

El campo Descripción no se está rellenando en el panel de revisión de incidentes para los elementos de Notables.

Aplicabilidad

Seguridad empresarial Splunk - 7.3.x

Descripción

El problema parece afectar a todas las búsquedas de correlación personalizadas, ya que varios campos no se rellenan en el panel de revisión de incidentes. A continuación se muestra un ejemplo de una búsqueda de correlación personalizada.

Búsqueda de correlación: "Amenaza - Ejemplo_de_prueba_1"

Description		
unknown		
Additional Fields	Value	Action
Disposition	Undetermined	▼
Owner	unassigned	▼
Security Domain	threat	▼
Severity	high	▼
Status	New	▼
Time	2024-10-09T22:37:03.000+05:30	
Title	Test_Sample_1	▼
Type	notable	
Urgency	medium	▼

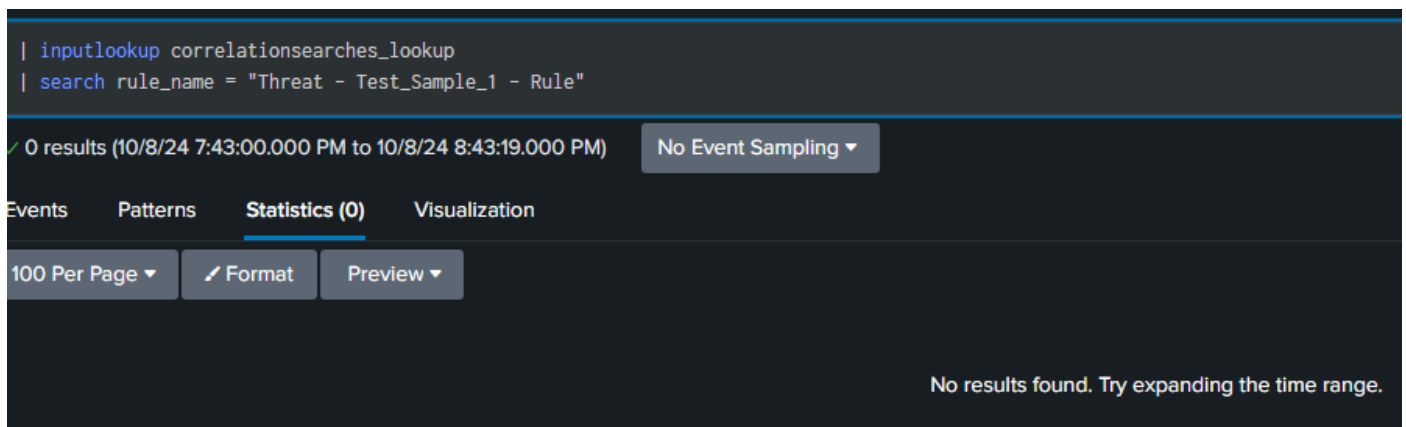
Investigación

1. Se ha ejecutado la siguiente búsqueda manualmente para comprobar si los campos asociados estaban produciendo resultados. Al revisar el campo "rule_description", se muestra "unknown" (desconocido), a pesar del valor configurado durante la creación de la

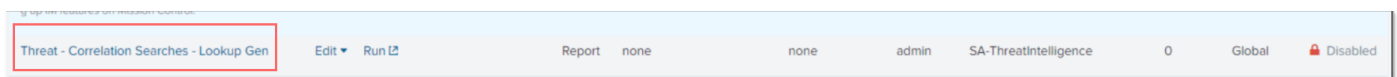
búsqueda de correlación.

```
| savedsearch "Incident Review - Main" time_filter="" event_id_filter="" source_filter="" secur  
| search  
| eval _position=1  
| accum _position  
| eval _offset=_position - 1
```

2. Se ejecutó la búsqueda "Correlation searches_lookup" para comprobar si los datos se rellenan para la regla "Threat - [BDS] Anormal Webdav Execution - Rule", pero no se obtiene ningún resultado.



3. Se comprobó si la búsqueda que generaba la búsqueda "Threat - Correlation searches - Lookupgen" estaba habilitada o no y se encontró que la búsqueda estaba deshabilitada.



Resolución

Para resolver el problema, siga estos pasos:

1. Vaya a Configuración -> Búsquedas, informes y alertas
2. Busque "Threat - Correlation searches - Lookupgen".
3. Habilite la búsqueda haciendo clic en Edit -> Enable.

Name	Actions	Type	Next Scheduled Time	Display View	Owner	App	Alerts	Sharing	Status
Threat - Correlation Searches - Lookup Gen	EditRun	Report	none	none	admin	SA-ThreatIntelligence	0	Global	Disabled
Edit Search Edit Permissions Edit Schedule Edit Acceleration Edit Summary Indexing Enable									

Después, al habilitar la búsqueda, la descripción y otros campos asociados se rellenaron en el panel de revisión de incidentes.

Description		
Just a sample Description		
Additional Fields	Value	Action
Disposition	Undetermined	▼
Owner	unassigned	▼
Security Domain	threat	▼
Severity	high	▼
Status	New	▼
Time	2024-10-09T22:08:04.000+05:30	
Title	Test_Sample_1	▼
Type	notable	
Urgency	medium	▼

Enlaces relacionados

Documentación relacionada: [Enlace](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).