SIRTFI

IDEM DAY 2018
Roma 7-9 Maggio 2018
Davide Vaghetti - IDEM GARR AAI
davide.vaghetti@garr.it

SIRTFI

Security Incident Response Trust Framework for Federated Identity (Sirtfi)

- Un assurance framework per la gestione e il coordinamento degli incidenti di sicurezza nel contesto dei servizi federati.
- Certifica il rispetto di determinati requisiti operativi per Identity e Service Provider.
- Stabilisce un contatto di sicurezza certo per la gestione degli incidenti.
- Indica modalita’ e finalita’ della comunicazione degli incidenti di sicurezza sia nella fase di gestione dell’incidente, sia nella fase di condivisione delle informazioni con altre entita’ non direttamente coinvolte, ma potenzialmente interessate.

SIRTFI

Quale problema risolve il Sirtfi trust framework?

- storicamente la comunita' della ricerca ha usufruito di policy di sicurezza per la protezione delle identita' e delle risorse (ad es. IGTF).
- eduGAIN permette ai ricercatori di utilizzare risorse provenienti da organizzazioni e federazioni diverse dalla propria, ma:
  - eduGAIN con piu' di 2500 IdP e 1500 SP rappresenta un enorme ampliamento della superficie di attacco.
  - mancano policy di sicurezza condivise tra federazioni e procedure di gestione degli incidenti di sicurezza.

Sirtfi aumenta il livello di fiducia delle organizzazioni federate, e quindi favorisce l'uso di identita' e risorse federate, stabilendo una base di misure di sicurezza e sopratutto procedure per la gestione degli incidenti di sicurezza.

SIRTFI: Step 1

Self Assessment sulla parte Normativa (sezione 2) del Sirtfi trust framework:

le organizzazioni che vogliono partecipare al Sirtfi trust framework asseriscono autonomamente che i seguenti requisiti sono da loro rispettati:

- Operational Security [OS]
- Incident Response [IR]
- Traceability [TR]
- Participant Responsibilities [PR]

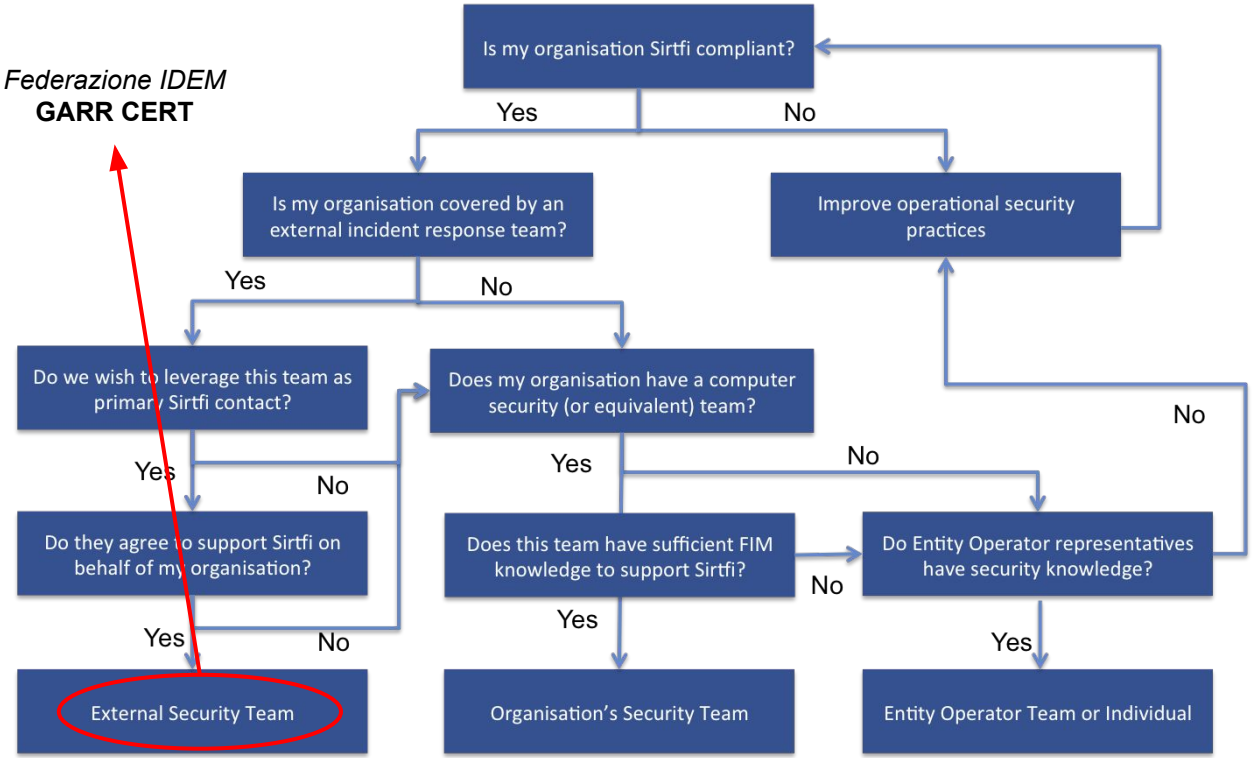
Diamo un'occhiata: https://refeds.org/wp-content/uploads/2016/01/Sirtfi-1.0.pdf

