WORKSHOP GARR 2026

NET MAKERS

Mettiamoci Insieme Su una Piattaforma!

Simona Venuti

GARR

Chi sono

Simona Venuti – Coordinatore di GARR-CERT

- Migliorare l'universo
- Cercare di convincere le persone a "fare sicurezza"
- [... un sacco di altre cose...]

Membro del GARR-CERT dal 2007

- Sfrenata ed incontenibile passione per la sicurezza informatica fin da piccola
- Gattara sfegatata, mi nutro di gattini su internet
- Altro: cucire e cucinare



Ringrazio il mio mentore Roberto Cecchini
per avermi fatto scoprire questo mondo 30 anni fa (la sicurezza, non il cucito o i gattini)

Elvis – It Hurts Me



https://thehackernews.com/2026/10/weekly-recap-this2shell-that2shell.html

Erik Clapton – It Hurts Me Too



I have a dream....



Mettiamoci Insieme Su una Piattaforma!

M-I-S-P

MISP – From Threat sharing to Intelligence Sharing

MISP 2.4

- Condivisione IoC
- Aiuto per reverse engineering
- Informazioni strutturate
- Informazioni normalizzate
- Possibilità di import/export



MISP 2.5

- Database PostgreSQL
- Interfaccia decisamente migliorata
- Migliori performance e (ovviamente)**AI**
- Migliore gestione ruoli
- API più granulari



In cantiere MISP 3!

GARR-CERT: da «Perché no!» a «Perché no?»

Pensiamo alle nostre organizzazioni e alle esigenze di un servizio

- Semplicità - Scalabilità
- Affidabilità – Fiducia – Pochi falsi positivi
- Soluzioni federate e collaborative
- Utilità pratica e non teorica

Scarsa affidabilità dei feed

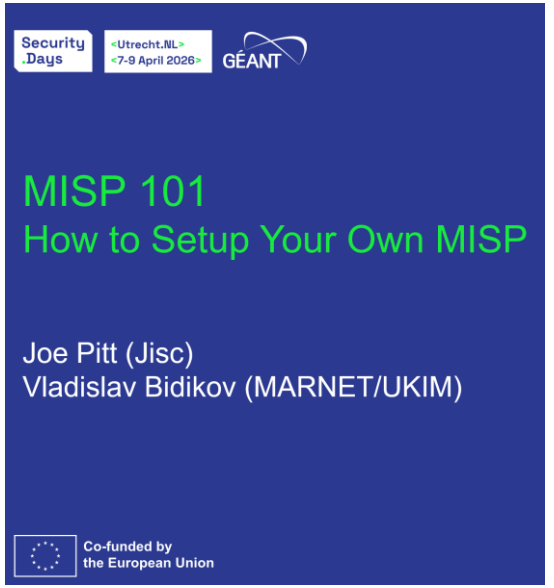
Nessun controllo – esubero dei falsi positivi

Molta confusione – difficoltà di scelta dei feed «buoni» - scarsa qualità

➔ ➔ ➔ ➔ ➔ ➔ **Poca utilità**

ADESSO E' IL MOMENTO!

Task di Geant GN5-2 confermato in GN5-3



MISP Federato: Geant – NREN – Organizzazioni

Feed controllati:

- Only enable feeds and servers you are going to action
- Share guides on integrating into your chosen vendors' systems
- Share what you can to the GÉANT MISP
- Consider creating a sharing group with your constituents

Feed integrati con quelli prodotti dalle altre NREN – CERN etc!

Abbiamo quasi tutti gli ingredienti

Procedimento della ricetta:

- **GARR-CERT** ha intenzione di *testare il MISP di Geant* per vedere se può diventare un ***servizio GARR***, per la comunità, come SCARR
- **IDEM-GARR** ha intenzione di studiare e implementare attraverso MISP un *sistema di diffusione IoC relativi ad incidenti nella Federazione* IDEM ed eduGAIN – SIRTFI2
- L'idea è di mettere su un *prototipo di test per i GARR Security Days* e **cercare volontari** della comunità per le configurazioni/prove

Tutte le informazioni saranno disponibili ai GARR Security Days

Ultimo ingrediente: VOI!

Per fare le cose al meglio abbiamo bisogno della vostra collaborazione

A seguito dei gruppi di lavoro usciti dagli scorsi Security Days
Noi contatteremo le persone che hanno già comunicato interesse
Nel gruppo «tool» lavoreremo su MISP

Che voi siate interessati al MISP
sia per IoC di sicurezza che per incidenti della Federazione IDEM/eduGAIN

SCRIVETE
securitydays@garr.it

GRAZIE!

securitydays@garr.it
cert@garr.it
idem-help@garr.it

WORKSHOP GARR 2026
NET MAKERS