

مدع - ServiceNow لة فاضإل Splunk ة فظو نم مدختسم لل ثدح عاشنإ

قېب طتلا ةېلباق

Splunk تاقېب طت ة فاضإ

فصولا

ل ة فاضإل ة فظولا مادختساب نآلا ة مدخلال عل ثداوح عاشنإ نم لوؤسمال نكمت
كلذب ماقلال نم مدختسمال عل رذعت نكلو ServiceNow.

(اموعدم دعل مل) ServiceNow نم 3.1 رادصلال Splunk ة فاضإل ة فظولا مادختسا
7.2.3 رادصلال، Splunk Search Head عل

snow_ta_ticket.log عل أطخ ة لاسر رقلل:

```
2019-07-30 20:00:01,597 ERROR pid=24194 tid=MainThread file=snow_ticket.py:_get_service_
account:158 | username=<encrypted>, password=<encrypted>, url=https://something.com
2019-07-30 20:00:01,618 ERROR pid=24194 tid=MainThread file=snow_ticket.py:_get_service_
account:162 | url=https://something.com, app=Splunk_TA_snow
2019-07-30 20:00:01,618 ERROR pid=24194 tid=MainThread file=snow_ticket.py:_get_service_
account:165 | Failed to get clear credentials for https://something.com
```

ءالجتسا

؛اهتئيهتو جولثلل تېبثت نم ىرخأ ةرم ققحت

- جثلثلل بئاج نم اءدب -

1. جثلثلل لئثم عل لولخدلا لئجستب مق.
2. وأ "نآلا ة مدخلال رجتم" نم قېب طتلا تېبثت كنكمي.
3. دهاشتسو فلمال عل لولصولاب مق، هنئىعت اغلإو Splunk_TA_SNOW لئزنل دنع
(نآلا ة مدخلال تائىدحت تاعومجم هههه) Export ل ىمسي رخأ افلم
• خسنل تائىلمع ارجإو فئاظو ة فاضإل ونس اهمدختسي تئلا تائىلآل ههه
ءءاعتسالل اوائى طائىتال
4. "كنولبس" عم لصاوتلل "ونس" دادعل اذه مدختسنس.

5. دحاو رخآ ىلع لصح.
6. (ثي دحتل تاعومجم عجرتسا وأ) ثي دحت قوف رقناو لي ثمل ىل عجرا.
7. فلم طاق تلاب تمق يذلا فلملا دحوو فلم رتخاو، xml نم ةعومجم داري تسلا قوف رقنا مٲ . لبق نم هيلا
8. ناوٲ عضب كلذ قرغتسي دق . "لي مٲت" قوف رقنا مٲ .
9. Splunk لم اٲت قوف رقنلاب تاٲي دحتل ةعومجم حتفا مٲ .
10. هذو يف عاطخأل ضعب ىلع تلصح اذا قلقت ال . "ثي دحتل ةعومجم ةنياعم" ىلع رقنا . ةلحرملا
11. تاءارجا "قوف رقنلاب اهلوبقو A لئاسرلا ةفاك دي دحت . لشف ام ققحتو . ةذفانلا قلغأ . "ةددم فوفص ىلع
12. "ثي دحتل ةعومجم ذي فنٲ" ىلع رقنا مٲ .
13. نآلا ةمدخلال عم Splunk ب لصتيس يذلا مدختسملا ةفاضلا ىل اٲاتحن .
14. نذا كي لعلف ، كب صاخال "نآلا ةمدخلال" باسح ىلع لوؤسمك كلوخذ لچست مل اذا كلذل . دحو "مدختسملا" بيوبتل ةمالع قوف رقنا طقف (security_admin ىل كرود ةيقرت "راودألا ةيقرت")
15. كلقنيس . مدختسملا لوؤسم : ةشاشلا عون نم رسيألا بناجال ىلع ثحبلا طيرش يف . نيمدختسملا ةرادا ىل اذو
16. اذل رورملا ةملكو مدختسملا عاشناب مقو دجال نيمدختسملا/نيمدختسملا قوف رقنا . مدختسملا
 - دي قعتلا دويقب يفٲ رورملا ةملك نا نم دكأت
 - "يلخادلا لم اٲتلا مدختسم" و "Active" يعبرم دي دحت نم دكأت
17. "ريرت" ىلع رقنا راودألا رايخ تحت .
18. x_splu2_splunk_ser.splunk رودلا دحو
19. هظفح .

جلثلا بناج ىلع هٲاتحن يذلا بيترتلا ريبك دح ىل اذو

رخآ قيبتات يأل لثم Splunk ىلع قيبتاتلا تيبتت ىل نآلا اٲاتحن

1. قيبتاتلا تيبتت دعب Splunk ليغشت ةداعاب مق .
2. قيبتاتلا ىل لاقتنالا
3. ةملكو Snow ىلع هتأشنأ يذلا مدختسملا كب صاخال جلثلا لي ثمل URL ناونع عض . نيوكتل طفحو هب ةصاخال رورملا
 - اٲان ناك لاصتالا نا ينع ي اذو ، ةي لمعل هذو اناثأ أطخ ةلاسري أ كلصت مل اذا
4. SNOW نع ثحبلا وٲاقيبتاتلا ىل لاقتنالا
5. "تانئلكال ضرع" ىلع رقنا

هيلا اٲاتحت ام نيكم تب مق . ةنكمم ريغ ثحبلا تايللمع ضعب نا ىرتس

لغتشي ب اذا فوشو:

1. جلثلا قيبتات ىل لاقتنا
2. "ةمدخلال نمض ثداوخلال جم د" بيوبتل ةمالع ىرت نا بچي ، "تاءارجالا" يف

قيبتاتلا ىلع ةباتكو ةءارق تانوذأ مدختسملا ىدل نوكي نا بچي

مالعتسالا اذو مادختساب Snow ىلع لوؤسمك ثداح ليچست نكمي

```
|snowincident --category "Network" --short_description "testing search" --contact_type  
"email" --urgency "3" --subcategory "intranet" --state "1" --location "Hawaii" --impact  
--priority "5" --assignment_group "network" --opened_by "ME" --ci_identifier "1234567"  
--comments "these are Don's comments" --splunk_url "www.splunk.com" --correlation_id "12
```

رځاً مدختسم مادختساب هديلوت انيلى رذعت نكلو

SNOW_TA_TICKET.log: ىلى هذه أطخلال ةلاسرىلى لصحن انك

```
2019-07-30 20:00:01,597 ERROR pid=24194 tid=MainThread file=snow_ticket.py:_get_service_  
account:158 | username=<encrypted>, password=<encrypted>, url=https://something.com  
2019-07-30 20:00:01,618 ERROR pid=24194 tid=MainThread file=snow_ticket.py:_get_service_  
account:162 | url=https://something.com, app=Splunk_TA_snow  
2019-07-30 20:00:01,618 ERROR pid=24194 tid=MainThread file=snow_ticket.py:_get_service_  
account:165 | Failed to get clear credentials for https://something.com
```

رارق

مدختسمال رودىلى ةينالكمإلا هذه انفضأ كذل

```
list_storage_passwords
```

چلثلىلى عثداوح قلخىلى ارداق ناك مدختسمال كذل لمع دعب

مالعتسالال اذهب هانربتخإ دقل

```
index=servicenow_eo sourcetype="snow:incident" "Splunk provided the following enrichment  
information" | table number, short_description, dv_state, dv_cmdb_ci, dv_assignment_grou  
dv_opened_at | sort dv_state
```

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب Cisco ي ل خ ت . ف ر ت ح م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا