-1717527356-3680816920-1387935965-501) matches the Guest account SID, confirming the same account was escalated through multiple privilege groups.
```

```
### Actions taken
```

1. Alert verdict updated to `true_positive`
2. Alert linked to existing Case #408 (same host within 24 hours)
3. Comprehensive alert notes added with investigation details

4. Case comment added documenting the attack chain
5. Observables attached to case (host, Administrator user, Guest account)
6. SOC2 task created for deep investigation

```
### Case information
```

- Case ID: #408
- Case title: "Guest Account Activation - win10-stand-alone-test-3 - 2025-11-28"
- Status: Open (in_progress attempted but API error occurred)
- SOC2 task created: "Investigate Guest Account Privilege Escalation - Remote Desktop Users Group Addition"

The alert has been triaged and escalated to SOC2 for investigation of the full privilege escalation attack chain.

[11/28/2025, 2:04:31 PM]

```
> [CONDITION CHECK] get_recent_alerts
```

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

[11/28/2025, 2:04:41 PM]

```
> [CONDITION CHECK] get_recent_alerts
```

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

[11/28/2025, 2:04:51 PM]

```
> [CONDITION CHECK] get_recent_alerts
```

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

[11/28/2025, 2:05:01 PM]

```
> [CONDITION CHECK] get_recent_alerts
```

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

[11/28/2025, 2:05:11 PM]

```
> [CONDITION CHECK] get_recent_alerts
```

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

[11/28/2025, 2:05:21 PM]

> [CONDITION CHECK] get_recent_alerts

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

[11/28/2025, 2:05:31 PM]

> [CONDITION CHECK] get_recent_alerts

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

[11/28/2025, 2:05:41 PM]

> [CONDITION CHECK] get_recent_alerts

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

[11/28/2025, 2:05:41 PM]

> 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:** `JqgjypoBZrhotbUSxaWM` - "Malware Detection Alert"
```

```
### Investigation findings
```

1. Threat intelligence: MALICIOUS

- Malware family: Win64/ShellcodeRunner.BPS trojan
- AV detection: 39/76 engines flagged as malicious
- VirusTotal: 7 malicious, 65 undetected
- File type: PE32+ executable (Windows x64)

2. KB verification:

- Host `win10-stand-alone-test-3` verified as known workstation
- User `Administrator` verified as known admin account
- File hash not in expected/internal software list

3. SIEM context:

- Found 2 related alerts with the same hash
- Multiple alerts today involving Administrator user

```
### Assessment: TRUE POSITIVE
```

Confirmed malicious malware detected on workstation.

```
### Actions completed
```

1. Alert verdict set to `in-progress` (locked for triage)
2. Case created: Case #409 - "Malware Detection - win10-stand-alone-test-3 - 2025-11-28"
3. Observables attached:
 - File hash (SHA256)
 - Hostname (win10-stand-alone-test-3)
 - User (Administrator)
4. Case comment added with investigation details
5. Alert note added with triage summary
6. Alert verdict updated to `true_positive`
7. SOC2 task created: "Deep Investigation - Malware Analysis and Endpoint Investigation"

```
### Escalation
```

Alert escalated to SOC2 via Case #409. SOC2 should:

- Perform endpoint deep investigation on win10-stand-alone-test-3
- Analyze file behavior and execution context
- Investigate malware introduction vector
- Review Administrator account activity
- Correlate with other alerts involving Administrator user today

Triage complete per the initial alert triage runbook.

[11/28/2025, 2:06:36 PM]

```
> [CONDITION CHECK] get_recent_alerts
```

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

[11/28/2025, 2:06:36 PM]

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

```
## Triage Summary
```

Alert: FqgjypoBZrhotbUSxaWM - Malware Detection Alert

Key Findings:

- Hash verified as malicious: Win64/ShellcodeRunner.BPS trojan
- Threat intelligence: 39/72 AV detections, VirusTotal 7/72 malicious
- Affected host: win10-stand-alone-test-3 (known workstation)
- User: Administrator (known admin account)

Investigation Steps Completed:

1. Set alert verdict to "in-progress" to lock it
2. KB verification: Host and user verified as known entities
3. Threat intelligence lookup: Confirmed malicious classification
4. IOC checks: No matches in SIEM (but TI confirms malicious)
5. Case correlation: No existing cases for this host within 24 hours
6. Assessment: TRUE POSITIVE

Actions Taken:

- Created Case #410: "Malware Detection - win10-stand-alone-test-3 - 2025-11-28"
- Attached observable: File hash (SHA256) marked as malicious
- Added case comment with triage findings
- Updated alert verdict to "true_positive"
- Added alert note documenting investigation
- Created SOC2 task: "SOC2 - Deep Malware Analysis - Win64/ShellcodeRunner.BPS trojan" (Priority: High)

Escalation: Escalated to SOC2 for deep malware analysis, impact assessment, infection timeline, lateral movement analysis, and containment recommendations.

The alert has been triaged and escalated to SOC2 for further investigation.

[11/28/2025, 2:07:36 PM]

> **[CONDITION CHECK] get_recent_alerts**

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

[11/28/2025, 2:07:36 PM]

> **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:** G6gjypoBZrhotbUSxaWM - "Potential Browser Information
Discovery"
```