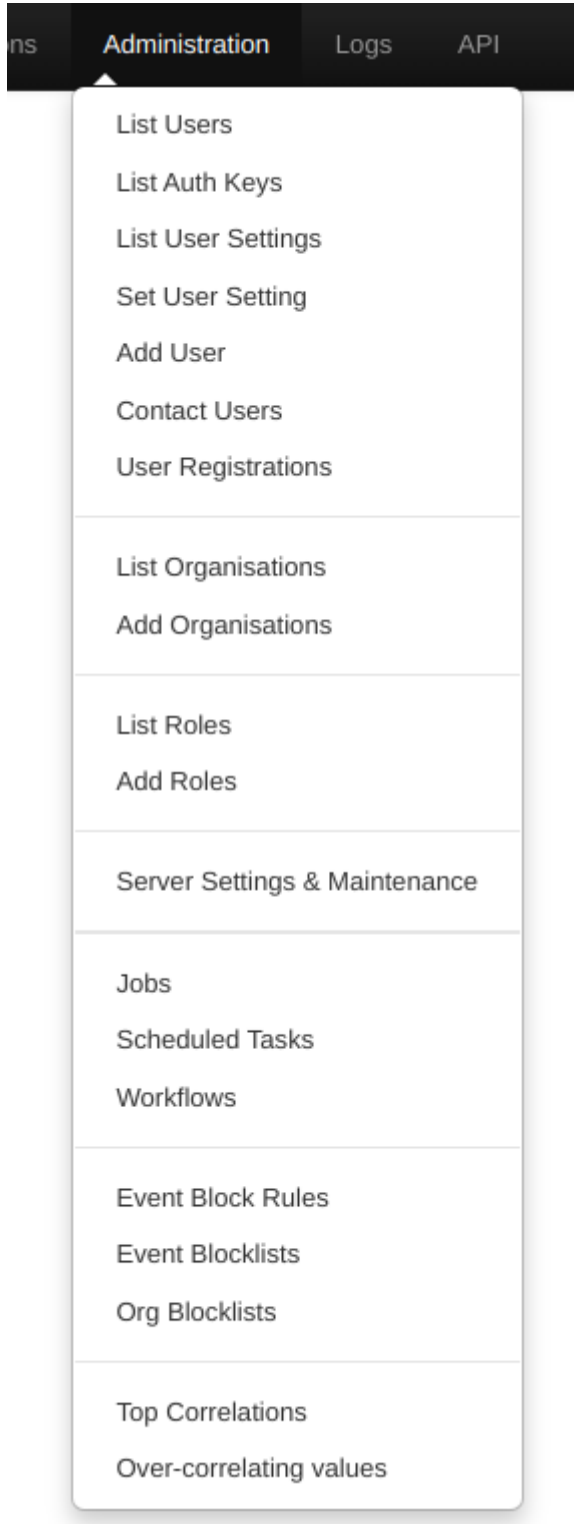


ADMINISTRATIONS

Yöneticiler kullanıcı hesaplarını ve kullanıcı rollerini ekleyebilir, düzenleyebilir veya kaldırabilir. Roller, olayların yayınlanması, REST arayüzünün kullanımı veya verilen role ait herhangi bir kullanıcının senkronizasyonu gibi belirli özelliklere erişim haklarını tanımlar.

Site yöneticileri kullanıcıların şifrelerini sıfırlamanın veya şifreli e-mail yoluyla onlarla iletişime geçmenin mümkün olduğu bir iletişim formuna da erişebilir.



- **List Users:** Şu anda kayıtlı olan kullanıcılar görüntülenebilir, değiştirilebilir veya silinebilir.
- **List Auth Keys:** Gelişmiş yetkilendirme anahtarı sisteminden alınan yetkilendirme anahtarlarının bir listesini ve bunların yorumlarını gösterir. Yetkilendirme anahtarı, bilgisayar sistemlerine erişim izni sağlayan bir kimlik doğrulama aracıdır. Özel bir dizi karakter veya sayıdan oluşur ve belirli kaynaklara erişim izni verir.
- **List User Setting:** Kullanıcı ayarlarını listeler.
- **Set User Setting:** Kullanıcılar için kullanıcıya özel ayarları belirler.
- **Add User:** Kuruluşlar için yeni bir kullanıcı hesabı oluşturulabilir. Site yöneticileri, herhangi bir kuruluş için kullanıcı hesapları oluşturabilirler.

