Özel Sorular

MISP Şifreli Bildirim E-postalarını Nasıl Yapılandırabilirim?

MISP'te şifreli bildirim e-postalarını yapılandırmak için 'MISP.extished_alert_subject' ayarını kullanabilirsiniz. Bu ayar, genişletilmiş bir event başlığı kullanmanızı sağlar.

Ancak, dikkat edilmesi gereken önemli bir nokta var: şifreleme kullanıyorsanız, event başlığı şifrelenmez. Bu nedenle, hassas bilgilerin sızdırılabileceğini unutmamanız önemlidir.

Aşağıda, seçeneğin devre dışıyken ve etkinleştirildiğinde iki farklı event türünün nasıl göründüğüne dair bir örnek bulunmaktadır:

Örnek Event Başlıkları:

- Event 7 - Low - TLP Amber
- Event 8 - OSINT - Dissecting XXX... - Low - TLP Amber

Workers'ları Nasıl Yeniden Başlatabilirim?

Workers'lar web arayüzü üzerinden yeniden başlatılabilir:

Yönetim -> Sunucu Ayarları -> Workers -> Tümünü Yeniden Başlat

Ayrıca aşağıdaki manuel işlemi de izleyebilirsiniz.

Ubuntu / Debian tabanlı sistemlerdeyseniz:

```
sudo su -l www-data -s /bin/bash -c "bash /var/www/MISP/app/Console/worker/start.sh"
```

RHEL / Fedora tabanlı sistemlerdeyseniz:

```
su -s /bin/bash apache -c 'bash /var/www/MISP/app/Console/worker/start.sh'
```

HTTP'i HTTPS'e Yönlendirme Nasıl Yapılır?

```
<VirtualHost *:80>
    ServerAdmin misp@misp.misp
    ServerName misp.misp.misp
    ServerAlias misp-int.misp.misp

    Redirect permanent / https://misp.misp.misp

    LogLevel warn
    ErrorLog /var/log/apache2/misp.local_error.log
    CustomLog /var/log/apache2/misp.local_access.log combined
    ServerSignature Off
</VirtualHost>

<VirtualHost *:443>
    ServerAdmin misp@misp.misp
    ServerName misp.misp.misp
    ServerAlias misp-int.misp.misp

    DocumentRoot /var/www/MISP/app/webroot
    <Directory /var/www/MISP/app/webroot>
        Options -Indexes
        AllowOverride all
        Order allow,deny
        allow from all
    </Directory>

    SSLEngine On
    SSLCertificateFile /etc/ssl/misp.misp.misp/misp.crt
    SSLCertificateKeyFile /etc/ssl/misp.misp.misp/misp.key
    SSLCertificateChainFile /etc/ssl/misp.misp.misp/mispCA.crt

    LogLevel warn
    ErrorLog /var/log/apache2/misp.local_error.log
    CustomLog /var/log/apache2/misp.local_access.log combined
    ServerSignature Off
</VirtualHost>
```

Yeni Kurulumuma Erişmeye Çalıştığımda, localhost:8443'e Yönlendiriliyorum ve Hata Alıyorum

Varsayılan olarak, MISP yerel bir örnek üzerinde çalışır ve kurulum sırasında yerel erişim için yapılandırılır. Bu, başka bir yerde kullanıma sunmadan önce güvenlik ve özelleştirmeleri yapılandırmanıza olanak tanır. MISP örneğine uzaktan erişim sağlamak istiyorsanız (başka bir sanal makine ana bilgisayarına/müşteriye dahil), MISP ana bilgisayarına bir IP atayın ve tarayıcınızı buna göre ayarlayın. Komut satırından baseurl'yi nasıl ayarlayacağınıza ilişkin bilgilere bakınız. Güncelleme tamamlandıktan sonra, ayarlanan IP/DNS adını kullanarak örneğe erişebilmelisiniz.

