Correlation Search

Search Name: test-seach

App: Enterprise Security

App Context: Enterprise Security

Set an app to use for links such as the drill-down search in a notable event or email adaptive response action. If set to None, the setting defaults to the current application context.

Description: test

Mode: Guided | Manual

Search:

```
splunk_server=* index=* host[redacted]="login" | stats count by src_ip | where count > 3
```

Annotations

CIS 20: Type an attribute and press enter

Kill Chain: Type an attribute and press enter

Annotations

CIS 20: Type an attribute and press enter

Kill Chain: Type an attribute and press enter

MITRE ATT&CK: Type an attribute and press enter

NIST: Type an attribute and press enter

Confidence:

Impact:

Analytic Story: Type an attribute and press enter

Context: Type an attribute and press enter

Unmanaged Annotations

+ Framework

Time Range

Earliest Time: -24h

Set a time range of events to search. Type an earliest time using relative time modifiers.

Time Range

Earliest Time: -24h

Set a time range of events to search. Type an earliest time using relative time modifiers.

Latest Time: now

Type a latest time using relative time modifiers.

Cron Schedule: */5 * * * *

Enter a cron-style schedule. For example "*/5 * * * *" (every 5 minutes) or "0 21 * * *" (every day at 9 PM). Real-time searches use a default schedule of "*/5 * * * *".

Scheduling: Real-time | Continuous

Controls the way the scheduler computes the next execution time of a scheduled search. This controls the realtime_schedule setting. Learn more

Schedule Window: No window

Time interval during which to run the report.

Schedule Priority: Default

Setting to increase the priority of a report over other searches. Use with caution.

Trigger Conditions

Trigger alert when: Number of Results

is greater than 1

Trigger: Once | For each result

Notable response actions and risk response actions are always triggered for each result.

Throttling

Window duration: 0 second(s)

Specify the time duration during which events that match the values specified in the "Fields to group by" might be ignored.

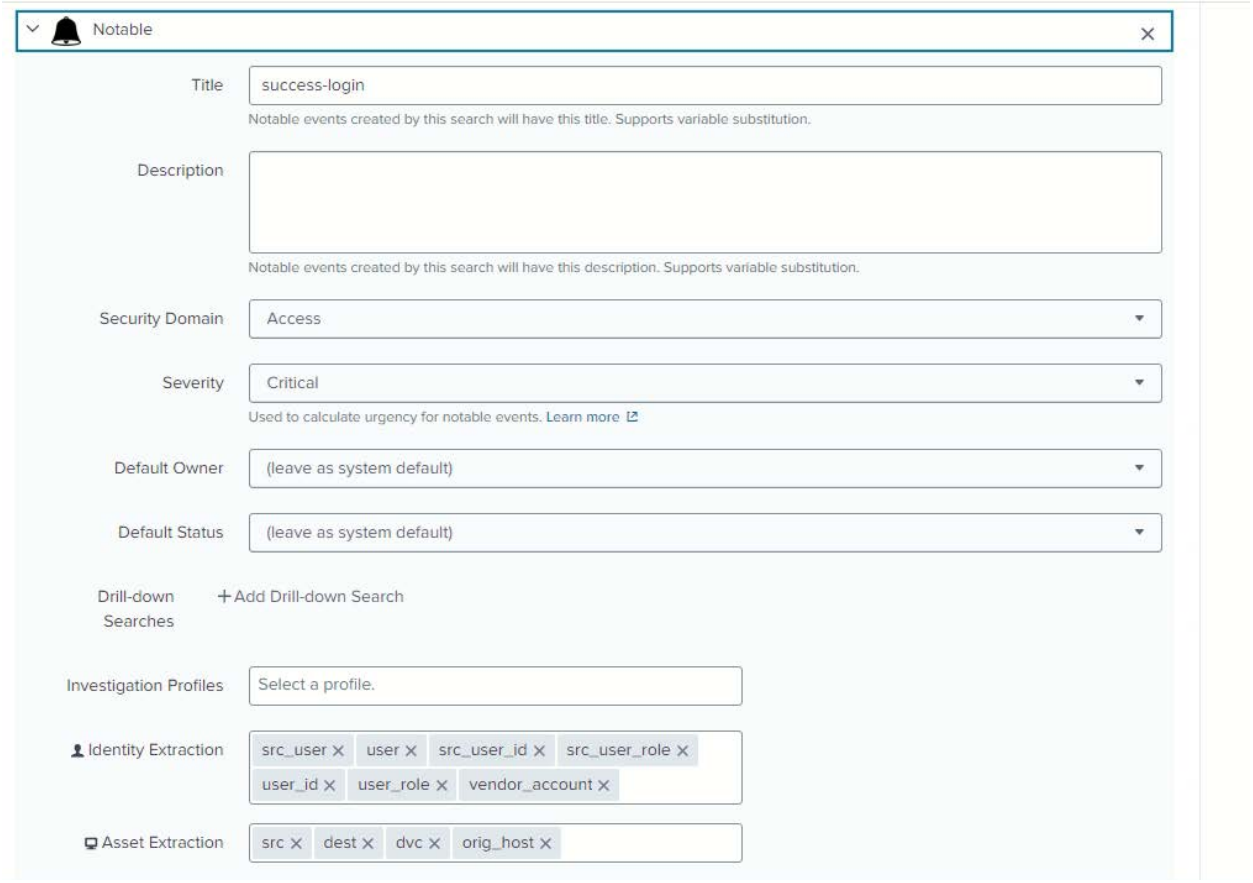
Fields to group by: Type a field and press enter