Yeni bir kullanıcı eklemek için soldaki yönetim menüsündeki "Add User" butonu ile yeni bir kullanıcı eklenebilir.

Add User

List Users

Pending registrations

User settings

Set Setting

Contact Users

Add Organisation

List Organisations

Add Role

List Roles

Server Settings & Maintenance

Update Progress

Jobs

Scheduled Tasks

Event Block Rules

Blocklists Event

Manage Event Blocklists

Blocklists Organisation

Manage Org Blocklists

Admin Add User

Email

☐ Set password

Organisation

Choose organisation

Role

User

NIDS SID

PGP key

Paste the user's PGP key here or try to retrieve it from the CIRCL key server by clicking on "Fetch PGP key" below.

Fetch PGP key

☒ Receive email alerts when events are published

☒ Receive email alerts from "Contact reporter" requests

☐ Immediately disable this user account

☒ Send credentials automatically

Create user

E-Mail: Kullanıcı e-mail adresi, kullanıcı adı olarak giriş yapmak ve otomatik e-mailleri göndermek için bir adres olarak kullanılacaktır.

Set Password: Kullanıcı için geçici bir kullanıcı şifresi tanımlamak isteniyorsa kutu işaretlenir. Eğer istenmiyorsa, bir şifre oluşturmak ve bunu kullanıcıya e-mail ile göndermek için 'List Users' görünümündeki 'reset password' butonu kullanılmalıdır.

Password: 'Set Password' işaretlendiğinde yalnızca bu metin kutusu görüntülenir. Kullanıcı için ilk girişten sonra değiştirmesi gereken geçici bir şifre tanımlanmalıdır. Parola MISP Parola politikasına uygun olmalıdır.

☒ Set password

Password ⓘ

Confirm Password

Organisation: Kullanıcı için organizasyon seçilmesini sağlayan açılır bir listedir. Organizasyon hakkında detaylı bilgi aşağıda verilmiştir.

Role: Kullanıcının ait olması gereken bir rol grubunun seçilmesini sağlayan açılır bir listedir. Roller, kullanıcıya atanan kullanıcı ayrıcalıklarını tanımlar. Roller hakkında detaylı bilgi aşağıda verilmiştir.

Authkey: Belirtilen kullanıcının benzersiz yetkilendirme anahtarıdır ve otomatik olarak atanır. (kullanıcı bunu sıfırlayabilir ve yeni bir anahtar alabilir). Bir sunucuyu başka bir sunucuya bağlamak için kullanılır, ancak kullanıcının yetkilendirme izni etkinleştirilmiş bir rolle atandığından emin olunması gerekir.

NIDS SID: Ağ sızma algılama sisteminde kullanılan bir imza kimliğidir. Kullanıcı tarafından oluşturulan Snort kuralları, kullanıcının tanımladığı ofsetle başlayan artan bir SID ile dışa aktarılır. Ofset belirtilmemişse, varsayılan olarak bir SID atanır, ancak bu bir rastgele değer olabilir.

Sync user for: Eğer bu seçenek ayarlanırsa, yerel kullanıcı bir uzak sunucudan çekim yaparken seçilen sunucunun itme kuralları da uygulanır. Bu seçenek, yönetici, Kuruluş Yöneticisi ve Senkronizasyon kullanıcı rolü için kullanılabilir.

Çekim (Pull): Bir cihazın veya sistemdeki bir kaynağın, diğer bir kaynaktan veri almak için aktif olarak talepte bulunması anlamına gelir. Yani, veri kaynağı, belirli bir zaman aralığında veya belirli bir olay gerçekleştiğinde veriyi çeken cihaz veya sistemdir. Örneğin, bir kullanıcının e-posta istemcisi, sunucudaki yeni e-postaları çekmek için düzenli aralıklarla sunucuya talepte bulunur.

İtme (Push): Bir cihazın veya sistemdeki bir kaynağın, veriyi otomatik olarak hedefe gönderdiği eylemidir. Kaynak, veri değişiklikleri olduğunda veya belirli bir koşul gerçekleştiğinde veriyi hedefe iletir. Örneğin, bir sunucu, yeni bir dosya oluşturulduğunda veya var olan bir dosya değiştirildiğinde, bu değişiklikleri hedef cihaza veya sisteme itebilir.

Gpgkey: Sistem üzerinden gönderilen e-mailleri şifrelemek için kullanılan anahtar temsil eder.

Fetch GnuPG (PGP) key: GnuPG genel anahtarını getirir. GnuPG'nin genel anahtarı, diğer kullanıcıların verileri şifrelemek için kullandığı, herkese açık bir anahtardır.