Varsayılan Paylaşım Seviyesini Nasıl Tanımlayabilirim?

MISP, tehdit verilerinizi paylaşmak istediğiniz kişiler grubunu tanımlamanıza olanak tanır. Varsayılan tercihinize göre ayarlamazsanız, yanlışlıkla istihbaratınızı yanlış gruba paylaşma olasılığınız yüksektir. Paylaşım seviyesini tanımlamak, yapılandırma dosyasındaki "**default_event_distribution**" ayarıyla yapılır.

Üç seviye bulunur:

0: Yalnızca kuruluşunuz (varsayılan)

1: Yalnızca bu topluluk

2: Bağlı topluluklar

3: Tüm topluluklar

Benzer bir yapılandırma ayarını attributeler için de yapabilirsiniz. "**default_attribute_distribution** " ayarı, "**default_event_distribution**" ile aynı değerlere sahiptir. Ayrıca, "Event"e ait ayarları almak için event değerine sahip olacak şekilde attribute ayarlanabilir.

Kuruluş Logosu ve/veya Alt bilgi Logosu Nasıl Eklenir?

MISP, bazı grafikler ekleyerek daha göz alıcı hale getirilebilir.

Site yöneticisi olarak,

Yönetim -> Kuruluşları Listele ve ilgili kuruluşu düzenleyin. Bu düzenleyicide logoyu güncelleyebilirsiniz.

Bunun başka yolları:

Kuruluş logonuzu, /var/www/MISP/app/webroot/img/orgs/ dizininde kuruluşunuzla aynı adı taşıyan bir resim (.png) ekleyerek ayarlayabilirsiniz.

Başka bir yöntem, MISP örneğinize Yönetici haklarıyla giriş yaparak,

Yönetim -> Sunucu Ayarları, sekmesine gidin -> Dosyaları Yönet.

Alt bilgi logosu ekleyebilirsiniz. Bir resmi /var/www/MISP/app/webroot/img/custom/ dizinine ekleyin ve ayar dosyasında (config.php) veya Yönetim -> Sunucu Ayarları... -> MISP ayarları (ara: "footer_logo") altında resmin diskteki konumuna işaret edin.

Tüm "Worker"lar Doğru Bir Şekilde Başlatılmıştır, Ancak schdlr Doğru Çalışmıyor. Bunu Nasıl Düzeltirim?

Örneği barındıran sunucunun FQDN'sinin değiştiği durumlarda meydana gelebilir. Bunun düzeltilmesinin bir yolu, redis'te depolanan geçici verileri temizlemektir. Bunun için redis'e giriş yapılabilir, örneğin redis-cli ile giriş yapılır ve flushall komutu verilir.

PDF Raporlarından Veri Nasıl Doğrudan Alınır?

PDF raporlarından veri doğrudan almak için birkaç seçenek vardır. IOC analizcisi adlı genel bir betik kullanabilir veya IOC analizcisinin çıktısını MISP olayına dönüştüren Palo Alto tarafından yayınlanan bir betik kullanabilirsiniz. Ayrıca, tüm metni seçip ücretsiz metin içe aktarma formuna yapıştırma seçeneğiniz de vardır.

Başka bir seçenek ise, metin içeri aktarım formu aracılığıyla kullanılabilecek yeni OCR içe aktarma modülüdür. OCR yazılımı tesseract'in kurulu olması gerekecektir.

2.4.50'den Sonraki Sürümlere Güncelleme Sorunları

2.4.50'den sonraki sürümlere güncelleme sırasında herhangi bir sayfayı geçememe sorunu yaşıyorsanız, muhtemelen 2.4.51'e kadar MISP'in oturumları otomatik olarak temizlemediği ve zaman zaman bir site yöneticisinin bunu temizlemesi gerektiği gerçeğinden kaynaklanır. 2.4.51'e güncelledikten sonra, MISP bir site yöneticisinin her bir sayfa yüklendiğinde tabloyu temizlemeye çalışacaktır, ancak tablo aşırı büyüdüyse bazı durumlarda bu işlemde takılabilir. Sorunu çözmek için mysql'e giriş yapın:

```
mysql -u [misp-db-user-name] -p [misp-db-name];
```

Ve aşağıdaki komutları çalıştırın:

```
DROP cake_sessions; CREATE TABLE IF NOT EXISTS cake_sessions ( id varchar(255) COLLATE utf8_bin NOT NULL DEFAULT '', data text COLLATE utf8_bin NOT NULL, expires int(11) NOT NULL, PRIMARY KEY (id), INDEX expires (expires) ) ENGINE=InnoDB DEFAULT CHARSET=utf8 COLLATE=utf8_bin;
```

Bu işlem sonrasında her şey düzgün çalışmalı ve bir site yöneticisi sayfayı her yüklediğinde oturum tablosu güncellenmelidir.

E-posta Bildirimleri Yaparken Birçok Başarısız İş Var, Ne Yapmalıyım?

Bu muhtemelen bazı kullanıcılar için şifrelemenin başarısız olduğu durumlardan kaynaklanmaktadır. Mevcut PGP anahtarlarını gözden geçirmenizi ve anahtarların süresinin dolmamış veya belki de artık desteklenmeyen (zayıf anahtarlar) olmadığından emin olmanızı kesinlikle öneririz. Anahtarlar, MISP'te aşağıdaki konumda incelenebilir:

https://<MISP URL'niz>/users/verifyGPG

MISP 2.4.65'ten MISP 2.4.66'ya Güncelleme - Kompozit Dosyası Nedeniyle Birleştiremiyorum.

MISP 2.4.66'da, Composer, indirme ve PHP yürütme yoluyla sahte bir PHP Composer sürümünün indirilme riskini önlemek için varsayılan olarak dahil edilir. Ancak, bir güncelleme sırasında (bir git çekme işlemi yoluyla) git birleştirme işlemi hala composer phar dosyasının olduğunu belirtebilir. Bu dosyayı güvenle kaldırabilir ve ardından tekrar git pull origin 2.4 komutunu çalıştırabilirsiniz.

Etkinlikleri İtmekle İlgili Sorunlarım Var

Belirli bir sunucu için 'Bağlantı testi' ne rapor veriyor? (Senkronizasyon İşlemleri -> Sunucu Listesi)

İtmek/çekmek için hazır olduğunu düşündüğünüz etkinlik var mı?

Dağıtım düzeyi çok kısıtlı olarak ayarlandı mı?

Etkinlikleri itmek istediğiniz sunucularda itmeyi etkinleştirdiniz mi?

Etkinlik itme kurallarında herhangi bir sınırlama var mı, örneğin belirli bir TLP Seviyesi etiketine veya başka bir şeye sınırlı mı?

İş günlüğünüzde ne yazıyor?

https:///jobs/index

Ayrıntılar için /var/www/MISP/app/tmp/logs ve /var/log/apache2/misp (veya ilgili apache günlüğü klasörü) dizinlerine bakın.

Çok Sayıda Kullanıcım veya API Erişimim Var, En İyi PHP Oturum İşleyicisi Nedir?

Üretim düzeyindeki MISP kurulumları için PHP oturumlarının Redis'te yapılmasını kesinlikle öneririz. Redis, zaten standart bir MISP kurulumunun bir parçası olduğundan, redis oturum işlemenin etkinleştirilmesini öneririz.

Redis oturum işleme ayarını PHP'de yapılandırmak için aşağıdaki adımları izleyin:

```
session.save_handler = redis
session.save_path = "tcp://127.0.0.1:6379
```

TAXII Desteği Var mı?