SIRTFI: Step 2

Aggiunta del contatto per la gestione degli incidenti di sicurezza (**Security Contact**)

1. Scelta del Sirtfi Contact.
2. Aggiunta del REFEDS security contact nei metadata dell'entita'.

SIRTFI: Step 2



Fonte: https://wiki.refeds.org/display/SIRTFI/Choosing+a+Sirtfi+Contact

Diagramma per la scelta e l'indicazione del security contact.

Federazione IDEM

L'implementazione di Sirtfi nella federazione IDEM prevede l'utilizzo del CERT di GARR come "External Security Team" a disposizione dei membri della federazione come contatto per la gestione degli incidenti di sicurezza.

SIRTFI: Step 2

Aggiunta del REFEDS security contact nei metadata dell'entita'

```
<EntityDescriptor entityID=$$IDEM-MEMBER-ENTITYID$$>
[...]
    <ContactPerson
       contactType="other"
       remd:contactType="http://refeds.org/metadata/contactType/security">
        <GivenName>GARR-CERT</GivenName>
        <EmailAddress>mailto:cert@garr.it</EmailAddress>
    </ContactPerson>
</EntityDescriptor>
```

SIRTFI: Step 3

Aggiunta dell'asserzione per indicare l'adesione a Sirtfi

```
<mdattr:EntityAttributes
        xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
  <saml:Attribute
        xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
        Name="urn:oasis:names:tc:SAML:attribute:assurance-certification">
      <saml:AttributeValue>https://refeds.org/sirtfi</saml:AttributeValue>
  </saml:Attribute>
</mdattr:EntityAttributes>
```

SIRTFI: chi distribuisce la fiducia?

Sirtfi non ha un registro centralizzato, ne' procedure di adesione e certificazione parimenti accentrate. Tramite l'auto valutazione rappresenta, di fatto, un framework di assurance distribuito.

In questo contesto le federazioni di identita' nazionali, pur non essendo agenti certificatori, firmando i metadata con le asserzioni Sirtfi attestano la bonta' del processo di auto valutazione.

Le strategie impiegate dalla federazioni per assolvere a questo compito non sono del tutto omogenee, ma tutte hanno la responsabilita' di impedire l'asserzione di Sirtfi alle organizzazioni che non rispettino i requisiti del framework.

SIRTFI: federazione IDEM

Dal wiki di IDEM: https://wiki.idem.garrservices.it/wiki/index.php/IDEM:Guide#SIRTFI

1. Effettuare una "autovalutazione" assicurandosi di aver risposto positivamente a tutte le affermazioni contenute nel documento https://refeds.org/wp-content/uploads/2016/01/Sirtfi-1.0.pdf (OS1-OS6, IR1-IR6, TR1-TR2, PR1-PR2)
2. IDEM consiglia di uniformare il Security Contact a Given name=GARR-CERT, email=cert@garr.it. In questo caso tutti gli scambi di informazioni relativi agli incidenti vanno esclusivamente condotti con questo contatto.
3. Compilare tramite Registry la sezione apposita ed i relativi elementi richiesti:
   - (Contacts -> Add Contact -> [Type=Security, Given name=GARR-CERT, email=cert@garr.it]
   - (Edit Provider -> Entity Attribute -> spunta su SIRTFI)
4. Attendere l'approvazione del servizio IDEM: il supporto a SIRTFI apparirà nei metadati della vostra entità a partire dal giorno successivo l'approvazione del servizio IDEM-help