Uyumluluk

GDPR

> Bu özellik, THeHive 5.x'in Platinum planı ile yalnızca mevcuttur.

TheHive, veritabanındaki veri saklama politikasını yönetmeye yönelik bir özelliğe sahiptir, bu özellik varsayılan olarak etkin değildir.

Stratejiler

İki strateji mevcuttur:

1. Hassas değerleri <redacted> ile değiştirin
2. Verileri silme

Değerleri <redacted> ile Değiştirin

- Vakalar için aşağıdaki alanlar redakte edilir:

davanin `summary` ve `message`
yorumların `message`
görev günlüklerinde `message`
`gdpr.dataTypesToDelete` yapılandırma özelliğinde seçilen ve doldurulan veri tipleri için gözlemlenebilirlerin `message`
sayfaların `content`
TTP'lerdeki prosedürlerin `description`

- Uyarılar için aşağıdaki alanlar redakte edilir:

uyarı `message`
gözlemlenebilirlerin `message` (bkz. `gdpr.dataTypesToDelete` yapılandırma özelliği)
prosedürlerin `description` (ttp)

Denetimler İçin:

alan `details` redakte edilmiştir.

Verileri Sil

Strateji `delete` seçilirse:

Vaka ve bileşenleri - *tasks, task logs, procedures, comments, pages, custom events in timelines, values of custom field and observables* - are deleted
Uyarı ve bileşenleri- *procedures, comments, values of custom field and observables* - are deleted.
Denetim silinir

Saklama

RetentionPeriod parametresi, silinecek veya redakte edilecek verilerin minimum yaşını tanımlar. GDPR süreci, bu ayardan daha eski verilere uygulanacaktır. Yaş, son güncelleme tarihine (veya hiç güncellenmemişse oluşturma tarihine) dayanır. Biçim bir sayı ve bir zaman birimidir. Desteklenen birimler şunlardır:

gün: `d`, `day`
saat: `h`, `hr`, `hour`
dakika: `m`, `min`, `minute`
saniye: `s`, `sec`, `second`
milisaniye: `ms`, `milli`, `millisecond`

Yapılandırma

Bunu etkinleştirmek için /etc/thehive/application.conf yapılandırma dosyası güncellenmelidir. Aşağıdaki yapılandırmayı dosyaya ekleyin:

```
gdpr {
  enabled = true

  ## Format http://www.quartz-scheduler.org/documentation/quartz-2.3.0/tutorials/crontrigger.html
  ## Every Sunday at 02:30

  schedule = "0 30 2 ? * SUN"

  ## Possible GDPR strategies:
  ##   delete: remove the documents
  ##   redact: replace sensitive values by "<redacted>" (cf. dataTypesToDelete)

  strategy = "delete"

  ## if the strategy is "redacted", the observable with dataType in
  ## "dataTypesToDelete" will be removed
  ## for other observables, message will be "<redacted>", not the data
  ## Uncomment following line to select datatypes
```

```
    # dataTypesToDelete = [] ## ["ip", "domain"]

    ## only documents older than the "retentionPeriod" will be processed

    retentionPeriod = 730 days # 2 years

    ## Advanced parameters (should not be modified)

    jobTimeout = 24 days ## maximum time the job is executed
    batchSizeCase = 5     ## how many cases is processed per transaction
    batchSizeAlert = 10   ## how many cases is processed per transaction
    batchSizeAudit = 100  ## how many cases is processed per transaction
}
```

Ardından uygulamayı yeniden başlatın.

Revision #2
Created 12 April 2024 22:22:01 by Güldeniz Akca
Updated 13 April 2024 15:05:30 by Güldeniz Akca