TAXII 1 uygulaması, https://github.com/MISP/MISP-Taxii-Server adresinde bulunabilir. Bu, genellikle MISP'e bağlı bir TAXII sunucusudur; STIX dosyalarını gelen kutusuna almak ve bunları MISP'e yüklemek için kullanılır. Ayrıca, yayınlandığında MISP olaylarını TAXII sunucusuna itmek için bir deneysel özellik vardır - bu, "**scripts/push_published_to_taxii.py**" içindedir. Bu özellik çalışıyor gibi görünüyor, ancak bazen MISP'e tekrarlanan olaylar yükleyebilir.

MISP Verisini Temizlemek - Tüm Veriyi Kaldırmak

MISP veri tabanınızla sıfırdan başlamak ve tüm veriyi kaldırmak istiyorsanız, tools/ klasöründe bulunan "**misp-wipe**" betiğini kullanabilirsiniz.

Kendi Kendine İmzalı Sertifikamı Sürekli Kabul Etmem Neden Oluyor?

Tarayıcınız ve işletim sisteminizde yapılmalıdır.

Sertifikayı CLI üzerinden kurmak için şu adımları izleyin:

```
sudo mkdir -m 0755 /usr/local/share/ca-certificates/MISP
sudo cp /etc/ssl/private/misp.local.crt /usr/local/share/ca-certificates/MISP
sudo chmod 0644 /usr/local/share/ca-certificates/MISP/misp.local.crt
sudo update-ca-certificates
```

Google Chrome için:

1. "Advanced Settings" -> chrome://settings/?search=Manage+certificates ziyaret edin.
2. Aşağı kaydırın: Yönetilen Sertifikalar (tıklayın) "Authorities" seçin "Import"e tıklayın .
3. crt dosyanıza göz atın ve içe aktarın.
4. Sonraki ekranda: "Bu sertifikayı web sitelerini tanımlamak için güvenin" işaretleyin.
5. Tüm bu adımları tamamladıktan sonra yeni kazanılan yaşam kalitesinin tadını çıkarın.
6. **Not:** Chrome'un bir Alternatif Konu Adı isteyebilir, sertifikanızı '-extension san' ile oluşturduğunuzdan emin olun.

Güvenilmeyen localhost bağlantılarına izin vermek için bu seçeneği etkinleştirin: chrome://flags/#allow-insecure-localhost

Firefox Tarayıcısı İçin

Firefox tarayıcısı için, aşağıdaki adımları izleyin:

1. "Ayarlar" menüsüne gidin.
2. "Gelişmiş Ayarlar" sekmesine tıklayın.
3. "Sertifikaları Yönet" seçeneğine tıklayın.
4. "Yetkililer" sekmesine gidin.
5. "İçe Aktar" düğmesine tıklayın.
6. .crt dosyanıza göz atın ve içe aktarın.
7. Sonraki ekranda "Bu sertifikayı web sitelerini tanımlamak için güvenin" seçeneğini işaretleyin.
8. Tamam'a tıklayarak işlemi tamamlayın.

Temayı Nasıl Değiştirebilirim?

MISP, bootstrap.css kullanır ve özel CSS dosyası tipik bir MISP kurulumunda /var/www/MISP/app/webroot/css/bootstrap.css dizininde bulunabilir.

Bu dosyayı kendi gereksinimlerinize göre özelleştirebilirsiniz. Ayrıca, kullanabileceğiniz veya üzerine inşa edebileceğiniz hazır boostrap temaları da mevcuttur.

Herhangi bir değişiklik yapmadan önce, kullanılan bootstrap sürümünü onaylayın:

```
head -5 /var/www/MISP/app/webroot/css/bootstrap.css
```

Bootswatch gibi sitelerde hazır temalar bulabilirsiniz.

Mevcut temayı Bootswatch'tan bulduğunuz bir tema ile değiştirmek için şu komutu çalıştırın:

```
sudo -u www-data wget https://bootswatch.com/2/readable/bootstrap.css -O
```

URL'yi ihtiyacınıza göre değiştirin.