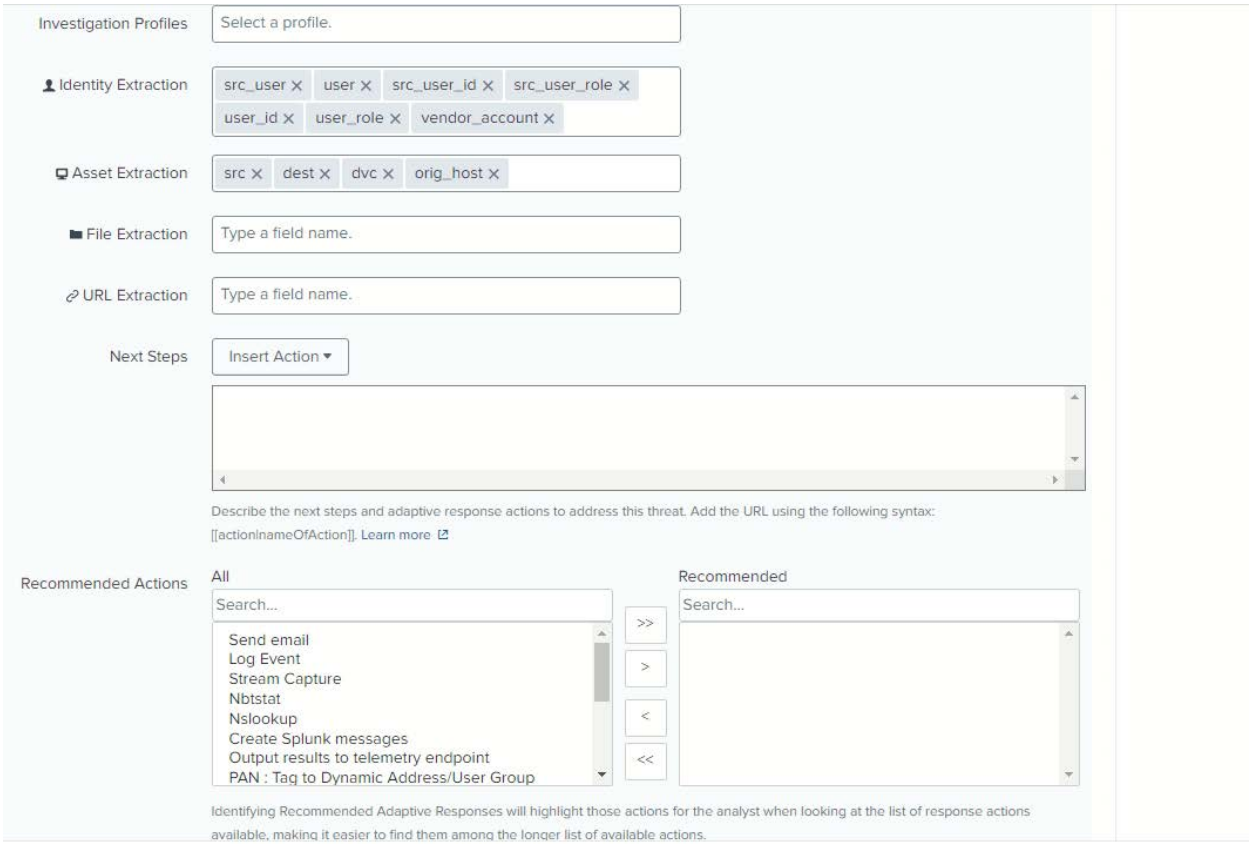
Type the fields to consider for matching events for throttling. Learn more

Adaptive Response Actions

+ Add New Response Action

> Notable ×


Notable
Title
success-login
Notable events created by this search will have this title. Supports variable substitution.
Description
Notable events created by this search will have this description. Supports variable substitution.
Security Domain
Access
Severity
Critical
Used to calculate urgency for notable events. Learn more
Default Owner
(leave as system default)
Default Status
(leave as system default)
Drill-down Searches
+ Add Drill-down Search
Investigation Profiles
Select a profile.
Identity Extraction
src_user
user
src_user_id
src_user_role
user_id
user_role
vendor_account
Asset Extraction
src
dest
dvc
orig_host


Investigation Profiles
Select a profile.
Identity Extraction
src_user ×
user ×
src_user_id ×
src_user_role ×
user_id ×
user_role ×
vendor_account ×
Asset Extraction
src ×
dest ×
dvc ×
orig_host ×
File Extraction
Type a field name.
URL Extraction
Type a field name.
Next Steps
Insert Action
Describe the next steps and adaptive response actions to address this threat. Add the URL using the following syntax: [[actionInameOfAction]]. Learn more
Recommended Actions
All
Search...
Send email
Log Event
Stream Capture
Nbtstat
Nslookup
Create Splunk messages
Output results to telemetry endpoint
PAN : Tag to Dynamic Address/User Group
>>
>
<
<<
Recommended
Search...
Identifying Recommended Adaptive Responses will highlight those actions for the analyst when looking at the list of response actions available, making it easier to find them among the longer list of available actions.