Receive alerts when events are published: Bu seçenek, bir "Event" yayımlandığında yeni bir kullanıcıyı, otomatik olarak oluşturulan e-postaların alıcı

listesine ekleyecektir.

Receive alerts from "contact reporter" requests: Olayın raporlayıcısı veya kaynaklarından daha fazla bilgi sağlamalarını istemek için yapılan bir iletişim isteğidir.

Immediately disable this user account: Kullanıcı hesabını hemen devre dışı bırakma işlemini belirtir. Bu seçeneği işaretlediğinizde, kullanıcı hesabı derhal etkisiz hale getirilir ve kullanıcı o andan itibaren sistemde erişim hakkını kaybeder.

Send credentials automatically: Otomatik olarak kimlik bilgilerini gönderme işlemini belirtir. Bu seçeneği işaretlediğinizde, kullanıcıya otomatik olarak bir kullanıcı adı ve şifre gönderilir. Bu, genellikle yeni bir kullanıcı hesabı oluşturulduğunda veya bir kullanıcının şifresi sıfırlandığında kullanılır. Kullanıcıya kimlik bilgileri e-mail yoluyla gönderilir ve böylece kullanıcı, hesabına erişim sağlayabilir.

- **Contact Users:** Bu görünüm, mevcut veya gelecekteki kullanıcılara mesaj göndermek veya onlara geçici bir şifre göndermek için kullanılabilir.

Site yöneticileri, tüm kullanıcılara veya bireysel kullanıcılara e-mail göndermek için "Contact Users" özelliğini kullanabilir. GnuPG (PGP) anahtar setine sahip olan kullanıcılar e-maillerini şifrelenmiş olarak alacaklardır.

Contact User(s)

Messaging - here's a quick guide on how this feature works

You can use this view to send messages to your current or future users or send them a temporary password.

- When adding a new user to the system, or when you want to manually reset the password for a user, just use the "Send temporary password" setting.
- After selecting the action, choose who the target of the e-mails should be (all users, a single user or a user not yet in the system).
- You can then specify (if eligible) what the e-mail address of the target is (for existing users you can choose from a dropdown menu).
- In the case of a new user, you can specify the future user's PGP key, to send his/her new key in an encrypted e-mail.
- The system will automatically generate a message for you, but it is also possible to write a custom message if you tick the check-box, but don't worry about assigning a temporary password manually, the system will do that for you your custom message.

Action	Subject
Custom message	
Recipient	Recipient Email
A single user	admin@admin.test

Message

Submit

Action: Belirli bir e-mail türünü açıklar; ya özel bir ileti ya da şifre sıfırlama işlemi için kullanılır. Şifre sıfırlama e-postaları, otomatik olarak geçici bir şifreyi içeren bir mesajı alt kısmına ekler ve kullanıcının şifresini otomatik olarak bu yeni geçici şifreyle değiştirir.

Subject: Özel bir e-mail durumunda, buraya bir konu satırı girilebilir.

Recipient: Bu özellik, üç farklı kullanıcı grubuna ulaşmanıza olanak tanır:

1. **Tüm Kullanıcılar:** Platformdaki tüm kullanıcılara ulaşılmasını sağlar.

2. **Tek Bir Kullanıcıya:** Belirli bir kullanıcıya özel bir mesaj gönderilmesine olanak tanır. Tüm kullanıcıların e-mail adreslerinin bulunduğu ikinci bir açılır liste oluşturarak gerçekleştirilir.
3. **Potansiyel Gelecekteki Kullanıcılara:** Gelecekteki kullanıcıların hedef alınmasını sağlar. e-mail adresi için bir metin alanı ve bir GnuPG (PGP) genel anahtarı için bir metin alanı sağlayarak gerçekleştirilir. Bu şekilde henüz platforma katılmamış kişilere de ulaşabilirsiniz.

Message: Şifre sıfırlamaları ve hoş geldin mesajları için kullanılabilir. Kendi mesajınızı yazabilirsiniz (geçici bir anahtar ve imza ile birlikte eklenecektir) veya sistem tarafından otomatik olarak bir tane oluşturmaya izin verebilirsiniz.

Not: Sisteme yeni bir kullanıcı eklerken veya bir kullanıcının şifresini manuel olarak sıfırlamak isterken sadece "Send credentials automatically" ayarı kullanılır.

Uyarı: GnuPG (PGP) örneği anahtarı, yalnızca MISP örneği tarafından kullanılan ve yalnızca bildirimleri imzalamak için kullanılan GnuPG (PGP) anahtarıdır. MISP örneğinde kullanılan GnuPG (PGP) anahtarı başka hiçbir yerde kullanılmamalı ve değerli olmamalıdır.

- **Organisations:** Her kullanıcı bir kuruluşa aittir. Yöneticiler bu organizasyonu yönetebilir.

Add Organisation:

Add Organisation

Mandatory Fields

☒ Local organisation

ℳ If the organisation should have access to this instance, make sure that the Local organisation setting is checked. If you would only like to add a known external organisation for inclusion in sharing groups, uncheck the Local organisation setting.

Organisation Identifier

Brief organisation identifier

UUID

Paste UUID or click generate

Generate UUID

Optional Fields

A brief description of the organisation

A description of the organisation that is purely informational.

Bind user accounts to domains (line separated)

Enter a (list of) domain name(s) to enforce when creating users.

Logo (48×48 PNG)

Dosya seçilmedi

Nationality

Not specified

Sector

For example "financial".

Type of organisation

Freetext description of the org.

Contact details

You can add some contact details for the organisation here, if applicable.

Submit

Local Organisation: Organizasyonun bu örneğe erişimi olması gerekiyorsa, onay kutusunu işaretlenir. Yalnızca paylaşım gruplarına dahil etmek için bilinen bir dış organizasyon eklemek isteniyorsa, işaret kaldırılır.

Organisation Identifier: Organizasyon adı girilir.

Bir resim eklemek istenirse, 'Sunucu Ayarları' menüsünü kullanılarak web sunucusuna bir dosya eklenmelidir. Resmin aynı adı taşıması gerekir.

Uuid: Evrensel olarak benzersiz tanımlayıcı anlamına gelir. UUID'ler genellikle bilgisayar sistemlerinde benzersiz kimlikler oluşturmak için kullanılır.

MISP çoklu örneği arasında organizasyon paylaşımı yapmak istiyorsanız, aynı Uuid'yi kullanabilirsiniz.

Nationality: Organizasyonun ülkesini seçmek için açılır listeden bir seçenek belirtilebilir.

Sector: Organizasyonun faaliyet gösterdiği sektör belirtilebilir (finansal, ulaşım, telekomünikasyon vb.).

Type of Organisations: Organizasyonun türü belirtilebilir.

Contact Details: Organizasyon için bazı iletişim bilgileri eklenebilir.

List Organisations: Bir sistem veya platformda bulunan organizasyonların bir listesini görüntülemek için kullanılır.

Bu menü, kullanıcıların belirli bir kategorideki veya belirli bir özellikteki organizasyonları bulmasına ve bunlarla etkileşime geçmesine olanak tanır. Örneğin, bir veri paylaşım platformunda, "List Organization" menüsü, kullanıcıların kayıtlı olan tüm organizasyonların isimlerini, ülkelerini, sektörlerini ve iletişim bilgilerini görüntülemesine olanak sağlayabilir.

Kullanıcıların istedikleri organizasyonları aramalarına, filtrelemelerine ve bu organizasyonlarla ilgili daha fazla bilgi almak veya iletişime geçmek için gerekli adımları atmalarına imkan tanır.

Local organisations, both local and remote

« previous

next »

ID	Name	UUID	Description
1	ORGNAME	30ae48c2-e039-4369-8c0b-ba55f342c106	Automatically generated admin organisation

Page 1 of 1, showing 1 records out of 1 total, starting on record 1, ending on 1

« previous

next »

Bu görünümde yerel organizasyonları (Local Organizations), uzak organizasyonları (Known remote organizations) veya her ikisini birden (All organization) filtrelemek için 3 seçenek vardır.

- **Roles:** Kullanıcılara ayrıcalıklar, rol gruplarına atayarak verilir. Rol grupları, etkinliklerle ne yapabileceklerini belirleyen dört seçenekten birini kullanır; ayrıca dört ek ayrıcalık yükseltme ayarı sağlar.

Add Roles: Yeni bir rol oluştururken, oluşturulacak rol için bir ad girilmesi, açılır menüyü ve ilgili onay kutularını kullanarak izinlerin ayarlanması gerekecektir.

Add Role

☐ Restrict to site admins

Name

Permissions

Manage and Publish Organisa ▼

Memory limit (2048M)

Maximum execution time (300s)

☐ Enforce search rate limit

☐ Site Admin

☐ Org Admin

☐ Sync Actions

☐ Audit Actions

☐ Auth key access

☐ Regex Actions

☐ Tagger

☐ Tag Editor

☐ Template Editor

☐ Sharing Group Editor

☐ Delegations Access

☐ Sighting Creator

☐ Object Template Editor

☐ Galaxy Editor

☐ Decaying Model Editor

☐ ZMQ publisher

☐ Kafka publisher

☐ Warninglist Editor

☐ View Feed Correlations

☐ Analyst Data Creator

Submit

Permissions:

Permissions

Manage and Publish Organisa ▼

Read Only

Manage Own Events

Manage Organisation Events

Manage and Publish Organisation Events

Read Only: Kullanıcının, kuruluşunun erişim sahibi olduğu "Event"lere göz atmasına izin verir, ancak veritabanında herhangi bir değişiklik yapılmasına izin vermez.

Manage Own Events: Kullanıcıların kendi "Event"lerini oluşturmaya, değiştirmesine veya silmesine olanak tanır, ancak bunları yayınlamazlar.

Manage Organisation Events: Kullanıcıların, organizasyonlarının bir üyesi tarafından oluşturulan "Event"leri oluşturmaya veya değiştirmesine ve silmesine olanak tanır.

Manage and Publish Organisation Events: Kullanıcılara yukarıdakilerin tümünü yapma ve kuruluşlarının etkinliklerini yayınlama hakkı verir.

List Roles: Bir sistem veya platformda tanımlanmış olan rollerin bir listesini görüntülemek için kullanılır. Bu özellik, sistem yöneticilerinin hangi kullanıcıların hangi rollerle ilişkilendirildiğini kolayca görmelerini sağlar.

Roles

Instance specific permission roles.

« previous next »

+ Add role

Enter value to search

				Permissions																						
ID	Default	Name	Permission	Site Admin	Org Admin	Sync Actions	Audit Actions	Auth key access	Regex Actions	Tagger	Tag Editor	Template Editor	Sharing Group Editor	Delegations Access	Sighting Creator	Object Template Editor	Galaxy Editor	Decaying Model Editor	ZMQ publisher	Kafka publisher	Warninglist Editor	View Feed Correlations	Analyst Data Creator	Memory Limit	Max execution time	Searches / 15 mins
1	<input type="checkbox"/>	admin	Manage and Publish Organisation Events	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	2048M	300 s	Unlimited	
2	<input type="checkbox"/>	Org Admin	Manage and Publish Organisation Events	✗	✓	✗	✓	✓	✗	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✗	✓	✓	2048M	300 s	Unlimited	
3	<input checked="" type="checkbox"/>	User	Manage Organisation Events	✗	✗	✗	✓	✓	✗	✓	✗	✗	✗	✓	✗	✗	✓	✗	✗	✗	✓	✓	2048M	300 s	Unlimited	
4	<input type="checkbox"/>	Publisher	Manage and Publish Organisation Events	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✓	✗	✗	✓	✓	✓	✗	✓	✓	2048M	300 s	Unlimited	
5	<input type="checkbox"/>	Sync user	Manage and Publish Organisation Events	✗	✗	✓	✓	✓	✗	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✗	✓	✓	2048M	300 s	Unlimited	
6	<input type="checkbox"/>	Read Only	Read Only	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	2048M	300 s	Unlimited	

- **Blocklists and block rules:** Belirli etkinlik veya organizasyonların sisteme eklenmesini engellemek mümkündür. Yöneticiler engellenen öğeler listesine ekleyebilir, düzenleyebilir veya silebilir.

Event Blocklist: Bir etkinliğin örneğe eklenmesini engeller. Var olan bir "Event"i bloke etmek, "Event"in kaldırılmasına neden olmaz. Event hala düzenlenebilir durumda olacaktır.

Event bloke etme işlevselliği varsayılan olarak etkindir. Event bloke etme etkinleştirildiğinde, silinen eventler otomatik olarak "event Blocklist"ine eklenir. Event bloke etme işlevselliğini

etkinleştirme/devre dışı bırakma işlemi, MISP ayarlar görünümü kullanılarak yapılabilir.

Event Block Rules: "Event"lerin eklenmesini veya senkronize edilmesini engellemek için basit bir etiket filtresi eklenmesine olanak tanır.

Revision #6

Created 8 April 2024 23:41:21 by İlayda Durlanık

Updated 9 April 2024 22:09:46 by İlayda Durlanık