Bazı Bootswatch temaları:

1. Theme 1
2. Theme 2
3. Theme 3
4. Theme 4
5. Theme 5

6. Theme 6

Beslemeleri tekrar tekrar yeni olaylara çeken, yüzlerce GB önemsiz korelasyon üreten ve örneği kullanılamaz hale getiren bir MISP örneğiyle nasıl başa çıkabilirim?

Adım 1: CSV/freetext kaynak_formatı beslemelerinizin tümünün "**fixed_event**" ayarını kullanıp kullanmadığınızı kontrol edin. Bunu manuel olarak yapmak yerine, aşağıdaki SQL sorgusunu çalıştırarak da yapabilirsiniz:

```
UPDATE feeds SET fixed_event = 1 WHERE source_format="csv" OR source_format="freetext";
```

Adım 2: Tüm korelasyonlarınızı temizleyin (bir sonraki adımları daha hızlı yapmanızı sağlar), bunun için iki yönteminiz vardır:

- Yönetici panonuza gidin -> sunucu ayarları -> MISP sekmesi ve "**MISP.completely_disable_correlation**" ayarını "**true**" olarak ayarlayın.
- MYSQL üzerinden "**TRUNCATE correlations**" komutunu çalıştırın.

Adım 3: Birden fazla etkinliğe çekilen tüm besleme verilerinizi temizleyin. Bunun en kolay yolu, etkin olan tüm beslemelerinizi kontrol etmek (misp kaynak biçimi beslemelerini dikkate almayın, bunlar sorunlara neden olmazlar) ve ID'lerini not etmektir. Daha sonra, tüm besleme etkinliklerinizi kaldırmak için CLI temizleme aracını kullanın:

```
/var/www/MISP/app/Console/cake Admin purgeFeedEvents [user_id] [feed_id]
```

Bu komutu, etkinleştirilmiş olan her besleme için çalıştırın, user_id'yi yönetici kullanıcınızın kimliğiyle ve feed_id'yi listenizdeki her besleme için bireysel besleme kimlikleriyle değiştirin.

Adım 4: Verilerinizi yeniden korele edin, Adım 2'de hangi yöntemi kullandığınıza bağlı olarak, iki seçeneğiniz vardır:

- Yönetici panelinize gidin -> Sunucu Ayarları... -> MISP... sekmesi ve "**MISP.completely_disable_correlation**" ayarını "**false**" olarak ayarlayın.
- Mevcut veri kümenizi /pages/display/administration'daki "**recorrelate attributes**" aracıyla yeniden korele edin.

API Aracılığıyla Silmek İstediğim Uzun Bir Olay Listem Var, Her Birini Silmek İçin Tek Tek Silme İsteği Göndermem Gerekir mi?

Hayır, silme işlemi, toplu olay silmeleri için de ID listesini kabul eder.

Sadece ID listenizi /events/delete adresine aşağıdaki formatta POST edin:

```
{
  "id": [1,3,5,7,9]
}
```

Bu listeyi kendi olaylarınızın ID'leriyle değiştirin.

Artık Giriş Yapamıyorum. Yönetici Şifresini Nasıl Sıfırlarım?

Şifreyi konsol aracılığıyla sıfırlayabilirsiniz. Issue #1160'ı göz atın.

```
/var/www/MISP/app/Console/cake Password [email] [password]
```

Komut Satırından Baseurl Nasıl Ayarlanır?

Baseurl'i konsol aracılığıyla değiştirebilirsiniz.

```
sudo -u www-data /var/www/MISP/app/Console/cake Baseurl [baseurl]
```

Baseurl'in doğru bir şekilde güncellendiğini, "config.php" dosyasını kontrol ederek onaylayabilirsiniz.

```
grep baseurl /var/www/MISP/app/Config/config.php
```

Revision #1
Created 14 April 2024 10:45:25 by İlayda Durlanık
Updated 14 April 2024 11:34:05 by İlayda Durlanık